RESEARCH CENTRE

Inria Centre at the University of Bordeaux

IN PARTNERSHIP WITH:

CNRS, Université de Bordeaux

2023 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, from Oct 2023, HDR]
- Razvan Barbulescu [CNRS, Researcher, from Jul 2023]
- Xavier Caruso [CNRS, Senior Researcher, from Jul 2023, HDR]
- Andreas Enge [INRIA, Senior Researcher, from Jul 2023, HDR]
- Fredrik Johansson [INRIA, Researcher, from Jul 2023]
- Aurel Page [INRIA, Researcher, from Jul 2023]
- Alice Pellet Mary [CNRS, Researcher, from Jul 2023]

Faculty Members

- Karim Belabas [UNIV BORDEAUX, Professor, from Jul 2023, HDR]
- Guilhem Castagnos [UNIV BORDEAUX, Associate Professor, from Jul 2023, HDR]
- Henri Cohen [UNIV BORDEAUX, Emeritus, from Jul 2023]
- Jean-Marc Couveignes [UNIV BORDEAUX, Professor, from Jul 2023, HDR]
- Qing Liu [UNIV BORDEAUX, Associate Professor Delegation, from Sep 2023]

Post-Doctoral Fellows

- Sabrina Kunzweiler [INRIA, Post-Doctoral Fellow, from Jul 2023]
- Wessel Van Woerden [UNIV BORDEAUX, Post-Doctoral Fellow, from Jul 2023]

PhD Students

- Agathe Beaugrand [UNIV BORDEAUX, from Jul 2023]
- Elie Bouscatie [ORANGE, CIFRE, from Jul 2023 until Nov 2023]
- Pierrick Dartois [IMT, from Jul 2023]
- Fabrice Etienne [UNIV BORDEAUX, from Jul 2023]
- Jean Gasnier [UNIV BORDEAUX, from Jul 2023]
- Guilhem Mureau [INRIA, from Sep 2023]
- Nicolas Sarkis [UNIV BORDEAUX, from Jul 2023]
- Anne-Edgar Wilke [UNIV BORDEAUX, ATER, from Jul 2023]

Technical Staff

- Bill Allombert [CNRS, Engineer, from Jul 2023]

Administrative Assistant

- Joelle Rodrigues [INRIA]

External Collaborators

- Luca De Feo [IBM RESEARCH EUROPE, from Jul 2023, HDR]
- Benjamin Wesolowski [CNRS, from Jul 2023]

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.

[1] The commitment letter

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

Wessel van Woerden defended his PhD thesis, *Lattice Cryptanalysis: from cryptanalysis to new foundations*, February 2023, Leiden.

Élie Bouscatié defended his PhD thesis, *Chiffrement compatible avec l'analyse de flux*, December 2023.

6.1 Major releases

FLINTsaw a new major release 3.0, merging ARB and CALCIUM.

6.2 Awards

The article [24] received the Eurocrypt honorable mention award.

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 widely used computer algebra system designed for fast computations in number theory (factorisation, algebraic number theory, elliptic curves, modular forms ...), but it also contains a large number of other useful functions to compute with mathematical entities such as matrices, polynomials, power series, algebraic numbers, etc., and many transcendental functions.

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

Contact: Aurel Page

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

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), Allemagne

7.1.3 GNU MPC

Keyword: Arithmetic

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 Théveny

7.1.4 Arb

Name: Arb

Keywords: Multiple-Precision, Interval arithmetic, Interval analysis, Computational number theory, Numerical algorithm

Functional Description: C library for arbitrary-precision ball arithmetic

URL: http://arblib.org

Contact: Fredrik Johansson

7.1.5 Calcium

Name: Calcium

Keywords: Computer algebra, Numerical analysis

Functional Description: C library for exact computation with real and complex numbers

Contact: Fredrik Johansson

7.1.6 SQISignHD

Keyword: Cryptography

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

Contact: Damien Olivier Robert

7.1.7 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

7.1.8 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

7.1.9 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: Changes in version 0.4 ("Fitzebohnen"): - increase minimal version number for mpfrcx to 0.6.3 and for pari to 2.11. - add decomposition of the class field into a tower of prime degree extensions - add a fastECPP implementation, including a version for MPI

URL: http://www.multiprecision.org/cm/home.html

Contact: Andreas Enge

Participant: Andreas Enge

8 New results

8.1 Higher dimensional number theory

Participants: Karim Belabas, Xavier Caruso, Henri Cohen, Pınar Kılıçer, Aurel Page.

Number fields

In [26], H. Cohen wrote a survey on Computational Number Theory.

In [5], K. Belabas, F. Diaz y Diaz and E. Friedman study special values of narrow ray class partial zeta functions.

In [28], B. Allombert and D. Mayer study capitulation of cubic number fields.

In [35], H. Cohen exhibits parametric continued fractions for some well known number theoretic constants.

The paper [12] by P. Kılıçer, M. Streng which list all CM quartic fields with CM class number one has been published.

The article [14], which gives faster quantum algorithms to compute unit groups of cyclotomic fields has been published in AFRICACRYPT 2023.

Drinfeld modules

Drinfeld modules can be considered as an analogue of elliptic curves when working over a function field over $\mathbb{F}_q$ instead of a number field. The $\mathbb{F}_q$-linearity is a quite important additional feature, which often makes it possible to devise better algorithms. In [34], X. Caruso and Antoine Leudière use this yoga to design fast algorithm for computing the caracteristic polynomials and/or the norm of isogenies between Drinfeld modules over finite fields. With David Ayotte and Joseph Musleh, they also provide the first comprehensive implementation of Drinfeld modules in SAGEMATH [4].

Deformations of Galois representations

X. Caruso, Agnès David and Ariane Mézard continued their study of the potentially Barsotti–Tate deformation rings of a Galois representation. Using the Breuil–Mézard conjecture, they showed in [8] that the *gene* entirely determine the special fibre of those deformation rings. In [25], they investigated the independence of their constructions with respect to the underlying prime number p and propose a new programme of research, that they called the 1-adic Langlands correspondence, for explaining these phenomena.

Algebraic differential equations

Alin Bostan, X .Caruso and Julien Roques wrote a survey [32] on the theory of linear differential equations over number fields and finite fields, focusing on algebraic criteria for the existence of algebraic solutions.

In [27], Boris Adamczewski, Alin Bostan, X. Caruso gave an effective proof of the multivariate version of Christol's theorem about algebraic power series with coefficients in finite fields. This proof allows for sharp effective estimates on the algebraic degree of many functions in positive characteristic, including diagonals of multivariate algebraic power series.

Automorphic forms

In [42], A. Page and B. Wesolowski leverage the theory of automorphic forms (the Jacquet–Langlands correspondence) to prove a powerful equidistribution theorem for graphs of supersingular elliptic curves equipped with extra structure: they introduce a new category-theoretic framework to describe suitable extra structures, prove a generalised Deuring correspondence for these structures (using adélic language), and relate them to structures coming from adélic groups, allowing the use of automorphic tools. The algorithmic and cryptographic consequences are described in Subsection 8.4.

8.2 Algorithms for number theory

Participants: Razvan Barbulescu, Jean-Marc Couveignes.

In [13], Q. Liu gives an algorithm to compute the minimal Weierstrass equation of an hyperelliptic curve over principal ideal domains. This generalizes Tate's algorithm from elliptic curves to hyperelliptic curves.

In [30], R. Barbulescu and F. Jouve use the Elliott-Halberstam conjecture to measure how ECM friendly an elliptic curve with complex multiplication is. The ECM method is a probabilistic integer factorisation method using elliptic curves, the probability of success can be improved by selecting suitable elliptic curves, and this paper investigates ECM friendly elliptic curves.

In [36], J.-M. Couveignes and T. Ezome use the arithmetic and geometry of elliptic curves to study the complexity of multiplication of two elements in a finite field extension given by their coordinates in a normal basis.

8.3 Cryptography

Participants: Guilhem Castagnos, Élie Bouscatié.

In [7], Bouvier, Castagnos, Imbert and Laguillaumie introduce BICYCL, an Open Source C++ library that implements arithmetic in the ideal class groups of imaginary quadratic fields, together with a set of cryptographic primitives based on class groups. It is available at bicycl under the GNU General Public License version 3 or any later version. It provides significant speed-ups on the implementation of the arithmetic of class groups. Concerning cryptographic applications, BICYCL is orders of magnitude faster than any previous implementation of the Castagnos–Laguillaumie linearly homomorphic encryption scheme, making it faster than Paillier's encryption scheme at any security level. Linearly homomorphic encryption is the core of many multi-party computation protocols, sometimes involving a huge number of encryptions and homomorphic evaluations: class group based protocols become the best solution in terms of bandwidth and computational efficiency to rely upon.

Due to their use in crypto-currencies, threshold ECDSA signatures have received much attention in recent years. Though efficient solutions now exist both for the two party, and the full threshold scenario, there is still much room for improvement, be it in terms of protocol functionality, strengthening security or further optimising efficiency.

In the past few months, a range of protocols have been published, allowing for a non interactive – and hence extremely efficient – signing protocol; providing new features, such as identifiable aborts (parties can be held accountable if they cause the protocol to fail), fairness in the honest majority setting (all parties receive output or nobody does) and other properties. In some cases, security is proven in the strong simulation based model. In [10], G. Castagnos, D. Catalano, F. Laguillaumie, F. Savasta and I. Tucker combine ideas from the aforementioned articles with the suggestion of Castagnos *et al.* (PKC 2020) to use the class group based CL framework so as to drastically reduce bandwidth consumption.

Building upon this latter protocol they present a new, maliciously secure, full threshold ECDSA protocol that achieves additional features without sacrificing efficiency. Their most basic protocol boasts a non interactive signature algorithm and identifiable aborts. They also propose a more advanced variant that achieves adaptive security (for the n-out-of-n case) and proactive security. The resulting constructions improve upon state of the art Paillier's based realisations achieving similar goals by up to a 10 factor in bandwidth consumption.

Functional encryption features secret keys, each associated with a key function f, which allow to directly recover $f(x)$ from an encryption of x, without learning anything more about x. This property is particularly useful when delegating data processing to a third party as it allows the latter to perform its task while ensuring minimum data leakage. However, this generic term conceals a great diversity in the cryptographic constructions that strongly differ according to the functions f they support.

A recent series of works has focused on the ability to search a pattern within a data stream, which can be expressed as a function f. One of the conclusions of these works was that this function f was not supported by the current state-of-the-art, which incited their authors to propose a new primitive called Stream Encryption supporting Pattern Matching (SEPM). Some concrete constructions were proposed but with some limitations such as selective security or reliance on non-standard assumptions.

In [16], É. Bouscatié, G. Castagnos and O. Sanders revisit the relations between this primitive and two major subclasses of functional encryption, namely Hidden Vector Encryption (HVE) and Inner Product Encryption (IPE). They indeed first exhibit a generic transformation from HVE to SEPM, which immediately yields new efficient SEPM constructions with better features than existing ones. Then, they revisit the relations between HVE and IPE and show that they can actually do better than the transformation proposed by Katz, Sahai and Waters in their seminal paper on predicate encryption. This allows to fully leverage the vast state-of-the-art on IPE which contains adaptively secure constructions proven under standard assumptions. This results in countless new SEPM constructions, with all the features one can wish for. Beyond that, this work sheds a new light on the relations between IPE schemes and HVE schemes and in particular shows that some of the former are more suitable to construct the latter.

In [6], K. Belabas, T. Kleinjung, A. Sanso and B. Wesolowski show that in some particular class groups of quadratic imaginary orders, it is easier than expected to find elements of low order. This breaks an assumption used for VDF using class groups.

8.4 Isogeny based cryptography

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

The impossibility to hash to supersingular elliptic curves require a trusted setup to build a supersingular elliptic curve with unknown endomorphism ring. In [15], A. Basso, G. Codogni, D. Connolly, L. de Feo, B. Fouotsa, G. Lido, T. Morrison, L. Panny, S. Patranabis, and B. Wesolowski builds SECUER, a multipartite scheme to build such a curve, relying on a zero-knowledge isogeny proof built from pushforward diagrams.

In [19], L. de Feo, A. Leroux, P. Longa and B. Wesolowski improve the SQISign signature scheme by developing a new algorithm for the Deuring correspondance using endomorphisms to refresh the intermediate torsion.

A completely unexpected direction in isogeny based cryptography was the spectacular breaking of SIDH[47] using isogenies in dimension 2. This attack was originally heuristic and applying only to a very special starting curve, but was soon extended by L. Maino, C. Martindale, L. Panny, G. Pope and B. Wesolowski, ini [22] to a subexponential heuristic attack on all curves, and then in [24] by D. Robert to a proved polynomial attack in all cases by moving to dimensions 4 and 8.

Moving to higher dimension allows considerable flexibility in manipulating isogenies, thanks to the following embedding lemma proved in [24] using earlier work by Zarhin [50] and Kani [49]: For every $N' \geqslant N$, an N-isogeny f in dimension g can be embedded into an N'-isogeny F in dimension $8g$ (and sometimes $4g$ or $2g$).

This powerful tool soon led the way to new algorithms. In [43], D. Robert proves that every isogeny admits an efficient representation, which allows for evaluation in polynomial time (in the logarithm of its degree). And in [44], he proves that the endomorphism ring of an ordinary elliptic curve can be computed in polynomial time given the factorisation of its conductor, and that canonical lifts of ordinary elliptic curves can be computed in polynomial time (among others). Such powerful results were completely unexpected (the previous best algorithms being subexponential time). This lead to a new point counting algorithm for elliptic curve $E/\mathbb{F}_{p^n}$, in $\tilde{O}(n^2 \log^8 p + n \log^{11} p)$.

These new algorithms in turn led to new cryptosystems, using higher dimensional cryptography as a fundamental block. In [38], P. Dartois, A. Leroux, D. Robert and B. Wesolowski present the SQISignHD protocol, which has a much cleaner security proof than SQISign, even more compact signatures, and much faster signing times. The verification uses a 2^n-isogeny in dimension 4; such high degree smooth isogenies had never been computed until now.

With the rise of higher dimensional cryptography, optimising the speed of 2^n-isogenies is of paramount importance. The case of dimension 2 is tackled in [39] by P. Dartois, L. Maino, G. Pope and D. Robert, using optimised theta duplication formula to speed up 2^n-isogenies between product of two elliptic curves. Our SageMath implementation gains a factor 10 compared to using Richelot isogenies, and our low level Rust implementation a factor up to 40. In [17], T. Decru and S. Kunzweiler give faster formula for 3^n-isogenies in dimension two on the Jacobian model. The general case, by D. Lubicz and D. Robert of an arbitrary isogeny in any dimension has been published in [21].

In [29], S. Arpin, C. James, P. Dartois, J. Eriksen, K. Jonathan, P. Kutas, and B. Wesolowski, prove that the computing an orientation reduces in subexponential time to he equivalent decision problem.

In [42], A. Page and B. Wesolowski prove another algorithmic reduction, showing that being able to find a single endomorphism of an arbitrary supersingular elliptic curve is no easier than being able to find the entire endomorphism ring. As applications, they prove the collision-resistance of the CGL hash function and the soundness of the SQIsign identification scheme, under the standard assumption of hardness of the endomorphism ring problem.

In [20], L. Feo, B. Fouotsa, P. Kutas, A. Leroux, S. Merz, L. Panny, and B. Wesolowski introduce SCALLOP, a new commutative action isogeny scheme using orientations of supersingular elliptic curve. The idea is

to build up an orientation by a quadratic order of large prime conductor to speed up computing the class group relations.

In [41], A. Page and D. Robert introduce Clapoti(s), a new algorithm to compute the class group action on an oriented elliptic curve in polynomial time. This solves a long standing problem in isogeny based cryptography: all existing algorithms were asymptotically subexponential.

8.5 Pairings

Participants: Damien Robert.

In [45], D. Robert gives a geometric interpretation of the Tate pairing on abelian varieties. This interpretation shows that the Tate pairing can be used to probe the Galois structure of the isogenous abelian variety, generalising some ad-hoc construction in the literature. It also solves a conjecture by Castryck and Decru on multiradical isogenies.

In [40], J. Gasnier and A. Guillevic revisit the generation of pairing friendly curves from an algebraic point of view.

8.6 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. J. Bos, O. Bronchain,L. Ducas, S. Fehr, Y. Huang, T. Pornin, E. Postlethwaite, T. Prest, L. Pulles, and W. van Woerden submitted the Hawk signature scheme to this standardization process, which is based on the article [48] by L. Ducas, E. Postlethwaite, T. Prest, L. Pulles, and W. van Woerden.

The security of most cryptographic schemes based on lattices relies on the hardness of computing short vectors in lattices. Very often, the lattices in question enjoy some additional properties, which makes the cryptographic schemes based on them more efficient. An important question is then to understand how hard is the problem of finding short vectors in these lattice, which enjoy some additional structure.

A very common way to add structure to a lattice is to consider module lattices, that is, lattices that are also $\mathcal{O}_K$-modules in some K^m, where K is a number field and $\mathcal{O}_K$ is its ring of integers. Some of these modules may be free, meaning that they possess a basis, but most of them are not (they are finitely generated, but it is not possible to obtain a basis from a generating set). In [23], G. De Micheli, D. Micciancio, A. Pellet-Mary and N. Tran showed that computing a short vector in *free* modules is as hard as computing a short vector in any module: if we have a polynomial time algorithm computing short vectors when given as input any *free* module, then there is a polynomial time algorithm computing short vectors when given as input any module (not necessarily free).

A special case of module lattices are ideal lattices, which are modules of rank $m = 1$ (they live in K). In [18], J. Felderhoff, A. Pellet-Mary, D. Stehlé, and B. Wesolowski proved a quantum reduction from finding short vectors in all ideals of a number field K, to finding short vectors in random prime ideals of small algebraic norm in the same field K. In other words, if finding short vectors in ideal lattices of K is quantumly hard in the worst-case (i.e., there is no quantum algorithm solving this problem efficiently on all inputs), then finding a short vector in a uniformly chosen prime ideal of small algebraic norm is also hard.

8.7 Coding theory

[2] NIST's call

Participants: Xavier Caruso, Jean-Marc Couveignes, Fabrice Drain, Amaury Durand, Jean Gasnier.

X. Caruso continued his work towards the development of coding theory in the sum-rank metric context. With A. Durand [9], he described the duals of Martinez-Penas' linearized Reed–Solomon codes. In collaboration with Elena Berardini [31], he introduced a linearized version of Algebraic Geometry codes and studied its parameters; in particular, they showed that the codes they introduced beat the (sum-rank analogue of the) Gilbert–Varshamov bound.

In [33], 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.

Effective geometry of curves and applications

In [37], J.-M. Couveignes and J. Gasnier study the effective aspects of group actions on algebraic curves and more precisely the $K[G]$-structure of the linear spaces associated to equivariant divisors. They find simple criteria for such a space of sections to be a free $K[G]$-module. In case G is abelian, freeness is granted under mild conditions. This results in a much more compact representation of these spaces and more efficient ways of computing them. Over finite fields, abelian covers with large Galois groups are classified by geometric class field theory. Algorithms and existence results presented in this work provide efficient decompositions of the multiplication tensor in finite field extensions and also good geometric codes that can be encoded and decoded efficiently. In particular, excellent codes are constructed that can be encoded in quasilinear time and decoded in quasiquadratic time.

8.8 Analysis

Participants: Anne-Edgar Wilke.

In [46], A.-E. Wilke makes the analogy between between convexity and plurisubharmonicity in Banach spaces more precise.

8.9 Effective analysis and certified arithmetic

Participants: Fredrik Johansson.

In [11], F. Johansson presents improved algorithms for arbitrary-precision computation of the gamma function and related classical special functions.

9 Partnerships and cooperations

9.1 International research visitors

9.1.1 Visits of international scientists

Other international visits to the team

- Wouter Castryck, from KU Leuven (Belgium), visited the team for 2 weeks in January 2023.

The following international researchers have given a presentation in the CANARI team seminar:

- Wouter Castryck (KU Leuven, Belgium)
- Donghyeok Lim (Yonsei University, Korea)

- Maxime Bombar (CWI)
- Stefano Marseglia (Utrecht University)
- Lorenzo Furio (Università di Pisa)
- Monika Trimoska (Eindhoven University of Technology)
- Yining Hu (Harbin Institute of Technology)
- Marc Houben (Leiden University)

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€

ANR ClapClap Correspondance de Langlands p-adique: une approche constructive et algorithmique (PI X. Caruso)
with ENS Lyon, Paris Rive Gauche, Rennes
2019–2023, 198 k€

ANR Flair Familles de fonctions L: analyse, interactions, résultats effectifs
with Besançon
2017–2021

10 Dissemination

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

10.1 Promoting scientific activities

10.1.1 Scientific events: organisation

Member of the organizing committees

- B. Allombert was an organiser of the COUNT conference at CIRM (Luminy, France).

10.1.2 Scientific events: selection

Member of the conference program committees

- A. Page
  - LMFDB, Computation, and Number Theory – LuCaNT 2023
- A. Pellet--Mary
  - Public Key Cryptography – PKC 2023
  - Asiacrypt 2023

10.1.3 Journal

Member of the editorial boards

- K. Belabas is an editor of *Archiv der Mathematik* since 2006.
- X. Caruso is an editor and one of the founders of the journal *Annales Henri Lebesgue*.
- 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.

10.1.4 Invited talks

- J.-M. Couveignes
  - *The algebraic complexity of multiplication in finite field extensions*, plenary talk, Explicit methods in automorphic forms and arithmetic geometry, (Dublin 2023).
- F. Johansson
  - *Computing special functions using integral representations*, at *Recent Trends in Computer Algebra* (Lyon, 2023).
  - *The practical complexity of arbitrary-precision functions*, at *Recent Trends in Computer Algebra* (Paris, 2023).
- A. Page
  - PARI/GP*, playing the L-functions game of number theorists* at the workshop *Recent Trends in Computer Algebra* (Lyon, 2023).
- D. Robert
  - *Arithmetic and pairings on Kummer lines*, Leuven isogeny days 4 (Leuven, October 2023).
  - *Efficient representation of isogenies*, EWHA-KMS International Workshop on Cryptography (Korea, July 2023).
  - *Applications of isogenies between abelian varieties to elliptic curves*, Arithmétique en Plat Pays (Leuven, March 2023) and VaNTAGe Seminar (Online, December 2022).
- A. Pellet--Mary
  - *Lattices in cryptography: cryptanalysis, constructions and reductions.* Journées Code et Cryptographie 2023 (Najac, October 2023).

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.
- K. Belabas was member of the scientific board of the Société Mathématique de France from 2017 to 2023.
- X. Caruso is vice-head of *Institut de Mathématiques de Bordeaux*, in charge of the IT department.
- X. Caruso was member of the *Comité National des Universités* from 2020 to 2023.
- 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.
- G. Castagnos was responsible for the bachelor programme in mathematics and informatics of the University of Bordeaux since 2018 to 2023.

10.2 Teaching - Supervision - Juries

- 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
  - mini-course on p-adic random polynomials at the 12th Swiss-French Workshop in Algebraic Geometry (Charmey, 2023)
- G. Castagnos and D. Robert
  - 60h course on elliptic curve cryptography, Master 2, University of Bordeaux
- G. Castagnos
  - 60h course on cryptanalysis, 30h on advanced cryptography, Master 2, University of Bordeaux
  - 24h course on arithmetic and cryptography, 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

10.2.1 Supervision

- PhD: Élie Bouscatié, *Conception d'algorithmes de chiffrement cherchable*, defended December 2023, supervised by G. Castagnos
- 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 analysys 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: Raphaël Pagès, *Factorization of differential operators in positive characteristic*, since September 2020, supervised by Alin Bostan and Xavier Caruso.

- 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.

10.2.2 Juries

- D. Robert
  - Sulamithe Tsakou, Université de Picardie Jules Verne, 2023: *Algebraic cryptanalysis of hyperelliptic curves based cryptosystems* (report)
- B. Allombert
  - Valentin Petit, Université de Franche-Comté, 2023: *Points spéciaux et modularité des courbes elliptiques définies sur* $\mathbb{Q}$ *et* $\mathbb{F}_q(T)$ (committee)
- G. Castagnos
  - Chloé Gravouil, Université Rennes 1, 2023: *Boolean Fault-Resistant Masking and White-Boxability of Lightweight Cryptography* (report)
  - Anaïs Barthoulot, Université de Limoges, 2023: *Advanced Encryption for the Sharing of Sensitive Data* (report)
- J.-M. Couveignes
  - Béranger Séguin, Université de Lille, 2023: *Geometry and Arithmetic of Components of Hurwitz Spaces* (report)
  - Eddy Brandon, Université de Dijon, 2023: *Computational Approach to the Schottky Problem* (committee)

10.3 Popularization

10.3.1 Internal or external Inria responsibilities

R. Barbulescu organises each year the contest Alkindi and the TFJM^2 (*Tournoi des Jeunes Mathématiciennes et Mathématiciens*).

X. Caruso was in charge of the dissemination at *Institut Mathématique de Bordeaux* until 2023; he was then replaced by R. Barbulescu.

10.3.2 Education

A. Pellet--Mary participated as a lecturer to two CIMPA schools on post-quantum cryptography (in Rabat in october, and in Pondicherry in December).

A. Page gave a talk about cryptography for high school teachers during the IREM conference in Bordeaux in 2023.

10.3.3 Interventions

X. Caruso and A. Pellet--Mary moderated a workshop at the event *Les échappées inattendues* (organized by the local delegation of CNRS).

X. Caruso realised an art exhibition on mathematics, see exth.

X. Caruso animated a general audience conference and a *Rencontre à l'heure du thé* (meeting at tea time) at Maison Poincaré in Paris.

X. Caruso coordinated a workshop *Regard de géomètre* (five interventions in a high school) and gave a talk for the final conference of this program.

A. Pellet--Mary animated a workshop during the week *moi informaticienne moi mathématicienne* for high school female students.

A. Page gave general audience talks about cryptography during the *Fête de la Science* event (4 groups of high-school students).

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] 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.

[3] 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

[4] D. Ayotte, X. Caruso, A. Leudière and J. Musleh. 'Drinfeld modules in SageMath'. In: *ACM Communications in Computer Algebra* 57.2 (June 2023), pp. 65–71. DOI: 10.1145/3614408.3614417. URL: https://hal.science/hal-04086308.

[5] K. Belabas, F. Diaz y Diaz and E. Friedman. 'Special values of ray class partial zeta functions'. In: *International Journal of Number Theory* 19.03 (Apr. 2023), pp. 481–493. DOI: 10.1142/S1793042123500227. URL: https://hal.science/hal-04046224.

[6] K. Belabas, T. Kleinjung, A. Sanso and B. Wesolowski. 'A note on the low order assumption in class groups of imaginary quadratic number fields'. In: *Mathematical Cryptology* 3.1 (2023), pp. 44–51. URL: https://hal.science/hal-04174483.

[7] C. Bouvier, G. Castagnos, L. Imbert and F. Laguillaumie. 'I want to ride my BICYCL: BICYCL Implements CryptographY in CLass groups'. In: *Journal of Cryptology* 36.3 (July 2023), p. 17. DOI: 10.1007/s00145-023-09459-1. URL: https://hal-lirmm.ccsd.cnrs.fr/lirmm-03863678.

[8] X. Caruso, A. David and A. Mézard. 'Combinatorics of Serre weights in the potentially Barsotti-Tate setting'. In: *Moscow Journal of Combinatorics and Number Theory* 12.1 (2023), pp. 1–56. DOI: 10.2140/moscow.2023.12.1. URL: https://cnrs.hal.science/hal-03221168.

[9] X. Caruso and A. Durand. 'Duals of linearized Reed-Solomon codes'. In: *Designs, Codes and Cryptography* 91.1 (2023), pp. 241–271. DOI: 10.1007/s10623-022-01102-7. URL: https://hal.science/hal-03395402.

[10] G. Castagnos, D. Catalano, F. Laguillaumie, F. Savasta and I. Tucker. 'Bandwidth-efficient threshold EC-DSA revisited: Online/Offline Extensions, Identifiable Aborts Proactive and Adaptive Security'. In: *Theoretical Computer Science* 939 (2023), pp. 78–104. DOI: 10.1016/j.tcs.2022.10.016. URL: https://hal.science/hal-03927198.

[11] F. Johansson. 'Arbitrary-precision computation of the gamma function'. In: *Maple Transactions* 3.1 (1st Feb. 2023). DOI: 10.5206/mt.v3i1.14591. URL: https://inria.hal.science/hal-03346642.

[12] P. Kılıçer and M. Streng. 'The CM class number one problem for curves of genus 2'. In: *Research in Number Theory* 9.1 (Mar. 2023), article 15. DOI: 10.1007/s40993-022-00417-7. URL: https://inria.hal.science/hal-01248630.

[13] Q. Liu. 'Computing minimal Weierstrass equations of hyperelliptic curves'. In: *Research in Number Theory* 9.4 (31st Oct. 2023), p. 76. DOI: 10.1007/s40993-023-00483-5. URL: https://hal.science/hal-04415457.

International peer-reviewed conferences

[14] R. Barbulescu and A. Poulalion. 'The special case of cyclotomic fields in quantum algorithms for unit groups'. In: *Progress in cryptology – AFRICACRYPT 2023Lecture notes in computer science (LNCS)*. AFRICACRYPT 2023. Vol. 14064. Progress in Cryptology – AFRICACRYPT 2023. Soussa, Tunisia: Springer, 21st July 2023, p. 229. URL: https://hal.science/hal-04012986.

[15] A. Basso, G. Codogni, D. Connolly, L. de Feo, T. B. Fouotsa, G. M. Lido, T. Morrison, L. Panny, S. Patranabis and B. Wesolowski. 'Supersingular Curves You Can Trust'. In: Eurocrypt 2023. Lyon, France, 23rd Apr. 2023. URL: https://inria.hal.science/hal-04052486.

[16] É. Bouscatié, G. Castagnos and O. Sanders. 'Pattern Matching in Encrypted Stream from Inner Product Encryption'. In: *Lecture Notes in Computer Science*. PKC 2023 - 26th IACR International Conference on Practice and Theory of Public-Key Cryptography. Vol. 13940. Public-Key Cryptography – PKC 2023. Atlanta (Georgia), United States: Springer Nature Switzerland, 2nd May 2023, pp. 774–801. DOI: 10.1007/978-3-031-31368-4_27. URL: https://inria.hal.science/hal-04087741.

[17] T. Decru and S. Kunzweiler. 'Efficient Computation of $(3^n,3^n)$-Isogenies'. In: *Lecture Notes in Computer Science*. AfricaCrypt 2023. Vol. 14064. Lecture Notes in Computer Science. Sousse, Tunisia, 13th July 2023, pp. 53–78. DOI: 10.1007/978-3-031-37679-5_3. URL: https://hal.science/hal-04098198.

[18] J. Felderhoff, A. Pellet-Mary, D. Stehlé and B. Wesolowski. 'Ideal-SVP is Hard for Small-Norm Uniform Prime Ideals'. In: *Lecture Notes in Computer Science*. Theory of Cryptography, TCC 2023. Vol. 14372. Lecture Notes in Computer Science. Taipei (Taiwan), Taiwan: Springer Nature Switzerland, 27th Nov. 2023, pp. 63–92. DOI: 10.1007/978-3-031-48624-1_3. URL: https://hal.science/hal-04326750.

[19] L. de Feo, A. Leroux, P. Longa and B. Wesolowski. 'New algorithms for the Deuring correspondence Towards practical and secure SQISign signatures'. In: Eurocrypt 2023. Lyon, France, 23rd Apr. 2023. URL: https://inria.hal.science/hal-04052502.

[20] L. D. Feo, T. B. Fouotsa, P. Kutas, A. Leroux, S.-P. Merz, L. Panny and B. Wesolowski. 'SCALLOP: scaling the CSI-FiSh'. In: PKC 2023. Vol. 13940. Lecture Notes in Computer Science. Atlanta, United States: Springer Nature Switzerland, 2nd May 2023, pp. 345–375. DOI: 10.1007/978-3-031-31368-4_13. URL: https://inria.hal.science/hal-04052532.

[21] D. Lubicz and D. Robert. 'Fast change of level and applications to isogenies'. In: *Research in Number Theory*. ANTS 2022 - Fifteenth Algorithmic Number Theory Symposium. Vol. 9. 1. Bristol, United Kingdom, 2023, article n°7. DOI: 10.1007/s40993-022-00407-9. URL: https://inria.hal.science/hal-03738315.

[22] L. Maino, C. Martindale, L. Panny, G. Pope and B. Wesolowski. 'A Direct Key Recovery Attack on SIDH'. In: Advances in Cryptology – EUROCRYPT 2023. Vol. 14008. Lecture Notes in Computer Science. Lyon, France: Springer Nature Switzerland; Springer Nature Switzerland, 16th Apr. 2023, pp. 448–471. DOI: 10.1007/978-3-031-30589-4_16. URL: https://hal.science/hal-04023441.

[23] G. de Micheli, D. Micciancio, A. Pellet-Mary and N. Tran. 'Reductions from Module Lattices to Free Module Lattices, and Application to Dequantizing Module-LLL'. In: *Advances in Cryptology – CRYPTO 2023*. Crypto 2023. Vol. 14085. Lecture Notes in Computer Science. Santa Barbara, United States: Springer Nature Switzerland, 9th Aug. 2023, pp. 836–865. DOI: 10.1007/978-3-031-38554-4_27. URL: https://hal.science/hal-04284684.

[24] D. Robert. 'Breaking SIDH in polynomial time'. In: Advances in Cryptology – EUROCRYPT 2023. Vol. 14008. Lecture Notes in Computer Science. Lyon, France: Springer Nature Switzerland; 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.

Scientific book chapters

[25] 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.

[26] 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.

Reports & preprints

[27] B. Adamczewski, A. Bostan and X. Caruso. *A sharper multivariate Christol's theorem with applications to diagonals and Hadamard products*. 5th June 2023. URL: https://hal.science/hal-04116793.

[28] B. Allombert and D. C. Mayer. *Cyclic cubic number fields with harmonically balanced capitulation*. 5th Dec. 2023. URL: https://inria.hal.science/hal-04324884.

[29] S. Arpin, J. Clements, P. Dartois, J. K. Eriksen, P. Kutas and B. Wesolowski. *Finding Orientations of Supersingular Elliptic Curves and Quaternion Orders*. 2023. DOI: 10.48550/arXiv.2308.11539. URL: https://hal.science/hal-04186188.

[30] R. Barbulescu and F. Jouve. *ECM And The Elliott-Halberstam Conjecture For Quadratic Fields*. Jan. 2023. URL: https://hal.science/hal-03485435.

[31] E. Berardini and X. Caruso. *Algebraic Geometry codes in the sum-rank metric*. 15th Mar. 2023. URL: https://hal.science/hal-04034810.

[32] A. Bostan, X. Caruso and J. Roques. *Algebraic solutions of linear differential equations: an arithmetic approach*. 11th Apr. 2023. URL: https://hal.science/hal-04065092.

[33] X. Caruso and F. Drain. *Selfdual skew cyclic codes*. 13th June 2023. URL: https://hal.science/hal-04127001.

[34] X. Caruso and A. Leudière. *Algorithms for computing norms and characteristic polynomials on general Drinfeld modules*. 11th Dec. 2023. URL: https://hal.science/hal-04151171.

[35] H. Cohen. *Parametric Continued Fractions for π^2, $\zeta(3)$, and other Constants*. 23rd Apr. 2023. URL: https://inria.hal.science/hal-04223108.

[36] J.-M. Couveignes and T. Ezome. *The equivariant complexity of multiplication in finite field extensions*. 11th Jan. 2023. URL: https://hal.science/hal-03410146.

[37] J.-M. Couveignes and J. Gasnier. *Explicit Riemann-Roch spaces in the Hilbert class field*. 13th Sept. 2023. URL: https://hal.science/hal-04219975.

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

[39] 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*. 21st Nov. 2023. URL: https://hal.science/hal-04297088.

[40] J. Gasnier and A. Guillevic. *An Algebraic Point of View on the Generation of Pairing-Friendly Curves*. 13th Sept. 2023. URL: https://hal.science/hal-04205681.

[41] A. Page and D. Robert. *Introducing Clapoti(s): Evaluating the isogeny class group action in polynomial time*. 15th Nov. 2023. URL: https://hal.science/hal-04327451.

[42] A. Page and B. Wesolowski. *The supersingular Endomorphism Ring and One Endomorphism problems are equivalent*. 10th Oct. 2023. URL: https://inria.hal.science/hal-04209824.

[43] D. Robert. *Evaluating isogenies in polylogarithmic time*. 2023. URL: https://hal.science/hal-03943970.

[44] D. Robert. *Some applications of higher dimensional isogenies to elliptic curves (overview of results)*. 2023. URL: https://hal.science/hal-03943973.

[45] D. Robert. *The geometric interpretation of the Tate pairing and its applications*. 20th Nov. 2023. URL: https://hal.science/hal-04295743.

[46] A.-E. Wilke. *Convexity, plurisubharmonicity and the strong maximum modulus principle in Banach spaces*. 7th Sept. 2023. URL: https://hal.science/hal-03826538.

11.3 Cited publications

[47] W. Castryck and T. Decru. 'An efficient key recovery attack on SIDH'. In: *Annual International Conference on the Theory and Applications of Cryptographic Techniques*. Springer. 2023, pp. 423–447.

[48] L. Ducas, E. W. Postlethwaite, L. N. Pulles and W. v. Woerden. 'Hawk: Module LIP makes lattice signatures fast, compact and simple'. In: *International Conference on the Theory and Application of Cryptology and Information Security*. Springer. 2022, pp. 65–94.

[49] E. Kani. 'The number of curves of genus two with elliptic differentials.' In: *Journal für die reine und angewandte Mathematik* 485 (1997), pp. 93–122.

[50] J. G. Zarhin. 'A remark on endomorphisms of abelian varieties over function fields of finite characteristic'. In: *Mathematics of the USSR-Izvestiya* 8.3 (1974), p. 477.