RESEARCH CENTRE

Inria Saclay Centre at Institut Polytechnique de Paris

IN PARTNERSHIP WITH:

CNRS, Institut Polytechnique de Paris

2023 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

Inria

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 [INRIA, Researcher]
- Benjamin Smith [INRIA, Researcher, HDR]

Faculty Members

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

Post-Doctoral Fellows

- Matthieu Lequesne [INRIA, Post-Doctoral Fellow, until Nov 2023]
- Rakhi Pratihar [INRIA, Post-Doctoral Fellow, from May 2023]
- Bruno Sydney Sterner [INRIA, Post-Doctoral Fellow, from Oct 2023]
- Natkamon Tovanich [LIX, Post-Doctoral Fellow]

PhD Students

- Maxime Anvari [Ministère Armées]
- Nadja Aoutouf [INRIA, from Sep 2023]
- Anaïs Barthoulot [ORANGE, until Sep 2023]
- Maxime Bombar [LIX, until Aug 2023]
- Sana Boussam [THALES, CIFRE, from Mar 2023]
- Hugo Delavenne [LIX, from Sep 2023]
- Clément Ducros [UNIV PARIS]
- Shane Gibbons [CWI, from Mar 2023 until Apr 2023, Visitor]
- Anaelle Le Devehat [INRIA]
- Pierre Loisel [INRIA, from Sep 2023]
- Angelo Saadeh [TELECOM PARIS]
- Eric Sageloli [THALES, from Sep 2023]
- Nihan Tanısalı [INRIA, from Oct 2023]

Technical Staff

- Bruno Sydney Sterner [INRIA, Engineer, from Jul 2023 until Sep 2023]

Interns and Apprentices

- Pierre Loisel [INRIA, Intern, from Apr 2023 until Aug 2023]
- Elie Raspaud [INRIA, Intern, from Apr 2023 until Sep 2023]

Administrative Assistant

- Mariana De Almeida [INRIA, from Mar 2023]

External Collaborators

- Philippe Lebacque [UNIV FRANCHE-COMTE]
- Tanguy Medevielle [UNIV RENNES I, from Dec 2023]
- Matthieu Rambaud [MINESPARISTECH, until Sep 2023]
- 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* $\mathscr{X}$ over a field
K is defined by an equation

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

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

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

3.3 Curve-Based cryptology

Participants: 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. Furthermore, in order to increase the diversity in the future post-quantum standardized crypto-systems the NIST has launched in 2023 (see this website) a second call for standardization.

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.

D. Augot is advising Hugo Delavenne on the second topic, more precisely on the interplay on model of computations and so called arithmetization, to which is applied the cryptographic treatment itself (curve-based or code-based). D. Augot is also co-advisor of Tangue Medevielle with Jade Nardi (IRMAR, CNRS, Rennes) on the algebraic and coding side. Hugo Delavenne and Tanguy Medevielle are collaborating on the two facets of the topic.

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.

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 provide 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.

These proofs allows to move data and computation off chain, pushing the burden to off-chain servers that play the role of provers, who then commit short commitments of the updated data , accompanied by short proofs which are easy to verify onchain, where validators play the role of verifiers. 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 Wave post-quantum signatures

Participants: Alain Couvreur, Thomas Debris-Alazard, Benjamin Smith.

Wave is a post-quantum signature scheme based on hard problems in coding theory, originally proposed by T. Debris–Alazard in his PhD thesis. In response to NIST's 2023 call for new post-quantum signature schemes, we developed a full specification [39] and portable reference implementation software (see bil-5053, in collaboration with Nicolas Sendrier of EPI COSMIQ, Gustavo Banegas of Qualcomm France, and Ruben Niederhagen of Academia Sinica) integrating theoretical and practical improvements from [41]. with parameters meeting a range of standard post-quantum security levels. The full submission is public and available for download from this website.

5.2 HDR's

Participants: B. Smith.

Benjamin Smith defended his *Habilitation à diriger les recherches* entitled: **Advances in asymmetric cryptographic algorithms** on October 6, 2023.

6 New software, platforms, open data

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 library implements finite field and elliptic curve arithmetic for BN curves (Barreto-Naehrig), BLS (Barreto-Lynn-Scott), KSS (Kachisa-Schaefer-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 two papers and is not optimized.

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

Publications: hal-03667798, hal-03371573

Contact: Aurore Guillevic

6.1.2 WaveSign

Name: Wave Signatures: Reference Implementation

Keywords: Post-quantum, Digital signature, Cryptographic protocol, Cryptography

Functional Description: This software provides a complete and functional reference implementation in C99 for Wave, a post-quantum digital signature scheme based on hard problems in coding theory. Key generation, signing, and verification functions are provided, compliant with the API specified by NIST for their post-quantum signature on-ramp call. The emphasis is on portability, rather than targeted optimizations.

URL: https://wave-sign.org

Contact: Nicolas Sendrier

Partner: Qualcomm France

7 New results

7.1 Post–quantum cryptography

7.1.1 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 [44], 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.

In [19], we revisit the tool called the OHCP framework (for Oracle with Hidden Center Problem) which has been introduced by Peikert et al. (STOC 2017) in the lattice-based context. This framework has proved to be very useful as a black box inside reductions and we have adapted it in the code-based context by extracting its very essence, namely the Oracle Comparison Problem (OCP). It has yield to a new worst-case to average-case search-to-decision reduction. We have then turned to the structured versions and explain why this is not as straightforward as for Euclidean lattices. If we fail to give a search-to-decision reduction for structured codes, we believe that our work opens the way towards new reductions for structured codes, given that the OHCP framework proved to be so powerful in lattice-based cryptography. Furthermore, we also believe that this technique could be extended to codes endowed with other metrics, such as the rank metric, for which no reduction is known.

7.1.2 New algorithms 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 [46], 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.

In [31] we revisit RLPN-decoding by noticing that, in this algorithm, decoding is in fact reduced to a sparse-LPN problem, namely with a secret whose Hamming weight is small. Our new approach consists this time in making an additional reduction from sparse-LPN to plain-LPN with a coding approach inspired by coded-BKW. It outperforms significantly the ISD's and RLPN for code rates smaller than 0.42. This algorithm can be viewed as the code-based cryptography cousin of recent dual attacks in lattice-based cryptography. We depart completely from the traditional analysis of this kind of algorithm which uses a certain number of independence assumptions that have been strongly questioned recently in the latter domain. We give instead a formula for the LPN noise relying on duality which allows to analyze the behavior of the algorithm by relying only on the analysis of a certain weight distribution. By using only a minimal assumption whose validity has been verified experimentally we are able to justify the correctness of our algorithm. This key tool, namely the duality formula, can be readily adapted to the lattice setting and is shown to give a simple explanation for some phenomena observed on dual attacks in lattices.

7.1.3 Cryptanalysis

Participants: Alain Couvreur.

In [23], we propose a new attack on rank metric based encryption schemes by revisiting and extending Overbeck's attack. This novel approach involving the computation of code's stabilizer algebras and their Artin-Wedderburn decomposition. This permitted in particular to break the system proposed in [48].

In another work [22], we proposed a new distinguisher on binary and q–ary Goppa codes: the codes used in NIST submission Classic McEliece which runs in the 4th round of NIST's standardisation process. Our distinguisher consists in reducing the Goppa distinguishing problem to a MinRank instance in a space of symmetric matrices. Despite, the obtained distinguisher works only on high rate Goppa codes and hence does not break Classic McEliece, this is a completely novel approach and the first result on binary Goppa codes cryptanalysis for over 10 years.

7.1.4 Isogeny evaluation algorithms over extension fields

Participants: Anaëlle Le Dévéhat, Benjamin Smith.

Consider the basic problem of efficiently evaluating an isogeny $\phi : E \to E/H$ of elliptic curves over $\mathbb{F}_q$, where the kernel $H = \langle G \rangle$ is a cyclic group of odd (prime) order: given E, G, and one or more points P on E, we want to compute $\phi(P)$. This problem is at the heart of essentially all efficient implementations of group-action- and isogeny-based post-quantum cryptosystems, such as CSIDH. Algorithms based on Vélu's formulæ give an efficient solution to this problem when the kernel generator G is defined over $\mathbb{F}_q$. However, for general isogenies, G is only defined over some extension $\mathbb{F}_{q^k}$, even though the kernel subgroup $H = \langle G \rangle$ as a whole (and thus ϕ) is defined over the base field $\mathbb{F}_q$; and the performance of Vélu-style algorithms degrades rapidly as k grows. In [29], joint work with our former postdoc Gustavo Banegas and former intern Valerie Gilchrist, we revisit the isogeny-evaluation problem with a special focus on the case where $1 \leq k \leq 12$. We improve Vélu-style isogeny evaluation for many cases where $k = 1$ using special addition chains, and combine this with the action of Galois to give greater improvements when $k > 1$.

7.2 Secure multiparty computation

Participants: Maxime Bombar, Alain Couvreur, Clément Ducros.

Secure Multiparty Computation is a famous paradigm where each player has secret data and are able to perform a computation involving all these secret data without getting more information than the result of the computation. Following the seminal work from Beaver [42], efficient secure multi party computation can be performed thanks to a precomputation step where the parties receive correlated pseudo-random strings called *Oblivious Linear Evaluation* (OLE). In [18], we proposed a new efficient construction of OLE's which security rests on a new problem called *Quasi-Abelian Syndrome Decoding*. This new construction permits to construct very long pseudo-random correlated strings over small fields while the best construction up to now required to work over a very large field.

7.3 Verifiable computation

Participants: Daniel Augot.

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, Tanguy Medevielle.

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.

An 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 [45], 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 [43]. 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.

The internship of Tanguy Medevielle in Spring 2023 allowed to prove that these codes admit a quasi linear encoding algorithm under mild constraints.

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 [49], 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 [47] 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 [50], 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.

A. Saadeh defended his thesis on these topics [27], with two accompanying publications [25, 37].

7.5 Cloud storage

Participants: Françoise Levy-Dit-Vehel.

During the period, we investigated the Updatable Encryption (UE) functionality. UE protocols allow a client, who outsourced his encrypted data, to make it updated by an untrusted server. To do so, the client generates a token, dependent on the old key and the new key, and gives it to the server to update all ciphertexts (ciphertext-independent setting); of course, the token should not reveal anything about the keys. An issue here, besides security, is maintaining the communication complexity as low as possible. The security definitions for UE schemes have been constantly updated since the seminal paper of D. Boneh in 2013. However, the security notion that is best suited for a paricular application remains unclear. We solved the problem in the ciphertext-independent setting. In particular, we proved that IND-UE-RCCA security[1] is the right notion for many practical UE schemes. As a consequence, we notably rectify a previously believed assertion, according to which IND-UE security is stronger than IND-ENC+UPD notions, in that it hides the ages of ciphertexts. We show that this is true only when ciphertexts can leak at most once per epoch (an epoch being a time period between to key updates). We also give a clear description of post-compromise security guarantees of such schemes. This work has been submitted to Journal of Cryptology.

7.6 Algorithmic number theory

7.6.1 Modular polynomials

Participants: François Morain.

Basic isogeny computations require the use of modular polynomials in two ways. The roots of a modular polynomial first indicate the existence of curves isogenous to the curve of interest. Second, these isogenous curves are computed using explicit formulas involving derivatives of the modular polynomial, as first described by Atkin for two families of modular polynomials. The height of the polynomial is critical, since it is the dominant parameter in the complexity analysis of the various methods used to compute them. We started to investigate the theory and practice of modular polynomials, in search of smaller and easier families to be used for the efficient computation of isogenies. See the two preprints [35] and [36].

8 Bilateral contracts and grants with industry

8.1 Bilateral contracts with industry

[1] A UE scheme is IND-UE secure if, upon submitting m and c to the game, the adversary has a negligible advantage in guessing whether the challenger's response is an encryption of m or an update of c. IND-UE-RCCA is a variant of it.

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.
- B. Smith is coordinating Inria's involvement in the Bpifrance-funded HYPERFORM consortium, which aims to develop a pre- and post-quantum hybrid cryptographic reference platform. So far this project, which started in September 2023, is funding B. Sterner's postdoc.

9 Partnerships and cooperations

9.1 International initiatives

Shane Gibbons, PhD student from CWI Amsterdam Visitedthe team for one month in march 2023 in order to work on code and lattices equivalence problems.

9.2 European initiatives

9.2.1 Horizon Europe

ENCODE ENCODE project on cordis.europa.eu

Title: European Network in Coding Theory and Applications

Duration: From March 1, 2023 to February 28, 2027

Partners:

- INSTITUT NATIONAL DE RECHERCHE EN INFORMATIQUE ET AUTOMATIQUE (INRIA), France
- UNIVERSITY COLLEGE DUBLIN, NATIONAL UNIVERSITY OF IRELAND, DUBLIN (NUID UCD), Ireland
- WORLDLINE (WORLDLINE), France
- INSTITUT POLYTECHNIQUE DE PARIS, France
- Bitwards Oy, Finland
- AALTO KORKEAKOULUSAATIO SR (AALTO), Finland
- UNIVERSITE DE NEUCHATEL (UNINE), Switzerland
- DEUTSCHES ZENTRUM FUR LUFT - UND RAUMFAHRT EV (DLR), Germany
- NXP SEMICONDUCTORS NETHERLANDS BV, Netherlands
- WITHSECURE OYJ (WITHSECURE CORPORATION), Finland
- TECHNISCHE UNIVERSITEIT EINDHOVEN (TU/e), Netherlands
- Roseman Labs B.V. (Roseman Labs), Netherlands

Inria contact: Francoise Levy-dit-Vehel

Coordinator:

Summary: Coding theory is a cornerstone of the mathematics of communications. It an interdisciplinary field, lying at the intersection of mathematics, computer science and electrical engineering. It is a fundamental tool of every system of digital communications, with applications to error-correction, distributed storage, wireless communications, secure multi-party computation and post-quantum cryptography. The ENCODE doctoral network will focus on fundamentals and applications of coding theory to security, privacy and efficiency of distributed communication & computation. The DN will leverage the complementary expertise of 7 academic and 5 non-academic partners, to guide its 8 DCs to address and solve deep problems in coding theory and its applications. The DN will offer a superior supervisory experience for each DC, who will each benefit from the expertise of multiple advisors in academia and industry. The non-academic partners include 5 companies working at the cutting edge of cybersecurity, who will offer invaluable contributions to the training programme via hosting of DCs and input in advanced training sessions. DCs will be exposed to current technical challenges faced by industry and will have the opportunity to apply mathematics to tackle real-world problems during industrial secondments. ENCODE will create a unique training programme, designed to equip its DCs with the scientific tools and transferable skills required for them to become future leaders in the field, both in academia and in industry. The ENCODE programme will implement all EC Principles for Innovative Doctoral Training, adhere to best practice as outlined in the EU Charter & Code, the MSCA Green Charter, and ensure gender equality in all aspects of its activities, to create a lasting international, intersectoral, interdisciplinary doctoral network, dedicated to excellence in science, ethical standards & communications that will extend far beyond the DN.

QSNP QSNP project

Title: Quantum Secure Networks Partnership

Duration: From March 1, 2023 to August 31, 2028

Partners:

- 23 european academic partners
- 18 european industry partners

Inria contact: Olivier Blazy

Coordinator:

Summary: QSNP is a European Quantum Flagship project that aims to develop quantum cryptography technology to secure the transmission of information over the internet.

QSNP will contribute to the European sovereignty in quantum technology for cybersecurity protecting the privacy and the sensitive information of European citizens transmitted over the internet.

9.3 National initiatives

9.3.1 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.

9.3.2 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.

9.3.3 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.

9.3.4 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.

9.3.5 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.

9.3.6 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.

9.3.7 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.

9.3.8 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.

9.3.9 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

10.1 Promoting scientific activities

10.1.1 Scientific events: selection

Member of the conference program committees

- A. Couvreur was served on the PC of IEEE *Information Theory Workshop* 2023.
- B. Smith served on the PC of CRYPTO 2023.
- B. Smith served on the PC of IMACC 2023.
- B. Smith served on the PC of SAC 2023.
- D. Augotserved on the PCs of:
  - Workshop on Trusted Smart Contracts 2023;
  - Cryptocurrencies and Blockchain Technology workshop 2023;
  - IEEE International Conference on Blockchain and Cryptocurrency 2023.
- O. Blazyserved on the PCs of:
  - Eurocrypt 2024;
  - Selected Areas in Cryptography (SAC)2023;
  - PQCrypto 2023;
  - CT-RSA 2024;
  - ARES 2023;
  - IMACCS 2023.

  O. Blazyalso served on the Jury of the Prix CNIL-Inria 2023.

Reviewer

- A. Couvreur served as a reviewer for the conference *Asiacrypt 2023*.

10.1.2 Journal

Member of the editorial boards

- B. Smith became a member of the editorial board of IACR Communications in Cryptology.
- A. Couvreur became associate editor of SIAM Journal on Applied Algebra and Geometry (SIAGA)
- A. Couvreur is member of the editorial board of Publications Mathématiques de Besançon
- O. Blazyis on the editorial board of *Computer Law and Security Review*.

Reviewer - reviewing activities

- A. Couvreur served as a referee for the journal *Cryptography and Communications, Designs Codes and Cryptography, Journal of Algebra, Journal of Pure and Applied Algebra, IEEE, Transactions on Information Theory, SIAM Journal on Applied Algebra and Geometry*.

10.1.3 Invited talks

- A. Couvreur was invited to give a talk at the special session *Algebraic coding theory and cryptography* of the 29th Nordic Congress of Mathematicians

10.1.4 Leadership within the scientific community

- O. Blazy and A. Couvreur are co-responsible of the *Groupe de Travail Codes et Cryptographie (C2)* of the GdR's *Informatique Mathématiques* and *Sécurité Informatique*.

10.1.5 Scientific expertise

- A. Couvreur was referee for the PhD commitee of **Mathieu Lhotel** (Université de Franche-Comté, 3/7/2023)
- A. Couvreur was referee for the PhD commitee of **Thibauld Feneuil** (Sorbonne Université, 23/10/2023)
- A. Couvreur was referee for the HDR commitee of **Eleonora Guerrini** (Université de Montpellier, 4/12/2023)
- O. Blazy was referee for the PhD commitee of **Cyrius Nugier** (Insa Toulouse, 04/07/2023)
- O. Blazy was referee for the PhD commitee of **Vigile Dossou Yovo** (Université d'Abomey-Calavi (Bénin), 09/08/2023)
- O. Blazy was referee for the PhD commitee of **Lucas Prabel** (Université de Rennes, 05/10/2023)
- O. Blazy was referee for the PhD committee of **Elie Bouscatié** (Université de Bordeaux, 19/12/2023)

10.1.6 Research administration

- D. Augot was member of a *Comité de sélection* for a *Maître de conférence* position at Université de Limoges.
- D. Augot was member of the scientific PhD jury of Institut Polytechnique de Paris (attributing PhD fundings in computer science).
- D. Augot was in the HCERÉS visiting committee of lab LIP6 (CNRS and Sciences Sorbonne Université), 21-24 November 2023.
- A. Couvreur is elected member of Inria's *Commission d'Évaluation*. He served in the recruitment juries:
  - CRCN Centre Inria de Lyon;

  - DR2 National.

- A. Couvreur is coordiator for Inria of the Axis PQ-TLS of PEPR quantique and in charge of the work package on code-based cryptography with Philippe Gaborit (University of Limoges).
- B. Smith is in charge of the work package on isogeny-based cryptography of the axis PQ-TLS of PEPR quantique.
- O. Blazy is a member of the *Conseil Scientifique et Pédagogique* for the EUR Tactic.

10.2 Teaching - Supervision - Juries

10.2.1 Teaching

- Licence :
  - O. Blazy: *CSE101: Introduction to Computer Programming* (Tutorials), 58h, L1, École polytechnique, France
  - M. Bombar: *INF361: Introduction à l'informatique* (tutorials), 40h (equiv TD), 1st year (L3), École polytechnique.
  - T. Debris–Alazard, Exercises for INF361: "Introduction à l'informatique", 15h (equiv TD), 1st year (L3), École polytechnique.
  - F. Morain, Lectures for INF361: "Introduction à l'informatique", 15h (equiv TD), 1st year (L3), École polytechnique. Coordinator of this module (350 students).
  - B. Smith: *CSE101: Introduction to Computer Programming*, 31.5h, L1, École polytechnique, France
  - B. Smith: *CSE207: Introduction to Networks* (Tutorials), 14h, L2, École polytechnique, France
- Master:
  - D. Augot: lectures and Labs on crypto in blockchains, 24h, M2, École polytechnique, France.
  - D. Augot designed with Julien Prat the cursus of a course in blockchains and economics, and made lectures on zero-knowledge.
  - 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
  - T. Debris–Alazard, Lectures for INF587: "Introduction to quantum computer science", 45h, École polytechnique.
  - A. Couvreur and T. Debris–Alazard : Lectures in *MPRI 2-13-2: Error Correcting codes and applications to cryptography*
  - F. Morain, INF558, Lectures and labs *Introduction to cryptology*, 36h, M1, École Polytechnique
  - F. Levy-dit-Vehel, Lectures on discrete maths, 21h, M1, ENSTA
  - F. Levy-dit-Vehel, Lectures on cryptography, 24h, M2, ENSTA.
  - Matthieu Lequesne, INF558, labs *Introduction to cryptology*, 36h, M1, École Polytechnique
  - G. Renault: Lectures and Labs for *INF565: Information Systems Security*, 60h, M1, École polytechnique, France
  - 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
  - B. Smith: *INF568: Advanced Cryptography*, 45h, M1, École polytechnique, France

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

- Professional training:
  - D. Augot gave a two hours lecture at System-X.

10.2.2 Supervision

- Master : F. Morain is the scientific leader of the Master of Science and Technology *Cybersecurity: Threats and Defense* of École Polytechnique.
- Bachelor: O. Blazy is one of the academic advisor for the Computer Science Bachelor of École Polytechnique.
- Master : O. Blazy is one of the academic advisor of the new Master of Science and Technology *Cybersecurity* of École Polytechnique.

10.2.3 Juries

- T. Debris–Alazard was member of the jury for **Gilles Kahn PhD award**
- B. Smithwas an examiner for the PhD of **Marc Houben** (KU Leuven, Belgium, 22/11/2023)
- D. Augotwas a reviewer of the PhD of **Simona Etinksi** (Université Paris Cité, 28/6/2023)
- D. Augotwas president of the PhD committee of **Mathieu Lhotel** (Université de Franche-Comté, 3/7/2023)
- A. Couvreur was president for the PhD commiteed of **Rocco Mora** (Sorbonne université, 7/4/2023)
- A. Couvreur was member the PhD commitee of **Mathieu Lhotel** (Université de Franche-Comté, 3/7/2023)
- A. Couvreur was member of the PhD commitee of **Thibauld Feneuil** (Sorbonne Université, 23/10/2023)
- A. Couvreur was member of the HDR commitee of **Eleonora Guerrini** (Université de Montpellier, 4/12/2023)
- O. Blazywas member for the PhD commitee of **Quoc-Huy Vu** (Panthéon-Assas, 01/02/2023).
- O. Blazy was president for the PhD commitee of **Cyrius Nugier** (Insa Toulouse, 04/07/2023)
- O. Blazy was member for the PhD commitee of **Vigile Dossou Yovo** (Université d'Abomey-Calavi (Bénin), 09/08/2023)
- O. Blazywas president for the PhD commitee of **Hugo Senet** (Panthéon-Assas, 22/09/2023).
- O. Blazy was member for the PhD commitee of **Lucas Prabel** (Université de Rennes, 05/10/2023)
- O. Blazy was member for the PhD committee of **Elie Bouscatié** (Université de Bordeaux, 19/12/2023)

10.3 Popularization

10.3.1 Internal or external Inria responsibilities

- A. Couvreur was *référent médiation scientifique* of Inria Saclay research centre until september 2023. In this context,
  - he organised with the *Service Communication et Médiation* of Inria Saclay *Les Rendez-vous des Jeunes Mathématiciennes et Informaticiennes* at Inria Saclay;
  - he coordinated with the *Service Communication et Médiation* of Inria Saclay the *La fête de la science* at *Institut Polytechnique de Paris* and *Université Paris Saclay*
- O. Blazy is *Référent Europe* for the GDR Sécurité Informatique.

10.3.2 Articles and contents

- D. Augot was interviewed in a Polytechnique insights video on blockchains.
- O. Blazy gave numerous interview in national / international media about cybersecurity concerns, especially age verification / children onlinde protection. (L'Express, BFMTV, La Croix, Public Sénat, ...)

10.3.3 Interventions

- B. Smith gave the keynote at the 2023 BNP Paribas FRESH (Finance and Risk) team-building event on *The transition to quantum-safe cryptography*.
- B. Smith gave a keynote talk at the 2023 GFA Flag Attack ("the French–German CTF") on *The transition to quantum-safe cryptography*
- A. Couvreur gave a popularization talk on the history of cryptography at the award ceremony of the *Olympiades de Mathématiques de l'accadémie de Créteil*.
- O. Blazy gave a presentation at the ERGA academy about age verification. (ERGA being the European Regulators Group for Audiovisual media).

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] G. Banegas and R. Villanueva-Polanco. 'On recovering block cipher secret keys in the cold boot attack setting'. In: *Cryptography and Communications - Discrete Structures, Boolean Functions and Sequences* (2023). DOI: 10.1007/s12095-022-00625-z. URL: https://hal.science/hal-03970576.

[9] G. Botrel and Y. El Housni. 'Faster Montgomery multiplication and Multi-Scalar-Multiplication for SNARKs'. In: *IACR Transactions on Cryptographic Hardware and Embedded Systems* (9th June 2023), pp. 504–521. DOI: 10.46586/tches.v2023.i3.504-521. URL: https://hal.science/hal-03922635.

[10] T. Debris-Alazard, L. Ducas, N. Resch and J.-P. Tillich. 'Smoothing Codes and Lattices: Systematic Study and New Bounds'. In: *IEEE Transactions on Information Theory* 69.9 (Sept. 2023), pp. 6006–6027. DOI: 10.1109/TIT.2023.3276921. URL: https://inria.hal.science/hal-04276505.

[11] T. Debris-Alazard, M. Remaud and J.-P. Tillich. 'Quantum Reduction of Finding Short Code Vectors to the Decoding Problem'. In: *IEEE Transactions on Information Theory* (2023), pp. 1–1. DOI: 10.1109/TIT.2023.3327759. URL: https://inria.hal.science/hal-04276190.

[12] E. Guerrini, K. Lairedj, R. Lebreton and I. Zappatore. 'Simultaneous Rational Function Reconstruction with Errors: Handling Multiplicities and Poles'. In: *Journal of Symbolic Computation* 116 (2023), pp. 345–364. DOI: 10.1016/j.jsc.2022.10.007. URL: https://hal.science/hal-03620179.

International peer-reviewed conferences

[13] G. Banegas, J. Krämer, T. Lange, M. Meyer, L. Panny, K. Reijnders, J. Sotáková and M. Trimoska. 'Disorientation Faults in CSIDH'. In: EUROCRYPT 2023: Advances in Cryptology – EUROCRYPT 2023. Vol. 14008. Lecture Notes in Computer Science. Lyon, France: Springer Nature Switzerland, 16th Apr. 2023, pp. 310–342. DOI: 10.1007/978-3-031-30589-4_11. URL: https://inria.hal.science/hal-04333521.

[14] A. Barthoulot, O. Blazy and S. Canard. 'Dually Computable Cryptographic Accumulators and Their Application to Attribute Based Encryption'. In: *Lecture Notes in Computer Science*. CANS 2023 - Cryptology and Network Security. Vol. LNCS-14342. Cryptology and Network Security 22nd International Conference, CANS 2023. Augusta, United States: Springer Nature Singapore, 31st Oct. 2023, pp. 538–562. DOI: 10.1007/978-981-99-7563-1_24. URL: https://hal.science/hal-04271645.

[15] L. Bettale, J. Eynard, S. Montoya, G. Renault and R. Strullu. 'Security Assessment of NTRU Against Non-Profiled SCA'. In: CARDIS 2022 - 21st Smart Card Research and Advanced Application Conference. Vol. 13820. Lecture Notes in Computer Science. Birmingham, United Kingdom: Springer International Publishing, 29th Jan. 2023, pp. 248–268. DOI: 10.1007/978-3-031-25319-5_13. URL: https://hal.science/hal-03950393.

[16] 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: *Proceedings of the 32nd USENIX Conference on Security Symposium*. USENIX 2023 - The 32nd USENIX Security Symposium. Vol. 1. Anaheim, United States: USENIX Association, 9th Aug. 2023, pp. 5917–5934. URL: https://hal.science/hal-03770735.

[17] O. Blazy, C. Chevalier, G. Renaut, T. Ricosset, É. Sageloli and H. Senet. 'Efficient Implementation of a Post-Quantum Anonymous Credential Protocol'. In: *ARES '23: Proceedings of the 18th International Conference on Availability, Reliability and Security*. ARES 2023: The 18th International Conference on Availability, Reliability and Security. Benevento, Italy: ACM, 1st Aug. 2023, pp. 1–11. DOI: 10.1145/3600160.3600188. URL: https://hal.science/hal-04283083.

[18] M. Bombar, G. Couteau, A. Couvreur and C. Ducros. 'Correlated Pseudorandomness from the Hardness of Quasi-Abelian Decoding'. In: *Lecture Notes in Computer Science*. CRYPTO 2023 - 43rd Annual International Cryptology Conference. Vol. LNCS-14084. Advances in Cryptology – CRYPTO 2023. Santa Barbara, United States: Springer Nature Switzerland, 9th Aug. 2023, pp. 567–601. DOI: 10.1007/978-3-031-38551-3_18. URL: https://hal.science/hal-04265638.

[19] M. Bombar, A. Couvreur and T. Debris-Alazard. 'Pseudorandomness of Decoding, Revisited: Adapting OHCP to Code-Based Cryptography'. In: *Lecture notes in Computer Science*. ASIACRYPT 2023 - International Conference on the Theory and Application of Cryptology and Information Security. Guang Zhou, China, 4th Dec. 2023. URL: https://inria.hal.science/hal-04308091.

[20] G. Couteau and C. Ducros. 'Pseudorandom Correlation Functions fromVariable-Density LPN, Revisited'. In: 26th IACR International Conference on Practice and Theory of Public-Key Cryptography. Vol. 13941. Lecture Notes in Computer Science. Atlanta, United States: Springer Nature Switzerland, 2nd May 2023, pp. 221–250. DOI: 10.1007/978-3-031-31371-4_8. URL: https://hal.science/hal-03947831.

[21] A. Couvreur. 'Improved decoding of symmetric rank metric errors'. In: 2023 IEEE Information Theory Workshop (ITW). Saint-Malo, France: IEEE, 16th Dec. 2022, pp. 238–242. DOI: 10.1109/ITW55543.2023.10161649. URL: https://inria.hal.science/hal-03920845.

[22] A. Couvreur, R. Mora and J.-P. Tillich. 'A new approach based on quadratic forms to attack the McEliece cryptosystem'. In: ASIACRYPT 2023. Guangzhou, China: Springer, 4th Dec. 2023. URL: https://inria.hal.science/hal-04215135.

[23] A. Couvreur and I. Zappatore. 'An extension of Overbeck's attack with an application to cryptanalysis of Twisted Gabidulin-based schemes'. In: *Lecture Notes in Computer Science*. Post-Quantum Cryptography. PQCrypto 2023. Vol. 14154. Lecture Notes in Computer Science. College Park, United States: Springer Nature Switzerland, 2nd May 2023, pp. 3–37. DOI: 10.1007/978-3-031-40003-2_1. URL: https://hal.science/hal-04088012.

[24] 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.

[25] A. Saadeh, P. Senellart and S. Bressan. 'Confidential Truth Finding with Multi-Party Computation'. In: DEXA 2023 - 34th International Conference on Database and Expert Systems Applications. Penang, Malaysia, 28th Aug. 2023. URL: https://inria.hal.science/hal-04139281.

Doctoral dissertations and habilitation theses

[26] M. Bombar. 'Structured Codes for Cryptography: from Source of Hardness to Applications'. École Polytechnique, 15th Dec. 2023. URL: https://inria.hal.science/tel-04386153.

[27] A. Saadeh. 'Applications of secure multi-party computation in Machine Learning'. Institut Polytechnique de Paris, 8th June 2023. URL: https://inria.hal.science/tel-04299101.

[28] B. Smith. 'Advances in asymmetric cryptographic algorithms'. Institut polytechnique de Paris, 6th Oct. 2023. URL: https://inria.hal.science/tel-04238166.

Reports & preprints

[29] G. Banegas, V. Gilchrist, A. Le Dévéhat and B. Smith. *Fast and Frobenius: Rational Isogeny Evaluation over Finite Fields*. June 2023. URL: https://inria.hal.science/hal-04143067.

[30] G. Banegas, J. Krämer, T. Lange, M. Meyer, L. Panny, K. Reijnders, J. Sotáková and M. Trimoska. *Disorientation faults in CSIDH*. 2023. URL: https://hal.science/hal-03970597.

[31] K. Carrier, T. Debris-Alazard, C. Meyer-Hilfiger and J.-P. Tillich. *Reduction from Sparse LPN to LPN, Dual Attack 3.0*. 7th Dec. 2023. URL: https://inria.hal.science/hal-04328262.

[32] P. Dartois, A. Leroux, D. Robert and B. Wesolowski. *SQISignHD: New Dimensions in Cryptography*. 25th Mar. 2023. URL: https://hal.science/hal-04056062.

[33] T. Debris-Alazard and N. Resch. *Worst and average case hardness of decoding via smoothing bounds*. 6th Dec. 2023. URL: https://inria.hal.science/hal-04326764.

[34] A. Leroux and M. Roméas. *Updatable Encryption from Group Actions*. 12th Jan. 2024. URL: https://hal.science/hal-04389878.

[35] F. Morain. *Computing the Charlap-Coley-Robbins modular polynomials*. 9th Feb. 2023. URL: https://inria.hal.science/hal-03980413.

[36] F. Morain. *Using the Charlap-Coley-Robbins polynomials for computing isogenies*. 1st Mar. 2023. URL: https://inria.hal.science/hal-04009243.

[37] A. Saadeh, P. Senellart and S. Bressan. *Confidential Truth Finding with Multi-Party Computation (Extended Version)*. 24th May 2023. DOI: 10.48550/arXiv.2305.14727. URL: https://inria.hal.science/hal-04139243.

[38] B. Sterner. *Towards Optimally Small Smoothness Bounds for Cryptographic-Sized Twin Smooth Integers and its Isogeny-based Applications*. Oct. 2023. URL: https://inria.hal.science/hal-04254512.

Other scientific publications

[39] G. Banegas, K. Carrier, A. Chailloux, A. Couvreur, T. Debris-Alazard, P. Gaborit, P. Karpman, J. Loyer, R. Niederhagen, N. Sendrier, B. Smith and J.-P. Tillich. *WAVE: Round 1 Submission*. 21st June 2023. URL: https://inria.hal.science/hal-04278563.

11.3 Other

Educational activities

[40] T. Debris-Alazard. 'Code-based Cryptography: Lecture Notes'. Doctoral. France, 7th Apr. 2023. URL: https://hal.science/hal-04311471.

11.4 Cited publications

[41] 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.

[42] D. Beaver. 'Efficient Multiparty Protocols Using Circuit Randomization'. In: *Advances in Cryptology — CRYPTO '91*. Ed. by J. Feigenbaum. Berlin, Heidelberg: Springer Berlin Heidelberg, 1992, pp. 420–432.

[43] 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.

[44] M. Bombar, A. Couvreur and T. Debris-Alazard. 'On Codes and Learning With Errors over Function Fields'. In: *CRYPTO 2022*. Ed. by Y. Dodis and T. Shrimpton. Vol. 13508. Advances in Cryptology – CRYPTO 2022. Santa Barbara (CA), United States: Springer Nature Switzerland, Aug. 2022, pp. 513–540. DOI: 10.1007/978-3-031-15979-4. URL: https://hal.science/hal-03597834.

[45] S. Bordage, M. Lhotel, J. Nardi and H. Randriam. 'Interactive Oracle Proofs of Proximity to Algebraic Geometry Codes'. In: *CCC 2022 - 37th Computational Complexity Conference*. Ed. by S. D.-.-L.-Z. fuer InformatikDagstuhlGermany. Philadelphie, United States, July 2022, 30:1–30:45. DOI: 10.4230/LIPIcs.CCC.2022.30. URL: https://telecom-paris.hal.science/hal-03832439.

[46] 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*. Vol. 13794. Lecture Notes in Computer Science. Taipei, Taiwan: Springer, Dec. 2022, pp. 477–507. DOI: 10.1007/978-3-031-22972-5. URL: https://inria.hal.science/hal-03919778.

[47] 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.

[48] S. Puchinger, J. Renner and A. Wachter-Zeh. *Twisted Gabidulin Codes in the GPT Cryptosystem*. 2018. arXiv: 1806.10055 [cs.IT].

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

[50] 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).