IN PARTNERSHIP WITH:
CNRS

Université de Lorraine

Activity Report 2016

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:

1.1.2. - Hardware accelerators (GPGPU, FPGA, etc.)
4.3.1. - Public key cryptography
4.3.2. - Secret key cryptography
4.8. - Privacy-enhancing technologies
6.2.7. - High performance computing
7.1. - Parallel and distributed algorithms
7.6. - Computer Algebra
7.7. - Number theory
7.12. - Computer arithmetic

Other Research Topics and Application Domains:

8.5. - Smart society
9.4.1. - Computer science
9.4.2. - Mathematics
9.8. - Privacy

1. Members

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]

PhD Students

Simon Abelard [Univ. Lorraine]
Svyatoslav Covanov [Univ. Lorraine]
Laurent Grémy [Univ. Lorraine]
Hugo Labrande [Univ. Lorraine, until Aug 2016]

Post-Doctoral Fellows

Enea Milio [Inria, from April 2016]
Shashank Singh [Inria, from Oct 2016]

Administrative Assistants

Virginie Priester [CNRS, from Apr 2016]
Sophie Drouot [Inria]
Laurence Félicité [Univ. Lorraine]

Others

Robin Fedele [Inria, Internship, from May 2016 until Jun 2016]
Nicolas Levy [ENS Lyon, intern, from Jun 2016 until Jul 2016]
Joshua Peignier [ENS Rennes, intern, from May 2016 until Jul 2016]
Luc Sanselme [Min. de l'Éducation Nationale, Teacher]
Élise Tasso [Univ. Lorraine, intern, from Sep 2016 until Jun 2016]

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.

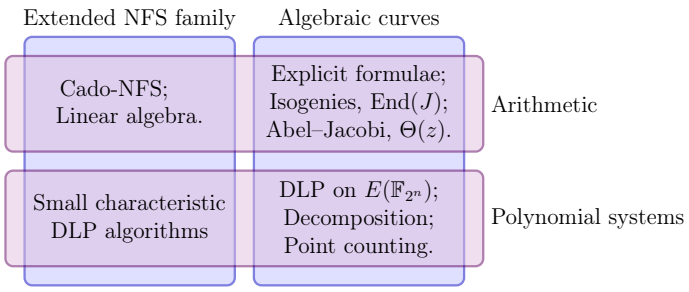

Figure 1. Visual representation of the thematic organization of CARAMBA.

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 the industry [36], [23].

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 to 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 [24], [31], [30], [29]. A stream of computational records have been obtained since 2013 using 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 of course 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 [34]. 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 [28].

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 [37] (for a glimpse of some of the reactions within the academic community, the reference [33] 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 [22].

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 workplan 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 [34].

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 advances 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. 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 [27], [26].

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 6.3, 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.
- Recent hirings (Minier) are likely to lead the team to study particular polynomial systems in context which are more 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 [27], [26]. 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 [22] are understood as being serious concerns thanks to our convincing proof-of-concepts. In the LogJam context, this impact has led to rapid worldwide security advisories and software updates that eventually defeat some potential intelligence threats and improve confidentiality of communications.

[1] In [23], the minimal recommended RSA key size is 2048 bits for an usage up to 2030. See also Annex B, in particular Section B.1 "Records de calculs cryptographiques".

[2] The work [32] is one of the only two academic works cited by NIST in the initial version (2011) of the report [36].

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 project-team was created on January 1st, 2016!

In October 2016, Pierrick Gaudry and Emmanuel Thomé, together with colleagues from the University of Pennsylvania (USA), have performed a discrete logarithm computation of a 1024-bit trapdoored prime [18].

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 verifiability relies on the fact that the ballot box is public (voters can check that their ballots have been taken into account) 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.

In 2016 our online platform has been used for several elections, for instance: representatives at the "comité de centre" in several Inria research centers, at the "conseil de laboratoire" at IRISA, and for the head of the "GT Calcul Formel" of the GDR-IM.

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

6.2. Kalray-ECM

KEYWORDS: Factorization - Kalray
FUNCTIONAL DESCRIPTION

Implementation of the factorization algorithm based on elliptic curves (ECM) for the MPPA-256 Kalray processor.

- Authors: Jérémie Detrey, Pierrick Gaudry and Masahiro Ishii
- Partner: Nara Institute of Science and Technology, Japan
- Contact: Jérémie Detrey
- URL: https://gforge.inria.fr/projects/kalray-ecm

6.3. TinyGB

- Author: Pierre-Jean Spaenlehauer
- Contact: Pierre-Jean Spaenlehauer
- URL: https://gforge.inria.fr/projects/tinygb/
- Licence: LGPL-3.0+

`TinyGB` is a software implementing tools for computing Gröbner bases of ideals in polynomial rings over finite fields. It has been released in April 2016.

It is not competitive with state-of-art software for computations over small prime fields. However, for polynomial systems over $\mathbb{Z}/p\mathbb{Z}$, with $p > 2^{31}$, its timings are competitive with the computer algebra system `Magma-2.22-2` (although the `Magma` is much better in terms of memory requirements). This is due to the fact that `TinyGB` relies on the library `MPFQ` (developed in the Caramba team) for the efficient arithmetic over large prime fields. For instance, computing the grevlex Gröbner basis of a system of 13 dense homogeneous quadratic equations in 13 variables over the field $\mathbb{Z}/(2^{31}+11)\mathbb{Z}$ can be achieved within 907 seconds with `TinyGB`, whereas `Magma-2.22-2` requires 4459 seconds (on an Intel Core i5-4590@3.30GHz).

The distribution of `TinyGB` contains the libraries `OpenBLAS`, `FFLAS-FFPACK` and `MPFQ`.

7. New Results

7.1. Collecting Relation for the Number Field Sieve in Medium Characteristic

Participants: Pierrick Gaudry, Laurent Grémy [contact], Marion Videau.

We study the relation collection of NFS in medium characteristic, especially in $\mathrm{GF}(p^6)$ [4]. We compare different polynomial selections that affect drastically the relation collection step, by giving the explicit formula in 3 dimensions of two functions to select the best polynomials. For the relation collection, we design new sieve algorithms in 3 dimensions and do the practical comparison of the different polynomial selections for different p. Finally, we perform the relation collection step for a field of 389 bits in 800 days, the largest computed relation collection in this type of field.

7.2. Recent Progress on the Elliptic Curve Discrete Logarithm Problem

Participant: Pierrick Gaudry [contact].

A survey on the elliptic curve discrete logarithm problem has been written in collaboration with S. Galbraith (Auckland). It appeared in a special issue of DCC [3], for the 25th birthday of the journal.

7.3. A Modified Block Lanczos Algorithm with Fewer Vectors

Participant: Emmanuel Thomé [contact].

In the context of a book project entitled "Topics in Computational Number Theory inspired by Peter L. Montgomery" (edited by Joppe W. Bos and Arjen K. Lenstra), E. Thomé contributed a chapter on "the Block Lanczos algorithm" (owed to Peter L. Montgomery [35]). This was the occasion to rework and streamline the presentation of the block Lanczos algorithm. In fact, several new characteristics of the algorithm were obtained in this process: a version adapted to homogeneous systems, an improvement on the memory footprint of the algorithm, and a heuristic justification for the success probability of the algorithm. While the collated book is still not published yet (publication is expected in 2017), the chapter is published in preprint form as [14].

7.4. Factorization of RSA-220 with CADO-NFS

Participants: Pierrick Gaudry, Emmanuel Thomé, Paul Zimmermann [contact].

In May 2016 we have completed with CADO-NFS the factorization of RSA-220 [15], which was started in December 2013. The sieving was completed in September 2014, and the first phase of the linear algebra (`krylov`) in October 2014. However we had to improve CADO-NFS to be able to run the `lingen` sub-step of the linear algebra. This was completed in January 2016, and the end of the factorization ran smoothly. This factorization is the largest one done with CADO-NFS, and the third largest one overall, after RSA-768 (232 digits) factored in December 2009, and $3^{697}+1$ (221 digits) factored by NFS@Home in February 2015.

7.5. Linear Time Interactive Certificates for the Minimal Polynomial and the Determinant of a Sparse Matrix

Participant: Emmanuel Thomé [contact].

Following discussion with Jean-Guillaume Dumas which began in March 2015 on the topic of computing checkpoints for the `krylov` step of the block Wiedemann algorithm, we determined that a scheme very similar to this checkpointing technique (originally designed to spot data corruption errors) was able to provide a proving algorithm —in the cryptographic sense— for the computation of the minimal polynomial of a sparse matrix, or for its determinant. This led to a joint paper with Jean-Guillaume Dumas, Erich Kaltofen and Gilles Villard, published at ISSAC 2016 [8].

7.6. A Kilobit Hidden SNFS Discrete Logarithm Computation

Participants: Pierrick Gaudry, Emmanuel Thomé [contact].

In collaboration with Josh Fried and Nadia Heninger from University of Pennsylvania, we worked on discrete logarithm computation modulo primes of a special form, amenable to computation with the Special Number Field Sieve (SNFS). Our original interest in this question came from the observation that primes which are conspicuous SNFS targets *are* found in the wild, as we observed in the context of the LogJam attack in 2015. We first ran a test computation on such a prime in March ($p = 2^{784} - 2^{28} + 1027679$, found in the LibTomcrypt library. For modern cryptographic uses, such a prime qualifies undoubtedly as "not good'). Based on the computational data obtained, and on further work, we expanded to larger sizes. We crafted a prime which was chosen as a "best case" for SNFS, yet with the property that this SNFS-optimality cannot be detected. We call such primes "trapdoored primes". We showed that computing discrete logarithms modulo trapdoored primes is entirely feasible for 1024-bit primes. In the article [18], we also showed that there are primes which are found in the wild (e.g., in RFC 5114) which could plausibly be trapdoored primes, given that no justification of their origin is provided. In fact, while cryptographic best practice is to provide "rigid" choices whenever random choices are to be set publicly, the sad truth is that random data lacking a justification is found quite often.

In the context of [18], we also put into practice an improvement of the implementation of the block Wiedemann algorithm in Cado-NFS, that allowed to reduce the time for the linear algebra computation significantly.

7.7. Solving Discrete Logarithms on a 170-bit MNT Curve by Pairing Reduction

Participants: Aurore Guillevic [contact], Emmanuel Thomé [contact].

The project of computing discrete logarithms in finite fields of the form $\mathrm{GF}(p^n)$ for small n comes from the need to estimate precisely the security level of pairing-based cryptography. After the two record computations of 2014 and 2015 in $\mathrm{GF}(p^2)$ of 160 and 180 decimal digits (532 and 597 bits) we investigated $\mathrm{GF}(p^3)$ and took a real-life elliptic curve proposed in 2001 by Miyaji, Nakabayashi and Takano (MNT-3 curve). Thanks to a pairing computation (in few milliseconds), a discrete logarithm computation in the 170-bit MNT-3 curve, which is hard, can be done instead by a discrete logarithm computation in $\mathrm{GF}(p^3)$ of 508 bits, which is much faster. This computation involved Aurore Guillevic (post-doctoral fellow in 2016 at the University of Calgary, Canada), Emmanuel Thomé, and François Morain (LIX/École Polytechnique/Inria Saclay, GRACE team). The computation took 2.97 years in total: 1.81 years for the relation collection, 1.16 years for the linear algebra and 2 days for the individual discrete logarithm computation. The work was presented at the Selected Areas in Cryptography conference in Newfoundland, Canada, and published in the proceedings [11].

The next step will be to adapt the new NFS variant called Extended-Tower-NFS to attack MNT-4 and MNT-6 curves, which means computing discrete logarithms in $\mathrm{GF}(p^4)$ and $\mathrm{GF}(p^6)$. This new challenge will require the higher dimension sieve developed by Laurent Grémy.

7.8. Computing Jacobi's Theta in Quasi-linear Time

Participant: Hugo Labrande [contact].

Most of the results have been obtained in 2015. The article was accepted for publication in 2016 [5].

We study the multiprecision computation of the theta function in genus 1, *i.e.,* the Jacobi theta function. The main result is that $\theta(z, \tau)$ can be computed in time that is quasi-linear in the precision P, using an algorithm which follows the same strategy as the case of theta-constants (Dupont, 2006). A thorough analysis of the precision loss is given in order to prove correctness.

Along with this work, we have publicly released an open source implementation of the algorithm in C (using the GNU MPC library). This implementation shows this algorithm is faster than a more naive approach for precisions greater than 300,000 digits.

7.9. Computing Theta Functions in Quasi-linear Time in Genus 2 and Above

Participants: Hugo Labrande, Emmanuel Thomé [contact].

We study the multiprecision computation of the theta function in genus 2. We extend the quasi-linear algorithm for Jacobi's theta to genus 2, generalizing the approach we undertook in previous work; this required finding workarounds, most notably for the choice of signs and for being able to apply Newton's method. We also give an outline of an algorithm for the theta function in genus g, but the workarounds we found in genus 2 would need to be generalized to this case before claiming any sort of result in genus g [6].

We released along with this work a Magma implementation of our fast genus 2 algorithm, along with an implementation of a somewhat naive (but previously state-of-the-art) algorithm for genus 2. Our results show that our algorithm is faster than the naive one for precisions greater than 3,000 digits.

7.10. Computing Small Certificates of Inconsistency of Quadratic Fewnomial Systems

Participant: Pierre-Jean Spaenlehauer [contact].

This is a joint work with Jean-Charles Faugère (Inria, EPI Polsys) and Jules Svartz (Inria EPI Polsys/Ministère Éducation Nationale). Most of the results have been obtained in 2015. This work was finalized and published in 2016 [10].

We study how Gröbner bases algorithms can be adapted to compute certificates that *quadratic fewnomial systems* (*i.e.*, systems in which only a small subset of monomials occur in the equations) do not have any solution. The main results are algorithms and complexity bounds which take into account the sparsity of the monomial support of the system, under some mild genericity assumptions on the coefficients of the systems.

7.11. Critical Point Computations on Smooth Varieties: Degree and Complexity Bounds

Participant: Pierre-Jean Spaenlehauer [contact].

This is a joint work with Mohab Safey El Din (Univ. Paris 6, EPI Polsys). This work led to a publication in the proceedings of the ISSAC conference [13].

Let $V \subset \mathbb{C}^n$ be an equidimensional algebraic set and g be an n-variate polynomial with rational coefficients. Computing the critical points of the map that evaluates g at the points of V is a cornerstone of several algorithms in real algebraic geometry and optimization. Under the assumption that the critical locus is finite and that the projective closure of V is smooth, we provide sharp upper bounds on the degree of the critical locus which depend only on $\deg(g)$ and the degrees of the generic polar varieties associated to V. Using these degree bounds and an algorithm due to Bank, Giusti, Heintz, Lecerf, Matera and Solernó, we derive complexity bounds which are quadratic in the degree bounds (up to logarithmic factors) and polynomial in all the other parameters of the problem.

7.12. Constructing Sparse Polynomial Systems with Many Positive Solutions

Participant: Pierre-Jean Spaenlehauer [contact].

This is a joint work with Frédéric Bihan (Univ. de Savoie, LAMA). Most of the results have been obtained in 2015 [25]; we improved the results during 2016.

Consider a regular triangulation of the convex-hull P of a set $\mathcal{A}$ of n points in $\mathbb{R}^d$, and a real matrix C of size $d \times n$. A version of Viro's method allows to construct from these data an unmixed polynomial system with support $\mathcal{A}$ and coefficient matrix C whose number of positive solutions is bounded from below by the number of d-simplices which are positively decorated by C (a d-simplex is positively decorated by C if the $d \times (d+1)$ sub-matrix of C corresponding to the simplex has a kernel vector all coefficients of which are positive). We show that all the d-simplices of a triangulation can be positively decorated if and only if the triangulation is balanced, which in turn is equivalent to the fact that its dual graph is bipartite. This allows us to identify, among classical families, monomial supports which admit maximally positive systems, giving some evidence in favor of a conjecture due to Bihan. We also use this technique in order to construct fewnomial systems with many positive solutions.

7.13. Modular Arithmetic and ECM on the Kalray MPPA-256 Processor

Participants: Jérémie Detrey [contact], Pierrick Gaudry.

In collaboration with Masahiro Ishii from the Nara Institute of Science and Technology, Nara (Japan) we have developed a fast modular arithmetic library for the Kalray MPPA-256, which is a many-core processor with a VLIW architecture. Carefully written assembly allowed us to obtain a close to optimal use of the computing units of all the cores for the multiprecision multiplication of integers. As an application, the ECM factoring algorithm was implemented on top of our library. The performances are very interesting compared to other architectures like GPU, especially in terms of power consumption [19].

7.14. Determinism and Computational Power of Real Measurement-based Quantum Computation

Participant: Luc Sanselme [contact].

This is a joint work with Simon Perdrix (CNRS, Carte Team at Loria). This work has begun in 2014.

The starting point for this work was about a problem in «Quantum cloud computing». A person with a classical resource wants to perform a quantum computation. To do so he asks some quantum resources to perform his computation. The difficult part is that he wants to be sure that the quantum resources he asks to perform his computation don't cheat and return him the good results. This kind of «Quantum cloud computing» is called interactive proofs. The quantum resources are called the provers. Real Measurement-based quantum computing (MBQC) has been used for interactive proofs by McKague.

Measurement-based quantum computing (MBQC) is a universal model for quantum computation. The combinatorial characterization of determinism in this model, powered by measurements, and hence, fundamentally probabilistic, is the cornerstone of most of the breakthrough results in this field. To answer our question, we needed to develop some tools in this MBQC field. The most general known sufficient condition for a deterministic MBQC to be driven is that the underlying graph of the computation has a particular kind of flow called Pauli flow. The necessity of the Pauli flow was an open question. We showed that the Pauli flow is necessary for real-MBQC, and not in general providing counter-examples for (complex) MBQC. We explored the consequences of this result for real MBQC and its applications. Real MBQC and more generally real quantum computing is known to be universal for quantum computing. In the interactive proofs developed by McKague, the two-prover case corresponds to real-MBQC on bipartite graphs. While (complex) MBQC on bipartite graphs are universal, the universality of real MBQC on bipartite graphs was an open question. We showed that real bipartite MBQC is not universal: we proved that all measurements of real bipartite MBQC can be parallelized. Therefore, real bipartite MBQC leads to constant depth computations. As a consequence, McKague techniques cannot lead to two-prover interactive proofs.

7.15. Fast Integer Multiplication Using Generalized Fermat Primes

Participants: Svyatoslav Covanov [contact], Emmanuel Thomé.

The paper [17] describes 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 give evidence in favor of this assumption. This article has been submitted to Mathematics of Computation and some corrections, that have been requested, are processed currently.

7.16. Search for Primitive Trinomials

Participant: Paul Zimmermann [contact].

This is a joint work with Richard Brent (University of Newcastle, Australia).

We have performed a search for primitive trinomials $x^r + x^s + 1$ over $\mathrm{GF}(2)$ of degree $r = 42\,643\,801$, $r = 43\,112\,609$, $r = 57\,885\,161$ and $r = 74\,207\,281$, which are the new Mersenne prime exponents found by the GIMPS project. We found respectively 5, 4, 0 and 3 primitive trinomials [16], for example the three primitive trinomials of degree $74\,207\,281$ are (with their reverse trinomials):

$$x^{74207281} + x^{9156813} + 1, \qquad x^{74207281} + x^{9999621} + 1, \qquad x^{74207281} + x^{30684570} + 1.$$

8. Bilateral Contracts and Grants with Industry

8.1. Training and Consulting with HTCS

The training and consulting activities begun in 2012 with the HTCS company have been pursued, and the existing contract has been renewed in identical form.

9. Partnerships and Cooperations

9.1. National Initiatives

9.1.1. PEPS JCJC INS2I SPICE

The SPICE proposal ("Systèmes Polynomiaux et calcul d'Indice sur les Courbes Elliptiques : indicateurs de complexité en petite caractéristique") has been accepted in the PEPS JCJC INS2I program in 2016. It involves Pierre-Jean Spaenlehauer (CARAMBA) and Vanessa Vitse (Université Joseph Fourier). This project is coordinated by Vanessa Vitse.

10. Dissemination

10.1. Promoting Scientific Activities

10.1.1. Scientific Events Organization

10.1.1.1. Member of the Organizing Committees

- Together with Anne-Lise Charbonnier (Inria Nancy – Grand Est), the Caramba team is organizing 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).

10.1.2.2. Member of the Conference Program Committees

- Emmanuel Thomé was a member of the program committee of the 35th Annual International Conference on the Theory and Applications of Cryptographic Techniques (Eurocrypt 2016).
- Marine Minier was a member of the Program Committee of the conference MyCrypt 2016.
- Pierrick Gaudry was a member of the Program Committee of the conference Selected Areas in Cryptography SAC 2016 and of EUROCRYPT 2017.

- Paul Zimmermann was a member of the Program Committee of the International Workshop on the Arithmetic of Finite Fields (WAIFI 2016).

10.1.3. Journal

10.1.3.1. Member of the Editorial Boards

- Pierrick Gaudry is a member of the editorial board of the journal Applicable Algebra in Engineering, Communication and Computing.

10.1.3.2. Reviewer - Reviewing Activities

Members of the project-team did 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 as a Distinguished Lecturer for the Computer and Information Security Seminar at the University of Pennsylvania in November 2016.
- Pierrick Gaudry was invited speaker at the YACC 2016 conference in Porquerolles, at the workshop "Mathematical Structures for Cryptography" in Leiden (Netherlands), and at the "Journées Aléa 2016" in Marseille.

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).
  - the *Comité Local Hygiène, Sécurité, et Conditions de Travail* 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;
- 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*, and was member until August of the Inria Evaluation Board and the CoSI (*Commission Scientifique*).

10.1.6. Research Administration

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

10.2. Teaching - Supervision - Juries

10.2.1. Teaching

Master: Jérémie Detrey, *Sécurité des systèmes d'information*, 6 hours (practical sessions), M2 Informatique, Université de Lorraine, Faculté des sciences et technologies, Vandœuvre-les-Nancy, France.

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

Master: Pierre-Jean Spaenlehauer, *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*, 12 hours (lectures), 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.

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.

Jérémie Detrey, *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*, 48 hours (practical sessions), L1, Université de Lorraine, Faculté des sciences et technologies, Vandœuvre-lès-Nancy, France.

10.2.2. Supervision

Internship: Nicolas Levy, *Algorithmes de factorisation d'entiers basés sur la structure des corps quadratiques réels*, L3 ÉNS Lyon, June-July, Pierre-Jean Spaenlehauer.

Internship: Joshua Peigner, *Factorisation d'idéaux pour l'implantation du crible algébrique*, ÉNS Rennes, June-July, Emmanuel Thomé.

Internship: Robin Fedele, *Consolidation de la couche Python de CADO-NFS*, Univ. Lorraine, May-June, Paul Zimmermann.

Internship: Élise Tasso, *Étude comparative de divers algorithmes de friabilisation*, Mines Nancy, October-June (1 day each week), Pierrick Gaudry.

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. in progress: Laurent Grémy, *Analyse et optimisation d'algorithmes de cribles arithmétiques*, since Oct. 2013, Pierrick Gaudry & Marion Videau.

Ph.D. defended: Hugo Labrande, *Explicit computation of the Abel-Jacobi map and its inverse* [1], defended on November 14th, 2016.

10.2.3. Juries

Marine Minier: reviewer of the PhD *Implantation sécurisée de protocoles cryptographiques basés sur les codes correcteurs d'erreurs* by Tania Richmont defended at Univ. Jean Monnet Saint-Etienne, October 24th, 2016.

Pierrick Gaudry: reviewer of the PhD *Computational Aspects of Jacobians of Hyperelliptic Curves* by Alina Dudeanu defended at EPFL, Switzerland; member of the jury for the PhD of Florent Ulpat Rovetta (Marseille) and of Hugo Labrande (Nancy).

Emmanuel Thomé: reviewer (and president of jury) of the Habilitation Thesis *Contributions à la Résolution Algébrique et Applications en Cryptologie* by Guénaël Renault, defended at University Pierre et Marie Curie, December 8th, 2016.

Emmanuel Thomé: jury member (advisor) for the PhD of Hugo Labrande (see above).

10.3. Popularization

- Laurent Grémy and Pierre-Jean Spaenlehauer have animated a stand in the "Village des Sciences du Loria" in March 2016.
- Laurent Grémy and Pierre-Jean Spaenlehauer have animated a stand during the celebration of the Loria's 40 years anniversary in June 2016.

- Pierrick Gaudry organized and participated to a debate fed by excerpts from movies on the topic of cryptography and privacy in October 2016.

11. Bibliography

Publications of the year

Doctoral Dissertations and Habilitation Theses

[1] H. LABRANDE. *Explicit computation of the Abel-Jacobi map and its inverse*, Université de Lorraine ; University of Calgary, November 2016, https://tel.archives-ouvertes.fr/tel-01403849

Articles in International Peer-Reviewed Journals

[2] C. CHEN, S. COVANOV, F. MANSOURI, R. H. C. MOIR, M. MORENO MAZA, N. XIE, Y. XIE. *The Basic Polynomial Algebra Subprograms*, in "ACM Communications in Computer Algebra", November 2016 [*DOI :* 10.1145/3015306.3015312], https://hal.archives-ouvertes.fr/hal-01404718

[3] S. GALBRAITH, P. GAUDRY. *Recent progress on the elliptic curve discrete logarithm problem*, in "Designs, Codes and Cryptography", 2016, vol. 78, n^{o} 1, pp. 51-72 [*DOI :* 10.1007/s10623-015-0146-7], https://hal.inria.fr/hal-01215623

[4] P. GAUDRY, L. GRÉMY, M. VIDEAU. *Collecting relations for the number field sieve in $GF(p^6)$*, in "LMS Journal of Computation and Mathematics", 2016, vol. 19, pp. 332 - 350 [*DOI :* 10.1112/S1461157016000164], https://hal.inria.fr/hal-01273045

[5] H. LABRANDE. *Computing Jacobi's θ in quasi-linear time*, in "Mathematics of Computation", November 2016, https://hal.inria.fr/hal-01227699

[6] H. LABRANDE, E. THOMÉ. *Computing theta functions in quasi-linear time in genus 2 and above*, in "LMS Journal of Computation and Mathematics", August 2016, vol. 19, n^{o} A, pp. 163-177 [*DOI :* 10.1112/S1461157016000309], https://hal.inria.fr/hal-01277169

[7] J.-P. ÉCHARD, P. GAUDRY. *An harmonious encoding of instrument values by a 19th century Parisian violin dealer*, in "Cryptologia", 2016, À paraître, forthcoming, https://hal.inria.fr/hal-01393625

International Conferences with Proceedings

[8] J.-G. DUMAS, E. KALTOFEN, E. THOMÉ, G. VILLARD. *Linear Time Interactive Certificates for the Minimal Polynomial and the Determinant of a Sparse Matrix*, in "International Symposium on Symbolic and Algebraic Computation", Waterloo, Canada, X.-S. GAO (editor), ISSAC'2016, Proceedings of the 2016 ACM International Symposium on Symbolic and Algebraic Computation, ACM, July 2016, https://hal.archives-ouvertes.fr/hal-01266041

[9] N. EYROLLES, L. GOUBIN, M. VIDEAU. *Defeating MBA-based Obfuscation*, in "2nd International Workshop on Software PROtection", Vienna, Austria, ACM (editor), October 2016 [*DOI :* 10.1145/2995306.2995308], https://hal.archives-ouvertes.fr/hal-01388109

[10] J.-C. FAUGÈRE, P.-J. SPAENLEHAUER, J. SVARTZ. *Computing Small Certificates of Inconsistency of Quadratic Fewnomial Systems*, in "International Symposium on Symbolic and Algebraic Computation (ISSAC 2016)", Waterloo, Canada, ACM, July 2016, pp. 223-230 [*DOI :* 10.1145/2930889.2930927], https://hal.inria.fr/hal-01314651

[11] A. GUILLEVIC, F. MORAIN, E. THOMÉ. *Solving discrete logarithms on a 170-bit MNT curve by pairing reduction*, in "Selected Areas in Cryptography 2016", St. John's, Canada, R. AVANZI, H. HEYS (editors), Selected Areas in Cryptography 2016, Springer, August 2016, to appear in the Lecture Notes in Computer Science (LNCS), https://hal.inria.fr/hal-01320496

[12] A. GUINET, N. EYROLLES, M. VIDEAU. *Arybo: Manipulation, Canonicalization and Identification of Mixed Boolean-Arithmetic Symbolic Expressions*, in "GreHack 2016", Grenoble, France, Proceedings of GreHack 2016, November 2016, https://hal.archives-ouvertes.fr/hal-01390528

[13] M. SAFEY EL DIN, P.-J. SPAENLEHAUER. *Critical Point Computations on Smooth Varieties: Degree and Complexity bounds*, in "International Symposium on Symbolic and Algebraic Computation (ISSAC)", Waterloo, Canada, July 2016, pp. 183–190 [*DOI :* 10.1145/2930889.2930929], https://hal.inria.fr/hal-01312750

Scientific Books (or Scientific Book chapters)

[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, 2016, https://hal.inria.fr/hal-01293351

Other Publications

[15] S. BAI, P. GAUDRY, A. KRUPPA, E. THOMÉ, P. ZIMMERMANN. *Factorisation of RSA-220 with CADO-NFS*, May 2016, working paper or preprint, https://hal.inria.fr/hal-01315738

[16] R. P. BRENT, P. ZIMMERMANN. *Twelve new primitive binary trinomials*, October 2016, working paper or preprint, https://hal.inria.fr/hal-01378493

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

[18] J. FRIED, P. GAUDRY, N. HENINGER, E. THOMÉ. *A kilobit hidden SNFS discrete logarithm computation*, September 2016, working paper or preprint, https://hal.inria.fr/hal-01376934

[19] 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*, April 2016, working paper or preprint, https://hal.inria.fr/hal-01299697

[20] S. PERDRIX, L. SANSELME. *Determinism and Computational Power of Real Measurement-based Quantum Computation*, October 2016, working paper or preprint, https://hal.archives-ouvertes.fr/hal-01377339

[21] P. ZIMMERMANN, F. BASTIEN. *Paul Zimmermann - CADO-NFS: Atelier PARI/GP 2016*, January 2016, https://hal.archives-ouvertes.fr/medihal-01346718

References in notes

[22] 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

[23] 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

[24] 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

[25] F. BIHAN, P.-J. SPAENLEHAUER. *Sparse polynomial systems with many positive solutions from bipartite simplicial complexes*, 2015, arXiv preprint arXiv:1510.05622

[26] 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

[27] 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

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

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

[30] 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

[31] 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

[32] T. KLEINJUNG, K. AOKI, J. FRANKE, A. K. LENSTRA, E. THOMÉ, J. BOS, P. GAUDRY, A. KRUPPA, P. L. MONTGOMERY, D. A. OSVIK, H. TE RIELE, A. TIMOFEEV, 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

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

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

[35] P. L. MONTGOMERY. *A block Lanczos algorithm for finding dependencies over* $\mathrm{GF}(2)$, in "EUROCRYPT '95", L. C. GUILLOU, J.-J. QUISQUATER (editors), Lecture Notes in Comput. Sci., 1995, vol. 921, pp. 106–120, Proceedings

[36] 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

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