
IN PARTNERSHIP WITH:
**CNRS**

**Université de Lorraine**

Activity Report 2015

# Project-Team CARAMEL

## Cryptology, Arithmetic: Hardware and Software

IN COLLABORATION WITH: Laboratoire lorrain de recherche en informatique et ses applications (LORIA)

RESEARCH CENTER
**Nancy - Grand Est**

THEME
**Algorithmics, Computer Algebra and Cryptology**

# Table of contents

# Project-Team CARAMEL

*Creation of the Team: 2010 January 01, updated into Project-Team: 2011 January 01, end of the Project-Team: 2015 December 31*

**Keywords:**

**Computer Science and Digital Science:**

4.3.1. - Public key cryptography
6.2.7. - High performance computing
7.12. - Computer arithmetic
7.6. - Computer Algebra

**Other Research Topics and Application Domains:**

6.3. - Network functions
9.4.1. - Computer science
9.4.2. - Mathematics
9.8. - Privacy

# 1. Members

**Research Scientists**

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

**Faculty Member**

Marion Videau [Univ. Lorraine, Associate Professor, on secondment to Quarkslab since Jan 2015]

**Engineer**

Alexander Kruppa [Inria, until Mar 2015, funded by ANR Subv CATREL project]

**PhD Students**

Simon Abelard [Univ. Lorraine, from Sep 2015]
Cyril Bouvier [Univ. Lorraine, until June 2015, now Postdoc in Bordeaux]
Svyatoslav Covanov [Univ. Lorraine]
Laurent Grémy [Inria, granted by Univ. Lorraine]
Hamza Jeljeli [Univ. Lorraine, until July 2015, now with Gemalto]
Hugo Labrande [Univ. Lorraine]

**Post-Doctoral Fellows**

Nicholas Coxon [Inria, until Nov 2015]
Maike Massierer [Inria]

**Administrative Assistants**

Sophie Drouot [Inria]
Laurence Félicité [Univ. Lorraine]
Christelle Levêque [CNRS]

**Others**

Élise Tasso [ENSM Nancy, Internship, from Oct 2015]
Masahiro Ishii [Visiting Ph.D. student, NIST(JP), until Aug 2015]

Luc Sanselme [Min. de l'Éducation Nationale]

# 2. Overall Objectives

## 2.1. Overall Objectives

A general keyword that could encompass most of our research objectives is *arithmetic*. Indeed, in the CARAMEL team, the goal is to push forward the possibilities to compute efficiently with objects having an arithmetic nature. This includes integers, real and complex numbers, polynomials, finite fields, and, last but not least, algebraic curves.

Our main application domains are public-key cryptography and computer algebra systems. Concerning cryptography, we concentrate on the study of the primitives based on the factorization problem or on the discrete-logarithm problem in finite fields or (Jacobians of) algebraic curves. Both the constructive and destructive sides are of interest to CARAMEL. For applications in computer algebra systems, we are mostly interested in arithmetic building blocks for integers, floating-point numbers, polynomials, and finite fields. Also some higher level functionalities like factoring and discrete-logarithm computation are usually desired in computer algebra systems.

Since we develop our expertise at various levels, from most low-level software or hardware implementation of basic building blocks to complicated high-level algorithms like integer factorization or point counting, we have remarked that it is often too simple-minded to separate them: we believe that the interactions between low-level and high-level algorithms are of utmost importance for arithmetic applications, yielding important improvements that would not be possible with a vision restricted to low- or high-level algorithms.

We emphasize three main directions in the CARAMEL team:

- Integer factorization and discrete-logarithm computation in finite fields.

  We are in particular interested in the number field sieve algorithm (NFS) that is the best algorithm known for factoring large RSA-like integers, and for solving discrete logarithms in prime finite fields and small extension degree finite fields. In the case of discrete logarithm in small characteristic, recent progress led to algorithms that are less similar to the NFS algorithm; on the other hand they involve Gröbner basis computations.

  In all these cases, we plan to improve on existing algorithms, with a view towards practical considerations and setting new records.

- Algebraic curves and cryptography.

  Our two main research interests on this topic lie in genus-2 cryptography and in the arithmetic of pairings, mostly on the constructive side in both cases. For genus-2 curves, a key algorithmic tool that we develop is the computation of explicit isogenies; this allows improvements for cryptography-related computations such as point counting in large characteristic, complex-multiplication construction and computation of the ring of endomorphisms.

  The pairing-based cryptography landscape has been greatly modified recently, due to the progress in the discrete logarithm problem. Therefore, this is no longer a priority for us.

- Arithmetic.

  Integer, finite-field and polynomial arithmetic are ubiquitous to our research. We consider them not only as tools for other algorithms, but as a research theme *per se*. We are interested in algorithmic advances, in particular for large input sizes where asymptotically fast algorithms become of practical interest. We also keep an important implementation activity, both in hardware and in software.

Polynomial system solving is a transverse theme to these research directions. 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 also intend to develop algorithms and tools that, when possible, take advantage of these specificities.

# 3. Research Program

## 3.1. Cryptography, Arithmetic: Hardware and Software

One of the main topics for our project is public-key cryptography. After 20 years of hegemony, the classical public-key algorithms (whose security is based on integer factorization or discrete logarithm in finite fields) are currently being overtaken by elliptic curves. The fundamental reason for this is that the best algorithms known for factoring integers or for computing discrete logarithms in finite fields have — at best — a subexponential complexity, whereas the best attack known for elliptic-curve discrete logarithms has exponential complexity. As a consequence, for a given security level $2^n$, the key sizes must grow linearly with $n$ for elliptic curves, whereas they grow like $n^3$ for RSA-like systems. As a consequence, several governmental agencies, like the NSA (National Security Agency, USA) or the BSI (Bundesamt für Sicherheit in der Informationstechnik, Germany), now recommend to use elliptic-curve cryptosystems for new products that are not bound to RSA for backward compatibility.

Besides RSA and elliptic curves, there are several alternatives currently under study. There is a recent trend to promote alternate solutions that do not rely on number theory, with the objective of building systems that would resist a quantum computer (in contrast, integer factorization and discrete logarithms in finite fields and elliptic curves have a polynomial-time quantum solution). Among them, we find systems based on hard problems in lattices (NTRU is the most famous), those based on coding theory (McEliece system and improved versions), and those based on the difficulty to solve multivariate polynomial equations (UOV, for instance). None of them has yet reached the same level of popularity as RSA or elliptic curves for various reasons, including the presence of unsatisfactory features (like a huge public key), or the non-maturity (system still alternating between being fixed one day and broken the next day).

Returning to number theory, an alternative to RSA and elliptic curves is to use other curves and in particular genus-2 curves. These so-called hyperelliptic cryptosystems have been proposed in 1989 [28], soon after the elliptic ones, but their deployment is by far more difficult. The first problem was the group law. For elliptic curves, the elements of the group are just the points of the curve. In a hyperelliptic cryptosystem, the elements of the group are points on a 2-dimensional variety associated to the genus-2 curve, called the Jacobian variety. Although there exist polynomial-time methods to represent and compute with them, it took some time before getting a group law that could compete with the elliptic one in terms of speed. Another question that is still not yet fully answered is the computation of the group order, which is important for assessing the security of the associated cryptosystem. This amounts to counting the points of the curve that are defined over the base field or over an extension, and therefore this general question is called point-counting. In the past ten years there have been major improvements on the topic, but there are still cases for which no practical solution is known.

Another recent discovery in public-key cryptography is the fact that having an efficient bilinear map that is hard to invert (in a sense that can be made precise) can lead to powerful cryptographic primitives. The only examples we know of such bilinear maps are associated with algebraic curves, and in particular elliptic curves: this is the so-called Weil pairing (or its variant, the Tate pairing). Initially considered as a threat for elliptic-curve cryptography, they have proven to be quite useful from a constructive point of view, and since the beginning of the decade, hundreds of articles have been published, proposing efficient protocols based on pairings. A long-lasting open question, namely the construction of a practical identity-based encryption scheme, has been solved this way. The first standardization of pairing-based cryptography has recently occurred (see ISO/IEC 14888-3 or IEEE P1363.3), but the recent progress in discrete logarithms in finite fields will probably slow down its large deployment.

Despite the rise of elliptic curve cryptography and the variety of more or less mature alternatives, classical systems (based on factoring or discrete logarithm in finite fields) are still going to be widely used in the next decade, at least, due to resilience: it takes a long time to adopt new standards, and then an even longer time to renew all the software and hardware that is widely deployed.

This context of public-key cryptography motivates us to work on integer factorization, for which we have acquired expertise, both in factoring moderate-sized numbers, using the ECM (Elliptic Curve Method) algorithm, and in factoring large RSA-like numbers, using the number field sieve algorithm. The goal is to follow the transition from RSA to other systems and continuously assess its security to adjust key sizes. We also work on the discrete-logarithm problem in finite fields. This second task is not only necessary for assessing the security of classical public-key algorithms, but is also crucial for the security of pairing-based cryptography.

Another general application for the project is computer algebra systems (CAS), that rely in many places on efficient arithmetic. Nowadays, the objective of a CAS is not only to support an increasing number of features that the user might wish, but also to compute the results fast enough, since in many cases, the CAS are used interactively, and a human is waiting for the computation to complete. To tackle this question, more and more CAS use external libraries, that have been written with speed and reliability as first concern. For instance, most of today's CAS use the GMP library for their computations with big integers. Many of them will also use some external Basic Linear Algebra Subprograms (BLAS) implementation for their needs in numerical linear algebra.

During a typical CAS session, the libraries are called with objects whose sizes vary a lot; therefore being fast on all sizes is important. This encompasses small-sized data, like elements of the finite fields used in cryptographic applications, and larger structures, for which asymptotically fast algorithms are to be used. For instance, the user might want to study an elliptic curve over the rationals, and as a consequence, check its behaviour when reduced modulo many small primes; and then [s]he can search for large torsion points over an extension field, which will involve computing with high-degree polynomials with large integer coefficients.

Writing efficient software for arithmetic as it is used typically in CAS requires the knowledge of many algorithms with their range of applicability, good programming skills in order to spend time only where it should be spent, and finally good knowledge of the target hardware. Indeed, it makes little sense to disregard the specifics of the intended hardware platforms, even more so since in the past years, we have seen a paradigm shift in terms of available hardware: so far, it used to be reasonable to consider that an end-user running a CAS would have access to a single-CPU processor. Nowadays, even a basic laptop computer has a multi-core processor and a powerful graphics card, and a workstation with a reconfigurable coprocessor is no longer science-fiction.

In this context, one of our goals is to investigate and take advantage of these influences and interactions between various available computing resources in order to design better algorithms for basic arithmetic objects. Of course, this is not disconnected from the other goals, since they all rely more or less on integer or polynomial arithmetic.

# 4. Application Domains

## 4.1. Cryptology

The first application domain for our research is cryptology. This includes cryptography (constructive side) and cryptanalysis (breaking systems). For the cryptanalysis part, although it has practical implications, we do not expect any transfer in the classical sense of the term: it is more directed to governmental agencies and the end-users who build their trust, based on the cryptanalysis effort. It is noteworthy that analysis documents from governmental agencies (see e.g., [24]) use cryptanalysis results as their key material.

### *4.1.1. Cryptography*

Our cryptographic contributions are related to multiple facets of the large realm of curve-based cryptology. While it is quite clear that enough algorithms exist in order to provide cryptographers with elliptic curves having a suitably hard discrete logarithm (as found in cryptographic standards for instance), one must bear in mind that refinements of the requirements and extensions to curves of higher genus raise several interesting problems. Our work contributes to expanding the cryptographer's capabilities in these areas.

In the context of genus-2 curves, our work aims at two goals. First, improvements on the group law on selected curves yield better speed for the associated cryptosystems. The cryptographic primitives, and then the whole suite of cryptographic protocols built upon such curves would be accelerated. The second goal is the expansion of the set of curves that can be built given a set of desired properties. Using point counting algorithms for arbitrary curves, a curve offering a 128-bit security level, together with nice properties for fast arithmetic, has been computed by CARAMEL [5]. Another natural target for construction of curves for cryptography is also the suitability of curves for pairings. We expect to be able to compute such curves.

Important objects related to the structure of genus-2 curves are the isogenies between their Jacobians. Computing such isogenies is a key point in understanding important underlying objects such as the endomorphism ring, and can be useful in various situations, including for cryptographic or cryptanalytic applications. The team has produced important results in this context [7], [3].

### *4.1.2. Cryptanalysis*

Our research on cryptanalysis is important for the cryptographic industry: by detecting weak instances, and setting new records we contribute to the definition of recommended families of systems together with their key sizes. The user's confidence in a cryptographic primitive is also related to how well the underlying problem is studied by researchers.

In particular, our involvement in computations with "NFS-like" algorithms encompasses of course the task of assessing the computational limits for integer factorization (as was done by the team by factoring RSA-768 [6]) and discrete-logarithm computations (as was done by the team in 2013 for the field $\mathrm{GF}(2^{809})$ [25]). The impact of the former is quite clear as it concerns the RSA algorithm; record-sized computations attract broad interest and determine updates on key-length recommendations. The latter are particularly important for pairing-based cryptography, since, in this context, one naturally encounters discrete-logarithm problems in extension fields of large degree. To this regard the breakthrough provided by the new quasi-polynomial discrete logarithm [26] is of course of utmost importance.

## 4.2. Computer Algebra Systems

Some of our software libraries are being used by computer algebra systems. Most of those libraries are free software, with a license that allows proprietary systems to link them. This gives us a maximal visibility, with a large number of users.

### *4.2.1. Magma*

Magma is a very large computational algebra package. It provides a mathematically rigorous environment for computing with algebraic, number-theoretic, combinatorial, and geometric objects. It is developed in Sydney, by the team around John Cannon. It is non-commercial (in the sense that its goal is not to make profit), but is not freely distributed and is not open-source.

Several members of the team have visited Sydney — several years ago — to contribute to the development of Magma, by implementing their algorithms or helping in integrating their software. Our link to Magma exists also via the libraries it uses: it currently links GNU MPFR and GNU MPC for its floating-point calculations, and links GMP-ECM as part of its factorization suite.

### *4.2.2. Pari/GP*

Pari/GP is a computational number theory system that is composed of a C library and an interpreter on top of it. It is developed in Bordeaux, where Karim Belabas from the LFANT project-team is the main maintainer. Its license is GPL. Although we do not directly contribute to this package, we have good contact with the developers.

### *4.2.3. Sage*

Sage is a fairly large scale and open-source computer algebra system written in Python. Sage aggregates a large amount of existing free software, aiming at selecting the fastest free software package for each given task. The motto of Sage is that instead of "reinventing the wheel" all the time, Sage is "building the car". To date, Sage links GNU MPFR, GMP-ECM, and GNU MPC as standard packages.

## 4.3. Standardization

### *4.3.1. Floating-point arithmetic*

The IEEE 754 standard for floating-point arithmetic was revised in 2008. The main new features are some new formats for decimal computations, and the recommendation of correctly rounded transcendental functions. The new decimal formats should not have an impact on our work, since we either use integer-only arithmetic, or arbitrary-precision binary floating-point arithmetic through the GNU MPFR library.

A new standard (P1788) is currently under construction for interval arithmetic. We are not officially involved in this standard, but we follow the discussions, to check in particular that the proposed standard will also cover arbitrary precision (interval) arithmetic.

# 5. Highlights of the Year

## 5.1. Highlights of the Year

### *5.1.1. Awards*

The LOGJAM attack has received the best paper award at the conference ACM CCS 2015 (Conference on Computer and Communications Security). It has also received a Pwnie award [1] in the category *Most innovative research*.

The Tower NFS article was one of the two ASIACRYPT 2015 papers invited to submit a long version to Journal of Cryptology.

BEST PAPERS AWARDS:

[15]
D. ADRIAN, K. BHARGAVAN, Z. DURUMERIC, P. GAUDRY, M. GREEN, J. A. 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 "ACM CCS 2015", Denver, Colorado, United States, 2015 ACM SIGSAC Conference on Computer and Communications Security, October 2015, 14 p. [*DOI :* 10.1145/2810103.2813707], https://hal.inria.fr/hal-01184171

[17]
R. BARBULESCU, P. GAUDRY, T. KLEINJUNG. *The Tower Number Field Sieve*, in "ASIACRYPT 2015", Auckland, New Zealand, T. IWATA, J. H. CHEON (editors), Advances in cryptology-Asiacrypt 2015, Springer, November 2015, vol. 9453, pp. 31-58, https://hal.archives-ouvertes.fr/hal-01155635

# 6. New Software and Platforms

## 6.1. Belenios

Belenios - Verifiable online voting system
KEYWORD: E-voting
FUNCTIONAL DESCRIPTION

[1] http://pwnies.com/

In collaboration with the CASSIS team, we develop an open-source private and verifiable electronic voting protocol, named BELENIOS. Our system is an evolution of an existing system, Helios, developed by Ben Adida, and used e.g., by UCL and the IACR association in real elections. The main differences with Helios are the following ones:

- In Helios, the ballot box publishes the encrypted ballots together with their corresponding voters. This raises a privacy issue in the sense that whether someone voted or not shall not necessarily be publicized on the web. Publishing this information is in particular forbidden by CNIL's recommendation. BELENIOS no longer publishes voters' identities, still guaranteeing correctness of the tally.
- Helios is verifiable except that one has to trust that the ballot box will not add ballots. The addition of ballots is particularly hard to detect as soon as the list of voters is not public. We have therefore introduced an additional authority that provides credentials that the ballot box can verify but not forge [27].

This new version has been implemented by Stéphane Glondu [2]. The first public release has been done in January 2014. Belenios has been used in Sep 2015 for the election of the new leader of the GT-C2 (Groupe de Travail Codes et Cryptographie) which is part of the GdR-IM (Groupement de Recherche Informatique Mathématique). The GT calcul formel of the GdR-IM plans to use Belenios in 2016 for the election of its new leader.

An online platform [3] has been released in September 2015, so that setting up a new election can be done entirely from within a browser.

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

## 6.2. CADO-NFS

Crible Algébrique: Distribution, Optimisation - Number Field Sieve
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: Emmanuel Thomé, Pierrick Gaudry, Paul Zimmermann, Alexander Kruppa, François Morain, Cyril Bouvier.
- Contact: Emmanuel Thomé
- URL: http://cado-nfs.gforge.inria.fr/

In December 2015, a major new release of CADO-NFS, version 2.2.0, was published. It contains several bug fixes, efficiency improvements, and the computation of discrete logarithms is now almost "push-button".

## 6.3. CMH

Computation of Igusa Class Polynomials
KEYWORDS: Mathematics - Cryptography - Number theory
FUNCTIONAL DESCRIPTION

[2] http://belenios.gforge.inria.fr/
[3] https://belenios.loria.fr/

Cmh computes Igusa class polynomials, parameterizing two-dimensional abelian varieties (or, equivalently, Jacobians of hyperelliptic curves of genus 2) with given complex multiplication.

- Participants: Emmanuel Thomé, Andreas Enge
- Contact: Emmanuel Thomé
- URL: http://cmh.gforge.inria.fr/

## 6.4. GF2X

FUNCTIONAL DESCRIPTION

GF2X is a software library for polynomial multiplication over the binary field, developed together with Richard Brent (Australian National University, Canberra, Australia). It holds state-of-the-art implementation of fast algorithms for this task, employing different algorithms in order to achieve efficiency from small to large operand sizes (Karatsuba and Toom-Cook variants, and eventually Schönhage's or Cantor's FFT-like algorithms). FG2X takes advantage of specific processor instructions (SSE, PCLMULQDQ).

- Participants: Pierrick Gaudry, Emmanuel Thomé and Paul Zimmermann
- Contact: Emmanuel Thomé
- URL: https://gforge.inria.fr/projects/gf2x/

## 6.5. GNU MPC

FUNCTIONAL DESCRIPTION

MPC is a C library for the arithmetic of complex numbers with arbitrarily high precision and correct rounding of the result. It is built upon and follows the same principles as MPFR. The library is written by Andreas Enge, Philippe Théveny and Paul Zimmermann.

- Participants: Andreas Enge, Paul Zimmermann, Philippe Théveny and Mickaël Gastineau
- Contact: Andreas Enge
- URL: http://www.multiprecision.org/

## 6.6. GNU-MPFR

KEYWORDS: Multiple-Precision - Floating-point - Correct Rounding
FUNCTIONAL DESCRIPTION

GNU MPFR is an efficient multiple-precision floating-point library with well-defined semantics (copying the good ideas from the IEEE-754 standard), in particular correct rounding in 5 rounding modes. GNU MPFR provides about 80 mathematical functions, in addition to utility functions (assignments, conversions...). Special data (Not a Number, infinities, signed zeros) are handled like in the IEEE-754 standard.

- Participants: Vincent Lefèvre, Guillaume Hanrot, Philippe Théveny and Paul Zimmermann
- Contact: Vincent Lefèvre
- URL: http://www.mpfr.org/

## 6.7. MPFQ

FUNCTIONAL DESCRIPTION

MPFQ is (yet another) library for computing in finite fields, with automatic generation of code for fields known at compile-time. It consists of roughly 18,000 lines of Perl code, which generate most of the C code. MPFQ is used in CADO-NFS, in particular for the linear algebra step during discrete logarithm computations.

- Participants: Emmanuel Thomé, Pierrick Gaudry and Luc Sanselme
- Contact: Pierrick Gaudry
- URL: http://mpfq.gforge.inria.fr/

## 6.8. Tinygb

Tinygb is a small software tool written in C++. Its aim is to provide an interface between several existing libraries (finite field arithmetic, linear algebra) for Gröbner bases computations occurring in problems investigated by the CARAMEL group. The focus is not on the efficiency of the implementation, since this is already successfully achieved in other existing software such as *FGb* (developed by Jean-Charles Faugère) or in the CAS Magma (Gröbner bases algorithms are implemented by Alan Steel). The goal of Tinygb is to be a flexible research tool where variants of classical algorithms can be tested. Tinygb is still in development since it requires more testing and packaging before being released.

- Participants: Pierre-Jean Spaenlehauer

## 6.9. Platforms

### *6.9.1. CATREL cluster*

Installed in 2013, the CATREL computer cluster now plays an essential role in providing the team with the necessary resources to achieve significant computations, which illustrate well the efficiency of the algorithms developed in our research, together with their implementations.

In 2015, the CATREL cluster was in particular used for the precomputations performed for the LOGJAM attack [15]. It was the main computing resource for a record discrete logarithm computation in finite fields of the form $\mathbb{F}_{p^3}$ of 512 bits, and a larger computation for this kind of fields is currently running. It was also used intensively to optimize the sieving parameters of CADO-NFS for factoring numbers from 60 to 155 digits, in the preparation of the release 2.2.0. It was used to factor 47 large integers from nine aliquot sequences starting from 276 to 204828, the largest one being a 190-digit composite number from sequence 660. The current largest element known from an aliquot sequence has 197 digits (sequence 19560), and we expect the 200-digit frontier will be reached in 2016. Several experiments were also made with variations of the polynomial selection algorithm from [10] on RSA-896 and RSA-1024.

# 7. New Results

## 7.1. The Logjam attack against the discrete logarithm

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

Together with colleagues from the Prosecco project-team and with other colleagues, we exhibited a new attack again the TLS protocol when using discrete logarithms [15]. A proof-of-concept of the attack was demonstrated using the CADO-NFS software. This paper obtained the best paper award at the ACM CCS 2015 conference, and received significant media coverage both in the specialized and non-specialized press.

## 7.2. Other results related to discrete logarithm

**Participant:** Pierrick Gaudry [contact].

Our 2014 work [16], in collaboration with Barbulescu, Guillevic and Morain, improving the practical aspects of discrete logarithm computation in quadratic extensions and reducing the theoretical complexity in the "medium characteristic case" has been published in Eurocrypt 2015.

In collaboration with Barbulescu and Kleinjung we have proposed in [17] to revisit an old construction of Schirokauer for discrete logarithms in extension fields. It is well suited for problems coming from pairings where the primes often have a special form.

With Galbraith we wrote a survey about the discrete logarithm problem in the context of elliptic curves [13].

## 7.3. Fast arithmetic for faster integer multiplication

**Participants:** Svyatoslav Covanov [contact], Emmanuel Thomé.

The paper [20] 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. A journal submission is planned shortly.

## 7.4. Certificates for exact linear algebra computations

**Participant:** Emmanuel Thomé [contact].

The paper [21], in collaboration with Jean-Guillaume Dumas and Erich Kaltofen, is a preliminary version of a research work that has then been pursued, and that solves an open question of proving the correctness of some specific linear algebra computations. It emerged from practical techniques which had been used for this purpose for a while, and for which improvements were obtained. Submission plans for this work are yet to be finalized.

## 7.5. Computing Jacobi's theta function in quasi-linear time

**Participant:** Hugo Labrande [contact].

We designed a new algorithm that improves the complexity of computing the value of the Jacobi theta function, $\theta(z, \tau)$ to arbitrary precision [23]. The algorithm uses a quadratically convergent sequence similar to the complex AGM, as well as Newton's method; its complexity is $O(\mathcal{M}(n) \log n)$ for computing the value up to an error bounded by $2^{-n}$, which is an improvement over the state-of-the-art complexity of $O(\mathcal{M}(n)\sqrt{n})$. Here, $\mathcal{M}(n)$ denotes the time taken by a multiplication of two $n$-bit numbers. We provide bounds on the loss of significant digits incurred during the computation. The algorithm was implemented using GNU MPC, showing practical improvement over (our optimized implementation of) existing algorithms for precision above approximately $300,000$ bits. The paper was submitted to *Mathematics of Computation*.

## 7.6. Construction of sparse polynomial systems with many positive solutions

**Participant:** Pierre-Jean Spaenlehauer [contact].

In collaboration with Frédéric Bihan (Univ. Savoie Mont-Blanc), we propose a variant of the classical Viro method to construct polynomial systems with prescribed monomial support and many solutions whose coordinates are all positive [19]. This is an asymptotic construction which has strong connections with tropical and convex geometry, and which involves computational problems such as low-rank matrix completion.

## 7.7. Small certificates of inconsistency of quadratic fewnomial systems

**Participant:** Pierre-Jean Spaenlehauer [contact].

In collaboration with Jean-Charles Faugère (EPI PolSys) and Jules Svartz (Min. de Éducation Nationale), we studied the problem of certifying the inconsistency of sparse quadratic polynomial systems. Finding certificates of inconsistency is a classical problem in computational commutative algebra, and these certificates are in general of size exponential in the input size. We identify families of quadratic fewnomial systems for which there exist certificates of size linear in the size of the input and we propose algorithms to compute them in polynomial time.

## 7.8. Cracking passphrases based on famous sentences

**Participant:** Hugo Labrande [contact].

We proposed a method to attack passwords based on famous sentences, which are rather widespread [18]: we showed a method to construct large dictionaries using only publicly-available sources (e.g. Wikipedia) and modest computing power. The resulting dictionaries were able to crack millions of passphrases, among which a 55-character long one, and some that do not appear to have been cracked before. Our work thus shows that using famous sentences as passwords is not secure at all, as any attacker, even those with low skills and very modest computational resources, can guess them.

# 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 for 2013, 2014 and 2015.

## 8.2. Consulting with Docapost

In the context of our activities on electronic voting, in collaboration with the Cassis team, we had a consulting contract with the Docapost company. The goal was to evaluate their e-voting product and to propose various directions for future improvements.

# 9. Partnerships and Cooperations

## 9.1. Regional Initiatives

In the context of the research grant "CPER Cyberentreprises", involving the French ministry of research, Région Lorraine, Inria, CNRS, and the European fund FEDER, we solicited and obtained funding for a new computer equipment dedicated to the computation of large polynomial systems. The corresponding machine has been delivered in November 2015, and will be put into service in the first weeks of 2016.

## 9.2. National Initiatives

The team participates in the "Calcul formel, arithmétique, protection de l'information" research pole of the GDR-IM (CNRS Research Group on Mathematical Computer Science). The team is a member of the "Arithmétique", "Calcul formel" and "Codage et Cryptographie" working groups.

### *9.2.1. ANR CATREL (Cribles: Améliorations Théoriques et Résolution Effective du Logarithme discret)*

**Participants:** Cyril Bouvier, Nicholas Coxon, Jérémie Detrey, Pierrick Gaudry, Laurent Grémy, Hamza Jeljeli, Emmanuel Thomé [contact], Marion Videau, Paul Zimmermann.

The CATREL proposal has been accepted in ANR "programme Blanc" in 2012. This project involves CARAMEL as a leading team, in cooperation with two other partners which are INRIA project-team GRACE (INRIA Saclay, LIX, École Polytechnique), and the ARITH team of the LIRMM Laboratory (Montpellier). The project targets algorithms for solving the discrete logarithm problem in finite fields, using the Number Field Sieve and the Function Field Sieve algorithms. Actual work on the CATREL project started in January 2013. According to the schedule, the project ended on Dec. 31st, 2015. Two project meetings were held in 2015: in Nancy on January 13-14, 2015, and in Palaiseau on October 1-2, 2015. The last project meeting was attached to an international workshop which brought together international experts on the Discrete Logarithm Problem to discuss the massive advances on this topic during the last years. A mid-term project review of the CATREL project was conducted by ANR in March 2015. The review outcome was very positive.

#### 9.2.2. PEPS JCJC INSII RiCoRé (Résolution de systèmes polynomiaux pour les codes correcteurs et la robotique)

**Participant:** Pierre-Jean Spaenlehauer.

The RiCoRé proposal has been accepted in the PEPS JCJC INSII program in 2015. This project is coordinated by Romain Lebreton (Maître de Conférence, Univ. Montpellier). The other participants are Salih Abdelaziz (Maître de Conférence, Univ. Montpellier) and Eleonora Guerrini (Maître de Conférence, Univ. Montpellier). The aim of this project is to study the interactions of symbolic algorithms for polynomial system solving with some problems arising in coding theory and robotics.

## 9.3. International Research Visitors

### 9.3.1. Visits of International Scientists

- Masahiro Ishii, a PhD student from the Nara Institute of Science and Technology, Nara (Japan), visited us from February 2014 until February 2015. His PhD supervisors are Atsuo Inomata and Kazutoshi Fujikawa. Locally, he was supervised by Jérémie Detrey and Pierrick Gaudry.

  During his stay here, he worked on implementing the elliptic curve factorization method (ECM) on the Kalray MPPA-256 manycore processor. A paper is currently in progress.
- Nadia Heninger, Assistant Professor at the University of Pennsylvania, visited us from June 22 to June 26.

# 10. Dissemination

## 10.1. Promoting Scientific Activities

### 10.1.1. Scientific events organisation

Maike Massierer and Pierre-Jean Spaenlehauer organized a minisymposium on “Applications of polynomial system solving in cryptology” [4] within the SIAM conference on applied algebraic geometry conference, held in Daejeon (Corea) on August 3-7, 2015.

### 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*

- Jérémie Detrey was a member of the program committee of
  - the *Conférence d'informatique en Parallélisme, Architecture et Système* (Compas 2015);
  - the Fourth International Conference on Cryptology and Information Security in Latin America (Latincrypt 2015).
- Pierrick Gaudry was a member of the program committee of
  - the 9th International Workshop on Coding and Cryptography (WCC 2015);
  - the 7th International Workshop on Parallel Symbolic Computation (PASCO 2015).
- Emmanuel Thomé was a member of the program committee for
  - the 19th Workshop on Elliptic Curve Cryptography (ECC 2015);
  - the 8th International Symposium on Foundations & Practice of Security (FPS 2015);

[4] http://wiki.siam.org/siag-ag/index.php/Applications_of_Polynomial_System_Solving_in_Cryptology

  - the 35th Annual International Conference on the Theory and Applications of Cryptographic Techniques (Eurocrypt 2016).
- Marion Videau was a member of the program commitee of
  - the Symposium sur la sécurité des technologies de l'information et des communications, SSTIC 2015;
  - the International Conference on Information Security and Cryptology, ICISC 2015;
  - the GreHack, 2015.

*10.1.2.3. Reviewing activities*

- Jérémie Detrey reviewed submissions to
  - the 22nd IEEE Symposium on Computer Arithmetic (ARITH 22);
  - the *Conférence d'informatique en Parallélisme, Architecture et Système* (Compas 2015);
  - the Fourth International Conference on Cryptology and Information Security in Latin America (Latincrypt 2015);
  - the 19th International Conference on the Theory and Practice of Public-Key Cryptography (PKC 2016).
- Pierre-Jean Spaenlehauer reviewed submissions to
  - the 40th International Symposium on Symbolic and Algebraic Computations (ISSAC 2015);
  - the 21st Annual Conference on the Theory and Application of Cryptology and Information Security (Asiacrypt 2015);
  - 6th International Conference on Mathematical Aspects of Computer and Information Sciences (MACIS 2015);
  - The 28th International Conference of the Jangjeon Mathematical Society (ICJMS 2015).
- Maike Massierer reviewed a submission to the IACR International Conference on Practice and Theory of Public-Key Cryptography (PKC 2015).
- Pierrick Gaudry reviewed submissions to
  - the 30th ACM/SIGAPP Symposium On Applied Computing (SAC 2015);
  - the 22nd IEEE Symposium on Computer Arithmetic (ARITH 22);

### *10.1.3. Journal*

*10.1.3.1. Member of the editorial boards*

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

*10.1.3.2. Reviewing activities*

- Jérémie Detrey reviewed submissions to
  - the IEEE Transactions on Dependable and Secure Computing (TDSC);
  - the ACM Transactions on Mathematical Software (TOMS).
- Pierre-Jean Spaenlehauer reviewed submissions to
  - the Journal of Symbolic Computation (JSC);
  - Commentationes Mathematicae Universitatis Carolinae (CMUC);
  - Mathematical Modeling and Numerical Analysis (ESAIM-M2AN);
  - the Journal of Cryptographic Engineering (JCEN).
- Maike Massierer reviewed submissions to
  - Finite Fields and Applications (FFA);

  - Applicable Algebra in Engineering, Communication and Computing (AAECC).
- Pierrick Gaudry reviewed submissions to
  - Applicable Algebra in Engineering, Communication and Computing (AAECC).
  - Journal of Cryptology;

### *10.1.4. Invited talks*

- Jérémie Detrey gave invited talks at
  - the tutorial session of the 22nd IEEE Symposium on Computer Arithmetic (ARITH 22, June, Lyon, France);
  - the summer school of the 19th Workshop on Elliptic Curve Cryptography (ECC 2015, September, Bordeaux, France).
- Pierre-Jean Spaenlehauer gave invited talks at
  - the Workshop on Structured Low-Rank Approximation (June, Grenoble, France);
  - the SIAM conference on Applied Algebraic Geometry, Minisymposium on Algorithms and Complexity in Polynomial System Solving (August, Daejeon, Corea);
  - the SIAM conference on Applied Algebraic Geometry, Minisymposium on ML Degree and Critical Points (August, Daejeon, Corea);
  - the Third Workshop on Hybrid Methodologies for Symbolic-Numeric Computations (August, Beijing, China);
  - the Workshop on Algebra, Geometry and Proofs in Symbolic Computation (December, Toronto, Canada).
- Pierrick Gaudry gave invited talks at
  - the CATREL Workshop: Advances in Discrete Logarithms (October, Palaiseau, France);
  - the Colloquium Jacques Morgenstern (Nice-Sophia).
- Emmanuel Thomé gave an invited talk at the CATREL Workshop: Advances in Discrete Logarithms (October, Palaiseau, 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.
- Pierre-Jean Spaenlehauer is a member of the *Commission des développements technologiques* (CDT) of the Inria Nancy – Grand Est research center.
- Pierrick Gaudry was a member in 2015 of
  - the *Commission de mention Informatique* of the *École doctorale IAEM* of the University of Lorraine;
  - the hiring committee for an associate professor position Univ. Montpellier;
  - the committee for the HCERES evaluation of the LITIS laboratory in Rouen;
  - the evaluation committee for the *Algorithmics, Computer Algebra and Cryptology* Inria theme, acting as *coordinator*.
- 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.
- Marion Videau was a member of the hiring committee for the 2015 junior research positions (CR2) at Inria Saclay.
- Laurent Grémy is a member of the *Conseil de laboratoire* of the Loria.

### *10.1.6. Seminar organisation*

#### *10.1.6.1. CARAMEL seminar*

Five speakers were invited in our seminar in 2015: Matthieu Rambaud, Roland Wen, Jan Tuitman, Frédéric Bihan, Chenqi Mou.

*10.1.6.2. Joint security seminar with the university master in computer science*

The team is involved with other teams and the university master in computer science in the organization of the security seminar which started in 2013. Fifteen speakers were invited in 2015: Graham Steel, Nicolas Fischbach, Georges Bossert, Jean-Philippe Aumasson, Khartik Bhargavan, Kenny Paterson, Bertrand Wallrich, Cédric Lauradoux, Nora Cuppens, Christian Grothoff, Éric Freyssinet, Maxime Clementz, Kostas Chatzikokolakis, Emmanuel Thomé, Olivier Levillain.

## 10.2. Teaching - Supervision - Juries

### *10.2.1. Teaching*

**Licence**

Jérémie Detrey, *Security of websites*, 2 hours (lecture), L1, Université de Lorraine, IUT Charlemagne, Nancy, France.

Jérémie Detrey, *Introduction to Cryptology and Information Security*, 10 hours (lectures) + 10 hours (tutorial sessions) + 10 hours (practical sessions), L3, Université de Lorraine, Faculté des sciences et technologies, Vandœuvre-les-Nancy, France.

Pierrick Gaudry, *Algorithmique et Programmation*, 16 hours (practical sessions), L1, Université de Lorraine, Faculté des sciences et technologies, Vandœuvre-les-Nancy, France.

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

**Master**

Pierre-Jean Spaenlehauer, *Introduction to Cryptography*, 12 hours (lectures), M1, Université de Lorraine, Faculté des sciences et technologies, Vandœuvre-les-Nancy, France.

Emmanuel Thomé, *Introduction to Cryptography*, 12 hours (lectures), M1, Télécom Nancy, Vandœuvre-les-Nancy, France.

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

Marion Videau and Stéphane Glondu supervised the semestrial project of all the students of M2, SSSR-SAW, Université de Lorraine, departement d'informatique, France.

**Other**

Emmanuel Thomé, *Discrete logarithms in Finite Fields*, advanced course for the ECC 2015 summer school, Bordeaux, France.

### *10.2.2. Supervision*

- **Ph.D. in progress**

  Simon Abelard, *Comptage de points de courbes algébriques sur les corps finis et interactions avec les systèmes polynomiaux*, since Sep. 2015, Pierrick Gaudry & Pierre-Jean Spaenlehauer.

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

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

  Hugo Labrande, *Calcul effectif d'isogénies entre jacobiennes de courbes algébriques par une méthode d'analyse complexe*, since Sep 2013, Emmanuel Thomé & Michael J. Jacobson, Jr. (Univ. Calgary, Canada).

- **Ph.D. defended in 2015**

Cyril Bouvier, *Algorithmes pour la factorisation d'entiers et le calcul de logarithme discret*, supervised by Paul Zimmermann, defended in June.

Hamza Jeljeli, *Accélérateurs logiciels et matériels pour l'algèbre linéaire creuse sur les corps finis*, supervised by Jérémie Detrey & Emmanuel Thomé, defended in July.

### *10.2.3. Juries*

- Jérémie Detrey was a member of the jury of the ÉNS competitive entrance exam.
- Pierrick Gaudry was a reviewer and member of the jury for the PhD thesis of Enea Milio (Univ. Bordeaux); he was in the jury for the PhD thesis of Florent Rovetta (Univ. Aix-Marseille).
- Emmanuel Thomé was a reviewer and member of the jury for the PhD thesis of Bastien Vialla (Montpellier).
- Marion Videau was a reviewer and member of the jury for the PhD thesis of Stéphanie Riaud (Rennes).

## 10.3. Popularization

- Jérémie Detrey gave a presentation on the Enigma machine and its cryptanalysis to high-school teachers as part as the *journée EPI-ISN*.
- Laurent Grémy has given in April an introductory course about the Diffie-Hellman protocol for high school students during a discovery day of the Université de Lorraine.
- Pierre-Jean Spaenlehauer has participated in a session "activités débranchées" organized by Marie Duflot-Kremer (MCF Univ. Lorraine) during the event MathC2+ which was held in CRI Nancy – Grand Est. The aim of this session was to provide junior high school students with an initiation to computer science through a set of algorithmic games.
- Pierre-Jean Spaenlehauer has animated a stand in the "Village des Sciences du Loria" in April 2015.

# 11. Bibliography

## Major publications by the team in recent years

[1] 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

[2] R. BRENT, P. ZIMMERMANN. *Modern Computer Arithmetic*, Cambridge Monographs on Applied and Computational Mathematics, Cambridge University Press, 2010, vol. 18, 221 p. , http://hal.inria.fr/inria-00424347

[3] R. COSSET, D. ROBERT. *Computing (l,l)-isogenies in polynomial time on Jacobians of genus 2 curves*, 2013, Accepté pour publication à Mathematics of Computations, http://hal.inria.fr/hal-00578991

[4] A. ENGE, P. GAUDRY, E. THOMÉ. *An $L(1/3)$ Discrete Logarithm Algorithm for Low Degree Curves*, in "Journal of Cryptology", 2011, vol. 24, pp. 24-41 [*DOI :* 10.1007/s00145-010-9057-y], http://hal.inria.fr/inria-00383941

[5] P. GAUDRY, É. SCHOST. *Genus 2 point counting over prime fields*, in "Journal of Symbolic Computation", 2012, vol. 47, n° 4, pp. 368-400 [*DOI :* 10.1016/j.jsc.2011.09.003], http://hal.inria.fr/inria-00542650

[6] T. KLEINJUNG, K. AOKI, J. FRANKE, A. K. LENSTRA, E. THOMÉ, J. W. 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", Santa Barbara, United States, T. RABIN (editor), Lecture Notes in Computer Science, Springer Verlag, 2010, vol. 6223, pp. 333-350, http://link.springer.com/chapter/10.1007/978-3-642-14623-7_18

[7] D. LUBICZ, D. ROBERT. *Computing isogenies between Abelian Varieties*, in "Compositio Mathematica", September 2012, vol. 148, n° 05, pp. 1483–1515 [*DOI :* 10.1112/S0010437X12000243], http://hal.inria.fr/hal-00446062

## Publications of the year

### Doctoral Dissertations and Habilitation Theses

[8] C. BOUVIER. *Algorithms for integer factorization and discrete logarithms computation*, Université de Lorraine, June 2015, https://tel.archives-ouvertes.fr/tel-01167281

[9] H. JELJELI. *Hardware and Software Accelerators for Sparse Linear Algebra over Finite Fields*, Université de Lorraine, July 2015, https://tel.archives-ouvertes.fr/tel-01178931

### Articles in International Peer-Reviewed Journals

[10] S. BAI, C. BOUVIER, A. KRUPPA, P. ZIMMERMANN. *Better polynomials for GNFS*, in "Mathematics of Computation / Mathematics of Computation", December 2015, 12 p. , https://hal.inria.fr/hal-01089507

[11] R. BARBULESCU. *Selecting polynomials for the Function Field Sieve*, in "Mathematics of Computation", March 2015, S0025-5718-2015-02940-8, https://hal.inria.fr/hal-00798386

[12] R. COSSET, D. ROBERT. *Computing (l,l)-isogenies in polynomial time on Jacobians of genus 2 curves*, in "Mathematics of Computation", 2015, vol. 84, n° 294, pp. 1953-1975, Accepté pour publication à Mathematics of Computations [*DOI :* 10.1090/S0025-5718-2014-02899-8], https://hal.archives-ouvertes.fr/hal-00578991

[13] S. GALBRAITH, P. GAUDRY. *Recent progress on the elliptic curve discrete logarithm problem*, in "Designs, Codes and Cryptography", 2015 [*DOI :* 10.1007/s10623-015-0146-7], https://hal.inria.fr/hal-01215623

[14] É. SCHOST, P.-J. SPAENLEHAUER. *A Quadratically Convergent Algorithm for Structured Low-Rank Approximation*, in "Foundations of Computational Mathematics", March 2015, pp. 1-36, https://hal.archives-ouvertes.fr/hal-00953684

### International Conferences with Proceedings

[15] *Best Paper*
D. ADRIAN, K. BHARGAVAN, Z. DURUMERIC, P. GAUDRY, M. GREEN, J. A. 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 "ACM CCS 2015", Denver, Colorado, United States, 2015 ACM SIGSAC Conference on Computer and Communications Security, October 2015, 14 p. [*DOI :* 10.1145/2810103.2813707], https://hal.inria.fr/hal-01184171.

[16] R. BARBULESCU, P. GAUDRY, A. GUILLEVIC, F. MORAIN. *Improving NFS for the discrete logarithm problem in non-prime finite fields*, in "Eurocrypt 2015, 34th Annual International Conference on the Theory and Applications of Cryptographic Techniques", Sofia, Bulgaria, M. FISCHLIN, E. OSWALD (editors), April 2015, 27 p. , https://hal.inria.fr/hal-01112879

[17] *Best Paper*
R. BARBULESCU, P. GAUDRY, T. KLEINJUNG. *The Tower Number Field Sieve*, in "ASIACRYPT 2015", Auckland, New Zealand, T. IWATA, J. H. CHEON (editors), Advances in cryptology-Asiacrypt 2015, Springer, November 2015, vol. 9453, pp. 31-58, https://hal.archives-ouvertes.fr/hal-01155635.

### National Conferences with Proceedings

[18] H. LABRANDE. *Crack me, I'm famous!: Cracking weak passphrases using freely available sources*, in "SSTIC 2015", Rennes, France, June 2015, https://hal.inria.fr/hal-01238600

### Other Publications

[19] F. BIHAN, P.-J. SPAENLEHAUER. *Sparse Polynomial Systems with many Positive Solutions from Bipartite Simplicial Complexes*, October 2015, working paper or preprint, https://hal.inria.fr/hal-01217547

[20] S. COVANOV, E. THOMÉ. *Fast arithmetic for faster integer multiplication*, January 2015, working paper or preprint, https://hal.inria.fr/hal-01108166

[21] J.-G. DUMAS, E. KALTOFEN, E. THOMÉ. *Interactive certificate for the verification of Wiedemann's Krylov sequence: application to the certification of the determinant, the minimal and the characteristic polynomials of sparse matrices*, July 2015, working paper or preprint, https://hal.archives-ouvertes.fr/hal-01171249

[22] S. IONICA, E. THOMÉ. *Isogeny graphs with maximal real multiplication*, January 2015, working paper or preprint, https://hal.archives-ouvertes.fr/hal-00967742

[23] H. LABRANDE. *Computing Jacobi's $\theta$ in quasi-linear time*, November 2015, working paper or preprint, https://hal.inria.fr/hal-01227699

## References in notes

[24] AGENCE NATIONALE DE LA SÉCURITÉ DES SYSTÈMES D'INFORMATION. *Référentiel général de sécurité, annexe B1*, 2013, http://www.ssi.gouv.fr/fr/reglementation-ssi/referentiel-general-de-securite/

[25] R. BARBULESCU, C. BOUVIER, J. DETREY, P. GAUDRY, H. JELJELI, E. THOMÉ, M. VIDEAU, P. ZIMMERMANN. *Discrete logarithm in GF($2^{809}$) with FFS*, in "PKC 2014 - International Conference on Practice and Theory of Public-Key Cryptography", Buenos Aires, Argentina, H. KRAWCZYK (editor), LNCS, Springer, 2014 [*DOI :* 10.1007/978-3-642-54631-0_13], https://hal.inria.fr/hal-00818124

[26] 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

[27] V. CORTIER, D. GALINDO, S. GLONDU, M. IZABACHÈNE. *Election Verifiability for Helios under Weaker Trust Assumptions*, in "Proceedings of the 19th European Symposium on Research in Computer Security (ESORICS'14)", Wroclaw, Poland, September 2014, https://hal.inria.fr/hal-01080292

[28] N. KOBLITZ. *Hyperelliptic cryptosystems*, in "J. Cryptology", 1989, vol. 1, pp. 139–150