RESEARCH CENTRE

Nancy - Grand Est

IN PARTNERSHIP WITH:

CNRS, Université de Lorraine

2020
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 Team: 2016 January 01, updated into 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

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]
- 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 Member

- Marine Minier [Univ de Lorraine, Professor, HDR]

Post-Doctoral Fellow

- Bimal Mandal [Inria, until Feb 2020]

PhD Students

- Hamid Boukerrou [Univ de Lorraine]
- Gabrielle De Micheli [Inria]
- Le Phuc Huynh [CNRS]
- Aude Le Gluher [Univ de Lorraine]
- Simon Masson [Thales, CIFRE]
- Andrianina Sandra Rasoamiaramanana [Orange Gardens, CIFRE, until May 2020]
- Quentin Yang [Inria, from Oct 2020]

Interns and Apprentices

- Ambroise Baudot [Univ de Lorraine, from Mar 2020 until Aug 2020]
- Marc Simard [Univ de Lorraine, from Oct 2020]

Administrative Assistants

- Emmanuelle Deschamps [Inria]
- Virginie Priester [CNRS]

Visiting Scientist

- Santanu Sarkar [Indian Institute of Technology Bombay, until Feb 2020]

External Collaborators

- Gilles Millérioux [Univ de Lorraine, until Oct 2020]
- 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 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.

  One of the challenges we address here is point counting. In a wider perspective, we also study the link between abelian varieties over finite fields and principally polarized abelian varieties over fields of characteristic zero, together with their endomorphism ring. In particular, we work in the direction of making this link an effective one. We are also investigating various approaches for attacking the discrete logarithm problem in Jacobians of algebraic curves. Questions more recently studied include the development of cryptosystems based on isogenies.

- Symmetric key cryptography. This topic has emerged recently in the team, with the recruiting of Marine Minier and Virginie Lallemand. 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.

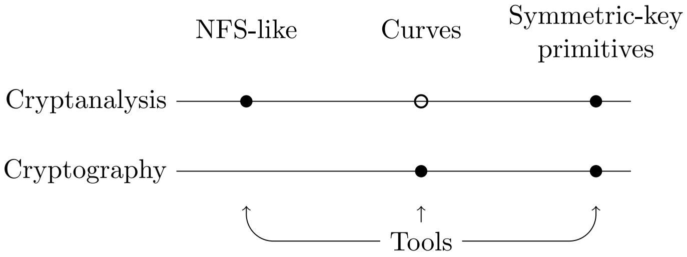

Figure 1: Visual representation of the thematic organization of CARAMBA. Solid dots: major interaction; clear dots: minor interaction.

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.

- 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). In Lausanne, 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. With the standardization of TLS 1.3 in 2018 [35], the curves x25519 and x448 have entered the base specification of the standard. These curves were designed by academia and offer an excellent compromise between efficiency and security.

On the cryptanalytic side, the discrete logarithm problem on (Jacobians of) curves has resisted all attempts for many years. Among the currently active topics, the decomposition algorithms raise interesting problems related to polynomial system solving, as do attempts to solve the discrete logarithm problem on curves defined over binary fields. In particular, while it is generally accepted that the so-called Koblitz curves (base field extensions of curves defined over GF(2)) are likely to be a weak class among the various curve choices, no concrete attack supports this claim fully.

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

- Work on the practical realization of some of the rich mathematical theory behind algebraic curves. In particular, some of the fundamental mathematical objects have potentially important connections to the broad topic of cryptology: Abel-Jacobi map, Theta functions, computation of isogenies, computation of endomorphisms, complex multiplication.
- Improve the point counting algorithms so as to be able to tackle larger problems. This includes significant work connected to polynomial systems.
- Seek improvements on the computation of discrete logarithms on curves, including by identifying weak instances of this problem.

3.3 Symmetric Cryptography

Since the recruiting of Marine Minier in September 2016 as a Professor at the Université de Lorraine, and of Virginie Lallemand as a CNRS researcher in October 2018, a new research domain has emerged in the CARAMBA team: symmetric key cryptology. Accompanied in this adventure by non-permanent team members, we are tackling problems related to both design and analysis. A large part of our recent researches 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 finding 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.

[1] National Institute of Standard and Technology.

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 (we rarely, if ever, focus on small-precision floating-point data, which explains our lack of mention of libraries relevant to it).

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.

3.5 Polynomial Systems

Systems of polynomial equations have been part of the cryptographic landscape for quite some time, with applications to the cryptanalysis of block and stream ciphers, as well as multivariate cryptographic primitives.

Polynomial systems arising from cryptology are usually not generic, in the sense that they have some distinct structural properties, such as symmetries, or bi-linearity for example. During the last decades, several results have shown that identifying and exploiting these structures can lead to dedicated Gröbner basis algorithms that can achieve large speedups compared to generic implementations [29, 30].

Solving polynomial systems is well done by existing software, and duplicating this effort is not relevant. However we develop test-bed open-source software for ideas relevant to the specific polynomial systems that arise in the context of our applications. The TinyGB software is our platform to test new ideas.

We aim to work on the topic of polynomial system solving in connection with our involvement in the aforementioned topics.

- We have high expertise on Elliptic Curve Cryptography in general. On the narrower topic of the Elliptic Curve Discrete Logarithm Problem on small characteristic finite fields, the highly structured polynomial systems that are involved match well our expertise on the topic of polynomial systems. Once a very hot topic in 2015, activity on this precise problem seems to have slowed down. Yet, the conjunction of skills that we have may lead to results in this direction in the future.

- More centered on polynomial systems *per se*, we will mainly pursue the study of the specificities of the polynomial systems that are strongly linked to our targeted applications, and for which we have significant expertise [29, 30]. We also want to see these recent results provide practical benefits compared to existing software, in particular for systems relevant for cryptanalysis.

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 [26] 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.

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[4], 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

On February 28th, 2020, the factorization of RSA-250 was announced.

[2] In [27], 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 [32] is one of only two academic works cited by NIST in the initial version (2011) of the report [34].

[4] [36]

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: Belenios now supports verifiable mixnets for the tally procedure. Mixnets allow to shuffle and randomize ballots so that ballots can no longer be linked to the original ones. Then ballots can be decrypted one by one, yielding the set of the original votes, in a random order. As a result, arbitrary type of elections can be organized with Belenios, where voters rank or grade the candidates. Belenios offers a complete support of Condorcet, STV, and Majority Judgement but any function can be applied to the raw results.

Moreover, Belenios now features crowd-sourcing for translating the voter and the administrator interface. Anyone can contribute on https://hosted.weblate.org/projects/belenios/. Thanks to this development, Belenios now offers a dozen of languages.

Due to the pandemic, the use of our voting platform has increased by a factor of 10 in 2020, with more than 1400 elections organized with our platform and a cumulated total of more than 100 000 voters.

URL: http://www.belenios.org/

Authors: Stéphane Glondu, Pierrick Gaudry, Véronique Cortier

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: Cado-NFS has undergone little important change during year 2020. However, some specific parts of the code have been improved. - the simulation code that is used to try to predict matrix sizes is evolving. - the I/O layer in the linear algebra code has been simplified. - the central step of binary linear algebra is being prepared for an improvement of some operations that are currently costlier than they should be. - cofactorisation code has been improved.

Additionally, Cado-NFS has moved to the Inria gitlab platform. At this point, there is no certainty as to the permanent URL of the Cado-NFS software.

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

Authors: Pierrick Gaudry, Laurent Gremy, François Morain, Emmanuel Thomé, Paul Zimmermann

Contacts: Pierrick Gaudry, Emmanuel Thomé, Paul Zimmermann

Participants: Pierrick Gaudry, Emmanuel Thomé, Paul Zimmermann

6.1.3 BW6-761

Name: Brezing-Weng-6 761 bits

Keywords: Cryptography, Blockchain

Functional Description: This small library implements finite field and elliptic curve arithmetic for the chain of curves BLS12-381 and BW6-761 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 and is not optimized. An optimized implementation is developed in C++ at https://github.com/EYBlockchain/zk-swap-libff/tree/ey/libff/algebra/curves/bw6_761 and in Rust at https://github.com/yelhousni/zexe/tree/youssef/BW6-761-Fq-ABLR-2ML-M

URL: `https://gitlab.inria.fr/zk-curves/bw6-761/`

Publication: hal-02962800

Contacts: Youssef El Housni, Aurore Guillevic

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 generalisation to extensions of the exact implementation of alpha in the software cado-nfs. The software contains an implementation of the estimator E of B. A. Murphy (Murphy's E) of the quality of the choices polynomials 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-02263098, hal-02396352

Contacts: Aurore Guillevic, Shashank Singh

6.2 New platforms

Since 2018, the CARAMBA team has been using in particular a computer cluster called `grvingt`, acquired in 2018. This equipment was funded by the CPER «CyberEntreprises» (French Ministry of Research, Région Grand Est, Inria, CNRS) and comprises a 64-node, 2,048-core cluster. This cluster is installed in the Inria facility. Other slightly older hardware (a medium-size cluster called `grcinq` from 2013, funded by ANR, and a special machine funded by the aforementioned CPER grant) is also installed in the same location, to form a coherent platform with about 3,000 cpu cores, 100 TB of storage, and specific machines for RAM-demanding computations. As a whole, this platform provides an excellent support for the computational part of the work done in CARAMBA. This platform is also embedded in the larger Grid'5000/Silecs platform (and accessible as a normal resource within this platform). Technical administration is done by the Grid'5000 staff.

This equipment has played a key role in the record factorization of RSA-240 done in February 2020, as well as the computation of discrete logarithms modulo a 240-digit prime, completed at the end of 2019.

7 New results

7.1 Algebraic Curves for Cryptology

7.1.1 Cocks-Pinch Curves of Embedding Degrees Five to Eight and Optimal Ate Pairing Computation

Participants Aurore Guillevic, Simon Masson, Emmanuel Thomé.

The preprint version of [7] appeared in the report of 2019, this paper was published in 2020 in the journal *Designs, Codes and Cryptography*. In this work we explored a modification of the Cocks-Pinch method to generate pairing-friendly curves resistant to the Special-Tower-NFS algorithm (STNFS). We carefully estimated the cost of the STNFS attack for existing families of curves, and chose curves of embedding degree five to eight. For prime embedding degrees 5 and 7, our curves are naturally immune to the STNFS attack, but their performance level is not high. For composite embedding degrees 6 and 8 for which the TNFS attack applies, we chose the parameters from a family that is general enough to thwart the "special" variant STNFS; we also optimized these parameter choices so that these curves can have a reasonably efficient pairing computation, close with the very best possible curve choices.

7.1.2 A Short-List of Pairing-Friendly Curves Resistant to Special TNFS at the 128-bit Security Level

Participants Aurore Guillevic.

The preprint version of [16] appeared in the report of 2019, this paper was published in 2020 in the proceedings of the (online) conference *Public Key Cryptography*, together with a 20' video at `https://youtube.com/watch?v=Nk69Ltmb5jY`. This paper applies the refinements of the paper [8] to estimate the cost of the Special Tower NFS algorithm for particular pairing-friendly curves, whose target group is $\mathbb{F}_{p^n}$, and where the characteristic is special, parameterized by a low degree polynomial. We show that with a new variant of the polynomial selection, the estimated cost is reduced, but stays above the theoretical bound of the Special NFS $L_{p^n}(1/3, (32/9)^{1/3})$. This variant does not apply to the Cocks-Pinch curves of [7]. We list nine interesting pairing-friendly curves of embedding degrees between 10 and 16 at the 128-bit security level. This paper was completed with a webpage listing pairing-friendly curves at `https://members.loria.fr/AGuillevic/pairing-friendly-curves/`.

7.1.3 Optimized and secure pairing-friendly elliptic curves suitable for one layer proof composition

Participants Aurore Guillevic.

This work with Youssef El Housni, PhD student in the GRACE team at Inria Saclay and at EY–Ernst & Young (now at ConsenSys), selects a new elliptic curve for SNARKs (Succint Non-interactive ARguments of Knowledge) [14]. The curve is named BW6-761 for a Brezing–Weng pairing-friendly curve of embedding degree 6 and defined over a 761-bit prime field. The curve is dedicated for recursive proofs of knowledge from Groth [31]. The curve is coined with the elliptic curve BLS12-377, a Barreto–Lynn–Scott pairing-friendly curve over a 377-bit prime field $\mathbb{F}_p$. For recursive proofs, the prime subgroup order of the curve BW6-761 is p, the base field of the curve BLS12-377. The new curve BW6-761 is an improvement of the *ZEXE* curve [28] and provides a faster arithmetic; in particular, faster scalar multiplication and much faster pairing computation, resulting in a 30–fold speed-up in Groth'16 proof verification in RUST. The curve is deployed in many SNARK libraries and listed in Ethereum Improvement Proposals (EIP). The security estimate of the new curve uses [7] and [8]. This joint work will be continued in 2021.

7.1.4 A Practical Attack on ECDSA Implementations Using wNAF Representation

Participants Gabrielle De Micheli, Cécile Pierrot, Rémi Piau.

The preprint version of [13] appeared in the report of 2019, this paper was published in 2020 in the proceedings of the (online) conference *Africacrypt 2020*. ECDSA is a widely deployed public key signature protocol that uses elliptic curves. One way of attacking ECDSA with wNAF implementation for the scalar multiplication is to perform a side-channel analysis to collect information, then use a lattice based method to recover the secret key. In [13], we re-investigate the construction of the lattice used in one of these methods, the Extended Hidden Number Problem (EHNP). We find the secret key with only 3 signatures, thus reaching the theoretical bound never achieved before. Our attack is more efficient than previous attacks, has better probability of success, and is still able to find the secret key with a small amount of erroneous traces, up to 2% of false digits.

7.1.5 Recovering cryptographic keys from partial information, by example

Participants Gabrielle De Micheli.

Side-channel attacks targeting cryptography may leak only partial or indirect information about the secret keys. There are a variety of techniques in the literature for recovering secret keys from partial information. In this tutorial [22], we survey several of the main families of partial key recovery algorithms for RSA, (EC)DSA, and (elliptic curve) Diffie-Hellman, the public-key cryptosystems in common use today. We categorize the known techniques by the structure of the information that is learned by the attacker, and give simplified examples for each technique to illustrate the underlying ideas.

7.1.6 Modular polynomials on Hilbert surfaces

This article, written in 2017 when the first author was in the group has been published in [10].

7.2 The Number Field Sieve – High-Level Results

7.2.1 Comparing the difficulty of factorization and discrete logarithm: a 240-digit experiment

Participants Aurore Guillevic, Pierrick Gaudry, Emmanuel Thomé, Paul Zimmermann.

In [1], we reported on our computational records that were completed at the end of 2019 (integer factorization and discrete logarithms for 240-digit, 795-bit key sizes) and beginning of 2020 (integer factorization for 250-digit, 829-bit key sizes). This work was made possible by a series of improvements in the Number Field Sieve algorithm, and by the flexibility of the Cado-NFS software implementation which enabled us to experiment with a vast variety of parameter selection strategies. Our conclusions are two-fold. First, our computations were much faster than expected. At the 240-digit (795-bit) level, we show that our computation of discrete logarithms took actually 25% less time (measured on identical hardware) than the time that was reported for the computation of discrete logarithms modulo a 232-digit (768-bit) prime. Second, we simultaneously computed two records of the same size, one on integer factoring, and one on discrete logarithms. This double achievement gives a crucial data point regarding how to compare these problems, which are of utmost importance for public-key cryptography. We show that contrary to the common belief that discrete logarithms are very considerably harder to compute than integer factoring for similar key sizes, the difference is only a factor of roughly 3 for 795-bit key sizes, which is much less than previously thought. This paper was published in the proceedings of the conference Crypto 2020.

We also wrote a non-technical article in French, which aims at dissemination towards a more general public [25].

7.2.2 Asymptotic complexities of discrete logarithm algorithms in pairing-relevant finite fields

Participants Gabrielle De Micheli, Pierrick Gaudry, Cécile Pierrot.

In [2], we study the discrete logarithm problem at the boundary case between small and medium characteristic finite fields, which is precisely the area where finite fields used in pairing-based cryptosystems live. In order to evaluate the security of pairing-based protocols, we thoroughly analyze the complexity of all the algorithms that coexist at this boundary case. We adapt the Function Field Sieve to the particular case where the extension degree is composite, and show how to lower the complexity by working in a shifted function field. All this study finally allows us to give precise values for the characteristic asymptotically achieving the highest security level for pairings. Surprisingly enough, there exist special characteristics that are as secure as general ones. This paper was published in the proceedings of the conference Crypto 2020.

7.2.3 Refined Analysis of the Asymptotic Complexity of the Number Field Sieve

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

In [23], 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 [23], 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.

7.3 The Number Field Sieve – Implementation Results

7.3.1 New Discrete Logarithm Computation for the Medium Prime Case Using the Function Field Sieve

Participants Emmanuel Thomé.

In [11], we study how the Function Field Sieve algorithm can extend to the medium prime range, and provide concrete experimental results for a kilobit finite field of 22-bit characteristic. The linear algebra step was manageable in this example thanks to the CARAMBA expertise. We also show that the linear algebra step can be expected to dominate in two chosen examples of slightly larger characteristic. This article was published in 2020 in the journal Advances in Mathematics of Communications.

7.3.2 Parallel Structured Gaussian Elimination for the Number Field Sieve

Participants Paul Zimmermann.

Together with Charles Bouillaguet (now Sorbonne University, Paris, France), we completely redesigned the structured Gaussian elimination step of Cado-NFS (called `merge`). The new algorithm is fully parallel, and scales quite well. It was used for the new 240- and 250-digit record factorizations and discrete logarithm computations [1]. The article describing the new parallel algorithm was finally accepted for publication in 2020, and will appear in *Mathematical Cryptology* [4].

7.4 Symmetric Cryptology

7.4.1 Cryptanalysis Results on Spook: Bringing Full-round Shadow-512 to the Light

Participants Paul Huynh, Virginie Lallemand.

Together with Patrick Derbez[5], María Naya-Plasencia, Léo Perrin and André Schrottenloher[6] we found a series of structural properties on Spook, one of the second round candidates of the NIST Lightweight Cryptography Standardization process. In [3], we managed to extend these properties and to build practical distinguishers of the full 6-step version of the underlying permutations of Spook, namely Shadow-512 and Shadow-384. We also proposed practical forgeries with 4-step Shadow for the S1P mode of operation in the nonce misuse scenario, which is allowed by the CIML2 security game considered by the authors. Our findings have led the designers of Spook to propose a tweaked version of their candidate in order to improve the security margins. This paper was published in the proceedings of the conference Crypto 2020.

7.4.2 On the Feistel Counterpart of the Boomerang Connectivity Table: Introduction and Analysis of the FBCT

Participants Hamid Boukerrou, Paul Huynh, Virginie Lallemand, Bimal Mandal,
Marine Minier.

The article [5] involved all the team members working in symmetric cryptography. It studied how to adapt the BCT, a recent tool introduced to better estimate the strength of so-called boomerang

[5] Univ Rennes, CNRS, IRISA, France

[6] All three are in Inria, Paris, France.

distinguishers, to the case of Feistel constructions. We investigated the properties of the newly introduced table (that we call the FBCT) and showed that its coefficients are related to the second order derivative of the function at play. We compared the properties of the BCT and of the FBCT, and concluded with an extension to more rounds and with an application of the results. This article was published in Transactions on Symmetric Cryptology.

7.4.3 Analysis of Boolean Functions in a Restricted (Biased) Domain

Participants Bimal Mandal.

This work [9] with Subhamoy Maitra and Dibyendu Roy[7] and Thor Martinsen and Pantelimon Stanica[8] is a substantially revised and extended version of the paper "Tools in analyzing linear approximation for Boolean functions related to FLIP" that appeared in the proceedings of Indocrypt 2018 [33]. We proposed a technique to study the cryptographic properties of Boolean functions, whose inputs do not follow uniform distribution, and obtain a lower bound for the bias of the nonlinear filter function of FLIP by using a biased Walsh–Hadamard transform. Our results provided more accurate calculation of the biases of Boolean function over restricted domain, which help to determine the security parameter of FLIP type ciphers.

7.4.4 Computing AES Related-Key Differential Characteristics With Constraint Programming

Participants Marine Minier.

In [6], with David Gérault[9], Pascal Lafourcade[10], and Christine Solnon[11], we improve existing Constraint Programming (CP) approaches for computing optimal related-key differential characteristics: we add new constraints that detect inconsistencies sooner, and we introduce a new decomposition of the problem in two steps. These improvements allow us to compute all optimal related-key differential characteristics for AES-128, AES-192 and AES-256 in a few hours. This article was published in 2020 in the journal Artificial Intelligence.

7.4.5 Participation in the NIST Lightweight Cryptography Standardization Process

Participants Marine Minier, Paul Huynh, Virginie Lallemand.

The team is actively taking part in the lightweight cryptography standardization process of the NIST. The two major actions that have been taken are the following:

- Proposition of two candidates, namely Lilliput-AE (Alexandre Adomnicai, Thierry P. Berger, Christophe Clavier, Julien Francq, Paul Huynh, Virginie Lallemand, Kévin Le Gouguec, Marine Minier, Léo Reynaud and Gaël Thomas) and ForkAE (Elena Andreeva, Virginie Lallemand, Antoon Purnal, Reza Reyhanitabar, Arnab Roy and Damian Vizár). ForkAE made it to the second round, but unfortunately a weak point has been detected in the design of Lilliput-AE.
- Organization of two cryptanalysis meetings with other French cryptographers at the beginning of the year, continuing a series started in May 2019. Unfortunately, we had to stop short in March because of the pandemic. The last editions resulted in interesting observations on two candidates, namely Tiny Jambu and Spook.

[7] Indian Statistical Institute, Kolkata, West Bengal, India
[8] Naval Postgraduate School, Monterey, CA, USA
[9] University of Surrey, UK.
[10] University Clermont Auvergne, France
[11] INSA de Lyon, France

7.4.6 A White-Box Encryption Scheme using Physically Unclonable Functions

Participants Marine Minier, Sandra Rasoamiaramanana.

When a cryptographic algorithm is executed in a potentially hostile environment, techniques of white-box cryptography are used to protect a secret key from a fully-privileged adversary. However, even if the adversary is not able to extract the secret key from the implementation, they might lift the entire white-box code and execute it (this is called a code lifting attack). In [17], we introduce an encryption scheme that can be implemented on an untrusted environment and is still secure even if the white-box code has been lifted. We base our proposal on a Physically Unclonable Function (PUF) to ensure the execution context of our so-called PUF-based encryption scheme. This way, the encryption is "locked" by a particular device. This article was published in the proceedings of the 17th International Conference on Security and Cryptography.

7.5 E-voting

7.5.1 How to fake zero-knowledge proofs, again

Participants Véronique Cortier, Pierrick Gaudry, Quentin Yang.

In a short paper [12], contributed to the E-Vote-Id 2020 conference, we explain how, in the Belenios voting system, while not using the weak version of Fiat-Shamir, there is still a gap that allows to fake a zero-knowledge proof in certain circumstances. Therefore an attacker who corrupts the voting server and the decryption trustees could break verifiability.

7.5.2 Breaking the Encryption Scheme of the Moscow Internet Voting System

Participants Pierrick Gaudry.

The article [15] has been published in the proceedings of the Financial Crypto conference. It was also presented as invited contribution at Real World Crypto 2020 and the Workshop on Attacks in Crypto (Satellite of the Crypto 2020 conference).

7.6 Other

7.6.1 Three Cousins of Recamán's Sequence

Participants Paul Zimmermann.

Following a question of Neil Sloane, the author of the *Online Encyclopedia of Integer Sequences* (OEIS), Paul Zimmermann designed an efficient algorithm to compute the sequence $C(n)$ defined in `http://oeis.org/A332580`: $C(n)$ is the minimal positive k such that the concatenation of the decimal digits of $n, n+1, \ldots, n+k$ is divisible by $n+k+1$, or -1 if no such k exists. The new algorithm enabled to find the (previously unknown) values $C(44) = 2783191412912$ and $C(98) = 218128159460$ and other values for $n \leq 1000$. The corresponding article is submitted for publication in the *Fibonacci Quarterly* [24].

7.6.2 Le traçage anonyme, dangereux oxymore: Analyse de risques à destination des non-spécialistes

Participants Pierrick Gaudry, Emmanuel Thomé.

The article [21], in French, examined the potential privacy implications of Covid-19 contact tracing systems that were to be deployed in various countries. We show that despite claims of "privacy by design", privacy concerns do exist and cannot be dismissed light-heartedly.

8 Bilateral contracts and grants with industry

8.1 Bilateral contracts with industry

- Together with the PESTO team, we have a contract with the Idemia company about e-voting.
- With the Nomadic Labs company, we have a contract to propose technical solutions to introduce vote secrecy in the e-voting system that is part of the Tezos cryptocurrency protocol and is used to validate the amendments to the protocol itself.

8.2 Bilateral grants with industry

- A contract with Thales (Thales Communication & Security, Gennevilliers, subsidiary of Thales Group) is dedicated to the supervision of Simon Masson's PhD thesis about elliptic curves for bilinear and post-quantum cryptography. The co-supervisor for Thales is Olivier Bernard. Simon Masson defended his PhD on December 4th, 2020 [19].

9 Partnerships and cooperations

9.1 International initiatives

Informal international partners 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 of international scientists

Santanu Sarkar from Indian Institute of Technology Bombay, visited our team until Feb 2020. His three-months stay was the opportunity to work with him on secret key cryptography.

9.3 National initiatives

9.3.1 FUI Industrial Partnership on Lightweight Cryptography

We have a contract with several partners dedicated to the definition of new lightweight cryptographic primitives for the IoT. Here is the main information about this partnership. See the web site for a full presentation.

- Program: FUI (Fonds Unique Interministériel)
- Project acronym: PACLIDO
- Project title: Protocoles et Algorithmes Cryptographiques Légers pour l'Internet Des Objets
- Duration: 12/2017 - 12/2020

- Coordinator: Airbus Cybersecurity
- Other partners: Airbus Cybersecurity, LORIA-CNRS, Rtone, Trusted Objects, CEA, Sophia Engineering, Université de Limoges, Saint-Quentin-en-Yvelines.

9.3.2 ANR Decrypt

- 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: selection

Member of the conference program committees

- Aurore Guillevic was a member of the Program Committee of WAIFI 2020.
- Virginie Lallemand was a member of the Program Committee of CFAIL 2020 and of the SILC workshop.
- Marine Minier was a member of the Program Committee of LATINCRYPT 2020.
- Cécile Pierrot was a member of the Program Committees of EUROCRYPT 2020 and of Journées Codage et Cryptography 2020.
- Emmanuel Thomé was a member of the Program Committees of EUROCRYPT 2021 and ANTS XIV, as well as a member of the scientific directorate of the Dagstuhl computer science seminar series.

Member of the Conference Steering Committees

- Emmanuel Thomé was a member of the steering committee of the Algorithmic Number Theory Symposium (ANTS), until August 2020.

Reviewer 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.

10.1.2 Journal

Member of the editorial boards

- Virginie Lallemand is a member of the editorial board of the IACR Transactions on Symmetric Cryptology (ToSC) Journal for 2020 and 2021. This journal is the open-access journal associated to the International Conference on Fast Software Encryption (FSE).

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

- Virginie Lallemand was invited to give a talk during the Dagstuhl Seminar 20041 on Symmetric Cryptography in January 2020.
- Gabrielle De Micheli was invited to give a talk at the Security Seminar at Boston University, USA and at the Theory Seminar at Northeastern University, Boston, USA, in February 2020.
- Pierrick Gaudry was invited to give a talk at Real World Crypto 2020 in New York in January 2020, and at the (online) Workshop on Attacks in Crypto 2020 in August 2020.
- Aurore Guillevic was invited to give a talk at the Diamant Symposium in Utrecht, Netherlands in November 2020 (online event).

10.1.4 Scientific expertise

- Pierrick Gaudry was member of a jury for the Innoviris LAUNCH program, whose goal is to fund start-ups created on the basis of academic work.
- Emmanuel Thomé
  - was a member of the scientific directorate of the Dagstuhl computer science seminar series.
  - was a member of the Inria competitive selection process for *directeur de recherche* (DR2) positions in 2020.
  - was a member of the Inria competitive selection process for *chargés de recherche* (CR) positions in 2020 (nationwide selection).
  - was a member of the Inria competitive selection process for *chargés de recherche* (CR) positions in Grenoble 2020 (specific local selection).

10.1.5 Research administration

- Pierre-Jean Spaenlehauer is a member of the *Commission des Développements Technologiques* of the Inria Nancy – Grand Est research center.
- Marine Minier
  - is the scientific leader of the LUE impact project Digitrust;
  - is an elected member of the Collégium “sciences et techniques” from University of Lorraine.
  - is a member of the steering committee of the *LHS – Laboratoire Haute Sécurité* of LORIA.
- Emmanuel Thomé
  - is a member of the *Comipers* of the Inria Nancy – Grand Est research center, in charge of deciding the attribution of Inria PhD and post-doc grants.

  - is an elected member of the Inria evaluation committee (CE), and a member of the committee “bureau”.
  - is a member of the management committee for the research project “CPER Cyberentreprises” (co-chair).
  - is an elected member of the Inria technical committee (CTI).

- Pierrick Gaudry
  - is vice-head of the *Commission de mention Informatique* of the *École doctorale IAEM* of the University of Lorraine.
  - is a member of the *Conseil Scientifique du GdR IM*.
  - is a member of the steering committee of the *LHS – Laboratoire Haute Sécurité* of LORIA.

10.2 Teaching - Supervision - Juries

10.2.1 Teaching

- Licence
  - Pierrick Gaudry, *Intégration Web*, 48h eq. TD, IUT 1A, Université de Lorraine, IUT Charlemagne, Nancy, France.
  - Aurore Guillevic, *Introduction to algorithms* (CSE103), 32h eq. TD, L1, École Polytechnique, Palaiseau, 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
  - Aurore Guillevic, *Introduction à la cryptographie asymétrique : RSA, Diffie-Hellman, factorisation d'entiers, logarithme discret*, 4.5h eq. TD, Master Cybersécurité des systèmes embarqués, Université de Bretagne Sud, Lorient, 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.
- Engineering school
  - Paul Huynh, *Sensibilisation et initiation à la cyber-sécurité*, 7h eq. TD, 1A, Télécom, Nancy, France.
  - Gabrielle De Micheli, *Introduction à la cryptographie*, 16h eq. TD, 2A, Télécom, Nancy, France.
  - Gabrielle De Micheli, *Cryptographie et authentification*, 30h eq. TD, 2A, Télécom, Nancy, France.
  - Emmanuel Thomé, *Protocoles de sécurité et Vérification* (sub-part dedicated to cryptographic primitives), 18h eq. TD, 3A, Télécom, Nancy, France.
  - Pierrick Gaudry, *Protocoles de sécurité et Vérification* (sub-part dedicated to verification) 8h eq. TD, 3A, Télécom, Nancy, France.
  - Gabrielle De Micheli, *Introduction à la programmation* (TCSS5AC Info 1), 20h eq. TD, 1A, École des Mines, Nancy, France.
  - Cécile Pierrot, *Introduction à LaTeX*, 4.5h eq. TD, 2A, École des Mines, Nancy, France.

  - Gabrielle De Micheli, *Introduction à l'apprentissage automatique*, 8h eq. TD, 2A, École des Mines, Nancy, France.
  - Cécile Pierrot, *Cryptographie et cryptanalyse*, 91h eq. TD, Mastère spécialisé en sécurité, École des Mines, Nancy, France.
  - Aurore Guillevic, *Introduction à l'informatique* (INF361), 40 eq. TD, 1A, École Polytechnique, Palaiseau, France.

- Head of the curriculum for Master 2 SIRAV *Sécurité Informatique, Réseaux et Architectures Virtuelles*, 30 students: Marine Minier. Université de Lorraine, Faculté des sciences et technologies, Vandœuvre-lès-Nancy, France.

10.2.2 Supervision

- Ph.D.: Sandra Rasoamiaramanana, *Design of white-box encryption schemes for mobile applications security* [20], Université de Lorraine, defended June 12, 2020, Marine Minier. CIFRE Orange Gardens.

- Ph.D.: Paul Huynh, *Analyse et conception de chiffrements authentifiés à bas coût* [18], Université de Lorraine, defended November 26, 2020, Marine Minier.

- Ph.D.: Simon Masson, *Algorithmique des courbes destinées aux contextes de la cryptographie bilinéaire et post-quantique* [19], Université de Lorraine, defended December 4, 2020, Emmanuel Thomé and Aurore Guillevic. CIFRE Thales Communication & Security.

- PhD in progress: Aude Le Gluher, *Analyse algorithmique fine et simulation du crible algébrique*, since Sep. 2018, Pierre-Jean Spaenlehauer and Emmanuel Thomé.

- PhD in progress: Gabrielle De Micheli, *Le logarithme discret dans les corps finis*, since Oct. 2018, Cécile Pierrot and Pierrick Gaudry.

- PhD in progress: Hamid Boukerrou, *Design of New Finite State Dynamical Systems Admitting a Matrix Representation: Application to Cryptography*, since Oct. 2019, Marine Minier and Gilles Millerioux.

- PhD in progress: Quentin Yang, *Conception et analyse d'un système de vote électronique satisfaisant aux exigences de sécurité modernes*, since Oct. 2020, Véronique Cortier and Pierrick Gaudry.

- M2 internship: Ambroise Baudot *Rijndael with Constraint Programming*, 6 months from March 2020, Marine Minier.

- M2 internship: Benoît Chauvière *Estimating the energy consumption of the NIST ligthweight finalists on the RIoT OS*, 6 months from April 2020, Marine Minier.

- M2 internship: Quentin Yang *Comparaison des méthodes de mixnets et de chiffrement homomorphe pour des scrutins électroniques complexes*, 6 months from March 2020, Véronique Cortier and Pierrick Gaudry.

10.2.3 Juries

- Pierrick Gaudry was reviewer of the PhD thesis *Combinatorics in Algebraic and Logical Cryptanalysis* defended by Monika Trimoska, January 2021, l'Université de Picardie Jules Verne.

- Marine Minier was:

  - President of the PhD thesis jury: Analyse de trafic https pour la supervision d'utilisateurs defended by Pierre-Olivier Brissaud, December 2020, Université de Lorraine, Nancy.
  - President of the PhD thesis jury: Experimental Methods for the Evaluation of Big Data Systems defended by Abdulqawi Saif, January 2020, Université de Lorraine, Nancy.

  - Member of the PhD thesis jury: Évaluation de la fiabilité des systèmes modélisés par arbres de défaillances grâce aux techniques de satisfabilité defended by Margaux Duroeulx, March 2020, Université de Lorraine, Nancy.

- Pierre-Jean Spaenlehauer was member of the PhD thesis jury: *Homotopy algorithms for solving structured determinantal systems* defended by Thi Xuan Vu, December 2020, Sorbonne Université and the University of Waterloo (Canada).

10.3 Popularization

10.3.1 Articles and contents

In connection with our recent factoring and discrete logarithm record computations, we wrote a non-technical article in French, which aims at dissemination towards a more general public [25].

10.3.2 Education

- Aurore Guillevic gave a talk at the *Journée des métiers des maths* AMIES at IECL on March 4, organized for high school teachers of science in Meurthe et Moselle, to help their students know more about scientific careers.

- Cécile Pierrot was invited to:

  - present research and computer science in December 2020 to Table ronde "Osez les Sciences !" a meeting for high school students in Reims initiated by Accustica an association that promotes science to young people.
  - collaborate with scientific facilitators at La Cité des Sciences, Paris, about short workshops for students dealing with cryptography.

10.3.3 Interventions

Cécile Pierrot gave a wide audience talk about cryptography at La Cité des Sciences, Paris, for the the exhibition "Espions" - October 2019 to June 2021.

11 Scientific production

11.1 Major publications

[1] 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: *Advances in Cryptology – CRYPTO 2020*. Ed. by D. Micciancio and T. Ristenpart. Vol. 12171. Lecture Notes in Computer Science. Santa Barbara CA, United States: Springer, Aug. 2020, pp. 62–91. DOI: 10.1007/978-3-030-56880-1_3. URL: https://hal.inria.fr/hal-02863525.

[2] G. De Micheli, P. Gaudry and C. Pierrot. 'Asymptotic complexities of discrete logarithm algorithms in pairing-relevant finite fields'. In: *CRYPTO 2020 - 40th Annual International Cryptology Conference*. Ed. by D. Micciancio and T. Ristenpart. Vol. 12171. Lecture Notes in Computer Science. Santa Barbara / Virtual, United States: Springer, Aug. 2020, pp. 32–61. URL: https://hal.archives-ouvertes.fr/hal-02871839.

[3] 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 - Annual International Cryptology Conference*. Ed. by D. Micciancio and T. Ristenpart. Santa Barbara / Virtual, United States, Aug. 2020. DOI: 10.1007/978-3-030-56877-1_13. URL: https://hal.inria.fr/hal-02944908.

11.2 Publications of the year

International journals

[4] C. Bouillaguet and P. Zimmermann. 'Parallel Structured Gaussian Elimination for the Number Field Sieve'. In: *Mathematical Cryptology* (2021). URL: https://hal.inria.fr/hal-02098114.

[5] H. Boukerrou, P. Huynh, V. Lallemand, B. Mandal and M. Minier. 'On the Feistel Counterpart of the Boomerang Connectivity Table: Introduction and Analysis of the FBCT'. In: *IACR Transactions on Symmetric Cryptology* 2020.1 (7th May 2020), pp. 331–362. DOI: 10.13154/tosc.v2020.i1.331-362. URL: https://hal.inria.fr/hal-02945065.

[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.

[7] A. Guillevic, S. Masson and E. Thomé. 'Cocks-Pinch curves of embedding degrees five to eight and optimal ate pairing computation'. In: *Designs, Codes and Cryptography* (8th Mar. 2020). DOI: 10.1007/s10623-020-00727-w. URL: https://hal.inria.fr/hal-02305051.

[8] A. Guillevic and S. Singh. 'On the Alpha Value of Polynomials in the Tower Number Field Sieve Algorithm'. In: *Mathematical Cryptology* 1.1 (20th Feb. 2021), p. 39. URL: https://hal.inria.fr/hal-02263098.

[9] S. Maitra, B. Mandal, T. Martinsen, D. Roy and P. Stanica. 'Analysis on Boolean function in a restricted (biased) domain'. In: *IEEE Transactions on Information Theory* 66.2 (2020), pp. 1219–1231. DOI: 10.1109/TIT.2019.2932739. URL: https://hal.inria.fr/hal-02374194.

[10] E. Milio and D. Robert. 'Modular polynomials on Hilbert surfaces'. In: *Journal of Number Theory* (May 2020). DOI: 10.1016/j.jnt.2020.04.014. URL: https://hal.archives-ouvertes.fr/hal-01520262.

[11] M. Mukhopadhyay, P. Sarkar, S. Singh and E. Thomé. 'New Discrete Logarithm Computation for the Medium Prime Case Using the Function Field Sieve'. In: *Advances in Mathematics of Communications* (2020). DOI: 10.3934/amc.2020119. URL: https://hal.inria.fr/hal-02964002.

International peer-reviewed conferences

[12] V. Cortier, P. Gaudry and Q. Yang. 'How to fake zero-knowledge proofs, again'. In: E-Vote-Id 2020 - The International Conference for Electronic Voting. Bregenz / virtual, Austria, 2020. URL: https://hal.inria.fr/hal-02928953.

[13] G. De Micheli, R. E. Piau and C. Pierrot. 'A Tale of Three Signatures: practical attack of ECDSA with wNAF'. In: *Progress in Cryptology - AFRICACRYPT 2020.* AFRICACRYPT 2020. Vol. 12174. Lecture Notes in Computer Science. Cairo, Egypt, 5th July 2020, pp. 361–381. DOI: 10.1007/978-3-030-51938-4_18. URL: https://hal.archives-ouvertes.fr/hal-02393302.

[14] 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.

[15] P. Gaudry and A. Golovnev. 'Breaking the encryption scheme of the Moscow Internet voting system'. In: Financial Cryptography and Data Security. Kota Kinabalu, Malaysia, 2020, pp. 32–49. DOI: 10.1007/978-3-030-51280-4_3. URL: https://hal.inria.fr/hal-02266264.

[16] 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.

[17] S. Rasoamiaramanana, M. Minier and G. Macario-Rat. 'A White-Box Encryption Scheme using Physically Unclonable Functions'. In: 17th International Conference on Security and Cryptography. Lieusaint - Paris, France, 8th July 2020, pp. 279–286. DOI: 10.5220/0009781002790286. URL: https://hal.inria.fr/hal-02944654.

Doctoral dissertations and habilitation theses

[18] P. Huynh. 'Design and Analysis of Lightweight Encryption Schemes'. Université de Lorraine, Nancy, France, 26th Nov. 2020. URL: https://hal.archives-ouvertes.fr/tel-03086269.

[19] S. Masson. 'Algorithmic of curves in the context of bilinear and post-quantum cryptography'. Université de Lorraine, 4th Dec. 2020. URL: https://tel.archives-ouvertes.fr/tel-03052499.

[20] S. Rasoamiaramanana. 'Design of white-box encryption schemes for mobile applications security'. Université de Lorraine, 12th June 2020. URL: https://hal.univ-lorraine.fr/tel-02949394.

Reports & preprints

[21] X. Bonnetain, A. Canteaut, V. Cortier, P. Gaudry, L. Hirschi, S. Kremer, S. Lacour, M. Lequesne, G. Leurent, L. Perrin, A. Schrottenloher, E. Thomé, S. Vaudenay and C. Vuillot. *Le traçage anonyme, dangereux oxymore: Analyse de risques à destination des non-spécialistes*. 21st Apr. 2020. URL: https://hal.inria.fr/hal-02997228.

[22] G. De Micheli and N. Heninger. *Recovering cryptographic keys from partial information, by example*. 8th Dec. 2020. URL: https://hal.archives-ouvertes.fr/hal-03045663.

[23] A. Le Gluher, P.-J. Spaenlehauer and E. Thomé. *Refined Analysis of the Asymptotic Complexity of the Number Field Sieve*. 9th Sept. 2020. URL: https://hal.inria.fr/hal-02934273.

[24] J. S. Myers, R. Schroeppel, S. R. Shannon, N. J. A. Sloane and P. Zimmermann. *Three Cousins of Recamán's Sequence*. 28th Sept. 2020. URL: https://hal.inria.fr/hal-02951011.

Other scientific publications

[25] F. Boudot, P. Gaudry, A. Guillevic, N. Heninger, E. Thomé and P. Zimmermann. 'New factorization and discrete logarithm record computations'. In: *Techniques de l'Ingenieur* (8th Dec. 2020), p. 17. URL: https://hal.inria.fr/hal-03045666.

11.3 Cited publications

[26] 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*. ACM, 2015, pp. 5–17. URL: http://dl.acm.org/citation.cfm?doid=2810103.2813707.

[27] 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.

[28] S. Bowe, A. Chiesa, M. Green, I. Miers, P. Mishra and H. Wu. 'ZEXE: Enabling Decentralized Private Computation'. In: *2020 IEEE Symposium on Security and Privacy (SP)*. Los Alamitos, CA, USA: IEEE Computer Society, May 2020, pp. 1059–1076. eprint: https://eprint.iacr.org/2018/962. URL: https://www.computer.org/csdl/proceedings-article/sp/2020/349700b059/1i0rIqoBYD6.

[29] J.-C. Faugère, M. Safey El Din and P.-J. Spaenlehauer. 'Gröbner Bases of Bihomogeneous Ideals generated by Polynomials of Bidegree $(1,1)$: Algorithms and Complexity'. In: *J. Symbolic Comput.* 46.4 (2011), pp. 406–437.

[30] J.-C. Faugère, P.-J. Spaenlehauer and J. Svartz. 'Sparse Gröbner bases: the unmixed case'. In: *ISSAC 2014*. Ed. by K. Nabeshima. Proceedings. ACM, 2014, pp. 178–185.

[31] J. Groth. 'On the Size of Pairing-Based Non-interactive Arguments'. In: *Advances in Cryptology - EUROCRYPT 2016 - 35th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Vienna, Austria, May 8-12, 2016, Proceedings, Part II*. Ed. by M. Fischlin and J.-S. Coron. Vol. 9666. Lecture Notes in Computer Science. Springer, 2016, pp. 305–326. DOI: 10.1007/978-3-662-49896-5_11. URL: http://eprint.iacr.org/2016/260.

[32] 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.

[33] S. Maitra, B. Mandal, T. Martinsen, D. Roy and P. Stanica. 'Tools in Analyzing Linear Approximation for Boolean Functions Related to FLIP'. In: *Progress in Cryptology - INDOCRYPT 2018 - 19th International Conference on Cryptology in India, New Delhi, India, December 9-12, 2018, Proceedings*. Ed. by D. Chakraborty and T. Iwata. Vol. 11356. Lecture Notes in Computer Science. Springer, 2018, pp. 282–303. DOI: 10.1007/978-3-030-05378-9_16. URL: https://doi.org/10.1007/978-3-030-05378-9%5C_16.

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

[35] E. Rescorla. *The Transport Layer Security (TLS) Protocol Version 1.3*. RFC 8446. 2018. URL: https://tools.ietf.org/html/rfc8446.

[36] 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.