Activity Report 2015

Project-Team GRACE

Geometry, arithmetic, algorithms, codes and encryption

RESEARCH CENTER
Saclay - Île-de-France

THEME
Algorithmics, Computer Algebra and Cryptology

Table of contents

1. **Members** 1
2. **Overall Objectives** 2
3. **Research Program** 2
   3.1. Algorithmic Number Theory 2
   3.2. Arithmetic Geometry: Curves and their Jacobians 2
   3.3. Curve-Based cryptology 3
   3.4. Algebraic Coding Theory 4
4. **Application Domains** 4
5. **Highlights of the Year** 5
6. **New Software and Platforms** 7
   6.1. Fast Compact Diffie-Hellman 7
   6.2. Platforms 7
7. **New Results** 8
   7.1. Weight distribution of Algebraic-Geometry codes 8
   7.2. Faster elliptic and hyperelliptic curve cryptography 8
   7.3. Quantum factoring 8
   7.4. Cryptanalysis of code based cryptosystems by filtration attacks 8
   7.5. Quantum LDPC codes 9
   7.6. Discrete Logarithm computations in finite fields with the NFS algorithm 9
      7.6.1. DL Record computation in a quadratic finite field GF(p^2) 9
      7.6.2. Individual discrete logarithm computation 10
   7.7. Information sets of multiplicity codes 10
   7.8. Rank metric codes over infinite fields 11
   7.9. Hash function cryptanalysis 11
   7.10. Block cipher design and analysis 11
8. **Bilateral Contracts and Grants with Industry** 12
9. **Partnerships and Cooperations** 12
   9.1. Regional Initiatives 12
      9.1.1. PEPS Aije-bitcoin 12
      9.1.2. IDEALCODES 13
   9.2. National Initiatives 13
      9.2.1. ANR 13
      9.2.2. DGA 13
   9.3. European Initiatives 13
      9.3.1. FP7 & H2020 Projects 13
      9.3.2. Major European Organizations with which the Team have followed Collaborations 14
   9.4. International Initiatives 15
   9.5. International Research Visitors 15
10. **Dissemination** 15
   10.1. Promoting Scientific Activities 15
      10.1.1. Scientific events organisation 15
      10.1.2. Scientific events selection 15
         10.1.2.1. Member of the conference program committees 15
         10.1.2.2. Reviewer 16
      10.1.3. Journal 16
         10.1.3.1. Member of the editorial boards 16
         10.1.3.2. Reviewer - Reviewing activities 16
      10.1.4. Invited talks 17
      10.1.5. Leadership within the scientific community 17

10.1.6. Scientific expertise 17
10.1.7. Research administration 17
10.2. Teaching - Supervision - Juries 18
10.2.1. Teaching 18
10.2.2. Supervision 18
10.2.3. Juries 18
10.3. Popularization 19
10.4. Institutional commitment 19
11. Bibliography **19**

Project-Team GRACE

Creation of the Team: 2012 January 01, updated into Project-Team: 2013 July 01

Keywords:

Computer Science and Digital Science:

4.2. - Correcting codes
4.3.1. - Public key cryptography
7.7. - Number theory

Other Research Topics and Application Domains:

9.4.2. - Mathematics
9.8. - Privacy

1. Members

Research Scientists

Daniel Augot [Team leader, Inria, Senior Researcher, HdR]
Alain Couvreur [Inria, Researcher]
Benjamin Smith [Inria, Researcher]

Faculty Members

Philippe Lebacque [Univ. Franche-Comté, Associate Professor]
Francoise Levy-Dit-Vehel [ENSTA, Associate Professor, HdR]
François Morain [Ecole Polytechnique, Professor, HdR]

Engineers

Nicholas Coxon [Inria, since Dec 2015]
David Lucas [Inria]

PhD Students

Elise Barelli [Inria, since Oct 2015]
Nicolas Duhamel [ENS Cachan, since Feb 2015]
Cécile Goncalves [Inria, until Jul 2015]
Pierre Karpman [Inria, DGA grant]
Gwezheneg Robert [Univ. Rennes I, until Oct 2015]
Julien Lavauzelle [Ecole Polytechnique, since Oct 2015]
Manh Cuong Ngo [Inria, until Sep 2015]

Post-Doctoral Fellows

Virgile Ducet [Inria, since Oct 2015]
Aurore Guillevic [Inria, until Dec 2015]
Johan Nielsen [Inria, until Aug 2015]

Visiting Scientist

Christian Berghoff [Bonn Universität PhD student, since Sep 2015]

Administrative Assistants

Helene Bessin Rousseau [Inria, since Sep 2015]
Myriam Brettes [Inria, until Sep 2015]
Tien Bui [Inria, from Dec 2015]

Others

Emily Clement [Inria, M1 intern, from May 2015 until Jul 2015]

Kofi Manful [Inria, M2 intern, from Mar 2015 until Aug 2015]
Eleonora Palazzolo [Inria, M2 intern, from Dec 2015]

2. Overall Objectives

2.1. Scientific foundations

GRACE has two broad application domains—cryptography and coding theory—linked by a common foundation in algorithmic number theory and the geometry of algebraic curves. In our research, which combines theoretical work with practical software development, we use algebraic curves to *create better cryptosystems*, to *provide better security assessments* for cryptographic key sizes, and to *build the best error-correcting codes*.

Coding and cryptography deal (in different ways) with securing communication systems for high-level applications. In our research, the two domains are linked by the computational issues related to algebraic curves (over various fields) and arithmetic rings. These fundamental number-theoretic algorithms, at the crossroads of a rich area of mathematics and computer science, have already proven their relevance in public key cryptography, with industrial successes including the RSA cryptosystem and elliptic curve cryptography. It is less well-known that the same branches of mathematics can be used to build very good codes for error correction. While coding theory has traditionally had an electrical engineering flavour, recent developments in computer science have shed new light on coding theory, leading to new applications more central to computer science.

3. Research Program

3.1. Algorithmic Number Theory

Algorithmic Number Theory is concerned with replacing special cases with general algorithms to solve problems in number theory. In the Grace project, it appears in three main threads:

- fundamental algorithms for integers and polynomials (including primality and factorization);
- algorithms for finite fields (including discrete logarithms); and
- algorithms for algebraic curves.

Clearly, we use computer algebra in many ways. Research in cryptology has motivated a renewed interest in Algorithmic Number Theory in recent decades—but the fundamental problems still exist *per se*. Indeed, while algorithmic number theory application in cryptanalysis is epitomized by applying factorization to breaking RSA public key, many other problems, are relevant to various area of computer science. Roughly speaking, the problems of the cryptological world are of bounded size, whereas Algorithmic Number Theory is also concerned with asymptotic results.

3.2. Arithmetic Geometry: Curves and their Jacobians

Theme: Arithmetic Geometry: Curves and their Jacobians

Arithmetic Geometry is the meeting point of algebraic geometry and number theory: that is, the study of geometric objects defined over arithmetic number systems (such as the integers and finite fields). The fundamental objects for our applications in both coding theory and cryptology are curves and their Jacobians over finite fields.

An algebraic *plane curve* $\mathcal{X}$ over a field $\mathbf{K}$ is defined by an equation

$$\mathcal{X} : F_{\mathcal{X}}(x, y) = 0 \quad \text{where } F_{\mathcal{X}} \in \mathbf{K}[x, y].$$

(Not every curve is planar—we may have more variables, and more defining equations—but from an algorithmic point of view, we can always reduce to the plane setting.) The *genus* $g_{\mathcal{X}}$ of $\mathcal{X}$ is a non-negative integer classifying the essential geometric complexity of $\mathcal{X}$; it depends on the degree of $F_{\mathcal{X}}$ and on the number of singularities of $\mathcal{X}$. The simplest curves with nontrivial Jacobians are curves of genus 1, known as *elliptic curves*; they are typically defined by equations of the form $y^2 = x^3 + Ax + B$. Elliptic curves are particularly important given their central role in public-key cryptography over the past two decades. Curves of higher genus are important in both cryptography and coding theory.

The curve $\mathcal{X}$ is associated in a functorial way with an algebraic group $J_{\mathcal{X}}$, called the *Jacobian* of $\mathcal{X}$. The group $J_{\mathcal{X}}$ has a geometric structure: its elements correspond to points on a $g_{\mathcal{X}}$-dimensional projective algebraic group variety. Typically, we do not compute with the equations defining this projective variety: there are too many of them, in too many variables, for this to be convenient. Instead, we use fast algorithms based on the representation in terms of classes of formal sums of points on $\mathcal{X}$.

3.3. Curve-Based cryptology

Theme: Curve-Based Cryptology

Jacobians of curves are excellent candidates for cryptographic groups when constructing efficient instances of public-key cryptosystems. Diffie–Hellman key exchange is an instructive example.

Suppose Alice and Bob want to establish a secure communication channel. Essentially, this means establishing a common secret *key*, which they will then use for encryption and decryption. Some decades ago, they would have exchanged this key in person, or through some trusted intermediary; in the modern, networked world, this is typically impossible, and in any case completely unscalable. Alice and Bob may be anonymous parties who want to do e-business, for example, in which case they cannot securely meet, and they have no way to be sure of each other's identities. Diffie–Hellman key exchange solves this problem. First, Alice and Bob publicly agree on a cryptographic group G with a generator P (of order N); then Alice secretly chooses an integer a from $[1..N]$, and sends aP to Bob. In the meantime, Bob secretly chooses an integer b from $[1..N]$, and sends bP to Alice. Alice then computes $a(bP)$, while Bob computes $b(aP)$; both have now computed abP, which becomes their shared secret key. The security of this key depends on the difficulty of computing abP given P, aP, and bP; this is the Computational Diffie–Hellman Problem (CDHP). In practice, the CDHP corresponds to the Discrete Logarithm Problem (DLP), which is to determine a given P and aP.

This simple protocol has been in use, with only minor modifications, since the 1970s. The challenge is to create examples of groups G with a relatively compact representation and an efficiently computable group law, and such that the DLP in G is hard (ideally approaching the exponential difficulty of the DLP in an abstract group). The Pohlig–Hellman reduction shows that the DLP in G is essentially only as hard as the DLP in its largest prime-order subgroup. We therefore look for compact and efficient groups of prime order.

The classic example of a group suitable for the Diffie–Hellman protocol is the multiplicative group of a finite field $\mathbf{F}_q$. There are two problems that render its usage somewhat less than ideal. First, it has too much structure: we have a subexponential Index Calculus attack on the DLP in this group, so while it is very hard, the DLP falls a long way short of the exponential difficulty of the DLP in an abstract group. Second, there is only one such group for each q: its subgroup treillis depends only on the factorization of $q - 1$, and requiring $q - 1$ to have a large prime factor eliminates many convenient choices of q.

This is where Jacobians of algebraic curves come into their own. First, elliptic curves and Jacobians of genus 2 curves do not have a subexponential index calculus algorithm: in particular, from the point of view of the DLP, a generic elliptic curve is currently *as strong as* a generic group of the same size. Second, they provide some diversity: we have many degrees of freedom in choosing curves over a fixed $\mathbf{F}_q$, with a consequent diversity of possible cryptographic group orders. Furthermore, an attack which leaves one curve vulnerable may not necessarily apply to other curves. Third, viewing a Jacobian as a geometric object rather than a pure group allows us to take advantage of a number of special features of Jacobians. These features include efficiently computable pairings, geometric transformations for optimised group laws, and the availability of efficiently computable non-integer endomorphisms for accelerated encryption and decryption.

3.4. Algebraic Coding Theory

Theme: Coding theory

Coding Theory studies originated with the idea of using redundancy in messages to protect against noise and errors. The last decade of the 20th century has seen the success of so-called iterative decoding methods, which enable us to get very close to the Shannon capacity. The capacity of a given channel is the best achievable transmission *rate* for reliable transmission. The consensus in the community is that this capacity is more easily reached with these iterative and probabilistic methods than with algebraic codes (such as Reed–Solomon codes).

However, algebraic coding is useful in settings other than the Shannon context. Indeed, the Shannon setting is a random case setting, and promises only a vanishing error probability. In contrast, the algebraic Hamming approach is a worst case approach: under combinatorial restrictions on the noise, the noise can be adversarial, with strictly zero errors.

These considerations are renewed by the topic of *list decoding* after the breakthrough of Guruswami and Sudan at the end of the nineties. List decoding relaxes the uniqueness requirement of decoding, allowing a small list of candidates to be returned instead of a single codeword. List decoding can reach a capacity close to the Shannon capacity, with zero failure, with small lists, in the adversarial case. The method of Guruswami and Sudan enabled list decoding of most of the main algebraic codes: Reed–Solomon codes and Algebraic–Geometry (AG) codes and new related constructions “capacity-achieving list decodable codes”. These results open the way to applications again adversarial channels, which correspond to worst case settings in the classical computer science language.

Another avenue of our studies is AG codes over various geometric objects. Although Reed–Solomon codes are the best possible codes for a given alphabet, they are very limited in their length, which cannot exceed the size of the alphabet. AG codes circumvent this limitation, using the theory of algebraic curves over finite fields to construct long codes over a fixed alphabet. The striking result of Tsfasman–Vladut–Zink showed that codes better than random codes can be built this way, for medium to large alphabets. Disregarding the asymptotic aspects and considering only finite length, AG codes can be used either for longer codes with the same alphabet, or for codes with the same length with a smaller alphabet (and thus faster underlying arithmetic).

From a broader point of view, wherever Reed–Solomon codes are used, we can substitute AG codes with some benefits: either beating random constructions, or beating Reed–Solomon codes which are of bounded length for a given alphabet.

Another area of Algebraic Coding Theory with which we are more recently concerned is the one of Locally Decodable Codes. After having been first theoretically introduced, those codes now begin to find practical applications, most notably in cloud-based remote storage systems.

4. Application Domains

4.1. Cryptography and Cryptanalysis

In the twenty-first century, cryptography plays two essential roles: it is used to ensure *security* and *integrity* of communications and communicating entities. Contemporary cryptographic techniques can be used to hide private data, and to prove that public data has not been modified; to provide anonymity, and to assert and prove public identities. The creation and testing of practical cryptosystems involves

1. The design of provably secure protocols;
2. The design and analysis of compact and efficient algorithms to implement those protocols, and to attack their underlying mathematical and computational problems;
3. The robust implementation of those algorithms in low-level software and hardware, and their deployment in the wild.

While these layers are interdependent, GRACE's cryptographic research is focused heavily on the middle layer: we design, implement, and analyze the most efficient algorithms for fundamental tasks in contemporary cryptography. Our "clients", in a sense, are protocol designers on the one hand, and software and hardware engineers on the other.

F. Morain and B. Smith work primarily on the number-theoretic algorithms that underpin the current state-of-the-art in public-key cryptography (which is used to establish secure connections, and create and verify digital signatures, among other applications). For example, their participation in the ANR CATREL project aims to give a realistic assessment of the security of systems based on the Discrete Logarithm Problem, by creating a free, open, algorithmic package implementing the fastest known algorithms for attacking DLP instances. This will have an extremely important impact on contemporary pairing-based cryptosystems, as well as legacy finite field-based cryptosystems. On a more constructive note, F. Morain' elliptic curve point counting and primality proving algorithms are essential tools in the everyday construction of strong public-key cryptosystems, while B. Smith's recent work on elliptic curves aims to improve the speed of curve-based cryptosystems (such as Elliptic Curve Diffie–Hellman key exchange, a crucial step in establishing secure internet connections) without compromising their security.

D. Augot, F. Levy-dit-Vehel, and A. Couvreur's research on codes has far-reaching applications in *code-based cryptography*. This is a field which is growing rapidly in importance—partly due to the supposed resistance of code-based cryptosystems to attacks from quantum computing, partly due to the range of new techniques on offer, and partly because the fundamental problem of parameter selection is relatively poorly understood. For example, A. Couvreur's work on filtration attacks on codes has an important impact on the design of code-based systems using wild Goppa codes or algebraic geometry codes, and on the choice of parameter sizes for secure implementations.

Coding theory also has important practical applications in the improvement of conventional symmetric cryptosystems. For example, D. Augot's recent work on MDS matrices via BCH codes gives a more efficient construction of optimal diffusion layers in block ciphers. Here we use combinatorial, non-algorithmic properties of codes, in the internals of designs of block ciphers.

While coding theory brings tools as above for the classical problems of encryption, authentication, and so on, it can also provide solutions to new cryptographic problems. This is classically illustrated by the use of Reed-Solomon codes in secret sharing schemes. Grace is involved in the study, construction and implementation of locally decodable codes, which have applications in quite a few cryptographic protocols : *Private Information Retrieval*, *Proofs of Retrievability*, *Proofs of Ownership*, etc.

5. Highlights of the Year

5.1. Highlights of the Year

Freestart collision for the full SHA-1.

Together with M. Stevens and T. Peyrin, P. Karpman gave the first freestart collision for the full SHA-1 hash function [32]. Although theoretical attacks on this function were known since 2005, this work is an important milestone in SHA-1 cryptanalysis and it had a concrete impact on the use of SHA-1 in existing systems, such as TLS certificates. In particular, the CA/Browser forum (which regroups some of the major industries of the internet) withdrew an internal ballot proposing to extend the use of SHA-1 in new certificates through 2016. Major browser developers such as Mozilla are also encouraging the timely withdrawal of SHA-1 certificates by updating the in-browser security warnings when such certificates are used. This result was also vulgarised in technical press such as *Ars Technica* and more general newspapers such as *Le monde*.

Discrete logarithm record computation in finite fields

F. Morain and A. Guillevic together with P. Gaudry (CARAMEL team, Inria Nancy Grand Est) and R. Barbulescu (CNRS, IMJ) published a new discrete logarithm record in a finite field of 180 decimal digits (dd), i.e. 595 bits. This result was presented at the Eurocrypt 2015 conference [19]. The Discrete Logarithm Problem (DLP) is widely studied in prime fields GF(p) and was broken in small characteristic finite fields of the form GF(2^n) and GF(3^n) with smooth n very recently. It was not known whether the DLP is as hard in extensions of finite fields compared to prime fields, for the same global size. With this record of the same size as the most recent record in a prime field, F. Morain and A. Guillevic showed that DLP in GF(p^2) is much faster than in a prime field of the same size, and even faster than a factorization of an RSA modulus of the same size.

Table 1. Comparison of running time for integer factorization (NFS-IF), discrete logarithm in prime field (NFS-DL(p)) and in quadratic field (NFS-DL(p 2)) of same global size 180 dd.

Algorithm	relation collection	linear algebra	total
NFS-IF	5 years	5.5 months	5.5 years
NFS-DL(p)	50 years	80 years	130 years
NFS-DL(p^2)	157 days	18 days (GPU)	0.5 years

F. Morain and A. Guillevic contributed with P. Gaudry and E. Thomé to other DL computation records in finite fields GF(p^3) of 508 bits and 512 bits, and GF(p^4) of 392 bits. The practical difficulty is increasing with the extension degree.

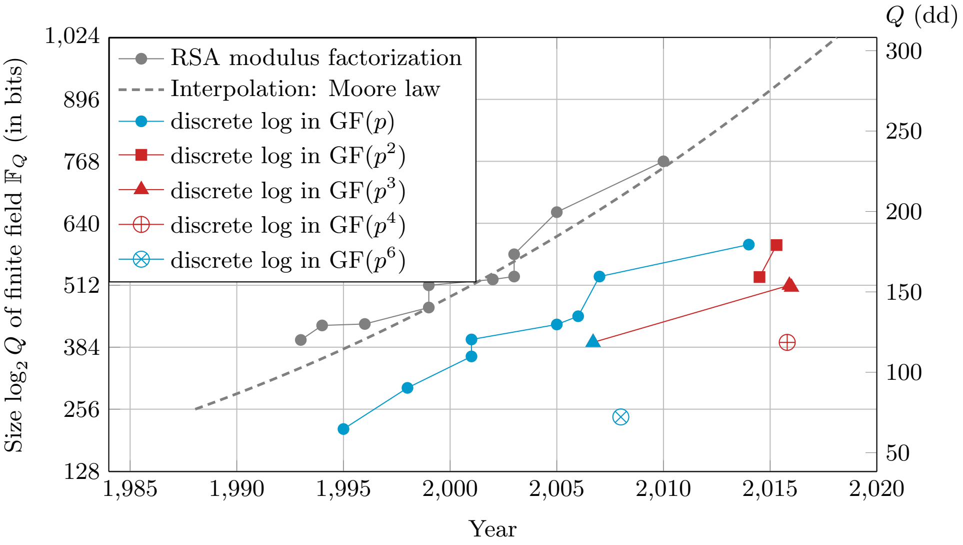

Figure 1. Records of DL computation in finite fields, and RSA modulus factorization. F. Morain and A. Guillevic contributed to the records in red in 2014–2015.

CATREL conference

The 1st and 2nd of October 2015, F. Morain, B. Smith and A. Guillevic organized an international workshop to conclude the CATREL project. There were 14 invited speakers from all around the world, from Palaiseau with A. Guillevic to as far as Auckland in New Zealand with S. Galbraith. A. Joux presented an historical summary of DL computation from the 80’s. P. Gaudry, E. Thomé and C. Bouvier from the Caramel Team

(Inria Nancy), presented their contribution, and K. Bhargavan presented the Logjam attack. There were also members of abroad teams leader in discrete logarithm record breaking. G. Adj from Mexico and R. Granger and T. Kleinjung presented their recent records in small characteristic.

We hosted more than 50 participants for the two intensive days of the workshop. The schedule of the workshop is available on the following link. http://www.lix.polytechnique.fr/cryptologie/CATREL-workshop

AGC^{2}T 15

A. Couvreur was one of the organizers of the conference AGC^{2}T 15 (Arithmetic Geometry Cryptography and Coding Theory) at CIRM (Marseille).

6. New Software and Platforms

6.1. Fast Compact Diffie-Hellman

KEYWORD: Cryptography
FUNCTIONAL DESCRIPTION

A competitive, high-speed, open implementation of the Diffie–Hellman protocol, targeting the 128-bit security level on Intel platforms. This download contains Magma files that demonstrate how to compute scalar multiplications on the x-line of an elliptic curve using endomorphisms. This accompanies the EuroCrypt 2014 paper by Costello, Hisil and Smith, the full version of which can be found here: http://eprint.iacr.org/2013/692 . The corresponding SUPERCOP-compatible crypto_dh application can be downloaded from http://hhisil.yasar.edu.tr/files/hisil20140318compact.tar.gz .

- Participant: Benjamin Smith
- Contact: Benjamin Smith
- URL: http://research.microsoft.com/en-us/downloads/ef32422a-af38-4c83-a033-a7aafbc1db55/

6.2. Platforms

6.2.1. ACTIS: Algorithmic Coding Theory in Sage

FUNCTIONAL DESCRIPTION

The aim of this project is to vastly improve the state of the error correcting library in Sage. The existing library does not present a good and usable API, and the provided algorithms are very basic, irrelevant, and outdated. We thus had two directions for improvement:

1. renewing the APIs to make them actually usable by researchers, and
2. incorporating efficient programs for decoding, like J. Nielsen's CodingLib, which contains many new algorithms.

After a year on the project, which started October 1st, 2014, we have been able to completely rethink and rewrite the API to a new structure able to support many mathematical constructions and integrate it in Sage. We also implemented numerous code classes and decoding algorithms, including cyclic codes over any finite field and list decoding of GRS codes, which are not available in Maple, Magma and Mathematica. As integrating code in Sage is a slow process, which requires external developers, we attended two Sage workshops (Sage Days 66 in Liège and Sage Days 70 in Berkeley) and welcomed one at Inria Saclay http://wiki.sagemath.org/GroupeUtilisateursParis#mercredi-1er-juillet-2015-module-de-codage-actis-pour-sage to spread the word on the project and meet the main Sage developers. We're now trusted members of the community, and we were able to integrate several patches in Sage.

- Contact: David Lucas
- URL: https://bitbucket.org/lucasdavid/sage_coding_project/wiki/Home
- One can check a full list of accepted and pending ACTIS patches for Sage here : http://trac.sagemath.org/ticket/18846.

7. New Results

7.1. Weight distribution of Algebraic-Geometry codes

V. Ducet worked on the weight distribution of geometric codes following a method initiated by Duursma. More precisely he implemented his method in magma and was able to compute the weight distribution of the geometric codes coming from two optimal curves of genus 2 and 3 over the finite fields of size 16 and 9 respectively. The aim is to compute the weight distribution of the Hermitian code over the finite field of size 16, for which computational improvements of the implementation are necessary.

7.2. Faster elliptic and hyperelliptic curve cryptography

B. Smith made several contributions to the development of faster arithmetic on elliptic curves and genus 2 Jacobians in 2015. First, an extended and more detailed treatment of his $\mathbb{Q}$-curve construction for endomorphism-accelerated elliptic curves (previously presented at ASIACRYPT 2013, and the basis of a successful implementation with C. Costello and H. Hisil presented at EUROCRYPT 2014) appeared in the Journal of Cryptology. A simplified approach to essential precomputations was published in the proceedings of AGCT-14. Finally, with C. Costello and P.-N. Chung, he gave a new, efficient, uniform, and constant-time scalar multiplication algorithm for genus 2 Jacobians exploiting fast Kummer surface arithmetic and features of differential addition chains.

7.3. Quantum factoring

Integer factorization via Shor's algorithm is a benchmark problem for general quantum computers, but surprisingly little work has been done on optimizing the algorithm for use as a serious factoring tool once large quantum computers are built (rather than as a proof of concept). In the meantime, given the limited size of contemporary quantum computers and the practical difficulties involved in building them, any optimizations to quantum factoring algorithms can lead to significant practical improvements. In a new interdisciplinary project with physicists F. Grosshans and T. Lawson, F. Morain and B. Smith have derived a simple new quantum factoring algorithm for cryptographic integers; its expected runtime is lower than Shor's factoring algorithm, and it should also be easier to implement in practice.

7.4. Cryptanalysis of code based cryptosystems by filtration attacks

The McEliece encryption scheme based on binary Goppa codes was one of the first public-key encryption schemes [35]. Its security rests on the difficulty of decoding an arbitrary code. The original proposal uses classical Goppa codes, and while it still remains unbroken, it requires a huge size of key. On the other hand, many derivative systems based on other families of algebraic codes have been subject to key recovery attacks. Up to now, key recovery attacks were based either on a variant of Sidelnikov and Shestakov's attack [36], where the first step involves the computation of minimum-weight codewords, or on the resolution of a system of polynomial equations using Gröbner bases.

In [3], A. Couvreur, P. Gaborit, V. Gauthier, A. Otmani and J.-P. Tillich introduced a new paradigm of attack called *filtration attacks*. The general principle decomposes in two steps:

1. **Distinguishing** the public code from a random one using the square code operation.
2. **Computing a filtration** of the public code using the distinguisher, and deriving from this filtration an efficient decoding algorithm for the public code.

This new style of attack allowed A. Couvreur, A. Otmani and J.-P. Tillich to break (in polynomial time) McEliece based on wild Goppa codes over quadratic extensions [7] and more recently to break the BBCRS cryptosystem [20]. A. Couvreur, Irene Márquez–Corbella, and R. Pellikaan broke McEliece based on algebraic geometry codes from curves of arbitrary genus [5], [6] by reconstructing optimal polynomial time decoding algorithms from the raw data of a generator matrix.

7.5. Quantum LDPC codes

Quantum codes are the analogous of error correcting codes for a quantum computer. A well known family of quantum codes are the CSS codes due to Calderbank, Shor and Steane can be represented by a pair of matrices (H_X, H_Z) such that $H_X H_Z^T = 0$. As in classical coding theory, if these matrices are sparse, then the code is said to be LDPC. An open problem in quantum coding theory is to get a family of quantum LDPC codes whose asymptotic minimum distance is in $\Omega(n^\alpha)$ for some $\alpha > 1/2$. No such family is known and actually, only few known families of quantum LDPC codes have a minimum distance tending to infinity.

In an article in preparation, Benjamin Audoux (I2M, Marseille) and A. Couvreur investigate a problem suggested by Bravyi and Hastings. They studied the behaviour of iterated tensor powers of CSS codes and prove in particular that such families always have a minimum distance tending to infinity. They propose also 3 families of LDPC codes whose minimum distance is in $\Omega(n^\beta)$ for all $\beta < 1/2$.

7.6. Discrete Logarithm computations in finite fields with the NFS algorithm

The best discrete logarithm record computations in prime fields and large characteristic finite fields are obtained with Number Field Sieve algorithm (NFS) at the moment. This algorithm is made of four steps:

1. polynomial selection;
2. relation collection (with a sieving technique);
3. linear algebra (computing the kernel of a huge matrix, of millions of rows and columns);
4. individual discrete logarithm computation.

The two more time consuming steps are the relation collection step and the linear algebra step. The polynomial selection is quite fast but is very important since it determines the complexity of the algorithm. Selecting better polynomials is a key to improve the overall running-time of the NFS algorithm. The final step: individual discrete logarithm, was though to be quite fast but F. Morain and A. Guillevic showed that it has an increasing complexity with respect to the extension degree of the finite field. A. Guillevic proposed a new method to reduce considerably the complexity, with at most a factor two speed-up in the exponent [22].

In 2015, F. Morain and A. Guillevic released with P. Gaudry and R. Barbulescu a major discrete logarithm record in a quadratic finite field GF(p^2) of 180 decimal digits (dd), corresponding to 595 bits. This was presented at the international conference Eurocrypt [19].

7.6.1. *DL Record computation in a quadratic finite field GF*(p^2)

In order to compare the practical running time of discrete logarithm computation in prime fields and quadratic finite fields, F. Morain and A. Guillevic with P. Gaudry and R. Barbulescu launched a DL record in a 180dd finite field. The last DL record in a prime field was held by the CARAMEL team of Nancy, in 2014, in a 180 dd prime field. The parameters chosen for the quadratic finite field are the following.

$$\begin{aligned}
p &= \texttt{314159265358979323846264338327950288419716939937510582097494459230}\diagdown \\
& \texttt{781640628620899877709223} \\
\ell &= \texttt{392699081698724154807830422909937860524646174921888227621868074038}\diagdown \\
& \texttt{47705078577612484713653} \\
p-1 &= 6 \cdot h_0 \text{ with } h_0 \text{ a 89 dd prime number} \\
p+1 &= 8 \cdot \ell
\end{aligned}$$

The discrete logarithm computation was made modulo ℓ, the largest prime factor of the multiplicative subgroup $GF(p^2)^*$, so that a DL computation with generic methods of complexity $O(\sqrt{\ell})$ was impracticable.

The two polynomials used in the NFS algorithm were chosen to be the following:

$$\begin{aligned} f &= x^4+1 \\ g &= \texttt{448225077249286433565160965828828303618362474}\ x^2 - \texttt{29606109908476368046927513730655796265782} \\ &\quad + \texttt{448225077249286433565160965828828303618362474}\ . \end{aligned}$$

We indeed designed a new polynomial selection method, that we called the Conjugation method. It is very well suited for quadratic and cubic finite fields GF(p^2) and GF(p^3) for the size range of the records.

We finally computed the discrete logarithm in basis $G = T + 2$ of the target $s = \lfloor(\pi(2^{298})/8)\rfloor t + \lfloor(\gamma \cdot 2^{298})\rfloor$

$$\begin{aligned} \log_G s \ \equiv\ & \texttt{2762142436179128043003373492683066054037581738194144186101}\diagdown \\ & \texttt{98322785683188853924304990580l2}\ \bmod\ \ell. \end{aligned}$$

The running time was very surprising: our record was much faster than the concurrent DL computation in a prime field of the same global size of 180dd, and even faster than the RSA modulus factorization of the same size.

Table 2. Comparison of running time for integer factorization (NFS-IF), discrete logarithm in prime field (NFS-DL(p)) and in quadratic field (NFS-DL(p 2)) of same global size 180 dd.

Algorithm	relation collection	linear algebra	total
NFS-IF	5 years	5.5 months	5.5 years
NFS-DL(p)	50 years	80 years	130 years
NFS-DL(p^2)	157 days	18 days (GPU)	0.5 years

7.6.2. Individual discrete logarithm computation

A big difference between prime fields and finite fields of small extension such as GF(p^3), GF(p^4) and GF(p^6) is the complexity of the final step of the NFS algorithm: computing the individual discrete logarithm of the target, given the large table of discrete logarithm of *small* elements. This table was obtained at the end of the linear algebra step. The target needs to be decomposed into small enough elements whose discrete logarithm is in the table, so that one can recompose the discrete logarithm of the target. This decomposition is quite fast for prime fields but we realized that is becomes more and more time consuming when the extension degree increase. A. Guillevic developed a new technique to improve considerably this step. The main idea is to use the structure of the finite field: the subfields. These improvements were presented at the Asiacrypt 2015 conference in Auckland, New Zealand and published in the proceedings [22].

7.7. Information sets of multiplicity codes

The codes we used in our PIR protocols, namely Reed-Muller and their generalization Multiplicity codes, are locally *correctable* : that means that local decoding allows to retrieve encoded symbols. In most applications, it is very desirable to retrieve *information* symbols. Another line of work in this topic was thus to find an encoding method for multiplicity codes so as to directly recover an information symbol from local correction, and not an encoded symbol. To do so we defined information sets for multiplicity codes, and design a systematic encoding based on this information set. This work was presented at ISIT'2015 in Hong-Kong in June [18].

7.8. Rank metric codes over infinite fields

Rank metric and Gabidulin codes over the rationals promise interesting applications to space-time coding. We have constructed optimal codes, similar to Gabidulin codes, in the case of infinite fields. We use algebraic extensions, and we have determined the condition on the considered extension to enable this construction. For example: we can design codes with complex coefficients, using number fields and Galois automorphisms. Then, in the rank metric setting, codewords can be seen as matrices. In this setting, a channel introduces errors (a matrix of small rank r added to the codeword) and erasures (s_r rows and s_c columns of the matrix are erased). We have developed an algorithm (adapted from the Welch–Berlekamp algorithm) to recover the right codeword in the presence of an error of rank weight up to $r + s_c + s_r \leqslant d - 1$, where d is the minimal distance of the code. As opposed to the finite field case, we are confronted by coefficient size growth. We solve this problem by computing modulo prime ideals. Using these codes we can completely bypass intermediate constructions using finite fields, which were the stumbling-block in classic constructions.

We also have used this framework to build rank-metric codes over the field of rational functions, using algebraic function fields with cyclic Galois group (Kummer and Artin extensions). These codes can be seen as a generator of infinitely many convolutional codes.

7.9. Hash function cryptanalysis

Cryptographic hash functions are versatile primitives that are used in many cryptographic protocols. The security of a hash function h is usually evaluated through two main notions: its preimage resistance (given a target t, the difficulty of finding a message m s.t. $h(m) = t$) and its collision resistance (the difficulty of finding two messages m, m' s.t. $h(m) = h(m')$).

A popular hash function is the SHA-1 algorithm. Although theoretical collision attacks were found in 2005, it is still being used in some applications, for instance as the hash function in some TLS certificates. Hence cryptanalysis of SHA-1 is still a major topic in cryptography.

In 2015, we improved the state-of-the-art on SHA-1 analysis in two ways:

- T. Espitau, P.-A. Fouque and P. Karpman improved the previous preimage attacks on SHA-1, reaching up to 62 rounds (out of 80), up from 57. The corresponding paper was published at CRYPTO 2015 [21].
- P. Karpman, T. Peyrin and M. Stevens developed collision attacks on the compression function of SHA-1 (i.e. freestart collisions). This exploits a model that is slightly more generous to the attacker in order to find explicit collisions on more rounds than what was previously possible. A first work resulted in freestart collisions for SHA-1 reduced to 76 steps; this attack takes less than a week to compute on a common GPU. The corresponding paper was published at CRYPTO 2015 [24]. This was later improved to attack the full compression function. Although the attack is more expensive it is still practical, taking less than two weeks on a 64 GPU cluster. The corresponding paper is currently under review for EUROCRYPT 2016 [32].

7.10. Block cipher design and analysis

Block ciphers are one of the most basic cryptographic primitives, yet block cipher analysis is still a major research topic. In recent years, the community also shifted focus to the more general setting of *authenticated encryption*, where one specifies an (set of) algorithm(s) providing both encryption and authentication for messages of arbitrary length. A major current event in that direction is the CAESAR academic competition, which aims to select a portfolio of good algorithms.

During this year, we helped to improve the state of the art in block cipher research in several ways:

- P. Karpman found a very efficient related-key attack on the CAESAR candidate Prøst-OTR. A related-key model is very generous to the attacker, but the attack in this case can be run instantaneously. The corresponding paper was published at ISC 2015 [23]

- B. Minaud, P. Derbez, P.-A. Fouque and P. Karpman developed a family of attacks that breaks all the remaining unbroken instances of the ASASA construction, that was presented at ASIACRYPT 2014. Using algebraic properties of the ciphers, for each type of instance, the attack allows to recover an algorithm equivalent to the secret key in near-practical time. This applies to a multivariate public-key scheme, a classical block cipher and small block ciphers used in white-box constructions. The corresponding paper was published at ASIACRYPT 2015 and was honoured as one of the three best papers of the conference [25].
- P. Karpman developed a compact 8-bit S-box with branch number three, which can be used as a basis to construct a lightweight block cipher particularly efficient on 8-bit microcontrollers. The corresponding paper is currently under review for FSE 2016.

8. Bilateral Contracts and Grants with Industry

8.1. Bilateral Grants with Industry

8.1.1. Alcatel-Lucent

Within the framework of the joint lab Inria-ALU, Grace and Alcatel-Lucent collaborate on the topic of Private Information Retrieval: that is, enabling a user to retrieve data from a remote database while revealing neither the query nor the retrieved data. (This is not the same as data confidentiality, which refers to the need for users to ensure secrecy of their data; this is classically obtained through encryption, which prevents access to data in the clear.)

A typical application would be a centralized database of medical records, which can be accessed by doctors, nurses, and so on. A desirable privacy goal would be that the central system does not know which patient is queried for when a query is made, and this goal is precisely achieved by a Private Information Retrieval protocol. Note also that in this scenario the database is not encrypted, since many users are allowed to access it.

We are exploring applications of Locally Decodable Codes to Private Information Retrieval in the multi-cloud (multi-host) setting, to ensure both secure, reliable storage, and privacy of database queries.

Our progress on information sets of multiplicity codes was presented at the ISIT 2015 conference [18]

9. Partnerships and Cooperations

9.1. Regional Initiatives

9.1.1. PEPS Aije-bitcoin

Within the group PAIP (Pour une Approche Interdisciplinaire de la Privacy), D. Augot presented the cryptographic and peer-to-peer principles at the heart of the Bitcoin protocol (electronic signature, hash functions, and so on). Most of the information is publicly available: the history of all transactions, evolution of the source code, developers' mailing lists, and the Bitcoin exchange rate. It was recognized by the economists in our group that such an amount of data is very rare for an economic phenomenon, and it was decided to start research on the history of Bitcoin, to study the interplay between the development of protocol and the development of the economical phenomenon.

The project **Aije-Bitcoin** (analyse informatique, juridique et économique de Bitcoin) was accepted as interdisciplinary research for a PEPS (Projet exploratoire Premier Soutien) cofunded by the CNRS and Université de Paris-Saclay. This one-year preliminary program will enable the group to master the understanding of Bitcoin from various angles, allowing more advanced research in the following years.

Two M2 interns, Loïs Saublet and Kofi Manful, have been hired, located in Aviz team, and D. Augot co-supervised them with Petra and Tobias Isenberg.

9.1.2. IDEALCODES

Idealcodes is a two-year Digiteo research project, started in October 2014. The partners involved are the École Polytechnique (X) and the Université de Versailles–Saint-Quentin-en-Yvelines (Luca de Feo, UVSQ). After hiring J. Nielsen the first year, we have hired V. Ducet for the second year, both working at the boundary between coding theory, cryptography, and computer algebra

Idealcodes spans the three research areas of algebraic coding theory, cryptography, and computer algebra, by investigating the problem of lattice reduction (and root-finding). In algebraic coding theory this is found in Guruswami and Sudan's list decoding of algebraic geometry codes and Reed–Solomon codes. In cryptography, it is found in Coppersmith's method for finding small roots of integer equations. These topics were unified and generalised by H. Cohn and N. Heninger [33], by considering algebraic geometry codes and number field codes under the deep analogy between polynomials and integers. Sophisticated results in coding theory could be then carried over to cryptanalysis, and vice-versa. The generalized view raises problems of computing efficiently, which is one of the main research topics of Idealcodes.

9.2. National Initiatives

9.2.1. ANR

- CATREL (accepted June 2012, ending December 2015): "Cribles: Améliorations Théoriques et Résolution Effective du Logarithme" (Sieve Algorithms: Theoretical Advances and Effective Resolution of the Discrete Logarithm Problem). This project aims to make effective "attacks" on reduced-size instances of the discrete logarithm problem (DLP). This is a key ingredient for the assessment of the security of cryptosystems relying on the hardness of the DLP in finite fields, and for deciding on relevant key sizes.
- MANTA (accepted July 2015, starting January 2016): "Curves, surfaces, codes and cryptography". This project deals with applications of coding theory error correcting codes to in cryptography, multiparty computation, and complexity theory, using advanced topics in algebraic geometry and number theory. See http://anr-manta.inria.fr/

9.2.2. DGA

- DIFMAT-3: this one-year project aims to find matrices with good diffusion properties over small finite fields. The principle is to find non-maximal matrices, but with better coefficients and implementation properties. The relevant cryptographic properties to be studied correspond to the weight distribution of the associated code. Since we use Algebraic-Geometry codes, much more powerful techniques can be used for computing these weight distribution, using and improving Duursma's ideas [34].
- Cybersecurity. Inria and DGA contracted for three PhD topics at the national level, one of them involving Grace. Grace started a new PhD, and hired P. Karpman. The topic of this PhD is complementary to the above DIFMAT-3: while DIFMAT-3 provides fundamental methods for dealing with AG codes, in application for diffusion layers in block ciphers, the topic here is to make concrete propositions of block ciphers using these matrices. P. Karpman is coadvised by T. Peyrin (Nanyang Technological University, Singapore), by P.-A. Fouque (Université de Rennes), and D. Augot.

9.3. European Initiatives

9.3.1. FP7 & H2020 Projects

9.3.1.1. PQCRYPTO

Title: Post-quantum cryptography for long-term security

Programm: H2020

Duration: March 2015 - March 2018

Coordinator: TECHNISCHE UNIVERSITEIT EINDHOVEN

Partners:

Academia Sinica (Taiwan)

Bundesdruckerei (Germany)

Danmarks Tekniske Universitet (Denmark)

Katholieke Universiteit Leuven (Belgium)

Nxp Semiconductors Belgium Nv (Belgium)

Ruhr-Universitaet Bochum (Germany)

Stichting Katholieke Universiteit (Netherlands)

Coding Theory and Cryptology group, Technische Universiteit Eindhoven (Netherlands)

Technische Universitaet Darmstadt (Germany)

University of Haifa (Israel)

Inria contact: Nicolas Sendrier

Online security depends on a very few underlying cryptographic algorithms. Public-key algorithms are particularly crucial since they provide digital signatures and establish secure communication. Essentially all applications today are based on RSA or on the discrete-logarithm problem in finite fields or on elliptic curves. Cryptographers optimize parameter choices and implementation details for these systems and build protocols on top of these systems; cryptanalysts fine-tune attacks and establish exact security levels for these systems.

It might seem that having three systems offers enough variation, but these systems are all broken as soon as large quantum computers are built. The EU and governments around the world are investing heavily in building quantum computers; society needs to be prepared for the consequences, including cryptanalytic attacks accelerated by these computers. Long-term confidential documents such as patient health-care records and state secrets have to guarantee security for many years, but information encrypted today using RSA or elliptic curves and stored until quantum computers are available will then be as easy to decipher.

PQCRYPTO will allow users to switch to post-quantum cryptography: cryptographic systems that are not merely secure for today but that will also remain secure long-term against attacks by quantum computers. PQCRYPTO will design a portfolio of high-security post-quantum public-key systems, and will improve the speed of these systems, with reference implementations.

9.3.2. Major European Organizations with which the Team have followed Collaborations

Program: COST

Project acronym: COST 4175/11

Project title: Random Network Coding and Designs over GF(q) http://www.network-coding.eu/index.html

Duration: 04/2012 - 04/2016

Coordinator: Marcus Greferath

Other partners: Camilla Hollanti, Aalto University, Finland Simon R. Blackburn, Royal Holloway, University of London, UK Tuvi Etzion, Technion, Israel Ángeles Vázquez-Castro, Autonomous University of Barcelona, Spain Joachim Rosenthal, University of Zurich, Switzerland (Chairs of the five working groups).

Abstract: Random network coding emerged through an award-winning paper by R. Koetter and F. Kschischang in 2008 and has since then opened many new directions in networking, internet, wireless communication systems, and cloud computing. This COST Action will set up a European research network and establish network coding as a European core area in communication technology. Its aim is to bring together experts from pure and applied mathematics, computer science, and electrical engineering, who are working in the areas of discrete mathematics, coding theory, information theory, and related fields.

9.4. International Initiatives

9.4.1. Inria International Partners

9.4.1.1. Informal International Partners

- P. Beelen, J. Nielsen, DTU Lyngby
- M. Bossert, Ulm Universität
- S. Galbraith, Department of Mathematics, University of Auckland.

9.5. International Research Visitors

9.5.1. Internships

- C. Berghoff is a visiting Phd student, from Bonn Universität.

10. Dissemination

10.1. Promoting Scientific Activities

10.1.1. Scientific events organisation

10.1.1.1. Member of the organizing committees

- D. Augot is member of the committee of the CCA seminar on coding and cryptology. This seminar regularly attracts around 30 participants.
- A. Couvreur organized with David Kohel (I2M, Marseille) and Alp Bassa (Bogazici University, Turkey) the conference AGC^{2}T 15 (Arithmetic Geometry, Cryptography, and Coding Theory) at CIRM (Marseille). This 15th edition of this international conference happened from May 18 to 22, 2015.
- F. Morain, B. Smith and A. Guillevic were the organizers of Advances in Discrete Logarithms, an international workshop on discrete logarithms to conclude the CATREL project, at École polytechnique from October 1 to 2, 2015.
- P. Lebacque and B. Smith organized Arithmetic Geometry: Explicit Methods and Applications with C. Ritzenthaler and A. Zykin. This was an international number theory conference, held in Moscow from December 7 to 11, 2015.
- A. Guillevic and P. Karpman were members of the local organizing team of CHES 2015 (Cryptographic Harware and Embedded Systems), at Saint-Malo, France, in September.

10.1.2. Scientific events selection

10.1.2.1. Member of the conference program committees

- A. Couvreur was member of the program committee of *Journées Codes et Cryptographie 2015*, La Londe les Maure. October 2015.

- A. Couvreur was member of the program committee of WCC (Workshop on Codes and Cryptology) 2015. Paris, May 2015.
- A. Couvreur was member of the scientific committee of the *École Mathématique Africaine: Theorie des nombres et Cryptologie, Équations aux dérivées partielles, analyse numérique et calcul scientifique*. March 2015, Franceville (Gabon).

10.1.2.2. Reviewer

- D. Augot was reviewer for
  - ISIT 2015 (International Symposium on Information Theory)
  - CAI 2015 (6th International Conference on Algebraic Informatics)
  - SODA 2016 (Symposium on Discrete Algorithms)
- A. Couvreur was reviewer for
  - PQCrypto 2016.
- P. Karpman was reviewer for
  - ACNS 2015
  - CRYPTO 2015
  - ASIACRYPT 2015
  - INDOCRYPT 2015
  - EUROCRYPT 2016
  - FSE 2016
- B. Smith was a reviewer for
  - MEGA 2015
  - PKC 2015
  - EUROCRYPT 2016

10.1.3. Journal

10.1.3.1. Member of the editorial boards

- D. Augot is member of the editorial board of the *RAIRO - Theoretical Informatics and Applications*, a Cambridge journal published by EDP Sciences.
- D. Augot is member of the editorial board of the *International Journal of Information and Coding Theory*, InderScience publishers.

10.1.3.2. Reviewer - Reviewing activities

- D. Augot was a reviewer for
  - Designs, Codes and Cryptography
  - IEEE Transactions on Information Theory
  - Discrete Mathematics
  - Transactions on Computers
  - Applicable Algebra in Engineering, Communication and Computing
  - Advances in Mathematics of Communications
  - Ars Comb
- A. Couvreur was reviewer for
  - Finite Fields Appl.
  - Des. Codes Cryptogr.
  - Mosc. Math. J.
  - J. Numbers.

- B. Smith was a reviewer for
  - Journal of Cryptology
  - SICOMP (SIAM Journal on Computing)

10.1.4. Invited talks

- D. Augot was invited to the colloquium of IRMAR, Rennes
- D. Augot was invited to the workshop "Codage et cryptographie", USTHB, Algiers, November 2-5.
- A. Couvreur was invited at the seminar of number theory of University of Oxford.
- A. Couvreur was invited speaker at the conference *Arithmetic Geometry: explicit methods and applications*, Moscow, december 2015.
- A. Guillevic was invited at the Workshop in Elliptic Curve Cryptography (ECC), Bordeaux, September 2015.
- A. Guillevic was invited at the CATREL Workshop on Discrete Logarithms organized by the GRACE team at Palaiseau, October 2015.
- P. Karpman was invited at the RISC seminar of CWI, Amsterdam.
- B. Smith was an invited speaker in the LFANT seminar, Bordeaux, February 2015
- B. Smith was an invited speaker in the security seminar at University College London, UK, May 2015
- B. Smith was an invited speaker at the Colóquio de Geometria e Aritmética (Geometry and Arithmetic Colloquium) at IMPA, Rio de Janeiro, Brazil, October 2015
- B. Smith gave an invited Tech Talk at Cisco France, Paris, November 2015
- B. Smith gave an invited talk in the cryptography and security seminar at Radboud University Nijmegen, Netherlands, December 2015

10.1.5. Leadership within the scientific community

Together with Inria Nancy Caramel team, we are leader on records discrete logarithms, thanks to the CATREL project, which delivered the CADO-NFS software, and to our experience to run hard computationnal projects to achieve these records. We have also proposed the best curves for cryptographic computations.

10.1.6. Scientific expertise

- D. Augot explained the fundamental concepts underlying bitcoin to the “Direction de la prospective de la Poste”

10.1.7. Research administration

Committees

- A. Couvreur is an elected member of Saclay’s *comité de centre*.
- A. Couvreur is an elected member of Saclay’s *Comité local Hygiène, Sécurité et Conditions de Travail*.
- A. Couvreur is the *jeune chercheur référent* for the *commission de suivi doctoral* of Inria Saclay.
- D. Augot is a member of LIX’s *conseil de direction*.
- D. Augot is the vice-head of Inria’s *comité de suivi doctoral*
- D. Augot is a member of LIX’s *conseil de laboratoire*
- D. Augot is elected member of the *conseil académique consultatif* of Paris-Saclay University.
- B. Smith was a reviewer for ANRT CIFRE funding.
- F. Morain and B. Smith are elected members of the *Conseil de Laboratoire* of the LIX.
- F. Morain is vice-head of the Département d’informatique of Ecole Polytechnique.
- F. Morain represents École polytechnique in the committee in charge of *Mention HPC* in the *Master de l’université Paris Saclay*.
- F. Morain is member of the Board of Master Parisien de Recherche en Informatique (MPRI).
- B. Smith is a *Correspondant* for International Relations at Saclay.
- B. Smith is a member of the COST-GTRI.
- B. Smith is a member of the teaching committee of the Department of Computer Science of the École polytechnique.

Juries

- D. Augot was in committee assessing candidates for Institut Mines-Télécom.

10.2. Teaching - Supervision - Juries

10.2.1. Teaching

Licence

A. Couvreur, INF311: “Introduction à l’informatique”, 40h (equiv TD), L3, École polytechnique, France

A. Couvreur INF411: “Les bases de la programmation et de l’algorithmique”, 32h (equiv TD), M1, École polytechnique, France

F. Levy-dit-Vehel, “Cours de Cryptographie”, 30h. (equiv TD), 3rd year (M1), ENSTA ParisTech, France.

F. Levy-dit-Vehel, “Mathématiques discrètes pour la protection de l’information”, 24h (equiv TD), 2nd year (L3), ENSTA ParisTech, France.

F. Morain, Lectures for INF311: “Introduction à l’informatique”, 15h (equiv TD), 1st year (L3), École polytechnique. Coordinator of this module (350 students).

B. Smith, INF442: “Traitement des données massives”, 32h (equiv TD), L4, École polytechnique, France

Master

A. Couvreur, “Error-correcting codes and applications to cryptography”, 12h (equiv TD), M2, MPRI, France.

F. Morain, “Algorithmes arithmétiques pour la cryptologie”, 9h (equiv TD), M2, MPRI, France.

F. Morain, Lectures for INF568: “Cryptology”, 13.5h (equiv TD), 3rd year (M1), École polytechnique, France.

B. Smith, “Algorithmes arithmétiques pour la cryptologie”, 13.5h (equiv TD), M2, MPRI, France.

B. Smith, Cryptologie, 18h (equiv TD), M1, École polytechnique, France

10.2.2. Supervision

- PhD: G. Robert defended his thesis on December 4th, 2015 [12].
- PhD in progress. J. Lavauzelle has began his Ph.D. on locally decodable codes and cryptogra[hic applications, on October 1st, 2015, under the supervision of D. Augot and F. Levy-dit-Vehel.
- PhD in progress. E. Barelli has begun his PhD on Algebraic-Geometry codes for code-based crypto on October 1st, 2015, under the supervision of D. Augot and A. Couvreur.
- PhD in progress. N. Duhamel has begun his PhD on genus 2 curves for cryptography, under the supervision of B. Smith and F. Morain.
- PhD in progress. P. Karpman, starting in 2013, will defend in 2016 his PhD on security of symmetric crytographic primitives.

10.2.3. Juries

- D. Augot was reviewer of
  - J. Roué PhD thesis, “Analyse de la résistance des chiffrements par blocs aux attaques linéaires et différentielles”, Université Pierre et Marie Curie
  - F. de Portzamparc PhD thesis, “Algebraic and Physical Security in Code-Based Cryptography”, Université Pierre et Marie Curie
- A. Couvreur

  - was reviewer of F. de Portzamparc PhD thesis, “Algebraic and Physical Security in Code-Based Cryptography”, Université Pierre et Marie Curie
  - is member of the Jury of Agrégation de Mathématiques and in charge of option C (*Algèbre et calcul formel*)
- B. Smith
  - was an examiner for L. Xu’s PhD thesis, “Vérification formelle de la vie privée dans les systèmes concurrents”, École polytechinique, 4/5/2015.

10.3. Popularization

- D. Augot gave a lecture about bits, exclusive-or, coding and digital pictures, at Lycée de la vallée de Chevreuse (Jan 22)
- D. Augot, N. Duhamel, A. Guillevic, J. Lavauzelle, D. Lucas, and B. Smith participated in the Fête la Science at École polytechnique (Oct 12)
- A. Couvreur gave a conference “Les mathématiques pour protéger l’information” for the pupils of Collège Moreau in Monthléry (91).

10.4. Institutional commitment

- F. Levy-dit-Vehel is member of ENSTA ParisTech working group “compétences et validation des acquis de l’expérience”.
- B. Smith was “responsable des bureaux” (responsible for allocating desks and offices) at LIX.

11. Bibliography

Major publications by the team in recent years

[1] D. Augot, M. Finiasz. *Direct Construction of Recursive MDS Diffusion Layers using Shortened BCH Codes*, in "21st International Workshop on Fast Software Encryption, FSE 2014", London, United Kingdom, C. Cid, C. Rechberger (editors), springer, March 2014, https://hal.inria.fr/hal-01044597

[2] A. Couvreur. *Codes and the Cartier Operator*, in "Proceedings of the American Mathematical Society", March 2014, vol. 142, pp. 1983-1996, https://hal.inria.fr/hal-00710451

[3] A. Couvreur, P. Gaborit, V. Gauthier-Umana, A. Otmani, J.-P. Tillich. *Distinguisher-based attacks on public-key cryptosystems using Reed-Solomon codes*, in "Designs, Codes and Cryptography", 2014, vol. 73, n^{o} 2, pp. 641-666 [*DOI :* 10.1007/s10623-014-9967-z], https://hal.archives-ouvertes.fr/hal-01096172

[4] A. Couvreur, P. Gaborit, V. Gautier, A. Otmani, J.-P. Tillich. *Distinguisher-Based Attacks on Public-Key Cryptosystems Using Reed-Solomon Codes*, in "WCC 2013 - International Workshop on Coding and Cryptography", Bergen, Norway, Selmer Center at the University of Bergen, Norway and Inria, Rocquencourt, France, April 2013, pp. 181-193, https://hal.archives-ouvertes.fr/hal-00830594

[5] A. Couvreur, I. Márquez-Corbella, R. Pellikaan. *A Polynomial Time Attack against Algebraic Geometry Code Based Public Key Cryptosystems*, in "Information Theory (ISIT), 2014 IEEE International Symposium on", Honolulu, United States, IEEE, June 2014, pp. 1446-1450 [*DOI :* 10.1109/ISIT.2014.6875072], https://hal.archives-ouvertes.fr/hal-00937476

[6] A. Couvreur, I. Márquez-Corbella, R. Pellikaan. *Cryptanalysis of public-key cryptosystems that use subcodes of algebraic geometry codes*, in "4th ICMCTA - Fourth International Castle Meeting on Coding Theory and Applications", Palmela, Portugal, September 2014, https://hal.inria.fr/hal-01069272

[7] A. Couvreur, A. Otmani, J.-P. Tillich. *Polynomial Time Attack on Wild McEliece Over Quadratic Extensions*, in "EUROCRYPT 2014", Copenhagen, Denmark, May 2014, pp. 17-39, https://hal.archives-ouvertes.fr/hal-00931774

[8] P. Lebacque, A. Zykin. *On the Number of Rational Points of Jacobians over Finite Fields*, in "Acta Arith.", 2015, vol. 169, pp. 373–384, https://hal.archives-ouvertes.fr/hal-01081468

[9] F. Morain. *Implementing the asymptotically fast version of the elliptic curve primality proving algorithm*, in "Math. Comp.", 2007, vol. 76, pp. 493–505

[10] B. Smith. *Isogenies and the discrete logarithm problem in Jacobians of genus 3 hyperelliptic curves*, in "J. of Cryptology", 2009, vol. 22, n^{o} 4, pp. 505-529

[11] B. Smith. *Families of fast elliptic curves from Q-curves*, in "Advances in Cryptology - ASIACRYPT 2013", Bangalore, India, K. Sako, P. Sarkar (editors), Lecture Notes in Computer Science, Springer, December 2013, vol. 8269, pp. 61-78 [*DOI :* 10.1007/978-3-642-42033-7_4], https://hal.inria.fr/hal-00825287

Publications of the year

Doctoral Dissertations and Habilitation Theses

[12] G. Robert. *Gabidulin codes in characteristic 0. Application to space-time coding*, Université de Rennes 1, December 2015, https://hal.inria.fr/tel-01243508

Articles in International Peer-Reviewed Journals

[13] C. Gonçalves. *A Point Counting Algorithm for Cyclic Covers of the Projective Line*, in "Contemporary Mathematics Series", April 2015, vol. 637, 145 p. , https://hal.archives-ouvertes.fr/hal-01054645

[14] J. S. R. Nielsen, P. Beelen. *Sub-quadratic Decoding of One-point Hermitian Codes*, in "IEEE Transactions on Information Theory", April 2015, vol. 61, n^{o} 6, pp. 3225-3240 [*DOI :* 10.1109/TIT.2015.2424415], https://hal.inria.fr/hal-01245062

[15] J. Pieltant, H. Randriam. *New uniform and asymptotic upper bounds on the tensor rank of multiplication in extensions of finite fields*, in "Mathematics of Computation", July 2015, vol. 84, n^{o} 294, pp. 2023–2045 [*DOI :* 10.1090/S0025-5718-2015-02921-4], https://hal.archives-ouvertes.fr/hal-00828153

[16] B. Smith. *Easy scalar decompositions for efficient scalar multiplication on elliptic curves and genus 2 Jacobians*, in "Contemporary Mathematics Series", May 2015, vol. 637, 15 p. , https://hal.inria.fr/hal-00874925

[17] B. Smith. *The Q-curve construction for endomorphism-accelerated elliptic curves*, in "Journal of Cryptology", 2015, 27 p. [*DOI :* 10.1007/s00145-015-9210-8], https://hal.inria.fr/hal-01064255

International Conferences with Proceedings

[18] D. AUGOT, F. LEVY-DIT-VEHEL, M. C. NGÔ. *Information Sets of Multiplicity Codes*, in "Information Theory (ISIT), 2015 IEEE International Symposium on", Hong-Kong, China, IEEE, June 2015, pp. 2401 - 2405 [*DOI :* 10.1109/ISIT.2015.7282886], https://hal.inria.fr/hal-01188935

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

[20] A. COUVREUR, A. OTMANI, J.-P. TILLICH, V. GAUTHIER-UMANA. *A Polynomial-Time Attack on the BBCRS Scheme*, in "Practice and Theory in Public-Key Cryptography - PKC 2015", Washington, United States, LNCS, March 2015, https://hal.archives-ouvertes.fr/hal-01104078

[21] T. ESPITAU, P.-A. FOUQUE, P. KARPMAN. *Higher-Order Differential Meet-in-the-middle Preimage Attacks on SHA-1 and BLAKE*, in "35th International Cryptology Conference - CRYPTO 2015", Santa Barbara, United States, R. GENNARO, M. ROBSHAW (editors), Springer, August 2015, pp. 683-701 [*DOI :* 10.1007/978-3-662-47989-6_33], https://hal.inria.fr/hal-01183070

[22] A. GUILLEVIC. *Computing Individual Discrete Logarithms Faster in GF(p^n) with the NFS-DL Algorithm*, in "Asiacrypt 2015", Auckland, New Zealand, T. IWATA, J. H. CHEON (editors), Springer, November 2015, https://hal.inria.fr/hal-01157378

[23] P. KARPMAN. *From Distinguishers to Key Recovery: Improved Related-Key Attacks on Even-Mansour*, in "Information Security Conference 2015", Trondheim, Norway, Information Security, Springer Verlag, September 2015 [*DOI :* 10.1007/978-3-319-23318-5_10], https://hal.inria.fr/hal-01245365

[24] P. KARPMAN, T. PEYRIN, M. STEVENS. *Practical Free-Start Collision Attacks on 76-step SHA-1*, in "35th International Cryptology Conference - CRYPTO 2015", Santa Barbara, United States, R. GENNARO, M. ROBSHAW (editors), Springer, August 2015, pp. 623-642 [*DOI :* 10.1007/978-3-662-47989-6_30], https://hal.inria.fr/hal-01183066

[25] B. MINAUD, P. DERBEZ, P.-A. FOUQUE, P. KARPMAN. *Key-Recovery Attacks on ASASA*, in "International Conference on the Theory and Application of Cryptology and Information Security 2015 - ASIACRYPT 2015", Auckland, New Zealand, T. IWATA, J. H. CHEON (editors), Advances in Cryptology - ASIACRYPT 2015, Springer Verlag, November 2015 [*DOI :* 10.1007/978-3-662-48800-3_1], https://hal.inria.fr/hal-01245381

Conferences without Proceedings

[26] W. LI, J. S. R. NIELSEN, S. PUCHINGER, V. SIDORENKO. *Solving Shift Register Problems over Skew Polynomial Rings using Module Minimisation*, in "International Workshop on Coding and Cryptography 2015", Paris, France, April 2015, https://hal.inria.fr/hal-01245068

Other Publications

[27] B. AUDOUX, A. COUVREUR. *On tensor products of CSS Codes*, December 2015, working paper or preprint, https://hal.archives-ouvertes.fr/hal-01248760

[28] P. N. Chung, C. Costello, B. Smith. *Fast, uniform, and compact scalar multiplication for elliptic curves and genus 2 Jacobians with applications to signature schemes*, October 2015, working paper or preprint, https://hal.inria.fr/hal-01214259

[29] F. Grosshans, T. Lawson, B. Smith, F. Morain. *Factoring Safe Semiprimes with a Single Quantum Query*, November 2015, working paper or preprint, https://hal.inria.fr/hal-01229587

[30] P. Karpman. *Exercice de style*, January 2016, working paper or preprint, https://hal.inria.fr/hal-01263735

[31] C. Ritzenthaler, R. Lercier, F. Rovetta, J. Sijsling, B. Smith. *Distributions of traces of Frobenius for smooth plane curves over finite fields*, October 2015, working paper or preprint, https://hal.inria.fr/hal-01217995

[32] M. Stevens, P. Karpman, T. Peyrin. *Freestart collision on full SHA-1*, October 2015, working paper or preprint, https://hal.inria.fr/hal-01251023

References in notes

[33] H. Cohn, N. Heninger. *Ideal forms of Coppersmith's theorem and Guruswami-Sudan list decoding*, in "Innovations in Computer Science - ICS 2010, Tsinghua University, Beijing, China, January 7-9, 2011. Proceedings", B. Chazelle (editor), Tsinghua University Press, 2011, pp. 298-308

[34] I. M. Duursma. *Weight distributions of geometric Goppa codes*, in "Trans. Amer. Math. Soc.", 1999, vol. 351, n^{o} 9, pp. 3609–3639, http://dx.doi.org/10.1090/S0002-9947-99-02179-0

[35] R. J. McEliece. *A Public-Key System Based on Algebraic Coding Theory*, Jet Propulsion Lab, 1978, pp. 114–116, DSN Progress Report 44

[36] V. Sidelnikov, S. Shestakov. *On the insecurity of cryptosystems based on generalized Reed-Solomon codes*, in "Discrete Math. Appl.", 1992, vol. 1, n^{o} 4, pp. 439-444