RESEARCH CENTRE

Inria Centre at the University of Bordeaux

IN PARTNERSHIP WITH:

CNRS, Université de Bordeaux

2024 ACTIVITY REPORT

Project-Team CANARI

Cryptography ANalysis and ARIthmetic

IN COLLABORATION WITH: Institut de Mathématiques de Bordeaux (IMB)

DOMAIN

Algorithmics, Programming, Software and Architecture

THEME

Algorithmics, Computer Algebra and Cryptology

Inria

Contents

Project-Team CANARI

Creation of the Project-Team: 2023 July 01

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

1 Team members, visitors, external collaborators

Research Scientists

- Damien Olivier Robert [Team leader, INRIA, Senior Researcher]
- Razvan Barbulescu [CNRS, Researcher]
- Xavier Caruso [CNRS, Senior Researcher]
- Andreas Enge [INRIA, Senior Researcher]
- Fredrik Johansson [INRIA, Researcher]
- Sabrina Kunzweiler [INRIA, ISFP, from Oct 2024]
- Aurel Page [INRIA, Researcher]
- Alice Pellet Mary [CNRS, Researcher]

Faculty Members

- Karim Belabas [UNIV BORDEAUX, Professor]
- Elena Berardini [CNRS, Professor, from Jun 2024]
- Guilhem Castagnos [UNIV BORDEAUX, Associate Professor]
- Henri Cohen [UNIV BORDEAUX, Emeritus]
- Jean-Marc Couveignes [UNIV BORDEAUX, Professor]
- Qing Liu [UNIV BORDEAUX, Associate Professor Delegation, until Aug 2024]

Post-Doctoral Fellows

- Marcel Houben [INRIA, Post-Doctoral Fellow, from Oct 2024]
- Sabrina Kunzweiler [INRIA, Post-Doctoral Fellow, until Sep 2024]
- Wessel Van Woerden [UNIV BORDEAUX, Post-Doctoral Fellow, from Nov 2024]
- Wessel Van Woerden [UNIV BORDEAUX, Post-Doctoral Fellow, until Oct 2024]

PhD Students

- Alix Barraud [UNIV BORDEAUX, from Aug 2024]
- Agathe Beaugrand [UNIV BORDEAUX]
- Pierrick Dartois [IMT]
- Fabrice Etienne [UNIV BORDEAUX]
- Jean Gasnier [UNIV BORDEAUX]
- Afonso Li [UNIV BORDEAUX, from Aug 2024]
- Guilhem Mureau [INRIA]
- Nicolas Sarkis [UNIV BORDEAUX]
- Anne-Edgar Wilke [UNIV BORDEAUX, from Sep 2024]
- Anne-Edgar Wilke [UNIV BORDEAUX, ATER, until Aug 2024]

Technical Staff

- Bill Allombert [CNRS, Engineer]

Interns and Apprentices

- Rayane Bait [INRIA, Intern, from May 2024 until Sep 2024]

Administrative Assistant

- Flavie Blondel [INRIA]

External Collaborators

- Maxime Bombar [UNIV BORDEAUX, from Sep 2024]
- Luca De Feo [IBM RESEARCH EUROPE]
- 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 approching 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 activites 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

Raphaël Pagès defended his PhD thesis 'Factorisation des opérateurs différentiels en caractéristique positive' in February 2024 [29].

6.1 Awards

The PARI/GP software won the price 'Prix science ouverte du logiciel libre de la recherche' from the ministère de l'Enseignement supérieur et de la Recherche in the category 'Communauté'.

The paper [20] by P. Dartois, A. Leroux, D. Robert and B. Wesolowski won the best paper award of Eurocrypt 2024.

7 New software, platforms, open data

7.1 New software

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

Participants: Bill Allombert, Karim Belabas, Henri Cohen, Andreas Enge, Aurel Page

Partner: CNRS

[1] The commitment letter

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

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 |Re(z)| and tiny |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 2n̂ 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 0.4.3 "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 Higher dimensional number theory

Participants: Xavier Caruso, Henri Cohen, Aurel Page.

In [34], A. Bartel and A. Page develop a new approach to the isospectrality of the orbifolds constructed by Vignéras.

In [50], H. Cohen explains how to accelerate continued fractions, and then in [49] he builds a database of continued fractions of polynomial type.

Drinfeld modules

In [12], X. Caruso and Quentin Gazda designed an implemented an efficient algorithm for computing L-series of Drinfeld modules and Anderson motives over $\mathbb{F}_q[t]$. Based on a large dataset produced by this algorithm, they formulated a conjecture stating that the order of vanishing at 1 of the v-adic L-series of an Anderson motive is independent of v

In [39], X. Caruso, Quentin Gazda and Alexis Lucas studied Wieferich primes in the context of Drinfeld modules. They managed to relate the property of being Wieferich to the vanihsing of the L-series. They also obtained probabilistic results (confirming standard heuristics) about the repartition of Wieferich primes for many families of Drinfeld modules.

Algebraic differential equations

Alin Bostan, X .Caruso and Julien Roques published a survey [11] on the theory of linear differential equations over number fields and finite fields, focusing on algebraic criteria for the existence of algebraic solutions.

8.2 Algorithms for number theory

Participants: Razvan Barbulescu, Karim Belabas, Jean-Marc Couveignes, Andreas Enge, Fabrice Etienne.

In [22], A. Enge presents his implementation of the FastECPP algorithm for primality proving. He carries out a complexity analysis with particular emphasis on the parallelisation aspects and presents the parameter choices that have made possible the record of a primality proof for $(10^{86453}-1)/9$ using his CM software [51]. This free software has been used for 18 primality proofs out of the 20 largest primes without special properties referenced at `https://t5k.org/top20/page.php?id=27`.

In [42], F. Etienne describes an algorithm to compute class groups by induction with generalised norm relations.

The paper [7] by R. Barbulescu and F. Jouve useing the Elliott-Halberstam conjecture to measure how ECM friendly an elliptic curve with complex multiplication is was published in Acta Arithmetica.

In [8], published in Mathematics of Computation, K. Belabas and D. Simon give an algorithm for power detection in number fields.

8.3 Cryptography

Participants: Guilhem Castagnos.

In [19], L. Braun, G. Castagnos, I. Damgård, F. Laguillaumie, K. Melissaris, C. Orlandi, I. Tucker present distributed key generation and decryption protocols for an additively homomorphic cryptosystem based on class groups, CL, improving on a similar system proposed by Braun, Damgård, and Orlandi at CRYPTO'23. Their key generation is similarly constant round but achieves lower communication complexity than the previous work. This improvement is in part the result of relaxing the reconstruction property required of the underlying integer verifiable secret sharing scheme. This eliminates the reliance on potentially costly proofs of knowledge in unknown order groups. They present a new method to batch zero-knowledge proofs in unknown order groups which strengthens these improvements. They also present a protocol which is proven secure against adaptive adversaries in the single inconsistent player (SIP) model. Theirs protocols are secure in the universal composability (UC) framework and provide guaranteed output delivery. They demonstrate the relative efficiency of our techniques by presenting the running times and communication costs associated with our implementation of the statically secure protocol and provide a direct comparison with alternate state of the art constructions.

8.4 Isogeny based cryptography

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

The paper [20], P. Dartois, A. Leroux, D. Robert and B. Wesolowski, which present the SQISignHD protocol, has been published in Eurocrypt 2024 and won the best paper awards.

The verification step of SQISignHD requires computing dimension 4 2^e-isogenies. The algorithmic aspects of this task was tackled in [40] by P. Dartois, using theta coordinates.

In [18], published at Asiacrypt 2024, A. Basso, L. de Feo, P. Dartois, A. Leroux, L. Maino, G. Pope, D. Robert, and B. Wesolowski introduce the SQISign2d protocol (in its 'West' variant). This version improves on the SQISignHD version by keeping the fast signature and strong security proof while improving significantly on the verification time.

In [44], S. Kunzweiler, L. Maino T. Moriya C. Petit, G. Pope D. Robert, M. Stopar and Y.B. Ti look at hash functions from isogeny graphs in dimension up to $g = 3$. They show that dimension 3 is more efficient than dimension 1 or 2.

The paper [27], by D. Robert, written for the NuTMiC 2024 invited talk, contains a survey on the representation of isogenies. It notably focus on the recent HD representation, which allows to give an efficient representation of any isogeny, and which had tremendous impacts on the field of isogeny based cryptography.

In [46], D. Robert introduces MIKE (module isogeny key exchange) a new Non Interactive Key Exchange protocol, which combine the best advantages of CSIDH and full non commutative supersingular isogeny graphs.

Using commutative isogeny graphs, like in CSIDH, allow to build a NIKE. But the graphs result from a commutative group action (by ideals of a class group), and the protocol is susceptible to a subexponential quantum attack. The idea of exploiting non commutative supersingular graphs was used in SIDH, but the protocol relied on extra torsion information (due to the difficulty of building a NIKE on a non commutative graph), and was spectacularly broken in 2022.

The idea of MIKE is to replace the ideal action by a Hermitian module action to get the benefit of a nice NIKE without the subexponential attack. In [46], D. Robert shows that supersingular graphs fit into this framework via their Weil restriction, which can be described by a rank 2 module action.

In [31], B. Allombert, J-F. Biasse, J. K. Eriksen, P. Kutas, C. Leonardi, A .Page, R .Scheidler, M. T. Bagi give new efficient parameters for SCALLOP, an isogeny based (full) group action. The main difference compared to SCALLOP is that they start from a non trivial class group at the top of the volcano. This required a large class group computation, done via tweaks to the PARI/GP algorithm.

The paper [6] by S. Arpin, J. Clements, P .Dartois, J. K. Eriksen, P. Kutas and B Wesolowski on finding orientations was published in esigns, Codes and Cryptography.

The paper [17] by B. Wesolowski on attacking the isogeny path problems in Drinfeld modules was published in IACR Communications in Cryptology.

The paper [21] by P. Dartois, L. Maino, G. Pope and D. Robert, using optimised formula for 2^n-isogenies in dimension 2 was published in Asiacrypt 2024.

The paper [26] by A. Page and B. Wesolowski on the equivalence between the one endomorphism and the full endomorphism problem for supersingular elliptic curves has been published in Eurocrypt 2024.

8.5 Elliptic curves and abelian varieties

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

In [15], published at ANTS 2024, S. Kunzweiler and D. Robert give a new method, using deformation and higher dimensional isogenies, to compute modular polynomials on elliptic curves. The algorithm is quasi-linear and does not rely on any assumption.

In [16], published in IACR Communications in Cryptology, D. Robert and N. Sarkis improve some formulas for computing 2-isogenies between Kummer lines, notably on variants of the Montgomery models.

They use these results in [47] to give new (faster) formulas for scalar multiplications on Montgomery curves.

A. Enge and M. Streng have completely rewritten their preprint [41]. Using Shimura reciprocity and quadratic forms over totally real number fields they provide an easy to implement algorithm for deciding whether special values of Siegel modular functions of higher level define moduli of polarised abelian varieties and lead to class invariants defining unramified abelian field extensions. In this case, they determine a complete set of Galois conjugates. They also examine in detail under which conditions the invariants are real.

In [37] E. Berardini, A. Giangreco–Maidana and S. Marseglia characterize abelian surfaces defined over finite fields containing no curves of genus less than or equal to 3. They complete and expand the characterisation of isogeny classes of abelian surfaces with no curves of genus up to 2, then show that for simple abelian surfaces, containing a curve of genus 3 is equivalent to admitting a polarisation of degree 4. Thanks to this result, they can use existing algorithms to check which isomorphism classes in the isogeny classes containing no genus 2 curves have a polarisation of degree 4. Besides, they describe absolutely irreducible genus 3 curves lying on abelian surfaces containing no curves of genus less than or equal to 2, and show that their number of rational points is far from the Serre–Weil bound.

The paper [14] by J. Kieffer, A. Page and D. Robert on computing isogenies from modular polynomials in dimension 2 was published in Journal of Algebra.

8.6 Pairings

Participants: Damien Robert, Jean Gasnier.

In [45], D. Robert give new formulas to compute pairings on elliptic curves and abelian varieties by developing the arithmetic of biextensions and cubical arithmetic.

In [43], J. Gasnier and A. Guillevic given an algebraic point of view on the generation of pairing-friendly curves.

8.7 Lattices and Lattice-based cryptography

Participants: Guilhem Mureau, Alice Pellet-Mary, Wessel van Woerden.

In June 2023, the NIST started an additional post-quantum signature standardization process.[2] The objective of this new call is to standardize one or more post-quantum signature scheme, different from the ones standardized so far. Members of the Canari team have studied the security of some of the new submissions, based on lattices and codes.

In [24], published in Crypto 2024, Felicitas Hörmann and Wessel van Woerden described a polynomial time attack against a NIST submission called FuLeeca. This submission uses codes in the Lee metric, which make the algorithmic problems very similar to lattice problems. Exploiting this connection with lattices, the authors were able to exploit leakage from the signatures to obtain a key-recovery attack against the scheme.

In [25], Guilhem Mureau, Alice Pellet-Mary, Heorhii Pliatsok and Alexandre Wallet studied the hardness of the module lattice isomorphism problem (module-LIP), which serve as a foundation for the security of Hawk, another signature scheme submitted to the NIST competition. The authors showed that when instantiated over totally real fields, the module-LIP problem becomes easy, and can be heuristically solved in polynomial time (when the modules have rank 2). This does not threaten the Hawk signature scheme since they use modules over a totally complex field, which is not subject to the attack.

[2] NIST's call

In [13], published in Acta Crystallographica, M. D. Sikirić and W. van Woerden give a Complete classification of six-dimensional iso-edge domains.

In [28], published in Asiacrypt 2024, W. van Woerden shows that dense and smooth lattices exist in any genus.

8.8 Quantum algorithms for cryptanalysis

Participants: Razvan Barbulescu.

In [32], Razvan Barbulescu, Muguel Barcau and Vicentiu Pasol extended Regev's quantum algorithm to elliptic curves. Indeed, the extension is not direct because there is no natural notion of smallness for the points of an elliptic curve over a finite field. The speedup with respect to Shor tends to infinity with the input size and corresponds to a speedup pf factor 4 for some curves of the NIST list.

In [33], Razvan Barbulescu and Gaëtan Bisson proposed a variant of Regev's algorithm for hyperelliptic curves. When the genus g is large the speed-up is $\min(g, \sqrt(n))$ which corresponds to the full potential of Regev's idea when the genus is very large, i.e. $g \geq \sqrt{n}$. In cryptography only the case $g = 2$ is used and they propos a different improvement in this case, obtaining a speedup by a factor 7 for a curve used in cryptography. The algorithm suggests that, for quantum computing, the hypperelliptic curves are slightly weaker than elliptic curves.

8.9 Coding theory

Participants: Elena Berardini, Xavier Caruso, Fabrice Drain.

In a series of paper [10, 35], E. Berardini and X. Caruso defined new families of codes for the sum-rank metric. They first introduced linearized versions of Algebraic Geometry codes and studied their parameter, showing in particular that the obtained codes beat the (sum-rank analogue of the) Gilbert–Varshamov bound. They also introduced a linearized analogue of Reed–Muller codes.

In [38], X. Caruso and F. Drain obtained a complete classification of self-dual skew cyclic and skew negacyclic codes. They also provided efficient algorithms for sampling and enumerating them.

In [9], E. Berardini, A. Caminata and A. Ravagnani investigate CSS and CSS-T quantum error-correcting codes from the point of view of their existence, rarity, and performance.

In [36], E. Berardini, R. Dastbasteh, J. Etxezarreta Martinez, S. Jain and O. Sanz Larrarte give a new construction of binary quantum codes that enables the generation of a CSS-T code from any given CSS code. Using this construction, they prove the existence of asymptotically good binary CSS-T codes, resolving a previously open problem in the literature.

8.10 Effective analysis and certified arithmetic

Participants: Fredrik Johansson.

In [23], F. Johansson and J. van der Hoeven gave efficient algorithms to take advantage of precomputations when evaluating elementary functions in multiple precision arithmetic.

In [48], L .Stempfle, A .James, J .Josse, T .Gauss, F .Johansson study interpretable machine learning models with missing data.

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

9.1.1 Visits of international scientists

Other international visits to the team The following international speakers gave a talk at the Canari seminar in 2024: Thomas Decru (KU Leuven), Semyon Novoselov (University of Kaliningrad), Rocco Mora (CISPA), Dmitrii Koshelev (Ethereum Foundation), Simona Etinski (CWI), Lars Ran (Radboud University), Oana Padurariu (Max-Planck-Institut für Mathematik, Bonn), Bram Bekker (TU Delft), Valentijn Karemaker (Universiteit Utrecht), Eric Ahlqvist (University of Edinburgh), Maria Corte-Real Santos (University College London), Reza Dasbasteh (Universidad de Navarra), Sam Frengley (University of Bristol), Florian Breuer (University of Newcastle, Australia), Rob de Jeu (Vrije Universiteit Amsterdam).

9.2 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 Toulouse, Paris
2021–2025, 45k€ for Bordeaux

ANR Ciao Isogeny based cryptosystems, applications to verifiable delay functions and post-quantum cryptography (PI D. Robert)
with Paris, Montpellier
2019–2024, 150k€ for Bordeaux

ANR/NSF Charm Cryptographic hardness of module lattices
with Florida Atlantic, Cornell, ENS Lyon
2021–2024, 205k€ 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 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€

PEPS Groupe des points des variétés abéliennes sur les corps finis
E. Berardini and F. Campagna (LMBP, UCA)
2024, 4000€

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

- X. Caruso co-organized a one-week workshop SageDays 125
- E. Berardini co-organized a two-day symposium called CAIPI (Coding theory, cryptogrAphy, arIthmetic geometry, and comPuter Algebra) three times during 2024 in Marseille (February), Rennes (May) and Limoges (December)
- A. Enge organized a three-day MPFR/MPC/MPFI/ARB Developers Meeting
- A. Enge and F. Johansson co-organized a one-week 2024 FLINT development workshop

Member of the conference program committees

- G. Castagnos was part of the program committee of Crypto 2024
- G. Castagnos was part of the program committee of SCN 2024
- F. Johanssson was part of the program committee of ANTS 2024
- S. Kunzweiler was part of the program committee of PKC 2025
- A. Pellet-Mary was part of the program committee of Crypto 2024
- W. van Woerden was part of the program committee of Eurocrypt 2025

10.1.2 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*

10.1.3 Invited talks

- Alice Pellet-Mary gave an invited talk at the conference SCN 2024
- D. Robert gave an invited talk 'On the efficient representation of isogenies' at the conference NuTMiC 2024, and a talk 'From ideals to modules for isogeny based cryptography' at the Leuven Isogeny Days 5. He also gave a talk 'Quand l'ajout de structure casse un cryptosystème : quelques exemples de cryptanalyse' at the Journées Scientifiques Inria.
- S. Kunzweiler gave an invited talk on 'Recent developments in isogeny-based cryptography' at the conference PQCrypto 2024 , and an invited talk on 'Isogeny Computations in Higher Dimensions' at the workshop ECC 2024.
- E. Berardini gave an invited talk on 'From curves to surfaces: a walk through Algebraic Geometry codes' at the conference Mathematics for Post-Quantum Cryptanalysis in Budapest, Hungary.

10.1.4 Scientific expertise

- X. Caruso was part of the HCERES committee that evaluates the LAGA (Université Paris 13).

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.

10.2 Teaching - Supervision - Juries

- Andreas Enge has given a series of lectures on elementary, analytic and algorithmic number theory at the CIMPA school *Algèbre, géométrie algébrique et applications à la théorie de l'information* in Douala (Cameroun) `https://douala2024.gaati.org/`.
- Alice Pellet-Mary has given a series of lectures on lattice based cryptography at the same CIMPA school in Douala (Cameroun).

- Sabrina Kunzweiler gave a lecture at the autumn school in supersingular isogenies in Taipei (Taiwan).
- 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 (undegraduate program for student in engineering)
- A. Page
  - 27h exercise sessions on computer algebra, Master 2 (preparation for the Agrégation national competitive examination), 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

10.2.1 Supervision

- PhD in progress: Anne-Edgar Wilke, *Enumerating integral orbits of prehomogeneous representations*, since September 2019, supervised by K. Belabas.
- PhD in progress: Agathe Beaugrand, *Conception de systèmes cryptographiques utilisant des groupes de classes de corps quadratiques*, since September 2021, supervised by Guilhem Castagnos and Fabien Laguillaumie.
- PhD in progress: Fabrice Étienne, *Techniques d'induction pour l'algorithmique des représentations galoisiennes*, since September 2022, supervised by Aurel Page.
- PhD in progress: Nicolas Sarkis, *Recherche de courbes planes de genre 2 adaptée à la factorisation des entiers*, since September 2022, supervised by Razvan Barbulescu and Damien Robert.
- PhD in progress: Pierrick Dartois *Improvement and security analysis of isogeny-based cryptographic schemes*, since September 2022, supervised by Damien Robert and Benjamin Wesolowski.
- PhD in progress: Jean Gasnier, *Algorithmique des isogénies et applications*, since October 2022, 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: Guilhem Mureau, *Isomorphism of algebraic lattices*, since September 2023, supervised by Alice Pellet--Mary and Renaud Coulangeon.
- PhD in progress: Alix Barraud, *Algebraic geometry codes from surfaces and quantum codes*, since September 2024, supervised by Elena Berardini and Gilles Zémor.

10.2.2 Juries

- X. Caruso
  - Cécile Armana (HDR), Université de Bourgogne Franche-Comté, 2024: *Contributions à l'étude des formes modulaires sur les corps de fonctions*
  - Bianca Gouthier, Université de Bordeaux, 2024: *Actions rationnelles de schémas en groupes infinitésimaux*
  - Raphaël Pagès, Université de Bordeaux, 2024: *Factorisation des opérateurs différentiels en caractéristique positive*
  - Martin Weimann (HDR), Université Caen-Normandie, 2024: *Incursions en géométrie algébrique effective et calcul formel*
- G. Castagnos
  - Ambroise Fleury, Université Paris-Saclay, 2024: *Amélioration des algorithmes de crible. Application à la factorisation des entiers* (report)
- A. Enge
  - Sorina Ionica (HDR), Université de Picardie Jules Verne, 2024: *Variétés abéliennes, multiplication complexe et cryptographie* (report)
- S. Kunzweiler
  - Jonathan Komada Eriksen, Norwegian University of Science and Technology (Trondheim, Norway), 2024: *Supersingular Endomorphism Rings: Algorithms and Applications*
- E. Berardini
  - Raphaël Pagès, Université de Bordeaux, 2024: *Factorisation des opérateurs différentiels en caractéristique positive*
  - Antonio de Marti i Olius, University of Navarra–TECNUN (San Sebastian, Spain), 2024: *Decoding Algorithms for Quantum Error Correcting Codes*
  - Antoine Leudière, Université de Lorraine, 2024: *Morphismes de modules de Drinfeld et leurs algorithmes*

10.3 Popularization

- X. Caruso gave a general audience talk "Les idéaux d'Emmy Noether" at the Bibliothèque Nationale de France in the programme *Un texte, un mathématicien*

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

- X. Caruso and Pierre Grangé-Pradéras realized an art exposition Théorèmes; they presented several times this exposition to various audiences (including pupils and high school students).

10.3.2 Participation in Live events

- A. Pellet-Mary organized 4 "ateliers" for high school female students during the week "Moi informaticienne Moi Mathématicienne" at IMB.
- X. Caruso participated to the programmes "Fête de la Science" and "Village des Sciences"
- E. Berardini participated to the "Circuit Scientifique Bordelais", leading a workshop on error-correcting codes

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. 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. 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. 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. URL: https://hal.science/hal-03943959.

11.2 Publications of the year

International journals

[6] S. Arpin, J. Clements, P. Dartois, J. K. Eriksen, P. Kutas and B. Wesolowski. 'Finding Orientations of Supersingular Elliptic Curves and Quaternion Orders'. In: *Designs, Codes and Cryptography* 92.11 (Nov. 2024), pp. 3447–3493. DOI: 10.48550/arXiv.2308.11539. URL: https://hal.science/hal-04186188 (cit. on p. 10).

[7] R. Barbulescu and F. Jouve. 'ECM And The Elliott-Halberstam Conjecture For Quadratic Fields'. In: *Acta Arithmetica* 213.4 (2024), pp. 289–324. DOI: 10.4064/aa230110-21-2. URL: https://hal.science/hal-03485435 (cit. on p. 9).

[8] K. Belabas and D. Simon. 'Power detection over number fields'. In: *Mathematics of Computation* 93.348 (27th Feb. 2024), pp. 1953–1961. DOI: 10.1090/mcom/3913. URL: https://normandie-univ.hal.science/hal-04561403 (cit. on p. 9).

[9] E. Berardini, A. Caminata and A. Ravagnani. 'Structure of CSS and CSS-T Quantum Codes'. In: *Designs, Codes and Cryptography* 92.10 (24th May 2024), pp. 2801–2823. DOI: 10.1007/s10623-024-01415-9. URL: https://hal.science/hal-04590650 (cit. on p. 12).

[10] E. Berardini and X. Caruso. 'Algebraic Geometry codes in the sum-rank metric'. In: *IEEE Transactions on Information Theory* 70.5 (25th Apr. 2024), pp. 3345–3356. DOI: 10.1109/TIT.2024.3366751. URL: https://hal.science/hal-04034810 (cit. on p. 12).

[11] A. Bostan, X. Caruso and J. Roques. 'Algebraic solutions of linear differential equations: An arithmetic approach'. In: *Bulletin of the American Mathematical Society* 61.4 (2024), pp. 609–658. DOI: 10.1090/bull/1835. URL: https://hal.science/hal-04065092 (cit. on p. 9).

[12] 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 (cit. on p. 9).

[13] 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. URL: https://hal.science/hal-04905930 (cit. on p. 12).

[14] 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 (cit. on p. 11).

[15] S. Kunzweiler and D. Robert. 'Computing modular polynomials by deformation'. In: *Research in Number Theory* 11.1 (10th Dec. 2024), p. 10. DOI: 10.1007/s40993-024-00596-5. URL: https://hal.science/hal-04671239 (cit. on p. 10).

[16] D. Robert and N. Sarkis. 'Computing 2-isogenies between Kummer lines'. In: *IACR Communications in Cryptology* (9th Apr. 2024). DOI: 10.62056/abvua69p1. URL: https://hal.science/hal-04382643 (cit. on p. 11).

[17] B. Wesolowski. 'Computing isogenies between finite Drinfeld modules'. In: *IACR Communications in Cryptology* (9th Apr. 2024). DOI: 10.62056/avommp-3y. URL: https://hal.science/hal-03941045 (cit. on p. 10).

International peer-reviewed conferences

[18] A. Basso, P. Dartois, L. D. Feo, A. Leroux, L. Maino, G. Pope, D. Robert and B. Wesolowski. 'SQIsign2D-West The Fast, the Small, and the Safer'. In: ASIACRYPT. Vol. 15486. Lecture Notes in Computer Science. Kolkata, India: Springer Nature Singapore, 10th Dec. 2024, pp. 339–370. DOI: 10.1007/978-981-96-0891-1_11. URL: https://hal.science/hal-04603556 (cit. on p. 10).

[19] 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: *Lecture Notes in Computer Science*. SCN 2024 - 14th International Conference on Security and Cryptography for Networks. Vol. LNCS-14974. Security and Cryptography for Networks. Amalfi, Italy: Springer Nature Switzerland, 10th Sept. 2024, pp. 24–46. DOI: 10.1007/978-3-031-71073-5_2. URL: https://inria.hal.science/hal-04820390 (cit. on p. 9).

[20] 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. URL: https://hal.science/hal-04562459 (cit. on pp. 6, 10).

[21] 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. URL: https://hal.science/hal-04297088 (cit. on p. 10).

[22] A. Enge. 'FastECPP over MPI'. In: Mathematical Software – ICMS 2024. Vol. 14749. Lecture Notes in Computer Science. Durham, United Kingdom: Springer Nature Switzerland, 17th July 2024, pp. 36–45. DOI: 10.1007/978-3-031-64529-7_4. URL: https://inria.hal.science/hal-04522492 (cit. on p. 9).

[23] J. van der Hoeven and F. Johansson. 'Fast multiple precision exp(x) with precomputations'. In: 2024 IEEE 31st Symposium on Computer Arithmetic (ARITH). Malaga, Spain: IEEE; IEEE, 4th July 2024, pp. 80–87. DOI: 10.1109/ARITH61463.2024.00023. URL: https://hal.science/hal-04454093 (cit. on p. 12).

[24] F. Hörmann and W. van Woerden. 'FuLeakage: Breaking FuLeeca by Learning Attacks'. In: Crypto 2024. Vol. 14925. Lecture Notes in Computer Science. Santa Barbara, CA, United States: Springer Nature Switzerland, 17th Aug. 2024, pp. 253–286. DOI: 10.1007/978-3-031-68391-6_8. URL: https://hal.science/hal-04905898 (cit. on p. 11).

[25] G. Mureau, A. Pellet-Mary, G. Pliatsok and A. Wallet. 'Cryptanalysis of rank-2 module-LIP in Totally Real Number Fields'. In: *Advances in Cryptology – EUROCRYPT 202443rd Annual International Conference on the Theory and Applications of Cryptographic Techniques, Zurich, Switzerland, May 26–30, 2024, Proceedings, Part VII*. Eurocrypt 2024 - 43rd Annual International Conference on the Theory and Applications of Cryptographic Techniques. Vol. 14657. Lecture Notes in Computer Science. Zurich, Switzerland: Springer Nature Switzerland, 28th Apr. 2024, pp. 226–255. DOI: 10.1007/978-3-031-58754-2_9. URL: https://hal.science/hal-04701342 (cit. on p. 11).

[26] A. Page and B. Wesolowski. 'The supersingular Endomorphism Ring and One Endomorphism problems are equivalent'. In: Advances in Cryptology – EUROCRYPT 2024. Vol. 14656. Lecture Notes in Computer Science. Zurich (CH), Switzerland: Springer Nature Switzerland, 29th Apr. 2024, pp. 388–417. DOI: 10.1007/978-3-031-58751-1_14. URL: https://inria.hal.science/hal-04209824 (cit. on p. 10).

[27] 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. Szczecin, Poland, 24th June 2024. URL: https://hal.science/hal-04848010 (cit. on p. 10).

[28] 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. URL: https://hal.science/hal-04905912 (cit. on p. 12).

Doctoral dissertations and habilitation theses

[29] R. Pagès. 'Factoring differential operators in positive characteristic.' Université de Bordeaux, 21st Feb. 2024. URL: https://hal.science/tel-04490793 (cit. on p. 6).

Reports & preprints

[30] A. Ahlbäck and F. Johansson. *Fast basecases for arbitrary-size multiplication*. 2nd Jan. 2025. URL: https://hal.science/hal-04861755.

[31] B. Allombert, J.-F. Biasse, J. K. Eriksen, P. Kutas, C. Leonardi, A. Page, R. Scheidler and M. Tot Bagi. *PEARL-SCALLOP: Parameter Extension Applicable in Real Life for SCALLOP*. 31st Oct. 2024. URL: https://inria.hal.science/hal-04755827 (cit. on p. 10).

[32] R. Barbulescu, M. Barcau and V. Pasol. *A comprehensive analysis of Regev's quantum algorithm*. 12th Dec. 2024. URL: https://hal.science/hal-04833072 (cit. on p. 12).

[33] R. Barbulescu and G. Bisson. *Regev's attack on hyperelliptic cryptosystems*. 12th Dec. 2024. URL: https://hal.science/hal-04832839 (cit. on p. 12).

[34] A. Bartel and A. Page. *Vignéras orbifolds: isospectrality, regulators, and torsion homology*. 9th July 2024. URL: https://inria.hal.science/hal-04672815 (cit. on p. 8).

[35] E. Berardini and X. Caruso. *Reed-Muller codes in the sum-rank metric*. May 2024. URL: https://hal.science/hal-04577005 (cit. on p. 12).

[36] E. Berardini, R. Dastbasteh, J. E. Martinez, S. Jain and O. S. Larrarte. *Asymptotically good CSS-T codes exist*. 11th Dec. 2024. URL: https://hal.science/hal-04834836 (cit. on p. 12).

[37] E. Berardini, A. G. Maidana and S. Marseglia. *Abelian surfaces over finite fields containing no curves of genus* 3 *or less*. 10th Sept. 2024. URL: https://hal.science/hal-04692637 (cit. on p. 11).

[38] X. Caruso and F. Drain. *Selfdual skew cyclic codes*. Oct. 2024. URL: https://hal.science/hal-04127001 (cit. on p. 12).

[39] X. Caruso, Q. Gazda and A. Lucas. *Wieferich primes for Drinfeld modules*. 13th Dec. 2024. URL: https://hal.science/hal-04837662 (cit. on p. 9).

[40] P. Dartois. *Fast computation of 2-isogenies in dimension 4 and cryptographic applications*. 22nd July 2024. URL: https://hal.science/hal-04662137 (cit. on p. 10).

[41] A. Enge and M. Streng. *Schertz style class invariants for higher degree CM fields*. 2024. URL: https://inria.hal.science/hal-01377376 (cit. on p. 11).

[42] F. Etienne. *Computing class groups by induction with generalised norm relations*. Nov. 2024. URL: https://hal.science/hal-04778100 (cit. on p. 9).

[43] J. Gasnier and A. Guillevic. *An Algebraic Point of View on the Generation of Pairing-Friendly Curves*. 16th Dec. 2024. URL: https://hal.science/hal-04205681 (cit. on p. 11).

[44] S. Kunzweiler, L. Maino, T. Moriya, C. Petit, G. Pope, D. Robert, M. Stopar and Y. B. Ti. *Radical 2-isogenies and cryptographic hash functions in dimensions 1, 2 and 3*. 13th Dec. 2024. URL: https://hal.science/hal-04837057 (cit. on p. 10).

[45] D. Robert. *Fast pairings via biextensions and cubical arithmetic*. 19th Dec. 2024. URL: https://hal.science/hal-04848028 (cit. on p. 11).

[46] D. Robert. *The module action for isogeny based cryptography*. Oct. 2024. URL: https://hal.science/hal-04848019 (cit. on p. 10).

[47] D. Robert and N. Sarkis. *Halving differential additions on Kummer lines*. 2024. URL: https://hal.science/hal-04724019 (cit. on p. 11).

[48] L. Stempfle, A. James, J. Josse, T. Gauss and F. Johansson. *Expert Study on Interpretable Machine Learning Models with Missing Data*. 2024. DOI: 10.48550/arXiv.2411.09591. URL: https://hal.science/hal-04894332 (cit. on p. 12).

11.3 Cited publications

[49] H. Cohen. *A Database of Continued Fractions of Polynomial Type*. 2024. arXiv: 2409.06086 [math.NT]. URL: https://arxiv.org/abs/2409.06086 (cit. on p. 8).

[50] H. Cohen. *Apéry Acceleration of Continued Fractions*. 2024. arXiv: 2401.17720 [math.NT]. URL: https://arxiv.org/abs/2401.17720 (cit. on p. 8).

[51] [SW Rel.] A. Enge, *CM* version 0.4.3, Feb. 2024. LIC: GPL-3.0-or-later. SWHID: ⟨swh:1:dir:056fba450fbd9406efd86a5db93895fa63d212df;origin=https://gitlab.inria.fr/enge/cm;visit=swh:1:snp:d0a38ff75431aab4c91e1a50a51b26a573e17784;anchor=swh:1:rev:7a6567cf2d98aa9a37166b2c4c99f7dfcecfea58⟩ (cit. on p. 9).