RESEARCH CENTRE

Inria Saclay Center at Institut Polytechnique de Paris

IN PARTNERSHIP WITH:

CNRS, Institut Polytechnique de Paris

2022 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 Project-Team: 2013 July 01

Keywords

Computer sciences and digital sciences

A2.3.1. – Embedded systems

A4.2. – Correcting codes

A4.3.1. – Public key cryptography

A4.3.3. – Cryptographic protocols

A4.4. – Security of equipment and software

A4.6. – Authentication

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

B6.4. – Internet of things

B6.6. – Embedded systems

B9.5.1. – Computer science

B9.5.2. – Mathematics

B9.10. – Privacy

1 Team members, visitors, external collaborators

Research Scientists

- Alain Couvreur [Team leader, INRIA, Senior Researcher, HDR]
- Daniel Augot [INRIA, Senior Researcher, HDR]
- Thomas Debris-Alazard [INRIA, Researcher]
- Benjamin Smith [INRIA, Researcher]

Faculty Members

- Olivier Blazy [LIX, Professor, HDR]
- Françoise Levy-Dit-Vehel [ENSTA, Associate Professor, HDR]
- François Morain [LIX, Professor, HDR]

Post-Doctoral Fellows

- Gustavo Banegas [Inria, until Jul 2022]
- Matthieu Lequesne [Inria, from Dec 2022]
- Azam Soleimanian [LIX, until Feb 2022]
- Ilaria Zappatore [Inria, until Aug 2022]

PhD Students

- Anaïs Barthoulot [ORANGE]
- Maxime Bombar [LIX]
- Sarah Bordage [École Polytechnique, until Jun 2022]
- Alexis Challande [QUARKSLAB, until Oct 2022]
- Clément Ducros [UNIV PARIS CITÉ]
- Youssef El Housni [CONSENSYS, until Nov 2022]
- Anaelle Le Devehat [Inria, from Jul 2022]
- Antonin Leroux [LIX, until Aug 2022]
- Simon Montoya [IDEMIA, until Oct 2022]
- Maxime Romeas [LIX, until Nov 2022]
- Angelo Saadeh [TELECOM PARIS, until Aug 2022]

Administrative Assistant

- Maria Ronco [INRIA]

External Collaborators

- Philippe Lebacque [UNIV FRANCHE-COMTE]
- Matthieu Rambaud [MINESPARISTECH, from Sep 2022]
- Guenael Renault [SGDSN]

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 implementations, 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 geometry 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: François Morain, Benjamin Smith, 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: François Morain, Benjamin Smith, 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: Gustavo Banegas, François Morain, Benjamin Smith, Anaelle Le Devehat, 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, Maxime Bombar, Clément Ducros.

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 against 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.

3.5 Post-quantum cryptography

Participants: Gustavo Banegas, Maxime Bombar, Alain Couvreur, Thomas Debris-Alazard, Anaelle Le Devehat, Antonin Leroux, Benjamin Smith, O. Blazy
.

Theme: Cryptography

A huge amount of work is being put into developing an efficient quantum computer. But even if the advent of such a computer may wait for decades, it is urgent to deploy post-quantum cryptography (PQC), *i.e:* solutions on our current devices that are quantum-safe. Indeed, an attacker could store encrypted sessions and wait until a quantum computer is available to decrypt. In this context the National Institute of Standard Technology (NIST) has launched in 2017 (see this website) a call for standardizing public-key PQC schemes (key exchanges and signatures). Among the mathematical objects to design post quantum primives, one finds error correcting codes, Euclidean lattices and isogenies.

We are currently in the final step of the standardization of the NIST and most of the selected solutions are based on codes and lattices. These preliminary results tend to show that codes and lattices will be in a near future at the ground of our numerical security. If isogenies are less represented, they remain of deep interest since they appear to be the post quantum solution providing the smallest key sizes. The purpose of our research program is to bring closer these solutions for a post-quantum security in order to improve their efficiency, diversity and to increase our trust in these propositions.

3.6 Proofs of Computation

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

Proofs of computation are cryptographic protocols which allow a prover to convince a verifier that a statement or an output of a computation is correct. The prover is untrusted in the sense that it may try to convince the verifier that a false statement is true. On the other hand the prover is computationnally restricted, and have very small prower: the proof should be short and easy to verify. They can be interactive or not.

While the topic originates back to 1990, several important steps towards praticality has been made in last decade, with efficient, real-life implementations and industrial deployments in the last years, thanks to huge fundings.

There are several cryptographic paths for designing such proof systems. Within Grace, two main techniques are investigated. The first one relies on elliptic curves and pairings, and produce very short (constant-size) proofs. Y. El Housni defended his PhD on this topic, in particular on the arithmetic and implementation aspects. The second techniques relies on algebraic coding theory, with smaller cryptographic assumptions (cryptographic hash functions), and is post-quantum, but provides longer proofs. S. Bordage defended her PhD on this second kind of techniques, extending existing proofs using Reed-Solomon codes to more general class of codes, like product of codes and algebraic-geometry codes.

4 Application domains

4.1 Application Domain: cybersecurity

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

We are interested 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, Youssef El Housni, François Morain, Matthieu Rambaud.

The huge hype about blockchains attracted the attention of many companies towards advanced cryptographic protocols. While basic and standard blockchain ideas rely, on the cryptographic side, on very basic and standard cryptographic primitives like signatures and hash functions, more elaborate techniques from crypto can alleviate some shortcomings of blockchain, like the poor bandwith and the lack of privacy.

The topic of verifiable computation consists in verifying heavy computations done by a remote computer, using a lightweight computer which is not able to do the computation. The remore computer, called the prover, is allowed to provided a proof aside the result of the computation. This proof must be very short and fast to verify. It can also be made zero-knowledge, where the prover hides some inputs to the computation, and yet prove the result is correct.

There are two competing propositions which provide a mathematical and algorithmic background for these proof techniques: one based on a line of research dating back to the celebrated 1990 PCP theorem (error correcting codes), and one based on the discrete logarithm problem and pairing based protocols (elliptic curves over finite fields). D. Augot is advising S. Bordage on the first topic, also known in the blockchain world as “STARKS” (Scalable Transparent Arguments of Knowledge), and F. Morain is advising Youssef El Housni on the second topic, known as “SNARKS” (Succint Non Interactive Arguments of Knowledge).

These proofs allows to move data and computation off chain, pushing the burden to off-chain servers, who then commit short commitments of the update of their offchain data , accompanied by short proofs which are easy to verify onchain. This mecanism is called a *rollup* and is at the core of the proposed path for scaling Ethereum, a predominant blockchain, which will be “rollup-centric”.

Also Daniel Augot, together with Julien Prat (economist, ENSAE), is co-leading a Polytechnique teaching and research “chair”, called *Blockchain and B2B plaforms*, funded by CapGemini, Caisse des dépots and NomadicLabs. This is patronage, which funded Sarah Bordage’s PhD thesis. This gives visiblity and outreach beyond the academic sphere.

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 for the effective constuction of protocols. To this respect, we mainly use locally decodable codes and in particular high-rate lifted codes.

Maxime Roméas is a PhD student of the team. (PhD grant from IP Paris/Ecole Polytechnique for a 3-year doctorate, Oct 2019-Sept 2022). The subject of his thesis is "The Constructive Cryptography paradigm applied to Interactive Cryptographic Proofs".

The Constructive Cryptography framework, introduced by Maurer in 2011, 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. Another axis of the PhD is to augment the CC model by, e.g., introducing new functionalities to a so-called Server Memory Resource.

5 Highlights of the year

5.1 European Project ENCODE granted

Participants: D. Augot , A. Couvreur , F. Levy-dit-Vehel .

The project ENCODE is a doctoral network project submitted to the call *Horizons Marie Słodowska-Curie Actions - Doctoral Networks 2021*. The project's principal investigator is Eimear Byrne from university college Dublin. Grace Team is one of the 5 poles of the project. The project has been granted and got the grade 100%. It was ranked 1st among more than 1000 projects. ENCODE starts in march 2023.

5.2 AEx CACHAÇA

Participants: B. Smith .

The *Action Exploratoire* CACHAÇA, led by Benjamin Smith and based at Campus Cyber, started in 2022. Fast, safe, and strong cryptography is essential for secure networked communications. Currently, high-assurance techniques from formal methods are only applied once cryptosystems reach maturity and standardization. CACHAÇA will bring these techniques to the initial design and implementation phase for new postquantum cryptosystems, to produce fast, safe, and portable software implementations, especially for constrained environments such as IoT devices.

5.3 Defences

Participants: Sarah Bordage, Alexis Challande, Youssef El Housni, Antonin Leroux, Simon Montoya, Maxime Roméas.

6 Ph.D. Students of the team defended their thesis during the last year:

- Sarah Bordage (June 16, 2022)
- Antonin Leroux (September 7, 2022)

- Alexis Challande (October 11, 2022)
- Simon Montoya (October 12, 2022)
- Youssef El Housni (November 18, 2022)
- Maxime Roméas (November 29, 2022)

5.4 Lack of consideration for research from our management

Participants: Whole Team.

We are concerned that our management neglects research of high quality, or even research by itself, showing preference for short term, short lived activities, judged by their “impact”, whatever it means.

We are proud that INRIA has a quality national evaluation committee (“commission d’évaluation”, CE) in charge of evaluating the scientific activity and merit of individual researchers. The committee members do a deep, sensible and thorough scientific analysis of each researcher’s file, well beyond publications and bibliometrics. This give us strong confidence that recruitments are of high quality, that promotions are done on the core, real-life, and meaningful basis of our activity. Yet, during last year, our evaluation committee has been under veiled and constant criticism by our top management. We fear that future recruitments will be not based on scientific merit, lowering the quality of research done at INRIA.

Finally, please take note also that new information system “EKSAE” has been deployed at INRIA. EKSAE is completely malfunctioning and is a plague to administrative staff, who can not handle basic tasks. Ph.D. students are not reimbursed for their trips to conferences, invited researchers are not reimbursed for their cost, experts doing reports for the evaluation committee (CE) are not paid. At the international level, this destroys any credit INRIA could have, ashames us, and forbid us to establish important scientific connections.

6 New software and platforms

6.1 New software

6.1.1 snark-2-chains

Name: Families of SNARK-friendly 2-chains of elliptic curves

Keywords: Cryptography, Cryptocurrency, Blockchain

Functional Description: This small library implements finite field and elliptic curve arithmetic for BN curves (Barreto-Naehrig), BLS curves (Barreto-Lynn-Scott), and 2-chains made of BW6 (Brezing-Weng curves of embedding degree 6), CP8, CP12 (Cocks-Pinch curves of embedding degree 8 and 12) 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 tied to a preprint and is not optimized.

News of the Year: The library was first released in October 2021.

URL: `https://gitlab.inria.fr/zk-curves/snark-2-chains`

Publication: hal-03371573

Contact: Aurore Guillevic

7 New results

7.1 Post–quantum cryptography

7.1.1 Improved decoding of Gabidulin codes for various noise models

Participants: Maxime Bombar, Alain Couvreur.

When considering error correcting codes, one usually endows the ambient space with the Hamming metric. However, other metrics have been considered, and in particular, codes endowed with the rank metric have found applications in cryptography, in network communications or in data storage. Compared to the Hamming world, only few families of codes endowed with the rank metric are known to have efficient decoding algorithms. As the rank metric analogues of Reed-Solomon codes, $[n,k]$ Gabidulin codes are of particular interest because they are somehow optimal: they reach the rank-metric Singleton bound and benefit from efficient decoders uniquely correcting any error pattern of weight up to $\frac{n-k}{2}$. However, in general, there exists no known decoders in polynomial time beyond this bound, even probabilistic ones. Nonetheless, previous works have considered different noise models for which decoders can be given. For instance, when considering u codewords in parallel such that the channel corrupts all of them at once (this process is known as *interleaving*), it is possible to give a probabilistic decoder correcting up to $\frac{u}{u+1}(n-k)$ rank errors, or when the error has a specific symmetric structure (more precisely when the row and column spaces of the error are equal), it is possible correct errors up to rank $\frac{3}{2}(n-k)$.

In [42], A. Couvreur and M. Bombar build on their previous work [67] to give a new decoder of interleaved Gabidulin codes, working on the right-hand side, which gives a simpler point of view on the decoding of such error patterns.

In [67], A. Couvreur proves that when the codes have rate $\frac{k}{n} < \frac{1}{2}$, it is possible to correct any symmetric error pattern, whatever its rank, without failure. This algorithm works for a broad family of codes which includes the aforementioned Gabidulin codes. Moreover, when the rate is larger than $\frac{1}{2}$, it achieves the best decoding radius conjectured in the literature for such noise model.

7.1.2 Search-to-decision reductions in code–based cryptography

Participants: A. Couvreur , M. Bombar , T. Debris–Alazard .

The security of most code–based cryptosystem relies on the hardness of the so–called Decoding Problem. If its search version (Given a random linear code, and a noisy codeword, it should be hard to decode, *i.e.* to remove the error and recover the original message) is quite well understood, many proposals actually rely on the *decision version* which can be formulated as follows: Given a random linear code it should be hard to distinguish between a uniformly random vector of the ambiant space, and a noisy codeword. This decision version can be thought as the code–based analogue of the Decisional Diffie Hellman problem, and for general random linear codes both search and decision problem are known to be equivalent. Such a result is known as a *search to decision reduction.* However, for efficiency purposes, it is very appealing to use algebraically structured codes such as quasi-cyclic codes, that can be represented more compactly. In this situation, the hardness of the decision Decoding problem is only conjectured. On the other hand, one of the reasons of the success of lattice–based cryptography is that it benefits from a rich literature of security reductions for both general lattices and so–called *structured lattices, i.e.* lattices arising from orders of number fields.

In [29], based on a strong analogy between number fields and function fields, and especially using Carlitz modules which can be somehow considered as an analogue of cyclotomic number fields in positive characteristics, we introduce a new generic problem that we call FUNCTION FIELD DECODING PROBLEM, and derive the first search to decision reduction in this context.

7.1.3 New algorithm to solve the generic decoding problem

Participants: T. Debris–Alazard .

The security of code-based cryptography relies primarily on the hardness of generic decoding with linear codes. The best generic decoding algorithms are all improvements of an old algorithm due to Prange: they are known under the name of information set decoders (ISD). A while ago, a generic decoding algorithm which does not belong to this family was proposed: statistical decoding. It is a randomized algorithm that requires the computation of a large set of parity-checks of moderate weight, and uses some kind of majority voting on these equations to recover the error we are looking for in the decoding problem. This algorithm was long forgotten because even the best variants of it performed poorly when compared to the simplest ISD algorithm. In [31], we revisit this old algorithm by using parity-check equations in a more general way. Here the parity-checks are used to get LPN samples with a secret which is part of the error and the LPN noise is related to the weight of the parity-checks we produce. The corresponding LPN problem is then solved by standard Fourier techniques. By properly choosing the method of producing these low weight equations and the size of the LPN problem, we are able to outperform in this way significantly information set decoders at code rates smaller than 0.3. It gives for the first time after 60 years, a better decoding algorithm for a significant range which does not belong to the ISD family. »»»> 5a27469fe7075e10a50ee82951408ab3de01783b

In [42], A. Couvreur and M. Bombar build on their previous work [66] to give a new decoder of *interleaved* Gabidulin codes, working on the *right-hand side*, which gives a simpler point of view on the decoding of such error pattern.

In [55], A. Couvreur proves that when the codes have rate $\frac{k}{n} < 1/2$, it is possible to correct *any* symmetric error pattern, whatever its rank, without failure. This algorithm works for a broad family of codes which includes the aformentioned Gabidulin codes. Moreover, when the rate is larger than $1/2$, he achieves the best decoding radius conjectured in the litterature for such noise model.

7.1.4 Quantum reduction

Participants: Thomas Debris-Alazard.

We give a quantum reduction from finding short codewords in a random linear code to decoding for the Hamming metric. This is the first time such a reduction (classical or quantum) has been obtained. Our reduction adapts to linear codes Stehlé-Steinfield-Tanaka- Xagawa's re-interpretation of Regev's quantum reduction from finding short lattice vectors to solving the Closest Vector Problem. The Hamming metric is a much coarser metric than the Euclidean metric and this adaptation has needed several new ingredients to make it work. For instance, in order to have a meaningful reduction it is necessary in the Hamming metric to choose a very large decoding radius and this needs in many cases to go beyond the radius where decoding is unique. Another crucial step for the analysis of the reduction is the choice of the errors that are being fed to the decoding algorithm. For lattices, errors are usually sampled according to a Gaussian distribution. However, it turns out that the Bernoulli distribution (the analogue for codes of the Gaussian) is too much spread out and can not be used for the reduction with codes. Instead we choose here the uniform distribution over errors of a fixed weight and bring in orthogonal polynomials tools to perform the analysis and an additional amplitude amplification step to obtain the aforementioned result.

The result is presented in the preprint [56].

7.1.5 LLL like algorithm for codes

Participants: Thomas Debris-Alazard.

In [18], we have proposed an adaptation of the algorithmic reduction theory of lattices to binary codes. This includes the celebrated LLL algorithm (Lenstra, Lenstra, Lovasz, 1982), as well as adaptations of associated algorithms such as the Nearest Plane Algorithm of Babai (1986). Interestingly, the adaptation of LLL to binary codes can be interpreted as an algorithmic version of the bound of Griesmer (1960) on the minimal distance of a code. Using these algorithms, we demonstrate —both with a heuristic analysis and in practice— a small polynomial speed-up over the Information-Set Decoding algorithm of Lee and Brickell (1988) for random binary codes. This appears to be the first such speed-up that is not based on a time-memory trade-off. The above speed-up should be read as a very preliminary example of the potential of a reduction theory for codes, for example in cryptanalysis.

7.1.6 Wavelet: Code-based postquantum signatures with fast verification on microcontrollers

Participants: Gustavo Banegas, Thomas Debris-Alazard, Benjamin Smith.

This work [63] has presented the first full implementation of Wave, a postquantum code-based signature scheme. We define Wavelet, a concrete Wave scheme at the 128-bit classical security level (or NIST postquantum security Level 1) equipped with a fast verification algorithm targeting embedded devices. Wavelet offers 930- byte signatures, with a public key of 3161 kB. We include implementation details using AVX instructions, and on ARM Cortex-M4, including a solution to deal with Wavelet's large public keys, which do not fit in the SRAM of a typical embedded device. Our verification algorithm is approximately 4.65 times faster then the original, and verifies in 1 087 538 cycles using AVX instructions, or 13 172 ticks in an ARM Cortex-M4.

7.1.7 Quantum-resistant software update security on low-power networked embedded devices

Participants: Gustavo Banegas, Benjamin Smith.

Bringing practical post-quantum security to low-end IoT devices is a pressing challenge. In [64] we evaluate a range of pre- and post-quantum secure signature schemes in the context of SUIT software updates (specified by the IETF), on three popular, off-the-shelf microcontroller boards (ARM Cortex-M4, ESP32, and RISC-V) that are representative of the 32-bit landscape. We show that upgrading to postquantum security is practical now, and reflect on the best choices for various use cases. This work was selected for presentation at Real World Crypto 2022, and was published at ACNS 2022.

7.1.8 On Using RSA/ECC Coprocessor for Ideal Lattice-Based Key Exchange

Participants: Guenael Renault, Simon Montoya.

Polynomial multiplication is one of the most costly operations of ideal lattice-based cryptosystems. In [71], with Aurélien Greuet (Idemia), we study its optimizations when one of the operands has coefficients close to 0. We focus on this structure since it is at the core of lattice-based Key Encapsulation Mechanisms submitted to the NIST call for post-quantum cryptography. In particular, we propose optimization of this operation for embedded devices by using a RSA/ECC coprocessor that provides efficient and secure large-integer arithmetic. In this context, we compare Kronecker Substitution, with two specific algorithms that we introduce: KSV, a variant of this substitution, and an adaptation of the schoolbook multiplication, denoted Shift&Add. All these algorithms rely on the transformation of polynomial multiplication to large-integer arithmetic. Then, thanks to these algorithms, existing secure coprocessors dedicated to large-integer can be re-purposed in order to speed-up post-quantum schemes. The efficiency of these algorithms depends on the component specifications and the cryptosystem parameters set. Thus, we establish a methodology to determine which algorithm to use, for a given component, by only implementing basic large-integer operations. Moreover, the three algorithms are assessed on a chip ensuring that the theoretical methodology matches with practical results.

7.1.9 Security Assessment of NTRU Against Non-Profiled SCA

Participants: Guenael Renault, Simon Montoya.

NTRU was first introduced by J. Hoffstein, J. Pipher and J.H Silverman in 1998. Its security, efficiency and compactness properties have been carefully studied for more than two decades. A key encapsulation mechanism (KEM) version was even submitted to the NIST standardization competition and made it to the final round. Even though it has not been chosen to be a new standard, NTRU remains a relevant, practical and trustful post-quantum cryptographic primitive. In [25], with Luk Bettale (Idemia), Julien Eynard (ANSSI) and Rémi Strullu (ANSSI), we investigate the side-channel resistance of the NTRU Decrypt procedure. In contrast with previous works about side-channel analysis on NTRU, we consider a weak attacker model and we focus on an implementation that incorporates some side-channel countermeasures. The attacker is assumed to be unable to mount powerful attacks by using templates or by forging malicious ciphertexts for instance. In this context, we show how a non-profiled side-channel analysis can be done against a core operation of NTRU decryption. Despite the considered countermeasures and the weak attacker model, our experiments show that the secret key can be fully retrieved with a few tens of traces.

7.1.10 Post-quantum Public Key Encryption from Isogenies

Participants: Luca De Feo, Antonin Leroux.

Together with Cyprien Delpech de Saint Guilhem (KU Leuven), Tako Boris Fouotsa (Universit'a Degli Studi Roma Tre), Peter Kutas (University of Birmingham), Christophe Petit (Université Libre de Bruxelles), Javier Silva (Universitat Pompeu Fabra)and Benjamin Wesolowski (Institut Mathématiques de Bordeaux), Luca de Feo and Antonin Leroux have introduced a new post-quantum public key encryption scheme that uses constructively the torsion point attack against the SIDH key exchange. The publication includes an implementation in C of this new construction. Another contribution of this work is the "uber-isogeny assumption" which aims at generalizing some computational assumption encountered in various scheme of the literature.

7.1.11 High-speed supersingularity testing for elliptic curves

Participants: Gustavo Banegas, Benjamin Smith.

Elliptic curves over finite fields are either *ordinary* or *supersingular*. Distinguishing supersingular elliptic curves is an important task in algorithmic number theory, and now forms a crucial step in public-key validation for some isogeny-based cryptosystems such as CSIDH. In [13], we improve the state-of-the-art of supersingularity testing, especially over $\mathbb{F}_p$ for cryptographic applications, with faster algorithms backed up with high-speed software implementations.

7.1.12 The suborder isogeny representation and pSIDH

Participants: Antonin Leroux.

The tasks of evaluating and verifying isogenies are fundamental for isogeny-based cryptography. The *suborder representation* introduced in [37] and presented at ASIACRYPT 2022 targets the case of (big) prime-degree isogenies. The core of our new method is the revelation of endomorphisms of smooth norm inside a well-chosen suborder of the codomain's endomorphism ring. This new representation appears to be opening interesting prospects for isogeny-based cryptography under the hardness of a new computational problem: the SubOrder to Ideal Problem (SOIP). As an application, we introduce pSIDH, a new NIKE based on the suborder representation. Studying new assumption appears to be particularly crucial in the light of the recent attacks against isogeny-based cryptography.

7.1.13 The supersingular isogeny graph of abelian surfaces

Participants: Benjamin Smith.

The special combinatorial properties of the elliptic supersingular isogeny graph have made it a fruitful setting for new isogeny-based cryptosystems. Naturally, then, we seek to understand the properties of their generalizations, starting with the isogeny graphs formed by supersingular and superspecial abelian surfaces. In [20] we investigate the intricate local structure of these graphs.

7.1.14 New isogeny-based key exchange algorithms

Participants: Benjamin Smith.

In [17] we investigate the isogeny graphs of supersingular elliptic curves over $\mathbb{F}_{p^2}$ equipped with a d-isogeny to their Galois conjugate. These curves are interesting because they are, in a sense, a generalization of curves defined over $\mathbb{F}_p$, and there is an action of the ideal class group of $\mathbb{Q}(\sqrt{-dp})$ on the isogeny graphs. We investigate constructive and destructive aspects of these graphs in isogeny-based cryptography, including generalizations of the CSIDH cryptosystem and the Delfs-Galbraith algorithm.

7.2 Secure multiparty computation

Participants: C. Ducros .

Pseudorandom correlation functions (Boyle et al. [68]) allow two parties to locally generate, from short correlated keys, a near-unbounded amount of pseudorandom samples, according to a target correlation. The candidate introduced by Boyle et al. was constructed over a new assumption, variable-density learning parity with noise (VDLPN), for which they provide support by showing its resistance to a large class of attacks (called linear attacks). In [57], G. Couteau and C. Ducros first improved the construction with a slightly different VDLPN assumption and a new analysis, giving us provable usable parameters. Second, we identify a flaw in the security analysis of Boyle et al. which we repair.

7.3 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 a waek 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).

Two directions for building these protocols are discrete logarithms (and pairings) in elliptic curves or 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.

7.3.1 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. The short non interactive 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. The performance does not degrade badly with respect to the basic Reed-Solomon case [12]. 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 to have a smaller alphabet, and this can be done using algebraic-geometric codes. This was done by Sarah Bordage, Matthieu Lhotel, Jade Nardi and Hugues Randriambololona [30], 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 [65]. Their protocol has very good perfomance, akin to the Reed-Solomon case. Towers of curves are considered for this construction, to enable good asymptotic results.

7.3.2 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 [72] and made practical in [73]. 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 [70][34]. These curves beat the competition, an implementation has been provided here. Some other blockchain players CELO, Consensys also have used these curves in their implentations of verifiable computation and zero-knowledge proofs. A. Guillevic and Y. El Housni made a survey of relevant curves for recursive SNARKS [11].

Once the curves are built, it remains to do other ellitpic curves operations, which are particular to SNARKS, for instance doing a sum of a lot of scalar multiplication with differents points. Y. El Housni produced such multiscalar operations for SNARKS [54]. Other technicalites also have been improved [35].

7.4 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 [74], 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 [69] 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 [75], 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.

7.5 Cloud storage

Participants: Françoise Levy-Dit-Vehel, Maxime Roméas.

Proofs of Retrievability (PoR) protocols ensure that a client can fully retrieve a large outsourced file from an untrusted server. In [40] we design a good PoR based on a family of graph codes called expander codes. We use expander codes based on graphs derived from point-line incidence relations of finite affine planes. These codes have good dimension and minimum distance over a relatively small alphabet. Moreover, expander codes possess very efficient unique decoding algorithms. We take advantage of these results to design a PoR scheme that extracts the outsourced file in quasi-linear time and features better concrete parameters than state-of-the-art schemes w.r.t storage overhead and size of the outsourced file. This work has been presented at CANS 2022. Another line of work on PoRs was to design good PoR schemes with simple security proofs. To this end, in [39], we propose a framework for the design of secure and efficient PoR schemes that is based on Locally Correctable Codes, and whose security is phrased in the Constructive Cryptography model by Maurer. We give an instantiation of our framework using the high rate lifted codes introduced by Guo et al. This yields an infinite family of good PoRs. We assert their security by solving a finite geometry problem, giving an explicit formula for the probability of an adversary to fool the client. This was presented at I4CS 2022.

7.6 Algorithmic number theory

7.6.1 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 is to be submitted at ISSAC'2022 and the code is to be available on gitlab.

7.6.2 Pre-quantum factoring using elliptic curves

Participants: François Morain.

One of the most powerful factoring algorithm is ECM that uses elliptic curves. To improve it, families of curves are traditionally built over the rationals. In this work, number fields are used to treat the special numbers $b^n \pm 1$. See the preliminary results in [60].

7.6.3 Trustless unknown-order groups

Participants: Benjamin Smith.

Groups of unknown order are a classic setting for asymmetric cryptosystems—RSA being the most famous example. In recent times, unknown-order groups have returned to prominence as a setting for new, advanced cryptosystems including accumulators and VDFs (Verifiable Delay Functions). In these applications, *trustless setup* becomes critical: not even the constructor of the group should know its order. In [19] (joint work with Samuel Dobson and Steven Galbraith), we re-evaluate the security of ideal class groups—the most popular source of trustless unknown-order groups—and show that generally accepted parameters do not meet claimed security levels. We also propose a more efficient alternative: Jacobians of genus-3 hyperelliptic curves.

8 Bilateral contracts and grants with industry

8.1 Bilateral contracts with industry

Participants: Daniel Augot, Sarah Bordage, François Morain, Guénaël Renault, Benjamin Smith.

- Through École polytechnique, D. Augot is leader of a teaching and research chair on Blockchains "Blockchains and B2B platforms", funded by CapGemini, NomadicLabs and Caisse des dépôts, 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 this website). Sarah Bordage (PhD since 2019) was funded by this chair.

- Since October 2019, F. Morain and Aurore Guillveic are provided PhD advisorship to one of the employees of Consensys (main company for producing software for the Ethereum Blockchain) Y. El Housni, on the topic of zero-knowledge proofs.

- From October 2019 to October 2022, Idemia funds a CIFRE PhD student, Simon Montoya on the secure implementation in constrained environement of post-quantum cryptosystems.

- From October 2019 to october 2022, Quarkslab funds a CIFRE PhD student, Alexis Challande, on the analysis of malware code.

- From November 2019 to october 2022, French Min. Arm. funds a PhD student, Maxime Anvari, on the analysis of the ToR network.

- Since October 2020, Orange funds a CIFRE PhD student, Anaïs Barthoulot on Advanced encryption for Sensitive data sharing.

- Nomadic Labs are funding the Jasmin-EasyCrypt project, a collaboration between B. Smith, Benjamin Gregoire (Inria project-team STAMP), and Pierre-Yves Strub (Meta).

9 Partnerships and cooperations

9.1 European initiatives

9.1.1 H2020 projects

SPARTA SPARTA project on cordis.europa.eu

Title: Strategic programs for advanced research and technology in Europe

Duration: From February 1, 2019 to June 30, 2022

Partners:

- INSTITUT NATIONAL DE RECHERCHE EN INFORMATIQUE ET AUTOMATIQUE (INRIA), France
- CESNET ZAJMOVE SDRUZENI PRAVNICKYCH OSOB (CESNET), Czechia
- JOANNEUM RESEARCH FORSCHUNGSGESELLSCHAFT MBH (JOANNEUM RESEARCH), Austria
- NAUKOWA I AKADEMICKA SIEC KOMPUTEROWA - PANSTWOWY INSTYTUT BADAWCZY (NASK), Poland
- TARTU ULIKOOL (UNIVERSITY OF TARTU), Estonia
- MYKOLO ROMERIO UNIVERSITETAS (MYKOLAROMERIS UNIVERSITY), Lithuania
- LATVIJAS MOBILAIS TELEFONS SIA, Latvia
- SECURITY MADE IN LETZEBUERG (SMILE), Luxembourg
- FRAUNHOFER GESELLSCHAFT ZUR FORDERUNG DER ANGEWANDTEN FORSCHUNG EV (FHG), Germany
- FUNDACION TECNALIA RESEARCH & INNOVATION (TECNALIA), Spain

- TECHNISCHE UNIVERSITAET MUENCHEN (TUM), Germany
- THALES SIX GTS FRANCE SAS (THALES SIX GTS France), France
- COMMISSARIAT A L ENERGIE ATOMIQUE ET AUX ENERGIES ALTERNATIVES (CEA), France
- STOWARZYSZENIE POLSKA PLATFORMA BEZPIECZENSTWA WEWNETRZNEGO (PPBW), Poland
- INSTITUT NATIONAL DES SCIENCES APPLIQUEES DE LYON (INSA LYON), France
- SAP SE, Germany
- FORTISS GMBH, Germany
- LUXEMBOURG INSTITUTE OF SCIENCE AND TECHNOLOGY (LIST), Luxembourg
- VYSOKE UCENI TECHNICKE V BRNE (BRNO UNIVERSITY OF TECHNOLOGY), Czechia
- FUNDACION CENTRO DE TECNOLOGIAS DE INTERACCION VISUAL Y COMUNICACIONES VICOMTECH (VICOM), Spain
- INDRA SISTEMAS SA (INDRA), Spain
- INSTITUT MINES-TELECOM, France
- RHEINISCHE FRIEDRICH-WILHELMS-UNIVERSITAT BONN, Germany
- UNIVERSITE DU LUXEMBOURG (uni.lu), Luxembourg
- CONSIGLIO NAZIONALE DELLE RICERCHE (CNR), Italy
- "NATIONAL CENTER FOR SCIENTIFIC RESEARCH ""DEMOKRITOS""" ("NCSR ""D"""), Greece
- LIETUVOS KIBERNETINIU NUSIKALTIMU KOMPETENCIJU IR TYRIMU CENTRAS (LITHUANIAN CYBERCRIME CENTER OF EXCELLENCE FOR TRAINING RESEARCH & EDUCATIO), Lithuania
- KENTRO MELETON ASFALEIAS (CENTER FORSECURITY STUDIES CENTRE D'ETUDES DE SECURITE), Greece
- INDRA FACTORIA TECNOLOGICA SL, Spain
- UNIVERSITAT KONSTANZ (UKON), Germany
- LEONARDO - SOCIETA PER AZIONI (LEONARDO), Italy
- KAUNO TECHNOLOGIJOS UNIVERSITETAS (UNIVERSITY OF TECHNOLOGY, KAUNAS), Lithuania
- TECHNIKON FORSCHUNGS- UND PLANUNGSGESELLSCHAFT MBH (TECHNIKON), Austria
- ITTI SP ZOO (ITTI), Poland
- DIREZIONE GENERALE PER LE TECNOLOGIE DELLE COMUNICAZIONI E LA SICUREZZA INFORMATICA - ISTITUTO SUPERIORE DELLE COMUNICAZIONI E DELLE TECNOLOGIE DELL'INFORMAZIONE (DG TCSI-ISCOM), Italy
- GENEROLO JONO ZEMAICIO LIETUVOS KARO AKADEMIJA (GENERAL JONAS ZEMAITISMILITARY ACADEMY OF LITHUANIA), Lithuania
- FUNDACIO EURECAT (EURECAT), Spain
- CONSORZIO NAZIONALE INTERUNIVERSITARIO PER LE TELECOMUNICAZIONI (CNIT), Italy
- CENTRALESUPELEC (CentraleSupélec), France
- YES WE HACK (YWH), France
- INSTITUTO SUPERIOR TECNICO (IST), Portugal
- SECRETARIAT GENERAL DE LA DEFENSE ET DE LA SECURITE NATIONALE (SGDSN), France
- UNIVERSITE DE NAMUR ASBL (UNamur), Belgium

- INOV INSTITUTO DE ENGENHARIA DE SISTEMAS E COMPUTADORES INOVACAO (INOV), Portugal
- CENTRE D'EXCELLENCE EN TECHNOLOGIES DE L'INFORMATION ET DE LA COMMUNICATION (CETIC), Belgium
- CZ.NIC, ZSPO (CZ.NIC), Czechia
- CONSORZIO INTERUNIVERSITARIO NAZIONALE PER L'INFORMATICA (CINI), Italy

Inria contact: Thomas Jensen

Coordinator:

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 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.

9.2.2 ANR CBCRYPT

Participants: Alain Couvreur, Olivier Blazy.

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.

9.2.3 ANR COLA

Participants: Alain Couvreur, Thomas Debris–Alazard.

ANR **COLA** (An interface between COde and LAttice-based cryptography) 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 (ANR JCJC), starting in october 2021 led by Thomas Debris-Alazard focusses on bringing closer post-quantum solutions based on codes and lattices to improve our trust in cryptanalysis and to open new perspectives in terms of design.

9.2.4 ANR BARRACUDA

Participants: Daniel Augot, Alain Couvreur, Françoise Levy-dit-Vehel.

BARRACUDA is a collaborative ANR project accepted in 2021 and led by A. Couvreur.
Website : barracuda.inria.fr

The project gathers specialists of coding and cryptology on one hand and specialists of number theory and algebraic geometry on the other hand. The objectives concern problems arising from modern cryptography which require the use of advanced algebra based objects and techniques. It concerns for instance mathematical problems with applications to distributed storage, multi-party computation or zero knowledge proofs for protocols.

9.2.5 ANR SANGRIA

Participants: Olivier Blazy.

SANGRIA is a collaborative ANR project accepted in 2021.
Website : lip6.fr/Damien.Vergnaud/projects/sangria/

The main scientific challenge of the SANGRIA (Secure distributed computAtioN - cryptoGRaphy, combinatorIcs and computer Algebra) project are (1) to construct specific protocols that take into account practical constraints and prove them secure, (2) to implement them and to improve the efficiency of existing protocols significantly. The SANGRIA project (for Secure distributed computAtioN: cryptoGRaphy, combinatorIcs and computer Algebra) aims to undertake research in these two aspects while combining research from cryptography, combinatorics and computer algebra. It is expected to impact central problems in secure distributed computation, while enriching the general landscape of cryptography.

9.2.6 ANR MobiS5

Participants: Olivier Blazy.

MobiS5 is a collaborative ANR project accepted in 2018.
Website : mobis5.limos.fr/

MobiS5 will aim to foresee and counter the threats posed in 5G architectures by the architectural modifications suggested in TR 22.861-22.864. Concretely, we will provide a provably-secure cryptographic toolbox for 5G networks, validated formally and experimentally, responding to the needs of 5G architectures at three levels:

* Challenge 1: security in the network infrastructure and end points: including core network security and attack detection and prevention; * Challenge 2: cryptographic primitives and protocols, notably : a selection of basic primitives, an authenticated key-exchange protocol, tools to compute on encrypted

data, and post-quantum cryptographic countermeasures * Challenge 3: mobile applications, specifically in the use-case of a secure server that aids or processes outsourced computation; and the example of a smart home.

9.2.7 ANR CryptiQ

Participants: Olivier Blazy.

CryptiQ is a collaborative ANR project accepted in 2018.

The goal of the CryptiQ project is to major changes due to Quantum Computing by considering three plausible scenarios, from the closest to the furthest foreseeable future, depending on the means of the adversary and the honest parties. In the first scenario, the honest execution of protocols remains classical while the adversary may have oracle access to a quantum computer. This is the so-called post-quantum cryptography, which is the best known setting. In the second scenario (quantum-enhanced classical cryptography), we allow honest parties to have access to quantum technologies in order to achieve enhanced properties, but we restrict this access to those quantum technologies that are currently available (or that can be built in near-term). The adversary is still allowed to use any quantum technology. Finally, in the third scenario (cryptography in a quantum world), we allow the most general quantum operations to an adversary and we consider that anybody can now have access to both quantum communication and computation.

9.2.8 PEPR sur les technologues quantiques - Projet intégré "Un cadenas post-quantique pour les navigateurs web"

Participants: Alain Couvreur, Thomas Debris–Alazard, Benjamin Smith, Anaëlle Le Devehat, Matthieu Lequesne.

This *projet intégré* aims to develop post quantum cryptographic primitives in 5 years which would be implemented in an open source web browser. The evolution of cryptographic standards has already begun. The choice of new primitives will be made soon and the transition should be operated in a few years. The objective of the project is to play a crucial role in this evolution so that french researchers, which are already strongly implied in this process could influence the choice of cryptographic standards in the next years.

9.2.9 Inria Défi RIOT-fp: *Reconcile IoT and Future-Proof Security*

Participants: Benjamin Smith, Gustavo Banegas.

RIOT-fp is a research project on cyber-security targeting low-end, microcontroller-based IoT devices, on which run operating systems such as RIOT and a low-power network stack. It links the project-teams EVA, GRACE, PROSECCO, TRiBE, and TEA. Taking a global and practical approach, RIOT-fp gathers partners planning to enhance RIOT with an array of security mechanisms. The main challenges tackled by RIOT-fp are:

1. developing high-speed, high-security, low-memory IoT crypto primitives,

2. providing guarantees for software execution on low-end IoT devices, and

3. enabling secure IoT software updates and supply-chain, over the network.

Beyond academic outcomes, the output of RIOT-fp is open source code published, maintained and integrated in the open source ecosystem around RIOT. As such, RIOT-fp strives to contribute usable building blocks for an open source IoT solution improving the typical functionality vs. risk tradeoff for end-users.

9.2.10 Inria AEx CACHAÇA

Participants: Benjamin Smith, Guenael Renault, Anaelle Le Devehat.

The *Action Exploratoire* CACHAÇA, led by Benjamin Smith and based at Campus Cyber, started in 2022. CACHAÇA aims to bring high-assurance techniques from formal methods to the initial design and implementation phase for new postquantum cryptosystems, to produce fast, safe, and portable software implementations, especially for constrained environments such as IoT devices. Guenael Renault has associate researcher status, and so CACHAÇA is an anchor-point for collaborations between GRACE and the Secure Components laboratory at ANSSI. It will also englobe GRACE's contribution to planned industrial consortia (expected to begin in 2023).

10 Dissemination

Participants: Daniel Augot, Olivier Blazy, Maxime Bombar, Alain Couvreur, Thomas Debris-Alazard, Françoise Levy-dit-Vehel, François Morain, Guenael Renault, Benjamin Smith.

10.1 Promoting scientific activities

10.1.1 Scientific events: organisation

- O. Blazy and A. Couvreur participated in the organisation of the *Journées Codage et Cryptographie (C2) 2022*.
- A. Couvreur organised the CIMPA Summer School *SUmmer School in Applied Arithmetic at Nesin (SUSAAN)* in Nesin math Village (Sirince, Turkey).
- D. Augot is member of the programm committee of the seminar of the "groupe de travail codage et cryptographie (GT C2) du groupement de recherche informatique mathématique (GDR IM)"

10.1.2 Scientific events: selection

Chair of conference program committees

- B. Smith was PC chair for SAC 2022 (Selected Areas in Cryptography, Windsor, Canada).

Member of the conference program committees

- A. Couvreur was member of the program committee of Journées scientifiques Inria 2022.
- O. Blazy was a member of the programm committees of CT-RSA, Eurocrypt, SAC, PQCrypto
- F. Levy-dit-Vehel was a member of the program committee of 2022 IEEE International Symposium on Information Theory (ISIT2022)
- D. Augot was a member of the program committee of 2022 IEEE International Symposium on Information Theory (ISIT2022)

- D. Augot was a member of the program committee of the 6th International Workshop on Cryptocurrencies and Blockchain Technology
- D. Augot was a member of the program committee of the IEEE International Conference on Blockchain and Cryptocurrency
- D. Augot was a member of the program committee of the WCC 2022: The Twelfth International Workshop on Coding and Cryptography
- D. Augot was a member of the program committee of the 6th Workshop on Trusted Smart Contracts (WTSC2022)
- T. Debris–Alazard was a member of the jury for the PhD award Gilles Kahn of the Société Informatique de France.
- B. Smith was a member of the program committee of PQCrypto 2022
- B. Smith was a member of the program committee of ANTS-XV
- T. Debris–Alazard was a member of the jury for the PhD award Gilles Kahn of the Société Informatique de France.

Reviewer

- A. Couvreur has been reviewer for the conferences *Asiacrypt 2022*; *Workshop on Coding and Cryptograny (WCC) 2022* and *IEEE Information Theory Workshop (ITW) 2022*.
- O. Blazy has been a reviewer for the conferences *Asiacrypt 2022*; *Crypto 2022*; *Workshop on Coding and Cryptograny (WCC) 2022* and *Conference on Security and Cryptography for Networks (SCN) 2°22*.
- T. Debris–Alazard has been reviewer for the conferences *Asiacrypt 2022* and *Post-Quantum Crypto 2022*.
- D. Augot has been reviewer for the conference 2022 Information Theory Workshop
- D. Augot has been reviewer for the conference Workshop on Coding and Cryptography (WCC22)
- M. Bombar has been reviewer for the conferences *Workshop on Coding and Cryptography (WCC) 2022*, *Asiacrypt 2022*, *PKC 2023*.
- B. Smith was a reviewer for the conference CT-RSA 2022.

10.1.3 Journal

Member of the editorial boards

- A. Couvreur is member of the editorial board of Publications Mathématiques de Besançon.
- O. Blazy is a member of the editorial board of Computer Law & Security Review

Reviewer - reviewing activities

- A. Couvreur has been reviewer for the journals, *Advances in Mathematics of Communication*; *Designs, Codes and Cryptography*; *IEEE, Transactions on Information Theory*; *Journal of Algebraic Combinatorics* and *Applicable Algebra in Engeneering, Communication and Computing*.
- O. Blazy had been a review for the journals, *IEEE, Transactions on Services Computing* ; *Designs, Codes and Cryptography*; *Journal of Cryptography*; *IEEE access*
- T. Debris–Alazard has been reviewer for the journals, *Advances in Mathematics of Communication*; *Designs, Codes and Cryptography* and *Journal of Cryptography*.

- D. Augot has been reviewer for *Designs, Codes and Cryptography, Discrete Maths, SIAM Journal on Discrete Mathematics*
- M. Bombar has been reviewer for the journals *Advances in Mathematics of Communication*; *IEEE, Transactions on Information Theory*.
- B. Smith was a reviewer for journals including *Mathematics of Computation* and *Mathematical Cryptology*

10.1.4 Invited talks

- A. Couvreur has been invited to give a lecture at the *Algebraic Coding Theory (ACT) summer school* 2022. [62].
- O. Blazy has been an invited panelist at Conference Privacy, Data Protection (CPDP) 2022.
- T. Debris–Alazard has been invited to give lectures at the *Summer school in post-quantum cryptography* 2022.
- M. Bombar has been invited to give tutorials in code–based cryptography at the *Summer school in post-quantum cryptography* 2022.

10.1.5 Leadership within the scientific community

- O. Blazy and A. Couvreur lead the CNRS' *Groupe de travail Codage et Cryptographie* of *Groupes de recherche Sécurité Informatique* and *Informatique Mathématique*.
- A. Couvreur was member of the *Commité de Culture Mathématiques (CCM)* of *Institut Henri Poincaré*.
- A. Couvreur is coordinator for Inria of the *projet intégré "Un cadenas post–quantique pour les navigateurs web" (PQ-TLS)* of the *PEPR quantique*.
- A. Couvreur is the principal investigator of the collaborative ANR project *Barracuda*.

10.1.6 Scientific expertise

- A. Couvreur was referee of the PhD thesis of Leonardo Landi (*Danmarks Tekniske Universitet*, Lyngby, Danemark).
- A. Couvreur was referee of the PhD of Étienne Marcatel (Université de Grenoble Alpes).
- A. Couvreur was referee of the PhD of Amaury Durand (Université de Bordeaux).
- A. Couvreur was referee of the PhD of Maxime Bros (Université de Limoges).
- O. Blazy was a referee of the PhD of Meryem Cherkaoui Semmouni (Ecole Nationale d'Informatique et d'Analyse des Systèmes, Rabat, Morocco).
- O. Blazy was a referee for the PhD of Tang Khai Hanh (Nanyang Technological University, Singapore, Singapore)
- G. Renault was referee for the PHD of Mohamed Traore (*Université Grenoble Alpes*)
- G. Renault was referee for the PHD of Davide Poggi (*Université de Montpellier*)
- G. Renault was referee for the PHD of Simon Landry (*Sorbonne Université*)
- G. Renault was referee for the PHD of Axel Mathieu-Mahias (*Université Paris-Saclay*)
- T. Debris–Alazard has been mandated as an expert for the ANR.
- B. Smith served as a scientific expert for Bpifrance.

10.1.7 Research administration

- A. Couvreur is elected member of Inria's *Commission d'évaluation.*
- A. Couvreur is member of the *Comité scientifique du programme Maths et IA* of the *Labex Mathématiques Jacques Hadamard.*
- O. Blazy was appointed *référent europe* for the GDR sécurité informatique
- O. Blazy was appointed as one of the academic member of the PostQuantum Cryptography Workgroup at Campus Cyber.
- B. Smith is a member of the Post-Quantum Cryptography working group at Campus Cyber.
- B. Smith was a member of the Research and Innovation Committee of Labex *Digicosme*
- B. Smith is a member of the *Commission Scientifique* of Inria Saclay.

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 : T. Debris–Alazard, Exercises for INF361: "Introduction à l'informatique", 15h (equiv TD), 1st year (L3), École polytechnique.
- Licence : M. Bombar: *INF361: Introduction à l'informatique* (tutorials), 40h (equiv TD), 1st year (L3), École polytechnique.
- Licence : B. Smith: *CSE101: Introduction to Computer Programming*, 42h, L1, École polytechnique, France
- Licence : O. Blazy: *CSE101: Introduction to Computer Programming* (Tutorials), 58h, L1, École polytechnique, France
- Master : T. Debris–Alazard, Lectures for "Post-quantum cryptography", 8h, 4th year, ENS Lyon,
- Master : A. Couvreur : *MPRI 2-13-2: Error Correcting codes and applications to cryptography.*
- Master : T. Debris–Alazard : *MPRI 2-13-2: Error Correcting codes and applications to cryptography.*
- Master A. Couvreur : *Master QDCS Calcul quantique avancé et codes correcteurs. 10h.*
- Master: D. Augot: lectures and labs on crypto in blockchains, 24h, M2, École polytechnique, France.
- Master: D. Augot designed with Julien Prat the cursus of a course in blockchains and economics, and made lectures on zero-knowledge.
- 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 : M. Bombar: *INF558 : Introduction to cryptology* (tutorials), 22.5h (equiv TD), M1, École Polytechnique.
- Master : M. Bombar: *INF550 : Advanced algorithms* (tutorials), 18h (equiv TD), M1, École Polytechnique.
- Master : B. Smith: *INF568: Advanced Cryptography*, 45h, 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, Lectures on discrete maths, 21h, M1, ENSTA.
- Master : F. Levy-dit-Vehel, Lectures on 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
- Master : O. Blazy: Lectures and Labs for *INF646: Introduction to formal methods*, 20h, M2, École polytechnique, France
- Master : O. Blazy: Lectures and Labs for *Authentification, VPN et Chiffrement*, 6h, M2, Telecom Sud Paris, France
- Professionnal training: D. Augot gave a two hours lecture at System-X.

10.2.2 Juries

- A. Couvreur was president of the PhD jury of Simon Montoya (Institut Polytechnique de Paris).
- O. Blazy and A. Couvreur were members of the PhD Jury of Maxime Bros (Université de Limoges).
- A. Couvreur was member of the PhD jury of Manon Bertin (Université de Rouen Normandie).
- O. Blazy was president of the PhD jury of Manon Bertin (Université de Rouen Normandie).
- A. Couvreur was member of the PhD jury of Étienne Marcatel (Université Grenoble Alpes).
- A. Couvreur was member of the PhD jury of Christophe Levrat (Sorbonne université).
- A. Couvreur was member of the PhD jury of Amaury Durand (Université de Bordeaux)
- A. Couvreur was member of the PhD jury of Leonardo Landi (*Danmarks Tekniske Universitet*, Lyngby, Danemark).
- O. Blazy was president of the PhD jury of Octavio Perez Kempner (*Ecole Normale Supérieure-PSL, Paris, France*).
- O. Blazy was member of the PhD jury of Souha Masmoudi (*Telecom Sud Paris, Evry, France*).
- D. Augot was member of the HDR jury of Pascal Véron (*Université de Toulon*)
- D. Augot was member of the PhD jury of Marina Dehez-Clementi (*Université de Toulouse*)
- B. Smith was a member of the PhD jury of Natalia Kulatova (*ENS/PSL Université Paris*).
- G. Renault was member of the HDR jury of Charles Bouillaguet (*Sorbonne Université*)
- G. Renault was member of the PHD jury of Mohamed Traore (*Université Grenoble Alpes*)
- G. Renault was member of the PHD jury of Davide Poggi (*Université de Montpellier*)
- G. Renault was member of the PHD jury of Simon Landry (*Sorbonne Université*)
- G. Renault was member of the PHD jury of Axel Mathieu-Mahias (*Université Paris-Saclay*)
- G. Renault was member of the PHD jury of Gabriel Destouet (*Université Grenoble Alpes*)

10.3 Popularization

10.3.1 Internal or external Inria responsibilities

- A. Couvreur is the *référent médiation scientifique* of Saclay's research center.
  - He organised the *Rendez-vous des Jeunes Mathématiciennes et Informaticiennes* on February 21 and 22th 2022. The event happened online due to the pandemic.
  - He participated in the organisation of *Fête de la science* 2022.

11 Scientific production

11.1 Major publications

[1] D. Augot, S. Bordage and J. Nardi. 'Efficient multivariate low-degree tests via interactive oracle proofs of proximity for polynomial codes'. In: *Designs, Codes and Cryptography* (2022). DOI: 10.1007/s10623-022-01134-z. URL: https://hal.inria.fr/hal-03454113.

[2] G. Banegas, K. Zandberg, E. Baccelli, A. Herrmann and B. Smith, eds. *Quantum-Resistant Software Update Security on Low-Power Networked Embedded Devices.* Vol. 13269. Lecture Notes in Computer Science. Springer International Publishing, 18th June 2022, pp. 872–891. DOI: 10.1007/978-3-031-09234-3_43. URL: https://hal.science/hal-03931075.

[3] O. Blazy, I. Boureanu, P. Lafourcade, C. Onete and L. Robert. 'How fast do you heal? A taxonomy for post-compromise security in secure-channel establishment'. In: *USENIX 2023 - The 32nd USENIX Security Symposium.* USENIX 2023 - The 32nd USENIX Security Symposium. Anaheim, United States, 9th Aug. 2023. URL: https://hal.science/hal-03815803.

[4] M. Bombar, A. Couvreur and T. Debris-Alazard. 'On Codes and Learning With Errors over Function Fields'. In: *Lecture Notes in Computer Science.* CRYPTO 2022. Vol. 13508. Advances in Cryptology – CRYPTO 2022. Santa Barbara (CA), United States: Springer Nature Switzerland, 13th Oct. 2022, pp. 513–540. DOI: 10.1007/978-3-031-15979-4_18. URL: https://hal.science/hal-03597834.

[5] T. Debris-Alazard, L. Ducas and W. P. Van Woerden. 'An Algorithmic Reduction Theory for Binary Codes: LLL and more'. In: *IEEE Transactions on Information Theory* (14th Jan. 2022). DOI: 10.1109/TIT.2022.3143620. URL: https://hal.inria.fr/hal-03529739.

[6] F. Levy-Dit-Vehel and M. Roméas. 'Efficient Proofs of Retrievability using Expander Codes'. In: Cryptography and Network Security, CANS 2022. Abu Dhabi, United Arab Emirates, 16th Nov. 2022. URL: https://hal.science/hal-03886784.

[7] F. Morain, G. Renault and B. Smith. 'Deterministic factoring with oracles'. In: *Applicable Algebra in Engineering, Communication and Computing* (16th Sept. 2021). DOI: 10.1007/s00200-021-00521-8. URL: https://hal.inria.fr/hal-01715832.

11.2 Publications of the year

International journals

[8] S. Abelard, E. Berardini, A. Couvreur and G. Lecerf. 'Computing Riemann-Roch spaces via Puiseux expansions'. In: *Journal of Complexity* (20th Apr. 2022). DOI: 10.1016/j.jco.2022.101666. URL: https://hal.inria.fr/hal-03281757.

[9] S. Abelard, A. Couvreur and G. Lecerf. 'Efficient computation of Riemann-Roch spaces for plane curves with ordinary singularities'. In: *Applicable Algebra in Engineering, Communication and Computing* (1st Dec. 2022). DOI: 10.1007/s00200-022-00588-x. URL: https://hal.archives-ouvertes.fr/hal-03110135.

[10] N. Aragon, O. Blazy, J.-C. Deneuville, P. Gaborit and G. Zemor. 'Ouroboros An efficient and provably secure KEM family'. In: *IEEE Transactions on Information Theory* (22nd Apr. 2022), pp. 1–1. DOI: 10.1109/TIT.2022.3168439. URL: https://hal-enac.archives-ouvertes.fr/hal-03679752.

[11] D. F. Aranha, Y. El Housni and A. Guillevic. 'A survey of elliptic curves for proof systems'. In: *Designs, Codes and Cryptography*. Special Issue: Mathematics of Zero-Knowledge (21st Dec. 2022), p. 46. DOI: 10.1007/s10623-022-01135-y. URL: https://hal.inria.fr/hal-03667798.

[12] D. Augot, S. Bordage and J. Nardi. 'Efficient multivariate low-degree tests via interactive oracle proofs of proximity for polynomial codes'. In: *Designs, Codes and Cryptography* (2022). DOI: 10.1007/s10623-022-01134-z. URL: https://hal.inria.fr/hal-03454113.

[13] G. Banegas, V. Gilchrist and B. Smith. 'Efficient supersingularity testing over F_p and CSIDH key validation'. In: *Mathematical Cryptology* 2.1 (4th Oct. 2022), pp. 21–35. URL: https://hal.inria.fr/hal-03739021.

[14] S. Bettaieb, L. Bidoux, O. Blazy, Y. Connan and P. Gaborit. 'A gapless code-based hash proof system based on RQC and its applications'. In: *Designs, Codes and Cryptography* (Aug. 2022). DOI: 10.1007/s10623-022-01075-7. URL: https://hal.archives-ouvertes.fr/hal-03815797.

[15] O. Blazy, L. Brouilhet, E. Conchon and M. Klingler. 'Anonymous attribute-based designated verifier signature'. In: *Journal of Ambient Intelligence and Humanized Computing* 68.9 (Sept. 2022), pp. 6233–6244. DOI: 10.1007/s12652-022-03827-8. URL: https://hal.archives-ouvertes.fr/hal-03815798.

[16] A. Canteaut, A. Couvreur and L. Perrin. 'Recovering or Testing Extended-Affine Equivalence'. In: *IEEE Transactions on Information Theory* 68.9 (Sept. 2022), pp. 6187–6206. DOI: 10.1109/TIT.2022.3166692. URL: https://hal.inria.fr/hal-03156177.

[17] M. Chenu and B. Smith. 'Higher-degree supersingular group actions'. In: *Mathematical Cryptology* 1.2 (25th Mar. 2022), pp. 85–101. URL: https://hal.inria.fr/hal-03288075.

[18] T. Debris-Alazard, L. Ducas and W. P. van Woerden. 'An Algorithmic Reduction Theory for Binary Codes: LLL and more'. In: *IEEE Transactions on Information Theory* (14th Jan. 2022). DOI: 10.1109/TIT.2022.3143620. URL: https://hal.inria.fr/hal-03529739.

[19] S. Dobson, S. Galbraith and B. Smith. 'Trustless unknown-order groups'. In: *Mathematical Cryptology* 1.2 (23rd Mar. 2022), pp. 25–39. URL: https://hal.inria.fr/hal-02882161.

[20] E. Florit and B. Smith. 'An atlas of the Richelot isogeny graph'. In: *RIMS Kôkyûroku Bessatsu*. Theory and Applications of Supersingular Curves and Supersingular Abelian Varieties B90 (June 2022), pp. 195–219. URL: https://hal.inria.fr/hal-03094296.

[21] F. Morain. 'Modular curves over number fields and ECM'. In: *Research in Number Theory* (2022). URL: https://hal.inria.fr/hal-03606355.

[22] N. Tovanich, N. Soulié, N. Heulot and P. Isenberg. 'The evolution of mining pools and miners' behaviors in the Bitcoin blockchain'. In: *IEEE Transactions on Network and Service Management* 19.3 (1st Sept. 2022), pp. 3633–3644. DOI: 10.1109/TNSM.2022.3159004. URL: https://hal.science/hal-03610424.

International peer-reviewed conferences

[23] A. Barthoulot, O. Blazy and S. Canard. '(Augmented) Broadcast Encryption from Identity Based Encryption with Wildcard'. In: *Cryptology and Network Security. 21st International Conference, CANS 2022 Dubai, United Arab Emirates, November 13–16, 2022, Proceedings.* CANS 2022 - 21st International Conference on Cryptology and Network Security. Vol. LNCS-13641. Cryptology and Network Security. Dubai, United Arab Emirates: Springer International Publishing, 10th Nov. 2022, pp. 143–164. DOI: 10.1007/978-3-031-20974-1_7. URL: https://hal.inria.fr/hal-03856239.

[24] S. Bettaieb, L. Bidoux, O. Blazy, B. Cottier and D. Pointcheval. 'Post-Quantum and UC-secure Oblivious Transfer from SPHF with Grey Zone'. In: *15th International Symposium on Foundations & Practice of Security (FPS–2022)*. 15th International Symposium on Foundations & Practice of Security (FPS – 2022). Ottawa, Canada, 12th Dec. 2022. URL: https://hal.science/hal-03772089.

[25] L. Bettale, J. Eynard, S. Montoya, G. Renault and R. Strullu. 'Security Assessment of NTRU Against Non-Profiled SCA'. In: CARDIS 2022. Birmingham, United Kingdom, 7th Nov. 2022. URL: https://hal.science/hal-03950393.

[26] O. Blazy, I. Boureanu, P. Lafourcade, C. Onete and L. Robert. 'How fast do you heal? A taxonomy for post-compromise security in secure-channel establishment'. In: *USENIX 2023 - The 32nd USENIX Security Symposium*. USENIX 2023 - The 32nd USENIX Security Symposium. Anaheim, United States, 9th Aug. 2023. URL: https://hal.science/hal-03815803.

[27] O. Blazy, P.-A. Fouque, T. Jacques, P. Lafourcade, C. Onete and L. Robert. 'MARSHAL: Messaging with Asynchronous Ratchets and Signatures for faster HeALing'. In: *Symposium on Applied Computing (SAC)*. The 37th ACM/SIGAPP Symposium on Applied Computing, SAC (2022). Virtual, Czech Republic: ACM, Apr. 2022, pp. 1–8. DOI: 10.1145/3477314.3507044. URL: https://hal.uca.fr/hal-03510612.

[28] O. Blazy and S. Kakvi. 'Identity-Based Encryption in DDH Hard Groups'. In: *Lecture Notes in Computer Science*. AFRICACRYPT 2022 - 13th International Conference on Cryptology in Africa. Vol. LNCS-13503. Progress in Cryptology - AFRICACRYPT 2022. Fes, Morocco: Springer Nature Switzerland; Springer Nature Switzerland, 6th Oct. 2022, pp. 81–102. DOI: 10.1007/978-3-031-17433-9_4. URL: https://hal.science/hal-03815800.

[29] M. Bombar, A. Couvreur and T. Debris-Alazard. 'On Codes and Learning With Errors over Function Fields'. In: *Lecture Notes in Computer Science*. CRYPTO 2022. Vol. 13508. Advances in Cryptology – CRYPTO 2022. Santa Barbara (CA), United States: Springer Nature Switzerland, 13th Oct. 2022, pp. 513–540. DOI: 10.1007/978-3-031-15979-4_18. URL: https://hal.archives-ouvertes.fr/hal-03597834.

[30] S. Bordage, M. Lhotel, J. Nardi and H. Randriam. 'Interactive Oracle Proofs of Proximity to Algebraic Geometry Codes'. In: *CCC '22: Proceedings of the 37th Computational Complexity Conference*. CCC 2022 - 37th Computational Complexity Conference. Philadelphie, United States, 13th Sept. 2022, 30:1–30:45. DOI: 10.4230/LIPIcs.CCC.2022.30. URL: https://hal.telecom-paris.fr/hal-03832439.

[31] K. Carrier, T. Debris-Alazard, C. Meyer-Hilfiger and J.-P. Tillich. 'Statistical Decoding 2.0: Reducing Decoding to LPN'. In: ASIACRYPT 2022 - 28th Annual International Conference on the Theory and Application of Cryptology and Information Security. Taipei, Taiwan, 5th Dec. 2022. URL: https://hal.inria.fr/hal-03919778.

[32] A. Challande, R. David and G. Renault. 'Building a Commit-level Dataset of Real-world Vulnerabilities'. In: CODASPY 2022 - 12th ACM Conference on Data and Application Security and Privacy. Baltimore MD USA, United States: ACM, 25th Apr. 2022, pp. 101–106. DOI: 10.1145/1122445.1122456. URL: https://hal.archives-ouvertes.fr/hal-03477866.

[33] Y. El Housni. 'Pairings in Rank-1 Constraint Systems'. In: ACNS2023 - 21st International Conference on Applied Cryptography and Network Security. Kyoto, Japan, 19th June 2023. URL: https://hal.science/hal-03777499.

[34] Y. El Housni and A. Guillevic. 'Families of SNARK-friendly 2-chains of elliptic curves'. In: *LNCS*. Advances in Cryptology - EUROCRYPT 2022 - 41st Annual International Conference on the Theory and Applications of Cryptographic Techniques. Vol. 13276. EUROCRYPT 2022. Trondheim / Hybrid, Norway: Springer, 30th May 2022, pp. 367–396. DOI: 10.1007/978-3-031-07085-3_13. URL: https://hal.inria.fr/hal-03371573.

[35] Y. El Housni, A. Guillevic and T. Piellard. 'Co-factor clearing and subgroup membership testing on pairing-friendly curves'. In: AFRICACRYPT 2022 - 13th International Conference on Cryptology. Vol. 13503. LNCS. Fes, Morocco: Springer, 6th Oct. 2022, pp. 518–536. DOI: 10.1007/978-3-031-17433-9_22. URL: https://hal.inria.fr/hal-03608264.

[36] K. Eldefrawy, T. Lepoint and A. Leroux. ‘Communication-Efficient Proactive MPC for Dynamic Groups with Dishonest Majorities’. In: *ACNS 2022*. ACNS 2022. Rome, Italy, 2021. URL: https://hal.inria.fr/hal-03471927.

[37] A. Leroux. ‘A New Isogeny Representation and Applications to Cryptography’. In: ASIACRYPT 2022. Taipei, Taiwan, 5th Dec. 2022. URL: https://hal.inria.fr/hal-03886737.

[38] A. Leroux. ‘An Effective Lower Bound on the Number of Orientable Supersingular Elliptic Curves’. In: SAC 2022 - Selected Areas in Cryptography. Windsor, Canada, 22nd Aug. 2022. URL: https://hal.inria.fr/hal-03886746.

[39] F. Levy-Dit-Vehel and M. Roméas. ‘A Framework for the Design of Secure and Efficient Proofs of Retrievability’. In: *LNCS*. International Conference on Cryptology, Coding Theory, and Cybsersecurity, I4CS. Casablanca, Morocco, Morocco, Oct. 2022. URL: https://hal.science/hal-03886792.

[40] F. Levy-Dit-Vehel and M. Roméas. ‘Efficient Proofs of Retrievability using Expander Codes’. In: Cryptography and Network Security, CANS 2022. Abu Dhabi, United Arab Emirates, 16th Nov. 2022. URL: https://hal.science/hal-03886784.

[41] F. Morain. ‘Implementing the Thull-Yap algorithm for computing Euclidean remainder sequences’. In: ISSAC2022. Villeneuve-d’Ascq, France, 4th July 2022. URL: https://hal.inria.fr/hal-03572271.

Conferences without proceedings

[42] M. Bombar and A. Couvreur. ‘Right-hand side decoding of Gabidulin codes and applications’. In: WCC 2022 : The Twelfth International Workshop on Coding and Cryptography. Rostock, Germany, 7th Mar. 2022. URL: https://hal.archives-ouvertes.fr/hal-03481406.

[43] A. Challande, R. David and G. Renault. ‘Quokka: A Fast and Accurate Binary Exporter’. In: GreHack 2022 - 10th International Symposium on Research in Grey-Hat Hacking. Grenoble, France, 18th Nov. 2022. URL: https://hal.science/hal-03845728.

Edition (books, proceedings, special issue of a journal)

[44] G. Banegas, K. Zandberg, E. Baccelli, A. Herrmann and B. Smith, eds. *Quantum-Resistant Software Update Security on Low-Power Networked Embedded Devices*. Vol. 13269. Lecture Notes in Computer Science. Springer International Publishing, 18th June 2022, pp. 872–891. DOI: 10.1007/978-3-031-09234-3_43. URL: https://hal.science/hal-03931075.

Doctoral dissertations and habilitation theses

[45] S. Bordage. ‘Efficient protocols for testing proximity to algebraic codes’. Institut Polytechnique de Paris, 16th June 2022. URL: https://theses.hal.science/tel-03744182.

[46] A. Challande. ‘Towards 1-day Vulnerability Detection using Semantic Patch Signatures’. Institut polytechnique de Paris, 11th Oct. 2022. URL: https://hal.science/tel-03950382.

[47] Y. El Housni. ‘The Arithmetic of Pairing-Based Proof Systems’. Institut Polytechnique de Paris, 18th Nov. 2022. URL: https://hal.archives-ouvertes.fr/tel-03922488.

[48] A. Leroux. ‘Quaternion Algebra and isogeny-based cryptography’. Ecole doctorale de l’Institut Polytechnique de Paris, 7th Sept. 2022. URL: https://hal.inria.fr/tel-03886810.

[49] S. Montoya. ‘Embedded lattice-based cryptography’. Institut polytechnique de Paris, 12th Oct. 2022. URL: https://hal.science/tel-03950386.

[50] M. Roméas. ‘Modeling and construction of interactive cryptographic protocols for outsourced storage’. Institut Polytechnique de Paris; Ecole Polytechnique, 29th Nov. 2022. URL: https://hal.science/tel-03887128.

Reports & preprints

[51] R. Barbulescu, P. Gaudry, A. Guillevic and F. Morain. *Improvements to the number field sieve for non-prime finite fields*. 24th Aug. 2022. URL: https://hal.inria.fr/hal-01052449.

[52] E. Berardini, A. Couvreur and G. Lecerf. *A proof of the Brill-Noether method from scratch*. 29th Aug. 2022. URL: https://hal.archives-ouvertes.fr/hal-03762780.

[53] J. Booher, R. Bowden, J. Doliskani, T. B. Fouotsa, S. Galbraith, S. Kunzweiler, S.-P. Merz, C. Petit, B. Smith, K. E. Stange, Y. B. Ti, C. Vincent, J. F. Voloch, C. Weitkämper and L. Zobernig. *Failing to hash into supersingular isogeny graphs*. 26th July 2022. URL: https://hal.inria.fr/hal-03739041.

[54] G. Botrel and Y. El Housni. *EdMSM: Multi-Scalar-Multiplication for recursive SNARKs and more*. 16th Oct. 2022. URL: https://hal.archives-ouvertes.fr/hal-03922635.

[55] A. Couvreur. *Improved decoding of symmetric rank metric errors*. 16th Dec. 2022. URL: https://hal.inria.fr/hal-03920845.

[56] T. Debris-Alazard, M. Remaud and J.-P. Tillich. *Quantum Reduction of Finding Short Code Vectors to the Decoding Problem*. 17th Jan. 2022. URL: https://hal.inria.fr/hal-03529802.

[57] C. Ducros and G. Couteau. *Pseudorandom Correlation Functions fromVariable-Density LPN, Revisited*. 19th Jan. 2023. URL: https://hal.science/hal-03947831.

[58] E. Guerrini, K. Lairedj, R. Lebreton and I. Zappatore. *Simultaneous Rational Function Reconstruction with Errors: Handling Multiplicities and Poles*. 25th Mar. 2022. URL: https://hal.archives-ouvertes.fr/hal-03620179.

[59] F. Levy-Dit-Vehel and M. Roméas. *A Composable Look at Updatable Encryption*. 18th Jan. 2022. URL: https://hal.inria.fr/hal-03531837.

[60] F. Morain. *Some factors of numbers of the form* b^nś1 *found using ECM with new classes of curves*. 31st Mar. 2022. URL: https://hal.inria.fr/hal-03437714.

Other scientific publications

[61] D. Augot, S. Bordage, Y. El Housni, G. Fedak and A. Simonet. *Zero-Knowledge : trust and privacy on an industrial scale*. 5th Jan. 2022. URL: https://hal.inria.fr/hal-03512005.

11.3 Other

Educational activities

[62] A. Couvreur. 'Codes and modular curves'. Doctoral. Switzerland, 4th July 2022. URL: https://hal.inria.fr/hal-03932020.

11.4 Cited publications

[63] G. Banegas, T. Debris-Alazard, M. Nedeljković and B. Smith. 'Wavelet: Code-based postquantum signatures with fast verification on microcontrollers'. working paper or preprint. Oct. 2021. URL: https://hal.inria.fr/hal-03403225.

[64] G. Banegas, K. Zandberg, A. Herrmann, E. Baccelli and B. Smith. 'Quantum-Resistant Security for Software Updates on Low-power Networked Embedded Devices'. working paper or preprint. June 2021. URL: https://hal.inria.fr/hal-03255844.

[65] 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.

[66] M. Bombar and A. Couvreur. 'Decoding Supercodes of Gabidulin Codes and Applications to Cryptanalysis'. In: *Post-Quantum Cryptography*. Ed. by J. H. Cheon and J.-P. Tillich. Cham: Springer International Publishing, 2021, pp. 3–22.

[67] M. Bombar and A. Couvreur. 'Decoding supercodes of Gabidulin codes and applications to cryptanalysis'. In: *Post-Quantum Cryptography 2021*. Ed. by J. H. Cheon and J.-P. Tillich. Vol. 12841. Post-Quantum Cryptography. PQCrypto 2021. PQCrypto 2021. The Sage code is available on Github: https://github.com/mbombar/Attack_on_LIGA. Daejeon, South Korea: Springer, July 2021, pp. 3–22. DOI: 10.1007/978-3-030-81293-5_1. URL: https://hal.inria.fr/hal-03256980.

[68] E. Boyle, G. Couteau, N. Gilboa, Y. Ishai, L. Kohl and P. Scholl. 'Correlated Pseudorandom Functions from Variable-Density LPN'. In: *FOCS 2020 - Annual IEEE Symposium on Foundations of Computer Science*. Durham, United States, Nov. 2020. URL: https://hal.science/hal-03374160.

[69] 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.

[70] 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*. Ed. by H. Shulman and S. Vaudenay. Vol. 12579. Lecture Notes in Computer Science. Vienna / Virtual, Austria: Springer, Dec. 2020, pp. 259–279. URL: https://hal.inria.fr/hal-02962800.

[71] A. Greuet, S. Montoya and G. Renault. 'On Using RSA/ECC Coprocessor for Ideal Lattice-Based Key Exchange'. In: *COSADE 2021*. Lugano, Switzerland, Oct. 2021. DOI: 10.1007/978-3-030-89915-8_10. URL: https://hal.inria.fr/hal-03330066.

[72] 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.

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

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

[75] 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).