IN PARTNERSHIP WITH:
CNRS

Université de Lorraine

Activity Report 2012

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
Algorithms, Certification, and Cryptography

Table of contents

Project-Team CARAMEL

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

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

1. Members

Research Scientists

Pierrick Gaudry [Team leader, Senior Researcher, CNRS, HdR]
Jérémie Detrey [Junior Researcher, Inria]
Emmanuel Thomé [Junior Researcher, Inria, HdR defended on December 13th, HdR]
Paul Zimmermann [Senior Researcher, Inria, part time, HdR]

Faculty Member

Marion Videau [Associate Professor, Université de Lorraine]

Engineers

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

PhD Students

Răzvan Bărbulescu [Contrat doctoral, Université de Lorraine; started in September 2011]
Cyril Bouvier [Contrat doctoral, Université de Lorraine; started in September 2012]
Nicolas Estibals [ATER, ENS Lyon; defense planned in 2013]
Hamza Jeljeli [Contrat doctoral, Université de Lorraine; started in September 2011]

Post-Doctoral Fellow

Sorina Ionica [One year contract with the ANR project CHIC, until September 2012]

Administrative Assistant

Emmanuelle Deschamps [part time]

Others

Luc Sanselme [Teacher from classes préparatoires aux grandes écoles]
Cyril Bouvier [Internship, ENS Paris, until August 2012]
Benjamin Dadoun [Internship, ENS Cachan, June – July 2012]
Nathan Lecoanet [Internship, ESIAL, June – July 2012]
Florent Noyer [Internship, ESIAL, June – July 2012]
Vlad-Cristian Miclea [Internship, Technical University of Cluj-Napoca (Romania), June – September 2012]

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

- The ANR proposal “CATREL” (in French, “Cribles, Améliorations Théoriques et Résolution Effective du Logarithme discret”) has been one of the eight accepted proposals among 59 submitted to the “programme blanc” in computer science for the year 2012. The ANR-CATREL project is beginning on January 1st, 2013.
- A new (second place) integer factorization record was set using the CADO-NFS software developed by the team, namely the factorization of RSA-704.
- Members of the team received the “Prix La Recherche” 2012 for their work on integer factorization.

3. Scientific Foundations

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 [17], 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.

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 [3]. 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.

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.

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 and discrete-logarithm computations. 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.

4.2. Standardization

4.2.1. 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.

4.3. 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.

4.3.1. 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.

4.3.2. 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.

4.3.3. 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.

5. Software

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 2012 is the release of version 3.1.1 (the “canard à l’orange” release) in July. With respect to version 3.1.0, this new version improves the reference manual, and fixes a few bugs. Also, a workshop was organized in June in Bordeaux, on the development of GNU MPFR and GNU MPC. In particular, the test coverage of GNU MPFR was improved.

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.

A new version, GNU MPC 1.0 (Fagus silvatica), was released in July 2012. Up from this release, GNU MPC is considered to be a mature library. Due to a security issue in automake, we had to release a bug-fix version 1.0.1 in September 2012.

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 January 2012, a new version 6.4 was released, followed by 6.4.1 and 6.4.2 in March, and 6.4.3 in June. Apart from bug fixes, and the fact that GMP-ECM is now distributed under the LGPL version 3, those new releases provide a new *-batch* option with faster Stage 1 code, and an improved tuning mechanism.

In February, Paul Leyland found a 43-digit factor using the GPU implementation of Stage 1 written by C. Bouvier, and in August, a new record prime of 79 digits was found by Sam Wagstaff (Purdue University) using GMP-ECM.

5.5. Finite fields

Participants: Pierrick Gaudry, Emmanuel Thomé [contact].

$\mathtt{mp}\mathbb{F}_q$ 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*. $\mathtt{mp}\mathbb{F}_q$ is not restricted to a finite field in particular, and 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.

$\mathtt{mp}\mathbb{F}_q$’s ability to generate specialized code for desired finite fields differentiates this library from its competitors. The performance achieved is far superior. For example, $\mathtt{mp}\mathbb{F}_q$ can be readily used to assess the throughput of an efficient software implementation of a given cryptosystem. Such an evaluation is the purpose of the “eBATS” benchmarking tool [1]. $\mathtt{mp}\mathbb{F}_q$ entered this trend in 2007, establishing 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. These timings are now comparison references for other implementations [18].

[1] http://www.ecrypt.eu.org/ebats/

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 2012, $\mathtt{mp}\mathbb{F}_q$ evolved somewhat, in order to do the required code generation needed for evolutions of CADO-NFS, notably in relation with linear algebra over prime fields. A new release is planned soon, once hindrances related to the license of some code fragments are dealt with.

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.

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. No new release was made in 2012, but several improvements have been made in the development version, with the help of Alain Filbois (SED engineer) and of Alexander Kruppa, recruited in October for a 2-year engineer contract.

Alain Filbois improved the *purge* program for filtering, by gaining a factor of about 5 in the input-output routines. Together with P. Zimmermann, he also wrote a special-purpose *clique removal* code for huge factorizations requiring out-of-core computing; this code has been used for a new filtering experiment on the relations collected for RSA-768 (not yet finished at the time of writing).

The *Objectif 1024* ADT started in 2012, with the recruitment of Alexander Kruppa as a engineer for 2 years. The four main objectives of this ADT are: (1) be able to use CADO-NFS routinely on clusters of 20 to 100 nodes, including on Amazon EC2; (2) develop precise tools to optimize parameters in the sieving phase; (3) develop more professional test mechanisms; (4) make two major releases of CADO-NFS, and advertize them on potential users.

Overall, CADO-NFS keeps improving its competitivity over alternative code bases. Improvements in CADO-NFS and new results obtained with CADO-NFS are described below.

6. New Results

6.1. Sieve for FFS

Participants: Jérémie Detrey, Pierrick Gaudry [contact], Marion Videau.

Jérémie Detrey, Pierrick Gaudry and Marion Videau have worked on the relation collection step of the Function Field Sieve and especially on its implementation. This is still an ongoing work but the first results have been accepted for publication [13] in the ARITH-2013 conference.

6.2. Bilinear Maps

Participants: Răzvan Bărbulescu, Jérémie Detrey, Nicolas Estibals, Paul Zimmermann [contact].

As a result of an internal working group in the team, we have found and published at the WAIFI conference a new algorithm to find optimal formulae for bilinear maps [8]. This algorithm enables one to rediscover Karatsuba's multiplication algorithm, but has many other applications, for example to matrix multiplication.

6.3. Number Field Sieve

Participants: Emmanuel Thomé, Paul Zimmermann [contact].

Together with Shi Bai (Australian National University), E. Thomé and P. Zimmermann used CADO-NFS to factor RSA-704, a 212-digit number, to check scalability of the software on large factorizations [10]. This is the second largest number factored by any GNFS software so far, and the largest one factored by CADO-NFS. This experiment was very helpful, since it demonstrated several weaknesses of the code, that have been addressed since then.

Together with Shi Bai (Australian National University), P. Zimmermann wrote a preprint describing the algorithm used in CADO-NFS for the size-optimization of sextic polynomials [11].

Alain Filbois, Shi Bai (Australian National University) and P. Zimmermann improved the polynomial selection code. With parameters used to find good polynomials for RSA-896, a total speedup by a factor 14 was obtained, with both algorithmic and implementation improvements.

6.4. Sparse linear algebra modulo p

Participants: Hamza Jeljeli, Emmanuel Thomé [contact].

The resolution of linear algebra problems with subexponential methods, which is the topic of the ANR-CATREL project (to begin in 2013) calls for the resolution of large sparse linear systems defined over finite fields. In preparation for this, H. Jeljeli has developed software for performing sparse matrix times vector multiplication on NVIDIA GPUS [16]. This code provides a very significant speedup over the use of CPUs for this task, and achieves this speedup by a clever use of a "residue number system" representation of the finite field elements.

As a complement, a recent re-implementation of Thomé's algorithm for the (matrix) Berlekamp-Massey step in the block Wiedemann algorithm has been done. This program can of course be special-cased to the simple non-matrix case. The GPU code above and this special case, together, form the needed software to have a sparse linear system solver over finite fields using Wiedemann's algorithm. This has been put to use, and led to the completion of a discrete logarithm record in $\mathbb{F}_{2^{619}}$, the linear system part taking only 17 hours in total on one GPU (plus 1 hour on one CPU for the Berlekamp-Massey step).

6.5. Using symmetries in elliptic curve discrete logarithm

Participant: Pierrick Gaudry.

In a joint work by Jean-Charles Faugère, Pierrick Gaudry, Louise Huot and Guénaël Renault, it has been shown that the geometric symmetries of an elliptic curve, in particular, the symmetries of an Edwards curve, could be used to speed up the index calculus attack for computing discrete logarithms in an elliptic curve defined over an extension field. The corresponding article [14] is currently under revision.

6.6. Galois properties of curves for ECM

Participants: Răzvan Bărbulescu, Cyril Bouvier.

In collaboration with Joppe Bos, Peter Montgomery and Thorsten Kleinjung, Răzvan Bărbulescu and Cyril Bouvier proved some divisibility properties of the group order of an elliptic curve, using the Galois structure of its division polynomial. It explains the good behaviour of some curves that have been experimentally found to factor more numbers than others, and gives a way to find new curves with this property. The corresponding article [7] was presented in ANTS-X.

6.7. Computation of CM class polynomials for genus 2 Jacobians

Participants: Sorina Ionica, 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. A publication is in the works.

Using similar underlying tools and theory, and based on work by Sorina Ionica [15], 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.

6.8. Filtering step for NFS and FFS

Participant: Cyril Bouvier.

Cyril Bouvier studied the filtering step for the Number Field Sieve. A better weight function, used during the clique removal step, was found which allows to construct smaller matrices for the linear algebra step. A preprint is avalaible [12]. The filtering step for the Function Field Sieve was written in CADO-NFS.

7. Bilateral Contracts and Grants with Industry

7.1. Training and consulting with HTCS

Participants: Pierrick Gaudry, Emmanuel Thomé [contact].

We have a one-year contract with the HTCS company, for training and consulting activities, on topics related to our research. This contract is likely to be renewed in 2013.

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, Vlad-Cristian Miclea, 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.

The funding obtained was used to buy an FPGA ML-605 development board, on which Vlad-Cristian Miclea implemented operators for polynomial arithmetic in characteristic two and three during his internship; along with a GeForce GTX 580 graphics card, on which Hamza Jeljeli developed a GPU-based implementation of sparse linear algebra routines for solving discrete-logarithm problems [16].

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: Răzvan Bărbulescu, 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 is scheduled to start in January 2013, but the kick-off meeting has already taken place in Nancy on Dec. 14th, 2012.

8.2.2. ANR CHIC (Courbes Hyperelliptiques, Isogénies, Comptage)

Participants: Pierrick Gaudry, Sorina Ionica, Emmanuel Thomé [contact].

The team has obtained a financial support from the ANR (“programme blanc”) for a project, common with colleagues from IRMAR (Rennes) and IML (Marseille). The ANR CHIC grant covers the period 09/2009 to 08/2012, and has thus ended in 2012. The purpose of this ANR project is the study of several aspects of curves in genus 2, with a very strong focus on the computation of explicit isogenies between Jacobians.

In 2012, within the context of ANR CHIC, Ionica and Thomé worked on isogeny graphs in genus 2.

8.2.3. ANR DEMOTIS (Collaborative Analysis, Evaluation and Modelling of Health Information Technology)

Participant: Marion Videau.

The project from “programme ARPEGE” involved three Inria project-teams as a single partner (SMIS, SECRET and CARAMEL) together with colleagues from CECOJI (CNRS) and the company Sopinspace. It has been running from January 2009 and ended in March 2012.

The project experimented new methods for the multidisciplinary design of large information systems that have to take into account legal, social and technical constraints. Its main field of application is personal health information systems.

8.3. European Initiatives

8.3.1. PHC application with EPFL

The team obtained a PHC Germaine de Staël grant in collaboration with the LACAL team from EPFL (Lausanne, Switzerland), in 2011. The grant has been renewed for a second (and final) year 2012. This collaboration focuses on integer factorization and discrete logarithms.

8.4. International Research Visitors

8.4.1. Visits of International Scientists

8.4.1.1. Internships

Vlad-Cristian MICLEA (from Jun 2012 until Sep 2012)

Subject: Efficient FPGA implementation of finite-field multiplication algorithms

Institution: The Technical University of Cluj-Napoca (Romania)

9. Dissemination

9.1. Scientific Animation

9.1.1. Caramel seminar

Twenty speakers were invited to our seminar in 2012: Charles Bouillaguet, Stéphane Glondu, Marion Videau, Jérémie Detrey, Karim Khalfallah, Peter Schwabe, Jean-Charles Faugère, Luc Sanselme, Olivier Levillain, Aurore Guillevic, Cyril Bouvier, Răzvan Bărbulescu, Francisco Rodríguez-Henríquez, Laura Grigori, Hugo Labrande, Christophe Petit, Alexandre Benoit, Paul Zimmermann, Mohab Safey El Din, and Alin Bostan.

9.1.2. Committees memberships

- Jérémie Detrey
  - was a member of the program committee of the International Conference on Pairing-Based Cryptography (Pairing 2012),
  - was a member of the program committee of the International Workshop on the Arithmetic of Finite Fields (WAIFI 2012),
  - is a member of the program committee of the *Symposium en Architectures nouvelles de machines* (SympA 2013).
- Pierrick Gaudry
  - is a deputy director of LORIA until the end of 2012,
  - was in the hiring committees (Comités de Sélection) in Paris 6, Montpellier and Nancy,
  - with Cécile Dartyge (IECN), he organized a scientific day "Journée Charles Hermite" on cryptography and number theory,
  - was a member of the program committee of the 13th International Workshop on Information Security Applications (WISA 2012).
- Emmanuel Thomé
  - is an elected member of the Inria Evaluation Committee for the period 2011-2015,
  - was a member of the program committee of the Workshop on Elliptic Curve Cryptography (ECC 2012).
- Marion Videau
  - is a member of the scientific committee of the CCA seminar (*Codage, Cryptologie, Algorithmes*),
  - was a member of the program committee of the International Conference on Information Security and Cryptology (ICISC 2012),
  - is a member of the program committee of the *Symposium sur la sécurité des technologies de l'information et des communications* (SSTIC 2013).
- Paul Zimmermann
  - is an elected member of the Inria Scientific Board,
  - is a member of the program committee of the International Symposium on Symbolic and Algebraic Computation (ISSAC 2013).

9.1.3. Invited Conferences

- Jérémie Detrey was invited to give a talk at the Workshop on Elliptic Curve Cryptography (ECC 2012) in Querétaro, México.
- Emmanuel Thomé was invited to give a talk at the International Workshop on the Arithmetic of Finite Fields (WAIFI 2012) in Bochum, Germany.

9.2. Teaching - Supervision - Juries

9.2.1. Teaching

- Jérémie Detrey:

  Security of websites: 2 hours (lecture), L1, IUT Charlemagne, Nancy, France.

- Emmanuel Thomé:

  Cryptology: 20 hours, M1, ESIAL, Nancy, France.

  Algorithmic Number Theory: 9 hours (lectures), M2, University Paris 7 (Master Parisien de Recherche en Informatique), Paris, 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 sciences, Université de Lorraine, Nancy, France:

  Introduction to algorithmic and programming: 40 hours (lectures and tutorial sessions), 20 hours (practical sessions), L1.

  Introduction to information system design: 10 hours (practical sessions), L3.

  Introduction to cryptography: 15 hours (lectures), 15 hours (tutorial sessions), M1.

  Introduction to information system security: 15 hours (lectures), 15 hours (tutorial sessions), M1.

  Supervision and jury of M2 students internships: 10 hours.

9.2.2. Internships

Cyril Bouvier, ENS Paris, "Integer Factoring on High-Performance Architectures", September 2011–August 2012, supervised by Paul Zimmermann.

Benjamin Dadoun, ENS Cachan, "Isolation of complex roots of univariate polynomials with the CEVAL algorithm", June–July 2012, supervised by Paul Zimmermann.

Nathan Lecoanet, ESIAL, "What speedup can we expect in the Number Field Sieve with non-linear polynomials?", June–July 2012, supervised by Paul Zimmermann.

Vlad-Cristian Miclea, Technical University of Cluj-Napoca (Romania), "Efficient FPGA implementation of finite-field multiplication algorithms", June 2012–September 2012, supervised by Jérémie Detrey.

Florent Noyer, ESIAL, "Parallel reconstruction of a polynomial from its roots", June–July 2012, supervised by Emmanuel Thomé

9.2.3. Supervision

HdR: Emmanuel Thomé, "Théorie algorithmique des nombres et applications à la cryptanalyse de primitives cryptographiques", Université de Lorraine, 13/12/2012, [1].

PhD in progress:

- Nicolas Estibals, "Algorithmes et arithmétique pour l'implémentation de couplages cryptographiques", started in 2009, co-supervised by Jérémie Detrey and Pierrick Gaudry.
- Răzvan Bărbulescu, "Number and function field sieve for discrete logarithm", started in 2011, supervised by Pierrick Gaudry.
- 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.

9.2.4. Juries

- Paul Zimmermann was a member of the PhD thesis jury of Vincent Nivoliers (University of Lorraine), of the PhD thesis jury of Romain Lebreton (École Polytechnique), and of the “Habilitation à diriger des recherches” jury of Emmanuel Thomé (University of Lorraine).

9.3. Popularization

- With Nazim Fatès (MAIA project-team), Jérémie Detrey participated in a 2-hour television program dedicated to computer science and research, which was broadcast on the internal channel of the Nancy-Brabois children’s hospital.
- Pierrick Gaudry:
  - co-organized a cycle of 3 conferences in the honour of Turing in Nancy. The three speakers were Giuseppe Longo, François Morain, and Jean Lassègue.
  - gave a talk at the “7ème colloque de l’ARCSI”, in Metz for a general audience.
- Marion Videau:
  - participated to the film *Le Modèle Turing* of Catherine Bernstein (but her visual part was cut out during editing).
  - participated to a short television report for France 3 Lorraine about cryptography and her work as a researcher.
- Paul Zimmermann gave a 2-hour presentation about cryptography to students of “seconde” and “terminale” at the Lycée Jean de Pange in Sarreguemines.

10. Bibliography

Publications of the year

Doctoral Dissertations and Habilitation Theses

[1] E. THOMÉ. *Théorie algorithmique des nombres et applications à la cryptanalyse de primitives cryptographiques*, Université de Lorraine, December 2012, Habilitation à Diriger des Recherches, http://hal.inria.fr/tel-00765982.

Articles in International Peer-Reviewed Journals

[2] S. CHEVILLARD. *The functions erf and erfc computed with arbitrary precision and explicit error bounds*, in "Information and Computation", 2012, vol. 216, p. 72 – 95, The version available on the HAL server is slightly different from the published version because it contains full proofs., http://hal.inria.fr/ensl-00356709.

[3] P. GAUDRY, É. SCHOST. *Genus 2 point counting over prime fields*, in "Journal of Symbolic Computation", 2012, vol. 47, n^{o} 4, p. 368-400 [*DOI :* 10.1016/J.JSC.2011.09.003], http://hal.inria.fr/inria-00542650.

[4] T. KLEINJUNG, J. BOS, A. LENSTRA, D. A. OSVIK, K. AOKI, S. CONTINI, J. FRANKE, E. THOMÉ, P. JERMINI, M. THIÉMARD, P. LEYLAND, P. MONTGOMERY, A. TIMOFEEV, H. STOCKINGER. *A Heterogeneous Computing Environment to Solve the 768-bit RSA Challenge*, in "Cluster Computing", 2012, vol. 15, n^{o} 1, p. 53-68 [*DOI :* 10.1007/S10586-010-0149-0], http://hal.inria.fr/inria-00535765.

[5] D. LUBICZ, D. ROBERT. *Computing isogenies between Abelian Varieties*, in "Compositio Mathematica", September 2012, vol. 148, n^o 05, p. 1483–1515, 47 pages [*DOI :* 10.1112/S0010437X12000243], http://hal.inria.fr/hal-00446062.

International Conferences with Proceedings

[6] D. ARANHA, J.-L. BEUCHAT, J. DETREY, N. ESTIBALS. *Optimal Eta pairing on supersingular genus-2 binary hyperelliptic curves*, in "Cryptographer's Track at the RSA Conference 2012 (CT-RSA 2012)", San Francisco, United States, O. DUNKELMAN (editor), Springer, February 2012, 19, http://hal.inria.fr/inria-00540002.

[7] R. BARBULESCU, J. BOS, C. BOUVIER, T. KLEINJUNG, P. MONTGOMERY. *Finding ECM-friendly curves through a study of Galois properties*, in "ANTS-X 10th Algorithmic Number Theory Symposium - 2012", San Diego, United States, University of California, February 2012, http://hal.inria.fr/hal-00671948.

[8] R. BARBULESCU, J. DETREY, N. ESTIBALS, P. ZIMMERMANN. *Finding Optimal Formulae for Bilinear Maps*, in "4th International Workshop on Arithmetic in Finite Fields - WAIFI 2012", Bochum, Germany, F. ÖZBUDAK, F. RODRÍGUEZ-HENRÍQUEZ (editors), Lecture Notes in Computer Science, Ruhr Universitat Bochum, July 2012, vol. 7369, http://hal.inria.fr/hal-00640165.

[9] E. THOMÉ. *Square root algorithms for the number field sieve*, in "4th International Workshop on Arithmetic in Finite Fields - WAIFI 2012", Bochum, Germany, F. ÖZBUDAK, F. RODRÍGUEZ-HENRÍQUEZ (editors), Lecture Notes in Computer Science, Springer, July 2012, vol. 7369, p. 208-224, The original publication is available at www.springerlink.com [*DOI :* 10.1007/978-3-642-31662-3_15], http://hal.inria.fr/hal-00756838.

Other Publications

[10] S. BAI, E. THOMÉ, P. ZIMMERMANN. *Factorisation of RSA-704 with CADO-NFS*, 2012, http://hal.inria.fr/hal-00760322.

[11] S. BAI, P. ZIMMERMANN. *Size Optimization of Sextic Polynomials in the Number Field Sieve*, 2012, http://hal.inria.fr/hal-00760331.

[12] C. BOUVIER. *Improvement in the filtering step of integer factorization algorithms*, 2012, http://hal.inria.fr/hal-00734654.

[13] J. DETREY, P. GAUDRY, M. VIDEAU. *Relation collection for the Function Field Sieve*, 2012, http://hal.inria.fr/hal-00736123.

[14] J.-C. FAUGÈRE, P. GAUDRY, L. HUOT, G. RENAULT. *Using Symmetries in the Index Calculus for Elliptic Curves Discrete Logarithm*, 2012, 31 pages, http://hal.inria.fr/hal-00700555.

[15] S. IONICA. *Pairing-based algorithms for jacobians of genus 2 curves with maximal endomorphism ring*, 2012, http://hal.inria.fr/hal-00675045.

[16] H. JELJELI. *Accelerating Iterative SpMV for Discrete Logarithm Problem using GPUs*, 2012, http://hal.inria.fr/hal-00734975.

References in notes

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

[18] M. SCOTT. *New record breaking implementations of ECC on quadratic extensions using endomorphisms*, September 2008, Invited talk at the ECC 2008 Conference. Utrecht, the Netherlands, Sep. 22-24, 2008.