RESEARCH CENTRE

Nancy - Grand Est

IN PARTNERSHIP WITH:

Université de Lorraine, CNRS

2021 ACTIVITY REPORT

Project-Team CARAMBA

Cryptology, arithmetic : algebraic methods for better algorithms

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, until Jul 2021, HDR]
- Paul Zimmermann [Team leader, Inria, Senior Researcher, from Aug 2021, HDR]
- Xavier Bonnetain [Inria, Researcher, from Oct 2021]
- Pierrick Gaudry [CNRS, Senior Researcher, HDR]
- Aurore Guillevic [Inria, Researcher]
- Virginie Lallemand [CNRS, Researcher]
- Cécile Pierrot [Inria, Researcher]
- Pierre-Jean Spaenlehauer [Inria, Researcher]

Faculty Members

- Sébastien Duval [Univ de Lorraine, Associate Professor, from Sep 2021]
- Marine Minier [Univ de Lorraine, Professor, HDR]

PhD Students

- Haetham Al Aswad [Inria, from Oct 2021]
- Hamid Boukerrou [Univ de Lorraine]
- Gabrielle De Micheli [Inria, until Aug 2021]
- Le Phuc Huynh [CNRS, until Feb 2021]
- Aude Le Gluher [Univ de Lorraine, until Aug 2021]
- Antoine Leudière [Inria, from Oct 2021]
- Simon Masson [UDcast, CIFRE, Jan 2021]
- Ana Margarita Rodriguez Cordero [Univ de Lorraine, from Oct 2021]
- Quentin Yang [Inria]

Interns and Apprentices

- Haetham Al Aswad [Inria, from Mar 2021 until Sep 2021]
- Nathan Chiche [Univ de Lorraine, from Apr 2021 until Aug 2021]
- Antoine Leudière [Inria, from Apr 2021 until Sep 2021]
- Marc Simard [Univ de Lorraine, until Jun 2021]
- Samuel Vivien [Inria, from Jun 2021 until Jul 2021]

Administrative Assistants

- Emmanuelle Deschamps [Inria]
- Virginie Priester [CNRS, until Mar 2021]

External Collaborator

- Luc Sanselme [Ministère de l'Education Nationale]

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. In all cases, our work is geared towards making computations with these objects effective and fast.

The two facets of cryptology—cryptography and cryptanalysis—are central to our research. 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.

Our research connects to both symmetric and asymmetric key cryptography. While the basic principles of these domains are rather different—indeed their names indicate different handlings of 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 research topics can be listed either with broad applications domains in mind (a very coarse-grain view would have us list them under cryptography and cryptanalysis), or more thematically (see Figure 1). Either way, we also identify a set of *tools* that we sometimes develop *per se*, but most often as ingredients towards goals that are set in the context of other themes. Following the "vertical" reading direction in Figure 1, our research topics are as follows.

- Extended NFS family. A common algorithmic framework, called 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.

  We plan to improve on the existing state of the art in this domain by researching new algorithms, by optimizing the software performance, and by demonstrating the reach of our software with highly visible computations.

- Algebraic curves and their Jacobians. We develop algorithms and software for computing essential properties of algebraic curves for cryptology, eventually enabling their widespread cryptographic use.

  Closely related to the Tower Number Field Sieve are pairing-friendly curves. Pairings are bilinear maps $e\colon \mathbb{G}_1 \times \mathbb{G}_2 \to \mathbb{G}_T$ available on dedicated elliptic curves. The target group $\mathbb{G}_T$ is an extension $\mathrm{GF}(p^n)$ of small degree ($1 \leq n \leq 54$ in practice) where the TNFS algorithm and its variants apply. We study the security of these curves w.r.t. the TNFS algorithm, and we are interested in making recommendations of key-sizes, elliptic curve choices, and providing faster implementation of pairings.

  Questions more recently studied include the development of cryptosystems based on isogenies.

- Symmetric key cryptography. This topic has emerged in the team with several new hires since 2016. We are interested in particular in automatic tools for new paradigms of cryptanalysis, going beyond the classical linear and differential cryptanalysis techniques. Newer, more intricate techniques are rather hard to apply and are error-prone. The idea is then to automate the analysis process by developing tools implemented in constraint programming (CP) , satisfability (SAT) or mixed integer linear programming (MILP). We plan to pay special attention to the recent advances in cryptanalysis and to study recently proposed lightweight ciphers.

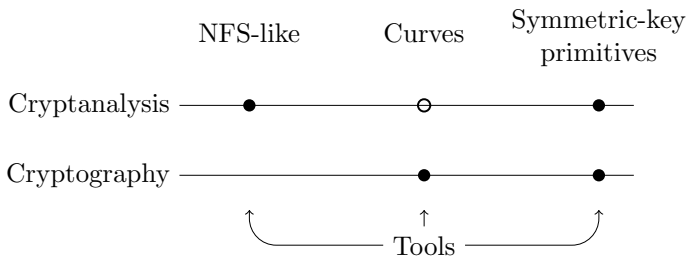

Figure 1: Visual representation of the thematic organization of CARAMBA. Solid dots: major interaction; clear dots: minor interaction.

In addition, we also study new designs. The challenge of the lightweight world pushes symmetric cryptography to be ever more efficient while guaranteeing the same level of security as before. It is thus very important to scrutinize each building block of the symmetric key primitives to be convinced of their security.

- Quantum cryptanalysis. Cryptanalysis is at the core of security assessments. 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.

- Tools. Several mathematical objects are pervasive in our research. We sometimes study them *per se*, but they most often play a key role in the work related to the topics above. In particular, we study computer arithmetic, polynomial systems, linear algebra. In the context of symmetric cryptography, the mathematical objects we deal with are rather different: we are mainly interested in small (4 or 8 bits) non-linear permutations (the so-called S-boxes) and in linear transformations based on coding theory (Maximum Distance Separable (MDS) matrices or quasi-MDS matrices).

  Our goals with all these basic objects include a strong commitment to providing high-quality software that can be used as a dependable building block in our research.

As a complement to the last point, we consider that the impact of our research on cryptology in general owes a lot to the publication of concrete practical results. We are strongly committed to making our algorithms available as software implementations. We thus have several long-term software development projects that are, and will remain, part of our research activity.

3 Research program

3.1 The Extended Family of the Number Field Sieve

The Number Field Sieve (NFS) has been the leading algorithm for factoring integers for more than 20 years, and its variants have been used to set records for discrete logarithms in finite fields. It is reasonable to understand NFS as a framework that can be used to solve various sorts of problems. Factoring integers and computing discrete logarithms are the most prominent for the cryptographic observer, but the same framework can also be applied to the computation of class groups.

The state of the art with NFS is built from numerous improvements of its inner steps. In terms of algorithmic improvements, the recent research activity on the NFS family has been rather intense. Several new algorithms have been discovered since 2014, notably for non-prime fields, and their practical reach has been demonstrated by actual experiments.

The algorithmic contributions of the CARAMBA members to NFS would hardly be possible without access to a dependable software implementation. To this end, members of the CARAMBA team have been developing the Cado-NFS software suite since 2007. Cado-NFS is now the most widely visible open-source implementation of NFS, and is a crucial platform for developing prototype implementations

for new ideas for the many sub-algorithms of NFS. Cado-NFS is free software (LGPL) and follows an open development model, with publicly accessible development repository and regular software releases. Competing free software implementations exist, such as `msieve`, developed by J. Papadopoulos (whose last commit is from August 2018). T. Kleinjung develops his own code base, which is unfortunately not public.

The work plan of CARAMBA on the topic of the Number Field Sieve algorithm and its cousins includes the following aspects:

- Pursue the work on NFS, which entails in particular making it ready to tackle larger challenges. Several of the important computational steps of NFS that are currently identified as stumbling blocks will require algorithmic advances and implementation improvements. We will illustrate the importance of this work by computational records.
- Work on the specific aspects of the computation of discrete logarithms in finite fields.
- As a side topic, the application of the broad methodology of NFS to the treatment of "ideal lattices" and their use in cryptographic proposals based on Euclidean lattices is also relevant.

3.2 Algebraic Curves for Cryptology

The challenges associated with algebraic curves in cryptology are diverse, because of the variety of mathematical objects to be considered. These challenges are also connected to each other. On the cryptographic side, efficiency matters, while cryptanalysis looks at the hardness of the discrete logarithm problem.

Several members have expertise in multiple facets of curve-based cryptology, but recent work in the team has been concentrated on a few precise topics. One of them is pairing-based cryptography. Pairing-friendly curves were introduced in 2001 in (constructive) cryptography and should be designed with a a very precise application goal in mind, contrary to the widespread curves such as x25519 or x448 in TLS, or the NIST curves, which can be used much more generically. The bilinear pairing has two aspects. First a destructive side: it transfers a discrete logarithm computation from the group of points of the curve (where the DLP is known to be hard, of exponential complexity in the size of the group), to a finite field extension $\mathrm{GF}(p^n)$ where better variants of the NFS algorithm apply. Hence pairing-friendly curves and in particular, wrong choices of parameters provide a large range of targets for record computations with the TNFS algorithm. Second, a constructive side: the pairing allows the multiplication in the exponents two hidden values (two secret scalars) without knowing them explicitly, thanks to the formula $e(g_1^a, g_2^b) = e(g_1, g_2)^{ab}$. We are looking for new curves that ensure a given security level, taking into account the latest advances in DL computation in $\mathrm{GF}(p^n)$, together with the development of faster pairing computation on these curves. Another growing area of interest for efficient pairings is zero-knowledge Succinct Non-interactive ARgument of Knowledge (zk-SNARK). Dedicated pairing-friendly curves are required and the team is interested in finding new such curves, while ensuring a security margin w.r.t. the TNFS algorithm.

We also investigate the practical security (e.g. against physical attacks) of elliptic curves and their implementations. Our focus here is more on the connection of such problems with Euclidean lattice theory, for example.

With NIST's competition on post-quantum cryptographic primitives, the new area of isogenies on elliptic curves is developing. Efficient implementation of isogenies is an active area of research nowadays, together with better parameter selection. The elliptic curves suitable for isogenies require different properties: they are supersingular contrary to the ordinary curves in classical cryptography. Selecting parameters is a difficult task, and in some cases, it requires a large computational effort of a class number computation.

The research objectives of CARAMBA on the topic of algebraic curves for cryptology are as follows:

- Ban obsolete parameters of pairing-friendly curves thanks to new discrete logarithm record computations. Investigate new parameter selections and build new cryptographic recommendations of pairing-friendly elliptic curves.
- Develop a full library of elliptic curves with their pairing computations in SageMath in the spirit of the Elliptic Curve Formula Database to bridge the gap between theoretical papers and efficient software library developments.

3.3 Symmetric Cryptography

In symmetric key cryptology, we are tackling problems related to both design and analysis. A large part of our recent research has been motivated by the Lightweight Cryptography Standardization Process of the NIST [1] that embodies a crucial challenge of the last decade: finding ciphers that are suitable for resource-constrained devices.

On a general note, the working program of CARAMBA in symmetric cryptography is defined as follows:

- Develop automatic tools based on constraint programming to help find optimum attack parameters. The effort will be focused on the AES standard and on recent lightweight cipher proposals.
- Contribute to the security and performance analysis effort required to sort out the candidates for the NIST Lightweight Cryptography Standardization Process.
- Study how to protect services execution on dedicated platforms using white-box cryptography and software obfuscation methods.

3.4 Computer Arithmetic

Computer arithmetic is part of the common background of all team members, and is naturally ubiquitous in our application domains. However involved the mathematical objects considered may be, dealing with them first requires to master more basic objects: integers, finite fields, polynomials, and real and complex floating-point numbers. Libraries such as GNU MP, GNU MPFR, GNU MPC do an excellent job for these, both for small and large sizes.

Most of our involvement in subjects related to computer arithmetic is to be understood in connection to our applications to the Number Field Sieve and to abelian varieties. As such, much of the research work we envision will appear as side-effects of developments in these contexts. On the topic of arithmetic work *per se*:

- We will seek algorithmic and practical improvements to the most basic algorithms. That includes for example the study of advanced algorithms for integer multiplication, and their practical reach.
- We will continue to work on the arithmetic libraries in which we have crucial involvement, such as GNU MPFR, GNU MPC, GF2X, MPFQ, and also GMP-ECM.

4 Application domains

4.1 Better Awareness and Avoidance of Cryptanalytic Threats

Our study of the Number Field Sieve family of algorithms aims at showing 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 the choice of appropriate cryptographic primitives. For example the French ANSSI [2], German BSI, or the NIST [3] 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 to cryptographic systems that are taking the security/efficiency/legacy compatibility trade-offs too lightly. Attacks such as LogJam [34] 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 confidentiality of communications.

[1] National Institute of Standard and Technology.

[2] In [35], 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”.

[3] The work [37] is one of only two academic works cited by NIST in the initial version (2011) of the report [38].

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 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 in 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), in Victor Shoup's Number Theory Library (NTL), or in the Sage computer algebra system. The availability of these software packages in most Linux distributions is also a good measure for the impact of our work.

We also develop more specialized software. Our flagship software package is Cado-NFS[39], 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 source of inspiring material for others, it is again important that these be developed in a free and open-source development model.

5 Highlights of the year

5.1 Awards

- The article [4] got one of the three best paper awards at the Asiacrypt conference in December 2021. This article achieved a record computation of a discrete logarithm in a 521-bit size finite field.

- Gabrielle De Micheli got the Price L'Oréal-UNESCO Young Talents France 2021 – for Women and Science. It aims to reward PhD students and postdoctoral researchers for their work in various area of Science.

- With colleagues from the PESTO team, Pierrick Gaudry was awarded a bug bounty for the discovery of a privacy attack in the SwissPost electronic voting system.

- Emmanuel Thomé was awarded a Fulbright grant to visit University of California San Diego for one year, and appointed as a visiting professor in San Diego for that time.

6 New software and platforms

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 order 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 2021, our platform was used for the organization of about 2000 elections, with about 70,000 ballots counted.

This year, we modified the voting platform to make it more user-friendly and responsive: it automatically adapts on a cell phone, for example. We also developed two new interfaces to vote by ranking the candidates (Condorcet) or by rating them (Majority Judgement). Following several requests, Belenios now offers weighted votes, where each voter has a certain number of votes. Less visible to users, an important change was the update of the cryptographic core, in order to better link a ballot to the context of the election. Finally, we initiated the development of a REST API and modernized the management of administrator accounts.

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: During year 2021, several internal aspects of the CADO-NFS code were modified. - some computations are now shared in order to save a significant number of modular inversions during the sieving step. - the Python script that orchestrates the computation has been improved. - 32-bit factor bases are now supported. - the filtering simulation code has been improved. - the continuous integration machinery has been considerably improved and extended. - tooling was put in place in order to automatically detect code defects with static analysis software (Coverity Scan).

In 2020, CADO-NFS has moved to the Inria gitlab platform. However, the question of a permanent URL that Cado-NFS could use is still awaiting validation by the relevant service.

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

Contact: Emmanuel Thome

Participants: Pierrick Gaudry, Emmanuel Thome, Paul Zimmermann

6.1.3 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.

News of the Year: The paper hal-02263098 was published in 2021 and the library was updated accordingly. The library was updated later in 2021 to estimate the security of the curves listed at https://members.loria.fr/AGuillevic/pairing-friendly-curves/ and other curves upon request (e.g. the Pluto BN curve).

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

Publications: hal-02263098, hal-02396352

Contact: Aurore Guillevic

6.1.4 ALPINAC

Name: ALgorithmic Process for Identification of Non-targeted Atmospheric Compounds

Keyword: Chemistry

Functional Description: ALPINAC identifies up to 95% of the measured signal obtained from an Electron-Impact Time-of-Flight High Resolution Mass Spectrometer (EI ToF HRMS) on air sampling, without a-priori knowledge on the encountered chemical compounds, without database search. The software was successfully tested on mass spectrum ranging from 23 m/z to 330 m/z.

News of the Year: ALPINAC was first released in July 2021.

URL: https://gitlab.inria.fr/guillevi/alpinac

Publication: hal-03176025

Contact: Aurore Guillevic

Partner: EMPA

6.1.5 snark-2-chains

Name: Families of SNARK-friendly 2-chains of elliptic curves

Keywords: Cryptography, Cryptocurrency, Blockchain

Functional Description: This small library implements finite field and elliptic curve arithmetic for BN curves (Barreto-Naehrig), BLS curves (Barreto-Lynn-Scott), and 2-chains made of BW6 (Brezing-Weng curves of embedding degree 6), CP8, CP12 (Cocks-Pinch curves of embedding degree 8 and 12) for use with zk-snarks (zero-knowledge succinct non-interactive argument of knowledge). The cryptographic applications are: pairing, scalar multiplication on the curves, hashing on the curves. The code is a proof of concept tied to a preprint and is not optimized.

News of the Year: The library was first released in October 2021.

URL: https://gitlab.inria.fr/zk-curves/snark-2-chains

Publication: hal-03371573

Contact: Aurore Guillevic

7 New results

7.1 Algebraic curves for cryptology

7.1.1 Families of SNARK-friendly 2-chains of elliptic curves

This work [30] is a generalization of [32] published last year at CANS'2020, with Youssef El Housni, PhD student in the GRACE team at Inria Saclay, and ConsenSys. This paper considers chains of two pairing-friendly elliptic curves for SNARKs (Succint Non-interactive ARguments of Knowledge). In the previous work, one 2-chain was investigated: the curves BLS12-381 and BW6-761. This work considers 2-chains of curves where the first (inner) curve can be a BN (Barreto–Naehrig), or a BLS12 or BLS24 (Barreto–Lynn–Scott) curve. The second (outer) curve is obtained with the Brezing–Weng construction (BW6 curves) of the Cocks-Pinch curve. The aim is to provide other trade-offs in terms of size, and arithmetic and pairing efficiency. This preprint improves the operations on BLS curves: a general proof of faster cofactor multiplication is provided for example. The companion code is referenced in Section 6.1.5, and a full Golang implementation is developed in the library GNARK.

7.2 The Number Field Sieve

7.2.1 On the Alpha value of polynomials in the Tower Number Field Sieve Algorithm

Participants: Aurore Guillevic.

The preprint version of [13] appeared in the report of 2019, this paper was published in 2021 in the new diamond open-access journal *Mathematical Cryptology*. With Shashank Singh from IISER Bhopal (former post-doc at CARAMBA in 2017), we generalized the ranking function α for the Tower setting of the Number Field Sieve in [13]. In the relation collection of the NFS algorithm, one tests the smoothness of algebraic norms (computed with resultants). The α function measures the bias of the average valuation at small primes of algebraic norms, compared to the average valuation at random integers of the same size. A negative α means more small divisors than average. We then estimate the total number of relations with a Monte-Carlo simulation, as a generalized Murphy's E function, and finally give a rough estimate of the total cost of TNFS for finite fields $\mathbb{F}_{p^k}$ of popular pairing-friendly curves. The companion code is referenced in Section 6.1.3. The results of this paper and the source code were reused to assess the security of pairing-friendly elliptic curves in the context of SNARKs [30], and the polynomial selection implementation was involved in the record computation [4].

7.2.2 Lattice enumeration for Tower NFS: a 521-bit discrete logarithm computation

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

The Tower variant of the Number Field Sieve (TNFS) is known to be asymptotically the most efficient algorithm to solve the discrete logarithm problem in finite fields of medium characteristic, when the extension degree is composite. A major obstacle to an efficient implementation of TNFS is the collection of algebraic relations, as it happens in dimension greater than 2. This requires the construction of new sieving algorithms which remain efficient as the dimension grows. In [4], we overcome this difficulty by considering a lattice enumeration algorithm which we adapt to this specific context. We also consider a new sieving area, a high-dimensional sphere, whereas previous sieving algorithms for the classical NFS considered an orthotope. Our new sieving technique leads to a much smaller running time, despite the larger dimension of the search space, and even when considering a larger target, as demonstrated by a record computation we performed in a 521-bit finite field $\mathbb{F}_{p^6}$. The target finite field is of the same form than finite fields used in recent zero-knowledge proofs in some blockchains. This is the first reported implementation of TNFS.

7.2.3 Refined analysis of the asymptotic complexity of the Number Field Sieve

Participants: Aude Le Gluher, Pierre-Jean Spaenlehauer, Emmanuel Thomé.

The preprint version of this work was written in 2020. This paper was published in 2021 in the new diamond open-access journal *Mathematical Cryptology*.

In [15], we examine how it is possible to refine the asymptotic complexity of the Number Field Sieve. Its most commonly used expression, for the factorization of an n-bit integer, is of the form $\exp((1+o(1))f(n))$. This $(1+o(1))$ factor is present for reasons that pertain to analytic number theoretic results. In practical terms however, this inaccuracy is problematic since it can swallow potentially huge factors. Yet, extrapolations on the hardness of integer factoring, or of finite field discrete logarithms, resort to setting $o(1)=0$ by lack of a better alternative. In [15], we try to see what hides behind $o(1)$. On the positive side, we show that symbolic computation tools can be used to provide an asymptotic expansion to arbitrarily many terms. On the negative side, we show that this expansion is basically useless, as $o(1)$ stands in fact for a series that *diverges* in a range that widely encompasses the practical range. A consequence of this is that predictions of the hardness of, say, 8000-bit RSA, given a data point for 800-bit RSA should be regarded with extreme care.

7.2.4 History of cryptographic key sizes

Participants: Emmanuel Thomé.

The book chapter [23] (online in 2021, to be published in 2022) was written in the context of a festschrift dedicated to Arjen K. Lenstra, and relates the progression of cryptanalysis over several decades, and its impact on the recommendation of key sizes. Both secret- and public-key settings are covered, and in particular the most recent computational records which were obtained by Caramba (and co-authors) using Cado-NFS are of course part of this history.

7.3 Symmetric cryptology

7.3.1 MOE: Multiplication Operated Encryption with Trojan resilience

Participants: Virginie Lallemand.

As most hardware design companies cannot afford having their own foundries, a common strategy consists in outsourcing the production of integrated circuits to external factories. While this solution allows them to reduce the production costs, it brings up the problem of trust in the third party. One of the most feared threats in this respect goes under the name of hardware Trojan, defined as a malicious modification of the circuit design. In this paper [10] we studied the possibility of building a symmetric cipher that would reach Trojan-resilience in an efficient manner. Our concrete proposal is called MOE, acronym for "Multiplication Operated Encryption". It can be implemented using (mostly) untrusted low-cost chips and provides robustness more efficiently than by exploiting secret sharing and multi-party computation on a standard block cipher. MOE exploits a simple round structure mixing a modular multiplication and a multiplication with a binary matrix. Besides being motivated as a new block cipher design for Trojan resilience, our research also exposes the cryptographic properties of the modular multiplication, which is of independent interest.

7.3.2 CTET+: A beyond-birthday-bound secure tweakable enciphering scheme using a single pseudorandom permutation

Participants: Virginie Lallemand, Marine Minier.

In this paper [11], we build upon the results on tweakable SPNs (Single Pseudorandom Permutations) with independent round keys and permutations from CRYPTO 2018 by constructing a 2-round tweakable substitution-permutation network using a single secret S-box. The construction is based on non-linear permutation layers using independent round keys, and achieves security beyond the birthday bound in the random permutation model. When instantiated with an n-bit block cipher with k-bit keys, the resulting tweakable block cipher, dubbed CTET+, can be viewed as a tweakable enciphering scheme that encrypts wn-bit messages for any integer $w > 1$ using $5n + k$-bit keys and n-bit tweaks, providing $2n/3$-bit security.

Furthermore, we propose a concrete instance with $n = 128$ named AES6-CTET+ which is a new tweakable enciphering scheme using a reduced round AES block cipher as the underlying secret S-box.

7.3.3 Efficient methods to search for best differential characteristics on SKINNY

Participants: Marine Minier.

In [19], we propose automatic tools to find the best differential characteristics on the SKINNY block cipher. As usually done in the literature, we split this search in two stages denoted by Step 1 and Step 2. In Step 1, we aim at finding all truncated differential characteristics with a low enough number of active Sboxes. Then, in Step 2, we try to instantiate each difference value while maximizing the overall differential characteristic probability. We solve Step 1 using an ad-hoc method inspired from the work of Fouque et al. whereas Step 2 is modelized for the Choco-solver library as it seems to outperform all previous methods on this stage.

Notably, for SKINNY-128 in the SK model and for 13 rounds, we retrieve the results of Abdelkhalek et al. within a few seconds (instead of 16 days) and we provide, for the first time, the best differential related-tweakey characteristics up to 14 rounds for the TK1 model. Regarding the TK2 and the TK3 models, we were not able to test all the solutions in Step 1, and thus the differential characteristics we found up to 16 and 17 rounds are not necessarily optimal.

7.3.4 Non-triangular self-synchronizing stream ciphers

Participants: Paul Huynh, Marine Minier.

In [12], we propose an instantiation, called Stanislas, of a dedicated Self-Synchronizing Stream Cipher (SSSC) involving an automaton with finite input memory using non-triangular state transition functions. Previous existing SSSCs are based on automata with shifts or triangular functions (T–functions) as state transition functions. Our algorithm Stanislas admits a matrix representation deduced from a general and systematic methodology called Linear Parameter Varying (LPV). This particular representation comes from the control theory, more specifically from a special property of dynamical systems called flatness. Hardware implementations and comparisons with some state-of-the-art stream ciphers on Xilinx FPGAs are presented. It turns out that Stanislas provides bigger throughput than the considered stream ciphers (synchronous and self-synchronizing) when straightforward implementations are considered. Moreover, its synchronization delay is much smaller than the SSSC Moustique (40 clock cycles instead of 105) and the standard approach CFB1-AES128 (40 clock cycles instead of 128).

7.3.5 Hybrid architecture of LPV dynamical systems in the context of cybersecurity

Participants: Marine Minier, Hamid Boukerrou.

The article [21] deals with an hybrid architecture involving LPV dynamical systems for encryption purposes, in the context of cybersecurity. Such an hybrid architecture is motivated by the fact that it is a natural model, recast in a control-theoretic framework, of a so-called statistical self-synchronizing stream cipher. It is shown that flatness is central to guarantee the necessary synchronization between the cipher and the decipher. In this context, beyond synchronization, security must be taken into account as well. We especially focus on diffusion as a security criterion. The hybrid architecture makes it possible to satisfy both properties simultaneously. An illustrative example presents a numerical application and must be considered as a proof-of-concept before further investigation.

7.4 E-voting

7.4.1 A privacy attack on the Swiss Post e-voting system

Participants: Pierrick Gaudry.

The Swiss Post company is in the process of certification of its new e-voting system, to be used by the Swiss Cantons in the course of 2022. In this context, the specification and the source code are gradually revealed for being studied by the community. A private bug bounty program has first been launched and a public bug bounty has followed.

Together with Alexandre Debant and Véronique Cortier, from the PESTO team, we have discovered a privacy issue in the protocol and its implementation that would allow a collusion of a subset of the trust parties to learn the vote of any voter of their choice. This is in contradiction with the trust model imposed by the Federal Chancellery that imposes that privacy should be preserved unless all the trustees are dishonest.

For this result [28], accepted to RWC 2022, we obtained a generous reward from the bug bounty program (40 k euros). The protocol has been fixed, and the certification process continues.

7.4.2 A toolbox for verifiable tally-hiding e-voting systems

Participants: Pierrick Gaudry, Quentin Yang.

In this work [29], we explore the possibility of revealing only the result of an election, without decrypting the individual ballots, or any side-information. The result must be computed in a way such that everyone can verify that it indeed corresponds to the (public) ballot box. Also, even the trust parties who possess the shares of the decryption key should not learn anything more than the winner of the election.

We propose a multi-party computation toolbox dedicated to this kind of problems, and show that it allows us to tackle all famous tally functions, including the most complicated, like the Condorcet-Schulze, D'Hondt, STV, or Majority Judgement. We also explain how the classical ElGamal encryption (typically based on elliptic curves) can be used, instead of the Paillier scheme that is often chosen in theoretical papers, but is far less frequent in standard crypto libraries.

7.5 Quantum security

7.5.1 Quantum period finding against symmetric primitives in practice

Participants: Xavier Bonnetain.

In this work [8], we propose the first full resource estimate of a quantum attack on symmetric ciphers that is not a generic key search. In more details, we give complete quantum circuits for the Offline Simon's algorithm, instanciated to attack the block cipher PRINCE, the MAC (and ISO standard) Chaskey and the authenticated encryption scheme Elephant. This work shows that the attack has reasonable qubit requirements and a low time overhead compared to a simple asymptotic exponent-based analysis.

7.5.2 Quantum linearization attacks

Participants: Xavier Bonnetain.

In this work [17], we introduce the *quantum linearization attack*, which is a novel way to use Simon's algorithm to attack symmetric schemes. It leverages a linear structure inside the construction.

We also present some variants of this attack that use other quantum algorithms, which are much less common in quantum symmetric cryptanalysis: Deutsch's, Bernstein-Vazirani's, and Shor's. To the best of our knowledge, this is the first time these algorithms have been used in quantum forgery or key-recovery attacks.

Our attacks break most parallelizable MACs such as LightMac, PMAC, and numerous variants with (classical) beyond-birthday-bound security (LightMAC+, PMAC) or using tweakable block ciphers (ZMAC). More generally, it shows that constructing parallelizable quantum-secure PRFs might be a challenging task.

7.5.3 QCB: efficient quantum-secure authenticated encryption

Participants: Xavier Bonnetain.

In this work [16], we propose QCB, the first parallelizable rate-one authenticated encryption mode proven secure against quantum superposition attacks. It builds upon a tweakable block cipher and is secure up to the birthday bound.

We also generalize some quantum attacks, which allows us to show that a large class of authenticated encryption modes is broken in a quantum setting, and discuss the quantum security notions for authenticated encryption modes.

7.6 Other

7.6.1 Automated fragment formula annotation for electron ionisation, high resolution mass spectrometry: application to atmospheric measurements of halocarbons

Participants: Aurore Guillevic.

The work [14] has nothing to do with cryptography, except that it uses combinatorics and algorithms to recover structured information from raw data. Somehow, it is a kind of cryptanalysis. It started as an informal discussion between the first two co-authors. In 2019–2021, M. Guillevic was a post-doctoral researcher at EMPA. The companion code is referenced in Section 6.1.4.

7.6.2 The CORE-MATH project

Participants: Paul Zimmermann.

The year 2021 was devoted to the preparation of the CORE-MATH project, which was officially started in 2022. The aim of CORE-MATH 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 (simple precision, double precision, quadruple precision), and also the extended double precision (significand of 64 bits).

In 2021, two functions were implemented for the above four formats: the cubic root function (`cbrt`) and the arc-cosine function (`acos`). In parallel, the article about the accuracy of current mathematical libraries was extended with the help of Vincenzo Innocente to the Apple and CUDA mathematical libraries [31]. This article shows that current mathematical libraries return very different results, and are far from correct rounding, even for rounding to nearest.

7.6.3 Parallel integer multiplication

Participants: Emmanuel Thomé, Samuel Vivien, Paul Zimmermann.

During his L3 internship, Samuel Vivien designed a parallel integer multiplication algorithm and did efficiently implement it on top of GNU MP. His implementation outperforms the Flint library, which is the only other software tool providing parallel integer multiplication. For example, on a 32-core Xeon Gold, a speedup of 20 is obtained for the multiplication of two integers of 10^7 words of 64 bits (over the sequential code). The article describing this work has been accepted to the 30th Euromicro International Conference on Parallel, Distributed and Network-based Processing (PDP 2022) [20].

8 Bilateral contracts and grants with industry

8.1 Bilateral contracts with industry

Participants: Pierrick Gaudry.

Together with the PESTO team, we had a short contract with Swiss Post. The goal was to update the formal proofs of their e-voting protocol, in order to follow its evolution and to fix a few problems.

9 Partnerships and cooperations

9.1 International initiatives

9.1.1 Informal International Partners

Participants: Marine Minier, Virginie Lallemand.

Since January 2020 a virtual center for cybersecurity has been established between LORIA and CISPA in Saarbrucken (Germany). This virtual center is led by Marine Minier for LORIA and by Antoine Joux for CISPA.

9.2 International research visitors

9.2.1 Visits to international teams

Sabbatical programme

Emmanuel Thomé

Visited institution: University of California San Diego (États-Unis)

Dates of the stay: From Sun Aug 01 2021 to Sun Jul 31 2022

Summary of the stay: E. Thomé is visiting N. Heninger, associate professor in the Security and Cryptography group at University of California San Diego (UCSD). More precisely, the research topics of E. Thomé during his stay at UCSD are:

- Preparation for larger factoring and discrete logarithm computations.
- Better hardness estimates for the Number Field Sieve.
- Further development of the Factoring-as-a-service tool.

Aurore Guillevic

Visited institution: Aarhus Universitet (Danemark)

Dates of the stay: From Sun Aug 01 2021 to Sun Jul 31 2022

Summary of the stay: A. Guillevic is visiting Diego F. Aranha, associate professor in the Cryptography and Security Group led by Ivan P. Damgård. A. Guillevic is working on

- More precise estimates of the Special-Tower-NFS algorithm in extension fields GF(p^n) from pairing-based cryptographic examples such as GF(p^{12}) where p has a polynomial form (BN curves, BLS curves). This is based on [13] and the library in Section 6.1.3.
- A short-list of pairing-friendly curves at the 192-bit security level. Based on the results of the previous item, with Diego Aranha (Aarhus University) and Georgios Fotiadis from the University of Luxembourg, the work [33] will be extended to the 192-bit security level.
- Elliptic curves for SNARK, with Youssef El Housni, see Section 7.1.1.
- SageMath/Python implementation of pairings and pairing-friendly curves, for now this is released as a compagnion code with [30], see Section 6.1.5.
- Elliptic curves for isogenies and post-quantum cryptography.

A. Guillevic will be teaching in the Spring semester from January 31 to May 20 the Master course *Elliptic Curves, Number Theory and Cryptography*.

9.3 National initiatives

9.3.1 ANR Decrypt

Participants: Marine Minier, Virginie Lallemand.

- Program: ANR
- Project acronym: DECRYPT
- Duration: 01/2019 - 12/2022
- Coordinator: Caramba Team, LORIA
- Other partners: LIRIS (Lyon), LIMOS (Clermont-Ferrand), IRISA (Rennes), TASC (Nantes).

This project aims 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 will be to define global constraints dedicated to the case of symmetric cryptography.

Concerning constraint programming, this project will define new dedicated global constraints, will improve the underlying filtering and solution search algorithms, and will propose dedicated explanations generated automatically. See web site for more information.

10 Dissemination

10.1 Promoting scientific activities

10.1.1 Scientific events: organisation

- Pierre-Jean Spaenlehauer is a member of the organisation committee of the Journées Nationales du Calcul Formel 2022.

10.1.2 Scientific events: selection

Member of conference program committees

- Aurore Guillevic was PC member of IACR Asiacrypt'2021 and Latincrypt'2021.
- Marine Minier was PC member of Latincrypt'2021.
- Pierre-Jean Spaenlehauer was a member of the software presentation committee of ISSAC'2021.
- Pierrick Gaudry was a PC member of the CT-RSA 2022, PKC 2022 and Eurocrypt 2022 conferences.

10.1.3 Journals

Member of editorial boards

- Xavier Bonnetain, Sébastien Duval and Virginie Lallemand are members of the editorial board of the IACR Transactions on Symmetric Cryptology (ToSC) Journal for 2021. This journal is the open-access journal associated to the International Conference on Fast Software Encryption (FSE).
- Since October 2021, Emmanuel Thomé is a member of the editorial board of the *Computational Algebra* section of the Journal of 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.

Paul Zimmermann also did a review of the article *Integer Points Close to a Transcendental Curve and Correctly-Rounded Evaluation of a Function* by Nicolas Brisebarre and Guillaume Hanrot (AriC project-team, Inria Rhône-Alpes), and tested the accompanying software tools. His comments are taken into account in the latest version [36].

10.1.4 Invited talks

- Virginie Lallemand was invited to give a (remote) talk at the Séminaire Crypto & Sécurité of the GREYC Research Laboratory of Caen in June 2021. She also was invited to give two talks at the CISPA-LORIA workshops (February and November).
- Marine Minier was invited to give a talk to Cyber in Saclay, winter school of the GDR sécurité in February 2021.
- Cécile Pierrot was invited to give a talk to the Tutte Colloquium, University of Waterloo in June 2021.
- Xavier Bonnetain was invited to give two talks during the Dagstuhl Seminar 21421 on Quantum Cryptanalysis in October 2021.
- Aurore Guillevic was invited to give a talk at the online Journées Nationales Informatique Mathématique (Journées du GDR-IM), March 16.
- Paul Zimmermann was invited to give a talk at the online CaSToRC HPC Seminar Series (Cyprus Supercomputing Center), November 16.

10.1.5 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 du GdR IM.

10.1.6 Scientific expertise

- Pierrick Gaudry was a member of a jury for the Innoviris LAUNCH program, whose goal is to fund start-ups created on the basis of academic work.
- Paul Zimmermann was a reviewer for the “Appel à projets Emergence” for Sorbonne University (France).
- Jean-Michel Muller (AriC project-team, Inria Rhône-Alpes) and Paul Zimmermann were contacted by Andrew Haley to review the “Shubfach” algorithm proposed by Raffaello Giulietti for the double to string conversion (latest version here). This algorithm takes as input a binary64 number, and outputs a decimal string with minimal length so that, if we convert back that string to binary64 with rounding to nearest, we recover the original number. The corresponding OpenJDK patch had been stuck as an open pull request for nearly two years because of the difficulty of verifying the algorithm's correctness. A public review was made, which confirmed the correctness of the algorithm, and the OpenJDK patch will be included in the next release.

10.1.7 Research administration

- Marine Minier is (since September 2021) assistant director of the LORIA laboratory.
- Marine Minier is responsible for the LORIA laboratory of the cybersecurity axis.

- Marine Minier is co-head (with Antoine Joux from CISPA) of the German-French virtual center for cybersecurity between LORIA and CISPA (Saarbrucken, Germany).
- Marine Minier is the scientific head of the LUE[4] impact project DigiTrust (2018-2022, 2,2 Meuro).
- Marine Minier is an elected member of the Collégium "sciences et techniques" from University of Lorraine.
- Marine Minier is a member of the steering committee of the LHS – Laboratoire Haute Sécurité of LORIA.
- Marine Minier was president of the "comité de spécialistes" of the "poste 27MCF1352", and member of the "comité de spécialistes" of the "poste 27PR4310".
- Pierre-Jean Spaenlehauer is a member of the *Commission des Développements Technologiques* of the Inria Nancy – Grand Est research center.
- Pierrick Gaudry was a member of the hiring committee for two Professors in mathematics (25) in the Institut de Mathématiques de Jussieu-Paris Rive Gauche.
- Pierrick Gaudry is a member of the steering committee of the LHS – Laboratoire Haute Sécurité of LORIA.
- Cécile Pierrot is a member of the Comité de Centre Inria Nancy - Grand Est.
- Cécile Pierrot is a member of the working group concerning remote work at Inria.
- Cécile Pierrot is a leader and member of the local group for integration of young researchers in Nancy (Loria, Inria) and Strasbourg (Inria).
- Paul Zimmermann is member of the scientific committee of the EXPLOR computing center (Université de Lorraine).

10.2 Teaching - Supervision - Juries

10.2.1 Teaching

- Bachelor
  - Pierrick Gaudry, *Intégration Web*, 48h eq. TD, IUT 1A, Université de Lorraine, IUT Charlemagne, Nancy, France.
  - Sébastien Duval, *Algorithmique et Programmation 3*, 28h eq. TD, L2 Informatique, Université de Lorraine, Faculté des sciences et technologies, Vandœuvre-lès-Nancy, France.
  - Marine Minier, *Introduction à la sécurité et à la cryptographie*, 35h eq. TD, L3, Université de Lorraine, Faculté des sciences et technologies, Vandœuvre-lès-Nancy, France.
  - Marine Minier, *Mathématiques Discrètes*, 80h eq. TD, L2, Université de Lorraine, Faculté des sciences et technologies, Vandœuvre-lès-Nancy, France.
- Master
  - Sébastien Duval, *Analyse et Conception de Logiciels*, 22h 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.

[4] (Lorraine Université d'Excellence, I-SITE project)

  - Pierre-Jean Spaenlehauer, *Théorie analytique des nombres, géométrie algébrique, et applications à la cryptographie*, 24h eq. TD, M2 Mathématiques Fondamentales et Appliquées, 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.
  - 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, Université de Lorraine.
  - Marine Minier is head of the M2 SIRAV, Université de Lorraine, Faculté des sciences et technologies, Vandœuvre-lès-Nancy, France.

- Engineering school
  - Aurore Guillevic, *RSA, Integer Factorization, record computations*, 1h30 guest lecture, Master, MIT, Cambridge MA, Course 6.857: Computer and Network Security, Spring 2021
  - Cécile Pierrot, *Introduction to Modern Cryptography*, 27h eq. TD, Second year of Engineering school, TELECOM Nancy, France.
  - Cécile Pierrot, *Cryptography and Communication*, 15h eq. TD, Second year of Engineering school, TELECOM Nancy, France.
  - Cécile Pierrot, *Introduction to Cryptography*, 54h eq. TD, Mastère spécialisé de cybersécurité, École des Mines de Nancy, France.
  - Haetham AL ASWAD, *Programming and Data Structures: Python*, 22h eq. TD, First year of Engineering, École des Mines de Nancy, France.
  - Antoine Leudière, *Programming and Data Structures: Python*, 22h eq. TD, First year of Engineering, École des Mines de Nancy, France.

10.2.2 Supervision

- Ph.D.: Gabrielle De Micheli, *Discrete Logarithm Cryptanalyses : Number Field Sieve and Lattice Tools for Side-Channel Attacks*, Université de Lorraine, defended May 25, 2021, advised by Cécile Pierrot and Pierrick Gaudry [24].
- Ph.D.: Aude Le Gluher, *Symbolic Computation and Complexity Analyses for Number Theory and Cryptography*, Université de Lorraine, defended December 7, 2021, advised by Pierre-Jean Spaenlehauer and Emmanuel Thomé [25].
- 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: Loïc Rouquette, *Constraint Programming for symmetric key cryptography*, since Oct. 2019, Christine Solnon and Marine Minier, Ph.D. in Lyon.
- Ph.D. in progress: Hamid Boukerrou, *Control Theory for stream ciphers*, since Oct. 2019, Gilles Millerioux and Marine Minier, Ph.D. in the CRAN Lab.

10.2.3 Juries

- Virginie Lallemand was member of the PhD thesis jury *Selected Topics in Cryptanalysis of Symmetric Ciphers* defended by John-Petter Indrøy, October 2021, University of Bergen (Norway).
- Aurore Guillevic was reviewer of the PhD thesis *Conception de courbes elliptiques et applications* defended by Rémi Clarisse, December 16, 2021, Université de Rennes 1.
- Pierrick Gaudry was a member of the PhD thesis jury *Isolating the Singularities of the Plane Projection of Generic Space Curves and Applications in Robotics* defended by George Krait, May 2021, Université de Lorraine.
- Marine Minier was reviewer of the PhD thesis *Techniques de cryptanalyse dédiées au chiffrement à bas coût* defended by Daniele Coggia, October 8 2021, Sorbonne Université.
- Marine Minier was reviewer of the PhD thesis *La sécurité et l'optimisation des chaines à blocs et algorithmes associés* defended by Mirko Koscina, October 5 2021, Université Paris Sciences et Lettres.
- Marine Minier was reviewer of the PhD thesis *Modélisation de réseaux IoT hétérogènes à des fins d'évaluation de sécurité* defended by Jonathan Tournier, March 10 2021, Université de Lyon.
- Marine Minier was reviewer of the PhD thesis *On GDPR Compliant Data Processing* defended by Supriya Adhatarao, July 22 2021, Université Grenoble Alpes.
- Marine Minier was president of the PhD thesis *Conception, analyse et implémentation d'algorithmes de chiffrement symétrique sur FPGA* defended by Loïc Besson, December 22 2021, Université de Versailles Saint Quentin en Yvelines.
- Paul Zimmermann was reviewer and member of the PhD thesis *Software-based approximate computing for mathematical functions* defended by Nicholas Gerard Timmons on June 18, 2021, Cambridge University.
- Paul Zimmermann was reviewer of the PhD thesis *Building a Formally Verified High-Performance Multi-Platform Cryptographic Library in F** by Marina Polubelova, to be defended in 2022, PSL University (Paris, France).

10.3 Popularization

10.3.1 Interventions

- Cécile Pierrot, Pierre-Jean Spaenlehauer and Paul Zimmermann are involved in the animation of a MATh. en. JEANS activity at the Lycée Vauban, Luxembourg.
- Cécile Pierrot took part to the event "Chiche ! Une classe, un chercheur" that intends to present computer science studies and careers to young people. She met 5 groups of 30 students each at Lycée Margueritte, Verdun, France.

10.3.2 Education

- Cécile Pierrot was invited to take part to discussions about the NSI (Numérique et Science Informatique) courses with highschool teachers from Académie de Reims, France.

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] 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://hal.inria.fr/hal-02863525.

[3] G. De Micheli, P. Gaudry and C. Pierrot. 'Asymptotic complexities of discrete logarithm algorithms in pairing-relevant finite fields'. In: *Annual International Cryptology Conference*. CRYPTO 2020 - 40th Annual International Cryptology Conference. Vol. 12171. Lecture Notes in Computer Science. Santa Barbara / Virtual, United States: Springer, 2020, pp. 32–61. URL: https://hal.archives-ouvertes.fr/hal-02871839.

[4] G. De Micheli, P. Gaudry and C. Pierrot. 'Lattice Enumeration for Tower NFS: a 521-bit Discrete Logarithm Computation'. In: Asiacrypt 2021. Vol. 13090. ASIACRYPT. Virtual, Singapore: Springer, 2021, pp. 67–96. DOI: 10.1007/978-3-030-92062-3_3. URL: https://hal.inria.fr/hal-03242324.

[5] P. Derbez, P. Huynh, V. Lallemand, M. Naya-Plasencia, L. Perrin and A. Schrottenloher. 'Cryptanalysis Results on Spook: Bringing Full-round Shadow-512 to the Light'. In: CRYPTO 2020 - 40th Annual International Cryptology Conference. Vol. 12172. Lecture Notes in Computer Science. Santa Barbara / Virtual, United States, 10th Aug. 2020, pp. 359–388. DOI: 10.1007/978-3-030-56877-1_13. URL: https://hal.inria.fr/hal-02944908.

[6] D. Gérault, P. Lafourcade, M. Minier and C. Solnon. 'Computing AES related-key differential characteristics with constraint programming'. In: *Artificial Intelligence* 278 (Jan. 2020), p. 103183. DOI: 10.1016/j.artint.2019.103183. URL: https://hal.archives-ouvertes.fr/hal-02327893.

11.2 Publications of the year

International journals

[7] M. Alekseyev, J. S. Myers, R. Schroeppel, S. R. Shannon, N. J. A. Sloane and P. Zimmermann. 'Three Cousins of Recamán's Sequence'. In: *The Fibonacci Quarterly* (2021). URL: https://hal.inria.fr/hal-02951011.

[8] X. Bonnetain and S. Jaques. 'Quantum Period Finding against Symmetric Primitives in Practice'. In: *IACR Transactions on Cryptographic Hardware and Embedded Systems* 2022.1 (19th Nov. 2021), pp. 1–27. DOI: 10.46586/tches.v2022.i1.1-27. URL: https://hal.inria.fr/hal-03431518.

[9] C. Bouillaguet and P. Zimmermann. 'Parallel Structured Gaussian Elimination for the Number Field Sieve'. In: *Mathematical Cryptology* 0.1 (8th Jan. 2021), pp. 22–39. URL: https://hal.inria.fr/hal-02098114.

[10] O. Bronchain, S. Faust, V. Lallemand, G. Leander, L. Perrin and F.-X. Standaert. 'MOE: Multiplication Operated Encryption with Trojan Resilience'. In: *IACR Transactions on Symmetric Cryptology* 2021.1 (19th Mar. 2021), pp. 78–129. DOI: 10.46586/tosc.v2021.i1.78-129. URL: https://hal.inria.fr/hal-03453550.

[11] B. Cogliati, J. Ethan, V. Lallemand, B. Lee, J. Lee and M. Minier. 'CTET+: A Beyond-Birthday-Bound Secure Tweakable Enciphering Scheme Using a Single Pseudorandom Permutation'. In: *IACR Transactions on Symmetric Cryptology* 2021.4 (3rd Dec. 2021), pp. 1–35. DOI: 10.46586/tosc.v2021.i4.1-35. URL: https://hal.inria.fr/hal-03504330.

[12] 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.archives-ouvertes.fr/hal-03081725.

[13] A. Guillevic and S. Singh. 'On the Alpha Value of Polynomials in the Tower Number Field Sieve Algorithm'. In: *Mathematical Cryptology* 1.1 (19th Feb. 2021), pp. 1–39. URL: https://hal.inria.fr/hal-02263098.

[14] M. Guillevic, A. Guillevic, M. K. Vollmer, P. Schlauri, M. Hill, L. Emmenegger and S. Reimann. 'Automated fragment formula annotation for electron ionisation, high resolution mass spectrometry: application to atmospheric measurements of halocarbons'. In: *Journal of Cheminformatics* 13.78 (4th Oct. 2021), pp. 1–27. DOI: 10.1186/s13321-021-00544-w. URL: https://hal.inria.fr/hal-03176025.

[15] A. Le Gluher, P.-J. Spaenlehauer and E. Thomé. 'Refined Analysis of the Asymptotic Complexity of the Number Field Sieve'. In: *Mathematical Cryptology* 1.1 (2021), pp. 71–88. URL: https://hal.inria.fr/hal-02934273.

International peer-reviewed conferences

[16] R. Bhaumik, X. Bonnetain, A. Chailloux, G. Leurent, M. Naya-Plasencia, A. Schrottenloher and Y. Seurin. 'QCB: Efficient Quantum-Secure Authenticated Encryption'. 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. 668–698. DOI: 10.1007/978-3-030-92062-3_23. URL: https://hal.inria.fr/hal-03516739.

[17] 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.

[18] G. De Micheli, P. Gaudry and C. Pierrot. 'Lattice Enumeration for Tower NFS: a 521-bit Discrete Logarithm Computation'. In: ASIACRYPT 2021 - 27th Annual International Conference on the Theory and Application of Cryptology and Information Security. Vol. 13090. ASIACRYPT. Virtual, Singapore: Springer, 2021, pp. 67–96. DOI: 10.1007/978-3-030-92062-3_3. URL: https://hal.inria.fr/hal-03242324.

[19] S. Delaune, P. Derbez, P. Huynh, M. Minier, V. Mollimard and C. Prud'Homme. 'Efficient Methods to Search for Best Differential Characteristics on SKINNY'. In: *Proceedings of the 19th International Conference on Applied Cryptography and Network Security*. ACNS 2021 - 19th International Conference on Applied Cryptography and Network Security. Vol. 12727. 19th International Conference on Applied Cryptography and Network Security. Kamakura, Japan, 21st June 2021, pp. 184–207. DOI: 10.1007/978-3-030-78375-4_8. URL: https://hal.archives-ouvertes.fr/hal-03040548.

[20] S. Vivien. 'Parallel integer multiplication'. In: *30th Euromicro International Conference on Parallel, Distributed andNetwork-based Processing (PDP 2022)*. PDP 2022 - 30th Euromicron International Conference on Parallel, Distributed, and Network-Based Processing. Valladoid, Spain, 2022. URL: https://hal.archives-ouvertes.fr/hal-03541726.

Conferences without proceedings

[21] H. Boukerrou, G. Millérioux and M. Minier. 'Hybrid architecture of LPV dynamical systems in the context of cybersecurity'. In: LPVS 2021 - 4th IFAC Workshop on Linear Parameter Varying Systems. Milano, Italy, 19th July 2021. URL: https://hal.archives-ouvertes.fr/hal-03292416.

[22] C. Nugier, D. Leblanc-Albarel, A. Blaise, S. Masson, P. Huynh and Y. B. Wandji Piugie. 'An Upcycling Tokenization Method for Credit Card Numbers'. In: SECRYPT 2021 - 18th International Conference on Security and Cryptography. Online, France, July 2021. URL: https://hal.archives-ouvertes.fr/hal-03220739.

Scientific book chapters

[23] N. P. Smart and E. Thomé. 'History of Cryptographic Key Sizes'. In: *Computational Cryptography*. Vol. 469. London Mathematical Society Lecture Note Series. Cambridge University Press, Dec. 2021. URL: https://hal.inria.fr/hal-03408015.

Doctoral dissertations and habilitation theses

[24] G. De Micheli. 'Discrete Logarithm Cryptanalyses : Number Field Sieve and Lattice Tools for Side-Channel Attacks'. Université de Lorraine, 25th May 2021. URL: https://hal.univ-lorraine.fr/tel-03335360.

[25] A. Le Gluher. 'Symbolic Computation and Complexity Analyses for Number Theory and Cryptography'. Université de Lorraine, 7th Dec. 2021. URL: https://hal.univ-lorraine.fr/tel-03564208.

Reports & preprints

[26] A. Canteaut, M. A. Fernández, L. Maranget, S. Perin, M. Ricchiuto, M. Serrano and E. Thomé. *Évaluation des Logiciels*. Inria, 14th Jan. 2021. URL: https://hal.inria.fr/hal-03110723.

[27] A. Canteaut, M. A. Fernández, L. Maranget, S. Perin, M. Ricchiuto, M. Serrano and E. Thomé. *Software Evaluation*. Inria, 14th Jan. 2021. URL: https://hal.inria.fr/hal-03110728.

[28] V. Cortier, A. Debant and P. Gaudry. *A privacy attack on the Swiss Post e-voting system*. Université de Lorraine, CNRS, Inria, LORIA, 24th Nov. 2021. URL: https://hal.inria.fr/hal-03446801.

[29] V. Cortier, P. Gaudry and Q. Yang. *A toolbox for verifiable tally-hiding e-voting systems*. 16th Apr. 2021. URL: https://hal.inria.fr/hal-03367930.

[30] Y. El Housni and A. Guillevic. *Families of SNARK-friendly 2-chains of elliptic curves*. 8th Oct. 2021. URL: https://hal.inria.fr/hal-03371573.

[31] V. Innocente and P. Zimmermann. *Accuracy of Mathematical Functions in Single, Double, Extended Double and Quadruple Precision*. 10th Jan. 2022. URL: https://hal.inria.fr/hal-03141101.

11.3 Cited publications

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

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

[34] 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.

[35] Agence nationale de la sécurité des systèmes d'information. *Référentiel général de sécurité, annexe B1*. Version 2.03. 2014. URL: http://www.ssi.gouv.fr/uploads/2014/11/RGS_v-2-0_B1.pdf.

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

[37] 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.

[38] 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.

[39] 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.