IN PARTNERSHIP WITH:
CNRS

Université de Lorraine

Activity Report 2013

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

1. Members **1**
2. Overall Objectives **1**
2.1. Introduction 1
2.2. Highlights of the Year 2
3. Research Program **3**
4. Application Domains **4**
4.1. Cryptology 4
4.1.1. Cryptography 5
4.1.2. Cryptanalysis 5
4.2. Computer Algebra Systems 5
4.2.1. Magma 6
4.2.2. Pari-GP 6
4.2.3. Sage 6
4.3. Standardization 6
5. Software and Platforms **6**
5.1. Introduction 6
5.2. GNU MPFR 6
5.3. GNU MPC 7
5.4. GMP-ECM 7
5.5. Finite Fields 7
5.6. gf2x 8
5.7. CADO-NFS 8
5.8. Belenios 8
6. New Results **9**
6.1. Computation of Discrete Logarithms in $\mathrm{GF}(\mathbf{2^{809}})$ 9
6.2. A Quasi-polynomial Algorithm for the Computation of Discrete Logarithms in Finite Fields of Small Characteristic 9
6.3. Computation of CM Class Polynomials for Genus 2 Jacobians 10
6.4. Binary to Decimal Conversion 10
6.5. Fast Change of Ordering for Gröbner Bases 10
7. Bilateral Contracts and Grants with Industry **10**
7.1. Training and Consulting with HTCS 10
7.2. Study of the Kalray MPPA-256 Processor for Applications in Cryptology 10
7.3. Study of the electronic voting system of Voxaly 11
8. Partnerships and Cooperations **11**
8.1. Regional Initiatives 11
8.2. National Initiatives 11
8.2.1. ANR CATREL (Cribles: Améliorations Théoriques et Résolution Effective du Logarithme discret) 11
8.2.2. GDR-IM supported travel for PhD students 12
8.3. International Research Visitors 12
9. Dissemination **12**
9.1. Scientific Animation 12
9.1.1. Caramel seminar 12
9.1.2. Joint security seminar with the university master in informatics 12
9.1.3. Committees memberships 12
9.1.4. Invited Conferences 13
9.1.5. Calcul mathématique avec Sage 13
9.2. Teaching - Supervision - Juries 13

9.2.1. Teaching 13
9.2.2. Internships 14
9.2.3. Supervision 14
9.2.4. Juries 15
9.3. Popularization 15
10. Bibliography **15**

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]
Emmanuel Thomé [Inria, Researcher, HdR]
Paul Zimmermann [Inria, Senior Researcher, HdR]

Faculty Member
Marion Videau [Univ. Lorraine, Associate Professor]

External Collaborator
Luc Sanselme [Ministère de l'Éducation Nationale]

Engineers
Stéphane Glondu [Research Engineer, 50% with the Cassis team]
Alexander Kruppa [Inria, ADT grant until September 2014]

PhD Students
Razvan Barbulescu [Université de Lorraine; defended on 2013/12/04]
Cyril Bouvier [Université de Lorraine; started in September 2012]
Nicolas Estibals [ATER, ENS Lyon; defended on 2013/10/30]
Hamza Jeljeli [Université de Lorraine; started in October 2011]
Laurent Gremy [Université de Lorraine; started in October 2013]
Hugo Labrande [Université de Lorraine; cotutelle with University of Calgary; started in September 2013]

Visiting Scientist
Shi Bai [University of Auckland, Jun 2013]

Administrative Assistants
Emmanuelle Deschamps [Inria]
Aurélie Adam [Univ. Lorraine]

Others
Svyatoslav Covanov [École Polytechnique, intern, from Apr 2013 until Jul 2013]
David Lucas [Télécom Nancy, intern, from May 2013 until Jul 2013]
Fabien Nollet [Télécom Nancy, intern, from May 2013 until Jul 2013]
Alice Pellet Mary [ENS Lyon, intern, from Jun 2013 until Jul 2013]
Alexandre Talon [ENS Lyon, intern, from Jun 2013 until Jul 2013]
Sébastien Vandeneeckhoutte [Inria, intern, from Feb 2013 until Jun 2013]

2. Overall Objectives

2.1. Introduction

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 known algorithm for factoring large RSA-like integers, and for solving discrete logarithms in prime finite fields. A sibling algorithm, the function field sieve (FFS), is the best known algorithm for computing discrete logarithms in finite fields of small characteristic.

  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.

  For pairings, our principal concern is the optimization of pairing computations, in particular in hardware, or in constrained environments. Given the computational overhead incurred by prime-field arithmetic, we focus on supersingular elliptic and hyperelliptic curves defined over small-characteristic fields, and target the recommended 128-bit level of security.

- 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.

2.2. Highlights of the Year

- A spectacular new result has been obtained in the context of the cryptanalysis of the discrete logarithm problem in certain types of fields [22]. The complexity for solving this hard problem has been reduced from « sub-exponential » complexity, roughly $\exp(O(n^{1/3}))$ for an input size n, to the much lower « quasi-polynomial » complexity written as $\exp(O((\log n)^2))$. As a result, a whole range of cryptographic proposals have lost momentum, notably proposals related to pairing-based cryptography over small characteristic fields.
- Still in the realm of the computation of discrete logarithm, a new record computation has been completed by the team for binary fields of *prime* extension degree [15], using the Function Field Sieve algorithm. This establishes a useful comparison point between the Function Field Sieve and the newly proposed algorithm discussed above.

- The 2.0 release of the CADO-NFS software package, developed by the team, was made available in november. This releases incorporates an important number of improvements over the previous release which was 2 years earlier. CADO-NFS is available from the project page http://cado-nfs.gforge.inria.fr/.

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-known algorithms for factoring integers or for computing discrete logarithms in finite fields have a subexponential complexity, whereas the best known attack 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 or the BSI, 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 (HFE, 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 [30], 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), and a large deployment is to be expected in the next years.

Despite the raise of elliptic curve cryptography and the variety of more or less mature other 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 want to 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.

We also plan to investigate and promote the use of pairing-based and genus-2 cryptosystems. For pairings, this is mostly a question of how efficient can such a system be in software, in hardware, and using all the tools from fast implementation to the search for adequate curves. For genus 2, as said earlier, constructing an efficient cryptosystem requires some more fundamental questions to be solved, namely the point-counting problem.

We summarize in the following table the aspects of public-key cryptography that we address in the CARAMEL team.

public-key primitive	cryptanalysis	design	implementation
RSA	X	–	–
Finite Field DLog	X	–	–
Elliptic Curve DLog	–	–	Soft
Genus 2 DLog	–	X	Soft
Pairings	X	X	Soft/Hard

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 have more and more 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 possible hardware platforms intended, 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 others 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 document from governmental agencies (see e.g. [29]) 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]

Implementations of curve-based cryptography, both in hardware and software, are a necessary step on the way to assessing cryptographic speed. We plan to provide such implementations. In particular, on the hardware side, one of our goals is the design of a complete cryptographic coprocessor, including all the primitives for curve-based and pairing-based cryptography, providing optimized and configurable efficiency vs area trade-off. Such work has been proposed in [1].

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 $\mathrm{GF}(2^{809})$ [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 [22] 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 — a few 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 the goal of 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. 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, with the departure of Vincent Lefèvre to ENS Lyon, 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.

Several software systems use GNU MPFR, for example: the GCC and GFORTRAN compilers; the SAGE computer algebra system; the KDE calculator Abakus by Michael Pyne; CGAL (Computational Geometry Algorithms Library) developed by the Geometrica project-team (INRIA Sophia Antipolis - Méditerranée); Gappa, by Guillaume Melquiond; Sollya, by Sylvain Chevillard, Mioara Joldeş and Christoph Lauter; Genius Math Tool and the GEL language, by Jiri Lebl; Giac/Xcas, a free computer algebra system, by Bernard Parisse; the iRRAM exact arithmetic implementation from Norbert Müller (University of Trier, Germany); the Magma computational algebra system; and the Wcalc calculator by Kyle Wheeler.

The main development in 2013 is the release of version 3.1.2 (the "canard à l'orange" release) in March. This version fixes a few bugs from previous version.

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.

No new version of GNU MPC was released in 2013, which confirms the status of mature library.

5.4. GMP-ECM

Participants: Cyril Bouvier, Paul Zimmermann [contact].

GMP-ECM is a program to factor integers using the Elliptic Curve Method. Its efficiency comes both from the use of the GMP library, and from the implementation of state-of-the-art algorithms. GMP-ECM contains a library (LIBECM) in addition to the binary program (ECM). The binary program is distributed under GPL, while the library is distributed under LGPL, to allow its integration into other non-GPL software. The Magma computational number theory software and the SAGE computer algebra system both use LIBECM.

In February 2013, a new version 6.4.4 was released. Apart from bug fixes, this new release provides some improvements (better integration of the GPU code, of the new *-batch* option, ...).

In September 2013, a new record prime of 83 digits was found by R. Propper using GMP-ECM.

5.5. Finite Fields

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

$\texttt{mp}\mathbb{F}_q$ is (yet another) library for computing in finite fields. The purpose of $\texttt{mp}\mathbb{F}_q$ 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*. $\texttt{mp}\mathbb{F}_q$ can adapt to finite fields of any characteristic and any extension degree. However, one of the targets being the use in cryptology, $\texttt{mp}\mathbb{F}_q$ somehow focuses on prime fields and on fields of characteristic two.

When it was first written in 2007, $\texttt{mp}\mathbb{F}_q$ 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 $\texttt{mp}\mathbb{F}_q$ 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 $\texttt{mp}\mathbb{F}_q$ consists of roughly 18,000 lines of Perl code, which generate most of the `C` code. $\texttt{mp}\mathbb{F}_q$ is distributed at http://mpfq.gforge.inria.fr/.

In 2013, version 1.1 of $\texttt{mp}\mathbb{F}_q$ has been released. This new release includes new assembly code by Luc Sanselme providing optimized arithmetic over fields whose characteristic fits in a number of bits which fit within half-word boundaries.

In 2013, Hamza Jeljeli collaborated with Bastien Vialla from LIRMM, Montpellier to integrate experimental code based on RNS arithmetic (Residue Number System), intending to provide back-end functionality for the linear algebra code in CADO-NFS. This feature set is still experimental.

5.6. 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 processors instruction (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.

In 2013, the development version of GF2X has been updated to incorporate detection of Intel Haswell micro-processors, which provide much improved performance for the PCLMULQDQ instruction (this instruction if of utmost importance for GF2X).

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

5.7. CADO-NFS

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

CADO-NFS is a program to factor integers using the Number Field Sieve algorithm (NFS), originally developped 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 implementations.

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 2.0, was published in November 2013. The client/server framework was completely rewritten to allow the use of CADO-NFS routinely on clusters of 100 to 1000 nodes.

More and more people use CADO-NFS to perform medium to large factorizations. Also in 2013 some researchers in the field wrote some papers where they study the implementation and default parameters of CADO-NFS. This is very useful feedback from the scientific community.

5.8. 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 particylar 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 cretentials that the ballot box can verify but bot forge.

This new version has been implemented by Stéphane Glondu [1]. and has been tested in July 2013 in a mock election in the teams CASSIS and CARAMEL.

6. New Results

6.1. Computation of Discrete Logarithms in $\mathrm{GF}(2^{809})$

Participants: Razvan Barbulescu, Cyril Bouvier, Jérémie Detrey, Pierrick Gaudry, Hamza Jeljeli, Emmanuel Thomé [contact], Marion Videau, Paul Zimmermann.

In the context of the CATREL ANR project, most team members contributed to the achievement of a new record computation for discrete logarithms in $\mathrm{GF}(2^{809})$, with the Function Field Sieve (FFS) algorithm. This is, to date, the largest computation in a binary field of prime extension degree. Beyond the experimental data and the improvements related to "what it takes" to beat such a record, this work provides very useful basis information towards the assessment of the cut-off with the novel quasi-polynomial algorithm discussed below.

This work has been reported in the article [15], accepted for publication in the conference PKC 2014 (Public Key Cryptography). It was the occasion to illustrate several contributions of members of the teams to various phases of the algorithm: Răzvan Bărbulescu [21] analyzed the polynomial selection step for FFS; Jérémie Detrey, Pierrick Gaudry and Marion Videau [17] improved the practical implementation of the relation collection; Cyril Bouvier [23] studied the filtering step; and Hamza Jeljeli [28] proposed to use the Residue Number System representation for the linear algebra step on GPU and CPU.

6.2. A Quasi-polynomial Algorithm for the Computation of Discrete Logarithms in Finite Fields of Small Characteristic

Participants: Razvan Barbulescu, Pierrick Gaudry, Emmanuel Thomé [contact].

In collaboration with Antoine Joux (Université Pierre et Marie Curie), Răzvan Bărbulescu, Pierrick Gaudry, and Emmanuel Thomé designed a new algorithm of quasi-polynomial complexity for computing discrete logarithms in finite fields $\mathrm{GF}(p^n)$, under the constraint that the characteristic p is small: it must not grow faster than a polynomial in the input size $n \log p$. This constraint accomodates for instance the cryptographically relevant case of finite fields of fixed characteristic $\mathrm{GF}(2^n)$ and $\mathrm{GF}(3^n)$.

This new algorithm dramatically changes the complexity landscape of the computation of discrete logarithms in finite fields. This has in particular an immense impact on the small characteristic pairing-based cryptography proposals. As it turns out, the field of definition of the Weil pairing for curves over small characteristic fields lends itself incredibly well to the new algorithm, to the point that the key sizes which are necessary to claim a sufficient security suddenly become unacceptably large. The newly proposed algorithm practically kills such cryptosystems.

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

This work has been published in preprint form in June 2013 [22] and was immediately acclaimed as a breakthrough, receiving also some external publicity. Pending the submission outcome, a first publication is expected in 2014.

6.3. Computation of CM Class Polynomials for Genus 2 Jacobians

Participant: Emmanuel Thomé [contact].

In collaboration with Andreas Enge, Emmanuel Thomé has developed software for computing class polynomials, in the context of complex multiplication theory in genus 2. The current computations set new records which are well above the previous state of the art, as Igusa class polynomials for class number above 20,000 have been computed in december 2013 using this software. An article describing this work has been accepted for publication in *Experimental Mathematics* [11].

Using similar underlying tools and theory, and based on work by Sorina Ionica [13], Sorina Ionica and Emmanuel Thomé have worked on the analysis of isogeny graphs in genus 2, when certain properties of the endomorphism ring are satisfied. A publication is being worked on, and is expected to be submitted in early 2014.

6.4. Binary to Decimal Conversion

Participants: Cyril Bouvier, Paul Zimmermann.

Cyril Bouvier and Paul Zimmermann designed a new algorithm to convert a large binary integer to decimal (or more generally any non-power-of-two radix). Compared to the reference implementation in GNU MP, this algorithm replaces divisions by multiplications, and exhibits a speedup of up to a factor of two (or more) in some cases [24].

6.5. Fast Change of Ordering for Gröbner Bases

Participant: Pierrick Gaudry.

When solving polynomial systems, the usual approach is to compute a Gröbner basis for a monomial order that is compatible with the degree with the F4 or F5 algorithm, and then compute a Gröbner basis for the lexicographical order using the FGLM algorithm. In collaboration with Jean-Charles Faugère, Louise Huot and Guénaël Renault, Pierrick Gaudry designed another approach [27] for this second step, leading to a better asymptotic complexity: the cubic complexity is replaced by the complexity of the linear algebra where the exponent can theoretically be as small as 2.37.

7. Bilateral Contracts and Grants with Industry

7.1. 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 and 2014.

7.2. Study of the Kalray MPPA-256 Processor for Applications in Cryptology

Participants: Jérémie Detrey, Pierrick Gaudry [contact].

A 5-month contract has been signed between CARAMEL (through Inria) and Kalray, a French company which has recently designed and manufactured the MPPA-256 processor, a 256-core VLIW architecture targeted at embedded applications. The objective of this contract was to study the performance of this processor in a cryptographic context. Several key arithmetic primitives, such as multi-precision modular arithmetic or polynomial multiplication in binary and ternary fields, were implemented and optimized to take advantage of the specific micro-architecture and instruction set of the VLIW cores of the MPPA-256. The results are encouraging and prompt us to explore further the possible benefits of this processor for cryptanalytic applications.

7.3. Study of the electronic voting system of Voxaly

Participants: Pierrick Gaudry, Stéphane Glondu [contact].

A 4-month contract has been signed between CARAMEL, CASSIS and Voxaly, a French company who is proposing solutions for the organization of on-line elections. During several meetings, we discussed their current solution and proposed improvements to gradually add security features that get close to the academic standards.

8. Partnerships and Cooperations

8.1. Regional Initiatives

8.1.1. Function field sieve: implementation and hardware acceleration

Participants: Jérémie Detrey [contact], Pierrick Gaudry, Hamza Jeljeli, Emmanuel Thomé.

The team has obtained for the years 2012 and 2013 a financial support from the Région Lorraine and Inria for a project focusing on the hardware implementation and acceleration of the function field sieve (FFS).

The FFS algorithm is currently the best known method to compute discrete logarithms in small-characteristic finite fields, such as may occur in pairing-based cryptosystems. Its study is therefore crucial to accurately assess the key-lengths which such cryptosystems should use. More precisely, this project aims at quantifying how much this algorithm can benefit from recent hardware technologies such as GPUs or CPU-embedded FPGAs, and how this might impact current key length recommendations.

While the more FPGA-related aspects of this project were put on hold in 2013, the GPU option was explored further. To this end, eight NVIDIA GeForce GTX 680 graphics cards were bought and installed in four nodes connected by an InfiniBand. Hamza Jeljeli was able to extend his GPU implementation of sparse linear algebra routines so as to take multi-GPU and multi-node computations into account. This setup was for instance used to break the discrete-logarithm record over an 809-bit binary field [15].

8.2. National Initiatives

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

8.2.1. ANR CATREL (Cribles: Améliorations Théoriques et Résolution Effective du Logarithme discret)

Participants: Razvan Barbulescu, Cyril Bouvier, Jérémie Detrey, Pierrick Gaudry, 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 the 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. Three meetings have taken place already: in Nancy on Dec. 14th, 2012 (kick-off), in Palaiseau on June 19, 2013, and in Monpellier on November 12-13, 2013.

8.2.2. GDR-IM supported travel for PhD students

Hamza Jeljeli collaborated with Bastien Vialla from LIRMM, Montpellier to integrate RNS-based code in $\mathtt{mp}\mathbb{F}_q$ and CADO-NFS. This collaboration was funded by the GDR-IM program "visite de doctorants".

8.3. International Research Visitors

8.3.1. Visits of International Scientists

Shi Bai from the univeristy of Auckland, NZ, visited us in June 2013.

Thorsten Kleinjung, from the EPFL, visited us in October 2013.

9. Dissemination

9.1. Scientific Animation

9.1.1. Caramel seminar

Sixteen speakers were invited to our seminar in 2013: Pierre-Jean Spaenlehauer, Maike Massierer, Emmanuel Jeandel, Jérémy Parriaux, Adeline Langlois, Antoine Joux, François Morain, Mourad Gouicem, Hamza Jeljeli, Svyatoslav Covanov, Alice Pellet-Mary, Bastien Vialla, Julia Pieltant, Clément Pernet, Cécile Pierrot, and Luca De Feo.

9.1.2. 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. Six speakers were invited during the last months of 2013: Olivier Heen, Frédéric Raynal, Stéphanie Lacour, Alexandre Dulaunoy, Vincent Strubel and Cédric Blancher.

9.1.3. Committees memberships

- Jérémie Detrey
  - was a member of the program committee of the International Conference on Pairing-Based Cryptography (Pairing 2013).
- Pierrick Gaudry
  - was a member of the program committee of the ASIACRYPT 2013 conference,
  - was in a hiring committee (Comité de Sélection) in Université de Lorraine.
- Emmanuel Thomé
  - is an elected member of the Inria Evaluation Committee for the period 2011-2014,
  - is an elected member of the Inria Nancy *Comité Hygiène, Sécurité, et Conditions de Travail*,
  - is an appointed member of the Inria Nancy *Comité de développement durable*,
  - is a member of the *Bureau du département de formation doctorale* in computer science at Université de Lorraine,

  - was in a hiring committee (Comités de Sélection) in Université de Lorraine,
  - was in the hiring committee for the Inria *Chargé de recherches* positions both in Bordeaux and Rocquencourt.
- Marion Videau
  - is a member of the scientific committee of the CCA seminar (*Codage, Cryptologie, Algorithmes*),
  - is a member of the program committee of the *Symposium sur la sécurité des technologies de l'information et des communications* (SSTIC 2013),
  - was a member of the program committee of the 16th annual International Conference on Information Security and Cryptology (ICISC 2013),
  - is an elected member of the LORIA laboratory council,
  - is a member of the *Commission des développements technologiques* (CDT) of the Inria-NGE research center.
- Paul Zimmermann
  - is an elected member of the Inria Scientific Board,
  - is (from September) "délégué scientifique´´ of the Nancy Grand Est center, and as a consequence member of the Inria Evaluation Committee.

9.1.4. Invited Conferences

- Pierrick Gaudry was invited to give a talk at the Workshop on Elliptic Curve Cryptography (ECC 2013) in Leuven, Belgium and to give two lectures at the Summer School that preceded it; he was invited to give a talk at the Pairing 2013 conference in Beijing, China; he was also invited to give a talk at the Workshop on Emerging Applications of Finite Fields at Linz, Austria.

9.1.5. Calcul mathématique avec Sage

Together with nine other colleagues, Paul Zimmermann wrote a book about doing mathematics with Sage [18]. This book is available in electronic version under a Creative Commons license, and is also available in paper form from Amazon under a very low price.

9.2. Teaching - Supervision - Juries

9.2.1. Teaching

- Jérémie Detrey:
  - Security of websites: 2 hours (lecture), L1, IUT Charlemagne, Nancy, France.
- Pierrick Gaudry
  - Algorithmic Number Theory: 5 hours (lectures), M2, University Paris 7 (Master Parisien de Recherche en Informatique), Paris, France.
- Emmanuel Thomé:
  - Cryptology: 24 hours, M1, ESIAL, Nancy, France.
  - Introduction to cryptology: 3 hours (lecture), M2, École des Mines de Nancy, France.
  - Training for "Informatique et Sciences du Numérique", Cryptology, Networks: 9 h, Université de Lorraine, Nancy, France. (Training for high school teachers who intend to teach this topic in high school).
- Marion Videau, teaching at the faculty of technology and sciences, Université de Lorraine, Nancy, France:
  - Introduction to algorithmic and programming: 40 hours (lectures and tutorial sessions), 20 hours (practical sessions), L1.

- Programming methodology in C: 21 hours (lectures and tutorial sessions), L1.
- Students supervisor for about 12 L1 students: 12 hours, L1.
- Introduction to information system security: 15 hours (lectures), 15 hours (tutorial sessions), M1.
- Information System Security: 21 hours (lectures and tutorial sessions), M2, IGA, Maroc
- Information System Security: 12 hours (lectures and tutorial sessions), M2
- Software Validation, Verification and Certification: 12 hours (lectures and tutorial sessions), M2
- Supervision of two M1 students for their *Introduction to research* practical course throughout one semester
- Supervision of M2 students projects: 15 hours
- Supervision and jury of M2 students internships: 10 hours.
- Responsability of the M2 *parcours Services, Sécurité des Systèmes et des Réseaux / Sécurité des Architectures Web*

9.2.2. Internships

- Svyatoslav Covanov, École Polytechnique, "Fürer's integer multiplication algorithm", Apr–July 2013, supervised by Emmanuel Thomé.
- David Lucas, Télécom Nancy, "Recherche de bitcoins : implémentation et accélération sur le MPPA-256 de Kalray", May–Jul 2013, supervised by Jérémie Detrey.
- Fabien Nollet, Télécom Nancy, "Parallelization of the multiplication of polynomials over $\mathrm{GF}(2)$", May–Jul 2013, supervised by Emmanuel Thomé.
- Alice Pellet Mary, ÉNS Lyon, "Test rapide de cubicité modulaire", Jun–Jul 2013, supervised by Pierrick Gaudry.
- Alexandre Talon, ÉNS Lyon, "Non linear polynomial selection for NFS´´, Jun–Jul 2013, supervised by Paul Zimmermann.
- Sébastien Vandeneeckhoutte, Télécom Nancy, "Énumération efficace des polynômes irréductibles sur un corps fini" Feb–Jun, 2013, supervised by Marion Videau and Pierrick Gaudry.

9.2.3. Supervision

Defended PhDs:

- Nicolas Estibals, "Algorithmes et arithmétique pour l'implémentation de couplages cryptographiques", started in 2009, co-supervised by Jérémie Detrey and Pierrick Gaudry [9]. Defended on 2013/10/30.
- Răzvan Bărbulescu, "Number and function field sieve for discrete logarithm", started in 2011, supervised by Pierrick Gaudry [8]. Defended on 2013/12/04.

PhD in progress:

- Hamza Jeljeli, "Using graphics accelerators for problems arising in the Number Field Sieve and Function Field Sieve algorithms", started in 2011, supervised by Jérémie Detrey and Emmanuel Thomé.
- Cyril Bouvier, "Integer Factoring on High-Performance Architectures", started in 2012, supervised by Paul Zimmermann.
- Laurent Grémy, "Analysis and optimization of sieves arithmetic algorithms" started in oct. 2013, co-supervised by Pierrick Gaudry and Marion Videau.
- Hugo Labrande, "Explicit computation of isogenies between Jacobians of curves using a complex analytic method", started in sep. 2013, cotutelle supervision between Emmanuel Thomé and Michael J. Jacobson, University of Calgary.

9.2.4. Juries

- Jérémie Detrey
  - was a member of the jury of the Polytechnique/ÉNS competitive entrance exam,
  - was a member of the PhD thesis jury of Nicolas Estibals (Université de Lorraine).
- Pierrick Gaudry was a member of the PhD thesis jury of Razvan Barbulescu (Université de Lorraine), Nicolas Estibals (Université de Lorraine), Jean-Gabriel Kammerer (Université de Rennes 1), Aurore Guillevic (École Normale Supérieure), Louise Huot (Université de Paris 6).
- Emmanuel Thomé was a member of the PhD thesis jury of Kisoon Yoon (Université de Caen Basse-Normandie).
- Marion Videau was president of one of the scientific baccalaureate juries in Nancy in July 2013.

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".
- Pierrick Gaudry gave a presentation at the "journée de l'Association francophone des spécialistes de l'investigation numérique".
- Marion Videau:
  - gave a talk for the awards ceremony of the *Olympiades de maths* in Lorraine.
  - gave a practical session of cryptography and information security for students from *lycées* taking part in an immersion day at the faculty.
  - participated to events on information about university studies for pupils and students (Clés de la réussite, Portes ouvertes de la faculté des sciences, Oriaction).
- Paul Zimmermann takes part in the "Maths-en-Jeans" program, with about 20 students in "troisième" at the Collège Pierre Brossolette in Réhon.

10. Bibliography

Major publications by the team in recent years

[1] J.-L. BEUCHAT, J. DETREY, N. ESTIBALS, E. OKAMOTO, F. RODRÍGUEZ-HENRÍQUEZ. *Fast architectures for the eta_T pairing over small-characteristic supersingular elliptic curves*, in "IEEE Transactions on Computers", February 2011, vol. 60, n^{o} 2, pp. 266-281 [*DOI :* 10.1109/TC.2010.163], http://hal.inria.fr/inria-00424016

[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. LENSTRA, E. THOMÉ, J. BOS, P. GAUDRY, A. KRUPPA, P. 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, http://hal.inria.fr/inria-00444693

[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] R. BARBULESCU. , *Algorithmes de logarithmes discrets dans les corps finis*, Université de Lorraine, December 2013, http://hal.inria.fr/tel-00925228

[9] N. ESTIBALS. , *Algorithmes et arithmétique pour l'implémentation de couplages cryptographiques*, Université de Lorraine, October 2013, http://hal.inria.fr/tel-00924743

Articles in International Peer-Reviewed Journals

[10] S. BAI, R. BRENT, E. THOMÉ. *Root optimization of polynomials in the number field sieve*, in "Mathematics of Computation", 2014, Accepted for publication, http://hal.inria.fr/hal-00919367

[11] A. ENGE, E. THOMÉ. *Computing class polynomials for abelian surfaces*, in "Experimental Mathematics", 2014, Accepted for publication, http://hal.inria.fr/hal-00823745

[12] J.-C. FAUGÈRE, P. GAUDRY, L. HUOT, G. RENAULT. *Using Symmetries in the Index Calculus for Elliptic Curves Discrete Logarithm*, in "Journal of Cryptology", May 2013, pp. 1-40 [*DOI :* 10.1007/S00145-013-9158-5], http://hal.inria.fr/hal-00700555

[13] S. IONICA. *Pairing-based algorithms for Jacobians of genus 2 curves with maximal endomorphism ring*, in "Journal of Number Theory", July 2013, vol. 133, pp. 3755-3770 [*DOI :* 10.1016/J.JNT.2013.04.023], http://hal.inria.fr/hal-00675045

[14] G. MELQUIOND, W. G. NOWAK, P. ZIMMERMANN. *Numerical Approximation of the Masser-Gramain Constant to Four Decimal Digits: delta=1.819...*, in "Mathematics of Computation", 2013, vol. 82, pp. 1235-1246 [*DOI :* 10.1090/S0025-5718-2012-02635-4], http://hal.inria.fr/hal-00644166

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(2809) with FFS*, in "PKC 2014 - International Conference on Practice and Theory of Public-Key Cryptography", Buenos Aires, Argentina, H. KRAWCZYK (editor), LNCS, Springer, 2014, http://hal.inria.fr/hal-00818124

[16] V. CORTIER, D. GALINDO, S. GLONDU, M. IZABACHÈNE. *Distributed ElGamal à la Pedersen - Application to Helios*, in "WPES 2013 - Proceedings of the 12th ACM workshop on privacy in the electronic society - 2013", Berlin, Germany, ACM, 2013, pp. 131-142 [*DOI :* 10.1145/2517840.2517852], http://hal.inria.fr/hal-00881076

[17] J. DETREY, P. GAUDRY, M. VIDEAU. *Relation collection for the Function Field Sieve*, in "ARITH 21 - 21st IEEE International Symposium on Computer Arithmetic", Austin, Texas, United States, A. NANNARELLI, P.-M. SEIDEL, P. T. P. TANG (editors), IEEE, 2013, pp. 201-210 [*DOI :* 10.1109/ARITH.2013.28], http://hal.inria.fr/hal-00736123

Scientific Books (or Scientific Book chapters)

[18] A. CASAMAYOU, G. CONNAN, T. DUMONT, L. FOUSSE, F. MALTEY, M. MEULIEN, M. MEZZAROBBA, C. PERNET, N. M. THIÉRY, P. ZIMMERMANN. , *Calcul mathématique avec Sage*, Amazon, 2013, 468 p. , electronic version available under Creative Commons license, http://hal.inria.fr/inria-00540485

[19] P. GAUDRY. *Algorithmes de comptage de points d'une courbe définie sur un corps fini*, in "Explicit Methods in Number Theory Rational Points and Diophantine Equations", K. BELABAS (editor), Panoramas et synthèses, SMF, 2013, vol. 36, http://hal.inria.fr/hal-00840136

[20] A. LENSTRA, T. KLEINJUNG, E. THOMÉ. *Universal Security; From bits and mips to pools, lakes - and beyond*, in "Number Theory and Cryptography", M. FISCHLIN, S. KATZENBEISSER (editors), Lecture Notes in Computer Science, Springer, 2013, vol. 8260, pp. 121-124, Humoristic [*DOI :* 10.1007/978-3-642-42001-6_9], http://hal.inria.fr/hal-00925622

Other Publications

[21] R. BARBULESCU. , *Selecting polynomials for the Function Field Sieve*, March 2013, http://hal.inria.fr/hal-00798386

[22] R. BARBULESCU, P. GAUDRY, A. JOUX, E. THOMÉ. , *A quasi-polynomial algorithm for discrete logarithm in finite fields of small characteristic*, 2013, http://hal.inria.fr/hal-00835446

[23] C. BOUVIER. , *The filtering step of discrete logarithm and integer factorization algorithms*, June 2013, http://hal.inria.fr/hal-00734654

[24] C. BOUVIER, P. ZIMMERMANN. , *Division-Free Binary-to-Decimal Conversion*, 2014, http://hal.inria.fr/hal-00864293

[25] V. CORTIER, D. GALINDO, S. GLONDU, M. IZABACHÈNE. , *A generic construction for voting correctness at minimum cost - Application to Helios*, 2013, Cryptology ePrint Archive, Report 2013/177, http://hal.inria.fr/hal-00881079

[26] 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

[27] J.-C. FAUGÈRE, P. GAUDRY, L. HUOT, G. RENAULT. , *Polynomial Systems Solving by Fast Linear Algebra*, 2013, 27 pages, http://hal.inria.fr/hal-00816724

[28] H. JELJELI. , *Accelerating Iterative SpMV for Discrete Logarithm Problem using GPUs*, 2013, http://hal.inria.fr/hal-00734975

References in notes

[29] 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/

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