RESEARCH CENTRE

Inria Centre
at Université de Lorraine

IN PARTNERSHIP WITH:

Université de Lorraine, CNRS

2023
ACTIVITY REPORT

Project-Team

CARAMBA

Cryptology, arithmetic : algebraic methods for better algorithms

IN COLLABORATION WITH: Laboratoire lorrain de recherche en informatique et ses applications (LORIA)

DOMAIN

Algorithmics, Programming, Software and Architecture

THEME

Algorithmics, Computer Algebra and Cryptology

Contents

Project-Team CARAMBA

Creation of the Project-Team: 2016 September 01

Keywords

Computer sciences and digital sciences

A1.1.2. – Hardware accelerators (GPGPU, FPGA, etc.)

A4.3.1. – Public key cryptography

A4.3.2. – Secret key cryptography

A4.8. – Privacy-enhancing technologies

A6.2.7. – High performance computing

A7.1. – Algorithms

A7.1.4. – Quantum algorithms

A8.4. – Computer Algebra

A8.5. – Number theory

A8.10. – Computer arithmetic

Other research topics and application domains

B8.5. – Smart society

B9.5.1. – Computer science

B9.5.2. – Mathematics

B9.10. – Privacy

1 Team members, visitors, external collaborators

Research Scientists

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

Faculty Members

- Sébastien Duval [UL, Associate Professor]
- Marine Minier [UL, Professor Delegation, HDR]

Post-Doctoral Fellows

- Paul Frixons [INRIA, Post-Doctoral Fellow]
- Loïc Rouquette [UL, Post-Doctoral Fellow, until Aug 2023]

PhD Students

- Haetham Al Aswad [INRIA]
- Marie Bolzer [CNRS, from Oct 2023]
- Medhi Kermaoui [INRIA, from Oct 2023]
- Antoine Leudière [INRIA]
- Léo Louistisserand [CNRS, from Oct 2023, (with PESTO team)]
- Ana Rodriguez Cordero [UL]
- Julien Soumier [INRIA, from Oct 2023]
- Quentin Yang [INRIA, until Sep 2023]

Interns and Apprentices

- Marie Bolzer [CNRS, Intern, from Feb 2023 until Aug 2023, M2 internship]
- Fatou Diao [UL, Intern, from Feb 2023 until Aug 2023, M2 internship]
- Mathis Georgel [UL, Intern, from May 2023 until Jun 2023]
- Medhi Kermaoui [INRIA, Intern, from Apr 2023 until Sep 2023, M2 internship]
- Kevin Lodovici [UL, Intern, from May 2023 until Jul 2023]
- Victor Matrat [UL, Intern, from Oct 2023]

- Tristan Parcollet [UL, Intern, from Jun 2023 until Aug 2023]
- Joseph Schlesinger [UL, Intern, from May 2023 until Jun 2023]
- Julien Soumier [INRIA, Intern, from Mar 2023 until Sep 2023, M2 internship]
- Lucas Villaume [UL, Intern, from Apr 2023 until Jul 2023]

Administrative Assistants

- Virginie Colnet [CNRS]
- Emmanuelle Deschamps [INRIA]

2 Overall objectives

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

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

A second part of our work (axes §3.2 and §3.3) is centered on cryptographic motivations. Quite often, our work here happens to be rooted in exactly the same core competences as the ones we use in our first research axis. We consider the two facets of cryptology: cryptography and cryptanalysis. The key challenges are the assessment of the classical and quantum security of proposed cryptographic primitives (both public- and secret-key), as well as the introduction of new cryptographic primitives, or the performance improvement of existing ones. While the basic principles of symmetric and asymmetric cryptography are rather different—indeed their names indicate different ways to handle the key—research in both domains is led by the same objective of finding the best trade-offs between efficiency and security. In addition to this, both require to study design and analysis together as these two aspects nurture each other.

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

3 Research program

3.1 Research axis 1: mathematical objects

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

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

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

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

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

- We develop algorithms and software for the computation of essential properties of algebraic curves and abelian varieties like group structure, characteristic polynomials, rings of endomorphisms, or Riemann-Roch spaces. This perspective towards effective algebra is also found in our interest in sparse polynomial systems, with a particular eye towards the specificities of their monomial structure. We explore possible ways to exploit this monomial structure in order to obtain faster algorithms for the computation of Gröbner bases.

Examples of publications in the recent past that illustrate our positioning on this research topic are [13, 35, 29, 7].

3.2 Research axis 2: secret-key cryptology

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

- We work on the formalization of various statistical cryptanalysis techniques, starting with boomerang attacks on which we recently gained strong expertise. We aim to properly define how to build such distinguishers and how to estimate their probability, two central points for cryptanalysts. We intend to explore the potential of alternative techniques, such as differential-linear attacks for instance, to attack the most recent cipher primitives (such as the NIST lightweight AEAD ciphers, as well as others at various stages of their development).

- Beyond the classical linear and differential cryptanalysis techniques, we are interested in the automation of the analysis process by the development of tools based on constraint programming (CP), satisfiability (SAT) or mixed integer linear programming (MILP) settings.

- We also study new designs, and in particular new building blocks for future cryptographic primitives with design criteria that include resistance to advanced cryptanalysis techniques, using minimal resources.

- With the current progress of quantum computing, we need to know the security of cryptosystems against a quantum computer, especially for long-term security. Hence, we study quantum cryptanalysis. We focus on quantum algorithms that are the most distinct from classical algorithms, like the algorithms for the hidden subgroup problem, and on quantum variants of our classical cryptanalyses. This research direction is also connected to public-key cryptography.

Examples of publications in the recent past that illustrate our positioning on this research topic are [1, 2, 11, 16, 9].

3.3 Research axis 3: public-key cryptographic primitives

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

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

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

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

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

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

Examples of publications in the recent past that illustrate our positioning on this research topic are [3, 12, 8], as well as the Cado-NFS software described in 6.1.2.

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

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

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

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

Examples of publications in the recent past that illustrate our positioning on this research topic are [5, 6, 4, 10].

4 Application domains

4.1 Better awareness and avoidance of cryptanalytic threats

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

The software we make available to achieve these cryptanalytic computations also allows us to give cost estimates for potential attacks on cryptographic systems that are taking the security/efficiency/legacy compatibility trade-offs too lightly. Attacks such as LogJam [41] are understood as being serious concerns thanks to our convincing proof-of-concepts. In the LogJam context, this impact has led to rapid worldwide security advisories and software updates that eventually defeat some potential intelligence threats and improve the confidentiality of communications.

4.2 Promotion of better cryptography

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

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

4.3 Key software tools

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

[1] In [42], the minimal recommended RSA key size is 2048 bits for usage up to 2030. See also Annex B, in particular Section B.1 "Records de calculs cryptographiques".

[2] The work [43] is one of only two academic works cited by NIST in the initial version (2011) of the report [47].

We also develop more specialized software. Our flagship software package is Cado-NFS [48], and we also develop some others with various levels of maturity, such as GMP-ECM, CMH, or Belenios, aiming at quite diverse targets. Within the lifespan of the CARAMBA project, we expect more software packages of this kind to be developed, specialized towards tasks relevant to our research targets: important mathematical structures attached to genus 2 curves, generation of cryptographically secure curves, or tools for attacking cryptographically hard problems. Such software both illustrates our algorithms, and provides a base on which further research work can be established. Because of the very nature of these specialized software packages as research topics in their own right, needing both to borrow material from other projects, and being possible sources of inspiring material for others, it is again important that these be developed in a free and open-source development model.

5 Highlights of the year

The CORE-MATH project reached a significant milestone in 2023, with correctly rounded implementations of all mathematical functions in C99 and C23, in double precision.

5.1 Awards

Véronique Cortier (team PESTO) and Pierrick Gaudry were awarded the Grand Prix de l'Académie Lorraine des Sciences for their book entitled *Le vote électronique* [5].

6 New software, platforms, open data

6.1 New software

6.1.1 Belenios

Name: Belenios - Verifiable online voting system

Keyword: E-voting

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

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

Belenios is available in several languages for the voters as well as the administrators of an election. More languages can be freely added by users.

News of the Year: In 2023, our platform was used to run about 1500 elections, with about 175,000 registered voters and 55,000 ballots counted.

Some of the improvements made during this year are invisible for users. This includes the use of elliptic curves instead of finite fields, as a base group where the discrete logarithm problem is supposed to be hard. Also, some modifications have been made, so that the server can handle larger elections. This was successfully tested, with a real election of more than 30,000 voters.

Other changes are visible to users. A new election administration interface based on a REST API is now available for beta-testing to the users. Also, the voter's journey has been slightly simplified, without impact on security. Finally, the STV counting system for preferential voting is now fully supported.

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

Contact: Stéphane Glondu

Participants: Pierrick Gaudry, Stéphane Glondu, Véronique Cortier

Partners: CNRS, Inria

6.1.2 CADO-NFS

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

Keywords: Cryptography, Number theory

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

News of the Year: In 2023, we worked on implementing in Cado-NFS some of the ideas planned in the context of the Kleptomaniac ANR project. In particular, the "double-matrix" feature is under active development. We also worked on removing the dependency on the MPFQ software library, which we are no longer developing, in favor of a more maintainable approach.

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

Contact: Emmanuel Thomé

Participants: Pierrick Gaudry, Emmanuel Thomé, Paul Zimmermann

6.1.3 Drinfeld modules in SageMath

Keywords: Computer algebra, Number theory

Functional Description: This project is an implementation, starting from scratch, of Drinfeld modules in SageMath. This module has been directly merged into SageMath with version 10.0, and keeps evolving.

Drinfeld modules are mathematical objects similar to elliptic curves, but in another setting, which is that of function fields.

The aim of this implementation is to provide researchers with all basic computational tools for Drinfeld modules, and to build a reliable basis for future, more sophisticated algorithms.

URL: https://github.com/sagemath/sage/pull/35026

Contact: Antoine Leudière

Participant: Antoine Leudière

6.1.4 TNFS-alpha

Name: alpha for the Tower Number Field Sieve algorithm

Keyword: Cryptography

Functional Description: This library implements a simulation tool for the tower number field sieve algorithm computing discrete logarithms in extension fields of small degree (tested up to 54). The library contains an implementation of the exact computation of alpha, the bias between the expected smoothness of an integer and the expected smoothness of a norm of an algebraic integer in a number field made of two extensions. The algorithm is a generalization to extensions of the exact implementation of alpha in the software CADO-NFS. The software contains an implementation of the E-function of B. A. Murphy (Murphy's E) which estimates the quality of the polynomial selection step in TNFS through a simulation of the yield of the relation collection in the TNFS algorithm. Finally it contains a database of pairing-friendly curve seeds with the estimated level of security w.r.t a discrete logarithm computation in the corresponding finite field.

URL: https://gitlab.inria.fr/tnfs-alpha/alpha

Publications: hal-03667798, hal-03371573, hal-02263098, hal-02396352

Contact: Aurore Guillevic

Participant: Aurore Guillevic

6.1.5 CORE-MATH

Name: CORE-MATH

Keywords: Arithmetic code, Floating-point, Correct Rounding

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

News of the Year: In 2023, all double-precision (binary64) functions from the C99 and C23 standards were designed with correct-rounding. These first implementations compete well in efficiency with the GNU libc or the Intel math library, which are not correctly rounded.

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

Publication: hal-03721525

Contact: Paul Zimmermann

Participant: Paul Zimmermann

6.1.6 GNU-MPFR

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

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

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

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

Contact: Vincent Lefèvre

Participants: Guillaume Hanrot, Paul Zimmermann, Philippe Théveny, Vincent Lefèvre

7 New results

7.1 Mathematical objects

7.1.1 The CORE-MATH project

Participants: Paul Zimmermann.

The aim of the CORE-MATH project is to provide on-the-shelf open-source mathematical functions with correct rounding that will be integrated into current mathematical libraries (GNU libc, Intel Math Library, AMD Libm, Newlib, OpenLibm, Musl, Apple Libm, llvm-libc, CUDA libm, ROCm). These functions are implemented in the C language and target the three IEEE 754 binary formats (single precision, double precision, quadruple precision), and also the extended double precision (significand of 64 bits). This project is motivated by the fact that current mathematical libraries are far from giving the best possible results, as demonstrated in [34].

The development of CORE-MATH forced us to revisit some classical algorithms, for example FastTwoSum in the context of directed rounding [37]. In 2023, a full set of binary64 (double-precision) functions for the C99 and C23 standards was developed, with correct-rounding, and efficiency close to that of the current mathematical libraries (GNU libc, Intel mathematical library, LLVM). In particular, efficient algorithms were designed and implemented for the power function [24]. The long version of this article with full proofs is available [35], which enabled our colleagues Laurent Théry and Laurence Rideau (Inria Sophia-Antipolis) to make a formal proof of the "fast path".

7.1.2 Computing norms and characteristic polynomials on Drinfeld modules

Participants: Antoine Leudière.

Drinfeld modules are mathematical objects that lie at the intersection of number theory and computer science. They were introduced by Vladimir Drinfeld in 1974 to be the counterpart of *elliptic curves* in the setting of *function fields*. Drinfeld modules are now established as a standard tool for studying function fields.

We introduced new algorithms to compute *characteristic polynomials* of *endomorphisms* of Drinfeld modules, as well as *norms* of *isogenies* of Drinfeld modules [31]. The former problem is a Drinfeld module equivalent to the problem of counting points on an elliptic curve; the latter is a generalization of the former. Works by Musleh and Schost already computed characteristic polynomials in a very specific case [45]. Thanks to a new approach, our algorithms work in full generality and rely on simple linear algebra techniques. To our knowledge, it is also the first time that the problem of computing norms of isogenies is addressed.

We stress that in 2023, Schost and Musleh published an article in which they also compute characteristic polynomials of Drinfeld module endomorphisms [46]. Their method, providing valuable insights, works for all endomorphisms and ranks. We provided a thorough comparison of the articles, and show that in many regimes, our algorithms are the fastest.

7.1.3 Drinfeld modules in SageMath

Participants: Antoine Leudière.

In April 2022, we began the first-ever implementation of Drinfeld modules to be included in the standard distribution of SageMath. Our contribution was merged in March 2023 and made available with version 10.0. The implementation is thoroughly integrated within the SageMath ecosystem and includes all basic operations on Drinfeld modules and their morphisms, as well as implementations of the algorithms mentioned in the previous point. A *software presentation* of our work was accepted at the 2023 International Symposium on Symbolic and Algebraic Computation (ISSAC) [15].

7.1.4 Dimension results for sparse polynomial systems

Participants: Pierre-Jean Spaenlehauer.

Polynomial systems arising in applications (for instance in cryptography) often feature monomial structures. Therefore, it is an important question to investigate how these structures can be used to speed up solving algorithms. This is the main topic of the collaboration between Pierre-Jean Spaenlehauer and Matías Bender (EPI TROPICAL). Toric varieties built from polyhedral fans provide a way to homogenize such sparse structures. In [29], we study in which cases such homogenizations may introduce generically high-dimensional artefacts that may harm the efficiency of the computations.

7.1.5 Search for worst cases

Participants: Paul Zimmermann.

To design correctly-rounded functions as in the CORE-MATH project, it is of utmost importance to know the “worst cases” of mathematical functions, i.e., inputs x such that $f(x)$ has many zeros or ones after the round bit. Worst cases have been computed for the new C99 or C23 functions that have been developed in 2023. These worst cases are available from the CORE-MATH git repository, so that they can be used to check correct-rounding of other mathematical libraries.

7.2 Secret-key cryptology

7.2.1 On boomerang attacks on quadratic Feistel ciphers: new results on KATAN and Simon

Participants: Xavier Bonnetain, Virginie Lallemand.

This article [16] studies the application of the cryptanalysis technique called the *boomerang attack* to ciphers following a Feistel construction and having a quadratic round function. We prove that many previously published papers give erroneous approximations of the probability of the distinguishers they use (most of the time it invalidates the attacks while in a few cases they are better than expected). We next propose a new SMT model that takes into account our findings and we are able to propose a 19-round distinguisher of the cipher Simon-32/64 that we convert into a 25-round attack, which to the best of our knowledge reaches one more round than previously published results.

7.2.2 Flatness and structural analysis for the design of stream ciphers involving hybrid automata

Participants: Hamid Boukerrou, Marine Minier.

In [17], we deal with hybrid dynamical systems in the context of cybersecurity and Cyber–Physical Systems. It is shown how the design of a cipher, called self-synchronizing stream cipher, can be recast as control-theoretic issues, in particular left inversion, flatness and structural analysis. From an automatic control point of view, the main contribution lies in a methodology to construct generic flat LPV systems. Beyond pure control theoretic matters, the design also addresses computational complexity and security concerns. Those considerations motivate a hybrid architecture involving switched automata. A Proof-Of-Concept example illustrates the design of a statistical self-synchronizing stream cipher and the way how it operates to encrypt data flows. Those results and all the ones with the CRAN laboratory are also summarized in [26].

7.2.3 Finding many collisions via reusable quantum walks

Participants: Xavier Bonnetain.

This article [19] proposes an improved quantum algorithm to find multiple collisions. This new algorithm matches the lower bound for a large range of parameters. It has many direct cryptographic implications, such as impossible differentials in symmetric cryptography, or lattice sieving. In particular, thanks to our algorithm we obtain the most efficient generic heuristic algorithm for lattice reduction. It is a sieving algorithm with complexity $2^{0.2563d+o(d)}$, with d the dimension of the lattice.

7.3 Public-key cryptology

7.3.1 Individual discrete logarithm with sublattice reduction

Participants: Haetham Al Aswad, Cécile Pierrot.

The work [14] deals with the splitting step in the number field sieve for finite fields of composite extension degree. The splitting step consists in finding an element R with a smooth norm and such that the logarithm of the target T can be easily deduced from the logarithm of R. The current state of the art takes advantage of lattice-reduction algorithms, such as LLL and BKZ in order to find such an element R. In this work, the authors explore the use of sublattices of the lattices usually used and perform experiments to validate this idea. Moreover, the authors give an asymptotic analysis of the individual logarithm step in NFS when LLL or BKZ are used as lattice-reduction in this new algorithm. This work is published in the journal Designs, Codes and Cryptography.

7.3.2 Discrete logarithm factory

Participants: Haetham Al Aswad, Cécile Pierrot, Emmanuel Thomé.

In [28] we generalize Coppersmith's factory's algorithm to compute discrete logarithms in several non-prime finite fields. The Number Field Sieve and its variants are the best algorithms to solve the discrete logarithm problem in finite fields (except for the weak small characteristic case). The Factory variant accelerates the computation when several prime fields are targeted. This article adapts the Factory variant to non-prime finite fields of medium and large characteristic. This idea is combined with two other variants of NFS, namely the tower and special variants. This combination improves the asymptotic complexity. Besides, this work provides estimates of the practicality of this method for 1024-bit targets of extension degree 6: our findings indicate that the factory approach begins to pay off when the cryptanalysis target consists of a few dozen of such finite fields.

7.3.3 Discrete logarithm with Tower NFS

Participants: Gabrielle De Micheli, Pierrick Gaudry, Cécile Pierrot.

The long version [18] of a previous work published in Asiacrypt 2021 has been published in the Journal of Cryptology. This describes the use of lattice techniques to implement the Tower NFS technique efficiently for discrete logarithm computations in finite fields in the so-called medium characteristic range. This long version includes in particular a new algorithm for making use of automorphisms in the linear algebra phase, by choosing appropriate Schirokauer maps.

7.3.4 An algebraic point of view on the generation of pairing-friendly curves

Participants: Aurore Guillevic.

The paper [33] with Jean Gasnier from the CANARI Team (Bordeaux) is the achievement of Jean Gasnier's Masters internship in 2022 co-advised in Bordeaux by Jean-Marc Couveignes and remotely from Denmark by Aurore Guillevic. It aims to generalize The Kachisa–Schaefer–Scott technique to find more pairing-friendly curves. The method allowed to obtain new curves for interesting embedding degrees, such as $k = 20$. It also closed some dead-ends in the quest of finding prime-order pairing-friendly curves (only three constructions are known, the latest discovery being in 2005). It comes with two implementations, one written by Jean Gasnier to find curve families (see the CANARI team report and Subfield Method Gitlab Project), the other one to implement pairings on the new curves, see Pairings on Gasnier–Guillevic Curves Gitlab Project. The results were presented at the SIAM-AG conference and the paper is under review.

7.4 Implications in computer security and the real world

7.4.1 Coercion resistance in e-voting

Participants: Pierrick Gaudry, Quentin Yang.

In [22], we show that the JCJ e-voting protocol that is the basis of many coercion-resistant systems is flawed, in the sense that the tally phase leaks more information than it should. In some specific scenarios, this can give an advantage to a coercer. Therefore, we propose a new version of JCJ, CHide, which relies on the multi-party toolbox that we designed earlier in the context of tally-hiding [40]. We also refine the existing formal definitions of coercion-resistance, in order to highlight the flaw, and prove that CHide fixes the problem.

In another work related to coercion resistance [23], in collaboration with Université Catholique de Louvain, we explore the relations between the notions of coercion resistance, receipt freeness, and cast as intended. We show some impossibility results and propose adapting the security notions, to make possible some of the combinations of these properties.

7.4.2 Cast-as-intended in e-voting

Participants: Pierrick Gaudry, Stéphane Glondu.

The cast-as-intended property in e-voting means that the system remains secure, even if the device used by the voter is compromised: if malware is present on the voter's computer, the voter should still have the guarantee that the encrypted ballot that is sent to the server contains their intended choice. In [20] we propose a new approach for this question, based on an audit procedure made by the voter, that does not leak their choice, and will detect a fraudulent device, with a probability of at least one-half. An attacker who would like to change many votes is likely to be detected.

7.4.3 Historical cryptology

Participants: Pierrick Gaudry, Cécile Pierrot, Paul Zimmermann.

An unknown and almost fully encrypted letter written in 1547 by Emperor Charles V to his ambassador at the French Court, Jean de Saint-Mauris, was identified in a public library, the Bibliothèque Stanislas (Nancy, France). As no decryption of this letter was previously published or even known, a team of cryptographers and historians gathered together to study the letter and its encryption system. First, multiple approaches and methods were tested in order to decipher the letter without any other specimen. Then, the letter has now been inserted within the whole correspondence between Charles and Saint-Mauris, and the key has been consolidated thanks to previous key reconstructions. Finally, the decryption effort enabled us to uncover the content of the letter and investigate more deeply both cryptanalysis challenges and encryption methods [25]. This is joint work with Camille Desenclos (University of Picardie).

8 Bilateral contracts and grants with industry

8.1 Bilateral contracts with industry

8.1.1 Consulting with Swiss Post

Participants: Pierrick Gaudry.

Together with the PESTO team, we have a long-term consulting activity with Swiss Post on the e-voting topic. In 2023 we started a new contract to help them design the next generation of their e-voting protocol.

8.1.2 Verifiability during the French legislative elections

Participants: Pierrick Gaudry, Stéphane Glondu.

Together with the PESTO team, we had a contract with the French Ministry of Foreign Affairs (MEAE), in the context of the legislative elections, for which the French citizens from abroad had the possibility to vote over the Internet. We played the role of external third-party, as required by the CNIL recommendations for such high-stake elections. While the contract was signed with the MEAE, it also involved interactions with the vendor of the solution (Voxaly), and the ANSSI who was the security advisor for the MEAE. In three districts, the 2022 elections were cancelled and therefore had to be done again in 2023.

This experiment of verifiability for a high stake election was documented and discussed in a research article that we published in the E-Vote-Id conference [21].

8.2 Start-up creation

8.2.1 Preparation of the VCast start-up

Participants: Pierrick Gaudry, Stéphane Glondu.

In 2023, Stéphane Glondu joined the Inria Startup Studio program to prepare the creation of a society to exploit commercially the Belenios software. Michael Houalef, a person with a business background, joined the project. The society, called VCast, is to be launched in the first semester of 2024. Véronique Cortier (from PESTO) and Pierrick Gaudry, as co-founders of Belenios, were involved in the discussions concerning this creation.

9 Partnerships and cooperations

9.1 International research visitors

9.1.1 Visits of international scientists

Our team received several international visits in 2023 (at most a week in duration, and most often a day or two): Yixin Shen (Royal Holloway University of London), Katharina Boudgoust (Aarhus University), Keegan Ryan (University of California San Diego), Steven Galbraith (University of Auckland).

9.2 National initiatives

9.2.1 PEPR Quantique, project PQ-TLS

Participants: Xavier Bonnetain, Pierre-Jean Spaenlehauer.

- Program: PEPR Quantique
- Project acronym: PQ-TLS
- Duration: 01/2022 - 12/2026
- Coordinator: Université de Rennes 1
- Other partners: Université de Limoges, Université de Rouen, Université de Bordeaux, Université de Saint-Quentin-en Yvelines, Université de Saint-Étienne, ENS de Lyon, Inria (GRACE, CARAMBA, COSMIQ, PROSECCO), CEA (Grenoble LETI), CNRS Labstic (Lorient).

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

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

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

9.2.2 PEPR Cybersécurité, project CRYPTANALYSE

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

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

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

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

9.2.3 Projet ANR KLEPTOMANIAC

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

- Program: ANR AAPG
- Project acronym: KLEPTOMANIAC
- Duration: 01/2022 - 12/2025
- Coordinator: Inria Nancy
- Other partners: ANSSI, LIP6

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

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

We plan to employ our expertise to provide solid hardness assessments for key sizes that are relevant today, and for which accuracy in the prediction is important. Our targets for accurate assessment are RSA-1024 and DH-1024 as well as specific discrete logarithm-related problems that arise in the blockchain context. We also intend to develop simulation software that would enable more accurate estimates.

In 2023, the work on the "double matrix" subtask initiated in 2022 was continued, in collaboration with Charles Bouillaguet (Sorbonne University). This work is integrated into a branch of Cado-NFS.

9.2.4 ANR Decrypt

Participants: Virginie Lallemand, Marine Minier.

- Program: ANR
- Project acronym: DECRYPT
- Duration: 01/2019 - 12/2023
- Coordinator: CARAMBA Team, LORIA
- Other partners: LIRIS (Lyon), LIMOS (Clermont-Ferrand), IRISA (Rennes), TASC (Nantes).

This project aimed to propose a declarative language dedicated to cryptanalytic problems in symmetric key cryptography using constraint programming (CP) to simplify the representation of attacks, to improve existing attacks and to build new cryptographic primitives that withstand these attacks. We also want to compare the different tools that can be used to solve these problems: SAT and MILP where the constraints are homogeneous and CP where the heterogeneous constraints can allow a more complex treatment.

One of the challenges of this project was to define global constraints dedicated to the case of symmetric cryptography.

Concerning constraint programming, this project defined new dedicated global constraints, improved the underlying filtering and solution search algorithms, and proposed dedicated explanations generated automatically. See the website for more information.

9.2.5 ANR OREO

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

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

This ANR project focuses on the use of Mixed Integer Linear Programming (MILP) in symmetric-key cryptography, a direction that enjoyed rapid recognition in the symmetric-key community following the article by Mouha *et al* [44].

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

9.2.6 Cooperation with ANSSI on e-voting regulation

Participants: Pierrick Gaudry.

We participate in a working group led by ANSSI, the purpose of which is to help the governmental actors (CNIL, ANSSI) in defining the next documents regulating the use of electronic voting in France.

9.3 Regional initiatives

- Marine Minier is co-supervisor with Antoine Joux of the virtual cybersecurity center between CISPA and LORIA (2023-2026).

10 Dissemination

Participants: Xavier Bonnetain, Sébastien Duval, Pierrick Gaudry, Aurore Guillevic, Virginie Lallemand, Marine Minier, Cécile Pierrot, Pierre-Jean Spaenlehauer, Emmanuel Thomé, Paul Zimmermann.

10.1 Promoting scientific activities

10.1.1 Scientific events: organisation

Member of the organizing committees

- Pierrick Gaudry, Paul Zimmermann and Pierre-Jean Spaenlehauer organized the *Rencontres de l'Arithmétique en Informatique Mathématique 2023* (RAIM 2023) at LORIA in Nancy. The RAIM is the main scientific event of the GT-ARITH of the CNRS GDR-IM. Website: `raim2023.loria.fr`
- Aurore Guillevic organized a minisymposium on Elliptic curves and pairings in cryptography at the SIAM-AG 2023 conference in Eindhoven, The Netherlands.

Member of the conference program committees

- Marine Minier was committee member of SPACE 2023, AfricaCrypt 2023, Indocrypt 2023, C2SI 2023.
- Aurore Guillevic was committee member of IMACC 2023, SAC 2023.
- Emmanuel Thomé was a program committee member of one of the workshops of the year-long RTCA2023 series of workshops organized in Lyon and Paris in 2023.
- Xavier Bonnetain and Virginie Lallemand were committee members of ACNS 2023.
- Xavier Bonnetain and Pierrick Gaudry were committee members of Eurocrypt 2024.
- Pierre-Jean Spaenlehauer is a member of the Scientific Committee of the *Journées Nationales du Calcul Formel* (JNCF), which is the main scientific event of the GT-calculformel of the CNRS GDR-IM.

Member of the Conference Steering Committees

- Pierrick Gaudry is a member of the steering committee of the Elliptic Curve Cryptography (ECC) workshop.

10.1.2 Journal

Member of the editorial boards

- Xavier Bonnetain and Virginie Lallemand were members of the editorial board of IACR Transactions on Symmetric Cryptology (ToSC) Journal for 2023. This journal is the open-access journal associated to the International Conference on Fast Software Encryption (FSE).
- Emmanuel Thomé is a member of the editorial board of the Journal of Algebra, dealing with the section on computational algebra.

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

10.1.3 Invited talks

- Pierre-Jean Spaenlehauer was invited to give a talk at the Workshop *Geometry of Polynomial System Solving, Optimization and Topology* at Institut Henri Poincaré, Paris. (Workshop M5 of RTCA2023.)
- Marine Minier was invited to Journées de la Fédération Charles Hermite at Nancy, December 2023.
- Marine Minier was invited to the Codes Sources Seminar, Paris, February 2023.
- Emmanuel Thomé was invited to give a talk at RTCA2023 (workshop M3) in Lyon.

- Pierrick Gaudry was invited to give a talk at the Digistrust workshop, Nancy, December 2023.
- Pierrick Gaudry was invited to give a talk at the workshop in honor of Véronique Cortier, Nancy, January 2023.
- Aurore Guillevic was invited to give a talk at the WRACH 2023 workshop at Roscoff, France.
- Virginie Lallemand was invited to give a talk for the French-American Doctoral Exchange (FADex) program on cybersecurity.
- Cécile Pierrot was invited to give a talk at Ecole de Guerre, an event organised by l'Académie des Sciences.

10.1.4 Leadership within the scientific community

- Cécile Pierrot is a member of the steering committee of the French working group Code and Cryptography.
- Pierrick Gaudry is a member of the Conseil Scientifique of GdR IM.

10.1.5 Scientific expertise

- Marine Minier was a member of comité de sélection 61MCF1719, Université de Toulouse; comité de sélection 27MCF1634, Université de Lorraine; comité de sélection 27MCF0073, Université Clermont-Auvergne.
- Since November 2023, Marine Minier is a nominated member of the CNU 27.
- Emmanuel Thomé was a member of the recruitment panel for Inria Chargé de recherche and Starting Faculty positions at Inria Paris.
- Aurore Guillevic was a member of the comité de sélection 26MCF161, Université Grenoble Alpes.
- Pierrick Gaudry was a member of the comité de sélection 27MCF1053, Université de Montpellier.

10.1.6 Research administration

- Pierre-Jean Spaenlehauer is a member of the *Commission de Développement Technologique* (CDT) of the Centre Inria de l'Université de Lorraine. From December 2023, he is the head of the CDT.
- Aurore Guillevic was a member of the COMIPERS (commission du personnel).
- Marine Minier was adjoint director of the LORIA Lab until September 2023.
- Pierrick Gaudry is head of the Department 1 of LORIA, since June 2023.
- Pierrick Gaudry was a member of the *Commission de Mention Informatique* (CMI) of the *École doctorale IAEM*, and a member of the *Comité des utilisateurs des moyens de calcul INRIA*.
- Pierrick Gaudry and Marine Minier are members of the steering committee of the LHS – Laboratoire Haute Sécurité of LORIA.
- Xavier Bonnetain is the local coordinator of the Inria activity reports for the Inria Centre at Université de Lorraine (among them, this very document).
- Paul Zimmermann is member of the scientific committee of the EXPLOR computing center (Université de Lorraine).
- Cécile Pierrot is a member of the Bureau du Comité des Projets (BCP) at Inria Nancy.

10.2 Teaching - Supervision - Juries

10.2.1 Teaching

Marine Minier obtained an half Inria Delegation in 2023.

- Bachelor
  - Sébastien Duval, *Algorithmique et Programmation 2*, 40h eq. TD, L1 Informatique, Université de Lorraine, Faculté des sciences et technologies, Vandœuvre-lès-Nancy, France.
  - Sébastien Duval, *Algorithmique et Programmation 3*, 26h eq. TD, L2 Informatique, Université de Lorraine, Faculté des sciences et technologies, Vandœuvre-lès-Nancy, France.
  - Sébastien Duval, *Mathématiques Discrètes 2*, 16h eq. TD, L2 Informatique, Université de Lorraine, Faculté des sciences et technologies, Vandœuvre-lès-Nancy, France.
  - Sébastien Duval, *Introduction à la sécurité et à la cryptographie*, 20h eq. TD, L3 Informatique, Université de Lorraine, Faculté des sciences et technologies, Vandœuvre-lès-Nancy, France.
  - Marine Minier, *Introduction à la sécurité et à la cryptographie*, 35h eq. TD, L3, Université de Lorraine, Faculté des sciences et technologies, Vandœuvre-lès-Nancy, France.
- Master
  - Sébastien Duval, *Introduction à la cryptographie*, 12h eq. TD, M1 Informatique, Université de Lorraine, Faculté des sciences et technologies, Vandœuvre-lès-Nancy, France.
  - Sébastien Duval, *Sécurité des Systèmes d'Information*, 32h eq. TD, M2 Informatique, Université de Lorraine, Faculté des sciences et technologies, Vandœuvre-lès-Nancy, France.
  - Sébastien Duval, *Sécurité des Applications Web*, 32h eq. TD, M2 Informatique, Université de Lorraine, Faculté des sciences et technologies, Vandœuvre-lès-Nancy, France.
  - Marine Minier, *Contrôle d'accès*, 40h eq. TD, M2 Informatique, Université de Lorraine, Faculté des sciences et technologies, Vandœuvre-lès-Nancy, France.
  - Marine Minier, *Intégration Méthodologique*, 36h eq. TD, M2 Informatique, Université de Lorraine, Faculté des sciences et technologies, Vandœuvre-lès-Nancy, France.
  - Marine Minier *Sécurité Informatique*, 18h eq. TD, M2 droit IPIT, Université de Lorraine, France.
  - Marine Minier *Introduction à la cryptographie*, 18h eq. TD, M1 Informatique, Université de Lorraine Faculté des sciences et technologies, Vandœuvre-lès-Nancy, France.
  - Marine Minier is head of the M2 SIRAV, Université de Lorraine, Faculté des sciences et technologies, Vandœuvre-lès-Nancy, France.
- Engineering school
  - Cécile Pierrot, *Introduction to Cryptography*, 57h eq. TD, Mastère spécialisé de cybersécurité, École des Mines de Nancy, France.
  - Aurore Guillevic, *Cryptographie avancée*, 5A FISE IA2R (Master 2), 30h eq. TD, Université de Lorraine, Polytech Nancy, France.
  - Xavier Bonnetain, *Algorithmique et complexité*, 50h eq. TD, 1ere année (L3), Université de Lorraine, École des Mines de Nancy, France.

10.2.2 Supervision

- Ph.D. completed: Quentin Yang, *Résistance à la coercition en vote électronique : conception et analyse* [27], defended in June 2023, Pierrick Gaudry and Véronique Cortier (PESTO team).
- Ph.D. completed: Hamid Boukerrou, *Design of new finite state dynamical systems admitting a matrix representation: Application to cryptography* [26], defended in April 2023, Marine Minier and Gilles Millerioux.

- Ph.D. in progress: Haetham Al Aswad, *Number field sieve for discrete logarithm*, since Oct. 2021, Cécile Pierrot and Emmanuel Thomé.
- Ph.D. in progress: Antoine Leudière, *Isogenies of Drinfeld modules and post-quantum cryptography*, since Oct. 2021, Pierre-Jean Spaenlehauer and Emmanuel Thomé.
- Ph.D. in progress: Ana Rodriguez Cordero, *Design and Cryptanalysis of New Symmetric Key Cryptographic Primitives*, since Oct. 2021, Virginie Lallemand and Marine Minier.
- Ph.D. in progress: Leo Louistisserand, *Conception et analyse de protocoles de vote utilisés ou utilisables en pratique*, since Oct. 2023, Pierrick Gaudry and Véronique Cortier (PESTO team).
- Ph.D. in progress: Marie Bolzer, *Algorithmique et outils automatiques pour la construction et l'analyse de composants de cryptographie symétrique*, since Oct. 2023, Sébastien Duval and Marine Minier.
- Ph.D. in progress: Medhi Kermaoui, *Quantum cryptanalysis of public-key cryptosystems*, since Oct. 2023, Xavier Bonnetain and Pierrick Gaudry.
- Ph.D. in progress: Julien Soumier, *Algorithmic of Isogenies of Abelian Varieties and Post-Quantum Cryptography*, since Oct. 2023, Pierre-Jean Spaenlehauer and Pierrick Gaudry.

10.2.3 Juries

- Marine Minier was President of the PhD Jury of Aina Toky Rasoamanana (June 2023, Institut Polytechnique de Paris); president of the PhD jury of Tristan Benoît (December 2023, Lorraine University).
- Marine Minier was reviewer of the HDR of Hélène Le Bouder (October 2023, Université de Rennes); reviewer of the PhD thesis of Nicolas David (November 2023, Sorbonne Université); reviewer of the PhD thesis of Pierre Galissant (Décember 2023, Université de Versailles-Saint-Quentin-en-Yvelines).
- Emmanuel Thomé was President of the HDR jury of Benjamin Smith (October 2023, Institut Polytechnique de Paris).
- Paul Zimmermann was reviewer of the PhD thesis of Mehdi El Arar (December 2023, Université Paris-Saclay).

10.3 Popularization

The deciphering of the encrypted letter from Emperor Charles V (see §7.4.3) had a large media coverage, both in French and international media. To cite a few: the French television (France 2, France 3, BFM TV, Arte), the French radio (France Inter, Europe 1, France Info, France Culture), French newspapers (Le Monde, Le Point), an excellent video on Nota Bonus, some international media (The Guardian, Radio Canada, BBC, RTVE, The Scientist).

10.3.1 Internal or external Inria responsibilities

- Emmanuel Thomé was an elected member of the Inria Evaluation Committee until August 2023, and contributed to writing the summary of the four-year term of the committee [30].

10.3.2 Education

- Pierre-Jean Spaenlehauer and Paul Zimmermann participated in the Math-En-Jeans project. They supervised a group of teenagers from the Lycée Français Vauban du Luxembourg.
- Aurore Guillevic visited two classes at Saint Dié des Vosges and three at Saint-Louis (Haut-Rhin) for 1 scientifique 1 classe chiche.

- Aurore Guillevic participated to the Maths camp for high school female teenagers Cigognes in Ramonchamp, Vosges.

- Aurore Guillevic gave a talk at the Maths-en-Jeans day in Nancy, May 2.

- Paul Zimmermann participated to the “Fête de la Science” in Bouxurulles, a small village 50 kilometers in the south of Nancy, where he presented the work on deciphering the letter from Emperor Charles V, and the new MATh.en.JEANS problem proposed for 2023-2024 (October 2023).

10.3.3 Interventions

- Pierrick Gaudry gave a talk at the Cycle de conférences Sciences et Société, on the topic of electronic voting, in January 2023, Polytech, Nancy.

- Lucas Villaume and Paul Zimmermann organized an animation on the encrypted letter from Emperor Charles V at the “Nuit européenne des chercheurs” (Metz, November 2023).

11 Scientific production

11.1 Major publications

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

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

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

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

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

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

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

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

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

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

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

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

[13] A. Sibidanov, P. Zimmermann and S. Glondu. ‘The CORE-MATH Project’. In: ARITH 2022 - 29th IEEE Symposium on Computer Arithmetic. virtual, France, 12th Sept. 2022. URL: https://hal.inria.fr/hal-03721525.

11.2 Publications of the year

International journals

[14] H. Al Aswad and C. Pierrot. ‘Individual Discrete Logarithm with Sublattice Reduction’. In: *Designs, Codes and Cryptography* 91.12 (2nd Sept. 2023), pp. 4059–4091. DOI: 10.1007/s10623-023-01282-w. URL: https://hal.science/hal-03737874.

[15] 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.

[16] X. Bonnetain and V. Lallemand. ‘On Boomerang Attacks on Quadratic Feistel Ciphers: New results on KATAN and Simon’. In: *IACR Transactions on Symmetric Cryptology* 2023.3 (19th Sept. 2023), pp. 101–145. DOI: 10.46586/tosc.v2023.i3.101-145. URL: https://inria.hal.science/hal-04214762.

[17] H. Boukerrou, G. Millérioux, M. Minier and T. Boukhobza. ‘Flatness and structural analysis for the design of stream ciphers involving hybrid automata’. In: *Nonlinear Analysis: Hybrid Systems* 52 (May 2024), p. 101443. DOI: 10.1016/j.nahs.2023.101443. URL: https://hal.science/hal-04319635.

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

International peer-reviewed conferences

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

[20] V. Cortier, A. Debant, P. Gaudry and S. Glondu. 'Belenios with cast as intended'. In: Voting 2023 - 8th Workshop on Advances in Secure Electronic Voting. Bol, Brač, Croatia, 5th May 2023. URL: https://inria.hal.science/hal-04020110.

[21] V. Cortier, P. Gaudry, S. Glondu and S. Ruhault. 'French 2022 legislatives elections: a verifiability experiment'. In: *Proceedings E-Vote-Id 2023*. The E-Vote-ID Conference 2023. Luxembourg City, Luxembourg, 3rd Oct. 2023. URL: https://inria.hal.science/hal-04205615.

[22] V. Cortier, P. Gaudry and Q. Yang. 'Is the JCJ voting system really coercion-resistant?' In: 37th IEEE Computer Security Foundations Symposium (CSF). CSF 2024. Enschede, Netherlands: IEEE, 2024. URL: https://inria.hal.science/hal-03629587.

[23] H. Devillez, O. Pereira, T. Peters and Q. Yang. 'Can we cast a ballot as intended and be receipt free?' In: IEEE Symposium on Security and Privacy 2024. San Francisco, United States, 20th May 2024. URL: https://inria.hal.science/hal-04371905.

[24] T. Hubrecht, C.-P. Jeannerod and P. Zimmermann. 'Towards a correctly-rounded and fast power function in binary64 arithmetic'. In: 2023 IEEE 30th Symposium on Computer Arithmetic (ARITH 2023). Vol. 2023 IEEE 30th Symposium on Computer Arithmetic (ARITH). Portland, Oregon (USA), United States, 2023. URL: https://inria.hal.science/hal-04326201.

[25] C. Pierrot, C. Desenclos, P. Gaudry and P. Zimmermann. 'Deciphering Charles Quint (A diplomatic letter from 1547)'. In: *Linköping Electronic Conference Proceedings*. 6th International Conference on Historical Cryptology, HistoCrypt. Vol. 195. Munich, Germany, 20th June 2023, pp. 148–158. DOI: 10.3384/ecp195704. URL: https://hal.science/hal-04083014.

Doctoral dissertations and habilitation theses

[26] H. Boukerrou. 'Design of new finite state dynamical systems admitting a matrix representation : Application to cryptography'. Université de Lorraine, 4th Apr. 2023. URL: https://hal.univ-lorraine.fr/tel-04205174.

[27] Q. Yang. 'Résistance à la coercition en vote électronique : conception et analyse'. Université de Lorraine, 23rd June 2023. URL: https://theses.hal.science/tel-04206190.

Reports & preprints

[28] H. Al Aswad, C. Pierrot and E. Thomé. *Discrete Logarithm Factory*. 5th Oct. 2023. URL: https://hal.science/hal-04117298.

[29] M. R. Bender and P.-J. Spaenlehauer. *Dimension results for extremal-generic polynomial systems over complete toric varieties*. 12th May 2023. URL: https://inria.hal.science/hal-04102564.

[30] A. Canteaut, M. Serrano, C. Grandmont, G. Pallez, V. Perrier, X. Rival and E. Thomé. *Bilan de la mandature 2019-2023 de la Commission d'Évaluation Inria*. Inria, 31st Aug. 2023. URL: https://inria.hal.science/hal-04193082.

[31] 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.

[32] P. Frixons, S. Canard and L. Ferreira. *Quantum Security of the UMTS-AKA Protocol and its Primitives, Milenage and TUAK*. 11th Dec. 2023. URL: https://hal.science/hal-04334580.

[33] 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.

[34] B. Gladman, V. Innocente and P. Zimmermann. *Accuracy of Mathematical Functions in Single, Double, Extended Double and Quadruple Precision*. 25th Sept. 2023. URL: https://inria.hal.science/hal-03141101.

[35] T. Hubrecht, C.-P. Jeannerod and P. Zimmermann. *Towards a correctly-rounded and fast power function in binary64 arithmetic*. 12th July 2023. URL: https://inria.hal.science/hal-04159652.

[36] M. Naya Plasencia, R. Bhaumik, A. Chailloux, P. Frixons and B. Mennink. *Block Cipher Doubling for a Post-Quantum World*. 7th Dec. 2023. URL: https://inria.hal.science/hal-04328717.

[37] P. Zimmermann. *Note on FastTwoSum with Directed Roundings*. 19th Sept. 2023. URL: https://inria.hal.science/hal-03798376.

11.3 Other

Patents

[38] M. Minier, S. Rasoamiaramanana and G. Macario-Rat. 'Secure method for data exchange between a terminal and a server'. US Patent App. 17/777,906 (France). 23rd Jan. 2023. URL: https://inria.hal.science/hal-04313153.

Softwares

[39] [SW] G. Hanrot, P. Zimmermann, V. Lefèvre, P. Pélissier and P. Théveny, *GNU MPFR* version 4.2.0, 6th Jan. 2023. LIC: GNU General Public License. HAL: ⟨hal-03940504⟩, URL: https://inria.hal.science/hal-03940504, VCS: https://gitlab.inria.fr/mpfr/mpfr, SWHID: ⟨swh:1:rel:b5e308c5dd459a81d8523e1dcb84c19dbc47b51b;origin=https://gitlab.inria.fr/mpfr/mpfr;visit=swh:1:snp:15595615280f9f91d107c1f4e9fa915fda0076dc⟩.

11.4 Cited publications

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

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

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

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

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

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

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

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

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