IN PARTNERSHIP WITH:
CNRS

Université de Lorraine

Activity Report 2017

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
B9.4.1. - Computer science
B9.4.2. - Mathematics
B9.8. - Privacy

1. Personnel

Research Scientists

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

Faculty Members

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

Post-Doctoral Fellows

Enea Milio [Inria, until Aug 2017]
Shashank Singh [Inria, until Sep 2017]

PhD Students

Simon Abelard [Univ. Lorraine]
Svyatoslav Covanov [Univ. Lorraine]
Laurent Grémy [Univ. Lorraine, until Aug 2017]
Andrianina Sandra Rasoamiaramanana [Univ. Lorraine and Orange, from May 2017]
Paul Huynh [Univ. Lorraine, from Oct 2017]

Interns

Léo Barré [Univ. Bordeaux, from Mar 2017 until Sep 2017]
Nicolas David [École Normale Supérieure Cachan, from Jun 2017 until Jul 2017]
Quentin Deschamps [École Normale Supérieure Lyon, from Jul 2017 until Aug 2017]

Joël Felderhoff [École Normale Supérieure Lyon, from Jun 2017 until Jul 2017]

Administrative Assistants

Emmanuelle Deschamps [Inria]
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 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 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.

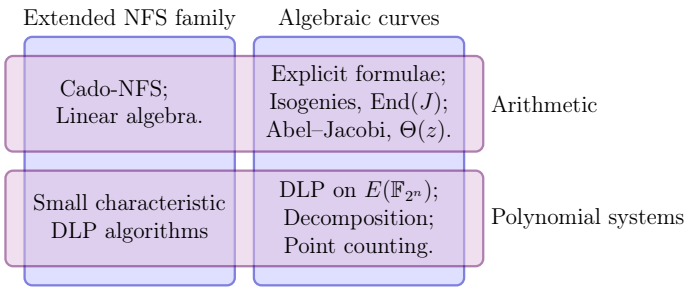

Figure 1. Visual representation of the thematic organization of CARAMBA.

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 [40], [25].

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 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 [27], [35], [34], [32]. 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 to solve 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 [38]. 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 [31].

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 [41] (for a glimpse of some of the reactions within the academic community, the reference [37] 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 [24].

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 in over 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 to 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 [38].

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. 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.

3.4. Symmetric Cryptography

Since the recruiting of Marine Minier in September 2016 as a Professor at Université of Lorraine, 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.

3.5. 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 bases algorithms that can achieve large speedups compared to generic implementations [30], [29].

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, that we describe further in 6.2, 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 Discrete Logarithm Problem on small characteristic finite fields, because it also involves highly structured polynomial systems. While so far we have not contributed to this hot topic, this could of course change in the future.
- The recent hiring of 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 [30], [29]. 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.

[1] In [25], 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 [36] is one of only two academic works cited by NIST in the initial version (2011) of the report [40].

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 [24] 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 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

The CARAMBA team organized the "Journées Codage et Cryptographie 2017", whose objective is to regroup the French speaking community working on error-correcting codes and on cryptography. It is affiliated with the "Groupe de travail C2" of the GDR-IM.

6. New Software and Platforms

6.1. Belenios

Belenios - Verifiable online voting system
KEYWORD: E-voting
FUNCTIONAL DESCRIPTION: Belenios is an 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.

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

6.2. tinygb

KEYWORD: Gröbner bases
FUNCTIONAL DESCRIPTION: Tinygb is a free software which implements tools for computing Gröbner bases with Faugère's F4 algorithm.
NEWS OF THE YEAR: The code has been largely rewritten and optimized. A new release is planned for the beginning of 2018.

- Author: Pierre-Jean Spaenlehauer
- Contact: Pierre-Jean Spaenlehauer
- URL: https://gforge.inria.fr/projects/tinygb/

6.3. 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.

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

7. New Results

7.1. Improved Complexity Bounds for Counting Points on Hyperelliptic Curves

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

In [16], we present 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.

7.2. Deciphering of a Code Used by a 19th Century Parisian Violin Dealer

Participant: Pierrick Gaudry.

This paper [4] is joint work with Jean-Philippe Échard, Curator at the Cité de la Musique, Paris.

The study of three ledgers from the archives of a prominent Parisian violin maker's workshop (active from 1796 to 1948) reveals that some of their content was encrypted. We present the deciphering of the code, and a discussion of its use in the context of the workshop. Charles-Adolphe Gand introduced this code around 1847 to encrypt values of antique/used violins he would buy and resell. His successors maintained the use of this code at least until 1921. Taking a few examples of instruments by Stradivari and other violin makers, we illustrate how the decoded ledgers – listing transactions for more than 2,500 instruments – are of high interest as historical sources documenting the margins, rebates, and commercial practices of these violin dealers. More generally, we contribute to better describing the evolution of the market for antique instruments of the violin family.

7.3. Discrete Logarithm Record Computation in Extension Fields

Participants: Laurent Grémy, Aurore Guillevic, Emmanuel Thomé.

Together with F. Morain from the GRACE team, we reached new record sizes for the discrete logarithm problems over non-prime finite fields of small extension degrees [19], [8]. Assessing the hardness of the discrete logarithm problem in such fields is highly relevant to the security of cryptographic pairings. Our computations are not terribly large computations compared to other record-size computations for integer factoring or discrete logarithm over prime fields, but on the other hand more novelty is present in these contexts: use of automorphisms, higher degree sieving, for example.

Further research in this direction is needed, especially regarding the effectiveness of the variants of the "tower" number field sieve variants.

Furthermore, A. Guillevic and L. Grémy have gathered in a database all published records of discrete logarithm computations in all kinds of finite fields. The database is hosted on gitlab and is open to external contributions. A web interface for browsing the database is available at http://perso.ens-lyon.fr/laurent.gremy/dldb/index.html.

7.4. Using Constraint Programming to Solve a Cryptanalytic Problem

Participant: Marine Minier.

In [7], we describe Constraint Programming (CP) models to solve a cryptanalytic problem: the related key differential attack against the standard block cipher AES. We show that CP solvers are able to solve these problems quicker than dedicated cryptanalysis tools, and we prove that the 11 rounds solution on AES-192 claimed to be optimal is wrong. Instead, we provide the best related key differential characteristic on 10 rounds of AES-192. We also improved the related-key distinguisher and the basic related-key differential attack on the full AES-256 by a factor 2^6 and the q-multicollisions by a factor 2.

7.5. Optimized Binary64 and Binary128 Arithmetic with GNU MPFR

Participant: Paul Zimmermann.

Together with Vincent Lefèvre (ARIC team, Inria Rhône-Alpes), Paul Zimmermann wrote an article "Optimized Binary64 and Binary128 Arithmetic with GNU MPFR", and presented it at the 24th IEEE Symposium on Computer Arithmetic [9]. This article describes algorithms used to optimize the GNU MPFR library when the operands fit into one or two words. On modern processors, a correctly rounded addition of two quadruple precision numbers is now performed in 22 cycles, a subtraction in 24 cycles, a multiplication in 32 cycles, a division in 64 cycles, and a square root in 69 cycles. It also introduces a new faithful rounding mode, which enables even faster computations. These optimizations will be available in version 4 of MPFR.

7.6. A New Measure for Root Optimization

Participants: Nicolas David, Paul Zimmermann.

In the General Number Field Sieve (GNFS) for integer factorization or discrete logarithm, the first stage is polynomial selection. Polynomial selection itself consists in two steps: size-optimization and root-optimization. The classical measures used to rank polynomials during the root-optimization are the so-called α and Murphy-E values. During the internship of Nicolas David, it was shown that these classical measures might be off by up to 15% between two polynomial pairs, compared to a sieving test. A new measure that better corresponds to sieving tests was designed. An article describing these new results is in preparation.

7.7. Mathematical Computation with SageMath

Participant: Paul Zimmermann.

Starting in March, Paul Zimmermann coordinated the English translation of the book "Calcul mathématique avec Sage", and the update from version 5.9 to 8.0 of Sage. He also translated several chapters and proof-read the translation of all chapters. The current state of the English translation is available under a Creative Commons license (CC BY-SA) at https://members.loria.fr/PZimmermann/sagebook/english.html. A discussion is in process with an editor to publish a paper version.

7.8. Topics in Computational Number Theory Inspired by Peter L. Montgomery

Participants: Emmanuel Thomé, Paul Zimmermann.

Emmanuel Thomé and Paul Zimmermann contributed two chapters of the book "Topics in Computational Number Theory Inspired by Peter L. Montgomery", coordinated by Arjen Lenstra and Joppe Bos, and published by Cambridge University Press. Together with Richard P. Brent and Alexander Kruppa, Paul Zimmermann wrote a chapter entitled "FFT extension for algebraic-group factorization algorithms" [12]. Emmanuel Thomé contributed a chapter entitled "The block Lanczos algorithm" [14].

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

Participant: Svyatoslav Covanov.

In [17], we describe a method improving on the exhaustive search algorithm developed in [26]. 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 prove 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.

7.10. Big Prime Field FFT on the GPU

Participant: Svyatoslav Covanov.

In colloboration with L. Chen, D. Mohajerani and M. Moreno Maza, in [11], we compare various methods for the multiplication of polynomials, using the GPU. We compare the CRT method, using k machine-word primes, to the generalized Fermat prime method, for a prime of k machine-words, inspired by the work in [28]. For some degrees and k, we prove that the arithmetic operations with the generalized Fermat primes offer attractive performance both in terms of algebraic complexity and parallelism.

7.11. CM Plane Quartics

Participant: Hugo Labrande.

As a by-product of his PhD thesis defended in late 2016, Hugo Labrande contributed to a joint work with several authors, leading to an article [21] that provides examples of smooth plane quartics over $\mathbb{Q}$ with complex multiplication over $\overline{\mathbb{Q}}$ by a maximal order with primitive CM type. Several algorithms are used, in tight connection to the computation of Theta functions which was improved in Labrande's PhD thesis: reduction of period matrices, fast computation of Dixmier-Ohno invariants, and reconstruction from these invariants.

7.12. Explicit Isogenies in Genus 2 and 3

Participant: Enea Milio.

In [22], we present a quasi-linear algorithm to compute isogenies between Jacobians of curves of genus 2 and 3 starting from the equation of the curve and a maximal isotropic subgroup of the ℓ-torsion, for ℓ an odd prime number, generalizing Vélu's formula of genus 1. This work is based on the paper "Computing functions on Jacobians and their quotients" of Jean-Marc Couveignes and Tony Ezome. We improve their genus 2 case algorithm, generalize it for genus 3 hyperelliptic curves and introduce a way to deal with the genus 3 non-hyperelliptic case, using algebraic Theta functions.

7.13. Modular Polynomials of Hilbert Surfaces

Participant: Enea Milio.

In [23], together with Damien Robert from the LFANT team, we describe an evaluation/interpolation approach to compute modular polynomials on a Hilbert surface, which parametrizes abelian surfaces with maximal real multiplication. Under some heuristics we obtain a quasi-linear algorithm. The corresponding modular polynomials are much smaller than the ones on the Siegel threefold. We explain how to compute even smaller polynomials by using pullbacks of Theta functions to the Hilbert surface, and give an application to the CRT method to construct class polynomials.

7.14. Individual Logarithm Step in Non-prime Fields

Participant: Aurore Guillevic.

In [20], the previous work [33] on speeding-up the first phase of the individual discrete logarithm computation, the initial splitting, a.k.a. smoothing phase, is extended to any non-prime finite field $\mathbb{F}_{p^n}$ where n is composite. It is also applied to the new variant Tower-NFS.

7.15. Last Year Results that Appeared in 2017

Our work [6], in collaboration with J. Fried and N. Heninger from the University of Pennsylvania, describing a kilobit discrete logarithm computation for a trapdoored prime number has been published in Eurocrypt 2017.

A paper detailing the implementation of the ECM factoring algorithm on the Kalray MPPA-256 many-core processor, written as a collaboration between Jérémie Detrey and Pierrick Gaudry from CARAMBA, and Masahiro Ishii, Atsuo Inomata, and Kazutoshi Fujikawa from NAIST (Nara, Japan), was published in IEEE Transaction on Computers [2].

In [39], the notions of Square, saturation, integrals, multisets, bit patterns and tuples cryptanalysis are revised. A new Slice & Fuse paradigm to better exploit multiset type properties of block ciphers is proposed. With this refined analysis, we improve the best bounds proposed in such contexts against the following block ciphers: Threefish, Prince, Present and Rectangle.

In [3], we improve the existing impossible-differential attacks against Rijndael-160 and Rijndael-224.

Our work [10] about the computational power of the Measurement-based Quantum Computation model, written by Luc Sanselme and Simon Perdrix (from the CARTE team at LORIA), has appeared.

8. Bilateral Contracts and Grants with Industry

8.1. Training and Consulting with French Ministry of Defense

We have training and consulting activities with the French Ministry of Defense.

8.2. Consulting with Docapost

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

8.3. Consulting with Canton of Geneva

In this contract the goal is to audit and prove security properties of a new e-voting protocol to be used in a few cantons of Switzerland.

8.4. Research Contract with Orange

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.

8.5. FUI Industrial Partnership on Lightweight Cryptography

This contract, called PACLIDO, is an FUI project with many companies dedicated to the definition of new lightweight cryptographic primitives for the IoT.

9. Partnerships and Cooperations

9.1. National Initiatives

9.1.1. PEPS CHARIoT

The PEPS CHARIoT ("CHiffrement Authentifié pour Renforcer l'IoT") project is dedicated to the study of authenticated encryption schemes, especially the CAESAR candidates, and to the performance analysis of those schemes on dedicated embedded architectures such as micro-controllers (MSP430, ARM and AVR). It involves Marine Minier (CARAMBA), Franck Rousseau (IMAG - Grenoble) and Pascal Lafourcade (LIMOS-UCA - Clermont-Ferrand).

9.2. International Research Visitors

9.2.1. Visits of International Scientists

Thorsten Kleinjung from EPFL visited the team from 6 to 10 February to work on the Number Field Sieve algorithm.

10. Dissemination

10.1. Promoting Scientific Activities

10.1.1. Scientific Events Organisation

10.1.1.1. Member of the Organizing Committees

- Together with Anne-Lise Charbonnier (Inria Nancy – Grand Est), the Caramba team organized the "Journées Codage et Cryptographie 2017", whose objective is to regroup the French speaking community working on error-correcting codes and on cryptography. It is affiliated with the "Groupe de travail C2" of the GDR-IM.

10.1.2. Scientific Events Selection

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).
- Emmanuel Thomé is a member of the steering committee of the conference series "Algorithmic Number Theory Symposium" (ANTS).
- Emmanuel Thomé is a member of the scientific directorate of the Dagstuhl computer science seminar series.

10.1.2.2. Member of the Conference Program Committees

- Jérémie Detrey was a member of the Program Committee of ECC 2017.
- Pierrick Gaudry was a member of the Program Committee of EUROCRYPT 2017.
- Aurore Guillevic was a member of the Program Commitee of PKC 2018, Latincrypt 2017 and JC2 2017.
- Marine Minier was a member of the Program Commitee of WCC 2017 and JC2 2017.
- Pierre-Jean Spaenlehauer was a member of the Program Commitee of ISSAC 2017.

10.1.3. Journal

10.1.3.1. 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

- Jérémie Detrey was invited to give a talk at the Rencontres "Arithmétique de l'Informatique Mathématique" (RAIM 2017), Lyon, France.
- Aurore Guillevic was invited to give a talk at the Elliptic Curve Cryptography Conference (ECC17), Nijmegen, Netherlands.
- Emmanuel Thomé was invited to give a talk at the Elliptic Curve Cryptography Conference (ECC17), Nijmegen, Netherlands.
- Marine Minier was invited to give a talk at the Journées Nationales du pré-GDR Sécurité, Paris, France and at the CCA seminar, Paris, France.

10.1.5. Other committees

- Jérémie Detrey is chairing the *Commission des Utilisateurs des Moyens Informatiques* (CUMI) 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.
  - was a member of the hiring committee for the 2015 junior research positions (CR2) at Inria Bordeaux.
- Pierrick Gaudry is vice-head of the *Commission de mention Informatique* of the *École doctorale IAEM* of the University of Lorraine;
- Pierre-Jean Spaenlehauer is a member of the *Commission développement technologique* (CDT) of the Inria Nancy – Grand Est research center.
- 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, and chair of the organizing committee of the EJCIM (*École Jeunes Chercheurs Informatique Informatique Mathématique*) which will take place in Nancy in 2018.
- Marine Minier is
  - member of the CoS, poste MCF number 27MCF4376, Université de Rouen, November 2017.
  - member of the CoS, poste MCF number 27MCF575, Université de Grenoble Alpes, May 2017.
  - president of the CoS, poste MCF number 27MCF0955, Université de Lorraine, May 2017.
  - member of the CoS, poste MCF number 27MCF4191, Université de Lyon, May 2017.
  - member of the CoS, poste PR number 27PR0154, Université de Toulouse, May 2017.
  - in charge of the redaction for the LORIA of the Impact Project *Digital Trust*.

10.1.6. Research Administration

- Laurent Grémy was a member of the *Conseil de laboratoire* of the Loria.

10.2. Teaching - Supervision - Juries

10.2.1. Teaching

Master: Marine Minier, *Sécurité des systèmes d'information*, 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.

Master: Marine Minier, *Introduction à la sécurité des systèmes et à la cryptographie*, 32h eq. TD, M2 Mathématiques IMOI, Université de Lorraine, Faculté des sciences et technologies, Vandœuvre-les-Nancy, France.

Master: Emmanuel Thomé, *Introduction to Cryptography*, 24 hours (lectures + exercises), M1, Télécom Nancy, Villers-lès-Nancy, France.

Master: Emmanuel Thomé, *Cryptography and Security*, 20 hours (lectures + exercises), M2, Télécom Nancy and École des Mines de Nancy, France.

Master: Pierre-Jean Spaenlehauer, *Initiation aux méthodes analytiques de la théorie des nombres, applications à la cryptographie*, 15h eq. TD, M2 Mathématiques MFA, Université de Lorraine, Faculté des sciences et technologies, Vandœuvre-les-Nancy, France.

Licence: Jérémie Detrey, *Méthodologie*, 24 hours (practical sessions), L1, Université de Lorraine, Faculté des sciences et technologies, Vandœuvre-les-Nancy, France.

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

Master: Jérémie Detrey, *Introduction à la cryptographie*, 8 hours (lectures) + 10 hours (tutorial sessions) + 12 hours (practical sessions), Master Spécialisé, École des Mines de 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: Pierrick Gaudry, *Méthodologie*, 24 hours (practical sessions), L1, Université de Lorraine, Faculté des sciences et technologies, Vandœuvre-lès-Nancy, France.

2e année École Polytechnique, Aurore Guillevic, *Les bases de la programmation et de l'algorithmique*, (INF411), 32 hours (lab sessions), Palaiseau, France ("chargée d'enseignement").

10.2.2. Supervision

Internship: Léo Barré, *cube attacks and cube testers*, Université de Bordeaux, March–September (6 months), Pierre-Jean Spaenlehauer and Marine Minier.

Internship: Nicolas David, *Impact des racines réelles sur la sélection polynomiale pour le crible algébrique*, ENS Cachan, June–July (6 weeks), Paul Zimmermann.

Internship: Quentin Deschamps, *Étude de la sécurité du logarithme discret dans* $\mathrm{GF}(p^n)$ *lorsque* n *est composé*, ENS Lyon, July–August (6 weeks), Aurore Guillevic.

Internship: Joël Felderhoff, *infrastructures in complex cubic fields*, ENS-Lyon, June–July (6 weeks), Pierre-Jean Spaenlehauer.

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

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

Ph.D. in progress: Simon Abelard, *Comptage de points de courbes algébriques sur les corps finis et interactions avec les systèmes polynomiaux*, Univ. Lorraine; since Sep. 2015, Pierrick Gaudry & Pierre-Jean Spaenlehauer.

Ph.D. in progress: Svyatoslav Covanov, *Algorithmes de multiplication : complexité bilinéaire et méthodes asymptotiquement rapides*, since Sep. 2014, Jérémie Detrey et Emmanuel Thomé.

Ph.D. defended [1]: Laurent Grémy, *Sieve algorithms for the discrete logarithm in medium characteristic finite fields*, defended on September 29th, 2017, Pierrick Gaudry & Marion Videau.

10.2.3. Juries

Marine Minier: president of the jury of the PhD: *Synchronisation et systèmes dynamiques : application à la cryptographie* defended by Brandon Dravie, July 2017, Université de Lorraine.

Marine Minier: president of the jury of the PhD: *Réseaux de capteurs et vie privée* defended by Jessye Dos Santos, August 2017, Université de Grenoble Alpes.

Marine Minier: president of the jury of the PhD: *Système de détection d'intrusion adapté au système de communication aéronautique ACARS* defended by Eric Asselin, June 2017, Université de Toulouse.

Marine Minier: president of the jury of the PhD: *Probabilistic models of partial enforcement in distributed systems* defended by Jordi Martori-Adrian, June 2017, Université de Lorraine.

Marine Minier: president of the jury of the PhD: *Méthodes de calculs sur les données chiffrées* defended by Marie Paindavoine, January 2017, Université de Lyon.

Emmanuel Thomé: reviewer of the PhD thesis: *Formules de Thomae pour les courbes algébriques résolubles* defended by Alexandre Le Meur, August 2017, Université de Rennes 1.

Paul Zimmermann: member of the jury of the PhD thesis: *Investigations in Computer-Aider Mathematics: Experimentation, Computation, and Certification* defended by Thomas Sibut-Pinote, December 2017, École polytechnique.

10.3. Popularization

- Pierrick Gaudry organized and participated in a debate fed by excerpts from movies on the topic of cryptography and privacy in March 2017. He also gave a podcast interview about electronic voting for Interstices [15].
- Pierre-Jean Spaenlehauer did a short presentation of asymetric cryptography to middle school students who were award winners of the Alkindi competition.
- Paul Zimmermann co-animated a “Math-en-Jeans” atelier with lycée Vauban in Luxembourg city (Luxembourg).

11. Bibliography

Publications of the year

Doctoral Dissertations and Habilitation Theses

[1] L. GRÉMY. *Sieve algorithms for the discrete logarithm in medium characteristic finite fields*, Université de Lorraine, September 2017, https://tel.archives-ouvertes.fr/tel-01647623

Articles in International Peer-Reviewed Journals

[2] M. ISHII, J. DETREY, P. GAUDRY, A. INOMATA, K. FUJIKAWA. *Fast Modular Arithmetic on the Kalray MPPA-256 Processor for an Energy-Efficient Implementation of ECM*, in "IEEE Transactions on Computers", December 2017, vol. 66, n^{o} 12, pp. 2019-2030 [*DOI :* 10.1109/TC.2017.2704082], https://hal.inria.fr/hal-01299697

[3] M. MINIER. *Improving impossible-differential attacks against Rijndael-160 and Rijndael-224*, in "Designs, Codes and Cryptography", January 2017, vol. 82, n^{o} 1-2, pp. 117 - 129 [*DOI :* 10.1007/s10623-016-0206-7], https://hal.inria.fr/hal-01593371

[4] J.-P. ÉCHARD, P. GAUDRY. *An harmonious encoding of instrument values by a 19th century Parisian violin dealer*, in "Cryptologia", 2017, vol. 41, n^{o} 5, pp. 448-458 [*DOI :* 10.1080/01611194.2016.1257524], https://hal.inria.fr/hal-01393625

International Conferences with Proceedings

[5] M. ALAGGAN, M. CUNCHE, M. MINIER. *Non-interactive (t, n)-Incidence Counting from Differentially Private Indicator Vectors*, in "3rd International Workshop on Security and Privacy Analytics (IWSPA 2017)", Scottsdale, United States, March 2017, https://hal.inria.fr/hal-01485412

[6] J. FRIED, P. GAUDRY, N. HENINGER, E. THOMÉ. *A kilobit hidden SNFS discrete logarithm computation*, in "36th Annual International Conference on the Theory and Applications of Cryptographic Techniques - Eurocrypt 2017", Paris, France, J.-S. CORON, J. B. NIELSEN (editors), Advances in Cryptology – EUROCRYPT 2017, Springer, April 2017, vol. 10210, https://arxiv.org/abs/1610.02874 [*DOI :* 10.1007/978-3-319-56620-7_8], https://hal.inria.fr/hal-01376934

[7] D. GERAULT, M. MINIER, C. SOLNON. *Using Constraint Programming to solve a Cryptanalytic Problem*, in "IJCAI 2017 - International Joint Conference on Artificial Intelligence - Sister Conference Best Paper Track", Melbourne, Australia, August 2017, 5 p. , https://hal.archives-ouvertes.fr/hal-01528272

[8] L. GRÉMY, A. GUILLEVIC, F. MORAIN, E. THOMÉ. *Computing discrete logarithms in $GF(p^6)$*, in "24th Annual Conference on Selected Areas in Cryptography", Ottawa, Canada, August 2017, https://hal.inria.fr/hal-01624662

[9] V. LEFÈVRE, P. ZIMMERMANN. *Optimized Binary64 and Binary128 Arithmetic with GNU MPFR*, in "24th IEEE Symposium on Computer Arithmetic (ARITH 24)", London, United Kingdom, July 2017, https://hal.inria.fr/hal-01502326

[10] S. PERDRIX, L. SANSELME. *Determinism and Computational Power of Real Measurement-based Quantum Computation*, in "FCT'17- 21st International Symposium on Fundamentals of Computation Theory", Bordeaux, France, September 2017, https://arxiv.org/abs/1610.02824 [*DOI :* 10.1007/978-3-662-55751-8_31], https://hal.archives-ouvertes.fr/hal-01377339

Conferences without Proceedings

[11] L. CHEN, S. COVANOV, D. MOHAJERANI, M. MORENO MAZA. *Big Prime Field FFT on the GPU*, in "ISSAC 2017", Kaiserslautern, Germany, July 2017, https://hal.archives-ouvertes.fr/hal-01518830

Scientific Books (or Scientific Book chapters)

[12] R. P. BRENT, A. KRUPPA, P. ZIMMERMANN. *FFT extension for algebraic-group factorization algorithms*, in "Topics in Computational Number Theory Inspired by Peter L. Montgomery", J. W. BOS, A. K. LENSTRA (editors), Cambridge University Press, 2017, pp. 189-205, https://hal.inria.fr/hal-01630907

[13] 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, P. ZIMMERMANN. *Mathematical Computation with SageMath (temporary title)*, published by the authors, 2017, forthcoming, https://hal.inria.fr/hal-01646401

[14] E. THOMÉ. *A modified block Lanczos algorithm with fewer vectors*, in "Topics in Computational Number Theory inspired by Peter L. Montgomery", Cambridge University Press, 2017, https://arxiv.org/abs/1604.02277 [*DOI :* 10.1017/9781316271575.008], https://hal.inria.fr/hal-01293351

Scientific Popularization

[15] P. GAUDRY, J. JONGWANE. *À propos du vote par Internet*, in "Interstices", March 2017, https://hal.inria.fr/hal-01533682

Other Publications

[16] S. ABELARD, P. GAUDRY, P.-J. SPAENLEHAUER. *Improved Complexity Bounds for Counting Points on Hyperelliptic Curves*, October 2017, working paper or preprint, https://hal.inria.fr/hal-01613530

[17] S. COVANOV. *Improved method for finding optimal formulae for bilinear maps in a finite field*, November 2017, working paper or preprint, https://hal.inria.fr/hal-01519408

[18] P. GAUDRY. *Some ZK security proofs for Belenios*, 2017, working paper or preprint, https://hal.inria.fr/hal-01576379

[19] L. GRÉMY, A. GUILLEVIC, F. MORAIN. *Breaking DLP in $GF(p^5)$ using 3-dimensional sieving*, July 2017, working paper or preprint, https://hal.inria.fr/hal-01568373

[20] A. GUILLEVIC. *Faster individual discrete logarithms with the QPA and NFS variants*, August 2017, working paper or preprint, https://hal.inria.fr/hal-01341849

[21] P. KILICER, H. LABRANDE, R. LERCIER, C. RITZENTHALER, J. SIJSLING, M. STRENG. *Plane quartics over Q with complex multiplication*, 2017, https://arxiv.org/abs/1701.06489 - 34 pages, https://hal.archives-ouvertes.fr/hal-01455036

[22] E. MILIO. *Computing isogenies between Jacobian of curves of genus 2 and 3*, September 2017, working paper or preprint, https://hal.archives-ouvertes.fr/hal-01589683

[23] E. MILIO, D. ROBERT. *Modular polynomials on Hilbert surfaces*, September 2017, working paper or preprint, https://hal.archives-ouvertes.fr/hal-01520262

References in notes

[24] 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

[25] 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

[26] 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. RODRÍGUEZ-HENRÍQUEZ (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

[27] 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

[28] S. COVANOV, E. THOMÉ. *Fast integer multiplication using generalized Fermat primes*, January 2016, working paper or preprint, https://hal.inria.fr/hal-01108166

[29] 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

[30] 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

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

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

[33] 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

[34] 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

[35] 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

[36] 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

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

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

[39] M. MINIER, R. C.-W. PHAN. *Tuple Cryptanalysis: Slicing and Fusing Multisets*, in "Paradigms in Cryptology – Mycrypt 2016", Kuala Lumpur, Malaysia, R. C.-W. PHAN, M. YUNG (editors), Lecture Notes in Computer Science, Springer, December 2016, vol. 10311, pp. 294-320 [*DOI :* 10.1007/978-3-319-61273-7], https://hal.inria.fr/hal-01593382

[40] 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

[41] NATIONAL SECURITY AGENCY. *Cryptography Today*, 2015, https://www.nsa.gov/ia/programs/suiteb_cryptography/index.shtml