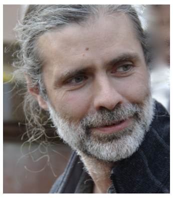
Department 1

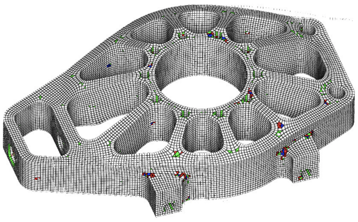
Algorithms, Computation, Geometry and Image

Department Head: Sylvain Lazard



Synopsis

Department 1 entitled *Algorithms, Computation, Image and Geometry* regroups seven teams that share scientific interests on these topics. Beside *algorithms* which is a common center of interest to all these teams (and of course to some teams of other departments as well), we share several other areas of interest. *Geometry* plays an important role in all teams. *Symbolic and algebraic computing* is of common interest to CARAMBA and GAMBLE, *image* is of interest to ADAGIO, PIXEL and TANGRAM, *combinatorics and complexity* also concerns several groups as ADAGIO, CARAMBA, and GAMBLE, *certified computing* (in a sense that sometimes requires computing with arbitrary precision numbers) is also of common interest to CARAMBA, GAMBLE, ADAGIO, and PIXEL. Finally *machine learning* concerns ABC, PIXEL and TANGRAM.



Overview of Department 1

1 Department Composition

Department leader

Sylvain Lazard

List of teams

ABC Apprentissage et Biologie Computationnelle (statistical learning theory, bioinformatics)

ADAGIO Applying Discrete Algorithms to Geometry and Imagery

CARAMBA Cryptology, arithmetic: algebraic methods for better algorithms (EPC Inria)

GAMBLE
Geometric Algorithms and Models: Beyond the Linear and Euclidean realm (EPC Inria)

MFX Matter from Graphics, 3D printing (EPC Inria)

PIXEL Digital geometry processing (EPC Inria)

TANGRAM Visual Registration with Physically Coherent Models (EPC Inria)

	2016	2017	2018	2019	2020	2021	Total
PR	3	3	5	5	5	5	5
MCF	14	15	14	13	14	15	18
DR	10	10	10	9	9	9	10
CR	11	11	13	14	14	15	16
Total (permanent positions)	38	39	42	41	42	44	49
Guest researchers				2	1		2
Post-doct. researchers	7	7	3	4	5	2	14
PhD Students	25	27	31	33	35	37	69
Master students M2	3	8	5	10	11	13	50
Master Students M1	2	2	3	3	7	11	28
L3 students	3	4	4	9	4	7	31
Engineers	4	4	5	7	9	8	13
Total (temporary positions)	44	52	51	68	72	78	207

Notes: The "Total" column does not always correspond to the sum of the individual columns, since for example a post-doctoral researcher might stay several years. The MCF and CR lines include 1 MCF LRU and 1 ISFP.

Permanents

ABC: Matthieu Geist (MCF LRU CentraleSupélec, arrived 2016, left 08/2017), Yann Guermeur[1] (DR CNRS), Fabien Lauer (MCF UL), Parisa Rastin (MCF UL, arrived 09/2019).

ADAGIO: Isabelle Debled-Rennesson (PR UL), Eric Domenjoud (CR CNRS), Philippe Even (PR UL), Bertrand Kerautret (MCF UL, left 08/2018), Phuc Ngo (MCF UL).

[1] Teams' heads are underlined.

CARAMBA: Xavier Bonnetain (CR INRIA, arrived 10/2021), Jérémie Detrey (CR INRIA, left 01/2020), Sébastien Duval (MCF UL, arrived 09/2021), Pierrick Gaudry (DR CNRS), Aurore Guillevic (CR INRIA, arrived 11/2016), Virginie Lallemand (CR CNRS, arrived 10/2018), Marine Minier (PR UL, arrived 09/2016), Cécile Pierrot (CR INRIA, arrived 01/2018), Pierre-Jean Spaenlehauer (CR INRIA), Emmanuel Thomé (DR INRIA), Marion Videau (MCF UL, on leave to Quarkslab since 01/2015, left 04/2019), Paul Zimmermann (DR INRIA).

GAMBLE: Vincent Despré (MCF UL, arrived 09/2018), Olivier Devillers (DR INRIA), Laurent Dupont (MCF UL), Xavier Goaoc (PR UL, arrived 09/2018), Sylvain Lazard (DR INRIA), Alba Marina Málaga Sabogal (MCF UL, arrived 09/2020), Guillaume Moroz (CR INRIA), Marc Pouget (CR INRIA), Monique Teillaud (DR INRIA).

MFX:Jonàs Martínez (CR INRIA, arrived 02/2017), Samuel Hornus (CR INRIA), Cédric Zanni (MCF UL, arrived 09/2016), Camille Schreck (ISFP INRIA, arrived 09/2020), Sylvain Lefebvre (DR Inria).

PIXEL: Laurent Alonso (CR INRIA), Dobrina Boltcheva (MCF UL), Étienne Corman (CR CNRS, arrived Dec 2019), Bruno Lévy (DR INRIA, left Oct 2018), Nicolas Ray (CR INRIA), Dmitry Sokolov (MCF UL).

TANGRAM: Marie-Odile Berger (DR INRIA), Erwan Kerrien (CR INRIA), Fabien Pierre (MCF UL, arrived 1/09/2017), Gilles Simon (MCF UL), Frédéric Sur (PR UL), Pierre-Frédéric Villard (MCF UL), Brigitte Wrobel-Dautcourt (MCF UL).

Others: Damien Jamet (MCF UL).

Post-doctoral fellows

ABC: Rahimeh Rouhi (2019-2020). CARAMBA: Enea Milio (2016 – 08/2017), Shashank Singh (2016 – 09/2017), Bimal Mandal (11/2018 – 02/2020). GAMBLE: Vincent Despré (10/2017 – 08/2018), Rémi Imbach (11/2014 – 10/2016), Benedikt Kolbe (11/2019 – 10/2021), Ji-won Park (09/2019 – 04/2021). MFX: Shuo Jin (2016 – 2017), Haichuan Song (2015 – 2017), Tim-Christopher Reiner (2015 – 2016) PIXEL: Erica Schwindt (postdoc, 2017–2018), Sebastian Von Hausegger (postdoc, 2019–2020). TANGRAM: Cong Yang (2016 – 2017).

Engineers

CARAMBA: Stéphane Glondu (2016 – 2021 part time, also with PESTO team). GAMBLE: Éric Biagioli (2016 – 2017), Mohamed Essia (2018). MFX: Jean Baptiste Austruy (2019-2021), Adrien Bedel (2020 – 2021), Pierre Bedell (2018 – 2021), Pierre-Alexandre Hugron (2019 – 2021), Salim Perchy (2016 – 2021), Nathaniel Seyler (2021), Noemie Vennin (2017 – 2019). TANGRAM: Pierre-Jean Petitprez (2014 – 2016), Thomas Mangin (2019 – 2020), Vincent Gaudillière (2020), Romain Boisseau (2020 – 2023).

Doctoral students

ABC: Aya El Dakdouki (Walid Joumblatt Foundation for University Studies 2015 – 2019) [15], Félix Gaschi (Cifre, 2020 – current), Mounia Hendel (USTO-MB, 2016 – 2017) [7], Antoine Mahé (FEDER-Région, 2017 – 2020) [25], Louis Massucci (FCH-Région, 2019 – current), Erinc Merdivan (Marie Curie grant, 2016 – 2019) [18], Antoine Moniot (UL, 2018 – current), Khadija Musayeva (UL, 2015 – 2019) [19], Tom Masini (UL, 2021 – current).

ADAGIO: Nicolas Aubry (CIFRE Numalliance, 2013 – 2017) [3], Hayat Nasser (Erasmus, 2013 – 2018) [13], Rémi Decelle (ANR, 2018 – current), Florian Delconte (ANR, 2020 – current), Bastien Laboureix (ENS, 2021 – current).

CARAMBA: Simon Abelard (UL-ENS, 2015 – 2018) [10], Haetham Al Aswad (Inria, 2021 – current), Hamid Boukerrou (LUE Digitrust, 2019 – current), Ana Rodriguez Cordero (UL, 2021 – current), Svyatoslav Covanov (UL-AMX Polytechnique, 2014 – 2018) [11], Gabrielle De Micheli (INRIA CORDI-S, 2018 – 2021) [29], Laurent Grémy (INRIA team's funding, 2013 – 2017) [6], Paul Huynh (FUI PACLIDO, 2017 – 2020) [23], Hugo Labrande (UL-ENS / Univ. of Calgary, 2013 – 2016) [2], Antoine Leudière-Hugounet (Inria, 2021 – current), Aude Le Gluher (UL-ENS, 2018 – 2021), [] Simon Masson (Cifre Thales, 2018 – 2020) [26], Sandra Rasoamiaramanana (Cifre Orange, 2017 – 2020) [27], Loïc Rouquette (2019 – current), Quentin Yang (INRIA team's funding, 2020 – current).

GAMBLE: Sény Diatta (Ziguinchor, Eiffel grant, 2014 – 2020) [21], Charles Duménil (UL, 2016 – current), Matthias Fresacher (UL, 2021 – current), Galatée Hemery Vaglica (UL, 2018 – abandoned in 2020), Nuwan Herath Mudiyanselage (INRIA, 2019 – current), Iordan Iordanov (UL, 2016 – 2019) [17], George Krait (INRIA 2017 – 2021), Fernand Kuibové Pefireko (Region-ANR, 2018 – stopped in 2019), Leo Valque (UL-ENS, 2020 – current).

MFX: Jean Hergel (ERC 2014 – 2017) [8], Jérémie Dumas (ERC 2014 – 2017) [5], Semyon Efremov (Region-ANR, 2018 – 2021), Jimmy Etienne (CNRS, 2018 – 2021), Thibault Tricard (UL, 2018 – 2021), Melike Aydinlilar (ANR, 2019 – current), Marco Freire (UL, 2020 – current).

PIXEL: Arnaud Botella (2012 – 2016) [1], Maxence Reberol (2015 – 2018) [14], Julien Renaudeau (2016 – 2019) [20], Justine Basselin (CIFRE RhinoTerrain, 2019 – current), François Protais (INRIA CORDI-S, 2019 – current), David Desobry (Total-INRIA, 2020 – current), Guillaume Coiffier (UL-ENS, 2020 – current), David Lopez (INRIA team's funding, 2020 – 2021) [32], Yoann Coudert-Osmont (UL, 2021 – current).

TANGRAM: Charlotte Delmas (CIFRE GE-Healthcare, 2013 – 2017) [4], Pierre Rolin (UL, 2013 – 2017) [9], Antoine Fond (UL, 2014 – 2018) [12], Jaime-Garcia Guevara (Région, 2015 – 2019) [16], Rafffaela Trivisonne (INRIA, 2015 – 2020) [28], Vincent Gaudillère (INRIA-DGA, 2016 – 2020) [22], Daryna Panicheva (UL, 2017 – 2021) [33], Igor Tominec (Uppsala, 2017 – current), Matthieu Zins (INRIA CORDI-S, 2019 – current), Youssef Assis (UL, 2020 – current), Karim Elassam (INRIA-DFKI, 2020 – current), Nariman Khaledian (INRIA CORDI-S, 2020 – current), Nathan Boulangeot (UL, 2021 – current), Radhouane Jilani (Inria, 2021 – current).

Others : Florian Liétard (UL, 2016 – 2020) [24].

	2016-2021
Phd's defended	35
Phd's abandoned	2
On-going PhD's	33
Average duration of PhD thesis (in month)	43.8

Positions of former PhD students

ABC. Aya El Dadouki: ATER at Université Grenoble Alpes. Mounia Hendel: MCF at USTO-MB. Antoine Mahé: robotics engineer at Neofarm. Erinc Merdivan: consultant at Helmotz AI. Khadija Musayeva: postdoc at the Université Côte d'Azur.

ADAGIO. Hayat Nasser: teacher and researcher in Lebanon. Nicolas Aubry: research engineer at the Numalliance company.

CARAMBA. Simon Abelard: Cryptography engineer at Thales Communications & Security. Svyatoslav Covanov: engineer, Zhor-tech, Nancy. Laurent Grémy: Cryptography engineer at Quarkslab. Paul Huynh: job search. Hugo Labrande: Teacher in classes préparatoires, later moved to Canada, currently in job search. Simon Masson: Cryptography engineer at Heliax. Sandra Rasoamiaramanana: Cryptography engineer at Ledger.

GAMBLE. Iordan Iordanov: engineer at Corpy & Co in Japan. Sény Diatta: high-school teacher in Senegal. Fernand Kuibové: unknown (PhD was stopped after one year). Galatée Hemery: high-school teacher.

MFX. Jean Hergel: intellectual property manager for GamerStream (France). Jérémie Dumas: researcher at Adobe Seattle (USA).

PIXEL. Arnaud Botella: CEO and co-founder of Geode-solutions (a company proposing solutions for advanced meshing). Maxence Reberol: postdoc in Louvain. Julien Renaudeau: engineer at Schlumberger.

TANGRAM. Charlotte Delmas: engineer at GE-Helthcare. Antoine Fond: researcher in the start-up Synthesia (London). Pierre Rolin: postdoc at CEA. Vincent Gaudillière: posdoc in Luxembourg. Raffaela Trivisonne: Translational Research Project Manager at Inserm Institute of Viral and Liver Diseases, University of Strasbourg. Jaime Garcia Guevara: software developer in image processing.

Others : Florian Liétard: high-school teacher.

Current positions of former 2016-2020 PhD's	
Industries	16
Academics	2
Post-docs	6
Teacher	4
Others	3

Departement evolutions

Team evolutions: Four new teams, GAMBLE, TANGRAM, MFX and PIXEL were created during the period in replacement of the three teams VEGAS, MAGRIT and ALICE. They were all created as joint teams of Inria, University of Lorraine and CNRS.

The GAMBLE team was created from the former team VEGAS in 2017. The TANGRAM team was created from the former team MAGRIT in 2020. The two teams PIXEL and MFX both stemmed from the ALICE team. The MFX team emerged from the ERC ShapeForge project and was created in 2018. The PIXEL team was created in 2019 as the follow up of the ALICE team after its leader, Bruno Levy, became the head of the INRIA center of Nancy - Grand Est in 2018.

Staff evolutions: 16 new permanent members joined the departement since the last evaluation and 5 left. We also had 1 promotion from MCF to PR (Fréderic Sur in 2018). Namely, we recruited:

- 2 new Professors (PR): Marine Minier (2016) and Xavier Goaoc (2018).
- 6 Assistant Professors (MCF): Cédric Zanni (2016), Fabien Pierre (2017), Vincent Despré (2018), Parisa Rastin (2019), Alba Málaga (2020), and Sébastien Duval (2021).
- 5 INRIA Research Scientist (CR and ISFP): Aurore Guillevic (2016), Jonas Martinez (2016), Cécile Pierrot (2018), Camille Schreck (2020) and Xavier Bonnetain (2021).
- 2 CNRS Research Scientist (CR): Virginie Lallemand (2018) and Étienne Corman (2019).
- 1 MCF joined the lab from CentraleSupélec Metz: Matthieu Geist (2016).

For the staff departures:

- Bruno Lévy left the department when he became the head of the INRIA center Nancy - Grand Est in 2018.
- Marion Videau (MCF) on secondment to Quarkslab since 2015 quit University of Lorraine in 2019.
- Jérémie Detrey (INRIA CR) changed his career path by going into non-scientific publishing in 2020.
- Mathieu Geist and Bertrand Kerautret left the lab when they got promoted to full Professor (PR) in Metz in 2017 and Lyon in 2018, respectively.

2 Research topics

Keywords: algorithms, computing (symbolic, algebraic and numerical), geometry (computational, discrete, probabilistic and non-linear), classification and statistical learning, image processing, 3D printing, computer vision.

Before detailing the research topics of each team, we briefly describe here the main common centers of interest of these teams, in *Algorithms and computation*, *Geometry* and *Image*.

Algorithms and computation is central to the scientific culture of the department and it covers various domains. First, research on *combinatorics and complexity analysis* (worst case or probabilistic) naturally concern several groups, in particular, ADAGIO, CARAMBA, and GAMBLE. On an algorithmic level, *optimization* problems, including convex programming, mixed-integer programming and non-convex optimization are central to the teams ABC, PIXEL, MFX, and TANGRAM, while they also are of some interest to the GAMBLE team. *Learning theory* and *classification* are also of concern to several groups; it is central to ABC's research but other groups share some interest on this topic, in particular TANGRAM and PIXEL (constrained optimization, spectral analysis). *Arithmetic and certified computing*, in the sense that algorithms are usually designed over the reals although they are implemented with integers or floating-point numbers, plays an important role in CARAMBA, GAMBLE, ADAGIO, and PIXEL. On an algorithmic level, CARAMBA and GAMBLE are also very involved in *symbolic and algebraic computing*.

Geometry: As hinted above, geometry plays an important role in all teams. Geometry refers here to a wide spectrum of theories, each of which depending both on the mathematical objects under considerations (e.g. simplicial and cellular complexes, algebraic curves and surfaces) and on the properties that are studied (e.g. intersections, topology, singularities, combinatorial structure). The forms of geometry known as *discrete, projective, digital, algebraic*, and *computational* are each of interest to several groups.

Image: Finally, the department is interested in methods that use images as input data *(image analysis, image processing, registration, modeling from images)* and methods that produce images *(image synthesis, texture generation)*. These two classes of methods share a common background of interest to half the teams of the department, namely PIXEL, TANGRAM, MFX and ADAGIO.

The application domains of the department include geometric modeling, imaging, augmented reality, numerical simulation, videogames, bioinformatics, computer algebra systems and cryptography. This spectrum of applications is quite large and it should be mentioned that most teams have fairly disjoint such application domains. This can be explained by the fact that departments were created to bring together teams with the same scientific culture rather than with an application-based view. The rest of this section summarizes the research topics of the six teams.

ABC contributes to three different fields: learning theory, statistics and biology. Its contribution to the learning theory regards pattern recognition, regression and unsupervised learning. It primarily takes the form of guaranteed risks and model selection methods. The main topic addressed in statistics is the specification and analysis of semi-parametric models, including kernel machines. In biology, the focus is on the empirical inference of structures.

ADAGIO's goal is to develop efficient algorithms on **discrete and digital structures.** In order to develop efficient algorithms, the properties of the underlying structures need to be understood thoroughly. The main objective of ADAGIO is to study these properties, which can be *geometrical*, *arithmetical* or *combinatorial* depending on the situation. More specifically, ADAGIO is interested in the fundamental aspects of *discrete and digital geometry*, which characterizes discrete objects that have a geometric (planar or spatial) interpretation. The general goal is to define a theoretical framework to translate to $\mathbb{Z}^n$ basic notions of the Euclidean geometry (such as distance, length and convexity) as faithfully as possible. The algorithms developed by ADAGIO are naturally used in imagery applications.

CARAMBA studies the algorithmic aspects of **cryptography and cryptanalysis** from the top-level mathematical background down to the optimized high-performance software implementations. CARAMBA strives in particular to develop and provide fast software dealing with various mathematical objects. These mathematical objects are of utmost importance for cryptology, as they are the background of the most widely developed cryptographic primitives, such as the RSA cryptosystem or the Diffie-Hellman key exchange. One central challenge is the assessment of the security of proposed cryptographic primitives through the study of two cornerstone problems: the integer factorization and discrete logarithm problems. Another key challenge is to produce cryptographic implementations that are both efficient and secure.

GAMBLE's objective is to contribute to the development of an effective geometric computing dedicated to non-trivial geometric objects and spaces. Our main axes of research focus on the design of data structures and algorithms in **computational geometry** and the study of their **combinatorial and probabilistic properties.** We focus in particular on **non-linear objects** and **non-Euclidean spaces**.

MFX focusses on the computational aspects of shape modeling and processing for **Additive Manufacturing (3D printing).** We address the challenges that arise in the shape modeling task and its processing for AM as a single unified process. The **modeling techniques** we develop take into account the geometric constraints imposed by the manufacturing processes (e.g., minimal thickness, overhang angles, trapped material) as well as the desired object functionality (e.g., rigidity, porosity). We also develop novel AM **deposition strategies and geometric algorithms** for the actual fabrication of the modeled objects.

PIXEL is a research team in digital geometry processing. We are interested in **parameterization techniques, meshing and reconstruction of objects from 3D point clouds.** We investigate mathematically correct, scalable and numerically stable solutions, by studying the properties of the objective function in order to develop efficient optimization algorithms. In cooperation with industrial partners, we also develop applications of our research in various fields, in particular in oil exploration, bio-chemistry and computer-aided design.

TANGRAM does research in **computer vision** and aims at addressing some specific aspects of modeling and visual registration which are still largely unsolved. Indeed, difficulties originate in the nature of the scene (poorly textured or specular environments), or in the motion undergone by the object. Physically coherent modeling, accurate registration and development of associated robust estimation techniques are the main focus of the team. Targeted transdisciplinary applications are mixed and augmented reality, computational photomechanics and minimally invasive medical interventions.

3 Main results

We shortly present some main results we obtained in our three axes of research, namely *Algorithms and Computation*, *Geometry* and *Image*.

Algorithms and Computation

NFS-like algorithms for factoring and discrete logarithm (Caramba). The number field sieve (NFS) is the best known algorithm for factoring integers used in the RSA cryptosystem, with time and space complexities that are not fully exponential but still far from polynomial.[2] Many variants of NFS have been designed to handle other problems, in particular the discrete logarithm problem (DLP) in finite fields.

Our main results concern both the fundamental algorithms used in NFS and setting new records. The progress in fundamental algorithms enables us to set new records, and in many cases targetting new records forces us to invent new algorithms.

Among the fundamental algorithms, we have made progress on the DLP over elliptic curves [55], the search and ranking of polynomials for NFS [43, 175], sieving for DLP [6], saving vectors in the block Lanczos algorithm [459], computations with sparse matrices [243], faster individual logarithms for DLP [144], elliptic bases in DLP [521], and studying asymptotic complexities [330, 224].

We have set new (and current) records for integer factorization with the factorization of RSA with 250 decimal digits [328, 437] and for discrete logarithm computations, both over prime fields and prime-power fields [57, 247, 494, 270, 328, 194].

On the cryptanalysis side, we had two major contributions: we performed a record kilobit DLP computation over a kilobit field, which had a nice impact since it showed that one could "forge" a DLP key [267]; and in the LogJam attack [101] we showed how one could defeat some still currently used 512-bit DLP keys.

Isolating singular points & Certified drawing of plane curves (Gamble). Almost all systems for drawing planar curves are subject to errors such as missing self-intersections or components. A key subproblem, which has received a lot of attention in the literature, is to isolate the singular and critical points of such curves. We reached a major achievement on this subproblem by presenting algorithms that are morally optimal in the sense that improving them would essentially require to improve bounds on several other fundamental problems (on resultants and roots isolation of univariate polynomials) that have hold for decades [46, 91]. We also developped an efficient software for providing certified drawings, which can be queried on a web server: *Isotop*. For possibly-analytic generic manifolds that often appear in applications, we also developed a new certified numerical approach based on Catastrophe Theory that allows us to handle 2D projections of smooth nD curves and 3D projections of smooth 4D surfaces that were beyond reach with previous state-of-the-art algorithms [116, 308, 381, 21, 539]. The originality of these works resides in the design of *certified and numerical* approaches.

Fast roots isolation (Gamble). We developed a breakthrough method for the two fundamental problems of evaluating a polynomial on multiple points and finding its complex roots, with a bit complexity quasi-linear in the degree. In particular, our approach solves a problem that has been open for 50 years. It was selected to the prestigious conference

[2] Complexities are expressed with the function $L_N(\alpha, \beta) = \exp(\beta(\log N)^\alpha(\log\log N)^{1-\alpha})$, with $\alpha = \frac{1}{3}$ for NFS.

FOCS [431], and the practical efficiency of this method led to a transfer contract with Waterloo Maple Inc.

Theory of margin multi-category pattern classification (ABC). One of the main open problems of this theory is the characterization of how the confidence interval of an upper bound on the probability of error should vary as a function of the three basic parameters which are the sample size m, the number C of categories and the margin parameter γ. We made two major contributions on these dependences. First, we refuted a classical conjecture and stated that, irrespective of the choice of the margin loss function, even when no hypotheses are made regarding a coupling among the outputs of the classifier, it is always possible to obtain a confidence interval depending sublinearly on C [85]. Our second contribution (preprint) deals with the use of combinatorial dimensions to measure the *capacity* of the class of margin functions [536]. We established that sharper bounds could be obtained by replacing the standard scale-sensitive combinatorial dimension, the fat-shattering dimension, with γ-Ψ-dimensions. This time, the gain is located in the dependence on γ.

Switching regression (ABC). Regression is a standard problem in machine learning for which numerous methods and analyses are available. However, most assume that the optimal target model is a smooth function. Switching regression is a setting closely related to piecewise-smooth regression, where the data generating process can switch between the different operating modes or models arbitrarily. Our main achievements are the development of global optimization algorithms for two particularly difficult non-convex problems raised by switching regression: switching linear regression and bounded-error estimation [119]. While most works focus on local optimization heuristics without global optimality guarantees or with guarantees valid only under restrictive conditions, our approach always yields a solution with a certificate of global optimality. We also obtained statistical guarantees for those models [189, 341].

Department 1

Geometry

Hexahedral meshes (Pixel). Meshes composed of hexahedra (deformed cubes) are desirable for certain numerical simulations because they can improve both performances and precision. However, they are very difficult to generate. We developed in 2010 one of the first fully automatic algorithms that generates "hex-dominant" hybrid meshes; see Figure 1.1 (left) where non-hexahedra are colored. Based on an optimization of a direction field [257] and a global parameterization steered by the direction field [72], we made a quantum leap in 2016 where we succeeded to significantly reduce the number of non-hexahedral elements as shown in Figure 1.1 (right).

Robustness of 3D meshes (Gamble). We presented a breakthrough result on the problem of removing self-intersections in 3D polygonal meshes [176]. The problem is to compute a set of interior-disjoint triangles whose geometry is close to that of the input and such that the output vertices have coordinates of fixed precision, typically *doubles*. This problem is important in academic and industrial contexts because many applications require models without self intersections. Despite its theoretical and practical relevance, there was almost no literature on the subject and we presented the first satisfactory theoretical solution.

Infill structures for additive manufacturing (MFX). We introduced the notion of procedural stochastic foams for Additive Manufacturing [69, 95, 125, 147, 196, 226]. These

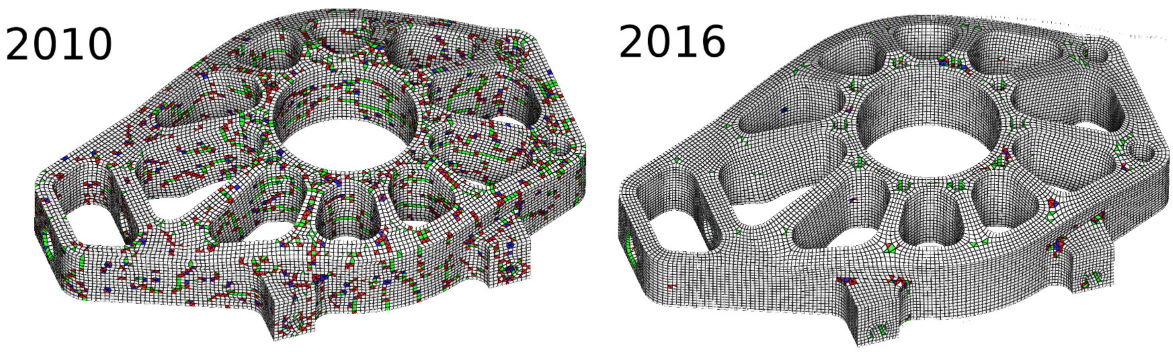


Figure 1.1: Hexahedral meshes.

methods provide an efficient way to process and fabricate complex internal micro-structures whose density and orientation can be freely scaled in space, which produces oriented orthotropic mechanical responses within the volume of the object. This yields lightweight objects whose deformations can be controlled.

Geometry Processing for additive manufacturing (MFX). We contributed several advances on the topic of geometry processing for additive manufacturing: novel techniques for the computation of offset surfaces [351, 495], slicing strategies [77, 201] and algorithms [498, 522], trajectory generation for curved deposition [73, 109, 139, 152], and variable width 2D offsetting [184].

Discrete geometric structures (Gamble). We proved that order types of various classical models of random point sets typically encounter only a vanishingly small fraction of all order types (of the given size) [339]. This reveals that these combinatorial structures are hard to sample in practice, and therefore that the geometric algorithms that *de facto* operate on them are difficult to test. We also presented solutions for two open problems from the 1970's: the algorithmic complexity of deciding the shellability of a simplicial complex [141] and a conjecture of Bondy and Hajnal on the growth function of hypergraphs [135].

Pose from ellipsoid-ellipse correspondences (Tangram). Given an ellipsoid, there is an infinity of planes and projection centers (i.e. poses) that produce the same projected ellipse. We have investigated novel ways to infer the pose from a small number of ellipse-ellipsoid correspondences.We proved that a closed form estimate of the translation can be uniquely inferred from the rotation matrix of the pose [311]. The trajectory of a camera for one correspondence was derived in [22]. This approach is however sentive to errors on the detected ellipses. With more than two correspondences, we proposed [178] a robust full 6D pose method which operates from at least two object detections and reduces the DoF to only one thanks to two simplifying yet realistic assumptions.

Image

Localization and 3D tracking (Tangram). The challenge of image-based localization is to compute pose estimates with a good accuracy regardless of the user's motion, the nature of the scene or the environmental conditions. One of our main achievement is the development of new strategies that take advantage of the impressive progress made by object recognition techniques, and especially of their good invariance to illumination and viewpoint changes. Contrary to existing techniques that require an accurate model of the scene for training, our methods work from generic algorithms such as semantic labeling or object detection. In the context of registration of buildings for urban augmented reality, we have proposed an original Expectation-Maximization framework which jointly refines registration and semantic segmentation and allows us to cope with inherently noisy semantic maps [266, 12]. Another achievement is the development of pose algorithms which use objects as landmarks and approximate 2D detected objects with ellipses and 3D objects with ellipsoids. These contributions [312, 349] build on our theoretical results on pose from ellipsoid-ellipse correspondences described above.

Biomechanical models for modeling and tracking curved and deformable objects & Applications to medical imaging (Tangram). We focussed on biomechanical models for handling shape and deformation constraints, and improving the modeling and tracking of curved and deformable objects. We addressed in particular the problems of image registration applied to minimally invasive liver surgery [287, 16, 177], image segmentation of heart mitral valve chordae in Computerized Tomography (CT) images [130, 319, 320], and 3D reconstruction of the catheter from 2D X-ray images in interventional radiology [241, 4, 282, 28, 197]. All these projects were based on strong collaborations with partners in clinical research and biomechanical simulation (CHRU Nancy, IHU Strasbourg, Mimesis Inria team and the Biorobotics lab in Harvard).

Contactless measurement for experimental solid mechanics (Tangram). We are engaged in a trandisciplinary collaboration with Institut Pascal on image-based estimation of displacement and strain fields at the surface of materials subjected to mechanical deformation. The aim is to assess and improve the metrological performance of both measurement techniques routinely used in experimental mechanics, namely digital image correlation (DIC) based on random speckle patterns, and the so-called grid method based on Fourier analysis of a regular grid. For instance, measurement resolution of DIC was characterized by taking into account subpixel interpolation in [45], a comprehensive analysis of the grid method was discussed in [60] (2016 Fylde prize for the best paper in the Strain journal), and both methods were confronted in a principled analysis [84] and enhanced through image restoration techniques [142]. A variant of grids, namely checkerboard patterns [143], turned out to give the best compromise between metrological indicators [181], see patent [572]. A synthetic speckle image generator [129] permitted us to build datasets included in the international DIC challenge.[3] This is of uttermost importance to assess the metrological performance of the available DIC variants. A patent was also filed [572].

Geometric tools for noisy digital contour analysis (Adagio). We developed tools for computing geometric characteristics on the discrete noisy curves. In particular, we proposed a new discrete structure called the *Adaptive Tangential Cover* (ACT) [254, 97], which is composed of a sequence of maximum blurred segments[4] of variable thicknesses adapted to the irregular noise present along the curve. This permits to compute decompositions of curves into circular arcs and segments as well as polygonal simplifications [357, 358, 272, 126, 318]. The experimental results demonstrate the efficiency and robustness of the approach and we applied it to hand gesture recognition [278].

[3] https://sem.org/dicchallenge

[4] I. Debled-Rennesson, F. Feschet, and J. Rouyer-Degli. "Optimal Blurred Segments Decomposition of Noisy Shapes in Linear Times". In: *Computers and Graphics* 30 (2006), pp. 30–36. URL: doi.org/10.1016/j.cag.2005.10.007.

CT scans of wood trunks (Adagio). Through a collaboration started in 2010 with INRAE, we worked on the analysis of wood quality based on Lidar data from CT scanners and photos taken in the forest or in a sawmill. One particular issue is the detection of wood knots in trunks in order to optimize their cuts [356]. We also worked on tracking logs from the forest to the sawmill, using biometric information from images of log sections. Here, the images come from low-cost sensors such as smartphone cameras and we developped several methods [376, 377] for automatically detecting different characteristics on log-end images such as pith, growth rings, heartwood and sapwood. Another nice achievment is the detection of defects on tree trunks from high resolution TLS (Terrestrial Laser Scanner) point cloud [350, 261, 457, 195] based on our work on the detection of the center line of 3D objects [251, 355].

Scientific production and quality

❶ Synthesis of publications

	2016-2021
PhD Thesis	35
H.D.R	6
Journals	189
Major conferences	143
Other conferences	52
Book chapters	12
Books (written)	4
Special issues (edited)	3
Other productions from workshops	
General audience papers	3
Participation in editorial committees	29
Evaluation of labs and research structures	5
European projects (as project manager/Member)	2/0
Other international projects (as project manager/Member)	3/2
ANR, PHRC, FUI, INCA, etc. (as project manager/Member)	7/14
Projects with Region Grand Est, etc (as project manager/Member)	2/1
PIA (as project manager/Member)	
Others (as project manager/Member)	3/5
Prizes and distinctions	19
IUF	1
Responsibilities in scientific communities (GDR etc.)	8
Organizations of Conferences (national/international)	8/17
Invitations (national/international)	17/50
Stays in foreign laboratories	24

List of top journals in which we have published

In Computer Graphics, all the proceedings of the top conferences are published as a special issue of a journal (ACM Transactions on Graphics for SIGGRAPH and SIGGRAPH ASIA; Computer Graphics Forum for

EUROGRAPHICS and ACM Symposium on Geometry Processing).

TOG – ACM Transactions on Graphics (21) [50, 69, 257, 72, 77, 81, 95, 109, 125, 127, 131, 139, 145, 147, 152, 156, 184, 196, 201, 218, 232] (15 SIGGRAPH and 6 SIGGRAPH ASIA)
JoCG – Journal of Computational Geometry (8) [42, 52, 53, 58, 82, 106, 107, 167]
DCG – Discrete and Computational Geometry (4) [48, 124, 165, 176]
Mathematics of Computation (4) [66, 136, 144, 190]
Designs, Codes and Cryptography (4) [55, 96, 111, 183]
Computer-Aided Design (7) [73, 80, 296, 212, 215, 216, 226]
Journal of Mathematical Imaging and Vision (3) [75, 122, 129]
Experimental Mechanics (3) [45, 59, 84]
Journal of the ACM (2) [138, 141]
Automatica (3) [68, 119, 203]
Journal of Number Theory (2) [187, 193]
Computer Graphics Forum (4) [93, 155, 204, 205]
IEEE Transactions on Information Theory (1) [191]
TNNLS – IEEE Transactions on Neural Networks and Learning Systems (1) [189]
Bulletin of the AMS (1) [137]
Medical Image Analysis (1) [90]
International Journal of Control (1) [134]
IEEE Transactions on Automatic Control (1) [199]

This list is not exhaustive of our publications in top-rank venues.

List of top conferences in which we have published

SIGGRAPH (15) [50, 69, 72, 77, 95, 109, 125, 131, 139, 147, 152, 156, 184, 218, 232]
SoCG – Symp. on Computational Geometry (8) [238, 242, 271, 286, 313, 333, 339, 425]
DGCI – Int. Conf. on Discrete Geometry for Computer Imagery (7) [254, 272, 277, 98, 283, 309, 321]
SIGGRAPH ASIA (6) [257, 81, 127, 145, 196, 201]
ISSAC –Int. Symp. on Symbolic and Algebraic Computation (5) [243, 245, 253, 259, 265]
ISMAR – Int. Symp. on Mixed and Augmented Reality (4) [249, 255, 266, 312]
Crypto (3) [328, 330, 332]
ESA – European Symp. on Algorithms (3) – [285, 303, 345]
ICPR – Int. Conf. on Pattern Recognition (3) [251, 261, 293]
Asiacrypt (5) [302, 305, 403, 404, 414]
FOCS – Symp. on Foundations of Computer Science (1) [431]
ECCV – European Conf. on Computer Vision (1) [299]
Eurocrypt (1) [267]
AISTATS – Int. Conf. on Artificial Intelligence and Statistics (1) [341]
IJCAI – Int. Joint Conf. on Artificial Intelligence (1) [269]
NeurIPS (formerly NIPS) – Conf. on Neural Information Processing Systems (1) [276]

This list is not exhaustive of our publications in top-rank venues.

❷ Software

We highlight here some of our principal software.

CADO-NFS is a complete implementation in C/C++ of the Number Field Sieve (NFS) algorithm for factoring integers and computing discrete logarithms in finite fields (`https://cado-nfs.gitlabpages.inria.fr/`). It consists in various programs corresponding to all the phases of the algorithm, and a general script that runs them, possibly in parallel over a network of computers. Started around 2007, CADO-NFS is released under the LGPL free software license. There are about 250,000 lines of source code (excluding some automatically generated code). The development of CADO-NFS is led by three members of our team (Caramba; P. Gaudry, E. Thomé, P. Zimmermann). Over the evaluation period, a huge effort has been put into making CADO-NFS usable for larger and larger problems, which made it possible to set new factorization and discrete logarithm records (RSA-240, DLP-240, RSA-250) [328].

Arithmetic libraries. We, Caramba, develop and maintain libraries for various arithmetic building blocks. The GNU MPFR and GNU MPC libraries are mature projects that provide multiprecision floating-point arithmetic with correct rounding up to the last bit. Since both are required to compile GCC, these libraries now enjoy a very high visibility. They are regularly maintained and enhanced. In particular in 2020, new functions have been implemented in GNU MPFR to match the reserved names for correctly-rounded functions in the N2596 draft of the C language standard.[5] We also develop the GF2X and MPFQ libraries that are more specialized. Both are used by CADO-NFS, and GF2X is used by SageMath, and can be used as an auxiliary package for the widespread software library NTL.

Belenios – Verifiable online voting system is an open-source online voting system that provides strong security guarantees such as vote confidentiality (votes are encrypted, the decryption key is distributed so that no one knows the full secret key) and verifiability (voters can check that their ballots have been received, and anyone can recount the votes). Belenios (`http://www.belenios.org/`) is developed by S. Glondu and P. Gaudry in our team (Caramba) and by V. Cortier in Dept. 2 (Pesto team).

In the early years, most of the elections were related to the academic community. Since 2019, and even more during the pandemic, users from various horizons organized elections with our platform, often in associations or for professional elections in small companies (CSE). The multilingual support attracted users from non-English speaking countries (Italy, Mexico, Brazil, Czech Republic). In 2020, more than 1400 elections were organized with our platform, corresponding to a total of more than 100,000 voters.

Isotop is a software for drawing plane algebraic curves (i.e., polyline approximations isotopic to the input curves) in a certified way, that is without missing connected components, self-intersections, etc. Our (Gamble) effort during the evaluation period was put on the developpment of a web server for online queries (`https://isotop.gamble.loria.fr/`). Only a hand-full implementations solve this fundamental problem and Isotop is the only one that can be queried online.

CGAL is the state-of-the-art international *Computational Geometry Algorithms Library* (`http://www.cgal.org`). We, Gamble, contributed during the evaluation period to 4 packages[6] on 2D and 3D periodic and hyperbolic triangulations and mesh generation [566, 567, 569].

IceSL is a 3D modeler for additive manufacturing developped by our team (MFX), which directly drives 3D printers (`https://icesl.loria.fr`). Most of our research results are available within IceSL.

Geogram-Vorpaline-Graphite are three linked software developped by our team (Pixel). Geogram (`http://alice.loria.fr/software/geogram/doc/html/index.html`) is an open-source library of data structures and geometric algorithms for reconstruction, remeshing, 3D Delaunay triangulations, Lloyd relaxation in nD, restricted Voronoi diagram in nD, numerical solvers and generation of predicates (from their formulas). Vorpaline is a proprietary extension of Geogram and Graphite (`http://alice.loria.fr/software/graphite/doc/html/`) is a graphical user interface built on top of them. We focussed our work during the evaluation period on optimal

[5] `http://www.open-std.org/jtc1/sc22/wg14/www/docs/n2596.pdf`

[6] `https://doc.cgal.org/latest/Manual/packages.html#PkgPeriodic3Triangulation3`,
`https://doc.cgal.org/latest/Manual/packages.html#PkgMesh3`,
`https://doc.cgal.org/latest/Manual/packages.html#PkgHyperbolicTriangulation2`,
`https://doc.cgal.org/latest/Manual/packages.html#PkgHyperbolicTriangulation2`

transport and hexadral meshes. Geogram and Graphite enjoy a large visibility with, respectively 43 000 and 56 000 downloads on gforge.inria.fr since 2016.

Machine Learning on the web. MLweb (`http://mlweb.loria.fr/`) is an open source software developped by our team (ABC) in which we implement state-of-the-art machine learning algorithms for the web. It aims at bringing machine learning capabilities into web pages and web applications, while maintaining all computations on the client side [120]. It was downloaded about 6 500 times on MLOSS.org.

DGtal library is an open source library for Digital Geometry programming (`https://github.com/DGtal-team/DGtal/`). We, ADAGIo, contribute to its development and we were part of its main development team until the departure of B. Kerautret in 2018.

TheGridMethod toolbox (`http://www.thegridmethod.net/`) implements several efficient and state-of-the art algorithms to estimate displacement and strain fields from grid images deposited on the surface of a specimen submitted to mechanical testing. It was released in 2016 in collaboration with Institut Pascal (Clermond-Ferrand) and is dedicated both to researchers and practitioners of experimental mechanics community.

>V< is a fast and effective tool to detect vanishing points in uncalibrated images of urban or indoor scenes (`https://members.loria.fr/GSimon/v/`). This tool also allows automatic rectification of the vertical planes in the scene, namely generating images where these planes appear as if they were observed from a fronto-parallel view. It is the Matlab implementation of the algorithm published at ECCV 2018 [299].

Other software. The above list is non-exhaustive and we refer to the teams's full reports for details on our other software contributions: SubdivisionSolver (isolating roots of polynomial systems), Voxelize (subdivision solver for visualizing surfaces), Clenshaw (real root subdivision solver for chebyshev polynomials), Dpp (generation of determinantal point processes), Siropa (singularities in parallel mechanisms), IPOL (Image Processing On Line), PoLAR (Portable Library for Augmented Reality), NoLoDuDoCT (decomposition into cartoon and texture components), BSpeckleRender (deformed speckle rendering), and EllCV (pose computations from ellipse/oid).

Academic reputation and appeal

1 Participation in projects and External funding

The extenal funding of the department comes from 2 ERC grant (1 starting grants 2012–2017 and 1 Proofs of Concept 2018), 1 IUF junior (2014–2019), 18 ANR projects (8 of which as coordinator), and from many other different sources (1 FUI, 2 PEPS, 1 CPER, 1 Region, 1 PIC, 2 UL interdisciplinary projects, 1 PHC, 1 Inria exploratory program, 1 DGA, 1 GDR). We also have/had 14 contracts with compagnies: Docapost, Idemia, NomadicLabs, Canton of Geneva, GE Healthcare, Geometry Factory, AddUp, MapleSoft, Schlumberger, RhinoTerrain, Polygonal Design, CEA, Total, Saint Gobain (see Section 1 for details).

2 Prizes and Distinctions

Distinctions

- Simon Abelard: PhD prize of Université de Lorraine, IAEM doctoral school, in 2018 [10].
- Cécile Pierrot: PhD Prize of the DGA (Direction Générale de l'Armement), shortly after she joined the team in 2018 (url).
- Jérémie Dumas: PhD award from the GDR IG-RV in 2018
- Sylvain Lefebvre: ERC Proof of Concept grant (IceXL) in 2018.
- Xavier Goaoc: IUF junior 2014–2019.

- Pierrick Gaudry won 2,000,000 rubles of bug bounty for the discovery of weaknesses in the Moscow Internet voting system in 2019 [338]. He also obtained in 2021, with Véronique Cortier and Alexandre Debant (Pesto team, Department 2) a bug bounty of 40 000 euros by Swiss Post on their electronic voting protocol.
- Record for the factorization of RSA-240 and the computation of a 240-digit discrete logarithm in 2019 [328].
- Gabrielle De Micheli: PhD award Gilles Kahn in 2021 awarded by SiF (and sponsored by the Académie des Sciences) and the Price L'Oréal-UNESCO Young Talents France 2021 – for Women and Science, which rewards PhD students and postdoctoral researchers for their work in various area of Science.
- Emmanuel Thomé was awarded a Fulbright grant in 2021 to visit University of California San Diego for one year, and appointed as a visiting professor in San Diego for that time.

Best papers

- Aurore Guillevic: best paper award at the 2018 International Workshop on the Arithmetic of Finite Fields (WAIFI) for her paper *A New Family of Pairing-Friendly elliptic curves* [298].
- Xavier Goaoc: best paper award at the 2020 International Symposium on Computational Geometry (SoCG) for his paper *Convex Hulls of Random Order Types* [339].
- Monique Teillaud: best paper award at the 2020 European Symposium on Algorithms (ESA) for her paper *Generalizing CGAL Periodic Delaunay Triangulations* [345].
- Rémi Decelle: best paper award 2021 IAPR International Conference on Discrete Geometry and Mathematical Morphology (DGMM) for his paper *Digital Straight Segment Filter for Geometric Description* [416].
- Frédéric Sur: Fylde Best Paper in Strain Prize 2016 by the British Society for Strain Measurement (BSSM) for his paper *The grid method for in-plane displacement and strain measurement: a review and analysis* [60].
- Caramba: best paper award at the Asiacrypt conference 2021 [414] for their record computation of a discrete logarithm in a 521-bit size finite field.
- Pixel: Best paper award at the 2021 Symposium on Solid and Physical Modeling (SPM) for their work on 2D and 3D Non-Orthogonal Frame Fields [215].

Invited talks Department members were invited speakers at at least 56 international and 29 national events.

This includes the following 5 keynote presentations:

- Marie-Odile Berger at the 2017 IEEE International Symposium on Mixed and Augmented Reality (ISMAR) (url).
- Monique Teillaud at the 2020 European Workshop on Computational Geometry (EuroCG) (url). [236].
- Sylvain Lefebvre at the 2018 WCCM workshop Expanding the Frontiers of Engineering Design using Computation (url).
- Sylvain Lefebvre at the 2020 Symposium on Solid and Physical Modeling (SPM) (url).
- Bruno Levy at Eurographics 2017 (url).

3 Editorial and organizational activities

Program and Paper Committees. Department members participated to the PCs of many major conferences in our fields and in particular, SIGGRAPH, SIGGRAPH ASIA, SGP, SMI, Pacific Graphics and Euro Graphics in computer graphics, Eurocrypt and Asiacrypt in Cryptology, ISSAC in computer algebra, SoCG in computational geometry, DGCI and IWCIA in discrete geometry, and ICML in machine learning.

Editorial responsibilities. Department members are editors of many of the main journals in our fields. In particular, JoCG, CGTA, IJCGA in computational geometry, IPOL in image processing, ToSC and the *Journal of Algebra* in Cryptology and computational algebra, and *Graphical Models* and TOG in computer graphics. We also have two members in the CGAL Editorial Board.

Steering committees. We are member of the steering committees of several conferences: Computational Geometry (chair), ESA in algorithmic, Elliptic Curve Cryptography and ANTS in cryptography and number theory, and DGCI in discrete geometry.

Workshop organizations. Our department regularly organizes various conferences and workshops with, in particular, 17 international events and 7 French ones during the evaluation period.

❹ Services as expert or evaluator

Thesis and habilitation committees, Hiring committees. We participated to at least 126 PhD and Habilitation committees including 52 as external examiners (rapporteurs), from 2016 to 2020 and excluding those as advisor.

We also served in 59 hiring committees for faculty positions or INRIA CRCN positions from 2016 to 2020.

Non-local scientific responsibilities. We chair(ed) the followings commitees and panels: Association française pour la reconnaissance et l'interprétation des formes (AFRIF), its thesis prize committe, and the INRIA Mission Jeunes Chercheurs. We also serve(d) in the followings: HCERES visiting commitees of LTSI (Rennes) and CRIStAL (Lille), CNU 27, Inria evaluation committee, Conseil Scientifique and Conseil D'Administration de la Société Informatique de France (SIF), INRIA BIL, Commission Pédagogique Nationale du MENRT multimedia et Internet, Young Researcher Fellow EGFR, Conseil Scientifique du GdR IM, Comité de direction du GdR IG-RV, CA de l'AFIG, International Association for Pattern Recognition (IAPR, TC18), Comité de pilotage GT-C2 (groupe de travail Codage et Cryptographie).

Department 1

❺ Collaborations

We have a large set of collaborators with about 460 co-authors over the evaluation period. We have many long-term collaborations with French collegues (see the team's reports for details). Among our main international collaborations we cite those with

- N. Heninger from University of California, San Diego on Cryptography [267, 101, 328, 437, 533].
- Gert Vegter (Groningen) [238, 364, 365, 379] and with Jean-Marc Schlenker and Hugo Parlier (Luxembourg) [504, 518] on non-Euclidean computational geometry, through the Inria Associate Team OrbiCG[7] and the international ANR–FNR SoS project.[8]
- Daniele Panozzo (New York) [139, 201], Marc Alexa (TU Berlin) [77, 139], Charlie CL Wang and Tim Kuipers (TU Delft) [109, 139, 184] and Li-Yi Wei and Wenping Wang (Hong Kong) [50, 81, 102, 558] on 3D printing.
- Peter Hammer at the Harvard Biorobotics Lab. through the Inria CURATIVE Associate Team[9] whose aim is to produce patient-based simulation of a closing mitral valve on pathological cases [319, 320].

Finally, we mention two interesting strong inter-disciplinary collaborations we built with:

- The University Hospital of Nancy, GE Healthcare, and MIMESIS Inria team in the context of interventional radiology. Several PhDs were co-supervised with these partners [4, 16, 28]. The PhD thesis of Y. Assis is currently co-supervided by Tangram and CHRU.
- INRAE on image processing applications for the detection of tree defects and wood knots from images of wood trunks [350, 356, 65, 261, 457, 377, 195].[10] The PhD of Remi Decelle is currently co-supervided is this context.

❻ Invitations and stays outside

We refer to the teams' detailed reports for the list of 85 invited talks (56 international) given by the department members.

[7] https://members.loria.fr/Monique.Teillaud/collab/Astonishing/
[8] https://members.loria.fr/Monique.Teillaud/collab/SoS/
[9] https://team.inria.fr/curative/
[10] Jean-Romain Roussel, Frédéric Mothe, Adrien Krähenbühl, Bertrand Kerautret, Isabelle Debled-Rennesson, and Fleur Longuetaud. "Automatic knot segmentation in CT images of wet softwood logs using a tangential approach". In: *Computers and Electronics in Agriculture* 104 (June 2014), pp. 46–56. DOI: 10.1016/j.compag.2014.03.004. hal-00981419.

E. Thomé was awarded a Fullbright grant to spend a sabbatical year at University of California in SanDiego in 2021-2022. He was also invited a week at the University of Pennsylvania in October 2016. A. Guillevic spends a sabbatical year (2021-2022) at University Aarhus Universitet in Danemark. She also visited EMPA, Switzerland, 3 weeks over 2019 and 2020. P.-F. Villard spent one year and a half on sabbatical (2014-2016) in Harvard University in Cambridge (USA) working on heart valve modeling, then again 3 times 1 month from 2017 to 2019. D. Panicheva also spent two weeks there 2019. P.-F. Villard spent 3 times 1 month from 2017 to 2019 at Uppsala University (Sweden). F. Pierre spent 1 week in the university of Kaiserslautern in 2019. I. Iordanov spent one month at University of Luxembourg in 2016. V. Despré spent 3 weeks there in 2019. O. Devillers spent 1 month at Carleton University, Canada in 2017 and a week in 2019. C. Dumesnil spent 2 weeks there in 2018 and S. Lazard also 2 weeks in 2019 and M. Teillaud 1 week in 2019. M. Teillaud and I. Iordanov spent 1 month each at University of Groningen, Netherlands, in 2018 and again 2 weeks for M. Teillaud in 2019 and in 2020. X. Goaoc spent 1 week at UNAM Queretaro, in Mexico in 2019.

The following colleagues also visited our team during the evaluation period: Robert Howe (Biorobotics Lab, Cambridge, USA, one week), Peter Hammer (Harvard Medical School, Boston, MA, USA , 2 weeks), Douglas Perin (Harvard School of Engineering and Applied Sciences, two weeks), Gert Vegter (Univerity of Groningen, Netherlands, about 3 times 1 month plus 2 weeks), Matthijs Ebbens (University of Groningen, 1 week), Jean-Lou De Carufel and Prosenjit Bose (Carleton Univ., Canada, 1 week each), Martin Tancer, Vojta Kalusza and Pavel Paták (Charles University, Prague, 1 week each), Andreas Holmsen and Otfried Cheong (KAIST, South Korea, 1 week each), Zuzanna Patáková (IST Austria, Vienna, 1 week) also visited the team during the evaluation period.

Involvement with social, economic and cultural environment

	2016-2020
Software	35
APP (Software)	15
Patents (Brevet)	3
Contracts with companies	12
Cifre	7
Contracts, Consortium	10
Start-up	1
Expertizes	12
Radio broadcasts, TV, Newspapers	5
Scientific mediation : articles, interviews, videos, etc.	15

1 Relations with companies and economic players

We had 7 Cifre grants over the period: S. Rasoamiaramanana (Caramba, 2017–2020) with Orange Gardens at Châtillon-Montrouge (url) [27]; S. Masson (Caramba, 2018–2020) with Thales Communication & Security, Gennevilliers (url) [26]; F. Gaschi (ABC, 2020–current) with Posos (url); N. Aubry (Adagio, 2013–2018) with Numalliance (url) [3]; J. Renaudeau (Pixel, 2016–2019) with Schlumberger (url) [20]; J. Basselin (Pixel, 2019–current) with RhinoTerrain (url); C. Delmas (Tangram, 2013–2017) with GE Healthcare (url) [4].

Start-up. We have launched in 2020 the start-up Tessael with Wan-Chiu Li, former PhD of the team, as the CEO. It provides meshing solutions based on a technology that we have been developing since 2010. It yields extremely accurate 3D simulations of subsurface environments, opening up new opportunities in three sectors: geothermal energy, geological storage and the oil and gas industry.

Patents. We had three patent during the period: *Method for measuring fields of movements and of deformations with check pattern marking and spectral method processing* (Tangram) [572] relates to computational photomechanics. *Dispositif de traitement de prise de vue* (Tangram) [571] relates to image-based localization from object detections. We also have one patent pending (Caramba).

Clinical partners: Nancy Hospital, IHU Strasbourg, GE Healthcare. Activities in medical imaging are conducted in tight collaborations both with clinical (CHRU Nancy and IHU Strasbourg) and industrial partners (GE Healthcare). Their aim is to promote the use of AR and simulation in the clinical routines and in particular the planning of interventional procedures.

Cryptanalysis. Our work on integer factorization and discrete logarithm is of interest for governmental agencies and standardization bodies for tuning accurately their key size recommendations. We worked on training and consulting activities with the French Ministry of Defense in 2016–2018. Due to confidentiality clauses, we cannot say much.

E-voting. In connection with our work on the Belenios software, we have participated in five contracts (Docapost, Idemia, NomadicLabs, Canton of Geneva, Swiss Post) where we evaluated the e-voting solutions of the companies and proposed them directions for improvements.

Geometry Factory. CGAL packages developed in Gamble are commercialized by Geometry Factory. There is a permanent contract between Geometry Factory and Inria. During the period, three packages have been released: [566, 567, 569].

3D printing. We have a continued collaboration with the French metal additive manufacturing company *AddUp*. Details are confidential. We also have regular discussions with potential industrial partners regarding our technologies. Some are ongoing and all are covered by strict non-disclosure agreements.

MapleSoft. A renewable two-years licence and cooperation agreement was signed in 2018 between Waterloo Maple Inc., Canada and Inria, which involves the teams Gamble and Ouragan (Paris) and is coordinated by F. Rouillier (Ouragan). One objective is to transfer to MapleSoft our software Isotop for drawing curves. As part of this contract, we also started in 2021 the transfert of our new software HEFROOTS for the isolation of the complex roots of a univariate polynomial [431].

Meshing. Following our results on parameterizations, we participated in five contracts (Schlumberger, RhinoTerrain, Polygonal Design, CEA, Total) where we developed efficient algorithms to compute and optimize meshes to improve numerical simulations.

2 General public audience activities

Medias: Radio broadcasts, TV, Newspapers. We wrote two articles in Binaire (hosted by Le Monde) about cryptography [472, 473] (Binaire 2018, Binaire 2019). Several newspapers articles were also written about our work: Le Monde 2016, Ars Technica 2016, Le Monde 2019, Ars Technica 2019. Sylvain Lefebvre participated to the radio program ”La méthode scientifique” on France Culture in 2017 (podcast). Bruno Lévy appeared in a documentary on France 3 which talked about our project with the astrophysicists of the IAP and the Paris Observatory, and the mathematicians of MOKAPLAN (youtube).

General public activities. We gave a talk on cryptography at La Cité des Sciences, a museum dedicated to science in Paris in 2019. We participate every year to the Fête de la Science and we participated to 3 Ateliers Google during the period.

Actions aimed at young people. We organized MATh.en.JEANS ateliers in 2016, 2017 and 2018 with high-school classes. Several lectures were also given towards middle and high school students and teachers. We gave interviews (video, radio) to promote scientific studies in 2018 and led online panel discussions to help students in high-school to have a clear picture on research in computer science in 2020. We participate to the committee for the Olympiades de mathematiques. We also participated in 2018 to the Ada Lovelace Day, an international celebration of the achievements of women in science, technology, engineering and maths. Workshops were led to introduce computer science unplugged activities at APMEP (Maths teacher association) Lorraine and NSI (computer science teachers) yearly meetings.

Popularization. The research paper [328] on RSA-240, RSA-250 factorization and discrete logarithm computation was vulgarized in [437], targetting engineers (without specific knowledge in cryptography). We also wrote a general audience paper on augmented reality [470] and two on Jan van Eyck's perspective system elucidated through computer vision [474, 475].

3D printing. We promoted 3D printing to several Maker Faire: the Maker Faire Rome 2017 (url), a major event with 100K+ visitors every year. We presented our software IceSL to students, general public and 3D printing enthusiasts and received a *Maker of Merit award* for our project. We also participated in 2019 to the Maker Faire Lille, an Inria Tech Talk at Station-F in Paris (url), the OctoberMAKE of the French FabLabs network (url) and to the Biennale du design Grand Est (url). Sylvain Lefebvre also created quick tutorial videos on Youtube (channel icesl-fr), to help introduce new users to IceSL.

The involvement in training through research

	2016-2020
Course books, etc	5
E-learnings, MOOC	6
Heads of masters (mention and parcours)	4
Heads of international courses (Erasmus-mundus, etc)	

❶ Involvement of the team in training through research

We regularly supervise research internships at various level (L3, M1 and M2). In total, we have undertaken 78 such students over the period. We also participate to Master level courses as well as research schools (see below).

❷ Involvement in E-Educations

Dmitry Sokolov's series of e-courses on computer graphics (url1, url2, url3, url2) is widely known: 5M visitors and code used by Xamarin Workbooks (Microsoft) (url), Ogre3D (url), and Bullet (url).

Erwan Kerrien participated in the creation of a MOOC for teachers of the new ICN option (Informatique et Création Numérique), which is part of the Class'Code project (url) as well as its evolution to adapt to the new Digital Science and Technology (SNT) class that is included in the 1st year core curriculum in upper secondary education. He also participated to the creation of a MOOC related to digital usages and sciences (url) in MOOCFOLIO, a PIA3-funded MOOC project (url) whose objective is to help students choose their undergraduate studies after high school.

❸ Courses and research schools

Our department is involved in training of qualified personnel at different levels. We are naturally much involved in the Master specialities of computer sciences at Lorraine University and in particular in the *Apprentissage, Vision et Robotique (AVR) parcours*. We are also involved in several Engineering Schools (Mines Nancy, Telecom Nancy, ENSEM, SUPELEC Metz, Geology School). Of course, our 18 faculty staff play a critical role there but several researchers also give courses. We refer to appendices for details.

We also gave courses and lectures in several research schools: P. Gaudry gave a lecture at the Winter School "Mathematical foundations of asymmetric cryptography", in Aussois, France (2019). E. Thomé and A. Guillevic taught cryptography, cryptanalysis, and CADO-NFS tutorials, at an Autumn school at ISI New Delhi in 2017. S. Lefebvre gave a short course at the 2018 SPG Graduate School (url). We participated to the organization of the research school EJCIM2018 (url) in which B. Lévy, N. Ray and D. Sokolov gave and wrote a course on digital geometry.[11] X. Goaoc also gave a course EJCIM2020 on combinatorial convexity (url).

[11] https://ejcim2018.sciencesconf.org/data/pages/ejcim2018.pdf

4 Responsibilities

F. Lauer is the head of the computer science Master 1st year in Nancy since 2016. In the 2nd year of this Master, I. Debled-Rennesson is co-responsible of the *Apprentissage, Vision et Robotique (AVR)* track and M. Minier is in charge of the *Sécurité Informatique, Réseaux et Architectures Virtuelles orientation* sub-track. V. Despré is head of the Ingeneer diploma speciality *Systèmes d'Information et Réseaux* (SIR) at Polytech Nancy.

I. Debled-Rennesson is an elected member of the Collegium Science & technology, which which structures the UFR, faculties, engineering schools and training institutes of Lorraine University.

P. Gaudry was vice-head (2016–2020) of the Commission de mention Informatique of the École doctorale IAEM of the University of Lorraine and 3 department members were in the board (url).

S. Lazard is head of the Inria *Young researcher council* (url) and head of the hiring committee for PhD and postdoc positions at Inria Nancy Grand Est; two other department members are in the committee.

L. Dupont is the secretary of the *Commission Pédagogique Nationale Carrières Sociales / Information-Communication / Métiers du Multimédia et de l'Internet* in the Ministère de l'Enseignement Supérieur, de la Recherche et de l'Inovation (MESRI) since 2017. He is also the representant of this commission for the national working group on D.U.T/B.U.T reform held by MESRI (2020). He is co-creator and head of two Bachelor diplomas (1 until and 1 since 2020) and responsible of fablab "Charlylab" of I.U.T. Nancy-Charlemagne (since 2018).

M. Minier is assistant director of the LORIA Lab (since Sept. 2021), co-head of the German-French virtual center for cybersecurity between LORIA and CISPA (Saarbrucken, Germany) and head of the LUE impact project DigiTrust (2018-2022, 2,2 Meuro).

M.-O. Berger is the president of the Association française pour la reconnaissance et l'interprétation des formes (AFRIF).

Life of the department

Seminars

We have several types of seminars. First, we have regular meetings where team members explain an article she/he recently read or on-going work. The informal atmosphere of those is critical and since the department has about a hundred members (including non-permanents), these seminars are organized at the level of the 7 teams of the department in order to keep them small and scientifically focussed. Precisely, MFX, Gamble and Tangram organize such meetings about weekly, bi-weekly and monthly respectively, and Caramba organize them weekly with more formal monthly events. Since the beginning of the pandemic, all these events have moved online with an increased frequency and including other means of interactions (Gathertown, twitter, online chat service, etc.)

Second, we organize department seminars where we invite outside speakers. These seminars are held about monthly (url) and have been on halt since the beginning of the pandemic.

We also organize every year a day of the department in which our PhD students present their work (url) (cancelled in 2020). This is both a way to interact scientifically within the departement and it also helps the thesis committes (Comités de suivi individuel de thèse) to follow the work and help detect possible difficulties that PhD students may have.

Finally, we also co-organize a joint inter-department seminar on the topic of security (SSL). It is held roughly on a monthly-basis and organized by the teams Caramba (dept. 1), Carbone and Pesto (dept. 2), and Resist and Coast (dept. 3). This complement team seminars, with less technical talks targeting a larger audience. While the core participants are from teams working in computer security, there are often participants from other teams or even from outside the lab. This seminar is also on halt since the beginning of the pandemic.

Governance

We run our department with a council that consists of the head of the department and the heads of the teams. This council handles matters at the level of the department such as the recruitment evaluations for PhD candidates and interns on UL contracts, the department bugdet, and the needs for new faculty positions (*profils de postes*). It is also involved in the evaluation process when creating new teams within the department.

It should also be noted that the atmosphere in our department is very pleasant at all levels. We also tend to share the same scientific culture and standards, which naturally facilitates our governance and life.

Recruitments and gender parity

We started the period with 32 permanent members[12] and we recruited 16 new members and lost 5. Hence, 37% of our current permanent members (16 out of 43) were not here at the beginning of the period. This is an important evolution but it has been accomplished smoothly.

In terms of gender parity, we started the period with 7 women in 32 permanent members, that is 22%, and we now have 13 women in 43 members, that is 30%. We are very happy to have substantially improved it. However, our gender parity is sadly still at 22% among PhD students.

[12] We recruited 5 new members in 2016, which explains the value 37 in the 2016 column in the first table.

Doctoral Dissertations

[1] Arnaud Botella. “Unstructured volumetric meshing of geological models for physical phenomenon Simulations”. PhD thesis. Université de Lorraine, April 2016. tel-01435058.

[2] Hugo Labrande. “Explicit computation of the Abel-Jacobi map and its inverse”. PhD thesis. Université de Lorraine, November 2016. tel-01403849.

[3] Nicolas Aubry. “Segmentation and geometric measurements : application to metal tubular objects”. PhD thesis. Université de Lorraine, July 2017. tel-01649874.

[4] Charlotte Delmas. “3D reconstruction of curvilinear micro-devices for interventionnal neuroradiology”. PhD thesis. Université de Lorraine, November 2017. tel-01653707.

[5] Jérémie Dumas. “Controllable shape synthesis for digital fabrication”. PhD thesis. Université de Lorraine, February 2017. tel-01547313.

[6] Laurent Grémy. “Sieve algorithms for the discrete logarithm in medium characteristic finite fields”. PhD thesis. Université de Lorraine, September 2017. tel-01647623.

[7] Mounia Hendel. “Bio-inspired methods applied to real-time analysis of biomedical signals”. PhD thesis. Université Mohamed Boudiaf des Sciences et de la Technologie - Mohamed Boudiaf d’Oran, February 2017. tel-03042290.

[8] Jean Hergel. “Synthesis of fabricable shape from partial specifications”. PhD thesis. Université de Lorraine, February 2017. tel-01546383.

[9] Pierre Rolin. “Viewpoint synthesis for camera pose initialisation”. PhD thesis. Université de Lorraine, March 2017. tel-01536649.

[10] Simon Abelard. “Counting points on hyperelliptic curves in large characteristic : algorithms and complexity”. PhD thesis. Université de Lorraine, September 2018. tel-01876314.

[11] Svyatoslav Covanov. “Multiplication algorithms : bilinear complexity and fast asymptotic methods”. PhD thesis. Université de Lorraine, June 2018. tel-01825744.

[12] Antoine Fond. “Image-based localization in urban environment : application to augmented reality”. PhD thesis. Université de Lorraine, April 2018. tel-01789709.

[13] Hayat Nasser. “Tools for the analysis of noisy discrete curves”. PhD thesis. Université de Lorraine, October 2018. tel-01947024.

[14] Maxence Reberol. “Hex-dominant meshes : generation, simulation and evaluation”. PhD thesis. Université de Lorraine, March 2018. tel-01771056.

[15] Aya El Dakdouki. “Hyperbolic Support Vector Machine and Kernel design”. PhD thesis. Université de Lille 1, Sciences et Technologies ; Loria & Inria Grand Est ; LORIA - ALGO - Department of Algorithms, Computation, Image and Geometry, September 2019. tel-03087889.

[16] Jaime Garcia Guevara. “Biomechanical graph matching for hepatic intra-operative image registration”. PhD thesis. Universite de Lorraine, December 2019. tel-02408339.

[17] Iordan Iordanov. “Delaunay triangulations of a family of symmetric hyperbolic surfaces in practice”. PhD thesis. Université de Lorraine, March 2019. tel-02072155.

[18] Erinc Merdivan. “Ambient Assisted Living with Deep Learning”. PhD thesis. CentraleSupélec, December 2019. tel-02927785.

[19] Khadija Musayeva. “Generalization Performance of Margin Multi-category Classifiers”. PhD thesis. Université de Lorraine, September 2019. tel-02387124.

[20] Julien Renaudeau. “Continuous formulation of implicit structural modeling discretized with mesh reduction methods”. PhD thesis. Université de Lorraine, April 2019. tel-02331238.

[21] Seny Diatta. “Topology of real algebraic curves and projection of real analytic surfaces.” PhD thesis. Université Assane Seck de Ziguinchor (UASZ), January 2020. tel-03101708.

[22] Vincent Gaudillière. “Visual positioning in a world of objects”. PhD thesis. Université de Lorraine, June 2020. tel-02915866.

[23] Paul Huynh. “Design and Analysis of Lightweight Encryption Schemes”. PhD thesis. Université de Lorraine, November 2020. tel-03086269.

[24] Florian Lietard. “Avoidability of additive powers in combinatoric on words”. PhD thesis. Université de Lorraine, December 2020. tel-03203854.

[25] Antoine Mahé. “System identification with neural networks for model predictive control”. PhD thesis. CentraleSupélec, Université Paris-Saclay, December 2020. tel-03081633.

[26] Simon Masson. “Algorithmic of curves in the context of bilinear and post-quantum cryptography”. PhD thesis. Université de Lorraine, December 2020. tel-03052499.

[27] Sandra Rasoamiaramanana. “Design of white-box encryption schemes for mobile applications security”. PhD thesis. Université de Lorraine, June 2020. tel-02949394.

[28] Raffaella Trivisonne. “Image-guided Interactive Simulation for Endovascular Surgery”. PhD thesis. Université de Strasbourg, October 2020. tel-03021043.

[29] Gabrielle De Micheli. “Discrete Logarithm Cryptanalyses : Number Field Sieve and Lattice Tools for Side-Channel Attacks”. PhD thesis. Université de Lorraine, May 2021. tel-03335360.

[30] George Krait. “Isolating the Singularities of the Plane Projection of Generic Space Curves and Applications in Robotics”. PhD thesis. Université de Lorraine, May 2021. tel-03241794.

[31] Aude Le Gluher. “Symbolic Computation and Complexity Analyses for Number Theory and Cryptography”. PhD thesis. Université de Lorraine, December 2021. tel-03564208.

[32] David Lopez. “Voronoi diagrams and evolving surfaces”. PhD thesis. Université de Lorraine, October 2021. tel-03530955.

[33] Daryna Panicheva. “Image-based mitral valve modeling for biomechanical applications”. PhD thesis. Université de Lorraine, March 2021. tel-03213275.

Habilitation Theses

[34] Dmitry Sokolov. “Modelisation geometrique”. Habilitation à diriger des recherches. Université de Lorraine (UL), Vandoeuvre-lès-Nancy, FRA., June 2016. tel-03180395.

[35] Frédéric Sur. “Quelques contributions à l’analyse et au traitement des images numériques”. Habilitation à diriger des recherches. Université de Lorraine, November 2016. tel-01399973.

[36] Bertrand Kerautret. “Analyse d’objets discrets pour l’estimation géométrique et la détection d’échelle”. Habilitation à diriger des recherches. Université de Lorraine (Nancy), December 2017. tel-03029250.

[37] Erwan Kerrien. “Quelques contributions à l’imagerie médicale multimodale et interventionnelle”. Habilitation à diriger des recherches. Université de Lorraine, January 2018. tel-01754699.

[38] Fabien Lauer. “Optimization and statistical learning theory for piecewise smooth and switching regression”. Habilitation à diriger des recherches. Université de Lorraine, October 2019. tel-02307957.

[39] Gilles Simon. “Positionnement visuel pour la réalité augmentée en environnement plan”. Habilitation à diriger des recherches. Université de Lorraine, December 2019. tel-02403014.

[40] Jeanne Pellerin. “Mesh Generation”. Habilitation à diriger des recherches. Université de Lorraine, June 2021. tel-03249549.

Articles in International Peer-Reviewed Journal

[41] Michaël Aron, Marie-Odile Berger, Erwan Kerrien, Brigitte Wrobel-Dautcourt, Blaise Potard, and Yves Laprie. “Multimodal acquisition of articulatory data: Geometrical and temporal registration”. In: *Journal of the Acoustical Society of America* 139.2 (2016), p. 13. DOI: 10.1121/1.4940666. hal-01269578.

[42] Dominique Attali, Olivier Devillers, Marc Glisse, and Sylvain Lazard. “Recognizing Shrinkable Complexes Is NP-Complete”. In: *Journal of Computational Geometry* 7.1 (2016), pp. 430–443. DOI: 10.20382/jocg.v7i1a18. hal-01384396.

[43] Shi Bai, Cyril Bouvier, Alexander Kruppa, and Paul Zimmermann. “Better polynomials for GNFS”. In: *Mathematics of Computation* 85 (2016), p. 12. DOI: 10.1090/mcom3048. hal-01089507.

[44] Benoît Blaysat, Michel Grediac, and Frédéric Sur. “Effect of interpolation on noise propagation from images to DIC displacement maps”. In: *International Journal for Numerical Methods in Engineering* 108.3 (2016), pp. 213–232. DOI: 10.1002/nme.5212. hal-01255944.

[45] Benoît Blaysat, Michel Grediac, and Frédéric Sur. “On the propagation of camera sensor noise to displacement maps obtained by DIC - an experimental study”. In: *Experimental Mechanics* 56.6 (2016), pp. 919–944. DOI: 10.1007/s11340-016-0130-9. hal-01269655.

[46] Yacine Bouzidi, Sylvain Lazard, Guillaume Moroz, Marc Pouget, Fabrice Rouillier, and Michael Sagraloff. “Solving bivariate systems using Rational Univariate Representations”. In: *Journal of Complexity* 37 (2016), pp. 34–75. DOI: 10.1016/j.jco.2016.07.002. hal-01342211.

[47] Nicolas Broutin, Olivier Devillers, and Ross Hemsley. “Efficiently navigating a random Delaunay triangulation”. In: *Random Structures and Algorithms* 49.1 (2016), pp. 95–136. DOI: 10.1002/rsa.20630. hal-00940743.

[48] Manuel Caroli and Monique Teillaud. "Delaunay triangulations of closed Euclidean d-orbifolds". In: *Discrete and Computational Geometry* 55.4 (2016), pp. 827–853. DOI: 10.1007/s00454-016-9782-6. hal-01294409.

[49] Changbo Chen, Svyatoslav Covanov, Farnam Mansouri, Robert H. C. Moir, Marc Moreno Maza, Ning Xie, and Yuzhen Xie. "The Basic Polynomial Algebra Subprograms". In: *ACM Communications in Computer Algebra* 50.3 (November 2016), pp. 97–100. DOI: 10.1145/3015306.3015312. hal-01404718.

[50] Weikai Chen, Xiaolong Xia, Shiqing Xin, Yang XIA, Sylvain Lefebvre, and Wenping Wang. "Synthesis of Filigrees for Digital Fabrication". In: *ACM Transactions on Graphics*. ACM Transactions on Graphics 35.4 (July 2016). DOI: 10.1145/2897824.2925911. hal-01401520.

[51] Pauline P. Collon, Alexandre Pichat, Charlie Kergaravat, Arnaud Botella, Guillaume Caumon, Jean-Claude Ringenbach, and Jean-Paul Callot. "3D modelling from outcrop data in a salt tectonic context: Example from the Inceyol mini-basin, Sivas Basin, Turkey". In: *Interpretation* 4.3 (August 2016), SM17–SM31. DOI: 10.1190/INT-2015-0178.1. hal-01342928.

[52] Olivier Devillers, Marc Glisse, Xavier Goaoc, and Rémy Thomasse. "Smoothed complexity of convex hulls by witnesses and collectors". In: *Journal of Computational Geometry* 7.2 (2016), pp. 101–144. DOI: 10.20382/jocg.v7i2a6. hal-01285120.

[53] Olivier Devillers and Ross Hemsley. "The worst visibility walk in a random Delaunay triangulation is $O(\sqrt{n})$ ". In: *Journal of Computational Geometry* 7.1 (2016), pp. 332–359. DOI: 10.20382/jocg.v7i1a16. hal-01348831.

[54] Eric Domenjoud, Xavier Provençal, and Laurent Vuillon. "Palindromic language of thin discrete planes". In: *Theoretical Computer Science* (2016), pp. 101–108. DOI: 10.1016/j.tcs.2015.11.023. hal-01262289.

[55] Steven Galbraith and Pierrick Gaudry. "Recent progress on the elliptic curve discrete logarithm problem". In: *Designs, Codes and Cryptography* 78.1 (2016), pp. 51–72. DOI: 10.1007/s10623-015-0146-7. hal-01215623.

[56] Joris Galland, Shirine Mohamed, Sabine Revuz, Emmanuel De Maistre, Bas de Laat, Pierre-Yves Marie, Stéphane Zuily, Bruno Lévy, Véronique Regnault, and Denis Wahl. "Lupus anticoagulant-hypoprothrombinemia syndrome and catastrophic antiphospholipid syndrome in a patient with antidomain I antibodies". In: *Blood Coagulation and Fibrinolysis* 27.5 (2016), pp. 580–582. DOI: 10.1097/MBC.0000000000000545. hal-03567151.

[57] Pierrick Gaudry, Laurent Grémy, and Marion Videau. "Collecting relations for the number field sieve in $GF(p^6)$". In: *LMS Journal of Computation and Mathematics*. Special issue: Algorithmic Number Theory Symposium XII 19 (2016), pp. 332–350. DOI: 10.1112/S1461157016000164. hal-01273045.

[58] Marc Glisse, Sylvain Lazard, Julien Michel, and Marc Pouget. "Silhouette of a random polytope". In: *Journal of Computational Geometry* 7.1 (2016), p. 14. DOI: 10.20382/jocg.v7i1a5. hal-01289699.

[59] Michel Grediac, Frédéric Sur, and Benoît Blaysat. "Removing quasi-periodic noise in strain maps by filtering in the Fourier domain". In: *Experimental Techniques* 40.3 (2016), pp. 959–971. DOI: 10.1007/s40799-016-0100-2. hal-01163838.

[60] Michel Grediac, Frédéric Sur, and Benoît Blaysat. "The grid method for in-plane displacement and strain measurement: a review and analysis". In: *Strain* 52.3 (2016), pp. 205–243. DOI: 10.1111/str.12182. hal-01317145.

[61] Mounia Hendel, Abdelkader Benyettou, and Fatiha Hendel. "Hybrid self organizing map and probabilistic quadratic loss multi-class support vector machine for mental tasks classification". In: *Informatics in Medicine Unlocked* 4 (September 2016), pp. 1–9. DOI: 10.1016/j.imu.2016.09.001. hal-03033964.

[62] Franck Hétroy-Wheeler, Eric Casella, and Dobrina Boltcheva. "Segmentation of tree seedling point clouds into elementary units". In: *International Journal of Remote Sensing* 37.13 (2016), pp. 2881–2907. DOI: 10.1080/01431161.2016.1190988. hal-01285419.

[63] Rémi Imbach, Guillaume Moroz, and Marc Pouget. "A certified numerical algorithm for the topology of resultant and discriminant curves". In: *Journal of Symbolic Computation* 80, Part 2 (2016), pp. 285–306. DOI: 10.1016/j.jsc.2016.03.011. hal-01402194.

[64] Pegah Kamousi, Sylvain Lazard, Anil Maheshwari, and Stefanie Wuhrer. "Analysis of Farthest Point Sampling for Approximating Geodesics in a Graph". In: *Computational Geometry* 57 (August 2016), pp. 1–7. DOI: 10.1016/j.comgeo.2016.05.005. hal-01297624.

[65] Adrien Krähenbühl, Jean-Romain Roussel, Bertrand Kerautret, Isabelle Debled-Rennesson, Frédéric Mothe, and Fleur Longuetaud. "Un algorithme robuste de segmentation des nœuds du bois sur des images obtenues par tomographie x". In: *Revue forestière française* 2 (December 2016). DOI: 10.4267/2042/61869. hal-02987202.

[66] Hugo Labrande. "Computing Jacobi's θ in quasi-linear time". In: *Mathematics of Computation* (November 2016). arXiv: 1511.04248. DOI: 10.1090/mcom/3245. hal-01227699.

[67] Hugo Labrande and Emmanuel Thomé. "Computing theta functions in quasi-linear time in genus 2 and above". In: *LMS Journal of Computation and Mathematics*. Special issue: Algorithmic Number Theory Symposium XII 19.A (August 2016), pp. 163–177. DOI: 10.1112/S1461157016000309. hal-01277169.

[68] Fabien Lauer. "On the complexity of switching linear regression". In: *Automatica* 74 (2016). arXiv: 1510.06920, pp. 80–83. DOI: 10.1016/j.automatica.2016.07.027. hal-01219794.

[69] Jonàs Martínez, Jérémie Dumas, and Sylvain Lefebvre. "Procedural Voronoi Foams for Additive Manufacturing". In: *ACM Transactions on Graphics* 35 (2016), pp. 1–12. DOI: 10.1145/2897824.2925922. hal-01393741.

[70] Guillaume Moroz and Boris Aronov. "Computing the Distance between Piecewise-Linear Bivariate Functions". In: *ACM Transactions on Algorithms* 12.1 (February 2016), 3:1–3:13. DOI: 10.1145/2847257. hal-01112394.

[71] Éric Schost and Pierre-Jean Spaenlehauer. "A Quadratically Convergent Algorithm for Structured Low-Rank Approximation". In: *Foundations of Computational Mathematics* 16.2 (2016). arXiv: 1312.7279, pp. 457–492. DOI: 10.1007/s10208-015-9256-x. hal-00953684.

[72] Dmitry Sokolov, Nicolas Ray, Lionel Untereiner, and Bruno Lévy. "Hexahedral-Dominant Meshing". In: *ACM Transactions on Graphics* 35.5 (2016), pp. 1–23. DOI: 10.1145/2930662. hal-01397846.

[73] Hai-Chuan Song, Nicolas Ray, Dmitry Sokolov, and Sylvain Lefebvre. "Anti-aliasing for fused filament deposition". In: *Computer-Aided Design* 89 (September 2016). arXiv: 1609.03032 - 14 pages, 22 figures, pp. 25–34. DOI: 10.1016/j.cad.2017.04.001. hal-01400686.

[74] Frédéric Sur, Benoît Blaysat, and Michel Grediac. "Determining displacement and strain maps immune from aliasing effect with the grid method". In: *Optics and Lasers in Engineering* 86 (2016), pp. 317–328. DOI: 10.1016/j.optlaseng.2016.06.010. hal-01352868.

[75] Frédéric Sur and Michel Grediac. "Influence of the analysis window on the metrological performance of the grid method". In: *Journal of Mathematical Imaging and Vision* 56.3 (2016), pp. 472–498. DOI: 10.1007/s10851-016-0650-z. hal-01298523.

[76] Franck Vidal and Pierre-Frédéric Villard. "Development and Validation of Real-time Simulation of X-ray Imaging with Respiratory Motion". In: *Computerized Medical Imaging and Graphics* 49 (April 2016), p. 15. DOI: 10.1016/j.compmedimag.2015.12.002. hal-01266065.

[77] Marc Alexa, Kristian Hildebrand, and Sylvain Lefebvre. "Optimal discrete slicing". In: *ACM Transactions on Graphics* 36.1 (February 2017), pp. 1–16. DOI: 10.1145/2999536. hal-01660773.

[78] Nicolas Aubry, Bertrand Kerautret, Philippe Even, and Isabelle Debled-Rennesson. "Photometric Intensity Profiles Analysis for Thick Segment Recognition and Geometric Measures". In: *Mathematical Morphology - Theory and Applications* 2.1 (December 2017), pp. 34–54. DOI: 10.1515/mathm-2017-0003. hal-02077892.

[79] Razvan Barbulescu and Armand Lachand. "Some mathematical remarks on the polynomial selection in NFS". In: *Mathematics of Computation* 86 (2017). arXiv: 1403.0184, pp. 397–418. DOI: 10.1090/mcom/3112. hal-00954365.

[80] Dobrina Boltcheva and Bruno Levy. "Surface reconstruction by computing restricted Voronoi cells in parallel". In: *Computer-Aided Design* 90 (September 2017), pp. 123–134. DOI: 10.1016/j.cad.2017.05.011. hal-01596553.

[81] Weikai Chen, Yuexin Ma, Sylvain Lefebvre, Shiqing Xin, Jonàs Martínez, and Wenping Wang. "Fabricable Tile Decors". In: *ACM Transactions on Graphics* 36.6 (2017). DOI: 10.1145/3130800.3130817. hal-01592098.

[82] Olivier Devillers, Menelaos Karavelas, and Monique Teillaud. "Qualitative Symbolic Perturbation: Two Applications of a New Geometry-based Perturbation Framework". In: *Journal of Computational Geometry* 8.1 (2017), pp. 282–315. DOI: 10.20382/jocg.v8i1a11. hal-01586511.

[83] Jean-Philippe Échard and Pierrick Gaudry. "An harmonious encoding of instrument values by a 19th century Parisian violin dealer". In: *Cryptologia* 41.5 (2017), pp. 448–458. DOI: 10.1080/01611194.2016.1257524. hal-01393625.

[84] Michel Grédiac, Benoît Blaysat, and Frédéric Sur. "A Critical Comparison of Some Metrological Parameters Characterizing Local Digital Image Correlation and Grid Method". In: *Experimental Mechanics* 57.6 (2017), pp. 871–903. DOI: 10.1007/s11340-017-0279-x. hal-01509611.

[85] Yann Guermeur. "L p -norm Sauer-Shelah Lemma for Margin Multi-category Classifiers". In: *Journal of Computer and System Sciences* 89 (November 2017), pp. 450–473. DOI: 10.1016/j.jcss.2017.06.003. hal-01371331.

[86] Samuel Hornus. “Detecting the intersection of two convex shapes by searching on the 2-sphere”. In: *Computer-Aided Design* (2017). Special issue: Proceedings of Solid and Physical Modeling (SPM 2017). DOI: 10.1016/j.cad.2017.05.009. hal-01522903.

[87] Tamás S. ILLES, Máté Burkus, Szabolcs Somoskeoy, Fabien LAUER, François Lavaste, and Jean F. DUBOUSSET. “The horizontal plane appearances of scoliosis: what information can be obtained from top-view images?” In: *International Orthopaedics* 41.11 (2017), pp. 2303–2311. DOI: 10.1007/s00264-017-3548-5. hal-01665134.

[88] Rémi Imbach, Pascal Mathis, and Pascal Schreck. “A robust and efficient method for solving point distance problems by homotopy”. In: *Mathematical Programming* 163.1-2 (May 2017), pp. 115–144. DOI: 10.1007/s10107-016-1058-7. hal-02077912.

[89] Masahiro Ishii, Jérémie Detrey, Pierrick Gaudry, Atsuo Inomata, and Kazutoshi Fujikawa. “Fast Modular Arithmetic on the Kalray MPPA-256 Processor for an Energy-Efficient Implementation of ECM”. In: *IEEE Transactions on Computers* 66.12 (December 2017), pp. 2019–2030. DOI: 10.1109/TC.2017.2704082. hal-01299697.

[90] Erwan Kerrien, Ahmed Yureidini, Jeremie Dequidt, Christian Duriez, René Anxionnat, and Stéphane Cotin. “Blood vessel modeling for interactive simulation of interventional neuroradiology procedures”. In: *Medical Image Analysis* 35 (January 2017), pp. 685–698. DOI: 10.1016/j.media.2016.10.003. hal-01390923.

[91] Sylvain Lazard, Marc Pouget, and Fabrice Rouillier. “Bivariate triangular decompositions in the presence of asymptotes”. In: *Journal of Symbolic Computation* 82 (2017), pp. 123–133. DOI: 10.1016/j.jsc.2017.01.004. hal-01468796.

[92] Benjamin Levy, Cécile Prudent, Florian Liétard, and Renaud Evrard. “From querulous to suicidal : self-immolation in public places as a symbolic response to the feeling of injustice”. In: *Frontiers in Psychology* 8 (2017), p. 1901. DOI: 10.3389/fpsyg.2017.01901. halshs-02136925.

[93] Marco Livesu, Stefano Ellero, Jonàs Martínez, Sylvain Lefebvre, and Marco Attene. “From 3D models to 3D prints: an overview of the processing pipeline”. In: *Computer Graphics Forum* 36.2 (2017). DOI: 10.1111/cgf.13147. hal-01518469.

[94] Roman M Luchin, Ilya Y. Shirokolobov, Iakov A. Kirilenko, Andrey Nikolaevich Terekhov, Anastasia Stone, and Dmitry Sokolov. “Improving control engineering education with TRIK cybernetic system”. In: *IFAC-PapersOnLine* 50.1 (July 2017), pp. 15716–15721. DOI: 10.1016/j.ifacol.2017.08.2412. hal-01658734.

[95] Jonàs Martínez, Haichuan Song, Jérémie Dumas, and Sylvain Lefebvre. “Orthotropic k-nearest foams for additive manufacturing”. In: *ACM Transactions on Graphics* 36.4 (July 2017), 121:1–121:12. DOI: 10.1145/3072959.3073638. hal-01577859.

[96] Marine Minier. “Improving impossible-differential attacks against Rijndael-160 and Rijndael-224”. In: *Designs, Codes and Cryptography* 82.1-2 (January 2017), pp. 117–129. DOI: 10.1007/s10623-016-0206-7. hal-01593371.

[97] Phuc Ngo, Isabelle Debled-Rennesson, Bertrand Kerautret, and Hayat Nasser. “Analysis of Noisy Digital Contours with Adaptive Tangential Cover”. In: *Journal of Mathematical Imaging and Vision* 59.1 (2017), pp. 123–135. DOI: 10.1007/s10851-017-0723-7. hal-01486969.

[98] Phuc Ngo, Yukiko Kenmochi, Akihiro Sugimoto, Hugues Talbot, and Nicolas Passat. “Discrete rigid registration: A local graph-search approach”. In: *Discrete Applied Mathematics* 216.2 (2017), pp. 461–481. DOI: 10.1016/j.dam.2016.05.005. hal-01306035.

[99] Jeanne Pellerin, Arnaud Botella, Antoine Mazuyer, Benjamin Chauvin, François Bonneau, Guillaume Caumon, and Bruno Lévy. "RINGMesh: A programming library for developing mesh-based geomodeling applications". In: *Computers & Geosciences* (2017). DOI: 10.1016/j.cageo.2017.03.005. hal-01493204.

[100] Frédéric Sur, Benoît Blaysat, and Michel Grediac. "Towards Computational Photomechanics". In: *ERCIM News* 108 (January 2017), pp. 30–31. hal-01430636.

[101] David Adrian, Karthikeyan Bhargavan, Zakir Durumeric, Pierrick Gaudry, Matthew Green, J. Alex Halderman, Nadia Heninger, Drew Springall, Emmanuel Thomé, Luke Valenta, Benjamin Vandersloot, Eric Wustrow, Santiago Zanella-Béguelin, and Paul Zimmermann. "Imperfect forward secrecy: How Diffie-Hellman fails in practice". In: *Communications of the ACM* 62.1 (December 2018), pp. 106–114. DOI: 10.1145/3292035. hal-01982426.

[102] Xiaojun Bian, Li-Yi Wei, and Sylvain Lefebvre. "Tile-based Pattern Design with Topology Control". In: *Proceedings of the ACM on Computer Graphics and Interactive Techniques* 1 (2018), pp. 23–38. DOI: 10.1145/3203204. hal-01811874.

[103] Frederic Bihan, Francisco Santos, and Pierre-Jean Spaenlehauer. "A Polyhedral Method for Sparse Systems with many Positive Solutions". In: *SIAM Journal on Applied Algebra and Geometry* 2.4 (2018). arXiv: 1804.05683, pp. 620–645. DOI: 10.1137/18M1181912. hal-01877602.

[104] Enka Blanchard. "Building Trust for Sample Voting". In: *International Journal of Decision Support System Technology* 10.4 (October 2018), pp. 50–64. DOI: 10.4018/IJDSST.2018100104. hal-02556370.

[105] David Bremner, Olivier Devillers, Marc Glisse, Sylvain Lazard, Giuseppe Liotta, Tamara Mchedlidze, Guillaume Moroz, Sue Whitesides, and Stephen Wismath. "Monotone Simultaneous Paths Embeddings in $\mathbb{R}^d$". In: *Discrete Mathematics and Theoretical Computer Science* Vol. 20 no. 1.1 (January 2018), pp. 1–11. DOI: 10.23638/DMTCS-20-1-1. hal-01529154.

[106] Luca Castelli Aleardi and Olivier Devillers. "Array-based Compact Data Structures for Triangulations: Practical Solutions with Theoretical Guarantees". In: *Journal of Computational Geometry* 9.1 (2018), pp. 247–289. DOI: 10.20382/jocg.v9i1a8. hal-01846652.

[107] Luca Castelli Aleardi, Olivier Devillers, and Eric Fusy. "Canonical Ordering for Graphs on the Cylinder with Applications to Periodic Straight-line Drawings on the Flat Cylinder and Torus". In: *Journal of Computational Geometry* 9.1 (2018), pp. 391–429. DOI: 10.20382/jocg.v9i1a14. hal-01959590.

[108] Nicolas Chenavier and Olivier Devillers. "Stretch Factor in a Planar Poisson-Delaunay Triangulation with a Large Intensity". In: *Advances in Applied Probability* 50.1 (2018), pp. 35–56. DOI: 10.1017/apr.2018.3. hal-01700778.

[109] Chengkai Dai, Charlie C.L. Wang, Chenming Wu, Sylvain Lefebvre, Guoxin Fang, and Yong-Jin Liu. "Support-free volume printing by multi-axis motion". In: *ACM Transactions on Graphics* 37.4 (July 2018), pp. 1–14. DOI: 10.1145/3197517.3201342. hal-01887571.

[110] Olivier Devillers and Louis Noizet. "Walking in a Planar Poisson-Delaunay Triangulation: Shortcuts in the Voronoi Path". In: *International Journal of Computational Geometry and Applications* 28.3 (2018), pp. 255–269. DOI: 10.1142/S0218195918500061. hal-01712628.

[111] Léo Ducas and Cécile Pierrot. "Polynomial Time Bounded Distance Decoding near Minkowski's Bound in Discrete Logarithm Lattices". In: *Designs, Codes and Cryptography* (October 2018). DOI: 10.1007/s10623-018-0573-3. hal-01891713.

[112] Isabelle Dumand, Christophe Clesse, Samira Salime, Florian Liétard, Michel Decker, Joëlle Lighezzolo-Alnot, and Martine Batt. "L'âge psychosocial : un outil au service d'une réduction de la stigmatisation institutionnelle des sujets âgés porteurs de troubles psychiques". In: *Gériatrie et psychologie neuropsychiatrie du vieillissement* 16.4 (2018), pp. 439–448. DOI: 10.1684/pnv.2018.0761. hal-02004800.

[113] Jaime Garcia Guevara, Igor Peterlik, Marie-Odile Berger, and Stephane Cotin. "Biomechanics-based graph matching for augmented CT-CBCT". In: *International Journal of Computer Assisted Radiology and Surgery* 13.6 (April 2018), pp. 805–813. DOI: 10.1007/s11548-018-1755-1. hal-01761521.

[114] David Gérault, Pascal Lafourcade, Marine Minier, and Christine Solnon. "Revisiting AES Related-Key Differential Attacks with Constraint Programming". In: *Information Processing Letters* 139 (2018), pp. 24–29. DOI: 10.1016/j.ipl.2018.07.001. hal-01827727.

[115] Tamás Illés, Máté Burkus, Szabolcs Somoskeöy, Fabien Lauer, François Lavaste, and Jean Dubousset. "Axial plane dissimilarities of two identical Lenke-type 6C scoliosis cases visualized and analyzed by vertebral vectors". In: *European Spine Journal* 27.9 (2018), pp. 2120–2129. DOI: 10.1007/s00586-018-5577-1. hal-02060150.

[116] Rémi Imbach, Guillaume Moroz, and Marc Pouget. "Reliable Location with Respect to the Projection of a Smooth Space Curve". In: *Reliable Computing* 26 (2018), pp. 13–55. hal-01920444.

[117] Ranjan Jha, Damien Chablat, Luc Baron, Fabrice Rouillier, and Guillaume Moroz. "Workspace, Joint space and Singularities of a family of Delta-Like Robot". In: *Mechanism and Machine Theory* 127 (September 2018), pp. 73–95. DOI: 10.1016/j.mechmachtheory.2018.05.004. hal-01796066.

[118] Wouter Kuijper, Victor Ermolaev, and Olivier Devillers. "Celestial Walk: A Terminating, Memoryless Walk for Convex Subdivisions". In: *Journal of Computer Graphics Techniques* 7.3 (2018), pp. 29–49. hal-01867771.

[119] Fabien Lauer. "Global optimization for low-dimensional switching linear regression and bounded-error estimation". In: *Automatica* 89 (2018). arXiv: 1707.05533, pp. 73–82. DOI: 10.1016/j.automatica.2017.11.026. hal-01563788.

[120] Fabien Lauer. "MLweb: A toolkit for machine learning on the web". In: *Neurocomputing* 282 (2018), pp. 74–77. DOI: 10.1016/j.neucom.2017.11.069. hal-01646613.

[121] Fabien Lauer. "On the exact minimization of saturated loss functions for robust regression and subspace estimation". In: *Pattern Recognition Letters* 112 (2018). arXiv: 1806.05833, pp. 317–323. DOI: 10.1016/j.patrec.2018.08.004. hal-01815451.

[122] Friederike Laus, Fabien Pierre, and Gabriele Steidl. "Nonlocal Myriad Filters for Cauchy Noise Removal". In: *Journal of Mathematical Imaging and Vision* (April 2018). arXiv: 1710.03015, pp. 1–31. DOI: 10.1007/s10851-018-0816-y. hal-01814104.

[123] Bruno Lévy and Erica Schwindt. "Notions of optimal transport theory and how to implement them on a computer". In: *Computers and Graphics* (February 2018), pp. 1–22. DOI: 10.1016/j.cag.2018.01.009. hal-01717967.

[124] Pedro Machado Manhães De Castro and Olivier Devillers. "Expected Length of the Voronoi Path in a High Dimensional Poisson-Delaunay Triangulation". In: *Discrete and Computational Geometry* 60.1 (2018), pp. 200–219. DOI: 10.1007/s00454-017-9866-y. hal-01477030.

[125] Jonàs Martínez, Samuel Hornus, Haichuan Song, and Sylvain Lefebvre. "Polyhedral Voronoi diagrams for additive manufacturing". In: *ACM Transactions on Graphics*. Proceedings of SIGGRAPH 2018 37.4 (August 2018), p. 15. DOI: 10.1145/3197517.3201343. hal-01697103.

[126] Hayat Nasser, Phuc Ngo, and Isabelle Debled-Rennesson. "Dominant point detection based on discrete curve structure and applications". In: *Journal of Computer and System Sciences* 95 (2018), pp. 177–192. DOI: 10.1016/j.jcss.2017.07.007. hal-01584733.

[127] Nicolas Ray, Dmitry Sokolov, Sylvain Lefebvre, and Bruno Lévy. "Meshless Voronoi on the GPU". In: *ACM Transactions on Graphics* 37.6 (December 2018), pp. 1–12. DOI: 10.1145/3272127.3275092. hal-01927559.

[128] Igor Ryadchikov, Semyon Sechenev, Michail Drobotenko, Alexander Svidlov, Pavel Volkodav, Renat Vishnykov, Dmitry Sokolov, and Evgeny Nikulchev. "Stabilization system of a bipedal non-anthropomorphic robot AnyWalker". In: *Journal of Engineering Science and Technology Review* (August 2018). DOI: 10.25103/jestr.115.15. hal-01927623.

[129] Frédéric Sur, Benoît Blaysat, and Michel Grediac. "Rendering Deformed Speckle Images with a Boolean Model". In: *Journal of Mathematical Imaging and Vision* 60.5 (2018), pp. 634–650. DOI: 10.1007/s10851-017-0779-4. hal-01664997.

[130] Pierre-Frédéric Villard, Peter E. Hammer, Douglas P. Perrin, Pedro J. Del Nido, and Robert Howe. "Fast Image-Based Mitral Valve Simulation from Individualized Geometry". In: *The International Journal of Medical Robotics and Computer Assisted Surgery* 14.2 (2018), e1880. DOI: 10.1002/rcs.1880. hal-01643868.

[131] Zichun Zhong, Wenping Wang, Bruno Lévy, Jing Hua, and Xiaohu Guo. "Computing a high-dimensional euclidean embedding from an arbitrary smooth riemannian metric". In: *ACM Transactions on Graphics* 37.4 (August 2018), pp. 1–16. DOI: 10.1145/3197517.3201369. hal-03214192.

[132] Simon Abelard, Pierrick Gaudry, and Pierre-Jean Spaenlehauer. "Improved Complexity Bounds for Counting Points on Hyperelliptic Curves". In: *Foundations of Computational Mathematics* 19.3 (2019). arXiv: 1710.03448, pp. 591–621. DOI: 10.1007/s10208-018-9392-1. hal-01613530.

[133] Stanislav Aranovskiy, Andrei Biryuk, Evgeny V. Nikulchev, Igor Ryadchikov, and Dmitry Sokolov. "Observer Design for an Inverted Pendulum with Biased Position Sensors". In: *Izvestia Rossiiskoi Akademii Nauk.Teoriya i Systemy Upravleniya / Journal of Computer and Systems Sciences International* 58.2 (March 2019), pp. 297–304. DOI: 10.1134/S1064230719020023. hal-02282919.

[134] Stanislav Aranovskiy, Romeo Ortega, Jose Guadalupe Romero, and Dmitry Sokolov. "A Globally Exponentially Stable Speed Observer for a Class of Mechanical Systems: Experimental and Simulation Comparison with High-Gain and Sliding Mode Designs". In: *International Journal of Control* 92.7 (July 2019), pp. 1620–1633. DOI: 10.1080/00207179.2017.1404130. hal-01658753.

[135] Boris Bukh and Xavier Goaoc. "Shatter functions with polynomial growth rates". In: *SIAM Journal on Discrete Mathematics* 33.2 (2019). arXiv: 1701.06632, pp. 784–794. DOI: 10.1137/17M1113680. hal-02050524.

[136] Svyatoslav Covanov and Emmanuel Thomé. "Fast integer multiplication using generalized Fermat primes". In: *Mathematics of Computation* 88.317 (2019). arXiv: 1502.02800, pp. 1449–1477. DOI: 10.1090/mcom/3367. hal-01108166.

[137] Jesús A. De Loera, Xavier Goaoc, Frédéric Meunier, and Nabil Mustafa. "The discrete yet ubiquitous theorems of Caratheodory, Helly, Sperner, Tucker, and Tverberg". In: *Bulletin of the American Mathematical Society* 56 (2019). arXiv: 1706.05975, pp. 415–511. DOI: 10.1090/bull/1653. hal-02050466.

[138] Vincent Despré and Francis Lazarus. "Computing the Geometric Intersection Number of Curves". In: *Journal of the ACM (JACM)* 66.6 (November 2019). arXiv: 1511.09327 - 59 pages, 33 figures, revised version accepted to Journal of the ACM. The time complexity for testing if a curve is homotopic to a simple one has been reduced to $O(n + \ell \log \ell)$, pp. 1–49. DOI: 10.1145/3363367. hal-02385419.

[139] Jimmy Etienne, Nicolas Ray, Daniele Panozzo, Samuel Hornus, Charlie C.L. Wang, Jonàs Martínez, Sara Mcmains, Marc Alexa, Brian Wyvill, and Sylvain Lefebvre. "CurviSlicer: Slightly curved slicing for 3-axis printers". In: *ACM Transactions on Graphics* 38.4 (August 2019), pp. 1–11. DOI: 10.1145/3306346.3323022. hal-02120033.

[140] Alvaro Javier Fuentes Suárez, Evelyne Hubert, and Cédric Zanni. "Anisotropic convolution surfaces". In: *Computers and Graphics* 82 (2019), pp. 106–116. DOI: 10.1016/j.cag.2019.05.018. hal-02137325.

[141] Xavier Goaoc, Pavel Paták, Zuzana Patáková, Martin Tancer, and Uli Wagner. "Shellability is NP-complete". In: *Journal of the ACM (JACM)* 66.3 (June 2019). arXiv: 1711.08436, pp. 1–18. DOI: 10.1145/3314024. hal-02050505.

[142] Michel Grediac, Benoît Blaysat, and Frédéric Sur. "A robust-to-noise deconvolution algorithm to enhance displacement and strain maps obtained with local DIC and LSA". In: *Experimental Mechanics* 59.2 (2019), pp. 219–243. DOI: 10.1007/s11340-018-00461-4. hal-01926058.

[143] Michel Grediac, Benoît Blaysat, and Frédéric Sur. "Extracting displacement and strain fields from checkerboard images with the Localized Spectrum Analysis". In: *Experimental Mechanics* 59.2 (2019), pp. 207–218. DOI: 10.1007/s11340-018-00439-2. hal-01926054.

[144] Aurore Guillevic. "Faster individual discrete logarithms in finite fields of composite extension degree". In: *Mathematics of Computation* 88.317 (January 2019). arXiv: 1809.06135, pp. 1273–1301. DOI: 10.1090/mcom/3376. hal-01341849.

[145] Jean Hergel, Kevin Hinz, Sylvain Lefebvre, and Bernhard Thomaszewski. "Extrusion-Based Ceramics Printing with Strictly-Continuous Deposition". In: *ACM Transactions on Graphics* (November 2019). DOI: 10.1145/3355089.3356509. hal-02363424.

[146] Sylvain Lazard, William Lenhart, and Giuseppe Liotta. "On the Edge-length Ratio of Outerplanar Graphs". In: *Theoretical Computer Science* 770 (2019), pp. 88–94. DOI: 10.1016/j.tcs.2018.10.002. hal-01886947.

[147] Jonàs Martínez, Mélina Skouras, Christian Schumacher, Samuel Hornus, Sylvain Lefebvre, and Bernhard Thomaszewski. "Star-Shaped Metrics for Mechanical Metamaterial Design". In: *ACM Transactions on Graphics* 38.4 (July 2019). Special issue, SIGGRAPH 2019, Article No. 82 :1–13. DOI: 10.1145/3306346.3322989. hal-02118846.

[148] Erinc Merdivan, Deepika Singh, Sten Hanke, and Andreas Holzinger. "Dialogue Systems for Intelligent Human Computer Interactions". In: *Electronic Notes in Theoretical Computer Science* 343 (May 2019), pp. 57–71. DOI: 10.1016/j.entcs.2019.04.010. hal-03081682.

[149] Khadija Musayeva, Fabien Lauer, and Yann Guermeur. "Rademacher Complexity and Generalization Performance of Multi-category Margin Classifiers". In: *Neurocomputing* 342 (2019). arXiv: 1812.00584, pp. 6–15. DOI: 10.1016/j.neucom.2018.11.096. hal-01941089.

[150] Phuc Ngo, Nicolas Passat, Yukiko Kenmochi, and Isabelle Debled-Rennesson. "Geometric preservation of 2D digital objects under rigid motions". In: *Journal of Mathematical Imaging and Vision* 61 (2019), pp. 204–223. DOI: 10.1007/s10851-018-0842-9. hal-01695370.

[151] Pierre Rolin, Marie-Odile Berger, and Frédéric Sur. "View synthesis for pose computation". In: *Machine Vision and Applications* 30.7-8 (2019), pp. 1209–1227. DOI: 10.1007/s00138-019-01045-5. hal-02279616.

[152] Haichuan Song, Jonàs Martínez, Pierre Bedell, Noemie Vennin, and Sylvain Lefebvre. "Colored fused filament fabrication". In: *ACM Transactions on Graphics* 38.5 (June 2019), pp. 1–11. DOI: 10.1145/3183793. hal-01660621.

[153] Frédéric Sur. "A non-local dual-domain approach to cartoon and texture decomposition". In: *IEEE Transactions on Image Processing* 28.4 (2019), pp. 1882–1894. DOI: 10.1109/TIP.2018.2881906. hal-01925890.

[154] Pauline Tan, Fabien Pierre, and Mila Nikolova. "Inertial Alternating Generalized Forward-Backward Splitting for Image Colorization". In: *Journal of Mathematical Imaging and Vision* 61.5 (February 2019), pp. 672–690. DOI: 10.1007/s10851-019-00877-0. hal-01792432.

[155] Thibault Tricard, Frédéric Claux, and Sylvain Lefebvre. "Ribbed support vaults for 3D printing of hollowed objects". In: *Computer Graphics Forum* (June 2019). DOI: 10.1111/cgf.13750. hal-02155929.

[156] Thibault Tricard, Semyon Efremov, Cédric Zanni, Fabrice Neyret, Jonàs Martínez, and Sylvain Lefebvre. "Procedural Phasor Noise". In: *ACM Transactions on Graphics* 38.4 (July 2019), Article No. 57:1–13. DOI: 10.1145/3306346.3322990. hal-02118508.

[157] L. Wendling, I Debled-Rennesson, and H. Nasser. "Multilevel Polygonal Descriptor Matching Defined By Combining Discrete Lines And Force Histogram Concepts". In: *Multimedia Tools and Applications* (April 2019). DOI: 10.1007/s11042-019-7531-6. hal-02931272.

[158] Simon Abelard. "Counting points on hyperelliptic curves with explicit real multiplication in arbitrary genus". In: *Journal of Complexity* 57 (April 2020), p. 101440. DOI: 10.1016/j.jco.2019.101440. hal-01905580.

[159] Stanislav Aranovskiy, Igor Ryadchikov, Evgeny Nikulchev, Jian Wang, and Dmitry Sokolov. "Bias Propagation and Estimation in Homogeneous Differentiators for a Class of Mechanical Systems". In: *IEEE Access* 8 (2020), pp. 19450–19459. DOI: 10.1109/ACCESS.2020.2968219. hal-02516559.

[160] Stanislav Aranovskiy, Igor Ryadchikov, Evgeny Nikulchev, Jian Wang, and Dmitry Sokolov. "Experimental Comparison of Velocity Observers: A Scissored Pair Control Moment Gyroscope Case Study". In: *IEEE Access* 8 (2020), pp. 21694–21702. DOI: 10.1109/ACCESS.2020.2968221. hal-02516558.

[161] Imre Barany, Matthieu Fradelizi, Xavier Goaoc, Alfredo Hubard, and Günter Rote. "Random polytopes and the wet part for arbitrary probability distributions". In: *Annales Henri Lebesgue* 3 (2020). arXiv: 1902.06519, pp. 701–715. DOI: 10.5802/ahl.44. hal-02937527.

[162] Enka Blanchard. "Crip spatialities and temporalities 2 : a systematic typology of temporal taxes". In: *EspacesTemps.net* (June 2020). DOI: 10.26151/espacestemps.net-g7ca-v287. hal-03133413.

[163] Enka Blanchard. "Crip spatialities and temporalities I : discreet crips in a discrete world". In: *EspacesTemps.net* (March 2020). DOI: 10.26151/espacestemps.net-vmak-xq38. hal-02549867.

[164] Benoît Blaysat, Jan Neggers, Michel Grediac, and Frédéric Sur. "Towards Criteria Characterizing the Metrological Performance of Full-field Measurement Techniques : Application to the Comparison Between Local and Global Versions of DIC". In: *Experimental Mechanics* 60.3 (2020), pp. 393–407. DOI: 10.1007/s11340-019-00566-4. hal-02436541.

[165] Jean-Daniel Boissonnat, Olivier Devillers, Kunal Dutta, and Marc Glisse. "Randomized incremental construction of Delaunay triangulations of nice point sets". In: *Discrete and Computational Geometry* 64 (2020), p. 33. DOI: 10.1007/s00454-020-00235-7. hal-02937624.

[166] Dobrina Boltcheva, Justine Basselin, Clément Poull, Herve Barthelemy, and Dmitry Sokolov. "Topological-based roof modeling from 3D point clouds". In: *Journal of WSCG* 28.1-2 (2020), pp. 137–146. DOI: 10.24132/JWSCG.2020.28.17. hal-02983073.

[167] Prosenjit Bose, Jean-Lou De Carufel, and Olivier Devillers. "Expected Complexity of Routing in Θ_6 and Half-Θ_6 Graphs". In: *Journal of Computational Geometry* 11.1 (2020), pp. 212–234. DOI: 10.20382/jocg.v11i1a9. hal-02922660.

[168] Hamid Boukerrou, Paul Huynh, Virginie Lallemand, Bimal Mandal, and Marine Minier. "On the Feistel Counterpart of the Boomerang Connectivity Table : Introduction and Analysis of the FBCT". In: *IACR Transactions on Symmetric Cryptology* 2020.1 (May 2020), pp. 331–362. DOI: 10.13154/tosc.v2020.i1.331-362. hal-02945065.

[169] Steven Chaplick, Thomas C Van Dijk, Myroslav Kryven, Ji-won Park, Alexander Ravsky, and Alexander Wolff. "Bundled Crossings Revisited". In: *Journal of Graph Algorithms and Applications* (June 2020). DOI: 10.7155/jgaa.00534. hal-02972975.

[170] Guillaume Coiffier, Philippe Renard, and Sylvain Lefebvre. "3D Geological Image Synthesis From 2D Examples Using Generative Adversarial Networks". In: *Frontiers in Water* 2 (October 2020). DOI: 10.3389/frwa.2020.560598. hal-02992194.

[171] Sophie Cortese, Erwan Kerrien, Ilya Yakavets, Rokia Meilender, Romina Mastronicola, Sophie Renard, Agnès Leroux, Lina Bezdetnaya, and Gilles Dolivet. "ICG-induced NIR fluorescence mapping in patients with head & neck tumors after the previous radiotherapy". In: *Photodiagnosis and Photodynamic Therapy* 31 (September 2020), p. 101838. DOI: 10.1016/j.pdpdt.2020.101838. hal-02888671.

[172] Alfredo Cuzzocrea. "SPPOLAP: Computing Privacy-Preserving OLAP Data Cubes Effectively and Efficiently Algorithms, Complexity Analysis and Experimental Evaluation". In: *Procedia Computer Science* 176 (2020), pp. 3831–3842. DOI: 10.1016/j.procs.2020.09.337. hal-03284184.

[173] Alfredo Cuzzocrea, Carson K Leung, Bryan H Wodi, S Sourav, and Edoardo Fadda. "An Effective and Efficient Technique for Supporting Privacy-Preserving Keyword-Based Search over Encrypted Data in Clouds". In: *Procedia Computer Science* 177 (2020), pp. 509–515. DOI: 10.1016/j.procs.2020.10.070. hal-03274605.

[174] Alfredo Cuzzocrea, Enzo Mumolo, Edoardo Fadda, and Marco Tessarotto. "A Novel Big Data Analytics Approach for Supporting Cyber Attack Detection via Non-linear Analytic Prediction of IP Addresses". In: *Lecture Notes in Computer Science*. Computational Science and Its Applications – ICCSA 2020 (2020), pp. 978–991. DOI: 10.1007/978-3-030-58799-4_70. hal-03274600.

[175] Nicolas David and Paul Zimmermann. "A New Ranking Function for Polynomial Selection in the Number Field Sieve". In: *Contemporary mathematics*. 75 Years of Mathematics of Computation 754 (2020), pp. 315–325. DOI: 10.1090/CONM/754/15139. hal-02151093.

[176] Olivier Devillers, Sylvain Lazard, and William Lenhart. "Rounding meshes in 3D". In: *Discrete and Computational Geometry* (April 2020). DOI: 10.1007/s00454-020-00202-2. hal-02549290.

[177] Jaime Garcia Guevara, Igor Peterlik, Marie-Odile Berger, and Stéphane Cotin. "Elastic registration based on compliance analysis and biomechanical graph matching". In: *Annals of Biomedical Engineering* 48 (2020). arXiv: 1912.06353, pp. 447–462. DOI: 10.1007/s10439-019-02364-4. hal-02401280.

[178] Vincent Gaudillière, Gilles Simon, and Marie-Odile Berger. "Perspective-2-Ellipsoid: Bridging the Gap Between Object Detections and 6-DoF Camera Pose". In: *IEEE Robotics and Automation Letters* 5.4 (October 2020), pp. 5189–5196. DOI: 10.1109/LRA.2020.3005387. hal-02886633.

[179] David Gérault, Pascal Lafourcade, Marine Minier, and Christine Solnon. "Computing AES related-key differential characteristics with constraint programming". In: *Artificial Intelligence* 278 (January 2020), p. 103183. DOI: 10.1016/j.artint.2019.103183. hal-02327893.

[180] Michel Grediac, Benoît Blaysat, and Frédéric Sur. "Comparing several spectral methods used to extract displacement fields from checkerboard images". In: *Optics and Lasers in Engineering* 127 (2020), p. 105984. DOI: 10.1016/j.optlaseng.2019.105984. hal-02436572.

[181] Michel Grédiac, Benoît Blaysat, and Frédéric Sur. "On the Optimal Pattern for Displacement Field Measurement: Random Speckle and DIC, or Checkerboard and LSA?" In: *Experimental Mechanics* 60.4 (2020), pp. 509–534. DOI: 10.1007/s11340-019-00579-z. hal-02462030.

[182] Yann Guermeur. "Rademacher Complexity of Margin Multi-category Classifiers". In: *Neural Computing and Applications*. Neural Computing and Applications 32.24 (December 2020), pp. 17995–18008. DOI: 10.1007/s00521-018-3873-7. hal-02377345.

[183] Aurore Guillevic, Simon Masson, and Emmanuel Thomé. "Cocks-Pinch curves of embedding degrees five to eight and optimal ate pairing computation". In: *Designs, Codes and Cryptography* 88.6 (March 2020), pp. 1047–1081. DOI: 10.1007/s10623-020-00727-w. hal-02305051.

[184] Samuel Hornus, Tim Kuipers, Olivier Devillers, Monique Teillaud, Jonàs Martínez, Marc Glisse, Sylvain Lazard, and Sylvain Lefebvre. "Variable-width contouring for additive manufacturing". In: *ACM Transactions on Graphics* 39.4 (Proc. SIGGRAPH) (July 2020). DOI: 10.1145/3386569.3392448. hal-02568677.

[185] Tamás Illés, Stig M. Jespersen, Pieter Reynders, Fabien Lauer, J.-C. Le Huec, and Jean-François DUBOUSSET. "Axial plane characteristics of thoracic scoliosis and their usefulness for determining the fusion levels and the correction technique". In: *European Spine Journal* 29 (2020), pp. 2000–2009. DOI: 10.1007/s00586-020-06390-y. hal-03382549.

[186] Rémi Imbach, Marc Pouget, and Chee Yap. "Clustering Complex Zeros of Triangular Systems of Polynomials". In: *Mathematics in Computer Science* (June 2020). DOI: 10.1007/s11786-020-00482-0. hal-02878388.

[187] Sorina Ionica and Emmanuel Thomé. "Isogeny graphs with maximal real multiplication". In: *Journal of Number Theory* 207 (February 2020). arXiv: 1407.6672, pp. 385–422. DOI: 10.1016/j.jnt.2019.06.019. hal-00967742.

[188] Benedikt Kolbe and Myfanwy Evans. "Isotopic tiling theory for hyperbolic surfaces". In: *Geometriae Dedicata* (July 2020). DOI: 10.1007/s10711-020-00554-2. hal-02981001.

[189] Fabien Lauer. "Error Bounds for Piecewise Smooth and Switching Regression". In: *IEEE Transactions on Neural Networks and Learning Systems* 31.4 (2020). arXiv: 1707.07938, pp. 1183–1195. DOI: 10.1109/TNNLS.2019.2919444. hal-01566136.

[190] Aude Le Gluher and Pierre-Jean Spaenlehauer. "A Fast Randomized Geometric Algorithm for Computing Riemann-Roch Spaces". In: *Mathematics of Computation* 89 (2020). arXiv: 1811.08237, pp. 2399–2433. DOI: 10.1090/mcom/3517. hal-01930573.

[191] Subhamoy Maitra, Bimal Mandal, Thor Martinsen, Dibyendu Roy, and Pantelimon Stanica. "Analysis on Boolean function in a restricted (biased) domain". In: *IEEE Transactions on Information Theory* 66.2 (2020), pp. 1219–1231. DOI: 10.1109/TIT.2019.2932739. hal-02374194.

[192] Erinc Merdivan, Deepika Singh, Sten Hanke, Johannes Kropf, Andreas Holzinger, and Matthieu Geist. "Human Annotated Dialogues Dataset for Natural Conversational Agents". In: *Applied Sciences* 10.3 (February 2020), p. 762. DOI: 10.3390/app10030762. hal-03081727.

[193] Enea Milio and Damien Robert. "Modular polynomials on Hilbert surfaces". In: *Journal of Number Theory* (May 2020). DOI: 10.1016/j.jnt.2020.04.014. hal-01520262.

[194] Madhurima Mukhopadhyay, Palash Sarkar, Shashank Singh, and Emmanuel Thomé. "New Discrete Logarithm Computation for the Medium Prime Case Using the Function Field Sieve". In: *Advances in Mathematics of Communications* (2020). DOI: 10.3934/amc.2020119. hal-02964002.

[195] Van-Tho Nguyen, Thiéry Constant, Bertrand Kerautret, Isabelle - Debled-Rennesson, and Francis Colin. "A Machine-Learning Approach for Classifying Defects on Tree Trunks using Terrestrial LiDAR". In: *Computers and Electronics in Agriculture* 171 (April 2020), pp. 1–12. DOI: 10.1016/j.compag.2020.105332. hal-02931277.

[196] Thibault Tricard, Vincent Tavernier, Cédric Zanni, Jonàs Martínez, Pierre-Alexandre Hugron, Fabrice Neyret, and Sylvain Lefebvre. "Freely orientable microstructures for designing deformable 3D prints". In: *ACM Transactions on Graphics* 39.6 (December 2020), pp. 1–16. DOI: 10.1145/3414685.3417790. hal-02524371.

[197] Raffaella Trivisonne, Erwan Kerrien, and Stéphane Cotin. "Constrained Stochastic State Estimation of Deformable 1D Objects: Application to Single-view 3D Reconstruction of Catheters with Radio-opaque Markers". In: *Computerized Medical Imaging and Graphics* 81 (February 2020). DOI: 10.1016/j.compmedimag.2020.101702. hal-02469093.

[198] Félix Vanneste, Olivier Goury, Jonas Martinez, Sylvain Lefebvre, Hervé Delingette, and Christian Duriez. "Anisotropic soft robots based on 3D printed meso-structured materials: design, modeling by homogenization and simulation". In: *IEEE Robotics and Automation Letters* 5.2 (January 2020), pp. 2380–2386. DOI: 10.1109/LRA.2020.2969926. hal-02475589.

[199] Jian Wang, Stanislav Aranovskiy, Emilia Fridman, Dmitry Sokolov, Denis Efimov, and Alexey Bobtsov. "Robust adaptive stabilization by delay under state parametric uncertainty and measurement bias". In: *IEEE Transactions on Automatic Control* (2020). DOI: 10.1109/TAC.2020.3045125. hal-03059893.

[200] Cong Yang, Gilles Simon, John See, Marie-Odile Berger, and Wenyong Wang. "WatchPose: A View-Aware Approach for Camera Pose Data Collection in Industrial Environments". In: *Sensors* 20.11 (May 2020). DOI: 10.3390/s20113045. hal-02735272.

[201] Jinfan Yang, Chrystiano Araújo, Nicholas Vining, Zachary Ferguson, Enrique Rosales, Daniele Panozzo, Sylvain Lefebvre, Paolo Cignoni, and Sheffer Alla. "DHFSlicer: Double Height-Field Slicing for Milling Fixed-Height Materials". In: *ACM Transactions on Graphics* 39.6 (November 2020). DOI: 10.1145/3414685.3417810. hal-02992003.

[202] Max Alekseyev, Joseph Samuel Myers, Richard Schroeppel, Scott R Shannon, Neil James Alexander Sloane, and Paul Zimmermann. "Three Cousins of Recamán's Sequence". In: *The Fibonacci Quarterly* (2021). arXiv: 2004.14000. hal-02951011.

[203] Stanislav Aranovskiy, Denis Efimov, Dmitry Sokolov, Jian Wang, Igor Ryadchikov, and Alexey Bobtsov. "Switched Observer Design For a Class of Locally Unobservable Time-Varying Systems". In: *Automatica* 130 (August 2021), p. 109715. DOI: 10.1016/j.automatica.2021.109715. hal-03273675.

[204] Melike Aydinlilar and Cédric Zanni. "Fast ray tracing of scale-invariant integral surfaces". In: *Computer Graphics Forum* 40.6 (September 2021), pp. 117–134. DOI: 10.1111/cgf.14208. hal-03169283.

[205] Justine Basselin, Laurent Alonso, Nicolas Ray, Dmitry Sokolov, Sylvain Lefebvre, and Bruno Lévy. "Restricted Power Diagrams on the GPU". In: *Computer Graphics Forum* 40.2 (June 2021). DOI: 10.1111/cgf.142610. hal-03169575.

[206] Enka Blanchard, Zacharie Boubli, and Charlotte Lemaistre. "La Covid au prisme des minorités vulnérables". In: *EspacesTemps.net* (February 2021). DOI: 10.26151/espacestemps.net-1978-7z05. hal-03133414.

[207] Xavier Bonnetain and Samuel Jaques. "Quantum Period Finding against Symmetric Primitives in Practice". In: *IACR Transactions on Cryptographic Hardware and Embedded Systems* 2022.1 (November 2021), pp. 1–27. DOI: 10.46586/tches.v2022.i1.1-27. hal-03431518.

[208] Charles Bouillaguet and Paul Zimmermann. "Parallel Structured Gaussian Elimination for the Number Field Sieve". In: *Mathematical Cryptology* 0.1 (January 2021), pp. 22–39. hal-02098114.

[209] Seyfeddine Boukhtache, Kamel Abdelouahab, François Berry, Benoît Blaysat, Michel Grediac, and Frédéric Sur. "When Deep Learning Meets Digital Image Correlation". In: *Optics and Lasers in Engineering* 136 (January 2021), p. 106308. DOI: 10.1016/j.optlaseng.2020.106308. hal-02933431.

[210] Olivier Bronchain, Sebastian Faust, Virginie Lallemand, Gregor Leander, Léo Perrin, and François-Xavier Standaert. "MOE: Multiplication Operated Encryption with Trojan Resilience". In: *IACR Transactions on Symmetric Cryptology* 2021.1 (March 2021), pp. 78–129. DOI: 10.46586/tosc.v2021.i1.78-129. hal-03453550.

[211] Benoît Cogliati, Jordan Ethan, Virginie Lallemand, Byeonghak Lee, Jooyoung Lee, and Marine Minier. "CTET+: A Beyond-Birthday-Bound Secure Tweakable Enciphering Scheme Using a Single Pseudorandom Permutation". In: *IACR Transactions on Symmetric Cryptology* 2021.4 (December 2021), pp. 1–35. DOI: 10.46586/tosc.v2021.i4.1-35. hal-03504330.

[212] Guillaume Coiffier, Justine Basselin, Nicolas Ray, and Dmitry Sokolov. "Parametric Surface Fitting on Airborne Lidar Point Clouds for Building Reconstruction". In: *Computer-Aided Design* 140 (July 2021), p. 103090. DOI: 10.1016/j.cad.2021.103090. hal-03281816.

[213] Alfredo Cuzzocrea, Edoardo Fadda, and Enzo Mumolo. "Cyber-attack detection via non-linear prediction of IP addresses: an innovative big data analytics approach". In: *Multimedia Tools and Applications* (September 2021). DOI: 10.1007/s11042-021-11390-1. hal-03352525.

[214] Laurent Decreusefond and Guillaume Moroz. "Optimal transport between determinantal point processes and application to fast simulation". In: *Modern Stochastics: Theory and Applications* 8.2 (2021), pp. 209–237. DOI: 10.15559/21-VMSTA180. hal-02984323.

[215] David Desobry, Yoann Coudert-Osmont, Etienne Corman, Nicolas Ray, and Dmitry Sokolov. "Designing 2D and 3D Non-Orthogonal Frame Fields". In: *Computer-Aided Design* 139 (July 2021), pp. 1–9. DOI: 10.1016/j.cad.2021.103081. hal-03287233.

[216] Semyon Efremov, Jonàs Martínez, and Sylvain Lefebvre. "3D periodic cellular materials with tailored symmetry and implicit grading". In: *Computer-Aided Design* 140 (November 2021). DOI: 10.1016/j.cad.2021.103086. hal-03290606.

[217] Antoine Fond, Marie-Odile Berger, and Gilles Simon. "Model-image registration of a building's facade based on dense semantic segmentation". In: *Computer Vision and Image Understanding* 206 (May 2021), p. 103185. DOI: 10.1016/j.cviu.2021.103185. hal-03204477.

[218] Vladimir Garanzha, Igor Kaporin, Liudmila Kudryavtseva, François Protais, Nicolas Ray, and Dmitry Sokolov. "Foldover-free maps in 50 lines of code". In: *ACM Transactions on Graphics* 40.4 (July 2021). arXiv: 2102.03069, Article No.102, pp 1–16. DOI: 10.1145/3450626.3459847. hal-03127350.

[219] Xavier Goaoc, Andreas Holmsen, and Cyril Nicaud. "An experimental study of forbidden patterns in geometric permutations by combinatorial lifting". In: *Journal of Computational Geometry*. Special Issue of Selected Papers from SoCG 2019 11.2 (January 2021). arXiv: 1903.03014, pp. 131–161. DOI: 10.20382/jocg.v11i2a6. hal-03152958.

[220] Aurore Guillevic and Shashank Singh. "On the Alpha Value of Polynomials in the Tower Number Field Sieve Algorithm". In: *Mathematical Cryptology* 1.1 (February 2021), pp. 1–39. hal-02263098.

[221] Myriam Guillevic, Aurore Guillevic, Martin K Vollmer, Paul Schlauri, Matthias Hill, Lukas Emmenegger, and Stefan Reimann. "Automated fragment formula annotation for electron ionisation, high resolution mass spectrometry: application to atmospheric measurements of halocarbons". In: *Journal of Cheminformatics* 13.78 (October 2021). arXiv: 2103.13807 - There is a supplement (PDF document) with figures and four ZIP archive files., pp. 1–27. DOI: 10.1186/s13321-021-00544-w. hal-03176025.

[222] Damien Jamet, Pierre Popoli, and Thomas Stoll. "Maximum order complexity of the sum of digits function in Zeckendorf base and polynomial subsequences". In: *Cryptography and Communications - Discrete Structures, Boolean Functions and Sequences* (July 2021). arXiv: 2106.09959. DOI: 10.1007/s12095-021-00507-w. hal-03283528.

[223] George Krait, Sylvain Lazard, Guillaume Moroz, and Marc Pouget. "Certified numerical algorithm for isolating the singularities of the plane projection of generic smooth space curves". In: *Journal of Computational and Applied Mathematics* 394 (October 2021), p. 113553. DOI: 10.1016/j.cam.2021.113553. hal-03161393.

[224] Aude Le Gluher, Pierre-Jean Spaenlehauer, and Emmanuel Thomé. "Refined Analysis of the Asymptotic Complexity of the Number Field Sieve". In: *Mathematical Cryptology* 1.1 (2021). arXiv: 2007.02730, pp. 71–88. hal-02934273.

[225] Bruno Lévy, Roya Mohayaee, and Sebastian von Hausegger. "A fast semidiscrete optimal transport algorithm for a unique reconstruction of the early Universe". In: *Monthly Notices of the Royal Astronomical Society* 506.1 (June 2021). arXiv: 2012.09074, pp. 1165–1185. DOI: 10.1093/mnras/stab1676. hal-03115841.

[226] Jonàs Martínez. "Random Auxetic Porous Materials from Parametric Growth Processes". In: *Computer-Aided Design* 139 (June 2021). DOI: 10.1016/j.cad.2021.103069. hal-02911788.

[227] Daryna Panicheva, Pierre-Frédéric Villard, Peter E Hammer, Douglas Perrin, and Marie-Odile Berger. "Automatic extraction of the mitral valve chordae geometry for biomechanical simulation". In: *International Journal of Computer Assisted Radiology and Surgery*. Proceedings of IPCAI 2021 16.5 (May 2021), pp. 709–720. DOI: 10.1007/s11548-021-02368-3. hal-03262496.

[228] Fabien Pierre, Mathieu Amendola, Clémence Bigeard, Timothé Ruel, and Pierre-Frédéric Villard. "Segmentation with Active Contours". In: *Image Processing On Line* 11 (May 2021), pp. 120–141. DOI: 10.5201/ipol.2021.298. hal-03235096.

[229] Siyi Qin, Michel Grédiac, Benoît Blaysat, Shaopeng Ma, and Frédéric Sur. "Influence of the sampling density on the noise level in displacement and strain maps obtained by processing periodic patterns". In: *Measurement - Journal of the International Measurement Confederation (IMEKO)* 173 (March 2021), p. 108570. DOI: 10.1016/j.measurement.2020.108570. hal-02965328.

[230] Rahimeh Rouhi, Marianne Clausel, Julien Oster, and Fabien Lauer. "An Interpretable Hand-Crafted Feature-Based Model for Atrial Fibrillation Detection". In: *Frontiers in Physiology* 12 (May 2021), p. 657304. DOI: 10.3389/fphys.2021.657304. hal-03382590.

[231] Nathan J. Secrest, Sebastian von Hausegger, Mohamed Rameez, Roya Mohayaee, Subir Sarkar, and Jacques Colin. "A Test of the Cosmological Principle with Quasars". In: *The Astrophysical journal letters* 908.2 (2021). arXiv: 2009.14826, p. L51. DOI: 10.3847/2041-8213/abdd40. hal-03022647.

[232] Gilles Simon. “Jan Van Eyck’s Perspectival System Elucidated Through Computer Vision”. In: *Proceedings of the ACM on Computer Graphics and Interactive Techniques* 4.2 (July 2021). (SIGGRAPH 2021). DOI: 10.1145/3465623. hal-03287031.

[233] Frédéric Sur, Benoît Blaysat, and Michel Grédiac. “On Biases in Displacement Estimation for Image Registration, with a Focus on Photomechanics”. In: *Journal of Mathematical Imaging and Vision* 63.7 (May 2021), pp. 777–806. DOI: 10.1007/s10851-021-01032-4. hal-03226201.

Invited Conferences

[234] Walter C.P.M. Blondel, Faiza Abdat, Marine Amouroux, and Yann Guermeur. “Multi-modality fibered in vivo spectroscopy applied to skin hyperplastic and dysplastic class discrimination: spatially resolved data fusion-based classification”. In: *Asia Communications and Photonics Conference, ACP 2017*. Guangzhou, China, November 2017. hal-01637378.

[235] Véronique Cortier, Pierrick Gaudry, and Stephane Glondu. “Belenios: a simple private and verifiable electronic voting system”. In: *Foundations of Security, Protocols, and Equational Reasoning*. Ed. by Joshua D. Guttman, Carl E. Landwehr, José Meseguer, and Dusko Pavlovic. Vol. 11565. LNCS. Fredericksburg, Virgina, United States: Springer, 2019, pp. 214–238. DOI: 10.1007/978-3-030-19052-1_14. hal-02066930.

[236] Monique Teillaud. “Triangulations in CGAL - To non-Euclidean spaces and beyond!” In: *EuroCG 2020 - 36th European Workshop on Computational Geometry*. Würzburg, Germany, March 2020. hal-02510046.

Major International Conferences

[237] Benoît Blaysat, Michel Grédiac, and Frédéric Sur. “Assessing the Metrological Performance of DIC Applied on RGB Images”. In: *iDICS 2016 Conference*. Ed. by M. Sutton and P. Reu. Proceedings of the first Conference of the International Digital Imaging Correlation Society. Philadelphia, United States: Springer, November 2016, pp. 109–111. DOI: 10.1007/978-3-319-51439-0_26. hal-01500324.

[238] Mikhail Bogdanov, Monique Teillaud, and Gert Vegter. “Delaunay triangulations on orientable surfaces of low genus”. In: *32nd International Symposium on Computational Geometry*. Boston, United States, June 2016, 20:1–20:15. DOI: 10.4230/LIPIcs.SoCG.2016.20. hal-01276386.

[239] David Bremner, Olivier Devillers, Marc Glisse, Sylvain Lazard, Giuseppe Liotta, Tamara Mchedlidze, Sue Whitesides, and Stephen Wismath. “Monotone Simultaneous Paths Embeddings in $\mathbb{R}^d$”. In: *24th International Symposium on Graph Drawing & Network Visualization*. Vol. 9801. Proceedings of 24th International Symposium on Graph Drawing & Network Visualization. arXiv: 1608.08791. Athens, Greece: Springer, September 2016. hal-01366148.

[240] Changbo Chen, Svyatoslav Covanov, Farnam Mansouri, Marc Moreno Maza, Ning Xie, and Yuzhen Xie. “Parallel Integer Polynomial Multiplication”. In: *SYNASC 2016 - 18th International Symposium on Symbolic and Numeric Algorithms for Scientific Computing*. Timisoara, Romania, September 2016, pp. 72–80. DOI: 10.1109/SYNASC.2016.024. hal-01520021.

[241] Charlotte Delmas, Cyril Riddell, Yves Trousset, Erwan Kerrien, Marie-Odile Berger, René Anxionnat, and Serge Bracard. "Intra-operative 3D micro-coil imaging using subsampled tomographic acquisition patterns on a biplane C-arm system". In: *Proceedings of the 4th International Conference on Image Formation in X-Ray Computed Tomography (CT meeting'16)*. Bamberg, Germany, July 2016. hal-01303153.

[242] Olivier Devillers, Menelaos Karavelas, and Monique Teillaud. "Qualitative Symbolic Perturbation". In: *Proceedings of the 32nd International Symposium on Computational Geometry*. Boston, United States, June 2016, 33:1–33:15. DOI: 10.4230/LIPIcs.SoCG.2016.33. hal-01276444.

[243] Jean-Guillaume Dumas, Erich Kaltofen, Emmanuel Thomé, and Gilles Villard. "Linear Time Interactive Certificates for the Minimal Polynomial and the Determinant of a Sparse Matrix". In: *ISSAC'2016, Proceedings of the 2016 ACM International Symposium on Symbolic and Algebraic Computation*. arXiv: 1602.00810. Waterloo, Canada: ACM, July 2016, pp. 199–206. DOI: 10.1145/2930889.2930908. hal-01266041.

[244] Ninon Eyrolles, Louis Goubin, and Marion Videau. "Defeating MBA-based Obfuscation". In: *2nd International Workshop on Software PROtection*. Ed. by ACM. Vienna, Austria, October 2016. DOI: 10.1145/2995306.2995308. hal-01388109.

[245] Jean-Charles Faugère, Pierre-Jean Spaenlehauer, and Jules Svartz. "Computing Small Certificates of Inconsistency of Quadratic Fewnomial Systems". In: *International Symposium on Symbolic and Algebraic Computation (ISSAC 2016)*. arXiv: 1605.05889. Waterloo, Canada: ACM, July 2016, pp. 223–230. DOI: 10.1145/2930889.2930927. hal-01314651.

[246] Martine Gautier and Brigitte Wrobel-Dautcourt. "artEoz - dynamic program visualization". In: *International Conference on Informatics in Schools: Situation, Evolution, and Perspectives, ISSEP 2016*. Munster, Germany, October 2016, p. 2. hal-01388703.

[247] Aurore Guillevic, François Morain, and Emmanuel Thomé. "Solving discrete logarithms on a 170-bit MNT curve by pairing reduction". In: *Selected Areas in Cryptography – SAC 2016*. Ed. by Roberto Avanzi and Howard Heys. Vol. 10532. Lecture Notes in Computer Science. arXiv: 1605.07746. St. Johns, Newfoundland, Canada: Springer, August 2016, pp. 559–578. DOI: 10.1007/978-3-319-69453-5_30. hal-01320496.

[248] Adrien Guinet, Ninon Eyrolles, and Marion Videau. "Arybo: Manipulation, Canonicalization and Identification of Mixed Boolean-Arithmetic Symbolic Expressions". In: *GreHack 2016*. Proceedings of GreHack 2016. Grenoble, France, November 2016. hal-01390528.

[249] Nazim Haouchine, Marie-Odile Berger, and Stephane Cotin. "Simultaneous Pose Estimation and Augmentation of Elastic Surfaces from a Moving Monocular Camera". In: *International Symposium on Mixed and Augmented Reality*. Merida, Mexico, September 2016. hal-01353189.

[250] Ranjan Jha, Damien Chablat, Fabrice Rouillier, and Guillaume Moroz. "Influence of the trajectory planning on the accuracy of the orthoglide 5-axis". In: *ASME International Design Engineering Technical Conference and the Computer and Information in Engineering Conference (IDETC/CIE)*. Charlotte, NC, United States, August 2016. hal-01309190.

[251] Bertrand Kerautret, Adrien Krähenbühl, Isabelle Debled-Rennesson, and Jacques-Olivier Lachaud. "Centerline Detection on Partial Mesh Scans by Confidence Vote in Accumulation Map". In: *ICPR 2016 - IAPR International Conference on Pattern Recognition*. Cancùn, Mexico, December 2016. DOI: 10.1109/ICPR.2016.7899829. hal-01435271.

[252] Marine Minier and Raphael C.-W. Phan. "Tuple Cryptanalysis: Slicing and Fusing Multisets". In: *Paradigms in Cryptology – Mycrypt 2016*. Ed. by Raphael C.-W. Phan and Moti Yung. Vol. 10311. Lecture Notes in Computer Science. Kuala Lumpur, Malaysia: Springer, December 2016, pp. 294–320. DOI: 10.1007/978-3-319-61273-7. hal-01593382.

[253] Guillaume Moroz and Éric Schost. "A Fast Algorithm for Computing the Truncated Resultant". In: *ISSAC '16*. Ed. by Markus Rosenkranz. Proceedings of the ACM on International Symposium on Symbolic and Algebraic Computation. arXiv: 1609.04259. Sergei A. Abramov and Eugene V. Zima. Waterloo, Canada: ACM, July 2016, pp. 341–348. DOI: 10.1145/2930889.2930931. hal-01366386.

[254] Phuc Ngo, Hayat Nasser, Isabelle Debled-Rennesson, and Bertrand Kerautret. "Adaptive Tangential Cover for Noisy Digital Contours". In: *DGCI 2016 - 19th international conference on Discrete Geometry for Computer Imagery*. Vol. LNCS 9647. DGCI 2016: Discrete Geometry for Computer Imagery. Nantes, France, April 2016, pp. 439–451. DOI: 10.1007/978-3-319-32360-2_34. hal-01266033.

[255] Pierre-Jean Petitprez, Erwan Kerrien, and Pierre-Frédéric Villard. "PoLAR: a Portable Library for Augmented Reality". In: *15th IEEE International Symposium on Mixed and Augmented Reality (ISMAR)*. IEEE. Merida, Mexico, September 2016, p. 4. hal-01356012.

[256] Kacper Pluta, Guillaume Moroz, Yukiko Kenmochi, and Pascal Romon. "Quadric Arrangement in Classifying Rigid Motions of a 3D Digital Image". In: *The 18th International Workshop on Computer Algebra in Scientific Computing*. Vol. 9890. Lecture Notes in Computer Science. Bucharest, Romania: Springer, September 2016, pp. 426–443. DOI: 10.1007/978-3-319-45641-6_27. hal-01334257.

[257] Nicolas Ray, Dmitry Sokolov, and Bruno Lévy. "Practical 3D frame field generation". In: *SIGGRAPH ASIA 2016*. Vol. 35. macao, Macau SAR China, December 2016, pp. 1–9. hal-01397711.

[258] Pierre Rolin, Marie-Odile Berger, and Frédéric Sur. "Enhancing pose estimation through efficient patch synthesis". In: *27th British Machine Vision Conference (BMVC 2016)*. Proceedings of BMVC 2016. York, United Kingdom, September 2016. hal-01368843.

[259] Mohab Safey El Din and Pierre-Jean Spaenlehauer. "Critical Point Computations on Smooth Varieties: Degree and Complexity bounds". In: *International Symposium on Symbolic and Algebraic Computation (ISSAC)*. arXiv: 1605.02518. Waterloo, Canada, July 2016, pp. 183–190. DOI: 10.1145/2930889.2930929. hal-01312750.

[260] Gilles Simon, Antoine Fond, and Marie-Odile Berger. "A Simple and Effective Method to Detect Orthogonal Vanishing Points in Uncalibrated Images of Man-Made Environments". In: *Eurographics 2016*. Lisbon, Portugal, May 2016. hal-01275628.

[261] - Van-Tho Nguyen, Bertrand Kerautret, Isabelle Debled-Rennesson, Francis Colin, Alexandre Piboule, and Thiéry Constant. "Segmentation of defects on log surface from terrestrial lLidar data". In: *23rd International Conference on Pattern Recognition (ICPR)*. Mexico, Mexico: IEEE COMPUTER SOC, December 2016, p. 6. hal-02740896.

[262] Yinoussa Adagolodjo, Raffaella Trivisonne, Nazim Haouchine, Stéphane Cotin, and Hadrien Courtecuisse. "Silhouette-based Pose Estimation for Deformable Organs Application to Surgical Augmented Reality". In: *IROS 2017 - IEEE/RSJ International Conference on Intelligent Robots and Systems*. Vancouver, Canada, September 2017. hal-01578815.

[263] Mohammad Alaggan, Mathieu Cunche, and Marine Minier. “Non-interactive (t, n)-Incidence Counting from Differentially Private Indicator Vectors”. In: *3rd International Workshop on Security and Privacy Analytics (IWSPA 2017)*. Scottsdale, United States, March 2017. hal-01485412.

[264] Yacine Bouzidi, Thomas Cluzeau, Guillaume Moroz, and Alban Quadrat. “Computing effectively stabilizing controllers for a class of nD systems”. In: *The 20th World Congress of the International Federation of Automatic Control*. Vol. 50. 1. arXiv: 1801.04982. Toulouse, France, July 2017, pp. 1847–1852. DOI: 10.1016/j.ifacol.2017.08.200. hal-01667161.

[265] Liangyu Chen, Svyatoslav Covanov, Davood Mohajerani, and Marc Moreno Maza. “Big Prime Field FFT on the GPU”. In: *ISSAC 2017*. Kaiserslautern, Germany: ACM Press, July 2017, pp. 85–92. DOI: 10.1145/3087604.3087657. hal-01518830.

[266] Antoine Fond, Marie-Odile Berger, and Gilles Simon. “Facade Proposals for Urban Augmented Reality”. In: *ISMAR 2017 - 16th IEEE International Symposium on Mixed and Augmented Reality*. Nantes, France, October 2017. hal-01562392.

[267] Joshua Fried, Pierrick Gaudry, Nadia Heninger, and Emmanuel Thomé. “A kilobit hidden SNFS discrete logarithm computation”. In: *Advances in Cryptology – EUROCRYPT 2017*. Ed. by Jean-Sébastien Coron and Jesper Buus Nielsen. Vol. 10210. Lecture Notes in Computer Science. arXiv: 1610.02874. Paris, France: Springer, April 2017, pp. 202–231. DOI: 10.1007/978-3-319-56620-7_8. hal-01376934.

[268] Jaime Garcia Garcia Guevara, Igor Peterlik, Marie-Odile Berger, and Stéphane Cotin. “Automatic biomechanical graph matching CT-CBCT fusion”. In: *Surgetica 2017*. Strasbourg, France, November 2017. hal-01587952.

[269] David Gerault, Marine Minier, and Christine Solnon. “Using Constraint Programming to solve a Cryptanalytic Problem”. In: *IJCAI 2017 - International Joint Conference on Artificial Intelligence (Sister Conference Best Paper Track)*. Melbourne, Australia, August 2017, pp. 4844–4848. hal-01528272.

[270] Laurent Grémy, Aurore Guillevic, François Morain, and Emmanuel Thomé. “Computing discrete logarithms in $GF(p^6)$”. In: *Selected Areas in Cryptography – SAC 2017*. Ed. by Carlisle Adams and Jan Camenisch. Vol. 10719. Lecture Notes in Computer Science. Ottawa, Canada: Springer, August 2017, pp. 85–105. DOI: 10.1007/978-3-319-72565-9_5. hal-01624662.

[271] Iordan Iordanov and Monique Teillaud. “Implementing Delaunay Triangulations of the Bolza Surface”. In: *33rd International Symposium on Computational Geometry (SoCG 2017)*. Brisbane, Australia, July 2017, 44:1–44:15. DOI: 10.4230/LIPIcs.SoCG.2017.44. hal-01568002.

[272] Bertrand Kerautret, Phuc Ngo, Yukiko Kenmochi, and Antoine Vacavant. “Greyscale Image Vectorization from Geometric Digital Contour Representations”. In: *DGCI'17 - 20th International Conference on Discrete Geometry for Computer Imagery*. Vol. 34. Vienna, Austria, September 2017, pp. 2379–331. DOI: 10.1007/978-3-319-66272-5_26. hal-01588695.

[273] Sylvain Lazard, William Lenhart, and Giuseppe Liotta. “On the Edge-length Ratio of Outerplanar Graphs”. In: *International Symposium on Graph Drawing and Network Visualization*. Boston, United States, 2017. hal-01591699.

[274] Vincent Lefèvre and Paul Zimmermann. "Optimized Binary64 and Binary128 Arithmetic with GNU MPFR". In: *24th IEEE Symposium on Computer Arithmetic (ARITH 24)*. Ed. by Neil Burgess, Javier Bruguera, and Florent de Dinechin. London, United Kingdom, July 2017, pp. 18–26. DOI: 10.1109/ARITH.2017.28. hal-01502326.

[275] Anush Manukyan, Olivares-Mendez Miguel, Holger Voos, and Matthieu Geist. "Real time degradation identification of UAV using machine learning techniques". In: *International Conference on Unmanned Aircraft Systems (ICUAS)*. Miami, United States, 2017. hal-01629680.

[276] Erinc Merdivan, Mohammad Reza Loghmani, and Matthieu Geist. "Reconstruct & Crush Network". In: *Advances in Neural Information Processing Systems*. Long Beach, United States, 2017. hal-01629742.

[277] Phuc Ngo, Yukiko Kenmochi, Isabelle Debled-Rennesson, and Nicolas Passat. "Convexity-preserving rigid motions of 2D digital objects". In: *Discrete Geometry for Computer Imagery (DGCI)*. Vol. 10502. Lecture Notes in Computer Science. Vienna, Austria, 2017, pp. 69–81. DOI: 10.1007/978-3-319-66272-5_7. hal-01565028.

[278] Soumi Paul, Hayat Nasser, Mita Nasipuri, Phuc Ngo, Subhadip Basu, and Isabelle Debled-Rennesson. "A Statistical-Topological Feature Combination for Recognition of Isolated Hand Gestures from Kinect Based Depth Images". In: *IWCIA*. Vol. 10256. LNCS. Plovdiv, Bulgaria, June 2017. DOI: 10.1007/978-3-319-59108-7. hal-01517817.

[279] Simon Perdrix and Luc Sanselme. "Determinism and Computational Power of Real Measurement-based Quantum Computation". In: *FCT'17- 21st International Symposium on Fundamentals of Computation Theory*. arXiv: 1610.02824. Bordeaux, France, September 2017. DOI: 10.1007/978-3-662-55751-8_31. hal-01377339.

[280] Deepika Singh, Erinc Merdivan, Ismini Psychoula, Johannes Kropf, Sten Hanke, Matthieu Geist, and Andreas Holzinger. "Human activity recognition using recurrent neural networks". In: *1st International Cross-Domain Conference for Machine Learning and Knowledge Extraction (CD-MAKE)*. Ed. by Andreas Holzinger, Peter Kieseberg, A Min Tjoa, and Edgar Weippl. Vol. LNCS-10410. Machine Learning and Knowledge Extraction. Part 5: MAKE AAL. Reggio, Italy: Springer International Publishing, August 2017, pp. 267–274. DOI: 10.1007/978-3-319-66808-6_18. hal-01629704.

[281] Aaron Sujar, Andreas Meuleman, Pierre-Frédéric Villard, Marcos Garcia, and Franck P. Vidal. "gVirtualXRay: Virtual X-Ray Imaging Library on GPU". In: *Computer Graphics and Visual Computing*. Ed. by Tao Ruan Wan and Franck Vidal. Computer Graphics and Visual Computing. Manchester, United Kingdom: The Eurographics Association, September 2017, pp. 61–68. DOI: 10.2312/cgvc.20171279. hal-01588532.

[282] Raffaella Trivisonne, Erwan Kerrien, and Stéphane Cotin. "Augmented 3D Catheter Navigation using Constrained Shape from Template". In: *Hamlyn Symposium*. London, United Kingdom, June 2017. hal-01545693.

[283] Antoine Vacavant, Bertrand Kerautret, Tristan Roussillon, and Fabien Feschet. "Reconstructions of Noisy Digital Contours with Maximal Primitives Based on Multi-Scale/Irregular Geometric Representation and Generalized Linear Programming". In: *20th IAPR International Conference on Discrete Geometry for Computer Imagery*. Vol. 10502. Lecture Notes in Computer Science. Vienna, Austria: Springer, September 2017, pp. 291–303. DOI: 10.1007/BFb0038202. hal-01621504.

[284] Simon Abelard, Pierrick Gaudry, and Pierre-Jean Spaenlehauer. “Counting points on genus-3 hyperelliptic curves with explicit real multiplication”. In: *ANTS-XIII - Thirteenth Algorithmic Number Theory Symposium*. Madison, United States, July 2018, pp. 1–19. hal-01816256.

[285] Nicolas Bonichon, Prosenjit Bose, Jean-Lou De Carufel, Vincent Despré, Darryl Hill, and Michiel Smid. “Improved Routing on the Delaunay Triangulation”. In: *ESA 2018 - 26th Annual European Symposium on Algorithms*. Helsinki, Finland, August 2018. DOI: 10.4230/LIPIcs.ESA.2018.22. hal-01881280.

[286] Olivier Devillers, Sylvain Lazard, and William Lenhart. “3D Snap Rounding”. In: *Proceedings of the 34th International Symposium on Computational Geometry*. Budapest, Hungary, June 2018, 30:1–30:14. DOI: 10.4230/LIPIcs.SoCG.2018.30. hal-01727375.

[287] Jaime Garcia Guevara, Igor Peterlik, Marie-Odile Berger, and Stephane Cotin. “Biomechanics-based graph matching for augmented CT-CBCT”. In: *IPCAI 2018 - 9th International Conference on Information Processing in Computer-Assisted Interventions*. Berlin, Germany, June 2018. hal-01761538.

[288] Vincent Gaudillière, Gilles Simon, and Marie-Odile Berger. “Region-Based Epipolar and Planar Geometry Estimation in Low Textured Environments”. In: *ICIP 2018 - 25th IEEE International Conference on Image Processing*. Athens, Greece: IEEE, October 2018, pp. 898–902. DOI: 10.1109/ICIP.2018.8451244. hal-01802596.

[289] Michel Grediac, Benoît Blaysat, and Frédéric Sur. “Speckles and DIC or Checkerboards and LSA?” In: *SEM Annual Conference & Exposition on Experimental and Applied Mechanics*. Ed. by Luciano Lamberti, Ming-Tzer Lin, Cosme Furlong, Cesar Sciammarella, Phillip L. Reu, and Michael A Sutton. Vol. 3. Greenville, United States: Springer, June 2018, pp. 79–80. DOI: 10.1007/978-3-319-97481-1_9. hal-01896817.

[290] Claude-Pierre Jeannerod, Jean-Michel Muller, and Paul Zimmermann. “On various ways to split a floating-point number”. In: *ARITH 2018 - 25th IEEE Symposium on Computer Arithmetic*. Amherst (MA), United States: IEEE, June 2018, pp. 53–60. DOI: 10.1109/ARITH.2018.8464793. hal-01774587.

[291] Antoine Mahé, Cédric Pradalier, and Matthieu Geist. “Trajectory-control using deep system identification and model predictive control for drone control under uncertain load”. In: *2018 22nd International Conference on System Theory, Control and Computing (ICSTCC)*. Sinaia, Romania: IEEE, October 2018. DOI: 10.1109/ICSTCC.2018.8540719. hal-01927035.

[292] Khadija Musayeva, Fabien Lauer, and Yann Guermeur. “A sharper bound on the Rademacher complexity of margin multi-category classifiers”. In: *ESANN 2018*. Proceedings of the 26th European Symposium on Artificial Neural Networks, Computational Intelligence and Machine Learning (ESANN), Bruges, Belgium. Bruges, Belgium, April 2018, pp. 503–508. hal-03011325.

[293] Phuc Ngo, Nicolas Passat, Yukiko Kenmochi, and Isabelle Debled-Rennesson. “Convexity invariance of voxel objects under rigid motions”. In: *International Conference on Pattern Recognition (ICPR)*. Beijing, China, 2018, pp. 1157–1162. DOI: 10.1109/ICPR.2018.8545023. hal-01695388.

[294] Fabien Pierre. “Exemplar-based face colorization using image morphing”. In: *SIAM Conference on IMAGING SCIENCE*. Bologne, Italy, June 2018. hal-01824827.

[295] Ismini Psychoula, Erinc Merdivan, Deepika Singh, Liming Chen, Feng Chen, Sten Hanke, Johannes Kropf, Andreas Holzinger, and Matthieu Geist. “A Deep Learning Approach for Privacy Preservation in Assisted Living”. In: *2018 IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom Workshops)*. Athens, Greece: IEEE, March 2018, pp. 710–715. DOI: 10.1109/PERCOMW.2018.8480247. hal-03081669.

[296] Nicolas Ray, Dmitry Sokolov, Maxence Reberol, Franck Ledoux, and Bruno Lévy. “Hex-dominant meshing: mind the gap!” In: *SPM 2018 - International Conference on Solid and Physical Modeling*. Bilbao, Spain, June 2018. hal-01927557.

[297] Igor Ryadchikov, Dmitry Sokolov, Andrei Biryuk, Semyon Sechenev, Alexander Svidlov, Pavel Volkodav, Yury Mamelin, Kirill Popko, and Evgeny Nikulchev. “Stabilization of a hopper with three reaction wheels”. In: *ISR 2018 - 50th International Symposium on Robotics*. Munich, Germany, June 2018. hal-01927624.

[298] Michael Scott and Aurore Guillevic. “A New Family of Pairing-Friendly elliptic curves”. In: *International Workshop on the Arithmetic of Finite Fields - WAIFI*. Ed. by Lilya Budaghyan and Francisco Rodriguez-Henríquez. Vol. 11321. LNCS. Lilya Budaghyan and Tor Helleseth. Bergen, Norway: Springer, June 2018, pp. 43–57. DOI: 10.1007/978-3-030-05153-2_2. hal-01875361.

[299] Gilles Simon, Antoine Fond, and Marie-Odile Berger. “A-Contrario Horizon-First Vanishing Point Detection Using Second-Order Grouping Laws”. In: *ECCV 2018 - European Conference on Computer Vision*. Munich, Germany, September 2018, pp. 323–338. hal-01865251.

[300] Frédéric Sur, Benoît Blaysat, and Michel Grediac. “Speckle Image Rendering for DIC Performance Assessment”. In: *SEM Annual Conference & Exposition on Experimental and Applied Mechanics*. Ed. by Luciano Lamberti, Ming-Tzer Lin, Cosme Furlong, Cesar Sciammarella, Phillip L. Reu, and Michael A Sutton. Vol. 3. Greenville, United States: Springer, June 2018, pp. 75–77. DOI: 10.1007/978-3-319-97481-1_8. hal-01896811.

[301] Jose Terius-Padron, Georgios Kapidis, Sarah Fallmann, Erinc Merdivan, Sten Hanke, Rebeca Garcia-Betances, and Maria Fernanda Cabrera-Umpierrez. “Towards Self-management of Chronic Diseases in Smart Homes : Physical Exercise Monitoring for Chronic Obstruction Pulmonary Disease Patients”. In: *2018 IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom Workshops)*. Athens, Greece: IEEE, March 2018, pp. 776–781. DOI: 10.1109/PERCOMW.2018.8480163. hal-03081677.

[302] Elena Andreeva, Virginie Lallemand, Antoon Purnal, Reza Reyhanitabar, Arnab Roy, and Damian Vizár. “Forkcipher: A New Primitive for Authenticated Encryption of Very Short Messages”. In: *ASIACRYPT 2019 - 25th Annual International Conference on the Theory and Application of Cryptology and Information Security*. Advances in Cryptology – ASIACRYPT 2019. This is an extended version of the article with the same title accepted at Asiacrypt 2019. Kobe, Japan, December 2019, pp. 153–182. DOI: 10.1007/978-3-030-34621-8_6. hal-02388234.

[303] Jean-Daniel Boissonnat, Olivier Devillers, Kunal Dutta, and Marc Glisse. “Randomized incremental construction of Delaunay triangulations of nice point sets”. In: *ESA 2019 - 27th Annual European Symposium on Algorithms*. Munich, Germany, September 2019. DOI: 10.4230/LIPIcs.ESA.2019.22. hal-02185566.

[304] Nicola Cacciani, Elisabeth Larsson, Igor Tominec, and Pierre-Frédéric Villard. "Meshfree Simulation of Human Respiratory Muscles". In: *CSE 19 - SIAM Conference on Computational Science and Engineering*. Spokane, United States, February 2019. hal-02057413.

[305] Luca De Feo, Simon Masson, Christophe Petit, and Antonio Sanso. "Verifiable Delay Functions from Supersingular Isogenies and Pairings". In: *Advances in Cryptology - ASIACRYPT 2019 - 25th International Conference on the Theory and Application of Cryptology and Information Security*. Vol. 1. Advances in Cryptology - ASIACRYPT 2019. Kobe, Japan, December 2019, pp. 248–277. DOI: 10.1007/978-3-030-34578-5_10. hal-02388349.

[306] Patrick Derbez, Virginie Lallemand, and Aleksei Udovenko. "Cryptanalysis of SKINNY in the Framework of the SKINNY 2018-2019 Cryptanalysis Competition". In: *SAC 2019 - Selected Areas in Cryptography*. Waterloo, Canada, August 2019. hal-02388239.

[307] Jérémie Detrey and Laurent Imbert. "Breaking randomized mixed-radix scalar multiplication algorithms". In: *LATINCRYPT 2019 - 6th International Conference on Cryptology and Information Security in Latin America*. Vol. 11774. Lecture Notes in Computer Science. Santiago de Chile, Chile, October 2019, pp. 24–39. DOI: 10.1007/978-3-030-30530-7_2. lirmm-02309203.

[308] Sény Diatta, Guillaume Moroz, and Marc Pouget. "Reliable Computation of the Singularities of the Projection in R3 of a Generic Surface of R4". In: *MACIS 2019 - Mathematical Aspects of Computer and Information Sciences*. Gebze-Istanbul, Turkey, November 2019. hal-02406758.

[309] Eric Domenjoud, Bastien Laboureix, and Laurent Vuillon. "Facet Connectedness of Arithmetic Discrete Hyperplanes with Non-Zero Shift". In: *DGCI 2019: 21st International Conference on Discrete Geometry for Computer Imagery*. Discrete Geometry for Computer Imagery. Paris, France, March 2019, pp. 38–50. DOI: 10.1007/978-3-030-14085-4_4. hal-02316870.

[310] Philippe Even, Phuc Ngo, and Bertrand Kerautret. "Thick Line Segment Detection with Fast Directional Tracking". In: *ICIAP 2019 -20th International Conference on Image Analysis and Processing*. Ed. by E. Ricci et al. LNCS 11752. trento, Italy: Springer, September 2019, pp. 159–170. DOI: 10.1007/978-3-030-30645-8_15. hal-02189916.

[311] Vincent Gaudillière, Gilles Simon, and Marie-Odile Berger. "Camera Pose Estimation with Semantic 3D Model". In: *IROS 2019 - 2019 IEEE/RSJ International Conference on Intelligent Robots and Systems*. Macau, Macau SAR China, November 2019. DOI: 10.1109/IROS40897.2019.8968180. hal-02181962.

[312] Vincent Gaudillière, Gilles Simon, and Marie-Odile Berger. "Camera Relocalization with Ellipsoidal Abstraction of Objects". In: *ISMAR 2019 - 18th IEEE International Symposium on Mixed and Augmented Reality*. Beijing, China: IEEE, October 2019, pp. 19–29. DOI: 10.1109/ISMAR.2019.00017. hal-02170784.

[313] Xavier Goaoc, Andreas Holmsen, and Cyril Nicaud. "An experimental study of forbidden patterns in geometric permutations by combinatorial lifting". In: *35th International Symposium on Computational Geometry*. arXiv: 1903.03014. Portland, United States, 2019. DOI: 10.4230/LIPIcs.SoCG.2019.40. hal-02050539.

[314] Rémi Imbach, Marc Pouget, and Chee Yap. "Clustering Complex Zeros of Triangular System of Polynomials". In: *CASC 2019 - 21st International Workshop on Computer Algebra in Scientific Computing*. arXiv: 1806.10164. Moscow, Russia, August 2019. hal-01825708.

[315] Antoine Mahé, Antoine Richard, Benjamin Mouscadet, Cedric Pradalier, and Matthieu Geist. “Importance Sampling for Deep System Identification”. In: *19th International Conference on Advanced Robotics (ICAR)*. Belo Horizonte, Brazil, 2019. DOI: 10.1109/ICAR46387.2019.8981590. hal-02278171.

[316] Erinc Merdivan, Anastasios Vafeiadis, Dimitrios Kalatzis, Sten Hanke, Joahannes Kroph, Konstantinos Votis, Dimitrios Giakoumis, Dimitrios Tzovaras, Liming Chen, Raouf Hamzaoui, and Matthieu Geist. “Image-Based Text Classification using 2D Convolutional Neural Networks”. In: *2019 IEEE SmartWorld, Ubiquitous Intelligence & Computing, Advanced & Trusted Computing, Scalable Computing & Communications, Cloud & Big Data Computing, Internet of People and Smart City Innovation (SmartWorld/SCALCOM/UIC/ATC/CBDCom/IOP/SCI)*. Leicester, United Kingdom: IEEE, August 2019, pp. 144–149. DOI: 10.1109/SmartWorld-UIC-ATC-SCALCOM-IOP-SCI.2019.00066. hal-03081713.

[317] Thomas Mouzon, Fabien Pierre, and Marie-Odile Berger. “Joint CNN and Variational Model for Fully-automatic Image Colorization”. In: *SSVM 2019 - Seventh International Conference on Scale Space and Variational Methods in Computer Vision*. Scale Space and Variational Methods in Computer Vision. Hofgeismar, Germany, June 2019, pp. 535–546. hal-02059820.

[318] Phuc Ngo. “A discrete approach for polygonal approximation of irregular noise contours”. In: *CAIP 2019 - Computer Analysis of Images and Patterns*. Vol. 11678. LNCS. Salerno, Italy, September 2019, pp. 433–446. DOI: 10.1007/978-3-030-29888-3_35. hal-02163606.

[319] Daryna Panicheva, Pierre-Frédéric Villard, and Marie-Odile Berger. “Toward an automatic segmentation of mitral valve chordae”. In: *SPIE Medical Imaging*. Ed. by Barjor Gimi and Andrzej Kro. Vol. 10953. SPIE. San Diego, United States, February 2019, pp. 1095315–1095323. DOI: 10.1117/12.2511943. hal-02050846.

[320] Daryna Panicheva, Pierre-Frédéric Villard, Peter Hammer, and Marie-Odile Berger. “Physically-coherent Extraction of Mitral Valve Chordae”. In: *International Conference in Computing in Cardiology*. Vol. 46. Proceedings of Computers in Cardiology. Singapore, Singapore: IEEE Engineering in Medicine and Biology Society, September 2019, p. 4. hal-02368810.

[321] Nicolas Passat, Yukiko Kenmochi, Phuc Ngo, and Kacper Pluta. “Rigid motions in the cubic grid: A discussion on topological issues”. In: *Discrete Geometry for Computer Imagery (DGCI)*. Vol. 11414. Lecture Notes in Computer Science. Marne-la-Vallée, France: Springer, 2019, pp. 127–140. DOI: 10.1007/978-3-030-14085-4_11. hal-01892944.

[322] Sandra Rasoamiaramanana, Gilles Macario-Rat, and Marine Minier. “White-Box Traitor-Tracing from Tardos Probabilistic Codes”. In: *SecITC 2019: Innovative Security Solutions for Information Technology and Communications*. Bucharest, Romania, November 2019, pp. 125–141. DOI: 10.1007/978-3-030-41025-4_9. hal-02944663.

[323] Arthur Renaudeau, François Lauze, Fabien Pierre, Jean-François Aujol, and Jean-Denis Durou. “Alternate Structural-Textural Video Inpainting for Spot Defects Correction in Movies”. In: *SSVM 2019 - Seventh International Conference on Scale Space and Variational Methods in Computer Vision*. Hofgeismar, Germany, June 2019. hal-02433997.

[324] Igor Ryadchikov, Stanislav Aranovskiy, Evgeny Nikulchev, Jian Wang, and Dmitry Sokolov. “Differentiator-based velocity observer with sensor bias estimation: an inverted pendulum case study”. In: *11th IFAC Symposium on Nonlinear Control Systems*. Vienna, Austria, September 2019. hal-02383471.

[325] Deng Tang, Bimal Mandal, and Subhamoy Maitra. "Vectorial Boolean Functions with Very Low Differential-Linear Uniformity Using Maiorana-McFarland Type Construction". In: *INDOCRYPT 2019 - The 20th International Conference on Cryptology in India*. Hyderabad, India, December 2019. DOI: 10.1007/978-3-030-35423-7_17. hal-02374286.

[326] Stanislav Aranovskiy, Denis Efimov, Dmitry Sokolov, Jian Wang, Igor Ryadchikov, and Alexey Bobtsov. "State estimation for a locally unobservable parameter-varying system: one gradient-based and one switched solutions". In: *IFAC 2020 - 21rst IFAC World Congress*. Berlin, Germany, July 2020. hal-02634576.

[327] Victor Blanchi, Etienne Corman, Nicolas Ray, and Dmitry Sokolov. "Global parametrization based on Ginzburg-Landau functional". In: *NUMGRID 2020 - Numerical Geometry, Grid Generation and Scientific Computing*. Moscow/Virtual, Russia, November 2020. hal-02985282.

[328] Fabrice Boudot, Pierrick Gaudry, Aurore Guillevic, Nadia Heninger, Emmanuel Thomé, and Paul Zimmermann. "Comparing the difficulty of factorization and discrete logarithm: a 240-digit experiment". In: *Advances in Cryptology – CRYPTO 2020*. Ed. by Daniele Micciancio and Thomas Ristenpart. Vol. 12171. Lecture Notes in Computer Science. Santa Barbara CA, United States: Springer, August 2020, pp. 62–91. DOI: 10.1007/978-3-030-56880-1_3. hal-02863525.

[329] Véronique Cortier, Pierrick Gaudry, and Quentin Yang. "How to fake zero-knowledge proofs, again". In: *E-Vote-Id 2020 - The International Conference for Electronic Voting*. Bregenz / virtual, Austria, 2020. hal-02928953.

[330] Gabrielle De Micheli, Pierrick Gaudry, and Cécile Pierrot. "Asymptotic complexities of discrete logarithm algorithms in pairing-relevant finite fields". In: *CRYPTO 2020 - 40th Annual International Cryptology Conference*. Ed. by Daniele Micciancio and Thomas Ristenpart. Vol. 12171. Lecture Notes in Computer Science. Santa Barbara / Virtual, United States: Springer, August 2020, pp. 32–61. hal-02871839.

[331] Gabrielle De Micheli, Rémi E. Piau, and Cécile Pierrot. "A Tale of Three Signatures: practical attack of ECDSA with wNAF". In: *AFRICACRYPT 2020*. Ed. by Youssef A. Nitaj A. Vol. 12174. Lecture Notes in Computer Science. Cairo, Egypt, July 2020, pp. 361–381. DOI: 10.1007/978-3-030-51938-4_18. hal-02393302.

[332] Patrick Derbez, Paul Huynh, Virginie Lallemand, María Naya-Plasencia, Léo Perrin, and André Schrottenloher. "Cryptanalysis Results on Spook: Bringing Full-round Shadow-512 to the Light". In: *CRYPTO 2020 - 40th Annual International Cryptology Conference*. Ed. by Daniele Micciancio and Thomas Ristenpart. Vol. 12172. Lecture Notes in Computer Science. Santa Barbara / Virtual, United States, August 2020, pp. 359–388. DOI: 10.1007/978-3-030-56877-1_13. hal-02944908.

[333] Vincent Despré, Jean-Marc Schlenker, and Monique Teillaud. "Flipping Geometric Triangulations on Hyperbolic Surfaces". In: *SoCG 2020 - 36th International Symposium on Computational Geometry*. Zurich, Switzerland, June 2020. DOI: 10.4230/LIPIcs.SoCG.2020.35. hal-02886493.

[334] Denis Efimov, Stanislav Aranovskiy, Emilia Fridman, Dmitry Sokolov, Jian Wang, and Alexey Bobtsov. "Adaptive stabilization by delay with biased measurements". In: *IFAC 2020 - 21st IFAC World Congress*. Berlin, Germany, July 2020. hal-02634582.

[335] Youssef El Housni and Aurore Guillevic. "Optimized and secure pairing-friendly elliptic curves suitable for one layer proof composition". In: *CANS 2020 - 19th International Conference on Cryptology and Network Security*. Ed. by Haya Shulman and Serge Vaudenay. Vol. 12579. Lecture Notes in Computer Science. Vienna / Virtual, Austria: Springer, December 2020, pp. 259–279. DOI: 10.1007/978-3-030-65411-5_13. hal-02962800.

[336] Philippe Even and Phuc Ngo. "Live extraction of curvilinear structures from lidar raw data". In: *XXIV ISPRS Congress*. Vol. V-2-2020. IAPRS Annals of Photogrammetry, Remote Sensing and Spatial Information Sciences. Nice, France, 2020, pp. 211–219. DOI: 10.5194/isprs-annals-V-2-2020-211-2020. hal-02872075.

[337] Vincent Gaudillière, Gilles Simon, and Marie-Odile Berger. "Perspective-2-Ellipsoid: Bridging the Gap Between Object Detections and 6-DoF Camera Pose". In: *IROS 2020 – 2020 IEEE/RSJ International Conference on Intelligent Robots and Systems*. Las Vegas, United States, October 2020. hal-02889146.

[338] Pierrick Gaudry and Alexander Golovnev. "Breaking the encryption scheme of the Moscow Internet voting system". In: *Financial Cryptography and Data Security*. Ed. by Joseph Bonneau and Nadia Heninger. arXiv: 1908.05127 - This work is a merger of arXiv:1908.09170 and arXiv:1908.05127. Kota Kinabalu, Malaysia: Springer, 2020, pp. 32–49. DOI: 10.1007/978-3-030-51280-4_3. hal-02266264.

[339] Xavier Goaoc and Emo Welzl. "Convex Hulls of Random Order Types". In: *SoCG 2020 - 36th International Symposium on Computational Geometry*. Ed. by Sergio Cabello and Danny Z. Chen. Vol. 164. 36th International Symposium on Computational Geometry (SoCG 2020). arXiv: 2003.08456 - Best paper award. Zürich / Virtual, Switzerland, June 2020, 49:1–49:15. DOI: 10.4230/LIPIcs.SoCG.2020.49. hal-02879289.

[340] Aurore Guillevic. "A short-list of pairing-friendly curves resistant to Special TNFS at the 128-bit security level". In: *PKC 2020 - IACR International Conference on Practice and Theory of Public-Key Cryptography*. Ed. by Aggelos Kiayias. Vol. 12111. LNCS. https://www.iacr.org/docs/pub_2013-16.html This paper is the IACR version. It can be made freely available on the homepages of authors, on their employer's institutional page, and in non-commercial archival repositories such as the Cryptology ePrint Archive, ArXiv/CoRR, HAL, etc. Edinburgh, United Kingdom: Springer, June 2020, pp. 535–564. DOI: 10.1007/978-3-030-45388-6_19. hal-02396352.

[341] Fabien Lauer. "Risk Bounds for Learning Multiple Components with Permutation-Invariant Losses". In: *23rd International Conference on Artificial Intelligence and Statistics (AISTATS)*. Vol. PMLR: Volume 108. Proceedings of the 23rd International Conference on Artificial Intelligence and Statistics (AISTATS), Palermo, Italy. arXiv: 1904.07594. Palermo, Italy, 2020. hal-02100779.

[342] Louis Massucci, Fabien Lauer, and Marion Gilson. "Structural risk minimization for switched system identification". In: *59th IEEE Conference on Decision and Control, CDC 2020*. Proceedings of the 59th IEEE Conference on Decision and Control (CDC). Jeju Island, South Korea, December 2020. hal-02942279.

[343] Erinc Merdivan, Sten Hanke, and Matthieu Geist. "Modified Actor-Critics". In: *AAMAS2020 - International Conference on Autonomous Agents and MultiAgent Systems*. virtual, New Zealand, May 2020. hal-03081704.

[344] Phuc Ngo. "Digital hyperplane fitting". In: *20th International Workshop on Combinatorial Image Analysis (IWCIA)*. Vol. 12148. LNCS. Novi Sad, Serbia, July 2020, pp. 164–180. DOI: 10.1007/978-3-030-51002-2_12. hal-02586206.

[345] Georg Osang, Mael Rouxel-Labbé, and Monique Teillaud. "Generalizing CGAL Periodic Delaunay Triangulations". In: *ALGO 2020 - 28th European Symposium on Algorithms*. Best Paper Award (Track B: Engineering and Applications). Pise / Virtual, Italy, September 2020, 75:1–75:17. DOI: 10.4230/LIPIcs.ESA.2020.75. hal-02923439.

[346] Sandra Rasoamiaramanana, Marine Minier, and Gilles Macario-Rat. "A White-Box Encryption Scheme using Physically Unclonable Functions". In: *17th International Conference on Security and Cryptography*. Lieusaint - Paris, France: SCITEPRESS - Science and Technology Publications, July 2020, pp. 279–286. DOI: 10.5220/0009781002790286. hal-02944654.

[347] Arthur Renaudeau, Travis Seng, Axel Carlier, Fabien Pierre, François Lauze, Jean-François Aujol, and Jean-Denis Durou. "Learning Defects in Old Movies from Manually Assisted Restoration". In: *ICPR 2020 - 25th International Conference on Pattern Recognition*. Milan / Virtual, Italy, September 2020. hal-02965296.

[348] Dmitry Sokolov, Stanislav Aranovskiy, Alexander A Gusev, and Igor Ryadchikov. "Experimental comparison of velocity estimators for a control moment gyroscope inverted pendulum". In: *AMC 2020 - 16th IEEE International Workshop on Advanced Motion Control*. Kristiansand / Virtual, Norway, September 2020. hal-02313600.

[349] Matthieu Zins, Gilles Simon, and Marie-Odile Berger. "3D-Aware Ellipse Prediction for Object-Based Camera Pose Estimation". In: *3DV 2020 - International Virtual Conference on 3D Vision*. Fukuoka / Virtual, Japan, November 2020. hal-02975379.

Secondary International Conferences

[350] Thiéry Constant, Van Tho Nguyen, Estelle Noyer, Frédéric Mothe, Francis Colin, Alexandre Piboule, Bertrand Kerautret, and Isabelle Debled-Rennesson. "Towards wood quality assessment of standing trees fromT-LiDAR: What's Going on in France?" In: *8th meeting of IUFRO Working Parties 5.01.04 and 3.04.02: "Modelling Wood Quality, Supply and Value Chain Networks"*. Quebec, Canada, June 2016. hal-02793063.

[351] Samuel Hornus, Sylvain Lefebvre, Jérémie Dumas, and Frédéric Claux. "Tight printable enclosures and support structures for additive manufacturing". In: *Eurographics Workshop on Graphics for Digital Fabrication*. Ed. by Asla Medeiros e Sá, N. Pietroni, and K. Rodriguez Echavarria. Lisbonne, Portugal: The Eurographics Association, May 2016. hal-01399931.

[352] Damien Jamet, Xavier Provençal, and Lafrenière Nadia. "Generation of Digital Planes Using Generalized Continued-Fractions Algorithms". In: *19th IAPR International Conference on Discrete Geometry for Computer Imagery*. Ed. by Springer. Vol. 9647. Discrete Geometry for Computer Imagery 19th IAPR International Conference, DGCI 2016, Nantes, France, April 18-20, 2016. Proceedings. Nantes, France, April 2016, pp. 45–56. DOI: 10.1007/978-3-319-32360-2_4. hal-01364622.

[353] Bertrand Kerautret, Miguel Colom, and Pascal Monasse. "Preface of the proceedings of the First International Workshop on Reproducible Research in Pattern Recognition, RRPR 2016". In: *First International Workshop on Reproducible Research in Pattern Recognition, RRPR 2016*. Mexico, Mexico, 2016. hal-01616745.

[354] Bertrand Kerautret, Adrien Krähenbühl, Isabelle Debled-Rennesson, and Jacques-Olivier Lachaud. "Analyse géométrique d'objets tubulaires 3D basée sur l'accumulation de normales". In: *RFIA 2016 - Reconnaissance des Formes et l'Intelligence Artificielle*. Clermont Ferrand, France, June 2016. hal-01359558.

[355] Bertrand Kerautret, Adrien Krähenbühl, Isabelle Debled-Rennesson, and Jacques-Olivier Lachaud. "On the Implementation of Centerline Extraction Based on Confidence Vote in Accumulation Map". In: *RRPR 2016 1st Workshop on Reproducible Research in Pattern Recognition*. Vol. 10214. RRPR: International Workshop on Reproducible Research in Pattern Recognition. Bertrand Kerautret and Miguel Colom and Pascal Monasse. Cancùn, Mexico, December 2016, pp. 116–130. DOI: 10.1007/978-3-319-56414-2_9. hal-01571434.

[356] Adrien Krähenbühl, Jean-Romain Roussel, Bertrand Kerautret, Isabelle Debled-Rennesson, Frédéric Mothe, and Fleur Longuetaud. "Robust Knot Segmentation by Knot Pith Tracking in 3D Tangential Images". In: *ICCVG 2016*. Vol. 9972. Computer Vision and Graphics. Warsaw, Poland: Springer International Publishing AG, September 2016, pp. 581–593. DOI: 10.1007/978-3-319-46418-3_52. hal-01421205.

[357] Phuc Ngo, Hayat Nasser, and Isabelle Debled-Rennesson. "A discrete approach for decomposing noisy digital contours into arcs and segments". In: *ACCV Workshop 2016*. ACCV 2016 Workshops. Taipei, Taiwan, November 2016. DOI: 10.1007/978-3-319-54427-4_36. hal-01375089.

[358] Phuc Ngo, Hayat Nasser, Isabelle Debled-Rennesson, and Bertrand Kerautret. "An algorithm to decompose noisy digital contours". In: *RRPR 2016- 1st Workshop on Reproducible Research in Pattern Recognition*. Cancun, Mexico, December 2016. DOI: 10.1007/978-3-319-56414-2_10. hal-01415925.

[359] Tim Reiner and Sylvain Lefebvre. "Interactive Modeling of Support-free Shapes for Fabrication". In: *EUROGRAPHICS*. Proceedings of EUROGRAPHICS (short papers). Lisbonne, Portugal, May 2016. hal-01401470.

[360] Yann Guermeur. "Rademacher complexity of margin multi-category classifiers". In: *12th International Workshop on Self-Organizing Maps and Learning Vector Quantization, Clustering and Data Visualization (WSOM+)*. Nancy, France, June 2017. hal-02982728.

[361] Sofiane Lagraa, Jerome Francois, Abdelkader Lahmadi, Marine Minier, Christian Hammerschmidt, and Radu State. "BotGM: Unsupervised Graph Mining to Detect Botnets in Traffic Flows". In: *CSNet 2017 - 1st Cyber Security in Networking Conference*. Rio de Janeiro, Brazil, October 2017. hal-01636480.

[362] Khadija Musayeva, Fabien Lauer, and Yann Guermeur. "Metric entropy and Rademacher complexity of margin multi-category classifiers". In: *26th International Conference on Artificial Neural Networks (ICANN)*. Vol. 10614 of LNCS. Proceedings of the 26th International Conference on Artificial Neural Networks (ICANN) 2. Alghero, Italy, September 2017, p. 767. hal-03011347.

[363] Isabelle Debled-Rennesson, Philippe Févotte, Monique Grandbastien, David Langlois, and Hélène Tanoh. "La formation des professeurs de la spécialité ISN dans l'Académie de Nancy-Metz – Récit et analyse de six ans d'expérience". In: *Didapro 7 – DidaSTIC. De 0 à 1 ou l'heure de l'informatique à l'école*. Lausanne, Switzerland, February 2018. hal-01753067.

[364] Matthijs Ebbens, Iordan Iordanov, Monique Teillaud, and Gert Vegter. "Delaunay triangulations of regular hyperbolic surfaces". In: *9th International Conference on Curves and Surfaces*. Arcachon, France, June 2018. hal-01801136.

[365] Matthijs Ebbens, Iordan Iordanov, Monique Teillaud, and Gert Vegter. "Systole of regular hyperbolic surfaces with an application to Delaunay triangulations". In: *9th International Conference on Curves and Surfaces*. Arcachon, France, June 2018. hal-01803443.

[366] Samuel Hornus and Sylvain Lefebvre. "Iterative carving for self-supporting 3D printed cavities". In: *Eurographics 2018 - Short Papers*. Delft, Netherlands, April 2018. hal-01764291.

[367] Phuc Ngo, Yukiko Kenmochi, Nicolas Passat, and Isabelle Debled-Rennesson. "Discrete regular polygons for digital shape rigid motion via polygonization". In: *International Workshop on Reproducible Research on Pattern Recognition (RRPR)*. Vol. 11455. Lecture Notes in Computer Science. Beijing, China, 2018, pp. 55–70. DOI: 10.1007/978-3-030-23987-9_4. hal-01853795.

[368] Ted Selker and Enka Blanchard. "Improving voting technology is hard: the trust-legitimacy-participation loop and related problems". In: *8th International Workshop on Socio-Technical Aspects in Security and Trust- STAST'18*. San Juan, Puerto Rico, December 2018. hal-02560643.

[369] Cédric Zanni, Frédéric Claux, and Sylvain Lefebvre. "HCSG: Hashing for real-time CSG modeling". In: *Proceedings of the ACM SIGGRAPH Symposium on Interactive 3D Graphics and Games*. Montreal, Canada, May 2018. DOI: 10.1145/3203198. hal-01792866.

[370] Enka Blanchard, Xavier Coquand, and Ted Selker. "Moving to client-side hashing for online authentication". In: *9th International Workshop on Socio-Technical Aspects in SecuriTy*. Proceedings of the 9th International Workshop on Socio-Technical Aspects in SecuriTy. Luxembourg Ville, Luxembourg, September 2019. hal-02560695.

[371] Enka Blanchard and Siargey Kachanovich. "A note on the inflating enclosing ball problem". In: *Bordeaux Graph Workshop*. Bordeaux Graph Workshop 2019. Bordeaux, France, October 2019. hal-02549818.

[372] Enka Blanchard and Siargey Kachanovich. "Counting authorised paths in constrained control-flow graphs". In: *Bordeaux Graph Workshop*. Bordeaux Graph Workshop 2019. Bordeaux, France, October 2019. hal-02549827.

[373] Nikola K Blanchard. "Password typo correction using discrete logarithms". In: *IC-CSCE 2019 - 8th International Conference on Computer Science and Communication Engineering*. International Conference on Business, Technology and Innovation. Pristine, Kosovo, October 2019. hal-02550719.

[374] Nikola K Blanchard and Olivier Pivot. "A proposal for the New Shape Prize: CIVICS: Changing Incentives for Voters in International Cooperation through Sampling". In: *VIII International Smolny Student Conference 2019*. Saint Petersburg, Russia, April 2019. hal-02273387.

[375] Kevin Buchin, Pedro M. M. de Castro, Olivier Devillers, and Menelaos Karavelas. "Hardness results on Voronoi, Laguerre and Apollonius diagrams". In: *CCCG 2019 - Canadian Conference on Computational Geometry*. Edmonton, Canada, August 2019. hal-02186693.

[376] Rémi Decelle and Ehsaneddin Jalilian. "Neural Networks for Cross-Section Segmentation in Raw Images of Log Ends". In: *Fourth IEEE International Conference on Image Processing, Applications and Systems (IPAS 2020)*. Gênes, Italy, September 2019. hal-03058259.

[377] Rémi Decelle, Phuc Ngo, Isabelle Debled-Rennesson, Frederic MOTHE, and Fleur Longuetaud. "A new algorithm to automatically detect the pith on rough log-end images". In: *21st International Nondestructive Testing and Evaluation (NDTE) of Wood Symposium*. Freiburg, Germany, September 2019. hal-02275651.

[378] Olivier Devillers and Charles Duménil. "A Poisson sample of a smooth surface is a good sample". In: *EuroCG 2019 - 35th European Workshop on Computational Geometry*. Utrecht, Netherlands, March 2019. hal-02394144.

[379] Matthijs Ebbens, Iordan Iordanov, Monique Teillaud, and Gert Vegter. "Delaunay triangulations of symmetric hyperbolic surfaces". In: *EuroCG 2019 - 35th European Workshop on Computational Geometry*. Utrecht, Netherlands, March 2019. hal-02940717.

[380] Leila R Gabasova, B Schmitt, Nikola K Blanchard, W.M. Grundy, C. B. Olkin, J.R. R Spencer, L.A. Young, K. Ennico, H.A. Weaverc, and S.A. Stern. "Pluto surface composition from spectral model inversion with metaheuristics". In: *EPSC-DPS Joint Meeting 2019*. Geneve, Switzerland, September 2019. hal-03099265.

[381] George Krait, Sylvain Lazard, Guillaume Moroz, and Marc Pouget. "Numerical Algorithm for the Topology of Singular Plane Curves". In: *EuroCG 2019 - 35th European Workshop on Computational Geometry*. Utrecht, Netherlands, March 2019. hal-02294028.

[382] Viviane Ledoux and Guillaume Moroz. "Evaluation of Chebyshev polynomials on intervals and application to root finding". In: *Mathematical Aspects of Computer and Information Sciences 2019*. arXiv: 1912.05843. Gebze, Turkey, November 2019. hal-02405752.

[383] Stanislav Aranovskiy, Igor Ryadchikov, Nikita Mikhalkov, Dmitry Kazakov, Alexey Simulin, and Dmitry Sokolov. "Scissored pair control moment gyroscope inverted pendulum". In: *14th International Symposium "Intelligent Systems - 2020"*. Moscow, Russia, December 2020. hal-02985412.

[384] Enka Blanchard and Ted Selker. "Origami voting: a non-cryptographic approach to transparent ballot verification". In: *FC 2020 - 5th Workshop on Advances in Secure Electronic Voting*. Financial Cryptography and Data Security: FC 2020 International Workshops. Kota Kinabalu, Malaysia, February 2020. hal-02550738.

[385] Enka Blanchard, Ted Selker, and Florentin Waligorski. "Towards an Empirical Cost Model for Mental Password Algorithms". In: *CHI Conference on Human Factors in Computing Systems*. Extended Abstracts of the 2020 CHI Conference on Human Factors in Computing Systems. Honolulu, United States, April 2020. DOI: 10.1145/3334480.3382990. hal-02560611.

[386] Prosenjit Bose, Jean-Lou De Carufel, and Olivier Devillers. "Expected Complexity of Routing in Θ_6 and Half-Θ_6 Graphs". In: *EuroCG 2020 - 36th European Workshop on Computational Geometry*. Würzburg, Germany, March 2020. hal-02479502.

[387] Alfredo Cuzzocrea. "Advanced, Privacy-Preserving and Approximate Big Data Management and Analytics in Distributed Environments: What is Now and What is Next". In: *2020 IEEE 44th Annual Computers, Software, and Applications Conference (COMPSAC)*. Madrid, Spain, July 2020. DOI: 10.1109/compsac48688.2020.00-32. hal-03284139.

[388] Alfredo Cuzzocrea. “Multidimensional Clustering over Big Data : Models, Issues, Analysis, Emerging Trends”. In: *SSDBM 2020: 32nd International Conference on Scientific and Statistical Database Management*. Vienna, Austria, July 2020. DOI: 10.1145/3400903.3409117. hal-03284149.

[389] Alfredo Cuzzocrea. “Uncertainty and Imprecision in Big Data Management : Models, Issues, Paradigms, and Future Research Directions”. In: *ICCBDC '20: Proceedings of the 2020 4th International Conference on Cloud and Big Data Computing*. Virtual, United Kingdom, August 2020. DOI: 10.1145/3416921.3416943. hal-03284166.

[390] Alfredo Cuzzocrea, Vincenzo De Maio, and Edoardo Fadda. “Experimenting and Assessing a Distributed Privacy-Preserving OLAP over Big DataFramework: Principles, Practice, and Experiences”. In: *2020 IEEE 44th Annual Computers, Software, and Applications Conference (COMPSAC)*. Madrid, France, July 2020. DOI: 10.1109/compsac48688.2020.00-69. hal-03284134.

[391] Alfredo Cuzzocrea and Edoardo Fadda. “Data-Intensive Object-Oriented Adaptive Web Systems : Implementing and Experimenting the OO-XAHM Framework”. In: *MEDES'20 : the 12th International Conference on Management of Digital EcoSystems*. Virtual Event (Abu Dhabi), United Arab Emirates, November 2020. DOI: 10.1145/3415958.3433051. hal-03284179.

[392] Alfredo Cuzzocrea, Enzo Mumolo, Edoardo Fadda, and Marco Tessarotto. “Supporting Cyber Attack Detection via Non-Linear Analytic Prediction of IP Addresses: A Big Data Analytics Technique”. In: *26th International DMS Conference on Visualization and Visual Languages*. Pittsburgh, United States, July 2020. DOI: 10.18293/DMSVIVA2020-018. hal-03274631.

[393] Vincent Despré, Michaël Rao, and Stéphan Thomassé. “Testing Balanced Splitting Cycles in Complete Triangulations”. In: *Canadian Conference on Computational Geometry (CCCG 2020)*. Saskatchewan/Online, Canada, August 2020. DOI: 10.4230/LIPIcs. hal-03059811.

[394] Jimmy Etienne and Sylvain Lefebvre. “Procedural band patterns”. In: *Symposium on Interactive 3D Graphics and Games*. Symposium on Interactive 3D Graphics and Games. arXiv: 2003.01408. San Francisco, United States: Association for Computing Machinery, September 2020, pp. 1–7. DOI: 10.1145/3384382.3384522. hal-02457161.

[395] Andrey Getmanskiy, Semen Sechenev, Igor Ryadchikov, Alexander Gusev, Nikita Mikhalkov, Dmitry Kazakov, Alexey Simulin, and Dmitry Sokolov. “Real-time system architecture design practices”. In: *14th International Symposium "Intelligent Systems - 2020"*. Moscow, Russia, December 2020. hal-02984042.

[396] Benedikt Kolbe and Myfanwy Evans. “Enumerating tilings of triply-periodic minimal surfaces with rotational symmetries”. In: *EuroCG 2020- 36th European Workshop on Computational Geometry*. Würzburg, Germany, 2020. hal-02961522.

[397] Oxana Korzh, Ashish Sharma, Mikel Joaristi, Edoardo Serra, and Alfredo Cuzzocrea. “An Innovative Framework for Supporting Remote Sensing in Image Processing Systems via Deep Transfer Learning”. In: *2020 IEEE International Conference on Big Data (Big Data)*. Atlanta, United States, December 2020. DOI: 10.1109/bigdata50022.2020.9378306. hal-03284181.

[398] Antoine Moniot, Rohit Roy, Yann Guermeur, and Isaure Chauvot de Beauchêne. "Docking of RNA Hairpin on Protein Using a Fragment-Based Method". In: *JOBIM 2020 - Journées Ouvertes en Biologie, Informatique et Mathématiques*. Montpellier, France, June 2020. hal-02927185.

[399] Carlos Ordonez, Zhibo Chen, Alfredo Cuzzocrea, and Javier Garcia-Garcia. "An Intelligent Visual Big Data Analytics Framework for Supporting Interactive Exploration and Visualization of Big OLAP Cubes". In: *24th International Conference Information Visualisation (IV)*. Melbourne, Australia, September 2020. DOI: 10.1109/iv51561.2020.00074. hal-03284172.

[400] Ji-won Park and Otfried Cheong. "Smallest Universal Covers for Families of Triangles". In: *EuroCG 2020 - 36th European Workshop on Computational Geometry*. Würzburg, Germany, March 2020. hal-02972966.

[401] Gilles Simon and Salvatore Tabbone. "Generic Document Image Dewarping by Probabilistic Discretization of Vanishing Points". In: *ICPR 2020 - 25th International Conference on Pattern Recognition*. Milan / Virtual, Italy, September 2020. hal-02987029.

[402] Youssef Assis, Liang Liao, Fabien Pierre, René Anxionnat, and Erwan Kerrien. "An efficient data strategy for the detection of brain aneurysms from MRA with deep learning". In: *DALI 2021 - MICCAI workshop on Data Augmentation, Labeling, and Imperfections*. Vol. 13003. Deep Generative Models, and Data Augmentation, Labelling, and Imperfections. Strasbourg, France: Springer, September 2021, pp. 226–234. DOI: 10.1007/978-3-030-88210-5_22. hal-03391884.

[403] Ritam Bhaumik, Xavier Bonnetain, André Chailloux, Gaëtan Leurent, María Naya-Plasencia, André Schrottenloher, and Yannick Seurin. "QCB: Efficient Quantum-Secure Authenticated Encryption". In: *ASIACRYPT 2021 - 27th Annual International Conference on the Theory and Application of Cryptology and Information Security*. Ed. by Mehdi Tibouchi and Huaxiong Wang. Vol. 13090. Lecture Notes in Computer Science. Singapore / Virtual, Singapore: Springer International Publishing, December 2021, pp. 668–698. DOI: 10.1007/978-3-030-92062-3_23. hal-03516739.

[404] Xavier Bonnetain, Gaëtan Leurent, María Naya-Plasencia, and André Schrottenloher. "Quantum Linearization Attacks". In: *ASIACRYPT 2021 - 27th Annual International Conference on the Theory and Application of Cryptology and Information Security*. Ed. by Mehdi Tibouchi and Huaxiong Wang. Vol. 13090. Lecture Notes in Computer Science. Singapore / Virtual, Singapore: Springer International Publishing, December 2021, pp. 422–452. DOI: 10.1007/978-3-030-92062-3_15. hal-03516730.

[405] Hamid Boukerrou, Gilles Millérioux, and Marine Minier. "Hybrid architecture of LPV dynamical systems in the context of cybersecurity". In: *4th IFAC Workshop on Linear Parameter Varying Systems, LPVS 2021*. Milano, Italy, July 2021. hal-03292416.

[406] Christophe Cerisara and Alfredo Cuzzocrea. "Unsupervised Risk for Privacy". In: *IEEE BigData, Special Session on Privacy and Security of Big Data*. Orlando (virtual), United States, December 2021. hal-03407454.

[407] Antonio Coronato and Alfredo Cuzzocrea. "A Markovian Probabilistic Model for Risk Analysis and Forecasting in Big Healthcare Data Settings". In: *2021 IEEE 45th Annual Computers, Software, and Applications Conference (COMPSAC)*. Madrid, Spain: IEEE, July 2021, pp. 652–662. DOI: 10.1109/COMPSAC51774.2021.00095. hal-03352319.

[408] Alfredo Cuzzocrea. "Big Data Lakes: Models, Frameworks, and Techniques". In: *2021 IEEE International Conference on Big Data and Smart Computing (BigComp)*. Jeju Island, South Korea: IEEE, January 2021, pp. 1–4. DOI: 10.1109/BigComp51126.2021.00010. hal-03352268.

[409] Alfredo Cuzzocrea, Luca Camilotti, and Enzo Mumolo. "A Novel Framework for Supporting Mobile Object Self-Localization via Emerging Artificial Intelligence Tools". In: *27th International DMS Conference on Visualization and Visual Languages*. KSIR Virtual Conference Center, United States, June 2021. hal-03352346.

[410] Alfredo Cuzzocrea, Luca Camilotti, and Enzo Mumolo. "An Innovative Monocular Mobile Object Self-localization Approach Based on Ceiling Vision". In: *International Conference on Advanced Information Networking and Applications*. Toronto, Canada, May 2021, pp. 713–730. DOI: 10.1007/978-3-030-75100-5_61. hal-03352296.

[411] Alfredo Cuzzocrea and Edoardo Fadda. "Adaptive Complex Data-Intensive Web Systems via Object-oriented Paradigms: A Real-life Case Study". In: *23rd International Conference on Enterprise Information Systems*. Online Streaming, Portugal: SCITEPRESS - Science and Technology Publications, April 2021, pp. 565–572. DOI: 10.5220/0010481705650572. hal-03355056.

[412] Alfredo Cuzzocrea, Francesco Mercaldo, and Fabio Martinelli. "A Framework for Supporting Ransomware Detection and Prevention Based on Hybrid Analysis". In: *ICCSA 2021: Computational Science and Its Applications –*. Cagliari, Italy, September 2021, pp. 16–27. DOI: 10.1007/978-3-030-86970-0_2. hal-03352387.

[413] Alfredo Cuzzocrea, Francesco Mercaldo, and Fabio Martinelli. "A Machine-Learning-Based Framework for Supporting Malware Detection and Analysis". In: *ICCSA 2021: Computational Science and Its Applications – ICCSA 2021*. Cagliari, Italy, September 2021, pp. 353–365. DOI: 10.1007/978-3-030-86970-0_25. hal-03352391.

[414] Gabrielle De Micheli, Pierrick Gaudry, and Cécile Pierrot. "Lattice Enumeration for Tower NFS: a 521-bit Discrete Logarithm Computation". In: *ASIACRYPT 2021 - 27th Annual International Conference on the Theory and Application of Cryptology and Information Security*. Ed. by M. Tibouchi and H. Wang. Vol. 13090. ASIACRYPT. Virtual, Singapore: Springer, December 2021, pp. 67–96. DOI: 10.1007/978-3-030-92062-3_3. hal-03242324.

[415] Rémi Decelle, Phuc Ngo, Isabelle Debled-Rennesson, Frédéric Mothe, and Fleur Longuetaud. "Pith Estimation on Tree Log End Images". In: *Reproducible Research on Pattern Recognition (RRPR)*. Vol. LNCS 12636. Milan, Italy, 2021, pp. 101–120. DOI: 10.1007/978-3-030-76423-4_7. hal-03006060.

[416] Rémi Decelle, Phuc Ngo, Isabelle Debled-Rennesson, Frédéric F. Mothe, and Fleur Longuetaud. "Digital Straight Segment Filter for Geometric Description". In: *DGMM 2021 - IAPR International Conference on Discrete Geometry and Mathematical Morphology*. Vol. LNCS 12708. Uppsala, Sweden, May 2021, pp. 255–268. DOI: 10.1007/978-3-030-76657-3_18. hal-03144152.

[417] Alix Delannoy, Antoine Moniot, Yann Guermeur, and Isaure Chauvot de Beauchêne. "Feature extraction for the clustering of small 3D structures: application to RNA fragments". In: *JOBIM 2021 - Journées Ouvertes en Biologie, Informatique et Mathématiques*. Paris/Virtual, France, July 2021, pp. 1–6. hal-03540927.

[418] Stéphanie Delaune, Patrick Derbez, Paul Huynh, Marine Minier, Victor Mollimard, and Charles Prud'Homme. "Efficient Methods to Search for Best Differential Characteristics on SKINNY". In: *ACNS 2021 - 19th International Conference on Applied Cryptography and Network Security*. Ed. by Kazue Sako and Nils Ole Tippenhauer. Vol. 12727. 19th International Conference on Applied Cryptography and Network Security. Kamakura, Japan, June 2021, pp. 184–207. DOI: 10.1007/978-3-030-78375-4_8. hal-03040548.

[419] Florian Delconte, Phuc Ngo, Isabelle Debled-Rennesson, Bertrand Kerautret, Van Tho Nguyen, and Thiéry Constant. "Tree Defect Segmentation using Geometric Features and CNN". In: *Reproducible Research on Pattern Recognition (RRPR)*. Vol. LNCS 12636. Milan, Italy, 2021, pp. 80–100. DOI: 10.1007/978-3-030-76423-4_6. hal-03006063.

[420] Olivier Devillers and Charles Duménil. "Stochastic Analysis of Empty-Region Graphs". In: *CCCG 2021 - 33rd Canadian Conference on Computational Geometry*. Halifax / Virtual, Canada, August 2021. hal-03296186.

[421] Philippe Even, Axelle Grzesznik, Anne Gebhardt, Thomas Chenal, Pierre Even, and Phuc Ngo. "Interactive extraction of linear structures from LiDAR raw data for archaeomorphological structure prospection". In: *XXIV ISPRS Congress*. Vol. XLIII-B2-2021. The International Archives of the Photogrammetry, Remote Sensing and Spatial Information Sciences. Nice (en ligne), France, July 2021, pp. 153–161. DOI: 10.5194/isprs-archives-XLIII-B2-2021-153-2021. hal-03189641.

[422] Philippe Even and Phuc Ngo. "Automatic forest road extraction from LiDAR data of mountainous areas". In: *DGMM 2021 - IAPR International Conference on Discrete Geometry and Mathematical Morphology*. Vol. LNCS12708. Uppsala, Sweden, May 2021, pp. 93–106. DOI: 10.1007/978-3-030-76657-3_6. hal-03144147.

[423] Vladimir Garanzha, Igor Kaporin, Liudmila Kudryavtseva, François Protais, Nicolas Ray, and Dmitry Sokolov. "On Local Invertibility and Quality of Free-boundary Deformations". In: *IMR 2021 - 29th International Meshing Roundtable*. Proceedings of the 29th International Meshing Roundtable. Virtual, United States, June 2021. hal-03341392.

[424] Félix Gaschi, Parisa Rastin, and Yannick Toussaint. "Unsupervised Word embedding Alignment in the biomedical domain". In: *CIFSD 2021 - Conférence Internationale Francophone sur la Science des Données*. Marseille/Virtuel, France, June 2021. hal-03259987.

[425] Xavier Goaoc, Andreas Holmsen, and Zuzana Patáková. "A Stepping-Up Lemma for Topological Set Systems". In: *SoCG 2021 - 37th International Symposium on Computational Geometry*. Vol. 189. arXiv: 2103.09286. Buffalo/virtual, United States, June 2021, 40:1–40:17. DOI: 10.4230/LIPIcs.SoCG.2021.40. hal-03341599.

[426] Elisabeth Larsson, Pierre-Frédéric Villard, Igor Tominec, and Nicola Cacciani. "Geometry Reconstruction from Noisy Data using a Radial Basis Function Partition of Unity Method". In: *CSE 2021 - SIAM Conference on Computational Science and Engineering*. Fort Worth/Virtual, United States, March 2021. hal-03147251.

[427] Wan-Chiu Li, Cédric Borgese, Alexandre Benedicto, Nicolas Ray, and Dmitry Sokolov. "Singular Structured Hexahedral Grid". In: *RING Meeting 2021*. 2021 RING Meeting Papers. Vandoeuvre-lès-Nancy, France, September 2021. hal-03375671.

[428] Louis Massucci, Fabien LAUER, and Marion Gilson. "How statistical learning can help to estimate the number of modes in switched system identification?" In: *19th IFAC Symposium on System Identification, SYSID 2021*. Padova (Virtual Event), Italy, July 2021. hal-03324069.

[429] Louis Massucci, Fabien LAUER, and Marion Gilson. “Regularized switched system identification: A statistical learning perspective”. In: *7th IFAC International Conference on Analysis and Design of Hybrid Systems, ADHS'2021*. Brussel (Virtual Event), Belgium, July 2021. hal-03324120.

[430] Nikita Mikhalkov, Alexey Prutskiy, Semyon Sechenev, Dmitry Kazakov, Alexey Simulin, Dmitry Sokolov, and Igor Ryadchikov. “Gyrubot: nonanthropomorphic stabilization for a biped”. In: *ICRA 2021 - IEEE International Conference on Robotics and Automation*. 2021 IEEE International Conference on Robotics and Automation (ICRA). Xi'an / Virtual, China, May 2021. hal-03172031.

[431] Guillaume Moroz. “New data structure for univariate polynomial approximation and applications to root isolation, numerical multipoint evaluation, and other problems”. In: *FOCS 2021 - 62nd Annual IEEE Symposimum on Foundations of Computer Science*. arXiv: 2106.02505. Denver, United States, February 2021. hal-03249123.

[432] Phuc Ngo, Nicolas Passat, and Yukiko Kenmochi. “Quasi-regularity verification for 2D polygonal objects based on medial axis analysis”. In: *International Conference on Image Processing (ICIP)*. Anchorage, Alaska, United States, 2021, pp. 1584–1588. DOI: 10.1109/ICIP42928.2021.9506543. hal-03121428.

[433] Cyrius Nugier, Diane Leblanc-Albarel, Agathe Blaise, Simon Masson, Paul Huynh, and Yris Brice Wandji Piugie. “An Upcycling Tokenization Method for Credit Card Numbers”. In: *SECRYPT 2021 - 18th International Conference on Security and Cryptography*. Online, France, July 2021. hal-03220739.

[434] Nicolas Passat, Phuc Ngo, and Yukiko Kenmochi. “Homotopic Digital Rigid Motion: An Optimization Approach on Cellular Complexes”. In: *International Conference on Discrete Geometry and Mathematical Morphology (DGMM)*. Vol. 12708. Lecture Notes in Computer Science. Uppsala (virtual), Sweden, 2021, pp. 189–201. DOI: 10.1007/978-3-030-76657-3_13. hal-02994752.

[435] Pierre-Alexandre Simon, Radu S. Stoica, and Frédéric Sur. “An application of neural point processes to geophysical data”. In: *RING Meeting 2021*. Nancy, France, September 2021, pp. 1–13. hal-03294911.

[436] Thibault Tricard, Jimmy Etienne, Cédric Zanni, and Sylvain Lefebvre. “A brick in the wall: Staggered orientable infills for additive manufacturing”. In: *SCF 2021 - ACM Symposium on Computational Fabrication*. Boston/Virtual, United States, October 2021. DOI: 10.1145/3485114.3485117. hal-03352656.

Articles in National Peer-Reviewed Journal

[437] Fabrice Boudot, Pierrick Gaudry, Aurore Guillevic, Nadia Heninger, Emmanuel Thomé, and Paul Zimmermann. “New factorization and discrete logarithm record computations”. In: *Techniques de l'Ingenieur* (December 2020), p. 17. hal-03045666.

National Peer-Reviewed Conferences

[438] Antoine Fond, Marie-Odile Berger, and Gilles Simon. “Generation of facade hypotheses based on contextual and structural information”. In: *Reconnaissance des Formes et Intelligence Artificielle*. Clermont Ferrand, France, June 2016. hal-01318680.

[439] Vincent Gaudillière, Gilles Simon, and Marie-Odile Berger. “Estimation des géométries planaire et épipolaire en environnement faiblement texturé basée sur la mise en correspondance de régions”. In: *RFIAP 2018 - Congrès Reconnaissance des Formes, Image, Apprentissage et Perception*. Marne-la-Vallée, France, June 2018. hal-01802538.

[440] Fabien Lauer. “Error bounds with almost radical dependence on the number of components for multi-category classification, vector quantization and switching regression”. In: *CAP2018 - Conférence sur l’Apprentissage automatique (CAp) - French Conference on Machine Learning (FCML)*. Proc. of the French Conference on Machine Learning (CAp/FCML). Rouen, France, June 2018. hal-01815406.

[441] Vincent Gaudillière, Gilles Simon, and Marie-Odile Berger. “Estimation de pose de caméra à partir de correspondances ellipse - ellipsoïde”. In: *ORASIS 2019 - 17ème journées francophones des jeunes chercheurs en vision par ordinateur*. Saint-Dié-des-Vosges, France, May 2019. hal-02148633.

[442] Arthur Renaudeau, François Lauze, Fabien Pierre, Jean-François Aujol, and Jean-Denis Durou. “Inpainting vidéo pour la restauration de films par reconstructions alternées de la structure et de la texture”. In: *ORASIS 2019 - 17ème journées francophones des jeunes chercheurs en vision par ordinateur*. Saint-Dié-des-Vosges, France, May 2019. hal-02433990.

[443] Youssef Assis, Liang Liao, Fabien Pierre, René Anxionnat, and Erwan Kerrien. “Une stratégie de données efficace pour la détection des anévrismes cérébraux avec l’apprentissage profond”. In: *ORASIS 2021 - 18èmes journées francophones des jeunes chercheurs en vision par ordinateur*. Centre National de la Recherche Scientifique [CNRS]. Saint Ferréol, France, September 2021. hal-03339672.

[444] Rémi Decelle, Phuc Ngo, Isabelle Debled-Rennesson, Frédéric F. Mothe, and Fleur Longuetaud. “Description géometrique à l’aide de segments discrets”. In: *Journée du Groupe de Travail de Géométrie Discrète et Morphologie Mathématique (GT GDMM)*. Nancy, France, 2021. hal-03215817.

[445] Abdelkarim Elassam, Marie-Odile Berger, and Gilles Simon. “Détection de la ligne d’horizon et des points de fuite par apprentissage profond”. In: *ORASIS 2021 - 18èmes journées francophones des jeunes chercheurs en vision par ordinateur*. Centre National de la Recherche Scientifique [CNRS]. Saint Ferréol, France, September 2021. hal-03339639.

[446] Arthur Renaudeau, Travis Seng, Axel Carlier, Fabien Pierre, François Lauze, Jean-François Aujol, and Jean-Denis Durou. “Détection des défauts dans les vieux films par apprentissage profond à partir d’une restauration semi-manuelle”. In: *ORASIS 2021 - 18èmes journées francophones des jeunes chercheurs en vision par ordinateur*. Centre National de la Recherche Scientifique [CNRS] and Equipe REVA, IRIT : Institut de Recherche en Informatique de Toulouse. Saint Ferréol, France, September 2021. hal-03339640.

[447] Matthieu Zins, Gilles Simon, and Marie-Odile Berger. “3D-Aware Ellipse Prediction for Object-Based Camera Pose Estimation”. In: *ORASIS 2021 - 18èmes journées francophones des jeunes chercheurs en vision par ordinateur*. Ce travail a déjà été publié lors de la conférence 3DV 2020. Centre National de la Recherche Scientifique [CNRS]. Saint Ferréol, France, September 2021. hal-03339617.

Book (written)

[448] Marco Attene, Marco Livesu, Sylvain Lefebvre, Thomas Funkhouser, Stefano Ellero, Szymon Rusinkiewicz, Jonàs Martínez, and Amit Haim Bermano. *Design, Representations, and Processing for Additive Manufacturing*. Vol. 10. Synthesis Lectures on Visual Computing: Computer Graphics, Animation, Computational Photography, and Imaging 2. Morgan & Claypool Publishers, June 2018, p. 146. hal-01836525.

[449] Paul Zimmermann, Alexandre Casamayou, Nathann Cohen, Guillaume Connan, Thierry Dumont, Laurent Fousse, Francois Maltey, Matthias Meulien, Marc Mezzarobba, Clément Pernet, Nicolas M. Thiery, Erik Bray, John Cremona, Marcelo Forets, Alexandru Ghitza, and Hugh Thomas. *Computational Mathematics with SageMath*. SIAM, December 2018. DOI: 10.1137/1.9781611975468. hal-01646401.

[450] Fabien Lauer and Gérard Bloch. *Hybrid System Identification : Theory and Algorithms for Learning Switching Models*. Springer, 2019. hal-01860332.

[451] Christian Gentil, Gilles Gouaty, and Dmitry Sokolov. *Modélisation géométrique de formes fractales pour la CAO*. ISTE Editions, January 2020. hal-02462416.

Books or Proceedings Editing

[452] Damien Jamet. *Foreword - Special issue dedicated to the fifteenth "Journées Montoises d'Informatique Théorique*. Vol. 50. 1. June 2016. DOI: 10.1051/ita/2016012. hal-01364597.

[453] Bertrand Kerautret, Miguel Colom, Daniel Lopresti, Pascal Monasse, and Hugues Talbot. *Reproducible Research in Pattern Recognition, Second International Workshop, RRPR 2018*. August 2018. hal-02172999.

[454] Daniel Augot, Faina Solov'Eva, Marine Minier, Victor A. Zinoviev, and Thomas Johansson. *Editorial: Special issue on coding and cryptography*. Vol. 87. 2-3. Springer, March 2019. DOI: 10.1007/s10623-018-00601-w. hal-02373772.

Book Chapters

[455] Yann Guermeur and Fabien Lauer. "A generic approach to biological sequence segmentation problems, application to protein secondary structure prediction". In: *Pattern Recognition in Computational Molecular Biology: Techniques and Approaches*. Ed. by Mourad Elloumi, Costas Iliopoulos, Jason T. L. Wang, and Albert Y. Zomaya. Wiley, 2016, pp. 114–128. DOI: 10.1002/9781119078845.ch7. hal-01253820.

[456] Richard P. Brent, Alexander Kruppa, and Paul Zimmermann. "FFT extension for algebraic-group factorization algorithms". In: *Topics in Computational Number Theory Inspired by Peter L. Montgomery*. Ed. by Joppe W. Bos and Arjen K. Lenstra. Cambridge University Press, 2017, pp. 189–205. hal-01630907.

[457] Van Tho Nguyen, Bertrand Kerautret, Isabelle Debled-Rennesson, Francis Colin, Alexandre Piboule, and Thiéry Constant. "Algorithms and Implementation for Segmenting Tree Log Surface Defects". In: *Reproducible Research in Pattern Recognition : First International Workshop, RRPR 2016, Cancún, Mexico, December 4, 2016, Revised Selected Papers*. Lecture Notes in Computer Science Chapter 11. Springer International Publishing AG, 2017. DOI: 10.1007/978-3-319-56414-2_11. hal-02788140.

[458] Deepika Singh, Erinc Merdivan, Sten Hanke, Johannes Kropf, Matthieu Geist, and Andreas Holzinger. "Convolutional and Recurrent Neural Networks for Activity Recognition in Smart Environment". In: *Towards Integrative Machine Learning and Knowledge Extraction*. Ed. by A. Holzinger, R. Goebel, M. Ferri, and V. Palade. Vol. 10344. Lecture Notes in Computer Science. springer, 2017, pp. 194–205. hal-01629732.

[459] Emmanuel Thomé. "A modified block Lanczos algorithm with fewer vectors". In: *Topics in Computational Number Theory inspired by Peter L. Montgomery*. Ed. by Joppe W. Bos and Arjen K. Lenstra. arXiv: 1604.02277. Cambridge University Press, 2017, pp. 175–188. DOI: 10.1017/9781316271575.008. hal-01293351.

[460] Nikola K Blanchard, Siargey Kachanovich, Ted Selker, and Florentin Waligorski. "Reflexive Memory Authenticator: A Proposal for Effortless Renewable Biometrics". In: *Emerging Technologies for Authorization and Authentication*. Vol. 11967. September 2019, pp. 104–121. DOI: 10.1007/978-3-030-39749-4_7. hal-02550765.

[461] Parisa Rastin, Guénaël Cabanes, Rosanna Verde, Younès Bennani, and Thierry Couronne. "Generative Histogram-Based Model Using Unsupervised Learning". In: *Neural Information Processing*. December 2019, pp. 634–646. DOI: 10.1007/978-3-030-36718-3_53. hal-02994819.

[462] Nicola Cacciani, Elisabeth Larsson, Alberto Lauro, Marco Meggiolaro, Alessio Scatto, Igor Tominec, and Pierre-Frédéric Villard. "A First Meshless Approach to Simulation of the Elastic Behaviour of the Diaphragm". In: *Spectral and High Order Methods for Partial Differential Equations ICOSAHOM 2018*. Ed. by Sherwin S., Moxey D., Peiró J., Vincent P., and Schwab C. Vol. 134. Lecture Notes in Computational Science and Engineering. Springer, August 2020, pp. 501–512. DOI: 10.1007/978-3-030-39647-3_40. hal-02917575.

[463] Damien Chablat, Guillaume Moroz, Fabrice Rouillier, and Philippe Wenger. "Using Maple to analyse parallel robots". In: *Maple in Mathematics Education and Research*. Ed. by Jürgen Gerhard and Ilias Kotsireas. Maple in Mathematics Education and Research. Springer, Cham, February 2020, pp. 50–64. DOI: 10.1007/978-3-030-41258-6_4. hal-02289699.

[464] Xavier Goaoc. "Convexité combinatoire". In: *Informatique Mathématique : Une photographie en 2020*. 2020. hal-03130356.

[465] Fabien Pierre and Jean-François Aujol. "Recent Approaches for Image Colorization". In: *Handbook of Mathematical Models and Algorithms in Computer Vision and Imaging*. 2020. DOI: 10.1007/978-3-030-03009-4_55-1. hal-02965137.

[466] Igor Ryadchikov, Semyon Sechenev, Nikita Mikhalkov, Andrey Biryuk, Alexander Svidlov, Aleksandr Gusev, Dmitry Sokolov, and Evgeny Nikulchev. "Feedback Control with Equilibrium Revision for CMG-Actuated Inverted Pendulum". In: *Proceedings of 14th International Conference on Electromechanics and Robotics "Zavalishin's Readings"*. August 2020, pp. 431–440. DOI: 10.1007/978-981-13-9267-2_35. hal-02282908.

[467] Deepika Singh, Ismini Psychoula, Erinc Merdivan, Johannes Kropf, Sten Hanke, Emanuel Sandner, Liming Chen, and Andreas Holzinger. "Privacy-Enabled Smart Home Framework with Voice Assistant". In: *Smart Assisted Living*. August 2020, pp. 321–339. DOI: 10.1007/978-3-030-25590-9_16. hal-03081721.

[468] Félix Gaschi, Parisa Rastin, and Yannick Toussaint. "Handling the Deviation from Isometry Between Domains and Languages in Word Embeddings: Applications to Biomedical Text Translation". In: *Neural Information Processing*. Vol. 13109. Lecture Notes in Computer Science. Springer International Publishing, December 2021, pp. 216–227. DOI: 10.1007/978-3-030-92270-2_19. hal-03477901.

[469] Nigel P Smart and Emmanuel Thomé. "History of Cryptographic Key Sizes". In: *Computational Cryptography*. Ed. by Joppe Bos and Martijn Stam. Vol. 469. London Mathematical Society Lecture Note Series. Cambridge University Press, December 2021. hal-03408015.

General Audience

[470] Marie-Odile Berger and Gilles Simon. "Réalité augmentée : entre mythes et réalités". In: *Interstices* (March 2016). hal-01350456.

[471] Pierrick Gaudry and Joanna Jongwane. "À propos du vote par Internet". In: *Interstices* (March 2017). hal-01533682.

[472] Véronique Cortier, Pierrick Gaudry, and Stephane Glondu. *(a voté) Euh non : a cliqué*. Blog Binaire LeMonde.fr. March 2018. hal-01936863.

[473] Cécile Pierrot. *De la nécessité des problèmes que l'on ne sait pas résoudre*. Blog Binaire Le Monde.frArticle de vulgarisation https://www.lemonde.fr/blog/binaire/2019/12/06/de-la-necessite-des-problemes-que-lon-ne-sait-pas-resoudre/. December 2019. hal-03213156.

[474] Gilles Simon. "La machine à perspective de Jan Van Eyck". In: *Interstices* (November 2021). hal-03517010.

[475] Gilles Simon. "La véritable invention de Jan van Eyck : une machine à représenter l'espace tel que nous le percevons". In: *The Conversation* (August 2021). hal-03521172.

Other Publication

[476] Shi Bai, Pierrick Gaudry, Alexander Kruppa, Emmanuel Thomé, and Paul Zimmermann. "Factorisation of RSA-220 with CADO-NFS". working paper or preprint. May 2016. hal-01315738.

[477] Frédéric Bihan and Pierre-Jean Spaenlehauer. "Sparse Polynomial Systems with many Positive Solutions from Bipartite Simplicial Complexes". arXiv: 1510.05622 - working paper or preprint. April 2016. hal-01217547.

[478] Dobrina Boltcheva and Bruno Lévy. *Simple and Scalable Surface Reconstruction*. Research Report. LORIA - Université de Lorraine ; INRIA Nancy, July 2016. hal-01349023.

[479] Richard P Brent and Paul Zimmermann. "Twelve new primitive binary trinomials". arXiv: 1605.09213 - working paper or preprint. October 2016. hal-01378493.

[480] Nicolas Chenavier and Olivier Devillers. *Stretch Factor of Long Paths in a planar Poisson-Delaunay Triangulation*. Research Report RR-8935. arXiv: 1607.05770. Inria, July 2016, p. 34. hal-01346203.

[481] Olivier Devillers and Louis Noizet. *Walking in a Planar Poisson-Delaunay Triangulation: Shortcuts in the Voronoi Path*. Research Report RR-8946. INRIA Nancy, August 2016. hal-01353585.

[482] Rémi Imbach. *A Subdivision Solver for Systems of Large Dense Polynomials*. Technical Report RT-0476. arXiv: 1603.07916. INRIA Nancy, March 2016, p. 13. hal-01293526.

[483] Rémi Imbach, Pascal Mathis, and Pascal Schreck. *A Robust and Efficient Method for Solving Point Distance Problems by Homotopy*. Research Report RR-8705. arXiv: 1503.07901. INRIA, July 2016. hal-01135230.

[484] Iordan Iordanov and Monique Teillaud. *Implementing Delaunay triangulations of the Bolza surface*. Research Report RR-8994. INRIA Nancy, 2016. hal-01411415.

[485] Pedro Machado Manhães De Castro and Olivier Devillers. *Expected Length of the Voronoi Path in a High Dimensional Poisson-Delaunay Triangulation*. Research Report RR-8947. Inria, August 2016. hal-01353735.

[486] Nicolas Ray and Dmitry Sokolov. "On Smooth Frame Field Design". working paper or preprint. January 2016. DOI: 10.1145/1559755.1559763. hal-01245657.

[487] Maxence Reberol and Bruno Lévy. *Low-order continuous finite element spaces on hybrid non-conforming hexahedral-tetrahedral meshes*. Research Report. arXiv: 1605.02626. INRIA Nancy, équipe ALICE, May 2016. hal-01313285.

[488] Paul Zimmermann and Fanny Bastien. *Paul Zimmermann - CADO-NFS : PARI/GP Workshop 2016*. Videos. January 2016. medihal-01346718.

[489] Jean-Daniel Boissonnat, Olivier Devillers, Kunal Dutta, and Marc Glisse. "Delaunay triangulation of a random sample of a good sample has linear size ". working paper or preprint. December 2017. hal-01673170.

[490] Luca Castelli Aleardi and Olivier Devillers. *Explicit array-based compact data structures for triangulations: practical solutions with theoretical guarantees*. Research Report RR-7736. INRIA, 2017, p. 39. inria-00623762.

[491] Luca Castelli Aleardi, Olivier Devillers, and Eric Fusy. "Canonical ordering for graphs on the cylinder, with applications to periodic straight-line drawings on the flat cylinder and torus". arXiv: 1206.1919 - 37 pages. 2017. hal-01646724.

[492] Olivier Devillers and Marc Glisse. *Delaunay triangulation of a random sample of a good sample has linear size*. Research Report RR-9082. Inria Saclay Ile de France ; Inria Nancy - Grand Est, July 2017, p. 6. hal-01568030.

[493] Pierrick Gaudry. "Some ZK security proofs for Belenios". working paper or preprint. 2017. hal-01576379.

[494] Laurent Grémy, Aurore Guillevic, and François Morain. "Breaking DLP in $GF(p^5)$ using 3-dimensional sieving". working paper or preprint. July 2017. hal-01568373.

[495] Samuel Hornus and Sylvain Lefebvre. *Iterative carving for self-supporting 3D printed cavities*. Research Report RR-9083. Inria Nancy - Grand Est, July 2017, p. 19. hal-01570330.

[496] Rémi Imbach, Guillaume Moroz, and Marc Pouget. *Reliable location with respect to the projection of a smooth space curve*. Research Report. INRIA, November 2017. hal-01632344.

[497] Wouter Kuijper, Victor Ermolaev, and Olivier Devillers. *Celestial Walk: A Terminating Oblivious Walk for Convex Subdivisions*. Research Report RR-9099. arXiv: 1710.01620. INRIA Nancy, 2017. hal-01610205.

[498] Sylvain Lefebvre. *Visualizing and Fabricating Complex Internal Structures*. Technical Report RT-0493. Inria Nancy - Grand Est, November 2017, p. 15. hal-01636963.

[499] Nicolas Ray, Dmitry Sokolov, Maxence Reberol, Franck Ledoux, and Bruno Lévy. "Hexahedral Meshing: Mind the Gap!" working paper or preprint. June 2017. hal-01551603.

[500] Maxence Reberol and Bruno Lévy. "Computing the distance between two finite element solutions defined on different 3D meshes on a GPU". working paper or preprint. August 2017. hal-01634176.

[501] David Bernhard, Véronique Cortier, Pierrick Gaudry, Mathieu Turuani, and Bogdan Warinschi. "Verifiability Analysis of CHVote". working paper or preprint. 2018. hal-03001923.

[502] Svyatoslav Covanov. "Improved method for finding optimal formulae for bilinear maps in a finite field". arXiv: 1705.07728 - working paper or preprint. November 2018. hal-01519408.

[503] Thuy Hong Dao, Phuc Ngo, Isabelle Debled-Rennesson, Yukiko Kenmochi, and Nicolas Passat. "Transformations rigides pour les objets discrets non-convexes en 2D". In: *Journées du Groupe de Travail en Modélisation Géométrique (GTMG)*. Aix-en-Provence, France, 2018. hal-01740074.

[504] Vincent Despré, Olivier Devillers, Hugo Parlier, and Jean-Marc Schlenker. "Delaunay Triangulations of Points on Circles". arXiv: 1803.11436 - working paper or preprint. April 2018. hal-01780607.

[505] Olivier Devillers and Charles Duménil. *A Poisson sample of a smooth surface is a good sample*. Research Report RR-9239. INRIA Nancy, 2018, p. 8. hal-01962631.

[506] Olivier Devillers, Sylvain Lazard, and William Lenhart. *3D Snap Rounding*. Research Report RR-9149. Inria Nancy - Grand Est, February 2018, pp. 1–22. hal-01698928.

[507] Xavier Goaoc, Alfredo Hubard, Rémi De Joannis De Verclos, Jean-Sébastien Sereni, and Jan Volec. "Limits of Order Types *". working paper or preprint. November 2018. hal-01913144.

[508] Phuc Ngo, Nicolas Passat, Yukiko Kenmochi, and Isabelle Debled-Rennesson. "Geometric-preserving rigid motions of digital objects". In: *Journées Informatique et Géométrie (JIG)*. Lyon, France, 2018. hal-01822122.

[509] Imre Barany, Matthieu Fradelizi, Xavier Goaoc, Alfredo Hubard, and Günter Rote. *Random polytopes and the wet part for arbitrary probability distributions*. Research Report. arXiv: 1902.06519. Rényi Institute of Mathematics ; University College London ; Université Paris-Est ; Université de Lorraine ; Freie Universität Berlin, 2019. hal-02050632.

[510] Enka Blanchard and Siargey Kachanovich. "Usable everlasting encryption using the pornography infrastructure". working paper or preprint. July 2019. hal-02556366.

[511] Jean-Daniel Boissonnat, Olivier Devillers, Kunal Dutta, and Marc Glisse. *Randomized incremental construction of Delaunay triangulations of nice point sets*. Research Report. INRIA, 2019. hal-01950119.

[512] Dobrina Boltcheva, Chouaib Fellah, Damien Liehn, and Clément Poull. *Modélisation de toitures à partir de nuages de points 3D*. Research Report. LORIA–INRIA Grand Est ; Université de Lorraine (Nancy), December 2019. hal-02409136.

[513] Prosenjit Bose, Jean-Lou De Carufel, and Olivier Devillers. *Expected Complexity of Routing in Θ_6 and Half-Θ_6 Graphs*. Research Report. arXiv: 1910.14289. INRIA, 2019, p. 18. hal-02338733.

[514] Baptiste Caramiaux, Fabien Lotte, Joost Geurts, Giuseppe Amato, Malte Behrmann, Frédéric Bimbot, Fabrizio Falchi, Ander Garcia, Jaume Gibert, Guillaume Gravier, Hadmut Holken, Hartmut Koenitz, Sylvain Lefebvre, Antoine Liutkus, Andrew Perkis, Rafael Redondo, Enrico Turrin, Thierry Viéville, and Emmanuel Vincent. *AI in the media and creative industries*. Research Report. arXiv: 1905.04175. New European Media (NEM), April 2019, pp. 1–35. hal-02125504.

[515] Véronique Cortier, Jannik Dreier, Pierrick Gaudry, and Mathieu Turuani. "A simple alternative to Benaloh challenge for the cast-as-intended property in Helios/Belenios". working paper or preprint. 2019. hal-02346420.

[516] Rémi Decelle, Phuc Ngo, Isabelle Debled-Rennesson, Mothe Frédéric, and Fleur Longuetaud. *Détection automatique de la moelle sur des images d'extrémités de grumes de Douglas brutes de sciage*. GDR 2019 - 8èmes Journées du Groupement de Recherche 3544 Sciences du Bois. Poster. November 2019. hal-03029969.

[517] Florian Delconte. "Estimation de la qualité de grumes de bois". MA thesis. Université de Lorraine, September 2019, p. 38. hal-03603108.

[518] Vincent Despré, Jean-Marc Schlenker, and Monique Teillaud. *Flipping Geometric Triangulations on Hyperbolic Surfaces*. Research Report. arXiv: 1912.04640. INRIA, December 2019. hal-02400219.

[519] Philippe Even, Phuc Ngo, and Bertrand Kerautret. *Complementary Experiments of the Thick Line Segment Detection Algorithm: Evaluation of ADS and ATC Concepts*. Research Report. LORIA (Université de Lorraine, CNRS, INRIA), 2019. hal-03155787.

[520] Vincent Gaudillière, Gilles Simon, and Marie-Odile Berger. "Perspective-12-Quadric: An analytical solution to the camera pose estimation problem from conic - quadric correspondences". working paper or preprint. March 2019. hal-02054882.

[521] Antoine Joux and Cecile Pierrot. "Algorithmic aspects of elliptic bases in finite field discrete logarithm algorithms". arXiv: 1907.02689 - working paper or preprint. July 2019. hal-02173688.

[522] Sylvain Lefebvre. *Efficient Direct Slicing Of Dilated And Eroded 3d Models For Additive Manufacturing: Technical Report*. Research Report. arXiv: 1911.05992. Inria Nancy - Grand Est, November 2019. hal-02360401.

[523] Antoine Richard, Antoine Mahé, Cedric Pradalier, Offer Rozenstein, and Matthieu Geist. "A Comprehensive Benchmark of Neural Networks for System Identification". working paper or preprint. September 2019. hal-02278102.

[524] Raffaella Trivisonne, Erwan Kerrien, and Stéphane Cotin. "Constrained Stochastic State Estimation for 3D Shape Reconstruction of Catheters and Guidewires in Fluoroscopic Images". working paper or preprint. April 2019. hal-02072386.

[525] Leo Valque. "3D Snap Rounding". MA thesis. Université de Lyon, June 2019. hal-02393625.

[526] Leo Adams, Enka Blanchard, Inès Dardouri, Levi Gabasova, and Pierre Midavaine. ""Set up son? Scam set, asserts Bob": Semi-Automatic Generation of Bilingual Palindromes". working paper or preprint. May 2020. hal-02560680.

[527] Alexis BARTHELEMY. "Reconstruction de billon". MA thesis. Université de Lorraine, August 2020, p. 44. hal-03606199.

[528] Enka Blanchard. "Making more extensive and efficient typo-tolerant password checkers". © 2020 IEEE. Personal use of this material is permitted. Permission from IEEE must be obtained for all other uses, in any current or future media, including reprinting/republishing this material for advertising or promotional purposes, creating new collective works, for resale or redistribution to servers or lists, or reuse of any copyrighted component of this work in other works. May 2020. hal-02560665.

[529] Enka Blanchard, Ted Selker, and Alan T Sherman. "Boardroom Voting: Verifiable Voting with Ballot Privacy Using Low-Tech Cryptography in a Single Room". working paper or preprint. July 2020. hal-02908421.

[530] Xavier Bonnetain, Anne Canteaut, Véronique Cortier, Pierrick Gaudry, Lucca Hirschi, Steve Kremer, Stéphanie Lacour, Matthieu Lequesne, Gaëtan Leurent, Léo Perrin, André Schrottenloher, Emmanuel Thomé, Serge Vaudenay, and Christophe Vuillot. "Le traçage anonyme, dangereux oxymore : Analyse de risques à destination des non-spécialistes". working paper or preprint. April 2020. hal-02997228.

[531] Luce Brotcorne, Anne Canteaut, Aline Carneiro Viana, Céline Grandmont, Benjamin Guedj, Stéphane Huot, Valérie Issarny, Guillaume Pallez, Valérie Perrier, Vivien Quema, Jean-Baptiste Pomet, Xavier Rival, Sylvain Salvati, and Emmanuel Thomé. *Indicateurs de suivi de l'activité scientifique de l'Inria*. Research Report. Inria, December 2020. hal-03033764.

[532] Otfried Cheong, Olivier Devillers, Marc Glisse, and Ji-won Park. *Covering families of triangles*. Research Report RR-9378. INRIA, 2020, p. 31. hal-03031995.

[533] Gabrielle De Micheli and Nadia Heninger. "Recovering cryptographic keys from partial information, by example". working paper or preprint. December 2020. hal-03045663.

[534] Olivier Devillers, Philippe Duchon, Marc Glisse, and Xavier Goaoc. "On Order Types of Random Point Sets". arXiv: 1812.08525 - working paper or preprint. May 2020. hal-01962093.

[535] Xavier Goaoc and Emo Welzl. "Convex Hulls of Random Order Types". arXiv: 2003.08456 - working paper or preprint. March 2020. hal-02513054.

[536] Yann Guermeur. "Combinatorial and Structural Results for γ-Ψ-dimensions". arXiv: 1809.07310v3 - working paper or preprint. September 2020. hal-03230918.

[537] Benedikt Kolbe. "Towards a combinatorial algorithm for the enumeration of isotopy classes of symmetric cellular embeddings of graphs on hyperbolic surfaces". working paper or preprint. December 2020. hal-03047231.

[538] Benedikt Kolbe and Vanessa Robins. "Tile-transitive tilings of the Euclidean and hyperbolic planes by ribbons". working paper or preprint. December 2020. hal-03046798.

[539] George Krait, Sylvain Lazard, Guillaume Moroz, and Marc Pouget. "Isolating the singularities of the plane projection of a generic space curve". working paper or preprint. May 2020. hal-02612412.

[540] François Protais, Maxence Reberol, Nicolas Ray, Etienne Corman, Franck Ledoux, and Dmitry Sokolov. "Robust Quantization for Polycube Maps". working paper or preprint. December 2020. hal-03076711.

[541] Ted Selker and Enka Blanchard. "Design ideas to improve the usability and security of mail-in ballots". working paper or preprint. July 2020. hal-02908417.

[542] Frédéric Sur, Benoît Blaysat, and Michel Grédiac. *On biases in displacement estimation for image registration, with a focus on photomechanics - Extended version*. Research Report. LORIA (Université de Lorraine, CNRS, INRIA) ; Institut Pascal (Université Clermont-Auvergne, SIGMA, CNRS), June 2020. hal-02862808.

[543] Adrien Bedel, Yoann Coudert-Osmont, Jonàs Martínez, Rahnuma Islam Nishat, Sue Whitesides, and Sylvain Lefebvre. "Closed space-filling curves with controlled orientation for 3D printing". working paper or preprint. March 2021. hal-03185200.

[544] Enka Blanchard, Sébastien Bouchard, and Ted Selker. "Visual Secrets: a human security primitive". working paper or preprint. January 2021. hal-03133412.

[545] Enka Blanchard, Ryan Robucci, Ted Selker, and Alan T Sherman. "Phrase-Verified Voting: Verifiable Low-Tech Remote Boardroom Voting : (How We Voted on Tenure & Promotion Cases during the Pandemic)". working paper or preprint. March 2021. hal-03164487.

[546] Anne Canteaut, Miguel Angel Fernández, Luc Maranget, Sophie Perin, Mario Ricchiuto, Manuel Serrano, and Emmanuel Thomé. *Évaluation des Logiciels*. Research Report. Inria, January 2021. hal-03110723.

[547] Anne Canteaut, Miguel Angel Fernández, Luc Maranget, Sophie Perin, Mario Ricchiuto, Manuel Serrano, and Emmanuel Thomé. *Software Evaluation*. Research Report. Inria, January 2021. hal-03110728.

[548] Jin-San Cheng, Kai Jin, Marc Pouget, Junyi Wen, and Bingwei Zhang. "An Improved Complexity Bound for Computing the Topology of a Real Algebraic Space Curve". working paper or preprint. December 2021. hal-03469996.

[549] Véronique Cortier, Alexandre Debant, and Pierrick Gaudry. *A privacy attack on the Swiss Post e-voting system*. Research Report. Université de Lorraine, CNRS, Inria, LORIA, November 2021. hal-03446801.

[550] Véronique Cortier, Pierrick Gaudry, and Quentin Yang. "A toolbox for verifiable tally-hiding e-voting systems". Cryptology ePrint Archive: Report 2021/491 https://eprint.iacr.org/2021/491. April 2021. hal-03367930.

[551] Rémi Decelle, Phuc Ngo, Isabelle Debled-Rennesson, Frédéric F. Mothe, and Fleur Longuetaud. "Ant Colony Optimization for Estimating Pith Position on Images of Tree Log Ends". working paper or preprint. November 2021. hal-03442289.

[552] Vincent Despré, Loïc Dubois, Benedikt Kolbe, and Monique Teillaud. "Experimental analysis of Delaunay flip algorithms on genus two hyperbolic surfaces". working paper or preprint. December 2021. hal-03462834.

[553] Vincent Despré, Benedikt Kolbe, and Monique Teillaud. "Representing infinite hyperbolic periodic Delaunay triangulations using finitely many Dirichlet domains". Version 3: Addition of discussion of optimality and another way to interpret the bound. July 2021. hal-03045921.

[554] Nicolas Donati, Etienne Corman, Simone Melzi, and Maks Ovsjanikov. "Complex Functional Maps : a Conformal Link Between Tangent Bundles". arXiv: 2112.09546 - working paper or preprint. December 2021. hal-03480605.

[555] Iris Dumeur, Yang Chen, Frédéric Sur, and Zheng-Shu Zhou. *Sentinel-2 RGB and NIR bands simulation after fire events using a multi-temporal conditional generative adversarial network*. Research Report. LORIA (Université de Lorraine, CNRS, INRIA), 2021. hal-03327421.

[556] Matthijs Ebbens, Iordan Iordanov, Monique Teillaud, and Gert Vegter. "Delaunay triangulations of generalized Bolza surfaces". arXiv: 2103.05960 - working paper or preprint. March 2021. hal-03080125.

[557] Youssef El Housni and Aurore Guillevic. "Families of SNARK-friendly 2-chains of elliptic curves". working paper or preprint. October 2021. hal-03371573.

[558] Sylvain Lefebvre, Li-Yi Wei, and Connelly Barnes. "Informational Texture Synthesis". working paper or preprint. June 2021. hal-01706539.

[559] Antoine Moniot, Isaure Chauvot de Beauchêne, and Yann Guermeur. *Agglomerative clustering of fragment 3D structures based on pairwise RMSD*. ISMB ECCB 2021. Poster. July 2021. hal-03432682.

[560] Antoine Moniot, Isaure Chauvot de Beauchêne, and Yann Guermeur. *New clustering method to infer prototypes covering the 3D structures of nucleic acid fragments*. RECOMB 2021 - 25th International conference on research in computational molecular biology. Poster. August 2021. hal-03432671.

[561] Guillaume Moroz. "Fast real and complex root-finding methods for well-conditioned polynomials". arXiv: 2102.04180 - working paper or preprint. February 2021. hal-03134259.

[562] Nuwan Herath Mudiyanselage, Guillaume Moroz, and Marc Pouget. "Fast Guaranteed Drawing of High Degree Algebraic Curves". working paper or preprint. December 2021. hal-03465123.

[563] Phuc Ngo. *Gauss Digitization of Simple Polygons*. Research Report. LORIA (Université de Lorraine, CNRS, INRIA), 2021. DOI: 10.13140/RG.2.2.32967.21925. hal-03125916.

[564] A. Poszwa, A. Grzesznik, A. Gebhardt, A. AGAT, P. Even, Phuc Ngo, D. CARTIER, V. Robin, C. Delangle, S. Occhietti, Alexis A. De Junet, Dominique Harmand, Charles Kraemer, T. Chenal, and D. Bartier. *1400 years of man-environment interactions and soil evolution in the Saint-Mont mountain (Remiremont, Vosges)*. Historical Ecology for the future - International conference in historical ecology. Poster. Colloque chairman: Vincent Robin, Interdisciplinary Laboratory for Continental Environments (LIEC - CNRS/UL), May 2021. hal-03236655.

[565] Dmitry Sokolov, Nicolas Ray, and Etienne Corman. "Least squares for programmers". Doctoral. Lecture. SIGGRAPH2021, Los Angeles, United States, August 2021. DOI: 10.1145/3450508.3464554. hal-03321301.

Software

[566] Mikhail Bogdanov, Aymeric Pellé, Mael Rouxel-Labbe, and Monique Teillaud, *CGAL 3D Periodic Mesh Generation* version CGAL 4.13, 2018. HAL: ⟨hal-02983420v1⟩, hal-02983420, VCS: https://github.com/CGAL/cgal/tree/master/Periodic_3_mesh_3.

[567] Mikhail Bogdanov, Iordan Iordanov, and Monique Teillaud, *CGAL 2D Hyperbolic Delaunay Triangulations* version CGAL 4.14, 2019. HAL: ⟨hal-02983422v1⟩, hal-02983422, VCS: https://github.com/CGAL/cgal/tree/master/Hyperbolic_triangulation_2.

[568] The CADO-NFS Development Team, *CADO-NFS, An Implementation of the Number Field Sieve Algorithm* version 2.3.0, April 2019. HAL: ⟨hal-02099620v1⟩, hal-02099620, VCS: http://cado-nfs.gforge.inria.fr/.

[569] Iordan Iordanov and Monique Teillaud, *CGAL 2D Periodic Hyperbolic Triangulations* version CGAL 4.14, 2019. HAL: ⟨hal-02983428v1⟩, hal-02983428, VCS: https://github.com/CGAL/cgal/tree/master/Periodic_4_hyperbolic_triangulation_2.

[570] Gaetan Bisson, Romain Cosset, and Damien Robert, *AVIsogenies* version git-47d34838, October 2021. HAL: ⟨hal-03371897v1⟩, hal-03371897, VCS: https://gitlab.inria.fr/roberdam/avisogenies.

Patents

[571] Marie-Odile Berger, Vincent Gaudillière, and Gilles Simon. “Dispositif de traitement de prise de vue”. FR1905535 (France). May 2019. hal-02429562.

[572] Michel Grediac, Benoît Blaysat, and Frédéric Sur. “Method for measuring fields of movements and of deformations with check pattern marking and spectral method processing”. FR3078190 WO2019162449 (France). August 2019. hal-02272747.

Apprentissage et Biologie Computationnelle

Synopsis

1 Team Composition

Permanents

Matthieu Geist (Other, CentraleSupélec, left 31/8/17), Yann Guermeur (DR CNRS), Fabien Lauer (MCF UL), Parisa Rastin (MCF UL, arrived 1/9/19).

	2016	2017	2018	2019	2020	Total
PR	0	0	0	0	0	0
MCF	1	1	1	2	2	2
DR	1	1	1	1	1	1
CR	0	0	0	0	0	0
Other	1	1	0	0	0	1
Total (permanent positions)	3	3	2	3	3	4
Pr emeritus	0	0	0	0	0	0
Guest researchers	0	0	0	0	0	0
Post-doct. researchers	0	0	0	0	1	1
PhD Students	4	5	4	5	2	8
Master students M2	0	0	0	1	1	2
Master Students M1	0	0	0	0	0	0
L3 students	0	0	0	0	0	0
Engineers	0	0	0	0	0	0
Other	0	1	0	0	0	1
Total (temporary positions)	4	6	4	6	4	10

Post-doctoral fellows

Rahimeh Rouhi (post-doctoral student 2019-2020),

Change in team composition

On August the 31th 2017, Matthieu Geist left to join the LIEC as a Full Professor.

On the first of September 2019, Parisa Rastin joined us as an Assistant Professor at the ENSMN.

Doctoral students

Aya El Dakdouki (Walid Joumblatt Foundation for University Studies, 2015-2018, ATER, 2018-2019), Félix Gaschi (Cifre, 2020-...), Mounia Hendel (USTO-MB, 2016-2017), Antoine Mahé (FEDER-Région, 2017-2020), Louis Massucci (FCH-Région, 2019-...), Erinc Merdivan (Marie Curie grant, 2016-2019), Antoine Moniot (UL, 2018-...), Khadija Musayeva (UL, 2015-2018, ATER, 2018-2019)

	2016-2020
Phd's defended	5
On-going PhD's	3
Average nb of papers by PhD student	4
Average duration of PhD thesis (in month)	42

Since 1/9/19, Aya El Dadouki has been an ATER at the Université Grenoble Alpes. Mounia Hendel is MCF at USTO-MB. Antoine Mahé is robotics engineer at Neofarm (https://neo.farm/). Erinc Merdivan is a consultant at Helmotz AI (https://www.helmholtz.ai/). Khadija Musayeva is a post-doctoral student at the Université Côte d'Azur.

2 Research topics

Keywords

- Computer science:
  - learning theory
  - machine learning
- Applied mathematics:
  - empirical inference
  - optimization
- Biology:
  - structural biology
  - computational biology

Research area and main goals

The main specificity of the ABC research team is to be a melting pot gathering researchers in learning theory, applied mathematics and biology. Our main goal is simply to make contributions in these three sciences and to take advantage of multidisciplinarity to bring out synergies.

❸ Main Achievements

We made two major contributions to the study of the generalization performance of margin multi-category classifiers. They both regard the derivation of upper bounds on the probability of error, named *guaranteed risks*, more precisely the dependence of the corresponding confidence intervals on the three basic parameters: the sample size m, the number C of categories and the margin parameter γ. The first contribution, reported in [9], refutes a classical conjecture. It states that irrespective of the choice of the margin loss function, even when no hypotheses are made regarding a coupling among the outputs of the classifier, it is always possible to obtain a confidence interval depending sublinearly on C. The second contribution deals with the use of combinatorial dimensions to measure the *capacity* of the class of margin functions. We established that sharper bounds could be obtained by replacing the standard scale-sensitive combinatorial dimension, the fat-shattering dimension, with γ-Ψ-dimensions. This time, the gain is located in the dependence on γ.

Regarding switching regression problems, our main achievements concern the development of global optimization approaches for the estimation of models from data [12] and the derivation of statistical guarantees for those models [19, 32].

D1 : ABC

❹ Research activities

Generalization performance of margin classifiers

Description One of the main open problems of the theory of margin multi-category pattern classification[13] is the characterization of the way the confidence interval of an upper bound on the probability of error should vary as a function of the three basic parameters which are the sample size m, the number C of categories and the margin parameter γ. When working under minimal learnability hypotheses, the derivation of such a *guaranteed risk*[14] is based on the handling of capacity measures[15] belonging to three main families: Rademacher/Gaussian complexities[16], metric entropies[17] and scale-sensitive combinatorial dimensions[18]. They are connected by means of tools from the theory of empirical processes[19], functional analysis and combinatorics. Furthermore, for each of them, *structural results*[20] are available to perform the transition from the multi-class case to the bi-class one. In that framework, advances spring from introducing new building blocks in the general scheme and involving them in a path leading to an upper bound on the capacity of the class of margin functions with improved dependence on one of the basic parameters.

[13] V. Koltchinskii and D. Panchenko. "Empirical Margin Distributions and Bounding the Generalization Error of Combined Classifiers". In: *The Annals of Statistics* 30.1 (2002), pp. 1–50.

[14] V.N. Vapnik. *Statistical Learning Theory*. John Wiley & Sons, Inc., New York, 1998.

[15] V. Vovk, H. Papadopoulos, and A. Gammerman, eds. *Measures of Complexity, Festschrift for Alexey Chervonenkis*. Springer, 2015.

[16] P.L. Bartlett and S. Mendelson. "Rademacher and Gaussian Complexities: Risk Bounds and Structural Results". In: *Journal of Machine Learning Research* 3 (2002), pp. 463–482.

[17] A.N. Kolmogorov and V.M. Tihomirov. "ϵ-entropy and ϵ-capacity of sets in functional spaces". In: *American Mathematical Society Translations, series 2* 17 (1961), pp. 277–364.

[18] N. Alon, S. Ben-David, N. Cesa-Bianchi, and D. Haussler. "Scale-Sensitive Dimensions, Uniform Convergence, and Learnability". In: *Journal of the ACM* 44.4 (1997), pp. 615–631, Y. Guermeur. "VC Theory of Large Margin Multi-Category Classifiers". In: *Journal of Machine Learning Research* 8 (2007), pp. 2551–2594.

[19] M. Talagrand. *Upper and Lower Bounds for Stochastic Processes: Modern Methods and Classical Problems*. Springer-Verlag, Berlin Heidelberg, 2014.

[20] H.H. Duan. "Bounding the Fat Shattering Dimension of a Composition Function Class Built Using a Continuous Logic Connective". In: *The Waterloo Mathematics Review* 2.1 (2012), pp. 1–21, A. Maurer. "A vector-contraction inequality for Rademacher complexities". In: *ALT'16*. 2016, pp. 3–17.

Main results Our first contribution, exposed in [9], is two-fold. We introduced a new structural result for the metric entropy and a combinatorial result involving the fat-shattering dimension. Their main feature is that they both hold for all L_p-norms. Combined with a dedicated implementation of the chaining method, they provide guaranteed risks whose confidence interval grows sublinearly with C. This dependence was improved in [16] thanks to the implementation of a simple idea: the value of the parameter p of the norm should be chosen as a function of C. In [17], the advantages and drawbacks inherent to the three major options to perform the transition from the multi-class case to the binary one: using Rademacher complexities, covering numbers or scale-sensitive combinatorial dimensions, were highlighted in the framework of a comparative study. Our most recent results regard the usefulness of the scale-sensitive dimensions that we introduced, the γ-Ψ-dimensions, to derive bounds with sharp dependences on the basic parameters. They are presented in a paper which is still under review. Two major conclusions can be drawn from them:

1. the γ-Ψ-dimensions always bring an improvement compared to the use of the fat-shattering dimension of the class of margin functions;

2. thanks to their capacity to take into account basic features of the classifier, they represent a promising alternative to performing the transition from the multi-class case to the binary one with covering numbers.

Piecewise smooth and switching regression

Description Regression is a standard problem in machine learning for which numerous methods and analyses are available. However, most works in this field assume that the optimal target model is a smooth function. Piecewise smooth regression arises when this is not the case and the target function is only locally smooth, with possible jumps of values or derivatives at unknown locations. In this setting, the learning problem involves the estimation of several smooth models and a classifier which implements a partition of the input space and assigns an input to a specific model. Switching regression is another closely related setting, in which the data generating process can switch between the different operating modes or models arbitrarily.

We look at these problems from two angles. First, we try to develop efficient optimization algorithms for the estimation of switching models from data. Second, we analyze the generalization performance of the resulting models in order to provide statistical guarantees.

Main results In [8], we analyzed the computational complexity of globally minimizing the error of switching linear regression models. In particular, we showed that, on the one hand the problem is NP-hard, but, on the other hand, it admits a polynomial-time algorithm with respect to the number of data points for any fixed data dimension and number of modes.

Similar results were obtained for robust regression and the problem of minimizing a saturated loss function, which sometimes appears as a core step in switching regression algorithms. In particular, we showed that an exact algorithm with polynomial time-complexity with respect to the number of data can be devised. This result is obtained by adopting a classification point of view and relating the problem to the search for a linear model that can approximate the maximal number of points with a given error. Approximate variants of the proposed algorithms based on ramdom sampling were also discussed and experiments showed that it offers an accuracy gain over the traditional RANSAC[21] for a similar algorithmic simplicity.

[21] M. A. Fischler and R. C. Bolles. "RANSAC random sample consensus: A paradigm for model fitting

In [12], we developed global optimization algorithms for two particularly difficult nonconvex problems raised by switching regression: switching linear regression and bounded-error estimation. While most works focus on local optimization heuristics without global optimality guarantees or with guarantees valid only under restrictive conditions, the proposed approach always yields a solution with a certificate of global optimality. In order to obtain scalable algorithms with respect to the number of data, we directly optimize the model parameters in a continuous optimization setting without involving integer variables and develop a branch-and-bound strategy based on lower bounds that can be efficiently computed.

In [19], we developed the statistical analysis of these particular regression problems. Specifically, we derived generalization error bounds for piecewise smooth regression (PWS) and switching regression by following the approach based on Rademacher complexities. For PWS regression, our derivation involves a chaining argument[22] and a decomposition of the covering numbers of PWS classes in terms of the ones of their component functions and the capacity of the classifier partitioning the input space. This yields error bounds with a radical dependency on the number of modes. For switching regression, the decomposition can be performed directly at the level of the Rademacher complexities, which yields bounds with a linear dependency on the number of modes. By using once more chaining and a decomposition at the level of covering numbers, we showed how to recover a radical dependency.

In [32], we proposed a simple approach to derive efficient error bounds for learning multiple components with sparsity-inducing regularization. We showed that for such regularization schemes, known decompositions of the Rademacher complexity over the components can be used in a more efficient manner to result in tighter bounds without too much effort. We gave examples of application to switching regression, center-based clustering/vector quantization and subspace clustering, for which decomposition results were not previously available. For all these problems, the proposed approach yields risk bounds with mild dependencies on the number of components and completely removes this dependency for nonconvex regularization schemes that could not be handled by previous methods such as[23].

In [33], we push the analysis of the generalization performance one step further in order to apply it to the identification of hybrid dynamical systems that switch arbitrarily between modes, a context where the basic assumption of data independence does not hold anymore. The aim in this context was to tackle the critical issue of estimating the number of modes. A novel method inspired by model selection techniques in statistical learning was proposed. Specifically, the method implements the structural risk minimization principle[24], which relies on the minimization of an upper bound on the expected prediction error of the model. This so-called generalization error bound is first derived for static switched systems using Rademacher complexities. Then, it is extended to handle non independent observations from a single trajectory of a dynamical system, using the approach of[25]. Finally, it is further tailored to the needs of model selection via a uniformization step. An illustrative example of the behavior of the method and its ability to recover the true number of modes was presented.

---

with applications to image analysis and automated cartography". In: *Communications of the ACM* 24.6 (1981), pp. 381–395.

[22] M. Talagrand. *Upper and Lower Bounds for Stochastic Processes: Modern Methods and Classical Problems.* Springer-Verlag, Berlin Heidelberg, 2014.

[23] Y. Lei, U. Dogan, A. Binder, and M. Kloft. "Multi-class SVMs: From Tighter Data-Dependent Generalization Bounds to Novel Algorithms". In: *Advances in Neural Information Processing Systems 28.* 2015, pp. 2035–2043, A. Maurer. "A vector-contraction inequality for Rademacher complexities". In: *ALT'16.* 2016, pp. 3–17.

[24] V.N. Vapnik. *Statistical Learning Theory.* John Wiley & Sons, Inc., New York, 1998.

[25] B. Yu. "Rates of Convergence for Empirical Processes of Stationary Mixing Sequences". In: *The Annals of Probability* 22.1 (1994), pp. 94–116, M. Mohri and A. Rostamizadeh. "Rademacher Complexity Bounds for Non-I.I.D. Processes". In: *Advances in Neural Information Processing Systems 21.* 2009, pp. 1097–1104.

Finally, we co-authored the monograph [43], which stands as the first book on the topics of hybrid dynamical system identification and the theory and practice of learning switching models.

Learning non-parametric models of the data distribution

Description The main idea of probabilistic approaches to clustering is to be able to estimate, given a set of observations, a probability distribution over a set of clusters, instead of only delivering the most similar cluster that the observation should belong to. Probabilistic approaches can be divided into two families: generative approaches and discriminative models. In generative approaches, the joint probability distribution can be used to generate new samples following the same distribution as the training data. On the contrary, discriminative models can compute membership probabilities, but are not suited to generate new data.

Main results In [46], we proposed non-parametric generative approaches based on the Expectation-Maximization algorithm, able to compute a Histogram Mixture Model of the data distribution, allowing it to deal with a much wider range of distributions than in previous algorithms. The main idea is to reduce the model complexity via different projections on independent axes and to compute a one-dimensional histogram for each of these axes. Axes being independent, the computation of the joint probability distribution is greatly simplified. The proposed approaches have a complexity comparable to the complexity of Gaussian Mixture Models, while being able to model a wider variety of distributions.

Scientific production and quality

	2016-2020
PhD Thesis	5
H.D.R	1
Journals	15
Major conferences	12
Other conferences	8
Book chapters	5
Books (written)	1
Special issues (edited)	0
Other productions from workshops	0
General audience papers	0
Participation in editorial committees	0
Evaluation of labs and research structures	0
European projects (as project manager/Member)	0
Other international projects (as project manager/Member)	0
ANR, PHRC, FUI, INCA, etc. (as project manager/Member)	0+2
Projects with Region Grand Est, etc (as project manager/Member)	0
PIA (as project manager/Member)	0
Others (as project manager/Member)	2+2
Prizes and distinctions	0
IUF	0
Responsibilities in scientific communities (GDR etc.)	0
Organizations of Conferences (national/international)	1+1
Invitations (national/international)	0+1
Stays in foreign laboratories	0

1 List of top journals in which we have published

Automatica (2) [8, 12]
IEEE Transactions on Neural Networks and Learning Systems (1) [19]
Journal of Computer and System Sciences (1) [9]
Neurocomputing (2) [13, 16]

2 List of top conferences in which we have published

AISTATS (1) [32]
NeurIPS (formerly NIPS) (1) [24]

3 Software

MLweb ([13], `http://mlweb.loria.fr/`) is an open source software that aims at bringing machine learning capabilities into web pages and web applications, while maintaining all computations on the client side. It includes:

- LALOLib: a Javascript library that enables and eases scientific computing in web pages or applications
- ML.js: a Javascript library that implements state-of-the-art machine learning algorithms for the web
- LALOLab: an online Matlab-like environment for numerical computing and machine learning

The academic reputation and appeal

❶ Participation in projects and External funding

From 2016 to 2018, Yann Guermeur was the leader of the PEPS "Apprentissage, Risques Garantis Multi-classes et Inférence de Noyau" (ARGMIN) that strengthened our collaboration with Nicolas Wicker's team (see Section 1.3.5). The other members of the team involved in the project are Aya El Dakdouki, Fabien Lauer and Khadija Musayeva.

Fabien Lauer is the project manager of the AIHD project funded for 140kE by the Mirabelle+ call of the Lorraine University of Excellence initiative (LUE) that aims at promoting interdisciplinary research. This project aims at proposing data-based solutions for diagnosis and prognosis applications related to heart diseases (the early detection of atrial fibrillation and the prediction of the outcome a catheter ablation).

❷ Prizes and Distinctions

Yann Guermeur gave an invited talk entitled "Rademacher complexity of margin multi-category classifiers" [17] at the WSOM+ 17 workshop. He addressed the same topic in the invited talk that he gave in 2018 at the Dagstuhl Seminar 18291 on Extreme Classification.

Parisa Rastin gave an invited talk at the "Workshop on Machine Learning and Applications" (IC|ECCO-2019).

❸ Editorial and organizational activities

Yann Guermeur has been a member of the program committee of the ICML conference since 2018 and the CAp conference since 2003. He also served as a member of the program committee of the conferences AAFD'16 & SFC'16, SFC'17-19, CIFSD'18-21, AISTATS 2017-2018, WCGO 2019 and WSOM+ 2019. He is an organizer of the conference "IA et entreprises" (https://www.mathconf.org/caic2021).

Parisa Rastin was an organizer of the "5th International Workshop on Advances in Learning from/with Multiple Learners" (ALML 2019, https://www-lipn.univ-paris13.fr/~grozavu/ALML2019/default.html).

❹ Services as expert or evaluator

Yann Guermeur is a regular evaluator for the ANR, the ANRT and the Croatian Science Foundation. During the evaluation period, he took part in 12 PHD and HDR committees.

Fabien Lauer was an evaluator for the artificial intelligence committee of the ANR in 2019. He was also a member of 2 Ass. Prof. selection committees.

Parisa Rastin took part in a PHD committee.

5 Collaborations

Our main collaboration in statistics is with Nicolas Wicker, at the Paul Painlevé laboratory, in Lille. He was with Yann Guermeur the PhD advisor of Aya El Dakdouki [2]. This thesis gave birth to two major contributions. The first one is the introduction of a new kernel function for pattern classification. Designed to detect translation invariance inside classes, it is obtained as a Fourier transform of a Gaussian mixture model. The second contribution is a class of quadratic kernel machines. The corresponding papers are currently under review.

Since september 2019, we are collaborating with the CAPSID research team on a problem of structural biology: the inference of the structure of protein-RNA complexes. Isaure Chauvot de Beauchêne and Yann Guermeur are the co-advisors of a PhD student working on this topic, Antoine Moniot [37].

We also have a collaboration with Marion Gilson, at the Center for Automatic Control of Nancy (CRAN), who is co-advisor of the PhD of Louis Massucci on the estimation of models of hybrid dynamical systems and, more broadly, the interplay between learning theory and system identification [33].

Other local collaborations with Marianne Clausel, at the Institut Elie Cartan de Lorraine (IECL), and Julien Oster, at the Diagnosis and interventional Adaptive Imaging (IADI, Inserm), were fostered in the framework of the AIHD project on data-driven solutions for applications related to heart diseases.

6 Invitations and stays outside

Involvement with social, economic and cultural environment

	2016-2020
Software	1
APP (Software)	0
Patents (Brevet)	0
Contracts with companies	0
Cifre	1
Contracts, Consortium	0
Start-up	0
Expertizes	0
Radio broadcasts, TV, Newspapers	0
Scientific mediation : articles, interviews, videos, etc.	0

1 Relations with companies and economic players

Félix Gaschi, PhD student advised by Parisa Rastin, is funded by a Cifre between Posos (https://www.posos.co/) and the UL. Parisa Rastin is also involved in a contract between the ENSMN and Saint Gobain.

❷ General public audience activities

Part of the MLweb software project ([13], http://mlweb.loria.fr/) aim was to democratize machine learning through the dissemination of scientific knowledge and practical tools at different levels and for different users (scientists, web developers, or merely curious people).

The involvement in training through research

	2016-2020
Course books, etc	0
E-learnings, MOOC	0
Heads of masters (mention and parcours)	1 (M1)
Heads of international courses (Erasmus-mundus, etc)	0

❶ Involvement of the team in training through research

Fabien Lauer is responsible for a number of artificial intelligence and machine learning courses that he created. In particular, he is in charge of the machine learning courses in the final year at Polytech Nancy and also involved in the *M2 AVR*, the speciality of the computer science master dealing with Learning, Vision and Robotics, where he teaches statistical learning.

❷ Involvement in E-Educations

❸ Courses and research schools.

❹ Responsibilities

Since 2016, Fabien Lauer has been the head of the *M1 Informatique* (1st year of Master in Computer Science) in Nancy. This responsibility includes the participation to the admission committee and the processing of about a thousand applications each year.

Life of the team

	2016-2020
Nb of seminars	12
Web site	1

References

Doctoral Dissertations

[1] Mounia Hendel. “Bio-inspired methods applied to real-time analysis of biomedical signals”. PhD thesis. Université Mohamed Boudiaf des Sciences et de la Technologie - Mohamed Boudiaf d'Oran, February 2017. tel-03042290.

[2] Aya El Dakdouki. “Hyperbolic Support Vector Machine and Kernel design”. PhD thesis. Université de Lille 1, Sciences et Technologies ; Loria & Inria Grand Est ; LORIA - ALGO - Department of Algorithms, Computation, Image and Geometry, September 2019. tel-03087889.

[3] Erinc Merdivan. “Ambient Assisted Living with Deep Learning”. PhD thesis. CentraleSupélec, December 2019. tel-02927785.

[4] Khadija Musayeva. “Generalization Performance of Margin Multi-category Classifiers”. PhD thesis. Université de Lorraine, September 2019. tel-02387124.

[5] Antoine Mahé. “System identification with neural networks for model predictive control”. PhD thesis. CentraleSupélec, Université Paris-Saclay, December 2020. tel-03081633.

Habilitation Theses

[6] Fabien Lauer. “Optimization and statistical learning theory for piecewise smooth and switching regression”. Habilitation à diriger des recherches. Université de Lorraine, October 2019. tel-02307957.

Articles in International Peer-Reviewed Journal

[7] Mounia Hendel, Abdelkader Benyettou, and Fatiha Hendel. “Hybrid self organizing map and probabilistic quadratic loss multi-class support vector machine for mental tasks classification”. In: *Informatics in Medicine Unlocked* 4 (September 2016), pp. 1–9. DOI: 10.1016/j.imu.2016.09.001. hal-03033964.

[8] Fabien Lauer. “On the complexity of switching linear regression”. In: *Automatica* 74 (2016). arXiv: 1510.06920, pp. 80–83. DOI: 10.1016/j.automatica.2016.07.027. hal-01219794.

[9] Yann Guermeur. “L p -norm Sauer-Shelah Lemma for Margin Multi-category Classifiers”. In: *Journal of Computer and System Sciences* 89 (November 2017), pp. 450–473. DOI: 10.1016/j.jcss.2017.06.003. hal-01371331.

[10] Tamás S. ILLES, Máté Burkus, Szabolcs Somoskeoy, Fabien LAUER, François Lavaste, and Jean F. DUBOUSSET. “The horizontal plane appearances of scoliosis: what information can be obtained from top-view images?” In: *International Orthopaedics* 41.11 (2017), pp. 2303–2311. DOI: 10.1007/s00264-017-3548-5. hal-01665134.

[11] Tamás Illés, Máté Burkus, Szabolcs Somoskeöy, Fabien Lauer, François Lavaste, and Jean Dubousset. “Axial plane dissimilarities of two identical Lenke-type 6C scoliosis cases visualized and analyzed by vertebral vectors”. In: *European Spine Journal* 27.9 (2018), pp. 2120–2129. DOI: 10.1007/s00586-018-5577-1. hal-02060150.

[12] Fabien Lauer. "Global optimization for low-dimensional switching linear regression and bounded-error estimation". In: *Automatica* 89 (2018). arXiv: 1707.05533, pp. 73–82. DOI: 10.1016/j.automatica.2017.11.026. hal-01563788.

[13] Fabien Lauer. "MLweb: A toolkit for machine learning on the web". In: *Neurocomputing* 282 (2018), pp. 74–77. DOI: 10.1016/j.neucom.2017.11.069. hal-01646613.

[14] Fabien Lauer. "On the exact minimization of saturated loss functions for robust regression and subspace estimation". In: *Pattern Recognition Letters* 112 (2018). arXiv: 1806.05833, pp. 317–323. DOI: 10.1016/j.patrec.2018.08.004. hal-01815451.

[15] Erinc Merdivan, Deepika Singh, Sten Hanke, and Andreas Holzinger. "Dialogue Systems for Intelligent Human Computer Interactions". In: *Electronic Notes in Theoretical Computer Science* 343 (May 2019), pp. 57–71. DOI: 10.1016/j.entcs.2019.04.010. hal-03081682.

[16] Khadija Musayeva, Fabien Lauer, and Yann Guermeur. "Rademacher Complexity and Generalization Performance of Multi-category Margin Classifiers". In: *Neurocomputing* 342 (2019). arXiv: 1812.00584, pp. 6–15. DOI: 10.1016/j.neucom.2018.11.096. hal-01941089.

[17] Yann Guermeur. "Rademacher Complexity of Margin Multi-category Classifiers". In: *Neural Computing and Applications*. Neural Computing and Applications 32.24 (December 2020), pp. 17995–18008. DOI: 10.1007/s00521-018-3873-7. hal-02377345.

[18] Tamás Illés, Stig M. Jespersen, Pieter Reynders, Fabien Lauer, J.-C. Le Huec, and Jean-François DUBOUSSET. "Axial plane characteristics of thoracic scoliosis and their usefulness for determining the fusion levels and the correction technique". In: *European Spine Journal* 29 (2020), pp. 2000–2009. DOI: 10.1007/s00586-020-06390-y. hal-03382549.

[19] Fabien Lauer. "Error Bounds for Piecewise Smooth and Switching Regression". In: *IEEE Transactions on Neural Networks and Learning Systems* 31.4 (2020). arXiv: 1707.07938, pp. 1183–1195. DOI: 10.1109/TNNLS.2019.2919444. hal-01566136.

[20] Erinc Merdivan, Deepika Singh, Sten Hanke, Johannes Kropf, Andreas Holzinger, and Matthieu Geist. "Human Annotated Dialogues Dataset for Natural Conversational Agents". In: *Applied Sciences* 10.3 (February 2020), p. 762. DOI: 10.3390/app10030762. hal-03081727.

[21] Rahimeh Rouhi, Marianne Clausel, Julien Oster, and Fabien Lauer. "An Interpretable Hand-Crafted Feature-Based Model for Atrial Fibrillation Detection". In: *Frontiers in Physiology* 12 (May 2021), p. 657304. DOI: 10.3389/fphys.2021.657304. hal-03382590.

Invited Conferences

[22] Walter C.P.M. Blondel, Faiza Abdat, Marine Amouroux, and Yann Guermeur. "Multimodality fibered in vivo spectroscopy applied to skin hyperplastic and dysplastic class discrimination: spatially resolved data fusion-based classification". In: *Asia Communications and Photonics Conference, ACP 2017*. Guangzhou, China, November 2017. hal-01637378.

Major International Conferences

[23] Anush Manukyan, Olivares-Mendez Miguel, Holger Voos, and Matthieu Geist. "Real time degradation identification of UAV using machine learning techniques". In: *International Conference on Unmanned Aircraft Systems (ICUAS)*. Miami, United States, 2017. hal-01629680.

[24] Erinc Merdivan, Mohammad Reza Loghmani, and Matthieu Geist. "Reconstruct & Crush Network". In: *Advances in Neural Information Processing Systems*. Long Beach, United States, 2017. hal-01629742.

[25] Deepika Singh, Erinc Merdivan, Ismini Psychoula, Johannes Kropf, Sten Hanke, Matthieu Geist, and Andreas Holzinger. "Human activity recognition using recurrent neural networks". In: *1st International Cross-Domain Conference for Machine Learning and Knowledge Extraction (CD-MAKE)*. Ed. by Andreas Holzinger, Peter Kieseberg, A Min Tjoa, and Edgar Weippl. Vol. LNCS-10410. Machine Learning and Knowledge Extraction. Part 5: MAKE AAL. Reggio, Italy: Springer International Publishing, August 2017, pp. 267–274. DOI: 10.1007/978-3-319-66808-6_18. hal-01629704.

[26] Antoine Mahé, Cédric Pradalier, and Matthieu Geist. "Trajectory-control using deep system identification and model predictive control for drone control under uncertain load". In: *2018 22nd International Conference on System Theory, Control and Computing (ICSTCC)*. Sinaia, Romania: IEEE, October 2018. DOI: 10.1109/ICSTCC.2018.8540719. hal-01927035.

[27] Khadija Musayeva, Fabien Lauer, and Yann Guermeur. "A sharper bound on the Rademacher complexity of margin multi-category classifiers". In: *ESANN 2018*. Proceedings of the 26th European Symposium on Artificial Neural Networks, Computational Intelligence and Machine Learning (ESANN), Bruges, Belgium. Bruges, Belgium, April 2018, pp. 503–508. hal-03011325.

[28] Ismini Psychoula, Erinc Merdivan, Deepika Singh, Liming Chen, Feng Chen, Sten Hanke, Johannes Kropf, Andreas Holzinger, and Matthieu Geist. "A Deep Learning Approach for Privacy Preservation in Assisted Living". In: *2018 IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom Workshops)*. Athens, Greece: IEEE, March 2018, pp. 710–715. DOI: 10.1109/PERCOMW.2018.8480247. hal-03081669.

[29] Jose Terius-Padron, Georgios Kapidis, Sarah Fallmann, Erinc Merdivan, Sten Hanke, Rebeca Garcia-Betances, and Maria Fernanda Cabrera-Umpierrez. "Towards Self-management of Chronic Diseases in Smart Homes : Physical Exercise Monitoring for Chronic Obstruction Pulmonary Disease Patients". In: *2018 IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom Workshops)*. Athens, Greece: IEEE, March 2018, pp. 776–781. DOI: 10.1109/PERCOMW.2018.8480163. hal-03081677.

[30] Antoine Mahé, Antoine Richard, Benjamin Mouscadet, Cedric Pradalier, and Matthieu Geist. "Importance Sampling for Deep System Identification". In: *19th International Conference on Advanced Robotics (ICAR)*. Belo Horizonte, Brazil, 2019. DOI: 10.1109/ICAR46387.2019.8981590. hal-02278171.

[31] Erinc Merdivan, Anastasios Vafeiadis, Dimitrios Kalatzis, Sten Hanke, Joahannes Kroph, Konstantinos Votis, Dimitrios Giakoumis, Dimitrios Tzovaras, Liming Chen, Raouf Hamzaoui, and Matthieu Geist. "Image-Based Text Classification using 2D Convolutional Neural Networks". In: *2019 IEEE SmartWorld, Ubiquitous Intelligence & Computing, Advanced & Trusted Computing, Scalable Computing & Communications, Cloud & Big*

D1 : ABC

Data Computing, Internet of People and Smart City Innovation (SmartWorld/SCALCOM/UIC/ATC/CBDCom/IOP/SCI). Leicester, United Kingdom: IEEE, August 2019, pp. 144–149. DOI: 10.1109/SmartWorld-UIC-ATC-SCALCOM-IOP-SCI.2019.00066. hal-03081713.

[32] Fabien Lauer. "Risk Bounds for Learning Multiple Components with Permutation-Invariant Losses". In: *23rd International Conference on Artificial Intelligence and Statistics (AISTATS)*. Vol. PMLR: Volume 108. Proceedings of the 23rd International Conference on Artificial Intelligence and Statistics (AISTATS), Palermo, Italy. arXiv: 1904.07594. Palermo, Italy, 2020. hal-02100779.

[33] Louis Massucci, Fabien Lauer, and Marion Gilson. "Structural risk minimization for switched system identification". In: *59th IEEE Conference on Decision and Control, CDC 2020*. Proceedings of the 59th IEEE Conference on Decision and Control (CDC). Jeju Island, South Korea, December 2020. hal-02942279.

[34] Erinc Merdivan, Sten Hanke, and Matthieu Geist. "Modified Actor-Critics". In: *AAMAS2020 - International Conference on Autonomous Agents and MultiAgent Systems*. virtual, New Zealand, May 2020. hal-03081704.

Secondary International Conferences

[35] Yann Guermeur. "Rademacher complexity of margin multi-category classifiers". In: *12th International Workshop on Self-Organizing Maps and Learning Vector Quantization, Clustering and Data Visualization (WSOM+)*. Nancy, France, June 2017. hal-02982728.

[36] Khadija Musayeva, Fabien Lauer, and Yann Guermeur. "Metric entropy and Rademacher complexity of margin multi-category classifiers". In: *26th International Conference on Artificial Neural Networks (ICANN)*. Vol. 10614 of LNCS. Proceedings of the 26th International Conference on Artificial Neural Networks (ICANN) 2. Alghero, Italy, September 2017, p. 767. hal-03011347.

[37] Antoine Moniot, Rohit Roy, Yann Guermeur, and Isaure Chauvot de Beauchêne. "Docking of RNA Hairpin on Protein Using a Fragment-Based Method". In: *JOBIM 2020 - Journées Ouvertes en Biologie, Informatique et Mathématiques*. Montpellier, France, June 2020. hal-02927185.

[38] Alix Delannoy, Antoine Moniot, Yann Guermeur, and Isaure Chauvot de Beauchêne. "Feature extraction for the clustering of small 3D structures: application to RNA fragments". In: *JOBIM 2021 - Journées Ouvertes en Biologie, Informatique et Mathématiques*. Paris/Virtual, France, July 2021, pp. 1–6. hal-03540927.

[39] Félix Gaschi, Parisa Rastin, and Yannick Toussaint. "Unsupervised Word embedding Alignment in the biomedical domain". In: *CIFSD 2021 - Conférence Internationale Francophone sur la Science des Données*. Marseille/Virtuel, France, June 2021. hal-03259987.

[40] Louis Massucci, Fabien LAUER, and Marion Gilson. "How statistical learning can help to estimate the number of modes in switched system identification?" In: *19th IFAC Symposium on System Identification, SYSID 2021*. Padova (Virtual Event), Italy, July 2021. hal-03324069.

[41] Louis Massucci, Fabien LAUER, and Marion Gilson. "Regularized switched system identification: A statistical learning perspective". In: *7th IFAC International Conference on Analysis and Design of Hybrid Systems, ADHS'2021*. Brussel (Virtual Event), Belgium, July 2021. hal-03324120.

D1 : ABC

National Peer-Reviewed Conferences

[42] Fabien Lauer. "Error bounds with almost radical dependence on the number of components for multi-category classification, vector quantization and switching regression". In: *CAP2018 - Conférence sur l'Apprentissage automatique (CAp) - French Conference on Machine Learning (FCML)*. Proc. of the French Conference on Machine Learning (CAp/FCML). Rouen, France, June 2018. hal-01815406.

Book (written)

[43] Fabien Lauer and Gérard Bloch. *Hybrid System Identification : Theory and Algorithms for Learning Switching Models*. Springer, 2019. hal-01860332.

Books or Proceedings Editing

Book Chapters

[44] Yann Guermeur and Fabien Lauer. "A generic approach to biological sequence segmentation problems, application to protein secondary structure prediction". In: *Pattern Recognition in Computational Molecular Biology: Techniques and Approaches*. Ed. by Mourad Elloumi, Costas Iliopoulos, Jason T. L. Wang, and Albert Y. Zomaya. Wiley, 2016, pp. 114–128. DOI: 10.1002/9781119078845.ch7. hal-01253820.

[45] Deepika Singh, Erinc Merdivan, Sten Hanke, Johannes Kropf, Matthieu Geist, and Andreas Holzinger. "Convolutional and Recurrent Neural Networks for Activity Recognition in Smart Environment". In: *Towards Integrative Machine Learning and Knowledge Extraction*. Ed. by A. Holzinger, R. Goebel, M. Ferri, and V. Palade. Vol. 10344. Lecture Notes in Computer Science. springer, 2017, pp. 194–205. hal-01629732.

[46] Parisa Rastin, Guénaël Cabanes, Rosanna Verde, Younès Bennani, and Thierry Couronne. "Generative Histogram-Based Model Using Unsupervised Learning". In: *Neural Information Processing*. December 2019, pp. 634–646. DOI: 10.1007/978-3-030-36718-3_53. hal-02994819.

[47] Deepika Singh, Ismini Psychoula, Erinc Merdivan, Johannes Kropf, Sten Hanke, Emanuel Sandner, Liming Chen, and Andreas Holzinger. "Privacy-Enabled Smart Home Framework with Voice Assistant". In: *Smart Assisted Living*. August 2020, pp. 321–339. DOI: 10.1007/978-3-030-25590-9_16. hal-03081721.

[48] Félix Gaschi, Parisa Rastin, and Yannick Toussaint. "Handling the Deviation from Isometry Between Domains and Languages in Word Embeddings: Applications to Biomedical Text Translation". In: *Neural Information Processing*. Vol. 13109. Lecture Notes in Computer Science. Springer International Publishing, December 2021, pp. 216–227. DOI: 10.1007/978-3-030-92270-2_19. hal-03477901.

Other Publication

[49] Antoine Richard, Antoine Mahé, Cedric Pradalier, Offer Rozenstein, and Matthieu Geist. "A Comprehensive Benchmark of Neural Networks for System Identification". working paper or preprint. September 2019. hal-02278102.

[50] Yann Guermeur. "Combinatorial and Structural Results for γ-Ψ-dimensions". arXiv: 1809.07310v3 - working paper or preprint. September 2020. hal-03230918.

[51] Antoine Moniot, Isaure Chauvot de Beauchêne, and Yann Guermeur. *Agglomerative clustering of fragment 3D structures based on pairwise RMSD*. ISMB ECCB 2021. Poster. July 2021. hal-03432682.

[52] Antoine Moniot, Isaure Chauvot de Beauchêne, and Yann Guermeur. *New clustering method to infer prototypes covering the 3D structures of nucleic acid fragments*. RECOMB 2021 - 25th International conference on research in computational molecular biology. Poster. August 2021. hal-03432671.

Applying Discrete Algorithms to Geometry and Imagery

Synopsis

1 Team Composition

Permanents

Isabelle Debled-Rennesson (PR UL), Eric Domenjoud (CR CNRS), Philippe Even (PR UL), Bertrand Kerautret (MCF UL, left 31/08/18), Phuc Ngo (MCF UL).

	2016	2017	2018	2019	2020	Total
PR	2	2	2	2	2	
MCF	2	2	2	1	1	
DR						
CR	1	1	1	1	1	
Other						
Total (permanent positions)	5	5	5	4	4	
Pr emeritus						
Guest researchers						
Post-doct. researchers						
PhD Students	2	2	1	1	2	
Master students M2	1	1	1	1	2	
Master Students M1	1	1		1	1	
L3 students				1	1	
Engineers						
Other	1		1	2		
Total (temporary positions)	5	4	3	6	6	

Change in team composition

Bertrand Kerautret left the ADAGIo team in September 2018. He is now professor at the University of Lyon, at the LIRIS.

Doctoral students

Nicolas Aubry (CIFRE contract with the Numalliance company, oct 2013 - jul 2017), Hayat Nasser (Erasmus doctoral contract, dec 2013 - oct 2018), Rémi Decelle (ANR TreeTrace doctoral contract, oct 2018 - ...), Florian Delconte (ANR WoodSeer-Region doctoral contract, janv 2020 - ...).

	2016-2020
Phd's defended	2
On-going PhD's	2
Average nb of papers by PhD student	4
Average duration of PhD thesis (in month)	50

Hayat Nasser is a teacher and researcher in Lebanon.
Nicolas Aubry is a research engineer at the Numalliance company where he did his CIFRE doctoral contract.

2 Research topics

Keywords

Discrete Geometry, Discrete Algorithms, Discrete Structures, Word Combinatorics, Image Analysis, Digital Topology and Transformations.

Research area and main goals

The general research area of our team is *discrete algorithms*. Constructing a discrete model of a real-world phenomenon means, in mathematical terms, representing it through a *discrete structure*, such as graphs, words, trees, sets of points in a space, etc.

In order to develop efficient algorithms on discrete structures and to analyze and optimize those algorithms, we have to understand thoroughly the properties of the underlying structures. These properties can be *geometrical*, *arithmetical* or *combinatorial* depending on the situation. The study of these properties is the main objective of our team.

To be more specific, we are mainly interested in the fundamental study within the area of *Discrete Geometry* of discrete objects having a geometric (planar or spatial) interpretation. The general goal of *Discrete Geometry* is to define a theoretical framework to translate to $\mathbb{Z}^n$ basic notions of the Euclidean geometry (such as distance, length, convexity, ...) as "faithfully" as possible. Several approaches exist to pursue this goal[26]. In our studies, we follow an arithmetical approach, where discrete objects, such as straight lines or planes, are defined with arithmetical definitions. These analytical definitions allow us to represent in a compact way any elementary digital object, to study some objects that are intrinsically discrete (and are not only approximations of continuous objects), and to define infinite discrete objects.

The study of the properties of discrete objects such as straight lines, circles, planes, curves and discrete surfaces always remains a topical subject in the last leading conferences of the domain (DGCI and IWCIA). These topics are studied by our team and more particularly the study of noisy discrete curves and surfaces. Our aim is to determine, in the framework of discrete geometry, a paradigm adapted to these objects, taking into account the noise associated with acquisition tools and methods.

[26] J-M. Chassery and A. Montanvert. *Géométrie discrète en imagerie*. Paris: Hermès, 1991.

Other points of interest of our team are the areas of *Text Algorithm and Words Combinatorics* which have been very actively developed for the last years, as witnessed by the publication of several monographs[27]. On the one hand, Sturmian words are well known to code the digitization of lines with irrational slopes. One of our main subject of interest is the study of *natural* extensions of such sequences in any dimension in order to code arithmetical discrete hyperplanes of any dimension. On the other hand, we focus on the introduction of relevant tools for such objects, such as multidimensional substitutions which have links with many other theories, such as number theory, topology or formal language theory.

Our algorithms are naturally used in the application area of Imagery.

3 Main Achievements

Since 2016, four important facts have oriented the research activities of ADAGIo team:
1. The study of ***facet connectedness of arithmetic discrete hyperplanes*** has been brought almost to an end by providing a method for computing the connecting thickness and general conditions on the normal vector and the shift under which the hyperplane is connected at this critical thickness.
2. A new discrete structure, called the ***Adaptive Tangential Cover*** (ACT), using a local noise estimator, permits to develop several performant tools to characterize discrete noisy curves and opens new research perspectives in 3D.
3. New digital geometry algorithms and tools have been developed (adaptive directional data scan and blurred segment thickness estimation), validated in different data structures (gray-level images, sparse 3D point cloud), and disseminated through publicly available softwares.
4. The ***collaboration with INRAE***, through two ANR projects and two PhD theses, was very fruitful (numerous publications in computer science and biology) on several subjects in relation with Discrete Geometry and Image Analysis.

4 Research activities

Discrete geometric primitives and transforms

Description Among the basic primitives available in geometry, we can find digital straight line segments. We focus on the arithmetical viewpoint, introduced by Jean-Pierre Reveillès[28]. In this framework, a **digital straight line** is the set of points with coordinates (x, y) of $\mathbb{Z}^2$ verifying the double diophantine inequality $\mu \leqslant ax - by < \mu + \omega$, with a, b, μ, ω integer. The notion of ***arithmetic discrete hyperplanes*** is a generalization in $\mathbb{Z}^2$ of this notion.

Words combinatorics provides many powerful tools for the study of discrete objects such as lines or planes. Such objects have natural encodings as finite or infinite words on finite alphabets. For instance, a discrete line is encoded as a balanced word over the alphabet $\{0, 1\}$ and a discrete plane may be encoded as a 2-dimensional word over the alphabet $\{0, 1\}$. We use tools from words combinatorics to count some patterns in these objects or to study some global properties such as the connectivity.

[27] D. Gusfield. *Algorithms on Strings, Trees, and Sequences.* Cambridge University Press, 1997, M. Crochemore, C. Hancart, and T. Lecroq. *Algorithmique du texte.* Vuibert Informatique, 2001.
[28] J-P. Reveillès. "Géométrie discrète, calculs en nombre entiers et algorithmique". Thèse d'état. Université Louis Pasteur, Strasbourg, 1991.

Main results

Connectedness of discrete hyperplanes

We continued our study of the facet connectedness of discrete digital hyperplanes. Given a normal vector $v \in \mathbb{R}^d$, a thickness $\theta \in \mathbb{R}$ and a shift $\mu \in \mathbb{R}$, the discrete digital hyperplane $\mathbb{P}(v, \theta, \mu)$ is the set of integral points defined by

$$\mathbb{P}(v, \theta, \mu) = \{x \in \mathbb{Z}^d \mid 0 \leqslant \langle v, x \rangle + \mu < \theta\}.$$

There always exists a critical thickness $\Theta(v, \mu)$ such that $\mathbb{P}(v, \theta, \mu)$ is non empty and connected for all $\theta > \Theta(v, \mu)$ and empty or disconnected for all $\theta < \Theta(v, \mu)$. In a previous work[29], we proved that when $\theta = \Theta(v, \mu)$, $\mathbb{P}(v, \theta, \mu)$ is almost always disconnected, excepted when v belongs to some Lebesgue-negligible set $\mathcal{K}_d$. In this case, $\Theta(v, \mu)$ does not depend on μ and $\mathbb{P}(v, \Theta(v), \mu)$ may be connected or not, depending on μ. In particular, we proved that when $v \in \mathcal{K}_d$, $\mathbb{P}(v, \Theta(v), 0)$ is always connected and $\mathbb{P}(v, \Theta(v), \Theta(v))$ is disconnected. We continued this study [21] and gave a full characterization of the shifts μ for which $\mathbb{P}(v, \Theta(v), \mu)$ is connected. The shift is encoded in a numeration system associated with the normal vector v. The codes of shifts for which the hyperplane is connected may then be recognized by an automaton which is finite when the normal vector has some additional property. In this case, the codes of shifts for which the hyperplane is connected belong to a regular language.
We also studied the hyperplanes at the critical thickness from a combinatorial point of view [4]. We showed that the adjacency graph of these hyperplanes is actually a tree, each leaf of which may be labelled with a palindrom in the language $\{1, \ldots, d\}^\star$.

Shape preservation under digital rigid motions

Rigid motion, composed of translation and rotation, is defined by a bijective function in continuous space. It is well-known that rigid motions preserve the shape of objects thanks to their isometry in $\mathbf{R}^n$. These transformations, when considered in the discrete spaces of digital images, generally lose these important properties comparing to their continuous counterparts, due to the digitization required to obtain a result in $\mathbf{Z}^n$. Indeed, this digitization leads to geometric and topological alterations in the transformed space [24]. These problems of geometric and topological preservation by geometric transformations have been little studied so far. In view of these considerations, we proposed a purely discrete framework for 2D / 3D rigid transformations, by relying on concepts of discrete geometry and topology. In particular, we are interested in the characterizations of digital images allowing to preserve their topological and geometric properties by arbitrary rigid motions. The motivation for this study is multiple, not only from a theoretical point of view but also in practice, because it is interested in many applications of image processing and analysis. More precisely, a condition on 2D digital images, called *quasi-r-regularity*, has been introduced in [17, 10] allowing to preserve convexity and topology by all digitized rigid motions. This notion is extended to 3D [20] and to 2D non-convex objects [35]. We also proposed an algorithmic scheme allowing the modeling and the manipulation of rigid motions, adapted to the discrete spaces of digital images. More particularly, this notion of quasi-r-regularity makes it possible to verify and characterize 2D / 3D objects preserving geometric and topological measurements by the digitization process.

Blurred segment detection in gray-level images

[29] Eric Domenjoud, Xavier Provençal, and Laurent Vuillon. "Facet Connectedness of Discrete Hyperplanes with Zero Intercept: The General Case". In: *18th IAPR International Conference, DGCI 2014*. Ed. by Elena Barcucci, Andrea Frosini, and Simone Rinaldi. Vol. 8668. 18th IAPR International Conference, DGCI 2014, Siena, Italy, September 10-12, 2014. Proceedings. Siena, Italy: Springer International Publishing, September 2014, pp. 1–12. DOI: 10.1007/978-3-319-09955-2_1. hal-01083101.

A blurred segment[30] is defined as a set of points that all belong to a digital straight segment of fixed thickness (the assigned thickness). A new blurred segment detector from gray-level images was realized [22]. The thickness value is used to enrich the image straight edges with a quality indication. The detection framework is based on the analysis of the image gradient magnitude and orientation. It solves two main defaults of a former detector[31]. The new detector works in supervised mode for live extraction of individual segments, as does the former one. A fully automatic algorithm was also devised to extract all the blurred segments found in the image. Compared to three recent detectors, it shows equivalent performance in execution time and accuracy. The source code was made available on a *GitHub* repository: https://github.com/evenp/FBSD and an on-line demonstration can be found at:
http://ipol-geometry.loria.fr/~kerautre/ipol_demo/FBSD_IPOLDemo

Analysis of Discrete Objects

Description The study of arithmetical, geometrical and combinatorial properties of the discrete primitives is crucial to obtain efficient algorithms (recognition, scanning, ...) and to extract geometrical parameters (perimeter, curvature, normal vector, area, ...) on the curves and surfaces. We used in this part the obtained recognition algorithms of discrete primitives such as digital straight line segments, blurred segments[32], pieces of blurred digital planes, ... The principal idea, used in several of the presented works, is to decompose a discrete curve (or surface) in a sequence of maximal primitives, it permits to obtain a significant information about the structure of the studied curve or surface. We then develop new tools to analyse discrete objects and to reconstruct some continuous representations of them. Two main axes can be distinguished:

- the ***multi-resolution analysis*** of discrete curves and surfaces provides progressive analysis and new information. This analysis is useful for the comparison, the classification or the simplification;
- the ***reconstruction of geometrical models*** with a controlled precision with respect to the original discrete curves or surfaces opens perspectives for the use of a post-processing task based on Euclidean geometry.

From these approaches, several applications are deduced.

Main results

Geometric tools for noisy digital contour analysis

With the increasing availability of digital images in which objects are scanned and recorded in the computer or by digital cameras, it becomes necessary to develop the appropriate approaches to this data. In this context, we investigated the different mathematical tools in the field of digital geometry to study such objects, and especially for discrete curves. These curves, derived

[30] I. Debled-Rennesson, F. Feschet, and J. Rouyer-Degli. "Optimal Blurred Segments Decomposition of Noisy Shapes in Linear Times". In: *Computers and Graphics* 30 (2006), pp. 30–36. URL: doi.org/10.1016/j.cag.2005.10.007.

[31] Bertrand Kerautret and Philippe Even. "Blurred segments in gray level images for interactive line extraction". In: *Proc. of Int. Workshop on Combinatorial Image Analysis*. Ed. by P. Wiederhold and R. P. Barneva. Vol. 5852. LNCS. 2009, pp. 176–186. URL: doi.org/10.1007/978-3-642-10210-3_14.

[32] I. Debled-Rennesson, F. Feschet, and J. Rouyer-Degli. "Optimal Blurred Segments Decomposition of Noisy Shapes in Linear Times". In: *Computers and Graphics* 30 (2006), pp. 30–36. URL: doi.org/10.1016/j.cag.2005.10.007.

from the contours of objects in the digital images, may contain noise induced by the physical properties inherent in the acquisition devices or by acquisition conditions.

Several tools have been developed to compute geometric characteristics on the discrete noisy curves. In particular, we proposed in [14, 7] a new discrete structure, called the *Adaptive Tangential Cover* (ACT), using the local noise estimator introduced in[33]. More precisely, ACT is composed of a sequence of maximum blurred segments[34] of variable thicknesses adapted to the irregular noise present along the curve. The sequence of segments in the ACT allows to extract the different geometric characteristics of the curve [32, 33, 16, 9, 23] such as dominant points, the curve length estimation, tangent and curvature at each point of the contour, polygonal simplification of the contour, the decomposition of a curve into circular arcs and segments.

The experimental results demonstrate the efficiency and robustness of the proposed structure, and it has been applied to hand gesture recognition [18]. This structure opens many perspectives and future works for studying and processing of noisy discrete curves, as well as applications in digital image processing such as pattern recognition, geometric analysis of the contour of the digital shapes.

Multilevel polygonal descriptor matching defined by combining discrete lines and force histogram concepts

We used a work[35] carried out in 2011 on the polygonalization of discrete shapes at several scales using discrete lines of increasing thickness. A force histogram[36] is calculated on each of the polygons obtained for a fixed number of directions, thus making it possible to obtain series of signatures giving spatial and discontinuities information which are characteristic of the shape. We deduced three pattern matching methods which were then tested experimentally and compared with approaches from the literature [11]. The results obtained are competitive and interesting, prospects are underway.

Center line extraction from 3D shapes and representation

In the framework of the industrial collaboration with the Numalliance company, we have studied a new method to analyse the shape of tubular objects [29, 13, 30]. The proposed method is based on surface normal accumulation and is able to extract a center line from various data types (from digital surface to 3d mesh of full or partial scan). This center line was used in several applications (see next subsection).

Applications in project frameworks

Description Since 2010, a strong collaboration has been initiated with INRAE researchers of Champenoux on problems related to the quality of wood from Lidar data, from CT scanners, from photos taken in the forest or in a sawmill. We are participating in two ANR projects in

[33] Bertrand Kerautret, Jacques-Olivier Lachaud, and Mouhammad Said. "Meaningful Thickness Detection on Polygonal Curve". In: *ICPRAM - International Conference on Pattern Recognition Applications and Methods - 2012*. Vilamoura, Portugal: SciTePress, February 2012, pp. 372–379. DOI: 10.5220/0003760903720379. hal-00780710.

[34] I. Debled-Rennesson, F. Feschet, and J. Rouyer-Degli. "Optimal Blurred Segments Decomposition of Noisy Shapes in Linear Times". In: *Computers and Graphics* 30 (2006), pp. 30–36. URL: doi.org/10.1016/j.cag.2005.10.007.

[35] Thanh Phuong Nguyen and Isabelle Debled-Rennesson. "A discrete geometry approach for dominant point detection". In: *Pattern Recognit.* 44.1 (2011), pp. 32–44.

[36] P. Matsakis and L. Wendling. "A New Way to Represent the Relative Position Between Areal Objects". In: *IEEE Transactions on Pattern Analysis and Machine Intelligence* 21(7) (1999), pp. 634–643.

this context : TreeTrace and WoodSeer (see descripton in next paragraph).

Our team also works in the scope of an interdisciplinary project of Université de Lorraine : (SolHoM-Fossard: *Interactions hommes-milieux et évolution des sols aux cours des deux derniers millénaires dans le massif du Fossard (Vosges)*), in collaboration with earth science laboratories in Nancy (LIEC, HISCANT, LOTERR).

In these different projects, we use models and algorithms developed in our team in discrete geometry as well as classic image analysis tools. New subjects in discrete geometry also appear in this context of applications.

Main results

Processing and analysis of wood images

The partnership with INRAE in Champenoux began with a project on the measurement of internal knots in logs from CT scanner images. A PhD thesis was defended on this subject in 2014 and work was continued in 2016 on the detection and measurement of nodes[37] [31, 5].

The **Franco-Austrian ANR project TreeTrace**, piloted by INRAE for France, started in 2018 and is interested in tracking logs from the forest to the sawmill in using biometric information from images of log sections. The solutions with low-cost and accessible technologies are investigated for estimating wood quality. For this, images of log cross-sections from low-cost sensors (digital or smartphone cameras) are considered with the exploitation of image processing techniques in order to extract geometric and biological characteristics from the wood images. Several methods [36, 37] are developed in the team for automatically detecting different characteristics on log-end images such as pith, growth rings, heartwood and sapwood.

Discrete geometry result on the detection of the center line of 3D objects [13, 30] has been used in a collaboration with another INRAE team (thesis committee of one of their doctoral student) on the detection of defects appearing on tree trunks from high resolution TLS (Terrestrial Laser Scanner) point cloud. Very interesting results were obtained during this collaboration [27, 15, 47, 12]. The **ANR WoodSeer project** started in 2019 following this work with similar objectives but with a greater scope. Our objective is to study a new approach by combining deep learning and geometry to realize these tasks; to our knowledge, very little work has been done in this direction. A PhD student works on this project and recently, a first approach, based on the notion of central line and the U-Net[38], has been proposed for detecting of defect zones. Further studies are under consideration for the robustness of the method as well as the implementation of a semantic segmentation for defect classification.

Linear structure extraction from LiDAR raw data

Airborne LiDAR is a 3D point acquisition technique based on a laser sensor embedded on a plane. This sensor has the capacity to penetrate a forest canopy to get ground point measurements. However, some dense vegetation can still intercept the laser signal, thus producing holes in the ground point distribution. Most processing tools use a digital terrain model, built by interpolating ground points. However, the users are not aware of possible interpolation errors in occluded areas. We propose a new supervised detector of linear structures (forest roads, ridge or hollow structures) from LiDAR raw data (i.e. the ground point cloud) [25]. Composed of

[37] Adrien Krähenbühl, Bertrand Kerautret, and Fabien Feschet. "Knot Detection from Accumulation Map by Polar Scan". In: *IWCIA*. vol. 9448. Combinatorial Image Analysis 0302-9743. Kolkata, India, November 2015. DOI: 10.1007/978-3-319-26145-4_26. hal-01261651.

[38] Olaf Ronneberger, Philipp Fischer, and Thomas Brox. "U-Net: Convolutional Networks for Biomedical Image Segmentation". In: *Medical Image Computing and Computer-Assisted Intervention – MICCAI 2015*. Ed. by Nassir Navab, Joachim Hornegger, William M. Wells, and Alejandro F. Frangi. Cham: Springer International Publishing, 2015, pp. 234–241.

500 m × 500 m large tiles, the digital terrain model is only used as user interface support. Ground points are mapped into a grid with 5 times smaller resolution (0.1 m × 0.1 m). Based on the digital geometry tools presented in 4 (adaptive directional scanners and control of assigned thickness to blurred segment recognition algorithm) and on quite simple models of the structures, the tool detects and tracks the cross profiles of the structure from the user-defined seed. Several hundred meters long structures are extracted in a fraction of a second. Time and accuracy tests on main forest roads confirmed the good performance of the framework.

Scientific production and quality

	2016-2020
PhD Thesis	2
H.D.R	1
Journals	9
Major conferences	25
Other conferences	4
Book chapters	1
Books (written)	0
Special issues (edited)	2
Other productions from workshops	0
General audience papers	0
Participation in editorial committees	
Evaluation of labs and research structures	
European projects (as project manager/Member)	
Other international projects (as project manager/Member)	
ANR, PHRC, FUI, INCA, etc. (as project manager/Member)	4
Projects with Region Grand Est, etc (as project manager/Member)	
PIA (as project manager/Member)	
Others (as project manager/Member)	
Prizes and distinctions	3
IUF	
Responsibilities in scientific communities (GDR etc.)	1
Organizations of Conferences (national/international)	2
Invitations (national/international)	
Stays in foreign laboratories	

❶ List of top journals in which we have published

Theoretical Computer Science (TCS) (1) [4]
Discrete Applied Mathematics (DAM) (1) [8]
Journal of Mathematical Imaging and Vision (JMIV) (2) [7, 10]
Journal of Computer and System Sciences (1) [9]

❷ List of top conferences in which we have published

International Conf. on Discrete Geometry for Computer Imagery (DGCI) (7) [14, 16, 17, 8, 19, 21, 24]
International Workshop on Combinatorial Image Analysis (IWCIA) (2) [18, 26]
International Conf. on Image Analysis and Processing (ICIAP) (1) [22]
International Conf. on Computer Analysis of Images and Patterns (CAIP) (2) [0, 23]
International Conference on Pattern Recognition (ICPR)(3) [13, 15, 20]
Congress of the International Society of Photogrammetry, Remote Sensing and Spatial Information SCiences (ISPRS) (1) [25]

❸ Software

DGtal library
B. Kerautret belongs to the main development team of the open source library for Digital Geometry programming (`DGtal`). The main objective is to structure different developments from the digital geometry and topology community. P. Ngo also contributes to DGtal library.
Image Processing On Line (IPOL): Partnership on Geometry
The partnership with the IPOL journal and the LORIA continues. IPOL is a research journal on image processing and image analysis, publishing algorithm description and source code with an online demonstration (http://ipol.im). The aim of this collaboration is to open the research domain of the journal to the topic of geometry and to facilitate/encourage journal submission on this field. This initiative was materialized by the purchase and the installation of a specialized server to host geometry based demonstrations. It is hosted at LORIA by the ADAGIo team (http://ipol-geometry.loria.fr/~kerautre/ipol_demo/).

The academic reputation and appeal

❶ Participation in projects and External funding

ADAGio team is a partner of two ANR projects :

- Franco-Austrian ANR project TreeTrace, piloted by INRAE for France, started in 2018. The PhD thesis of Rémi Decelle is funded by this project.
- ANR project WoodSeer, piloted by INRAE, started in 2019. The PhD thesis of Florian Delconte is co-funded by this project.

A grant from Region Grand-Est co-funded the PhD thesis of Florian Delconte.

We also participate to the ANR project VESSELX, piloted by Antoine Vacavant, institut Pascal, started in 2018.

P. Even and P. Ngo are members of an interdisciplinary project of Université de Lorraine : (SolHoM-Fossard: *Interactions hommes-milieux et évolution des sols aux cours des deux derniers millénaires dans le massif du Fossard (Vosges)*), in collaboration with earth science laboratories in Nancy (LIEC, HISCANT, LOTERR).

❷ Prizes and Distinctions

Rémi Decelle, PhD student, obtained a best paper award of the session *Low level Image Processing and Retrieval* at the IPAS conference [36] and he also obtained the prize of the best poster of the *Journées scientifiques du GDR Sciences du bois - nov 2019*.

The DGtal project (http://dgtal.org) has received the software award at the Symposium on Geometry Processing 2016 (june 20th-24th, Berlin). B. Kerautret, with other main developers, received this award.
He presented an invited talk at ”Journées de géométrie discrète et de morphologie mathématiques”, in 2017.

❸ Editorial and organizational activities

B. Kerautret was the co-chair and the co-organizer of the first and second edition of RRPR (workshop on Reproducible Research in Pattern Recognition.) in 2016 and 2018. He was co-editor of the proceedings, published in LNCS.
Members of ADAGIo team served as members of ***Steering Committee*** or ***Program Committee*** of international conferences (DGCI, IWCIA, ICPR, ICCVG, ICIAP, CIARP), as member of the ***Editorial Board*** of international journal (IPOL). They also participated in the review process of the international journals: PAMI, JMIV, PR, PRL, CVIU, DAM, TCS, RAIRO-TIA.

❹ Services as expert or evaluator

Members of ADAGIo team participated in 11 PhD committees, 2 HDR committees and were reviewers in 5 jurys. They were also asked to evaluate ANR projects.
Members of ADAGio team were members of 12 recruitment committees.

❺ Collaborations

A. Vacavant (ISIT lab, Le Puy en Velay): work on contour representation on irregular grid [16, 19].
J.-O. Lachaud (LAMA, Chambery): works related to centerline [29, 13, 30][39]
L. Vuillon (LAMA, Chambéry): work on digital hyperplanes [4, 21].
L. Wendling (LIPADE, Paris) : applications in image analysis[40].
F. Longuetaud, F Mothe (INRAE, Champenoux): work on the knot segmentation and work on TreeTrace project [31, 5, 37][41]

[39] Bertrand Kerautret, Adrien Krähenbühl, Isabelle Debled-Rennesson, and Jacques-Olivier Lachaud. “3D Geometric Analysis of Tubular Objects based on Surface Normal Accumulation”. In: *18th International Conference on Image Analysis and Processing*. Genova, Italy, September 2015. DOI: 10.1007/978-3-319-23231-7_29. hal-01139374.

[40] Isabelle Debled-Rennesson and Laurent Wendling. “Extraction of Successive Patterns in Document Images by a New Concept Based on Force Histogram and Thick Discrete Lines.” In: *18th International Conference on Image Analysis and Processing*. Vol. 9379. Image analysis and Processing - ICIAP 2015. Genova, Italy: springer, September 2015, pp. 387–397. hal-01262145.

[41] Jean-Romain Roussel, Frédéric Mothe, Adrien Krähenbühl, Bertrand Kerautret, Isabelle Debled-Rennesson, and Fleur Longuetaud. “Automatic knot segmentation in CT images of wet softwood logs using a tangential approach”. In: *Computers and Electronics in Agriculture* 104 (June 2014), pp. 46–56. DOI: 10.1016/j.compag.2014.03.004. hal-00981419.

VT Nguyen, T. Constant (INRAE, Champenoux): work on the tree defects and WoodSeer project [27, 15, 47, 12].
F. Feschet (IGCNC, Clermont): work on knot detection[42].
Y. Kenmochi (LIGM, Paris-Est), N. Passat(CRESTIC, Reims): digital rigid transformations [17, 8, 48, 35, 20, 49, 10, 24].

6 Invitations and stays outside

P. Ngo was invited to present her research results in seminars in two laboratories (LABRI, Bordeaux ; ICUBE, Strasbourg).
B. Kerautret presented an invited talk at "Journées de géométrie discrète et de morphologie mathématiques", in 2017. He also made several seminars about his research results and about Reproducible Research.

Involvement with social, economic and cultural environment

	2016-2020
Software	
APP (Software)	
Patents (Brevet)	
Contracts with companies	
Cifre	1
Contracts, Consortium	
Start-up	
Expertizes	
Radio broadcasts, TV, Newspapers	
Scientific mediation : articles, interviews, videos, etc.	1 [34]

1 Relations with companies and economic players

From September 2013 to July 2017, a collaboration was carried out with the *Numalliance* company through a CIFRE related to the segmentation and the measure of metal pipe generated by machine tools. Nicolas Aubry defended a PhD thesis on this topic with an ANRT grant.

2 General public audience activities

Most of our works is accompanied by a demonstration made available to the scientific community.

I. Debled-Rennesson organized each year from 2016 to 2019 a day of conferences and practical sessions for secondary school computer science teachers (see http://idees.loria.fr). P. Ngo and doctorants participated to the animation of a practical session.

[42] Adrien Krähenbühl, Bertrand Kerautret, and Fabien Feschet. "Knot Detection from Accumulation Map by Polar Scan". In: *IWCIA*. vol. 9448. Combinatorial Image Analysis 0302-9743. Kolkata, India, November 2015. DOI: 10.1007/978-3-319-26145-4_26. hal-01261651.

The involvement in training through research

	2016-2020
Course books, etc	
E-learnings, MOOC	
Heads of masters (mention and parcours)	1
Heads of international courses (Erasmus-mundus, etc)	

❶ Involvement of the team in training through research

Our team is implicated in the AVR (Apprentissage, Vision et Robotique) parcours of the computer science Master and more precisely in the modules *Initiation au Traitement d'Images et à la Vision* in master 1 and *Traitement et Analyse d'Images* in master 2.

Each year, we take on internship one or two Master 2 AVR students. Both doctoral students currently in our team come from this training. Moreover, each year, we propose research initiation subjects to students in master 1 or L3.

❷ Responsibilities

I. Debled-Rennesson is co-responsible of the second year of the AVR parcours computer science Master. She is a member of the jury of the computer science Master of the Université de Lorraine. She was also, until 2019, a member of the committee for computer science in the Doctoral school IAEM of Université de Lorraine.
She is elected member to Pole AM2I the council that gathers labs in mathematics, computer science, and control theory at Université de Lorraine. She is elected member of the Collegium technology of the Lorraine University.

Since 2020, she has been a member of the CA of the SIF (Société Informatique de France) and, since february 2021, she has been Vice President Education.

B. Kerautret is chair and P. Ngo is the secretary of the IAPR - TC18 Discrete Geometry and Mathematical Morphology.

Life of the team

	2016-2020
Nb of seminars	10
Web site	https://adagio.loria.fr/

Members have regularly meetings to discuss about the life of the team (projects, arrivals of new persons, missions, publications, equipment purchase) and to present their research work. We wish to recruit a new permanent member in ou team.

References

Doctoral Dissertations

[1] Nicolas Aubry. "Segmentation and geometric measurements : application to metal tubular objects". PhD thesis. Université de Lorraine, July 2017. tel-01649874.

[2] Hayat Nasser. "Tools for the analysis of noisy discrete curves". PhD thesis. Université de Lorraine, October 2018. tel-01947024.

Habilitation Theses

[3] Bertrand Kerautret. "Analyse d'objets discrets pour l'estimation géométrique et la détection d'échelle". Habilitation à diriger des recherches. Université de Lorraine (Nancy), December 2017. tel-03029250.

Articles in International Peer-Reviewed Journal

[4] Eric Domenjoud, Xavier Provençal, and Laurent Vuillon. "Palindromic language of thin discrete planes". In: *Theoretical Computer Science* (2016), pp. 101–108. DOI: 10.1016/j.tcs.2015.11.023. hal-01262289.

[5] Adrien Krähenbühl, Jean-Romain Roussel, Bertrand Kerautret, Isabelle Debled-Rennesson, Frédéric Mothe, and Fleur Longuetaud. "Un algorithme robuste de segmentation des nœuds du bois sur des images obtenues par tomographie x". In: *Revue forestière française* 2 (December 2016). DOI: 10.4267/2042/61869. hal-02987202.

[6] Nicolas Aubry, Bertrand Kerautret, Philippe Even, and Isabelle Debled-Rennesson. "Photometric Intensity Profiles Analysis for Thick Segment Recognition and Geometric Measures". In: *Mathematical Morphology - Theory and Applications* 2.1 (December 2017), pp. 34–54. DOI: 10.1515/mathm-2017-0003. hal-02077892.

[7] Phuc Ngo, Isabelle Debled-Rennesson, Bertrand Kerautret, and Hayat Nasser. "Analysis of Noisy Digital Contours with Adaptive Tangential Cover". In: *Journal of Mathematical Imaging and Vision* 59.1 (2017), pp. 123–135. DOI: 10.1007/s10851-017-0723-7. hal-01486969.

[8] Phuc Ngo, Yukiko Kenmochi, Akihiro Sugimoto, Hugues Talbot, and Nicolas Passat. "Discrete rigid registration: A local graph-search approach". In: *Discrete Applied Mathematics* 216.2 (2017), pp. 461–481. DOI: 10.1016/j.dam.2016.05.005. hal-01306035.

[9] Hayat Nasser, Phuc Ngo, and Isabelle Debled-Rennesson. "Dominant point detection based on discrete curve structure and applications". In: *Journal of Computer and System Sciences* 95 (2018), pp. 177–192. DOI: 10.1016/j.jcss.2017.07.007. hal-01584733.

[10] Phuc Ngo, Nicolas Passat, Yukiko Kenmochi, and Isabelle Debled-Rennesson. "Geometric preservation of 2D digital objects under rigid motions". In: *Journal of Mathematical Imaging and Vision* 61 (2019), pp. 204–223. DOI: 10.1007/s10851-018-0842-9. hal-01695370.

[11] L. Wendling, I Debled-Rennesson, and H. Nasser. "Multilevel Polygonal Descriptor Matching Defined By Combining Discrete Lines And Force Histogram Concepts". In: *Multimedia Tools and Applications* (April 2019). DOI: 10.1007/s11042-019-7531-6. hal-02931272.

[12] Van-Tho Nguyen, Thiéry Constant, Bertrand Kerautret, Isabelle - Debled-Rennesson, and Francis Colin. "A Machine-Learning Approach for Classifying Defects on Tree Trunks using Terrestrial LiDAR". In: *Computers and Electronics in Agriculture* 171 (April 2020), pp. 1–12. DOI: 10.1016/j.compag.2020.105332. hal-02931277.

Major International Conferences

[13] Bertrand Kerautret, Adrien Krähenbühl, Isabelle Debled-Rennesson, and Jacques-Olivier Lachaud. "Centerline Detection on Partial Mesh Scans by Confidence Vote in Accumulation Map". In: *ICPR 2016 - IAPR International Conference on Pattern Recognition*. Cancùn, Mexico, December 2016. DOI: 10.1109/ICPR.2016.7899829. hal-01435271.

[14] Phuc Ngo, Hayat Nasser, Isabelle Debled-Rennesson, and Bertrand Kerautret. "Adaptive Tangential Cover for Noisy Digital Contours". In: *DGCI 2016 - 19th international conference on Discrete Geometry for Computer Imagery*. Vol. LNCS 9647. DGCI 2016: Discrete Geometry for Computer Imagery. Nantes, France, April 2016, pp. 439–451. DOI: 10.1007/978-3-319-32360-2_34. hal-01266033.

[15] - Van-Tho Nguyen, Bertrand Kerautret, Isabelle Debled-Rennesson, Francis Colin, Alexandre Piboule, and Thiéry Constant. "Segmentation of defects on log surface from terrestrial lLidar data". In: *23rd International Conference on Pattern Recognition (ICPR)*. Mexico, Mexico: IEEE COMPUTER SOC, December 2016, p. 6. hal-02740896.

[16] Bertrand Kerautret, Phuc Ngo, Yukiko Kenmochi, and Antoine Vacavant. "Greyscale Image Vectorization from Geometric Digital Contour Representations". In: *DGCI'17 - 20th International Conference on Discrete Geometry for Computer Imagery*. Vol. 34. Vienna, Austria, September 2017, pp. 2379–331. DOI: 10.1007/978-3-319-66272-5_26. hal-01588695.

[17] Phuc Ngo, Yukiko Kenmochi, Isabelle Debled-Rennesson, and Nicolas Passat. "Convexity-preserving rigid motions of 2D digital objects". In: *Discrete Geometry for Computer Imagery (DGCI)*. Vol. 10502. Lecture Notes in Computer Science. Vienna, Austria, 2017, pp. 69–81. DOI: 10.1007/978-3-319-66272-5_7. hal-01565028.

[18] Soumi Paul, Hayat Nasser, Mita Nasipuri, Phuc Ngo, Subhadip Basu, and Isabelle Debled-Rennesson. "A Statistical-Topological Feature Combination for Recognition of Isolated Hand Gestures from Kinect Based Depth Images". In: *IWCIA*. Vol. 10256. LNCS. Plovdiv, Bulgaria, June 2017. DOI: 10.1007/978-3-319-59108-7. hal-01517817.

[19] Antoine Vacavant, Bertrand Kerautret, Tristan Roussillon, and Fabien Feschet. "Reconstructions of Noisy Digital Contours with Maximal Primitives Based on Multi-Scale/Irregular Geometric Representation and Generalized Linear Programming". In: *20th IAPR International Conference on Discrete Geometry for Computer Imagery*. Vol. 10502. Lecture Notes in Computer Science. Vienna, Austria: Springer, September 2017, pp. 291–303. DOI: 10.1007/BFb0038202. hal-01621504.

[20] Phuc Ngo, Nicolas Passat, Yukiko Kenmochi, and Isabelle Debled-Rennesson. "Convexity invariance of voxel objects under rigid motions". In: *International Conference on Pattern Recognition (ICPR)*. Beijing, China, 2018, pp. 1157–1162. DOI: 10.1109/ICPR.2018.8545023. hal-01695388.

[21] Eric Domenjoud, Bastien Laboureix, and Laurent Vuillon. "Facet Connectedness of Arithmetic Discrete Hyperplanes with Non-Zero Shift". In: *DGCI 2019: 21st International Conference on Discrete Geometry for Computer Imagery*. Discrete Geometry for Computer Imagery. Paris, France, March 2019, pp. 38–50. DOI: 10.1007/978-3-030-14085-4_4. hal-02316870.

[22] Philippe Even, Phuc Ngo, and Bertrand Kerautret. "Thick Line Segment Detection with Fast Directional Tracking". In: *ICIAP 2019 -20th International Conference on Image Analysis and Processing*. Ed. by E. Ricci et al. LNCS 11752. trento, Italy: Springer, September 2019, pp. 159–170. DOI: 10.1007/978-3-030-30645-8_15. hal-02189916.

[23] Phuc Ngo. "A discrete approach for polygonal approximation of irregular noise contours". In: *CAIP 2019 - Computer Analysis of Images and Patterns*. Vol. 11678. LNCS. Salerno, Italy, September 2019, pp. 433–446. DOI: 10.1007/978-3-030-29888-3_35. hal-02163606.

[24] Nicolas Passat, Yukiko Kenmochi, Phuc Ngo, and Kacper Pluta. "Rigid motions in the cubic grid: A discussion on topological issues". In: *Discrete Geometry for Computer Imagery (DGCI)*. Vol. 11414. Lecture Notes in Computer Science. Marne-la-Vallée, France: Springer, 2019, pp. 127–140. DOI: 10.1007/978-3-030-14085-4_11. hal-01892944.

[25] Philippe Even and Phuc Ngo. "Live extraction of curvilinear structures from lidar raw data". In: *XXIV ISPRS Congress*. Vol. V-2-2020. IAPRS Annals of Photogrammetry, Remote Sensing and Spatial Information Sciences. Nice, France, 2020, pp. 211–219. DOI: 10.5194/isprs-annals-V-2-2020-211-2020. hal-02872075.

[26] Phuc Ngo. "Digital hyperplane fitting". In: *20th International Workshop on Combinatorial Image Analysis (IWCIA)*. Vol. 12148. LNCS. Novi Sad, Serbia, July 2020, pp. 164–180. DOI: 10.1007/978-3-030-51002-2_12. hal-02586206.

Secondary International Conferences

[27] Thiéry Constant, Van Tho Nguyen, Estelle Noyer, Frédéric Mothe, Francis Colin, Alexandre Piboule, Bertrand Kerautret, and Isabelle Debled-Rennesson. "Towards wood quality assessment of standing trees fromT-LiDAR: What's Going on in France?" In: *8th meeting of IUFRO Working Parties 5.01.04 and 3.04.02: "Modelling Wood Quality, Supply and Value Chain Networks"*. Quebec, Canada, June 2016. hal-02793063.

[28] Bertrand Kerautret, Miguel Colom, and Pascal Monasse. "Preface of the proceedings of the First International Workshop on Reproducible Research in Pattern Recognition, RRPR 2016". In: *First International Workshop on Reproducible Research in Pattern Recognition, RRPR 2016*. Mexico, Mexico, 2016. hal-01616745.

[29] Bertrand Kerautret, Adrien Krähenbühl, Isabelle Debled-Rennesson, and Jacques-Olivier Lachaud. "Analyse géométrique d'objets tubulaires 3D basée sur l'accumulation de normales". In: *RFIA 2016 - Reconnaissance des Formes et l'Intelligence Artificielle*. Clermont Ferrand, France, June 2016. hal-01359558.

[30] Bertrand Kerautret, Adrien Krähenbühl, Isabelle Debled-Rennesson, and Jacques-Olivier Lachaud. "On the Implementation of Centerline Extraction Based on Confidence Vote in Accumulation Map". In: *RRPR 2016 1st Workshop on Reproducible Research in Pattern Recognition*. Vol. 10214. RRPR: International Workshop on Reproducible Research in Pattern Recognition. Bertrand Kerautret and Miguel Colom and Pascal Monasse. Cancùn, Mexico, December 2016, pp. 116–130. DOI: 10.1007/978-3-319-56414-2_9. hal-01571434.

[31] Adrien Krähenbühl, Jean-Romain Roussel, Bertrand Kerautret, Isabelle Debled-Rennesson, Frédéric Mothe, and Fleur Longuetaud. "Robust Knot Segmentation by Knot Pith Tracking in 3D Tangential Images". In: *ICCVG 2016*. Vol. 9972. Computer Vision and Graphics. Warsaw, Poland: Springer International Publishing AG, September 2016, pp. 581–593. DOI: 10.1007/978-3-319-46418-3_52. hal-01421205.

[32] Phuc Ngo, Hayat Nasser, and Isabelle Debled-Rennesson. "A discrete approach for decomposing noisy digital contours into arcs and segments". In: *ACCV Workshop 2016*. ACCV 2016 Workshops. Taipei, Taiwan, November 2016. DOI: 10.1007/978-3-319-54427-4_36. hal-01375089.

[33] Phuc Ngo, Hayat Nasser, Isabelle Debled-Rennesson, and Bertrand Kerautret. "An algorithm to decompose noisy digital contours". In: *RRPR 2016- 1st Workshop on Reproducible Research in Pattern Recognition*. Cancun, Mexico, December 2016. DOI: 10.1007/978-3-319-56414-2_10. hal-01415925.

[34] Isabelle Debled-Rennesson, Philippe Févotte, Monique Grandbastien, David Langlois, and Hélène Tanoh. "La formation des professeurs de la spécialité ISN dans l'Académie de Nancy-Metz – Récit et analyse de six ans d'expérience". In: *Didapro 7 – DidaSTIC. De 0 à 1 ou l'heure de l'informatique à l'école*. Lausanne, Switzerland, February 2018. hal-01753067.

[35] Phuc Ngo, Yukiko Kenmochi, Nicolas Passat, and Isabelle Debled-Rennesson. "Discrete regular polygons for digital shape rigid motion via polygonization". In: *International Workshop on Reproducible Research on Pattern Recognition (RRPR)*. Vol. 11455. Lecture Notes in Computer Science. Beijing, China, 2018, pp. 55–70. DOI: 10.1007/978-3-030-23987-9_4. hal-01853795.

[36] Rémi Decelle and Ehsaneddin Jalilian. "Neural Networks for Cross-Section Segmentation in Raw Images of Log Ends". In: *Fourth IEEE International Conference on Image Processing, Applications and Systems (IPAS 2020)*. Gênes, Italy, September 2019. hal-03058259.

[37] Rémi Decelle, Phuc Ngo, Isabelle Debled-Rennesson, Frederic MOTHE, and Fleur Longuetaud. "A new algorithm to automatically detect the pith on rough log-end images". In: *21st International Nondestructive Testing and Evaluation (NDTE) of Wood Symposium*. Freiburg, Germany, September 2019. hal-02275651.

[38] Rémi Decelle, Phuc Ngo, Isabelle Debled-Rennesson, Frédéric Mothe, and Fleur Longuetaud. "Pith Estimation on Tree Log End Images". In: *Reproducible Research on Pattern Recognition (RRPR)*. Vol. LNCS 12636. Milan, Italy, 2021, pp. 101–120. DOI: 10.1007/978-3-030-76423-4_7. hal-03006060.

[39] Rémi Decelle, Phuc Ngo, Isabelle Debled-Rennesson, Frédéric F. Mothe, and Fleur Longuetaud. "Digital Straight Segment Filter for Geometric Description". In: *DGMM 2021 - IAPR International Conference on Discrete Geometry and Mathematical Morphology*. Vol. LNCS 12708. Uppsala, Sweden, May 2021, pp. 255–268. DOI: 10.1007/978-3-030-76657-3_18. hal-03144152.

[40] Florian Delconte, Phuc Ngo, Isabelle Debled-Rennesson, Bertrand Kerautret, Van Tho Nguyen, and Thiéry Constant. "Tree Defect Segmentation using Geometric Features and CNN". In: *Reproducible Research on Pattern Recognition (RRPR)*. Vol. LNCS 12636. Milan, Italy, 2021, pp. 80–100. DOI: 10.1007/978-3-030-76423-4_6. hal-03006063.

[41] Philippe Even, Axelle Grzesznik, Anne Gebhardt, Thomas Chenal, Pierre Even, and Phuc Ngo. "Interactive extraction of linear structures from LiDAR raw data for archaeomorphological structure prospection". In: *XXIV ISPRS Congress*. Vol. XLIII-B2-2021. The International Archives of the Photogrammetry, Remote Sensing and Spatial Information Sciences. Nice (en ligne), France, July 2021, pp. 153–161. DOI: 10.5194/isprs-archives-XLIII-B2-2021-153-2021. hal-03189641.

[42] Philippe Even and Phuc Ngo. "Automatic forest road extraction from LiDAR data of mountainous areas". In: *DGMM 2021 - IAPR International Conference on Discrete Geometry and Mathematical Morphology*. Vol. LNCS12708. Uppsala, Sweden, May 2021, pp. 93–106. DOI: 10.1007/978-3-030-76657-3_6. hal-03144147.

[43] Phuc Ngo, Nicolas Passat, and Yukiko Kenmochi. "Quasi-regularity verification for 2D polygonal objects based on medial axis analysis". In: *International Conference on Image Processing (ICIP)*. Anchorage, Alaska, United States, 2021, pp. 1584–1588. DOI: 10.1109/ICIP42928.2021.9506543. hal-03121428.

[44] Nicolas Passat, Phuc Ngo, and Yukiko Kenmochi. "Homotopic Digital Rigid Motion: An Optimization Approach on Cellular Complexes". In: *International Conference on Discrete Geometry and Mathematical Morphology (DGMM)*. Vol. 12708. Lecture Notes in Computer Science. Uppsala (virtual), Sweden, 2021, pp. 189–201. DOI: 10.1007/978-3-030-76657-3_13. hal-02994752.

National Peer-Reviewed Conferences

[45] Rémi Decelle, Phuc Ngo, Isabelle Debled-Rennesson, Frédéric F. Mothe, and Fleur Longuetaud. "Description géometrique à l'aide de segments discrets". In: *Journée du Groupe de Travail de Géométrie Discrète et Morphologie Mathématique (GT GDMM)*. Nancy, France, 2021. hal-03215817.

Book (written)

Books or Proceedings Editing

[46] Bertrand Kerautret, Miguel Colom, Daniel Lopresti, Pascal Monasse, and Hugues Talbot. *Reproducible Research in Pattern Recognition, Second International Workshop, RRPR 2018*. August 2018. hal-02172999.

Book Chapters

[47] Van Tho Nguyen, Bertrand Kerautret, Isabelle Debled-Rennesson, Francis Colin, Alexandre Piboule, and Thiéry Constant. "Algorithms and Implementation for Segmenting Tree Log Surface Defects". In: *Reproducible Research in Pattern Recognition : First International Workshop, RRPR 2016, Cancún, Mexico, December 4, 2016, Revised Selected Papers*. Lecture Notes in Computer Science Chapter 11. Springer International Publishing AG, 2017. DOI: 10.1007/978-3-319-56414-2_11. hal-02788140.

Other Publication

[48] Thuy Hong Dao, Phuc Ngo, Isabelle Debled-Rennesson, Yukiko Kenmochi, and Nicolas Passat. "Transformations rigides pour les objets discrets non-convexes en 2D". In: *Journées du Groupe de Travail en Modélisation Géométrique (GTMG)*. Aix-en-Provence, France, 2018. hal-01740074.

[49] Phuc Ngo, Nicolas Passat, Yukiko Kenmochi, and Isabelle Debled-Rennesson. "Geometric-preserving rigid motions of digital objects". In: *Journées Informatique et Géométrie (JIG)*. Lyon, France, 2018. hal-01822122.

[50] Rémi Decelle, Phuc Ngo, Isabelle Debled-Rennesson, Mothe Frédéric, and Fleur Longuetaud. *Détection automatique de la moelle sur des images d'extrémités de grumes de Douglas brutes de sciage*. GDR 2019 - 8èmes Journées du Groupement de Recherche 3544 Sciences du Bois. Poster. November 2019. hal-03029969.

[51] Florian Delconte. "Estimation de la qualité de grumes de bois". MA thesis. Université de Lorraine, September 2019, p. 38. hal-03603108.

[52] Philippe Even, Phuc Ngo, and Bertrand Kerautret. *Complementary Experiments of the Thick Line Segment Detection Algorithm: Evaluation of ADS and ATC Concepts*. Research Report. LORIA (Université de Lorraine, CNRS, INRIA), 2019. hal-03155787.

[53] Alexis BARTHELEMY. "Reconstruction de billon". MA thesis. Université de Lorraine, August 2020, p. 44. hal-03606199.

[54] Rémi Decelle, Phuc Ngo, Isabelle Debled-Rennesson, Frédéric F. Mothe, and Fleur Longuetaud. "Ant Colony Optimization for Estimating Pith Position on Images of Tree Log Ends". working paper or preprint. November 2021. hal-03442289.

[55] Phuc Ngo. *Gauss Digitization of Simple Polygons*. Research Report. LORIA (Université de Lorraine, CNRS, INRIA), 2021. DOI: 10.13140/RG.2.2.32967.21925. hal-03125916.

[56] A. Poszwa, A. Grzesznik, A. Gebhardt, A. AGAT, P. Even, Phuc Ngo, D. CARTIER, V. Robin, C. Delangle, S. Occhietti, Alexis A. De Junet, Dominique Harmand, Charles Kraemer, T. Chenal, and D. Bartier. *1400 years of man-environment interactions and soil evolution in the Saint-Mont mountain (Remiremont, Vosges)*. Historical Ecology for the future - International conference in historical ecology. Poster. Colloque chairman: Vincent Robin, Interdisciplinary Laboratory for Continental Environments (LIEC - CNRS/UL), May 2021. hal-03236655.

Cryptology, arithmetic: algebraic methods for better algorithms

Synopsis

1 Team Composition

Permanents

Jérémie Detrey (CR INRIA, left 01/01/2020), Pierrick Gaudry (DR CNRS), Aurore Guillevic (CR INRIA, arrived 01/11/2016), Virginie Lallemand (CR CNRS, arrived 01/10/2018), Marine Minier (PR UL, arrived 01/09/2016), Cécile Pierrot (CR INRIA, arrived 01/01/2018), Pierre-Jean Spaenlehauer (CR INRIA), Emmanuel Thomé (DR INRIA), Marion Videau (MCF UL, on secondment to Quarkslab since 01/01/15, left 01/04/19), Paul Zimmermann (DR INRIA).

Note: The "Total" column does not always correspond to the sum of the individual columns, since for example a post-doctoral researcher might stay several years.

	2016	2017	2018	2019	2020	Total
PR	0+1					1
MCF	1			-1		0
DR	3					3
CR	2+1		+2		-1	4
Other						
Total (permanent positions)	6+2		+2	-1	-1	8
Pr emeritus						
Guest researchers						
Post-doct. researchers	2	2	1	1	1	3
PhD Students	4	5	7	6	7	11
Master students M2		1	1	1	1	4
Master Students M1	1		2		1	4
L3 students	2	3		2		7
Engineers	1	1	1	1	1	1
Other	1			2		3
Total (temporary positions)	11	12	12	13	11	33

Post-doctoral fellows and visiting researchers

Luc Sanselme (Éducation Nationale), Enea Milio (Post-doc), Shashank Singh (Post-doc), Bimal Mandal (Post-doc), Santanu Sarkar (Visiting professor)

Engineers

Stéphane Glondu (part time, also with PESTO team)

Change in team composition

Four permanent researchers joined the team since the last evaluation: Marine Minier as Professor, Virginie Lallemand as CNRS Research Scientist, Cécile Pierrot and Aurore Guillevic as INRIA Research Scientists. Marion Videau (Assistant Professor) and Jérémie Detrey (INRIA Research Scientist) left the team.

Doctoral students

Simon Abelard [UL / ENS] (Sept 2015–Aug 2018), Hamid Boukerrou [LUE Digitrust] (Oct 2019–Oct 2022), Svyatoslav Covanov [UL / AMX Polytechnique] (Sept 2014–Aug 2018), Gabrielle De Micheli [INRIA CORDI-S] (Oct 2018–), Laurent Grémy [INRIA, team own funding] (Oct 2013–Aug 2017), Paul Huynh [FUI PACLIDO] (Oct 2017–Dec 2020), Hugo Labrande [UL / ENS / Univ. of Calgary] (Sept 2013–Nov 2016), Aude Le Gluher [UL / ENS], (Sept 2018–), Simon Masson [Cifre Thales] (Jan 2018–Dec 2020), Sandra Rasoamiaramanana [Cifre Orange] (May 2017–May 2020), Quentin Yang [INRIA / team own funding] (Oct 2020–).

	2016-2020
PhD's defended	7
On-going PhD's	4
Average nb of papers by PhD student	2.5
Average duration of PhD thesis (in month)	40,5

Simon Abelard: Post-doc University of Waterloo, ON, Canada, then post-doc Inria Saclay, now Cryptography engineer at Thales Communications & Security https://www.thalesgroup.com. Svyatoslav Covanov: Post-doc Inria Saclay, then research engineer at Observatoire de Paris, now engineer, Zhor-tech, Nancy. Laurent Grémy: post-doc at LIP, Lyon, then Cryptography engineer at Quarkslab https://quarkslab.com. Paul Huynh: job search. Hugo Labrande: Teacher in classes préparatoires, later moved to Canada, currently in job search. Simon Masson: Cryptography engineer at Heliax https://heliax.dev/. Sandra Rasoamiaramanana: Cryptography engineer at Ledger https://www.ledger.com/.

2 Research topics

Keywords

Cryptography, Cryptanalysis, Symbolic computation, Computer arithmetic.

Research area and main goals

Caramba principally focuses on the design and analysis of cryptographic primitives. We address both public-key (asymmetric) and secret-key (symmetric) cryptography. Our public-key expertise is concentrated on so-called "classical" cryptographic primitives, which are known to be vulnerable to the hypothetical advent of a quantum computer. These primitives are the ones that are most used today, and their analysis is of utmost importance. In particular, we study the large family of algorithms that follow the number field sieve (NFS) strategy: these are well suited for factoring RSA keys and for computing discrete logarithms in finite fields. We also study the use of algebraic curves in cryptography, in particular elliptic curves and curves of higher genus.

The symmetric cryptography topic emerged in the team in 2016, following the recruitment of Marine Minier as a professor at the Université de Lorraine in September 2016, and Virginie Lallemand as a CNRS researcher in October 2018. We study the design and analysis of lightweight cryptographic primitives, as well as the use and design of automatic tools for cryptanalysis.

Other connected topics are also studied within the team, notably polynomial systems, and computer arithmetic. These are topics of study *per se*, but are also clearly connected to the above themes: polynomial systems are a means to address key problems related to algebraic curves, and computer arithmetic also encompasses questions that are relevant for either fast cryptography or fast cryptanalysis, e.g., via asymptotically fast algorithms.

3 Main Achievements

Our long-term investment on the NFS algorithm gave highly visible results over the period: we have set the current records for integer factorization and discrete logarithm in finite fields (250 and 240 decimal digits, respectively). We also computed discrete logarithms in a trapdoored (but innocent-looking) finite field of 1024 bits, thus demonstrating a practical risk to use untraceable primes. We have also become recognized experts in assessing the security of pairing-based cryptography, in particular in the very active realm of zero-knowledge proofs used in blockchains.

Our expertise in symmetric cryptography was highlighted through our investment in the NIST lightweight cryptography standardization process: we participated in 2 proposals, and analyzed propositions made by others.

4 Research activities

NFS-like algorithms for factoring and discrete logarithm

Description The number field sieve (NFS) is the best known algorithm for factoring integers used in the RSA cryptosystem, with time and space complexities that are not fully exponential but still far from polynomial[43]. Many variants of NFS have been designed to handle other problems, in particular the discrete logarithm problem (DLP) in finite fields.

During this evaluation period, we have reinforced our expertise on NFS for factorization, and acquired a good expertise in the context of discrete logarithm.

Main results Our main results in this research axis concern both the fundamental algorithms used in NFS, and setting new records. The progress in fundamental algorithms enables us to set new records, and in many cases targetting new records forces us to invent new algorithms.

[43] Complexities are expressed with the function $L_N(\alpha, \beta) = \exp(\beta(\log N)^\alpha(\log\log N)^{1-\alpha})$, with $\alpha = \frac{1}{3}$ for NFS.

Among the fundamental algorithms, we have made progress on the DLP over elliptic curves [12], the search and ranking of polynomials for NFS [10, 30], sieving for DLP [2], saving vectors in the block Lanczos algorithm [89], computations with sparse matrices [46], faster individual logarithms for DLP [27], elliptic bases in DLP [102], and studying asymptotic complexities [71, 43].

We have set new records both for integer factorization with the factorization of RSA-220 (which at the time was a record for CADO-NFS) [94], the factorization of RSA-240 and RSA-250 [69, 85], and discrete logarithm computations, both over prime fields and prime-power fields [13, 49, 98, 57, 69, 37]. Most of these records were achieved using CADO-NFS [111].

On the cryptanalysis side, we had two major contributions: we performed a record kilobit DLP computation over a kilobit field, which had a nice impact since it showed that one could "forge" a DLP key [55]; and in the LogJam attack [21] we showed how one could defeat some still currently used 512-bit DLP keys.

Algebraic curves and cryptography

Description The main algorithmic problems for algebraic curves in cryptography are: counting the number of elements in the group we want to use, in order to check that it is a prime; trying to solve the discrete logarithm problem; designing fast formulae for the group law; computing important invariants like the ring of endomorphisms.

Main results The team obtained a series of results on point counting over hyperelliptic curves of genus 2, 3 and higher [60, 25, 28]. Faster group law was investigated through Jacobi's Theta functions, with quasi-linear algorithms for genus 1, genus 2 and above [14, 15]. Other works related to algebraic curves also include isogeny graph computations [33], computing modular polynomials on Hilbert surfaces [36], and also the computation of Riemann–Roch spaces [34]. For explicit cryptographic purposes, our production covers new pairing-friendly curves resistant to the Tower-NFS algorithm [62, 76, 32], among which a best paper award at WAIFI'2018; elliptic curves with properties dedicated to blockchains: for verifiable delay functions [64] and for zero-knowledge proofs [74]. The team also challenges the security of elliptic curves in various cryptographic contexts: in ECDSA implementations [72] and other practical scenarios [105]. The discrete logarithm problem on elliptic curves is also covered [12, 49]. Finally elliptic curves are exploited as a tool in the quasi-polynomial-time algorithm [102].

Symmetric Cryptography

Description The main objectives of symmetric key cryptography can be split in two categories: first the design, that is the conception of new primitives answering the needs of specific use cases, and second the analysis, which corresponds to the study of the properties of a specific primitive in view of breaking it or at least bringing to light some unexpected behavior.

The constant evolution of the needs in cryptography, and in particular the recent boom of the Internet of Things, created a need for so-called lightweight primitives, that require less resources than the current standards. In view of this, the NIST (the US standardization agency) initiated in 2015 the lightweight cryptography standardization process and sollicited proposals and evaluations from researchers. The 10 finalists have just been announced, and the final round is expected to last approximately 12 months.

Besides the work directly dedicated to this process, an endless goal of symmetric cryptography is to better understand the existing attacks and to easily evaluate if a cipher resists them or not. A promising line of works in this direction is the use of automated tools (with solvers based on MILP, CP or SAT).

We also studied possible extensions of white box cryptography as part of the PhD thesis of Sandra Rasoamiramanana.

Main results The team members co-authored two candidates to the lightweight cryptography standardization process initiated by the NIST: Lilliput AE and ForkAE [63]. ForkAE has been selected in the second round (with 32 other candidates out of 56) but unfortunately did not make it as a finalist. They also contributed to the analysis of other teams' candidates and gave observations on Spook in a paper published at Crypto 2020 [73], and on Skinny (a cipher used in several candidates and in particular in the finalist ROMULUS) in a paper published at SAC 2019 [65]. If the results on Skinny do not contradict the claims made by its designers, the observations on Spook made the authors propose a tweaked version of their candidate to avoid the bad properties we reported.

The team also obtained results regarding the cryptanalysis of AES using constraint programming [56, 24, 31]. One of this paper is published in IJCAI 2017.

Concerning white-box cryptography, two possible extensions have been proposed in [67, 77].

Other results include a generic study of how to better evaluate the strength of so-called boomerang attacks on a specific primitive construction named Feistel ciphers [29], a generic study of Square, saturation, integrals and other multiset-based attacks in [51] and a refined analysis of impossible-differential attacks against Rijndael-160 and Rijndael-224 in [20].

Polynomial Systems

Polynomial systems are a transversal theme which arises in several flavors in the research activities of CARAMBA. Perhaps its most direct emanation lies in the study of algebraic curves. In particular, the PhD thesis of Simon Abelard involved state-of-the-art algorithmic tools for polynomial systems in order to obtain results on the asymptotic complexity of point counting for hyperelliptic curves [3, 60, 25, 28]. Polynomial systems also occur in less expected situations: for instance, computing the asymptotic complexity of the NFS-DL algorithm for pairing-relevant finite fields is done by solving some polynomial systems, see e.g., [71]. Finally, the design and the analysis of algorithms for structured polynomial systems arising from applications—sparse systems for instance—is one of the core research topics of Pierre-Jean Spaenlehauer [48, 52, 22].

Computer Arithmetic

Since arithmetic is a transversal theme for us, with a large part of implementation, our positioning is a bit atypical. We have a strong commitment to publishing and maintaining software libraries, and the corresponding activities are described in the Software section below. We emphasize in particular the GNU MPFR and GNU MPC libraries, that are used by the GCC compiler to compute accurately the constants that are known at compile-time.

The main results are related to the two PhD theses of Hugo Labrande about the Abel-Jacobi map [14, 1, 15], and that of Svyatoslav Covanov about fast multiplication algorithms [45, 54, 100, 4, 26]. We also had nice results on mixed-radix scalar multiplication [66] and on fast modular arithmetic on the Kalray processor [19]. We also maintain a small but important research activity on floating-point arithmetic, both on the fundamental side [61], and to improve the efficiency of the GNU MPFR library [58].

Scientific production and quality

	2016-2020
PhD Thesis	9
H.D.R	0
Journals	35
Major conferences	33
Other conferences	7
Book chapters	3
Books (written)	1
Special issues (edited)	1
Other productions from workshops	0
General audience papers	3
Participation in editorial committees	25
Evaluation of labs and research structures	3
European projects (as project manager/Member)	0
Other international projects (as project manager/Member)	0
ANR, PHRC, FUI, INCA, etc. (as project manager/Member)	1/1
Projects with Region Grand Est, etc (as project manager/Member)	1/0
PIA (as project manager/Member)	0
Others (as project manager/Member)	0/2
Prizes and distinctions	3
IUF	0
Responsibilities in scientific communities (GDR etc.)	2
Organizations of Conferences (national/international)	1/0
Invitations (national/international)	12/17
Stays in foreign laboratories	1

❶ List of top journals in which we have published

Mathematics of Computation (4) [14, 26, 27, 34]; IEEE Transactions on Computers (1) [19]; IEEE Transactions on Information Theory (1) [35]; Artificial Intelligence (1) [31]; Journal of Number Theory (2) [33, 36]; IACR Transactions on Symmetric Cryptology – ToSC (1) [29]; Designs, Codes and Cryptography (4) [12, 20, 23, 32].

❷ List of top conferences in which we have published

Major crypto / security conferences: Crypto (3) [69, 71, 73], Eurocrypt (1) [55], Asiacrypt (2) [63, 64]. Specialized crypto conferences: SAC (3) [49, 57, 65], PKC (1) [76], ANTS (1) [60], ISSAC (4) [46, 48, 52, 54]; ARITH (2) [58, 61]; WAIFI (1, best paper) [62]. FSE (IACR Fast Software Encryption conference) moved to a hybrid journal/conference model and appears above in Sec. 1. Other: IJCAI (1) [56].

❸ Software

CADO-NFS. CADO-NFS (https://cado-nfs.gitlabpages.inria.fr/) is a complete implementation in C/C++ of the Number Field Sieve (NFS) algorithm for factoring integers and computing discrete logarithms in finite fields. It consists in various programs corresponding to all the phases of the algorithm, and a general script that runs them, possibly in parallel over a network of computers. Started around 2007, CADO-NFS is released under the LGPL free software license. There are about 250,000 lines of source code (excluding some automatically generated code). The development of CADO-NFS is led by P. Gaudry, E. Thomé, P. Zimmermann. Over the evaluation period, a huge effort has been put into making CADO-NFS usable for larger and larger problems, which made it possible to set new factorization and discrete logarithm records (RSA-240, DLP-240, RSA-250) [69].

Arithmetic libraries. We develop and maintain libraries for various arithmetic building blocks. The GNU MPFR and GNU MPC libraries are mature projects that provide multiprecision floating-point arithmetic with correct rounding up to the last bit. Since both are required to compile GCC, these libraries now enjoy a very high visibility. They are regularly maintained and enhanced. In particular in 2020-2021, new functions have been implemented in GNU MPFR to match the reserved names for correctly-rounded functions in the N2596 draft of the C language standard.[44]

We also develop the GF2X and MPFQ libraries that are more specialized. Both are used by CADO-NFS, and GF2X is used by SageMath, and can be used as an auxiliary package for the widespread software library NTL.

Belenios (http://www.belenios.org/) is an open-source online voting system that provides strong security guarantees such as vote confidentiality (votes are encrypted, the decryption key is distributed so that no one knows the full secret key) and verifiability (voters can check that their ballots have been received, and anyone can recount the votes). Belenios is developed by S. Glondu, P. Gaudry, V. Cortier (PESTO team).

In the early years, most of the elections were related to the academic community. Since 2019, and even more during the pandemic, users from various horizons organized elections with our platform, often in associations or for professional elections in small companies (CSE). The multilingual support attracted users from non-English speaking countries (Italy, Mexico, Brazil, Czech Republic). In 2020, more than 1400 elections were organized with our platform, corresponding to a total of more than 100,000 voters.

Other Software Tools: We also develop prototype and companion code to illustrate papers and help reproducibility of reseach, see Appendix for a full description of these software tools.

Platform: computational resources

Since 2018, the CARAMBA team has been using in particular a computer cluster called `grvingt`, acquired in 2018. This equipment was funded by the CPER "CyberEntreprises" (French Ministry of Research, Région Grand Est, Inria, CNRS) and comprises a 64-node, 2,048-core cluster. This cluster is installed in the Inria facility. Other slightly older hardware (a medium-size cluster called `grcinq` from 2013, funded by ANR, and a special machine funded by the aforementioned CPER grant) is also installed in the same location, to form a coherent platform with about 3,000 cpu cores, 100 TB of storage, and specific machines for RAM-demanding computations. As a whole, this platform provides an excellent support for the computational part of the work

[44] http://www.open-std.org/jtc1/sc22/wg14/www/docs/n2596.pdf

done in CARAMBA. This platform is also embedded in the larger Grid'5000/Silecs platform (and accessible as a normal resource within this platform). Technical administration is done by the Grid'5000 staff.

This equipment has played a key role in the record factorizations of RSA-240 and RSA-250, as well as in the computation of discrete logarithms modulo a 240-digit prime, completed in the end of 2019.

The academic reputation and appeal

Members of the team are regularly invited for a talk at the Elliptic Curve Cryptography conference (ECC): 5 times over the period 2016–2020. The team members are regularly invited to international as well as national events such as the Journées GT-C2 or at the C2 seminar (previously CCA). A full list can be found in appendix.

Highlights of the evaluation period (except invited talks which are given in appendix):

2016	The Caramba project-team was created on January 1st, 2016. In October 2016, Pierrick Gaudry and Emmanuel Thomé, together with colleagues from the University of Pennsylvania (USA), have performed a discrete logarithm computation modulo a 1024-bit trapdoored prime [55].
2017	The CARAMBA team organized the Journées Codage et Cryptographie 2017 (C2), whose objective is to regroup the French speaking community working on error-correcting codes and on cryptography. It is affiliated with the "Groupe de travail C2" of the GDR-IM.
2018	Cécile Pierrot was awarded the DGA (Direction Générale de l'Armement) Prize from Florence Parly, the Minister of the Armed Forces, for her PhD thesis.
2019	On December 2nd, 2019, the factorization of RSA-240 and the computation of a 240-digit discrete logarithm were announced (results published in 2020 in [69]). In August 2019, Pierrick Gaudry found a vulnerability in the encryption scheme of the Internet voting system of Moscow [75].

❶ Participation in projects and External funding

ANR Decrypt

The CARAMBA team coordinates this 4-year ANR Project (started in January 2019) with the five following partners: LORIA, LIRIS (Lyon), LIMOS (Clermont-Ferrand), IRISA (Rennes), TASC (Nantes). This project aims to propose a declarative language dedicated to cryptanalytic problems in symmetric key cryptography using constraint programming (CP) to simplify the representation of attacks, to improve existing attacks and to build new cryptographic primitives that withstand these attacks. We also want to compare the different tools that can be used to solve these problems: SAT and MILP where the constraints are homogeneous and CP where the heterogeneous constraints can allow a more complex treatment.

One of the challenges of this project will be to define global constraints dedicated to the case of symmetric cryptography.

Concerning constraint programming, this project will define new dedicated global constraints, will improve the underlying filtering and solution search algorithms, and will propose dedicated explanations generated automatically. See web site for more information.

FUI: PACLIDO project

From December 2017 to December 2020 the team was part of the FUI (Fonds Unique Interministériel) named PACLIDO (acronym for *Protocoles et Algorithmes Cryptographiques Légers pour l'Internet Des Objets*) that focuses on Lightweight Cryptography. The project has been coordinated by Airbus Cybersecurity and its other partners were: LORIA-CNRS, Rtone, Trusted Objects, CEA, Sophia Engineering, Université de Limoges, Saint-Quentin-en-Yvelines. One of the main outcomes of the project was the design of Lilliput AE, a lightweight tweakable block cipher for authenticated encryption with associated data.

PEPS CHARIoT, 2017

The PEPS CHARIoT ("CHiffrement Authentifié pour Renforcer l'IoT") project was dedicated to the study of authenticated encryption schemes, especially the CAESAR candidates, and to the performance analysis of those schemes on dedicated embedded architectures such as micro-controllers (MSP430, ARM and AVR). It involved Marine Minier (CARAMBA), Franck Rousseau (IMAG - Grenoble) and Pascal Lafourcade (LIMOS-UCA - Clermont-Ferrand).

PEPS JCJC INS2I SPICE, 2016

The SPICE proposal ("Systèmes Polynomiaux et calcul d'Indice sur les Courbes Elliptiques : indicateurs de complexité en petite caractéristique") had been accepted in the PEPS JCJC INS2I program in 2016. It involved Pierre-Jean Spaenlehauer (CARAMBA) and Vanessa Vitse (Université Joseph Fourier, Grenoble). This project was coordinated by Vanessa Vitse.

CPER CyberEntreprises, 2015–2020

CPER CyberEntreprises was a region-wide project funded by Région Grand-Est, French Ministry of Research and Higher Education, INRIA, and CNRS. The project was coordinated by Emmanuel Thomé and Marc Jungers (CRAN). It funded research that goes well beyond the scope of CARAMBA, and was rather of interest to the local computer science community as a whole, extending to labs beyond LORIA (partners: INRIA, LORIA, CRAN, IECL, Centrale Supelec, LCFC). Among the funded projects is a high-performance computer cluster that was designed to be primarily used for our cryptanalytic work, and this cluster played a key role in our recent factoring and discrete logarithm records. This cluster is also mentioned in 3.

Bilateral Contracts with Industry

- 2017–2020 Together with the PESTO team, we had a contract with the Docapost company (that became Voxaly/Docaposte during the contract, after a merger of the two companies), the purpose of which was to improve their e-voting solution by adding some verifiability properties and switching to elliptic curve cryptography.
- 2019–2021 Together with the PESTO team, we had a contract with the Idemia company about e-voting. The goal was to design a protocol corresponding to their specific needs and formally prove its security.

2020	Together with the PESTO team, we had a contract with the NomadicLabs company with the objective of studying possible evolutions of the voting system used in the Tezos blockchain to amend the protocol.
2018	Consulting with Canton of Geneva. In this contract handled in collaboration with the University of Bristol and the PESTO team, the goal was to audit and prove security properties of a new e-voting protocol called CHVote, to be used in a few cantons of Switzerland.
2016–2018	During that period, we worked on training and consulting activities with the French Ministry of Defense.

Bilateral Grants with Industry

2017–2020	A grant with Orange Gardens at Châtillon-Montrouge is dedicated to the supervision of Sandra Rasoamiaramanana's PhD thesis about security in the white box context. The co-supervisor for Orange Gardens is Gilles Macario-rat.
2018–2020	A grant with Thales (Thales Communication & Security, Gennevilliers, subsidiary of Thales Group) is dedicated to the supervision of Simon Masson's PhD thesis about elliptic curves for bilinear and post-quantum cryptography. The co-supervisor for Thales is Olivier Bernard.

❷ Prizes and Distinctions

The full list of 29 invited talks (17 international, 12 in France) is given in appendix. Team members gave 5 invited talks at ECC over the period 2016–2020. A. Guillevic received a best paper award at the WAIFI'2018 conference in Bergen, Norway for the paper [62]. S. Abelard received the PhD prize of Université de Lorraine from the IAEM doctoral school (computer science, automatic) for his PhD thesis [3]. C. Pierrot was awarded the DGA (Direction Générale de l'Armement) Prize from Florence Parly, the Minister of the Armed Forces, for her PhD thesis. P. Gaudry won 2,000,000 rubles of bug bounty for the discovery of weaknesses in the Moscow Internet voting system.

❸ Editorial and organizational activities

Members of the team served as PC members for many conferences, including: Eurocrypt (2016, 2017, 2020, 2021), Asiacrypt (2019), MyCrypt (2016), Latincrypt (2017, 2019), ECC (2017), WCC (2017, 2019), SAC (2016), ANTS (2018, 2020), ISSAC (2017, 2019), WAIFI (2016, 2020), PKC (2018), CFAIL (2020), the SILC workshop (2020), the Journées C2 (2017, 2020).

The team is (or was) also present in the steering committees of the ECC Conference series (P. Gaudry, 2014–) and the ANTS conference series (E. Thomé, 2011–2020).

❹ Services as expert or evaluator

The complete list of evaluation and hiring committees as well as thesis juries to which we took part can be found in the appendix.

Collectively, we participated in 25 hiring committees at the assistant professor or professor positions, or juries for junior or senior research scientist positions.

In total, team members had 48 participations in PhD or habilitation thesis juries, including 11 as advisor or co-advisor, 12 as member, 14 as referee, and 12 as president of the jury (including one also as reviewer).

5 Collaborations

We have an informal collaboration with N. Heninger from University of California, San Diego (and previously University of Pennsylvania), which has led to several joint publications on different topics [55, 21, 69, 85, 105]. Pierre-Jean Spaenlehauer had a four-year collaboration from 2014 to 2018 with Frédéric Bihan (Université Savoie Mont-Blanc) on the topic of sparse polynomial systems; this has led to the joint publication [22]. We have a long-standing collaboration with the AriC team (LIP, Lyon) on the development and enhancement of the GNU MPFR library and related topics [58, 61]. Since 2014, Marine Minier collaborates with Christine Solnon from CITI Laboratory in Lyon. Together and partly with Pascal Lafourcade, they have published several papers [56, 24, 31], successfully obtained the ANR Decrypt Project and co-supervised the PhD thesis of Loïc Rouquette in Lyon. Since 2019, A. Guillevic works with Youssef El Housni, PhD student of the GRACE team (Inria Saclay) and research engineer at EY, now at Consensys, Daniel Augot, and François Morain, on pairing-friendly curves for blockchains [74]. In 2019 A. Guillevic started an informal collaboration with M. Guillevic and M. Vollmer, EMPA.

6 Invitations and stays outside

The list of 29 invited talks is given in the appendix. E. Thomé was invited during a week at the University of Pennsylvania in October 2016. A. Guillevic visited EMPA, Switzerland, July 15–18 2019, November 25–28, 2019, July 20–23, 2020 to work with M. Guillevic and M. Vollmer.

Involvement with social, economic and cultural environment

Activities related to cryptanalysis. Our work on integer factorization and discrete logarithm is of interest for governmental agencies and standardization bodies for tuning accurately their key size recommendations. In December 2020 we applied to the ANR on a joint project with ANSSI and LIP6 on this topic. We do not have any formal relation with the German BSI, but we know them very well.

After the conference PKC'2020, discussions on pairing-friendly curve key sizes because of IETF draft proposal led to the summary web page `https://members.loria.fr/AGuillevic/pairing-friendly-curves/` written by A. Guillevic.

During 2016–2018, we worked on training and consulting activities with the French Ministry of Defense. Due to confidentiality clauses, we cannot say much.

Activities related to e-voting. In connection with our work on the Belenios software, we have participated in four contracts (Docapost, Idemia, NomadicLabs, Canton of Geneva) where we evaluated the e-voting solutions of the companies and proposed them directions for improvements.

	2016-2020
Software	5 active + 5 new
APP (Software)	2
Patents (Brevet)	1
Contracts with companies	4
Cifre	2
Contracts, Consortium	1
Start-up	0
Expertizes	1
Radio broadcasts, TV, Newspapers	
Scientific mediation: articles, interviews, videos, etc.	13

In the above table, the number of software tools which were created or modified over the evaluation period was extracted from the BIL Inria database.

❶ Relations with companies and economic players

We had two Cifre grants over the period: S. Rasoamiaramanana, 2017–2020, supervised by Marine Minier, and Gilles Macario-rat for Orange Gardens at Châtillon-Montrouge; and S. Masson, 2018–2021, supervised by Emmanuel Thomé and Aurore Guillevic (ACT), and Olivier Bernard for Thales Communication & Security, Gennevilliers. (See also Sec. 1). The team has four contracts related to e-voting, listed in Sec. 1.

❷ General public audience activities

We wrote two articles in Le Monde, a well known French newspaper in 2019, and gave a talk at La Cité des Sciences, a museum dedicated to science in Paris in 2019. Concerning the youngsters, we organized a MATh.en.JEANS atelier in 2016-2017 and 2017-2018, both with a class from Lycée Vauban in Luxembourg; we presented computer science activities to a class in Toulouse in 2018; we gave interviews (video, radio) to promote scientific studies in 2018 and led online panel discussions to help students in high-school to have a clear picture on research in computer science in 2020.

The research paper [69] on RSA-240, RSA-250 factorization and discrete logarithm computation was vulgarized in [85], targetting engineers (without specific knowledge in cryptography).

The involvement in training through research

	2016-2020
Course books, etc	1
E-learnings, MOOC	
Heads of masters (mention and parcours)	1
Heads of international courses (Erasmus-mundus, etc)	

❶ Involvement of the team in training through research

SSL Seminar. With 4 other teams at LORIA, we have a regular joined seminar on the topic of security, about one per month on average. This complement team seminars, with less technical talks targeting a larger audience. While the core participants are from teams working in computer security, there are often participants from other teams or even from outside the lab. Due to the pandemic, the SSL seminar is currently asleep, waiting for better days to allow again people from various teams to meet together.

❷ Involvement in E-Educations

❸ Courses and research schools.

Pierrick Gaudry gave a lecture at the Winter School "Mathematical foundations of asymmetric cryptography", in Aussois, France (March 2019).

E. Thomé and A. Guillevic (with C. Bouvier from LIRMM) taught cryptography, cryptanalysis, and CADO-NFS tutorials, at an Autumn school at ISI New Delhi organized by Pr. Shanta Laishram, November 28 to December 7, 2017.

❹ Responsibilities

Marine Minier is in charge of the Master Degree SIRAV ("Sécurité Informatique, Réseaux et Architectures Virtuelles"), with around 20 students per year. She also gives some lectures in this Master for 64h eq. TD.

In 2016–2020, P. Gaudry is vice-head of the Commission de mention Informatique of the École doctorale IAEM of the University of Lorraine.

Life of the team

The Caramba team is a follow-up of the Caramel team (2010-2015), which was itself the successor of the Cacao team. The short life-time of our teams is mostly due to the INRIA rule of starting a new team each time the leader changes.

The scientific life of the team is ensured by a team seminar, on a more or less monthly basis, and some residential team workshops "Journées au vert" that we try to organize every 18 months (November 17–18, 2016 and September 12–14, 2018 in the Vosges mountains). We have also a less formal meeting during the noon coffee-break on Mondays, where a member of the team explains an article she/he recently read. Since the beginning of the Covid-19 pandemic, we have started virtual activities, including a Twitter account broadcasting the main news of Caramba, and the use of an online chat service to keep easy discussions among us.

	2016-2020
Nb of seminars	31
Web site	caramba.loria.fr

Conclusion

With the recruitment of four permanent researchers since the last evaluation, the gender parity of the team changed considerably. On the thematic side, while the "NFS-like" research axis was reinforced with the arrival of Aurore Guillevic and Cécile Pierrot, we were able to open a new research axis on symmetric cryptography thanks to the arrival of Marine Minier and Virginie Lallemand.

Not all aspects of diversity are equally satisfactory: all permanent team members are French, for example. The right course of action to lessen this imbalance is not clear however, since a multitude of different factors come into play. We encouraged foreign potential applicants to apply for fix-term or permanent positions with our group in the past, and will continue to do so.

References

Doctoral Dissertations

[1] Hugo Labrande. "Explicit computation of the Abel-Jacobi map and its inverse". PhD thesis. Université de Lorraine, November 2016. tel-01403849.

[2] Laurent Grémy. "Sieve algorithms for the discrete logarithm in medium characteristic finite fields". PhD thesis. Université de Lorraine, September 2017. tel-01647623.

[3] Simon Abelard. "Counting points on hyperelliptic curves in large characteristic : algorithms and complexity". PhD thesis. Université de Lorraine, September 2018. tel-01876314.

[4] Svyatoslav Covanov. "Multiplication algorithms : bilinear complexity and fast asymptotic methods". PhD thesis. Université de Lorraine, June 2018. tel-01825744.

[5] Paul Huynh. "Design and Analysis of Lightweight Encryption Schemes". PhD thesis. Université de Lorraine, November 2020. tel-03086269.

[6] Simon Masson. "Algorithmic of curves in the context of bilinear and post-quantum cryptography". PhD thesis. Université de Lorraine, December 2020. tel-03052499.

[7] Sandra Rasoamiaramanana. "Design of white-box encryption schemes for mobile applications security". PhD thesis. Université de Lorraine, June 2020. tel-02949394.

[8] Gabrielle De Micheli. "Discrete Logarithm Cryptanalyses : Number Field Sieve and Lattice Tools for Side-Channel Attacks". PhD thesis. Université de Lorraine, May 2021. tel-03335360.

[9] Aude Le Gluher. "Symbolic Computation and Complexity Analyses for Number Theory and Cryptography". PhD thesis. Université de Lorraine, December 2021. tel-03564208.

Articles in International Peer-Reviewed Journal

[10] Shi Bai, Cyril Bouvier, Alexander Kruppa, and Paul Zimmermann. "Better polynomials for GNFS". In: *Mathematics of Computation* 85 (2016), p. 12. DOI: 10.1090/mcom3048. hal-01089507.

[11] Changbo Chen, Svyatoslav Covanov, Farnam Mansouri, Robert H. C. Moir, Marc Moreno Maza, Ning Xie, and Yuzhen Xie. “The Basic Polynomial Algebra Subprograms”. In: *ACM Communications in Computer Algebra* 50.3 (November 2016), pp. 97–100. DOI: 10.1145/3015306.3015312. hal-01404718.

[12] Steven Galbraith and Pierrick Gaudry. “Recent progress on the elliptic curve discrete logarithm problem”. In: *Designs, Codes and Cryptography* 78.1 (2016), pp. 51–72. DOI: 10.1007/s10623-015-0146-7. hal-01215623.

[13] Pierrick Gaudry, Laurent Grémy, and Marion Videau. “Collecting relations for the number field sieve in $GF(p^6)$”. In: *LMS Journal of Computation and Mathematics*. Special issue: Algorithmic Number Theory Symposium XII 19 (2016), pp. 332–350. DOI: 10.1112/S1461157016000164. hal-01273045.

[14] Hugo Labrande. “Computing Jacobi’s θ in quasi-linear time”. In: *Mathematics of Computation* (November 2016). arXiv: 1511.04248. DOI: 10.1090/mcom/3245. hal-01227699.

[15] Hugo Labrande and Emmanuel Thomé. “Computing theta functions in quasi-linear time in genus 2 and above”. In: *LMS Journal of Computation and Mathematics*. Special issue: Algorithmic Number Theory Symposium XII 19.A (August 2016), pp. 163–177. DOI: 10.1112/S1461157016000309. hal-01277169.

[16] Éric Schost and Pierre-Jean Spaenlehauer. “A Quadratically Convergent Algorithm for Structured Low-Rank Approximation”. In: *Foundations of Computational Mathematics* 16.2 (2016). arXiv: 1312.7279, pp. 457–492. DOI: 10.1007/s10208-015-9256-x. hal-00953684.

[17] Razvan Barbulescu and Armand Lachand. “Some mathematical remarks on the polynomial selection in NFS”. In: *Mathematics of Computation* 86 (2017). arXiv: 1403.0184, pp. 397–418. DOI: 10.1090/mcom/3112. hal-00954365.

[18] Jean-Philippe Échard and Pierrick Gaudry. “An harmonious encoding of instrument values by a 19th century Parisian violin dealer”. In: *Cryptologia* 41.5 (2017), pp. 448–458. DOI: 10.1080/01611194.2016.1257524. hal-01393625.

[19] Masahiro Ishii, Jérémie Detrey, Pierrick Gaudry, Atsuo Inomata, and Kazutoshi Fujikawa. “Fast Modular Arithmetic on the Kalray MPPA-256 Processor for an Energy-Efficient Implementation of ECM”. In: *IEEE Transactions on Computers* 66.12 (December 2017), pp. 2019–2030. DOI: 10.1109/TC.2017.2704082. hal-01299697.

[20] Marine Minier. “Improving impossible-differential attacks against Rijndael-160 and Rijndael-224”. In: *Designs, Codes and Cryptography* 82.1-2 (January 2017), pp. 117–129. DOI: 10.1007/s10623-016-0206-7. hal-01593371.

[21] David Adrian, Karthikeyan Bhargavan, Zakir Durumeric, Pierrick Gaudry, Matthew Green, J. Alex Halderman, Nadia Heninger, Drew Springall, Emmanuel Thomé, Luke Valenta, Benjamin Vandersloot, Eric Wustrow, Santiago Zanella-Béguelin, and Paul Zimmermann. “Imperfect forward secrecy: How Diffie-Hellman fails in practice”. In: *Communications of the ACM* 62.1 (December 2018), pp. 106–114. DOI: 10.1145/3292035. hal-01982426.

[22] Frederic Bihan, Francisco Santos, and Pierre-Jean Spaenlehauer. “A Polyhedral Method for Sparse Systems with many Positive Solutions”. In: *SIAM Journal on Applied Algebra and Geometry* 2.4 (2018). arXiv: 1804.05683, pp. 620–645. DOI: 10.1137/18M1181912. hal-01877602.

[23] Léo Ducas and Cécile Pierrot. "Polynomial Time Bounded Distance Decoding near Minkowski's Bound in Discrete Logarithm Lattices". In: *Designs, Codes and Cryptography* (October 2018). DOI: 10.1007/s10623-018-0573-3. hal-01891713.

[24] David Gérault, Pascal Lafourcade, Marine Minier, and Christine Solnon. "Revisiting AES Related-Key Differential Attacks with Constraint Programming". In: *Information Processing Letters* 139 (2018), pp. 24–29. DOI: 10.1016/j.ipl.2018.07.001. hal-01827727.

[25] Simon Abelard, Pierrick Gaudry, and Pierre-Jean Spaenlehauer. "Improved Complexity Bounds for Counting Points on Hyperelliptic Curves". In: *Foundations of Computational Mathematics* 19.3 (2019). arXiv: 1710.03448, pp. 591–621. DOI: 10.1007/s10208-018-9392-1. hal-01613530.

[26] Svyatoslav Covanov and Emmanuel Thomé. "Fast integer multiplication using generalized Fermat primes". In: *Mathematics of Computation* 88.317 (2019). arXiv: 1502.02800, pp. 1449–1477. DOI: 10.1090/mcom/3367. hal-01108166.

[27] Aurore Guillevic. "Faster individual discrete logarithms in finite fields of composite extension degree". In: *Mathematics of Computation* 88.317 (January 2019). arXiv: 1809.06135, pp. 1273–1301. DOI: 10.1090/mcom/3376. hal-01341849.

[28] Simon Abelard. "Counting points on hyperelliptic curves with explicit real multiplication in arbitrary genus". In: *Journal of Complexity* 57 (April 2020), p. 101440. DOI: 10.1016/j.jco.2019.101440. hal-01905580.

[29] Hamid Boukerrou, Paul Huynh, Virginie Lallemand, Bimal Mandal, and Marine Minier. "On the Feistel Counterpart of the Boomerang Connectivity Table : Introduction and Analysis of the FBCT". In: *IACR Transactions on Symmetric Cryptology* 2020.1 (May 2020), pp. 331–362. DOI: 10.13154/tosc.v2020.i1.331-362. hal-02945065.

[30] Nicolas David and Paul Zimmermann. "A New Ranking Function for Polynomial Selection in the Number Field Sieve". In: *Contemporary mathematics.* 75 Years of Mathematics of Computation 754 (2020), pp. 315–325. DOI: 10.1090/CONM/754/15139. hal-02151093.

[31] David Gérault, Pascal Lafourcade, Marine Minier, and Christine Solnon. "Computing AES related-key differential characteristics with constraint programming". In: *Artificial Intelligence* 278 (January 2020), p. 103183. DOI: 10.1016/j.artint.2019.103183. hal-02327893.

[32] Aurore Guillevic, Simon Masson, and Emmanuel Thomé. "Cocks-Pinch curves of embedding degrees five to eight and optimal ate pairing computation". In: *Designs, Codes and Cryptography* 88.6 (March 2020), pp. 1047–1081. DOI: 10.1007/s10623-020-00727-w. hal-02305051.

[33] Sorina Ionica and Emmanuel Thomé. "Isogeny graphs with maximal real multiplication". In: *Journal of Number Theory* 207 (February 2020). arXiv: 1407.6672, pp. 385–422. DOI: 10.1016/j.jnt.2019.06.019. hal-00967742.

[34] Aude Le Gluher and Pierre-Jean Spaenlehauer. "A Fast Randomized Geometric Algorithm for Computing Riemann-Roch Spaces". In: *Mathematics of Computation* 89 (2020). arXiv: 1811.08237, pp. 2399–2433. DOI: 10.1090/mcom/3517. hal-01930573.

[35] Subhamoy Maitra, Bimal Mandal, Thor Martinsen, Dibyendu Roy, and Pantelimon Stanica. "Analysis on Boolean function in a restricted (biased) domain". In: *IEEE Transactions on Information Theory* 66.2 (2020), pp. 1219–1231. DOI: 10.1109/TIT.2019.2932739. hal-02374194.

[36] Enea Milio and Damien Robert. "Modular polynomials on Hilbert surfaces". In: *Journal of Number Theory* (May 2020). DOI: 10.1016/j.jnt.2020.04.014. hal-01520262.

[37] Madhurima Mukhopadhyay, Palash Sarkar, Shashank Singh, and Emmanuel Thomé. "New Discrete Logarithm Computation for the Medium Prime Case Using the Function Field Sieve". In: *Advances in Mathematics of Communications* (2020). DOI: 10.3934/amc.2020119. hal-02964002.

[38] Max Alekseyev, Joseph Samuel Myers, Richard Schroeppel, Scott R Shannon, Neil James Alexander Sloane, and Paul Zimmermann. "Three Cousins of Recamán's Sequence". In: *The Fibonacci Quarterly* (2021). arXiv: 2004.14000. hal-02951011.

[39] Xavier Bonnetain and Samuel Jaques. "Quantum Period Finding against Symmetric Primitives in Practice". In: *IACR Transactions on Cryptographic Hardware and Embedded Systems* 2022.1 (November 2021), pp. 1–27. DOI: 10.46586/tches.v2022.i1.1-27. hal-03431518.

[40] Charles Bouillaguet and Paul Zimmermann. "Parallel Structured Gaussian Elimination for the Number Field Sieve". In: *Mathematical Cryptology* 0.1 (January 2021), pp. 22–39. hal-02098114.

[41] Olivier Bronchain, Sebastian Faust, Virginie Lallemand, Gregor Leander, Léo Perrin, and François-Xavier Standaert. "MOE: Multiplication Operated Encryption with Trojan Resilience". In: *IACR Transactions on Symmetric Cryptology* 2021.1 (March 2021), pp. 78–129. DOI: 10.46586/tosc.v2021.i1.78-129. hal-03453550.

[42] Benoît Cogliati, Jordan Ethan, Virginie Lallemand, Byeonghak Lee, Jooyoung Lee, and Marine Minier. "CTET+: A Beyond-Birthday-Bound Secure Tweakable Enciphering Scheme Using a Single Pseudorandom Permutation". In: *IACR Transactions on Symmetric Cryptology* 2021.4 (December 2021), pp. 1–35. DOI: 10.46586/tosc.v2021.i4.1-35. hal-03504330.

[43] Aude Le Gluher, Pierre-Jean Spaenlehauer, and Emmanuel Thomé. "Refined Analysis of the Asymptotic Complexity of the Number Field Sieve". In: *Mathematical Cryptology* 1.1 (2021). arXiv: 2007.02730, pp. 71–88. hal-02934273.

D1 : Caramba

Invited Conferences

[44] Véronique Cortier, Pierrick Gaudry, and Stephane Glondu. "Belenios: a simple private and verifiable electronic voting system". In: *Foundations of Security, Protocols, and Equational Reasoning*. Ed. by Joshua D. Guttman, Carl E. Landwehr, José Meseguer, and Dusko Pavlovic. Vol. 11565. LNCS. Fredericksburg, Virgina, United States: Springer, 2019, pp. 214–238. DOI: 10.1007/978-3-030-19052-1_14. hal-02066930.

Major International Conferences

[45] Changbo Chen, Svyatoslav Covanov, Farnam Mansouri, Marc Moreno Maza, Ning Xie, and Yuzhen Xie. "Parallel Integer Polynomial Multiplication". In: *SYNASC 2016 - 18th International Symposium on Symbolic and Numeric Algorithms for Scientific Computing*. Timisoara, Romania, September 2016, pp. 72–80. DOI: 10.1109/SYNASC.2016.024. hal-01520021.

[46] Jean-Guillaume Dumas, Erich Kaltofen, Emmanuel Thomé, and Gilles Villard. “Linear Time Interactive Certificates for the Minimal Polynomial and the Determinant of a Sparse Matrix”. In: *ISSAC'2016, Proceedings of the 2016 ACM International Symposium on Symbolic and Algebraic Computation*. arXiv: 1602.00810. Waterloo, Canada: ACM, July 2016, pp. 199–206. DOI: 10.1145/2930889.2930908. hal-01266041.

[47] Ninon Eyrolles, Louis Goubin, and Marion Videau. “Defeating MBA-based Obfuscation”. In: *2nd International Workshop on Software PROtection*. Ed. by ACM. Vienna, Austria, October 2016. DOI: 10.1145/2995306.2995308. hal-01388109.

[48] Jean-Charles Faugère, Pierre-Jean Spaenlehauer, and Jules Svartz. “Computing Small Certificates of Inconsistency of Quadratic Fewnomial Systems”. In: *International Symposium on Symbolic and Algebraic Computation (ISSAC 2016)*. arXiv: 1605.05889. Waterloo, Canada: ACM, July 2016, pp. 223–230. DOI: 10.1145/2930889.2930927. hal-01314651.

[49] Aurore Guillevic, François Morain, and Emmanuel Thomé. “Solving discrete logarithms on a 170-bit MNT curve by pairing reduction”. In: *Selected Areas in Cryptography – SAC 2016*. Ed. by Roberto Avanzi and Howard Heys. Vol. 10532. Lecture Notes in Computer Science. arXiv: 1605.07746. St. Johns, Newfoundland, Canada: Springer, August 2016, pp. 559–578. DOI: 10.1007/978-3-319-69453-5_30. hal-01320496.

[50] Adrien Guinet, Ninon Eyrolles, and Marion Videau. “Arybo: Manipulation, Canonicalization and Identification of Mixed Boolean-Arithmetic Symbolic Expressions”. In: *GreHack 2016*. Proceedings of GreHack 2016. Grenoble, France, November 2016. hal-01390528.

[51] Marine Minier and Raphael C.-W. Phan. “Tuple Cryptanalysis: Slicing and Fusing Multisets”. In: *Paradigms in Cryptology – Mycrypt 2016*. Ed. by Raphael C.-W. Phan and Moti Yung. Vol. 10311. Lecture Notes in Computer Science. Kuala Lumpur, Malaysia: Springer, December 2016, pp. 294–320. DOI: 10.1007/978-3-319-61273-7. hal-01593382.

[52] Mohab Safey El Din and Pierre-Jean Spaenlehauer. “Critical Point Computations on Smooth Varieties: Degree and Complexity bounds”. In: *International Symposium on Symbolic and Algebraic Computation (ISSAC)*. arXiv: 1605.02518. Waterloo, Canada, July 2016, pp. 183–190. DOI: 10.1145/2930889.2930929. hal-01312750.

[53] Mohammad Alaggan, Mathieu Cunche, and Marine Minier. “Non-interactive (t, n)-Incidence Counting from Differentially Private Indicator Vectors”. In: *3rd International Workshop on Security and Privacy Analytics (IWSPA 2017)*. Scottsdale, United States, March 2017. hal-01485412.

[54] Liangyu Chen, Svyatoslav Covanov, Davood Mohajerani, and Marc Moreno Maza. “Big Prime Field FFT on the GPU”. In: *ISSAC 2017*. Kaiserslautern, Germany: ACM Press, July 2017, pp. 85–92. DOI: 10.1145/3087604.3087657. hal-01518830.

[55] Joshua Fried, Pierrick Gaudry, Nadia Heninger, and Emmanuel Thomé. “A kilobit hidden SNFS discrete logarithm computation”. In: *Advances in Cryptology – EUROCRYPT 2017*. Ed. by Jean-Sébastien Coron and Jesper Buus Nielsen. Vol. 10210. Lecture Notes in Computer Science. arXiv: 1610.02874. Paris, France: Springer, April 2017, pp. 202–231. DOI: 10.1007/978-3-319-56620-7_8. hal-01376934.

[56] David Gerault, Marine Minier, and Christine Solnon. “Using Constraint Programming to solve a Cryptanalytic Problem”. In: *IJCAI 2017 - International Joint Conference on Artificial Intelligence (Sister Conference Best Paper Track)*. Melbourne, Australia, August 2017, pp. 4844–4848. hal-01528272.

[57] Laurent Grémy, Aurore Guillevic, François Morain, and Emmanuel Thomé. "Computing discrete logarithms in $GF(p^6)$". In: *Selected Areas in Cryptography – SAC 2017*. Ed. by Carlisle Adams and Jan Camenisch. Vol. 10719. Lecture Notes in Computer Science. Ottawa, Canada: Springer, August 2017, pp. 85–105. DOI: 10.1007/978-3-319-72565-9_5. hal-01624662.

[58] Vincent Lefèvre and Paul Zimmermann. "Optimized Binary64 and Binary128 Arithmetic with GNU MPFR". In: *24th IEEE Symposium on Computer Arithmetic (ARITH 24)*. Ed. by Neil Burgess, Javier Bruguera, and Florent de Dinechin. London, United Kingdom, July 2017, pp. 18–26. DOI: 10.1109/ARITH.2017.28. hal-01502326.

[59] Simon Perdrix and Luc Sanselme. "Determinism and Computational Power of Real Measurement-based Quantum Computation". In: *FCT'17- 21st International Symposium on Fundamentals of Computation Theory*. arXiv: 1610.02824. Bordeaux, France, September 2017. DOI: 10.1007/978-3-662-55751-8_31. hal-01377339.

[60] Simon Abelard, Pierrick Gaudry, and Pierre-Jean Spaenlehauer. "Counting points on genus-3 hyperelliptic curves with explicit real multiplication". In: *ANTS-XIII - Thirteenth Algorithmic Number Theory Symposium*. Madison, United States, July 2018, pp. 1–19. hal-01816256.

[61] Claude-Pierre Jeannerod, Jean-Michel Muller, and Paul Zimmermann. "On various ways to split a floating-point number". In: *ARITH 2018 - 25th IEEE Symposium on Computer Arithmetic*. Amherst (MA), United States: IEEE, June 2018, pp. 53–60. DOI: 10.1109/ARITH.2018.8464793. hal-01774587.

[62] Michael Scott and Aurore Guillevic. "A New Family of Pairing-Friendly elliptic curves". In: *International Workshop on the Arithmetic of Finite Fields - WAIFI*. Ed. by Lilya Budaghyan and Francisco Rodriguez-Henríquez. Vol. 11321. LNCS. Lilya Budaghyan and Tor Helleseth. Bergen, Norway: Springer, June 2018, pp. 43–57. DOI: 10.1007/978-3-030-05153-2_2. hal-01875361.

[63] Elena Andreeva, Virginie Lallemand, Antoon Purnal, Reza Reyhanitabar, Arnab Roy, and Damian Vizár. "Forkcipher: A New Primitive for Authenticated Encryption of Very Short Messages". In: *ASIACRYPT 2019 - 25th Annual International Conference on the Theory and Application of Cryptology and Information Security*. Advances in Cryptology – ASIACRYPT 2019. This is an extended version of the article with the same title accepted at Asiacrypt 2019. Kobe, Japan, December 2019, pp. 153–182. DOI: 10.1007/978-3-030-34621-8_6. hal-02388234.

[64] Luca De Feo, Simon Masson, Christophe Petit, and Antonio Sanso. "Verifiable Delay Functions from Supersingular Isogenies and Pairings". In: *Advances in Cryptology - ASIACRYPT 2019 - 25th International Conference on the Theory and Application of Cryptology and Information Security*. Vol. 1. Advances in Cryptology - ASIACRYPT 2019. Kobe, Japan, December 2019, pp. 248–277. DOI: 10.1007/978-3-030-34578-5_10. hal-02388349.

[65] Patrick Derbez, Virginie Lallemand, and Aleksei Udovenko. "Cryptanalysis of SKINNY in the Framework of the SKINNY 2018-2019 Cryptanalysis Competition". In: *SAC 2019 - Selected Areas in Cryptography*. Waterloo, Canada, August 2019. hal-02388239.

[66] Jérémie Detrey and Laurent Imbert. "Breaking randomized mixed-radix scalar multiplication algorithms". In: *LATINCRYPT 2019 - 6th International Conference on Cryptology and Information Security in Latin America*. Vol. 11774. Lecture Notes in Computer Science. Santiago de Chile, Chile, October 2019, pp. 24–39. DOI: 10.1007/978-3-030-30530-7_2. lirmm-02309203.

[67] Sandra Rasoamiaramanana, Gilles Macario-Rat, and Marine Minier. "White-Box Traitor-Tracing from Tardos Probabilistic Codes". In: *SecITC 2019: Innovative Security Solutions for Information Technology and Communications*. Bucharest, Romania, November 2019, pp. 125–141. DOI: 10.1007/978-3-030-41025-4_9. hal-02944663.

[68] Deng Tang, Bimal Mandal, and Subhamoy Maitra. "Vectorial Boolean Functions with Very Low Differential-Linear Uniformity Using Maiorana-McFarland Type Construction". In: *INDOCRYPT 2019 - The 20th International Conference on Cryptology in India*. Hyderabad, India, December 2019. DOI: 10.1007/978-3-030-35423-7_17. hal-02374286.

[69] Fabrice Boudot, Pierrick Gaudry, Aurore Guillevic, Nadia Heninger, Emmanuel Thomé, and Paul Zimmermann. "Comparing the difficulty of factorization and discrete logarithm: a 240-digit experiment". In: *Advances in Cryptology – CRYPTO 2020*. Ed. by Daniele Micciancio and Thomas Ristenpart. Vol. 12171. Lecture Notes in Computer Science. Santa Barbara CA, United States: Springer, August 2020, pp. 62–91. DOI: 10.1007/978-3-030-56880-1_3. hal-02863525.

[70] Véronique Cortier, Pierrick Gaudry, and Quentin Yang. "How to fake zero-knowledge proofs, again". In: *E-Vote-Id 2020 - The International Conference for Electronic Voting*. Bregenz / virtual, Austria, 2020. hal-02928953.

[71] Gabrielle De Micheli, Pierrick Gaudry, and Cécile Pierrot. "Asymptotic complexities of discrete logarithm algorithms in pairing-relevant finite fields". In: *CRYPTO 2020 - 40th Annual International Cryptology Conference*. Ed. by Daniele Micciancio and Thomas Ristenpart. Vol. 12171. Lecture Notes in Computer Science. Santa Barbara / Virtual, United States: Springer, August 2020, pp. 32–61. hal-02871839.

[72] Gabrielle De Micheli, Rémi E. Piau, and Cécile Pierrot. "A Tale of Three Signatures: practical attack of ECDSA with wNAF". In: *AFRICACRYPT 2020*. Ed. by Youssef A. Nitaj A. Vol. 12174. Lecture Notes in Computer Science. Cairo, Egypt, July 2020, pp. 361–381. DOI: 10.1007/978-3-030-51938-4_18. hal-02393302.

[73] Patrick Derbez, Paul Huynh, Virginie Lallemand, María Naya-Plasencia, Léo Perrin, and André Schrottenloher. "Cryptanalysis Results on Spook: Bringing Full-round Shadow-512 to the Light". In: *CRYPTO 2020 - 40th Annual International Cryptology Conference*. Ed. by Daniele Micciancio and Thomas Ristenpart. Vol. 12172. Lecture Notes in Computer Science. Santa Barbara / Virtual, United States, August 2020, pp. 359–388. DOI: 10.1007/978-3-030-56877-1_13. hal-02944908.

[74] Youssef El Housni and Aurore Guillevic. "Optimized and secure pairing-friendly elliptic curves suitable for one layer proof composition". In: *CANS 2020 - 19th International Conference on Cryptology and Network Security*. Ed. by Haya Shulman and Serge Vaudenay. Vol. 12579. Lecture Notes in Computer Science. Vienna / Virtual, Austria: Springer, December 2020, pp. 259–279. DOI: 10.1007/978-3-030-65411-5_13. hal-02962800.

[75] Pierrick Gaudry and Alexander Golovnev. "Breaking the encryption scheme of the Moscow Internet voting system". In: *Financial Cryptography and Data Security*. Ed. by Joseph Bonneau and Nadia Heninger. arXiv: 1908.05127 - This work is a merger of arXiv:1908.09170 and arXiv:1908.05127. Kota Kinabalu, Malaysia: Springer, 2020, pp. 32–49. DOI: 10.1007/978-3-030-51280-4_3. hal-02266264.

[76] Aurore Guillevic. "A short-list of pairing-friendly curves resistant to Special TNFS at the 128-bit security level". In: *PKC 2020 - IACR International Conference on Practice and Theory of Public-Key Cryptography*. Ed. by Aggelos Kiayias. Vol. 12111. LNCS. https://www.iacr.org/docs/pub_2013-16.html This paper is the IACR version. It can be made freely available on the homepages of authors, on their employer's institutional page, and in non-commercial archival repositories such as the Cryptology ePrint Archive, ArXiv/CoRR, HAL, etc. Edinburgh, United Kingdom: Springer, June 2020, pp. 535–564. DOI: 10.1007/978-3-030-45388-6_19. hal-02396352.

[77] Sandra Rasoamiaramanana, Marine Minier, and Gilles Macario-Rat. "A White-Box Encryption Scheme using Physically Unclonable Functions". In: *17th International Conference on Security and Cryptography*. Lieusaint - Paris, France: SCITEPRESS - Science and Technology Publications, July 2020, pp. 279–286. DOI: 10.5220/0009781002790286. hal-02944654.

Secondary International Conferences

[78] Sofiane Lagraa, Jerome Francois, Abdelkader Lahmadi, Marine Minier, Christian Hammerschmidt, and Radu State. "BotGM: Unsupervised Graph Mining to Detect Botnets in Traffic Flows". In: *CSNet 2017 - 1st Cyber Security in Networking Conference*. Rio de Janeiro, Brazil, October 2017. hal-01636480.

[79] Ritam Bhaumik, Xavier Bonnetain, André Chailloux, Gaëtan Leurent, María Naya-Plasencia, André Schrottenloher, and Yannick Seurin. "QCB: Efficient Quantum-Secure Authenticated Encryption". In: *ASIACRYPT 2021 - 27th Annual International Conference on the Theory and Application of Cryptology and Information Security*. Ed. by Mehdi Tibouchi and Huaxiong Wang. Vol. 13090. Lecture Notes in Computer Science. Singapore / Virtual, Singapore: Springer International Publishing, December 2021, pp. 668–698. DOI: 10.1007/978-3-030-92062-3_23. hal-03516739.

[80] Xavier Bonnetain, Gaëtan Leurent, María Naya-Plasencia, and André Schrottenloher. "Quantum Linearization Attacks". In: *ASIACRYPT 2021 - 27th Annual International Conference on the Theory and Application of Cryptology and Information Security*. Ed. by Mehdi Tibouchi and Huaxiong Wang. Vol. 13090. Lecture Notes in Computer Science. Singapore / Virtual, Singapore: Springer International Publishing, December 2021, pp. 422–452. DOI: 10.1007/978-3-030-92062-3_15. hal-03516730.

[81] Hamid Boukerrou, Gilles Millérioux, and Marine Minier. "Hybrid architecture of LPV dynamical systems in the context of cybersecurity". In: *4th IFAC Workshop on Linear Parameter Varying Systems, LPVS 2021*. Milano, Italy, July 2021. hal-03292416.

[82] Gabrielle De Micheli, Pierrick Gaudry, and Cécile Pierrot. "Lattice Enumeration for Tower NFS: a 521-bit Discrete Logarithm Computation". In: *ASIACRYPT 2021 - 27th Annual International Conference on the Theory and Application of Cryptology and Information Security*. Ed. by M. Tibouchi and H. Wang. Vol. 13090. ASIACRYPT. Virtual, Singapore: Springer, December 2021, pp. 67–96. DOI: 10.1007/978-3-030-92062-3_3. hal-03242324.

[83] Stéphanie Delaune, Patrick Derbez, Paul Huynh, Marine Minier, Victor Mollimard, and Charles Prud'Homme. "Efficient Methods to Search for Best Differential Characteristics on SKINNY". In: *ACNS 2021 - 19th International Conference on Applied Cryptography and Network Security*. Ed. by Kazue Sako and Nils Ole Tippenhauer. Vol. 12727. 19th International Conference on Applied Cryptography and Network Security. Kamakura, Japan, June 2021, pp. 184–207. DOI: 10.1007/978-3-030-78375-4_8. hal-03040548.

[84] Cyrius Nugier, Diane Leblanc-Albarel, Agathe Blaise, Simon Masson, Paul Huynh, and Yris Brice Wandji Piugie. "An Upcycling Tokenization Method for Credit Card Numbers". In: *SECRYPT 2021 - 18th International Conference on Security and Cryptography*. Online, France, July 2021. hal-03220739.

Articles in National Peer-Reviewed Journal

[85] Fabrice Boudot, Pierrick Gaudry, Aurore Guillevic, Nadia Heninger, Emmanuel Thomé, and Paul Zimmermann. "New factorization and discrete logarithm record computations". In: *Techniques de l'Ingenieur* (December 2020), p. 17. hal-03045666.

Book (written)

[86] Paul Zimmermann, Alexandre Casamayou, Nathann Cohen, Guillaume Connan, Thierry Dumont, Laurent Fousse, Francois Maltey, Matthias Meulien, Marc Mezzarobba, Clément Pernet, Nicolas M. Thiery, Erik Bray, John Cremona, Marcelo Forets, Alexandru Ghitza, and Hugh Thomas. *Computational Mathematics with SageMath*. SIAM, December 2018. DOI: 10.1137/1.9781611975468. hal-01646401.

Books or Proceedings Editing

[87] Daniel Augot, Faina Solov'Eva, Marine Minier, Victor A. Zinoviev, and Thomas Johansson. *Editorial: Special issue on coding and cryptography*. Vol. 87. 2-3. Springer, March 2019. DOI: 10.1007/s10623-018-00601-w. hal-02373772.

Book Chapters

[88] Richard P. Brent, Alexander Kruppa, and Paul Zimmermann. "FFT extension for algebraic-group factorization algorithms". In: *Topics in Computational Number Theory Inspired by Peter L. Montgomery*. Ed. by Joppe W. Bos and Arjen K. Lenstra. Cambridge University Press, 2017, pp. 189–205. hal-01630907.

[89] Emmanuel Thomé. "A modified block Lanczos algorithm with fewer vectors". In: *Topics in Computational Number Theory inspired by Peter L. Montgomery*. Ed. by Joppe W. Bos and Arjen K. Lenstra. arXiv: 1604.02277. Cambridge University Press, 2017, pp. 175–188. DOI: 10.1017/9781316271575.008. hal-01293351.

[90] Nigel P Smart and Emmanuel Thomé. "History of Cryptographic Key Sizes". In: *Computational Cryptography*. Ed. by Joppe Bos and Martijn Stam. Vol. 469. London Mathematical Society Lecture Note Series. Cambridge University Press, December 2021. hal-03408015.

General Audience

[91] Pierrick Gaudry and Joanna Jongwane. “À propos du vote par Internet”. In: *Interstices* (March 2017). hal-01533682.

[92] Véronique Cortier, Pierrick Gaudry, and Stephane Glondu. *(a voté) Euh non : a cliqué*. Blog Binaire LeMonde.fr. March 2018. hal-01936863.

[93] Cécile Pierrot. *De la nécessité des problèmes que l'on ne sait pas résoudre*. Blog Binaire Le Monde.frArticle de vulgarisation https://www.lemonde.fr/blog/binaire/2019/12/06/de-la-necessite-des-problemes-que-lon-ne-sait-pas-resoudre/. December 2019. hal-03213156.

Other Publication

[94] Shi Bai, Pierrick Gaudry, Alexander Kruppa, Emmanuel Thomé, and Paul Zimmermann. “Factorisation of RSA-220 with CADO-NFS”. working paper or preprint. May 2016. hal-01315738.

[95] Richard P Brent and Paul Zimmermann. “Twelve new primitive binary trinomials”. arXiv: 1605.09213 - working paper or preprint. October 2016. hal-01378493.

[96] Paul Zimmermann and Fanny Bastien. *Paul Zimmermann - CADO-NFS : PARI/GP Workshop 2016*. Videos. January 2016. medihal-01346718.

[97] Pierrick Gaudry. “Some ZK security proofs for Belenios”. working paper or preprint. 2017. hal-01576379.

[98] Laurent Grémy, Aurore Guillevic, and François Morain. “Breaking DLP in $GF(p^5)$ using 3-dimensional sieving”. working paper or preprint. July 2017. hal-01568373.

[99] David Bernhard, Véronique Cortier, Pierrick Gaudry, Mathieu Turuani, and Bogdan Warinschi. “Verifiability Analysis of CHVote”. working paper or preprint. 2018. hal-03001923.

[100] Svyatoslav Covanov. “Improved method for finding optimal formulae for bilinear maps in a finite field”. arXiv: 1705.07728 - working paper or preprint. November 2018. hal-01519408.

[101] Véronique Cortier, Jannik Dreier, Pierrick Gaudry, and Mathieu Turuani. “A simple alternative to Benaloh challenge for the cast-as-intended property in Helios/Belenios”. working paper or preprint. 2019. hal-02346420.

[102] Antoine Joux and Cecile Pierrot. “Algorithmic aspects of elliptic bases in finite field discrete logarithm algorithms”. arXiv: 1907.02689 - working paper or preprint. July 2019. hal-02173688.

[103] Xavier Bonnetain, Anne Canteaut, Véronique Cortier, Pierrick Gaudry, Lucca Hirschi, Steve Kremer, Stéphanie Lacour, Matthieu Lequesne, Gaëtan Leurent, Léo Perrin, André Schrottenloher, Emmanuel Thomé, Serge Vaudenay, and Christophe Vuillot. “Le traçage anonyme, dangereux oxymore : Analyse de risques à destination des non-spécialistes”. working paper or preprint. April 2020. hal-02997228.

[104] Luce Brotcorne, Anne Canteaut, Aline Carneiro Viana, Céline Grandmont, Benjamin Guedj, Stéphane Huot, Valérie Issarny, Guillaume Pallez, Valérie Perrier, Vivien Quema, Jean-Baptiste Pomet, Xavier Rival, Sylvain Salvati, and Emmanuel Thomé. *Indicateurs de suivi de l'activité scientifique de l'Inria*. Research Report. Inria, December 2020. hal-03033764.

[105] Gabrielle De Micheli and Nadia Heninger. “Recovering cryptographic keys from partial information, by example”. working paper or preprint. December 2020. hal-03045663.

[106] Anne Canteaut, Miguel Angel Fernández, Luc Maranget, Sophie Perin, Mario Ricchiuto, Manuel Serrano, and Emmanuel Thomé. *Évaluation des Logiciels*. Research Report. Inria, January 2021. hal-03110723.

[107] Anne Canteaut, Miguel Angel Fernández, Luc Maranget, Sophie Perin, Mario Ricchiuto, Manuel Serrano, and Emmanuel Thomé. *Software Evaluation*. Research Report. Inria, January 2021. hal-03110728.

[108] Véronique Cortier, Alexandre Debant, and Pierrick Gaudry. *A privacy attack on the Swiss Post e-voting system*. Research Report. Université de Lorraine, CNRS, Inria, LORIA, November 2021. hal-03446801.

[109] Véronique Cortier, Pierrick Gaudry, and Quentin Yang. “A toolbox for verifiable tally-hiding e-voting systems”. Cryptology ePrint Archive: Report 2021/491 https://eprint.iacr.org/2021/491. April 2021. hal-03367930.

[110] Youssef El Housni and Aurore Guillevic. “Families of SNARK-friendly 2-chains of elliptic curves”. working paper or preprint. October 2021. hal-03371573.

Software

[111] The CADO-NFS Development Team, *CADO-NFS, An Implementation of the Number Field Sieve Algorithm* version 2.3.0, April 2019. HAL: ⟨hal-02099620v1⟩, hal-02099620, VCS: http://cado-nfs.gforge.inria.fr/.

Geometric Algorithms & Models Beyond the Linear & Euclidean realm

Synopsis

1 Team Composition

Permanents

Vincent Despré (MCf UL, arrived 1/9/18),
Olivier Devillers (DR INRIA),
Laurent Dupont (MCf UL),
Xavier Goaoc (Prof UL, arrived 1/9/18),
Sylvain Lazard (DR INRIA),
Alba Marina Málaga Sabogal (MCf UL, arrived 1/9/20),
Guillaume Moroz (CR INRIA),
Marc Pouget (CR INRIA),
Monique Teillaud (DR INRIA).

	2016	2017	2018	2019	2020	Total
PR			1	1	1	1
MCF	1	1	2	2	3	3
DR	3	3	3	3	3	3
CR	2	2	2	2	2	2
Other						
Total (permanent positions)	6	6	8	8	9	9
Pr emeritus						
Guest researchers						
Post-doct. researchers	1	1	1	2	2	4
PhD Students	3	4	6	5	5	8
Master students M2		1		1	1	3
Master Students M1			1		3	4
L3 students	1	1	1	3	1	7
Engineers	1	1	1			2
Other						
Total (temporary positions)	6	7	9	11	9	24

Post-doctoral fellows

Vincent Despré (Postdoc INRIA, arrived 1/10/17, MCF since 1/9/18),
Rémi Imbach (Postdoc INRIA, 11/2014 – 10/2016),
Benedikt Kolbe (Postdoc INRIA, 11/2019 – current),
Ji-won Park (Postdoc INRIA, 09/2019 – current).

Engineers

Éric Biagioli (Engineer Inria, 11/2016 – 03/2017),
Mohamed Essia (Engineer Inria, 03/2018 – 08/2018).

Changes in team composition

The team Gamble was created from the former team Vegas in Jan. 2017. Since then, the team recruited three faculty members: Vincent Despré (2018), Xavier Goaoc (2018), and Alba Málaga (2020).

Doctoral students

Sény Diatta (Ziguinchor, Eiffel grant, 11/2014 – 01/2020)
Charles Duménil (UL, 10/2016 – current)
Galatée Hemery Vaglica (UL, 09/2018 – abandoned in 08/2020)
Nuwan Herath Mudiyanselage (INRIA, 11/2019 – current)
Iordan Iordanov (UL, 01/2016 – 03/2019)
George Krait (INRIA 11/2017 – 05/2021)
Fernand Kuibové Pefireko (Region-ANR, 10/2018 – stopped in 08/2019)
Leo Valque (UL, 09/2020 – current)

	2016-2020
Phd's defended	2
On-going PhD's	4
Average nb of papers by PhD student	3
Average duration of PhD thesis (in month)	50

Iordan Iordanov is an engineer at Corpy & Co in Japan.
Sény Diatta is teacher in a private school in Senegal.
Fernand Kuibové PhD was stopped after one year. Galatée Hemery abandoned her PhD after 2 years and resumed her position as a high school mathematics teacher (agrégée).

2 Research topics

Keywords

Computational geometry, algorithms, computer algebra, probability, discrete geometry, non-Euclidean geometry.

Research area and main goals

Starting in the eighties, the emerging computational geometry community has put a lot of effort into designing and analyzing algorithms for geometric problems. The most commonly used framework was to study the worst-case theoretical complexity of geometric problems involving linear objects (points, lines, polyhedra...) in Euclidean spaces. This so-called *classical computational geometry* has some known limitations:

- Objects: dealing with objects only defined by linear equations.
- Ambient space: considering only Euclidean spaces.
- Complexity: worst-case complexities often do not capture realistic behaviour.
- Dimension: complexities are often exponential in the dimension.
- Robustness: ignoring degeneracies and rounding errors.

Even if these limitations have already got some attention from the community,[45] a quick look at the flagship conference SoCG[46] proceedings shows that these topics still need a big effort.

It should be stressed that, in this document, the notion of certified algorithms is to be understood with respect to robustness issues. In other words, certification does not refer to programs that are proven correct with the help of mechnical proof assistants such as Coq, but to algorithms that are proven correct on paper even in the presence of degeneracies and computer-induced numerical rounding errors.

We address several of the above limitations and organize our research in five main directions:

- Non-linear computational geometry.
- Non-Euclidean computational geometry.
- Probability in computational geometry.
- Robustness issues in computational geometry.
- Discrete geometric structures.

3 Main Achievements

Non-linear computational geometry Almost all systems for drawing planar curves are subject to errors such as missing self-intersections or components. A key subproblem, which has received a lot of attention in the literature, is to isolate the singular and critical points of such curves. We reached a major achievement on this subproblem by presenting algorithms that are morally optimal in the sense that improving them would essentially require to improve bounds on several other fundamental problems (on resultants and roots isolation of univariate polynomials) that have hold for decades [5, 16]. We also developped an efficient software for providing certified drawings, which can be queried on a web server (*Isotop*). For possibly-analytic generic manifolds that often appear in applications, we also developed a new certified numerical approach based on Catastrophe Theory that allows us to handle 2D projections of smooth nD curves and 3D projections of smooth 4D surfaces that were beyond reach with previous state-of-the-art algorithms [22, 55, 66, 2, 104].

Non-Euclidean computational geometry From a theoretical point of view, our most striking result is probably the proof that the flip graph of triangulations on a hyperbolic surface is

[45] Bernard Chazelle and others. "Application challenges to computational geometry: CG impact task force report". In: *Advances in Discrete and Computational Geometry*. Ed. by B. Chazelle, J. E. Goodman, and R. Pollack. Vol. 223. Contemporary Mathematics. Providence: American Mathematical Society, 1999, pp. 407–463.

[46] Symposium on Computational Geometry. http://www.computational-geometry.org/.

connected [58]; the result had been known for triangulations in the Euclidean plane for years, but no generalization was known.

More globally, a specificity of our international positioning is that our contributions range from theoretical results [43, 7, 100, 107] translating mathematic properties into explicit algorithms to more practical aspects [50, 60] and even publicly accessible implementations as packages [110, 111, 112] of the CGAL library.[47]

Probability in computational geometry We made great progresses in the simulation of determinantal point processes improving the size of simulation by an order of magnitude [39]. When analyzing routing algorithms in geometric graphs, the key point is the ratio between the length of a path in the graph and the Euclidean distance between its source and target; we get several intersting results for Θ_6 graphs and Delaunay triangulations for random point distribution, including the difficult problem of the lower bound on this expected length[20, 21, 25, 33].

Robustness issues in computational geometry We presented a breakthrough result on the problem of removing self-intersections in 3D meshes. The problem is to compute a set of interior-disjoint triangles whose geometry is close to that of the input and such that the output vertices have coordinates of fixed precision, typically *doubles*. This problem is of premium importance in academic and industrial contexts because many applications require models without self intersections. Despite its theoretical and practical relevance, there was almost no literature on the subject and we presented the first satisfactory theoretical solution [35].

Discrete geometric structures We proved [59] that order types of various classical models of random point sets typically encounter only a vanishingly small fraction of all order types (of the given size). This reveals that these combinatorial structures are hard to sample in practice, and therefore that the geometric algorithms that *de facto* operate on them are difficult to test. We also presented solutions for two open problems from the 1970's: the algorithmic complexity of deciding the shellability of a simplicial complex [29] and a conjecture of Bondy and Hajnal on the growth function of hypergraphs [26].

4 Research activities

Non-linear computational geometry

Description Curved objects are ubiquitous in the world we live in. However, despite this ubiquity and decades of research in several communities, curved objects are far from being robustly and efficiently manipulated by geometric algorithms. Our work on, for instance, quadric intersections and certified drawing of plane curves has proven that dramatic improvements can be accomplished when the right mathematics and computer science concepts are put into motion. In this direction, many problems are fundamental and solutions have potential industrial impact in Computer Aided Design and Robotics for instance. Intersecting NURBS (Non-uniform rational basis splines) and meshing singular surfaces in a certified manner are important examples of such problems.

[47] www.cgal.org

Main results

Bivariate polynomial systems. We developed an algorithm with the best state-of-the-art complexity to isolate the solutions of a polynomial system of two equations in two variables [5], and thus to isolate the singular points of algebraic curves. One of the mathematical object used in this work is the resultant $r(x)$ of two bivariate polynomials $p(x, y)$ and $q(x, y)$, that is a univariate polynomial that vanishes when p and q have a common root. We developed separately a quasi-optimal algorithm to compute the first coefficients of r [47], and the state-of-the-art algorithm to compute the triangular decomposition of a bivariate system in the presence of asymptotes [16].

Certified numerical algorithms. The usual advantages of numerical methods are their efficiency and locality (one can focus on a small region) but their main drawback is that they are not certified in general. We focused on the design of certified numerical methods for some classes of singular manifolds. Using Catastrophe Theory, we developed certified numerical algorithms to isolate the singularities of (possibly analytic) curves [22, 66, 104] and surfaces [55, 2] that are the projection of smooth manifolds given by implicit equations.

Drawing curves. Following our theoretical work on bivariate polynomial systems, we developed the *Isotop* software[48] for computing certified drawings of plane algebraic curves: it takes as input a bivariate polynomial equation and returns a piecewise-linear curve with the correct topology. Using symbolic methods based on resultants and subresultants, we also developed an efficient symbolic/numeric algorithm to draw the projection of a smooth algebraic 3D curve on a plane [11].

Applications in robotics, control theory, and digital geometry. During this period, we continued our longstanding collaboration with the researchers in robotics Damien Chablat and Philippe Wenger. We analyzed the singularities of a family of delta-like robots [23], and the accuracy of the orthoglide 5-axis robot [46]. We presented a software based on computer algebra to analyze the singularities of large families of robots [75].

We also developed new collaborations on non-linear problems coming from control theory [49] and digital geometry [48].

Non-Euclidean computational geometry

Description Triangulations are central geometric data structures in many areas of science and engineering. Traditionally, their study has been limited to the Euclidean setting. Needs for triangulations in non-Euclidean settings have emerged in many areas dealing with objects whose sizes range from the nuclear to the astrophysical scale, and both in academia and in industry. It has become timely to extend the traditional focus on $\mathbb{R}^d$ of computational geometry and encompass non-Euclidean spaces.

Main results

Delaunay triangulations in closed flat spaces. We gave a definition of the Delaunay triangulation of a point set in a closed Euclidean d-manifold, i.e., a compact quotient space of the Euclidean space for a discrete group of isometries [7]. We provided an incremental algorithm to compute the Delaunay triangulation of the manifold defined by a given set of input points, if it exists. The algorithm has optimal randomized worst-case time and space complexity. To the best of our knowledge, this is the first general result on this topic.

[48] *Isotop* online server: https://isotop.gamble.loria.fr/

The algorithm was implemented for the case of the 2D square flat torus[49] and 3D cubic flat torus.[50] This implementation serves as a basis for the generation of isotropic simplicial meshes discretizing periodic 3D domains, which we also distribute in CGAL [110]. Combining and generalizing previous work, we also presented the first practical algorithm for computing triangulations of infinite point sets with translational periodicity [60].

Delaunay triangulations on closed orientable hyperbolic surfaces. Earlier work on Delaunay triangulation of point sets on the 2D flat torus, which is locally isometric to the Euclidean plane, was based on lifting the point set to a locally isometric 9-sheeted covering space of the torus.[51] We improved and generalized this construction to the context of compact orientable surfaces of higher genus, which are locally isometric to the hyperbolic plane [43]. We investigated more thoroughly the Bolza surface, homeomorphic to a sphere with two handles, both because it is the hyperbolic surface with lowest genus, and because triangulations on the Bolza surface have applications in various fields such as neuromathematics and cosmological models [43]. We also proposed an extension of the above algorithm to generalized Bolza surfaces, where the octagon is replaced by a regular $4g$-gon, leading to a surface of genus g [61, 62, 65, 100]. To the best of our knowledge, these results were the first of this kind. We presented a CGAL implementation for the Bolza surface [50, 112], which is the only available software for computing Delaunay triangulations on a hyperbolic surface. These works led to the PhD thesis of Iordan Iordanov [1].

More generally, we considered geometric triangulations of surfaces, i.e., triangulations whose edges can be realized by disjoint geodesic segments [58]. We proved that the flip graph of geometric triangulations with fixed vertices of a flat torus or a closed hyperbolic surface is connected and we gave upper bounds on the number of edge flips that are necessary to transform any geometric triangulation on such a surface into a Delaunay triangulation. We also laid the foundations for a practical algorithm to compute Delaunay triangulations on an arbitrary hyperbolic surface, akin to the work for flat tori [60], by devising methods to work with finite point sets in hyperbolic surfaces based on small, but sufficient, subsets of the universal cover [107].

Computing the Geometric Intersection Number of Curves The geometric intersection number γ of a curve c on a surface is the minimal number of self-intersections of any curve homotopic to c. Given a curve c defined on a combinatorial surface (e.g., a mesh), we presented simple algorithms to (i) decide if $\gamma = 0$ (i.e., if c is homotopic to a simple curve), (ii) compute γ and (iii) construct a curve homotopic to c that realizes γ self-intersections [28]. No polynomial-time algorithm was known for (iii) and we improved the time complexity of known algorithms for (i) and (ii) by, in particular, removing the dependance to the genus of the surface; the complexity thus only depends on the combinatorial sizes ℓ and n of the curve and of surface. Notably, our solution for (i) gives a quasi-linear $O(n + \ell \log^2 \ell)$ time algorithm answering a problem raised by Poincaré more than a century ago.

Tilings on hyperbolic surfaces. We developed the mathematical tools needed to explore isotopy classes of tilings on hyperbolic surfaces of finite genus, possibly nonorientable, with boundary, and punctured [38]. More specifically, we generalized results on Delaney-Dress combinatorial

[49] Nico Kruithof. "2D Periodic Triangulations". In: *CGAL User and Reference Manual*. 4.3. CGAL Editorial Board, 2013. URL: https://doc.cgal.org/5.2/Manual/packages.html#PkgPeriodic2Triangulation2.

[50] Manuel Caroli and Monique Teillaud. "3D Periodic Triangulations". In: *CGAL User and Reference Manual*. 3.5. CGAL Editorial Board, 2009. URL: http://www.cgal.org/Manual/3.5/doc_html/cgal_manual/packages.html#Pkg:Periodic3Triangulation3.

[51] Manuel Caroli and Monique Teillaud. "Computing 3D Periodic Triangulations". In: *Proceedings 17th European Symposium on Algorithms*. Vol. 5757. Lecture Notes in Computer Science. 2009, pp. 59–70. DOI: 10.1007/978-3-642-04128-0_6.

tiling theory using an extension of mapping class groups to orbifolds. Based on these results, we presented a method for enumerating all isotopically distinct ways of tiling, with disks, a hyperbolic surface of finite genus, possibly nonorientable and with punctures and boundary [103]. This provided a generalization of the enumeration of Delaney-Dress combinatorial tiling theory on the basis of isotopic tiling theory.

Probability in computational geometry

Description The design of efficient algorithms is driven by the analysis of their complexity. Traditionally, worst-case input and sometimes uniform distributions are considered and many results in these settings have had a great influence on the domain. Nowadays, it is necessary to be more subtle and to prove new results in between these two extreme settings. For instance, smoothed analysis, which was introduced for the simplex algorithm and which we applied successfully to convex hulls, proves that such promising alternatives exist.

Main results

Walk in geometric graphs. Walking from a known vertex or triangle to get closer to a query target using neighboring relations in a geometric graph is a classic of computational geometry and has applications in point location and routing algorithms.

The main achievement deals with the expected length on some paths using the edges of the Delaunay triangulation of a Poisson point process. There are various possibilities to define a path between a starting vertex and a query point, and the quality of this path can be measured by its stretch: the ratio between the length of the path and the Euclidean length between its endpoints.

Two decades ago, Baccelli et al. proved that the expected stretch for the so-called Voronoi path in 2D is $\frac{4}{\pi} \simeq 1.27$[52]. We generalized this result to higher dimensions proving that the expected stretch is $\frac{3}{2}$ in 3D and goes to $\sqrt{\frac{2d}{\pi}}$ for high dimensions [25]. In 2D, we have refined Baccelli's result computing the standard deviation of the stretch, and improved the path using shortcuts. The improved path has a stretch of 1.16 [21]. We also analyzed another path, called the upper path, whose expected length is $\frac{35}{3\pi^2} \simeq 1.18$ [20].

These results deal with the length of paths constructed according to some local definition. To appreciate these bounds, it is interesting to compare them to the length of the (globally defined) shortest path between the query points. Hirsch et al. recently gave a non-constructive proof that the stretch of the shortest path is strictly greater than 1[53]. We improved this result by giving a constructive proof with an explicit lower bound, even though our bound of $1 + 10^{-9}$ is far from the experimental bound of 1.04 [20].

Dealing with another kind of geometric graph, the Θ_6-graph, we designed routing algorithms having simultaneously a good complexity for Poisson distributed point sets and for the worst case distribution [33].

Random samples vs good samples. A good sample of a domain is a sample that has no big voids nor clusters of points. Such a sample is deterministically defined and depends on a parameter ϵ characterizing the size of admissible voids.

[52] François Baccelli, Konstantin Tchoumatchenko, and Sergei Zuyev. "Markov paths on the Poisson-Delaunay graph with applications to routing in mobile networks". In: *Advances in Applied Probability* 32.1 (2000), pp. 1–18. DOI: 10.1239/aap/1013540019.

[53] Christian Hirsch, David Neuhäuser, and Volker Schmidt. "Moderate deviations for shortest-path lengths on random segment process". In: *ESAIM: Probability and Statistics* 20 (2016), pp. 261–292. DOI: 10.1051/ps/2016012.

We explored the probability for a set of points evenly distributed in the domain to be a good sample when the domain is a smooth surface in $\mathbb{R}^3$ [90] or a compact domain in $\mathbb{R}^d$ [83, 86, 94]. Such results have implications on the complexity of randomized algorithms for computing the Delaunay triangulation of these point sets.

Determinantal point processes. We analyze several optimal transportation problems between determinantal point processes (DPP). We show how to estimate some of the distances between distributions of DPP they induce. We then apply these results to evaluate the accuracy of a new and fast DPP simulation algorithm. We can now simulate in a reasonable amount of time more than ten thousands points [39].

Random polytopes and the wet part for arbitrary probability distributions . We examined how the measure and the number of vertices of the convex hull of a random sample of n points from an arbitrary probability measure in $\mathbb{R}^d$ relates to the wet part of that measure. This extends classical results for the uniform distribution from a convex set[54]. The lower bound of Bárány and Larman continues to hold in the general setting, but the upper bound must be relaxed by a factor of log . We show by an example that this is tight [31].

Robustness issues in computational geometry

See Section 3.

Discrete geometric structures

Description Many geometric algorithms work, explicitly or implicitly, over discrete structures such as graphs, hypergraphs, lattices that are induced by the geometric input data. For example, convex hulls or straight-line graph drawing are essentially based on orientation predicates, and therefore operate on the so-called *order type* of the input point set. Order types are a subclass of oriented matroids that remains poorly understood: for instance, we do not even know how to sample this space with reasonable bias. One of our goals is to contribute to the development of these foundations by better understanding these discrete geometric structures.

Main results

Order types. We made several progress in the study of order types. First, we formulated the conjecture that many models of random point sets induce very concentrated distributions on order types (so that sampling random point sets is a very inefficient way to explore the space of order types). We provided experimental evidence for this conjecture as well as a sharp bound on the average bit-complexity required to decide the order type of a random point set (drawn from certain models, like uniform samples in a square) [99]. We then proved [59] this conjecture for several models of random point sets based on a sharp bound on the average number of extreme points in an order type chosen uniformly at random among all n-points order types. This work introduces new techniques to work on order types, including a projective analogue that exhibits interesting symmetry properties.

Geometric permutations. A classical question in discrete geometry asks for the maximum number of orders in which n pairwise disjoint convex sets in $\mathbb{R}^d$ can be stabbed by a line. The answer is known for $d = 2$ (it is $2n - 2$); for $d \geq 3$, the answer is known to be $\Omega(n^{d-1})$ and $O(n^{2d-3} \log n)$. We made new progress on the combinatorial constraints that govern these orders

[54] Imre Bárány and David G Larman. "Convex bodies, economic cap coverings, random polytopes". In: *Mathematika* 35.70 (1988), pp. 274–291.

in $\mathbb{R}^3$ [56]. Our methods introduce a combinatorial analogue of the Veronese embedding that allows to decide purely combinatorially the emptiness of certain classes of semi-algebraic sets.

D1 : Gamble

Combinatorial geometry and topology. We also completed [27] a (90+ pages) survey on discrete convexity and topology and some of their applications in game theory, graph theory, optimization and geometric data analysis.

NP-completeness of shellability. We established [29] that the shellability problem is NP-complete. A pure d-dimensional simplicial complex is *shellable* if there exists a linear ordering $\sigma_1, \sigma_2, \ldots, \sigma_n$ of its facets such that, for every $i \geq 2$, $\sigma_i \cap (\cup_{j<i}\sigma_j)$ is a pure $(d-1)$-dimensional simplicial complex. The question of the complexity of the decision problem (given an input pure simplicial complex, decide whether it is shellable) was open since the 1970's. We proved that this problem is NP-complete, a property that extends to related problems in for instance polytope theory, topological combinatorics, and algebraic combinatorics.

Growth rates of shatter functions. The shatter function (or growth function) of a hypergraph $\mathcal{H}$ measures, as a function of k, the maximum number of traces $\mathcal{H}$ can have on k vertices. In statistical learning theory, this gives rise to a famous dichotomy: a growth function is either polynomially bounded or 2^k. We analyzed [26] how the asymptotic growth rate of a shatter function can be controlled by fixing a single of its values. As a consequence, we refute a conjecture of Bondy and Hajnal from the 1970's that proposed a refinement of the above-mentioned dichotomy.

Scientific production and quality

	2016-2020
PhD Thesis	3
H.D.R	0
Journals	38
Major conferences	18
Other conferences	14
Book chapters	2
Books (written)	0
Special issues (edited)	0
Other productions from workshops	0
General audience papers	0
Participation in editorial committees	4
Evaluation of labs and research structures	1
European projects (as project manager/Member)	
Other international projects (as project manager/Member)	3/0
ANR, PHRC, FUI, INCA, etc. (as project manager/Member)	3/2
Projects with Region Grand Est, etc (as project manager/Member)	
PIA (as project manager/Member)	
Others (as project manager/Member)	
Prizes and distinctions	2
IUF	1
Responsibilities in scientific communities (GDR etc.)	3
Organizations of Conferences (national/international)	2/12
Invitations (national/international)	0/1
Stays in foreign laboratories	12

❶ List of top journals in which we have published

Journal of Computational Geometry (8) [4, 8, 9, 10, 14, 18, 19, 33]
Discrete and Computational Geometry (4) [7, 25, 32, 35]
Journal of the ACM (2) [28, 29]
Journal of Symbolic Computation (2) [11, 16]
SIAM Journal on Discrete Mathematics (1) [26]
Bulletin of the AMS (1) [27]
Advances in Applied Probability (1) [20]
Journal of Complexity (1) [5]

❷ List of top conferences in which we have published

SoCG — International Symposium on Computational Geometry (7) [43, 45, 50, 53, 56, 58, 59]
ESA — European Symposium on Algorithms (3) [52, 54, 60]

GD — International Symposium on Graph Drawing & Network Visualization (2) [44, 51]
ISSAC — ACM International Symposium on Symbolic and Algebraic Computation (1) [47]

3 Software

Here is the list of software released during the period, see appendix for details:

- CGAL 3D periodic regular triangulations. Regular triangulation in the cubic 3D flat torus. https://doc.cgal.org/latest/Manual/packages.html#PkgPeriodic3Triangulation3.
- CGAL 3D Periodic Mesh Generation. Volumic meshes in the cubic 3D flat torus. https://doc.cgal.org/latest/Manual/packages.html#PkgMesh3 [110].
- CGAL 2D Hyperbolic Delaunay Triangulations. Delaunay triangulation in the Poincaré disk model. https://doc.cgal.org/latest/Manual/packages.html#PkgHyperbolicTriangulation2 [111].
- CGAL 2D Periodic Hyperbolic Triangulations. Delaunay triangulations of the Bolza surface. https://doc.cgal.org/latest/Manual/packages.html#PkgHyperbolicTriangulation2 [112].
- Isotop: Drawing algebraic plane curves with certified topology (polyline approximation isotopic to the input curve) https://isotop.gamble.loria.fr/.
- SubdivisionSolver. Subdivision solver to isolate the roots of 0-dimensional polynomial systems. http://subdiv-solver.gforge.inria.fr/, [79]
- Clenshaw. Real root solver based on subdivision for standard and chebyshev polynomials. https://gitlab.inria.fr/gmoro/clenshaw.
- Voxelize. Subdivision solver to enclose points, curves and surfaces. https://gitlab.inria.fr/gmoro/voxelize, [55].
- Dpp. Generation of determinantal point processes. https://gitlab.inria.fr/gmoro/point_process, [39]

The academic reputation and appeal

1 Participation in projects and External funding

We were leader of three ANR projects and participated in two others. We also had two Inria associated teams, one PHC, and one IUF Junior grant. See details in appendix.

2 Prizes and Distinctions

Best papers

Xavier Goaoc received the best paper award at the 36th International Symposium on Computational Geometry for his paper *Convex Hulls of Random Order Types* coauthored with Emo Welzl (ETH Zurich) [59].

Monique Teillaud received the best paper award at the 28th European Symposium on Algorithms (Track Engineering and Applications) for her paper *Generalizing CGAL Periodic Delaunay Triangulations* coauthored with Georg Osang (IST Austria) and Mael Rouxel-Labbé (Geometry Factory) [60].

Keynote talks

Monique Teillaud gave a keynote talk at the 36th European Workshop on Computational Geometry: *Triangulations in CGAL - To non-Euclidean spaces and beyond!* [42].

3 Editorial and organizational activities

Program Committees: Seven PC committees (SoCG, WoCG, WADS, ICCG, EuroCGx2, Maple conference. See appendix).

Editorial responsibilities. Managing editor of the *Journal of Computational Geometry* (JoCG). Editors of the journals *Graphical Models*, *Computational Geometry: Theory and Applications* (CGTA), and *International Journal of Computational Geometry and Applications* (IJCGA). Two members of the CGAL Editorial Board.

Steering committees. Computational Geometry steering committtee (chair) from 2016 to 2020. Steering committee of the *European Symposium on Algorithms* (ESA) until 2016.

Workshop organizations. Our team regularly organizes various workshops with, in particular, 16 workshops during the evaluation period (see appendix).

Hiring committees. Team members participated in 10 hiring committees for faculty positions or INRIA CRCN positions (3 times chairing the committee).

Other local responsabilities. Team members are or were involved in various committees managing the scientific life of the lab: LORIA conseil scientifique, LORIA conseil de laboratoire, pôle AM2I de l'UL, Fédération Charles Hermite, INRIA PhD and postdoc hiring committee (chair), INRIA Scientific Advisor for Technologic Development, INRIA Comité des utilisateurs des moyens informatiques (chair), INRIA Commission de développement technologique, INRIA Bureau du comité des projets, école doctorale IAEM, CLHSCT, Agos.

Other national responsabilities. Conseil Scientifique de la Société Informatique de France, INRIA BIL, INRIA Mission Jeunes Chercheurs (chair), Commission Pédagogique Nationale du MENRT multimedia et Internet.

4 Services as expert or evaluator

Members of GAMBLE are occasionally reviewing proposals or applications for foreign research agencies (e.g., FWF, NWO, NSERC, ISF, etc.) or foreign universities. We are not giving more details here to preserve anonymity.

We also participated to 9 PhD and Habilitation committees including 4 as external examiners (rapporteurs), but excluding those as advisor.

5 Collaborations

We have a large set of collaborators with 33 co-authors within France and 42 abroad over the evaluation period.

Our main collaboration about *non-linear computational geometry* is with Fabrice Rouiller [5, 46, 16, 23, 75][55] at Inria Paris. We also worked on robotic applications with Damien Chablat and Philippe Wenger at the CNRS laboratory LS2N [46, 23, 75].

[55] Daouda Niang Diatta, Sény Diatta, Fabrice Rouillier, Marie-Françoise Roy, and Michael Sagraloff. "Bounds for polynomials on algebraic numbers and application to curve topology". In: *Discrete and Computational Geometry* (February 2022). DOI: 10.1007/s00454-021-00353-w. hal-01891417.

We mostly collaborate with mathematicians in the axis *non-Euclidean computational geometry*. Our main partner in the Associate Team OrbiCG[56] (and later) is Gert Vegter (Groningen) [43, 61, 62, 65, 100] while we are working with Jean-Marc Schlenker and Hugo Parlier (Luxembourg) [89, 96] in SoS,[57] an international project co-funded by ANR and FNR.

Concerning *probability in computational geometry* our collaborations are structured by the associated team TRIP and the ANR project Aspag involving mathematicians and specialists of algorithm analysis [8, 10, 86, 20, 32, 33, 99].

Our main collaborations on *discrete geometric structures* have been with KAIST, Daejeon South Korea (Andreas Holmsen) [56], Charles University, Prague (Pavel Paták, Zuzana Patáková and Martin Tancer) and IST Austria, Vienna (Uli Wagner) [29], Carneggie Mellon University, Pittsburg (Boris Bukh) [26] and ETH Zürich (Emo Welzl) [59].

6 Invitations and stays outside

I. Iordanov spent one month at University of Luxembourg in 2016. V. Despré spent 3 weeks there in 2019. O. Devillers spent 1 month at Carleton University, Canada in 2017 and a week in 2019. C. Duménil spent 2 weeks there in 2018 and S. Lazard also 2 weeks in 2019 and M. Teillaud 1 week in 2019. M. Teillaud and I. Iordanov spent 1 month each at University of Groningen, Netherlands, in 2018 and again 2 weeks for M. Teillaud in 2019 and in 2020. Xavier Goaoc spent 1 week at UNAM Queretaro, in Mexico in 2019.

The following colleagues also visited our team during the evaluation period: Gert Vegter (Univerity of Groningen, Netherlands, about 3 times 1 month plus 2 weeks), Matthijs Ebbens (University of Groningen, 1 week), Jean-Lou De Carufel and Prosenjit Bose (Carleton Univ., Canada, 1 week each), Martin Tancer, Vojta Kalusza and Pavel Paták (Charles University, Prague, 1 week each), Andreas Holmsen and Otfried Cheong (KAIST, South Korea, 1 week each), Zuzanna Patáková (IST Austria, Vienna, 1 week).

Involvement with social, economic and cultural environment

	2016-2020
Software	3
APP (Software)	1 (+ 2 in progress)
Patents (Brevet)	
Contracts with companies	
Cifre	
Contracts, Consortium	
Start-up	
Expertizes	11
Radio broadcasts, TV, Newspapers	
Scientific mediation : articles, interviews, videos, etc.	

[56] https://members.loria.fr/Monique.Teillaud/collab/Astonishing/
[57] https://members.loria.fr/Monique.Teillaud/collab/SoS/

❶ Relations with companies and economic players

WATERLOO MAPLE INC

A two-years licence and cooperation agreement was signed on April 1st, 2018 between WATERLOO MAPLE INC., Ontario, Canada (represented by Laurent Bernardin, its Executive Vice President Products and Solutions) and Inria. On the Inria side, this contract involves the teams GAMBLE and OURAGAN (Paris), and it is coordinated by Fabrice Rouillier (OURAGAN).

F. Rouillier and GAMBLE are the developers of the ISOTOP software for the computation of topology of curves. One objective of the contract is to transfer a version of ISOTOP to WATERLOO MAPLE INC.

Geometry Factory

CGAL packages developed in Gamble are commercialized by Geometry Factory. There is a permanent contract between Geometry Factory and Inria.

During the period, three packages have been released: [110, 111, 112].

❷ General public audience activities

G. Moroz is member of the committee for the Olympiades de mathematiques.

L. Dupont was involved in many events for popularization of computer science for general audience or for high-school teachers (see appendix).

Alba Málaga is also very involved in popularization but since she was only recently hired, she has no activity to report yet.

The involvement in training through research

	2016-2020
Course books, etc	[76]
E-learnings, MOOC	
Heads of masters (mention and parcours)	1
Heads of international courses (Erasmus-mundus, etc)	

❶ Courses and research schools.

Team members are involved in about half a dozen courses at master's level, details are available in appendix.

❷ Responsibilities

Members of the team have responsabilities of several diploma and are involved in some national working groups (list in appendix).

Life of the team

Seminars

	2016-2020
Nb of seminars	8 + 75
Web site	`gamble.loria.fr`

The Gamble team contribute about twice a year to the departement seminar (Url).

Within the team, we organize twice a month a seminar where people present a result from the literature. With the Covid crisis, this internal seminar turned online and weekly.

Team management

Regular meetings (about twice a month) gather the permanent staff to manage the life of the team (budget, travels, interns,...). Recruitment policy at all levels (permanent, doc, postdoc,...) are discussed in these meetings.

Recruitment

Near the end of the VEGAS project-team, our number of PhD students was extremely low. With the creation of GAMBLE, we succeeded in seriously improving the situation and we have hosted 8 new PhD students since 2016, two defended and unfortunately two of these PhD candidates left prematurely. Nevertheless the recruitment of good students remains a difficulty and we are still facing a risk for the future. The main issue remains to attract good candidates fitting the expectancy of double competence in maths and computer science.

Parity

With 2/9 permanent female researchers, the parity score is average for the domain. We would be delighted to recruit female people if we have had more applications.

Life of the lab

Team members are involved in various committees managing the scientific life of the lab or at a national level.

- Pôle AM2I de l'UL (O. Devillers),
- INRIA Comission Information et Édition Scientifique (L.Dupont),
- Fédération Charles Hermite (X. Goaoc),
- INRIA Mission Jeunes Chercheurs (chair, S. Lazard),
- LORIA Conseil scientifique (S. Lazard),
- LORIA department chair (S. Lazard),
- UL Associate Prof hiring committee (chair, S. Lazard),
- INRIA PhD and postdoc hiring committee (chair, S. Lazard),
- École doctorale IAEM (S. Lazard),
- INRIA Comité des utilisateurs des moyens informatiques (chair, G. Moroz),
- INRIA Commission de développement technologique (G. Moroz),

- CLHSCT (G. Moroz),
- INRIA Comité de centre (M. Pouget),
- Agos (M. Pouget),
- INRIA Scientific Advisor for Technologic Development (M. Teillaud),
- LORIA Conseil de laboratoire (M. Teillaud),
- INRIA BIL work group (M. Teillaud).

References

Doctoral Dissertations

[1] Iordan Iordanov. "Delaunay triangulations of a family of symmetric hyperbolic surfaces in practice". PhD thesis. Université de Lorraine, March 2019. tel-02072155.

[2] Seny Diatta. "Topology of real algebraic curves and projection of real analytic surfaces." PhD thesis. Université Assane Seck de Ziguinchor (UASZ), January 2020. tel-03101708.

[3] George Krait. "Isolating the Singularities of the Plane Projection of Generic Space Curves and Applications in Robotics". PhD thesis. Université de Lorraine, May 2021. tel-03241794.

Articles in International Peer-Reviewed Journal

[4] Dominique Attali, Olivier Devillers, Marc Glisse, and Sylvain Lazard. "Recognizing Shrinkable Complexes Is NP-Complete". In: *Journal of Computational Geometry* 7.1 (2016), pp. 430–443. DOI: 10.20382/jocg.v7i1a18. hal-01384396.

[5] Yacine Bouzidi, Sylvain Lazard, Guillaume Moroz, Marc Pouget, Fabrice Rouillier, and Michael Sagraloff. "Solving bivariate systems using Rational Univariate Representations". In: *Journal of Complexity* 37 (2016), pp. 34–75. DOI: 10.1016/j.jco.2016.07.002. hal-01342211.

[6] Nicolas Broutin, Olivier Devillers, and Ross Hemsley. "Efficiently navigating a random Delaunay triangulation". In: *Random Structures and Algorithms* 49.1 (2016), pp. 95–136. DOI: 10.1002/rsa.20630. hal-00940743.

[7] Manuel Caroli and Monique Teillaud. "Delaunay triangulations of closed Euclidean d-orbifolds". In: *Discrete and Computational Geometry* 55.4 (2016), pp. 827–853. DOI: 10.1007/s00454-016-9782-6. hal-01294409.

[8] Olivier Devillers, Marc Glisse, Xavier Goaoc, and Rémy Thomasse. "Smoothed complexity of convex hulls by witnesses and collectors". In: *Journal of Computational Geometry* 7.2 (2016), pp. 101–144. DOI: 10.20382/jocg.v7i2a6. hal-01285120.

[9] Olivier Devillers and Ross Hemsley. "The worst visibility walk in a random Delaunay triangulation is $O(\sqrt{n})$ ". In: *Journal of Computational Geometry* 7.1 (2016), pp. 332–359. DOI: 10.20382/jocg.v7i1a16. hal-01348831.

[10] Marc Glisse, Sylvain Lazard, Julien Michel, and Marc Pouget. "Silhouette of a random polytope". In: *Journal of Computational Geometry* 7.1 (2016), p. 14. DOI: 10.20382/jocg.v7i1a5. hal-01289699.

[11] Rémi Imbach, Guillaume Moroz, and Marc Pouget. "A certified numerical algorithm for the topology of resultant and discriminant curves". In: *Journal of Symbolic Computation* 80, Part 2 (2016), pp. 285–306. DOI: 10.1016/j.jsc.2016.03.011. hal-01402194.

[12] Pegah Kamousi, Sylvain Lazard, Anil Maheshwari, and Stefanie Wuhrer. "Analysis of Farthest Point Sampling for Approximating Geodesics in a Graph". In: *Computational Geometry* 57 (August 2016), pp. 1–7. DOI: 10.1016/j.comgeo.2016.05.005. hal-01297624.

[13] Guillaume Moroz and Boris Aronov. "Computing the Distance between Piecewise-Linear Bivariate Functions". In: *ACM Transactions on Algorithms* 12.1 (February 2016), 3:1–3:13. DOI: 10.1145/2847257. hal-01112394.

[14] Olivier Devillers, Menelaos Karavelas, and Monique Teillaud. "Qualitative Symbolic Perturbation: Two Applications of a New Geometry-based Perturbation Framework". In: *Journal of Computational Geometry* 8.1 (2017), pp. 282–315. DOI: 10.20382/jocg.v8i1a11. hal-01586511.

[15] Rémi Imbach, Pascal Mathis, and Pascal Schreck. "A robust and efficient method for solving point distance problems by homotopy". In: *Mathematical Programming* 163.1-2 (May 2017), pp. 115–144. DOI: 10.1007/s10107-016-1058-7. hal-02077912.

[16] Sylvain Lazard, Marc Pouget, and Fabrice Rouillier. "Bivariate triangular decompositions in the presence of asymptotes". In: *Journal of Symbolic Computation* 82 (2017), pp. 123–133. DOI: 10.1016/j.jsc.2017.01.004. hal-01468796.

[17] David Bremner, Olivier Devillers, Marc Glisse, Sylvain Lazard, Giuseppe Liotta, Tamara Mchedlidze, Guillaume Moroz, Sue Whitesides, and Stephen Wismath. "Monotone Simultaneous Paths Embeddings in $\mathbb{R}^d$". In: *Discrete Mathematics and Theoretical Computer Science* Vol. 20 no. 1.1 (January 2018), pp. 1–11. DOI: 10.23638/DMTCS-20-1-1. hal-01529154.

[18] Luca Castelli Aleardi and Olivier Devillers. "Array-based Compact Data Structures for Triangulations: Practical Solutions with Theoretical Guarantees". In: *Journal of Computational Geometry* 9.1 (2018), pp. 247–289. DOI: 10.20382/jocg.v9i1a8. hal-01846652.

[19] Luca Castelli Aleardi, Olivier Devillers, and Eric Fusy. "Canonical Ordering for Graphs on the Cylinder with Applications to Periodic Straight-line Drawings on the Flat Cylinder and Torus". In: *Journal of Computational Geometry* 9.1 (2018), pp. 391–429. DOI: 10.20382/jocg.v9i1a14. hal-01959590.

[20] Nicolas Chenavier and Olivier Devillers. "Stretch Factor in a Planar Poisson-Delaunay Triangulation with a Large Intensity". In: *Advances in Applied Probability* 50.1 (2018), pp. 35–56. DOI: 10.1017/apr.2018.3. hal-01700778.

[21] Olivier Devillers and Louis Noizet. "Walking in a Planar Poisson-Delaunay Triangulation: Shortcuts in the Voronoi Path". In: *International Journal of Computational Geometry and Applications* 28.3 (2018), pp. 255–269. DOI: 10.1142/S0218195918500061. hal-01712628.

[22] Rémi Imbach, Guillaume Moroz, and Marc Pouget. "Reliable Location with Respect to the Projection of a Smooth Space Curve". In: *Reliable Computing* 26 (2018), pp. 13–55. hal-01920444.

[23] Ranjan Jha, Damien Chablat, Luc Baron, Fabrice Rouillier, and Guillaume Moroz. "Workspace, Joint space and Singularities of a family of Delta-Like Robot". In: *Mechanism and Machine Theory* 127 (September 2018), pp. 73–95. DOI: 10.1016/j.mechmachtheory.2018.05.004. hal-01796066.

[24] Wouter Kuijper, Victor Ermolaev, and Olivier Devillers. "Celestial Walk: A Terminating, Memoryless Walk for Convex Subdivisions". In: *Journal of Computer Graphics Techniques* 7.3 (2018), pp. 29–49. hal-01867771.

[25] Pedro Machado Manhães De Castro and Olivier Devillers. "Expected Length of the Voronoi Path in a High Dimensional Poisson-Delaunay Triangulation". In: *Discrete and Computational Geometry* 60.1 (2018), pp. 200–219. DOI: 10.1007/s00454-017-9866-y. hal-01477030.

[26] Boris Bukh and Xavier Goaoc. "Shatter functions with polynomial growth rates". In: *SIAM Journal on Discrete Mathematics* 33.2 (2019). arXiv: 1701.06632, pp. 784–794. DOI: 10.1137/17M1113680. hal-02050524.

[27] Jesús A. De Loera, Xavier Goaoc, Frédéric Meunier, and Nabil Mustafa. "The discrete yet ubiquitous theorems of Caratheodory, Helly, Sperner, Tucker, and Tverberg". In: *Bulletin of the American Mathematical Society* 56 (2019). arXiv: 1706.05975, pp. 415–511. DOI: 10.1090/bull/1653. hal-02050466.

[28] Vincent Despré and Francis Lazarus. "Computing the Geometric Intersection Number of Curves". In: *Journal of the ACM (JACM)* 66.6 (November 2019). arXiv: 1511.09327 - 59 pages, 33 figures, revised version accepted to Journal of the ACM. The time complexity for testing if a curve is homotopic to a simple one has been reduced to $O(n + \ell \log \ell)$, pp. 1–49. DOI: 10.1145/3363367. hal-02385419.

[29] Xavier Goaoc, Pavel Paták, Zuzana Patáková, Martin Tancer, and Uli Wagner. "Shellability is NP-complete". In: *Journal of the ACM (JACM)* 66.3 (June 2019). arXiv: 1711.08436, pp. 1–18. DOI: 10.1145/3314024. hal-02050505.

[30] Sylvain Lazard, William Lenhart, and Giuseppe Liotta. "On the Edge-length Ratio of Outerplanar Graphs". In: *Theoretical Computer Science* 770 (2019), pp. 88–94. DOI: 10.1016/j.tcs.2018.10.002. hal-01886947.

[31] Imre Barany, Matthieu Fradelizi, Xavier Goaoc, Alfredo Hubard, and Günter Rote. "Random polytopes and the wet part for arbitrary probability distributions". In: *Annales Henri Lebesgue* 3 (2020). arXiv: 1902.06519, pp. 701–715. DOI: 10.5802/ahl.44. hal-02937527.

[32] Jean-Daniel Boissonnat, Olivier Devillers, Kunal Dutta, and Marc Glisse. "Randomized incremental construction of Delaunay triangulations of nice point sets". In: *Discrete and Computational Geometry* 64 (2020), p. 33. DOI: 10.1007/s00454-020-00235-7. hal-02937624.

[33] Prosenjit Bose, Jean-Lou De Carufel, and Olivier Devillers. "Expected Complexity of Routing in Θ_6 and Half-Θ_6 Graphs". In: *Journal of Computational Geometry* 11.1 (2020), pp. 212–234. DOI: 10.20382/jocg.v11i1a9. hal-02922660.

[34] Steven Chaplick, Thomas C Van Dijk, Myroslav Kryven, Ji-won Park, Alexander Ravsky, and Alexander Wolff. "Bundled Crossings Revisited". In: *Journal of Graph Algorithms and Applications* (June 2020). DOI: 10.7155/jgaa.00534. hal-02972975.

[35] Olivier Devillers, Sylvain Lazard, and William Lenhart. "Rounding meshes in 3D". In: *Discrete and Computational Geometry* (April 2020). DOI: 10.1007/s00454-020-00202-2. hal-02549290.

[36] Samuel Hornus, Tim Kuipers, Olivier Devillers, Monique Teillaud, Jonàs Martínez, Marc Glisse, Sylvain Lazard, and Sylvain Lefebvre. "Variable-width contouring for additive manufacturing". In: *ACM Transactions on Graphics* 39.4 (Proc. SIGGRAPH) (July 2020). DOI: 10.1145/3386569.3392448. hal-02568677.

[37] Rémi Imbach, Marc Pouget, and Chee Yap. "Clustering Complex Zeros of Triangular Systems of Polynomials". In: *Mathematics in Computer Science* (June 2020). DOI: 10.1007/s11786-020-00482-0. hal-02878388.

[38] Benedikt Kolbe and Myfanwy Evans. "Isotopic tiling theory for hyperbolic surfaces". In: *Geometriae Dedicata* (July 2020). DOI: 10.1007/s10711-020-00554-2. hal-02981001.

[39] Laurent Decreusefond and Guillaume Moroz. "Optimal transport between determinantal point processes and application to fast simulation". In: *Modern Stochastics: Theory and Applications* 8.2 (2021), pp. 209–237. DOI: 10.15559/21-VMSTA180. hal-02984323.

[40] Xavier Goaoc, Andreas Holmsen, and Cyril Nicaud. "An experimental study of forbidden patterns in geometric permutations by combinatorial lifting". In: *Journal of Computational Geometry*. Special Issue of Selected Papers from SoCG 2019 11.2 (January 2021). arXiv: 1903.03014, pp. 131–161. DOI: 10.20382/jocg.v11i2a6. hal-03152958.

[41] George Krait, Sylvain Lazard, Guillaume Moroz, and Marc Pouget. "Certified numerical algorithm for isolating the singularities of the plane projection of generic smooth space curves". In: *Journal of Computational and Applied Mathematics* 394 (October 2021), p. 113553. DOI: 10.1016/j.cam.2021.113553. hal-03161393.

Invited Conferences

[42] Monique Teillaud. "Triangulations in CGAL - To non-Euclidean spaces and beyond!" In: *EuroCG 2020 - 36th European Workshop on Computational Geometry*. Würzburg, Germany, March 2020. hal-02510046.

Major International Conferences

[43] Mikhail Bogdanov, Monique Teillaud, and Gert Vegter. "Delaunay triangulations on orientable surfaces of low genus". In: *32nd International Symposium on Computational Geometry*. Boston, United States, June 2016, 20:1–20:15. DOI: 10.4230/LIPIcs.SoCG.2016.20. hal-01276386.

[44] David Bremner, Olivier Devillers, Marc Glisse, Sylvain Lazard, Giuseppe Liotta, Tamara Mchedlidze, Sue Whitesides, and Stephen Wismath. "Monotone Simultaneous Paths Embeddings in $\mathbb{R}^d$". In: *24th International Symposium on Graph Drawing & Network Visualization*. Vol. 9801. Proceedings of 24th International Symposium on Graph Drawing & Network Visualization. arXiv: 1608.08791. Athens, Greece: Springer, September 2016. hal-01366148.

[45] Olivier Devillers, Menelaos Karavelas, and Monique Teillaud. "Qualitative Symbolic Perturbation". In: *Proceedings of the 32nd International Symposium on Computational Geometry*. Boston, United States, June 2016, 33:1–33:15. DOI: 10.4230/LIPIcs.SoCG.2016.33. hal-01276444.

[46] Ranjan Jha, Damien Chablat, Fabrice Rouillier, and Guillaume Moroz. “Influence of the trajectory planning on the accuracy of the orthoglide 5-axis”. In: *ASME International Design Engineering Technical Conference and the Computer and Information in Engineering Conference (IDETC/CIE)*. Charlotte, NC, United States, August 2016. hal-01309190.

[47] Guillaume Moroz and Éric Schost. “A Fast Algorithm for Computing the Truncated Resultant”. In: *ISSAC '16*. Ed. by Markus Rosenkranz. Proceedings of the ACM on International Symposium on Symbolic and Algebraic Computation. arXiv: 1609.04259. Sergei A. Abramov and Eugene V. Zima. Waterloo, Canada: ACM, July 2016, pp. 341–348. DOI: 10.1145/2930889.2930931. hal-01366386.

[48] Kacper Pluta, Guillaume Moroz, Yukiko Kenmochi, and Pascal Romon. “Quadric Arrangement in Classifying Rigid Motions of a 3D Digital Image”. In: *The 18th International Workshop on Computer Algebra in Scientific Computing*. Vol. 9890. Lecture Notes in Computer Science. Bucharest, Romania: Springer, September 2016, pp. 426–443. DOI: 10.1007/978-3-319-45641-6_27. hal-01334257.

[49] Yacine Bouzidi, Thomas Cluzeau, Guillaume Moroz, and Alban Quadrat. “Computing effectively stabilizing controllers for a class of nD systems”. In: *The 20th World Congress of the International Federation of Automatic Control*. Vol. 50. 1. arXiv: 1801.04982. Toulouse, France, July 2017, pp. 1847–1852. DOI: 10.1016/j.ifacol.2017.08.200. hal-01667161.

[50] Iordan Iordanov and Monique Teillaud. “Implementing Delaunay Triangulations of the Bolza Surface”. In: *33rd International Symposium on Computational Geometry (SoCG 2017)*. Brisbane, Australia, July 2017, 44:1–44:15. DOI: 10.4230/LIPIcs.SoCG.2017.44. hal-01568002.

[51] Sylvain Lazard, William Lenhart, and Giuseppe Liotta. “On the Edge-length Ratio of Outerplanar Graphs”. In: *International Symposium on Graph Drawing and Network Visualization*. Boston, United States, 2017. hal-01591699.

[52] Nicolas Bonichon, Prosenjit Bose, Jean-Lou De Carufel, Vincent Despré, Darryl Hill, and Michiel Smid. “Improved Routing on the Delaunay Triangulation”. In: *ESA 2018 - 26th Annual European Symposium on Algorithms*. Helsinki, Finland, August 2018. DOI: 10.4230/LIPIcs.ESA.2018.22. hal-01881280.

[53] Olivier Devillers, Sylvain Lazard, and William Lenhart. “3D Snap Rounding”. In: *Proceedings of the 34th International Symposium on Computational Geometry*. Budapest, Hungary, June 2018, 30:1–30:14. DOI: 10.4230/LIPIcs.SoCG.2018.30. hal-01727375.

[54] Jean-Daniel Boissonnat, Olivier Devillers, Kunal Dutta, and Marc Glisse. “Randomized incremental construction of Delaunay triangulations of nice point sets”. In: *ESA 2019 - 27th Annual European Symposium on Algorithms*. Munich, Germany, September 2019. DOI: 10.4230/LIPIcs.ESA.2019.22. hal-02185566.

[55] Sény Diatta, Guillaume Moroz, and Marc Pouget. “Reliable Computation of the Singularities of the Projection in R3 of a Generic Surface of R4”. In: *MACIS 2019 - Mathematical Aspects of Computer and Information Sciences*. Gebze-Istanbul, Turkey, November 2019. hal-02406758.

[56] Xavier Goaoc, Andreas Holmsen, and Cyril Nicaud. “An experimental study of forbidden patterns in geometric permutations by combinatorial lifting”. In: *35th International Symposium on Computational Geometry*. arXiv: 1903.03014. Portland, United States, 2019. DOI: 10.4230/LIPIcs.SoCG.2019.40. hal-02050539.

[57] Rémi Imbach, Marc Pouget, and Chee Yap. "Clustering Complex Zeros of Triangular System of Polynomials". In: *CASC 2019 - 21st International Workshop on Computer Algebra in Scientific Computing*. arXiv: 1806.10164. Moscow, Russia, August 2019. hal-01825708.

[58] Vincent Despré, Jean-Marc Schlenker, and Monique Teillaud. "Flipping Geometric Triangulations on Hyperbolic Surfaces". In: *SoCG 2020 - 36th International Symposium on Computational Geometry*. Zurich, Switzerland, June 2020. DOI: 10.4230/LIPIcs.SoCG.2020.35. hal-02886493.

[59] Xavier Goaoc and Emo Welzl. "Convex Hulls of Random Order Types". In: *SoCG 2020 - 36th International Symposium on Computational Geometry*. Ed. by Sergio Cabello and Danny Z. Chen. Vol. 164. 36th International Symposium on Computational Geometry (SoCG 2020). arXiv: 2003.08456 - Best paper award. Zürich / Virtual, Switzerland, June 2020, 49:1–49:15. DOI: 10.4230/LIPIcs.SoCG.2020.49. hal-02879289.

[60] Georg Osang, Mael Rouxel-Labbé, and Monique Teillaud. "Generalizing CGAL Periodic Delaunay Triangulations". In: *ALGO 2020 - 28th European Symposium on Algorithms*. Best Paper Award (Track B: Engineering and Applications). Pise / Virtual, Italy, September 2020, 75:1–75:17. DOI: 10.4230/LIPIcs.ESA.2020.75. hal-02923439.

Secondary International Conferences

[61] Matthijs Ebbens, Iordan Iordanov, Monique Teillaud, and Gert Vegter. "Delaunay triangulations of regular hyperbolic surfaces". In: *9th International Conference on Curves and Surfaces*. Arcachon, France, June 2018. hal-01801136.

[62] Matthijs Ebbens, Iordan Iordanov, Monique Teillaud, and Gert Vegter. "Systole of regular hyperbolic surfaces with an application to Delaunay triangulations". In: *9th International Conference on Curves and Surfaces*. Arcachon, France, June 2018. hal-01803443.

[63] Kevin Buchin, Pedro M. M. de Castro, Olivier Devillers, and Menelaos Karavelas. "Hardness results on Voronoi, Laguerre and Apollonius diagrams". In: *CCCG 2019 - Canadian Conference on Computational Geometry*. Edmonton, Canada, August 2019. hal-02186693.

[64] Olivier Devillers and Charles Duménil. "A Poisson sample of a smooth surface is a good sample". In: *EuroCG 2019 - 35th European Workshop on Computational Geometry*. Utrecht, Netherlands, March 2019. hal-02394144.

[65] Matthijs Ebbens, Iordan Iordanov, Monique Teillaud, and Gert Vegter. "Delaunay triangulations of symmetric hyperbolic surfaces". In: *EuroCG 2019 - 35th European Workshop on Computational Geometry*. Utrecht, Netherlands, March 2019. hal-02940717.

[66] George Krait, Sylvain Lazard, Guillaume Moroz, and Marc Pouget. "Numerical Algorithm for the Topology of Singular Plane Curves". In: *EuroCG 2019 - 35th European Workshop on Computational Geometry*. Utrecht, Netherlands, March 2019. hal-02294028.

[67] Viviane Ledoux and Guillaume Moroz. "Evaluation of Chebyshev polynomials on intervals and application to root finding". In: *Mathematical Aspects of Computer and Information Sciences 2019*. arXiv: 1912.05843. Gebze, Turkey, November 2019. hal-02405752.

[68] Prosenjit Bose, Jean-Lou De Carufel, and Olivier Devillers. "Expected Complexity of Routing in Θ_6 and Half-Θ_6 Graphs". In: *EuroCG 2020 - 36th European Workshop on Computational Geometry*. Würzburg, Germany, March 2020. hal-02479502.

[69] Vincent Despré, Michaël Rao, and Stéphan Thomassé. “Testing Balanced Splitting Cycles in Complete Triangulations”. In: *Canadian Conference on Computational Geometry (CCCG 2020)*. Saskatchewan/Online, Canada, August 2020. DOI: 10.4230/LIPIcs. hal-03059811.

[70] Benedikt Kolbe and Myfanwy Evans. “Enumerating tilings of triply-periodic minimal surfaces with rotational symmetries”. In: *EuroCG 2020- 36th European Workshop on Computational Geometry*. Würzburg, Germany, 2020. hal-02961522.

[71] Ji-won Park and Otfried Cheong. “Smallest Universal Covers for Families of Triangles”. In: *EuroCG 2020 - 36th European Workshop on Computational Geometry*. Würzburg, Germany, March 2020. hal-02972966.

[72] Olivier Devillers and Charles Duménil. “Stochastic Analysis of Empty-Region Graphs”. In: *CCCG 2021 - 33rd Canadian Conference on Computational Geometry*. Halifax / Virtual, Canada, August 2021. hal-03296186.

[73] Xavier Goaoc, Andreas Holmsen, and Zuzana Patáková. “A Stepping-Up Lemma for Topological Set Systems”. In: *SoCG 2021 - 37th International Symposium on Computational Geometry*. Vol. 189. arXiv: 2103.09286. Buffalo/virtual, United States, June 2021, 40:1–40:17. DOI: 10.4230/LIPIcs.SoCG.2021.40. hal-03341599.

[74] Guillaume Moroz. “New data structure for univariate polynomial approximation and applications to root isolation, numerical multipoint evaluation, and other problems”. In: *FOCS 2021 - 62nd Annual IEEE Symposimum on Foundations of Computer Science*. arXiv: 2106.02505. Denver, United States, February 2021. hal-03249123.

Book Chapters

[75] Damien Chablat, Guillaume Moroz, Fabrice Rouillier, and Philippe Wenger. “Using Maple to analyse parallel robots”. In: *Maple in Mathematics Education and Research*. Ed. by Jürgen Gerhard and Ilias Kotsireas. Maple in Mathematics Education and Research. Springer, Cham, February 2020, pp. 50–64. DOI: 10.1007/978-3-030-41258-6_4. hal-02289699.

[76] Xavier Goaoc. “Convexité combinatoire”. In: *Informatique Mathématique : Une photographie en 2020*. 2020. hal-03130356.

Other Publication

[77] Nicolas Chenavier and Olivier Devillers. *Stretch Factor of Long Paths in a planar Poisson-Delaunay Triangulation*. Research Report RR-8935. arXiv: 1607.05770. Inria, July 2016, p. 34. hal-01346203.

[78] Olivier Devillers and Louis Noizet. *Walking in a Planar Poisson-Delaunay Triangulation: Shortcuts in the Voronoi Path*. Research Report RR-8946. INRIA Nancy, August 2016. hal-01353585.

[79] Rémi Imbach. *A Subdivision Solver for Systems of Large Dense Polynomials*. Technical Report RT-0476. arXiv: 1603.07916. INRIA Nancy, March 2016, p. 13. hal-01293526.

[80] Rémi Imbach, Pascal Mathis, and Pascal Schreck. *A Robust and Efficient Method for Solving Point Distance Problems by Homotopy*. Research Report RR-8705. arXiv: 1503.07901. INRIA, July 2016. hal-01135230.

[81] Iordan Iordanov and Monique Teillaud. *Implementing Delaunay triangulations of the Bolza surface*. Research Report RR-8994. INRIA Nancy, 2016. hal-01411415.

[82] Pedro Machado Manhães De Castro and Olivier Devillers. *Expected Length of the Voronoi Path in a High Dimensional Poisson-Delaunay Triangulation*. Research Report RR-8947. Inria, August 2016. hal-01353735.

[83] Jean-Daniel Boissonnat, Olivier Devillers, Kunal Dutta, and Marc Glisse. "Delaunay triangulation of a random sample of a good sample has linear size ". working paper or preprint. December 2017. hal-01673170.

[84] Luca Castelli Aleardi and Olivier Devillers. *Explicit array-based compact data structures for triangulations: practical solutions with theoretical guarantees*. Research Report RR-7736. INRIA, 2017, p. 39. inria-00623762.

[85] Luca Castelli Aleardi, Olivier Devillers, and Eric Fusy. "Canonical ordering for graphs on the cylinder, with applications to periodic straight-line drawings on the flat cylinder and torus". arXiv: 1206.1919 - 37 pages. 2017. hal-01646724.

[86] Olivier Devillers and Marc Glisse. *Delaunay triangulation of a random sample of a good sample has linear size*. Research Report RR-9082. Inria Saclay Ile de France ; Inria Nancy - Grand Est, July 2017, p. 6. hal-01568030.

[87] Rémi Imbach, Guillaume Moroz, and Marc Pouget. *Reliable location with respect to the projection of a smooth space curve*. Research Report. INRIA, November 2017. hal-01632344.

[88] Wouter Kuijper, Victor Ermolaev, and Olivier Devillers. *Celestial Walk: A Terminating Oblivious Walk for Convex Subdivisions*. Research Report RR-9099. arXiv: 1710.01620. INRIA Nancy, 2017. hal-01610205.

[89] Vincent Despré, Olivier Devillers, Hugo Parlier, and Jean-Marc Schlenker. "Delaunay Triangulations of Points on Circles". arXiv: 1803.11436 - working paper or preprint. April 2018. hal-01780607.

[90] Olivier Devillers and Charles Duménil. *A Poisson sample of a smooth surface is a good sample*. Research Report RR-9239. INRIA Nancy, 2018, p. 8. hal-01962631.

[91] Olivier Devillers, Sylvain Lazard, and William Lenhart. *3D Snap Rounding*. Research Report RR-9149. Inria Nancy - Grand Est, February 2018, pp. 1–22. hal-01698928.

[92] Xavier Goaoc, Alfredo Hubard, Rémi De Joannis De Verclos, Jean-Sébastien Sereni, and Jan Volec. "Limits of Order Types *". working paper or preprint. November 2018. hal-01913144.

[93] Imre Barany, Matthieu Fradelizi, Xavier Goaoc, Alfredo Hubard, and Günter Rote. *Random polytopes and the wet part for arbitrary probability distributions*. Research Report. arXiv: 1902.06519. Rényi Institute of Mathematics ; University College London ; Université Paris-Est ; Université de Lorraine ; Freie Universität Berlin, 2019. hal-02050632.

[94] Jean-Daniel Boissonnat, Olivier Devillers, Kunal Dutta, and Marc Glisse. *Randomized incremental construction of Delaunay triangulations of nice point sets*. Research Report. INRIA, 2019. hal-01950119.

[95] Prosenjit Bose, Jean-Lou De Carufel, and Olivier Devillers. *Expected Complexity of Routing in Θ_6 and Half-Θ_6 Graphs*. Research Report. arXiv: 1910.14289. INRIA, 2019, p. 18. hal-02338733.

[96] Vincent Despré, Jean-Marc Schlenker, and Monique Teillaud. *Flipping Geometric Triangulations on Hyperbolic Surfaces*. Research Report. arXiv: 1912.04640. INRIA, December 2019. hal-02400219.

[97] Leo Valque. "3D Snap Rounding". MA thesis. Université de Lyon, June 2019. hal-02393625.

[98] Otfried Cheong, Olivier Devillers, Marc Glisse, and Ji-won Park. *Covering families of triangles*. Research Report RR-9378. INRIA, 2020, p. 31. hal-03031995.

[99] Olivier Devillers, Philippe Duchon, Marc Glisse, and Xavier Goaoc. "On Order Types of Random Point Sets". arXiv: 1812.08525 - working paper or preprint. May 2020. hal-01962093.

[100] Matthijs Ebbens, Iordan Iordanov, Monique Teillaud, and Gert Vegter. "Delaunay triangulations of generalized Bolza surfaces". working paper or preprint. 2020. hal-03080125.

[101] Xavier Goaoc and Emo Welzl. "Convex Hulls of Random Order Types". arXiv: 2003.08456 - working paper or preprint. March 2020. hal-02513054.

[102] Benedikt Kolbe. "Towards a combinatorial algorithm for the enumeration of isotopy classes of symmetric cellular embeddings of graphs on hyperbolic surfaces". working paper or preprint. December 2020. hal-03047231.

[103] Benedikt Kolbe and Vanessa Robins. "Tile-transitive tilings of the Euclidean and hyperbolic planes by ribbons". working paper or preprint. December 2020. hal-03046798.

[104] George Krait, Sylvain Lazard, Guillaume Moroz, and Marc Pouget. "Isolating the singularities of the plane projection of a generic space curve". working paper or preprint. May 2020. hal-02612412.

[105] Jin-San Cheng, Kai Jin, Marc Pouget, Junyi Wen, and Bingwei Zhang. "An Improved Complexity Bound for Computing the Topology of a Real Algebraic Space Curve". working paper or preprint. December 2021. hal-03469996.

[106] Vincent Despré, Loïc Dubois, Benedikt Kolbe, and Monique Teillaud. "Experimental analysis of Delaunay flip algorithms on genus two hyperbolic surfaces". working paper or preprint. December 2021. hal-03462834.

[107] Vincent Despré, Benedikt Kolbe, and Monique Teillaud. "Representing infinite hyperbolic periodic Delaunay triangulations using finitely many Dirichlet domains". Version 3: Addition of discussion of optimality and another way to interpret the bound. July 2021. hal-03045921.

[108] Guillaume Moroz. "Fast real and complex root-finding methods for well-conditioned polynomials". arXiv: 2102.04180 - working paper or preprint. February 2021. hal-03134259.

[109] Nuwan Herath Mudiyanselage, Guillaume Moroz, and Marc Pouget. "Fast Guaranteed Drawing of High Degree Algebraic Curves". working paper or preprint. December 2021. hal-03465123.

Software

[110] Mikhail Bogdanov, Aymeric Pellé, Mael Rouxel-Labbe, and Monique Teillaud, *CGAL 3D Periodic Mesh Generation* version CGAL 4.13, 2018. HAL: ⟨hal-02983420v1⟩, hal-02983420, VCS: https://github.com/CGAL/cgal/tree/master/Periodic_3_mesh_3.

[111] Mikhail Bogdanov, Iordan Iordanov, and Monique Teillaud, *CGAL 2D Hyperbolic Delaunay Triangulations* version CGAL 4.14, 2019. HAL: ⟨hal-02983422v1⟩, hal-02983422, VCS: https://github.com/CGAL/cgal/tree/master/Hyperbolic_triangulation_2.

[112] Iordan Iordanov and Monique Teillaud, *CGAL 2D Periodic Hyperbolic Triangulations* version CGAL 4.14, 2019. HAL: ⟨hal-02983428v1⟩, hal-02983428, VCS: https://github.com/CGAL/cgal/tree/master/Periodic_4_hyperbolic_triangulation_2.

Matter from Graphics

Synopsis

1 Team Composition

Permanents

Jonàs Martínez (CR Inria, arrived 02/2017), Samuel Hornus (CR Inria, arrived 09/2008), Cédric Zanni (MCF UL, arrived 09/2016), Camille Schreck (ISFP Inria, arrived 09/2020), Sylvain Lefebvre (DR Inria, arrived 09/2006).

	2016	2017	2018	2019	2020	Total
PR						
MCF	1	1	1	1	1	1
DR	1	1	1	1	1	1
CR	2	2	2	2	2	2
Other (ISFP)					1	1
Total (permanent positions)	4	4	4	4	4	5
Post-doct. researchers	3	2				3
PhD Students	2	2	3	4	5	7
Engineers	1	2	3	4	4	5
Total (temporary positions)	6	6	6	8	9	15

Post-doctoral fellows

Shuo Jin (postdoc 2016-2017), Haichuan Song (postdoc 2015-2017), Tim-Christopher Reiner (postdoc 2015-2016).

Engineers

Salim Perchy (engineer 2016-2021), Noemie Vennin (engineer 2017-2019), Pierre Bedell (engineer 2018-2021), Pierre-Alexandre Hugron (engineer 2019-2021), Adrien Bedel (engineer 2020-2021).

Change in team composition

The MFX team was created in early 2018 as a joint Inria-University of Lorraine-CNRS team. It emerged from the ALICE team, and more specifically the ERC ShapeForge project. This report focuses the 2016–2017 period on the contributions from the MFX team members within the ALICE team.

The team was initially composed of Sylvain Lefebvre, Samuel Hornus, Jonàs Martínez and Cédric Zanni. Camille Schreck joined the MFX team in 2020.

Doctoral students

Jean Hergel (ERC 2014-2017), Jérémie Dumas (ERC 2014-2017), Semyon Efremov (Region-ANR, 2018-2021), Jimmy Etienne (CNRS, 2018-2021), Thibault Tricard (UL, 2018-2021), Melike Aydinlilar (ANR, 2019-2022), Marco Freire (UL, 2020-2023)

	2016-2020
Phd's defended	2
On-going PhD's	5
Average nb of papers by PhD student	6
Average duration of PhD thesis (in month)	40

(weighted averages by thesis months, duration reported for defended PhDs)

Jean Hergel is *intellectual property manager* for *GamerStream* (France). Jérémie Dumas is researcher at *Adobe Seattle* (USA).

2 Research topics

Keywords

Additive manufacturing, computer graphics, 3D modeling, procedural modeling, stochastic microstructures.

Research area and main goals

We focus on the computational aspects of shape modeling and processing for digital fabrication: dealing with shape complexity, revisiting design and customization of existing parts in view of the novel possibilities afforded by AM, and providing a stronger integration between modeling and the capabilities of the target processes.
We tackle the following challenges:

- develop **novel shape synthesis and shape completion algorithms** that can help users model shapes with features in the scale of microns to meters while following functional, structural, geometric, and fabrication requirements;
- propose methodologies to help *expert* designers **describe shapes** and designs that can later be **customized and adapted** to different use cases;
- develop novel algorithms to **adapt and prepare complex designs** for fabrication in a given technology, including the possibility to modify aspects of the design while preserving its functionality;

- develop novel techniques to **unlock the full potential of fabrication processes**, improving their versatility in terms of feasible shapes as well as their capabilities in terms of accuracy and quality of deposition;
- develop **novel shape representations, data-structures, visualization, and interaction techniques** to support the integration of our approaches into a single, unified software framework that covers the full chain from modeling to printing instructions;
- **integrate novel capabilities** enabled by advances in additive manufacturing processes and materials **in the modeling and processing chains**, in particular regarding the use of functional materials (e.g. piezoelectric, conductive, shrinkable).

Our approach is to cast a holistic view on the challenges above by considering modeling and fabrication as a single, unified process. Thus, the modeling techniques we seek to develop will take into account the geometric constraints imposed by the manufacturing processes (minimal thickness, overhang angles, trapped material) and the desired object functionality (rigidity, porosity). To allow for the modeling of complex shapes and adapt the same initial design to different technologies, we propose developing techniques that can automatically synthesize functional details within parts. At the same time, we will explore ways to increase the versatility of the manufacturing processes through algorithms that are capable of exploiting additional degrees of freedom (e.g., curved layering[58]), can introduce new capabilities (e.g., material mixing[59]) and improve part accuracy (e.g., adaptive slicing[60]).

Our research program is organized along with three main research directions. The first one focuses on the automatic synthesis of shapes with intricate multi-scale geometries that conform to additive manufacturing technologies' constraints. The second direction considers geometric and algorithmic techniques for the actual fabrication of the modeled object. We aim to improve further the capabilities of the manufacturing processes with novel deposition strategies. The third direction focuses on computational design algorithms to help model parts with a gradient of properties and help customize existing designs for their reuse.

These three research directions interact strongly and cross-pollinate: e.g., novel possibilities in manufacturing unlock novel possibilities in terms of shapes that can be synthesized. Stronger synthesis methods allow for further customization.

3 Main Achievements

We had significant contributions in two main areas:

- **Infill structures for additive manufacturing**. In a series of publications we introduced the notion of procedural stochastic foams for Additive Manufacturing [4, 10, 13, 18, 24, 29]. These methods allow for the efficient processing and fabrication of complex internal micro-structures, that can be freely spatially graded in density and orientation. This allows to optimize internal structures to obtain lightweight objects and controlled deformations, producing oriented orthotropic mechanical responses within the volume of a part.
- **Geometry Processing for additive manufacturing**. We contributed several advances on the topic of geometry processing for additive manufacturing: novel techniques for the computation of offset surfaces [30, 37], slicing strategies [6, 26] and algorithms [38, 40], trajectory generation for curved deposition [5, 12, 15, 19], variable width 2D offsetting [23].

[58] 12.
[59] 19.
[60] 6.

Finally, our team has gained international visibility beyond the academic domain through the *IceSL* software (icesl.loria.fr, 90K downloads, 75 objects processed everyday by the online version). A number of key technologies were developed and transferred to our industrial partner *AddUp* and are now used in their software for metal additive manufacturing.

4 Research activities

Internal structures for additively manufactured parts

Description AM processes form a 3D artifact by accumulating material in successive layers. This affords for unprecedented freedom of geometry in manufacturing. One important research direction is to leverage this in order to obtain lightweight yet robust parts, as well as parts that can be deformed in a controlled manner.

Main results We introduced several approaches to produce internal structure that can be freely graded. The key originality of our approaches is to exploit procedural techniques, that generate the structure in a streaming fashion, as they are required for manufacturing. This avoids producing the entire, extremely large geometry in memory. We rely on numerical analysis of the homogenized mechanical response of the structures to facilitate modeling by engineers. This approach is inspired by our work in the context of texturing for Computer Graphics [21].

Our approaches target different processes with different constraints: truss based structures for powder and resin systems [4, 10, 29], self-supporting structures for extrusion based systems [13, 24]. We also explored novel methodologies to produce gradation of quasi-regular structures [18]. Our work in this area is available in our software *IceSL*. This lead, for instance, to collaborations in soft-robotics [25].

Data structures and algorithm for interactive modeling and visualization

Description As the complexity of the manufactured parts increases, we need novel tools and algorithms to visualize, manipulate and process them. In particular, the vast majority of CAD software cannot efficiently display or allow interaction with the large, complex 3D models that result from modeling with internal structures.

Main results We have introduced several algorithms and methodologies to address these challenges. The key originality of our work is to rely on formulations diverging from 3D meshes (implicit surfaces, distance fields, voxels) that are efficiently rendered and processed by massively parallel algorithms. Our software *IceSL* is thus capable of modeling with all these representations, mixed together in a same 3D model that can be directly processed for AM [38]. This is performed through a novel CSG algorithm based on spatial hashing [33] – this is the first application of spatial hashing in this context, leading to an amortized constant time evaluation of CSG boolean epxressions. Recent work focuses on modeling of complex structures with implicit surfaces [16], combined with efficient visualization through novel root-finding techniques[61].

Slicing and trajectory generation for Additive Manufacturing

Description Many additive manufacturing processes require trajectories in every layer. These describe where and in which order the material is solidified (with a variety of methods: laser

[61] Melike Aydinlilar and Cédric Zanni. "Fast ray tracing of scale-invariant integral surfaces". In: *Computer Graphics Forum* (2021). DOI: 10.1111/cgf.14208. hal-03169283.

beam, extrusion, welding, etc.). The geometry, ordering and parameters of the trajectories is crucial: it determines how the volume of the part is formed and is a main factor in the final properties of the object.

We have contributed several methodologies for the generation of trajectories. We revisit the problem in light of our expertise in geometry processing and efficient computing. Our work focuses on exploiting new degrees of freedom in processes that were previously unexploited for lack of principled algorithmic approaches.

Main results We contributed novel algorithms for the determination of slicing plans [6, 26] and trajectory placement [5, 23] to reduce the error between the desired shape and the manufactured one. We contributed novel methodologies to produce colored shapes from off-the-shelf 3D printers, through specialized trajectories and micro-layering [19]. We introduce, for the first time, principled algorithms for generating *curved* trajectories in extrusion processes [12, 15]. We investigated how to produce continuous deposition paths for cermamics [17] and infill patterns [34]. Finally, we contributed techniques to print as empty as possible objects under fabrication constraints [32, 20] thus saving time and material, as well as advanced algorithm for slicing geometries under modeling operators [38, 40].

Scientific production and quality

	2016-2020
PhD Thesis	2
H.D.R	0
Journals	27
Major conferences	0
Other conferences	6
Book chapters	0
Books (written)	1
Special issues (edited)	0
Other productions from workshops	0
General audience papers	0
Participation in editorial committees	
Evaluation of labs and research structures	
European projects (as project manager/Member)	2/0
Other international projects (as project manager/Member)	
ANR, PHRC, FUI, INCA, etc. (as project manager/Member)	2/0
Projects with Region Grand Est, etc (as project manager/Member)	1/0
PIA (as project manager/Member)	
Others (as project manager/Member)	1/0
Prizes and distinctions	1
IUF	
Responsibilities in scientific communities (GDR etc.)	
Organizations of Conferences (national/international)	
Invitations (national/international)	
Stays in foreign laboratories	

1 List of top journals in which we have published

- ACM Transactions on Graphics [3, 4, 6, 7, 10, 12, 13, 14, 15, 17, 18, 19, 21, 23, 24, 26]
- Computer Graphics Forum [9, 20]

2 List of top conferences in which we have published

3 Software

Our main software activity is around IceSL `https://icesl.loria.fr`. Most of our research results are available within IceSL, with contributions from all team members.

Besides, we also have a number of open source implementations of our research on github `https://github.com/mfx-inria/`.

The academic reputation and appeal

Members of our team are regular participants in the program committees of the top conferences of our field (ACM SIGGRAPH, EUROGRAPHICS), are regularly invited to international workshops (Dagstuhl 2017, 2019, McGill-INRIA Workshop on Computational Geometry 2018, 2019, 2020, CECAM-Lorentz Workshop 2020). We actively participate in thesis committees and – as visible in our publication co-authors – have a wide international network of collaborators.

1 Participation in projects and External funding

- ERC StG Shapeforge, 2012-2017 (Sylvain Lefebvre)
- ERC PoC IceXL, 2018 (Sylvain Lefebvre)
- ANR jeune chercheur IMPRIMA (Cédric Zanni)
- ANR jeune chercheur MUFFIN (Jonàs Martínez)
- Project Orthosis4D (Lorraine Université d'Excellence, ANR)
- Project PIC (Région Grand-Est)

2 Prizes and Distinctions

- Jérémie Dumas, 2018 PhD award from IG-RV
- Sylvain Lefebvre received an ERC Proof of Concept grant (IceXL), 2018

Invited talks

- 2016, Sylvain Lefebvre: Computer Graphics lab of Aachen, led by Pr. Leif Kobbelt
- 2016, Sylvain Lefebvre: IST Austria, visiting Pr. Bernt Bickel
- 2016, Sylvain Lefebvre: invited at CNR Imati (Genova, Italy) for a week to present his work and collaborate on a joint survey paper submitted to EUROGRAPHICS 2017.
- 2018, Jonàs Martínez: invited talk in Journées Scientifiques Inria 2018.
- 2018, Sylvain Lefebvre: one hour class at the 2018 SPG Graduate School https://sgp2018.sciencesconf.org/resource/page/id/7.
- 2018, Sylvain Lefebvre: keynote speaker at the WCCM workshop Expanding the Frontiers of Engineering Design using Computation (http://www.wccm2018.org/MS_1407).
- 2018, Sylvain Lefebvre: invited talk at the JIGS (Journées Informatique et Géométrie 2018, June 21-22).
- Sylvain Lefebvre gave an invited IceSL tutorial at the Soft Robotics days in Lille (https://jrs2019.sciencesconf.org/).

- Sylvain Lefebvre gave a keynote at SPM 2020 (virtual conference), was invited at the CECAM EPFL Workshop on Computing Complex Mechanical Systems (22-24/01/2020) where he gave a presentation (https://www.cecam.org/workshop-details/76/), gave a (virtual) invited talk at the University of Hasselt (Belgium), and an invited presentation at the (virtual) symposium Impression 3D des polymères hosted by Ecole Polytechnique.

- Jonàs Martínez gave a virtual talk at Forum Cyberdéfense & Stratégie 2020 (France).

❸ Editorial and organizational activities

The team organized a free workshop on February 2017 (http://shapeforge.loria.fr/workshop/) in-between the PhD defenses of Jean Hergel and Jérémie Dumas. International jury members gave talks; the workshop was open to the public. We recorded all the talks and made them available online (https://www.youtube.com/playlist?list=PLfUzw-QfoyuWLPJpCCp6xwTAPMIjt7Q-k).

Sylvain Lefebvre co-organized the first multidisciplinary workshop on academic research in additive manufacturing within the Lorraine area, which hosted 70 participants over two days. The two days workshop started on May 31, 2018 at Inria-Nancy Grand Est and was co-organized with Sandrine Hoppe (LRGP), Samuel Kenzari (IJL) and Hakim Boudaoud (ERPI).

❹ Services as expert or evaluator

- Sylvain Lefebvre participated in a strategy meeting at ANRT on the topic of 4D printing, on November 12, 2018.

- Samuel Hornus lead the local “Commission du Dévelopement Technologique” until 2020, followed by Sylvain Lefebvre.

- Sylvain Lefebvre joined the Inria center bureau du comité des projets (BCP) in 2020.

- Jonàs Martínez is the scientific correspondent for Europe (Inria Nancy Grand-Est).

- Sylvain Lefebvre was ”rapporteur” for the PhD of Benoit Arbelot (Grenoble Universities, 2017), for the PhD thesis of Luigi Malomo (CNR Pisa, 2017) and Christian Santoni (Computational Design Lab, University of Rome, 2017). He was reviewer (rapporteur) on the PhD thesis of Geoffroy Guingo (University of Strasbourg, 2018) and participated in the thesis mid-term committees of Nicolas Lutz et Pascal Guehl (University of Strasbourg). He was reviewer (’rapporteur’) for the PhD defense of Hugo Loi (Université de Grenoble, 2019). He was a reviewer (rapporteur) on the Ph.D. thesis of Thomas Buffet (University of Strasbourg, 2020) and participated in the mid-term thesis committees of Nicolas Lutz and Pascal Guehl (University of Strasbourg, 2020). He was a reviewer (rapporteur) on the Habilitation defense of Guillaume Gilet (University of Limoges, 2020). He was a member of the Ph.D. jury of Adam Gaier (Lorraine University, 2020), and a commitee member on the Ph.D. jury of Ran Zhang (IST Austria, 2020) and Chengkai Dai (TU Delft, 2020).

- Jonàs Martínez was member of the jury for the 2020 CRCN competition at Inria Nancy Grand-Est.

- Sylvain Lefebvre was a member of the CR2 recruitment jury for Inria Nancy Grand-Est in 2016.

- Sylvain Lefebvre was a member of the jury for the Young Researcher Fellow EGFR in 2019 and 2020, which awards every year a young French researcher with outstanding research and community contributions in the field of Computer Graphics.

5 Collaborations

- University of New York (Daniele Panozzo) [15, 26]
- TU Berlin (Marc Alexa) [6, 15]
- TU Delft (Charlie CL Wang and Tim Kuipers) [12, 15, 23]
- Hong Kong University (Li-Yi Wei and Wenping Wang) [3, 7, 11, 42]

6 Invitations and stays outside

Involvement with social, economic and cultural environment

	2016-2020
Software	12
APP (Software)	9
Patents (Brevet)	-
Contracts with companies	1
Cifre	-
Contracts, Consortium	-
Start-up	-
Expertizes	-
Radio broadcasts, TV, Newspapers	1
Scientific mediation : articles, interviews, videos, etc.	

1 Relations with companies and economic players

We have a continued collaboration with the French metal additive manufacturing company *AddUp* (details are confidential).

We have regular discussions with potential industrial partners regarding our technologies. Some are ongoing and all are covered by strict non-disclosure agreements.

2 General public audience activities

Sylvain Lefebvre participated to the radio program "La méthode scientifique" on France Culture, aired on November 8 2017 (https://www.franceculture.fr/emissions/la-methode-scientifique/la-methode-scientifique-mercredi-8-novembre-2017).

Haichuan Song, Sylvain Lefebvre and Salim Perchy presented IceSL at a booth at the Maker Faire Rome 2017 (http://www.makerfairerome.eu/en/). This is a major event with 100K+ visitors every year. We presented the software to students, general public and 3D printing enthusiasts. We received a *Maker of Merit award* for our project.

On February 22, 2018 we organized and held in Paris an IceSL event for non-academic users. The objective was to bring together our community as well as new users. We invited external users, industrial partners and FabLabs at large (through national mailing lists). The gathering was a success, with 50 attendees – the maximum we could host – from a variety of backgrounds (makers and industry).

In the context of the Ada Lovelace Day, 9th October 2018, Noémie Vennin received about twenty young girls in our 3D printer room. The Ada Lovelace Day is an international celebration of the achievements of women in science, technology, engineering and maths (STEM).

In March 2019, IceSL was presented at the Maker Faire Lille, with a focus on color printing, printing big parts using cavities and polyfoams (all results from prior years now available in IceSL). IceSL was presented during an Inria Tech Talk at Station-F in Paris, along with a display of best prints (https://french-tech-central.com/events/du-modele-3d-a-la-piece-fabriquee-utilisez-icesl-pour-vos-prototypages/).

In April 2019, IceSL was presented to an audience of designers for the second part of Affinité Design (http://www.affinitedesign.com/), with a discussion about the transition from 3D printing to "4D printing", in a joint talk with Sylvain Lefebvre, Jean-Claude André and Samuel Kenzari (http://www.nancy.archi.fr/fr/biennale-du-design-grand-est-2019_-e.html).

In October 2019, Pierre Bedell and Pierre-Alexandre Hugron presented IceSL at October-MAKE, a meeting organised by the French FabLabs network (http://www.fablab.fr/octobermake/).

Sylvain Lefebvre created quick tutorial videos on Youtube (channel icesl-fr), to help introduce new users to IceSL.

The involvement in training through research

	2016-2020
Course books, etc	1
E-learnings, MOOC	-
Heads of masters (mention and parcours)	-
Heads of international courses (Erasmus-mundus, etc)	-

❶ Involvement of the team in training through research

We started classes in master programs and engineering schools around our research activities: parallel programming with GPUs (Master (M1), since before 2016), algorithms for Additive Manufacturing (ENSEM – since before 2016 – and Master (M2) since 2018). We also participate in a class on Soft-Robotics at Ecole Polytechnique since 2018.

We contributed to a book on algorithms for Additive Manufacturing [36].

❷ Involvement in E-Educations

❸ Courses and research schools.

Sylvain Lefebvre gave a one hour class at the 2018 SPG Graduate School https://sgp2018.sciencesconf.org/resource/page/id/7.

4 Responsibilities

Life of the team

	2016-2020
Nb of seminars	Weekly since 2016
Web site	https://mfx.loria.fr

References

Doctoral Dissertations

[1] Jérémie Dumas. "Controllable shape synthesis for digital fabrication". PhD thesis. Université de Lorraine, February 2017. tel-01547313.

[2] Jean Hergel. "Synthesis of fabricable shape from partial specifications". PhD thesis. Université de Lorraine, February 2017. tel-01546383.

Articles in International Peer-Reviewed Journal

[3] Weikai Chen, Xiaolong Xia, Shiqing Xin, Yang XIA, Sylvain Lefebvre, and Wenping Wang. "Synthesis of Filigrees for Digital Fabrication". In: *ACM Transactions on Graphics*. ACM Transactions on Graphics 35.4 (July 2016). DOI: 10.1145/2897824.2925911. hal-01401520.

[4] Jonàs Martínez, Jérémie Dumas, and Sylvain Lefebvre. "Procedural Voronoi Foams for Additive Manufacturing". In: *ACM Transactions on Graphics* 35 (2016), pp. 1–12. DOI: 10.1145/2897824.2925922. hal-01393741.

[5] Hai-Chuan Song, Nicolas Ray, Dmitry Sokolov, and Sylvain Lefebvre. "Anti-aliasing for fused filament deposition". In: *Computer-Aided Design* 89 (September 2016). arXiv: 1609.03032 - 14 pages, 22 figures, pp. 25–34. DOI: 10.1016/j.cad.2017.04.001. hal-01400686.

[6] Marc Alexa, Kristian Hildebrand, and Sylvain Lefebvre. "Optimal discrete slicing". In: *ACM Transactions on Graphics* 36.1 (February 2017), pp. 1–16. DOI: 10.1145/2999536. hal-01660773.

[7] Weikai Chen, Yuexin Ma, Sylvain Lefebvre, Shiqing Xin, Jonàs Martínez, and Wenping Wang. "Fabricable Tile Decors". In: *ACM Transactions on Graphics* 36.6 (2017). DOI: 10.1145/3130800.3130817. hal-01592098.

[8] Samuel Hornus. "Detecting the intersection of two convex shapes by searching on the 2-sphere". In: *Computer-Aided Design* (2017). Special issue: Proceedings of Solid and Physical Modeling (SPM 2017). DOI: 10.1016/j.cad.2017.05.009. hal-01522903.

[9] Marco Livesu, Stefano Ellero, Jonàs Martínez, Sylvain Lefebvre, and Marco Attene. "From 3D models to 3D prints: an overview of the processing pipeline". In: *Computer Graphics Forum* 36.2 (2017). DOI: 10.1111/cgf.13147. hal-01518469.

[10] Jonàs Martínez, Haichuan Song, Jérémie Dumas, and Sylvain Lefebvre. "Orthotropic k-nearest foams for additive manufacturing". In: *ACM Transactions on Graphics* 36.4 (July 2017), 121:1–121:12. DOI: 10.1145/3072959.3073638. hal-01577859.

[11] Xiaojun Bian, Li-Yi Wei, and Sylvain Lefebvre. "Tile-based Pattern Design with Topology Control". In: *Proceedings of the ACM on Computer Graphics and Interactive Techniques* 1 (2018), pp. 23–38. DOI: 10.1145/3203204. hal-01811874.

[12] Chengkai Dai, Charlie C.L. Wang, Chenming Wu, Sylvain Lefebvre, Guoxin Fang, and Yong-Jin Liu. "Support-free volume printing by multi-axis motion". In: *ACM Transactions on Graphics* 37.4 (July 2018), pp. 1–14. DOI: 10.1145/3197517.3201342. hal-01887571.

[13] Jonàs Martínez, Samuel Hornus, Haichuan Song, and Sylvain Lefebvre. "Polyhedral Voronoi diagrams for additive manufacturing". In: *ACM Transactions on Graphics*. Proceedings of SIGGRAPH 2018 37.4 (August 2018), p. 15. DOI: 10.1145/3197517.3201343. hal-01697103.

[14] Nicolas Ray, Dmitry Sokolov, Sylvain Lefebvre, and Bruno Lévy. "Meshless Voronoi on the GPU". In: *ACM Transactions on Graphics* 37.6 (December 2018), pp. 1–12. DOI: 10.1145/3272127.3275092. hal-01927559.

[15] Jimmy Etienne, Nicolas Ray, Daniele Panozzo, Samuel Hornus, Charlie C.L. Wang, Jonàs Martínez, Sara Mcmains, Marc Alexa, Brian Wyvill, and Sylvain Lefebvre. "CurviSlicer: Slightly curved slicing for 3-axis printers". In: *ACM Transactions on Graphics* 38.4 (August 2019), pp. 1–11. DOI: 10.1145/3306346.3323022. hal-02120033.

[16] Alvaro Javier Fuentes Suárez, Evelyne Hubert, and Cédric Zanni. "Anisotropic convolution surfaces". In: *Computers and Graphics* 82 (2019), pp. 106–116. DOI: 10.1016/j.cag.2019.05.018. hal-02137325.

[17] Jean Hergel, Kevin Hinz, Sylvain Lefebvre, and Bernhard Thomaszewski. "Extrusion-Based Ceramics Printing with Strictly-Continuous Deposition". In: *ACM Transactions on Graphics* (November 2019). DOI: 10.1145/3355089.3356509. hal-02363424.

[18] Jonàs Martínez, Mélina Skouras, Christian Schumacher, Samuel Hornus, Sylvain Lefebvre, and Bernhard Thomaszewski. "Star-Shaped Metrics for Mechanical Metamaterial Design". In: *ACM Transactions on Graphics* 38.4 (July 2019). Special issue, SIGGRAPH 2019, Article No. 82 :1–13. DOI: 10.1145/3306346.3322989. hal-02118846.

[19] Haichuan Song, Jonàs Martínez, Pierre Bedell, Noemie Vennin, and Sylvain Lefebvre. "Colored fused filament fabrication". In: *ACM Transactions on Graphics* 38.5 (June 2019), pp. 1–11. DOI: 10.1145/3183793. hal-01660621.

[20] Thibault Tricard, Frédéric Claux, and Sylvain Lefebvre. "Ribbed support vaults for 3D printing of hollowed objects". In: *Computer Graphics Forum* (June 2019). DOI: 10.1111/cgf.13750. hal-02155929.

[21] Thibault Tricard, Semyon Efremov, Cédric Zanni, Fabrice Neyret, Jonàs Martínez, and Sylvain Lefebvre. "Procedural Phasor Noise". In: *ACM Transactions on Graphics* 38.4 (July 2019), Article No. 57:1–13. DOI: 10.1145/3306346.3322990. hal-02118508.

[22] Guillaume Coiffier, Philippe Renard, and Sylvain Lefebvre. "3D Geological Image Synthesis From 2D Examples Using Generative Adversarial Networks". In: *Frontiers in Water* 2 (October 2020). DOI: 10.3389/frwa.2020.560598. hal-02992194.

[23] Samuel Hornus, Tim Kuipers, Olivier Devillers, Monique Teillaud, Jonàs Martínez, Marc Glisse, Sylvain Lazard, and Sylvain Lefebvre. "Variable-width contouring for additive manufacturing". In: *ACM Transactions on Graphics* 39.4 (Proc. SIGGRAPH) (July 2020). DOI: 10.1145/3386569.3392448. hal-02568677.

[24] Thibault Tricard, Vincent Tavernier, Cédric Zanni, Jonàs Martínez, Pierre-Alexandre Hugron, Fabrice Neyret, and Sylvain Lefebvre. "Freely orientable microstructures for designing deformable 3D prints". In: *ACM Transactions on Graphics* 39.6 (December 2020), pp. 1–16. DOI: 10.1145/3414685.3417790. hal-02524371.

[25] Félix Vanneste, Olivier Goury, Jonas Martinez, Sylvain Lefebvre, Hervé Delingette, and Christian Duriez. "Anisotropic soft robots based on 3D printed meso-structured materials: design, modeling by homogenization and simulation". In: *IEEE Robotics and Automation Letters* 5.2 (January 2020), pp. 2380–2386. DOI: 10.1109/LRA.2020.2969926. hal-02475589.

[26] Jinfan Yang, Chrystiano Araújo, Nicholas Vining, Zachary Ferguson, Enrique Rosales, Daniele Panozzo, Sylvain Lefebvre, Paolo Cignoni, and Sheffer Alla. "DHFSlicer: Double Height-Field Slicing for Milling Fixed-Height Materials". In: *ACM Transactions on Graphics* 39.6 (November 2020). DOI: 10.1145/3414685.3417810. hal-02992003.

[27] Justine Basselin, Laurent Alonso, Nicolas Ray, Dmitry Sokolov, Sylvain Lefebvre, and Bruno Lévy. "Restricted Power Diagrams on the GPU". In: *Computer Graphics Forum* 40.2 (June 2021). DOI: 10.1111/cgf.142610. hal-03169575.

[28] Semyon Efremov, Jonàs Martínez, and Sylvain Lefebvre. "3D periodic cellular materials with tailored symmetry and implicit grading". In: *Computer-Aided Design* 140 (November 2021). DOI: 10.1016/j.cad.2021.103086. hal-03290606.

[29] Jonàs Martínez. "Random Auxetic Porous Materials from Parametric Growth Processes". In: *Computer-Aided Design* 139 (June 2021). DOI: 10.1016/j.cad.2021.103069. hal-02911788.

Secondary International Conferences

[30] Samuel Hornus, Sylvain Lefebvre, Jérémie Dumas, and Frédéric Claux. "Tight printable enclosures and support structures for additive manufacturing". In: *Eurographics Workshop on Graphics for Digital Fabrication*. Ed. by Asla Medeiros e Sá, N. Pietroni, and K. Rodriguez Echavarria. Lisbonne, Portugal: The Eurographics Association, May 2016. hal-01399931.

[31] Tim Reiner and Sylvain Lefebvre. "Interactive Modeling of Support-free Shapes for Fabrication". In: *EUROGRAPHICS*. Proceedings of EUROGRAPHICS (short papers). Lisbonne, Portugal, May 2016. hal-01401470.

[32] Samuel Hornus and Sylvain Lefebvre. "Iterative carving for self-supporting 3D printed cavities". In: *Eurographics 2018 - Short Papers*. Delft, Netherlands, April 2018. hal-01764291.

[33] Cédric Zanni, Frédéric Claux, and Sylvain Lefebvre. "HCSG: Hashing for real-time CSG modeling". In: *Proceedings of the ACM SIGGRAPH Symposium on Interactive 3D Graphics and Games*. Montreal, Canada, May 2018. DOI: 10.1145/3203198. hal-01792866.

[34] Jimmy Etienne and Sylvain Lefebvre. “Procedural band patterns”. In: *Symposium on Interactive 3D Graphics and Games*. Symposium on Interactive 3D Graphics and Games. arXiv: 2003.01408. San Francisco, United States: Association for Computing Machinery, September 2020, pp. 1–7. DOI: 10.1145/3384382.3384522. hal-02457161.

[35] Thibault Tricard, Jimmy Etienne, Cédric Zanni, and Sylvain Lefebvre. “A brick in the wall: Staggered orientable infills for additive manufacturing”. In: *SCF 2021 - ACM Symposium on Computational Fabrication*. Boston/Virtual, United States, October 2021. DOI: 10.1145/3485114.3485117. hal-03352656.

Book (written)

[36] Marco Attene, Marco Livesu, Sylvain Lefebvre, Thomas Funkhouser, Stefano Ellero, Szymon Rusinkiewicz, Jonàs Martínez, and Amit Haim Bermano. *Design, Representations, and Processing for Additive Manufacturing*. Vol. 10. Synthesis Lectures on Visual Computing: Computer Graphics, Animation, Computational Photography, and Imaging 2. Morgan & Claypool Publishers, June 2018, p. 146. hal-01836525.

Other Publication

[37] Samuel Hornus and Sylvain Lefebvre. *Iterative carving for self-supporting 3D printed cavities*. Research Report RR-9083. Inria Nancy - Grand Est, July 2017, p. 19. hal-01570330.

[38] Sylvain Lefebvre. *Visualizing and Fabricating Complex Internal Structures*. Technical Report RT-0493. Inria Nancy - Grand Est, November 2017, p. 15. hal-01636963.

[39] Baptiste Caramiaux, Fabien Lotte, Joost Geurts, Giuseppe Amato, Malte Behrmann, Frédéric Bimbot, Fabrizio Falchi, Ander Garcia, Jaume Gibert, Guillaume Gravier, Hadmut Holken, Hartmut Koenitz, Sylvain Lefebvre, Antoine Liutkus, Andrew Perkis, Rafael Redondo, Enrico Turrin, Thierry Viéville, and Emmanuel Vincent. *AI in the media and creative industries*. Research Report. arXiv: 1905.04175. New European Media (NEM), April 2019, pp. 1–35. hal-02125504.

[40] Sylvain Lefebvre. *Efficient Direct Slicing Of Dilated And Eroded 3d Models For Additive Manufacturing: Technical Report*. Research Report. arXiv: 1911.05992. Inria Nancy - Grand Est, November 2019. hal-02360401.

[41] Adrien Bedel, Yoann Coudert-Osmont, Jonàs Martínez, Rahnuma Islam Nishat, Sue Whitesides, and Sylvain Lefebvre. “Closed space-filling curves with controlled orientation for 3D printing”. working paper or preprint. March 2021. hal-03185200.

[42] Sylvain Lefebvre, Li-Yi Wei, and Connelly Barnes. “Informational Texture Synthesis”. working paper or preprint. June 2021. hal-01706539.

Structure geometrical shapes

PIXEL is a research team in digital geometry processing. More specifically, we are interested in parameterization techniques, meshing and reconstruction of objects from 3D point clouds. We investigate mathematically correct, scalable and numerically stable solutions, by studying the properties of the objective function in order to develop efficient optimization algorithms. Our methods have applications in both Computer Graphics and Scientific Computing which we develop in cooperation with researchers and industrial partners from various fields. These applications include oil exploration, plasma physics, bio-chemistry and computer-aided design. Our main results are made available to the community in the form of original software.

Synopsis

1 Team Composition

	2016	2017	2018	2019	2020	Total
MCF	2	2	2	2	2	2
DR	1	1	1			1
CR	2	2	2	3	3	3
Total (permanent positions)	5	5	5	5	5	5
Guest researchers				1		1
Post-doct. researchers		1	1	1	1	2
PhD Students	3	2	2	3	5	8
Master students M2	1	3	1	3	3	11
Master Students M1		1		1	1	3
L3 students			3	3	2	8
Total (temporary positions)	3	4	6	9	9	31

Permanents

Laurent Alonso (CR INRIA), Dobrina Boltcheva (MCF UL), Étienne Corman (CR CNRS, arrived Dec 2019), Bruno Lévy (DR INRIA, left Oct 2018), Nicolas Ray (CR INRIA), Dmitry Sokolov (MCF UL).

Post-doctoral fellows and visiting researchers

Erica Schwindt (postdoc, 2017–2018), Sebastian Von Hausegger (postdoc, 2019–2020), Oleksandr Bondarenko (2019).

Change in team composition

Currently existing PIXEL and MFX teams stem from the same root: ALICE team. The ALICE project-team was created by Bruno Lévy in 2004 (as a local team), and then became an INRIA project in 2006.

In 2018 we had a major event: Bruno Lévy, scientific leader of ALICE, left the team to become the head of the INRIA Nancy Grand-Est research center. Moreover, conforming to the recommendation made during preceding INRIA evaluaton, ALICE was split in two teams with clear scientific focus:

- a part of the team "spun off" around Sylvain Lefebvre and his ERC project SHAPEFORGE to become the MFX team (on additive manufacturing and computer graphics),

- while PIXEL progressively moved the center of gravity of the rest of the team from computer graphics towards scientific computing and computational physics, in terms of cooperations, publications and industrial transfer.

The above team composition table corresponds to the "PIXEL half" for the 2016–2018 period (+ Étienne Corman who had joined the team in 2019).

Doctoral students

Arnaud Botella (2012–2016), Maxence Reberol (2015–2018), Julien Renaudeau (2016–2019), Justine Basselin (2019–..., CIFRE RhinoTerrain), François Protais (2019–..., INRIA scholarship), David Desobry (2020–..., contract Total–INRIA), Guillaume Coiffier (2020–..., ENS PhD program), David Lopez (2020–..., team funds)

Arnaud Botella is a CEO and co-founder of Geode-solutions, a company proposing solutions for advanced meshing. Maxence Reberol currently has a post-doctoral contract at the Catholic University of Louvain within Jean-François Remacle's research group. Julien Renaudeau is curenlty a computer science engineer at Schlumberger.

	2016-2020
Habilitations defended	1
PhD's defended	3
On-going PhD's	5

2 Research topics

Keywords

Geometry Processing: mesh generation, parameterization, optimal sampling, scientific computing, geometry processing, gpu algorithms

Research area and main goals

Numerical simulation is a key aspect in both industry and science: by replacing costly physical experiments (e.g. wind tunnel in fluid dynamics) with computer simulation, it dramatically reduces the overall cost of product development. In science, virtual experiments can be used to better understand various phenomena, especially when it is impossible to conduct direct experiments, as in astrophysics.

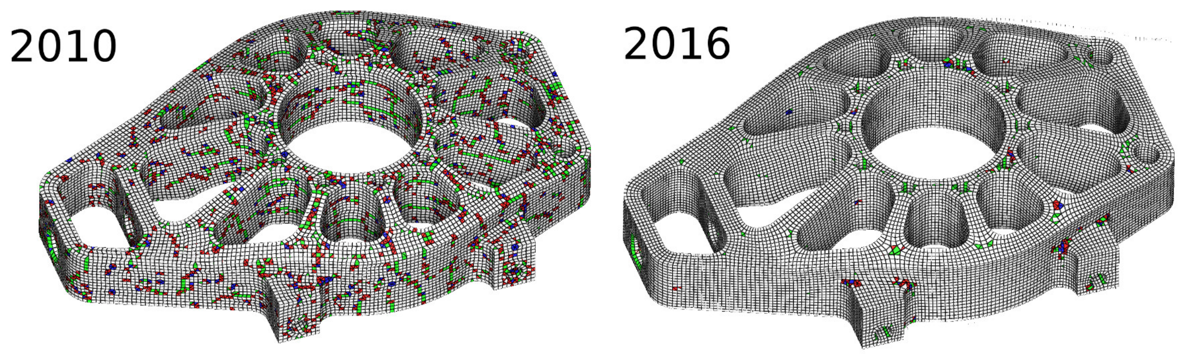
The prominent methods in numerical simulation (finite elements, finite differences, ...) depend on discretizations of the geometry (meshes), that are notoriously difficult to generate: a quick search on the NSF grant web page[62] with "mesh generation AND finite element" keywords returns more than 30 currently active grants for a total of $8 million. NASA indicates mesh generation as one of the major challenges for 2030[63], and estimates that it costs 80% of time and effort in numerical simulation. This is due to the need for constructing supports that match both the geometry and the physics of the system to be modeled.

It is very unsatisfactory that meshing, i.e. just "preparing the data" for the simulation, eats-up the major part of the time and effort. Our goal is to make the situation evolve, by (1) studying the influence of shapes and discretizations, and inventing new algorithms to automatically generate meshes that can be directly used by today's simulators and (2) studying new discretizations of the physics, that dynamically evolve in time.

PIXEL is a project-team in computer graphics, working on *geometry processing*, with a special focus to *meshing* problems. We study and develop new solutions to transform and optimize geometric representations. Our original approach to both issues is to restate the problems in terms of numerical optimization. We try to develop solutions that are provably correct, scalable and numerically stable. To reach these goals, our approach consists in transforming the geometric problem into a numerical optimization problem, studying the properties of the objective function and designing efficient minimization algorithms. Besides Computer Graphics, our goal is to develop cooperations with researchers and people from the industry, who experiment applications of our general solutions to various domains, comprising CAD, industrial design, oil exploration and plasma physics. Our solutions are distributed in both open-source software (Graphite, Geogram) and industrial software (Vorpaline).

3 Main Achievements

Meshes composed of hexahedra (deformed cubes) are desirable for certain numerical simulations, they can improve both performances and precision. They are very difficult to generate.



[62] https://www.nsf.gov/awardsearch

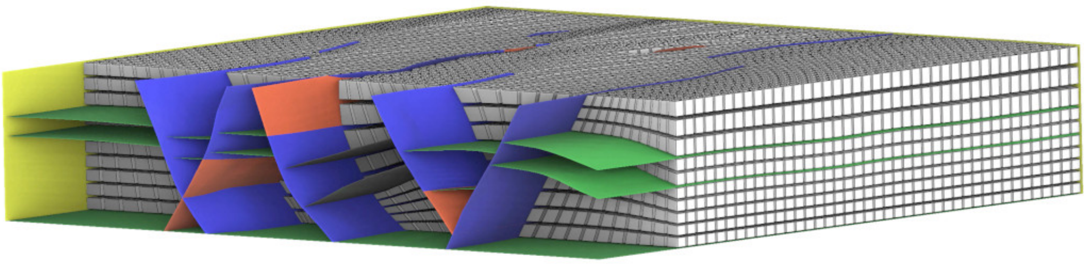
[63] J. Slotnick, A. Khodadoust, J. Alonso, D. Darmofal, G. William, L. Elizabeth, and D. Mavriplis. *CFD Vision 2030 Study: A Path to Revolutionary Computational Aerosciences.* Tech. rep. NASA/CR-2014-218178, NF1676L-18332, 2014.

We developed in 2010 one of the first fully automatic algorithms that generates a "hex-dominant" hybrid mesh (left image), with hexahedra and other elements (colored). In 2016, we made a quantum leap, and significantly reduced the number of non-hex elements (right image). Our approach is based on an optimization of a direction field [32] and a global parameterization steered by the direction field [10].

4 Research activities

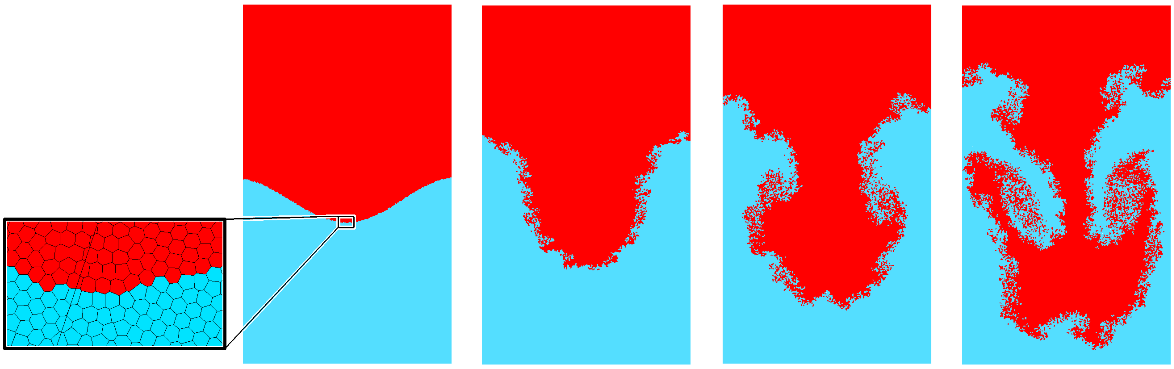
From "Hex-dominant" to "Full-Hex": meshes for today's numerical simulation ... Hexahedral meshes are composed of "deformed cubes" (hexahedra). They are appreciated for simulating certain physical phenomena (deformation mechanics, fluid dynamics ...), because they can significantly reduce computation times and improve precision. This is because (1) they contain a smaller number of elements (5 or 6 tetrahedra for 1 hexahedron), (2) the tri-linear function basis associated with them can capture finer variations and (3) they avoid "locking" phenomena encountered with tetrahedra. Unfortunately, creating a hexahedral mesh requires considerable manual intervention of the user (days, weeks, even months for the most complicated geometries).

We have a tight collaboration with geophysical modeling specialists via RING consortium. In particular, we produce hexahedral-dominant meshes for geomechanical simulations of gas and oil reservoirs. From a scientific point of view, this use case introduces new types of constraints (alignments with faults and horizons), and allows certain types of nonconformities that we did not consider until now.



This requires to solve very difficult problems, in particular around the **singularities**, that is the poles, or the zones where the mesh is different from a regular grid. We develop new **parameterization** methods [10], new **relaxation** methods [32] and exploit **combinatorics** [5, 33, 2]. We hope to **close one of the most important problems in meshing**. The result will be directly usable by existing numerical simulation softwares, and **directly transferable to the industry**, through our software VORPALINE.

Paving the road towards tomorrow's numerical simulation: the first "stones" (or cells!) Besides methods that can be directly applied to existing numerical methods, we are developing methods that use more non-conventional discretizations, such has time-evolving polyhedral meshes (Voronoi tessellations and power diagrams). Such meshes offer more degrees of freedom than more conventional fixed meshes, and may lead to easier-to-use numerical simulators, needing no manual intervention to mesh the domain.



On the other hand, a simulation that uses such a dynamic mesh is going to compute one mesh per timestep, so at first sight our approach is not reasonable! However, building on our Computer Graphics / computational geometry scientific culture, by relaxing some constraints, we can design algorithms and data structures that are much lighter than the classical ones used in scientific computing. With in head the goal of developing these new simulators, we developed efficient algorithms to compute and optimize Voronoi diagrams[64], made them available in our GEOGRAM software library, and developed a new algorithm highly efficient on the GPU [16]. Now, to simulate physics with such meshes, for instance to do fluid simulations (see figure), one needs to enforce conservation laws, the most natural one being volume conservation. The figure shows our numerical experiments with a fluid decomposed into cells. Controlling the volume of the cells requires an additional degree of freedom (moving from Voronoi to power diagrams), and we developed new numerical methods to solve the corresponding optimization problem, known as *semi-discrete optimal transport* [15]. We also developed anisotropic generalizations, using a higher-dimensional space [18].

Scientific production and quality

	2016-2020
PhD Thesis	3
H.D.R	2
Journals	25
Major conferences	8
Other conferences	10
Book chapters	1
Books (written)	1
ANR (project member)	3
Responsibilities in scientific communities (GDR etc.)	1
Organizations of Conferences (national/international)	2/1
Invitations (national/international)	1
Stays in foreign laboratories	1

[64] Zhonggui Chen, Wenping Wang, Bruno Lévy, Ligang Liu, and Feng Sun. "Revisiting Optimal Delaunay Triangulation for 3D Graded Mesh Generation". In: *SIAM Journal on Scientific Computing* (May 2015), A930–A954. hal-01101627.

❶ List of top journals in which we have published

ACM Transactions on Graphics (5) [32, 10, 16, 18, 21], Computer-Aided Design (3) [11, 12, 33], Computers and Graphics (1) [15], International Journal of Control (1) [20], IEEE Transactions on Automatic Control (1) [25].

❷ List of top conferences in which we have published

SIGGRAPH (1) [21], SIGGRAPH Asia (2) [32, 16], Symposium on Solid and Physical Modeling (2) [12, 33].

N.B. In computer graphics, there is a symbiosis between top conferences and top journals: conference papers are published in the journals, and journal papers are presented at the conferences. All above publications were already presented in the previous section.

We have also published in conferences on control theory: IFAC World Congress (3) [13, 36, 38], IFAC Symposium on Nonlinear Control Systems (NOLCOS) (1) [35].

❸ Software

We use here the self-assessement criteria provided by INRIA.

- **GRAPHITE** *Experimental 3D modeler and geometry processing software* Web site: `http://alice.loria.fr/software/graphite/doc/html/`. Self-assessment:
  - Audience: A-4 (large audience, used by people outside the team). (more than 43000 downloads on `gforge.inria.fr`)
  - Software originality: SO-4 (original software implementing a fair number of original ideas).
  - Software maturity: SM-4 (major software project, strong software engineering).
  - Evolution and maintenance: EM-4 (well-defined and implemented plans for future maintenance and evolution).
  - Software distribution and licensing: SDL-4 (public source or binary distribution on the Web). (GPL license)
- **GEOGRAM** *General-purpose 3D geometric algorithms software library* Web site: `http://alice.loria.fr/software/graphite/doc/html/`.
  - Audience: A-4 (large audience, used by people outside the team). (more than 56000 downloads on `gforge.inria.fr` since 2014 (**more than 13000 downloads per year**), used in several Open-Source and commercial products, including Houdini, Ovito, Trimble)
  - Software originality: SO-4 (original software implementing a fair number of original ideas).
  - Software maturity: SM-4 (major software project, strong software engineering).
  - Evolution and maintenance: EM-4 (well-defined and implemented plans for future maintenance and evolution).
  - Software distribution and licensing: SDL-4 (public source or binary distribution on the Web). (FreeBSD license)

- **VORPALINE** *3D mesh generation software* Web site: http://alice.loria.fr/software/graphite/doc/html/.
  - Audience: A-3 (ambitious software, usable by people outside the team). (used by our industrial contacts).
  - Software originality: SO-4 (original software implementing a fair number of original ideas).
  - Software maturity: SM-5 (high-assurance software, certified by an evaluation agency or formally verified). (we do systematic non-regression testing, memory tests and coverage analysis using Jenkins continuous integration platform)
  - Evolution and maintenance: EM-4 (well-defined and implemented plans for future maintenance and evolution).
  - Software distribution and licensing: SDL-3 (distributed to industrial partners in a contractual setting).

The academic reputation and appeal

❶ Participation in projects and External funding

- **ANR BECASIM (2013 – 2017)** 890 k€. X. Antoine heads the second partner, which includes Bruno Lévy. Budget for Nancy: 170 k€ of which 100 k€ are for IECL (team CORIDA). This project is managed by Inria. Becasim is a thematic "Numerical Models" ANR project granted by the French Agence Nationale de la Recherche for years 2013-2016. The acronym Becasim is related to Bose-Einstein Condensates: Advanced SIMulation Deterministic and Stochastic Computational Models, HPC Implementation, Simulation of Experiments. The members of the ANR Project Becasim belong to 10 different laboratories.

- **EXPLORAGRAM** Inria exploratory project EXPLORAGRAM (in cooperation with MOKAPLAN): We explored new algorithms for computational optimal transport. The project allowed us to hire a post-doc for 18 months (Erica Schwindt). She worked on the semi-discrete algorithm, and its application to the simulation of fluid-structure interactions. The project allowed to strengthen the cooperation with MOKAPLAN. It also allowed us to start exploring new cooperations, with Institut d'Astrophysique de Paris, on early universe reconstruction.

- **ANR MAGA (2016-2020)** We participated to the ANR MAGA (ANR-16-CE40-0014) on the Monge Ampere equation and computational geometry. In this ANR project, we cooperate with Quentin Merigot and other researchers of the MOKAPLAN Inria team on new computational methods for optimal transport.

- **ANR ROOT (2016-2020)** We participated to the Young Researcher ANR ROOT (ANR-16-CE23-0009) on Optimal Transport for computer graphics, with Nicolas Bonneel (CNRS Lyon) as Principal Investigator. In the context of this project, we develop a new symmetric algorithm for semi-discrete optimal transport that optimizes for both the location of the samples and their Lagrange multipliers.

❷ Editorial and organizational activities

N. Ray and D. Sokolov were PC members of the major conferences: SIGGRAPH, SIGGRAPH Asia, Eurographics, Pacific Graphics, SPM, ISVC, NUMGRID. We have co-organized FRAMES2020[65] and we have organized GTMG2020[66] and JFIG2020[67].

Involvement with social, economic and cultural environment

	2016-2020
APP (Software)	3
Contracts with companies	5
Cifre	2
Start-up	1
Radio broadcasts, TV, Newspapers	1

❶ Relations with companies and economic players

During the evaluation period, we have two CIFRE:

- Schlumberger (Julien Renaudeau)
- RhinoTerrain (Justine Basselin)

Besides these two projects, we have three more bilateral contracts with the industry:

- Polygonal Design (2018 – 2020)
- CEA (2019 - 2022)
- Total (2020 - 2024)

In May 2020, we have launched a start-up Tessael with Wan-Chiu Li as the CEO. The company provides meshing solutions based on GeO2 technology, which has been developed since 2010 by ALICE/PIXEL, a joint undertaking between Inria and Loria. Through its new GeO2 geological meshing technology, Tessael is able to perform and optimise extremely accurate 3D simulations of subsurface environments, opening up new opportunities in three sectors: geothermal energy, geological storage and the oil and gas industry. For these three key sectors, Tessael focuses on performing and optimising extremely accurate 3D simulations. GeO2 uses high quality meshes it generates, coupled with 3D visualisation technology, to make precise and accurate measurements within complex geological formations — a major breakthrough in the field of subsurface exploitation. GeO2 is also a decision-making aid for those operating in these industries, helping them minimise both environmental and financial risks while making exploration and production operations as efficient as possible.

[65] https://www.hextreme.eu/frames2020/
[66] https://gtmg2021.sciencesconf.org/
[67] https://jfig2020.sciencesconf.org/

❷ General public audience activities

Bruno Lévy appeared in a documentary on France 3[68] which talked about our project with the astrophysicists of the IAP and the Paris Observatory, and the mathematicians of MOKAPLAN.

The involvement in training through research

	2016-2020
Course books, etc	2
E-learnings, MOOC	4

❶ Involvement of the team in training through research

We have participated to the organization of a doctoral school l'EJCIM2018[69].

❷ Involvement in E-Educations

Dmitry Sokolov is an active participant of e-education actions. His series of courses on computer graphics[70][71][72][73] is widely known: 5M visitors, code used by Xamarin Workbooks (Microsoft)[74], Ogre3D[75] and Bullet[76].

❸ Courses and research schools.

We have written a course on digital geometry [77] as well as a course on least squares methods[78].

❹ Responsibilities

References

Doctoral Dissertations

[1] Arnaud Botella. "Unstructured volumetric meshing of geological models for physical phenomenon Simulations". PhD thesis. Université de Lorraine, April 2016. tel-01435058.

[2] Maxence Reberol. "Hex-dominant meshes : generation, simulation and evaluation". PhD thesis. Université de Lorraine, March 2018. tel-01771056.

[68] https://youtu.be/WNkk84_eK70
[69] https://ejcim2018.sciencesconf.org/
[70] https://github.com/ssloy/tinyrenderer/wiki
[71] https://github.com/ssloy/tinyraycaster/wiki
[72] https://github.com/ssloy/tinyraytracer/wiki
[73] https://github.com/ssloy/tinykaboom/wiki
[74] https://github.com/xamarin/Workbooks
[75] https://www.ogre3d.org/2021/02/12/ogre-1-12-11-released
[76] https://github.com/bulletphysics/bullet3
[77] https://ejcim2018.sciencesconf.org/data/pages/ejcim2018.pdf
[78] https://github.com/ssloy/least-squares-course

[3] Julien Renaudeau. “Continuous formulation of implicit structural modeling discretized with mesh reduction methods”. PhD thesis. Université de Lorraine, April 2019. tel-02331238.

[4] David Lopez. “Voronoi diagrams and evolving surfaces”. PhD thesis. Université de Lorraine, October 2021. tel-03530955.

Habilitation Theses

[5] Dmitry Sokolov. “Modelisation geometrique”. Habilitation à diriger des recherches. Université de Lorraine (UL), Vandoeuvre-lès-Nancy, FRA., June 2016. tel-03180395.

[6] Jeanne Pellerin. “Mesh Generation”. Habilitation à diriger des recherches. Université de Lorraine, June 2021. tel-03249549.

Articles in International Peer-Reviewed Journal

[7] Pauline P. Collon, Alexandre Pichat, Charlie Kergaravat, Arnaud Botella, Guillaume Caumon, Jean-Claude Ringenbach, and Jean-Paul Callot. “3D modelling from outcrop data in a salt tectonic context: Example from the Inceyol mini-basin, Sivas Basin, Turkey”. In: *Interpretation* 4.3 (August 2016), SM17–SM31. DOI: 10.1190/INT-2015-0178.1. hal-01342928.

[8] Joris Galland, Shirine Mohamed, Sabine Revuz, Emmanuel De Maistre, Bas de Laat, Pierre-Yves Marie, Stéphane Zuily, Bruno Lévy, Véronique Regnault, and Denis Wahl. “Lupus anticoagulant-hypoprothrombinemia syndrome and catastrophic antiphospholipid syndrome in a patient with antidomain I antibodies”. In: *Blood Coagulation and Fibrinolysis* 27.5 (2016), pp. 580–582. DOI: 10.1097/MBC.0000000000000545. hal-03567151.

[9] Franck Hétroy-Wheeler, Eric Casella, and Dobrina Boltcheva. “Segmentation of tree seedling point clouds into elementary units”. In: *International Journal of Remote Sensing* 37.13 (2016), pp. 2881–2907. DOI: 10.1080/01431161.2016.1190988. hal-01285419.

[10] Dmitry Sokolov, Nicolas Ray, Lionel Untereiner, and Bruno Lévy. “Hexahedral-Dominant Meshing”. In: *ACM Transactions on Graphics* 35.5 (2016), pp. 1–23. DOI: 10.1145/2930662. hal-01397846.

[11] Hai-Chuan Song, Nicolas Ray, Dmitry Sokolov, and Sylvain Lefebvre. “Anti-aliasing for fused filament deposition”. In: *Computer-Aided Design* 89 (September 2016). arXiv: 1609.03032 - 14 pages, 22 figures, pp. 25–34. DOI: 10.1016/j.cad.2017.04.001. hal-01400686.

[12] Dobrina Boltcheva and Bruno Levy. “Surface reconstruction by computing restricted Voronoi cells in parallel”. In: *Computer-Aided Design* 90 (September 2017), pp. 123–134. DOI: 10.1016/j.cad.2017.05.011. hal-01596553.

[13] Roman M Luchin, Ilya Y. Shirokolobov, Iakov A. Kirilenko, Andrey Nikolaevich Terekhov, Anastasia Stone, and Dmitry Sokolov. “Improving control engineering education with TRIK cybernetic system”. In: *IFAC-PapersOnLine* 50.1 (July 2017), pp. 15716–15721. DOI: 10.1016/j.ifacol.2017.08.2412. hal-01658734.

[14] Jeanne Pellerin, Arnaud Botella, Antoine Mazuyer, Benjamin Chauvin, François Bonneau, Guillaume Caumon, and Bruno Lévy. "RINGMesh: A programming library for developing mesh-based geomodeling applications". In: *Computers & Geosciences* (2017). DOI: 10.1016/j.cageo.2017.03.005. hal-01493204.

[15] Bruno Lévy and Erica Schwindt. "Notions of optimal transport theory and how to implement them on a computer". In: *Computers and Graphics* (February 2018), pp. 1–22. DOI: 10.1016/j.cag.2018.01.009. hal-01717967.

[16] Nicolas Ray, Dmitry Sokolov, Sylvain Lefebvre, and Bruno Lévy. "Meshless Voronoi on the GPU". In: *ACM Transactions on Graphics* 37.6 (December 2018), pp. 1–12. DOI: 10.1145/3272127.3275092. hal-01927559.

[17] Igor Ryadchikov, Semyon Sechenev, Michail Drobotenko, Alexander Svidlov, Pavel Volkodav, Renat Vishnykov, Dmitry Sokolov, and Evgeny Nikulchev. "Stabilization system of a bipedal non-anthropomorphic robot AnyWalker". In: *Journal of Engineering Science and Technology Review* (August 2018). DOI: 10.25103/jestr.115.15. hal-01927623.

[18] Zichun Zhong, Wenping Wang, Bruno Lévy, Jing Hua, and Xiaohu Guo. "Computing a high-dimensional euclidean embedding from an arbitrary smooth riemannian metric". In: *ACM Transactions on Graphics* 37.4 (August 2018), pp. 1–16. DOI: 10.1145/3197517.3201369. hal-03214192.

[19] Stanislav Aranovskiy, Andrei Biryuk, Evgeny V. Nikulchev, Igor Ryadchikov, and Dmitry Sokolov. "Observer Design for an Inverted Pendulum with Biased Position Sensors". In: *Izvestia Rossiiskoi Akademii Nauk.Teoriya i Systemy Upravleniya / Journal of Computer and Systems Sciences International* 58.2 (March 2019), pp. 297–304. DOI: 10.1134/S1064230719020023. hal-02282919.

[20] Stanislav Aranovskiy, Romeo Ortega, Jose Guadalupe Romero, and Dmitry Sokolov. "A Globally Exponentially Stable Speed Observer for a Class of Mechanical Systems: Experimental and Simulation Comparison with High-Gain and Sliding Mode Designs". In: *International Journal of Control* 92.7 (July 2019), pp. 1620–1633. DOI: 10.1080/00207179.2017.1404130. hal-01658753.

[21] Jimmy Etienne, Nicolas Ray, Daniele Panozzo, Samuel Hornus, Charlie C.L. Wang, Jonàs Martínez, Sara Mcmains, Marc Alexa, Brian Wyvill, and Sylvain Lefebvre. "CurviSlicer: Slightly curved slicing for 3-axis printers". In: *ACM Transactions on Graphics* 38.4 (August 2019), pp. 1–11. DOI: 10.1145/3306346.3323022. hal-02120033.

[22] Stanislav Aranovskiy, Igor Ryadchikov, Evgeny Nikulchev, Jian Wang, and Dmitry Sokolov. "Bias Propagation and Estimation in Homogeneous Differentiators for a Class of Mechanical Systems". In: *IEEE Access* 8 (2020), pp. 19450–19459. DOI: 10.1109/ACCESS.2020.2968219. hal-02516559.

[23] Stanislav Aranovskiy, Igor Ryadchikov, Evgeny Nikulchev, Jian Wang, and Dmitry Sokolov. "Experimental Comparison of Velocity Observers: A Scissored Pair Control Moment Gyroscope Case Study". In: *IEEE Access* 8 (2020), pp. 21694–21702. DOI: 10.1109/ACCESS.2020.2968221. hal-02516558.

[24] Dobrina Boltcheva, Justine Basselin, Clément Poull, Herve Barthelemy, and Dmitry Sokolov. "Topological-based roof modeling from 3D point clouds". In: *Journal of WSCG* 28.1-2 (2020), pp. 137–146. DOI: 10.24132/JWSCG.2020.28.17. hal-02983073.

[25] Jian Wang, Stanislav Aranovskiy, Emilia Fridman, Dmitry Sokolov, Denis Efimov, and Alexey Bobtsov. “Robust adaptive stabilization by delay under state parametric uncertainty and measurement bias”. In: *IEEE Transactions on Automatic Control* (2020). DOI: 10.1109/TAC.2020.3045125. hal-03059893.

[26] Stanislav Aranovskiy, Denis Efimov, Dmitry Sokolov, Jian Wang, Igor Ryadchikov, and Alexey Bobtsov. “Switched Observer Design For a Class of Locally Unobservable Time-Varying Systems”. In: *Automatica* 130 (August 2021), p. 109715. DOI: 10.1016/j.automatica.2021.109715. hal-03273675.

[27] Guillaume Coiffier, Justine Basselin, Nicolas Ray, and Dmitry Sokolov. “Parametric Surface Fitting on Airborne Lidar Point Clouds for Building Reconstruction”. In: *Computer-Aided Design* 140 (July 2021), p. 103090. DOI: 10.1016/j.cad.2021.103090. hal-03281816.

[28] David Desobry, Yoann Coudert-Osmont, Etienne Corman, Nicolas Ray, and Dmitry Sokolov. “Designing 2D and 3D Non-Orthogonal Frame Fields”. In: *Computer-Aided Design* 139 (July 2021), pp. 1–9. DOI: 10.1016/j.cad.2021.103081. hal-03287233.

[29] Vladimir Garanzha, Igor Kaporin, Liudmila Kudryavtseva, François Protais, Nicolas Ray, and Dmitry Sokolov. “Foldover-free maps in 50 lines of code”. In: *ACM Transactions on Graphics* 40.4 (July 2021). arXiv: 2102.03069, Article No.102, pp 1–16. DOI: 10.1145/3450626.3459847. hal-03127350.

[30] Bruno Lévy, Roya Mohayaee, and Sebastian von Hausegger. “A fast semidiscrete optimal transport algorithm for a unique reconstruction of the early Universe”. In: *Monthly Notices of the Royal Astronomical Society* 506.1 (June 2021). arXiv: 2012.09074, pp. 1165–1185. DOI: 10.1093/mnras/stab1676. hal-03115841.

[31] Nathan J. Secrest, Sebastian von Hausegger, Mohamed Rameez, Roya Mohayaee, Subir Sarkar, and Jacques Colin. “A Test of the Cosmological Principle with Quasars”. In: *The Astrophysical journal letters* 908.2 (2021). arXiv: 2009.14826, p. L51. DOI: 10.3847/2041-8213/abdd40. hal-03022647.

Major International Conferences

[32] Nicolas Ray, Dmitry Sokolov, and Bruno Lévy. “Practical 3D frame field generation”. In: *SIGGRAPH ASIA 2016*. Vol. 35. macao, Macau SAR China, December 2016, pp. 1–9. hal-01397711.

[33] Nicolas Ray, Dmitry Sokolov, Maxence Reberol, Franck Ledoux, and Bruno Lévy. “Hex-dominant meshing: mind the gap!” In: *SPM 2018 - International Conference on Solid and Physical Modeling*. Bilbao, Spain, June 2018. hal-01927557.

[34] Igor Ryadchikov, Dmitry Sokolov, Andrei Biryuk, Semyon Sechenev, Alexander Svidlov, Pavel Volkodav, Yury Mamelin, Kirill Popko, and Evgeny Nikulchev. “Stabilization of a hopper with three reaction wheels”. In: *ISR 2018 - 50th International Symposium on Robotics*. Munich, Germany, June 2018. hal-01927624.

[35] Igor Ryadchikov, Stanislav Aranovskiy, Evgeny Nikulchev, Jian Wang, and Dmitry Sokolov. “Differentiator-based velocity observer with sensor bias estimation: an inverted pendulum case study”. In: *11th IFAC Symposium on Nonlinear Control Systems*. Vienna, Austria, September 2019. hal-02383471.

[36] Stanislav Aranovskiy, Denis Efimov, Dmitry Sokolov, Jian Wang, Igor Ryadchikov, and Alexey Bobtsov. "State estimation for a locally unobservable parameter-varying system: one gradient-based and one switched solutions". In: *IFAC 2020 - 21rst IFAC World Congress*. Berlin, Germany, July 2020. hal-02634576.

[37] Victor Blanchi, Etienne Corman, Nicolas Ray, and Dmitry Sokolov. "Global parametrization based on Ginzburg-Landau functional". In: *NUMGRID 2020 - Numerical Geometry, Grid Generation and Scientific Computing*. Moscow/Virtual, Russia, November 2020. hal-02985282.

[38] Denis Efimov, Stanislav Aranovskiy, Emilia Fridman, Dmitry Sokolov, Jian Wang, and Alexey Bobtsov. "Adaptive stabilization by delay with biased measurements". In: *IFAC 2020 - 21st IFAC World Congress*. Berlin, Germany, July 2020. hal-02634582.

[39] Dmitry Sokolov, Stanislav Aranovskiy, Alexander A Gusev, and Igor Ryadchikov. "Experimental comparison of velocity estimators for a control moment gyroscope inverted pendulum". In: *AMC 2020 - 16th IEEE International Workshop on Advanced Motion Control*. Kristiansand / Virtual, Norway, September 2020. hal-02313600.

Secondary International Conferences

[40] Stanislav Aranovskiy, Igor Ryadchikov, Nikita Mikhalkov, Dmitry Kazakov, Alexey Simulin, and Dmitry Sokolov. "Scissored pair control moment gyroscope inverted pendulum". In: *14th International Symposium "Intelligent Systems - 2020"*. Moscow, Russia, December 2020. hal-02985412.

[41] Andrey Getmanskiy, Semen Sechenev, Igor Ryadchikov, Alexander Gusev, Nikita Mikhalkov, Dmitry Kazakov, Alexey Simulin, and Dmitry Sokolov. "Real-time system architecture design practices". In: *14th International Symposium "Intelligent Systems - 2020"*. Moscow, Russia, December 2020. hal-02984042.

[42] Vladimir Garanzha, Igor Kaporin, Liudmila Kudryavtseva, François Protais, Nicolas Ray, and Dmitry Sokolov. "On Local Invertibility and Quality of Free-boundary Deformations". In: *IMR 2021 - 29th International Meshing Roundtable*. Proceedings of the 29th International Meshing Roundtable. Virtual, United States, June 2021. hal-03341392.

[43] Wan-Chiu Li, Cédric Borgese, Alexandre Benedicto, Nicolas Ray, and Dmitry Sokolov. "Singular Structured Hexahedral Grid". In: *RING Meeting 2021*. 2021 RING Meeting Papers. Vandoeuvre-lès-Nancy, France, September 2021. hal-03375671.

[44] Nikita Mikhalkov, Alexey Prutskiy, Semyon Sechenev, Dmitry Kazakov, Alexey Simulin, Dmitry Sokolov, and Igor Ryadchikov. "Gyrubot: nonanthropomorphic stabilization for a biped". In: *ICRA 2021 - IEEE International Conference on Robotics and Automation*. 2021 IEEE International Conference on Robotics and Automation (ICRA). Xi'an / Virtual, China, May 2021. hal-03172031.

Book (written)

[45] Christian Gentil, Gilles Gouaty, and Dmitry Sokolov. *Modélisation géométrique de formes fractales pour la CAO*. ISTE Editions, January 2020. hal-02462416.

Books or Proceedings Editing

Book Chapters

[46] Igor Ryadchikov, Semyon Sechenev, Nikita Mikhalkov, Andrey Biryuk, Alexander Svidlov, Aleksandr Gusev, Dmitry Sokolov, and Evgeny Nikulchev. "Feedback Control with Equilibrium Revision for CMG-Actuated Inverted Pendulum". In: *Proceedings of 14th International Conference on Electromechanics and Robotics "Zavalishin's Readings"*. August 2020, pp. 431–440. DOI: 10.1007/978-981-13-9267-2_35. hal-02282908.

Other Publication

[47] Dobrina Boltcheva and Bruno Lévy. *Simple and Scalable Surface Reconstruction*. Research Report. LORIA - Université de Lorraine ; INRIA Nancy, July 2016. hal-01349023.

[48] Nicolas Ray and Dmitry Sokolov. "On Smooth Frame Field Design". working paper or preprint. January 2016. DOI: 10.1145/1559755.1559763. hal-01245657.

[49] Maxence Reberol and Bruno Lévy. *Low-order continuous finite element spaces on hybrid non-conforming hexahedral-tetrahedral meshes*. Research Report. arXiv: 1605.02626. INRIA Nancy, équipe ALICE, May 2016. hal-01313285.

[50] Nicolas Ray, Dmitry Sokolov, Maxence Reberol, Franck Ledoux, and Bruno Lévy. "Hexahedral Meshing: Mind the Gap!" working paper or preprint. June 2017. hal-01551603.

[51] Maxence Reberol and Bruno Lévy. "Computing the distance between two finite element solutions defined on different 3D meshes on a GPU". working paper or preprint. August 2017. hal-01634176.

[52] Dobrina Boltcheva, Chouaib Fellah, Damien Liehn, and Clément Poull. *Modélisation de toitures à partir de nuages de points 3D*. Research Report. LORIA–INRIA Grand Est ; Université de Lorraine (Nancy), December 2019. hal-02409136.

[53] François Protais, Maxence Reberol, Nicolas Ray, Etienne Corman, Franck Ledoux, and Dmitry Sokolov. "Robust Quantization for Polycube Maps". working paper or preprint. December 2020. hal-03076711.

[54] Nicolas Donati, Etienne Corman, Simone Melzi, and Maks Ovsjanikov. "Complex Functional Maps : a Conformal Link Between Tangent Bundles". arXiv: 2112.09546 - working paper or preprint. December 2021. hal-03480605.

[55] Dmitry Sokolov, Nicolas Ray, and Etienne Corman. "Least squares for programmers". Doctoral. Lecture. SIGGRAPH2021, Los Angeles, United States, August 2021. DOI: 10.1145/3450508.3464554. hal-03321301.

Visual Registration with Physically Coherent Models

Synopsis

1 Team Composition

Permanents

Marie-Odile Berger (DR Inria), Erwan Kerrien (CR Inria), Fabien Pierre (Assistant Professor, arrived 1/09/2017), Gilles Simon (Assistant Professor), Frédéric Sur (Professor), Pierre-Frédéric Villard (Assistant Professor), Brigitte Wobel-Dautcourt (Assistant Professor).

	2016	2017	2018	2019	2020	Total
PR			1	1	1	1
MCF	4	5	4	4	4	4
DR	1	1	1	1	1	1
CR	1	1	1	1	1	1
Other						
Total (permanent positions)	6	7	7	7	7	7
Pr emeritus						
Guest researchers						
Post-doct. researchers	1	1				1
PhD Students	6	6	7	7	7	13
Master students M2	1	2	2	3	3	10
Master Students M1				1	1	2
L3 students						
Engineers	1			1	3	4
Other						
Total (temporary positions)						

Post-doctoral fellows

Cong Yang (2016-2017),

Engineers

Pierre-Jean Petitprez (2014-2016), Thomas Mangin (2019-2020), Vincent Gaudillière (2020), Romain Boisseau (2020-2023).

Change in team composition

Fabien Pierre joined the team in september 2017 as an assistant professor.

Doctoral students

Charlotte Delmas (CIFRE GE-Healthcare, 2013-2017), Pierre Rolin (MENRT, 2013-2017), Antoine Fond (MENRT, 2014-2018), Jaime-Garcia Guevara (Région, 2015-2019), Rafffaela Trivisonne (INRIA, 2015-2020), Vincent Gaudillère (INRIA-DGA, 2016-2020), Daryna Panicheva (MENRT, 2017-2021), Matthieu Zins (INRIA, 2019–), Youssef Assis (MENRT, 2020–), Karim Elassam (INRIA-DFKI, 2020–), Nariman Khaledian (INRIA, 2020–)

Two PhD students outside UL were also supervised by members of the team: Arthur Renaudeau (Univ. Toulouse) was co-supervised by Fabien Pierre (Advisor: J.-D Durou, PhD defended in 2020), Igor Tominec is co-supervised by P.-F. Villard (Advisor: Elisabeth Larsson). This explains the (+1) in the table.

	2016-2020
Phd's defended	6 (+1)
On-going PhD's	5 (+1)
Average nb of papers by PhD student	3.4
Average duration of PhD thesis (in month)	45.9 (median:42)

Note: two PhD thesis had an unsual long duration, while the median is 42 months. Only international conferences or journals are considered in the number of papers.

Charlotte Delmas is an engineer at GE-Helthcare, Antoine Fond is a researcher in the start up Synthesia (London), Pierre Rolin is a postdoctoral student at CEA, Vincent Gaudillière is a posdoctoral student at Luxembourg university, Raffaela Trivisonne is Translational Research Project Manager (Inserm Institute of Viral and Liver Diseases, University of Strasbourg), Jaime Garcia Guevara is a software developer in image processing.

2 Research topics

Keywords

Image processing and analysis, computer vision, object recognition, localization, virtual and augmented reality, physics.

Research area and main goals

The evaluation period has seen the end of the Magrit team in 2019 and the creation of the Tangram team in 2020. The goal of Magrit was to develop vision-based methods which allow significant progress of *Augmented Reality* (AR) technologies. Important goals of the teams were thus the design of robust solutions for matching, 3D tracking, as well as means to produce automatically or interactively 3D scene model. With the recent mediatic explosion of activities around AR, the term *augmented reality* now goes far beyond its traditional definition, which focused on precise 3D tracking. We therefore moved from purely AR topics towards fundamental computer vision issues raised by accurate registration tasks. Physically coherent modeling, accurate registration and associated estimation techniques are thus the main focus of the Tangram team.

Targeted applications are mixed reality, interventional radiology and computational photomechanics. These fields correspond to areas where we have established trans-disciplinary collaborations with academic or industrial experts of the applicative fields.

3 Main Achievements

- The integration of semantic maps and the use of objects as landmarks for pose algorithms.
- The transdiciplinary collaboration on experimental mechanics for contactless measurement with both theoretical contributions in image processing, publications in mechanics journals and release of software.
- The use of biomechanical models as means to incorporate shape and deformation constraints to improve matching and reconstruction.

4 Research activities

Localization

Description The challenge of image-based localization is to compute pose estimates with a good accuracy whatever the user's motion and the nature of the scene.

Image-based solutions are prone to be robust and accurate but usually fail when an image is acquired in very different conditions from those experienced during the modeling stage or when the scene is poorly textured. With the aim to increase the robustness of pose computation, we have addressed various aspects of these issues, both with conventional point-based features and more recently from higher level features extracted with convolutional networks. Using objects as markers for pose computation has been an important topic of the evaluation period.

Main results

Pose computation is challenging when the camera is far from the views used to build the model. Several viewpoint simulation techniques have been proposed but they generally come with a high computational cost and are limited to specific scenes. In his PhD thesis [2], P. Rolin has proposed an accurate viewpoint simulation method, with a limited computational cost, suited to most scenes with two major contributions: the positioning of the virtual viewpoints with respect to the scene, and the synthesis of geometrically consistent patches [51, 28].

Within V. Gaudilliere's PhD thesis [79, 59, 5], we took advantage of global properties of the environment, both geometric - such as the presence of numerous vertical planes - and contextual - ConvNet descriptors of subregions- to guide matching. This enables us to circumvent problems encountered in poorly-textured images while taking advantage of the abundance of segments and vanishing points characteristic of industrial environments.

We then developed several strategies with the idea to better take advantage of the impressive progress made by object recognition techniques, and especially of their good invariance to illumination and viewpoint changes. In the context of urban augmented reality, we have proposed to perform registration with a reference facade model thanks to a semantic map where windows, doors, balconies... are extracted. As the semantic map can be noisy, registration and semantic segmentation were jointly refined in an Expectation-Maximization framework. We especially introduced a Bayesian model that uses prior semantic segmentation as well as geometric structure of the facade reference modeled by Generalized Gaussian Mixtures. This approach turned out to be robust to clutter and change of illumination [78, 54, 3, 40].

With the emergence of efficient object detectors, object-based reasoning now appears as a new and powerful way to solve traditional computer vision problems. In particular, some methods have shown that modelling 3D objects by ellipsoids and 2D detections by ellipses offers a convenient manner to link 2D and 3D data. Compared to learning-based pose computation methods that require a detailed model of object and need retraining for considering new scenes, considering objects as markers allow to take advantage of generic object detectors without having to retrain the system for considering new scenes. During the last two years, we have investigated the problem of pose computation from ellipse-ellipsoid correspondences with theoretical and methodological contributions. A patent was also filed on this work [95]. In [65], we have proved that a closed form estimate of the translation can be uniquely inferred from the the rotation matrix of the pose. In the general case, there is an infinity of camera solutions, described in [5], which can be inferred from one correspondence. In [66], we have considered the common case where an initial guess of the rotation is known, for instance with an inertial sensor, and shown the effectiveness of the method on real scenes.

We have then proposed in [34] a full 6D pose method which operates from at least two object detections and reduces the DoF to only one, thanks to two simplifying yet realistic assumptions. These approaches use the ellipses fitted to the detection bounding boxes as an approximation of the imaged objects. This may originate in possible large inaccuracies in the computed pose. Within the framework of Matthieu Zins's PhD Thesis, we have proposed a learning-based method which detects improved elliptic approximations of objects which are coherent with the 3D ellipsoid in terms of perspective projection [73].

Modeling and tracking curved and deformable objects

Description Registration, segmentation, and reconstruction are inherently ill-posed and require the addition of regularizing priors to reduce the solution set. Geometric constraints are adapted to man made environments. But they do not comply with medical images that often depict strongly deforming organs, whose shape may be very complex. In that context, the start of the evaluation period saw us consolidate our previous work on the use of implicit functions to model the deformation of the diaphragm [64, 86] and blood vessels [20] in 3D, as well as software tools for interactive visualization purpose [50, 18, 56]. But a particular focus of our research was put on biomechanical models as means to incorporate shape and deformation constraints to improve: registration applied to minimally invasive liver surgery, segmentation of mitral valve chordae in Computerized Tomography (CT) images, and 3D reconstruction of the catheter from 2D X-ray images in interventional radiology. All these projects were grounded on strong collaborations with partners in clinical research and biomechanical simulation (CHRU Nancy, IHU Strasbourg, Mimesis Inria team and the Biorobotics lab in Harvard).

Main results

Elastic multi modal non-rigid registration: Within Jaime Guevara's PhD thesis [4], we have continued to investigate non rigid registration methods which exploit the matching of the vascular trees and are able to cope with large deformations of the organ [58]. We have especially developed a compliance-based non rigid registration matching method which is entirely based on the mechanical properties of the organ [33]. We thus avoid tedious parameter tuning which is required by many methods and instead use parameters whose values are known or can be measured. This method reduces the computation time by predicting first the most plausible matching hypotheses on a mechanical basis.

Modeling the mitral valve Common surgical procedures on the mitral valve of the heart include modifications to the chordae tendineae, in order to prevent extensive leaflet prolapse or leaks caused by chordae rupture. The outcome however varies depending on the experience of the surgeon. We thus aim at developing patient-based methods to predict mitral valve behavior from a biomechanical model and geometries extracted from segmentation methods with minor human interactions. In [25], we developed a first framework including image acquisition, an interactive valve structure extraction and a fast FEM simulation of the valve closure. In the context of D. Panicheva's PhD thesis, topology-based methods which enable an automatic extraction of the chordaed have been proposed [68]. Finally, in [69, 41] a model-fitting approach was used in order to represent the extracted chordae in a form suitable for the mechanical model. Simulations correctly predict the valve behavior in the case of healthy valve with all the chordae and pathological valve with chordae deletion. These results are to the best of our knowledge the only ones directly obtained from patient data.

Interventional radiology requires that the medical practitioner navigates thread-like devices inside the patient's vasculature. The visual feedback offered by 2D live X-ray images does not always allow for a clear depiction of the vessel pathway and device shape. An online intra-operative reconstruction of the device in 3D, that would be visualized within 3D images of the blood vessels and surrounding anatomy, would therefore be highly beneficial to the medical practitioner. In the context of C. Delmas's PhD thesis [1], we tested the limit of two-view reconstruction algorithms and of sparse iterative tomographic reconstruction algorithms for coils reconstruction [47].

The challenging single view case was addressed during R. Trivisonne's PhD thesis [6]. We experimented with visual landmarks placed on the device to define geometric constraints for the biomechanical simulation [57]. Then, to further improve accuracy and make the reconstruction more robust, we devised an image-driven simulation framework based on Bayesian filtering where the model is instanciated through simulation steps and image observations are provided by landmarks [37]. The challenge consisted in managing multiple contacts between the blood vessel and the device, which account for non-linearities and even discontinuities in the dynamics. Our contribution is an Unscented Kalman Filter with a sigma-point generation process that incorporates contact management.

Image analysis

Description Camera pose estimation, scene reconstruction or modeling tasks often require signal or image processing techniques in order to extract cues specific to the targeted applications. Signal analysis and, more specifically, image analysis represent therefore the keystone of many of the team's work. First, a problem of direct interest for pose estimation or reconstruction is the detection of low-level features to rely on. The accurate detection of vanishing points and horizon lines has been developed for this purpose. Another contribution to the characterization of low-level features concerns texture detection. Tangram team also contributes to the study of variational methods, one of the most successful paradigms of image processing. Both theoretical aspects with mathematical proofs of the convergence of numerical algorithms and applications such as image colorization are addressed. Finally, we are engaged in a trandisciplinary collaboration with Institut Pascal about contactless measurement techniques in experimental mechanics.

Main results

Vanishing points are low-level primitives useful for guiding feature matching [59] for plane rectification [54] or camera orientation estimation [66]. However, they are tricky to identify as meeting points of line segments, because of the many spurious crossings that one gets when a large number of segments are detected. We were able to break this deadlock by noticing that the horizon line is often physically detectable in an image, i.e. independently of the vanishing points [62]. The search for horizontal vanishing points can be restricted to this line, which greatly limits ambiguities. The detection of the horizon line as well as the vanishing points along the horizon line relies on the *a contrario* methodology which, by finely characterizing the background noise of the expected events, allows to reach high performances in terms of accuracy, in addition to the robustness obtained thanks to the horizon-first strategy. In the continuity of this work, a paper at the confluence of art and computer vision was published at SIGGRAPH 2021 [44]. It elucitated how the Flemish painter Jan Van Eyck (1390-1441) used an advanced perspective machine with two degrees of freedom to represent space as closely as possible to human vision.

Decomposing an image as the sum of geometric and textural components is one of the fundamental problems of image analysis. We have developed a new approach [29] based on the non-local estimation of the spectrum of a stationary textures[79].

Variational methods The modeling of the noise is a challenging task in image processing. We have proposed new statistic estimation of the pepper-salt noise with efficient estimators based on optimization techniques [23]. The Myriad estimator uses a Cauchy random variable to model the noise and is used for local and non-local denoising. The particularity of this work is the convergence of the numerical scheme to a local minimum with probability 1, which is, up to our best knowledge, a novelty in the optimization community.

For some variational problem in imaging, the minimization algorithms have to be designed for non-convex problems. We have proposed some convergence proofs of alternating gradient descent algorithms for this kind of functional [30].

In the context of movies restauration and in collaboration with IRIT, we have proposed some approaches dedicated to the detection of defects in video sequences with deep learning methods [72] and their removal with variational techniques of inpainting [70, 81]. Ways to join CNN and variational method have been investigated for fully-automatic image colorization [67]. Exemplar-based colorization of faces has also been proposed with a variational approach in [61].

In experimental solid mechanics, a very important problem is to characterize properties of specimen subjected to mechanical constraints. This often makes it necessary to measure fields of tiny strains on the surface of a deformed specimen [21], by comparing images taken before and after deformation. The general aim of our contribution is to develop new measurement techniques and to establish predictive formulas for the metrological performance, limited in particular by the noise of the digital sensor and the estimation technique employed. Small deformations and metrological performance assessment make the originality of our work and its difficulty compared to classic problems in image analysis. We have contributions to the two measurement techniques routinely used in experimental mechanics. First, the most popular approach consists in estimating displacement fields on the surface of the deformed specimen by digital image correlation (DIC). In this technique, surfaces are prepared beforehand to show a contrasted fine pattern, generally made of black ink droplets. We have proposed new estimators for the measurement resolution of DIC, taking account of subpixel interpolation scheme [12, 13], Bayer demosaicing for low-cost cameras [46], or speckle pattern [93]. We have also designed a synthetic speckle image generator [24, 63], which is of uttermost importance to assess the

[79]Software code available at: `https://members.loria.fr/FSur/software/NoLoDuDoCT/`

metrological performance of DIC[80]. Second, we have also investigated the so-called grid method, in which a regular grid is transferred on the surface of the specimen, whose images are processed through windowed Fourier transform. We have discussed the effect of intrinsic parameters of the estimation process, such as the analysis window [17], or extrinsic parameters such as spectral aliasing caused by bad sampling conditions [14, 16]. We have also written a comprehensive analysis of the grid method [15] which has been awarded the 2016 Fylde prize for the best paper in the Strain journal[81]. Finally, DIC and Fourier-based methods were confronted in a principled analysis [19, 31, 43] and enhanced via image restoration techniques [26]. A variant of grids, namely checkerboard patterns [27], turned out to give the best compromise between metrological indicators [60, 35, 36]. A patent was filed [96]. Recent developments of our activity in experimental mechanics are focused on the use of deep convolutional networks for estimating displacement fields on the surface of deformed materials [82]

[80]Software code is available at https://members.loria.fr/FSur/software/BSpeckleRender/ and datasets are included in the international DIC challenge https://sem.org/dicchallenge

[81]A reference software implementation is distributed in a companion website: www.thegridmethod.net

[82]Boukhtache et al., When Deep Learning Meets Digital Image Correlation, Optics and Lasers in Engineering,(136), 2021

Scientific production and quality

	2016-2020
PhD Thesis	7
H.D.R	3
Journals	35
Major conferences	30
Other conferences	10
Book chapters	2
Books (written)	0 0
Special issues (edited)	0
Other productions from workshops	0
General audience papers	3
Participation in editorial committees	0
Evaluation of labs and research structures	1
European projects (as project manager/Member)	0
Other international projects (as project manager/Member)	0/2
ANR, PHRC, FUI, INCA, etc. (as project manager/Member)	1/3
Projects with Region Grand Est, etc (as project manager/Member)	0/1
PIA (as project manager/Member)	0
Others (as project manager/Member)	0/1
Prizes and distinctions	1
IUF	0
Responsibilities in scientific communities (GDR etc.)	1
Organizations of Conferences (national/international)	1/1
Invitations (national/international)	0/4
Stays in foreign laboratories	8

❶ List of top journals in which we have published

Medical Image Analysis [20], Annals of Biomedical Engineering [33], International Journal of Computer Assisted Radiology and Surgery[41], Experimental Mechanics [13, 14, 19], IEEE Robotics and Automation Letters [34], Journal of Mathematical Imaging and Vision [17, 23, 24], Computer Vision and Image Understanding [40], Optics and Lasers in Engineering [39].

❷ List of top conferences in which we have published

SIGGRAPH [44], European Conference on Computer Vision [62], International Symposyum on Mixed and Augmented Reality [49, 50, 54, 66], British Machine Vision Conference [51], IEEE/RSJ International Conference on Intelligent Robots and Systems [65, 71], International Conference on Information Processing in Computer-Assisted Interventions [58], International Conference on 3D vision(3DV) [73], Scale Space and Variational Methods in Computer Vision [67, 70].

3 Software

List of software packages available under free licences:

- PoLAR: (URL: https://polar.inria.fr)
  PoLAR (Portable Library for Augmented Reality) is a framework which aims to help creating graphical applications for augmented reality and medical imaging.

- >V< (URL: https://members.loria.fr/GSimon/v/) >V< is a fast and effective tool to detect vanishing points in uncalibrated images of urban or indoor scenes. It is the Matlab implementation of the algorithm published at ECCV 2018 [62].

- NoLoDuDoCT (URL: https://members.loria.fr/FSur/software/NoLoDuDoCT/) is an algorithm decomposing images into cartoon and texture components [29].

- BSpeckleRender: A Boolean model for deformed speckle rendering (URL: https://members.loria.fr/FSur/software/BSpeckleRender/)
  This library implements a new method for synthesizing speckle images deformed by an arbitrary deformation field set by the user.

- TheGridMethod (URL: URL:http://www.thegridmethod.net/)
  The grid method toolbox implements several efficient and state-of-the art algorithms to estimate displacement and strain fields from grid images deposited on the surface of a specimen submitted to mechanical testing. It is released since 2016 in collaboration with Institut Pascal (Clermond-Ferrand) and is dedicated both to researchers and practitioners of experimental mechanics community.

The library EllCV offers a number of functionalities for pose computation from ellipse (2D) - ellipsoid (3D) correspondences [66, 34]. A patent is attached to this work. It is distributed in a contractual setting.

The academic reputation and appeal

1 Participation in projects and External funding

EU contracts as partner.

- the MOVEON project (2020-2023) is a collaboration with DFKI Kaiserslautern. Its aim is to merge novel machine-learning approaches with geometrical reasoning for new localization methods.

- INVIVE project: Biomechanical simulation of the respiratory muscles http://www.it.uu.se/research/scientific_computing/project/rbf/biomech

National contracts as project leader.
ANR PRC PreSPIN (2021-2024): This project aims at improving the planning phase in the therapeutic management of cerebral ischemic strokes thanks to predictive simulation of both the therapeutic interventional gesture and post-interventional images.

National contracts as partner

- ANR JCJC ICaRes (2019-2022): The goal of the ICaRes project is to improve the performance of residual stress estimatioon through virtual digital image correation.
- RAPID EVORA (2016-2020) The objective is to develop a prototype for location and object recognition in large-scale industrial environments (factories, ships…), with the aim to enrich the operator's field of view with digital information and media.
- the TIMEX Project (2014-2017) aimed at investigating image processing tools for enhancing the metrological performances of contactless measurement systems in experimental mechanics

Contracts with "collectivités territoriales" as partner.
IRMGE project: (2018-2022): The project Imagerie et Robotique Médicale Grand Est (IRMGE) is supported the Région Grand Est region. The team is involved in the image processing axis.

Other contracts

- Bilateral contract with GE Healthcare (2013-2017): we have a long term collaboration with GE Healthcare about interventional neuroradiology. This contract was the support of Charlotte Delmas's PhD thesis with the aim to perform 3D reconstruction of tools in interventional neuroradiology.

2 Prizes and Distinctions

- The paper entitled "The grid method for in-plane displacement and strain measurement: a review and analysis" [15] has been awarded with the Fylde Best Paper in Strain Prize 2016 by the British Society for Strain Measurement (BSSM).
- Marie-Odile Berger was a key-note speaker at ISMAR 2017

3 Editorial and organizational activities

Conference organization

- Fabien Pierre co-organized an ICPR satellite Workshop on Reproducible Research in Pattern Recognition (RRPR 2018, Beijing, China).
- Marie-Odile Berger co-organized a one-day worshop on Augmented Reality in 2017.

4 Services as expert or evaluator

- HCERES: M.-O Berger was a member of the HCERES visiting commitee of LTSI in 2016
- CNU: Gilles Simon is a member of CNU 27
- PHD committes:
  Members of the teams were reviewers of 11 PhD thesis, examiner of 14 PhD thesis, reviewer or examiner of 4 HdR.

- Scientific expertise
  - Marie-Odile Berger is the president of the Association française pour la reconnaissance et l'interprétation des formes (AFRIF).
  - In 2016, Marie-Odile Berger was the president of the AFRIF thesis prize and member of the GDR Robotique thesis prize
  - members of the teams were reviewers for 1 ANR, 5 CIFRE grants, 1 Isite call for projects
- Research administration
  - Marie-Odile Berger was a member of the Inria evaluation committee (2014-2018)
  - members of the team took part to 6 hiring committees for assistant professor or professor positions
  - Gilles Simon is "chargé de mission" on the subject of *Industry of future* at Université de Lorraine for computer sciences.

5 Collaborations

- The Inria CURATIVE Associate Team (2017-2022, URL: `https://team.inria.fr/curative/`) is a joint collaboration between Inria Magrit/Tangram team and the Harvard Biorobotics Lab. It investigates solutions to develop methods to produce patient-based simulation of a closing mitral valve on pathological cases.[68, 69].
- Within our collaboration with Université Auvergne, we bring a solid foundation to methods that are used as off-the-shelf tools in the experimental mechanics community, and tackle problems that give rise to both theoretical contributions in image processing as well as contributions in experimental mechanics and software.
- We have built strong collaborations with the University Hospital of Nancy, GE Healthcare, and MIMESIS Inria team in the context of interventional radiology. Several PhD were co-supervised with these partners [1, 4, 6]. The PhD thesis of Y. Assis is currently co-supervided by Tangram and CHRU.
- Technische Universität Kaiserslautern: recent collaborations with Gabriele Steidl focused on the removal of Cauchy noise in natural images and led [23]. The extension of these techniques to structured data on Riemaniann variety will be considered in future works.
- A collaboration with Jean-Denis Durou (IRIT) started in 2017 about the detection of defects in video sequences with deep learning methods and their removal with variational techniques. The PhD thesis of A. Renaudeau was co-supervised by Fabien Pierre [70, 72].

6 Invitations and stays outside

Invitation Robert Howe (Biorobotics Lab, Cambridge, USA, one week), Peter Hammer (Harvard Medical School, Boston, MA, USA, 2 weeks), Douglas Perin (Harvard School of Engineering and Applied Sciences, two weeks), visited the team during the evaluation period.

Stays outside

- Pierre-Frederic Villard spent a one year and a half sabbatical years (2014-2016) in Harvard University in Cambridge (USA) working on heart valve modeling. In the context of the CURATIVE team, he also stayed 1 month in november in Harvard University in Cambridge (USA) from 2017 to 2019. D. Panicheva spent two weeks in Harvard in 2019.

- Pierre-Frédéric Villard spent one month in 2017, 2018 and 2019 at Uppsala University working on the INVIVE project.

- Fabien Pierre spent a week in the university of Kaiserslautern in the team of Gabriele Steidl in 2019 to work on color modeling with kärcher mean.

Invited talks
The list of talks given by the team is listed in the appendix.

Involvement with social, economic and cultural environment

	2016-2020
Software	6
APP (Software)	
Patents (Brevet)	2
Contracts with companies	2
Cifre	1
Contracts, Consortium	9
Start-up	
Expertizes	see text
Radio broadcasts, TV, Newspapers	
Scientific mediation : articles, interviews, videos, etc.	see text

1 Relations with companies and economic players

Patents

- *Method for measuring fields of movements and of deformations with check pattern marking and spectral method processing (Grediac, Blaysat, Sur)* [96] relates to computational photomechanics

- *Dispositif de traitement de prise de vue (Berger, Gaudillière, Simon)* [95] relates to image-based localization from object detections.

CIFRE grants
C. Delmas PhD thesis was supported by a Cifre grant with GE Healthcare [1]

Industrial contract and transfert

- Bilateral contract with GE Healthcare (2013-2017)
  This contract was the support of Charlotte Delmas's PhD thesis with the aim to perform 3D reconstruction of tools in interventional neuroradiology.
- ATT OBL
  An Inria technological transfer action (ATT) on the subject of object based localization started in January 2020 with the aim to produce a demonstrator for industrial maintenance in complex environments.

Partnerships with socioeconomic stakeholders

We have established collaborations with industry (SBS Studio, GE Healthcare), clinical partners (Nancy Hospital, IHU Strasbourg) or with user communities (applied mechanics). The way our work is transferred to these actors (open-source software, license, CIFRE grants...) naturally depends on each particular case.

2 General public audience activities

Erwan Kerrien is Chargé de Mission for scientific mediation at Inria Nancy-Grand Est. Members of the team have made demonstrations at the Fête de la Science each year. Several lectures were also given towards middle and high school students and teachers. We also wrote a general audience paper on augmented reality [88].

The involvement in training through research

	2016-2020
Course books, etc	0
E-learnings, MOOC	2
Heads of masters (mention and parcours)	0
Heads of international courses (Erasmus-mundus, etc)	0

1 Involvement of the team in training through research

All members of the team have part of their teaching activities in computer vision, shape recognition, image processing or machine learning. These courses are given mainly in the computer science Master of Nancy (Master Apprentiisage, Vision et Robotique) and in several Engineering Schools near Nancy (Ecole des Mines de Nancy, SUPELEC Metz, Ecole nationale supérieure de Géologie, Telecom).

2 Involvement in E-Educations

Erwan Kerrien participated in the creation of a MOOC for teachers of the new ICN option (Informatique et Création Numérique. This MOOC is part of the Class'Code project (https:

//pixees.fr/classcode-v2). He also took his part in the animation and participated in the evolution of this MOOC to adapt to the new SNT class (Sciences du Numérique et Technologie - *Digital Science and Technology*) that generalizes ICN, and is included in the 1st year core curriculum in upper secondary education. See other activities in appendix.

❸ Courses and research schools.

The list of master level courses to which the team makes a significant contribution in terms of training is the following

- ENSMN: Introduction to image processing (21h), Introduction to machine learning (60 h)
- Master AVR (Apprentissage, Vision et Robotique, UL): Shape recognition (24 h), Augmented Reality (24h)
- ENSG: Image processing for Geosciences (12h)
- M2 Cognitive Sciences and Applications: Augmented and Virtual Reality, (16h)

❹ Responsibilities

Life of the team

	2016-2020
Nb of seminars	one per month + invited talks
Web site	https://magrit.loria.fr

We have regular scientific meetings with all the team members (one per month) plus additional invited talks. Meetings restricted to the staff members are also organized. Supervision meetings with the PhD students are organized every week.

Half of the recruited students are from outside the European Community, with about 20% of women in the mean.

References

Doctoral Dissertations

[1] Charlotte Delmas. "3D reconstruction of curvilinear micro-devices for interventionnal neuroradiology". PhD thesis. Université de Lorraine, November 2017. tel-01653707.

[2] Pierre Rolin. "Viewpoint synthesis for camera pose initialisation". PhD thesis. Université de Lorraine, March 2017. tel-01536649.

[3] Antoine Fond. "Image-based localization in urban environment : application to augmented reality". PhD thesis. Université de Lorraine, April 2018. tel-01789709.

[4] Jaime Garcia Guevara. "Biomechanical graph matching for hepatic intra-operative image registration". PhD thesis. Universite de Lorraine, December 2019. tel-02408339.

[5] Vincent Gaudillière. “Visual positioning in a world of objects”. PhD thesis. Université de Lorraine, June 2020. tel-02915866.

[6] Raffaella Trivisonne. “Image-guided Interactive Simulation for Endovascular Surgery”. PhD thesis. Université de Strasbourg, October 2020. tel-03021043.

[7] Daryna Panicheva. “Image-based mitral valve modeling for biomechanical applications”. PhD thesis. Université de Lorraine, March 2021. tel-03213275.

Habilitation Theses

[8] Frédéric Sur. “Quelques contributions à l’analyse et au traitement des images numériques”. Habilitation à diriger des recherches. Université de Lorraine, November 2016. tel-01399973.

[9] Erwan Kerrien. “Quelques contributions à l’imagerie médicale multimodale et interventionnelle”. Habilitation à diriger des recherches. Université de Lorraine, January 2018. tel-01754699.

[10] Gilles Simon. “Positionnement visuel pour la réalité augmentée en environnement plan”. Habilitation à diriger des recherches. Université de Lorraine, December 2019. tel-02403014.

Articles in International Peer-Reviewed Journal

[11] Michaël Aron, Marie-Odile Berger, Erwan Kerrien, Brigitte Wrobel-Dautcourt, Blaise Potard, and Yves Laprie. “Multimodal acquisition of articulatory data: Geometrical and temporal registration”. In: *Journal of the Acoustical Society of America* 139.2 (2016), p. 13. DOI: 10.1121/1.4940666. hal-01269578.

[12] Benoît Blaysat, Michel Grediac, and Frédéric Sur. “Effect of interpolation on noise propagation from images to DIC displacement maps”. In: *International Journal for Numerical Methods in Engineering* 108.3 (2016), pp. 213–232. DOI: 10.1002/nme.5212. hal-01255944.

[13] Benoît Blaysat, Michel Grediac, and Frédéric Sur. “On the propagation of camera sensor noise to displacement maps obtained by DIC - an experimental study”. In: *Experimental Mechanics* 56.6 (2016), pp. 919–944. DOI: 10.1007/s11340-016-0130-9. hal-01269655.

[14] Michel Grediac, Frédéric Sur, and Benoît Blaysat. “Removing quasi-periodic noise in strain maps by filtering in the Fourier domain”. In: *Experimental Techniques* 40.3 (2016), pp. 959–971. DOI: 10.1007/s40799-016-0100-2. hal-01163838.

[15] Michel Grediac, Frédéric Sur, and Benoît Blaysat. “The grid method for in-plane displacement and strain measurement: a review and analysis”. In: *Strain* 52.3 (2016), pp. 205–243. DOI: 10.1111/str.12182. hal-01317145.

[16] Frédéric Sur, Benoît Blaysat, and Michel Grediac. “Determining displacement and strain maps immune from aliasing effect with the grid method”. In: *Optics and Lasers in Engineering* 86 (2016), pp. 317–328. DOI: 10.1016/j.optlaseng.2016.06.010. hal-01352868.

[17] Frédéric Sur and Michel Grediac. “Influence of the analysis window on the metrological performance of the grid method”. In: *Journal of Mathematical Imaging and Vision* 56.3 (2016), pp. 472–498. DOI: 10.1007/s10851-016-0650-z. hal-01298523.

[18] Franck Vidal and Pierre-Frédéric Villard. "Development and Validation of Real-time Simulation of X-ray Imaging with Respiratory Motion". In: *Computerized Medical Imaging and Graphics* 49 (April 2016), p. 15. DOI: 10.1016/j.compmedimag.2015.12.002. hal-01266065.

[19] Michel Grédiac, Benoît Blaysat, and Frédéric Sur. "A Critical Comparison of Some Metrological Parameters Characterizing Local Digital Image Correlation and Grid Method". In: *Experimental Mechanics* 57.6 (2017), pp. 871–903. DOI: 10.1007/s11340-017-0279-x. hal-01509611.

[20] Erwan Kerrien, Ahmed Yureidini, Jeremie Dequidt, Christian Duriez, René Anxionnat, and Stéphane Cotin. "Blood vessel modeling for interactive simulation of interventional neuroradiology procedures". In: *Medical Image Analysis* 35 (January 2017), pp. 685–698. DOI: 10.1016/j.media.2016.10.003. hal-01390923.

[21] Frédéric Sur, Benoît Blaysat, and Michel Grediac. "Towards Computational Photomechanics". In: *ERCIM News* 108 (January 2017), pp. 30–31. hal-01430636.

[22] Jaime Garcia Guevara, Igor Peterlik, Marie-Odile Berger, and Stephane Cotin. "Biomechanics-based graph matching for augmented CT-CBCT". In: *International Journal of Computer Assisted Radiology and Surgery* 13.6 (April 2018), pp. 805–813. DOI: 10.1007/s11548-018-1755-1. hal-01761521.

[23] Friederike Laus, Fabien Pierre, and Gabriele Steidl. "Nonlocal Myriad Filters for Cauchy Noise Removal". In: *Journal of Mathematical Imaging and Vision* (April 2018). arXiv: 1710.03015, pp. 1–31. DOI: 10.1007/s10851-018-0816-y. hal-01814104.

[24] Frédéric Sur, Benoît Blaysat, and Michel Grediac. "Rendering Deformed Speckle Images with a Boolean Model". In: *Journal of Mathematical Imaging and Vision* 60.5 (2018), pp. 634–650. DOI: 10.1007/s10851-017-0779-4. hal-01664997.

[25] Pierre-Frédéric Villard, Peter E. Hammer, Douglas P. Perrin, Pedro J. Del Nido, and Robert Howe. "Fast Image-Based Mitral Valve Simulation from Individualized Geometry". In: *The International Journal of Medical Robotics and Computer Assisted Surgery* 14.2 (2018), e1880. DOI: 10.1002/rcs.1880. hal-01643868.

[26] Michel Grediac, Benoît Blaysat, and Frédéric Sur. "A robust-to-noise deconvolution algorithm to enhance displacement and strain maps obtained with local DIC and LSA". In: *Experimental Mechanics* 59.2 (2019), pp. 219–243. DOI: 10.1007/s11340-018-00461-4. hal-01926058.

[27] Michel Grediac, Benoît Blaysat, and Frédéric Sur. "Extracting displacement and strain fields from checkerboard images with the Localized Spectrum Analysis". In: *Experimental Mechanics* 59.2 (2019), pp. 207–218. DOI: 10.1007/s11340-018-00439-2. hal-01926054.

[28] Pierre Rolin, Marie-Odile Berger, and Frédéric Sur. "View synthesis for pose computation". In: *Machine Vision and Applications* 30.7-8 (2019), pp. 1209–1227. DOI: 10.1007/s00138-019-01045-5. hal-02279616.

[29] Frédéric Sur. "A non-local dual-domain approach to cartoon and texture decomposition". In: *IEEE Transactions on Image Processing* 28.4 (2019), pp. 1882–1894. DOI: 10.1109/TIP.2018.2881906. hal-01925890.

[30] Pauline Tan, Fabien Pierre, and Mila Nikolova. "Inertial Alternating Generalized Forward-Backward Splitting for Image Colorization". In: *Journal of Mathematical Imaging and Vision* 61.5 (February 2019), pp. 672–690. DOI: 10.1007/s10851-019-00877-0. hal-01792432.

[31] Benoît Blaysat, Jan Neggers, Michel Grediac, and Frédéric Sur. “Towards Criteria Characterizing the Metrological Performance of Full-field Measurement Techniques : Application to the Comparison Between Local and Global Versions of DIC”. In: *Experimental Mechanics* 60.3 (2020), pp. 393–407. DOI: 10.1007/s11340-019-00566-4. hal-02436541.

[32] Sophie Cortese, Erwan Kerrien, Ilya Yakavets, Rokia Meilender, Romina Mastronicola, Sophie Renard, Agnès Leroux, Lina Bezdetnaya, and Gilles Dolivet. “ICG-induced NIR fluorescence mapping in patients with head & neck tumors after the previous radiotherapy”. In: *Photodiagnosis and Photodynamic Therapy* 31 (September 2020), p. 101838. DOI: 10.1016/j.pdpdt.2020.101838. hal-02888671.

[33] Jaime Garcia Guevara, Igor Peterlik, Marie-Odile Berger, and Stéphane Cotin. “Elastic registration based on compliance analysis and biomechanical graph matching”. In: *Annals of Biomedical Engineering* 48 (2020). arXiv: 1912.06353, pp. 447–462. DOI: 10.1007/s10439-019-02364-4. hal-02401280.

[34] Vincent Gaudillière, Gilles Simon, and Marie-Odile Berger. “Perspective-2-Ellipsoid: Bridging the Gap Between Object Detections and 6-DoF Camera Pose”. In: *IEEE Robotics and Automation Letters* 5.4 (October 2020), pp. 5189–5196. DOI: 10.1109/LRA.2020.3005387. hal-02886633.

[35] Michel Grediac, Benoît Blaysat, and Frédéric Sur. “Comparing several spectral methods used to extract displacement fields from checkerboard images”. In: *Optics and Lasers in Engineering* 127 (2020), p. 105984. DOI: 10.1016/j.optlaseng.2019.105984. hal-02436572.

[36] Michel Grédiac, Benoît Blaysat, and Frédéric Sur. “On the Optimal Pattern for Displacement Field Measurement: Random Speckle and DIC, or Checkerboard and LSA?” In: *Experimental Mechanics* 60.4 (2020), pp. 509–534. DOI: 10.1007/s11340-019-00579-z. hal-02462030.

[37] Raffaella Trivisonne, Erwan Kerrien, and Stéphane Cotin. “Constrained Stochastic State Estimation of Deformable 1D Objects: Application to Single-view 3D Reconstruction of Catheters with Radio-opaque Markers”. In: *Computerized Medical Imaging and Graphics* 81 (February 2020). DOI: 10.1016/j.compmedimag.2020.101702. hal-02469093.

[38] Cong Yang, Gilles Simon, John See, Marie-Odile Berger, and Wenyong Wang. “WatchPose: A View-Aware Approach for Camera Pose Data Collection in Industrial Environments”. In: *Sensors* 20.11 (May 2020). DOI: 10.3390/s20113045. hal-02735272.

[39] Seyfeddine Boukhtache, Kamel Abdelouahab, François Berry, Benoît Blaysat, Michel Grediac, and Frédéric Sur. “When Deep Learning Meets Digital Image Correlation”. In: *Optics and Lasers in Engineering* 136 (January 2021), p. 106308. DOI: 10.1016/j.optlaseng.2020.106308. hal-02933431.

[40] Antoine Fond, Marie-Odile Berger, and Gilles Simon. “Model-image registration of a building’s facade based on dense semantic segmentation”. In: *Computer Vision and Image Understanding* 206 (May 2021), p. 103185. DOI: 10.1016/j.cviu.2021.103185. hal-03204477.

[41] Daryna Panicheva, Pierre-Frédéric Villard, Peter E Hammer, Douglas Perrin, and Marie-Odile Berger. “Automatic extraction of the mitral valve chordae geometry for biomechanical simulation”. In: *International Journal of Computer Assisted Radiology and Surgery. Proceedings of IPCAI 2021* 16.5 (May 2021), pp. 709–720. DOI: 10.1007/s11548-021-02368-3. hal-03262496.

[42] Fabien Pierre, Mathieu Amendola, Clémence Bigeard, Timothé Ruel, and Pierre-Frédéric Villard. "Segmentation with Active Contours". In: *Image Processing On Line* 11 (May 2021), pp. 120–141. DOI: 10.5201/ipol.2021.298. hal-03235096.

[43] Siyi Qin, Michel Grédiac, Benoît Blaysat, Shaopeng Ma, and Frédéric Sur. "Influence of the sampling density on the noise level in displacement and strain maps obtained by processing periodic patterns". In: *Measurement - Journal of the International Measurement Confederation (IMEKO)* 173 (March 2021), p. 108570. DOI: 10.1016/j.measurement.2020.108570. hal-02965328.

[44] Gilles Simon. "Jan Van Eyck's Perspectival System Elucidated Through Computer Vision". In: *Proceedings of the ACM on Computer Graphics and Interactive Techniques* 4.2 (July 2021). (SIGGRAPH 2021). DOI: 10.1145/3465623. hal-03287031.

[45] Frédéric Sur, Benoît Blaysat, and Michel Grédiac. "On Biases in Displacement Estimation for Image Registration, with a Focus on Photomechanics". In: *Journal of Mathematical Imaging and Vision* 63.7 (May 2021), pp. 777–806. DOI: 10.1007/s10851-021-01032-4. hal-03226201.

Major International Conferences

[46] Benoît Blaysat, Michel Grédiac, and Frédéric Sur. "Assessing the Metrological Performance of DIC Applied on RGB Images". In: *iDICS 2016 Conference*. Ed. by M. Sutton and P. Reu. Proceedings of the first Conference of the International Digital Imaging Correlation Society. Philadelphia, United States: Springer, November 2016, pp. 109–111. DOI: 10.1007/978-3-319-51439-0_26. hal-01500324.

[47] Charlotte Delmas, Cyril Riddell, Yves Trousset, Erwan Kerrien, Marie-Odile Berger, René Anxionnat, and Serge Bracard. "Intra-operative 3D micro-coil imaging using subsampled tomographic acquisition patterns on a biplane C-arm system". In: *Proceedings of the 4th International Conference on Image Formation in X-Ray Computed Tomography (CT meeting'16)*. Bamberg, Germany, July 2016. hal-01303153.

[48] Martine Gautier and Brigitte Wrobel-Dautcourt. "artEoz - dynamic program visualization". In: *International Conference on Informatics in Schools: Situation, Evolution, and Perspectives, ISSEP 2016*. Munster, Germany, October 2016, p. 2. hal-01388703.

[49] Nazim Haouchine, Marie-Odile Berger, and Stephane Cotin. "Simultaneous Pose Estimation and Augmentation of Elastic Surfaces from a Moving Monocular Camera". In: *International Symposium on Mixed and Augmented Reality*. Merida, Mexico, September 2016. hal-01353189.

[50] Pierre-Jean Petitprez, Erwan Kerrien, and Pierre-Frédéric Villard. "PoLAR: a Portable Library for Augmented Reality". In: *15th IEEE International Symposium on Mixed and Augmented Reality (ISMAR)*. IEEE. Merida, Mexico, September 2016, p. 4. hal-01356012.

[51] Pierre Rolin, Marie-Odile Berger, and Frédéric Sur. "Enhancing pose estimation through efficient patch synthesis". In: *27th British Machine Vision Conference (BMVC 2016)*. Proceedings of BMVC 2016. York, United Kingdom, September 2016. hal-01368843.

[52] Gilles Simon, Antoine Fond, and Marie-Odile Berger. "A Simple and Effective Method to Detect Orthogonal Vanishing Points in Uncalibrated Images of Man-Made Environments". In: *Eurographics 2016*. Lisbon, Portugal, May 2016. hal-01275628.

[53] Yinoussa Adagolodjo, Raffaella Trivisonne, Nazim Haouchine, Stéphane Cotin, and Hadrien Courtecuisse. “Silhouette-based Pose Estimation for Deformable Organs Application to Surgical Augmented Reality”. In: *IROS 2017 - IEEE/RSJ International Conference on Intelligent Robots and Systems*. Vancouver, Canada, September 2017. hal-01578815.

[54] Antoine Fond, Marie-Odile Berger, and Gilles Simon. “Facade Proposals for Urban Augmented Reality”. In: *ISMAR 2017 - 16th IEEE International Symposium on Mixed and Augmented Reality*. Nantes, France, October 2017. hal-01562392.

[55] Jaime Garcia Garcia Guevara, Igor Peterlik, Marie-Odile Berger, and Stéphane Cotin. “Automatic biomechanical graph matching CT-CBCT fusion”. In: *Surgetica 2017*. Strasbourg, France, November 2017. hal-01587952.

[56] Aaron Sujar, Andreas Meuleman, Pierre-Frédéric Villard, Marcos Garcia, and Franck P. Vidal. “gVirtualXRay: Virtual X-Ray Imaging Library on GPU”. In: *Computer Graphics and Visual Computing*. Ed. by Tao Ruan Wan and Franck Vidal. Computer Graphics and Visual Computing. Manchester, United Kingdom: The Eurographics Association, September 2017, pp. 61–68. DOI: 10.2312/cgvc.20171279. hal-01588532.

[57] Raffaella Trivisonne, Erwan Kerrien, and Stéphane Cotin. “Augmented 3D Catheter Navigation using Constrained Shape from Template”. In: *Hamlyn Symposium*. London, United Kingdom, June 2017. hal-01545693.

[58] Jaime Garcia Guevara, Igor Peterlik, Marie-Odile Berger, and Stephane Cotin. “Biomechanics-based graph matching for augmented CT-CBCT”. In: *IPCAI 2018 - 9th International Conference on Information Processing in Computer-Assisted Interventions*. Berlin, Germany, June 2018. hal-01761538.

[59] Vincent Gaudillière, Gilles Simon, and Marie-Odile Berger. “Region-Based Epipolar and Planar Geometry Estimation in Low Textured Environments”. In: *ICIP 2018 - 25th IEEE International Conference on Image Processing*. Athens, Greece: IEEE, October 2018, pp. 898–902. DOI: 10.1109/ICIP.2018.8451244. hal-01802596.

[60] Michel Grediac, Benoît Blaysat, and Frédéric Sur. “Speckles and DIC or Checkerboards and LSA?” In: *SEM Annual Conference & Exposition on Experimental and Applied Mechanics*. Ed. by Luciano Lamberti, Ming-Tzer Lin, Cosme Furlong, Cesar Sciammarella, Phillip L. Reu, and Michael A Sutton. Vol. 3. Greenville, United States: Springer, June 2018, pp. 79–80. DOI: 10.1007/978-3-319-97481-1_9. hal-01896817.

[61] Fabien Pierre. “Exemplar-based face colorization using image morphing”. In: *SIAM Conference on IMAGING SCIENCE*. Bologne, Italy, June 2018. hal-01824827.

[62] Gilles Simon, Antoine Fond, and Marie-Odile Berger. “A-Contrario Horizon-First Vanishing Point Detection Using Second-Order Grouping Laws”. In: *ECCV 2018 - European Conference on Computer Vision*. Munich, Germany, September 2018, pp. 323–338. hal-01865251.

[63] Frédéric Sur, Benoît Blaysat, and Michel Grediac. “Speckle Image Rendering for DIC Performance Assessment”. In: *SEM Annual Conference & Exposition on Experimental and Applied Mechanics*. Ed. by Luciano Lamberti, Ming-Tzer Lin, Cosme Furlong, Cesar Sciammarella, Phillip L. Reu, and Michael A Sutton. Vol. 3. Greenville, United States: Springer, June 2018, pp. 75–77. DOI: 10.1007/978-3-319-97481-1_8. hal-01896811.

[64] Nicola Cacciani, Elisabeth Larsson, Igor Tominec, and Pierre-Frédéric Villard. “Meshfree Simulation of Human Respiratory Muscles”. In: *CSE 19 - SIAM Conference on Computational Science and Engineering*. Spokane, United States, February 2019. hal-02057413.

[65] Vincent Gaudillière, Gilles Simon, and Marie-Odile Berger. "Camera Pose Estimation with Semantic 3D Model". In: *IROS 2019 - 2019 IEEE/RSJ International Conference on Intelligent Robots and Systems*. Macau, Macau SAR China, November 2019. DOI: 10.1109/IROS40897.2019.8968180. hal-02181962.

[66] Vincent Gaudillière, Gilles Simon, and Marie-Odile Berger. "Camera Relocalization with Ellipsoidal Abstraction of Objects". In: *ISMAR 2019 - 18th IEEE International Symposium on Mixed and Augmented Reality*. Beijing, China: IEEE, October 2019, pp. 19–29. DOI: 10.1109/ISMAR.2019.00017. hal-02170784.

[67] Thomas Mouzon, Fabien Pierre, and Marie-Odile Berger. "Joint CNN and Variational Model for Fully-automatic Image Colorization". In: *SSVM 2019 - Seventh International Conference on Scale Space and Variational Methods in Computer Vision*. Scale Space and Variational Methods in Computer Vision. Hofgeismar, Germany, June 2019, pp. 535–546. hal-02059820.

[68] Daryna Panicheva, Pierre-Frédéric Villard, and Marie-Odile Berger. "Toward an automatic segmentation of mitral valve chordae". In: *SPIE Medical Imaging*. Ed. by Barjor Gimi and Andrzej Kro. Vol. 10953. SPIE. San Diego, United States, February 2019, pp. 1095315–1095323. DOI: 10.1117/12.2511943. hal-02050846.

[69] Daryna Panicheva, Pierre-Frédéric Villard, Peter Hammer, and Marie-Odile Berger. "Physically-coherent Extraction of Mitral Valve Chordae". In: *International Conference in Computing in Cardiology*. Vol. 46. Proceedings of Computers in Cardiology. Singapore, Singapore: IEEE Engineering in Medicine and Biology Society, September 2019, p. 4. hal-02368810.

[70] Arthur Renaudeau, François Lauze, Fabien Pierre, Jean-François Aujol, and Jean-Denis Durou. "Alternate Structural-Textural Video Inpainting for Spot Defects Correction in Movies". In: *SSVM 2019 - Seventh International Conference on Scale Space and Variational Methods in Computer Vision*. Hofgeismar, Germany, June 2019. hal-02433997.

[71] Vincent Gaudillière, Gilles Simon, and Marie-Odile Berger. "Perspective-2-Ellipsoid: Bridging the Gap Between Object Detections and 6-DoF Camera Pose". In: *IROS 2020 – 2020 IEEE/RSJ International Conference on Intelligent Robots and Systems*. Las Vegas, United States, October 2020. hal-02889146.

[72] Arthur Renaudeau, Travis Seng, Axel Carlier, Fabien Pierre, François Lauze, Jean-François Aujol, and Jean-Denis Durou. "Learning Defects in Old Movies from Manually Assisted Restoration". In: *ICPR 2020 - 25th International Conference on Pattern Recognition*. Milan / Virtual, Italy, September 2020. hal-02965296.

[73] Matthieu Zins, Gilles Simon, and Marie-Odile Berger. "3D-Aware Ellipse Prediction for Object-Based Camera Pose Estimation". In: *3DV 2020 - International Virtual Conference on 3D Vision*. Fukuoka / Virtual, Japan, November 2020. hal-02975379.

Secondary International Conferences

[74] Gilles Simon and Salvatore Tabbone. "Generic Document Image Dewarping by Probabilistic Discretization of Vanishing Points". In: *ICPR 2020 - 25th International Conference on Pattern Recognition*. Milan / Virtual, Italy, September 2020. hal-02987029.

[75] Youssef Assis, Liang Liao, Fabien Pierre, René Anxionnat, and Erwan Kerrien. "An efficient data strategy for the detection of brain aneurysms from MRA with deep learning". In: *DALI 2021 - MICCAI workshop on Data Augmentation, Labeling, and Imperfections*. Vol. 13003. Deep Generative Models, and Data Augmentation, Labelling, and Imperfections. Strasbourg, France: Springer, September 2021, pp. 226–234. DOI: 10.1007/978-3-030-88210-5_22. hal-03391884.

[76] Elisabeth Larsson, Pierre-Frédéric Villard, Igor Tominec, and Nicola Cacciani. "Geometry Reconstruction from Noisy Data using a Radial Basis Function Partition of Unity Method". In: *CSE 2021 - SIAM Conference on Computational Science and Engineering*. Fort Worth/Virtual, United States, March 2021. hal-03147251.

[77] Pierre-Alexandre Simon, Radu S. Stoica, and Frédéric Sur. "An application of neural point processes to geophysical data". In: *RING Meeting 2021*. Nancy, France, September 2021, pp. 1–13. hal-03294911.

National Peer-Reviewed Conferences

[78] Antoine Fond, Marie-Odile Berger, and Gilles Simon. "Generation of facade hypotheses based on contextual and structural information". In: *Reconnaissance des Formes et Intelligence Artificielle*. Clermont Ferrand, France, June 2016. hal-01318680.

[79] Vincent Gaudillière, Gilles Simon, and Marie-Odile Berger. "Estimation des géométries planaire et épipolaire en environnement faiblement texturé basée sur la mise en correspondance de régions". In: *RFIAP 2018 - Congrès Reconnaissance des Formes, Image, Apprentissage et Perception*. Marne-la-Vallée, France, June 2018. hal-01802538.

[80] Vincent Gaudillière, Gilles Simon, and Marie-Odile Berger. "Estimation de pose de caméra à partir de correspondances ellipse - ellipsoïde". In: *ORASIS 2019 - 17ème journées francophones des jeunes chercheurs en vision par ordinateur*. Saint-Dié-des-Vosges, France, May 2019. hal-02148633.

[81] Arthur Renaudeau, François Lauze, Fabien Pierre, Jean-François Aujol, and Jean-Denis Durou. "Inpainting vidéo pour la restauration de films par reconstructions alternées de la structure et de la texture". In: *ORASIS 2019 - 17ème journées francophones des jeunes chercheurs en vision par ordinateur*. Saint-Dié-des-Vosges, France, May 2019. hal-02433990.

[82] Youssef Assis, Liang Liao, Fabien Pierre, René Anxionnat, and Erwan Kerrien. "Une stratégie de données efficace pour la détection des anévrismes cérébraux avec l'apprentissage profond". In: *ORASIS 2021 - 18èmes journées francophones des jeunes chercheurs en vision par ordinateur*. Centre National de la Recherche Scientifique [CNRS]. Saint Ferréol, France, September 2021. hal-03339672.

[83] Abdelkarim Elassam, Marie-Odile Berger, and Gilles Simon. "Détection de la ligne d'horizon et des points de fuite par apprentissage profond". In: *ORASIS 2021 - 18èmes journées francophones des jeunes chercheurs en vision par ordinateur*. Centre National de la Recherche Scientifique [CNRS]. Saint Ferréol, France, September 2021. hal-03339639.

[84] Arthur Renaudeau, Travis Seng, Axel Carlier, Fabien Pierre, François Lauze, Jean-François Aujol, and Jean-Denis Durou. "Détection des défauts dans les vieux films par apprentissage profond à partir d'une restauration semi-manuelle". In: *ORASIS 2021 - 18èmes journées francophones des jeunes chercheurs en vision par ordinateur*. Centre National de la Recherche Scientifique [CNRS] and Equipe REVA, IRIT : Institut de Recherche en Informatique de Toulouse. Saint Ferréol, France, September 2021. hal-03339640.

[85] Matthieu Zins, Gilles Simon, and Marie-Odile Berger. "3D-Aware Ellipse Prediction for Object-Based Camera Pose Estimation". In: *ORASIS 2021 - 18èmes journées francophones des jeunes chercheurs en vision par ordinateur*. Ce travail a déjà été publié lors de la conférence 3DV 2020. Centre National de la Recherche Scientifique [CNRS]. Saint Ferréol, France, September 2021. hal-03339617.

Book (written)

Book Chapters

[86] Nicola Cacciani, Elisabeth Larsson, Alberto Lauro, Marco Meggiolaro, Alessio Scatto, Igor Tominec, and Pierre-Frédéric Villard. "A First Meshless Approach to Simulation of the Elastic Behaviour of the Diaphragm". In: *Spectral and High Order Methods for Partial Differential Equations ICOSAHOM 2018*. Ed. by Sherwin S., Moxey D., Peiró J., Vincent P., and Schwab C. Vol. 134. Lecture Notes in Computational Science and Engineering. Springer, August 2020, pp. 501–512. DOI: 10.1007/978-3-030-39647-3_40. hal-02917575.

[87] Fabien Pierre and Jean-François Aujol. "Recent Approaches for Image Colorization". In: *Handbook of Mathematical Models and Algorithms in Computer Vision and Imaging*. 2020. DOI: 10.1007/978-3-030-03009-4_55-1. hal-02965137.

General Audience

[88] Marie-Odile Berger and Gilles Simon. "Réalité augmentée : entre mythes et réalités". In: *Interstices* (March 2016). hal-01350456.

[89] Gilles Simon. "La machine à perspective de Jan Van Eyck". In: *Interstices* (November 2021). hal-03517010.

[90] Gilles Simon. "La véritable invention de Jan van Eyck : une machine à représenter l'espace tel que nous le percevons". In: *The Conversation* (August 2021). hal-03521172.

Other Publication

[91] Vincent Gaudillière, Gilles Simon, and Marie-Odile Berger. "Perspective-12-Quadric: An analytical solution to the camera pose estimation problem from conic - quadric correspondences". working paper or preprint. March 2019. hal-02054882.

[92] Raffaella Trivisonne, Erwan Kerrien, and Stéphane Cotin. "Constrained Stochastic State Estimation for 3D Shape Reconstruction of Catheters and Guidewires in Fluoroscopic Images". working paper or preprint. April 2019. hal-02072386.

[93] Frédéric Sur, Benoît Blaysat, and Michel Grédiac. *On biases in displacement estimation for image registration, with a focus on photomechanics - Extended version*. Research Report. LORIA (Université de Lorraine, CNRS, INRIA) ; Institut Pascal (Université Clermont-Auvergne, SIGMA, CNRS), June 2020. hal-02862808.

[94] Iris Dumeur, Yang Chen, Frédéric Sur, and Zheng-Shu Zhou. *Sentinel-2 RGB and NIR bands simulation after fire events using a multi-temporal conditional generative adversarial network*. Research Report. LORIA (Université de Lorraine, CNRS, INRIA), 2021. hal-03327421.

Patents

[95] Marie-Odile Berger, Vincent Gaudillière, and Gilles Simon. "Dispositif de traitement de prise de vue". FR1905535 (France). May 2019. hal-02429562.

[96] Michel Grediac, Benoît Blaysat, and Frédéric Sur. "Method for measuring fields of movements and of deformations with check pattern marking and spectral method processing". FR3078190 WO2019162449 (France). August 2019. hal-02272747.

D1 : Tangram

Report integrators: Laurent Andrey (Team Resist), Philippe Dosch (Department 4), and Sylvain Pogodalla (Team Sémagramme). Report designed under Linux using Emacs, and formated thanks to LuaLaTeX.
Crédits photos : Loria, CNRS, Université de Lorraine, Laurent Phialy, Flaticon, Nicolas Dohr, F. Nussbaumer/Inria, D. Betzinger/Inria