RESEARCH CENTRE

Saclay - Île-de-France

IN PARTNERSHIP WITH:

CNRS, Ecole Polytechnique

2020 ACTIVITY REPORT

Project-Team GRACE

Geometry, arithmetic, algorithms, codes and encryption

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

DOMAIN

Algorithmics, Programming, Software and Architecture

THEME

Algorithmics, Computer Algebra and Cryptology

Contents

Project-Team GRACE

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

Keywords

Computer sciences and digital sciences

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

A7.1. – Algorithms

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 members, visitors, external collaborators

Research Scientists

- Daniel Augot [Team leader, Inria, Senior Researcher, HDR]
- Alain Couvreur [Inria, Researcher]
- Thomas Debris-Alazard [Inria, Researcher, from Sep 2020]
- 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, until Oct 2020]

Post-Doctoral Fellows

- Thomas Debris-Alazard [Royal Holloway, Université de Londres - Angleterre, until Mar 2020]
- Adrien Hauteville [Inria]
- Jade Nardi [Inria]
- Gustavo Souza Banegas [Inria, from Dec 2020]
- Ilaria Zappatore [Inria, from Nov 2020]

PhD Students

- Maxime Anvari [Ministère des armées]
- Lucas Benmouffok [Institut de recherche technologique System X]
- Hanna-Mae Bisserier [Institut de recherche technologique System X]
- Maxime Bombar [École polytechnique, from Sep 2020]
- Sarah Bordage [École polytechnique]
- Alexis Challande [Quarkslab]
- Mathilde De La Morinerie [École polytechnique]
- Youssef El Housni [Ernst Et Young, CIFRE]
- Antonin Leroux [Ministère des armées]
- Simon Montoya [Idemia, CIFRE]
- Isabella Panaccione [Inria]
- Andrianina Sandra Rasoamiaramanana [Inria, from May 2020 until Jun 2020]
- Maxime Roméas [École polytechnique]
- Edouard Rousseau [Institut Telecom ex GET Groupe des Écoles des Télécommunications]
- Angelo Saadeh [Telecom ParisTech]

Interns and Apprentices

- Maxime Bombar [Inria, from Mar 2020 until Jul 2020]
- Elie Bouscatié [École polytechnique, from Mar 2020 until Sep 2020]
- Enric Florit Zacarias [Inria, from Mar 2020 until Jun 2020]
- Erik Pohle [École polytechnique, from Apr 2020 until Sep 2020]
- Edison Reshketa [École polytechnique, from Feb 2020 until Apr 2020]
- Maelys Solal [Inria, from Jun 2020 until Jul 2020]

Administrative Assistant

- Maria Agustina Ronco [Inria]

Visiting Scientist

- Alp Bassa [Université du Bosphore Istanbul - Turquie, from Dec 2020]

External Collaborators

- Guénaël Renault [Secrétariat Général de la Défense et de la Sécurité Nationale, from Oct 2020]
- Luca de Feo [Univ de Versailles Saint-Quentin-en-Yvelines, HDR]

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* $\mathscr{X}$ over a field
K is defined by an equation

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

(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* $g_{\mathscr{X}}$ of $\mathscr{X}$ is a non-negative integer classifying the essential geometric complexity of $\mathscr{X}$; it depends on the degree of $F_{\mathscr{X}}$ and on the number of singularities of $\mathscr{X}$. The curve $\mathscr{X}$ is associated in a functorial way with an algebraic group $J_{\mathscr{X}}$, called the *Jacobian* of $\mathscr{X}$. The group $J_{\mathscr{X}}$ has a geometric structure: its elements correspond to points on a $g_{\mathscr{X}}$-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 $\mathscr{X}$.

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

Participants Françoise Levy-Dit-Vehel, Maxime Roméas.

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 Highlights of the year

5.1 Awards

- A. Leroux and L. De Feo obtained the *Best Paper Award* at the international conference *Asyacrypt* 2020 for their work on the isogeny–based signature SQISign.

- T. Debris–Alazard obtained the *Prix de thèse Gilles Kahn* for his thesis : *Cryptographie fondée sur les codes : nouvelles approches pour constructions et preuves ; contribution en cryptanalyse.*

6 New software and platforms

6.1 New software

6.1.1 ACTIS

Name: 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.

Contacts: David Lucas, Daniel Augot, Johan Nielsen

Partner: Technical University Denmark

6.1.2 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.

Author: Guillaume Quintin

Contacts: Daniel Augot, Maike Gilliot

Participant: Guillaume Quintin

6.1.3 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 .

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

Contact: Ben Smith

Participant: Ben Smith

6.1.4 CADO-NFS

Name: 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: Cado-NFS has undergone little important change during year 2020. However, some specific parts of the code have been improved. - the simulation code that is used to try to predict matrix sizes is evolving. - the I/O layer in the linear algebra code has been simplified. - the central step of binary linear algebra is being prepared for an improvement of some operations that are currently costlier than they should be. - cofactorisation code has been improved.

Additionally, Cado-NFS has moved to the Inria gitlab platform. At this point, there is no certainty as to the permanent URL of the Cado-NFS software.

URL: https://cado-nfs.gitlabpages.inria.fr/

Authors: Pierrick Gaudry, Laurent Gremy, François Morain, Emmanuel Thomé, Paul Zimmermann

Contacts: Pierrick Gaudry, Emmanuel Thomé, Paul Zimmermann

Participants: Pierrick Gaudry, Emmanuel Thomé, Paul Zimmermann

6.1.5 BW6-761

Name: Brezing-Weng-6 761 bits

Keywords: Cryptography, Blockchain

Functional Description: This small library implements finite field and elliptic curve arithmetic for the chain of curves BLS12-381 and BW6-761 for use with zk-snarks (zero-knowledge succinct non-interactive argument of knowledge). The cryptographic applications are: pairing, scalar multiplication on the curves, hashing on the curves. The code is a proof-of-concept and is not optimized. An optimized implementation is developed in C++ at https://github.com/EYBlockchain/zk-swap-libff/tree/ey/libff/algebra/curves/bw6_761 and in Rust at https://github.com/yelhousni/zexe/tree/youssef/BW6-761-Fq-ABLR-2ML-M

URL: https://gitlab.inria.fr/zk-curves/bw6-761/

Publication: hal-02962800

Contacts: Youssef El Housni, Aurore Guillevic

7 New results

7.1 Code equivalence in rank metric

Participants Alain Couvreur, Thomas Debris–Alazard.

A code equivalence problem consists, given two groups $\mathscr{C}_1$ and $\mathscr{C}_2$ equipped with a metric, to decide whether they are isomorphic. This question is of interest for instance in cryptography.

- If this equivalence is easy to decide, it may permit to reduce the cost of an attack involving an exhaustive search on all the possible groups to that of an exhaustive search on all the possible isomorphism classes, entailing a drastic reduction of complexity.
- If the equivalence problem turns out to be hard, it is possible to use it to design digital signatures whose security relies on this hardness.

In Hamming metric, this problem has been studied since the 80's. It has been proved to be hard in the worst case but an algorithm due to Sendrier solves efficiently some set of instances in the average case.

A. Couvreur and T. Debris–Alazard, in collaboration with P. Gaborit [19] from university of Limoges investigated te hadness of the problem in rank metric: if the groups are spaces of matrices and the distance between two matrices A and B is $\mathrm{Rank}(B-A)$. In this context, they proved that:

- In the worst case the problem is at least as hard its Hamming metric counterpart;
- In the case of structured code called "$\mathbb{F}_{q^m}$–linear codes", they proved the problem to be in the complexity class $\mathscr{ZPP}$.

7.2 Effective Riemann–Roch

Participants Alain Couvreur.

Riemann–Roch spaces are spaces of rational functions on curves generalising spaces of polynomials of bounded degree. Their effective computation is fundamental for the construction of algebraic geometry codes.

In a common project with S. Abelard and G. Lecerf from Max team at LIX, A. Couvreur worked on the fast computation of Riemann–Roch spaces based on Brill–Noether method and using structured linear algebra. Their algorithm permits to compute a basis of rational functions in a Riemann-Roch space $L(D)$ on a plane curve X of degree δ with only ordinary singularities in time

$$\widetilde{O}(\delta^{\omega+1} + \delta^{\omega-1} \deg D),$$

where ω denotes the complexity exponent of linear algebra.

7.3 Post quantum cryptography

7.3.1 Attack on LAC Key Exchange in Misuse Situation

Participants Guenael Renault, Simon Montoya.

LAC is a Ring Learning With Error based cryptosystem that has been proposed to the NIST call for post-quantum standardization and passed the first round of the submission process. It did not pass to the third round but it is selected as the chinese standard for key exchange. The particularity of LAC is to use an error-correction code ensuring a high security level with small key sizes and small ciphertext sizes. LAC team proposes a CPA secure cryptosystem, LAC-CPA, and a CCA secure one, LAC-CCA, obtained by applying the Fujisaki-Okamoto transformation on LAC-CPA.

Together with Aurelien Greuet (IDEMIA), we study in [14] the security of LAC Key Exchange (KE) mechanism, using LAC-CPA, in a misuse context: when the same secret key is reused for several key exchanges and an active adversary has access to a *mismatch oracle*. This oracle indicates information on the possible mismatch at the end of the KE protocol. In this context, we show that an attacker needs at most 8 queries to the oracle to retrieve one coefficient of a static secret key. This result has been experimentally confirmed using the reference and optimized implementations of LAC. Since our attack can break the CPA version in a misuse context, the Authenticated KE protocol, based on the CCA version, is not impacted. However, this research provides a tight estimation of LAC resilience against this type of attacks.

7.3.2 Cryptanalysis of McEliece based on subspace subcodes of Reed–Solomon codes

Participants Alain Couvreur.

In a collaboration with M. Lequesne (Cosmiq, Inria Paris), A. Couvreur worked on the cryptanalysis of a code based encryption scheme designed by Kathuria, Rosenthal and Weger [30]. This scheme generalizes in some sense McEliece's original proposal but permits to have shorter public keys. Their attack permits to break the half of the possible keys.

7.3.3 Post-quantum Signatures from Isogenies

Participants Luca De Feo, Antonin Leroux.

Digital signature is one of the most basic and important cryptographic construction. It allows a signer to produce a string of bits (the signature) from a message in order to prove that he sent that message. Along with encryption schemes, signatures constitute one of the two types of cryptographic constructions assessed by the NIST in their Post-Quantum competition launched in 2016. No signature protocol based on isogenies have been submitted to this competition and it has become an active area of research since then.

Together with David Kohel (Université de Marseille), Christophe Petit (Université Libre de Bruxelles) and Benjamin Wesolowski (Institut Mathématiques de Bordeaux), Luca de Feo and Antonin Leroux have introduced a new post-quantum signature scheme constructed from the link between isogenies of supersingular elliptic curve and quaternion algebras [12]. This new construction is the most-compact post-quantum signature scheme when looking at signature and key sizes combined. The publication includes an implementation in C of this new construction. This implementation was used to assess the performances of the new construction and it proves to be quite efficient compared to other isogeny-based solutions.

7.3.4 Faster computation of isogenies

Participants Luca De Feo, Antonin Leroux, Benjamin Smith.

7.3.5 Isogeny-based cryptography in higher dimensions

Participants Benjamin Smith, Enric Florit.

7.4 Verifiable computation

Participants Daniel Augot, Sarah Bordage, Youssef El Housni, François Morain, Jade Nardi.

Suppose a user of a small device requires a powerful computer to perform a heavy computation for him. The computation can not be performed by the device. After completion of the computation, the powerful computer reports a result. Suppose now that the user has not full confidence that the remote computer performs correctly or behaves honestly. How can the user be assured that the correct result has been returned to him, given that he can not redo the computation ?

The topic of verifiable computation deals with this issue. Essentially it is a cryptographic protocol where the prover (i.e. the remote computer) provides a proof to the verifier (i.e. the user) that a computation is correct. The protocol may be interactive, in which case there may be one or more rounds of interactions between the prover and the verifier, or non interactive, in which case the prover sends a proof that the computation is correct.

These protocols incorporate zero-knowledge variants, where the scenario is different. A service performs a computation on date, part of which remaining private (for instance statistics on citizen's incomes). It is possible for the service to prove the correctness of the result without revealing the data (which has to be committed anyway).

The two main venues for building these protocols are the setting of discrete logarithms (and pairings) in elliptic curves and a coding theoretical setting (originating to the PCP theorem). Both variants admit

a zero-knowledge version, and the core of the research is more on provable computation than the zero-knowledge aspect, which comes rather easily in comparison.

7.4.1 Verifiable computation based on coding theory

Participants Daniel Augot, Sarah Bordage, Jade Nardi.

In the coding theoretic setting, these protocols are made popular, in particular in the blockchain area, under the name of (ZK-)STARKS, *Scalable Transparent Arguments of Knowledge*, introduced in 2018. In theoretical computer science, these proofs are derived for protocols which are called IOPs *Interactive Oracle Proofs*, which are combination of IPs *Interactive Proofs* and PCPs *Probabilistically Checkable Proofs*, for combining the best of both worlds, and making PCPs pratical.

At the core of these protocols lies the following coding problem: how to decide, with high confidence, that a very long ambient word is close to a given code, while looking at very few coordinates of it.

These protocols were originally designed for the simplest algebraic codes, Reed-Solomon codes. Daniel Augot and Sarah Bordage provided a generalization of these protocols to multivariate codes, i.e. product of Reed-Solomon codes and Reed-Muller codes. It remains to assert the revelance of these codes for building proof systems and to compare to litterature, where product of Reed-Solomon codes have been studied for more than twenty years.

A very important issue is have a smaller alphabet, and this can be done using algebraic-geometric codes. This was done by Sarah Bordage and Jade Nardi [18], using curves with a resoluble automorphims group, which enable to build codes which are foldable in way similar to the Reed-Solomon codes with are folded in the "FRI" protocol [26]. Their protocol has very good perfomance, akin to the Reed-Solomon case.

7.4.2 Verifiable computation based on elliptic curves

Participants Daniel Augot, Youssef El Housni, François Morain.

Verifiable computation can also be built using the theory of ellitpic curves, the hardness of the discrete logarithms, and pairings, as introduced in [28] and made practical in [31]. These proofs are much more shorter than the ones provided by the STARKS, with a higher cost for the prover. Furthermore, these systems are not post-quantum, and there are important issues in the setting of the proof system, where a trusted third party is required.

The verifiable computation problems leads to several new questions in elliptic curves cryptographic, since the required operations depart from the standard ones used for instance in signature algorithms.

A very interesting topic is the notion of "proof of proofs". Essentially, verifying a proof is a computation, and a proof that a proof has been verified can be given. The same idea applies for verifying hundreds of proofs. A single proof can report that hundred of proofs have been checked.

This is very strong in the elliptic curve setting because the size of a proof is a constant (a few hundred bytes, only depending on the security parameter, not the computation). This means that the above hundred of statements admits a very short proof. In the blockchain world, this translates into a very short proof that many offchain transactions are correct.

To achieve this goal, this requires an ellitpic curve for proving computations done over an other elliptic curve. The problem is that there is an arithmetic mismatch: the statement which is to be proved is defined over $\mathbb{F}_r$, for a prime r which is a size of a cyclic group provided by an elliptic curve defined over $\mathbb{F}_q$. Verifying the proof requires to do computations over $\mathbb{F}_q$, and thus, for the above recursion, one needs another curve over $\mathbb{F}_{q'}$ providing a group of prime order q. Furthermore both curves must be pairing-friendly. This raises quite challenging questions, which are solved using the theory of complex multiplication.

In collaboration with Aurore Guillevic, Youssef El Housni provided curves which are very efficient for this recursion [13]. These curves beat the competition, an implementation has been provided

https://bil.inria.fr/fr/software/view/3912/tab. Some other blockchain players CELO, Consensys also have implemented this curve.

7.5 Machine learning on private data using multiplication

Participants Daniel Augot, Angelo Saadeh.

In collaboration with Matthieu Rambaud (Télécom Paris), Daniel Augot is advising Angelo Saadeh. The issue which is adressed is the following. Two parties each hold privately some distinct slices of common data. compute a logistic regression on the whole set of data, without each party revealing its data to the other party.

Computing a common output from inputs of several participants in the above is done in cryptography using MPC *Secure Multiparty Computation*, as introduced by Yao [32], and made recently practical, with several implementations. Yet, as classically observed in MPC, the actual result, when learned, may leak information about the secret inputs. The same problem occurs here, where the model may leak information about the data.

Thus it is natural to investigate the use of ϵ-differential privacy, introduced by [27] on top of MPC. This raises the concern of obtaining a reasonnable accuracy, since noise has been introduced with differential privacy. Preliminary tests have been done, using the functional mechanism of [33], that Angelo Saadeh implemented in PySyft, which is a library of cryptographic primitives building on the PyTorch machine learning platform and the obtained accuracy is actually good. A publication is in preparation.

7.6 Secure multiparty computation in blockchains

Participants Daniel Augot, Lucas Benmouffok.

The topic of MPC enables several participants to obtain a common result of a computation of each one's data, while not revealing data of others participants, without any trusted third party. This seems quite related to the blockchain philosophy, where decentralisation and trustless environments are at the core of the claimed properties of blockchains.

Actually, this is not so clear, since MPC deals with privacy and secret data, while blockchains typically imply transparency and public data. A PhD, funded by System-X, studies this possible interactions, and a model is under design. We take the idea that blockchains can enable to allocate jobs to "workers", provide them a reward for doing so, and notarize the result in the ledger. MPC would complement this by having "MPC workers" which, under the security models of MPC, could do jobs on private data submitted by clients (this could be called MPC-as-a-service). We are implementing the work of Benhamouda et al [29], with improvements with respect to the hyperledger/fabric blockchain platform, and integrating into it the Scale-Mamba MPC library.

7.7 Cloud storage

Participants Françoise Levy-Dit-Vehel, Maxime Roméas.

We build upon the work of Maurer et al. on Constructive Cryptography (CC). We rephrase the Private Information Retrieval paradigm in the CC setting. Doing so, we introduce and explicitely model interactivity in CC in the client/server setting and in the presence of a semi-honest adversary.

Updatable Encryption (UE) allows a client, who outsourced his encrypted data, to make an untrusty server update it. We propose a composable treatment of UE using CC. This allows us to assert the exact security guarantees one needs for practical UE protocols. A paper has been submitted to Crypto'21.

7.8 Fast Cornacchia algorithm

Participants François Morain.

Cornacchia's algorithm is an important building block of CM elliptic curve cryptography. Sharing many properties with fast integer gcd algorithms, we worked on a fast version for this tool. A paper was submitted at ISSAC'2021 and the code is to be available on gitlab.

8 Bilateral contracts and grants with industry

8.1 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 "Blockchains and B2B platforms", funded by CapGemini, under the French patronage laws. This chair aims at fostering teaching and doing research in topics related to blockchains, from the points of view of both computer science and economics. This chair has a co-leader, Julien Prat from the department of economics. This started in 2018, for a five years duration. Another mission of the chair is networking and outreach, see https://blockchain-chair.io. Sarah Bordage (PhD) is funded by this chair since January 2019.
- IRT System-X funds and hosts a PhD student, Lucas Benmouffok for Secure Multiparty Computation in blockchains. System-X is an organisation connecting industry and research, where research topics are built in close collaboration with industrial partners. The thesis started in October 2018. System-X launched a larger initiative, called BART, with INRIA and Télécom as partners, "blockchain advanced research and topics", https://www.bart-blockchain.fr/ which hosts Lucas Benmouffoks' thesis.
- Since October 2019, Daniel Augot and François Morain are providing PhD advisorship to one of its employees, Youssef El Housni, on the topic of zero-knowledge proofs. Then Youssef El Housni moved to consensys, still doing a PhD under François Morain and Daniel Augot guidance.
- Since October 2019, Idemia funds a CIFRE PhD student, Simon Montoya on the secure implementation in constrained environement of post-quantum cryptosystems.
- Since October 2019, Quarkslab funds a CIFRE PhD student, Alexis Challande, on the analysis of malware code
- Since November 2019, French Min. Arm. funds a PhD student, Maxime Anvari, on the analysis of the ToR network
- Under an INRIA-wide contract with Nokia called Privacy "Action de recherche", a postdoc, Adrien Hauteville, was funded since February 2019 to December 2020 on the topic of code-based security for distributed storage.

9 Partnerships and cooperations

9.1 European initiatives

9.1.1 FP7 & H2020 Projects

SPARTA

Title: Special projects for advanced research and technology in Europe

Duration: *2019 - 2020*

Coordinator: *CEA*

Partners:

- *C*ENTRE D'EXCELLENCE EN TECHNOLOGIES DE L'INFORMATION ET DE LA COMMUNICATION (Belgium)
- *C*ESNET ZAJMOVE SDRUZENI PRAVNICKYCH OSOB (Czech Republic)
- *C*OMMISSARIAT A L ENERGIE ATOMIQUE ET AUX ENERGIES ALTERNATIVES (France)
- *C*ONSIGLIO NAZIONALE DELLE RICERCHE (Italy)
- *C*ONSORZIO INTERUNIVERSITARIO NAZIONALE PER L'INFORMATICA (Italy)
- *C*ONSORZIO NAZIONALE INTERUNIVERSITARIO PER LE TELECOMUNICAZIONI (Italy)
- *C*Z.NIC, ZSPO (Czech Republic)
- *D*IREZIONE GENERALE PER LE TECNOLOGIE DELLE COMUNICAZIONI E LA SICUREZZA INFORMATICA - ISTITUTO SUPERIORE DELLE COMUNICAZIONI E DELLE TECNOLOGIE DELL'INFORMAZIONE (Italy)
- *F*RAUNHOFER GESELLSCHAFT ZUR FOERDERUNG DER ANGEWANDTEN FORSCHUNG E.V. (Germany)
- *F*UNDACIO EURECAT (Spain)
- *F*UNDACION CENTRO DE TECNOLOGIAS DE INTERACCION VISUAL Y COMUNICACIONES VICOMTECH (Spain)
- *F*UNDACION TECNALIA RESEARCH & INNOVATION (Spain)
- *G*ENEROLO JONO ZEMAICIO LIETUVOS KARO AKADEMIJA (Lithuania)
- *I*NDRA SISTEMAS SA (Spain)
- *I*NOV INESC INOVACAO - INSTITUTO DE NOVAS TECNOLOGIAS (Portugal)
- *I*NSTITUT NATIONAL DES SCIENCES APPLIQUEES DE LYON (France)
- *I*NSTITUTO SUPERIOR TECNICO (Portugal)
- *I*TTI SP ZOO (Poland)
- *J*OANNEUM RESEARCH FORSCHUNGSGESELLSCHAFT MBH (Austria)
- *K*AUNO TECHNOLOGIJOS UNIVERSITETAS (Lithuania)
- *K*ENTRO MELETON ASFALEIAS *()*
- *L*EONARDO - SOCIETA PER AZIONI (Italy)
- *L*IETUVOS KIBERNETINIU NUSIKALTIMU KOMPETENCIJU IR TYRIMU CENTRAS (Lithuania)
- *L*UXEMBOURG INSTITUTE OF SCIENCE AND TECHNOLOGY (Luxembourg)
- *M*YKOLO ROMERIO UNIVERSITETAS (Lithuania)
- *N*ATIONAL CENTER FOR SCIENTIFIC RESEARCH "DEMOKRITOS" (Greece)
- *N*AUKOWA I AKADEMICKA SIEC KOMPUTEROWA - PANSTWOWY INSTYTUT BADAWCZY (Poland)
- *S*ECRETARIAT GENERAL DE LA DEFENSE ET DE LA SECURITE NATIONALE (France)
- *S*TOWARZYSZENIE POLSKA PLATFORMA BEZPIECZENSTWA WEWNETRZNEGO (Poland)
- *T*ARTU ULIKOOL (Estonia)
- *T*ECHNIKON FORSCHUNGS- UND PLANUNGSGESELLSCHAFT MBH (Austria)

- *T*ECHNISCHE UNIVERSITAET MUENCHEN (Germany)
- *T*HALES SIX GTS FRANCE SAS (France)
- *U*NIVERSITAT KONSTANZ (Germany)
- *U*NIVERSITE DE NAMUR ASBL (Belgium)
- *U*NIVERSITE DU LUXEMBOURG (Luxembourg)
- *V*YSOKE UCENI TECHNICKE V BRNE (Czech Republic)

Inria contact: *Thomas Jensen*

Summary: *In the domain of Cybersecurity Research and innovation, European scientists hold pioneering positions in fields such as cryptography, formal methods, or secure components. Yet this excellence on focused domains does not translate into larger-scale, system-level advantages. Too often, scattered and small teams fall short of critical mass capabilities, despite demonstrating world-class talent and results. Europe's strength is in its diversity, but that strength is only materialised if we cooperate, combine, and develop common lines of research. Given today's societal challenges, this has become more than an advantage – an urgent necessity. Various approaches are being developed to enhance collaboration at many levels. Europe's framework programs have sprung projects in cybersecurity over the past thirty years, encouraging international cooperation and funding support actions. More recently, the Cybersecurity PPP has brought together public institutions and industrial actors around common roadmaps and projects. While encouraging, these efforts have highlighted the need to break the mould, to step up investments and intensify coordination. The SPARTA proposal brings together a unique set of actors at the intersection of scientific excellence, technological innovation, and societal sciences in cybersecurity. Strongly guided by concrete and risky challenges, it will setup unique collaboration means, leading the way in building transformative capabilities and forming world-leading expertise centres. Through innovative governance, ambitious demonstration cases, and active community engagement, SPARTA aims at re-thinking the way cybersecurity research is performed in Europe across domains and expertise, from foundations to applications, in academia and industry.*

9.2 National initiatives

9.2.1 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/.

9.2.2 ANR CIAO

Participants Benjamin Smith, Luca De Feo, Antonin Leroux, Mathilde Chenu.

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.

9.2.3 ANR CBCRYPT

Participants 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.

10 Dissemination

*

10.1 Promoting scientific activities

10.1.1 Scientific events: selection

Member of the conference program committees

- A. Couvreur was member of the conference program of the Code Based Cryptography workshop 2020.
- B. Smith served on the PCs of SAC (Selected Areas in Cryptography) 2020, ECC (Elliptic Curve Cryptography Workshop) 2020, and Journées Codage et Cryptographie 2020.
- D. Augot served on the PCs of ICBC2020 (IEEE International Conference on Blockchain and Cryptocurrency), CBT20 (4rth International Workshop on Cryptocurrencies and Blockchain Technology), WTSC20 (4th International Workshop on Trusted Smart Contracts)

Reviewer

- A. Couvreur has been reviewer for the conferences ISSAC, Eurocrypt, Asiacrypt and PQCrypto 2020.
- B. Smith was a reviewer for ANTS 2020, FOCS 2020, STACS 2020, and ESA 2020.

10.1.2 Journal

Member of the editorial boards

- A. Couvreur is member of the editorial board of the Publications Mathématiques de Besançon.
- F. Morain was member of the editorial board of the AAECC journal.

Reviewer - reviewing activities

- A. Couvreur has been reviewer for the journal IEEE communication letters.
- B. Smith was a reviewer for Journal of Cryptology; Mathematical Cryptology; Finite Fields and Applications; Experimental Mathematics; Journal of Algebra; RIMS Kôkyûroku Bessatsu; Publications Mathématiques de Besançon; Association of Women in Mathematics; Journal of Parallel and Distributed Computing

10.1.3 Invited talks

- B. Smith was invited speaker at SAC 2020
- B. Smith was invited speaker at PQCrypto 2020
- B. Smith was invited speaker at the RIMS conference Theory and Applications of Supersingular Curves and Supersingular Abelian Varieties

10.1.4 Leadership within the scientific community

- A. Couvreur is responsible of the Groupe de travail C2 (codes et cryptographie) of the CNRS' GdR Informatique Mathématiques.

10.1.5 Scientific expertise

- A. Couvreur was member of a Comité de sélection for a Maître de conférences position at Université Paris 8.
- A. Couvreur was referee for the Spanish prize "Premio Banco de Sabadell for Science and Engineering".
- B. Smith was a selection committee member for a Maître des conférences position at Télécom Paris Sud.
- D. Augot was member of a selection committee member of Professeur Associé Universitaire at University of Rouen.
- G. Renault was member of a Comité de Sélection for a Maître de conférences position for the DIX at École Polytechnique.

10.1.6 Research administration

- A. Couvreur is elected member of Inria's Commission d'évaluation.
- A. Couvreur is appointed member (*membre nommé*) of Conseil National des Universités (CNU) Section 25 (Mathématiques)
- A. Couvreur was member of the Commission scientifique of Inria's Centre de Saclay Île-de-France up to september 2020.
- A. Couvreur is member of the comité scientifique of Labex de Mathématiques Jacques Hadamard.
- B. Smith is a member of the scientific committee of Labex Digicosme.
- B. Smith has been a member of the Commission scientifique of Inria's Saclay–Île-de-France research centre since November 2020.

10.2 Teaching - Supervision - Juries

10.2.1 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
- 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, INF558, *Introduction to cryptology*, 36h, M1, École Polytechnique. This special year included video making of all his courses.
- 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. The lectures were all given in live video.
- Master : F. Levy-dit-Vehel, discrete maths, 21h, M1, ENSTA.
- Master : F. Levy-dit-Vehel, cryptography, 24h, M2, ENSTA.
- Master Cybersecurity: D. Augot, cryptography in blockchains, 24h, M2.
- Master : G. Renault: Lectures and Labs for *INF565: Information Systems Security*, 60h, M1, École polytechnique, France
- Master : G. Renault: Lectures and Labs for *INF648: Embedded security: side-channel attacks; javacard*, 60h, M2, École polytechnique, France
- Master : G. Renault: Coordinator for *INF637: Reverse engineering vs Obfuscation*, 2h, M2, École polytechnique, France

10.2.2 Juries

- A. Couvreur was jury member and referee of the thesis of Nicolas Aragon (Université de Limoges)
- B. Smith was jury member for the thesis of Sudarshan Shinde (UPMC)
- D. Augot was review of the PhD thesis of Doriane Pérard, "Blockchain et stockage efficace", University of Toulouse, 16/12/2020
- D. Augot was member of the jury of the PhD defense of Hung Dang, "Complexité scalaire des algorithmes de type Chudnovsky de multilication dans les corps finis", University Aix-Marseille 25/05/2020
- D. Augot was member of the jury of the Habilitation à diriger des recherches de Delphine Boucher, "Autour de codes définis à l'aide de polynômes tordus", University of Rennes 2/6/2020
- D. Augot was reviewer of the PhD thesis ofIlaria Zappatore, "Reconstruction Rationnelle Simultanée et applications à la Théorie des Codes Correcteurs d'Erreurs", University of Montpellier, 16/10/2020
- D. Augot was reveiwer of the PhD thesis of Aido Diop, "Cryptographic Mechanisms for Device Authentication and Attestation in the Internet of Things", Institut Polytechnique de Paris, 30/11/2020
- D. Augot was member of the jury of Kevin Carrier, "Recherche de presque-collisions pour le décodage et la reconnaissance de codes correcteurs", Sorbonne University, 19/06/2020
- G. Renault was president of the jury of the phd thesis of Fangan Yssouf Dosso (Université de Toulon)
- G. Renault was jury member of the phd thesis of Lucas Barthelemy (Sorbonne Université)

10.3 Popularization

10.3.1 Internal or external Inria responsibilities

- A. Couvreur is member of the Comité de Culture Mathématiques of Institut Henri Poincaré.
- A. Couvreur is correspondant de médiation scientifique of Inria's centre de Saclay Île-de-France.

10.4 External duties

- F. Levy-dit-Vehel Represents the "enseignants-chercheurs" at the "conseil de laboratoire" of LIX.
- F. Morain represents the axis *networks and security* at the "conseil de direction" of LIX.

11 Scientific production

11.1 Major publications

[1] D. J. Bernstein, L. De Feo, A. Leroux and B. Smith. 'Faster computation of isogenies of large prime degree'. In: *ANTS-XIV - 14th Algorithmic Number Theory Symposium*. Ed. by S. Galbraith. Vol. 4. Proceedings of the Fourteenth Algorithmic Number Theory Symposium (ANTS-XIV). Auckland, New Zealand: Mathematical Sciences Publishers, June 2020, pp. 39–55. DOI: 10.2140/obs.2020.4.39. URL: https://hal.inria.fr/hal-02514201.

[2] L. De Feo, D. Kohel, A. Leroux, C. Petit and B. Wesolowski. 'SQISign: compact post-quantum signatures from quaternions and isogenies'. In: *ASIACRYPT 2020 - 26th Annual International Conference on the Theory and Application of Cryptology and Information Security*. Daejeon (virtual), South Korea: Association for Computing Machinery, Dec. 2020. URL: https://hal.archives-ouvertes.fr/hal-03038004.

11.2 Publications of the year

International journals

[3] R. Blache, A. Couvreur, E. Hallouin, D. Madore, J. Nardi, M. Rambaud and H. Randriambololona. 'Anticanonical codes from del Pezzo surfaces with Picard rank one'. In: *Transactions of the American Mathematical Society* (2020). DOI: 10.1090/tran/8119. URL: https://hal.archives-ouvertes.fr/hal-02075926.

[4] W. Castryck, T. Decru and B. Smith. 'Hash functions from superspecial genus-2 curves using Richelot isogenies'. In: *Journal of Mathematical Cryptology* 14.1 (7th Aug. 2020), p. 25. DOI: 10.1515/jmc-2019-0021. URL: https://hal.inria.fr/hal-02067885.

[5] D. Coggia and A. Couvreur. 'On the security of a Loidreau rank metric code based encryption scheme'. In: *Designs, Codes and Cryptography* 88.9 (Sept. 2020), pp. 1941–1957. DOI: 10.1007/s10623-020-00781-4. URL: https://hal.archives-ouvertes.fr/hal-03049694.

[6] A. Couvreur and I. Panaccione. 'Power Error Locating Pairs'. In: *Designs, Codes and Cryptography* 88.8 (Aug. 2020), pp. 1561–1593. DOI: 10.1007/s10623-020-00774-3. URL: https://hal.archives-ouvertes.fr/hal-02196650.

[7] N. Coxon. 'Fast transforms over finite fields of characteristic two'. In: *Journal of Symbolic Computation* 104 (2021), pp. 824–854. DOI: 10.1016/j.jsc.2020.10.002. URL: https://hal.archives-ouvertes.fr/hal-01845238.

[8] J. Lavauzelle, R. Tajeddine, R. Freij-Hollanti and C. Hollanti. 'Private Information Retrieval Schemes with Product-Matrix MBR Codes'. In: *IEEE Transactions on Information Forensics and Security* 16 (2021), pp. 441–450. DOI: 10.1109/TIFS.2020.3003572. URL: https://hal.archives-ouvertes.fr/hal-01951956.

International peer-reviewed conferences

[9] S. Abelard, A. Couvreur and G. Lecerf. 'Sub-quadratic time for Riemann-Roch spaces. The case of smooth divisors over nodal plane projective curves'. In: ISSAC 2020 - 45th International Symposium on Symbolic and Algebraic Computation. Proceedings of the 45th International Symposium on Symbolic and Algebraic Computation. Kalamata, Greece, 2020, pp. 14–21. DOI: 10.1145/3373207.3404053. URL: https://hal.inria.fr/hal-02477371.

[10] D. J. Bernstein, L. De Feo, A. Leroux and B. Smith. 'Faster computation of isogenies of large prime degree'. In: *Open Book Series*. ANTS-XIV - 14th Algorithmic Number Theory Symposium. Vol. 4. Proceedings of the Fourteenth Algorithmic Number Theory Symposium (ANTS-XIV). Auckland, New Zealand, 29th June 2020, pp. 39–55. DOI: 10.2140/obs.2020.4.39. URL: https://hal.inria.fr/hal-02514201.

[11] C. Costello and B. Smith. 'The supersingular isogeny problem in genus 2 and beyond'. In: PQCrypto 2020 - 11th International Conference on Post-Quantum Cryptography. Paris, France, 15th Apr. 2020. URL: https://hal.inria.fr/hal-02389073.

[12] L. De Feo, D. Kohel, A. Leroux, C. Petit and B. Wesolowski. 'SQISign: compact post-quantum signatures from quaternions and isogenies'. In: ASIACRYPT 2020 - 26th Annual International Conference on the Theory and Application of Cryptology and Information Security. Daejeon (virtual), South Korea, 7th Dec. 2020. URL: https://hal.archives-ouvertes.fr/hal-03038004.

[13] Y. El Housni and A. 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. Vienna, Austria: https://cans2020.at/, 14th Dec. 2020. URL: https://hal.inria.fr/hal-02962800.

[14] A. Greuet, S. Montoya and G. Renault. 'Attack on LAC Key Exchange in Misuse Situation'. In: CANS 2020 - 19th International conference on Cryptology and Network Security. Vienna, Austria, 14th Dec. 2020. URL: https://hal.inria.fr/hal-03046345.

Scientific book chapters

[15] A. Couvreur and H. Randriambololona. 'Algebraic geometry codes and some applications'. In: *A Concise Encyclopedia of Coding Theory*. A Concise Encyclopedia of Coding Theory. 2020. URL: https://hal.archives-ouvertes.fr/hal-02931167.

Reports & preprints

[16] S. Abelard, A. Couvreur and G. Lecerf. *Efficient computation of Riemann-Roch spaces for plane curves with ordinary singularities*. 14th Jan. 2021. URL: https://hal.archives-ouvertes.fr/hal-03110135.

[17] D. Augot, A. Couvreur, J. Lavauzelle and A. Neri. *Rank-metric codes over arbitrary Galois extensions and rank analogues of Reed-Muller codes*. 26th June 2020. URL: https://hal.archives-ouvertes.fr/hal-02882019.

[18] S. Bordage and J. Nardi. *Interactive Oracle Proofs of Proximity to Algebraic Geometry Codes*. 16th Feb. 2021. URL: https://hal.archives-ouvertes.fr/hal-03142459.

[19] A. Couvreur, T. Debris-Alazard and P. Gaborit. *On the hardness of code equivalence problems in rank metric*. 10th Nov. 2020. URL: https://hal.archives-ouvertes.fr/hal-02997801.

[20] A. Couvreur, P. Lebacque and M. Perret. *Toward good families of codes from towers of surfaces*. 7th Feb. 2020. URL: https://hal.archives-ouvertes.fr/hal-02470343.

[21] A. Couvreur and M. Lequesne. *On the security of subspace subcodes of Reed-Solomon codes for public key encryption*. 15th Sept. 2020. URL: https://hal.archives-ouvertes.fr/hal-02938812.

[22] S. Dobson, S. Galbraith and B. Smith. *Trustless Groups of Unknown Order with Hyperelliptic Curves*. June 2020. URL: https://hal.inria.fr/hal-02882161.

[23] E. Florit and B. Smith. *An atlas of the Richelot isogeny graph*. 4th Jan. 2021. URL: https://hal.inria.fr/hal-03094296.

[24] E. Florit and B. Smith. *Automorphisms and isogeny graphs of abelian varieties, with applications to the superspecial Richelot isogeny graph*. 2020. URL: https://hal.inria.fr/hal-03094375.

[25] J. Lavauzelle, P. Loidreau and B.-D. Pham. *RAMESSES, a Rank Metric Encryption Scheme with Short Keys*. 2nd Jan. 2020. URL: https://hal.archives-ouvertes.fr/hal-02426624.

11.3 Cited publications

[26] E. Ben-Sasson, I. Bentov, Y. Horesh and M. Riabzev. 'Fast Reed-Solomon Interactive Oracle Proofs of Proximity'. In: *45th International Colloquium on Automata, Languages, and Programming, ICALP 2018, July 9-13, 2018, Prague, Czech Republic*. 2018, 14:1–14:17.

[27] C. Dwork, F. McSherry, K. Nissim and A. Smith. 'Calibrating Noise to Sensitivity in Private Data Analysis'. In: *Theory of Cryptography*. Ed. by T. Halevi Shaiand Rabin. Berlin, Heidelberg, 2006, pp. 265–284.

[28] J. Groth. 'Short Pairing-Based Non-interactive Zero-Knowledge Arguments'. In: *Advances in Cryptology - ASIACRYPT 2010*. Ed. by M. Abe. Berlin, Heidelberg: Springer Berlin Heidelberg, 2010, pp. 321–340.

[29] T. Halevi, F. Benhamouda, A. D. Caro, S. Halevi, C. Jutla, Y. Manevich and Q. Zhang. 'Initial Public Offering (IPO) on Permissioned Blockchain Using Secure Multiparty Computation'. In: *2019 IEEE International Conference on Blockchain (Blockchain)*. 2019, pp. 91–98. DOI: 10.1109/Blockchain.2019.00021.

[30] K. Khathuria, J. Rosenthal and V. Weger. 'Encryption Scheme Based on Expanded Reed–Solomon Codes'. In: (2019). In Press. DOI: 10.3934/amc.2020053. URL: http://aimsciences.org//article/id/0f055199-6fe4-404f-b206-517ce7d02a58.

[31] B. Parno, J. Howell, C. Gentry and M. Raykova. 'Pinocchio: Nearly Practical Verifiable Computation'. In: *Commun. ACM* 59.2 (Jan. 2016), pp. 103–112.

[32] A. C.-C. Yao. 'Protocols for Secure Computations (Extended Abstract)'. In: *FOCS*. IEEE Computer Society, 1982, pp. 160–164.

[33] J. Zhang, Z. Zhang, X. Xiao, Y. Yang and M. Winslett. 'Functional mechanism: regression analysis under differential privacy'. In: *arXiv preprint arXiv:1208.0219* (2012).