

2025 Activity Report

RESEARCH CENTRE: Inria Centre at the University of Bordeaux
IN PARTNERSHIP WITH: CNRS, Université de Bordeaux

Project-Team

CANARI

Cryptography ANalysis and ARithmetic

In collaboration with Institut de Mathématiques de Bordeaux (IMB)



Project-Team CANARI

Creation of the Project-Team: 2023 July 01

Each year, Inria research teams publish an Activity Report presenting their work and results over the reporting period. These reports follow a common structure, with some optional sections depending on the specific team. They typically begin by outlining the overall objectives and research programme, including the main research themes, goals, and methodological approaches. They also describe the application domains targeted by the team, highlighting the scientific or societal contexts in which their work is situated. The reports then present the highlights of the year, covering major scientific achievements, software developments, or teaching contributions. When relevant, they include sections on software, platforms, and open data, detailing the tools developed and how they are shared. A substantial part is dedicated to new results, where scientific contributions are described in detail, often with subsections specifying participants and associated keywords. Finally, the Activity Report addresses funding, contracts, partnerships, and collaborations at various levels, from industrial agreements to international cooperations. It also covers dissemination and teaching activities, such as participation in scientific events, outreach, and supervision. The document concludes with a presentation of scientific production, including major publications and those produced during the year.

Keywords

Computer sciences and digital sciences

- A4.3.1. – Public key cryptography
- A4.3.3. – Cryptographic protocols
- A4.3.4. – Quantum Cryptography
- A8.5. – Number theory
- A8.10. – Computer arithmetic

Other research topics and application domains

- B9.5.1. – Computer science
- B9.5.2. – Mathematics
- B9.8. – Reproducibility
- B9.10. – Privacy

Contents

Project-Team CANARI	1
1 Team members, visitors, external collaborators	5
2 Overall objectives	6
3 Research program	7
3.1 Algorithms for higher dimensional number theory	7
3.2 Effective analysis	7
3.3 Next generation and post-quantum cryptography	8
4 Application domains	8
5 Social and environmental responsibility	9
5.1 Footprint of research activities	9
5.2 Impact of research results	9
6 Highlights of the year	9
6.1 Awards	9
7 Latest software developments, platforms, open data	10
7.1 Latest software developments	10
7.1.1 PARI/GP	10
7.1.2 FLINT	10
7.1.3 GNU MPC	10
7.1.4 SQISignHD	11
7.1.5 SQIsign2d	11
7.1.6 ThetaIsogenies	11
7.1.7 Kummer Line	11
7.1.8 CM	11
8 New results	12
8.1 Algorithms for number theory	12
8.2 Cryptography	12
8.3 Isogeny based cryptography	13
8.4 Elliptic curves and abelian varieties	13
8.5 Lattice-based cryptography	13
8.6 Quantum algorithms for cryptanalysis	14
8.7 Code-Based Cryptography	14
8.8 Coding theory	14
8.9 Effective analysis and certified arithmetic	15
9 Partnerships and cooperations	15
9.1 International research visitors	15
9.2 European initiatives	16
9.2.1 Horizon Europe	16
9.3 National initiatives	16
10 Dissemination	17
10.1 Promoting scientific activities	17
10.1.1 Scientific events: organisation	17
10.1.2 Scientific events: selection	17
10.1.3 Journal	17
10.1.4 Invited talks	18

10.1.5 Research administration	18
10.2 Teaching - Supervision - Juries - Educational and pedagogical outreach	18
10.2.1 Supervision	19
10.2.2 Juries	20
10.2.3 Educational and pedagogical outreach	21
11 Scientific production	21
11.1 Major publications	21
11.2 Publications of the year	22
11.3 Cited publications	25

1 Team members, visitors, external collaborators

Research Scientists

- Damien Olivier Robert [Team leader, INRIA, Senior Researcher, HDR]
- Razvan Barbulescu [CNRS, Researcher]
- Xavier Caruso [CNRS, Senior Researcher, HDR]
- Andreas Enge [INRIA, Senior Researcher, HDR]
- Fredrik Johansson [INRIA, Researcher]
- Sabrina Kunzweiler [INRIA, ISFP]
- Aurel Page [INRIA, Researcher, HDR]
- Alice Pellet Mary [CNRS, Researcher]

Faculty Members

- Karim Belabas [UNIV BORDEAUX, Professor, HDR]
- Elena Berardini [CNRS, Professor]
- Maxime Bombar [UNIV BORDEAUX, Associate Professor, from Feb 2025]
- Guilhem Castagnos [UNIV BORDEAUX, Associate Professor, HDR]
- Henri Cohen [UNIV BORDEAUX, Emeritus]
- Jean-Marc Couveignes [UNIV BORDEAUX, Professor, HDR]
- Fabrice Etienne [UNIV BORDEAUX, ATER, from Sep 2025]
- Jean Gasnier [UNIV BORDEAUX, ATER, from Oct 2025]
- Olivier Ruatta [INSPE - LIMOGES, Professor Delegation, from Sep 2025]

Post-Doctoral Fellows

- Marc Houben [INRIA, Post-Doctoral Fellow]
- Wenwen Xia [UNIV BORDEAUX, Post-Doctoral Fellow, from Oct 2025]

PhD Students

- Alix Barraud [CNRS]
- Rayane Baït [UNIV BORDEAUX, from Sep 2025]
- Agathe Beaugrand [UNIV BORDEAUX, from Apr 2025 until Aug 2025]
- Agathe Beaugrand [UNIV BORDEAUX, until Mar 2025]
- Pierrick Dartois [IMT, until Aug 2025]
- Fabrice Drain [UNIV BORDEAUX]
- Fabrice Etienne [UNIV BORDEAUX, until Aug 2025]
- Jean Gasnier [UNIV BORDEAUX, until Sep 2025]

- Brieuc Lair [UNIV BORDEAUX, from Sep 2025]
- Afonso Li [UNIV BORDEAUX]
- Guilhem Mureau [INRIA]
- Leo Noel [NOKIA, CIFRE, from May 2025]
- Nicolas Sarkis [UNIV BORDEAUX, until Aug 2025]
- Alexander Wiesner [UNIV BORDEAUX, from Sep 2025]
- Anne-Edgar Wilke [UNIV BORDEAUX, until Apr 2025]

Technical Staff

- Bill Allombert [CNRS, Engineer]

Administrative Assistants

- Flavie Blondel [INRIA]
- Anne-Laure Gautier [INRIA]

Visiting Scientist

- Giacomo Spriano [ENS PARIS, from Sep 2025]

External Collaborators

- Maxime Bombar [UNIV BORDEAUX, until Feb 2025]
- Luca De Feo [IBM RESEARCH EUROPE, HDR]
- Benjamin Wesolowski [CNRS]

2 Overall objectives

The primary goals of the CANARI project are, firstly, to design algorithmic solutions to manipulate the objects involved in the Langlands programme, secondly to develop algorithmic tools to handle the necessary arithmetic and analysis (real, complex and p -adic) involved, and thirdly, to derive concrete applications, in particular to cryptography.

The Langlands programme postulates deep relationships between objects of three apparently unrelated worlds: the automorphic world, the world of Galois representations, and the motivic world.

The automorphic world belongs to the realm of analysis and infinite-dimensional vector spaces: its main citizens are automorphic forms, which are certain smooth functions satisfying nice differential equations. The number-theoretic content comes from the domains of these functions: they are defined on so-called arithmetic manifolds, of which many classical objects are special cases: modular curves, moduli spaces of abelian varieties, the space of Euclidean lattices of a given dimension, Arakelov class groups, *etc.*

The world of Galois representations is about symmetry and algebra. The main citizen is the group of all symmetries of the field of all algebraic numbers, the absolute Galois group $G_{\mathbb{Q}}$. Galois representations are linear actions of $G_{\mathbb{Q}}$ on finite-dimensional vector spaces over a field (complex numbers, p -adic numbers and finite fields are all important). They are like powerful microscopes that allow us to visualise a tiny portion of $G_{\mathbb{Q}}$ as a group of geometric symmetries.

The motivic world is about geometry. Its main citizens are algebraic varieties, that is, sets of solutions of polynomial equations, and their associated cohomologies. Important examples are algebraic curves and abelian varieties. One can classify varieties by discrete, or cohomological, invariants such as dimension and genus (integers). On some families of algebraic varieties, after fixing these discrete invariants, the family is

classified by a continuous space which is itself an algebraic variety called a moduli space. Moduli spaces of curves and abelian varieties play a key role in number theory and in cryptography.

These worlds are tied together via the central notion of L -function: generating series adapted to number theory. Each world has its own recipe to produce L -functions, and the Langlands programme asserts that the L -functions coming from the three worlds are the same; this has striking consequences as each origin then brings special properties to the other ones. A large portion of current research in number theory is placed in this context. Thus L -functions can be seen as bridges between these three worlds, and the main goal of the team is to give algorithms to construct these bridges in practice.

A strong focus on the team is on making our algorithms available through open source software, notably PARI/GP, FLINT (ARB, CALCIUM) and MPC.

3 Research program

The team is organised around three axes. The goal of the first axis is to give a systematic computational treatment of objects from the Langlands programme, and to investigate algorithmic insight that can be gained by approaching problems in computational number theory from the Langlands programme point of view.

These algorithms will be of two kinds: exact or of analytic, approximated nature (p -adic, real or complex). Hence, the second axis is concerned with the development of effective complex and p -adic analysis to handle the analytic objects that appear naturally. Finally, the new objects and computational problems will provide potential bases for next-generation cryptosystems, and the third axis uses these new insights to analyse the security of post-quantum cryptography, build new cryptosystems and improve the existing ones and study their security.

3.1 Algorithms for higher dimensional number theory

The goal of this axis is to design and implement efficient algorithms to enumerate, construct, represent, and compute with the fundamental objects of the Langlands programme and to explore their interactions. This will provide versatile tools for mathematicians to progress on difficult problems by directly manipulating intricate objects, and a collection of new problems and algorithms for cryptographers to use for the design of next-generation cryptographic primitives. Since many of these objects have a strong analytic flavour, the methods from our effective analysis axis will be vital.

The main topics of this theme will be:

- Automorphic forms: compute spaces of automorphic forms (Siegel and Hilbert modular forms, . . .)
- Galois representations: compute Artin representations using tools from representation theory, Iwasawa theory, p -adic Hodge theory.
- Varieties: abelian varieties, curves of higher genus, Shimura varieties and moduli spaces, hypergeometric motives.
- Bridges from the Langlands programme.

3.2 Effective analysis

The goal of this axis is to develop algorithms for efficient and reliable arithmetics in various fields (real, complex, p -adic, finite), which is a prerequisite for computing with the number theoretical objects of both Axis 1 and Axis 3, and especially L -functions, which are analytic objects by nature (defined in terms of series and integrals). Beyond elementary arithmetic and linear and nonlinear algebra, we also frequently need effective algorithms in the realm of complex and p -adic analysis, including algorithms for solving differential equations.

There is a wealth of research questions to address to guarantee convergence, optimal complexities and efficiency at different precisions, as well as the exactness of the results.

The main topics of this theme will be:

- Real and complex analysis: rigorous algorithms for evaluating holonomic functions. For analytic operations like limits, differentiation, summation and integration, develop algorithms with guaranteed accuracy that can handle functions with singularities or pathological behaviour like strong oscillation.
- Symbolic-numeric representations: reduce the cost of computing with algebraic numbers of large degree or height, compute with mixed algebraic and purely transcendental fields.
- p -adic analysis: optimise p -adic linear algebra and p -adic commutative algebra (including Gröbner bases) with respect to precision loss and instabilities.

3.3 Next generation and post-quantum cryptography

While the objects mentioned in Axis 1 may appear excessively abstract, when suitably instantiated, they become basic building blocks for next generation cryptosystems. First, these algebraic objects make it possible to construct quantum-resistant public key cryptosystems, which may become indispensable to secure communications in a future where large-scale quantum computers have become a reality. Second, the richness of these objects enables the construction of cryptographic schemes with advanced properties, such as homomorphic encryption, decentralised cryptography, secure multiparty computation and verifiable delay functions. The cryptosystems that will be studied in the team are related to (generalisations) of ideals and class groups in number fields: algebraic lattices, actions of class groups of orders in number fields and actions of groupoids constructed from quaternion algebras. Building and analysing these cryptosystems requires a deep understanding of the mathematical structures underlying them, which cannot simply be treated as black boxes.

The main topics of this theme will be:

- Isogenies: new cryptographic protocols from higher dimensional isogenies.
- Lattices: investigate the hardness of finding short vectors in algebraically structured lattices.
- Pairings and discrete logarithms, quantum algorithms to compute unit and class groups .
- Orders of number fields: algorithms for computing with orders in number fields, as well as regulators and class groups. These algorithms can be used to construct groups of unknown order, which find applications in advanced cryptographic primitives, for instance in the area of homomorphic encryption or threshold cryptography.
- Verifiable delay functions.

4 Application domains

Our main existing and future impact is through our software, notably PARI/GP, FLINT (ARB, CALCIUM) and MPC, which are *world leaders* in their respective domains. PARI/GP is the leading package used in number theory, and integrated into wider platforms like SAGEMATH. FLINT focus on lower level building blocks for number theory, like polynomial arithmetic, interval arithmetic (ARB) and symbolic computations (CALCIUM). MPC, with its guarantees of correct rounding for basic complex arithmetic operations, operates on a lower level and thus has a larger scope. It serves as a reference for the GNU C library and is installed alongside GCC on each computer requiring the GNU Compiler Collection. The interval arithmetic of ARB provides a more flexible use case than MPC, whence it has the widest potential of applications, far beyond the need of algorithmic number theory. It is already used in Mathematica and Maple, and a goal of the team will be to develop its reach even more.

The main impact of Axis 1, apart from the cryptographic applications, will be to give new tools to mathematicians to explore the world of the Langlands programme, construct objects explicitly and carry out experimentations, in particular via PARI/GP.

The main impact of Axis 2 will be the improvement of tools to handle precision better (floating point, p -adic, interval arithmetic), broadening the scope outside the context of pure arithmetic. The focus of Axis 2 is different from scientific computing in that we require very high precision (hundreds to tens of thousands of digits), and if possible with certified approximation bounds.

Concerning Axis 3, the requirement by governmental agencies to have post-quantum cryptographic solutions means that the civil society already needs to pivot towards such solutions. The NIST has an ongoing post-quantum cryptography standardisation process. This is an international process and the CANARI team will contribute to the analysis (and improvement) of the security of some of these schemes (notably the isogeny based ones and the ideal lattices ones).

5 Social and environmental responsibility

5.1 Footprint of research activities

The main footprint of our research activities are:

- The ecological impact of attending international conferences. We have signed the University of Bordeaux ecological chart saying that we should try to reduce travel and privilege train as much as possible. Some of us also signed a more restrictive commitment, saying that we will try to limit ourselves to 20 000km traveled by plane over a period of two years.¹
- The impact of our computations. Some of our record computations (largest class polynomials, largest primality proof) require using a large cluster for a long time. To reduce this impact we aim to develop faster algorithms.

5.2 Impact of research results

Another possible impact of Axis 3 will be ecological. Moving blockchains from Proof of Work to Proof of Stake is key to reduce their ecological impact. Verifiable delay functions are a core component of proof of stake, so Axis 3 will play a small role in helping this transition. In the same vein, cryptography based on class groups makes it possible to reduce the bandwidth used for certain multiparty protocols.

6 Highlights of the year

Highlights of 2025 include the HDR defense of Aurel Page [36] *Hecke operators in algorithmic number theory* in June 2025, and of Razvan Barbulescu [31] *Cryptanalysis of factoring and the discrete logarithms problem and their ramifications on the smooth numbers and modular curves* in July 2025; along with 6 PhDs defenses: Agathe Beaugrand, Pierrick Dartois, Fabrice Étienne, Jean Gasnier Nicolas Sarkis, Anne-Edgar Wilke [32, 34, 37, 33, 35].

Canari was part of the submission of SQISign for round 2 of NIST’s call: Post-Quantum Cryptography: Additional Digital Signature Schemes, [SQISign project](#).

There were new releases of Pari/GP (pari-2.17.3) and Flint (flint-3.4.0).

In a collaboration with Paul Underwood, A. Enge has used his CM software to establish a new record for proving a generic prime, namely the “repunit” $(10^{109297} - 1)/9$, consisting of 109297 digits 1. The computation took place over 21 months and required 220 CPU years. Details can be found in a dedicated [blog post](#).

6.1 Awards

- Guilhem Mureau got the Luca Trevisan Best Young Researcher Paper Award for his article “Special Genera of Hermitian Lattices and Applications to HAWK ” published at TCC 2025.
- Fredrik Johansson received the Applications of Computer Algebra Early Researcher Award 2025.

¹The commitment letter

7 Latest software developments, platforms, open data

7.1 Latest software developments

7.1.1 PARI/GP

Keyword: Computational number theory

Functional Description: PARI/GP is a cross platform and open-source computer algebra system designed for fast computations in number theory: factorizations, algebraic number theory, elliptic curves, modular forms, L functions... It also contains a wealth of functions to compute with mathematical entities such as matrices, polynomials, power series, algebraic numbers, etc., and a lot of transcendental functions as well as numerical summation and integration routines. PARI is also available as a C library to allow for faster computations.

URL: <http://pari.math.u-bordeaux.fr/>

Contact: Aurel Page

Participant: 5 anonymous participants

Partner: CNRS

7.1.2 FLINT

Name: Fast Library for Number Theory

Keywords: Computer algebra, Computational number theory, Arithmetic

Functional Description: FLINT is a C library for doing number theory. At its core, FLINT provides arithmetic in standard rings such as the integers, rationals, algebraic, real, complex and p-adic numbers, finite fields, and number fields. It also provides polynomials (univariate and multivariate), power series, and matrices.

FLINT covers a wide range of functionality: primality testing, integer factorisation, multivariate polynomial GCD and factorisation, FFTs, multimodular reconstruction, special functions, exact and approximate linear algebra, LLL, finite field embeddings, and more.

URL: <https://flintlib.org>

Contact: Fredrik Johansson

Partner: Technische Universität Kaiserslautern (UniKL)

7.1.3 GNU MPC

Keywords: Complex number, Floating-point

Functional Description: Mpc is a C library for the arithmetic of complex numbers with arbitrarily high precision and correct rounding of the result. It is built upon and follows the same principles as Mpfr. The library is written by Andreas Enge, Philippe Théveny and Paul Zimmermann.

Release Contributions: Changes in version 1.3.1, released in December 2022: - Bug fix: It is again possible to include mpc.h without including stdio.h.

Changes in version 1.3.0 ("Ipomoea batatas"), released in December 2022: - New function: `mpc_agm` - New rounding modes "away from zero", indicated by the letter "A" and corresponding to `MPFR_RNDA` on the designated real or imaginary part. - New experimental ball arithmetic. - New experimental function: `mpc_eta_fund` - Bug fixes: - `mpc_asin` for `asin(z)` with small $|\operatorname{Re}(z)|$ and tiny $|\operatorname{Im}(z)|$ - `mpc_pow_fr`: sign of zero part of result when the base has up to sign the same real and imaginary part, and the exponent is an even positive integer - `mpc_fma`: the returned 'int' value was incorrect in some cases (indicating whether the rounded real/imaginary parts were smaller/equal/greater than the exact

values), but the computed complex value was correct. - Remove the unmaintained Makefile.vc, build files for Visual Studio can be found at <https://github.com/BrianGladman/mpc> .

URL: <http://www.multiprecision.org/>

Contact: Andreas Enge

Participants: Andreas Enge, Mickaël Gastineau, Paul Zimmermann, Philippe Theveny

7.1.4 SQISignHD

Keyword: Cryptography

Functional Description: Compact post-quantum signature algorithm using isogenies in higher dimension.

Contact: Benjamin Wesolowski

7.1.5 SQIsign2d

Name: Compact post-quantum signature algorithm using isogenies in dimension 2

Keyword: Cryptography

Functional Description: Compact post-quantum signature algorithm using isogenies in dimension 2, improving on SQIsign and SQIsignHD

Contact: Luca De Feo

7.1.6 ThetaIsogenies

Keyword: Cryptography

Functional Description: Fast computation of $2\hat{n}$ isogenies in dimension 2.

URL: <https://github.com/ThetaIsogenies/two-isogenies>

Contact: Damien Olivier Robert

7.1.7 Kummer Line

Keyword: Cryptography

Functional Description: Library for the arithmetic of Kummer lines (arithmetic, isogenies, pairings)

URL: <https://gitlab.inria.fr/roberdam/kummer-line>

Contact: Damien Olivier Robert

7.1.8 CM

Keyword: Arithmetic

Functional Description: The Cm software implements the construction of ring class fields of imaginary quadratic number fields and of elliptic curves with complex multiplication via floating point approximations. It consists of libraries that can be called from within a C program and of executable command line applications.

Release Contributions: Version 0.4.4 "Fitzebohnen", released in July 2025, comes with the following new features: - Fix build with gcc-14. - Change parameters to increase likelihood of success for serial ecpp.

Version 0.4.3 "Fitzebohnen", released in February 2024, comes with the following new features: - Support FLINT version 3. - Add an upper bound on the permitted class number in ECPP, to avoid choosing discriminants for which class polynomials cannot be computed in reasonable time and with reasonable memory. - Add a binary ecpp-check for checking certificates.

URL: <https://www.multiprecision.org/cm/index.html>

Contact: Andreas Enge

Participant: Andreas Enge

8 New results

8.1 Algorithms for number theory

Participants: Razvan Barbulescu, Karim Belabas, Xavier Caruso, Henri Cohen, Jean-Marc Couveignes, Andreas Enge, Fabrice Etienne, Aurel Page, Alice Pellet-Mary, Sabrina Kunzweiler, Wessel van Woerden.

In [44], K. de Boer, A. Pellet-Mary and B. Wesolowski gave a provable analysis of the heuristic algorithms of Buchmann/Biasse-Song, computing units and class groups of number fields in sub-exponential time.

The article [14], S. Kunzweiler and S. Wewers, has been published in Mathematics of Computation. They present a new algorithm to compute the lattice of integral differential forms of a superelliptic curve.

In [49], F. Étienne presents an algorithm to compute the Selmer groups of a finite Galois representation, using properties of Hecke operators of finite groups.

In [11], published in Acta Crystallographica, M. Sikirić, and W. van Woerden give a complete classification of six-dimensional iso-edge domains.

In [46], H. Cohen and W. Zudilin show how modifications of Apéry's continued fractions can give interesting results including new rapidly convergent continued fractions for certain interesting constants.

X. Caruso and his collaborators studied the algebraicity of the reductions modulo primes of D -finite series. In [45], they state a general conjecture predicting the behavior of the Galois groups of $f(x) \bmod p$ when p varies. Then, in [45, 53], they gave evidences towards their conjectures by computing or estimating the relevant Galois groups for several classes of D -finite series, including Gaussian hypergeometric functions and Apéry-like sequences.

C. Armana, E. Berardini, X. Caruso, A. Leudière, J. Nardi, F. Pazuki wrote a algorithm-oriented survey on Drinfeld modules [39], covering in particular several applications to symbolic computation, cryptography and coding theory. This paper is supplemented by an implementation of Drinfeld modules and Anderson motives in SageMath, which is currently submitted for integration in a future release.

The article [10] by X. Caruso and Q. Gazda on the computation of classical and v -adic L -series of t -motives has been published in Research in Number Theory.

8.2 Cryptography

Participants: Agathe Beaugrand, Guilhem Castagnos, Ida Tucker.

In [6], A. Beaugrand, G. Castagnos and F. Laguillaumie develop efficient zero-knowledge proofs and arguments for the CL linearly homomorphic encryption scheme, addressing challenges posed by class groups of unknown order. The paper introduces batched proofs for ciphertext correctness, succinct shuffle arguments, and a new notion of partial extractability enabling Bulletproof-style techniques in the CL setting. Implementation shows that this approach is practical and enables maliciously secure applications such as an improved private set intersection sum protocol.

In [9], L. Braun, I. Damgård, F. Laguillaumie, K. Melissaris, C. Orlandi and I. Tucker improve distributed key generation and threshold decryption for the CL cryptosystem, reducing communication complexity compared to prior work. This is achieved by relaxing reconstruction requirements in verifiable secret sharing and by batching zero-knowledge proofs in unknown order groups, avoiding expensive proofs of knowledge. The resulting protocols are UC-secure with guaranteed output delivery, resilient to adaptive adversaries in the SIP model, and shown to be efficient through implementation and comparison with existing schemes.

8.3 Isogeny based cryptography

Participants: Bill Allombert, Pierrick Dartois, Sabrina Kunzweiler, Aurel Page, Damien Robert.

The paper [29], S. Kunzweiler, L. Maino T. Moriya C. Petit, G. Pope D. Robert, M. Stopar and Y.B. Ti, has been published in the proceeding of PKC 2025. The article studies cryptographic hash functions from isogeny graphs in dimension up to $g = 3$.

The paper [25], by D. Robert, written for the NuTMiC 2024 invited talk, a survey on the representation of isogenies, has been published in the LNCS proceedings.

The paper [22], by P. Dartois, J. Eriksen, B. Fouotsa, A. Herlédan Le Merdy R. Invernizzi, D. Robert, R. Rueger, F. Vercauteren, and B. Wesolowski, has been presented at CRYPTO 2025. It contains the first efficient implementation of an unrestricted class group action in the context of CSIDH, using isogenies in dimension 4.

The paper [24] by S. Galbraith, V. Gilchrist, and D. Robert has been presented at LATINCRYPT 2025. It gives new method to navigate isogeny volcanoes using self pairings and higher dimensional isogenies.

The paper [23] by P. Dartois, L. Maino, G. Pope and D. Robert, on optimised formula for 2^n -isogenies in dimension 2, presented in Asiacypt 2024, was published in the LNCS proceedings.

The paper [18] by B. Allombert, F.-F. Biasse, J. K. Eriksen, P. Kutas, C. Leonardi, A. Page, R. Scheidler, and M. Tot Bagi, was published in PKC 2025.

8.4 Elliptic curves and abelian varieties

Participants: Razvan Barbulescu, Elena Berardini, Andreas Enge, Sabrina Kunzweiler, Aurel Page, Damien Robert, Nicolas Sarkis.

The paper [13] by J. Kieffer, A. Page and D. Robert on computing isogenies from modular polynomials in dimension 2 has appeared in Journal of Algebra.

The paper [30] by D. Robert and N. Sarkis has been presented at Eurocrypt 2025. It introduces the half ladder, factoring differential isogenies and doublings through 2-isogenies (leveraging theta groups in dimension 2), which gives a speed up on the standard Montgomery ladder for Montgomery curves.

In the preprint [40], R. Barbulescu, D. Robert and N. Sarkis study different models of Kummer lines through the prism of the theta group action. This gives a unified treatment of several families previously studied in the literature, along with some new characterisation of Montgomery curves.

The paper [12] by J. Gasnier and A. Guillevic on an algebraic point of view on the generation of pairing-friendly curves has been published in the SIAM Journal on Applied Algebra and Geometry.

The paper [17] by G. Pope, K. Reijnders, D. Robert, A. Sferlazza, and B. Smith was published in the journal IACR Communications in Cryptology. It leverages the cubical arithmetic introduced by D. Robert in [52] to simplify and accelerate computing pairings for isogeny based cryptography. The paper [15] by J. Lin, D. Robert, C. Zhao, and Y. Zheng, on using the biextension arithmetic also introduced in [52] for pairing based cryptography has been published in Designs, Codes and Cryptography.

The paper [16] by A. Maïga, D. Robert, D. Sow, on computing canonical lifts of elliptic curves in medium characteristic was published in Designs, Codes and Cryptography.

In the preprint [42] E. Berardini, A. Giangreco Maidana and S. Marseglia completely characterize abelian surfaces defined over finite fields which do not contain any possibly singular curve of genus less than or equal to 3, and explicitly describe the absolutely irreducible genus 3 curves lying on abelian surfaces containing no curves of genus less than or equal to 2.

8.5 Lattice-based cryptography

Participants: Afonso Li, Guilhem Mureau, Alice Pellet-Mary, Wenwen Xia.

In [21], C. Chevignard, G. Mureau, T. Espitau, A. Pellet-Mary, H. Pliatsok and A. Wallet studied the hardness of the module lattice isomorphism problem (module-LIP), which serve as a foundation for the security of Hawk, a signature scheme submitted to the NIST competition. In this work, they reduce the problem of breaking Hawk to the problem of computing a short element of a given norm, in a given ideal of some quaternion algebra. This problem, when instantiated with number fields instead of quaternion algebras, is known to be solvable in polynomial time. The quaternion algebra case however seems much more difficult to handle, and is still the subject of research from various teams, including the canari team.

In [28], B. Allombert, A. Pellet-Mary and W. van Woerden studied the hardness of module-LIP in number fields with at least one real embedding. They showed that in this case, there exists a polynomial time (heuristic) algorithm solving the problem. This does not impact the signature scheme Hawk, which is based on cyclotomic fields, i.e., fields with no real embeddings.

In [27], C. Chevignard and G. Mureau showed that there may be exponentially many ideals in a quaternion algebra that are above a given prime ideal of a number field. This shows that a previous algorithm used to solve module-LIP in totally real number fields cannot be immediately generalized to CM fields, since the naive generalization would require enumerating all the ideals mentioned above.

The paper [26] by W. van Woerden presented in Asiacrypt 2024 on Dense and Smooth Lattices in Any Genus was published in the LNCS proceedings.

In [43], K. de Boer, A. Page, R. Toma, and B. Wesolowski study the average hardness of the Short Independent Vector Problem (SIVP) in module lattices of fixed rank. They prove a worst case to average case reduction for this problem with a polynomial loss in the approximation factor, assuming the Generalized Riemann Hypothesis. The main tools are the theory of automorphic forms and the geometry of arithmetic orbifolds, which they use to prove a new quantitative fast equidistribution theorem for random walks in the space of module lattices.

8.6 Quantum algorithms for cryptanalysis

Participants: Razvan Barbulescu.

In [19], presented at LATINCRYPT 2025, R. Barbulescu, M. Barcau and V. Pasol extend Regev's Quantum Algorithm to Elliptic Curves.

8.7 Code-Based Cryptography

Participants: Bombar Maxime.

The paper [20], M. Bombar, N. Resch, E. Wiedijk, has been published in the proceedings of ISIT 2025. The article investigates a common assumption that has been used to analyse the security of post-quantum code-based cryptosystems based on algebraically structured codes, namely quasi-cyclic codes, such as the recently standardised HQC.

8.8 Coding theory

Participants: Elena Berardini, Alix Barraud, Xavier Caruso, Jean-Marc Couveignes, Fabrice Drain, Jean Gasnier.

The paper [7] by E. Berardini and X. Caruso has been published in the Journal of Algebra and its Applications. It presents the first construction in the sum-rank metric of Reed–Muller codes.

The paper [8] by E. Berardini, R. Dastbasteh, J. Etzezarreta Martinez, S. Jain O. Sanz Larrarte was published in IEEE Journal on Selected Areas in Information Theory. In this work, the authors solve an open question on the construction of asymptotically good so-called CSS-T codes. Besides, they also propose a new technique to construct triorthogonal codes, broadening the range of codes available for magic state distillation.

In the preprint [41], A. Barraud investigates the dual of Algebraic Geometry codes constructed from Hirzebruch surfaces. She is able to explicitly describe such dual codes, and give a lower bound on their minimum distance. The knowledge of the dual of a code finds applications in many aspect of coding theory, from the conception of a decoding algorithm to the construction and study of quantum codes.

Effective geometry of curves and applications

In [47], J.-M. Couveignes and R. Lercier extend the Gauss-Cooley-Tuckee butterflies for fast evaluation and interpolation to the context of elliptic curves. They give three applications : multiplication in time $O(d \log d)$ in extensions of degree d a power of two, over a large enough finite field; MDS $[d, d/2, d/2 + 1]$ -codes that can be encoded and checked in time $O(d \log d)$ and decoded up to $d/4$ -errors in quasi-linear time in d ; an efficient variant of LWE cryptography that is not cyclotomic.

8.9 Effective analysis and certified arithmetic

Participants: Fredrik Johansson.

In [38], A. Ahlback and F. Johansson present optimized basecase algorithms for multiplication of multiprecision integers and floating-point numbers on modern CPUs.

In [50], F. Johansson describes the implementation of generic rings in FLINT. A notable result is that algebraic structures and operations built on rings with inexact representation (such as intervals) are supported in a mathematically rigorous way.

9 Partnerships and cooperations

Participants: Bill Allombert, Razvan Barbulescu, Karim Belabas, Elena Berardini, Xavier Caruso, Guilhem Castagnos, Andreas Enge, Jean-Marc Couveignes, Fredrik Johansson, Sabrina Kunzweiler, Aurel Page, Alice Pellet-Mary, Damien Robert.

9.1 International research visitors

Other international visits to the team Marzio Mula and Sebastian Spindler (Universität der Bundeswehr, München) visited the team for 3 weeks. Katherine Stange (University of Colorado, Boulder) visited the team for 3 days. Nicolas Mascot (Trinity College, Dublin, Ireland) visited the team for 1 week.

The following international speakers gave a talk at the Canari seminar in 2025: Lam Pham (Ghent University), Lorenzo Furio (Institut de Mathématiques de Jussieu-Paris Rive Gauche), Maxime Roméas (ANSSI), Marzio Mula (Universität der Bundeswehr, München), Sebastian Spindler (Universität der Bundeswehr, München), Pierre Pébureau (Sorbonne Université), Michel Seck (École Polytechnique de Thies, Sénégal), Raymond van Bommel (University of Bristol), Clémence Bouvier (CARAMBA, INRIA Nancy), Katherine Stange (University of Colorado, Boulder), Elena Kirshanova (Technology Innovation Institute, Abu Dhabi), John Voight (University of Sydney), Jonathan Komada Eriksen (KU Leuven), Ludo Pulles (CWI Amsterdam), Camille Garnier (Université de Limoges), Axel Lemoine (INRIA Paris), Jean Kieffer (CNRS and CARAMBA), Philippe Moustrou (Institut de Mathématiques de Toulouse), Hugues Randriambololona

(ANSSI), Eric Pichon-Pharabod (Max-Planck Institute for Mathematics in the Sciences, Leipzig), Victor Dyseryn (Télécom Paris).

9.2 European initiatives

9.2.1 Horizon Europe

MSCA-DN COGENT Cohomology, Geometry, and Explicit Number Theory is a European Doctoral Network, funded by the European Commission (EC) as part of the MSCA programme and by UK Research and Innovation (UKRI), whose Network coordinator is Université Grenoble Alpes (UGA).

- 5 academic beneficiaries in the EU: Université Grenoble Alpes (France), Université de Bordeaux, TU Braunschweig (Germany), University of Galway (Ireland), Vrije Universiteit Amsterdam (Netherlands).
- 2 academic beneficiaries in the UK: University of Durham, University of Sheffield.
- 7 partner organizations: Colorado State University (USA), University of Massachusetts (USA), University of Michigan (USA), University of North Carolina-Greensboro (USA), University of Oklahoma (USA), ID Quantique (IDQ, Switzerland), MSM Programming (Croatia).

2024–2028, total budget 3M€ (EU) + 900k€ (UKRI), about 280k€ for Bordeaux.

9.3 National initiatives

PEPR Technologies Quantiques Integrated project *PQ-TLS: Post-quantum padlock for web browser* with INRIA teams GRACE, COSMIQ, PROSECCO Universities of Bordeaux, Rennes, Limoges, Versailles–St. Quentin, Rouen, St. Étienne, and ENS Lyon and CEA
2022–2027, total budget 4180k€, of which 456k€ for Bordeaux

PEPR Cybersécurité Integrated project *CRYPTANALYSE: Cryptanalysis of classical cryptographic primitives* with INRIA teams CARAMBA, COSMIQ, Universities of Rennes, Amiens, Sorbonne, and CNRS
2023–2028, total budget 5000k€, of which about 90k€ for Bordeaux

HQI project (HPC-Quantum Initiative, France 2030) France Hybrid HPC Quantum Initiative, R&D et support
17 partners in France; we will mainly work with LIP6 and ENS de Lyon
2021–2027, 165k€ for Bordeaux

ANR AGDE Arithmetic and geometry of discrete groups
with Aix-Marseille, Paris
2021–2025, 45k€ for Bordeaux

ANR NuSCAP Numerical safety for computer-aided proofs
with Lyon, Nantes, Paris, Sophia-Antipolis, Toulouse
2021–2025

ANR PadLEfAn p -adic properties of L -functions effective and analytic aspects
with Besançon, Caen
2022–2026

ANR PPaL Practical p -adic Langlands
with Lille, Lyon, Paris
2026–2030, 33k€ for Bordeaux

ANR Sangria Secure distributed computation: cryptography, combinatorics and computer algebra
with Paris and région Occitanie
2021–2025

ANR TOTORO Towards new assumptions in lattice-based cryptography (PI A. Pellet--Mary)
with Toulouse and Telecom Paris
2023–2027, 186k€

10 Dissemination

Participants: Bill Allombert, Razvan Barbulescu, Karim Belabas, Elena Berardini, Xavier Caruso, Guilhem Castagnos, Andreas Enge, Jean-Marc Couveignes, Fredrik Johansson, Sabrina Kunzweiler, Aurel Page, Alice Pellet-Mary, Damien Robert.

10.1 Promoting scientific activities

10.1.1 Scientific events: organisation

Member of the organizing committees

- We helped co-organize the 25th Forum des jeunes mathématiciennes and mathématiciens in Bordeaux, from November 26th to November 28th 2025 (3 days, 60 national participants). We thank Univ. Bordeaux and CNRS for fundings for this event.
- We organized the Charm workshop in Bordeaux, from June 16th to June 20th, on the hardness of module lattices (1 week, 30 international participants).
- We co-organized two FLINT development workshops in Saclay, in January and October.
- E. Berardini co-organises the CAIPI symposium, an itinerant symposium on coding theory, cryptography, arithmetic geometry and computer algebra.
- B. Allombert and A. Page organised the Atelier Pari/GP in Institut Pascal, Saclay, from January 6th to January 10th (45 participants).
- B. Allombert and A. Page organised the Atelier libpari in Bordeaux, from June 23rd to June 27th (12 participants).

10.1.2 Scientific events: selection

Member of the conference program committees

- S. Kunzweiler was part of the program committee of Crypto 2025 and PQCrypto 2026
- M. Bombar was part of the program committee of CT-RSA 2026.
- A. Page was part of the program committee of Lucant 2025.

10.1.3 Journal

Member of the editorial boards

- K. Belabas is an editor of *Archiv der Mathematik* since 2006.
- X. Caruso is member of the scientific board for the *Journal de Théorie des Nombres de Bordeaux* since 2022.
- J.-M. Couveignes is an editor of the *Publications mathématiques de Besançon* since 2019.
- J.-M. Couveignes was an editor of the *Journal de théorie des nombres de Bordeaux* from 2019 to 2023.
- A. Enge is an editor of *Designs, Codes and Cryptography* since 2004.

- A. Page is an associate editor of the *LMFDB* since 2022.
- E. Berardini is member of the editorial board of *De Cifris Koine* and of *Journal of Combinatorial Theory, Series A*

10.1.4 Invited talks

- P. Dartois gave an invited talk ‘Theta coordinates: an introduction’ at the Leuven Isogeny Days 6.
- A. Page gave an invited talk ‘Hecke operators: introduction and applications’ at the Leuven Isogeny Days 6.
- D. Robert gave an invited talk ‘Cubical arithmetic: an introduction’ at the Leuven Isogeny Days 6.
- G. Castagnos gave an invited talk ‘Threshold Cryptography based on Class Groups of Imaginary Quadratic Fields’ at WRACH 2025 : Workshop on Randomness and Arithmetics for Cryptographic Hardware, in Roscoff and at the Journées Nationales 2025 du GDR Sécurité Informatique in Caen
- E. Berardini gave an invited talk ‘Evaluation codes in the sum-rank metric’ at the Arithmetic Geometry Cryptography and Coding Theory (AGCT) conference at CIRM

10.1.5 Research administration

- K. Belabas is ‘Vice président en charge du numérique’ (vice-president in charge of digital strategy and policies) at the University of Bordeaux since March 2022.
- X. Caruso is vice-head of *Institut de Mathématiques de Bordeaux*, in charge of the IT department.
- J.-M. Couveignes is ‘Chargé de mission pour la sécurité numérique’ at the University of Bordeaux.
- D. Robert is ‘Chargé de mission Développement logiciel’ at the Institut Mathématiques de Bordeaux since 2018.
- A. Page and A. Enge are members of the *Conseil d’Administration* of the *Société Arithmétique de Bordeaux*, which publishes the *Journal de Théorie des Nombres de Bordeaux* and provides financial support for the organisation of number theory events.
- A. Enge is an elected member of the CAP chercheurs at INRIA since 2023.
- A. Enge is a member of the Comité Parité et Égalité des Chances of INRIA since 2024.
- G. Castagnos is responsible for the master’s degree in cryptography and IT security of the University of Bordeaux since 2024.
- G. Castagnos is a member of the Conseil national des universités (CNU) section 25 Mathématiques since 2023.

10.2 Teaching - Supervision - Juries - Educational and pedagogical outreach

- S. Kunzweiler
 - Project leader at the two-week CIMPA school *Effective Algebra and the LMFDB*, Makerere University (Uganda)
 - Two lectures at the summer school *Post-quantum cryptography in Bilbao* Basque Center for Applied Mathematics in Bilbao (Spain)
 - Online lecture series on *Mathematical cryptography and algorithms in number theory* for the Preliminary Arizona Winter School (online / USA)
- K. Belabas

- 64h course on computer algebra, Master 2 (preparation for the Agrégation national competitive examination), University of Bordeaux
- 35h course on quantum algorithms, Master 2, University of Bordeaux
- X. Caruso
 - 35h course on quantum computing, Master 2, University of Bordeaux
- G. Castagnos
 - 24h course on cryptology, Master 1, University of Bordeaux
 - 36h course on advanced cryptography, Master 2, University of Bordeaux
 - 35h course on algorithmics of integers and polynomials, Bachelor, University of Bordeaux
- J.-M. Couveignes
 - 25h course on algorithmic arithmetics, Master, Université of Bordeaux
 - 160h course at CPBX (undergraduate program for student in engineering)
- A. Page
 - Main lecturer at the two-week CIMPA school *Effective Algebra and the LMFDB*, Makerere University (Uganda)
 - Two lectures at the *COGENT Winter School*, University of Galway, Ireland.
 - 33h exercise sessions on computer algebra, Master 2 (preparation for the Agrégation national competitive examination), University of Bordeaux
- A. Pellet-Mary
 - 30h course on post-quantum cryptography, Master 2, University of Bordeaux
- E. Berardini
 - 24h course on information theory, Master 1, University of Bordeaux
 - 16h course on arithmetic and cryptology, Licence 3, University of Bordeaux
- M. Bombar
 - 60h course on cryptanalysis, Master 2, University of Bordeaux
 - 15h course on advanced cryptography, Master 2, University of Bordeaux
 - 56h course on computer algebra, Master 1, University of Bordeaux
 - 36h exercise session on arithmetic and cryptology, Licence 3, University of Bordeaux

10.2.1 Supervision

- PhD defended in June 2025: Anne-Edgar Wilke, *Actions de groupes arithmétiques : théories de la réduction et algorithmes d'énumération*, since September 2019, supervised by K. Belabas.
- PhD defended in July 2025 [32]: Agathe Beaugrand, *Conception de systèmes cryptographiques utilisant des groupes de classes de corps quadratiques*, supervised by Guilhem Castagnos and Fabien Laguillaumie.
- PhD defended in July 2025 [34]: Fabrice Étienne, *Algorithmic applications of Hecke operators of finite groups for Galois representations*, since September 2022, supervised by Aurel Page.
- PhD defended in July 2025 [37]: Nicolas Sarkis, *Recherche de courbes planes de genre 2 adaptée à la factorisation des entiers*, supervised by Razvan Barbulescu and Damien Robert.

- PhD defended in July 2025 [33]: Pierrick Dartois *Improvement and security analysis of isogeny-based cryptographic schemes*, supervised by Luca De Feo, Damien Robert and Benjamin Wesolowski.
- PhD defended in July 2025 [35]: Jean Gasnier, *Algorithmique des isogénies et applications*, supervised by Jean-Marc Couveignes.
- PhD in progress: Fabrice Drain, *Codes for the sum-rank metric*, since September 2023, supervised by Elena Berardini and Xavier Caruso.
- PhD in progress: Brieuc Lair, *Deformations spaces of p -adic Galois representations*, since September 2025, supervised by Xavier Caruso and Léo Poyeton.
- PhD in progress: Guilhem Mureau, *Isomorphism of algebraic lattices*, since September 2023, supervised by Alice Pellet--Mary and Renaud Coulangeon.
- PhD in progress: Afonso Li, *On the hardness of the NTRU problem*, since October 2024, supervised by Alice Pellet--Mary and Benjamin Wesolowski.
- PhD in progress: Alix Barraud, *Algebraic geometry codes from surfaces and quantum codes*, since September 2024, supervised by Elena Berardini and Gilles Zémor.
- PhD in progress: Léo Noël, *Solutions hybrides pour permettre une transition en douceur vers la cryptographie post quantique*, since May 2025 supervised by Guilhem Castagnos
- PhD in progress: Rayane Baït, *Algorithms for Galois representations coming from Shimura curves*, since September 2025, supervised by Aurel Page and Nicolas Mascot.
- PhD in progress: Alexander Wiesner, *Algorithms for polycyclic groups associated to number fields*, since September 2025, supervised by Bill Allombert, Karim Belabas, Aurel Page and Bettina Eick.
- PhD in progress: Thibault Monneret, *Hardness of lattice problems and automorphic forms*, since September 2025, supervised by Aurel Page and Benjamin Wesolowski.

10.2.2 Juries

- X. Caruso
 - Nhuan Le, Université de Caen (Caen, France) *Sur les valeurs zêta et multizêta en caractéristique positive*
 - Epiphane Nouetowa, Université de Rennes (Rennes, France) *Codes tordus, dualité et décodage : application à la cryptographie*
 - rapporteur, Lucas Legrand, Université de Limoges (Limoges, France) *Gröbner bases over polyhedral algebras*
 - rapporteur, Nicolas Saussay, Université de Limoges (Limoges, France) *Étude de la distance minimale des codes stabilisateurs locaux*
- J.-M. Couveignes
 - rapporteur, Candice Bernard, Université de Toulouse (Toulouse, France) *Propriétés des tours récursives de courbes sur les corps finis*
 - rapporteur, Martin Azon, Université de Clermont-Auvergne (Clermont-Ferrand, France) *Arithmétique des familles de courbes hyperelliptiques*
 - Jordi Pillet, Concordia (Canada) et Université de Bourgogne (Dijon, France) *Identités de Fay, crochet de Goldman et systèmes intégrables*
 - Paul Kirchner, Université de Rennes (Rennes, France) *Cryptanalysis of public-key cryptography*
 - directeur, Jean Gasnier, Université de Bordeaux (Bordeaux, France) *Arithmétique et algorithmique des courbes algébriques et applicationx aux codes correcteurs et à la cryptographie*

- F. Johansson
 - Alexandre Goyer, Université Paris-Saclay (Saclay, France) *Algorithmes symboliques-numériques en algèbre différentielle*
- G. Castagnos
 - directeur, Agathe Beaugrand, Université de Bordeaux (Bordeaux, France) *Arguments à divulgation nulle de connaissance efficaces et succincts dans le cadre du chiffrement CL et applications*
- S. Kunzweiler
 - Pierrick Dartois, Université de Bordeaux (Talence, France) *Fast computation of higher dimensional isogenies for cryptographic applications*
 - Nicolas Sarkis, Université de Bordeaux (Talence, France) *Arithmetic of Kummer lines*
 - Valerie Gilchrist, Université Libre de Bruxelles (Bruxelles, Belgium) *Improved algorithms of post-quantum cryptographic group actions*
- A. Page
 - directeur, Fabrice Étienne, Université de Bordeaux (Talence, France) *Algorithmic applications of Hecke operators of finite groups for Galois representations*
 - Anne-Edgar Wilke, Université de Bordeaux (Talence, France) *Actions de groupes arithmétiques : théories de la réduction et algorithmes d'énumération*

10.2.3 Educational and pedagogical outreach

- A. Pellet-Mary gave a 1h30 talk about post-quantum cryptography to students of Sciences Po Lille and Centrale Lille (co-organized by Inria Lille).
- A. Enge has given a series of three presentations about cryptology during “Village des Maths” at Lycée A. Claveille in Périgeux for pupils aged 12 to 16 years.
- A. Page gave a series of four presentations about cryptology to high school students during “Fête de la Science”, Circuit Scientifique Bordelais hors les murs, at Lycée Gaston Fébus in Orthez.
- A. Enge has written the first four entries in a of “**Goblins for number theory**”, explaining in a hands-on approach how the distributed, object capabilities based framework of Guile Goblins could be used in the context of number theoretical computations that are distributed over the network, be it over TCP or Tor.

11 Scientific production

11.1 Major publications

- [1] X. Caruso, A. David and A. Mézard. ‘Can we dream of a 1-adic Langlands correspondence?’ In: *Mathematics Going Forward*. Vol. 2313. Lecture Notes in Mathematics. Springer International Publishing, 2023, pp. 537–560. DOI: [10.48550/arXiv.2204.00658](https://doi.org/10.48550/arXiv.2204.00658). URL: <https://hal.science/hal-03648316>.
- [2] X. Caruso and Q. Gazda. ‘Computation of classical and v -adic L -series of t -motives’. In: *Research in Number Theory* (2024). URL: <https://hal.science/hal-04410981>. In press.
- [3] H. Cohen. ‘Computational Number Theory, Past, Present, and Future’. In: *Mathematics Going Forward*. Vol. 2313. Lecture Notes in Mathematics. Springer International Publishing, 2023, pp. 561–578. DOI: [10.1007/978-3-031-12244-6_38](https://doi.org/10.1007/978-3-031-12244-6_38). URL: <https://inria.hal.science/hal-04223668>.

- [4] P. Dartois, A. Leroux, D. Robert and B. Wesolowski. ‘SQIsignHD: New Dimensions in Cryptography’. In: Eurocrypt 2024 - 43rd Annual International Conference on the Theory and Applications of Cryptographic Techniques. Vol. 14651. Lecture Notes in Computer Science. Zurich (CH), Switzerland: Springer Nature Switzerland, 29th Apr. 2024, pp. 3–32. doi: [10.1007/978-3-031-58716-0_1](https://doi.org/10.1007/978-3-031-58716-0_1). URL: <https://hal.science/hal-04562459>.
- [5] D. Robert, ed. *Breaking SIDH in polynomial time*. Advances in Cryptology – EUROCRYPT 2023. Vol. 14008. Lecture Notes in Computer Science. Springer Nature Switzerland; Springer Nature Switzerland, 6th Mar. 2023, pp. 472–503. doi: [10.1007/978-3-031-30589-4_17](https://doi.org/10.1007/978-3-031-30589-4_17). URL: <https://hal.science/hal-03943959>.

11.2 Publications of the year

International journals

- [6] A. Beaugrand, G. Castagnos and F. Laguillaumie. ‘Efficient Succinct Zero-Knowledge Arguments in the CL Framework’. In: *Journal of Cryptology* 38.1 (3rd Jan. 2025), p. 13. doi: [10.1007/s00145-024-09534-1](https://doi.org/10.1007/s00145-024-09534-1). URL: <https://hal.science/hal-05288358> (cit. on p. 12).
- [7] E. Berardini and X. Caruso. ‘Reed-Muller codes in the sum-rank metric’. In: *Journal of Algebra and Its Applications* (2025). URL: <https://hal.science/hal-04577005> (cit. on p. 15).
- [8] E. Berardini, R. Dastbasteh, J. E. Martinez, S. Jain and O. S. Larrarte. ‘Asymptotically good CSS-T codes and a new construction of triorthogonal codes’. In: *IEEE Journal on Selected Areas in Information Theory* 6 (2025), pp. 189–198. doi: [10.1109/JSAIT.2025.3582156](https://doi.org/10.1109/JSAIT.2025.3582156). URL: <https://hal.science/hal-04834836> (cit. on p. 15).
- [9] L. Braun, G. Castagnos, I. Damgård, F. Laguillaumie, K. Melissaris, C. Orlandi and I. Tucker. ‘An Improved Threshold Homomorphic Cryptosystem Based on Class Groups’. In: *Cryptography and Communications - Discrete Structures, Boolean Functions and Sequences* 17.5 (10th Sept. 2025), pp. 1367–1406. doi: [10.1007/s12095-025-00826-2](https://doi.org/10.1007/s12095-025-00826-2). URL: <https://hal.science/hal-05288379> (cit. on p. 12).
- [10] X. Caruso and Q. Gazda. ‘Computation of classical and v -adic L -series of t -motives’. In: *Research in Number Theory* (Feb. 2025), <https://doi.org/10.1007/s40993-024-00588-5>. doi: [10.1007/s40993-024-00588-5](https://doi.org/10.1007/s40993-024-00588-5). URL: <https://hal.science/hal-04410981> (cit. on p. 12).
- [11] M. Dutour Sikirić and W. van Woerden. ‘Complete classification of six-dimensional iso-edge domains’. In: *Acta Crystallographica Section A : Foundations and Advances [2014-...]* 81.1 (1st Jan. 2025), pp. 9–15. doi: [10.1107/S2053273324010143](https://doi.org/10.1107/S2053273324010143). URL: <https://hal.science/hal-04905930> (cit. on p. 12).
- [12] J. Gasnier and A. Guillevic. ‘An Algebraic Point of View on the Generation of Pairing-Friendly Curves’. In: *SIAM Journal on Applied Algebra and Geometry* 9.2 (27th June 2025), pp. 456–480. doi: [10.1137/23M1601961](https://doi.org/10.1137/23M1601961). URL: <https://hal.science/hal-04205681> (cit. on p. 13).
- [13] 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](https://doi.org/10.1016/j.jalgebra.2024.11.029). URL: <https://hal.science/hal-02436133> (cit. on p. 13).
- [14] S. Kunzweiler and S. Wewers. ‘Integral differential forms for superelliptic curves’. In: *Mathematics of Computation* (24th June 2025). doi: [10.1090/mcom/4115](https://doi.org/10.1090/mcom/4115). URL: <https://hal.science/hal-05329838> (cit. on p. 12).
- [15] J. Lin, D. Robert, C.-A. Zhao and Y. Zheng. ‘Biextensions in pairing-based cryptography’. In: *Designs, Codes and Cryptography* 94.1 (15th Dec. 2025), p. 5. doi: [10.1007/s10623-025-01762-1](https://doi.org/10.1007/s10623-025-01762-1). URL: <https://inria.hal.science/hal-05468414> (cit. on p. 13).
- [16] A. Maïga, D. Robert and D. Sow. ‘Towards computing canonical lifts of ordinary elliptic curves in medium characteristic’. In: *Designs, Codes and Cryptography* 93.12 (1st Dec. 2025), pp. 5231–5255. doi: [10.1007/s10623-025-01719-4](https://doi.org/10.1007/s10623-025-01719-4). URL: <https://hal.science/hal-03702658> (cit. on p. 13).

- [17] G. Pope, K. Reijnders, D. Robert, A. Sferlazza and B. Smith. ‘Simpler and Faster Pairings from the Montgomery Ladder’. In: *IACR Communications in Cryptology 2025.2* (7th July 2025). DOI: [10.62056/ah2i893y6](https://doi.org/10.62056/ah2i893y6). URL: <https://inria.hal.science/hal-05142445> (cit. on p. 13).

International peer-reviewed conferences

- [18] B. Allombert, J.-F. Biasse, J. K. Eriksen, P. Kutas, C. Leonardi, A. Page, R. Scheidler and M. Tot Bagi. ‘Faster SCALLOP from Non-Prime Conductor Suborders in Medium Sized Quadratic Fields’. In: *Lecture Notes in Computer Science. Public-Key Cryptography - PKC 2025*. Vol. 15676. Lecture Notes in Computer Science. Røros, Norway: Springer Nature Switzerland, 5th May 2025, pp. 333–363. DOI: [10.1007/978-3-031-91826-1_11](https://doi.org/10.1007/978-3-031-91826-1_11). URL: <https://inria.hal.science/hal-04755827> (cit. on p. 13).
- [19] R. Barbulescu, M. Barcau and V. Pasol. ‘Extending Regev’s Quantum Algorithm to Elliptic Curves’. In: *Progress in Cryptology–LATINCRYPT, Lecture notes in computer science. 9th International Conference on Cryptology and Information Security in Latin America–LATINCRYPT 2025*. Vol. 16129. Lecture notes in computer science. Medellín, Colombia: Springer, 1st Dec. 2025, p. 234. DOI: [10.1007/978-3-540-68164-9_26](https://doi.org/10.1007/978-3-540-68164-9_26). URL: <https://hal.science/hal-04833072> (cit. on p. 14).
- [20] M. Bombar, N. Resch and E. Wiedijk. ‘On the Independence Assumption in Quasi-Cyclic Code-Based Cryptography’. In: *ISIT 2025 - IEEE International Symposium on Information Theory*. Ann Arbor, United States: IEEE, 22nd June 2025, pp. 1–6. DOI: [10.1109/ISIT63088.2025.11195347](https://doi.org/10.1109/ISIT63088.2025.11195347). URL: <https://inria.hal.science/hal-05466410> (cit. on p. 14).
- [21] C. Cheignard, G. Mureau, T. Espitau, A. Pellet-Mary, H. Pliatsok and A. Wallet. ‘A reduction from Hawk to the principal ideal problem in a quaternion algebra’. In: *Eurocrypt 2025 - 44th Annual International Conference on the Theory and Applications of Cryptographic Techniques. Lecture Notes in Computer Science*. Madrid, Spain, 5th May 2025. DOI: [10.1007/978-3-031-91124-8_6](https://doi.org/10.1007/978-3-031-91124-8_6). URL: <https://hal.science/hal-05233972> (cit. on p. 14).
- [22] P. Dartois, J. K. Eriksen, T. B. Fouotsa, A. Herlédan Le Merdy, R. Invernizzi, D. Robert, R. Rueger, F. Vercauteren and B. Wesolowski. ‘PEGASIS: Practical Effective Class Group Action using 4-Dimensional Isogenies’. In: *Advances in Cryptology – CRYPTO 2025*. CRYPTO 2025. Vol. 16000. Lecture Notes in Computer Science. Santa Barbara, United States: Springer Nature Switzerland, 17th Aug. 2025, pp. 67–99. DOI: [10.1007/978-3-032-01855-7_3](https://doi.org/10.1007/978-3-032-01855-7_3). URL: <https://hal.science/hal-04987747> (cit. on p. 13).
- [23] P. Dartois, L. Maino, G. Pope and D. Robert. ‘An Algorithmic Approach to (2, 2)-isogenies in the Theta Model and Applications to Isogeny-based Cryptography’. In: *Advances in Cryptology – ASIACRYPT 2024*. Vol. 15486. Lecture Notes in Computer Science. Kolkata, India: Springer Nature Singapore; Springer Nature Singapore, 12th Dec. 2025, pp. 304–338. DOI: [10.1007/978-981-96-0891-1_10](https://doi.org/10.1007/978-981-96-0891-1_10). URL: <https://hal.science/hal-04297088> (cit. on p. 13).
- [24] S. Galbraith, V. Gilchrist and D. Robert. ‘Improved Algorithms for Ascending Isogeny Volcanoes, and Applications’. In: *Lecture Notes in Computer Science. Latincrypt 2025 - International Conference on Cryptology and Information Security in Latin America*. Vol. 16129. Lecture Notes in Computer Science. Medellín, Colombia, 2nd Oct. 2025, pp. 174–208. DOI: [10.1007/978-3-032-06754-8_7](https://doi.org/10.1007/978-3-032-06754-8_7). URL: <https://inria.hal.science/hal-05466427> (cit. on p. 13).
- [25] D. Robert. ‘On the efficient representation of isogenies: A survey for NuTMiC 2024’. In: *Lecture Notes in Computer Science. NUTMIC 2024 - Number-Theoretic Methods in Cryptology*. Vol. 14966. Lecture Notes in Computer Science. Szczecin, Poland: Springer Nature Switzerland, 19th Feb. 2025, pp. 3–84. DOI: [10.1007/978-3-031-82380-0_1](https://doi.org/10.1007/978-3-031-82380-0_1). URL: <https://hal.science/hal-04848010> (cit. on p. 13).
- [26] W. van Woerden. ‘Dense and Smooth Lattices in Any Genus’. In: *Asiacrypt 2024*. Vol. 15487. Lecture Notes in Computer Science. Kolkata, India: Springer Nature Singapore, 13th Dec. 2025, pp. 386–417. DOI: [10.1007/978-981-96-0894-2_13](https://doi.org/10.1007/978-981-96-0894-2_13). URL: <https://hal.science/hal-04905912> (cit. on p. 14).

Conferences without proceedings

- [27] C. Chevignard and G. Mureau. ‘Ideally HAWKward: How Not to Break Module-LIP’. In: CFAIL 2025 - Conference for Failed Approaches and Insightful Losses in Cryptology (an affiliated workshop to Crypto 2025). Santa Barbara (CA), United States, 2025, pp. 1–7. URL: <https://hal.science/hal-05235811> (cit. on p. 14).

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

- [28] *Cryptanalysis of Rank-2 Module-LIP: A Single Real Embedding Is All It Takes*. Eurocrypt 2025. Vol. 15602. Lecture Notes in Computer Science. Madrid, Spain: Springer Nature Switzerland, 28th Apr. 2025, pp. 184–212. DOI: [10.1007/978-3-031-91124-8_7](https://doi.org/10.1007/978-3-031-91124-8_7). URL: <https://hal.science/hal-05233960> (cit. on p. 14).
- [29] *Radical 2-isogenies and cryptographic hash functions in dimensions 1, 2 and 3*. Public-Key Cryptography – PKC 2025. Vol. 15676. Lecture Notes in Computer Science. Røros, Norway: Springer Nature Switzerland, 5th May 2025, pp. 265–299. DOI: [10.1007/978-3-031-91826-1_9](https://doi.org/10.1007/978-3-031-91826-1_9). URL: <https://hal.science/hal-04837057> (cit. on p. 13).
- [30] *Halving differential additions on Kummer lines*. EUROCRYPT 2025. Vol. 15606. Lecture Notes in Computer Science VI. Madrid, Spain: Springer Nature, 28th Apr. 2025, pp. 416–445. DOI: [10.1007/978-3-031-91095-1_15](https://doi.org/10.1007/978-3-031-91095-1_15). URL: <https://hal.science/hal-04724019> (cit. on p. 13).

Doctoral dissertations and habilitation theses

- [31] R. Barbulescu. ‘Cryptanalysis of factoring and the discrete logarithm problem and their ramifications on the smooth numbers and modular curves’. Université de Bordeaux, 8th July 2025. URL: <https://theses.hal.science/tel-05169987> (cit. on p. 9).
- [32] A. Beaugrand. ‘Efficient and succinct zero-knowledge proofs in the CL encryption framework and applications’. Université de Bordeaux, 8th July 2025. URL: <https://theses.hal.science/tel-05316233> (cit. on pp. 9, 19).
- [33] P. Dartois. ‘Fast computation of higher dimensional isogenies for cryptographic applications’. Université de Bordeaux, 9th July 2025. URL: <https://theses.hal.science/tel-05229911> (cit. on pp. 9, 20).
- [34] F. Etienne. ‘Algorithmic applications of Hecke operators of finite groups for Galois representations’. Université de Bordeaux, 7th July 2025. URL: <https://theses.hal.science/tel-05290378> (cit. on pp. 9, 19).
- [35] J. Gasnier. ‘Arithmetics and algorithmics of algebraic curves and applications to coding theory and cryptography’. Université de Bordeaux, 10th July 2025. URL: <https://theses.hal.science/tel-05262850> (cit. on pp. 9, 20).
- [36] A. Page. ‘Hecke operators in algorithmic number theory’. Université de Bordeaux, 3rd June 2025. URL: <https://inria.hal.science/tel-05324989> (cit. on p. 9).
- [37] N. Sarkis. ‘Arithmetic of Kummer lines’. Université de Bordeaux, 9th July 2025. URL: <https://theses.hal.science/tel-05263203> (cit. on pp. 9, 19).

Reports & preprints

- [38] A. Ahlbäck and F. Johansson. *Fast basecases for arbitrary-size multiplication*. 2nd Jan. 2025. URL: <https://hal.science/hal-04861755> (cit. on p. 15).
- [39] C. Armana, E. Berardini, X. Caruso, A. Leudière, J. Nardi and F. Pazuki. *A computational approach to Drinfeld modules*. Dec. 2025. URL: <https://hal.science/hal-05423892> (cit. on p. 12).
- [40] R. Barbulescu, D. Robert and N. Sarkis. *Models of Kummer lines and Galois representations*. 24th Mar. 2025. URL: <https://hal.science/hal-05002656> (cit. on p. 13).
- [41] A. Barraud. *Dual of Algebraic Geometry Codes from Hirzebruch Surfaces*. 30th Sept. 2025. URL: <https://hal.science/hal-05290224> (cit. on p. 15).

- [42] E. Berardini, A. G. Maidana and S. Marseglia. *Abelian surfaces over finite fields containing no curves of genus 3 or less*. 23rd May 2025. URL: <https://hal.science/hal-04692637> (cit. on p. 13).
- [43] K. de Boer, A. Page, R. Toma and B. Wesolowski. *Average hardness of SIVP for module lattices of fixed rank*. 17th Nov. 2025. URL: <https://inria.hal.science/hal-05372629> (cit. on p. 14).
- [44] K. de Boer, A. Pellet-Mary and B. Wesolowski. *Rigorous Methods for Computational Number Theory*. 14th Nov. 2025. URL: <https://hal.science/hal-05365649> (cit. on p. 12).
- [45] X. Caruso, F. Fürnsinn and D. Vargas-Montoya. *Galois groups of reductions modulo p of D -finite series*. 13th Apr. 2025. URL: <https://hal.science/hal-05034178> (cit. on p. 12).
- [46] H. Cohen and W. Zudilin. *Variations on a theme of Apéry*. 17th Jan. 2025. URL: <https://inria.hal.science/hal-04932961> (cit. on p. 12).
- [47] J.-M. Couveignes and R. Lercier. *Elliptic butterflies*. 3rd Nov. 2025. URL: <https://hal.science/hal-05342789> (cit. on p. 15).
- [48] A. Enge and M. Streng. *Schertz style class invariants for higher degree CM fields*. 2025. URL: <https://inria.hal.science/hal-01377376>.
- [49] F. Etienne. *An algorithm to compute Selmer groups via resolutions by permutations modules*. 17th Apr. 2025. URL: <https://hal.science/hal-05038206> (cit. on p. 12).
- [50] F. Johansson. *Generic rings in FLINT*. 3rd June 2025. URL: <https://inria.hal.science/hal-05094763> (cit. on p. 15).

Software

- [51] [SW] A.-E. Wilke, *covariant* version 1.0, 8th Dec. 2025. LIC: GNU General Public License v3.0 or later. HAL: [hal-05404880](https://hal.science/hal-05404880), URL: <https://hal.science/hal-05404880>, SWHID: [swh:1:dir:c353ca1bcf87cfe197f10c503232e33222c8aeb3;origin=https://hal.archives-ouvertes.fr/hal-05404880;visit=swh:1:snp:8d87344d9cc4ed4f4d29de0a990d4ef86fb0a809;anchor=swh:1:rel:541e9b51c39428fa232446467a59461341602a13;path=/](https://hal.archives-ouvertes.fr/hal-05404880).

11.3 Cited publications

- [52] D. Robert. *Fast pairings via biextensions and cubical arithmetic*. 19th Dec. 2024. URL: <https://hal.science/hal-04848028> (cit. on p. 13).
- [53] X. Caruso, F. Fürnsinn, D. Vargas-Montoya and W. Zudilin. ‘Galois Groups of Apéry-like Series Modulo Primes’. In: *arXiv preprint arXiv:2510.23298* (2025) (cit. on p. 12).