IN PARTNERSHIP WITH:
CNRS

Ecole Polytechnique

Activity Report 2019

Project-Team GRACE

Geometry, arithmetic, algorithms, codes and encryption

IN COLLABORATION WITH: Laboratoire d'informatique de l'école polytechnique (LIX)

RESEARCH CENTER
Saclay - Île-de-France

THEME
Algorithmics, Computer Algebra and Cryptology

Table of contents

Project-Team GRACE

Creation of the Team: 2012 January 01, updated into Project-Team: 2013 July 01

Keywords:

Computer Science and Digital Science:

A1.2.5. - Internet of things
A1.2.8. - Network security
A1.3.3. - Blockchain
A2.3.1. - Embedded systems
A4.2. - Correcting codes
A4.3. - Cryptography
A4.3.1. - Public key cryptography
A4.3.3. - Cryptographic protocols
A4.3.4. - Quantum Cryptography
A4.4. - Security of equipment and software
A4.8. - Privacy-enhancing technologies
A4.9. - Security supervision
A8.1. - Discrete mathematics, combinatorics
A8.4. - Computer Algebra
A8.5. - Number theory

Other Research Topics and Application Domains:

B5.11. - Quantum systems
B9.5.1. - Computer science
B9.5.2. - Mathematics
B9.10. - Privacy

1. Team, Visitors, External Collaborators

Research Scientists

Daniel Augot [Team leader, Inria, Senior Researcher, HDR]
Alain Couvreur [Inria, Researcher, HDR]
Benjamin Smith [Inria, Researcher]

Faculty Members

Françoise Levy-Dit-Vehel [École Nationale Supérieure de Techniques Avancées, Professor, HDR]
François Morain [École polytechnique, Professor, HDR]
Guénaël Renault [École polytechnique, Professor, HDR]

Post-Doctoral Fellows

Adrien Hauteville [Inria, Post-Doctoral Fellow, from Feb 2019]
Jade Nardi [Inria, Post-Doctoral Fellow, from Oct 2019]

PhD Students

Maxime Anvari [FX-Conseil, PhD Student, from Nov 2019]
Lucas Benmouffok [Institut de recherche technologique System X, PhD Student]
Hanna-Mae Bisserier [Institut de recherche technologique System X, PhD Student]
Sarah Bordage [École polytechnique, PhD Student]

Alexis Challande [Quarkslab, PhD Student, from May 2019]
Mathilde Chenu de La Morinerie [École polytechnique, PhD Student]
Antonin Leroux [Ministère des armées, PhD Student, from Oct 2019]
Simon Montoya [Idemia, PhD Student, from Sep 2019]
Isabella Panaccione [Inria, PhD Student, from Oct 2018]
Maxime Roméas [École polytechnique, PhD Student, from Oct 2019]
Angelo Saadeh [Telecom ParisTech, PhD Student, from Sep 2019]

Interns and Apprentices

Joel Felderhoff [École Normale Supérieure de Lyon, until Jun 2019]
Quentin Hillebrand [Inria, from May 2019 until Jul 2019]
Tanguy Medevielle [Inria, from May 2019 until Jun 2019]

Administrative Assistant

Maria Agustina Ronco [Inria, Administrative Assistant]

Visiting Scientists

Gianira Alfarano [University of Zurich, from Sep 2019]
Vincent Neiger [Univ de Limoges, Nov 2019]
Sven Puchinger [DTY Lyngby, from Dec 2019]
Kazuhiro Yokoyama [Rikkyo University, Oct 2019]
Alessandro Neri [University of Zurich, from Sep 2019]

External Collaborators

Elise Barelli [Univ de Versailles Saint-Quentin-en-Yvelines]
Luca de Feo [Univ de Versailles Saint-Quentin-en-Yvelines]
Julien Lavauzelle [Univ de Rennes I]
Philippe Lebacque [Univ de Franche-Comté, until Aug 2019]
Matthieu Rambaud [Institut Telecom ex GET Groupe des Écoles des Télécommunications]

2. Overall Objectives

2.1. Scientific foundations

Grace combines expertise and deep knowledge in algorithmic number theory and algebraic geometry, to build and analyse (public-key) cryptosystems, design new error correcting codes, with real-world concerns like cybersecurity or blockchains (software and hardware implemntations, secure implementations in constrained environments, countermeasures against side channel attacks, white box cryptography).

The foundations of Grace therefore lie in algorithmic number theory (fundamental algorithms primality, factorization), number fields, the arithmetic geometry of curves, algebraic gemoetry and the theory of algebraic codes.

Arithmetic Geometry is the meeting point of algebraic geometry and number theory: the study of geometric objects defined over arithmetic number systems. In our case, the most important objects are curves and their Jacobians over finite fields; these are fundamental to our applications in both coding theory and cryptology. Jacobians of curves are excellent candidates for cryptographic groups when constructing efficient instances of public-key cryptosystems, of which Diffie–Hellman key exchange is an instructive example.

Coding Theory studies originated with the idea of using redundancy in messages to protect them against noise and errors. While the last decade of the 20th century has seen the success of so-called iterative decoding methods, we see now many new ideas in the realm of algebraic coding, with the foremost example being list decoding, (zero knowledge or not) proofs of computation.

Part of the activities of the team are oriented towards post-quantum cryptography, either based on elliptic curves (isogenies) or code-based. Also the team study relevant cryptography for the blockchain arena.

The group is strongly invested in cybersecurity: software security, secure hardware implementations, privacy, etc.

3. Research Program

3.1. Algorithmic Number Theory

Participants: Luca de Feo, François Morain, Benjamin Smith, Mathilde de La Morinerie, Antonin Leroux, Guénaël Renault.

Algorithmic Number Theory is concerned with replacing special cases with general algorithms to solve problems in number theory. In the Grace project, it appears in three main threads:

- fundamental algorithms for integers and polynomials (including primality and factorization);
- algorithms for finite fields (including discrete logarithms);
- algorithms for algebraic curves.

Clearly, we use computer algebra in many ways. Research in cryptology has motivated a renewed interest in Algorithmic Number Theory in recent decades—but the fundamental problems still exist *per se*. Indeed, while algorithmic number theory application in cryptanalysis is epitomized by applying factorization to breaking RSA public key, many other problems, are relevant to various area of computer science. Roughly speaking, the problems of the cryptological world are of bounded size, whereas Algorithmic Number Theory is also concerned with asymptotic results.

3.2. Arithmetic Geometry: Curves and their Jacobians

Participants: Luca de Feo, François Morain, Benjamin Smith, Mathilde de La Morinerie, Antonin Leroux.

Theme: Arithmetic Geometry: Curves and their Jacobians *Arithmetic Geometry* is the meeting point of algebraic geometry and number theory: that is, the study of geometric objects defined over arithmetic number systems (such as the integers and finite fields). The fundamental objects for our applications in both coding theory and cryptology are curves and their Jacobians over finite fields.

An algebraic *plane curve* $\mathcal{X}$ over a field $\mathbf{K}$ is defined by an equation

$$\mathcal{X} : F_{\mathcal{X}}(x, y) = 0 \quad \text{where } F_{\mathcal{X}} \in \mathbf{K}[x, y].$$

(Not every curve is planar—we may have more variables, and more defining equations—but from an algorithmic point of view, we can always reduce to the plane setting.) The *genus* $g_{\mathcal{X}}$ of $\mathcal{X}$ is a non-negative integer classifying the essential geometric complexity of $\mathcal{X}$; it depends on the degree of $F_{\mathcal{X}}$ and on the number of singularities of $\mathcal{X}$. The curve $\mathcal{X}$ is associated in a functorial way with an algebraic group $J_{\mathcal{X}}$, called the *Jacobian* of $\mathcal{X}$. The group $J_{\mathcal{X}}$ has a geometric structure: its elements correspond to points on a $g_{\mathcal{X}}$-dimensional projective algebraic group variety. Typically, we do not compute with the equations defining this projective variety: there are too many of them, in too many variables, for this to be convenient. Instead, we use fast algorithms based on the representation in terms of classes of formal sums of points on $\mathcal{X}$.

The simplest curves with nontrivial Jacobians are curves of genus 1, known as *elliptic curves*; they are typically defined by equations of the form $y^2 = x^3 + Ax + B$. Elliptic curves are particularly important given their central role in public-key cryptography over the past two decades. Curves of higher genus are important in both cryptography and coding theory.

3.3. Curve-Based cryptology

Participants: Luca de Feo, François Morain, Benjamin Smith, Mathilde de La Morinerie, Antonin Leroux.

Theme: Curve-Based Cryptology

Jacobians of curves are excellent candidates for cryptographic groups when constructing efficient instances of public-key cryptosystems. Diffie–Hellman key exchange is an instructive example.

Suppose Alice and Bob want to establish a secure communication channel. Essentially, this means establishing a common secret *key*, which they will then use for encryption and decryption. Some decades ago, they would have exchanged this key in person, or through some trusted intermediary; in the modern, networked world, this is typically impossible, and in any case completely unscalable. Alice and Bob may be anonymous parties who want to do e-business, for example, in which case they cannot securely meet, and they have no way to be sure of each other's identities. Diffie–Hellman key exchange solves this problem. First, Alice and Bob publicly agree on a cryptographic group G with a generator P (of order N); then Alice secretly chooses an integer a from $[1..N]$, and sends aP to Bob. In the meantime, Bob secretly chooses an integer b from $[1..N]$, and sends bP to Alice. Alice then computes $a(bP)$, while Bob computes $b(aP)$; both have now computed abP, which becomes their shared secret key. The security of this key depends on the difficulty of computing abP given P, aP, and bP; this is the Computational Diffie–Hellman Problem (CDHP). In practice, the CDHP corresponds to the Discrete Logarithm Problem (DLP), which is to determine a given P and aP.

This simple protocol has been in use, with only minor modifications, since the 1970s. The challenge is to create examples of groups G with a relatively compact representation and an efficiently computable group law, and such that the DLP in G is hard (ideally approaching the exponential difficulty of the DLP in an abstract group). The Pohlig–Hellman reduction shows that the DLP in G is essentially only as hard as the DLP in its largest prime-order subgroup. We therefore look for compact and efficient groups of prime order.

The classic example of a group suitable for the Diffie–Hellman protocol is the multiplicative group of a finite field $\mathbf{F}_q$. There are two problems that render its usage somewhat less than ideal. First, it has too much structure: we have a subexponential Index Calculus attack on the DLP in this group, so while it is very hard, the DLP falls a long way short of the exponential difficulty of the DLP in an abstract group. Second, there is only one such group for each q: its subgroup treillis depends only on the factorization of $q-1$, and requiring $q-1$ to have a large prime factor eliminates many convenient choices of q.

This is where Jacobians of algebraic curves come into their own. First, elliptic curves and Jacobians of genus 2 curves do not have a subexponential index calculus algorithm: in particular, from the point of view of the DLP, a generic elliptic curve is currently *as strong as* a generic group of the same size. Second, they provide some diversity: we have many degrees of freedom in choosing curves over a fixed $\mathbf{F}_q$, with a consequent diversity of possible cryptographic group orders. Furthermore, an attack which leaves one curve vulnerable may not necessarily apply to other curves. Third, viewing a Jacobian as a geometric object rather than a pure group allows us to take advantage of a number of special features of Jacobians. These features include efficiently computable pairings, geometric transformations for optimised group laws, and the availability of efficiently computable non-integer endomorphisms for accelerated encryption and decryption.

3.4. Algebraic Coding Theory

Participants: Daniel Augot, Alain Couvreur, Françoise Levy-Dit-Vehel, Maxime Roméas, Sarah Bordage, Adrien Hauteville, Isabella Panaccione.

Theme: Coding theory

Coding Theory studies originated with the idea of using redundancy in messages to protect against noise and errors. The last decade of the 20th century has seen the success of so-called iterative decoding methods, which enable us to get very close to the Shannon capacity. The capacity of a given channel is the best achievable transmission rate for reliable transmission. The consensus in the community is that this capacity is more easily reached with these iterative and probabilistic methods than with algebraic codes (such as Reed–Solomon codes).

However, algebraic coding is useful in settings other than the Shannon context. Indeed, the Shannon setting is a random case setting, and promises only a vanishing error probability. In contrast, the algebraic Hamming approach is a worst case approach: under combinatorial restrictions on the noise, the noise can be adversarial, with strictly zero errors.

These considerations are renewed by the topic of list decoding after the breakthrough of Guruswami and Sudan at the end of the nineties. List decoding relaxes the uniqueness requirement of decoding, allowing a small list of candidates to be returned instead of a single codeword. List decoding can reach a capacity close to the Shannon capacity, with zero failure, with small lists, in the adversarial case. The method of Guruswami and Sudan enabled list decoding of most of the main algebraic codes: Reed–Solomon codes and Algebraic–Geometry (AG) codes and new related constructions "capacity-achieving list decodable codes". These results open the way to applications again adversarial channels, which correspond to worst case settings in the classical computer science language.

Another avenue of our studies is AG codes over various geometric objects. Although Reed–Solomon codes are the best possible codes for a given alphabet, they are very limited in their length, which cannot exceed the size of the alphabet. AG codes circumvent this limitation, using the theory of algebraic curves over finite fields to construct long codes over a fixed alphabet. The striking result of Tsfasman–Vladut–Zink showed that codes better than random codes can be built this way, for medium to large alphabets. Disregarding the asymptotic aspects and considering only finite length, AG codes can be used either for longer codes with the same alphabet, or for codes with the same length with a smaller alphabet (and thus faster underlying arithmetic).

From a broader point of view, wherever Reed–Solomon codes are used, we can substitute AG codes with some benefits: either beating random constructions, or beating Reed–Solomon codes which are of bounded length for a given alphabet.

Another area of Algebraic Coding Theory with which we are more recently concerned is the one of Locally Decodable Codes. After having been first theoretically introduced, those codes now begin to find practical applications, most notably in cloud-based remote storage systems.

4. Application Domains

4.1. Application Domain: cybersecurity

Participants: Guénaël Renault, Benjamin Smith, François Morain, Alexis Challande, Simon Montoya, Maxime Anvari.

We are interesting in developing some interactions between cryptography and cybersecurity. In particular, we develop some researches in embedded security (side channels and fault attack), software security (finding vulnerability efficiently) and privacy (security of TOR).

4.2. Application Domain: blockchains

Participants: Daniel Augot, Sarah Bordage, Matthieu Rambaud, Lucas Benmouffok, Hanna-Mae Bisserier.

The huge interest shown by companies for blockchains and cryptocurrencies have attracted the attention of mainstream industries for new, advanced uses of cryptographic, beyond confidentiality, integrity and authentication. In particular, zero-knowledge proofs, computation with encrypted data, etc, are now revealing their potential in the blockchain context. Team Grace is investigating two topics in these areas: secure multiparty computation and so-called "STARKS".

Secure multiparty computation enables several participants to compute a common function of data they each secretly own, without each participant revealing his data to the other participants. This area has seen great progress in recent years, and the cryptogaphic protocols are now mature enough for practical use. This topic is new to project-team Grace, and we will investigate it in the context of blockchains, through the lenses of use for private "smart contracts". A PhD student has been hired since October, funded by IRT System-X.

Daniel Augot is involved in blockchains from the point of view of cryptography for better blockchains, mainly for improving privacy. A PhD student has been enrolled at IRT System-X, to study pratical use cases of Secure Multiparty Computaiton.

Also Daniel Augot, together with Julian Prat (economist, ENSAE), is leading a Polytechnique teaching and research “chair”, funded by CapGemini, for blockchains in the industry, B2B platforms, supply chains, etc.

4.3. Cloud storage

The team is concerned with several aspect of reliability and security of cloud storage, obtained mainly with tools from coding theory. On the privacy side, we build protocols for so-called Private Information Retrieval which enable a user to query a remote database for an entry, while not revealing his query. For instance, a user could query a service for stock quotes without revealing with company he is interested in. On the availability side, we study protocols for proofs of retrievability, which enable a user to get assurance that a huge file is still available on a remote server, with a low bandwith protocol which does not require to download the whole file. For instance, in a peer-to-peer distributed storage system, where nodes could be rewarded for storing data, they can be audited with proof of retrievability protocols to make sure they indeed hold the data.

We investigate these problems with algebraic coding theory, mainly codes with locality (locally decodable codes, locally recoverable codes, and so on).

An M2 intern, Maxime Roméas, Bordeaux university, studied the constructive cryptography model, "A study of the Constructive Cryptography model of Maurer et. al." 5 months, followed by a PhD grant from IP Paris/Ecole Polytechnique for a 3-year doctorate (Oct 2019-Sept 2022): "The Constructive Cryptography paradigm applied to Interactive Cryptographic Proofs".

The Constructive Cryptography framework redefines basic cryptographic primitives and protocols starting from discrete systems of three types (resources, converters, and distinguishers). This not only permits to construct them effectively, but also lighten and sharpen their security proofs. One strength of this model is its composability. The purpose of the PhD is to apply this model to rephrase existing interactive cryptographic proofs so as to assert their genuine security, as well as to design new proofs. The main concern here is security and privacy in Distributed Storage settings.

5. New Software and Platforms

5.1. ACTIS

Algorithmic Coding Theory in Sage

FUNCTIONAL DESCRIPTION: The aim of this project is to vastly improve the state of the error correcting library in Sage. The existing library does not present a good and usable API, and the provided algorithms are very basic, irrelevant, and outdated. We thus have two directions for improvement: renewing the APIs to make them actually usable by researchers, and incorporating efficient programs for decoding, like J. Nielsen’s CodingLib, which contains many new algorithms.

- Partner: Technical University Denmark
- Contact: Daniel Augot

5.2. DECODING

KEYWORD: Algebraic decoding

FUNCTIONAL DESCRIPTION: Decoding is a standalone C library. Its primary goal is to implement Guruswami–Sudan list decoding-related algorithms, as efficiently as possible. Its secondary goal is to give an efficient tool for the implementation of decoding algorithms (not necessarily list decoding algorithms) and their benchmarking.

- Participant: Guillaume Quintin
- Contact: Daniel Augot

5.3. Fast Compact Diffie-Hellman

KEYWORD: Cryptography

FUNCTIONAL DESCRIPTION: A competitive, high-speed, open implementation of the Diffie–Hellman protocol, targeting the 128-bit security level on Intel platforms. This download contains Magma files that demonstrate how to compute scalar multiplications on the x-line of an elliptic curve using endomorphisms. This accompanies the EuroCrypt 2014 paper by Costello, Hisil and Smith, the full version of which can be found here: http://eprint.iacr.org/2013/692. The corresponding SUPERCOP-compatible crypto_dh application can be downloaded from http://hhisil.yasar.edu.tr/files/hisil20140318compact.tar.gz.

- Participant: Ben Smith
- Contact: Ben Smith
- URL: http://research.microsoft.com/en-us/downloads/ef32422a-af38-4c83-a033-a7aafbc1db55/

5.4. CADO-NFS

Crible Algébrique: Distribution, Optimisation - Number Field Sieve

KEYWORDS: Cryptography - Number theory

FUNCTIONAL DESCRIPTION: CADO-NFS is a complete implementation in C/C++ of the Number Field Sieve (NFS) algorithm for factoring integers and computing discrete logarithms in finite fields. It consists in various programs corresponding to all the phases of the algorithm, and a general script that runs them, possibly in parallel over a network of computers.

NEWS OF THE YEAR: The main program for relation collection now supports composite "special-q". The memory footprint of the central step of linear algebra was reduced. Parallelism of many of the Cado-NFS programs was improved considerably (sieving, relation filtering, as well as the central step of linear algebra).

- Participants: Pierrick Gaudry, Emmanuel Thomé and Paul Zimmermann
- Contact: Emmanuel Thomé
- URL: http://cado-nfs.gforge.inria.fr/

6. New Results

6.1. Error Locating pairs

Participants: Alain Couvreur, Isabella Panaccione.

Algebraic codes such as Reed–Solomon codes and algebraic geometry codes benefit from efficient decoding algorithms permitting to correct errors up to half the minimum distance and sometimes beyond. In 1992, Pellikaan proved that many **unique** decoding could be unified using an object called *Error correcting pair*. In short, given an error correcting code $\mathcal{C}$, an error correcting pair for $\mathcal{C}$ is a pair of codes $(\mathcal{A}, \mathcal{B})$ whose component wise product $\mathcal{A} * \mathcal{B}$ is contained in the dual code $\mathcal{C}^{\perp}$ and such that $\mathcal{A}, \mathcal{B}$ satisfy some constraints of dimension and minimum distance.

On the other hand, in the late 90's, after the breakthrough of Sudan and Guruswami Sudan the question of list decoding permitting to decode beyond half the minimum distance. In a recently submitted article, A. Couvreur and I. Panaccione [15] proposed a unified point of view for probabilistic decoding algorithms decoding beyond half the minimum distance. Similarly to Pellikaan's result, this framework applies to any code benefiting from an *error locating pair* which is a relaxed version of error correcting pairs.

6.2. Factoring oracles

Participants: François Morain, Benjamin Smith, Guénaël Renault.

Integer factoring is an old topic, and the situation is as follows: in the classical world, we think integer factoring is hard and the algorithms we have are quite powerful though of subexponential complexity and factoring numbers with several hundred bits; whereas in the quantum world, it is assumed to be easy (i.e., there exists a quantum polynomial time algorithm) but never experienced and the record is something like a few bits. F. Morain, helped by B. Smith and G. Renault studied the theoretical problem of factoring integers given access to classical oracles, like the Euler totient function. They were able to give some interesting classes of numbers that could tackled, The manuscript [18] is currently being refereed.

7. Bilateral Contracts and Grants with Industry

7.1. Bilateral Contracts with Industry

Participants: Daniel Augot, Alain Couvreur, Guénaël Renault, François Morain.

- Through École polytechnique, Daniel Augot is leader of a teaching and research chair on Blockchains for business, funded by CapGemini.
- IRT System-X funds a PhD student for Secure Multiparty Computation in blockchains
- Ernst & Young funds a contract for providing PhD guidance to one of its employee, on the topic of blockchains
- Idemia funds a CIFRE PhD student on the secure implementation in constrained environement of post-quantum cryptosystems.
- Quarkslab funds a CIFRE PhD student on the analysis of malware code
- French Min. Arm. funds a PhD student on the analysis of the ToR network
- Grant with Nokia with the Privacy “Action de recherche”.

8. Partnerships and Cooperations

8.1. Regional Initiatives

Participants: Daniel Augot, Matthieu Rambaud.

Daniel Augot and Matthieu Rambaud (Institut Mines-Telecom) received a Digicosme Grant, to fund a new PhD student, A. Saadeh, starting November 2019, on the topic of Secure Multiparty Computation.

8.2. National Initiatives

8.2.1. ANR MANTA

Participants: Daniel Augot, Alain Couvreur, Françoise Levy-Dit-Vehel, Philippe Lebacque, Matthieu Rambaud, Isabella Panaccione, Luca de Feo.

MANTA (accepted July 2015, starting March 2016, Ended September 2019): “Curves, surfaces, codes and cryptography”. This project deals with applications of coding theory error correcting codes to in cryptography, multi-party computation, and complexity theory, using advanced topics in algebraic geometry and number theory.

We have four annual national retreats, the last one in January 2019, and we organized a closing international workshop in August 2019, with more than 40 participants, half French, half international.

See http://anr-manta.inria.fr/.

8.2.2. ANR CIAO

Participants: Benjamin Smith, Luca de Feo, Antonin Leroux, Mathilde de La Morinerie.

ANR **CIAO** (Cryptography, Isogenies, and Abelian varieties Overwhelming) is a JCJC 2019 project, led by Damien Robert (Inria EP LFANT). This project, which started in October 2019, will examine applications of higher-dimensional abelian varieties in isogeny-based cryptography.

8.2.3. ANR CBCRYPT

Participant: Alain Couvreur.

ANR **CBCRYPT** (Code–based Cryptography) This is a project from (*Appel à projets générique, Défi 9, Liberté et sécurité de l'Europe, de ses citoyens et de ses résidents, Axe 4 ; Cybersécurité*). This project, starting in october 2017 led by Jean-Pierre Tillich (Inria, EP Cosmiq) focusses on the design and the security analysis of code–based primitives, in the context of the current NIST competition.

8.3. European Initiatives

8.3.1. FP7 & H2020 Projects

Participant: Benjamin Smith.

- SPARTA https://www.sparta.eu/ is a cybersecurity competence network, with the objective to collaboratively develop and implement top-tier research and innovation actions

8.4. International Research Visitors

8.4.1. Visits of International Scientists

- Alessandro Neri visited us from September 2019 to December 2019, as post-doctoral visitor, to work on rank-metric codes.
- Vincent Neiger (Mcf, Univ. Limoges) visited our team twice. One week in march and one meek in november, to work on the decoding of Reed–Solomon codes.

9. Dissemination

9.1. Promoting Scientific Activities

9.1.1. Scientific Events: Selection

9.1.1.1. Member of the Conference Program Committees

- Tokenomics 2019, International Conference on Blockchain Economics, Security and Protocols, Paris: D. Augot.
- FAB 2019, Second International Symposium on Foundations and Applications of Blockchain, Los Angeles: D. Augot
- ICBC 2019 (IEEE International Conference on Blockchain and Cryptocurrency, Seoul): D. Augot
- CBT 2019 (3rd International Workshop on Cryptocurrencies and Blockchain Technology, Barcelona)
- ECC 2019 (23rd International Workshop on Elliptic Curve Cryptography, Bochum): B. Smith
- Latincrypt 2019 (Santiago de Chile): B. Smith
- C2SI (*Codes, Cryptographie et Sécurité Informatique*) 2019 (Rabat, Morocco) A. Couvreur

9.1.1.2. Reviewer

- Eurocrypt 2019: D. Augot, B. Smith
- Indocrypt 2019 (20th International Conference on Cryptology in India, Hyderabad):D. Augot
- ISIT (International Symposium on Information Theory) 2019: D. Augot, A. Couvreur.

- Latincrypt 2019. A. Couvreur.
- SAC 2019: B. Smith
- STACS 2020: B. Smith

9.1.2. Journal

9.1.2.1. Member of the Editorial Boards

- F. Morain is member of the editorial board of the *Applicable Algebra in Engineering, Communication and Computing*, Springer.
- A. Couvreur is member of the editorial board of the *Publications mathématiques de l'Institut de mathématiques de Besançon, Algèbre et Théorie des nombres*.

9.1.2.2. Reviewer - Reviewing Activities

- Applicable Algebra in Engineering, Communication, and Computing: B. Smith
- Journal of Cryptographic Engineering: B. Smith
- Journal of Cryptology: B. Smith
- Publications Mathématiques de Besançon: B. Smith
- Transactions on Mathematical Software: B. Smith
- Designs, Codes and Cryptography: A. Couvreur.
- IEEE, Transactions on Information Theory: A. Couvreur.
- IEEE, Transactions on Communication: A. Couvreur.

9.1.3. Invited Talks

- D. Augot was invited to the joint Caen-Rouen ArcoCrypt colloquium.
- F. Morain was invited to give a talk at the seminar of the ARIC project-team in Lyon.
- G. Renault was invited to give the main keynote at PHISIC'19 workshop (Gardanne)
- G. Renault was invited to give a talk at the Workshop on Randomness and Arithmetics for Cryptography on Hardware (Roscoff)
- G. Renault was invited to give a talk at the Journée Internationale Post-Quantique organized by Institut Cyber de Grenoble Alpes.
- B. Smith was invited to give a talk at the Workshop on Arithmetic of low-dimensional abelian varieties at ICERM (Providence, USA)
- B. Smith and A. Couvreur were invited to give a talk in the mini-symposium on isogeny-based cryptography at the SIAM Conference on Applied Algebraic Geometry (Bern, Switzerland)
- B. Smith was invited to give a talk in the Autumn session of *Arithmétique en Plat Pays* (Mons, Belgium)
- A. Couvreur was invited speaker at the conference *WCC (Workshop on Coding and Cryptography) 2019* Saint Jacut de la mer, France.
- A. Couvreur was invited speaker at the conference *NuTMIC (Number Theoretic Methods In Cryptography) 2019*, Paris.

9.1.4. Seminars

D. Augot is member of the scientific committee of the C2 seminar, which is the French wide, now itinerant, seminar of the subgroup "Codage et Cryptographie" of the CNRS GDR group "Informatique mathématique".

9.1.5. Scientific Expertise

G. Renault was member of the Comité d'Évaluation du LJK (Grenoble) pour l'Hcéres.

9.1.6. Research Administration

- F. Morain is vice-head of the Département d'informatique of Ecole Polytechnique; in charge of years 1 and 2 for Computer Science courses.
- F. Morain is member of the Board of Master Parisien de Recherche en Informatique (MPRI); also a member of the board of the Cybersecurity track in the CS Master of IPParis.
- Recruitment committees:
  - D. Augot participated in a selection committee for an Assistant Professor position at École polytechnique.
  - A. Couvreur is member of the *commission scientifique* of Inria Saclay's research centre.
- Funding
  - D. Augot belongs to the Inria-NomadicLabs committee.
  - D. Augot belongs to MATH-INFO subcommittee of Saclay labex Laboratoire Jacques Hadamard, and has been replaced by A. Couvreur.

9.2. Teaching - Supervision - Juries

9.2.1. Teaching

Licence : F. Morain, Lectures for INF361: "Introduction à l'informatique", 15h (equiv TD), 1st year (L3), École polytechnique. Coordinator of this module (350 students).

Licence : B. Smith: *CSE101: Introduction to Computer Programming*, 42h, L1, École polytechnique, France

Licence : G. Renault: INF361, *Introduction à l'informatique*, 50h, L3, École Polytechnique, France.

Master : A. Couvreur : *MPRI 2-13-2: Error Correcting codes and applications to cryptography*.

Master : D. Augot: lectures and labs on crypto in blockchains, 24h, M2, École polytechnique, France.

Master : F. Morain is the scientific leader of the Master of Science and Technology *Cybersecurity: Threats and Defense* of École Polytechnique.

Master : F. Morain and A. Couvreur, INF558, *Introduction to cryptology*, 36h, M1, École Polytechnique.

Master : B. Smith: *INF568: Advanced Cryptography*, 54h, M1, École polytechnique, France

Master : B. Smith and F. Morain: *MPRI 2-12-2: Algorithmes Arithmétiques pour la Cryptologie*, 22.5h, M2, Master Parisien de Recherche en Informatique, France

Master : F. Levy-dit-Vehel, discrete maths, 21h, M1, ENSTA.

Master : F. Levy-dit-Vehel, cryptography, 24h, M2, ENSTA.

9.2.2. Supervision

HdR : A. Couvreur, Codes algébriques et géométriques, applications à la cryptographie et à l'information quantique, Paris Diderot University, December 16, 2019.

9.2.3. Juries

- D. Augot was member of the thesis committee of Thomas Debris.
- G. Renault was president of the thesis committee of François Boutigny.
- G. Renault was member of the thesis committee of Ramtine Tofighi.
- B. Smith was a member of the thesis committee of Louiza Papachristodoulou (Radboud Universiteit Nijmegen)
- B. Smith was a member of the thesis committee of Joost Renes (Radboud Universiteit Nijmegen)

- B. Smith was a *rapporteur* on the thesis of Yan Bo Ti (University of Auckland).

9.3. Popularization

9.3.1. Interventions...

- D. Augot was invited to the mathematical colloquium of the University of Besançon.
- Colloque “Blockchains et compétences” à l’Assemblée nationale le 14 mars: D. Augot, who participated to three meetings at Ministry of Finance and Ministry of Industry about blockchains.
- A. Couvreur is *Correspondant de Médiation Scientifique* of Inria Saclay’s research centre.
- A. Couvreur organised the *Fête de la science 2019* at Inria Saclay on october 10 and 11 2019. J. Nardi, S. Bordage, M. Chenu de la Morinerie, M. Romeas participated to the event as volunteers.
- A. Couvreur organised the Rendez-vous des Jeunes Mathématiciennes et Informaticiennes (RJMI) at Inria Saclay on october 21 and 22, 2019.

10. Bibliography

Publications of the year

Doctoral Dissertations and Habilitation Theses

[1] A. COUVREUR. *Codes algébriques et géométriques, applications à la cryptographie et à l’information quantique*, Université Paris Diderot, December 2019, Habilitation à diriger des recherches, https://hal.archives-ouvertes.fr/tel-02438668

Articles in International Peer-Reviewed Journals

[2] B. AUDOUX, A. COUVREUR. *On tensor products of CSS Codes*, in "Annales de l’Institut Henri Poincaré (D) Combinatorics, Physics and their Interactions", 2019, vol. 6, n^{o} 2, pp. 239–287, https://arxiv.org/abs/1512.07081 [*DOI :* 10.4171/AIHPD/71], https://hal.archives-ouvertes.fr/hal-01248760

[3] N. COXON. *Fast Hermite interpolation and evaluation over finite fields of characteristic two*, in "Journal of Symbolic Computation", July 2019, https://arxiv.org/abs/1807.00645 [*DOI :* 10.1016/J.JSC.2019.07.014], https://hal.archives-ouvertes.fr/hal-01827583

[4] J. LAVAUZELLE. *Private Information Retrieval from Transversal Designs*, in "IEEE Transactions on Information Theory", 2019, vol. 65, n^{o} 2, pp. 1189-1205, https://arxiv.org/abs/1709.07952 [*DOI :* 10.1109/TIT.2018.2861747], https://hal.archives-ouvertes.fr/hal-01901014

[5] J. LAVAUZELLE, F. LEVY-DIT-VEHEL. *Generic constructions of PoRs from codes and instantiations*, in "Journal of Mathematical Cryptology", February 2019, vol. 13, n^{o} 2, pp. 81–106, forthcoming [*DOI :* 10.1515/JMC-2018-0018], https://hal.archives-ouvertes.fr/hal-02053948

[6] R. LERCIER, C. RITZENTHALER, F. ROVETTA, J. SIJSLING, B. SMITH. *Distributions of traces of Frobenius for smooth plane curves over finite fields*, in "Experimental Mathematics", January 2019, vol. 28, n^{o} 1, pp. 39-48, https://arxiv.org/abs/1510.05601 [*DOI :* 10.1080/10586458.2017.1328321], https://hal.inria.fr/hal-01217995

International Conferences with Proceedings

[7] M. BARDET, M. BERTIN, A. COUVREUR, A. OTMANI. *Practical Algebraic Attack on DAGS*, in "CBC 2019 - 7th Code-Based Cryptography Workshop", Darmstadt, Germany, LNCS, July 2019, vol. 11666, pp. 86-101, https://arxiv.org/abs/1905.03635 - 16 pages, accepted for publication in the 7th Code-Based Cryptography Workshop 2019 [*DOI :* 10.1007/978-3-030-25922-8_5], https://hal.archives-ouvertes.fr/hal-02125330

[8] D. CERVANTES-VÁZQUEZ, M. CHENU, J.-J. CHI-DOMÍNGUEZ, L. DE FEO, F. RODRÍGUEZ-HENRÍQUEZ, B. SMITH. *Stronger and Faster Side-Channel Protections for CSIDH*, in "Latincrypt 2019 - 6th International Conference on Cryptology and Information Security in Latin", Santiago de Chile, Chile, P. SCHWABE, N. THÉRIAULT (editors), LNCS - Lecture Notes in Computer Science, Springer, October 2019, vol. 11774, https://arxiv.org/abs/1907.08704 - This work has been accepted in LATINCRYPT-2019 [*DOI :* 10.1007/978-3-030-30530-7_9], https://hal.inria.fr/hal-02190863

[9] A. COUVREUR, M. LEQUESNE, J.-P. TILLICH. *Recovering short secret keys of RLCE encryption scheme in polynomial time*, in "PQCrypto 2019 - International Conference on Post-Quantum Cryptography", Chongqing, China, May 2019, https://arxiv.org/abs/1805.11489 [*DOI :* 10.1007/978-3-030-25510-7_8], https://hal.inria.fr/hal-01959617

Conferences without Proceedings

[10] D. AUGOT, H. CHABANNE, W. GEORGE. *Practical Solutions to Save Bitcoins Applied to an Identity System Proposal*, in "5th International Conference on Information Systems Security and Privacy", Prague, France, SCITEPRESS - Science and Technology Publications, February 2019, pp. 511-518 [*DOI :* 10.5220/0007443905110518], https://hal.telecom-paristech.fr/hal-02347238

[11] D. COGGIA, A. COUVREUR. *On the security of a Loidreau's rank metric code based encryption scheme*, in "WCC 2019 - The Eleventh International Workshop on Coding and Cryptography", Saint Jacut de la mer, France, March 2019, https://hal.archives-ouvertes.fr/hal-02064465

Scientific Books (or Scientific Book chapters)

[12] D. AUGOT, F. SOLOV'EVA, M. MINIER, V. A. ZINOVIEV, T. JOHANSSON. *Editorial: Special issue on coding and cryptography*, Springer, March 2019, vol. 87, n^{o} 2-3 [*DOI :* 10.1007/s10623-018-00601-w], https://hal.inria.fr/hal-02373772

Other Publications

[13] W. CASTRYCK, T. DECRU, B. SMITH. *Hash functions from superspecial genus-2 curves using Richelot isogenies*, June 2019, https://arxiv.org/abs/1903.06451 - working paper or preprint, https://hal.inria.fr/hal-02067885

[14] C. COSTELLO, B. SMITH. *The supersingular isogeny problem in genus 2 and beyond*, December 2019, https://arxiv.org/abs/1912.00701 - working paper or preprint, https://hal.inria.fr/hal-02389073

[15] A. COUVREUR, I. PANACCIONE. *Power Error Locating Pairs*, July 2019, https://arxiv.org/abs/1907.11658 - working paper or preprint, https://hal.archives-ouvertes.fr/hal-02196650

[16] N. COXON. *Fast transforms over finite fields of characteristic two*, September 2019, https://arxiv.org/abs/1807.07785 - working paper or preprint, https://hal.archives-ouvertes.fr/hal-01845238

[17] J. LAVAUZELLE, P. LOIDREAU, B.-D. PHAM. *RAMESSES, a Rank Metric Encryption Scheme with Short Keys*, January 2020, working paper or preprint, https://hal.archives-ouvertes.fr/hal-02426624

References in notes

[18] F. MORAIN, G. RENAULT, B. SMITH. *Deterministic factoring with oracles*, February 2018, https://arxiv.org/abs/1802.08444 - working paper or preprint, https://hal.inria.fr/hal-01715832