RESEARCH CENTRE

Inria Saclay Centre at Institut Polytechnique de Paris

IN PARTNERSHIP WITH:

CNRS, Institut Polytechnique de Paris

2024

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]
- Daniel Augot [INRIA, Senior Researcher]
- Thomas Debris [INRIA, Researcher]
- Benjamin Smith [INRIA, Researcher]
- Gustavo Souza Banegas [INRIA, ISFP, from Oct 2024]

Faculty Members

- Olivier Blazy [Ecole Polytechnique, Professor]
- Martino Borello [Université Paris 8, Associate Professor Delegation, from Feb 2024 until Jul 2024]
- Françoise Levy-Dit-Vehel [ENSTA, Professor]
- François Morain [Ecole Polytechnique, Professor]

Post-Doctoral Fellows

- Christophe Levrat [INRIA, Post-Doctoral Fellow, from May 2024]
- Rati Ludhani [INRIA, Post-Doctoral Fellow, from Oct 2024]
- Rakhi Pratihar [INRIA, Post-Doctoral Fellow]
- Bruno Sydney Sterner [INRIA, Post-Doctoral Fellow]

PhD Students

- Nadja Aoutouf [INRIA]
- Valentina Astore [INRIA, from Oct 2024]
- Estelle Blin [LIX, from Oct 2024]
- Sana Boussam [THALES, CIFRE]
- Hugo Delavenne [LIX]
- Clément Ducros [UNIV PARIS, until Sep 2024]
- Anaelle Le Devehat [INRIA]
- Pierre Loisel [INRIA]
- Lola-Baie Mallordy [LIX, from Mar 2024]
- Tanguy Medevielle [IRMAR]
- Antoine Moran [CEA, from May 2024]
- Antonio Ras [CEA, from May 2024 until Oct 2024]
- Eric Sageloli [THALES]
- Nihan Tanisali [INRIA]

Interns and Apprentices

- Estelle Blin [LIX, from Mar 2024 until Sep 2024]
- Penelope Forcioli [LIX, until Mar 2024]
- Maxence Jauberty [TELECOM PARIS, Intern, from Sep 2024]
- Elina Roussel [CENTRALESUPELEC, Intern, from Mar 2024 until Aug 2024]
- Alessandro Sferlazza [INRIA, Intern, from May 2024 until Sep 2024]
- Pauline Vinchon [INRIA, Intern, from Jun 2024 until Aug 2024]

Administrative Assistant

- Mariana De Almeida [INRIA]

External Collaborators

- Martino Borello [UNIV PARIS VIII, from Aug 2024]
- Lucien Francois [UNIV DUBLIN, from Oct 2024]
- Guenael Renault [SGDSN]
- Martin Scotti [UNIV PARIS VIII, from Sep 2024]
- Tamara Topalov [LIX, from Feb 2024 until Jun 2024]
- Neehar Verma [UNIV AALTO, from Nov 2024]

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, Guenaël Renault, Benjamin Smith, Bruno Sterner.

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.

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: François Morain, Anaëlle Le Dévéhat, Benjamin Smith, Gustavo Souza–Banegas, Bruno Sterner.

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, 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: Olivier Blazy, Alain Couvreur, Thomas Debris–Alazard, Anaëlle Le Dévéhat, Pierre Loisel, Antoine Moran, Antonio Ras, Benjamin Smith, Gustavo Souza–Banegas, Bruno Sterner.

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, 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. Youssef 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.

Daniel 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). Daniel 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: Olivier Blazy, François Morain, Antoine Moran, Guenaël Renault, Benjamin Smith, Gustavo Souza–Banegas.

We are interested in developing interactions between cryptography and cybersecurity. In particular, we are carrying out research in embedded security (side channels and fault attacks), software security (finding vulnerabilities efficiently and defining efficient countermeasures), 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.

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 Social and environmental responsibility

5.1 Impact of research results

The works of Olivier Blazy on age verification is cited as a reference basis by ARCOM in their October 2024 report. See page 7 of this report.

6 Highlights of the year

6.1 Awards

- Maxime Bombar, a former PhD student recieved the PhD Award in computer science of Institut Polytechnique de Paris.

- Bruno Sternerwon the *ANTSy (best lightning talk)* award at ANTS-XVI.

7 New software, platforms, open data

7.1 New software

7.1.1 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

7.1.2 WaveSign

Name: Wave Signatures: Reference Implementation

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

8 New results

8.1 Mathematical foundations

8.1.1 A Freiman-like Theorem for function fields

Participants: Alain Couvreur.

A famous Theorem of additive number theory due to Freiman claims that given $A \subset \mathbb{Z}$ whose Minkowski sum

$$A + A \stackrel{\text{def}}{=} \{a + b \mid a, b \in A\}$$

satisfies

$$|A + A| \leq 3|A| - 4$$

then A is contained in an arithmetic progression where at most $|A + A| - 2|A| + 1$ elements are missing.

Motivated by question from coding theory, secret sharing and code-based cryptography, Alain Couvreur in a collaboration with Gilles Zémor (*Institut de Mathématiques de Bordeaux*) obtained the following result in [28].

Theorem. Let K be a perfect field and F/K be an extension in which K is algebraically closed. Let $S \subset F$ be a K–subspace of finite dimension such that the subspace

$$S^2 \stackrel{\text{def}}{=} \text{Span}_K\{st \mid s,t \in S\}$$

satisfies $1 \in S$ and

$$\dim S^2 \leq 3 \dim S - 4.$$

Then S generates a subfield of F of transcendence degree 1 over K with genus g satisfying $g \leq \dim S^2 - 2\dim S + 1$. Moreover, S is contained in a Riemann-Roch space $\mathscr{L}(D)$ and has codimension at most $\dim S^2 - 2\dim S + 1 - g$ in this space.

8.1.2 Decoding of rank metric Reed–Muller codes

Participants: Alain Couvreur, , Rakhi Pratihar.

The notion of Θ-polynomials over a finite abelian extension $\mathbb{L}$ of an arbitrary field $\mathbb{K}$, where $\Theta = (\theta_1,\dots,\theta_m)$ gives a system of generators for $\mathrm{G} := \mathrm{Gal}(\mathbb{L}/\mathbb{K}) = \mathbb{Z}/n_1\mathbb{Z} \times \cdots \times \mathbb{Z}/n_m\mathbb{Z}$, is a generalization of the q-polynomials over finite fields introduced by Ore in 1933. A Θ-monomial $\theta_1^{i_1}\cdots\theta_m^{i_m}$ describes the m-tuple $(i_1,\dots,i_m) \in \mathbb{Z}/n_1\mathbb{Z} \times \cdots \times \mathbb{Z}/n_m\mathbb{Z}$ and every element in the skew group algebra $\mathbb{L}[\mathrm{G}]$ have a unique representation as a Θ-polynomial

$$P = \sum_{(i_1,\dots,i_m)} b_{(i_1,\dots,i_m)}\theta_1^{i_1}\cdots\theta_m^{i_m},$$

where $\deg_\Theta(P) \stackrel{\text{def}}{=} \max\{i_1+\cdots+i_m \colon b_{(i_1,\dots,i_m)} \neq 0\}$. Keeping the analogy with classical Reed–Muller codes defined as evaluation of multivariate polynomials of bounded degree, Augot, Couvreur, Lauvazelle, and Neri [36] introduced in 2021 the Θ-Reed–Muller codes in the rank metric as the $\mathbb{L}$-subspaces of $\mathbb{L}[\mathrm{G}]$ as follows:

For $0 < r \leq \sum_{i=1}^m (n_i - 1)$, the Θ-Reed-Muller code of order r and type $\boldsymbol{n} \stackrel{\text{def}}{=} (n_1,\dots,n_m)$ is defined as

$$\mathrm{RM}_\Theta(r,\boldsymbol{n}) \stackrel{\text{def}}{=} \{P \in \mathbb{L}[\mathrm{G}] \colon \deg_\Theta(P) \leq r\}.$$

In a joint work [26], Alain Couvreur and Rakhi Pratihar address the following decoding problem for $RM_\Theta(r,\boldsymbol{n})$:

Problem: Given $Y \in \mathbb{L}[\mathrm{G}]$ such that $Y = C + E$ for some $C \in \mathrm{RM}_{\boldsymbol{\theta}}(r,\mathbf{n})$ and $E \in \mathbb{L}[\mathrm{G}]$ with $\mathrm{Rk}(E) = t = \lfloor \frac{d-1}{2} \rfloor$, where d is the minimum distance of $\mathrm{RM}_{\boldsymbol{\theta}}(r,\mathbf{n})$, recover the pair (C,E).

The authors give a method for reconstructing the error Θ-polynomial by recovering its unknown coefficients by minor cancellations of the associated G-Dickson matrix, which leads to the following.

Theorem. Let $C = \sum_{i=0}^{N-1}$ be an element of $\mathrm{RM}_\Theta(r,\mathbf{n})$. and k and d denote the $\mathbb{L}$–dimension and the minimum distance of $\mathrm{RM}_\Theta(r,\mathbf{n})$, respectively. Let $Y = C + E$ be the received polynomial for some $E \in \mathbb{L}[\mathrm{G}]$ with $\mathrm{Rk}(E) \leq \lfloor \frac{d-1}{2} \rfloor$, then C can be recovered uniquely in $\mathcal{O}(kt^\omega)$ operations in $\mathbb{L}$, where ω denotes the complexity exponent of linear algebraic operations.

8.2 Post–quantum cryptography

8.2.1 Quantum oblivious LWE sampling and insecurity of standard model lattice-based SNARKs

Participants: Thomas Debris–Alazard.

The Learning With Errors (LWE) problem [44] is well-known for its conjectured intractability for quantum algorithms, inherited from the conjectured worst-case hardness of specific problems over Euclidean lattices. It has led to abundant cryptographic constructions that are presumably quantum resistant. For three integers m, n, q as well as a distribution χ_σ over $\mathbb{Z}/q\mathbb{Z}$ concentrated on values that are small modulo q and with standard deviation σ, the search version of LWE with parameters m, n, q and σ consists in recovering the secret $\mathbf{s}$ from the LWE instance $(\mathbf{A}, \mathbf{As}+\mathbf{e}) \in (\mathbb{Z}/q\mathbb{Z})^{m\times n} \times (\mathbb{Z}/q\mathbb{Z})^m$ where $\mathbf{e}$ is i.i.d. from χ_σ. From a hardness point of view, it was shown in [44] that the LWE problem with well chosen parameters m, n, q, σ is quantumly at least as hard as some worst-case lattice problems in dimension n. From an algorithmic viewpoint, there is no known polynomial time solvers (classical or quantum) for the aforementioned regime of parameters.

In this work, we did not focus on the hardness of LWE, but on the task of generating LWE samples: $\mathbf{b} = \mathbf{As}+\mathbf{e} \in (\mathbb{Z}/q\mathbb{Z})^m$. For parameters of cryptographic interest, a correctly distributed LWE pair $(\mathbf{A}, \mathbf{b})$ admits a unique pair $(\mathbf{s}, \mathbf{e})$ that is much more likely than any other pair to satisfy $\mathbf{b} = \mathbf{As}+\mathbf{e}$. As the correctly formed $\mathbf{b}$'s are extremely sparse in their range, the naive approach of sampling a uniform $\mathbf{b}$ and keeping it if it has the correct form is prohibitively expensive. Given this, it could seem that the only way to proceed to build LWE samples is to first create $\mathbf{s}$ and $\mathbf{e}$ and then return $\mathbf{As}+\mathbf{e}$. It has then been conjectured that all LWE samplers are such that they know the underlying secrets $\mathbf{s}$ and $\mathbf{e}$. It turns out that this natural assumption has been pivotal to serve as security foundation of Succinct Non-interactive Arguments of Knowledge (SNARKs) whose security inherits from lattice assumptions [41, 43, 42, 45, 39, 40].

Motivated by the task of invalidating the security assumption used in almost all known lattice-based SNARKs (claiming to be safe even against quantum computers), Thomas Debris–Alazard in collaboration with Pouria Fallahpour (*ENS Lyon*) and Damien Stehlé (*CryptoLab*) designed in [18] an efficient algorithm that generates LWE samples without knowing the underlying secret (under the assumption that LWE is intractable). This result, beyond showing that aforementioned lattice-based SNARKs are not quantumly secure, shows that "oblivious" LWE sampling can be performed quantumly efficiently while the problem seems to be hard classically. So far, only extremely few problems related to lattices admit a quantum polynomial-time algorithm while remaining conjecturally hard for classical algorithms.

8.2.2 Isogeny formulæ in dimension 2

Participants: Benjamin Smith.

While the basic arithmetic of genus-2 Jacobians and Kummer surfaces has matured, and cryptographic applications have driven great improvements in the efficiency of the resulting formulæ and algorithms, the corresponding explicit theory of isogenies lags behind. Just as elliptic isogenies factor naturally into compositions of scalar multiplications and isogenies with prime cyclic kernel (i.e., isomorphic to $\mathbb{Z}/N\mathbb{Z}$ with N prime), isogenies of abelian surfaces (including Jacobians of genus-2 curves) decompose into compositions of scalar multiplications and (N, N)-isogenies (with kernel isomorphic to $(\mathbb{Z}/N\mathbb{Z})^2$. The fundamental task, then, is to compute and evaluate prime (N, N)-isogenies. The problem is especially relevant today given the role of genus-2 isogenies in isogeny-based cryptography, where they have been the basis of both devastating attacks and radical optimizations since 2022. The case $N = 2$ is classical: explicit methods and formulæ go back to the 19th century, but the case of prime $N > 2$ has proven more complicated.

In [12], we give a general method for deriving explicit formulæ for isogenies of fast Kummer surfaces—the most relevant surfaces for genus-2 isogeny-based cryptography—exploiting their high symmetry to optimize the approach of Bruin, Flynn, and Testa. Our approach is elementary in the sense that it avoids explicitly using the heavy machinery of theta functions (though of course theta functions implicitly play a fundamental role behind the scenes). We apply these methods to give explicit examples for $N = 3$ and 5.

8.3 Secure multiparty computation: FOLEAGE

Participants: 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 [37], 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 [16], we proposed an optimised construction of OLE's over $\mathbb{F}_2$ from group algebras over $\mathbb{F}_4$. Its security rests on a new problem called *Quasi-Abelian Syndrome Decoding*. This new construction permits to construct very long pseudo-random correlated strings over the binary field. It can concretely produce over 12 million triples per second in the 2-party setting on one core of a commodity machine. Our construction significantly outperforms the state-of-the-art, which we demonstrate via a prototype implementation. This is achieved by introducing a number of protocol-level, algorithmic-level, and implementation-level optimizations on the recent PCG construction of Bombar et al. [38] from the Quasi-Abelian Syndrome Decoding assumption. This result is a part of Clément Ducros's PhD thesis [23]

8.4 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.

8.4.1 Verifiable computation based on coding theory

Participants: Daniel Augot, Hugo Delavenne, Tanguy Medevielle, Élina Roussel.

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 Interactive Oracle Proof of Proximity (IOPP) has been designed for codes on graphs. The soundness is significantly improved compared to the FRI, the complexity parameters are comparable, the domain of validity is provably better, and there are no restrictions on the field used, enabling to consider new codes to design code-based SNARKs. Under submission.

8.5 Algorithmic number theory

8.5.1 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. In our investigations, we resumed some old work of Fricke, see the two preprints [32] and [33]. In particular, new formulas for the final isogeny computation were worked out.

8.5.2 Factoring over number fields

Participants: François Morain.

This is an exploratory topic aiming at transposing classical integer factoring algorithms into the realm of euclidean number fields. The traditional strategy to factor an integer of a number field is to factor its norm over Z and then finding the ideals dividing the original integer. Here, we give some hints at factoring the number without going to Z. This approach was suggested following the solving of an ANSSI CTF.

8.5.3 Cryptographic smooth twins

Participants: Bruno Sterner.

A pair of consecutive integers is a *smooth twin* if their product is B-smooth for some small B (i.e., each prime factor in the product is $\leq B$). Smooth twins whose sum is a prime are used in some isogeny-based cryptosystems such as SQIsign. We have made progress on finding large smooth twins with smaller smoothness bounds. One approach to finding smooth twins is to find polynomials $f(x)$ and $g(x) = f(x)+1$ in $\mathbb{Q}[x]$ that both split into a product of small degree factors, then evaluate them at smooth integers. Costello, Meyer, and Naehrig (EUROCRYPT 2021) used polynomials that split completely into distinct linear factors, which they found using Diophantine number theory. Here is a degree-8 example that they found:

$$f(x) = x(x+4)(x+9)(x+23)(x+27)(x+41)(x+46)(x+50),$$
$$g(x) = (x+1)(x+2)(x+11)(x+20)(x+30)(x+39)(x+48)(x+49).$$

In our new work [20], we allow repeated linear factors and some quadratic factors. The overall smoothness probability is either better than or comparable with that of the prior polynomials. Here is a degree-8

example:

$$f(x) = (x+1)(x+4)(x+9)(x+10)(x+15)(x+18)(x^2+19x-12),$$
$$g(x) = x^2(x+6)^2(x+13)^2(x+19)^2.$$

We use these polynomials to search for large smooth twins whose sum is prime. We thus find 384 and 512-bit twins with significantly smaller smoothness bounds than those found at EUROCRYPT 2021.

9 Bilateral contracts and grants with industry

9.1 Bilateral contracts with industry

Participants: Daniel Augot, Guénaël Renault, Benjamin Smith.

- Through École polytechnique, Daniel 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.

10 Partnerships and cooperations

10.1 International research visitors

10.1.1 Visits of international scientists

Other international visits to the team

Lucien François

Status PhD Student

Institution of origin: University College Dublin

Country: Ireland

Dates: From October 7th 2024 to July 6th 2025.

Context of the visit: Secondment visit in the context of ENCODE Project. The thesis of Lucien François concerns tensor codes *i.e.* subspaces of tensor products of $m \geq 3$ finite dimensional vector spaces and decoding problems related to such spaces.

Mobility program/type of mobility: See ENCODE Section 10.2.1

Neehar Verma

Status PhD Student

Institution of origin: University of Aalto

Country: Finland

Dates: From November 1st 2024 to February 28th 2025.

Context of the visit: Secondment visit in the context of ENCODE Project. The beginning of Neehar Verma's PhD was dedicated to analyzing Private Information Retrieval (PIR) over graph-based distributed storage systems. Following a work of Raviv, Tamo and Yaakobi in 2020, we encode the files of a database, and distribute parts of each encoded file to a set of servers. This file dispersion induces a hypergraph, where the servers are the vertices and each file corresponds to a hyperedge consisting of the subset of servers that contain part of its encoding. Raviv et al. considered 2-replication, and modeled the privacy leakage by means of cycles in the induced graph. We extend their result to (MDS) encoding. We model and quantify the privacy leakage in terms of the presence of polychromatic cycles in the coloured multigraph corrresponding to the induced hypergraph.

Mobility program/type of mobility: See ENCODE Section 10.2.1

10.2 European initiatives

10.2.1 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: Françoise Levy-dit-Vehel

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.

10.3 National initiatives

10.3.1 ANR CIAO

Participants: Benjamin Smith.

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.

10.3.2 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.

10.3.3 ANR BARRACUDA

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

BARRACUDA is a collaborative ANR project accepted in 2021 and led by Alain 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.

10.3.4 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.

10.3.5 ANR Priva-SiQ

Participants: Benjamin Smith, Olivier Blazy, Thomas Debris–Alazard.

Priva-Siq is a collaborative ANR project accepted in 2023.
Website : anr.fr/Projet-ANR-23-CE39-0008
The Priva SIQ projects aims to manage threats to user-privacy in secure-channel establishment, at all levels. In this project, the goal is to specifically tackle the following threats:

- Interception: Privacy with respect to person-in-the-middle adversaries (exterior to the communication and aiming to track, deanonymize, or identify an endpoint of the channel);
- Subversion: Providing privacy-enhancing countermeasures against mass-surveillance attacks;
- Quantum adversaries: Designing protocols that preserve both user-privacy and security against powerful quantum adversaries.

10.3.6 ANR TRUST

Participants: Olivier Blazy.

Trust is a collaborative ANR project accepted in 2023.
Website : anr.fr/Project-ANR-23-CE39-0009
TRUST focuses on personal data protection measures to meet the objectives of the RGPD but also the texts in preparation such as the "Data Act" or the "Data Governance Act". This project aims to study and develop new security solutions, based on advanced cryptography, for use cases involving the reuse of personal data. These use cases will present various configurations in terms of actors, type of data and processing, opening the way to different technical and legal issues. This is done in order to anticipate legal evolutions and prepare technical architectures to allow the reuse of personal data in compliance with the various legal frameworks.

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

Participants: Alain Couvreur, Thomas Debris–Alazard, Anaëlle Le Dévéhat, Rakhi Pratihar, Antonio Ras, Benjamin Smith.

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.

10.3.8 Inria AEx CACHAÇA

Participants: Anaëlle Le Dévéhat, Guenaël Renault, Benjamin Smith, Bruno Sterner.

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).

10.3.9 HYPERFORM

Participants: Olivier Blazy, Guenaël Renault, Benjamin Smith, Bruno Sterner, Alessandro Sferlazza.

Benjamin Smith is coordinating Inria's involvement in the Bpifrance-funded HYPERFORM industrial consortium (2023–2026), which aims to develop a pre- and post-quantum hybrid cryptographic reference platform.

10.4 Public policy support

10.4.1 Regulation

Participants: Daniel Augot.

Daniel Augot participates to a working group jointly managed by ACPR (autorité de contrôle prudentiel et de résolution) and AMF (autorité des marchés financiers). This working group will report on proposals and recommendations for the regulation of smart contracts in the context of decentralized finance (blockchains).

10.4.2 Academia of Science and Technology

Daniel Augot contributed as an expert to a report on blockchains from Académie des sciences et technologies.

10.4.3 Eidas 2

Participants: Olivier Blazy.

Olivier Blazy participates to working groups supervised by the European commission around the implementation of the new European digital identity and wallet.

11 Dissemination

11.1 Promoting scientific activities

11.1.1 Scientific events: organisation

- Daniel Augot and Alain Couvreur organised the second Encode Training School for ENCODE project at *Institut Henri Poincaré* from April 29 to may 3rd 2024. This workshop was a sequence of mini-lectures and discussion dedicated to the training of the ENCODE PhD students.

Member of the organizing committees

- Benjamin Smith was *lightning talks chair* at ANTS-XVI.

11.1.2 Scientific events: selection

Member of the conference program committees

- Alain Couvreur served on the program committees of
  - ISIT 2024;
  - SCN 2024;
  - WCC 2024.
- Daniel Augot served on the program committee of
  - WCC 2024 (workshop on Coding and Cryptography);
  - CBT 2024 (International Workshop on Cryptocurrencies and Blockchain Technology)
  - ESORICS 2024 (European Symposium on Research in Computer Security)
  - WTSC 24 (Workshop on Trusted Smart Contracts);
  - ICBC 2024 (IEEE International Conference on Blockchain and Cryptocurrency)
- Benjamin Smith served on the program committees of
  - ANTS-XVIANTS-XVI (16th Algorithmic Number Theory Symposium)
  - SAC 2024 (Selected Areas in Cryptography)
  - CT-RSA 2025
  - PQCrypto 2025
- Olivier Blazy served on the program committees of
  - Eurocrypt 2024
  - CT-RSA 2025
  - PQCrypto 2024
  - Africacrypt 2024

Reviewer

- Alain Couvreur was external reviewer for the conferences
  - CRYPTO 2024;
  - ANTS 2024.
- Thomas Debris–Alazard was external reviewer for the conferences
  - CRYPTO 2024;

  - SCN 2024;
  - ISIT 2024.

- François Morain was external reviewer for the conferences
  - ANTS 2024.
  - ISSAC 2024.

- Daniel Augot was external reviewer for
  - ISSAC'24 (International Symposium of Symbolic and Algebraic Computation)

- Benjamin Smith was an external reviewer for
  - ISIT 2024;
  - AGC2T 2023 (post-proceedings);
  - ASIACRYPT 2024;
  - FSTTCS 2024.

- Bruno Sterner was external reviewer for
  - PKC 2024
  - SAC 2024
  - PQCrypto 2025

11.1.3 Journal

Member of the editorial boards

- Alain Couvreur is associate editor in the journals
  - *SIAM Journal on Applied Algebra and Geometry*;
  - *IEEE Transactions on Information Theory*;
  - *Publications Mathématiques de Besançon*.

- Thomas Debris–Alazardhas been guest editor for a special issue dedicated to coding theory in the journal Designs, Codes and Cryptography.

- Benjamin Smithis a member of the editorial board for IACR Communications in Cryptology.

- Olivier Blazyis a member of the editorial board for Computer law and security reviews

Reviewer - reviewing activities

- Alain Couvreur was reviewer for the journals:
  - *Finite Fields and their Applications*,
  - *SIAM Journal on Applied Algebra and Geometry*.

- Rakhi Pratihar was reviewer for the journals:
  - *Journal of Algebra and its applications*;
  - *Designs Codes and Cryptography*;
  - *Combinatorial Theory*

- Benjamin Smith was reviewer for *Mathematics of Computation*.

- Bruno Sterner was reviewer for *Designs, Codes and Cryptography*.

11.1.4 Invited talks

- Olivier Blazy was an invited speaker at
  - SAC 2024
  - Stanford Cyber Policy Center Spring Seminar
  - Alain Couvreur gave a talk at the *Algebraic Coding Theory* session at the joint AMS-UMI workshop 2024 in Palermo.
  - Thomas Debris–Alazard was invited speaker at:
    * the thirteenth International Workshop on Coding and Cryptography (WCC '24);
    * the conference Mathematics for post-quantum cryptanalysis
  - Rakhi Pratihar gave invited talks at
    * ADMA - ICDM 2024 : 20th Annual Conference of Academy of Discrete Mathematics and Applications & International Conference on Discrete Mathematics 2024;
    * International conference on Women in Pure and Applied Mathematics (India).
  - Benjamin Smith was an invited speaker at
    * Mathematics for post-quantum cryptanalysis
    * The kick-off event for the *Inria–Einstein Centre Digital Future* partnership, ECDF, Berlin.

11.1.5 Leadership within the scientific community

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

11.1.6 Scientific expertise

- Alain Couvreur was evaluator for the *Cum Laude Judicum* (an exceptional award for the PhD degree) for TUe (Eindhoven).
- Olivier Blazy was evaluator for the Horizon Cybersecurity Call CL3-CS-01
- Benjamin Smith is a member of the *Comité de Pilotage, Stratégie Nationale Quantique (volet Normalisation)*

11.1.7 Research administration

- Daniel Augot was member of a recruiting committee (*Comité de sélection*) for a *Chargé de conférences* at University of Bordeaux.
- Daniel Augot was member of a recruiting committee (*Comité de sélection*) for a *Chargé de conférences* at University of Grenoble.
- Olivier Blazy was a member of recruitment committees for *Mâitre de conférences* positions in Amiens, and Clermont-Ferrand.
- Olivier Blazy was president of the recruitement committee for Professor at Ecole polytechnique.
- Alain Couvreur is elected member of Inria's *Commission d'Évaluation*. He served in the recruitment jury CRCN centre Inria de Lille.
- Alain Couvreur is coordinator 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).
- Alain Couvreur was member of a recruiting committee (*Comité de sélection*) for a *Chaire de Professeur Junior* at University of Rennes.
- François Morain is a member of the Board of Master Parisien de Recherche en Informatique (MPRI).

- François Morain is a member of the board of the Cybersecurity track in the CS Master of IPParis.
- François Morain represents the axis networks and security at the "conseil de direction" of LIX.
- Benjamin Smith was a member of a recruitment committee (*Comité de sélection*) for a *Mâitre de conférences* position at the University of Nancy.
- Benjamin Smith is co-leader of the PEPR PQ-TLS work package on isogeny-based cryptography with Benjamin Wesolowski (CNRS).
- Benjamin Smith is the Inria coordinator for the HYPERFORM industrial consortium.

11.2 Teaching - Supervision - Juries

11.2.1 Teaching

- Licence:
  - Olivier Blazy: *CSE101: Introduction to Computer Programming* (Tutorials), 31.5h, L1, École polytechnique, France
  - Maxime Bombar: *INF361: Introduction à l'informatique* (tutorials), 40h (equiv TD), 1st year (L3), École polytechnique.
  - Thomas Debris–Alazard, Exercises for INF361: "Introduction à l'informatique", 15h (equiv TD), 1st year (L3), École polytechnique.
  - François Morain, Lectures for INF361: "Introduction à l'informatique", 15h (equiv TD), 1st year (L3), École polytechnique. Coordinator of this module (350 students).
  - Bruno Sterner, Tutorials for *CSE103: Introduction to Algorithms*, 28h, L1, École polytechnique.
- Master:
  - Daniel Augot designed with Julien Prat the cursus of a course in blockchains and economics, and made lectures on zero-knowledge.
  - Master : Olivier Blazy: Lectures and Labs for *Authentification, VPN et Chiffrement*, 6h, M2, Telecom Sud Paris, France
  - Thomas Debris–Alazard: Lectures for CSC_51063_EP: "Information Theory", 36h, M1, École Polytechnique
  - Thomas Debris–Alazard: Lectures for INF563: "Information Theory", 36h, M1, École Polytechnique
  - Thomas Debris–Alazard: Lectures for MDC_51002_EP: "Quantum Information and Computing", 18h, M1, École Polytechnique
  - Thomas Debris–Alazard: Lectures for INF587: "Introduction to quantum computer science", 36h, École polytechnique.
  - Alain Couvreur and Thomas Debris–Alazard : Lectures in *MPRI 2-13-2: Error Correcting codes and applications to cryptography*
  - François Morain, INF558, Lectures and labs *Introduction to cryptology*, 36h, M1, École Polytechnique
  - Françoise Levy-dit-Vehel, Lectures on discrete maths, 21h, M1, ENSTA
  - Françoise Levy-dit-Vehel, Lectures on cryptography, 24h, M2, ENSTA.
  - Matthieu Lequesne, INF558, labs *Introduction to cryptology*, 36h, M1, École Polytechnique
  - Guenaël Renault: Lectures and Labs for *INF565: Information Systems Security*, 60h, M1, École polytechnique, France
  - Guenaël Renault: Lectures and Labs for *INF648: Embedded security: side-channel attacks; javacard*, 60h, M2, École polytechnique, France

  - Master : Guenaël Renault: Coordinator for *INF637: Reverse engineering vs Obfuscation*, 2h, M2, École polytechnique, France
  - Benjamin Smith: *INF568: Advanced Cryptography*, 45h, M1, École polytechnique, France
  - Benjamin Smith: *MPRI 2-12-2: Algorithmes Arithmétiques pour la Cryptologie*, 22.5h, M2, Master Parisien de Recherche en Informatique, France.
  - Daniel Augot: *Structures de données distribuées, avec un focus sur les blockchains (2024-2025)*, 8h, M1 École polytechnique

11.2.2 Supervision

- Martino Borello advised the Master Project of Valentina Astore.
- Françoise Levy-dit-Vehel advised the Cybersecurity M2 IP Paris Internship of Elouan Gros on "Private Information Retrieval with Resut Verification".
- Benjamin Smith supervised
  - Alessandro Sferlazza's M2 internship (SNS Pisa)
  - Pauline Vinchon's M1 internship (ENSTA)
  - Cezara Petrui's Bachelor Thesis (École polytechnique Bachelor, L3)
  - Hongjie Zhang's Executive MSc&T Cybersecurity masters project (Renault and École polytechnique)
  - Luc Papadopoulos's Executive MSc&T Cybersecurity masters project (Crédit Agricole and École polytechnique)
  - Franck Wetie's Executive MSc&T Cybersecurity masters project (École polytechnique)

11.2.3 Juries

- Alain Couvreur was referee for the PhD theses of
  - Victor Dyseryn (Univerity of Limoges);
  - Antoine Leudière (University of Lorraine).
- Alain Couvreur was president of the jury for the PhD thesis of Quyen Ngyen (University of Caen);
- Alain Couvreur was jury member for the HDR of Martin Weimann (University of Caen);
- Daniel Augot was jury member of the thesis of Karima Maklouf (Institut Polytechnique de Paris)
- Daniel Augot was reviewer of the following theses:
  - Loïc Demange (Sorbonne Université)
  - Thomas Lavaur (Université de Toulouse)
- Benjamin Smith was referee for the PhDs of
  - Marc Houben (Leiden Universiteit, Netherlands)
  - Jonathan Komada Eriksen (NTNU Trondheim, Norway)
- Thomas Debris–Alazard was jury member for the PhD theses:
  - Pouria Fallahpour (ENS Lyon);
  - Étienne Burle (Université of Rouen).
- Olivier Blazy was president for the PhD theses:
  - Thibaut Jacques (Université de Limoges)

  - Charles Olivier-Anclin (Université de Clermont-Ferrand)
  - Hugo Beguinet (Ecole Normale Supérieure)

- Olivier Blazy was reviewer for the PhD theses:
  - Corentin Jeudy (Université de Rennes)
  - Calvin Abou Haidar (École normale supérieure de Lyon)
  - Colin Putman (Royal Holloway London)

11.3 Popularization

11.3.1 Productions (articles, videos, podcasts, serious games, ...)

- Nadja Aoutouf and Nihan Tanısalı are Encode members and published two YouTube videos about Coding Theory
  - YouTube channel AliceandBob
  - Coding Theory (Part 1/2)
  - Coding Theory (Part 2/2)

11.3.2 Participation in Live events

- Benjamin Smith was a panel member for the Webinar **Forum InCyber – ONE Conference** *Your Cryptography Will Be Broken. Prepare now! A NL-FR exchange of views* at Campus Cyber, La Défense Paris.

11.3.3 Others science outreach relevant activities

Participants: Daniel Augot, Christophe Levrat, Pierre Loisel.

We received a whole afternoon the whole promotion of M1 students of University of Versailles Saint-Quentin, to introduce them to cryptography, coding and INRIA.

12 Scientific production

12.1 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.

12.2 Publications of the year

International journals

[8] G. Alfarano, M. Borello and A. Neri. 'Outer strong blocking sets'. In: *The Electronic Journal of Combinatorics* (15th Mar. 2024). URL: https://hal.science/hal-04508476. In press.

[9] E. Berardini, A. Couvreur and G. Lecerf. 'A proof of the Brill-Noether method from scratch'. In: *ACM Communications in Computer Algebra* 57.4 (15th Mar. 2024), pp. 200–229. DOI: 10.1145/3653002.3653004. URL: https://hal.science/hal-03762780.

[10] M. Borello, W. Schmid and M. Scotti. 'The geometry of intersecting codes and applications to additive combinatorics and factorization theory'. In: *Journal of Combinatorial Theory, Series A* (2025). URL: https://hal.science/hal-04896981. In press.

[11] A. Chailloux and T. Debris-Alazard. 'New Solutions to Delsarte's Dual Linear Programs'. In: *IEEE Transactions on Information Theory* 71.1 (Jan. 2025), pp. 297–316. DOI: 10.1109/TIT.2024.3476974. URL: https://inria.hal.science/hal-04884027.

[12] M. Corte-Real Santos, C. Costello and B. Smith. 'Efficient $(3,3)$-isogenies on fast Kummer surfaces'. In: *Research in Number Theory* 11.1 (11th Jan. 2025), p. 25. DOI: 10.1007/s40993-024-00600-y. URL: https://inria.hal.science/hal-04433463 (cit. on p. 11).

[13] H. Delavenne and F. L. Gall. 'Quantum State Synthesis: Relation with Decision Complexity Classes and Impossibility of Synthesis Error Reduction'. In: *Quantum Information & Computation* 24.9&10 (3rd July 2024), pp. 745–765. DOI: 10.26421/QIC24.9-10-3. URL: https://hal.science/hal-04634958.

International peer-reviewed conferences

[14] N. Aragon, A. Couvreur, V. Dyseryn, P. Gaborit and A. Vinçotte. 'MinRank Gabidulin Encryption Scheme on Matrix Codes'. In: *Lecture Notes in Computer Science*. ASIACRYPT 2024 - 30th International Conference on the Theory and Application of Cryptology and Information Security. Vol. LNCS-15487. Advances in Cryptology – ASIACRYPT 2024. KOLKATA, India: Springer Nature Singapore, 13th Dec. 2024, pp. 68–100. DOI: 10.1007/978-981-96-0894-2_3. URL: https://inria.hal.science/hal-04894346.

[15] A. Barthoulot, O. Blazy and S. Canard. 'Cryptographic Accumulators: New Definitions, Enhanced Security, and Delegatable Proofs'. In: *Progress in Cryptology - AFRICACRYPT 2024*. AFRICACRYPT 2024 - 15th International Conference on Cryptology. Vol. 14861. Lecture Notes in Computer Science. Douala, Cameroon: Springer Nature Singapore, 2024, In press. URL: https://hal.science/hal-04618343.

[16] M. Bombar, D. Bui, G. Couteau, A. Couvreur, C. Ducros and S. Servan-Schreiber. 'FOLEAGE: F 4 OLE-Based Multi-Party Computation for Boolean Circuits'. In: *Advances in Cryptology – ASIACRYPT 2024*. ASIACRYPT 2024 - 30th International Conference on the Theory and Application of Cryptology and Information Security. Vol. 15489. Lecture Notes in Computer Science. Kolkata, India: Springer Nature Singapore, 13th Dec. 2024, pp. 69–101. DOI: 10.1007/978-981-96-0938-3_3. URL: https://hal.science/hal-04770551 (cit. on p. 12).

[17] A. Couvreur, A. Canteaut and L. Perrin. 'On the Properties of the Ortho-Derivatives of Quadratic Functions'. In: WCC 2024 - The Thirteenth International Workshop on Coding and Cryptography. Perugia, Italy, 17th June 2024. URL: https://inria.hal.science/hal-04648515.

[18] T. Debris-Alazard, P. Fallahpour and D. Stehlé. 'Quantum Oblivious LWE Sampling and Insecurity of Standard Model Lattice-Based SNARKs'. In: STOC 2024 - 56th Annual ACM Symposium on Theory of Computing. Vancouver BC, Canada: ACM, 11th June 2024, pp. 423–434. DOI: 10.1145/3618260.3649766. URL: https://hal.science/hal-04891122 (cit. on p. 11).

[19] T. Debris-Alazard, P. Loisel and V. Vasseur. 'Exploiting Signature Leakages: Breaking Enhanced pqsigRM'. In: 2024 IEEE International Symposium on Information Theory (ISIT). Athens, France: IEEE, 7th July 2024, pp. 2903–2908. DOI: 10.1109/ISIT57864.2024.10619553. URL: https://inria.hal.science/hal-04884051.

[20] B. Sterner. 'Towards Optimally Small Smoothness Bounds for Cryptographic-Sized Smooth Twins and their Isogeny-based Applications'. In: Selected Areas in Cryptography SAC 2024. Montreal (Canada), Canada, 28th Aug. 2024. URL: https://inria.hal.science/hal-04254512 (cit. on p. 13).

Conferences without proceedings

[21] A. Leroux and M. Roméas. 'Updatable Encryption from Group Actions'. In: PQC. Oxford, United Kingdom, 10th June 2024. URL: https://hal.science/hal-04389878.

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

[22] *Selected Areas in Cryptography: 29th International Conference, SAC 2022, Windsor, ON, Canada, August 24–26, 2022, Revised Selected Papers*. SAC 2022 - International Conference on Selected Areas in Cryptography. Vol. LNCS-13742. Selected Areas in Cryptography. Springer International Publishing; Springer, 2024. DOI: 10.1007/978-3-031-58411-4. URL: https://inria.hal.science/hal-04579052.

Doctoral dissertations and habilitation theses

[23] C. Ducros. 'Multiparty Computation from the Hardness of Coding Theory'. Université Paris Cité, 12th Nov. 2024. URL: https://hal.science/tel-04889558 (cit. on p. 12).

Reports & preprints

[24] V. Astore, M. Borello, M. Calderini and F. Salizzoni. *A geometric invariant of linear rank-metric codes*. 20th Jan. 2025. URL: https://hal.science/hal-04897043.

[25] M. Bonini, M. Borello and E. Byrne. *The geometry of covering codes in the sum-rank metric*. 2024. URL: https://hal.science/hal-04897367.

[26] A. Couvreur and R. Pratihar. *Decoding rank metric Reed-Muller codes*. 8th Jan. 2025. URL: https://inria.hal.science/hal-04894097 (cit. on p. 10).

[27] A. Couvreur, R. Pratihar, N. Tanısalı and I. Zappatore. *On the structure of the Schur squares of Twisted Generalized Reed-Solomon codes and application to cryptanalysis*. 19th Dec. 2024. URL: https://inria.hal.science/hal-04894232.

[28] A. Couvreur and G. Zémor. *Freiman's* $3k-4$ *Theorem for Function Fields*. 30th Sept. 2024. URL: https://inria.hal.science/hal-04894119 (cit. on p. 9).

[29] H. Delavenne, T. Medevielle and É. Roussel. *Interactive Oracle Proofs of Proximity to Codes on Graphs*. 2025. URL: https://hal.science/hal-04907297.

[30] S. R. Ghorpade, T. Johnsen, R. Ludhani and R. Pratihar. *Higher weight spectra and Betti numbers of Reed-Muller codes* $RM_q(2,2)$. 24th Jan. 2025. URL: https://hal.science/hal-04909589.

[31] S. R. Ghorpade, R. Pratihar, T. H. Randrianarisoa, H. Verdure and G. Wilson. *Homotopy type of shellable q-complexes and their homology groups*. 11th Mar. 2024. URL: https://hal.science/hal-04909598.

[32] F. Morain. *Using Fricke modular polynomials to compute isogenies*. 13th Feb. 2024. URL: https://inria.hal.science/hal-04455182 (cit. on p. 13).

[33] F. Morain. *Using modular polynomials for eta products to compute isogenies*. 29th Jan. 2024. URL: https://inria.hal.science/hal-04423470 (cit. on p. 13).

[34] R. Pratihar, T. H. Randrianarisoa and K. Stokes. *A lattice framework for generalizing shellable complexes and matroids*. 11th July 2024. URL: https://hal.science/hal-04909602.

[35] N. Willenborg, M. Borello, A.-L. Horlemann and H. Islam. *Dihedral Quantum Codes*. 16th May 2024. URL: https://hal.science/hal-04897228.

12.3 Cited publications

[36] D. Augot, A. Couvreur, J. Lavauzelle and A. Neri. 'Rank-metric codes over arbitrary Galois extensions and rank analogues of Reed-Muller codes'. In: *SIAM Journal on Applied Algebra and Geometry* 5.2 (Jan. 2021). 26 pages, 1 figure, pp. 165–199. DOI: 10.1137/20M1348583. URL: https://hal.science/hal-02882019 (cit. on p. 10).

[37] 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 (cit. on p. 12).

[38] M. Bombar, G. Couteau, A. Couvreur and C. Ducros. 'Correlated Pseudorandomness from the Hardness of Quasi-Abelian Decoding'. In: *Lecture Notes in Computer Science*. Vol. LNCS-14084. Advances in Cryptology – CRYPTO 2023. Santa Barbara, United States: Springer Nature Switzerland, Aug. 2023, pp. 567–601. DOI: 10.1007/978-3-031-38551-3_18. URL: https://hal.science/hal-04265638 (cit. on p. 12).

[39] H. Chung, D. Kim, J. H. Kim and J. Kim. 'Amortized efficient zk-SNARK from linear-only RLWE encodings'. In: *J. Comm. Netw.* (2023) (cit. on p. 11).

[40] C. Ganesh, A. Nitulescu and E. Soria-Vazquez. 'Rinocchio: SNARKs for Ring Arithmetic'. In: *J. Cryptol.* (2023) (cit. on p. 11).

[41] R. Gennaro, M. Minelli, A. Nitulescu and M. Orrù. 'Lattice-Based ZK-SNARKs from Square Span Programs'. In: *CCS*. 2018 (cit. on p. 11).

[42] Y. Ishai, H. Su and D. J. Wu. 'Shorter and Faster Post-Quantum Designated-Verifier zkSNARKs from Lattices'. In: *CCS*. 2021 (cit. on p. 11).

[43] K. Naganuma, M. Yoshino, A. Inoue, Y. Matsuoka, M. Okazaki and N. Kunihiro. 'Post-Quantum zk-SNARK for Arithmetic Circuits using QAPs'. In: *AsiaJCIS*. 2020 (cit. on p. 11).

[44] O. Regev. 'On Lattices, Learning with Errors, Random Linear Codes, and Cryptography'. In: *J. ACM* (2009) (cit. on p. 11).

[45] R. Steinfeld, A. Sakzad, M. F. Esgin and V. Kuchta. *Private Re-Randomization for Module LWE and Applications to Quasi-Optimal ZK-SNARKs*. Available at https://eprint.iacr.org/2022/1690. 2022 (cit. on p. 11).