Département
D1: Algorithms, Computation, Image & Geometry

Équipe CARAMBA

Cryptology, arithmetic : algebraic methods for better algorithms

Loria

Laboratoire lorrain de recherche en informatique et ses applications

Rapport d'activité 2025

cnrs UNIVERSITÉ DE LORRAINE

En partenariat avec

Inria CentraleSupélec

Project-Team CARAMBA

Creation of the Project-Team: 2016 September 01

Keywords

Computer sciences and digital sciences

A4.3.1. – Public key cryptography

A4.3.2. – Secret key cryptography

A4.8. – Privacy-enhancing technologies

A6.2.7. – HPC for machine learning

A7.1. – Algorithms

A7.1.4. – Quantum algorithms

A8.4. – Computer Algebra

A8.5. – Number theory

A8.10. – Computer arithmetic

Other research topics and application domains

B8.5. – Smart society

B9.5.1. – Computer science

B9.5.2. – Mathematics

B9.10. – Privacy

Contents

1 Team members, visitors, external collaborators

Research Scientists

- Emmanuel Thomé [Team leader, INRIA, Senior Researcher, HDR]
- Xavier Bonnetain [INRIA, Researcher]
- Clémence Bouvier [INRIA, Researcher]
- Pierrick Gaudry [CNRS, Senior Researcher, HDR]
- Jean Kieffer [CNRS, Researcher]
- Virginie Lallemand [CNRS, Researcher]
- Cécile Pierrot [INRIA, Researcher]
- Pierre Jean Spaenlehauer [INRIA, Researcher, HDR]
- Paul Zimmermann [INRIA, Senior Researcher, HDR]

Faculty Members

- Charles Bouillaguet [CNRS, Associate Professor, from Sep 2025, HDR]
- Camille Desenclos [UNIV PICARDIE, Associate Professor Delegation]
- Sébastien Duval [UL, Associate Professor]
- Marine Minier [UL, Professor, HDR]

PhD Students

- Marie Bolzer [CNRS]
- Gaspard Damoiseau-Malraux [UL, from Oct 2025]
- Medhi Kermaoui [INRIA]
- Hugo Nartz [UL, from Oct 2025]
- Ana Rodriguez Cordero [UL, until Jan 2025]
- Thierno Mamoudou Sabaly [CNRS]
- Thomas Sagot [INRIA, from Oct 2025]
- Julien Soumier [INRIA]

Technical Staff

- Desiree Gijon Gomez [INRIA, Engineer, from Nov 2025]
- Michael Mera [INRIA, Engineer, from Feb 2025]

Interns and Apprentices

- Leo Andre [UL, Intern, from Apr 2025 until Jun 2025]
- Diane Ducrocq [ENS PARIS-SACLAY, Intern, from Jun 2025 until Aug 2025]
- Ilan Ehrlich [INRIA, Intern, from Nov 2025]
- Baptiste Evrard [UL, Intern, from Apr 2025 until Jun 2025]
- Jocelyn Fagard [INRIA, Intern, from Apr 2025 until Oct 2025]
- Gregoire Fremion [CNRS, Intern, from Jul 2025 until Aug 2025]
- Saban Houssein [INRIA, Intern, from Apr 2025 until Jul 2025]
- Maxence Ponsardin [ENS DE LYON, Intern, from Jun 2025 until Jul 2025]
- Thomas Sagot [INRIA, Intern, from Apr 2025 until Sep 2025]
- Thibault Sanvoisin [CNRS, Intern, from Sep 2025]
- Benjamin Suel [UL, Intern, from Mar 2025 until Aug 2025]
- Charles Sutty [UL, Intern, from Oct 2025]

Administrative Assistants

- Antoinette Courrier [CNRS]
- Emmanuelle Deschamps [INRIA]
- Cecilia Olivier [INRIA]

Visiting Scientist

- Rocco Brunelli [UNIV ROME III, until Feb 2025]

2 Overall objectives

Our research addresses the broad application domain of cryptography and cryptanalysis from the algorithmic perspective. We study all the algorithmic aspects, from the top-level mathematical background down to optimized high-performance software implementations. Several kinds of mathematical objects are commonly encountered in our research. Some basic ones are truly ubiquitous: integers, finite fields, polynomials, real and complex numbers. We also work with more structured objects such as number fields, algebraic curves, or polynomial systems.

The first axis (§3.1) of our research work studies these mathematical objects mostly for their own sake. Our expertise in computational mathematics and computer algebra allows us to contribute to the general algorithmic toolbox that makes these mathematical objects easy to work with in practice: computations with these objects must be effective and fast. A sizeable portion of our work in this domain is realized in the form of software projects, which are developed over long periods of time (GNU MPFR, for example, was initiated by members of our group several decades ago, and is still maintained and developed).

A second part of our work (axes §3.2 and §3.3) is centered on cryptographic motivations. Our work in this axis is usually rooted in exactly the same core competences as the ones we use in our first research axis. We consider the two facets of cryptology: cryptography and cryptanalysis. The key challenges are the assessment of the classical and quantum security of proposed cryptographic primitives (both public- and secret-key), as well as the introduction of new cryptographic primitives, or the performance improvement of existing ones. While the basic principles of symmetric and asymmetric cryptography are rather different—indeed their names indicate different ways to handle the key—research in both domains

is led by the same objective of finding the best trade-offs between efficiency and security. In addition to this, both require to study design and analysis together as these two aspects nurture each other.

Our last research axis (§3.4) uses our cryptographic knowledge to connect to more real world concerns, in connection with topics closer to computer security. Long-term aspects of this part of our activity are practical and theoretical research on electronic voting, and practical impact on key sizes of our factoring and discrete logarithm record computations. More isolated works in this axis include for instance some works on whitebox cryptography or on Internet of Things (IoT). We also consider our growing activity on historical cryptography as part of this axis where cryptography is only one part of the study.

3 Research program

3.1 Research axis 1: mathematical objects

Several mathematical objects are pervasive in our research. We sometimes study them *per se*, but they also play a key role as tools in other research topics. In particular, we study computer arithmetic, polynomial systems, linear algebra, algebraic curves and abelian varieties.

In the context of this research axis, we work on the key algorithms and mathematical results, as well as on the realization of these results in terms of software. In our approach, software is a key step in a feedback loop that goes from mathematics to algorithms, implementation, software, and back. By software here, we mean free and open-source software tools, often developed over several years, that can be used as dependable building blocks by us as well as by peers for reproducible research.

Our past and future topics in this research axis include the following:

- We seek algorithmic and practical improvements to the most basic algorithms in computer arithmetic. This includes for example the study of advanced algorithms for integer multiplication, and their practical reach, or refinements of the implementation and accuracy of elementary functions in arbitrary precision arithmetic. Our work includes mathematical reasoning, complexity analysis, and proofs of correctness.

- We initiated work (sometimes several years or even decades ago) on several software libraries for computer arithmetic, such as GNU MPFR, GNU MPC, GF2X, GMP-ECM, or more recently the CORE-MATH project. These libraries are typical of our research output in terms of software, and our new research results are regularly implemented in such libraries (either these libraries or new ones). We sometimes contribute to other open-source libraries such as FLINT.

- We develop algorithms and software for the computation of essential attributes of algebraic curves and abelian varieties such as Riemann-Roch spaces, group structures, isogenies, and characteristic polynomials. This perspective towards effective algebra is also found in our interest in sparse polynomial systems, with a particular eye towards exploiting specificities of their monomial structure to obtain faster algorithms for the computation of Gröbner bases. These algorithms often find applications in cryptography, and are sometimes a powerful tool from the perspective of research in mathematics as well. Conversely, analyzing the complexity of those algorithms often calls for genuine mathematical work.

Examples of publications in the recent past that illustrate our positioning on this research topic are [15, 44, 52, 17, 33].

3.2 Research axis 2: secret-key cryptology

We study cryptographic and cryptanalytic aspects of secret-key primitives. We explore the following research directions in particular:

- We work on the formalization of various statistical cryptanalysis techniques, starting with boomerang attacks on which we recently gained strong expertise. We aim to properly define how to build such distinguishers and how to estimate their success probability, two central points for cryptanalysts. We intend to explore the potential of alternative techniques, such as differential-linear

attacks for instance, to attack the most recent cipher primitives (such as the NIST lightweight AEAD ciphers, as well as others at various stages of their development).

- Beyond the classical linear and differential cryptanalysis techniques, we are interested in the automation of the analysis process by the development of tools based on constraint programming (CP), satisfiability (SAT) or mixed integer linear programming (MILP) settings.
- We also study new designs, and in particular new building blocks for future cryptographic primitives with design criteria that include resistance to advanced cryptanalysis techniques, using minimal resources.
- With the current progress of quantum computing, we need to assess the security of cryptosystems against a quantum computer, especially for long-term security. Hence, we study quantum cryptanalysis. We focus on quantum algorithms that are the most distinct from classical algorithms, like the algorithms for the hidden subgroup problem, and on quantum variants of our classical cryptanalyses. This research direction is also connected to public-key cryptography.

Examples of publications in the recent past that illustrate our positioning on this research topic are [46, 47, 65, 45, 57].

3.3 Research axis 3: public-key cryptographic primitives

Our team has been studying the mathematical building blocks of public-key cryptography for a long time. More specifically, we have a long-established record on the study of the public-key cryptographic primitives based on integer factorization and finite field discrete logarithm, as well as on algebraic curves, abelian varieties, and their applications in cryptography.

The algorithmic framework of the Number Field Sieve (NFS) addresses both the integer factorization problem as well as the discrete logarithm problem over finite fields. We have numerous algorithmic contributions in this context, and develop software to illustrate them.

Several of our current research directions in public-key cryptography are strongly connected to our general expertise on NFS:

- We intend to improve the cryptanalysis techniques for various instances of the discrete logarithm problem with methods of the index calculus family. A good example of this research is our recent work on the Tower Number Field Sieve (TNFS), which touches upon algorithmic results related to number fields, Galois theory, and Euclidean lattices.
- We work on improving the practical reach of NFS as an algorithm for the factorization of RSA moduli or the computation of discrete logarithms in finite fields. We have established several computational records in this domain, and we seek further algorithmic improvements, or technological advances, that can contribute to pushing the feasibility limit further.
- None of our work on NFS would be possible without access to a dependable software implementation. To this end, we have been developing the Cado-NFS software suite since 2007. Cado-NFS is now the reference implementation of NFS, and is a crucial platform for developing prototype implementations for new ideas for the many sub-algorithms of NFS. The continuation of its development is part of our research plan.
- In the specific context of elliptic-curve cryptography, and in particular pairing-based cryptography, our expertise allows us to provide insights on the balance between implementation efficiency and security of the pairing constructions. This research is connected to the numerous application domains of pairings such as, for example, the Succinct Non-interactive ARgument of Knowledge, (zk-SNARKs). With A. Guillevic having left the group on February 2024, this theme ended.

In addition to the above, we also study other aspects of public-key cryptography, such as cryptographic constructions using isogenies between elliptic curves or more general algebraic structures, as well as their security. We have a strong record on this topic in general. The algorithmic toolbox to deal with such objects was enriched in 2022 with new practical results of Castryck-Decru, Robert, and Wesolowski. This topic is clearly in our research agenda.

As in the case of secret-key cryptology, some of our research work also takes into account quantum algorithms, and possibly the interplay of quantum and classical algorithms.

Examples of publications in the recent past that illustrate our positioning on this research topic are [4, 67], as well as the Cado-NFS software described in 6.1.2.

3.4 Research axis 4: implications in computer security and the real world

The questions that we address in this last research axis are less problem-centered than above, and rather revolve around how the different building blocks that we work with can be assembled, and whether this leads to impactful results in computer security.

In particular, we work on the following topics:

- We have been working since 2016 on electronic voting, and our most visible work in this domain is Belenios, which is a protocol with a complete specification, a free software implementation, and a free-of-charge web platform that anyone can use to set up their elections. Some desirable properties in electronic voting are very hard to obtain in practice, and we contributed to theoretical research by proposing or analysing new schemes that could be used, while providing improved guarantees with respect to some of these difficult properties such as coercion-resistance, cast-as-intended, or accountability.

- Our public key work includes improvements of NFS, and we sometimes discuss the implications of this work in computer security, which is not necessarily the same angle. A good example is the Logjam attack in 2015, where the underlying cryptanalytic task (computing discrete logarithms in 512-bit prime fields) is not exciting in itself, yet we showed that it was a key ingredient in an impactful research result. This positioning is also found in our more recent research.

- We work in collaboration with project-team CARBONE on the interactions between cryptography and malware. We study the current resilience of cryptographic secrets in environments compromised by malwares, and we propose countermeasures to protect cryptographic keys against such attackers.

- Together with project-team ALMANACH, we work in the field of historical cryptology. This project is called Back In Time, it's an interdisciplinary research effort (cryptography, computer vision and history) to build automation tools for the decryption of historical documents. Given the sheer number of pages and the variety of symbols and rules involved, our aim is to develop software to assist or even automate the deciphering of documents from ancient, medieval and modern History.

Examples of publications in the recent past that illustrate our positioning on this research topic are [51, 8, 48, 58].

4 Application domains

4.1 Better awareness and avoidance of cryptanalytic threats

Our study of the Number Field Sieve algorithm and its variants aims to show how the threats underlying various supposedly hard problems are real. Our record computations, as well as new algorithms, contribute to having a scientifically accurate assessment of the feasibility limit for these problems, given academic computing resources. The data we provide in this way is a primary ingredient for government agencies whose purpose includes guidance for choosing of appropriate cryptographic primitives. For example the French ANSSI [1], German BSI, or the NIST [2] in the United States base their recommendations on such computational achievements.

The software we make available to achieve these cryptanalytic computations also allows us to give cost estimates for potential attacks on cryptographic systems that are taking the security/efficiency/legacy

[1] In [43], the minimal recommended RSA key size is 2048 bits for usage up to 2030. See also Annex B, in particular Section B.1 "Records de calculs cryptographiques".

[2] The work [64] is one of only two academic works cited by NIST in the initial version (2011) of the report [71].

compatibility trade-offs too lightly. Attacks such as LogJam [42] are understood as being serious concerns thanks to our convincing proof-of-concepts. In the LogJam context, this impact has led to rapid worldwide security advisories and software updates that eventually defeat some potential intelligence threats and improve the confidentiality of communications.

4.2 Promotion of better cryptography

We also promote the switch to algebraic curves as cryptographic primitives. Those offer remarkable speed and excellent security, while primitives based on elementary number theory (integer factorization, discrete logarithm in finite fields), e.g., RSA, are gradually forced to adopt unwieldy key sizes to comply with the desired security guarantees of modern cryptography. Our contributions to the ultimate goal of having algebraic curves eventually take over the cryptographic landscape lie in a wide range of our research activities: contributions to fast arithmetic and to the point counting problem, expertise on the diverse surrounding mathematical objects, or on the special cases where the discrete logarithm problem is not hard enough and should be avoided.

We also promote cryptographically sound electronic voting, for which we develop the Belenios prototype software (licensed under the AGPL). It depends on research made in collaboration with the PESTO project-team, and provides stronger guarantees than the current state of the art.

4.3 Key software tools

The vast majority of our work is eventually realized as software. We can roughly categorize it into two groups: software covering fundamental objects and more specialized software.

Our software covering fundamental objects include GNU MPFR, GNU MPC, or GF2X packages. To their respective extent, these software packages are meant to be included or used in broader projects. For this reason, it is important that the license chosen for each software tool allows proper reuse, and we favor licenses such as the LGPL, which is not restrictive. We can measure the impact of each software tool by the way it is used in, e.g., the GNU Compiler Collection (GCC), Victor Shoup's Number Theory Library (NTL), or the Sage computer algebra system. The availability of these software packages in most Linux distributions is also a good measure of the impact of our work.

We also develop more specialized software, aiming at quite diverse targets. Our flagship software package is Cado-NFS [75], and we also develop some others with various levels of maturity, such as GMP-ECM or Belenios. Within the lifespan of the CARAMBA project, we expect more software packages of this kind to be developed, specialized towards tasks relevant to our research targets: important mathematical structures attached to genus 2 curves, generation of cryptographically secure curves, or tools for attacking cryptographically hard problems. Such software both illustrates our algorithms, and provides a base on which further research work can be established. Because of the very nature of these specialized software packages as research topics in their own right, needing both to borrow material from other projects, and being possible sources of inspiring material for others, it is again important that these be developed in a free and open-source development model.

5 Highlights of the year

5.1 Awards

Pierrick Gaudry, Emmanuel Thomé, and Paul Zimmermann got a Test-of-Time Award at the Crypto conference this year, for the paper about the Factorization of an RSA-768 modulus that they co-authored (with others) at Crypto 2010.

Pierrick Gaudry, Emmanuel Thomé, and Paul Zimmermann got the Levchin Prize for real-world cryptography 2025, at the Real World Crypto conference this year, for CADO-NFS and "for continued factorizations and discrete log records".

Pierrick Gaudry, together with Véronique Cortier and Alexandre Debant from the PESTO team, got the Best Paper Award at the Esorics conference for [27].

The GNU MPFR library, developed mainly by the Caramba team and the team Pascaline in Lyon, was awarded the "Prix du logiciel libre de recherche" in the category "scientifique et technique".

6 Latest software developments, platforms, open data

6.1 Latest software developments

6.1.1 Belenios

Name: Belenios - Verifiable online voting system

Keyword: E-voting

Functional Description: Belenios is an open-source online voting system that provides vote confidentiality and verifiability. End-to-end verifiability relies on the fact that the ballot box is public (voters can check that their ballots have been received) and on the fact that the tally is publicly verifiable (anyone can recount the votes). Vote confidentiality relies on the encryption of the votes and the distribution of the decryption key (no one detains the secret key).

Belenios supports various kind of elections. In the standard mode, Belenios supports simple elections where voters simply select one or more candidates. It also supports arbitrary counting functions at the cost of a slightly more complex tally procedure for the authorities. For example, Belenios supports Condorcet, STV, and Majority Judgement, where voters rank candidates and grade them.

Belenios is available in several languages for the voters as well as the administrators of an election.

Release Contributions: Belenios 3.1 mostly includes important fixes after the deployment of our new administrator interface.

It also includes some security enhancements. Some of them (missing checks from the auditors) follow remarks from Thomas Haines and Jarrod Rose. Others include use of AES-GCM instead of AES-CCM and reduced usage of SJCL.

News of the Year: In 2025, our platform was used to run about 1500 elections, with about 200,000 registered voters and 60,000 ballots counted.

Belenios 3.1 mostly includes important fixes after the deployment of our new administrator interface. It also includes some security enhancements. Some of them follow remarks from Thomas Haines and Jarrod Rose. Others (eg use of AES-GCM instead of AES-CCM, reduced usage of SJCL) have been suggested after the CSPN evaluation, unfortunately not successful for Belenios.

URL: https://www.belenios.org/

Contact: Stéphane Glondu

Participants: Pierrick Gaudry, Stéphane Glondu, Véronique Cortier

Partners: CNRS, Inria

6.1.2 CADO-NFS

Name: Crible Algébrique: Distribution, Optimisation - Number Field Sieve

Keywords: Cryptography, Number theory

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

News of the Year: In 2025, CADO-NFS included several long-overdue code base changes. Those are mostly intended to limit the divergence of the multiple code branches that we have. In particular, newly included features include having the option of enabling bucket-sieving for prime powers.

Beginning in 2025, Cado-NFS includes experimental adaptations that also support using the self-initializing quadratic sieve, in particular in the context of class group computations for quadratic fields. This development is still underway in 2026.

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

Contact: Emmanuel Thomé

Participants: Pierrick Gaudry, Emmanuel Thomé, Paul Zimmermann

6.1.3 CORE-MATH

Name: CORE-MATH

Keywords: Arithmetic code, Floating-point, Correct Rounding

Functional Description: CORE-MATH Mission: provide on-the-shelf open-source mathematical functions with correct rounding that can be integrated into current mathematical libraries (GNU libc, Intel Math Library, AMD Libm, Newlib, OpenLibm, Musl, Apple Libm, llvm-libc, CUDA libm, ROCm)

News of the Year: In 2025, several single-precision functions from CORE-MATH were integrated into the GNU libc. Also, a full set of functions was implemented for half-precision (FP16) and brain-float (BF16).

URL: https://core-math.gitlabpages.inria.fr/

Publication: hal-03721525

Contact: Paul Zimmermann

Participant: Paul Zimmermann

6.1.4 GNU MPFR

Keywords: Multiple-Precision, Floating-point, Correct Rounding

Functional Description: GNU MPFR is an efficient arbitrary-precision floating-point library with well-defined semantics (copying the good ideas from the IEEE 754 standard), in particular correct rounding in 5 rounding modes. It provides about 100 mathematical functions, in addition to utility functions (assignments, conversions...). Special data (Not a Number, infinities, signed zeros) are handled like in the IEEE 754 standard. GNU MPFR is based on the mpn and mpz layers of the GMP library.

URL: https://www.mpfr.org/

Publications: hal-01394289, hal-01502326, inria-00069930, inria-00070174, inria-00103655, inria-00000026

Contact: Vincent Lefèvre

Participants: Paul Zimmermann, Vincent Lefèvre, 2 anonymous participants

6.1.5 Riemann theta functions in FLINT

Keywords: Numerical algorithm, Number theory

Functional Description: This FLINT module, called acb_theta, allows the user to numerically evaluate Riemann theta functions in any dimension, with certified error bounds in the context of FLINT's interval arithmetic (ex-Arb). This implementation performs a lot better than other state-of-the-art software (SageMath, Magma). Moreover, the algorithm used is quasi-linear in terms of the required precision. The goal of this module is to encourage the use of numerical computations on Riemann theta functions, in particular for applications in number theory.

Release Contributions: FLINT 3.3.0 features a major rewrite of the acb_theta module with better performance (especially in higher dimensions up to 8-10), more compact code, and an enriched user interface. This also fixed a bug which caused the software to output enclosures of infinite radius in some cases was fixed. The software's performance is documented in the preprint https://hal.science/hal-05088784v2 .

News of the Year: FLINT 3.3.0, featuring a major rewrite of the acb_theta module, was released.

URL: https://github.com/flintlib/flint/

Publication: hal-05088784

Contact: Jean Kieffer

Participant: Jean Kieffer

6.1.6 rrspace

Name: Riemann-Roch spaces

Keyword: Riemann-Roch spaces

Functional Description: The C++/NTL software rrspace implements an algorithm for computing a basis of the Riemann-Roch space associated to a divisor on a curve defined over a finite field. It also implements an algorithm for computing the group law in the Jacobian of such curves. The main algorithm is a variant of Brill-Noether's approach, designed during Aude Le Gluher's Master internship in 2018.

News of the Year: State-of-the-art sub-quadratic methods have been implemented by using the PML library (https://github.com/vneiger/pml) for fast computations with polynomial matrices. The general quality of the code has been significantly improved (CI, unit tests, linting).

URL: https://gitlab.inria.fr/pspaenle/rrspace

Contact: Pierre Jean Spaenlehauer

Participant: Pierre Jean Spaenlehauer

6.2 New platforms

Participants: Paul Zimmermann, Emmanuel Thomé, Charles Bouillaguet.

In the context of the CRYPTANALYSE project of PEPR Cybersécurité, a computer cluster was acquired (to be used by all teams in the project). This cluster was installed in Fall 2024, and has been operational since December 2024. It is part of the Inria Abaca ("moyens de calcul") platform, and located in Nancy at the local datacenter (DCML, "Datacenter Mutualisé Lorrain"). The cluster comprises 16 nodes of 256 physical cores each, with 16TB total RAM and an Infiniband HDR interconnect. It was used in 2025 by members of the CRYPTANALYSE project, and also by CARAMBA (although mostly in relation with Paul Zimmermann's work on CORE-MATH, see Section 7.1.1).

7 New results

7.1 Mathematical objects

7.1.1 The CORE-MATH project

Participants: Paul Zimmermann.

The aim of the CORE-MATH project is to provide on-the-shelf open-source mathematical functions with correct rounding that will be integrated into current mathematical libraries (GNU libc, Intel Math Library, AMD Libm, Newlib, OpenLibm, Musl, Apple Libm, llvm-libc, CUDA libm, ROCm). These functions are implemented in the C language and target the three IEEE 754 binary formats (single precision, double precision, quadruple precision), and also the extended double precision (significand of 64 bits). This project is motivated by the fact that current mathematical libraries are far from giving the best possible results, as demonstrated in [35]. Together with Nicolas Brisebarre, Guillaume Hanrot and Jean-Michel Muller (AriC project and Cryptolab), we study why correctly-rounded results are important, how they can be obtained and at what cost [20].

In 2025, hard-to-round cases of the `tgamma` and `lgamma` functions were computed in double precision, which enabled an efficient implementation of these functions in CORE-MATH. The main result for 2025 was the computation of the hard-to-round cases for the trigonometric functions (sin, cos, tan) in double precision, using a new algorithm and the use of the CRYPTANALYSE cluster (see Section 6.2). This result was presented in Lyon in November at the RAIM workshop organized for the retirement of Jean-Michel Muller. This is joint work with Tue Ly (Google), and an article describing the new algorithm will be submitted to the Arith 2026 conference, with Tue Ly and Vincent Lefèvre (Pascaline team, Lyon).

Also, a complete set of C23 functions were implemented for half-precision (FP16) and "brain-float" (BF16).

New correctly-rounded single-precision functions from the CORE-MATH project have been integrated into the GNU C library, release 2.42: `acospi`, `asinpi`, `atanpi`, `cospi`, `sinpi`, `tanpi`, `atan2pi`. Seven double-precision functions should be integrated in GNU libc 2.43, which will be released end of January 2026: `acosh`, `asinh`, `atanh`, `erf`, `erfc`, `lgamma`, `tgamma`.

7.1.2 Computing isomorphisms between superspecial abelian surfaces

Participants: Pierrick Gaudry, Julien Soumier, Pierre-Jean Spaenlehauer.

Recent advances in isogeny-based post-quantum cryptography have shed light on the importance of algorithms for abelian varieties of dimension > 1 in cryptographic applications. Julien Soumier's Ph.D. focuses on the algorithmic aspects of products of supersingular elliptic curves. In particular, we propose in [34] a polynomial-time algorithm (complexity proven under the generalized Riemann hypothesis) to compute isomorphisms between such products. The existence of such isomorphisms is guaranteed by a classical theorem by Deligne, Ogus and Shioda, and our work makes this result effective.

7.1.3 Fast evaluation of Riemann theta functions

Participants: Jean Kieffer.

The Riemann theta functions are a family of complex-analytic special functions that are intimately related to the theory of abelian varieties (of any dimension g) over the complex numbers. In many algorithms, a crucial step is to numerically evaluate the Riemann theta functions at a given point; often, the result is an algebraic number that one can then try to identify exactly. This typically requires working with very high numerical precision and provably correct error bounds.

In collaboration with Noam D. Elkies, we constructed a new, fast algorithm for evaluating Riemann theta functions in any dimension g. In contrast to previous methods, it is not restricted to low dimensions such as $g \leq 2$, and allows for rigorous error bounds. This algorithm is presented in [33] along with a full complexity proof, experimental timings measured from our implementation in FLINT 3.3.0, and an application to the inverse Galois problem in number theory.

7.1.4 Point counting on abelian surfaces over finite fields

Participants: Ilan Ehrlich, Jean Kieffer.

Given a genus 2 curve over a finite field of cryptographic size, it is still a computational challenge today to compute its number of points, a necessary step for classical cryptography based on hyperelliptic curves. While the Schoof–Elkies–Atkin (SEA) algorithm, which solves the problem in the case of elliptic curves, has been known for 30 years, its generalization to genus 2 has only recently been described in Jean Kieffer's Ph.D. thesis [63] and a sizeable amount of work remains before its full implementation.

One key step in this algorithm is to compute isogenies between Jacobians of genus 2 curves from modular polynomials. The article presenting how to perform this task has been published this year [23]. Implementing this algorithm beyond toy examples remains to be done. Similarly, il will be necessary to re-implement the evaluation of modular polynomials in a clean way using our recent work on the evaluation of Riemann theta functions, as explained in [62].

Another aspect of this research is on the theoretical complexity analysis of point counting. Here, a key result is that on average, there exist sufficiently many small-degree isogenies from the Jacobian of our genus 2 curve that are defined over the base field. We proved this result in collaboration with Alexandre Benoist in 2024 when the genus 2 curves arise from the reduction of a fixed curve over a number field modulo primes. The associated article was published this year [17]. Work continues to adapt this result to another case of interest, when the genus 2 curve is drawn at random over a fixed base field.

Finally, Ilan Ehrlich's internship is also related to point counting. His work focuses on modular polynomials (in the genus 1 case) with alternative invariants, which can be much smaller than the "classical" modular polynomials that are often used in the SEA algorithm. Surprisingly, a proven explanation of this well-known phenomenon has never appeared in print to the best of our knowledge. While this work is still at a preliminary stage, pursuing similar ideas in genus 2 seems a fruitful topic for future work.

7.1.5 Isogeny classes of abelian surfaces over number fields

Participants: Hugo Nartz, Jean Kieffer, Emmanuel Thomé.

Another use for the fast algorithms to evaluate Riemann theta functions, more geared towards fundamental arithmetic geometry, is to compute isogeny classes. The situation for elliptic curves is well understood, so we consider dimension 2: we fix a number field K and a genus 2 curve C over K, and ask to compute the (finite) list of all genus 2 curves C' over K such that the Jacobians of C and C' are isogenous. Finding out which shapes of isogeny classes can appear helps our understanding of the classification of Galois representations attached to those curves, a major and difficult topic in number theory.

Hugo Nartz started his Ph.D. on this topic in October 2025, supervised by Emmanuel Thomé and Jean Kieffer. The goals will be to generalize the article [76] of Kieffer and his coauthors, which assumed simplifying hypotheses ($K = \mathbb{Q}$ and no nontrivial endomorphisms). Removing each hypothesis is a substantial challenge which will lead to new mathematical results and software implementations.

7.1.6 Formalization of Markovian Decision Processes in Lean

Participants: Pierre-Jean Spaenlehauer.

Pierre-Jean Spaenlehauer and Olivier Buffet (CR Inria, EPI LARSEN) were advisors for Jarod Galbrun's internship (ENS Lyon, L3), who worked on formalizing classical results on Markovian Decision Processes within the proof assistant Lean. Markovian Decision Processes are models which are sufficiently expressive to encode many decision-making situations, while being formalized in a mathematical language

which is convenient for formal proofs. The main contribution of Jarod Galbrun's internship is the formalization of a classical theorem which states that Markovian decision processes with finite states, finite possible actions, and finite time horizon admit an optimal solution which is deterministic (i.e., making an optimal decision does not require randomness) and Markovian (i.e., making an optimal decision only requires information about the present state and does not need any past information). The code is available on the ENS Lyon gitlab server.

7.1.7 HdR of Pierre-Jean Spaenlehauer

Participants: Pierre-Jean Spaenlehauer.

Pierre-Jean Spaenlehauer has defended his *Habilitation à Diriger des Recherches* in February 2025. The habilitation thesis [30] focuses on algorithmic interactions between arithmetic geometry and computer algebra.

7.2 Secret-key cryptology

7.2.1 A Note on the use of the Double Boomerang Connectivity Table (DBCT) for Spotting Impossibilities

Participants: Xavier Bonnetain, Virginie Lallemand.

This short note examines the impossible boomerang distinguisher on Skinny-128-384 proposed by Zhang, Wang and Tang at ToSC 2024 Issue 2 and shows that the use of the Double Boomerang Connectivity Table (DBCT) gave them an incorrect distinguisher. We discuss the limit of the DBCT in general and disprove the specific impossibility claim of Zhang and co-authors by displaying a counter-example. We conclude that the DBCT is a dangerous tool that does not capture the actual probability of a 2-round boomerang.

7.2.2 Improved Quantum Linear Attacks and Application to CAST

In [16], we show how to combine Quantum Fourier Transform-based linear attacks, that biaises a distribution of key guesses towards the correct one, and standard quantum key distinguishers, that can tell whether a key guess is correct. We apply this idea to Feistel ciphers and exemplify different attack strategies on LOKI91 before applying our idea on the CAST-128 and CAST-256 ciphers. We demonstrate the approach with two kinds of distinguishers, quantum distinguishers based on Simon's algorithm and linear distinguishers. The resulting attacks outperform the previous Grover-meet-Simon attacks.

7.2.3 A New Tool to Find Lightweight (And, Xor) Implementations of Quadratic Vectorial Boolean Functions up to Dimension 9

Participants: Marie Bolzer, Sébastien Duval, Marine Minier.

In this work [18], we build a new synthesiser, a tool that outputs an electronic circuit to implement a given function. This tool is specifically aimed at finding circuits efficient for lightweight protected implementations of cryptographic functions, minimising the number of AND gates in the circuit. It is limited to quadratic functions, but gives results far beyond the state of the art, which could only handle functions with up to 5, sometimes 6 input bits, while our tool can handle any quadratic function up to 9 bits, giving well-optimised circuits.

7.2.4 Skyscraper: Fast Hashing on Big Primes

Participants: Clémence Bouvier.

In this work [19], we present the arithmetization-oriented hash function Skyscraper, which is aimed at large prime fields and provides major improvements compared to Reinforced Concrete or Monolith. First, the design is exactly the same for all large primes, which simplifies analysis and deployment. Secondly, it achieves a performance comparable to cryptographic hash standards by using low-degree non-invertible transformations and minimizing modulo reductions. Concretely, it hashes two 256-bit prime field (BLS12-381 curve scalar field) elements in 135 nanoseconds, whereas SHA-256 needs 42 nanoseconds on the same machine.

7.2.5 Statistical properties of Butterfly-like constructions

Participants: Clémence Bouvier.

In this work [25], we present a classification of Butterfly-like constructions based on their statistical (differential and linear) properties. This work offers new perspectives on the cryptographic potential and limitations of these designs, which were originally introduced over binary fields and are now being explored over prime fields.

7.2.6 A Caribbean Directory-based Encryption during the American War of Independence

Participants: Cécile Pierrot, Gaspard Damoiseau-Malraux.

This work [29] focuses on a corpus of letters located at the Archives Nationales d'OutreMer in Aix-en-Provence, France. These late 18th-century letters come from Saint Domingue (now Haiti), a former French colony in the Caribbean Sea of which Bellecombe, the author, was governor. They were written in the context of the American War of Independence, in which France took part on the side of the Americans. We have reconstructed Bellecombe's correspondence with the Secretary of State for the Navy, in Versailles: the archives contain hundreds of letters in clear and three encrypted letters, including some clear/cipher pages that were our lever for reconstructing part of the key, and 96% of the encrypted letter that was opaque at first. From a cryptanalytical point of view, Bellecombe used a directory-based encryption. The common use of this type of cipher in the 17th and 18th-century European countries raises the question of the method to be used (then as now!) to decode such messages.

7.2.7 Decryption of an Encrypted Telegram from governor Hercílio Luz to Brazilian President Floriano Peixoto (1894)

Participants: Cécile Pierrot.

Floriano Peixoto was a Brazilian military officer and politician of the XIX° century. He was the second president of the Republic of Brazil following the abolition of the monarchy in 1889. He governed from 23 November 1891 to 15 November 1894 : the telegram we decrypted in [36] is dated 3 September 1894, so towards the end of his term of office. The sender is Hercílio Luz, governor of the Brazilian state of Santa Catarina from 1894 to 1898. The content of the message deals with the articulations of an election that took place in 1894.

7.2.8 Déchiffrement d'une lettre de François I^{er} à Christophe Richer (21 janvier 1547)

Participants: Camille Desenclos, Paul Zimmermann.

In [38], with the help of a young intern, Ioana Ionescu, we deciphered an isolated letter from François I^{er} to Christophe Richer kept in the Archives of the Ministry of Foreign Affairs, France.

7.3 Implications in computer security and the real world

7.3.1 Design of new voting protocols

Participants: Pierrick Gaudry, Léo Louistisserand.

The article [21] has been published. This work introduces our proposal of a new protocol called Vote&Check, a postal voting scheme.

In [32], together with colleagues from the PESTO team and from the Swiss Post company, we proposed a new protocol suitable for the Swiss context.

For a long time, the Federal Chancellery was accepting to trust an offline component to set up data and in particular the voting material. Today, the Chancellery aims at removing this strong trust assumption. Our proposition abides by this new will. At the heart of our system lies a setup phase where several parties create the voting material in a distributed way, while allowing one of the parties to remain offline during the voting phase. A complication arises from the fact that the voting material has to be printed, sent by postal mail, and then used by the voter to perform several operations that are critical for security. Usability constraints are taken into account in our design, both in terms of computation complexity (linear setup and tally) and in terms of user experience (we ask the voter to type a high-entropy string only once). The security of our scheme is proved in a symbolic setting, using the ProVerif prover, for various corruption scenarios, demonstrating that it fulfills the Chancellery's requirements and sometimes goes slightly beyond them.

7.3.2 Attacks on the CHVote e-voting protocol

Participants: Pierrick Gaudry.

CHVote is one of the two main electronic voting systems developed in the context of political elections in Switzerland, where the regulation requires a specific setting and specific trust assumptions. In [27], we show that actually, CHVote fails to achieve vote secrecy and individual verifiability (here, recorded-as-intended), as soon as one of the online components is dishonest, contradicting the security claims of CHVote. In total, we found 9 attacks or variants against CHVote, 2 of them being based on a bug in the reference implementation. We confirmed our findings through a proof-of-concept implementation of our attacks.

8 Bilateral contracts and grants with industry

8.1 Bilateral contracts with industry

8.1.1 Collaboration with Google on correct rounding

Participants: Paul Zimmermann.

Although this is not formalized by a contract, we maintain regular contacts (via monthly video conferences) with the LLVM/libc group (Google), in particular Tue Ly, discussing our different approaches for correct rounding of mathematical functions between CORE-MATH and LLVM/libc.

8.1.2 Training on floating-point algorithms

Participants: Paul Zimmermann.

In December, a training on floating-point algorithms was performed for engineers from AMD, at their request. The training consisted of 5 sessions (by visio conference) of 2 hours each, with 30-70 remote participants. The material is available online.

8.1.3 Consulting with Swiss Post

Participants: Pierrick Gaudry.

Together with the PESTO team, we have a long-term consulting activity with Swiss Post on the e-voting topic. In 2025 we have been working on the design of the next generation of their e-voting protocol. This is a long-term process, that involves interaction with the Federal Chancellery who coordinates the certification of the product for use in political elections. The protocol was advanced enough to be written as an academic-style preprint [32].

8.1.4 Consulting with the BSI

Participants: Pierrick Gaudry.

The Bundesamt für Sicherheit in der Informationstechnik (BSI) has issued a call for a report on the mechanisms that are used or that could be used to ensure end-to-end verifiability in electronic voting. The CNRS was a partner of the consortium that answered the call. More specifically, we participated in the analysis of the efficiency criteria, to be used for evaluating the mechanisms.

9 Partnerships and cooperations

9.1 International initiatives

Camille Desenclos and Cécile Pierrot organized a one-week research meeting at the Fondation des Treilles in November 2025. The other researchers attending were: Benjamin Kiessling (Inria Paris) and Beata Megyesi (University of Stockholm). The aim was to bring together the expertise from four different fields (history, cryptography, computer vision and computational linguistics) and lay the groundwork for a new interdisciplinary and international project.

9.2 International research visitors

9.2.1 Visits of international scientists

Other international visits to the team Luca De Feo, from IBM Research Zürich, visited the team during the 15-19 September week.

9.3 National initiatives

9.3.1 PEPR Quantique, project PQ-TLS

Participants: Xavier Bonnetain, Pierre-Jean Spaenlehauer.

- Program: PEPR Quantique
- Project acronym: PQ-TLS
- Duration: 01/2022 - 12/2028
- Coordinator: Université de Rennes 1
- Other partners: Université de Limoges, Université de Rouen, Université de Bordeaux, Université de Saint-Quentin-en Yvelines, Université de Saint-Étienne, ENS de Lyon, Inria (GRACE, CARAMBA, COSMIQ, PROSECCO), CEA (Grenoble LETI), CNRS Labstic (Lorient).

Since 1996 and the discovery of Shor's algorithm, new quantum threats emerged against classical security protocols and cryptographic primitives. The objective of the PQ-TLS project is to design a quantum-safe version of the security layer of web protocols, via the integration of post-quantum cryptographic primitives and the quantum cryptanalysis of existing systems. The project also aims at developing new techniques to compare existing primitives from the quantum viewpoint and at promoting arising solutions from academic and industrial research. The goal is to develop a large toolbox whose targets range from the mathematical foundations of post-quantum cryptography to its concrete implementations.

Xavier Bonnetain is the national coordinator of the work package 5 "Quantum cryptanalysis".

Pierre-Jean Spaenlehauer is the local scientific coordinator for the CARAMBA team.

9.3.2 PEPR Cybersécurité, project CRYPTANALYSE

Participants: Xavier Bonnetain, Clémence Bouvier, Sébastien Duval, Pierrick Gaudry, Virginie Lallemand, Marine Minier, Cécile Pierrot, Emmanuel Thomé.

- Program: PEPR Cybersécurité
- Duration: 10/2023 - 09/2028
- Coordinator: Inria
- Other partners: Inria (CARAMBA, COSMIQ, CANARI/LFANT, CAPSULE), CNRS (Loria, Irisa, IRIF, LMV, IMB, LIP6, LJK), Université de Rennes, Université de Montpellier, Université Paris Cité, Université de Picardie Jules Verne, Université de Versailles–Saint-Quentin en Yvelines, Université de Bordeaux, Université Grenoble Alpes, Sorbonne Université.

Within the context of the national PEPR program "cybersecurité" (launched in 2021), a call for proposals was published in July 2023 to complement the set of topics with three new projects, among which one on the classical cryptanalysis of cryptographic primitives. We coordinated the nationwide answer to this call for proposals, submitted in September 2022, and the project was accepted on March 27, 2023. The project started on October 1, 2023.

Emmanuel Thomé and Gaëtan Leurent (Inria COSMIQ, Paris) lead the project. Several teams are involved. The project is divided into eight work packages, and the CARAMBA team is involved in most of them.

9.3.3 Projet ANR KLEPTOMANIAC

Participants: Pierrick Gaudry, Cécile Pierrot, Pierre-Jean Spaenlehauer, Emmanuel Thomé, Paul Zimmermann.

- Program: ANR AAPG
- Project acronym: KLEPTOMANIAC
- Duration: 01/2022 - 12/2026
- Coordinator: Inria Nancy
- Other partners: ANSSI, LIP6

The RSA cryptosystem and the Diffie-Hellman key exchange protocol in finite fields were the first invented primitives of public-key cryptography.

It is hard to estimate the time and resources that are needed to factor an integer, and thereby how hard it is to break RSA. All regulatory bodies recommend that people either avoid RSA, or prefer large RSA key sizes for safety, above 2048 bits at least. In environments where computing power is plentiful, this recommendation is most often followed. Yet, it is a fact that we do rely on cryptography that uses smaller key sizes.

The goal of this project was to employ our expertise to provide solid hardness assessments for key sizes that are relevant today, and for which accuracy in the prediction is important. Our targets for accurate assessment were RSA-1024 and DH-1024 as well as specific discrete logarithm-related problems that arise in the blockchain context, together with the development of simulation software to enable more accurate estimates.

9.3.4 ANR OREO

Participants: Xavier Bonnetain, Sébastien Duval, Virginie Lallemand, Marine Minier.

- Program: ANR
- Project acronym: OREO
- Duration: 01/2023 - 12/2026
- Coordinator: Irisa (Rennes).
- Other partners: LORIA (Nancy), LMV (Versailles).

This ANR project focuses on the use of Mixed Integer Linear Programming (MILP) in symmetric-key cryptography, a direction that enjoyed rapid recognition in the symmetric-key community following the article by Mouha *et al.* [68].

MILP models can be used both to design and attack ciphers, but the technique suffers from several limitations, some of which we plan to address in this project. In particular, we aim to explore how to handle more complex cryptographic problems than what is done so far (yet ensuring a reasonable solving time). This might imply finding how to improve the modelization techniques or considering different approaches like first solving approximated models.

9.3.5 Action exploratoire Back In Time

Participants: Gaspard Damoiseau-Malraux, Camille Desenclos, Michaël Mera, Cécile Pierrot, Paul Zimmermann.

- Subject: Historical Cryptography
- Duration: October 2024 - 2026
- Coordinator: Cécile Pierrot
- Other partners: Inria Paris (ALMANACH), Université de Picardie.

BACK IN TIME brings together the expertise of researchers in three fields — artificial intelligence (ALMANACH team), cryptography (CARAMBA team) and history (Camille Desenclos) — to decipher encrypted historical documents. Given the sheer volume of data involved, our aim is to develop initial software to automate certain ancient decipherments.

9.4 Public policy support

9.4.1 Answer to CNIL consultation on e-voting

Participants: Pierrick Gaudry.

Together with members of the PESTO team, we wrote a detailed answer to the consultation organized by the CNIL on their project of updating their recommendations for the usage of electronic voting in France. This document was sent to the CNIL and also put online [37].

10 Dissemination

10.1 Promoting scientific activities

10.1.1 Scientific events: organisation

- Camille Desenclos has co-organized two workshops (journées d'études) with Pauline Ferrier-Viaud (Université d'Artois) in the context of the research project « Agir et pouvoir(s) : les marges de manœuvre des serviteurs de l'État à l'époque moderne ». The first workshop (« Définir le service : les mots des historiens » was held on May 22nd in Arras ; the second one (« Définir le service : les mots des acteurs ») took place on November 19th in Amiens.

Member of organizing committees

- Jean Kieffer acted as local organizer for the edition of the CAIPI symposium held in Nancy on April 7-8, 2025. CAIPI is a 2-day itinerant symposium on codes, cryptography, and computational arithmetic geometry whose audience consists mainly of Ph.D. students, for a total of about 40 participants. The topic for this edition was "Endomorphisms and invariants of abelian varieties".
- Virginie Lallemand was the local organizer for the C2 seminar held in Nancy on January 17, 2025.
- Pierrick Gaudry acted as local organizer, together with Alexandre Debant from the PESTO team, for the E-Vote-ID 2025 conference, in Nancy on October 2025. It gathered more than 120 participants, from acadmia, industry and governmental and regulation bodies.

10.1.2 Scientific events: selection

Chair of conference program committees

- Emmanuel Thomé was program committee chair of the Journées C2 2025, which is the yearly event of the French research community on coding theory and cryptography (more than 100 participants each year).
- Emmanuel Thomé is program committee chair of Eurocrypt 2026, which includes work that started well earlier in 2025.
- Pierrick Gaudry was track chair for the E-Vote-ID 2025 conference.

Member of conference program committees

- Xavier Bonnetain was a member of the program committee of SAC 2025 and Eurocrypt 2026 as well as the scientific committee of the Journées Codage et Cryptographie (JC2) 2026, which is the main scientific event of the GT-C2 of the CNRS GDR-IFM and GDR-SI.
- Xavier Bonnetain is a member of the scientific committee of the Loria security seminar.
- Camille Desenclos was member of the HistoCrypt2025 programme committee.
- Pierrick Gaudry was a member of the program committee of the Crypto 2025 conference, and of the artifact evaluation committee of the USENIX Security 2025 conference. He was also the technical assistant of the program committee of the ACM CCS 2025 conference.
- Marine Minier was a member of the program committee of Africacrypt 2025 and of Indocrypt 2025.
- Pierre-Jean Spaenlehauer is a member of the Scientific Committee of the Journées Nationales du Calcul Formel (JNCF), which is the main scientific event of the GT-calcul formel of the CNRS GDR-IFM.
- Emmanuel Thomé was a member of the program committee, and area chair, of Eurocrypt 2025.
- Paul Zimmermann is a member of the program committee of the PKC 2026 conference (Public Key Cryptography), whose work started in 2025.

10.1.3 Journal

Member of editorial boards

- Camille Desenclos is chief editor of the Bulletin de l'AHMUF, an online peer-reviewed journal for early modern studies.
- Xavier Bonnetain, Virginie Lallemand and Marine Minier were members of the editorial board of IACR Transactions on Symmetric Cryptology (ToSC) Journal for 2025. This journal is the open-access journal associated to the international conference on Fast Software Encryption (FSE).
- Sébastien Duval was a member of the editorial board of the Artifacts of IACR Transactions on Symmetric Cryptology (ToSC) Journal for 2025. This is a venue to publish peer-reviewed research software.
- Pierrick Gaudry was a member of the editorial board of the IACR Communication in Cryptography journal in 2025.
- Emmanuel Thomé is a member of the editorial board of Journal of Algebra.
- Camille Desenclos is a member of scientific committee of Études françaises de renseignement et de cyber, a peer-reviewed journal for intelligence studies.

Reviewer - reviewing activities Members of the project-team did their share in reviewing submissions to renowned conferences and journals. Actual publications venues are not disclosed for anonymity reasons.

10.1.4 Invited talks

- Xavier Bonnetain gave an invited talk at the IEMS-KMS International Workshop on Cryptography (South Korea).
- Xavier Bonnetain gave an invited lecture at the European Quantum Technology Summer School 2025 (Germany).
- Xavier Bonnetain gave an invited talk at the Dagstulh Seminar 25431 "Quantum Cryptanalysis" (Germany).
- Clémence Bouvier gave an invited talk at the C2 Seminar (Nancy), January 2025.
- Clémence Bouvier gave an invited lecture at the Winter School of PEPR Cybersécurité, Autrans, January 2025.
- Clémence Bouvier gave an invited talk at the ALPSY Workshop, Obergurgl, Austria, January 2025.
- Clémence Bouvier gave an invited talk at the APSIA Team seminar (Luxembourg), February 2025.
- Clémence Bouvier gave an invited lecture at the AMUSEC Workshop, CIRM, Marseille, March 2025.
- Clémence Bouvier gave an invited talk at the Grace Team seminar (Saclay), March 2025.
- Clémence Bouvier gave an invited talk at the WRACH Workshop, Roscoff, April 2025.
- Clémence Bouvier gave an invited lecture at the SAC Summer School, Toronto, Canada, August 2025.
- Clémence Bouvier gave an invited talk at the Canari Team seminar (Bordeaux), September 2025.
- Virginie Lallemand gave an invited talk at the Capsule Team seminar (Rennes), February 2025.
- Pierrick Gaudry gave an invited talk at the Collège de France, Paris, November 2025.
- Pierre-Jean Spaenlehauer gave an invited talk at the Polsys Team seminar (Paris), May 2025.
- Camille Desenclos gave an invited talk at Journées Cybersécurité et SHS (GDR Sécurité Informatique / GDR Internet, IA et Société), January 2025.
- Camille Desenclos gave an invited talk at the Archives nationales (conférence « Retour aux sources »), April 2025.
- Camille Desenclos gave an invited talk at the seminar Sciences, légitimités, médiation (IDHE.S-Paris 8), June 2025.
- Camille Desenclos gave an invited talk at the seminar Les mercredis du CRUHL (Université de Lorraine), November 2025.
- Gaspard Damoiseau-Malraux gave an invited talk for the ENACT cluster (biggest IA Cluster in Grand Est), December 2025.
- Cécile Pierrot gave an invited talk at Université Ouverte de Dole, France, April 2025.
- Cécile Pierrot gave an invited talk at University of Waterloo, Canada, May 2025.
- Cécile Pierrot and Camille Desenclos gave an invited talk at the computer science department of ENS Paris-Saclay, May 2025.

- Cécile Pierrot gave an invited talk at an online international biannual meeting for historians (Cipher Zoom), October 2025.
- Cécile Pierrot gave an invited talk at Laboratoire de Physique des Solides, Orsay University, November 2025.
- Emmanuel Thomé gave an invited talk at the WRACH Workshop, Roscoff, April 2025.

10.1.5 Leadership within the scientific community

- Pierrick Gaudry is co-head of the GdR Sécurité informatique.
- Pierrick Gaudry is a member of the steering committee of the École de Printemps d'Informatique Théorique (EPIT).
- Pierre-Jean Spaenlehauer is a member of the *bureau* of the Aathena axis (Aspects algorithmiques de la théorie des nombres et ses applications) of the *CNRS Réseau Thématique de Théorie des Nombres* (rt2n).
- Camille Desenclos is a member of the Steering Committee of the HistoCrypt international network.
- Camille Desenclos is a member of the bureau of the Association des historiens modernistes des universités françaises (AHMUF).
- Cécile Pierrot is a member of the steering committee of the Journées Code et Cryptographie.

10.1.6 Scientific expertise

- Pierrick Gaudry was a member of the selection committee for an assistant professor position in section 25 in Marseille.
- Marine Minier is a nominated member of the CNU 27 (2023-2027).
- Marine Minier was president of the selection committee for the professor position 25PR1187, Université de Lorraine and IECL.
- Cécile Pierrot was a member of the selection committee for "chargé de recherche" positions for Inria Center of Université de Lorraine.
- Paul Zimmermann was co-president of the selection committee for an assistant professor position in Telecom Nancy.

10.1.7 Research administration

- Xavier Bonnetain is the local coordinator of the Inria activity reports for the Inria Centre at Université de Lorraine (among them, this very document).
- Pierrick Gaudry is head of the Department 1 of LORIA, and, as such, member of the Scientific Council of LORIA.
- Pierrick Gaudry is a member of Comité des utilisateurs des moyens de calcul INRIA.
- Pierrick Gaudry and Marine Minier are members of the steering committee of the LHS – Laboratoire Haute Sécurité of LORIA.
- Virginie Lallemand is a member of the *commission du personnel* (COMIPERS) of the Inria research center.
- Pierre-Jean Spaenlehauer is head of the *Commission de Développement Technologique* (CDT) of the Centre Inria de l'Université de Lorraine.
- Cécile Pierrot is a member of Bureau du Comité des Projets (BCP), Inria Nancy.

- Cécile Pierrot is a member of the Comité de Centre (Loria/Inria Nancy).
- Emmanuel Thomé is a member of the *commission de recrutement des doctorants* (COMIDOC), in the LORIA context.
- Paul Zimmermann is member of the scientific committee of the EXPLOR computing center from University of Lorraine.

10.2 Teaching - Supervision - Juries - Educational and pedagogical outreach

- Bachelor
  - Sébastien Duval, *Algorithmique et Complexité*, 18h eq. TD, L2 Informatique, Université de Lorraine, Faculté des sciences et technologies, Vandœuvre-lès-Nancy, France.
  - Sébastien Duval, *Introduction à la cryptographie*, 6h eq. TD, L3 Informatique, Université de Lorraine, Faculté des sciences et technologies, Vandœuvre-lès-Nancy, France.
  - Sébastien Duval, *Introduction à la sécurité*, 20h eq. TD, L3 Informatique, Université de Lorraine, Faculté des sciences et technologies, Vandœuvre-lès-Nancy, France.
  - Marine Minier, *Introduction à la sécurité et à la cryptographie*, 35h eq. TD, L3, Université de Lorraine, Faculté des sciences et technologies, Vandœuvre-lès-Nancy, France.
  - Marine Minier, *Introduction à la cryptographie*, 15h eq. TD, L3, Université de Lorraine, Faculté des sciences et technologies, Vandœuvre-lès-Nancy, France.
- Master
  - Sébastien Duval, *Cryptographie*, 12h eq. TD, M1 Informatique, Université de Lorraine, Faculté des sciences et technologies, Vandœuvre-lès-Nancy, France.
  - Sébastien Duval, *Sécurité des Systèmes d'Information*, 64h eq. TD, M2 Informatique, Université de Lorraine, Faculté des sciences et technologies, Vandœuvre-lès-Nancy, France.
  - Sébastien Duval, *Sécurité des Applications Web*, 32h eq. TD, M2 Informatique, Université de Lorraine, Faculté des sciences et technologies, Vandœuvre-lès-Nancy, France.
  - Marine Minier, *Contrôle d'accès*, 40h eq. TD, M2 Informatique, Université de Lorraine, Faculté des sciences et technologies, Vandœuvre-lès-Nancy, France.
  - Marine Minier, *Intégration Méthodologique*, 36h eq. TD, M2 Informatique, Université de Lorraine, Faculté des sciences et technologies, Vandœuvre-lès-Nancy, France.
  - Marine Minier, *Sécurité Informatique*, 18h eq. TD, M2 droit IPIT, Université de Lorraine, France.
  - Marine Minier, *Introduction à la cryptographie*, 18h eq. TD, M1 Informatique, Université de Lorraine, Faculté des sciences et technologies, Vandœuvre-lès-Nancy, France.
  - Marine Minier is head of the M2 SIRAV, Université de Lorraine, Faculté des sciences et technologies, Vandœuvre-lès-Nancy, France.
- Engineering school
  - Xavier Bonnetain, *Algorithmique et complexité*, 30h eq. TD, 1ere année (L3), Université de Lorraine, École des Mines de Nancy, France.
  - Sébastien Duval, *Encadrement de projet de sécurité*, 20h eq. TD, 5A, Université de Lorraine, Polytech Nancy, France.
  - Jean Kieffer, *Algorithmique et complexité*, 20h eq. TD, 1ere année (L3), Université de Lorraine, École des Mines de Nancy, France.

10.2.1 Supervision

- Ph.D. in progress: Julien Soumier, *Algorithms for Isogenies of Abelian Varieties and Post-Quantum Cryptography*, since Oct. 2023, Pierre-Jean Spaenlehauer and Pierrick Gaudry.
- Ph.D. in progress: Marie Bolzer, *Algorithmique et outils automatiques pour la construction et l'analyse de composants de cryptographie symétrique*, since Oct. 2023, Sébastien Duval and Marine Minier.
- Ph.D. in progress: Thierno Sabaly, *Designs and cryptanalysis in symmetric key primitives especially block ciphers.*, since Oct. 2024, Marine Minier.
- Ph.D. in progress: Hugo Nartz, *Computing isogeny classes of abelian varieties over number fields*, Jean Kieffer and Emmanuel Thomé.
- Ph.D. in progress: Thomas Sagot, *Attack Modelling of Symmetric Primitives*, since Oct. 2025, Emmanuel Thomé, Xavier Bonnetain, Christina Boura (IRIF) and Virginie Lallemand.
- Ph.D. in progress: Léo Louistisserand, *Conception et analyse de protocoles de vote utilisés ou utilisables en pratique*, since Oct. 2023, Pierrick Gaudry and Véronique Cortier (PESTO team).
- Ph.D. in progress: Medhi Kermaoui, *Quantum cryptanalysis of public-key cryptosystems*, since Oct. 2023, Xavier Bonnetain and Pierrick Gaudry.
- Ph.D. in progress: Gaspard Damoiseau-Malraux, *Cryptanalysis of historial documents with optimisation algorithms*, since Oct. 2025, Cécile Pierrot and Charles Bouillaguet.
- Research Engineer: Michaël Mera, *Computer science Tools for the Back In Time project*, since February. 2025, Cécile Pierrot.

10.2.2 Juries

- Pierre-Jean Spaenlehauer was a reviewer for the Ph.D. thesis of Anaëlle Le Dévéhat (December 2025, Institut Polytechnique de Paris).
- Marine Minier was member of the jury for the Ph.D. thesis of Sara Majbour (July 2025, Université de Caen Normandie).
- Marine Minier was president of the Ph.D. thesis of Ala Eddine Laouir (November 2025, Université de Lorraine).
- Marine Minier was a reviewer of the Ph.D. thesis of Thomas Prévost (February 2026, Université Côte d'Azur).
- Marine Minier was Marraine of HDR and member of the jury for the HDR thesis of Abdelkader Lahmadi (March 2025, Université de Lorraine).
- Virginie Lallemand was member of the jury for the Ph.D. thesis of Phuong-Hoa Nguyen (February 2025, Université de Rennes).
- Emmanuel Thomé was a reviewer for the Ph.D. thesis of Nicolas Sarkis (July 2025, Université de Bordeaux).
- Emmanuel Thomé was a reviewer for the HDR thesis of Bruno Grenet (November 2025, Université de Grenoble Alpes).
- Pierrick Gaudry was a reviewer for the Ph.D. thesis of Jean Gasnier (July 2025, Université de Bordeaux).
- Pierrick Gaudry was president of the the Ph.D. thesis of Pierrick Dartois (July 2025, Université de Bordeaux).
- Pierrick Gaudry was president of the Ph.D. thesis of Camille Lanuel (November 2025, Université de Lorraine).

10.3 Popularization

- Emmanuel Thomé was invited to give a talk at the Sciences et Société colloquium in Nancy, in February 2025.
- Pierrick Gaudry gave a talk for the Emerites.Lorraine association, Nancy, November 2025.
- Pierrick Gaudry, together with Véronique Cortier from the PESTO team, was interviewed by a "Commission d'enquête de l'Assemblée Nationale" on the topic of electronic voting, Paris, February 2025.

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

- Camille Desenclos was interviewed by both the written press and TV media in 2025:
  - TV interview with TF1 for the midday news (February 2025),
  - TV interview with Arte for a documentary on Mary Stuart's encrypted letter ("Marie Stuart, l'énigme des lettres codées", réal. Augustin Viatte, broadcast on September 2025),
  - press conference for the latter documentary (July 2025) and interviews for Arte Magazine and Telepro.
- Cécile Pierrot wrote an article for The Conversation France, January 2025.
- Cécile Pierrot was interviewed for a short video for The Conversation France, January 2025.
- Cécile Pierrot was interviewed for TV interview with TF1 for the midday news, January 2025.

10.3.2 Participation in Live events

- Clémence Bouvier met with four classes from Charles Hermite high school for the Chiche project, Dieuze, March 2025.
- Clémence Bouvier participated in the European Women in Science Days at Féru des Sciences, Nancy, September 2025.
- Clémence Bouvier participated in the week-long event for high school girls Les Cigognes, Les Voivres, October 2025.
- Paul Zimmermann participated in the Fête de la Science in Bouxurulles, a small village in the south of Nancy, October 2025.
- Cécile Pierrot gave a talk at Château de Lunéville, France, for a large audience, June 2025.
- Cécile Pierrot and Paul Zimmermann hosted a scientific journalist for one week in their lab, as part of an exchange between media and research January 2025.

10.3.3 Others science outreach relevant activities

- Julien Soumier and Paul Zimmermann participated in the Math-En-Jeans project. They supervised a group of teenagers from the Lycée Français Vauban du Luxembourg.

11 Scientific production

11.1 Major publications

[1] X. Bonnetain, A. Chailloux, A. Schrottenloher and Y. Shen. 'Finding many Collisions via Reusable Quantum Walks: Application to Lattice Sieving'. In: *Lecture Notes in Computer Science*. EUROCRYPT 2023 - International Conference on the Theory and Applications of Cryptographic Techniques. Vol. 14008. Lecture Notes in Computer Science. Lyon, France: Springer Nature Switzerland, 16th Apr. 2023, pp. 221–251. DOI: 10.1007/978-3-031-30589-4_8. URL: https://inria.hal.science/hal-04261002.

[2] X. Bonnetain, G. Leurent, M. Naya-Plasencia and A. Schrottenloher. 'Quantum Linearization Attacks'. In: ASIACRYPT 2021 - 27th Annual International Conference on the Theory and Application of Cryptology and Information Security. Vol. 13090. Lecture Notes in Computer Science. Singapore / Virtual, Singapore: Springer International Publishing, 1st Dec. 2021, pp. 422–452. DOI: 10.1007/978-3-030-92062-3_15. URL: https://hal.inria.fr/hal-03516730.

[3] X. Bonnetain, A. Schrottenloher and F. Sibleyras. 'Beyond quadratic speedups in quantum attacks on symmetric schemes'. In: *Lecture Notes in Computer Science*. EUROCRYPT 2022 - 41st Annual International Conference on the Theory and Applications of Cryptographic Techniques. Vol. LNCS-13277. Advances in Cryptology – EUROCRYPT 2022 Part III. Trondheim, Norway: Springer International Publishing, 25th May 2022, pp. 315–344. DOI: 10.1007/978-3-031-07082-2_12. URL: https://hal.inria.fr/hal-03926591.

[4] F. Boudot, P. Gaudry, A. Guillevic, N. Heninger, E. Thomé and P. Zimmermann. 'Comparing the difficulty of factorization and discrete logarithm: a 240-digit experiment'. In: *Annual International Cryptology Conference*. Advances in Cryptology – CRYPTO 2020. Vol. 12171. Lecture Notes in Computer Science. Santa Barbara CA, United States: Springer, 10th Aug. 2020, pp. 62–91. DOI: 10.1007/978-3-030-56880-1_3. URL: https://inria.hal.science/hal-02863525.

[5] F. Boudot, P. Gaudry, A. Guillevic, N. Heninger, E. Thomé and P. Zimmermann. 'The State of the Art in Integer Factoring and Breaking Public-Key Cryptography'. In: *IEEE Security and Privacy Magazine* 20.2 (Mar. 2022), pp. 80–86. DOI: 10.1109/MSEC.2022.3141918. URL: https://hal.science/hal-03691141.

[6] H. Boukerrou, P. Huynh, V. Lallemand, B. Mandal and M. Minier. 'On the Feistel Counterpart of the Boomerang Connectivity Table: Introduction and Analysis of the FBCT'. In: *IACR Transactions on Symmetric Cryptology* 2020.1 (7th May 2020), pp. 331–362. DOI: 10.13154/tosc.v2020.i1.331-362. URL: https://inria.hal.science/hal-02945065.

[7] V. Cortier and P. Gaudry. *Le vote électronique - les défis du secret et de la transparence*. Odile Jacob, 25th May 2022. URL: https://hal.inria.fr/hal-03740465.

[8] V. Cortier, P. Gaudry and S. Glondu. 'Belenios: a simple private and verifiable electronic voting system'. In: *Foundations of Security, Protocols, and Equational Reasoning - Essays Dedicated to Catherine A. Meadows*. Vol. 11565. LNCS. Springer, 2019, pp. 214–238. DOI: 10.1007/978-3-030-19052-1_14. URL: https://inria.hal.science/hal-02066930.

[9] S. Covanov and E. Thomé. 'Fast integer multiplication using generalized Fermat primes'. In: *Mathematics of Computation* 88.317 (2019), pp. 1449–1477. DOI: 10.1090/mcom/3367. URL: https://inria.hal.science/hal-01108166.

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

[11] J. Francq, L. Besson, P. Huynh, P. Guillot, G. Millérioux and M. Minier. 'Non-triangular self-synchronizing stream ciphers'. In: *IEEE Transactions on Computers* 71.1 (Jan. 2022), pp. 134–145. DOI: 10.1109/TC.2020.3043714. URL: https://hal.science/hal-03081725.

[12] J. Fried, P. Gaudry, N. Heninger and E. Thomé. 'A kilobit hidden SNFS discrete logarithm computation'. In: *Annual International Conference on the Theory and Applications of Cryptographic Techniques*. Advances in Cryptology – EUROCRYPT 2017. Vol. 10210. Lecture Notes in Computer Science. Paris, France: Springer, 2017, pp. 202–231. DOI: 10.1007/978-3-319-56620-7_8. URL: https://inria.hal.science/hal-01376934.

[13] V. Lallemand, M. Minier and L. Rouquette. 'Automatic Search of Rectangle Attacks on Feistel Ciphers: Application to WARP'. In: *IACR Transactions on Symmetric Cryptology* 2022.2 (10th June 2022), pp. 113–140. DOI: 10.46586/tosc.v2022.i2.113-140. URL: https://hal.science/hal-03760280.

[14] G. de Micheli, P. Gaudry and C. Pierrot. 'Lattice Enumeration and Automorphisms for Tower NFS: a 521-bit Discrete Logarithm Computation'. In: *Journal of Cryptology* (2023). DOI: 10.1007/s00145-023-09487-x. URL: https://inria.hal.science/hal-04269837.

[15] A. Sibidanov, P. Zimmermann and S. Glondu. 'The CORE-MATH Project'. In: *2022 IEEE 29th Symposium on Computer Arithmetic (ARITH)*. ARITH 2022 - 29th IEEE Symposium on Computer Arithmetic. virtual, France: IEEE, 16th Dec. 2022, pp. 26–34. DOI: 10.1109/ARITH54963.2022.00014. URL: https://inria.hal.science/hal-03721525.

11.2 Publications of the year

International journals

[16] K. Bashiri, X. Bonnetain, A. Hosoyamada, N. Lang and A. Schrottenloher. 'Improved Quantum Linear Attacks and Application to CAST'. In: *IACR Transactions on Symmetric Cryptology* 2025.2 (11th June 2025), pp. 124–165. DOI: 10.46586/tosc.v2025.i2.124-165. URL: https://inria.hal.science/hal-05243650.

[17] A. Benoist and J. Kieffer. 'The asymptotic distribution of Elkies primes for reductions of abelian varieties is Gaussian'. In: *Research in Number Theory* 11.65 (2nd July 2025). DOI: 10.1007/s40993-025-00645-7. URL: https://hal.science/hal-04798225.

[18] M. Bolzer, S. Duval and M. Minier. 'A New Tool to Find Lightweight (And, Xor) Implementations of Quadratic Vectorial Boolean Functions up to Dimension 9'. In: *IEEE Transactions on Circuits and Systems I: Regular Papers* 73.1 (4th Sept. 2025), pp. 478–491. DOI: 10.1109/TCSI.2025.3602151. URL: https://hal.science/hal-05453538.

[19] C. Bouvier, L. Grassi, D. Khovratovich, K. Koschatko, C. Rechberger, F. Schmid and M. Schofnegger. 'Skyscraper: Fast Hashing on Big Primes'. In: *IACR Transactions on Cryptographic Hardware and Embedded Systems* 2025 (4th Mar. 2025), pp. 743–780. DOI: 10.46586/tches.v2025.i2.743-780. URL: https://hal.science/hal-05419160.

[20] N. Brisebarre, G. Hanrot, J.-M. Muller and P. Zimmermann. 'Correctly rounded evaluation of a function: why, how, and at what cost?' In: *ACM Computing Surveys* 58.1 (Jan. 2026). DOI: 10.1145/3747840. URL: https://hal.science/hal-04474530.

[21] V. Cortier, A. Debant, P. Gaudry and L. Louistisserand. 'Vote&Check: Secure Postal Voting with Reduced Trust Assumptions'. In: *Proceedings on Privacy Enhancing Technologies* 2025.3 (2025), pp. 333–348. DOI: 10.56553/popets-2025-0101. URL: https://inria.hal.science/hal-04813613.

[22] J. Di Mauro, H. Boukkerou, G. Millerioux, M. Minier and T. Stoll. 'Provable randomness over lightweight permutations'. In: *Cryptography and Communications - Discrete Structures, Boolean Functions and Sequences* 17 (Jan. 2025), pp. 27–40. DOI: 10.1007/s12095-024-00743-w. URL: https://hal.science/hal-04717465.

[23] J. Kieffer, A. Page and D. Robert. 'Computing isogenies from modular equations in genus two'. In: *Journal of Algebra* 666 (Mar. 2025), pp. 331–386. DOI: 10.1016/j.jalgebra.2024.11.029. URL: https://hal.science/hal-02436133.

International peer-reviewed conferences

[24] M. Amet, O. Ben Moussa, G. Bonfante and S. Duval. 'Monitoring the execution of cryptographic functions'. In: *Foundations and Practice of Security (FPS)*. FPS-2024 - 17th International Symposium on Foundations & Practice of Security. Vol. 15532. Lecture Notes in Computer Science. Montréal (Québec), Canada: Springer Nature Switzerland, 1st May 2025, pp. 377–392. DOI: 10.1007/978-3-031-87499-4_25. URL: https://hal.science/hal-04902977.

[25] C. Bouvier. 'Statistical properties of Butterfly-like constructions'. In: Fq16 - International Conference on Finite Fields and Their Applications 2025. Sao Carlos, Brazil, 7th July 2025. URL: https://inria.hal.science/hal-05419184.

[26] S. Corbineau and P. Zimmermann. 'Correct Rounding in Double Extended Precision'. In: *Proceedings of 32nd IEEE Symposium on Computer Arithmetic*. 32nd IEEE Symposium on Computer Arithmetic. El Paso, TX, United States, 4th May 2025. URL: https://inria.hal.science/hal-04861251.

[27] V. Cortier, A. Debant and P. Gaudry. 'Breaking verifiability and vote privacy in CHVote'. In: 30th European Symposium on Research in Computer Security - ESORICS 2025. Toulouse, France: Springer, 2025. URL: https://inria.hal.science/hal-04895582.

[28] C.-P. Jeannerod and P. Zimmermann. 'FastTwoSum revisited'. In: *Proceedings of 32nd IEEE Symposium on Computer Arithmetic*. 32nd IEEE Symposium on Computer Arithmetic (ARITH 2025). El Paso, TX, United States, 4th May 2025. URL: https://inria.hal.science/hal-04875749.

[29] C. Pierrot, G. Damoiseau-Malraux, P. Mekhail, O. Chaline and L. Perret. 'A Caribbean Directory-based Encryption during the American War of Independence: Bellecombe, governor of Saint-Domingue, 1782'. In: International Conference on Historical Cryptology (HistoCrypt 2025). Poznan, Poland, 17th June 2025. URL: https://hal.science/hal-05058227.

Doctoral dissertations and habilitation theses

[30] P.-J. Spaenlehauer. 'Fast Algebraic Algorithms for Arithmetic Geometry and Polynomial Systems'. Université de Lorraine, 12th Feb. 2025. URL: https://inria.hal.science/tel-04947331.

Reports & preprints

[31] X. Bonnetain, J. Loyer, A. Schrottenloher and Y. Shen. *A Tight Quantum Algorithm for Multiple Collision Search*. 2025. URL: https://hal.science/hal-05265077.

[32] V. Cortier, A. Debant, O. Esseiva, P. Gaudry, A. Hoegaasen and C. Spadafora. *A Practical and Fully Distributed E-Voting Protocol for the Swiss Context*. 17th Dec. 2025. URL: https://inria.hal.science/hal-05422264.

[33] N. D. Elkies and J. Kieffer. *Fast evaluation of Riemann theta functions in any dimension*. 28th May 2025. URL: https://hal.science/hal-05088784.

[34] P. Gaudry, J. Soumier and P.-J. Spaenlehauer. *Computing Isomorphisms between Products of Supersingular Elliptic Curves*. 27th Mar. 2025. URL: https://inria.hal.science/hal-05009640.

[35] B. Gladman, V. Innocente, J. Mather and P. Zimmermann. *Accuracy of Mathematical Functions in Single, Double, Double Extended, and Quadruple Precision*. 17th Feb. 2025. URL: https://inria.hal.science/hal-03141101.

[36] C. Pierrot. *Decryption of an Encrypted Telegram from governor Hercílio Luz to Brazilian President Floriano Peixoto (1894)*. July 2025. URL: https://hal.science/hal-05209528.

Other scientific publications

[37] V. Cortier, A. Debant, J. Dreier, P. Gaudry, L. Hirschi and S. Kremer. *Réponse au projet de mise à jour de la recommandation de la CNIL sur le vote électronique*. 2025. URL: https://inria.hal.science/hal-04971713.

[38] C. Desenclos, P. Zimmermann and I. Ionescu. *Déchiffrement d'une lettre de François Ier à Christophe Richer (21 janvier 1547)*. 19th Feb. 2025. URL: https://hal.science/hal-05149410.

11.3 Cited publications

[39] V. Cortier, P. Gaudry and Q. Yang. 'A toolbox for verifiable tally-hiding e-voting systems'. In: ESORICS 2022 - 27th European Symposium on Research in Computer Security. Copenhague, Denmark, 26th Sept. 2022. URL: https://hal.inria.fr/hal-03367930.

[40] Y. El Housni and A. Guillevic. 'Optimized and secure pairing-friendly elliptic curves suitable for one layer proof composition'. In: CANS 2020 - 19th International Conference on Cryptology and Network Security. Vienna, Austria: https://cans2020.at/, 14th Dec. 2020. URL: https://hal.inria.fr/hal-02962800.

[41] A. Guillevic. 'A short-list of pairing-friendly curves resistant to Special TNFS at the 128-bit security level'. In: PKC 2020 - IACR International Conference on Practice and Theory of Public-Key Cryptography. Vol. 12111. LNCS. Edinburgh, United Kingdom: https://pkc.iacr.org/2020/, 29th Apr. 2020, pp. 535–564. DOI: 10.1007/978-3-030-45388-6_19. URL: https://hal.inria.fr/hal-02396352.

[42] D. Adrian, K. Bhargavan, Z. Durumeric, P. Gaudry, M. Green, J. Alex Halderman, N. Heninger, D. Springall, E. Thomé, L. Valenta, B. VanderSloot, E. Wustrow, S. Zanella-Béguelin and P. Zimmermann. 'Imperfect Forward Secrecy: How Diffie-Hellman fails in practice'. In: *CCS '15: Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security*. Denver, Colorado, United States: ACM, Oct. 2015, pp. 5–17. DOI: 10.1145/2810103.2813707. URL: https://hal.inria.fr/hal-01184171.

[43] Agence nationale de la sécurité des systèmes d'information. *Référentiel général de sécurité, annexe B1*. Version 2.04. 2021. URL: https://www.ssi.gouv.fr/uploads/2021/03/anssi-guide-mecanismes_crypto-2.04.pdf.

[44] M. R. Bender and P.-J. Spaenlehauer. 'Dimension results for extremal-generic polynomial systems over complete toric varieties'. In: *Journal of Algebra* 646 (2024), pp. 156–182. DOI: 10.1016/j.jalgebra.2024.01.029. URL: https://inria.hal.science/hal-04102564.

[45] X. Bonnetain and V. Lallemand. 'On Boomerang Attacks on Quadratic Feistel Ciphers'. In: *IACR Transactions on Symmetric Cryptology* 2023.3 (Sept. 2023), pp. 101–145. DOI: 10.46586/tosc.v2023.i3.101-145. URL: https://inria.hal.science/hal-04214762.

[46] X. Bonnetain, G. Leurent, M. Naya-Plasencia and A. Schrottenloher. 'Quantum Linearization Attacks'. In: *Lecture Notes in Computer Science*. Ed. by M. Tibouchi and H. Wang. Vol. 13090. Lecture Notes in Computer Science. Singapore / Virtual, Singapore: Springer International Publishing, Dec. 2021, pp. 422–452. DOI: 10.1007/978-3-030-92062-3_15. URL: https://inria.hal.science/hal-03516730.

[47] X. Bonnetain, A. Schrottenloher and F. Sibleyras. 'Beyond quadratic speedups in quantum attacks on symmetric schemes'. In: *Lecture Notes in Computer Science*. Ed. by O. Dunkelman and S. Dziembowski. Vol. 13277. Advances in Cryptology – EUROCRYPT 2022 Part III. Colin Boyd. Trondheim, Norway: Springer International Publishing, May 2022, pp. 315–344. DOI: 10.1007/978-3-031-07082-2_12. URL: https://inria.hal.science/hal-03926591.

[48] F. Boudot, P. Gaudry, A. Guillevic, N. Heninger, E. Thomé and P. Zimmermann. 'The State of the Art in Integer Factoring and Breaking Public-Key Cryptography'. In: *IEEE Security and Privacy Magazine* 20.2 (Mar. 2022), pp. 80–86. DOI: 10.1109/MSEC.2022.3141918. URL: https://hal.science/hal-03691141.

[49] S. Bowe, A. Chiesa, M. Green, I. Miers, P. Mishra and H. Wu. 'ZEXE: Enabling Decentralized Private Computation'. In: *2020 IEEE Symposium on Security and Privacy (SP)*. Los Alamitos, CA, USA: IEEE Computer Society, May 2020, pp. 1059–1076. eprint: https://eprint.iacr.org/2018/962. URL: https://www.computer.org/csdl/proceedings-article/sp/2020/349700b059/1i0rIqoBYD6.

[50] N. Brisebarre and G. Hanrot. 'Integer points close to a transcendental curve and correctly-rounded evaluation of a function'. working paper or preprint. Nov. 2021. URL: https://hal.archives-ouvertes.fr/hal-03240179.

[51] V. Cortier and P. Gaudry. *Le vote électronique - les défis du secret et de la transparence*. Préface de Gérard Berry. Odile Jacob, May 2022. URL: https://inria.hal.science/hal-03740465.

[52] S. Covanov and E. Thomé. 'Fast integer multiplication using generalized Fermat primes'. In: *Mathematics of Computation* 88.317 (2019), pp. 1449–1477. DOI: 10.1090/mcom/3367. URL: https://inria.hal.science/hal-01108166.

[53] S. Delaune, P. Derbez and M. Vavrille. 'Catching the Fastest Boomerangs Application to SKINNY'. In: *IACR Trans. Symmetric Cryptol.* 2020.4 (2020), pp. 104–129. URL: https://doi.org/10.46586/tosc.v2020.i4.104-129.

[54] S. Delaune, P. Derbez and M. Vavrille. 'Catching the Fastest Boomerangs Application to SKINNY'. In: *IACR Trans. Symmetric Cryptol.* 2020.4 (2020), pp. 104–129. DOI: 10.46586/tosc.v2020.i4.104-129. URL: https://doi.org/10.46586/tosc.v2020.i4.104-129.

[55] J.-C. Faugère, M. Safey El Din and P.-J. Spaenlehauer. 'Gröbner Bases of Bihomogeneous Ideals generated by Polynomials of Bidegree (1, 1): Algorithms and Complexity'. In: *J. Symbolic Comput.* 46.4 (2011), pp. 406–437.

[56] J.-C. Faugère, P.-J. Spaenlehauer and J. Svartz. 'Sparse Gröbner bases: the unmixed case'. In: *ISSAC 2014*. Ed. by K. Nabeshima. Proceedings. ACM, 2014, pp. 178–185.

[57] J. Francq, L. Besson, P. Huynh, P. Guillot, G. Millérioux and M. Minier. 'Non-triangular self-synchronizing stream ciphers'. In: *IEEE Transactions on Computers* 71.1 (Jan. 2022), pp. 134–145. DOI: 10.1109/TC.2020.3043714. URL: https://hal.science/hal-03081725.

[58] J. Fried, P. Gaudry, N. Heninger and E. Thomé. 'A kilobit hidden SNFS discrete logarithm computation'. In: *Annual International Conference on the Theory and Applications of Cryptographic Techniques*. Ed. by J.-S. Coron and J. B. Nielsen. Vol. 10210. Lecture Notes in Computer Science. Paris, France: Springer, Apr. 2017, pp. 202–231. DOI: 10.1007/978-3-319-56620-7_8. URL: https://inria.hal.science/hal-01376934.

[59] J. Gasnier and A. Guillevic. 'An Algebraic Point of View on the Generation of Pairing-Friendly Curves'. working paper or preprint. Dec. 2024. URL: https://hal.science/hal-04205681.

[60] J. Groth. 'On the Size of Pairing-Based Non-interactive Arguments'. In: *Advances in Cryptology - EUROCRYPT 2016 - 35th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Vienna, Austria, May 8-12, 2016, Proceedings, Part II*. Ed. by M. Fischlin and J.-S. Coron. Vol. 9666. Lecture Notes in Computer Science. Springer, 2016, pp. 305–326. DOI: 10.1007/978-3-662-49896-5_11. URL: http://eprint.iacr.org/2016/260.

[61] G.-J. van der Heiden. 'Weil Pairing for Drinfeld Modules'. In: *Monatshefte für Mathematik* 143.2 (1st Oct. 2004), pp. 115–143. DOI: 10.1007/s00605-004-0261-4. URL: https://doi.org/10.1007/s00605-004-0261-4.

[62] J. Kieffer. *Evaluating modular equations for abelian surfaces*. 2022. URL: https://hal.science/hal-02971326.

[63] J. Kieffer. 'Higher-Dimensional Modular Equations, Applications to Isogeny Computations and Point Counting'. PhD thesis. Université de Bordeaux, 2021. URL: https://theses.hal.science/tel-03346032.

[64] T. Kleinjung, K. Aoki, J. Franke, A. K. Lenstra, E. Thomé, J. Bos, P. Gaudry, A. Kruppa, P. L. Montgomery, D. A. Osvik, H. te Riele, A. Timofeev and P. Zimmermann. 'Factorization of a 768-bit RSA modulus'. In: *CRYPTO 2010*. Ed. by T. Rabin. Vol. 6223. Lecture Notes in Comput. Sci. Proceedings. Springer–Verlag, 2010, pp. 333–350.

[65] V. Lallemand, M. Minier and L. Rouquette. 'Automatic Search of Rectangle Attacks on Feistel Ciphers: Application to WARP'. In: *IACR Transactions on Symmetric Cryptology* 2022.2 (June 2022), pp. 113–140. DOI: 10.46586/tosc.v2022.i2.113-140. URL: https://hal.science/hal-03760280.

[66] S. Maitra, B. Mandal, T. Martinsen, D. Roy and P. Stanica. 'Tools in Analyzing Linear Approximation for Boolean Functions Related to FLIP'. In: *Progress in Cryptology - INDOCRYPT 2018 - 19th International Conference on Cryptology in India, New Delhi, India, December 9-12, 2018, Proceedings*. Ed. by D. Chakraborty and T. Iwata. Vol. 11356. Lecture Notes in Computer Science. Springer, 2018, pp. 282–303. DOI: 10.1007/978-3-030-05378-9_16. URL: https://doi.org/10.1007/978-3-030-05378-9%5C_16.

[67] G. de Micheli, P. Gaudry and C. Pierrot. 'Lattice Enumeration and Automorphisms for Tower NFS: a 521-bit Discrete Logarithm Computation'. In: *Journal of Cryptology* (2023). This is the journal version of the article hal-03242324 published at Asiacrypt 2021. DOI: 10.1007/s00145-023-09487-x. URL: https://inria.hal.science/hal-04269837.

[68] N. Mouha, Q. Wang, D. Gu and B. Preneel. 'Differential and Linear Cryptanalysis Using Mixed-Integer Linear Programming'. In: *Information Security and Cryptology - 7th International Conference, Inscrypt 2011, Beijing, China, November 30 - December 3, 2011. Revised Selected Papers*. Ed. by C. Wu, M. Yung and D. Lin. Vol. 7537. Lecture Notes in Computer Science. Springer, 2011, pp. 57–76. DOI: 10.1007/978-3-642-34704-7_5. URL: https://doi.org/10.1007/978-3-642-34704-7%5C_5.

[69] Y. Musleh and É. Schost. 'Computing the Characteristic Polynomial of a Finite Rank Two Drinfeld Module'. In: *Proceedings of the 2019 on International Symposium on Symbolic and Algebraic Computation* (8th July 2019), pp. 307–314. DOI: 10.1145/3326229.3326256. URL: https://dl.acm.org/doi/10.1145/3326229.3326256.

[70] Y. Musleh and É. Schost. 'Computing the Characteristic Polynomial of Endomorphisms of a finite Drinfeld Module using Crystalline Cohomology'. In: *Proceedings of the 2023 International Symposium on Symbolic and Algebraic Computation*. ISSAC '23. New York, NY, USA: Association for Computing Machinery, 24th July 2023, pp. 461–469. DOI: 10.1145/3597066.3597080. URL: https://doi.org/10.1145/3597066.3597080.

[71] National Institute of Standards and Technology. *Transitions: Recommendation for Transitioning the Use of Cryptographic Algorithms and Key Lengths*. First revision. 2011. DOI: 10.6028/NIST.SP.800-131A.

[72] C. Pierrot, C. Desenclos, P. Gaudry and P. Zimmermann. 'Deciphering Charles Quint (A diplomatic letter from 1547)'. In: *Linköping Electronic Conference Proceedings*. Ed. by C. Dahlke and M. Göggerle. Vol. 195. Munich, Germany, June 2023, pp. 148–158. DOI: 10.3384/ecp195704. URL: https://hal.science/hal-04083014.

[73] L. Qin, X. Dong, X. Wang, K. Jia and Y. Liu. 'Automated Search Oriented to Key Recovery on Ciphers with Linear Key Schedule Applications to Boomerangs in SKINNY and ForkSkinny'. In: *IACR Trans. Symmetric Cryptol.* 2021.2 (2021), pp. 249–291. DOI: 10.46586/tosc.v2021.i2.249-291. URL: https://doi.org/10.46586/tosc.v2021.i2.249-291.

[74] E. Rescorla. *The Transport Layer Security (TLS) Protocol Version 1.3*. RFC 8446. 2018. URL: https://tools.ietf.org/html/rfc8446.

[75] The CADO-NFS Development Team. *CADO-NFS, An Implementation of the Number Field Sieve Algorithm*. Release 2.3.0. 2017. URL: https://hal.inria.fr/hal-02099620.

[76] R. van Bommel, S. Chidambaram, E. Costa and J. Kieffer. 'Computing isogeny classes of typical principally polarized abelian surfaces over the rationals'. In: *LMFDB, Computation, and Number Theory*. LuCaNT. ICERM, Providence: AMS Contemp. Math., 2024, pp. 187–214.