IN PARTNERSHIP WITH:
CNRS

Université de Lorraine

Activity Report 2018

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, from Oct 2018]
Cécile Pierrot [Inria, Researcher]
Pierre-Jean Spaenlehauer [Inria, Researcher]
Paul Zimmermann [Inria, Senior Researcher, HDR]

Faculty Members

Marine Minier [Université de Lorraine, Professor, HDR]
Marion Videau [Université de Lorraine, Associate Professor, on leave with Quarkslab since Jan 2015]

Post-Doctoral Fellow

Bimal Mandal [Inria, from Nov 2018]

PhD Students

Simon Abelard [Université de Lorraine, until Aug 2018]
Svyatoslav Covanov [Université de Lorraine, until Aug 2018]
Gabrielle de Micheli [Inria, from Oct 2018]
Paul Huynh [CNRS, from Oct 2017]
Aude Le Gluher [Université de Lorraine, from Sep 2018]
Simon Masson [Thales, from Jan 2018]
Andrianina Sandra Rasoamiaramanana [Orange, from May 2017]

Interns

Aude Le Gluher [École Normale Supérieure Rennes, from Feb 2018 until Jun 2018]
Jianyang Pan [Inria, from Jul 2018 until Aug 2018]
Kevin Trancho [CNRS, from May 2018 until Aug 2018]

Administrative Assistants

Emmanuelle Deschamps [Inria]
Annick Jacquot [CNRS, from Jul 2018]
Virginie Priester [CNRS]

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 mathematical objects we deal with are of utmost importance for the applications to cryptology, as they are the background of the most widely developed public-key cryptographic primitives, such as the RSA cryptosystem or the Diffie–Hellman key exchange. 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, through the study of the cornerstone problems, which are the integer factorization and discrete logarithm problems, as well as the optimization work in order to enable cryptographic implementations that are both efficient *and* secure.

Among the research themes we set forth, two are guided by the most important mathematical objects used in today's cryptography, and the two others are rather guided by the technological background we use to address these problems.

- 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.
- Arithmetic. Our work relies crucially on efficient arithmetic, be it for small or large sizes. We work on improving algorithms and implementations, for computations that are relevant to our application areas.

- Polynomial systems. It is rather natural with algebraic curves, and occurs also in NFS-related contexts, that many important challenges can be represented via polynomial systems, which have structural specificities. We intend to develop algorithms and tools that, when possible, take advantage of these specificities.

As represented by Figure 1, the first two challenges above interact with the latter two, which are also research topics in their own right. Both algorithmic and software improvements are the necessary ingredients for success. The different axes of our research form thus a coherent set of research directions, where we apply a common methodology.

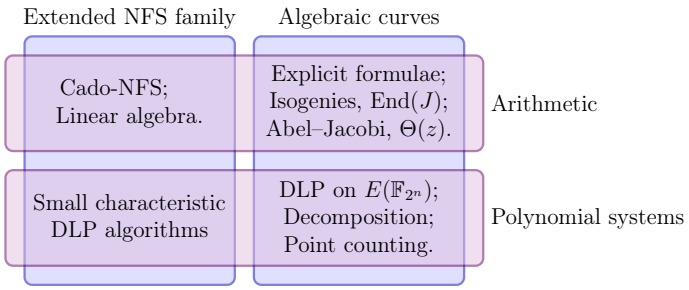


Figure 1. Visual representation of the thematic organization of CARAMBA.

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, parts of our research activity.

2.2. Scientific Grounds

Public-key cryptography is our main application target. We are interested in the study of the cryptographic primitives that serve as a basis for the most widespread protocols.

Since the early days of public-key cryptography, and through the practices and international standards that have been established for several decades, the most widespread cryptographic primitives have been the RSA cryptosystem, as well as the Diffie–Hellman key exchange using multiplicative groups of finite fields. The level of security provided by these cryptographic primitives is related to the hardness of the underlying mathematical problems, which are integer factorization and the discrete logarithm problem. The complexity of attacking them is known to be subexponential in the public key size, and more precisely written as $L_N(1/3, c)$ for factoring an integer N, where the L notation stands for

$$L_N(\alpha, c) = \exp\left(c(1 + o(1))(\log N)^{\alpha}(\log\log N)^{1-\alpha}\right).$$

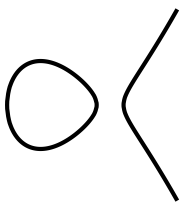
This complexity is achieved with the Number Field Sieve (NFS) algorithm and its many derivatives. This means that as the desired security level s grows, the matching public key size grows roughly like s^3. As to how these complexity estimates translate into concrete assessments and recommendations, the hard facts are definitely the computational records that are set periodically by academics, and used as key ingredients by governmental agencies emitting recommendations for industry [31], [18].

Software for NFS is obviously the entry point to computational records. Few complete NFS implementations exist, and their improvement is of crucial importance for better assessment of the hardness of the key cryptographic primitives considered. Here, "improvement" may be understood in many ways: better algorithms (outperforming the NFS algorithm as a whole is certainly a tremendous improvement, but replacing one of its numerous substeps is one, too), better implementations, better parallelization, or better adaptation to suitable hardware. The numerous sub-algorithms of NFS strongly depend on arithmetic efficiency. This concerns various mathematical objects, from integers and polynomials to ideals in number fields, lattices, or linear algebra.

Since the early 1990's, no new algorithm has improved on the complexity of NFS. As it is used in practice, the algorithm has complexity $L_N(1/3, (64/9)^{1/3})$ for factoring general integers or for computing discrete logarithms in prime fields of similar size (the so-called "multiple polynomial" variants have better complexity by a very thin margin, but this has not yet yielded a practical improvement). Given the wide use of the underlying hard problems, progress in this area is of utmost importance. In 2013, several new algorithms have modified the complexity of the discrete logarithm problem in small characteristic fields, which is a closely related problem, reaching a heuristic quasi-polynomial time algorithm [20], [27], [26], [24]. A stream of computational records have been obtained since 2013 with these algorithms, using in particular techniques from polynomial system solving, or from Galois theory. These new algorithms, together with these practical realizations, have had a very strong impact of course on the use of small-characteristic fields for cryptography (now clearly unsuitable), as well as on pairings on elliptic curves over small-characteristic finite fields (which are also no longer considered safe to use).

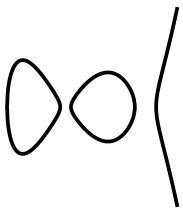
While it is relatively easy to set public key sizes for RSA or Diffie–Hellman that are "just above" the reach of academic computing power with NFS, the sensible cryptographic choice is to aim at security parameters that are well above this feasibility limit, in particular because assessing this limit precisely is in fact a very difficult problem. In line with the security levels offered by symmetric primitives such as AES-128, public key sizes should be chosen so that with current algorithmic knowledge, an attacker would need at least 2^{128} elementary operations to solve the underlying hard problem. Such security parameters would call for RSA key sizes above 3,000 bits, which is seldom seen, except in contexts where computing power is plentiful anyway.

Since the mid-1980's, elliptic curves, and more generally Jacobians of algebraic curves, have been proposed as alternative mathematical settings for building cryptographic primitives.



A genus-1 curve

$y^2 = x^3 + ax + b.$



A genus-2 curve

$y^2 = x^5 + a_4x^4 + \cdots + a_0.$

Figure 2.

The discrete logarithm problem in these groups is formidably hard, and in comparison to the situation with the traditional primitives mentioned above, the cryptanalysis algorithms are such that the appropriate public-key size grows only linearly with the desired security level: a 256-bit public key, using algebraic curves, is well suited to match the hardness of AES-128. This asset makes algebraic curves more attractive for the future of public-key cryptography.

Challenges related to algebraic curves in cryptology are rather various, and call for expertise in several areas. Suggesting curves to be used in the cryptographic context requires solving the point counting problem. This may be done by variants of the Schoof–Elkies–Atkin algorithm and its generalizations (which, in genus 2, require arithmetic modulo multivariate systems of equations), or alternatively the use of the complex multiplication method, a rich theory that opens the way to several problems in computational number theory.

The long-awaited transition from the legacy primitives to primitives based on curves is ready to happen, only circumstantially slowed down presently by the need to agree on a new set of elliptic curves (not because of any attack, but because of skepticism over how the currently widespread ones have been generated). The Internet Research Task Force has completed in 2015 a standardization proposal [30]. In this context, the recommended curves are not of the complex multiplication family, and enjoy instead properties that allow fast implementation, and avoid a few implementation difficulties. Those are also naturally chosen to be immune to the few known attacks on the discrete logarithm problem for curves. No curve of genus 2 has made its way to the standardization process so far, however one candidate exists for the 128-bit security level [23].

The discrete logarithm problem on curves is very hard. Some results were obtained however for curves over extension fields, using techniques such as the Weil descent, or the point decomposition problem. In this context, the algorithmic setup connects to polynomial system solving, fast arithmetic, and linear algebra.

Another possible route for transitioning away from RSA and finite field-based cryptography is suggested, namely the switch to the "post-quantum" cryptographic primitives. Public-key cryptographic primitives that rely on mathematical problems related to Euclidean lattices or coding theory have an advantage: they would resist the potential advent of a quantum computer. Research on these topics is quite active, and there is no doubt that when the efficiency challenges that are currently impeding their deployment are overcome, the standardization of some post-quantum cryptographic primitives will be a worthwhile addition to the general cryptographic portfolio. The NSA has recently devoted an intriguing position text to this topic [32] (for a glimpse of some of the reactions within the academic community, the reference [29] is useful). Post-quantum cryptography, as a research topic, is complementary to the topics we address most, which are NFS and algebraic curves. We are absolutely confident that, at the very least for the next decade, primitives based on integer factoring, finite fields, and algebraic curves will continue to hold the lion's share in the cryptographic landscape. We also expect that before the advent of standardized and widely developed post-quantum cryptographic primitives, the primitives based on algebraic curves will become dominant (despite the apparent restraint from the NSA on this move).

We acknowledge that the focus on cryptographic primitives is part of a larger picture. Cryptographic primitives are part of cryptographic protocols, which eventually become part of cryptographic software. All these steps constitute research topics in their own right, and need to be scrutinized (as part of independent research efforts) in order to be considered as dependable building blocks. This being said, the interplay of the different aspects, from primitives to protocols, sometimes spawns very interesting and fruitful collaborations. A very good example of this is the LogJam attack [17].

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 during the 2014–2016 period, 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. 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 in 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. As of 2016, the most widely used set of elliptic curves, the so-called NIST curves, are in the process of being replaced by a new set of candidate elliptic curves for future standardization. This is the topic of RFC 7748 [30].

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 Université of 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. The aim is to design and analyze symmetric key cryptographic primitives focusing on the following particular aspects:

- the use of constraint programming for the cryptanalysis, especially of block ciphers and the AES standard;

- the design of lightweight cryptographic primitives well-suited for constraint environment such as micro-controllers, wireless sensors, etc.
- white-box cryptography and software obfuscation methods to protect services execution on dedicated platforms.

3.4. Computer Arithmetic

Computer arithmetic is part of the common background of all team members, and is naturally ubiquitous in the two previous application domains mentioned. 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 [22], [21].

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.
- The recent 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 [22], [21]. 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 [1], German BSI, or the NIST [2] in the United States base their recommendations on such computational achievements.

The software we make available to achieve these cryptanalytic computations also allows us to give cost estimates for potential attacks to cryptographic systems that are taking the security/efficiency/legacy compatibility trade-offs too lightly. Attacks such as LogJam [17] 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.

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, 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

[1] In [18], the minimal recommended RSA key size is 2048 bits for usage up to 2030. See also Annex B, in particular Section B.1 "Records de calculs cryptographiques".

[2] The work [28] is one of only two academic works cited by NIST in the initial version (2011) of the report [31].

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

- Several Invited talks: Pierrick Gaudry was an invited speaker at the ECC 2018 workshop (Osaka, Japan); Emmanuel Thomé was an invited speaker at the ANTS-XIII conference in Madison, WI, USA (The biennial ANTS conference is the main international conference on algorithmic number theory); Paul Zimmermann was an invited speaker at the 75th anniversary celebration of the journal *Mathematics of Computation* (Providence, RI, USA).
- Cécile Pierrot was awarded the DGA (Direction Générale de l'Armement) Prize from Florence Parly, the Minister of the Armed Forces, for her PhD Thesis.

BEST PAPER AWARD:

[11]
M. SCOTT, A. GUILLEVIC. *A New Family of Pairing-Friendly elliptic curves*, in "International Workshop on the Arithmetic of Finite Fields - WAIFI", Bergen, Norway, L. BUDAGHYAN, F. RODRIGUEZ-HENRIQUEZ (editors), June 2018, https://hal.inria.fr/hal-01875361

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 verifiablity 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 total in 2018, more than 13000 ballots have been cast using the voting platform Belenios.

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

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", and also parallelizes better. The memory footprint of the central step of linear algebra has been reduced, and the parallelism of this step has been improved.

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

6.3. rrspace

RIemann-Roch spaces
KEYWORD: Riemann-Roch spaces
FUNCTIONAL DESCRIPTION: The software rrspace implements an algorithm for computing a basis of the Riemann-Roch space associated to a divisor on a curve defined over a finite field. It also implements an algorithm for computing the group law in the Jacobian of such curves. The main algorithm is a variant of Brill-Noether's approach, designed during Aude Le Gluher's Master thesis.

- Participants: Pierre-Jean Spaenlehauer and Aude Le Gluher
- Contact: Pierre-Jean Spaenlehauer
- URL: https://gitlab.inria.fr/pspaenle/rrspace

6.4. Platforms

6.4.1. Platform: computational resources

The computational resources of Caramba have increased significantly in 2018. On the one hand, the CPER «CyberEntreprises» (French Ministry of Research, Région Grand Est, Inria, CNRS) funded the acquisition of a 64-node, 2,048-core cluster called `grvingt`. 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) was moved 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 computation. 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.

7. New Results

7.1. A new family of pairing-friendly elliptic curves

Participant: Aurore Guillevic.

In [11], together with M. Scott from Miracl, we presented an algorithm to generate new families of pairing-friendly curves. It generalizes the very popular Barreto-Naehrig curves. This paper jointly received the best paper award of the conference.

7.2. Faster individual discrete logarithms in finite fields of composite extension degree

Participant: Aurore Guillevic.

We improved in [7] the previous work [25] 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 is now published.

7.3. Polynomial Time Bounded Distance Decoding near Minkowski's Bound in Discrete Logarithm Lattices

Participant: Cécile Pierrot [contact].

In [6], together with Léo Ducas, we proposed a concrete family of dense lattices of arbitrary dimension n in which the lattice Bounded Distance Decoding (BDD) problem can be solved in deterministic polynomial time. The lattice construction needs discrete logarithm computations that can be made in deterministic polynomial time for well-chosen parameters. Each lattice comes with a deterministic polynomial time decoding algorithm able to decode up to a large radius. Namely, we reached decoding radius within $O(\log n)$ Minkowski's bound, for both ℓ_1 and ℓ_2-norms.

7.4. Improved complexity bounds for counting points on hyperelliptic curves

Participants: Simon Abelard, Pierrick Gaudry [contact], Pierre-Jean Spaenlehauer [contact].

In [3], we presented a probabilistic Las Vegas algorithm for computing the local zeta function of a hyperelliptic curve of genus g defined over $\mathbb{F}_q$. It is based on the approaches by Schoof and Pila combined with a modeling of the ℓ-torsion by structured polynomial systems. Our main result improves on previously known complexity bounds by showing that there exists a constant $c > 0$ such that, for any fixed g, this algorithm has expected time and space complexity $O((\log q)^{cg})$ as q grows and the characteristic is large enough.

7.5. Counting points on genus-3 hyperelliptic curves with explicit real multiplication

Participants: Simon Abelard, Pierrick Gaudry [contact], Pierre-Jean Spaenlehauer [contact].

In [9], we proposed a Las Vegas probabilistic algorithm to compute the zeta function of a genus-3 hyperelliptic curve defined over a finite field $\mathbb{F}_q$, with explicit real multiplication by an order $\mathbb{Z}[\eta]$ in a totally real cubic field. Our main result states that this algorithm requires an expected number of $O((\log q)^6)$ bit-operations, where the constant in the $O()$ depends on the ring $\mathbb{Z}[\eta]$ and on the degrees of polynomials representing the endomorphism η. As a proof-of-concept, we computed the zeta function of a curve defined over a 64-bit prime field, with explicit real multiplication by $\mathbb{Z}[2\cos(2\pi/7)]$.

7.6. Counting points on hyperelliptic curves with explicit real multiplication in arbitrary genus

Participant: Simon Abelard.

In [14], we presented a probabilistic Las Vegas algorithm for computing the local zeta function of a genus-g hyperelliptic curve defined over $\mathbb{F}_q$ with explicit real multiplication (RM) by an order $\mathbb{Z}[\eta]$ in a degree-g totally real number field. It is based on the approaches by Schoof and Pila in a more favorable case where we can split the ℓ-torsion into g kernels of endomorphisms, as introduced by Gaudry, Kohel, and Smith in genus 2. To deal with these kernels in any genus, we adapted a technique that Abelard, Gaudry, and Spaenlehauer introduced to model the ℓ-torsion by structured polynomial systems. Applying this technique to the kernels, the systems we obtained are much smaller and so is the complexity of solving them. Our main result is that there exists a constant $c > 0$ such that, for any fixed g, this algorithm has expected time and space complexity $O((\log q)^c)$ as q grows and the characteristic is large enough. We proved that $c \leq 8$ and we also conjecture that the result still holds for $c = 6$.

7.7. A fast randomized geometric algorithm for computing Riemann-Roch spaces

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

In [16], we proposed a probabilistic Las Vegas 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. Our main result shows that this algorithm requires at most $O(\max(\deg(\mathcal{C})^{2\omega}, \deg(D_+)^{\omega}))$ arithmetic operations in k, where ω is a feasible exponent for matrix multiplication and D_+ is the smallest effective divisor such that $D_+ \geq D$. This improves the best known upper bounds on the complexity of computing Riemann-Roch spaces. Our algorithm may fail, but we showed that provided that a few mild assumptions are satisfied, the failure probability is bounded by $O(\max(\deg(\mathcal{C})^4, \deg(D_+)^2)/|E|)$, where E is a finite subset of k in which we pick elements uniformly at random. We provide a freely available C++/NTL implementation of the proposed algorithm, and experimental data. In particular, our implementation enjoys a speed-up larger than 9 on several examples compared to the reference implementation in the Magma computer algebra system. As a by-product, our algorithm also yields a method for computing the group law on the Jacobian of a smooth plane curve of genus g within $O(g^{\omega})$ operations in k, which slightly improves in this context the best known complexity $O(g^{\omega+\varepsilon})$ of Khuri-Makdisi's algorithm.

7.8. Formal proof of mpfr_add

Participants: Jianyang Pan, Paul Zimmermann [contact].

With the help of Karthik Bhargavan (Prosecco project-team), we proved formally the correctness of the `mpfr_add` code in case where all inputs and the output have the same precision, and this precision is less than one limb (i.e., less than 64 bits on modern computers). The algorithm was proven formally correct using the F^* language, and the extracted code, which was shown to be as efficient as the original MPFR code, is now available in MPFR. A similar work was done for the multiplication `mpfr_mul`, but the proof of correctness was only partly completed.

7.9. Various ways to split a floating-point number

Participant: Paul Zimmermann.

Together with Claude-Pierre Jeannerod and Jean-Michel Muller (AriC project-team), we revisited in an unified way the classical algorithms to split a floating-point number in two parts, and some applications of these algorithms. Some new algorithms were also designed. This work was presented at the 25th IEEE Symposium on Computer Arithmetic [10].

7.10. A polyhedral method for sparse systems with many positive solutions

Participant: Pierre-Jean Spaenlehauer.

Together with Frédéric Bihan (Université Savoie Mont Blanc) and Francisco Santos (Universidad de Cantabria), we investigated in [4] a version of Viro's method for constructing polynomial systems with many positive solutions, based on regular triangulations of the Newton polytope of the system. The number of positive solutions obtained with our method is governed by the size of the largest positively decorable subcomplex of the triangulation. Here, positive decorability is a property that we introduced and which is dual to being a subcomplex of some regular triangulation. Using this duality, we produced large positively decorable subcomplexes of the boundary complexes of cyclic polytopes. As a byproduct we obtained new lower bounds, some of them being the best currently known, for the maximal number of positive solutions of polynomial systems with prescribed numbers of monomials and variables. We also studied the asymptotics of these numbers and observed a log-concavity property.

7.11. Fast Integer Multiplication Using Generalized Fermat Primes

Participants: Svyatoslav Covanov, Emmanuel Thomé [contact].

In [5] we described an algorithm for the multiplication of two n-bit integers. It achieves the best asymptotic complexity bound $O(n \log n \cdot 4^{\log^* n})$ under a hypothesis on the distribution of generalized Fermat primes of the form $r^{2^\lambda} + 1$. This hypothesis states that there always exists a sufficiently small interval in which we can find such a prime. Experimental results support this assumption. This article was submitted to Mathematics of Computation and was completely rewritten in late 2017-early 2018. It is now accepted for final publication.

7.12. Improved Methods for Finding Optimal Formulae for Bilinear Maps in a Finite Field

Participant: Svyatoslav Covanov.

In [15], we described a method improving on the exhaustive search algorithm originally developed in [19]. We are able to compute new optimal formulae for the short product modulo X^5 and the circulant product modulo $(X^5 - 1)$. Moreover, we proved that there is essentially only one optimal decomposition of the product of 3×2 by 2×3 matrices up to the action of some group of automorphisms. This work has been submitted to *Theoretical Computer Science* and is tentatively accepted, pending minor revisions.

7.13. Using Constraint Programming to Solve a Cryptanalytic Problem

Participant: Marine Minier.

In [8], we described Constraint Programming (CP) models to solve a cryptanalytic problem: the related key differential attacks against the standard block cipher AES. We improved our models for those attacks and the time required to solve the related key differential attacks for all instances of this particular problem. In particular, we were able to find the best related key differential trails for all the instances of AES-128, AES-192 and AES-256 in less than 5 core-hours except for one instance (AES-128 with 5 rounds) that took 15 core-hours.

7.14. Preparation of a submission for the NIST call dedicated to standardization of lightweight cryptography

Participants: Marine Minier [contact], Paul Huynh, Virginie Lallemand.

During these last six months, we prepared a submission to the NIST call dedicated on lightweight cryptography. The criteria required by this call are various and concern both small embedded micro-controllers and efficient hardware implementation with side channel and fault attack resistance. The proposal will be submitted by the call deadline, at the latest on Feb 25th, 2019.

8. Bilateral Contracts and Grants with Industry

8.1. Bilateral Contracts with Industry

- We have training and consulting activities with the French Ministry of Defense.
- Together with the PESTO team, we have a contract with the Docapost company, the purpose of which is to impove their e-voting solution by adding some verifiability properties and switching to elliptic curve cryptography.
- In this contract handled in collaboration with the University of Bristol and the PESTO team, the goal is to audit and prove security properties of a new e-voting protocol called CHVote, to be used in a few cantons of Switzerland.

8.2. Bilateral Grants with Industry

- This 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.
- This contract with Thales (Thales Communication & Security, Genneviliers, 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, IECL, 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 6.4.

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: organisme, labo (pays) 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.

10. Dissemination

10.1. Promoting Scientific Activities

10.1.1. Scientific Events Organisation

10.1.1.1. Member of the Organizing Committees

Paul Zimmermann co-organized two workshops on the development of the iRRAM, GNU MPFR and GNU MPC libraries: one in Dagstuhl in April, with 10 participants, and one in Trier in November, with 12 participants.

Paul Zimmermann also chaired the organizing committee of the EJCIM (*École Jeunes Chercheurs Informatique Informatique Mathématique*) which took place in Nancy in 2018.

10.1.2. Scientific Events Selection

Emmanuel Thomé is a member of the scientific directorate of the Dagstuhl computer science seminar series.

10.1.2.1. Member of steering committees

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

10.1.2.2. Member of the Conference Program Committees

Paul Zimmermann was a member of the program committee of ANTS XIII (Thirteenth Algorithmic Number Theory Symposium, University of Wisconsin, Madison, WI, USA).

10.1.3. Journal

10.1.3.1. Member of the Editorial Boards

- Virginie Lallemand is a member of the editorial board of the IACR Transactions on Symmetric Cryptology (ToSC) Journal for 2018/2019. This journal is the open-access journal associated to the International Conference on Fast Software Encryption (FSE).
- Marine Minier is a guest editor of the special issue of Workshop on Coding and Cryptography (WCC) in the journal Designs, Codes and Cryptography (DCC).

10.1.3.2. 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.

10.1.4. Invited Talks

- Emmanuel Thomé was invited to give a talk at the ANTS-XIII conference (Madison, WI, USA).
- Marine Minier was invited to give a talk at the Journées Nationales du GT Codage & Cryptographie, Aussois, France.
- Marine Minier was invited to give a talk at Journée "Protection du code et des données, obfuscation & whitebox cryptography", Paris Saclay, France.
- Paul Zimmermann was invited to give a talk at the topical workshop Celebrating 75 Years of Mathematics of Computation (ICERM, Providence, RI, USA).
- Pierrick Gaudry was invited to give a talk at the 22nd Workshop on Elliptic Curve Cryptography (ECC 2018) in Osaka, Japan.

10.1.5. Research Administration

- Jérémie Detrey chairs the *Commission des Utilisateurs des Moyens Informatiques* (CUMI) of the Inria Nancy – Grand Est research center.
- Pierrick Gaudry is vice-head of the *Commission de mention Informatique* of the *École doctorale IAEM* of the University of Lorraine and is a member of the *Conseil Scientifique du GdR IM*.

  He was:
  - member of the CoS, poste MCF number 27MCF1087, Université de Lorraine;
  - member of the CoS, poste PR number 25PR1054, Université de Lorraine;
  - member of the CoS, poste MCF number 25MCF4159, Université de Toulon.
- Marine Minier is a member of Collegium of Science et Techniques of Université de Lorraine. She was:
  - president of the CoS, poste PR number 27PR1057, Université de Lorraine;
  - member of the CoS, poste MCF number 27MCF0403, Université de Grenoble;
  - member of the CoS, poste PR number 270001, École Navale de Brest;
  - member of the CoS, poste MCF number 27MCF4111, Université de Bretagne Sud;

- 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 *Comité Local Hygiène, Sécurité, et Conditions de Travail* of the Inria Nancy – Grand Est research center.
  - chaired the hiring committee for the junior research positions (CR) at Inria Nancy.
- Marion Videau
  - was a member of the hiring committee for the junior research positions (CR) at Inria Rennes.
- 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 advisory board of the OpenDreamKit european project, of the scientific council of the LIRMM laboratory in Montpellier.

10.2. Teaching - Supervision - Juries

10.2.1. Teaching

Licence: Cécile Pierrot, *Programmation avancée en Python - TCSS5AC*, 20 eq. TD, L3, Ecole des Mines, Nancy, France.

Master: Cécile Pierrot, *Introduction à Latex*, 3 eq. TD, M1, Ecole des Mines, Nancy, France.

Licence: Jérémie Detrey, *Sécurité des applications Web*, 2 hours (lecture), L1, Université de Lorraine, IUT Charlemagne, Nancy, France.

Licence, Aurore Guillevic, *Méthodologie de conception et de programmation*, 16 eq. TD (24 TP), L1, Université de Lorraine, Nancy, France.

Formation Continue, Aurore Guillevic, *Introduction à la cryptographie pour enseignants de l'option ISN (informatique et sciences du numérique) en lycée*, 7 eq. TD, Espé de Lorraine (École supérieure du professorat et de l'éducation), 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-les-Nancy, France.

Master: Marine Minier, *Introduction à la cryptographie*, 18h eq. TD, M1 Informatique, Université de Lorraine, Faculté des sciences et technologies, Vandœuvre-les-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-les-Nancy, France.

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

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

10.2.2. Supervision

Ph.D.: Simon Abelard, *Comptage de points de courbes algébriques sur les corps finis et interactions avec les systèmes polynomiaux*, Univ. Lorraine. Defended 7 sept 2018, Pierrick Gaudry & Pierre-Jean Spaenlehauer.

PhD: Svyatoslav Covanov, *Algorithmes de multiplication : complexité bilinéaire et méthodes asymptotiquement rapides*, Université de Lorraine. Defended 5 June 2018, Emmanuel Thomé and Jérémie Detrey.

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: 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: Gabrielle De Micheli, *Le logarithme discret dans les corps finis*, since Oct. 2018, Cécile Pierrot et Pierrick Gaudry.

PhD in progress: Paul Huynh, *analyse et conception de chiffrements authentifiés à bas coût*, since Oct. 2017, Marine Minier.

PhD in progress: Sandra Rasoamiaramanana, *Délivrance de contextes sécurisés par des approches hybrides*, since May 2017, Ph.D. CIFRE Orange Gardens, Marine Minier.

10.2.3. Juries

Pierrick Gaudry: reviewer of the PhD thesis: *Arithmetric and geometric structures in cryptography* defended by Benjamin Wesolowski, October 2018, EPFL (Switzerland).

Marine Minier:

- reviewer of the PhD thesis: *Trust evaluation in secure architectures* defended by Jean-Baptiste Orfila, July 2018, Université Grenoble Alpes.
- member of the PhD thesis jury: *Security analysis of contactless communication protocols* defended by David Gérault, November 2018, Université Clermont Auvergne.
- member of the PhD thesis jury: *Cryptanalysis of symmetric key algorithms* defended by Colin Chaigneau, November 2018, Université de Versailles.

10.3. Popularization

10.3.1. Articles and contents

- *In books/journals for the general public.*

  Paul Zimmermann coordinated (and largely contributed to) the translation into English of the 2013 book *Calcul mathématique avec Sage*. At the same time, the book was updated to a more recent version of the Sage software tool. The resulting book will be published by SIAM at the end of 2018, while an electronic version will remain available under a Creative Commons license [12].
- *For online publications.* Pierrick Gaudry co-authored a blog article about e-voting and the Belenios tool [13].
- *Interviews in order to popularize.* Cécile Pierrot gave a radio interview at France Bleue about being a cryptographer.
- *Videos.* Cécile Pierrot worked with Accustica, a company which promotes popularization. A portrait was created for the exhibition "Les filles, osez les sciences !" [3]. (video link).

10.3.2. Education

Cécile Pierrot was invited to the exhibition "Les filles, osez les sciences !" to make teachers considers how to deconstruct gender stereotypes in (Computer) Science.

[3] Girls, let's dare to do science!

10.3.3. Interventions

Pierrick Gaudry gave a talk about e-voting at the Académie des Sciences.

Emmanuel Thomé gave a talk for students of «classes préparatoires» in Nancy visiting the Inria Nancy research center, on the topic of trapdoored primes in cryptographic standards.

Paul Zimmermann participated in the *Maths-en-jeans* programme, with a class from Lycée Vauban in Luxembourg.

Paul Zimmermann (and Stéphane Glondu from the software development team SED) participated in *Fête de la Science* in October.

Cécile Pierrot co-organized and participated in *Ada Lovelace day*.

Cécile Pierrot gave a talk at Forum de l'Innovation des Armées 2018 about the discrete logarithm problem.

Cécile Pierrot led workshops for secondary-school pupils in Nancy, Reims and Toulouse about research in Computer Science.

11. Bibliography

Publications of the year

Doctoral Dissertations and Habilitation Theses

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

[2] S. COVANOV. *Multiplication algorithms : bilinear complexity and fast asymptotic methods*, Université de Lorraine, June 2018, https://tel.archives-ouvertes.fr/tel-01825744

Articles in International Peer-Reviewed Journals

[3] S. ABELARD, P. GAUDRY, P.-J. SPAENLEHAUER. *Improved Complexity Bounds for Counting Points on Hyperelliptic Curves*, in "Foundations of Computational Mathematics", 2018, https://hal.inria.fr/hal-01613530

[4] F. BIHAN, F. SANTOS, P.-J. SPAENLEHAUER. *A Polyhedral Method for Sparse Systems with many Positive Solutions*, in "SIAM Journal on Applied Algebra and Geometry", 2018, vol. 2, n^{o} 4, pp. 620–645, https://arxiv.org/abs/1804.05683 [*DOI :* 10.1137/18M1181912], https://hal.inria.fr/hal-01877602

[5] S. COVANOV, E. THOMÉ. *Fast integer multiplication using generalized Fermat primes*, in "Mathematics of Computation", 2018, https://arxiv.org/abs/1502.02800 [*DOI :* 10.1090/MCOM/3367], https://hal.inria.fr/hal-01108166

[6] L. DUCAS, C. PIERROT. *Polynomial Time Bounded Distance Decoding near Minkowski's Bound in Discrete Logarithm Lattices*, in "Designs, Codes and Cryptography", 2018, https://hal.archives-ouvertes.fr/hal-01891713

[7] A. GUILLEVIC. *Faster individual discrete logarithms in finite fields of composite extension degree*, in "Mathematics of Computation", 2018, https://arxiv.org/abs/1809.06135 [*DOI :* 10.1090/MCOM/3376], https://hal.inria.fr/hal-01341849

[8] D. GÉRAULT, P. LAFOURCADE, M. MINIER, C. SOLNON. *Revisiting AES Related-Key Differential Attacks with Constraint Programming*, in "Information Processing Letters", 2018, vol. 139, pp. 24-29, https://hal.archives-ouvertes.fr/hal-01827727

International Conferences with Proceedings

[9] S. ABELARD, P. GAUDRY, P.-J. SPAENLEHAUER. *Counting points on genus-3 hyperelliptic curves with explicit real multiplication*, in "ANTS-XIII - Thirteenth Algorithmic Number Theory Symposium", Madison, United States, July 2018, https://hal.inria.fr/hal-01816256

[10] C.-P. JEANNEROD, J.-M. MULLER, P. ZIMMERMANN. *On various ways to split a floating-point number*, in "ARITH 2018 - 25th IEEE Symposium on Computer Arithmetic", Amherst (MA), United States, IEEE, June 2018, pp. 53-60 [*DOI :* 10.1109/ARITH.2018.8464793], https://hal.inria.fr/hal-01774587

[11] *Best Paper*
M. SCOTT, A. GUILLEVIC. *A New Family of Pairing-Friendly elliptic curves*, in "International Workshop on the Arithmetic of Finite Fields - WAIFI", Bergen, Norway, L. BUDAGHYAN, F. RODRIGUEZ-HENRIQUEZ (editors), June 2018, https://hal.inria.fr/hal-01875361.

Scientific Books (or Scientific Book chapters)

[12] P. ZIMMERMANN, A. CASAMAYOU, N. COHEN, G. CONNAN, T. DUMONT, L. FOUSSE, F. MALTEY, M. MEULIEN, M. MEZZAROBBA, C. PERNET, N. M. THIERY, E. BRAY, J. CREMONA, M. FORETS, A. GHITZA, H. THOMAS. *Mathematical Computation with SageMath*, SIAM, 2018, https://hal.inria.fr/hal-01646401

Scientific Popularization

[13] V. CORTIER, P. GAUDRY, S. GLONDU. *(a voté) Euh non : a cliqué*, Le Monde, March 2018, https://hal.inria.fr/hal-01936863

Other Publications

[14] S. ABELARD. *Counting points on hyperelliptic curves with explicit real multiplication in arbitrary genus*, October 2018, working paper or preprint, https://hal.inria.fr/hal-01905580

[15] S. COVANOV. *Improved method for finding optimal formulae for bilinear maps in a finite field*, November 2018, https://arxiv.org/abs/1705.07728 - working paper or preprint, https://hal.inria.fr/hal-01519408

[16] A. LE GLUHER, P.-J. SPAENLEHAUER. *A Fast Randomized Geometric Algorithm for Computing Riemann-Roch Spaces*, November 2018, https://arxiv.org/abs/1811.08237 - working paper or preprint, https://hal.inria.fr/hal-01930573

References in notes

[17] 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

[18] 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

[19] R. BARBULESCU, J. DETREY, N. ESTIBALS, P. ZIMMERMANN. *Finding Optimal Formulae for Bilinear Maps*, in "International Workshop of the Arithmetics of Finite Fields", Bochum, Germany, F. ÖZBUDAK, F. RODRIGUEZ-HENRIQUEZ (editors), Lecture Notes in Computer Science, Ruhr Universitat Bochum, July 2012, vol. 7369 [*DOI :* 10.1007/978-3-642-31662-3_12], https://hal.inria.fr/hal-00640165

[20] R. BARBULESCU, P. GAUDRY, A. JOUX, E. THOMÉ. *A heuristic quasi-polynomial algorithm for discrete logarithm in finite fields of small characteristic*, in "Eurocrypt 2014", Copenhagen, Denmark, P. Q. NGUYEN, E. OSWALD (editors), Springer, May 2014, vol. 8441, pp. 1-16 [*DOI :* 10.1007/978-3-642-55220-5_1], https://hal.inria.fr/hal-00835446

[21] 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

[22] 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^{o} 4, pp. 406–437

[23] P. GAUDRY, É. SCHOST. *Genus 2 point counting over prime fields*, in "J. Symbolic Comput.", 2011, vol. 47, n^{o} 4, pp. 368–400

[24] R. GRANGER, T. KLEINJUNG, J. ZUMBRÄGEL. *On the Powers of 2*, 2014, Cryptology ePrint Archive report, http://eprint.iacr.org/2014/300

[25] 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

[26] F. GÖLOGLU, R. GRANGER, J. MCGUIRE. *On the Function Field Sieve and the Impact of Higher Splitting Probabilities*, in "CRYPTO 2013", R. CANETTI, J. A. GARAY (editors), Lecture Notes in Comput. Sci., Springer–Verlag, 2013, vol. 8043, pp. 109–128, Proceedings, Part II

[27] A. JOUX. *A New Index Calculus Algorithm with Complexity* $L(1/4+o(1))$ *in Small Characteristic*, in "Selected Areas in Cryptography – SAC 2013", T. LANGE, K. LAUTER, P. LISONĚK (editors), Lecture Notes in Comput. Sci., Springer–Verlag, 2014, vol. 8282, pp. 355–379, Proceedings, http://dx.doi.org/10.1007/978-3-662-43414-7_18

[28] 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

[29] N. KOBLITZ, A. J. MENEZES. *A Riddle Wrapped in an Enigma*, 2015, Cryptology ePrint Archive report, http://eprint.iacr.org/2015/1018

[30] A. LANGLEY, M. HAMBURG, S. TURNER. *Elliptic Curves for Security*, 2016, RFC 7748, https://tools.ietf.org/html/rfc7748

[31] 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

[32] NATIONAL SECURITY AGENCY. *Cryptography Today*, 2015, https://www.nsa.gov/