IN PARTNERSHIP WITH:
CNRS

Université de Lorraine

Activity Report 2019

Project-Team CARAMBA

Cryptology, arithmetic : algebraic methods for better algorithms

RESEARCH CENTER
Nancy - Grand Est

THEME
Algorithmics, Computer Algebra and Cryptology

Table of contents

Project-Team CARAMBA

Creation of the Team: 2016 January 01, updated into Project-Team: 2016 September 01

Keywords:

Computer Science and Digital Science:

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, Visitors, External Collaborators

Research Scientists

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

Faculty Members

Marine Minier [Univ de Lorraine, Professor, HDR]
Marion Videau [Univ de Lorraine, Associate Professor, until Apr 2019, on leave with Quarkslab since Jan 2015]

Post-Doctoral Fellow

Bimal Mandal [Inria]

PhD Students

Hamid Boukerrou [Univ de Lorraine, from Oct 2019]
Gabrielle de Micheli [Inria]
Paul Huynh [CNRS]
Aude Le Gluher [Univ de Lorraine]
Simon Masson [Thales]
Andrianina Sandra Rasoamiaramanana [Orange]

Interns and Apprentices

Hamid Boukerrou [Univ de Lorraine, from Mar 2019 until Sep 2019]
Félix Breton [ÉNS Paris, from Jun 2019 until Jul 2019]
Émilien Failly [CPP Nancy, from Apr 2019 until Jun 2019]
Liwei Liu [Peking University, China, from Jun 2019 until Sep 2019]
Rémi Piau [Inria, from May 2019 until Jul 2019]

Administrative Assistants
Emmanuelle Deschamps [Inria]
Virginie Priester [CNRS]

Visiting Scientist
Santanu Sarkar [IIT Madras, India, Associate Professor, from Dec 2019]

External Collaborator
Luc Sanselme [Ministère de l'Éducation Nationale]

2. Overall Objectives

2.1. 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 CP, SAT or MILP. We plan to pay special attention to the recent advances in cryptanalysis and to study recently proposed lightweight ciphers.

  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.

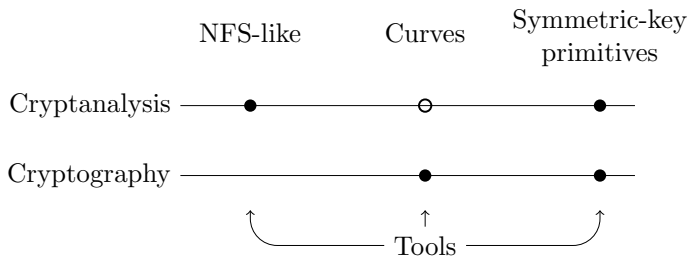

Figure 1. Visual representation of the thematic organization of CARAMBA. Solid dots: major interaction; clear dots: minor interaction.

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 [34], the curves x25519 and x448 have entered the base specification of 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 $\mathrm{GF}(2)$) 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.

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], [28].

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.

[1] National Institute of Standard and Technology.

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.
- The hiring of Marine Minier is likely to lead the team to study particular polynomial systems in contexts related to symmetric key cryptography.
- 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], [28]. 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 fast arithmetic contributions, 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.

[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 [31] is one of only two academic works cited by NIST in the initial version (2011) of the report [33].

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 [15], 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. Highlights of the Year

- On December 2nd, 2019, the factorization of RSA-240 and the computation of a 240-digit discrete logarithm were announced.
- In August 2019, Pierrick Gaudry found a vulnerability in the encryption scheme of the Internet voting system of Moscow.
- Pierrick Gaudry and Cécile Pierrot were invited speakers at the ECC 2019 conference (Bochum, Germany).

5.1.1. Awards

- Simon Abelard received the PhD prize of Université de Lorraine from the doctoral school IAEM (computer science, automatic) [25].

6. New Software and Platforms

6.1. Belenios

Belenios - Verifiable online voting system

KEYWORD: E-voting

FUNCTIONAL DESCRIPTION: Belenios is an open-source online voting system that provides 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). Confidentiality relies on the encryption of the votes and the distribution of the decryption key.

Belenios builds upon Helios, a voting protocol used in several elections. The main design enhancement of Belenios vs. Helios is that the ballot box can no longer add (fake) ballots, due to the use of credentials. Moreover, Belenios includes a practical threshold decryption system that allows splitting the decryption key among several authorities.

NEWS OF THE YEAR: Since 2015, it has been used by CNRS for remote election among its councils (more than 30 elections every year) and since 2016, it has been used by Inria to elect representatives in the “comités de centre” of each Inria center. In 2018, it has been used to organize about 250 elections (not counting test elections). Belenios is typically used for elections in universities as well as in associations. This goes from laboratory councils (e.g. Irisa, Cran), scientific societies (e.g. SMAI) to various associations (e.g. FFBS - Fédération Française de Baseball et Softball, or SRFA - Société du Rat Francophone et de ses Amateurs).

In 2019, a threshold encryption mode has been added that makes the system more robust to the case where (say) one trustee among three loses her part of the decryption key.

- Participants: Pierrick Gaudry, Stéphane Glondu and Véronique Cortier
- Partners: CNRS - Inria
- Contact: Stéphane Glondu
- URL: http://www.belenios.org/

6.2. CADO-NFS

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: The main program for relation collection now supports composite "special-q". The memory footprint of the central step of linear algebra was reduced. Parallelism of many of the Cado-NFS programs was improved considerably (sieving, relation filtering, as well as the central step of linear algebra).

- Participants: Pierrick Gaudry, Emmanuel Thomé and Paul Zimmermann
- Contact: Emmanuel Thomé
- URL: http://cado-nfs.gforge.inria.fr/

6.3. Platforms

6.3.1. Platform: computational resources

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 as well as the computation of discrete logarithms modulo a 240-digit prime, completed in 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.

In [21] 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

Participant: Aurore Guillevic.

The preprint [20] applies the refinements of the paper [22] 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 [21]. We list nine interesting pairing-friendly curves of embedding degrees between 10 and 16 at the 128-bit security level.

7.1.3. A Practical Attack on ECDSA Implementations Using wNAF Representation

Participants: Gabrielle de Micheli, Cécile Pierrot, Rémi Piau.

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 [18], 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.

7.1.4. Algorithmic Aspects of Elliptic Bases in Finite Field Discrete Logarithm Algorithms

Participant: Cécile Pierrot.

Elliptic bases give an elegant way of representing finite field extensions and were used as a starting point for small characteristic finite field discrete logarithm algorithms. This idea has been proposed by two groups, in order to achieve provable quasi-polynomial time algorithms for computing discrete logarithms in small characteristic finite fields. In [23], together with Antoine Joux, we do not try to achieve a provable algorithm, but instead we investigate the practicality of heuristic algorithms based on elliptic bases.

7.1.5. A Fast Randomized Geometric Algorithm for Computing Riemann-Roch Spaces

Participants: Aude Le Gluher, Pierre-Jean Spaenlehauer [contact].

In [7], we proposed a probabilistic variant of Brill-Noether's algorithm for computing a basis of the Riemann-Roch space $L(D)$ associated to a divisor D on a projective plane curve $\mathcal{C}$ over a sufficiently large perfect field k. Most of the results of this work have been obtained in 2018. In 2019, we have strengthened these results and revised the associated paper. This new version of the paper has been accepted for publication in the journal Mathematics of Computation.

7.1.6. Counting Points on Hyperelliptic Curves

Participants: Pierrick Gaudry, Pierre-Jean Spaenlehauer.

Two works with Simon Abelard [1], [2] following his PhD thesis about improved complexities for counting point algorithms of hyperelliptic curves with or without real multiplication are now formally published as journal articles.

7.1.7. Verifiable Delay Functions from Supersingular Isogenies and Pairings

Participant: Simon Masson.

Together with Luca De Feo, Christophe Petit and Antonio Sanso, we introduce in [11] two verifiable delay functions based on isogenies of supersingular elliptic curves and pairing. We discuss both the advantages and drawbacks of our constructions, we study their security and we demonstrate their practicality with a proof-of-concept implementation. This work appears in the proceedings of ASIACRYPT'2019.

7.1.8. Isogeny Graphs With Maximal Real Multiplication

Participant: Emmanuel Thomé.

Emmanuel Thomé and Sorina Ionica (post-doctoral fellow in the former CARAMEL team in 2012) worked on a new algorithm for computing isogeny graphs for Jacobians of curves having the special property that the intersection of their endomorphism ring with its real subfield is maximal. The resulting algorithm is the first depth-first algorithm for this task. The work [6] was finally published.

7.2. The Number Field Sieve – High-Level Results

7.2.1. A New Ranking Function for Polynomial Selection in the Number Field Sieve

Participant: Paul Zimmermann.

With Nicolas David (ÉNS Paris-Saclay, France), we designed a new ranking function for polynomial selection in the Number Field Sieve. The previous ranking function was only considering the *mean* of the so-called α-value, which measures how small primes divide the norm of the polynomial. The new function also takes into account the *variance* of the corresponding distribution. This partially explains why the previous function did sometimes fail to correctly identify the best polynomials. The new ranking function is implemented in Cado-NFS (branch `dist-alpha`) and is detailed in [3].

7.2.2. On the Alpha Value of Polynomials in the Tower Number Field Sieve Algorithm

Participant: Aurore Guillevic.

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 [22]. 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.

7.2.3. Faster Individual Discrete Logarithms in Finite Fields of Composite Extension Degree

Participant: Aurore Guillevic.

We improved the previous work [30] on speeding-up the first phase of the individual discrete logarithm computation, the initial splitting, a.k.a. the smoothing phase. We extended the algorithm to any non-prime finite field $\mathbb{F}_{p^n}$ where n is composite. We also applied it to the new variant Tower-NFS. The paper was finally published in 2019 [4].

7.3. The Number Field Sieve – Implementation Results

7.3.1. Parallel Structured Gaussian Elimination for the Number Field Sieve

Participant: Paul Zimmermann.

Together with Charles Bouillaguet (University of Lille, France), we completely re-designed the structured Gaussian elimination step of Cado-NFS (called `merge`). The new algorithm is fully parallel, and scales quite well. With 32 cores on modern hardware, the `merge`-step of RSA-512 (factored in 1999) now takes only 20 seconds, and for the hidden SNFS DLP-1024 record (done in 2017) it takes only 140 seconds [16].

7.4. Computer Arithmetic

7.4.1. Breaking Randomized Mixed-Radix Scalar Multiplication Algorithms

Participant: Jérémie Detrey.

Together with Laurent Imbert (LIRMM, France), we designed in [13] an attack against a recently published randomized elliptic-curve scalar multiplication scheme based on covering systems of congruences. We also proposed a more robust algorithm based on a mixed-radix representation of the scalar. However, under strong security hypotheses, this algorithm may still allow a virtual powerful attacker to recover much more information than what was first expected. This led us to the conclusion that randomized algorithms based on the mixed-radix number system should be avoided.

7.5. Symmetric Cryptology

7.5.1. Vectorial Boolean Functions with Very Low Differential-Linear Uniformity Using Maiorana-McFarland Type Construction

Participant: Bimal Mandal.

With Deng Tang and Subhamoy Maitra, we constructed in [14] a new class of balanced vectorial Boolean functions with very low differential-linear uniformity, whose coordinate functions are derived by modifying the Maiorana–McFarland bent functions. Further, we provided a combinatorial count of hardware gates required to implement such circuits.

7.5.2. Analysis of Boolean Functions in a Restricted (Biased) Domain

Participant: Bimal Mandal.

This work with Subhamoy Maitra, Thor Martinsen, Dibyendu Roy 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 [32]. 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 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.

7.5.3. Forkcipher: a New Primitive for Authenticated Encryption of Very Short Messages

Participant: Virginie Lallemand.

Together with Elena Andreeva, Antoon Purnal, Reza Reyhanitabar, Arnab Roy and Damian Vizár, we proposed a candidate to the NIST Lightweight competition that we also published at Asiacrypt 2019 [10]. Our proposal is based on the so-called forkcipher construction that was previously presented and investigated by a subset of the authors and which provides authenticated encryption optimized for short messages. Our NIST candidate is called ForkAE, and as required by NIST it is based on well investigated primitives, out of which the Skinny tweakable cipher. ForkAE is one of the 32 candidates that were selected to continue to Round 2 out of 56 valid submissions.

7.5.4. Computing AES Related-Key Differential Characteristics With Constraint Programming

Participant: Marine Minier.

In [5], with David Gérault, Pascal Lafourcade, and Christine Solnon, 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.

7.5.5. Participation in the NIST Lightweight Cryptography Standardization Process

Participants: Marine Minier [contact], 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 LeGouguec, 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 regular cryptanalysis meetings with other french cryptographers. Since the publication of the 56 proposals, four meetings have been held and some tangible results have already been achieved. As an example, the meeting participants found a practical differential forgery attack against the proposal named *Quartet*. The details have been made public on the NIST mailing list and they made the NIST remove this candidate from consideration.

7.5.6. Cryptanalysis of SKINNY in the Framework of the SKINNY 2018-2019 Cryptanalysis Competition

Participant: Virginie Lallemand.

Together with Patrick Derbez (University of Rennes) and Aleksei Udovenko (University of Luxembourg) we investigated in [12] the security of the SKINNY tweakable block cipher, a lightweight symmetric cipher proposed at Crypto in 2016. Our setting was the one of the SKINNY 2018-2019 Cryptanalysis Competition, that is we looked for attacks that can be run in practical time and that succeed with a data set reduced to the provided set of 2^{20} (plaintext, ciphertext). We solved the challenges (meaning that we experimentally recovered the 128-bit key) for up to 10-round SKINNY-128-128 and 12-round SKINNY-64-128. To this day these are the best results reported in this setting.

7.6. E-voting

7.6.1. Belenios: a Simple Private and Verifiable Electronic Voting System

Participant: Pierrick Gaudry.

In [9], written with Véronique Cortier and Stéphane Glondu, we have summarized the current state of our voting platform Belenios. It was the occasion to put in a single place the description of several sub-parts of the protocol that are otherwise spread in many articles. We also made statistics regarding the use of the platform during the year 2018, and discussed how security features were or were not activated by the users.

7.6.2. A Simple Alternative to Benaloh Challenge for the Cast-as-Intended Property in Helios/Belenios

Participant: Pierrick Gaudry.

In a short note [17] written with Véronique Cortier, Jannik Dreier, and Mathieu Turuani from the PESTO team, we propose a simple technique that can be added to an Helios-like e-voting protocol, so that the voter can check whether their potentially infected computer has not silently changed their vote.

7.6.3. Breaking the Encryption Scheme of the Moscow Internet Voting System

Participant: Pierrick Gaudry.

In [19], written in collaboration with Alexander Golovnev (Harvard), we explain the vulnerabilities we have found in an Internet voting system used for the election for the representatives of the Moscow Duma that took place in September 2019. The weaknesses in the encryption scheme (based on the discrete logarithm problem in finite fields) were found in the source code that was made available in July 2019 as part of a public testing.

8. Bilateral Contracts and Grants with Industry

8.1. Bilateral Contracts with Industry

- Together with the PESTO team, we had a contract with the Docapost company, the purpose of which is to improve their e-voting solution by adding some verifiability properties and switching to elliptic curve cryptography.
- Together with the PESTO team, we have a contract with the Idemia company about e-voting.

8.2. Bilateral Grants with Industry

- A contract with Orange Gardens at Chatillon-Montrouge is dedicated to the supervision of Sandra Rasoamiaramanana's PhD thesis about security in the white box context. The co-supervisor for Orange Gardens is Gilles Macario-rat.
- 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.

9. Partnerships and Cooperations

9.1. Regional Initiatives

9.1.1. CPER CyberEntreprises

Program: CPER (Contrat de Plan État Région)
Project title: Cyber-Entreprises
Duration: 01/07/2015 - 31/12/2020
Coordinator: Emmanuel Thomé and Marc Jungers (CRAN)
Other partners: Inria, LORIA, CRAN, IÉCL, Centrale Supelec, LCFC.
Abstract: cf web site (in French only).

A high-performance computer cluster was funded by the CPER Cyber-entreprises project (Région Grand-Est, French Ministry of Research and Higher Education, Inria, CNRS). This cluster is also mentioned in 6.3.

9.2. National Initiatives

9.2.1. FUI Industrial Partnership on Lightweight Cryptography

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.
This contract is dedicated to the definition of new lightweight cryptographic primitives for the IoT. See web site for a full presentation.

9.2.2. ANR Decrypt

The CARAMBA team coordinates this ANR Project (started in January 2019) with the 5 following partners: LORIA, 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. This 4-year project started in January 2019. See web site for more information.

9.3. International Research Visitors

9.3.1. Visits of International Scientists

- Diego Aranha from Aarhus University visited the team one week in May and presented his work on the Brazilian voting machines at the SSL seminar, and his work on fast pairing implementation at the team's seminar. As a result, some of the new secure pairing-friendly curves of [21], [22] are implemented in the C++ library RELIC [4] (free software).
- Santanu Sarkar from IIT Madras, Chennai, India is visiting the team from December 2019 to the end of February 2020.

9.3.1.1. Internships

- Hamid Boukerrou (Université Paris 8, from March 2019 until September 2019). Subject: cryptanalysis of LBlock.
- Félix Breton (ÉNS Paris, from June 2019 until July 2019). Félix Breton has formally proven in Coq the GNU MPFR subtraction routine in the case where all three operands (the two inputs and the result) have the same precision p, and $1 \leq p < w$, where w is the machine bit-size. This extends previous work done by Jianyang Pan in 2018 on the addition and multiplication routines.
- Émilien Failly (CPP Nancy, from April 2019 until June 2019). Émilien Failly studied the Multiple Polynomial General Number Field Sieve (MNFS). He compared the use of 2, 3, and 4 polynomials on three test numbers: a 60-digit number, a 70-digit number, and a 96-digit number. In each case, the sieving time was estimated, because Cado-NFS cannot currently fully deal with MNFS polynomials.
- Liwei Liu (Peking University, from June 2019 until September 2019). In the context of the computation of discrete logarithms in finite field extensions of small degree, using the Number Field Sieve, Liwei Liu worked on the individual logarithm step, in order to make it faster and more robust.
- Rémi Piau (ÉNS Rennes, from May 2019 until July 2019). Rémi Piau worked on the implementation in Python of our attack against ECDSA using wNAF representation. He was able to improve it by making it cleaner, and using small tricks to make it faster too.

10. Dissemination

10.1. Promoting Scientific Activities

10.1.1. Scientific Events: Selection

10.1.1.1. Member of steering committees

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

Emmanuel Thomé is a member of the steering committee of the Algorithmic Number Theory Symposium (ANTS).

[4] https://github.com/relic-toolkit/relic

10.1.1.2. Member of the Conference Program Committees

- Aurore Guillevic was a member of the Program Committee of Latincrypt 2019 and WCC 2019.
- Virginie Lallemand was a member of the Program Committee of Asiacrypt 2019.
- Cécile Pierrot was a member of the Program Committee of EUROCRYPT 2020 and Journées Codage et Cryptographie 2020.
- Pierre-Jean Spaenlehauer was a member of the Program Committee of ISSAC 2019.
- Emmanuel Thomé is a member of the scientific directorate of the Dagstuhl computer science seminar series.

10.1.2. Journal

10.1.2.1. Member of the Editorial Boards

- Virginie Lallemand is a member of the editorial board of the IACR Transactions on Symmetric Cryptology (ToSC) Journal for 2019/2020. This journal is the open-access journal associated to the International Conference on Fast Software Encryption (FSE). She is also a member of the editorial board for the Special Issue of ToSC on Designs for the NIST Lightweight Standardization Process.

10.1.2.2. 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

- Cécile Pierrot and Pierrick Gaudry were invited to give a talk at the Elliptic Curve Cryptography Conference (ECC19), Bochum, Germany.
- Marine Minier was invited to give a talk at the Journées Scientifiques Inria in Lyon, France, June 2019.
- Pierrick Gaudry gave a lecture during the Summer School Mathematical foundations of asymmetric cryptography, Aussois, France.
- Aurore Guillevic and Virginie Lallemand were invited to give a talk at the C2 seminar (formerly CCA seminar), Paris, France.
- Aurore Guillevic was invited to give a talk at the Workshop on Randomness and Arithmetics for Cryptography on Hardware in Roscoff, Brittany, France.

10.1.4. Research Administration

- Jérémie Detrey chaired the *Commission des Utilisateurs des Moyens Informatiques* (CUMI) of the Inria Nancy – Grand Est research center until November 2019.
- Pierrick Gaudry is:
  - vice-head of the *Commission de mention Informatique* of the *École doctorale IAEM* of the University of Lorraine;
  - a member of the *Conseil Scientifique du GdR IM*;
  - member of the visiting committee for the HCERES evaluation of the CRIStAL laboratory (Lille).
- Aurore Guillevic
  - was member of the CoS, poste MCF number 27MCF1087, Université de Clermont Auvergne;
  - was member of the CoS, poste Chargé d'Enseignement (ChE), École Polytechnique (Palaiseau).
- Marine Minier
  - is a member of Collegium of Science et Techniques of Université de Lorraine;

  - was a member of the CoS, poste MCF number 27MCF-0781944P-4184, Université de Versailles.
- Pierre-Jean Spaenlehauer is a member of the *commission développement technologique* (CDT) of the Inria Nancy - Grand Est research center.
- Emmanuel Thomé
  - is a member of the management committee for the research project "CPER Cyberentreprises" (co-chair);
  - 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 an elected member of the Inria technical committee (CTI).
- Paul Zimmermann is member of the Scientific Committee of the EXPLOR *Mésocentre*, of the "groupe de réflexion" *Calcul, Codage, Information* of the GDR-IM, of the scientific council of the LIRMM laboratory in Montpellier, France.

10.2. Teaching - Supervision - Juries

10.2.1. Teaching

Licence: Jérémie Detrey, *Sécurité des applications Web*, 2h eq. TD, LP, Université de Lorraine, IUT Charlemagne, Nancy, France.

Licence: Pierrick Gaudry, *Intégration Web*, 48h eq. TD, IUT 1A, Université de Lorraine, IUT Charlemagne, Nancy, France.

Licence: Aurore Guillevic, *Introduction to algorithms* (CSE103), 32 eq. TD, L1, École Polytechnique, Palaiseau, France.

Licence: Aurore Guillevic, *Les bases de la programmation et de l'algorithmique* (INF411), 40 eq. TD, 2e année, École Polytechnique, Palaiseau, France.

Master: Marine Minier, *Contrôle d'accès*, 40h eq. TD, M2 Informatique, Université de Lorraine, Faculté des sciences et technologies, Vandœuvre-lès-Nancy, France.

Master: Marine Minier, *Intégration Méthodologique*, 36h eq. TD, M2 Informatique, Université de Lorraine, Faculté des sciences et technologies, Vandœuvre-lès-Nancy, France.

Master: Marine Minier, *Introduction à la cryptographie*, 15h eq. TD, M1 Informatique, Université de Lorraine, Faculté des sciences et technologies, Vandœuvre-lès-Nancy, France.

Licence: Marine Minier, *Introduction à la sécurité et à la cryptographie*, 10 hours (lectures) + 10 hours (tutorial sessions) + 10 hours (practical sessions), L3, Université de Lorraine, Faculté des sciences et technologies, Vandœuvre-lès-Nancy, France.

Licence: Marine Minier, *Mathématiques Discrètes*, 80h eq. TD, L2, Université de Lorraine, Faculté des sciences et technologies, Vandœuvre-lès-Nancy, France.

Responsability of the M2 SIRAV *Sécurité Informatique, Réseaux et Architectures Virtuelles*, 30 students: Marine Minier. Université de Lorraine, Faculté des sciences et technologies, Vandœuvre-lès-Nancy, France.

Master: Cécile Pierrot, *Introduction à la cryptographie*, 60h eq. TD, Mastère spécialisé en sécurité, École des Mines de Nancy, France.

Master: Cécile Pierrot, *Introduction à LaTeX*, 6h eq. TD, Master 1, École des Mines de Nancy, France.

Master: Emmanuel Thomé, *Protocoles de sécurité et Vérification* (sub-part dedicated to cryptographic primitives), 8h (lectures) + 6h (tutorial sessions), Télécom Nancy.

10.2.2. Supervision

PhD in progress: Sandra Rasoamiaramanana, *Délivrance de contextes sécurisés par des approches hybrides*, since May 2017, PhD CIFRE Orange Gardens, Marine Minier. Planed to be defended in April 2020.

PhD in progress: Simon Masson, *Algorithmique des courbes destinées aux contextes de la cryptographie bilinéaire et post-quantique*, since Jan. 2018, Emmanuel Thomé and Aurore Guillevic.

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: Paul Huynh, *Analyse et conception de chiffrements authentifiés à bas coût*, since Oct. 2017, Marine Minier.

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.

10.2.3. Juries

Pierrick Gaudry was

- reviewer of the PhD thesis *Arithmétique rapide pour des corps finis* defended by Robin Larrieu, December 2019, École polytechnique;
- member of the PhD thesis jury *Delaunay triangulations of a family of symmetric hyperbolic surfaces in practice* defended by Iordan Iordanov, March 2019, Université de Lorraine;
- member of the HdR jury *Cryptographie basée sur les corps quadratiques : cryptanalyses, primitives et protocoles* defended by Guilhem Castagnos, November 2019, Université de Bordeaux.

Virginie Lallemand was member of the PhD thesis jury: *Optimization of Core Components of Block Ciphers* defended by Baptiste Lambin on the 22nd of October 2019 at the University of Rennes 1.

Marine Minier:

- reviewer of the PhD thesis: Secure Multi-Party Computation and Privacy defended by Aurélien Dupin, June 2019, ENS Ulm, Paris.
- reviewer of the PhD thesis: Optimization of Core Components of Block Ciphers defended by Baptiste Lambin, October 2019, Université de Rennes, Rennes.
- reviewer of the PhD thesis: Représentations adaptées à l'arithmétique modulaire et à la résolution de systèmes flous defended by Jérémie Marrez, December 2019, Université Paris 6, Paris.
- reviewer of the PhD thesis: Security for the Internet of Things: A bottom-up approach to the secure and standardized Internet of Things defended by Timothy Claeys, December 2019, Université Grenoble Alpes, Grenoble.
- President of the PhD thesis jury: Software Datapaths for Multi-Tenant Packet Processing defended by Paul Chaignon, June 2019, Université de Lorraine, Nancy.
- President of the PhD thesis jury: Usability: low tech, high security, defended by Nicolas Blanchard, June 2019, Université de Paris, Paris.
- President of the PhD thesis jury: Contributions à l'analyse de canaux auxiliaires sans connaissance des clairs et chiffrés, et à la recherche de S-boxs compactes, defended by Léo Reynaud, December 2019, Université de Limoges, Limoges.

Emmanuel Thomé was:

- reviewer for the HDR thesis *Algorithmes et implantations efficaces en algèbre linéaire exacte* defended by Pascal Giorgi, October 2019, Université de Montpellier.
- member of the PhD thesis jury *Vote électronique : définitions et techniques d'analyse* defended by Joseph Lallemand, November 2019, Université de Lorraine;

Paul Zimmermann was reviewer of the PhD thesis *Formalisations d'analyses d'erreurs en analyse numérique et en arithmétique à virgule flottante* defended by Florian Faissole, December 2019, Université Paris-Saclay.

10.3. Popularization

10.3.1. Internal or external Inria responsibilities

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.

10.3.2. Articles and contents

- Cécile Pierrot wrote a blog post for Le Monde Binaire.

10.3.3. Interventions

- Cécile Pierrot gave a talk about women in science at a meeting *Les Filles, osez les sciences !* in Reims, March 2019.
- Cécile Pierrot and Paul Zimmermann took part in La Fête de la Science, Nancy and Bouxurulles, October 2019.
- Cécile Pierrot gave a talk at La Cité des Sciences, Paris, to open the exhibition called *Espions*, November 2019.
- Pierre-Jean Spaenlehauer gave an introductory talk on polynomial systems to visiting students of the ÉNS Paris-Saclay.

11. Bibliography

Publications of the year

Articles in International Peer-Reviewed Journals

[1] S. ABELARD. *Counting points on hyperelliptic curves with explicit real multiplication in arbitrary genus*, in "Journal of Complexity", 2019, forthcoming [*DOI :* 10.1016/J.JCO.2019.101440], https://hal.inria.fr/hal-01905580

[2] S. ABELARD, P. GAUDRY, P.-J. SPAENLEHAUER. *Improved Complexity Bounds for Counting Points on Hyperelliptic Curves*, in "Foundations of Computational Mathematics", 2019, vol. 19, n° 3, pp. 591-621, https://arxiv.org/abs/1710.03448 [*DOI :* 10.1007/S10208-018-9392-1], https://hal.inria.fr/hal-01613530

[3] N. DAVID, P. ZIMMERMANN. *A New Ranking Function for Polynomial Selection in the Number Field Sieve*, in "Contemporary mathematics", 2019, forthcoming, https://hal.inria.fr/hal-02151093

[4] A. GUILLEVIC. *Faster individual discrete logarithms in finite fields of composite extension degree*, in "Mathematics of Computation", January 2019, vol. 88, n° 317, pp. 1273-1301, https://arxiv.org/abs/1809.06135 [*DOI :* 10.1090/MCOM/3376], https://hal.inria.fr/hal-01341849

[5] D. GÉRAULT, P. LAFOURCADE, M. MINIER, C. SOLNON. *Computing AES related-key differential characteristics with constraint programming*, in "Artificial Intelligence", January 2020, vol. 278, 103183 [*DOI :* 10.1016/J.ARTINT.2019.103183], https://hal.archives-ouvertes.fr/hal-02327893

[6] S. IONICA, E. THOMÉ. *Isogeny graphs with maximal real multiplication*, in "Journal of Number Theory", February 2020, vol. 207, pp. 385-422, https://arxiv.org/abs/1407.6672 [*DOI :* 10.1016/J.JNT.2019.06.019], https://hal.archives-ouvertes.fr/hal-00967742

[7] A. LE GLUHER, P.-J. SPAENLEHAUER. *A Fast Randomized Geometric Algorithm for Computing Riemann-Roch Spaces*, in "Mathematics of Computation", 2019, https://arxiv.org/abs/1811.08237 , forthcoming, https://hal.inria.fr/hal-01930573

[8] S. MAITRA, B. MANDAL, T. MARTINSEN, D. ROY, P. STANICA. *Analysis on Boolean function in a restricted (biased) domain*, in "IEEE Transactions on Information Theory", August 2019, pp. 1-13 [*DOI :* 10.1109/TIT.2019.2932739], https://hal.inria.fr/hal-02374194

Invited Conferences

[9] V. CORTIER, P. GAUDRY, S. GLONDU. *Belenios: a simple private and verifiable electronic voting system*, in "Foundations of Security, Protocols, and Equational Reasoning", Fredericksburg, Virgina, United States, J. D. GUTTMAN, C. E. LANDWEHR, J. MESEGUER, D. PAVLOVIC (editors), LNCS, Springer, 2019, vol. 11565, pp. 214-238 [*DOI :* 10.1007/978-3-030-19052-1_14], https://hal.inria.fr/hal-02066930

International Conferences with Proceedings

[10] E. ANDREEVA, V. LALLEMAND, A. PURNAL, R. REYHANITABAR, A. ROY, D. VIZÁR. *Forkcipher: A New Primitive for Authenticated Encryption of Very Short Messages*, in "ASIACRYPT 2019 - 25th Annual International Conference on the Theory and Application of Cryptology and Information Security", Kobe, Japan, Advances in Cryptology – ASIACRYPT 2019, November 2019, pp. 153-182 [*DOI :* 10.1007/978-3-030-34621-8_6], https://hal.inria.fr/hal-02388234

[11] L. DE FEO, S. MASSON, C. PETIT, A. SANSO. *Verifiable Delay Functions from Supersingular Isogenies and Pairings*, in "Advances in Cryptology - ASIACRYPT 2019 - 25th International Conference on the Theory and Application of Cryptology and Information Security", Kobe, Japan, Advances in Cryptology - ASIACRYPT 2019, August 2019, vol. 1, pp. 248-277 [*DOI :* 10.1007/978-3-030-34578-5_10], https://hal.inria.fr/hal-02388349

[12] P. DERBEZ, V. LALLEMAND, A. UDOVENKO. *Cryptanalysis of SKINNY in the Framework of the SKINNY 2018-2019 Cryptanalysis Competition*, in "SAC 2019 - Selected Areas in Cryptography", Waterloo, Canada, August 2019, https://hal.inria.fr/hal-02388239

[13] J. DETREY, L. IMBERT. *Breaking randomized mixed-radix scalar multiplication algorithms*, in "LATINCRYPT 2019 - 6th International Conference on Cryptology and Information Security in Latin America", Santiago de Chile, Chile, Lecture Notes in Computer Science, 2019, vol. 11774, pp. 24-39 [*DOI :* 10.1007/978-3-030-30530-7_2], https://hal-lirmm.ccsd.cnrs.fr/lirmm-02309203

[14] D. TANG, B. MANDAL, S. MAITRA. *Vectorial Boolean Functions with Very Low Differential-Linear Uniformity Using Maiorana-McFarland Type Construction*, in "Progress in Cryptology – INDOCRYPT 2019", Hyderabad, India, December 2019 [*DOI :* 10.1007/978-3-030-35423-7_17], https://hal.inria.fr/hal-02374286

Software

[15] T. CADO-NFS DEVELOPMENT TEAM. *CADO-NFS, An Implementation of the Number Field Sieve Algorithm*, April 2019, Version : 2.3.0, Software, https://hal.inria.fr/hal-02099620

Other Publications

[16] C. BOUILLAGUET, P. ZIMMERMANN. *Parallel Structured Gaussian Elimination for the Number Field Sieve*, April 2019, working paper or preprint, https://hal.inria.fr/hal-02098114

[17] V. CORTIER, J. DREIER, P. GAUDRY, M. TURUANI. *A simple alternative to Benaloh challenge for the cast-as-intended property in Helios/Belenios*, 2019, working paper or preprint, https://hal.inria.fr/hal-02346420

[18] G. DE MICHELI, R. PIAU, C. PIERROT. *A Tale of Three Signatures: practical attack of ECDSA with wNAF*, December 2019, working paper or preprint, https://hal.archives-ouvertes.fr/hal-02393302

[19] P. GAUDRY, A. GOLOVNEV. *Breaking the encryption scheme of the Moscow Internet voting system*, November 2019, https://arxiv.org/abs/1908.05127 - This work is a merger of arXiv:1908.09170 and arXiv:1908.05127., https://hal.inria.fr/hal-02266264

[20] A. GUILLEVIC. *A short-list of pairing-friendly curves resistant to Special TNFS at the 128-bit security level*, December 2019, working paper or preprint, https://hal.inria.fr/hal-02396352

[21] A. GUILLEVIC, S. MASSON, E. THOMÉ. *Cocks-Pinch curves of embedding degrees five to eight and optimal ate pairing computation*, October 2019, working paper or preprint, https://hal.inria.fr/hal-02305051

[22] A. GUILLEVIC, S. SINGH. *On the Alpha Value of Polynomials in the Tower Number Field Sieve Algorithm*, August 2019, working paper or preprint, https://hal.inria.fr/hal-02263098

[23] A. JOUX, C. PIERROT. *Algorithmic aspects of elliptic bases in finite field discrete logarithm algorithms*, July 2019, https://arxiv.org/abs/1907.02689 - working paper or preprint, https://hal.sorbonne-universite.fr/hal-02173688

[24] E. MILIO, D. ROBERT. *Modular polynomials on Hilbert surfaces*, June 2019, working paper or preprint, https://hal.archives-ouvertes.fr/hal-01520262

References in notes

[25] S. ABELARD. *Counting points on hyperelliptic curves in large characteristic : algorithms and complexity*, Université de Lorraine, September 2018, PhD thesis, https://tel.archives-ouvertes.fr/tel-01876314

[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, P. ZIMMERMANN. *Imperfect Forward Secrecy: How Diffie-Hellman fails in practice*, in "CCS'15", ACM, 2015, pp. 5–17, 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*, 2014, Version 2.03, http://www.ssi.gouv.fr/uploads/2014/11/RGS_v-2-0_B1.pdf

[28] J.-C. FAUGÈRE, P.-J. SPAENLEHAUER, J. SVARTZ. *Sparse Gröbner bases: the unmixed case*, in "ISSAC 2014", K. NABESHIMA (editor), ACM, 2014, pp. 178–185, Proceedings

[29] J.-C. FAUGÈRE, M. SAFEY EL DIN, P.-J. SPAENLEHAUER. *Gröbner Bases of Bihomogeneous Ideals generated by Polynomials of Bidegree* $(1,1)$*: Algorithms and Complexity*, in "J. Symbolic Comput.", 2011, vol. 46, n$^{\text{o}}$ 4, pp. 406–437

[30] A. GUILLEVIC. *Computing Individual Discrete Logarithms Faster in* $GF(p^n)$ *with the NFS-DL Algorithm*, in "Asiacrypt 2015", Auckland, New Zealand, T. IWATA, J. H. CHEON (editors), Lecture Notes in Computer Science, Springer, November 2015, vol. 9452, pp. 149-173 [*DOI :* 10.1007/978-3-662-48797-6_7], https://hal.inria.fr/hal-01157378

[31] 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, P. ZIMMERMANN. *Factorization of a 768-bit RSA modulus*, in "CRYPTO 2010", T. RABIN (editor), Lecture Notes in Comput. Sci., Springer–Verlag, 2010, vol. 6223, pp. 333–350, Proceedings

[32] S. MAITRA, B. MANDAL, T. MARTINSEN, D. ROY, 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", D. CHAKRABORTY, T. IWATA (editors), Lecture Notes in Computer Science, Springer, 2018, vol. 11356, pp. 282–303, https://doi.org/10.1007/978-3-030-05378-9_16

[33] NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY. *Transitions: Recommendation for Transitioning the Use of Cryptographic Algorithms and Key Lengths*, 2011, First revision, http://dx.doi.org/10.6028/NIST.SP.800-131A

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