IN PARTNERSHIP WITH:
CNRS

Université de Lorraine

Activity Report 2014

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

Keywords: Algorithmic Number Theory, Cryptography, Computer Arithmetic, Hardware Accelerators

Creation of the Team: 2010 January 01*, updated into Project-Team:* 2011 January 01.

1. Members

Research Scientists

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

Faculty Member

Marion Videau [Univ. Lorraine, Associate Professor]

Engineers

Alain Filbois [Inria, Research Engineer, until Sep 2014]
Stéphane Glondu [Inria, Research Engineer, 50% with the CASSIS team, until Sep 2014]
Alexander Kruppa [Inria, ADT grant, until Sep 2014, then grant from ANR CATREL project, from Oct 2014 until Mar 2015]
Thomas Richard [CNRS, from Oct 2014]

PhD Students

Cyril Bouvier [Univ. Lorraine, from Sep 2012]
Svyatoslav Covanov [Univ. Lorraine, from Sep 2014]
Laurent Grémy [Inria, from Oct 2013]
Hamza Jeljeli [Univ. Lorraine, from Oct 2011]
Hugo Labrande [Univ. Lorraine, cotutelle with Univ. Calgary (CA), from Sep 2013]

Post-Doctoral Fellows

Nicholas Coxon [Inria, from Jun 2014]
Maike Massierer [SNF (CH), from Feb 2014]

Administrative Assistants

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

Others

Masahiro Ishii [Visiting PhD student, NIST (JP), from Feb 2014 until Feb 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.

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 [32], 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., [31]) 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 [4]. 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 [6], [2].

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 [5]) and discrete-logarithm computations (as was done by the team in 2013 for the field $GF(2^{809})$ [15]). 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 [17] 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, combinatoric, 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. New Software and Platforms

5.1. Introduction

A major part of the research done in the CARAMEL team is published within software. On the one hand, this enables everyone to check that the algorithms we develop are really efficient in practice; on the other hand, this gives other researchers — and us of course — basic software components on which they — and we — can build other applications.

5.2. GNU MPFR

Participant: Paul Zimmermann [contact].

GNU MPFR is one of the main pieces of software developed by the CARAMEL team. Since end 2006, it has become a joint project between CARAMEL and the ARÉNAIRE project-team (now ARIC, INRIA Grenoble - Rhône-Alpes). GNU MPFR is a library for computing with arbitrary precision floating-point numbers, together with well-defined semantics, and is distributed under the LGPL license. All arithmetic operations are performed according to a rounding mode provided by the user, and all results are guaranteed correct to the last bit, according to the given rounding mode.

No new release was made in 2014. However a developers meeting was organized in January 20 to 22 in Nancy, together with the developers of GNU MPC.

5.3. GNU MPC

Participant: Paul Zimmermann [contact].

GNU MPC is a floating-point library for complex numbers, which is developed on top of the GNU MPFR library, and distributed under the LGPL license. It is co-written with Andreas Enge (LFANT project-team, INRIA Bordeaux - Sud-Ouest). A complex floating-point number is represented by $x + iy$, where x and y are real floating-point numbers, represented using the GNU MPFR library. The GNU MPC library provides correct rounding on both the real part x and the imaginary part y of any result. GNU MPC is used in particular in the TRIP celestial mechanics system developed at IMCCE (*Institut de Mécanique Céleste et de Calcul des Éphémérides*), and by the Magma and Sage computational number theory systems.

Version 1.0.2 (Fagus silvatica) was released in January, with a few bug fixes, some related to the use in our own work related to the computation of Igusa class polynomials.

5.4. Finite Fields

Participants: Pierrick Gaudry, Emmanuel Thomé [contact], Luc Sanselme.

$\mathtt{mp}\mathbb{F}_q$ is (yet another) library for computing in finite fields. The purpose of $\mathtt{mp}\mathbb{F}_q$ is not to provide a software layer for accessing finite fields determined at runtime within a computer algebra system like Magma, but rather to give a very efficient, optimized code for computing in finite fields precisely known at *compile time*. $\mathtt{mp}\mathbb{F}_q$ can adapt to finite fields of any characteristic and any extension degree. However, one of the targets being the use in cryptology, $\mathtt{mp}\mathbb{F}_q$ somehow focuses on prime fields and on fields of characteristic two.

When it was first written in 2007, $\mathtt{mp}\mathbb{F}_q$ established reference marks for fast elliptic curve cryptography: the authors improved over the fastest examples of key-sharing software in genus 1 and 2, both over binary fields and prime fields. A stream of academic works followed the idea behind $\mathtt{mp}\mathbb{F}_q$ and improved over such timings, notably by Scott, Aranha, Longa, Bos, Hisil, Costello.

The library's purpose being the *generation* of code rather than its execution, the working core of $\mathtt{mp}\mathbb{F}_q$ consists of roughly 18,000 lines of Perl code, which generate most of the `C` code. $\mathtt{mp}\mathbb{F}_q$ is distributed at http://mpfq.gforge.inria.fr/.

In 2014, $\mathtt{mp}\mathbb{F}_q$ has undergone some sanitization work, related to embedded assembly, build system, coverage test, and processor feature support. The fact that $\mathtt{mp}\mathbb{F}_q$ is used in CADO-NFS has played an important role in fostering these changes to the $\mathtt{mp}\mathbb{F}_q$ code. Future plans regarding the linear algebra code in CADO-NFS are expected to rely on the arithmetic part being implemented in $\mathtt{mp}\mathbb{F}_q$. Preliminary work in this direction has been implemented by Luc Sanselme. Preliminary code by Hamza Jeljeli and Bastien Vialla from LIRMM, Montpellier, based on RNS arithmetic (Residue Number System) is also to be integrated in this context. We therefore expect more work in this area in the coming months, eventually leading to a new release.

5.5. gf2x

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

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). GF2X takes advantage of specific processor instructions (SSE, PCLMULQDQ).

The current version of GF2X is 1.1, released in May 2012 under the GNU GPL. Since 2009, GF2X can be used as an auxiliary package for the widespread software library NTL, as of version 5.5. GF2X is also packaged in the Debian Linux distribution.

In 2014, the development version of GF2X has been updated to include some minor cleanups.

An LGPL-licensed portion of GF2X is also part of the CADO-NFS software package.

5.6. CADO-NFS

Participants: Cyril Bouvier, Alain Filbois, Pierrick Gaudry, Alexander Kruppa, Thomas Richard, Emmanuel Thomé [contact], Paul Zimmermann.

CADO-NFS is a program to factor integers using the Number Field Sieve algorithm (NFS), originally developed in the context of the ANR-CADO project (November 2006 to January 2010).

NFS is a complex algorithm which contains a large number of sub-algorithms. The implementation of all of them is now complete, but still leaves some places to be improved. Compared to existing implementations, the CADO-NFS implementation is already a reasonable player. Several factorizations have been completed using our implementation.

Since 2009, the source repository of CADO-NFS is publicly available for download, and is referenced from the software page at http://cado-nfs.gforge.inria.fr/. A major new release, CADO-NFS 2.1, was published in July 2014, with a bug-fix release (2.1.1) in October. Among the main improvements, the polynomial selection now runs in two stages, several unit tests have been added, various small speed-ups and bug fixes.

More and more people use CADO-NFS to perform medium to large factorizations. In February, Fabien Perigaud and Cédric Pernet from Cassidian Cybersecurity reverse-engineered a ransomware, which in the end boiled down to factoring numbers with CADO-NFS.

5.7. Belenios

Participants: Pierrick Gaudry, Stéphane Glondu [contact].

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 [18], [23].

This new version has been implemented by Stéphane Glondu [1]. The first public release has been done in January 2014. In the last public release (April 2014), BELENIOS still uses a major component of the Helios system, the booth. Since then, the booth has been reimplemented but is not yet part of a public release. This development version of BELENIOS has been used in December 2014 for selecting photos of LORIA's calendar (187 persons voted for 0 to 6 pictures, within a set of 52 choices).

5.8. CMH

Participant: Emmanuel Thomé [contact].

In collaboration with the LFANT project-team, INRIA Bordeaux – Sud-Ouest, we develop the CMH software package and library, which holds code for computing Igusa class polynomials. Those characterize principally polarized abelian varieties of dimension 2 having complex multiplication by the ring of integers of a quartic CM field.

The source repository of CMH is publicly available for download, and is referenced from the software page at http://cmh.gforge.inria.fr/.

Version 1.0 has been released in March 2014, simultaneously with the publication of a computation record.

5.9. Platforms

5.9.1. 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.

6. New Results

6.1. Highlights of the Year

Razvan Barbulescu, ex-PhD student in the team, has received the award "Prix Le Monde de la recherche universitaire", as one of the top-5 PhD thesis in exact science in 2014.

Emmanuel Thomé has received the "Prix Régional du Chercheur" of the Région Lorraine.

Emmanuel Thomé has received the "Prix de l'Association des Amis de l'Université de Lorraine".

BEST PAPER AWARD :

[17] **A heuristic quasi-polynomial algorithm for discrete logarithm in finite fields of small characteristic in Eurocrypt 2014**. R. BARBULESCU, P. GAUDRY, A. JOUX, E. THOMÉ.

[1] http://belenios.gforge.inria.fr/

6.2. Discrete logarithm computation in a prime finite field of 180 decimal digits

Participants: Cyril Bouvier, Pierrick Gaudry, Hamza Jeljeli, Emmanuel Thomé [contact].

In the context of the CATREL ANR project, we performed a new computation of a discrete logarithm modulo a 180 digit (596-bit) prime using the number field sieve algorithm. Previous records were 135-digit (448 bits, done in 2006) and 160-digit (530-bit, done in 2007) primes. This is, to date, the largest computation in a prime field. In total, this took the equivalent of 130 years on one CPU core.

6.3. Discrete logarithm in finite fields of small extension degree

Participant: Pierrick Gaudry [contact].

Together with Razvan Barbulescu (CNRS, IMJ-PRG), Aurore Guillevic and François Morain (GRACE project-team), we investigated the discrete logarithm problem in the case of finite fields of the form $\mathbb{F}_{p^n}$, where $n > 1$ is a small integer. We proposed in a preprint — a part of which was accepted to Eurocrypt 2015 — various theoretical and practical improvements [25]:

- new methods for selecting polynomials,
- better (heuristic) asymptotic complexity in the case where $n \approx \log p$, and
- use of algebraic number theory to show that in some cases we can skip the Schirokauer maps.

We have adapted CADO-NFS in order to perform a record computation in a field of the form $\mathbb{F}_{p^2}$, where p^2 has 180 digits. To our knowledge, this is the first time that the number field sieve algorithm is used in practice for record-size computations in this type of fields.

6.4. Igusa class polynomials computation for class number 20,016

Participant: Emmanuel Thomé [contact].

In collaboration with the LFANT project-team, Emmanuel Thomé and Andreas Enge completed the computation of Igusa class polynomials for a quartic CM field whose Igusa class number is 20,016. That is more than 20 times more than the previous state of the art. This has been made possible with the CMH software, which corresponds to the article [10].

6.5. Isogeny graphs for curves with maximal real multiplication

Participant: Emmanuel Thomé [contact].

Emmanuel Thomé and Sorina Ionica (currently with the LFANT project-team) worked on a new algorithm for computing isogeny graphs for Jacobians of curves having the special property that the intersection of their endomorphism ring with its real subfield is maximal. The resulting algorithm is the first depth-first algorithm for this task. This work has been submitted [29].

6.6. Polynomial selection for the Number Field Sieve

Participants: Cyril Bouvier, Nicholas Coxon, Alexander Kruppa, Paul Zimmermann [contact].

A new polynomial selection algorithm for GNFS (General Number Field Sieve) has been described in a preprint [24] and implemented in CADO-NFS. We demonstrate the efficiency of this algorithm by exhibiting a better polynomial than the one used for the factorization of RSA-768, and a polynomial for RSA-1024 that outperforms the best published one.

Montgomery's method of polynomial selection for GNFS has been analysed in a preprint [27]. Criteria for the selection of good parameters for Montgomery's method are given, and the existence of the modular geometric progressions used in the method is considered.

6.7. Beyond double precision

Participant: Paul Zimmermann [contact].

A project entitled “Beyond Double Precision” (BeDoP) has been submitted to the European Research Council (ERC) for funding (advanced grant category). The BeDoP project will (i) demonstrate the limits of double precision on large-scale applications, (ii) make multiple-precision tools easier to use in modern computer languages, and (iii) improve the efficiency and robustness of those tools, in particular by using formal proof techniques. Our dream with the BeDoP project is that scientific computations on exascale computers will no longer give very fast and very wrong results, but instead give very fast and very accurate results.

6.8. Gröbner bases for sparse algebraic systems

Participant: Pierre-Jean Spaenlehauer [contact].

In collaboration with Jean-Charles Faugère and Jules Svartz (POLSYS project-team), new Gröbner bases algorithms have been proposed in [20] to solve efficiently sparse systems of multivariate polynomial equations. Moreover, new complexity bounds have also been proved; they extend in a unified way previous bounds known for solving multi-homogeneous systems with Gröbner bases. For such systems, a proof-of-concept prototype implementation of these algorithms achieves large speed-ups compared to state-of-the-art optimized Gröbner bases algorithms.

6.9. Faster index calculus in algebraic curves

Participant: Maike Massierer [contact].

A possible application of the new ideas speeding up the function field sieve algorithm to index calculus in Jacobians of algebraic curves of large genus has been studied in [30]. Based on a number of practical experiments as well as theoretical considerations, a conjecture has been formulated. It implies that the new ideas only apply to curves which are not interesting in the context of the discrete logarithm problem.

6.10. FFS factory

Participant: Jérémie Detrey [contact].

An extension of Coppersmith’s “factorization factory” and Barbulescu’s “discrete logarithm factory” to the Function Field Sieve was proposed, dubbed the “FFS factory” [28]. The idea is to batch discrete logarithm computations in finite fields of different extension degrees, sharing the sieving step on the algebraic side between all these finite fields. A careful analysis proved that this approach can be used to lower the overall asymptotic complexity. This was also illustrated with a practical experiment in which the discrete logarithm problem was solved for all of the 50 binary fields of the form $\mathbb{F}_{2^n}$ with n odd ranging from 601 to 699.

7. Bilateral Contracts and Grants with Industry

7.1. Bilateral Contracts with Industry

7.1.1. Training and Consulting with HTCS

Participants: Pierrick Gaudry, Emmanuel Thomé [contact].

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. Partnerships and Cooperations

8.1. 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.

8.1.1. 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. Four meetings have taken place already: in Nancy on December 14, 2012 (kick-off), in Palaiseau on June 19, 2013, in Montpellier on November 12-13, 2013, and in Nancy in June 18-19, 2014.

8.2. International Research Visitors

8.2.1. Visits of International Scientists

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

9. Dissemination

9.1. Promoting Scientific Activities

9.1.1. Scientific events organisation

9.1.1.1. Steering committee membership

- Pierrick Gaudry is a member of the steering committee of the ECC (Elliptic Curve Cryptography) conference series.
- Emmanuel Thomé is a member of the steering committee of the ANTS (Algorithmic Number Theory Symposium) conference series (which gathers the program committee chairs and proceedings editors of previous conference editions).

9.1.2. Scientific events selection

9.1.2.1. Conference program committee chairing

- Jérémie Detrey was program chair for the poster session of the *Conférence en Parallélisme, Architecture et Système* (ComPAS 2014).

9.1.2.2. Conference program committee membership

- Jérémie Detrey was a member of the program committee of
  - the architecture track of the *Conférence en Parallélisme, Architecture et Système* (ComPAS 2014),
  - the Third International Conference on Cryptology and Information Security in Latin America (Latincrypt 2014).
- Pierrick Gaudry was a member of the program committee of
  - the 18th International Conference on Practice and Theory of Public-Key Cryptography (PKC 2015),
  - the 5th International Workshop on the Arithmetic of Finite Fields (WAIFI 2014).
- Emmanuel Thomé was a member of the program committee of

  - Selected Areas in Cryptography (SAC 2014),
  - the Third International Conference on Cryptology and Information Security in Latin America (Latincrypt 2014).
- Marion Videau was a member of the program committee of
  - Selected Areas in Cryptography (SAC 2014),
  - the 17th Annual International Conference on Information Security and Cryptology (ICISC 2014),
  - the *Symposium sur la sécurité des technologies de l'information et des communications* (SSTIC 2014).

9.1.2.3. Reviewing activities

- Jérémie Detrey reviewed submissions to
  - the architecture track of the *Conférence en Parallélisme, Architecture et Système* (ComPAS 2014),
  - Selected Areas in Cryptography (SAC 2014),
  - the Third International Conference on Cryptology and Information Security in Latin America (Latincrypt 2014),
  - the 16th Workshop on Cryptographic Hardware and Embedded Systems (CHES 2014),
  - the 6th International Conference on Post-Quantum Cryptography (PQCrypto 2014).
- Pierre-Jean Spaenlehauer reviewed submissions to
  - the 39th International Symposium on Symbolic and Algebraic Computation (ISSAC 2014),
  - Symbolic-Numeric Computation (SNC 2014).
- Hugo Labrande reviewed submissions to
  - Selected Areas in Cryptography (SAC 2014).
- Pierrick Gaudry reviewed submissions to
  - the 20th Annual International Conference on the Theory and Application of Cryptology and Information Security (Asiacrypt 2014),
  - the 12th International Conference on Applied Cryptography and Network Security (ACNS 2014).
- Emmanuel Thomé reviewed submissions to
  - Selected Areas in Cryptography (SAC 2014),
  - the Third International Conference on Cryptology and Information Security in Latin America (Latincrypt 2014),
  - the 33rd Annual International Conference on the Theory and Applications of Cryptographic Techniques (Eurocrypt 2014),
  - the 34rd International Cryptology Conference (Crypto 2014),
  - the 39th International Symposium on Symbolic and Algebraic Computation (ISSAC 2014).
- Marion Videau reviewed submissions to
  - Selected Areas in Cryptography (SAC 2014),
  - the 17th Annual International Conference on Information Security and Cryptology (ICISC 2014),
  - the *Symposium sur la sécurité des technologies de l'information et des communications* (SSTIC 2014).

9.1.3. Journal activities

9.1.3.1. Editorial board membership

- Pierrick Gaudry is an editor of the journal Applicable Algebra in Engineering, Communication and Computing.

9.1.3.2. Reviewing activities

- Jérémie Detrey reviewed submissions to
  - the IEEE Transactions on Computers (IEEE TC),
  - the Journal of Cryptographic Engineering (JCEN),
  - the ACM Transactions on Mathematical Software (TOMS).
- Pierre-Jean Spaenlehauer reviewed submissions to Designs, Codes and Cryptography.
- Paul Zimmermann reviewed submissions to Mathematics of Computation, and declined several reviews for open-access and hybrid journals.
- Pierrick Gaudry reviewed submissions to Finite field and their applications and Mathematics of Computation.
- Emmanuel Thomé reviewed submissions to Designs, Codes, and Cryptography and Security and Communication Networks.

9.1.4. Invited Conferences

- Pierrick Gaudry gave invited talks at
  - the DLP 2014 workshop, in Ascona (Switzerland, May);
  - the SAC 2014 conference, in Montreal (Canada, August);
  - the *Journées nationales du calcul formel 2014*, in Marseilles (November).
- Emmanuel Thomé gave invited talks at
  - the ECC 2014 conference, in Chennai (India, October);
  - the *Journées nationales du GDR IM 2014*, in Paris (January);
  - the *École de printemps Codage et Cryptographie 2014*, in Grenoble (March);
  - the *Journées de Sécurité des Systèmes d'information*, in Rouen (November).
- Pierre-Jean Spaenlehauer gave invited talks at
  - the *Journées nationales Codage et Cryptographie 2014*, in Les Sept Laux (March);
  - the conference on Effective Moduli Spaces and Applications to Cryptology, in Rennes (June).

9.1.5. Other committees

- Pierrick Gaudry was a member of
  - the hiring committees for *chargé de recherche* positions in INRIA Nancy – Grand Est, and associate professor positions in Univ. Lorraine and Univ. Montpellier 2.
- Marion Videau was a member of
  - the scientific committee of the CCA seminar (*Codage, Cryptologie, Algorithmes*),
  - the scientific committee of the *Journées Codage et Cryptographie* of GT-C2 of GdR-IM,
  - the LORIA laboratory council (elected),
  - the *Commission des développements technologiques* (CDT) of the INRIA Nancy – Grand Est research center,
  - hiring committee for an associate professor position in Univ. Lorraine,
  - hiring committee for temporary teaching and research attaché (ATER) positions in Univ. Lorraine,

  - hiring committee for teaching contracts for PhD students (DCCE) in Univ. Lorraine,
  - admission committee for student applications for a master degree in informatics in Nancy.
- Paul Zimmermann was a member of
  - the *jury d'admissibilité* for *chargé de recherche 1e classe* and *directeur de recherche 2e classe* positions at Inria, and the *jury d'admission* for *directeur de recherche 2e classe* positions at Inria.

9.1.6. Seminar organization

9.1.6.1. Caramel seminar

Ten speakers were invited to our seminar in 2014: Armand Lachand, Pierre-Jean Spaenlehauer, Guillaume Moroz, Irene Márquez-Corbella, Nicholas Coxon, Christian Eder, Andrea Miele, Thomas Richard, Enea Milio, and Sebastian Kochinke.

9.1.6.2. Joint security seminar with the university master in informatics

The team is involved with other teams and the university master in informatics in the organization of the security seminar which started in 2013. Fourteen speakers were invited during 2014: Éric Leblond, Philippe Biondi, Eric Jaeger, Pierre-Michel Ricordel, Pascal Urien, Jérôme François, Thomas Voegtlin, Mathieu Cunche, Sébastien Bardin, Gwendall Legrand, Pierrick Gaudry, Sylvain Ruhault, Aline Gouget, and Raphaël Rigo.

9.2. Teaching - Supervision - Juries

9.2.1. Teaching

Licence:

Jérémie Detrey, Security of websites, 2 hours, L1, IUT Charlemagne, Nancy, France.

Marion Videau, Introduction to algorithmic and programming, 16 hours, L1, Faculté des sciences et technologies, Vandœuvre-lès-Nancy, France.

Marion Videau, Programming methodology in C, 21 hours (lectures and tutorial sessions), L1, Faculté des sciences et technologies, Vandœuvre-lès-Nancy, France.

Marion Videau, Introduction to cryptology and information security, 20 hours (lectures and tutorial sessions), L3, Faculté des sciences et technologies, Vandœuvre-lès-Nancy, France.

Marion Videau, student supervisor (for about 12 L1 students): 12 hours, L1, Faculté des sciences et technologies, Vandœuvre-lès-Nancy, France.

Master:

Marion Videau and Pierrick Gaudry, Supervision of two M1 students for their *Introduction to research* practical course throughout one semester, M1, Faculté des sciences et technologies, Vandœuvre-lès-Nancy, France.

Marion Videau, Introduction to cryptology, 12 hours (lectures), M1, Faculté des sciences et technologies, Vandœuvre-lès-Nancy, France.

Marion Videau, Introduction to information system security, 24 hours (lectures and tutorial sessions), M1, Faculté des sciences et technologies, Vandœuvre-lès-Nancy, France.

Marion Videau, Information system security, 12 hours (lectures and tutorial sessions) and responsibility of coordinating with security seminars, M2, Faculté des sciences et technologies, Vandœuvre-lès-Nancy, France.

Marion Videau, Information system security, 21 hours+21 hours (lectures and tutorial sessions), M2, Faculté des sciences et technologies agreement with IGA, Maroc.

Marion Videau, Software validation, verification and certification: 4 hours (tutorial sessions) and responsibility of coordinating external teachers from industry.

Marion Videau and Stéphane Glondu, Supervision of the semester applied project for all M2 students from *parcours Sécurité des Architectures Web*, M2, Faculté des sciences et technologies, Vandœuvre-lès-Nancy, France.

Marion Videau, local supervision of M2 students engineering internships in industry, M2, Faculté des sciences et technologies, Vandœuvre-lès-Nancy, France.

Marion Videau, head of *parcours Sécurité des Architectures Web*, M2, Faculté des sciences et technologies, Vandœuvre-lès-Nancy, France.

Misc.:

Marion Videau, teaching supervisor (*tuteur*), of a PhD student with a teaching contract (DCCE), Faculté des sciences et technologies, Vandœuvre-lès-Nancy, France.

9.2.2. Internships

- David Lucas, Télécom Nancy, "Problème du rang bilinéaire : calcul et recherche de formules optimales", Apr–Sep 2014, supervised by Jérémie Detrey.
- Théo Karaboghossian, École Normale Supérieure de Cachan, "Nombres premiers à faiblesse cachée pour le problème du logarithme discret", Jun–Jul 2014, supervised by Pierrick Gaudry.

9.2.3. Supervision

PhD in progress:

Cyril Bouvier, Algorithmes pour la factorisation d'entiers et le calcul de logarithme discret, since Sep 2012, Paul Zimmermann.

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.

Hamza Jeljeli, Accélérateurs logiciels et matériels pour l'algèbre linéaire creuse sur les corps finis, since Oct 2011, Emmanuel Thomé.

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).

9.2.4. Juries

- Jérémie Detrey was a member of the jury of the ÉNS competitive entrance exam.
- Paul Zimmermann was reviewer and member of the jury for the PhD thesis of Fredrik Johansson (RISC, Linz).
- Pierre-Jean Spaenlehauer was a member of the jury for the PhD thesis of Jules Svartz (EPI POLSYS, Paris).
- Pierrick Gaudry was a reviewer of the PhD thesis of Christophe Tran (Univ. Rennes 1), and a member of the jury for the PhD thesis of Ivan Boyer (Univ. Paris 7).

9.3. Popularization

- Jérémie Detrey gave a presentation on the Enigma machine and its cryptanalysis to high-school teachers as part as the "journée EPI-ISN", where Paul Zimmermann gave a presentation of the Sage computer algebra system.
- Paul Zimmermann animated a "Maths-en-Jeans" group with students from the "collège" Pierre Brossolette in Réhon.
- Pierrick Gaudry gave a presentation at the "journée de l'Association francophone des spécialistes de l'investigation numérique".

- Marion Videau
  - participated to events on information about university studies for pupils and students (Cap sur l'enseignement supérieur, Portes ouvertes de la faculté des sciences, Oriaction), and about university studies and research to the general public (Sciences en marche),
  - gave a presentation at the "journée de l'Association francophone des spécialistes de l'investigation numérique".

10. Bibliography

Major publications by the team in recent years

[1] 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

[2] 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

[3] 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

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

[5] 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

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

Publications of the year

Articles in International Peer-Reviewed Journals

[7] S. Bai, R. Brent, E. Thomé. *Root optimization of polynomials in the number field sieve*, in "Mathematics of Computation", 2014, forthcoming, https://hal.inria.fr/hal-00919367

[8] C. Bouvier, P. Zimmermann. *Division-Free Binary-to-Decimal Conversion*, in "IEEE Transactions on Computers", August 2014, vol. 63, n^o 8, pp. 1895-1901 [*DOI :* 10.1109/TC.2014.2315621], https://hal.inria.fr/hal-00864293

[9] R. Cosset, D. Robert. *Computing (l,l)-isogenies in polynomial time on Jacobians of genus 2 curves*, in "Mathematics of Computation", November 2014, 23 p. , forthcoming [*DOI :* 10.1090/S0025-5718-2014-02899-8], https://hal.archives-ouvertes.fr/hal-00578991

[10] A. ENGE, E. THOMÉ. *Computing class polynomials for abelian surfaces*, in "Experimental Mathematics", 2014, vol. 23, pp. 129-145 [*DOI :* 10.1080/10586458.2013.878675], https://hal.inria.fr/hal-00823745

[11] E. GIOAN, S. BURCKEL, E. THOMÉ. *Computation with No Memory, and Rearrangeable Multicast Networks*, in "Discrete Mathematics and Theoretical Computer Science", February 2014, vol. 16, n^{o} 1, pp. 121-142, http://hal-lirmm.ccsd.cnrs.fr/lirmm-00959964

[12] G. OTTAVIANI, P.-J. SPAENLEHAUER, B. STURMFELS. *Exact Solutions in Structured Low-Rank Approximation*, in "SIAM Journal on Matrix Analysis and Applications", 2014, vol. 4, pp. 1521-1542, https://hal.archives-ouvertes.fr/hal-00953702

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

[14] P.-J. SPAENLEHAUER. *On the Complexity of Computing Critical Points with Gröbner Bases*, in "SIAM Journal on Optimization", 2014, vol. 24, n^{o} 3, pp. 1382-1401, 25 pages, https://hal.archives-ouvertes.fr/hal-01017032

International Conferences with Proceedings

[15] 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

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

[17] *Best Paper*
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.

[18] 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

[19] J.-C. FAUGÈRE, P. GAUDRY, L. HUOT, G. RENAULT. *Sub-cubic Change of Ordering for Gröner Basis: A Probabilistic Approach*, in "ISSAC '14 - Proceedings of the 39th International Symposium on Symbolic and Algebraic Computation", Kobe, Japan, ISSAC '14, ACM, July 2014, pp. 170–177 [*DOI :* 10.1145/2608628.2608669], https://hal.inria.fr/hal-01064551

[20] J.-C. FAUGÈRE, P.-J. SPAENLEHAUER, J. SVARTZ. *Sparse Gröbner Bases: the Unmixed Case*, in "ISSAC 2014", Kobe, Japan, July 2014, 20 pages, Corollary 6.1 has been corrected [*DOI :* 10.1145/2608628.2608663], https://hal.archives-ouvertes.fr/hal-00953501

[21] H. JELJELI. *Accelerating Iterative SpMV for Discrete Logarithm Problem Using GPUs*, in "International Workshop on the Arithmetic of Finite Fields WAIFI 2014", Gebze, Turkey, September 2014, https://hal.inria.fr/hal-00734975

[22] H. JELJELI. *Resolution of Linear Algebra for the Discrete Logarithm Problem Using GPU and Multi-core Architectures*, in "Euro-Par 2014 Parallel Processing", Porto, Portugal, August 2014, https://hal.inria.fr/hal-00946895

Research Reports

[23] V. CORTIER, D. GALINDO, S. GLONDU, M. IZABACHÈNE. *Election Verifiability for Helios under Weaker Trust Assumptions*, June 2014, n^{o} RR-8555, 20 p. , https://hal.inria.fr/hal-01011294

Other Publications

[24] S. BAI, C. BOUVIER, A. KRUPPA, P. ZIMMERMANN. *Better polynomials for GNFS*, September 2014, https://hal.inria.fr/hal-01089507

[25] R. BARBULESCU, P. GAUDRY, A. GUILLEVIC, F. MORAIN. *Improvements to the number field sieve for non-prime finite fields*, November 2014, https://hal.inria.fr/hal-01052449

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

[27] N. COXON. *Montgomery's method of polynomial selection for the number field sieve*, December 2014, https://hal.inria.fr/hal-01097069

[28] J. DETREY. *FFS Factory: Adapting Coppersmith's "Factorization Factory" to the Function Field Sieve*, May 2014, https://hal.inria.fr/hal-01002419

[29] S. IONICA, E. THOMÉ. *Isogeny graphs with maximal real multiplication*, March 2014, https://hal.archives-ouvertes.fr/hal-00967742

[30] M. MASSIERER. *Some experiments investigating a possible L(1/4) algorithm for the discrete logarithm problem in algebraic curves*, December 2014, https://hal.inria.fr/hal-01097362

References in notes

[31] 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/

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