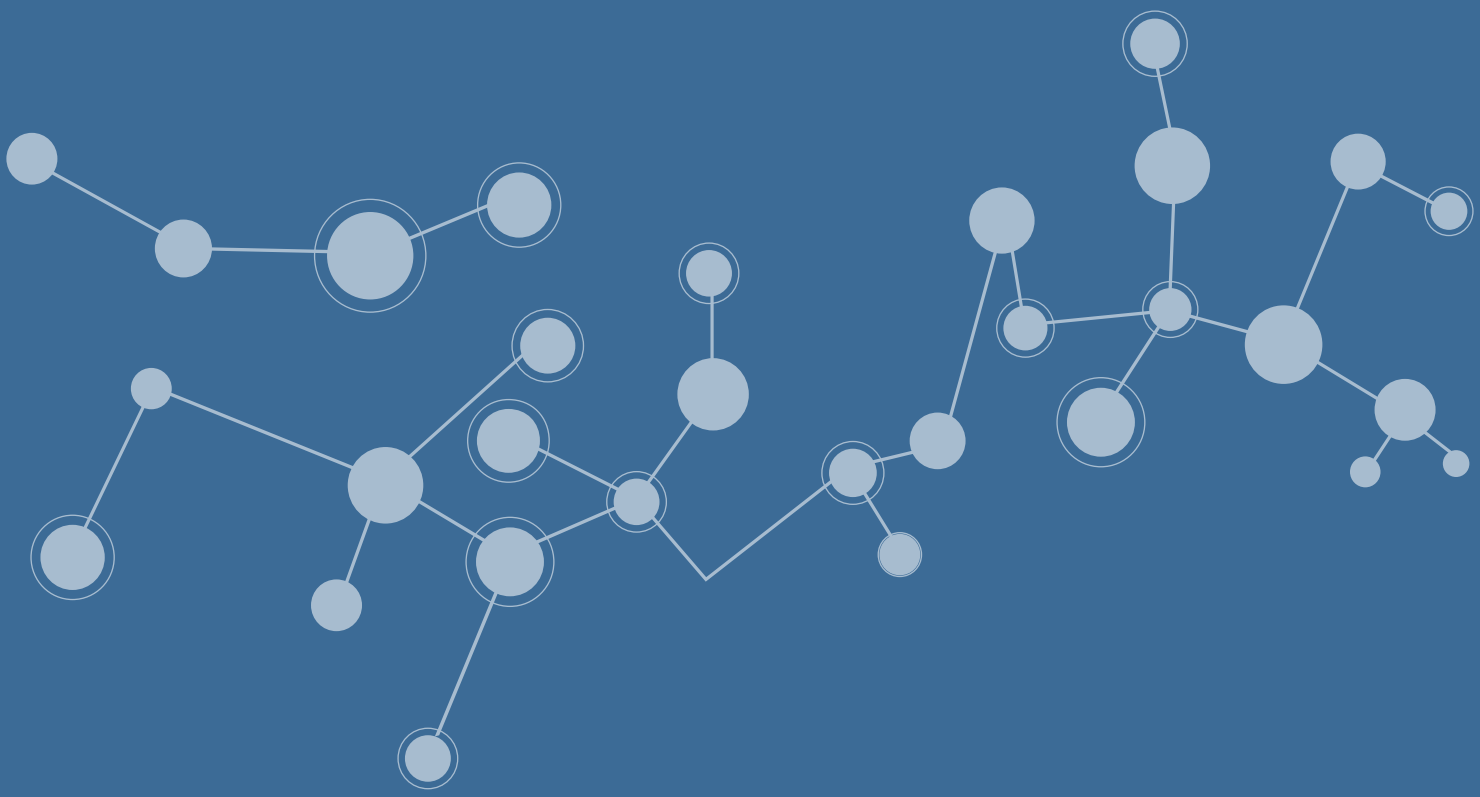
DOCUMENT D'AUTO-ÉVALUATION

DEPARTMENT 1

Algorithms, Computation, Geometry and Image



Loria cnrs Inria UNIVERSITÉ DE LORRAINE

En partenariat avec : CentraleSupélec

Table des matières

DAE Département 1 : Algorithmique, calcul, image et géométrie

DEPARTMENT HEAD
Sylvain Lazard

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.

DAE Département 1 : Algorithmique, calcul, image et géométrie

1. Retour sur l'évaluation 2011-2016

Critère 1 : qualité et production scientifiques

Appréciation et recommandations : Les équipes ont toutes une excellente dynamique, notamment autour de leurs leaders scientifiques. Les résultats scientifiques, toujours notables, quelquefois exceptionnels, se concrétisent par des publications significatives au meilleur niveau. Il faut continuer à viser l'excellence, tout en accompagnant davantage les scientifiques moins productifs, pour qu'elle soit le fait de tous.

Nous avons continué à viser l'excellence. Nous décrivons nos actions d'accompagnement des chercheurs les moins productifs dans le DAE du labo (§D3R2).

Critère 2 : rayonnement et attractivité académiques

Appréciation et recommandations : Toutes les équipes bénéficient d'un excellent rayonnement : de très nombreuses collaborations en France et à l'étranger ont débouché sur des publications communes, beaucoup d'articles et de démonstrations ont remporté de nombreux prix. Pour deux de ces équipes, ce rayonnement est exceptionnel. Les équipes ADAGIO et MAGRIT pourraient profiter des collaborations internationales de leurs partenaires nationaux pour accentuer leur reconnaissance internationale. Il faudrait mettre en place un recrutement de cadres (enseignants-chercheurs ou chercheurs) pour les équipes ADAGIO et MAGRIT, vraiment déficitaires de ce point de vue.

La reconnaissance internationale de l'équipe Magrit-Tangram est excellente ; en témoigne leur équipe associée CURATIVE [1] établie depuis 2017 avec le laboratoire de Biorobotics à l'université d'Harvard à Cambridge (voir pour plus de détails la section 6 ci-dessous et la Section 5 page 200 du Portefolio D1-1).

L'équipe Adagio est fortement impliquée dans une collaboration de long terme avec les acteurs académiques et socio-économiques français en foresterie ; ces actions sont soutenues par deux projets ANR (cf. section 1 page 89 du Portefolio D1-1) ; ce projet en lien avec des acteurs socio-économiques régionaux est national par nature.

Les recrutements de chercheurs et enseignants-chercheurs ne sont pas pilotés par les départements. L'equipe Magrit-Tangram à cependant recruté un PR (en promotion) durant la période, soit 1/3 des 3 cadres (PR/DR) recrutés par le département durant la période.

Critère 3 : interactions avec l'environnement économique, social, culturel et sanitaire

Appréciation et recommandations : Il y a de très importants développements logiciels, très visibles pour toutes les équipes, et une attention soutenue à la diffusion de leurs thèmes sociétaux ou pluridisciplinaires. Mais les collaborations avec les mathématiciens devraient être renforcées. Le département pourrait s'investir davantage dans la vulgarisation scientifique pour attirer des jeunes sur ses thèmes, et rester imaginatif sur de potentielles interactions sociétales, même dans les thématiques plus fondamentales.

1. https://team.inria.fr/curative/

Nos relations avec les mathématiciens sont soutenues sur le long terme. Nous listons nos collaborations avec des mathématiciens durant la periode d'évaluation en footnote. [2] Concernant la vulgarisation scientifique, nos actions sont également nombreuses : Cf. section 3 ci-dessous.

Critère 4 : organisation et vie du département

Appréciation et recommandations : Il faut développer l'animation scientifique du département [...] Le département ne devrait pas se limiter à élaborer une politique " réactive", mais développer davantage une politique scientifique prospective [...]

La politique scientifique prospective est a priori gérée par les équipes à l'interieur des départements, ce qui est un choix stratégique du laboratoire, décliné dans les départements. La direction du laboratoire et les responsables de départements pilotent néanmoins les réorganisations d'équipes quand cela est utile. Il faut également souligner que les équipes travaillent régulièrement à leur politique scientifique : Les équipes Inria (Caramba, Gamble, MFX, Pixel, Tangram) rédigent tous les 4-5 ans un document de prospective scientifique à l'occasion de leur évaluation Inria. Ces documents de prospective étaient aussi demandés à toutes les équipes lors des évaluations HCERES antérieures et ont été demandés par l'UL en 2021 en prévision de la présente vague d'évaluation (document qui n'est plus demandé in fine par l'HCERES). De plus, à la suite de ces travaux de prospective effectués par les equipes, la direction du laboratoire avec (tous) les responsables de départements ont organisé une journée par département de réflexion prospective avec les responsables d'équipes, à l'automne 2021.

Concernant l'animation scientifique, nous organisons au sein du département depuis 2016-2017 des séminaires mensuels et des journées annuelles ; cf. section 7 ci-dessous pour plus de détails.

2. Nous avons des collaborations avec des probabilistes, notamment avec Julien Michel (Laboratoire de Mathématiques et Applications, Poitier) [58], Nicolas Chenavier (Laboratoire de Mathématiques Pures et Appliquées, Univ. du Littoral Cote d'Opale) [108], Imre Barany (Institute of Mathematics, Budapest, Hongrie) [161] et Laurent Decreusefond (Telecom ParisTech) [214]. Ces collaborations sont structurées dans l'ANR Présage (2011-2015) et l'équipe associée Trip (2018-2020) portées par O. Devillers (LORIA) et impliquant de plus Nicolas Broutin (Laboratoire de Probabilités, Statistique et Modélisation, Sorbonne Univ.), Pierre Calka et Benjamin Dadoun (Laboratoire de Mathématiques, Rouen), Philippe Chassaing, Valentin Féray, et Régine Marchand (IECL, Nancy) et Arnaud Rousselle (Institut de Mathématiques, Dijon).

Nous collaborons avec des mathématiciens en géométrie non-Euclidienne : Gert Vegter (Bernoulli Institute for Mathematics and Computer Science, Groningen, Pays Bas) [238, 365, 366, 380, 481], Vanessa Robins (Mathématiques appliquées, Australian National University) [480], Myfanwy Evans (Institute for Mathematics, Postdam, Allemagne) (Benedikt Kolbe et Myfanwy E Evans. "Enumerating Isotopy Classes of Tilings guided by the symmetry of Triply-Periodic Minimal Surfaces". In : *SIAM Journal on Applied Algebra and Geometry* 6.1 [2022]. Accepted and to appear. doi : 10.1137/20M1358943. hal-03482422), ainsi qu'avec Jean-Marc Schlenker et Hugo Parlier (Dpt. de Mathématiques, Luxembourg) [477, 334] dans un projet ANR international (SoS).

En géométrie non-linéaire, nous avons une collaboration suivie avec Fabrice Rouillier (Inria, Institut de Mathématiques de Jussieu, Paris) [46, 250, 91, 117, 463] (Daouda Niang Diatta, Sény Diatta, Fabrice Rouillier, Marie-Françoise Roy et Michael Sagraloff. "Bounds for polynomials on algebraic numbers and application to curve topology". In : *Discrete and Computational Geometry* [février 2022]. doi : 10.1007/s00454-021-00353-w. hal-01891417) et également avec Marie-Françoise Roy (Institut de Recherche Mathématique de Rennes) (Daouda Niang Diatta, Sény Diatta, Fabrice Rouillier, Marie-Françoise Roy et Michael Sagraloff. "Bounds for polynomials on algebraic numbers and application to curve topology". In : *Discrete and Computational Geometry* [février 2022]. doi : 10.1007/s00454-021-00353-w. hal-01891417) et Frédéric Bihan (Laboratoire de Mathématiques LAMA, Université Savoie Mont Blanc) [103] géométrie algébrique.

Nous collaborons en géométrie discrète avec Andreas Holmsen (Department of Mathematical Sciences, KAIST, Corée du Sud), Martin Tancer (Department of Applied Mathematics, Charles Univ., Tchèquie) [141] et Boris Bukh (Carneggie Mellon University, Pittsburg, USA) [135].

Critère 5 : implication dans la formation par la recherche

Appréciation et recommandations : Les thèmes du D1 sont faiblement représentés dans les masters, même ceux de la géométrie et de l'image, malgré la mise en place d'une orientation très appliquée dans le Master " Apprentissage, Vision et Robotique " à partir de 2018. [...]

Même si la filière " Apprentissage, Vision et Robotique " peut ouvrir des perspectives au Continuum Géométrie- Image pour recruter des doctorants de profil plus appliqué, elle ne peut pas permettre le recrutement de doctorants sur la culture D1. On peut songer à monter un parcours dans le Master Informatique spécialisé dans les thèmes géométrie et image ; on peut aussi chercher à monter non pas une filière complète, mais quelques enseignements typiques de la culture " MathInfo " du D1, en collaboration avec des mathématiciens.

Il faudrait aussi ré-équilibrer la composition des membres du D1, et recruter au moins un PR (sur les thèmes géométrie et image par exemple) qui soit sur le site principal de l'UL, avec l'objectif de peser davantage dans les contenus au niveau L et porter une filière du master qui reflète la culture D1. Parallèlement, il serait important que les chercheurs du D1 comprennent leur intérêt à s'investir davantage dans les masters.

Dans cette situation défavorable, le D1 doit rester vigilant afin de garder l'accès aux allocations de l'université. C'est en particulier important pour des équipes comme ADAGIO.

Les membres du D1 s'investissent dans les responsabilités d'enseignement et de formation par la recherche. Citons notamment : F. Lauer est responsable du M1 Informatique à Nancy depuis 2016. I. Debled-Rennesson est co-responsable de la filière "Apprentissage, Vision et Robotique" du M2 Informatique. M. Minier est responsable de l'orientation "Sécurité Informatique, Réseaux et Architectures Virtuelles" du M2 Informatique. P. Gaudry a été entre 2016 et 2020 le vice-président de la Commission de mention Informatique de l'École doctorale IAEM. S. Lazard est responsable (national) de la Mission Jeunes Chercheurs Inria depuis 2018.

Concernant les contrats doctoraux, notons en premier lieu que le département recrute de façon substantielle des doctorants issus des formations locales.[3] Au sein du laboratoire, le D1 est bien doté de contrats doctoraux de l'université avec une ou deux allocations tous les ans (sur 6 ou 7). Enfin, l'équipe Adagio a une bonne dynamique avec les recrutements de 3 nouveaux doctorants sur les quatre dernières années.

Concernant les recrutements, comme déjà mentionné dans la section 1, le département a recruté 1 PR (en promotion) sur les thématiques d'image à Nancy, F. Sur, dans l'équipe Tangram.

Critère 6 : perspectives et stratégie scientifique à cinq ans

Appréciation et recommandations : [...] Il est essentiel que [l'équipe ABC] se rapproche des activités d'apprentissage et de fouille de données menées au sein des départements D4 et D5, et y apporte ses points de vue complémentaires. Ensuite, même s'il y a des arguments scientifiques qui justifient la scission de l'équipe ALICE, cette scission doit être accompagnée par le département, afin de préserver des interactions fortes entre les deux moitiés, et éviter un émiettement supplémentaire des équipes du D1. Enfin, comme CARAMBA et VEGAS sont deux équipes très proches, qui partagent beaucoup de méthodes et de compétences, elles devraient réfléchir à des collaborations plus précises, sur un sujet mieux délimité, où elles pourraient vraiment travailler ensemble.

L'équipe ABC s'est rapprochée de l'équipe Orpailleur (D4) sur des thématiques de fouille de données et co-encadre avec eux la thèse de F. Gaschi (depuis 2020) [424]. ABC s'est également

3. 16 doctorants issues des formations locales : Khaidja Musayeva, Rémi Decelle, Florian Delconte, Pierre Rolin, Daryna Panicheva, David Lopez, Jean Hergel et Jimmy Etienne : **Master FST informatique** ; Charles Duménil, Tom Masini : **Master FST Math** ; Nathan Boulangeot : **Master FST Physique** ; Arnaud Botella et Julien Renaudeau : **ENSG** ; Maxence Reberol : **Supelec Metz** ; Louis Masucci et Tom Masini : **Polytech Nancy** ; Justine Basselin, Rémi Decelle : **Télécom Nancy.**

rapprochée de l'équipe Capsid (D5) avec qui ils ont à présent un séminaire commun et co-encadrent la thèse d'A. Moniot (depuis 2019) [345, 483, 484].

Concernant ALICE : Comme mentionné plus haut (§ 1), notre stratégie est de déléguer le plus possible aux équipes leurs politiques scientifiques. Le département n'a donc pas "accompagné la scission de l'equipe ALICE afin de préserver des interactions fortes entre les deux moitiés" mais les membres des deux équipes ont néanmoins conservé des interactions importantes [73, 127, 139, 205].

Les équipes CARAMBA et VEGAS-GAMBLE sont deux équipes dont les cultures scientifiques ont une intersection non vide mais leurs thématiques de recherche sont assez éloignées.

2. Domaine 3 : Production scientifique

2.1. Référence 1 : La production scientifique de l'équipe satisfait à des critères de qualité.

2.1.1 Synopsis

L'UL a demandé aux laboratoires de rédiger pour juin 2021 les bilans des laboratoires en vue de l'évaluation HCERES 2016-2020. Ce document est présenté dans le Portefolio D1-1, et nous y faisons référence régulièrement dans le présent document. Pour faciliter la lecture des évaluateurs, nous avons extrait des éléments de notre rapport de juin 2021 pour les reproduire ici ; nous les avons cependant laissés en anglais, ce qui explique le mélange de langues dans ce présent document.

Les sections suivantes sont organisées comme suit : §2 Composition du département ; §3 Thématiques de recherche ; §4 Principaux résultats ; §5 Production scientifique et qualité ; §6 Réputation académique ; §7 Vie du département ; §8 Relations académiques.

2.1.2 Composition

Le département est composé (en 2021) de 44 enseignants-chercheurs et chercheurs permanents (5 PR, 15 MCF, 9 DR, 15 CR) et d'une soixantaine de non permanents dont une moitié de doctorants (37 sur 78 en 2021) ; voir Portefolio D1-1 pour les détails. Le département est de plus structuré en 7 équipes, de 4 à 10 permanents chacune, dont les thématiques scientifiques sont bien ciblées et cohérentes dans des projets d'équipes. Cette structuration en équipe-projets est historique et est héritée de l'époque où la direction du laboratoire et le centre Inria était commune. Cette structuration est efficace car l'impact scientifique de ces equipes est supérieure à la somme de ses parties et elle donne un excellent cadre pour l'accompagnement des doctorants, postdoctorants et jeunes chercheurs.

Ces équipes sont les suivantes :

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).

2.1.3 Research topics

[Extrait du Portfolio D1-1, Section 2.]

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.

2.1.4 Main Results

We shortly present some main results we obtained in our three axes of research, namely *Algorithms and Computation*, *Geometry* and *Image*. [Extrait du Portfolio D1-1 Section 3 page 7.]

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.[4] 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], and studying asymptotic complexities [331, 224].

We have set new (and current) records for integer factorization with the factorization of RSA with 250 decimal digits [329, 437] and for discrete logarithm computations, both over prime fields and prime-power fields [57, 247, 270, 329, 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, 309, 382, 21, 223]. 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 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

4. 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.

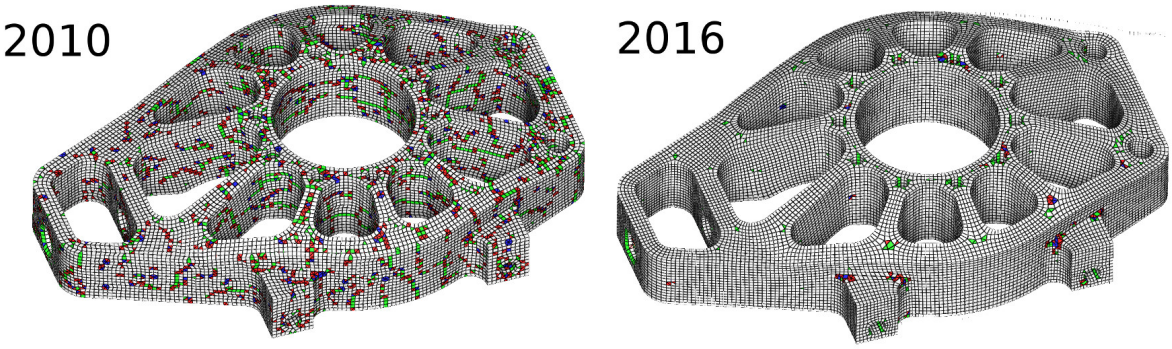


FIGURE 1.1 – Hexahedral meshes.

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 [479]. 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, 342].

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 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 [353, 367], slicing strategies [77, 201], trajectory generation algorithms 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) [340]. 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 [312]. 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 [313, 351] 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 [288, 16, 177], image segmentation of heart mitral valve chordae in Computerized Tomography (CT) images [130, 320, 321], and 3D reconstruction of the catheter from 2D X-ray images in interventional radiology [241, 4, 283, 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 [491]. A synthetic speckle image generator [129] permitted us to build datasets included in the international DIC challenge.[5] This is of uttermost importance to assess the metrological performance of the available DIC variants. A patent was also filed [491].

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 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 [359, 360, 272, 126, 319]. The experimental results demonstrate the efficiency and robustness of the approach and we applied it to hand gesture recognition [279].

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 [358]. 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 [377, 378] 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 [352, 261, 457, 195] based on our work on the detection of the center line of 3D objects [251, 357].

2.1.5 Scientific production and quality

La production scientifique sur les six années 2016-2021 pour le département est de 4 livres, 35 thèses, 6 HDR, 189 publications journaux, 143 publications dans des conférences majeures et

5. https://sem.org/dicchallenge

52 dans d'autres conférences.

En termes de qualité des supports de publications, nous avons publié 21 articles dans ACM Transactions on Graphics (TOG) correspondant à 15 articles SIGGRAPH et 6 SIGGRAPH Asia. En dehors de la communauté d'infographie, la diversité des supports de publication renommés est plus diverse et nous en donnons une cartographie ci-dessous.

List of top journals in which we have published (non-exhaustive)

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] [6]
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, 297, 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]

List of top conferences in which we have published (non-exhaustive)

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, 287, 314, 334, 340, 425]
DGCI – Int. Conf. on Discrete Geometry for Computer Imagery (7) [254, 272, 278, 98, 284, 310, 322]
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, 313]
Crypto (3) [329, 331, 333]
ESA – European Symp. on Algorithms (3) – [286, 304, 347]
ICPR – Int. Conf. on Pattern Recognition (3) [251, 261, 294]
Asiacrypt (5) [303, 306, 403, 404, 414]
FOCS – Symp. on Foundations of Computer Science (1) [431]
ECCV – European Conf. on Computer Vision (1) [300]
Eurocrypt (1) [267]
AISTATS – Int. Conf. on Artificial Intelligence and Statistics (1) [342]
IJCAI – Int. Joint Conf. on Artificial Intelligence (1) [269]
NeurIPS (formerly NIPS) – Conf. on Neural Information Processing Systems (1) [277]

Software. Nous avons également produit 35 logiciels durant la période. Nous citons très brièvement les plus importants ci-desssous et référons à la section "Software" page 13 du Portfolio D1-1 pour plus détails : **CADO-NFS** est un important software pour la factorisation d'entiers et le calcul de logarithmes discrets. **GNU MPFR** et **MPC** sont des bibliothèques d'arithmétique avec arrondi exact, lesquelles sont requises pour la compilation de GCC. **Belenios**, un

6. 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.

système de vote electronique sécurisé, utilisé en 2020 sur plus de 140 élections et 100 000 votants. **IceSL**, un modeleur 3D pour l'impression additive. **Geogram** et **Graphite** sont deux softwares de maillage et de modélisation 3D, téléchargés environ 50 000 fois chaque depuis 2016. **CGAL** est la bibliothèque de référence mondiale pour les algorithmes géométriques, dans laquelle nous avons contribué 4 packages de triangulation et maillage. **Isotop** est un des très rares algorithmes de tracé certifié de courbes algébriques dans le plan et le seul accessible en ligne. **DGtal** est une bibliothèque open source pour la géométrie des pixels. **TheGridMethod**, une boîte à outil pour la mesure de déplacement et déformation en mécanique expérimentale. >**V**< est un software rapide et efficace pour détecter les points de fuite dans les images non calibrées de scènes urbaines ou intérieures.

2.1.6 Academic reputation and appeal

Prix et distinctions. Nous avons obtenu 18 prix et distinctions : 4 prix de thèse, 2 ERC (starting grant et PoC), 1 IUF, 2 "bug bounties" (sur le vote électronique) , 1 record de calcul, 2 prix L'Oréal-UNESCO et Fullbright, et 8 prix de meilleurs articles. Voir la section "Prizes and Distinctions" page 15 du Portfolio D1-1 pour plus détails.

Invitations et visites. Nous avons été invités à donner des présentations dans au moins 56 évènements internationaux dont 5 " keynote presentations". Voir la section "Invited talks" page 16 du Portfolio D1-1 pour les détails.

E. Thomé a obtenu une bourse Fullbright pour passer une année sabbatique à l'Université de Californie à SanDiego en 2021-2022. A. Guillevic passe une année sabbatique (2021-2022) à l'Université Aarhus Universitet au Danemark. P.-F. Villard a passé un an et demi en année sabbatique (2014-2016) à l'Université Harvard à Cambridge (USA), puis à nouveau 3 fois 1 mois de 2017 à 2019. Il a également passé 3 fois 1 mois de 2017 à 2019 à l'Université d'Uppsala (Suède). De nombreux autres séjours internationaux d'une semaine à un mois ont eu lieu au cours de la période ; Voir la section 2.3.6 Portfolio D1-1 pour les détails.

Les collègues suivants nous ont également rendu visite au cours de la période : Robert Howe (Biorobotics Lab, Cambridge, USA, une semaine), Peter Hammer (Harvard Medical School, Boston, MA, USA, 2 semaines), Douglas Perin (Harvard School of Engineering and Applied Sciences, 2 semaines) semaines), Gert Vegter (Université de Groningue, Pays-Bas, environ 3 fois 1 mois plus 2 semaines), Matthijs Ebbens (Université de Groningue, 1 semaine), Jean-Lou De Carufel et Prosenjit Bose (Carleton Univ., Canada, 1 semaine chacun), Martin Tancer, Vojta Kalusza et Pavel Paták (Université Charles, Canada, 1 semaine chacun). Pavel Paták (Université Charles, Prague, 1 semaine chacun), Andreas Holmsen et Otfried Cheong (KAIST, Corée du Sud, 1 semaine chacun), Zuzanna Patáková (IST Austria, Vienne, 1 semaine) nous ont également rendu visite durant la période d'évaluation.

Projets et contrats. Durant la période 2016-2021, le département a eu, outre les 2 projets ERC (1 starting grant 2012–2017 et 1 Proof of Concept en 2018) et l'IUF junior (2014–2019), 18 projets ANR (dont 8 en tant que coordinateur), ainsi que de nombreuses autres contrats académiques (1 FUI, 2 PEPS, 1 CPER, 1 Région, 1 PIC, 2 projets interdisciplinaires de l'UL, 1 PHC, 1 programme exploratoire Inria, 1 DGA, 1 GDR).

Nous avons également eu 15 contrats avec des entreprises : Docapost, Idemia, NomadicLabs, Canton de Genève, Swiss Post, GE Healthcare, Geometry Factory, AddUp, MapleSoft, Schlumberger, RhinoTerrain, Polygonal Design, CEA, Total, Saint Gobain. Voir la section "Relations with companies and economic players" page 18 du Portfolio D1-1 pour les détails.

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 or were 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.

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 (url).

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).

Local scientific responsibilities. We chair(ed) or co-chair(ed) the followings commitees, panels and diplomas : computer science Master 1st year ; one tracks and one sub-track of the same Master in 2nd year (*Apprentissage, Vision et Robotique* and *Sécurité Informatique, Réseaux et Architectures Virtuelles orientation*) ; Polytech Ingeneer diploma speciality (*Systèmes d'Information et Réseaux*) ; Commission de mention Informatique of the École doctorale IAEM of the University of Lorraine (until 2020) (url) ; Inria "Comipers" hiring committee for PhD and postdoc positions ; two Bachelor diplomas and the fablab "Charlylab" at I.U.T. Nancy-Charlemagne (since 2018) ; German-French virtual center for cybersecurity between LORIA and CISPA (Saarbrucken, Germany) ; LUE impact project DigiTrust (2018-2022).

2.1.7 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 by 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 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.

2.1.8 Long-term academic relations

Collaborations. We have a large set of collaborators with about 460 co-authors outside the lab over the evaluation period. We have many long-term collaborations with French collegues (see the team's reports – Portfolio D1-1 – for details). Among our main international collaborations we cite those with

- N. Heninger from University of California, San Diego on Cryptography [267, 101, 329, 437, 478].
- Gert Vegter (Groningen) [238, 365, 366, 380, 481] and with Jean-Marc Schlenker and Hugo Parlier (Luxembourg) [477, 334] on non-Euclidean computational geometry, through the Inria Associate Team OrbiCG [7] and the international ANR–FNR SoS project. [8]

7. https://members.loria.fr/Monique.Teillaud/collab/Astonishing/
8. https://members.loria.fr/Monique.Teillaud/collab/SoS/

- 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, 482] 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 [320, 321].

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 [352, 358, 65, 261, 457, 378, 195]. The PhD of Remi Decelle is currently co-supervided in this context.

2.2. Référence 2 : La production scientifique est proportionnée au potentiel de recherche de l'équipe et répartie entre ses personnels

2.2.1 Homogénéité de la production scientifique entre les permanents.

Voir DAE labo.

2.2.2 Accompagnement des jeunes chercheurs.

Voir DAE labo.

2.2.3 Accompagnement des chercheurs qui reprennent l'activité recherche.

Voir DAE labo.

2.2.4 Production scientifique des doctorants.

3.5 publications en moyenne par doctorant en fin de thèse.

3. Domaine 4 : Inscription des activités de recherche dans la société

3.1. Référence 1 : L'équipe se distingue par la qualité de ses interactions non-académiques

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 department, as the CEO. It provides meshing solutions based on a technology that we have been

9. https://team.inria.fr/curative/

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.

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.

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).

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

3.2. Référence 2 : L'équipe développe des produits à destination du monde socio-économique

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) [491] relates to computational photomechanics. *Dispositif de traitement de prise de vue* (Tangram) [490] relates to image-based localization from object detections. We also have one patent pending (Caramba).

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 : [485, 486, 488].

MapleSoft. Within our contract with Maple, we started the transfer of our software HEFROOTS for the isolation of the complex roots of a univariate polynomial [431].

Vorpaline is our 3D mesh generation proprietary software distributed by our start-up Tessael.

3.3. Référence 3 : L'équipe partage ses connaissances avec le grand public et intervient dans des débats de société

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 [329] 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 [475, 476].

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.

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.

Références bibliographiques du département 1

Thèses

[1] Arnaud Botella. "Unstructured volumetric meshing of geological models for physical phenomenon Simulations". Thèse de doct. Université de Lorraine, avril 2016. tel-01435058.

[2] Hugo Labrande. "Explicit computation of the Abel-Jacobi map and its inverse". Thèse de doct. Université de Lorraine, novembre 2016. tel-01403849.

[3] Nicolas Aubry. "Segmentation and geometric measurements : application to metal tubular objects". Thèse de doct. Université de Lorraine, juillet 2017. tel-01649874.

[4] Charlotte Delmas. "3D reconstruction of curvilinear micro-devices for interventionnal neuroradiology". Thèse de doct. Université de Lorraine, novembre 2017. tel-01653707.

[5] Jérémie Dumas. "Controllable shape synthesis for digital fabrication". Thèse de doct. Université de Lorraine, février 2017. tel-01547313.

[6] Laurent Grémy. "Sieve algorithms for the discrete logarithm in medium characteristic finite fields". Thèse de doct. Université de Lorraine, septembre 2017. tel-01647623.

[7] Mounia Hendel. "Bio-inspired methods applied to real-time analysis of biomedical signals". Thèse de doct. Université Mohamed Boudiaf des Sciences et de la Technologie - Mohamed Boudiaf d'Oran, février 2017. tel-03042290.

[8] Jean Hergel. "Synthesis of fabricable shape from partial specifications". Thèse de doct. Université de Lorraine, février 2017. tel-01546383.

[9] Pierre Rolin. “Viewpoint synthesis for camera pose initialisation”. Thèse de doct. Université de Lorraine, mars 2017. tel-01536649.

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

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

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

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

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

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

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

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

[18] Erinc Merdivan. “Ambient Assisted Living with Deep Learning”. Thèse de doct. CentraleSupélec, décembre 2019. tel-02927785.

[19] Khadija Musayeva. “Generalization Performance of Margin Multi-category Classifiers”. Thèse de doct. Université de Lorraine, septembre 2019. tel-02387124.

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

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

[22] Vincent Gaudillière. “Visual positioning in a world of objects”. Thèse de doct. Université de Lorraine, juin 2020. tel-02915866.

[23] Paul Huynh. “Design and Analysis of Lightweight Encryption Schemes”. Thèse de doct. Université de Lorraine, novembre 2020. tel-03086269.

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

[25] Antoine Mahé. “System identification with neural networks for model predictive control”. Thèse de doct. CentraleSupélec, Université Paris-Saclay, décembre 2020. tel-03081633.

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

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

[28] Raffaella Trivisonne. “Image-guided Interactive Simulation for Endovascular Surgery”. Thèse de doct. Université de Strasbourg, octobre 2020. tel-03021043.

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

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

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

[32] David Lopez. “Voronoi diagrams and evolving surfaces”. Thèse de doct. Université de Lorraine, octobre 2021. tel-03530955.

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

Habilitations à diriger des recherches

[34] Dmitry Sokolov. “Modelisation geometrique”. Habilitation à diriger des recherches. Université de Lorraine (UL), Vandoeuvre-lès-Nancy, FRA., juin 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, novembre 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), décembre 2017. tel-03029250.

[37] Erwan Kerrien. “Quelques contributions à l’imagerie médicale multimodale et interventionnelle”. Habilitation à diriger des recherches. Université de Lorraine, janvier 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, octobre 2019. tel-02307957.

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

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

Journaux internationaux

[41] Michaël Aron, Marie-Odile Berger, Erwan Kerrien, Brigitte Wrobel-Dautcourt, Blaise Potard et 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 et Sylvain Lazard. "Recognizing Shrinkable Complexes Is NP-Complete". In : *Journal of Computational Geometry* 7.1 (2016), p. 430-443. doi : 10.20382/jocg.v7i1a18. hal-01384396.

[43] Shi Bai, Cyril Bouvier, Alexander Kruppa et 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 et 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), p. 213-232. doi : 10.1002/nme.5212. hal-01255944.

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

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

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

[48] Manuel Caroli et Monique Teillaud. "Delaunay triangulations of closed Euclidean d-orbifolds". In : *Discrete and Computational Geometry* 55.4 (2016), p. 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 et Yuzhen Xie. "The Basic Polynomial Algebra Subprograms". In : *ACM Communications in Computer Algebra* 50.3 (novembre 2016), p. 97-100. doi : 10.1145/3015306.3015312. hal-01404718.

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

[51] Pauline P. Collon, Alexandre Pichat, Charlie Kergaravat, Arnaud Botella, Guillaume Caumon, Jean-Claude Ringenbach et 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 (août 2016), SM17-SM31. doi : 10.1190/INT-2015-0178.1. hal-01342928.

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

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

[54] Eric Domenjoud, Xavier Provençal et Laurent Vuillon. “Palindromic language of thin discrete planes”. In : *Theoretical Computer Science* (2016), p. 101-108. doi : 10.1016/j.tcs.2015.11.023. hal-01262289.

[55] Steven Galbraith et Pierrick Gaudry. “Recent progress on the elliptic curve discrete logarithm problem”. In : *Designs, Codes and Cryptography* 78.1 (2016), p. 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 et 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), p. 580-582. doi : 10.1097/MBC.0000000000000545. hal-03567151.

[57] Pierrick Gaudry, Laurent Grémy et 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), p. 332-350. doi : 10.1112/S1461157016000164. hal-01273045.

[58] Marc Glisse, Sylvain Lazard, Julien Michel et 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 et Benoît Blaysat. “Removing quasi-periodic noise in strain maps by filtering in the Fourier domain”. In : *Experimental Techniques* 40.3 (2016), p. 959-971. doi : 10.1007/s40799-016-0100-2. hal-01163838.

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

[61] Mounia Hendel, Abdelkader Benyettou et 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 (septembre 2016), p. 1-9. doi : 10.1016/j.imu.2016.09.001. hal-03033964.

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

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

[64] Pegah Kamousi, Sylvain Lazard, Anil Maheshwari et Stefanie Wuhrer. “Analysis of Farthest Point Sampling for Approximating Geodesics in a Graph”. In : *Computational Geometry* 57 (août 2016), p. 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 et Fleur Longuetaud. “Un algorithme robuste de segmentation des nœuds du bois sur des images obtenues par tomographie x”. In : *Revue forestière française* 2 (décembre 2016). doi : 10.4267/2042/61869. hal-02987202.

[66] Hugo Labrande. “Computing Jacobi’s θ in quasi-linear time”. In : *Mathematics of Computation* (novembre 2016). arXiv : 1511.04248. doi : 10.1090/mcom/3245. hal-01227699.

[67] Hugo Labrande et 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 (août 2016), p. 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, p. 80-83. doi : 10.1016/j.automatica.2016.07.027. hal-01219794.

[69] Jonàs Martínez, Jérémie Dumas et Sylvain Lefebvre. “Procedural Voronoi Foams for Additive Manufacturing”. In : *ACM Transactions on Graphics* 35 (2016), p. 1-12. doi : 10.1145/2897824.2925922. hal-01393741.

[70] Guillaume Moroz et Boris Aronov. “Computing the Distance between Piecewise-Linear Bivariate Functions”. In : *ACM Transactions on Algorithms* 12.1 (février 2016), 3:1-3:13. doi : 10.1145/2847257. hal-01112394.

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

[72] Dmitry Sokolov, Nicolas Ray, Lionel Untereiner et Bruno Lévy. “Hexahedral-Dominant Meshing”. In : *ACM Transactions on Graphics* 35.5 (2016), p. 1-23. doi : 10.1145/2930662. hal-01397846.

[73] Hai-Chuan Song, Nicolas Ray, Dmitry Sokolov et Sylvain Lefebvre. “Anti-aliasing for fused filament deposition”. In : *Computer-Aided Design* 89 (septembre 2016). arXiv : 1609.03032 - 14 pages, 22 figures, p. 25-34. doi : 10.1016/j.cad.2017.04.001. hal-01400686.

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

[75] Frédéric Sur et 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), p. 472-498. doi : 10.1007/s10851-016-0650-z. hal-01298523.

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

[77] Marc Alexa, Kristian Hildebrand et Sylvain Lefebvre. “Optimal discrete slicing”. In : *ACM Transactions on Graphics* 36.1 (février 2017), p. 1-16. doi : 10.1145/2999536. hal-01660773.

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

[79] Razvan Barbulescu et Armand Lachand. “Some mathematical remarks on the polynomial selection in NFS”. In : *Mathematics of Computation* 86 (2017). arXiv : 1403.0184, p. 397-418. doi : 10.1090/mcom/3112. hal-00954365.

[80] Dobrina Boltcheva et Bruno Levy. “Surface reconstruction by computing restricted Voronoi cells in parallel”. In : *Computer-Aided Design* 90 (septembre 2017), p. 123-134. doi : 10.1016/j.cad.2017.05.011. hal-01596553.

[81] Weikai Chen, Yuexin Ma, Sylvain Lefebvre, Shiqing Xin, Jonàs Martínez et 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 et Monique Teillaud. “Qualitative Symbolic Perturbation : Two Applications of a New Geometry-based Perturbation Framework”. In : *Journal of Computational Geometry* 8.1 (2017), p. 282-315. doi : 10.20382/jocg.v8i1a11. hal-01586511.

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

[84] Michel Grédiac, Benoît Blaysat et Frédéric Sur. “A Critical Comparison of Some Metrological Parameters Characterizing Local Digital Image Correlation and Grid Method”. In : *Experimental Mechanics* 57.6 (2017), p. 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 (novembre 2017), p. 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 et Jean F. DUBOUSSET. “The horizontal plane appearances of scoliosis : what information can be obtained from top-view images ?” In : *International Orthopaedics* 41.11 (2017), p. 2303-2311. doi : 10.1007/s00264-017-3548-5. hal-01665134.

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

[89] Masahiro Ishii, Jérémie Detrey, Pierrick Gaudry, Atsuo Inomata et 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 (décembre 2017), p. 2019-2030. doi : 10.1109/TC.2017.2704082. hal-01299697.

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

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

[92] Benjamin Levy, Cécile Prudent, Florian Liétard et 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 et 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 et Dmitry Sokolov. “Improving control engineering education with TRIK cybernetic system”. In : *IFAC-PapersOnLine* 50.1 (juillet 2017), p. 15716-15721. doi : 10.1016/j.ifacol.2017.08.2412. hal-01658734.

[95] Jonàs Martínez, Haichuan Song, Jérémie Dumas et Sylvain Lefebvre. “Orthotropic k-nearest foams for additive manufacturing”. In : *ACM Transactions on Graphics* 36.4 (juillet 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 (janvier 2017), p. 117-129. doi : 10.1007/s10623-016-0206-7. hal-01593371.

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

[98] Phuc Ngo, Yukiko Kenmochi, Akihiro Sugimoto, Hugues Talbot et Nicolas Passat. “Discrete rigid registration : A local graph-search approach”. In : *Discrete Applied Mathematics* 216.2 (2017), p. 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 et 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 et Michel Grediac. “Towards Computational Photomechanics”. In : *ERCIM News* 108 (janvier 2017), p. 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 et Paul Zimmermann. “Imperfect forward secrecy : How Diffie-Hellman fails in practice”. In : *Communications of the ACM* 62.1 (décembre 2018), p. 106-114. doi : 10.1145/3292035. hal-01982426.

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

[103] Frederic Bihan, Francisco Santos et 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, p. 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 (octobre 2018), p. 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 et Stephen Wismath. “Monotone Simultaneous Paths Embeddings in $\mathbb{R}^d$”. In : *Discrete Mathematics and Theoretical Computer Science* Vol. 20 no. 1.1 (janvier 2018), p. 1-11. doi : 10.23638/DMTCS-20-1-1. hal-01529154.

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

[107] Luca Castelli Aleardi, Olivier Devillers et 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), p. 391-429. doi : 10.20382/jocg.v9i1a14. hal-01959590.

[108] Nicolas Chenavier et Olivier Devillers. “Stretch Factor in a Planar Poisson-Delaunay Triangulation with a Large Intensity”. In : *Advances in Applied Probability* 50.1 (2018), p. 35-56. doi : 10.1017/apr.2018.3. hal-01700778.

[109] Chengkai Dai, Charlie C.L. Wang, Chenming Wu, Sylvain Lefebvre, Guoxin Fang et Yong-Jin Liu. “Support-free volume printing by multi-axis motion”. In : *ACM Transactions on Graphics* 37.4 (juillet 2018), p. 1-14. doi : 10.1145/3197517.3201342. hal-01887571.

[110] Olivier Devillers et 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), p. 255-269. doi : 10.1142/S0218195918500061. hal-01712628.

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

[112] Isabelle Dumand, Christophe Clesse, Samira Salime, Florian Liétard, Michel Decker, Joëlle Lighezzolo-Alnot et 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), p. 439-448. doi : 10.1684/pnv.2018.0761. hal-02004800.

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

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

[115] Tamás Illés, Máté Burkus, Szabolcs Somoskeöy, Fabien Lauer, François Lavaste et 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), p. 2120-2129. doi : 10.1007/s00586-018-5577-1. hal-02060150.

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

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

[118] Wouter Kuijper, Victor Ermolaev et Olivier Devillers. “Celestial Walk : A Terminating, Memoryless Walk for Convex Subdivisions”. In : *Journal of Computer Graphics Techniques* 7.3 (2018), p. 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, p. 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), p. 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, p. 317-323. doi : 10.1016/j.patrec.2018.08.004. hal-01815451.

[122] Friederike Laus, Fabien Pierre et Gabriele Steidl. “Nonlocal Myriad Filters for Cauchy Noise Removal”. In : *Journal of Mathematical Imaging and Vision* (avril 2018). arXiv : 1710.03015, p. 1-31. doi : 10.1007/s10851-018-0816-y. hal-01814104.

[123] Bruno Lévy et Erica Schwindt. “Notions of optimal transport theory and how to implement them on a computer”. In : *Computers and Graphics* (février 2018), p. 1-22. doi : 10.1016/j.cag.2018.01.009. hal-01717967.

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

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

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

[127] Nicolas Ray, Dmitry Sokolov, Sylvain Lefebvre et Bruno Lévy. “Meshless Voronoi on the GPU”. In : *ACM Transactions on Graphics* 37.6 (décembre 2018), p. 1-12. doi : 10.1145/3272127.3275092. hal-01927559.

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

[129] Frédéric Sur, Benoît Blaysat et Michel Grediac. “Rendering Deformed Speckle Images with a Boolean Model”. In : *Journal of Mathematical Imaging and Vision* 60.5 (2018), p. 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 et 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 et Xiaohu Guo. “Computing a high-dimensional euclidean embedding from an arbitrary smooth riemannian metric”. In : *ACM Transactions on Graphics* 37.4 (août 2018), p. 1-16. doi : 10.1145/3197517.3201369. hal-03214192.

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

[133] Stanislav Aranovskiy, Andrei Biryuk, Evgeny V. Nikulchev, Igor Ryadchikov et 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 (mars 2019), p. 297-304. doi : 10.1134/S1064230719020023. hal-02282919.

[134] Stanislav Aranovskiy, Romeo Ortega, Jose Guadalupe Romero et 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 (juillet 2019), p. 1620-1633. doi : 10.1080/00207179.2017.1404130. hal-01658753.

[135] Boris Bukh et Xavier Goaoc. “Shatter functions with polynomial growth rates”. In : *SIAM Journal on Discrete Mathematics* 33.2 (2019). arXiv : 1701.06632, p. 784-794. doi : 10.1137/17M1113680. hal-02050524.

[136] Svyatoslav Covanov et Emmanuel Thomé. “Fast integer multiplication using generalized Fermat primes”. In : *Mathematics of Computation* 88.317 (2019). arXiv : 1502.02800, p. 1449-1477. doi : 10.1090/mcom/3367. hal-01108166.

[137] Jesús A. De Loera, Xavier Goaoc, Frédéric Meunier et 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, p. 415-511. doi : 10.1090/bull/1653. hal-02050466.

[138] Vincent Despré et Francis Lazarus. “Computing the Geometric Intersection Number of Curves”. In : *Journal of the ACM (JACM)* 66.6 (novembre 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 $O(n + \ell \log \ell)$, p. 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 et Sylvain Lefebvre. “CurviSlicer : Slightly curved slicing for 3-axis printers”. In : *ACM Transactions on Graphics* 38.4 (août 2019), p. 1-11. doi : 10.1145/3306346.3323022. hal-02120033.

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

[141] Xavier Goaoc, Pavel Paták, Zuzana Patáková, Martin Tancer et Uli Wagner. “Shellability is NP-complete”. In : *Journal of the ACM (JACM)* 66.3 (juin 2019). arXiv : 1711.08436, p. 1-18. doi : 10.1145/3314024. hal-02050505.

[142] Michel Grediac, Benoît Blaysat et 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), p. 219-243. doi : 10.1007/s11340-018-00461-4. hal-01926058.

[143] Michel Grediac, Benoît Blaysat et Frédéric Sur. “Extracting displacement and strain fields from checkerboard images with the Localized Spectrum Analysis”. In : *Experimental Mechanics* 59.2 (2019), p. 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 (janvier 2019). arXiv : 1809.06135, p. 1273-1301. doi : 10.1090/mcom/3376. hal-01341849.

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

[146] Sylvain Lazard, William Lenhart et Giuseppe Liotta. “On the Edge-length Ratio of Outerplanar Graphs”. In : *Theoretical Computer Science* 770 (2019), p. 88-94. doi : 10.1016/j.tcs.2018.10.002. hal-01886947.

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

[148] Erinc Merdivan, Deepika Singh, Sten Hanke et Andreas Holzinger. “Dialogue Systems for Intelligent Human Computer Interactions”. In : *Electronic Notes in Theoretical Computer Science* 343 (mai 2019), p. 57-71. doi : 10.1016/j.entcs.2019.04.010. hal-03081682.

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

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

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

[152] Haichuan Song, Jonàs Martínez, Pierre Bedell, Noemie Vennin et Sylvain Lefebvre. “Colored fused filament fabrication”. In : *ACM Transactions on Graphics* 38.5 (juin 2019), p. 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), p. 1882-1894. doi : 10.1109/TIP.2018.2881906. hal-01925890.

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

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

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

[157] L. Wendling, I Debled-Rennesson et H. Nasser. “Multilevel Polygonal Descriptor Matching Defined By Combining Discrete Lines And Force Histogram Concepts”. In : *Multimedia Tools and Applications* (avril 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 (avril 2020), p. 101440. doi : 10.1016/j.jco.2019.101440. hal-01905580.

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

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

[161] Imre Barany, Matthieu Fradelizi, Xavier Goaoc, Alfredo Hubard et Günter Rote. “Random polytopes and the wet part for arbitrary probability distributions”. In : *Annales Henri Lebesgue* 3 (2020). arXiv : 1902.06519, p. 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* (juin 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* (mars 2020). doi : 10.26151/espacestemps.net-vmak-xq38. hal-02549867.

[164] Benoît Blaysat, Jan Neggers, Michel Grediac et 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), p. 393-407. doi : 10.1007/s11340-019-00566-4. hal-02436541.

[165] Jean-Daniel Boissonnat, Olivier Devillers, Kunal Dutta et 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 et Dmitry Sokolov. “Topological-based roof modeling from 3D point clouds”. In : *Journal of WSCG* 28.1-2 (2020), p. 137-146. doi : 10.24132/JWSCG.2020.28.17. hal-02983073.

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

[168] Hamid Boukerrou, Paul Huynh, Virginie Lallemand, Bimal Mandal et 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 (mai 2020), p. 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 et Alexander Wolff. “Bundled Crossings Revisited”. In : *Journal of Graph Algorithms and Applications* (juin 2020). doi : 10.7155/jgaa.00534. hal-02972975.

[170] Guillaume Coiffier, Philippe Renard et Sylvain Lefebvre. “3D Geological Image Synthesis From 2D Examples Using Generative Adversarial Networks”. In : *Frontiers in Water* 2 (octobre 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 et Gilles Dolivet. “ICG-induced NIR fluorescence mapping in patients with head & neck tumors after the previous radiotherapy”. In : *Photodiagnosis and Photodynamic Therapy* 31 (septembre 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), p. 3831-3842. doi : 10.1016/j.procs.2020.09.337. hal-03284184.

[173] Alfredo Cuzzocrea, Carson K Leung, Bryan H Wodi, S Sourav et 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), p. 509-515. doi : 10.1016/j.procs.2020.10.070. hal-03274605.

[174] Alfredo Cuzzocrea, Enzo Mumolo, Edoardo Fadda et 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), p. 978-991. doi : 10.1007/978-3-030-58799-4_70. hal-03274600.

[175] Nicolas David et 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), p. 315-325. doi : 10.1090/CONM/754/15139. hal-02151093.

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

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

[178] Vincent Gaudillière, Gilles Simon et 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 (octobre 2020), p. 5189-5196. doi : 10.1109/LRA.2020.3005387. hal-02886633.

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

[180] Michel Grediac, Benoît Blaysat et 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 et Frédéric Sur. “On the Optimal Pattern for Displacement Field Measurement : Random Speckle and DIC, or Checkerboard and LSA ?” In : *Experimental Mechanics* 60.4 (2020), p. 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 (décembre 2020), p. 17995-18008. doi : 10.1007/s00521-018-3873-7. hal-02377345.

[183] Aurore Guillevic, Simon Masson et Emmanuel Thomé. “Cocks-Pinch curves of embedding degrees five to eight and optimal ate pairing computation”. In : *Designs, Codes and Cryptography* 88.6 (mars 2020), p. 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 et Sylvain Lefebvre. “Variable-width contouring for additive manufacturing”. In : *ACM Transactions on Graphics* 39.4 (Proc. SIGGRAPH) (juillet 2020). doi : 10.1145/3386569.3392448. hal-02568677.

[185] Tamás Illés, Stig M. Jespersen, Pieter Reynders, Fabien Lauer, J.-C. Le Huec et 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), p. 2000-2009. DOI : 10.1007/s00586-020-06390-y. hal-03382549.

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

[187] Sorina Ionica et Emmanuel Thomé. “Isogeny graphs with maximal real multiplication”. In : *Journal of Number Theory* 207 (février 2020). arXiv : 1407.6672, p. 385-422. DOI : 10.1016/j.jnt.2019.06.019. hal-00967742.

[188] Benedikt Kolbe et Myfanwy Evans. “Isotopic tiling theory for hyperbolic surfaces”. In : *Geometriae Dedicata* (juillet 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, p. 1183-1195. DOI : 10.1109/TNNLS.2019.2919444. hal-01566136.

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

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

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

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

[194] Madhurima Mukhopadhyay, Palash Sarkar, Shashank Singh et 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 et Francis Colin. “A Machine-Learning Approach for Classifying Defects on Tree Trunks using Terrestrial LiDAR”. In : *Computers and Electronics in Agriculture* 171 (avril 2020), p. 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 et Sylvain Lefebvre. “Freely orientable microstructures for designing deformable 3D prints”. In : *ACM Transactions on Graphics* 39.6 (décembre 2020), p. 1-16. DOI : 10.1145/3414685.3417790. hal-02524371.

[197] Raffaella Trivisonne, Erwan Kerrien et 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 (février 2020). DOI : 10.1016/j.compmedimag.2020.101702. hal-02469093.

[198] Félix Vanneste, Olivier Goury, Jonas Martinez, Sylvain Lefebvre, Hervé Delingette et 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 (janvier 2020), p. 2380-2386. doi : 10.1109/LRA.2020.2969926. hal-02475589.

[199] Jian Wang, Stanislav Aranovskiy, Emilia Fridman, Dmitry Sokolov, Denis Efimov et 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 et Wenyong Wang. “WatchPose : A View-Aware Approach for Camera Pose Data Collection in Industrial Environments”. In : *Sensors* 20.11 (mai 2020). doi : 10.3390/s20113045. hal-02735272.

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

[202] Max Alekseyev, Joseph Samuel Myers, Richard Schroeppel, Scott R Shannon, Neil James Alexander Sloane et 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 et Alexey Bobtsov. “Switched Observer Design For a Class of Locally Unobservable Time-Varying Systems”. In : *Automatica* 130 (août 2021), p. 109715. doi : 10.1016/j.automatica.2021.109715. hal-03273675.

[204] Melike Aydinlilar et Cédric Zanni. “Fast ray tracing of scale-invariant integral surfaces”. In : *Computer Graphics Forum* 40.6 (septembre 2021), p. 117-134. doi : 10.1111/cgf.14208. hal-03169283.

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

[206] Enka Blanchard, Zacharie Boubli et Charlotte Lemaistre. “La Covid au prisme des minorités vulnérables”. In : *EspacesTemps.net* (février 2021). doi : 10.26151/espacestemps.net-1978-7z05. hal-03133414.

[207] Xavier Bonnetain et Samuel Jaques. “Quantum Period Finding against Symmetric Primitives in Practice”. In : *IACR Transactions on Cryptographic Hardware and Embedded Systems* 2022.1 (novembre 2021), p. 1-27. doi : 10.46586/tches.v2022.i1.1-27. hal-03431518.

[208] Charles Bouillaguet et Paul Zimmermann. “Parallel Structured Gaussian Elimination for the Number Field Sieve”. In : *Mathematical Cryptology* 0.1 (janvier 2021), p. 22-39. hal-02098114.

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

[210] Olivier Bronchain, Sebastian Faust, Virginie Lallemand, Gregor Leander, Léo Perrin et François-Xavier Standaert. “MOE : Multiplication Operated Encryption with Trojan Resilience”. In : *IACR Transactions on Symmetric Cryptology* 2021.1 (mars 2021), p. 78-129. doi : 10.46586/tosc.v2021.i1.78-129. hal-03453550.

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

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

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

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

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

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

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

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

[219] Xavier Goaoc, Andreas Holmsen et 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 (janvier 2021). arXiv : 1903.03014, p. 131-161. doi : 10.20382/jocg.v11i2a6. hal-03152958.

[220] Aurore Guillevic et Shashank Singh. “On the Alpha Value of Polynomials in the Tower Number Field Sieve Algorithm”. In : *Mathematical Cryptology* 1.1 (février 2021), p. 1-39. hal-02263098.

[221] Myriam Guillevic, Aurore Guillevic, Martin K Vollmer, Paul Schlauri, Matthias Hill, Lukas Emmenegger et 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 (octobre 2021). arXiv : 2103.13807 - There is a supplement (PDF document) with figures and four ZIP archive files., p. 1-27. doi : 10.1186/s13321-021-00544-w. hal-03176025.

[222] Damien Jamet, Pierre Popoli et 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* (juillet 2021). arXiv : 2106.09959. doi : 10.1007/s12095-021-00507-w. hal-03283528.

[223] George Krait, Sylvain Lazard, Guillaume Moroz et 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 (octobre 2021), p. 113553. doi : 10.1016/j.cam.2021.113553. hal-03161393.

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

[225] Bruno Lévy, Roya Mohayaee et 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 (juin 2021). arXiv : 2012.09074, p. 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 (juin 2021). doi : 10.1016/j.cad.2021.103069. hal-02911788.

[227] Daryna Panicheva, Pierre-Frédéric Villard, Peter E Hammer, Douglas Perrin et 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 (mai 2021), p. 709-720. doi : 10.1007/s11548-021-02368-3. hal-03262496.

[228] Fabien Pierre, Mathieu Amendola, Clémence Bigeard, Timothé Ruel et Pierre-Frédéric Villard. “Segmentation with Active Contours”. In : *Image Processing On Line* 11 (mai 2021), p. 120-141. doi : 10.5201/ipol.2021.298. hal-03235096.

[229] Siyi Qin, Michel Grédiac, Benoît Blaysat, Shaopeng Ma et 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 (mars 2021), p. 108570. doi : 10.1016/j.measurement.2020.108570. hal-02965328.

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

[231] Nathan J. Secrest, Sebastian von Hausegger, Mohamed Rameez, Roya Mohayaee, Subir Sarkar et 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 (juillet 2021). (SIGGRAPH 2021). doi : 10.1145/3465623. hal-03287031.

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

Conférences invitées

[234] Walter C.P.M. Blondel, Faiza Abdat, Marine Amouroux et 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, novembre 2017. hal-01637378.

[235] Véronique Cortier, Pierrick Gaudry et Stephane Glondu. “Belenios : a simple private and verifiable electronic voting system”. In : *Foundations of Security, Protocols, and Equational Reasoning*. Sous la dir. de Joshua D. Guttman, Carl E. Landwehr, José Meseguer et Dusko Pavlovic. T. 11565. LNCS. Fredericksburg, Virgina, United States : Springer, 2019, p. 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, mars 2020. hal-02510046.

Conférences internationales majeures

[237] Benoît Blaysat, Michel Grédiac et Frédéric Sur. “Assessing the Metrological Performance of DIC Applied on RGB Images”. In : *iDICS 2016 Conference*. Sous la dir. de M. Sutton et P. Reu. Proceedings of the first Conference of the International Digital Imaging Correlation Society. Philadelphia, United States : Springer, novembre 2016, p. 109-111. doi : 10.1007/978-3-319-51439-0_26. hal-01500324.

[238] Mikhail Bogdanov, Monique Teillaud et Gert Vegter. “Delaunay triangulations on orientable surfaces of low genus”. In : *32nd International Symposium on Computational Geometry*. Boston, United States, juin 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 et Stephen Wismath. “Monotone Simultaneous Paths Embeddings in $\mathbb{R}^d$”. In : *24th International Symposium on Graph Drawing & Network Visualization*. T. 9801. Proceedings of 24th International Symposium on Graph Drawing & Network Visualization. arXiv : 1608.08791. Athens, Greece : Springer, septembre 2016. hal-01366148.

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

[241] Charlotte Delmas, Cyril Riddell, Yves Trousset, Erwan Kerrien, Marie-Odile Berger, René Anxionnat et 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, juillet 2016. hal-01303153.

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

[243] Jean-Guillaume Dumas, Erich Kaltofen, Emmanuel Thomé et 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, juillet 2016, p. 199-206. DOI : 10.1145/2930889.2930908. hal-01266041.

[244] Ninon Eyrolles, Louis Goubin et Marion Videau. “Defeating MBA-based Obfuscation”. In : *2nd International Workshop on Software PROtection*. Sous la dir. d'ACM. Vienna, Austria, octobre 2016. DOI : 10.1145/2995306.2995308. hal-01388109.

[245] Jean-Charles Faugère, Pierre-Jean Spaenlehauer et 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, juillet 2016, p. 223-230. DOI : 10.1145/2930889.2930927. hal-01314651.

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

[247] Aurore Guillevic, François Morain et Emmanuel Thomé. “Solving discrete logarithms on a 170-bit MNT curve by pairing reduction”. In : *Selected Areas in Cryptography – SAC 2016*. Sous la dir. de Roberto Avanzi et Howard Heys. T. 10532. Lecture Notes in Computer Science. arXiv : 1605.07746. St. Johns, Newfoundland, Canada : Springer, août 2016, p. 559-578. DOI : 10.1007/978-3-319-69453-5_30. hal-01320496.

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

[249] Nazim Haouchine, Marie-Odile Berger et 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, septembre 2016. hal-01353189.

[250] Ranjan Jha, Damien Chablat, Fabrice Rouillier et 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, août 2016. hal-01309190.

[251] Bertrand Kerautret, Adrien Krähenbühl, Isabelle Debled-Rennesson et 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, décembre 2016. doi : 10.1109/ICPR.2016.7899829. hal-01435271.

[252] Marine Minier et Raphael C.-W. Phan. “Tuple Cryptanalysis : Slicing and Fusing Multisets”. In : *Paradigms in Cryptology – Mycrypt 2016*. Sous la dir. de Raphael C.-W. Phan et Moti Yung. T. 10311. Lecture Notes in Computer Science. Kuala Lumpur, Malaysia : Springer, décembre 2016, p. 294-320. doi : 10.1007/978-3-319-61273-7. hal-01593382.

[253] Guillaume Moroz et Éric Schost. “A Fast Algorithm for Computing the Truncated Resultant”. In : *ISSAC ’16*. Sous la dir. de 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, juillet 2016, p. 341-348. doi : 10.1145/2930889.2930931. hal-01366386.

[254] Phuc Ngo, Hayat Nasser, Isabelle Debled-Rennesson et Bertrand Kerautret. “Adaptive Tangential Cover for Noisy Digital Contours”. In : *DGCI 2016 - 19th international conference on Discrete Geometry for Computer Imagery*. T. LNCS 9647. DGCI 2016 : Discrete Geometry for Computer Imagery. Nantes, France, avril 2016, p. 439-451. doi : 10.1007/978-3-319-32360-2_34. hal-01266033.

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

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

[257] Nicolas Ray, Dmitry Sokolov et Bruno Lévy. “Practical 3D frame field generation”. In : *SIGGRAPH ASIA 2016*. T. 35. macao, Macau SAR China, décembre 2016, p. 1-9. hal-01397711.

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

[259] Mohab Safey El Din et 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, juillet 2016, p. 183-190. doi : 10.1145/2930889.2930929. hal-01312750.

[260] Gilles Simon, Antoine Fond et 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, mai 2016. hal-01275628.

[261] - Van-Tho Nguyen, Bertrand Kerautret, Isabelle Debled-Rennesson, Francis Colin, Alexandre Piboule et 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, décembre 2016, p. 6. hal-02740896.

[262] Yinoussa Adagolodjo, Raffaella Trivisonne, Nazim Haouchine, Stéphane Cotin et 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, septembre 2017. hal-01578815.

[263] Mohammad Alaggan, Mathieu Cunche et 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, mars 2017. hal-01485412.

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

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

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

[267] Joshua Fried, Pierrick Gaudry, Nadia Heninger et Emmanuel Thomé. “A kilobit hidden SNFS discrete logarithm computation”. In : *Advances in Cryptology – EUROCRYPT 2017*. Sous la dir. de Jean-Sébastien Coron et Jesper Buus Nielsen. T. 10210. Lecture Notes in Computer Science. arXiv : 1610.02874. Paris, France : Springer, avril 2017, p. 202-231. doi : 10.1007/978-3-319-56620-7_8. hal-01376934.

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

[269] David Gerault, Marine Minier et 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, août 2017, p. 4844-4848. hal-01528272.

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

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

[272] Bertrand Kerautret, Phuc Ngo, Yukiko Kenmochi et Antoine Vacavant. “Greyscale Image Vectorization from Geometric Digital Contour Representations”. In : *DGCI'17 - 20th International Conference on Discrete Geometry for Computer Imagery*. T. 34. Vienna, Austria, septembre 2017, p. 2379-331. DOI : 10.1007/978-3-319-66272-5_26. hal-01588695.

[273] Sofiane Lagraa, Jerome Francois, Abdelkader Lahmadi, Marine Minier, Christian Hammerschmidt et 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, octobre 2017. hal-01636480.

[274] Sylvain Lazard, William Lenhart et 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.

[275] Vincent Lefèvre et Paul Zimmermann. “Optimized Binary64 and Binary128 Arithmetic with GNU MPFR”. In : *24th IEEE Symposium on Computer Arithmetic (ARITH 24)*. Sous la dir. de Neil Burgess, Javier Bruguera et Florent de Dinechin. London, United Kingdom, juillet 2017, p. 18-26. DOI : 10.1109/ARITH.2017.28. hal-01502326.

[276] Anush Manukyan, Olivares-Mendez Miguel, Holger Voos et 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.

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

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

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

[280] Simon Perdrix et 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, septembre 2017. DOI : 10.1007/978-3-662-55751-8_31. hal-01377339.

[281] Deepika Singh, Erinc Merdivan, Ismini Psychoula, Johannes Kropf, Sten Hanke, Matthieu Geist et Andreas Holzinger. “Human activity recognition using recurrent neural networks”. In : *1st International Cross-Domain Conference for Machine Learning and Knowledge Extraction (CD-MAKE)*. Sous la dir. d'Andreas Holzinger, Peter Kieseberg, A Min Tjoa et Edgar Weippl. T. LNCS-10410. Machine Learning and Knowledge Extraction. Part 5 : MAKE AAL. Reggio, Italy : Springer International Publishing, août 2017, p. 267-274. DOI : 10.1007/978-3-319-66808-6_18. hal-01629704.

[282] Aaron Sujar, Andreas Meuleman, Pierre-Frédéric Villard, Marcos Garcia et Franck P. Vidal. “gVirtualXRay : Virtual X-Ray Imaging Library on GPU”. In : *Computer Graphics and Visual Computing*. Sous la dir. de Tao Ruan Wan et Franck Vidal. Computer Graphics and Visual Computing. Manchester, United Kingdom : The Eurographics Association, septembre 2017, p. 61-68. doi : 10.2312/cgvc.20171279. hal-01588532.

[283] Raffaella Trivisonne, Erwan Kerrien et Stéphane Cotin. “Augmented 3D Catheter Navigation using Constrained Shape from Template”. In : *Hamlyn Symposium*. London, United Kingdom, juin 2017. hal-01545693.

[284] Antoine Vacavant, Bertrand Kerautret, Tristan Roussillon et 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*. T. 10502. Lecture Notes in Computer Science. Vienna, Austria : Springer, septembre 2017, p. 291-303. doi : 10.1007/BFb0038202. hal-01621504.

[285] Simon Abelard, Pierrick Gaudry et 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, juillet 2018, p. 1-19. hal-01816256.

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

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

[288] Jaime Garcia Guevara, Igor Peterlik, Marie-Odile Berger et 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, juin 2018. hal-01761538.

[289] Vincent Gaudillière, Gilles Simon et 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, octobre 2018, p. 898-902. doi : 10.1109/ICIP.2018.8451244. hal-01802596.

[290] Michel Grediac, Benoît Blaysat et Frédéric Sur. “Speckles and DIC or Checkerboards and LSA ?” In : *SEM Annual Conference & Exposition on Experimental and Applied Mechanics*. Sous la dir. de Luciano Lamberti, Ming-Tzer Lin, Cosme Furlong, Cesar Sciammarella, Phillip L. Reu et Michael A Sutton. T. 3. Greenville, United States : Springer, juin 2018, p. 79-80. doi : 10.1007/978-3-319-97481-1_9. hal-01896817.

[291] Claude-Pierre Jeannerod, Jean-Michel Muller et 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, juin 2018, p. 53-60. doi : 10.1109/ARITH.2018.8464793. hal-01774587.

[292] Antoine Mahé, Cédric Pradalier et 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, octobre 2018. doi : 10.1109/ICSTCC.2018.8540719. hal-01927035.

[293] Khadija Musayeva, Fabien Lauer et 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, avril 2018, p. 503-508. hal-03011325.

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

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

[296] Ismini Psychoula, Erinc Merdivan, Deepika Singh, Liming Chen, Feng Chen, Sten Hanke, Johannes Kropf, Andreas Holzinger et 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, mars 2018, p. 710-715. doi : 10.1109/PERCOMW.2018.8480247. hal-03081669.

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

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

[299] Michael Scott et Aurore Guillevic. “A New Family of Pairing-Friendly elliptic curves”. In : *International Workshop on the Arithmetic of Finite Fields - WAIFI*. Sous la dir. de Lilya Budaghyan et Francisco Rodriguez-Henríquez. T. 11321. LNCS. Lilya Budaghyan and Tor Helleseth. Bergen, Norway : Springer, juin 2018, p. 43-57. doi : 10.1007/978-3-030-05153-2_2. hal-01875361.

[300] Gilles Simon, Antoine Fond et 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, septembre 2018, p. 323-338. hal-01865251.

[301] Frédéric Sur, Benoît Blaysat et Michel Grediac. “Speckle Image Rendering for DIC Performance Assessment”. In : *SEM Annual Conference & Exposition on Experimental and Applied Mechanics*. Sous la dir. de Luciano Lamberti, Ming-Tzer Lin, Cosme Furlong, Cesar Sciammarella, Phillip L. Reu et Michael A Sutton. T. 3. Greenville, United States : Springer, juin 2018, p. 75-77. doi : 10.1007/978-3-319-97481-1_8. hal-01896811.

[302] Jose Terius-Padron, Georgios Kapidis, Sarah Fallmann, Erinc Merdivan, Sten Hanke, Rebeca Garcia-Betances et 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, mars 2018, p. 776-781. doi : 10.1109/PERCOMW.2018.8480163. hal-03081677.

[303] Elena Andreeva, Virginie Lallemand, Antoon Purnal, Reza Reyhanitabar, Arnab Roy et 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, décembre 2019, p. 153-182. doi : 10.1007/978-3-030-34621-8_6. hal-02388234.

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

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

[306] Luca De Feo, Simon Masson, Christophe Petit et 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*. T. 1. Advances in Cryptology - ASIACRYPT 2019. Kobe, Japan, décembre 2019, p. 248-277. doi : 10.1007/978-3-030-34578-5_10. hal-02388349.

[307] Patrick Derbez, Virginie Lallemand et Aleksei Udovenko. “Cryptanalysis of SKINNY in the Framework of the SKINNY 2018-2019 Cryptanalysis Competition”. In : *SAC 2019 - Selected Areas in Cryptography*. Waterloo, Canada, août 2019. hal-02388239.

[308] Jérémie Detrey et Laurent Imbert. “Breaking randomized mixed-radix scalar multiplication algorithms”. In : *LATINCRYPT 2019 - 6th International Conference on Cryptology and Information Security in Latin America*. T. 11774. Lecture Notes in Computer Science. Santiago de Chile, Chile, octobre 2019, p. 24-39. doi : 10.1007/978-3-030-30530-7_2. lirmm-02309203.

[309] Sény Diatta, Guillaume Moroz et 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, novembre 2019. hal-02406758.

[310] Eric Domenjoud, Bastien Laboureix et 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, mars 2019, p. 38-50. doi : 10.1007/978-3-030-14085-4_4. hal-02316870.

[311] Philippe Even, Phuc Ngo et Bertrand Kerautret. “Thick Line Segment Detection with Fast Directional Tracking”. In : *ICIAP 2019 -20th International Conference on Image Analysis and Processing*. Sous la dir. d’E. Ricci et al. LNCS 11752. trento, Italy : Springer, septembre 2019, p. 159-170. doi : 10.1007/978-3-030-30645-8_15. hal-02189916.

[312] Vincent Gaudillière, Gilles Simon et 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, novembre 2019. doi : 10.1109/IROS40897.2019.8968180. hal-02181962.

[313] Vincent Gaudillière, Gilles Simon et 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, octobre 2019, p. 19-29. doi : 10.1109/ISMAR.2019.00017. hal-02170784.

[314] Xavier Goaoc, Andreas Holmsen et 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.

[315] Rémi Imbach, Marc Pouget et 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, août 2019. hal-01825708.

[316] Antoine Mahé, Antoine Richard, Benjamin Mouscadet, Cedric Pradalier et 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.

[317] Erinc Merdivan, Anastasios Vafeiadis, Dimitrios Kalatzis, Sten Hanke, Joahannes Kroph, Konstantinos Votis, Dimitrios Giakoumis, Dimitrios Tzovaras, Liming Chen, Raouf Hamzaoui et 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, août 2019, p. 144-149. doi : 10.1109/SmartWorld-UIC-ATC-SCALCOM-IOP-SCI.2019.00066. hal-03081713.

[318] Thomas Mouzon, Fabien Pierre et 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, juin 2019, p. 535-546. hal-02059820.

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

[320] Daryna Panicheva, Pierre-Frédéric Villard et Marie-Odile Berger. “Toward an automatic segmentation of mitral valve chordae”. In : *SPIE Medical Imaging*. Sous la dir. de Barjor Gimi et Andrzej Kro. T. 10953. SPIE. San Diego, United States, février 2019, p. 1095315-1095323. doi : 10.1117/12.2511943. hal-02050846.

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

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

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

[324] Arthur Renaudeau, François Lauze, Fabien Pierre, Jean-François Aujol et 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, juin 2019. hal-02433997.

[325] Igor Ryadchikov, Stanislav Aranovskiy, Evgeny Nikulchev, Jian Wang et 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, septembre 2019. hal-02383471.

[326] Deng Tang, Bimal Mandal et 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, décembre 2019. doi : 10.1007/978-3-030-35423-7_17. hal-02374286.

[327] Stanislav Aranovskiy, Denis Efimov, Dmitry Sokolov, Jian Wang, Igor Ryadchikov et 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, juillet 2020. hal-02634576.

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

[329] Fabrice Boudot, Pierrick Gaudry, Aurore Guillevic, Nadia Heninger, Emmanuel Thomé et Paul Zimmermann. “Comparing the difficulty of factorization and discrete logarithm : a 240-digit experiment”. In : *Advances in Cryptology – CRYPTO 2020*. Sous la dir. de Daniele Micciancio et Thomas Ristenpart. T. 12171. Lecture Notes in Computer Science. Santa Barbara CA, United States : Springer, août 2020, p. 62-91. doi : 10.1007/978-3-030-56880-1_3. hal-02863525.

[330] Véronique Cortier, Pierrick Gaudry et 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.

[331] Gabrielle De Micheli, Pierrick Gaudry et Cécile Pierrot. “Asymptotic complexities of discrete logarithm algorithms in pairing-relevant finite fields”. In : *CRYPTO 2020 - 40th Annual International Cryptology Conference*. Sous la dir. de Daniele Micciancio et Thomas Ristenpart. T. 12171. Lecture Notes in Computer Science. Santa Barbara / Virtual, United States : Springer, août 2020, p. 32-61. hal-02871839.

[332] Gabrielle De Micheli, Rémi E. Piau et Cécile Pierrot. “A Tale of Three Signatures : practical attack of ECDSA with wNAF”. In : *AFRICACRYPT 2020*. Sous la dir. d’Youssef A. Nitaj A. T. 12174. Lecture Notes in Computer Science. Cairo, Egypt, juillet 2020, p. 361-381. doi : 10.1007/978-3-030-51938-4_18. hal-02393302.

[333] Patrick Derbez, Paul Huynh, Virginie Lallemand, María Naya-Plasencia, Léo Perrin et André Schrottenloher. “Cryptanalysis Results on Spook : Bringing Full-round Shadow-512 to the Light”. In : *CRYPTO 2020 - 40th Annual International Cryptology Conference*. Sous la dir. de Daniele Micciancio et Thomas Ristenpart. T. 12172. Lecture Notes in Computer Science. Santa Barbara / Virtual, United States, août 2020, p. 359-388. doi : 10.1007/978-3-030-56877-1_13. hal-02944908.

[334] Vincent Despré, Jean-Marc Schlenker et Monique Teillaud. “Flipping Geometric Triangulations on Hyperbolic Surfaces”. In : *SoCG 2020 - 36th International Symposium on Computational Geometry*. Zurich, Switzerland, juin 2020. doi : 10.4230/LIPIcs.SoCG.2020.35. hal-02886493.

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

[336] Youssef El Housni et 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*. Sous la dir. d’Haya Shulman et Serge Vaudenay. T. 12579. Lecture Notes in Computer Science. Vienna / Virtual, Austria : Springer, décembre 2020, p. 259-279. doi : 10.1007/978-3-030-65411-5_13. hal-02962800.

[337] Philippe Even et Phuc Ngo. “Live extraction of curvilinear structures from lidar raw data”. In : *XXIV ISPRS Congress*. T. V-2-2020. IAPRS Annals of Photogrammetry, Remote Sensing and Spatial Information Sciences. Nice, France, 2020, p. 211-219. doi : 10.5194/isprs-annals-V-2-2020-211-2020. hal-02872075.

[338] Vincent Gaudillière, Gilles Simon et 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, octobre 2020. hal-02889146.

[339] Pierrick Gaudry et Alexander Golovnev. “Breaking the encryption scheme of the Moscow Internet voting system”. In : *Financial Cryptography and Data Security*. Sous la dir. de Joseph Bonneau et Nadia Heninger. arXiv : 1908.05127 - This work is a merger of arXiv:1908.09170 and arXiv:1908.05127. Kota Kinabalu, Malaysia : Springer, 2020, p. 32-49. doi : 10.1007/978-3-030-51280-4_3. hal-02266264.

[340] Xavier Goaoc et Emo Welzl. “Convex Hulls of Random Order Types”. In : *SoCG 2020 - 36th International Symposium on Computational Geometry*. Sous la dir. de Sergio Cabello et Danny Z. Chen. T. 164. 36th International Symposium on Computational Geometry (SoCG 2020). arXiv : 2003.08456 - Best paper award. Zürich / Virtual, Switzerland, juin 2020, 49:1-49:15. doi : 10.4230/LIPIcs.SoCG.2020.49. hal-02879289.

[341] 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*. Sous la dir. d’Aggelos Kiayias. T. 12111. LNCS. @normalcrurlhttps://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, juin 2020, p. 535-564. doi : 10.1007/978-3-030-45388-6_19. hal-02396352.

[342] Fabien Lauer. “Risk Bounds for Learning Multiple Components with Permutation-Invariant Losses”. In : *23rd International Conference on Artificial Intelligence and Statistics (AISTATS)*. T. 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.

[343] Louis Massucci, Fabien Lauer et 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, décembre 2020. hal-02942279.

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

[345] Antoine Moniot, Rohit Roy, Yann Guermeur et 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, juin 2020. hal-02927185.

[346] Phuc Ngo. “Digital hyperplane fitting”. In : *20th International Workshop on Combinatorial Image Analysis (IWCIA)*. T. 12148. LNCS. Novi Sad, Serbia, juillet 2020, p. 164-180. doi : 10.1007/978-3-030-51002-2_12. hal-02586206.

[347] Georg Osang, Mael Rouxel-Labbé et 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, septembre 2020, 75:1-75:17. doi : 10.4230/LIPIcs.ESA.2020.75. hal-02923439.

[348] Sandra Rasoamiaramanana, Marine Minier et 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, juillet 2020, p. 279-286. doi : 10.5220/0009781002790286. hal-02944654.

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

[350] Dmitry Sokolov, Stanislav Aranovskiy, Alexander A Gusev et 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, septembre 2020. hal-02313600.

[351] Matthieu Zins, Gilles Simon et 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, novembre 2020. hal-02975379.

Autre conférences internationales

[352] Thiéry Constant, Van Tho Nguyen, Estelle Noyer, Frédéric Mothe, Francis Colin, Alexandre Piboule, Bertrand Kerautret et 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, juin 2016. hal-02793063.

[353] Samuel Hornus, Sylvain Lefebvre, Jérémie Dumas et Frédéric Claux. “Tight printable enclosures and support structures for additive manufacturing”. In : *Eurographics Workshop on Graphics for Digital Fabrication*. Sous la dir. d’Asla Medeiros e SÁ, N. Pietroni et K. Rodriguez Echavarria. Lisbonne, Portugal : The Eurographics Association, mai 2016. hal-01399931.

[354] Damien Jamet, Xavier Provençal et Lafrenière Nadia. “Generation of Digital Planes Using Generalized Continued-Fractions Algorithms”. In : *19th IAPR International Conference on Discrete Geometry for Computer Imagery*. Sous la dir. de Springer. T. 9647. Discrete Geometry for Computer Imagery 19th IAPR International Conference, DGCI 2016, Nantes, France, April 18-20, 2016. Proceedings. Nantes, France, avril 2016, p. 45-56. doi : 10.1007/978-3-319-32360-2_4. hal-01364622.

[355] Bertrand Kerautret, Miguel Colom et 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.

[356] Bertrand Kerautret, Adrien Krähenbühl, Isabelle Debled-Rennesson et 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, juin 2016. hal-01359558.

[357] Bertrand Kerautret, Adrien Krähenbühl, Isabelle Debled-Rennesson et 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*. T. 10214. RRPR : International Workshop on Reproducible Research in Pattern Recognition. Bertrand Kerautret and Miguel Colom and Pascal Monasse. Cancùn, Mexico, décembre 2016, p. 116-130. doi : 10.1007/978-3-319-56414-2_9. hal-01571434.

[358] Adrien Krähenbühl, Jean-Romain Roussel, Bertrand Kerautret, Isabelle Debled-Rennesson, Frédéric Mothe et Fleur Longuetaud. “Robust Knot Segmentation by Knot Pith Tracking in 3D Tangential Images”. In : *ICCVG 2016*. T. 9972. Computer Vision and Graphics. Warsaw, Poland : Springer International Publishing AG, septembre 2016, p. 581-593. doi : 10.1007/978-3-319-46418-3_52. hal-01421205.

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

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

[361] Tim Reiner et Sylvain Lefebvre. “Interactive Modeling of Support-free Shapes for Fabrication”. In : *EUROGRAPHICS*. Proceedings of EUROGRAPHICS (short papers). Lisbonne, Portugal, mai 2016. hal-01401470.

[362] 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, juin 2017. hal-02982728.

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

[364] Isabelle Debled-Rennesson, Philippe Févotte, Monique Grandbastien, David Langlois et 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, février 2018. hal-01753067.

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

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

[367] Samuel Hornus et Sylvain Lefebvre. “Iterative carving for self-supporting 3D printed cavities”. In : *Eurographics 2018 - Short Papers*. Delft, Netherlands, avril 2018. hal-01764291.

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

[369] Ted Selker et 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, décembre 2018. hal-02560643.

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

[371] Enka Blanchard, Xavier Coquand et 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, septembre 2019. hal-02560695.

[372] Enka Blanchard et Siargey Kachanovich. “A note on the inflating enclosing ball problem”. In : *Bordeaux Graph Workshop*. Bordeaux Graph Workshop 2019. Bordeaux, France, octobre 2019. hal-02549818.

[373] Enka Blanchard et Siargey Kachanovich. “Counting authorised paths in constrained control-flow graphs”. In : *Bordeaux Graph Workshop*. Bordeaux Graph Workshop 2019. Bordeaux, France, octobre 2019. hal-02549827.

[374] Nikola K Blanchard. “Password typo correction using discrete logarithms”. In : *ICCSCE 2019 - 8th International Conference on Computer Science and Communication Engineering*. International Conference on Business, Technology and Innovation. Pristine, Kosovo, octobre 2019. hal-02550719.

[375] Nikola K Blanchard et 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, avril 2019. hal-02273387.

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

[377] Rémi Decelle et 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, septembre 2019. hal-03058259.

[378] Rémi Decelle, Phuc Ngo, Isabelle Debled-Rennesson, Frederic MOTHE et 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, septembre 2019. hal-02275651.

[379] Olivier Devillers et Charles Duménil. “A Poisson sample of a smooth surface is a good sample”. In : *EuroCG 2019 - 35th European Workshop on Computational Geometry*. Utrecht, Netherlands, mars 2019. hal-02394144.

[380] Matthijs Ebbens, Iordan Iordanov, Monique Teillaud et Gert Vegter. “Delaunay triangulations of symmetric hyperbolic surfaces”. In : *EuroCG 2019 - 35th European Workshop on Computational Geometry*. Utrecht, Netherlands, mars 2019. hal-02940717.

[381] 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 et S.A. Stern. "Pluto surface composition from spectral model inversion with metaheuristics". In : *EPSC-DPS Joint Meeting 2019*. Geneve, Switzerland, septembre 2019. hal-03099265.

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

[383] Viviane Ledoux et 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, novembre 2019. hal-02405752.

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

[385] Enka Blanchard et 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, février 2020. hal-02550738.

[386] Enka Blanchard, Ted Selker et 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, avril 2020. doi : 10.1145/3334480.3382990. hal-02560611.

[387] Prosenjit Bose, Jean-Lou De Carufel et 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, mars 2020. hal-02479502.

[388] 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, juillet 2020. doi : 10.1109/compsac48688.2020.00-32. hal-03284139.

[389] 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, juillet 2020. doi : 10.1145/3400903.3409117. hal-03284149.

[390] 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, août 2020. doi : 10.1145/3416921.3416943. hal-03284166.

[391] Alfredo Cuzzocrea, Vincenzo De Maio et 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, juillet 2020. doi : 10.1109/compsac48688.2020.00-69. hal-03284134.

[392] Alfredo Cuzzocrea et 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, novembre 2020. doi : 10.1145/3415958.3433051. hal-03284179.

[393] Alfredo Cuzzocrea, Enzo Mumolo, Edoardo Fadda et 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, juillet 2020. doi : 10.18293/DMSVIVA2020-018. hal-03274631.

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

[395] Jimmy Etienne et 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, septembre 2020, p. 1-7. doi : 10.1145/3384382.3384522. hal-02457161.

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

[397] Benedikt Kolbe et 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.

[398] Oxana Korzh, Ashish Sharma, Mikel Joaristi, Edoardo Serra et 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, décembre 2020. doi : 10.1109/bigdata50022.2020.9378306. hal-03284181.

[399] Carlos Ordonez, Zhibo Chen, Alfredo Cuzzocrea et 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, septembre 2020. doi : 10.1109/iv51561.2020.00074. hal-03284172.

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

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

[402] Youssef Assis, Liang Liao, Fabien Pierre, René Anxionnat et 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*. T. 13003. Deep Generative Models, and Data Augmentation, Labelling, and Imperfec-

tions. Strasbourg, France : Springer, septembre 2021, p. 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 et 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*. Sous la dir. de Mehdi Tibouchi et Huaxiong Wang. T. 13090. Lecture Notes in Computer Science. Singapore / Virtual, Singapore : Springer International Publishing, décembre 2021, p. 668-698. DOI : 10.1007/978-3-030-92062-3_23. hal-03516739.

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

[405] Hamid Boukerrou, Gilles Millérioux et 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, juillet 2021. hal-03292416.

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

[407] Antonio Coronato et 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, juillet 2021, p. 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, janvier 2021, p. 1-4. DOI : 10.1109/BigComp51126.2021.00010. hal-03352268.

[409] Alfredo Cuzzocrea, Luca Camilotti et 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, juin 2021. hal-03352346.

[410] Alfredo Cuzzocrea, Luca Camilotti et 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, mai 2021, p. 713-730. DOI : 10.1007/978-3-030-75100-5_61. hal-03352296.

[411] Alfredo Cuzzocrea et 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, avril 2021, p. 565-572. DOI : 10.5220/0010481705650572. hal-03355056.

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

[413] Alfredo Cuzzocrea, Francesco Mercaldo et 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, septembre 2021, p. 353-365. doi : 10.1007/978-3-030-86970-0_25. hal-03352391.

[414] Gabrielle De Micheli, Pierrick Gaudry et 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*. Sous la dir. de M. Tibouchi et H. Wang. T. 13090. ASIACRYPT. Virtual, Singapore : Springer, décembre 2021, p. 67-96. doi : 10.1007/978-3-030-92062-3_3. hal-03242324.

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

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

[417] Alix Delannoy, Antoine Moniot, Yann Guermeur et 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, juillet 2021, p. 1-6. hal-03540927.

[418] Stéphanie Delaune, Patrick Derbez, Paul Huynh, Marine Minier, Victor Mollimard et 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*. Sous la dir. de Kazue Sako et Nils Ole Tippenhauer. T. 12727. 19th International Conference on Applied Cryptography and Network Security. Kamakura, Japan, juin 2021, p. 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 et Thiéry Constant. “Tree Defect Segmentation using Geometric Features and CNN”. In : *Reproducible Research on Pattern Recognition (RRPR)*. T. LNCS 12636. Milan, Italy, 2021, p. 80-100. doi : 10.1007/978-3-030-76423-4_6. hal-03006063.

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

[421] Philippe Even, Axelle Grzesznik, Anne Gebhardt, Thomas Chenal, Pierre Even et Phuc Ngo. “Interactive extraction of linear structures from LiDAR raw data for archaeo-morphological structure prospection”. In : *XXIV ISPRS Congress*. T. XLIII-B2-2021. The International Archives of the Photogrammetry, Remote Sensing and Spatial Information Sciences. Nice (en ligne), France, juillet 2021, p. 153-161. doi : 10.5194/isprs-archives-XLIII-B2-2021-153-2021. hal-03189641.

[422] Philippe Even et Phuc Ngo. “Automatic forest road extraction from LiDAR data of mountainous areas”. In : *DGMM 2021 - IAPR International Conference on Discrete Geometry and Mathematical Morphology*. T. LNCS12708. Uppsala, Sweden, mai 2021, p. 93-106. doi : 10.1007/978-3-030-76657-3_6. hal-03144147.

[423] Vladimir Garanzha, Igor Kaporin, Liudmila Kudryavtseva, François Protais, Nicolas Ray et 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, juin 2021. hal-03341392.

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

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

[426] Elisabeth Larsson, Pierre-Frédéric Villard, Igor Tominec et 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, mars 2021. hal-03147251.

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

[428] Louis Massucci, Fabien LAUER et 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, juillet 2021. hal-03324069.

[429] Louis Massucci, Fabien LAUER et 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, juillet 2021. hal-03324120.

[430] Nikita Mikhalkov, Alexey Prutskiy, Semyon Sechenev, Dmitry Kazakov, Alexey Simulin, Dmitry Sokolov et 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, mai 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, février 2021. hal-03249123.

[432] Phuc Ngo, Nicolas Passat et 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, p. 1584-1588. doi : 10.1109/ICIP42928.2021.9506543. hal-03121428.

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

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

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

[436] Thibault Tricard, Jimmy Etienne, Cédric Zanni et 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, octobre 2021. doi : 10.1145/3485114.3485117. hal-03352656.

Journaux nationaux

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

Conférences nationales

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

[439] Vincent Gaudillière, Gilles Simon et 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, juin 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, juin 2018. hal-01815406.

[441] Vincent Gaudillière, Gilles Simon et 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, mai 2019. hal-02148633.

[442] Arthur Renaudeau, François Lauze, Fabien Pierre, Jean-François Aujol et 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, mai 2019. hal-02433990.

[443] Youssef Assis, Liang Liao, Fabien Pierre, René Anxionnat et 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, septembre 2021. hal-03339672.

[444] Rémi Decelle, Phuc Ngo, Isabelle Debled-Rennesson, Frédéric F. Mothe et 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 et 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, septembre 2021. hal-03339639.

[446] Arthur Renaudeau, Travis Seng, Axel Carlier, Fabien Pierre, François Lauze, Jean-François Aujol et 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, septembre 2021. hal-03339640.

[447] Matthieu Zins, Gilles Simon et 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, septembre 2021. hal-03339617.

Ouvrages

[448] Marco Attene, Marco Livesu, Sylvain Lefebvre, Thomas Funkhouser, Stefano Ellero, Szymon Rusinkiewicz, Jonàs Martínez et Amit Haim Bermano. *Design,*

Representations, and Processing for Additive Manufacturing. T. 10. Synthesis Lectures on Visual Computing : Computer Graphics, Animation, Computational Photography, and Imaging 2. Morgan & Claypool Publishers, juin 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 et Hugh Thomas. *Computational Mathematics with SageMath*. SIAM, décembre 2018. doi : 10.1137/1.9781611975468. hal-01646401.

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

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

Ouvrages collectifs ou actes de conférence

[452] Damien Jamet. *Foreword - Special issue dedicated to the fifteenth "Journées Montoises d'Informatique Théorique*. T. 50. 1. Juin 2016. doi : 10.1051/ita/2016012. hal-01364597.

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

[454] Daniel Augot, Faina Solov'Eva, Marine Minier, Victor A. Zinoviev et Thomas Johansson. *Editorial : Special issue on coding and cryptography*. T. 87. 2-3. Springer, mars 2019. doi : 10.1007/s10623-018-00601-w. hal-02373772.

Chapitres de livres

[455] Yann Guermeur et 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*. Sous la dir. de Mourad Elloumi, Costas Iliopoulos, Jason T. L. Wang et Albert Y. Zomaya. Wiley, 2016, p. 114-128. doi : 10.1002/9781119078845.ch7. hal-01253820.

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

[457] Van Tho Nguyen, Bertrand Kerautret, Isabelle Debled-Rennesson, Francis Colin, Alexandre Piboule et 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 et Andreas Holzinger. “Convolutional and Recurrent Neural Networks for Activity Recognition in Smart Environment”. In : *Towards Integrative Machine Learning and Knowledge Extraction*. Sous la dir. d’A. Holzinger, R. Goebel, M. Ferri et V. Palade. T. 10344. Lecture Notes in Computer Science. springer, 2017, p. 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*. Sous la dir. de Joppe W. Bos et Arjen K. Lenstra. arXiv : 1604.02277. Cambridge University Press, 2017, p. 175-188. doi : 10.1017/9781316271575.008. hal-01293351.

[460] Nikola K Blanchard, Siargey Kachanovich, Ted Selker et Florentin Waligorski. “Reflexive Memory Authenticator : A Proposal for Effortless Renewable Biometrics”. In : *Emerging Technologies for Authorization and Authentication*. T. 11967. Septembre 2019, p. 104-121. doi : 10.1007/978-3-030-39749-4_7. hal-02550765.

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

[461] Parisa Rastin, Guénaël Cabanes, Rosanna Verde, Younès Bennani et Thierry Couronne. “Generative Histogram-Based Model Using Unsupervised Learning”. In : *Neural Information Processing*. Décembre 2019, p. 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 et 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*. Sous la dir. de Sherwin S., Moxey D., Peiró J., Vincent P. et Schwab C. T. 134. Lecture Notes in Computational Science and Engineering. Springer, août 2020, p. 501-512. doi : 10.1007/978-3-030-39647-3_40. hal-02917575.

[463] Damien Chablat, Guillaume Moroz, Fabrice Rouillier et Philippe Wenger. “Using Maple to analyse parallel robots”. In : *Maple in Mathematics Education and Research*. Sous la dir. de Jürgen Gerhard et Ilias Kotsireas. Maple in Mathematics Education and Research. Springer, Cham, février 2020, p. 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 et 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 et 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”*. Août 2020, p. 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 et Andreas Holzinger. “Privacy-Enabled Smart Home Framework with Voice Assistant”. In : *Smart Assisted Living*. Août 2020, p. 321-339. doi : 10.1007/978-3-030-25590-9_16. hal-03081721.

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

[469] Nigel P Smart et Emmanuel Thomé. “History of Cryptographic Key Sizes”. In : *Computational Cryptography*. Sous la dir. de Joppe Bos et Martijn Stam. T. 469. London Mathematical Society Lecture Note Series. Cambridge University Press, décembre 2021. hal-03408015.

Médiation scientifique

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

[471] Pierrick Gaudry et Joanna Jongwane. “À propos du vote par Internet”. In : *Interstices* (mars 2017). hal-01533682.

[472] Véronique Cortier, Pierrick Gaudry et Stephane Glondu. *(a voté) Euh non : a cliqué*. Blog Binaire LeMonde.fr. Mars 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 @normalcrurlhttps://www.lemonde.fr/blog/binaire/2019/12/06/de-la-necessite-des-problemes-que-lon-ne-sait-pas-resoudre/. Décembre 2019. hal-03213156.

[474] 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 et Christophe Vuillot. “Le traçage anonyme, dangereux oxymore : Analyse de risques à destination des non-spécialistes”. working paper or preprint. Avril 2020. hal-02997228.

[475] Gilles Simon. “La machine à perspective de Jan Van Eyck”. In : *Interstices* (novembre 2021). hal-03517010.

[476] Gilles Simon. “La véritable invention de Jan van Eyck : une machine à représenter l’espace tel que nous le percevons”. In : *The Conversation* (août 2021). hal-03521172.

Autres publications

[477] Vincent Despré, Olivier Devillers, Hugo Parlier et Jean-Marc Schlenker. “Delaunay Triangulations of Points on Circles”. arXiv : 1803.11436 - working paper or preprint. Avril 2018. hal-01780607.

[478] Gabrielle De Micheli et Nadia Heninger. “Recovering cryptographic keys from partial information, by example”. working paper or preprint. Décembre 2020. hal-03045663.

[479] Yann Guermeur. “Combinatorial and Structural Results for γ-Ψ-dimensions”. arXiv : 1809.07310v3 - working paper or preprint. Septembre 2020. hal-03230918.

[480] Benedikt Kolbe et Vanessa Robins. “Tile-transitive tilings of the Euclidean and hyperbolic planes by ribbons”. working paper or preprint. Décembre 2020. hal-03046798.

[481] Matthijs Ebbens, Iordan Iordanov, Monique Teillaud et Gert Vegter. “Delaunay triangulations of generalized Bolza surfaces”. arXiv : 2103.05960 - working paper or preprint. Mars 2021. hal-03080125.

[482] Sylvain Lefebvre, Li-Yi Wei et Connelly Barnes. “Informational Texture Synthesis”. working paper or preprint. Juin 2021. hal-01706539.

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

[484] Antoine Moniot, Isaure Chauvot de Beauchêne et 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. Août 2021. hal-03432671.

Logiciels

[485] Mikhail Bogdanov, Aymeric Pellé, Mael Rouxel-Labbe et 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.

[486] Mikhail Bogdanov, Iordan Iordanov et 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.

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

[488] Iordan Iordanov et 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.

[489] Gaetan Bisson, Romain Cosset et Damien Robert, *AVIsogenies* version git-47d34838, octobre 2021. hal : ⟨hal-03371897v1⟩, hal-03371897, vcs : https://gitlab.inria.fr/roberdam/avisogenies.

Brevets

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

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

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.