Activity Report 2014

Project-Team GRACE

Geometry, arithmetic, algorithms, codes and encryption

RESEARCH CENTER
Saclay - Île-de-France

THEME
Algorithmics, Computer Algebra and Cryptology

Table of contents

Project-Team GRACE

Keywords: Cryptography, Complexity, Algorithmic Number Theory, Error Detection And Correction, Security, Computer Algebra

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

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, on leave]
François Morain [Ecole Polytechnique, Professor, HdR]
Françoise Levy-Dit-Vehel [ENSTA, HdR]

Engineer
David Lucas [Inria]

PhD Students
Cécile Goncalves [Ecole Polytechnique]
Pierre Karpman [Inria]
Manh Cuong Ngo [Inria, from Feb 2014]
Gwezheneg Robert [Univ. Rennes I]

Post-Doctoral Fellows
Virgile Ducet [Ecole Polytechnique, from Oct 2014]
Aurore Guillevic [Inria]
Irene Marquez Corbella [Inria]
Johan Nielsen [Inria, granted by Fondation de Cooperation Scientifique "Campus Paris-Saclay"]
Razvan Barbulescu [AMN]
Julia Pieltant [Inria]

Visiting Scientist
Gerardus Rudolf Pellikaan [Digiteo, from Apr 2014 until May 2014]

Administrative Assistants
Myriam Brettes [Inria]
Hélèna Kutniak [Inria]
Valerie Annie Lecomte [Inria]

Others
Elise Barelli [Ecole Polytechnique, from Mar 2014]
Julien Lavauzelle [ENSTA, from Apr 2014]
Charlotte Scribot [Min. de l'Education Nationale]

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

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

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

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. New Software and Platforms

5.1. CADO-NFS-DLOG

F. Morain is one of the developers of CADO-NFS (available at http://cado-nfs.gforge.inria.fr/), which now includes new algorithms for discrete logarithm computations over finite fields.

5.2. Fast Compact Diffie–Hellman software

Working with C. Costello (Microsoft Research) and H. Hisil (Yasar), B. Smith contributed to the development of a competitive, high-speed, open implementation of the Diffie–Hellman protocol (described in [21]), targeting the 128-bit security level on Intel platforms. The source code is freely available at http://research.microsoft.com/en-us/downloads/ef32422a-af38-4c83-a033-a7aafbc1db55/ and http://hhisil.yasar.edu.tr/files/hisil20140318compact.tar.gz.

5.3. Platforms

5.3.1. ACTIS: Contribution to Sage

In the beginning of 2014,D. Augot and C. Pernet submitted an IJD proposal (ingénieur jeune diplomé) to Inria, called Projet Actis (Algorithmic Coding Theory In Sage). 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 have two directions for improvement: renewing the APIs to make them actually usable by researchers, and incorporating efficient programs for decoding, like J. Nielsen's CodingLib, which contains many new algorithms.

We hired D. Lucas on October 1st; he has started implementing various basic things, in a standalone manner. We plan to publish these snippets of code to the Sage community in January 2015. Our plan is to interact a lot with the Sage community, to ensure that our new APIs will cover most of the needs of various communities.

6. New Results

6.1. Highlights of the Year

- F. Morain and A. Guillevic (with their co-authors R. Barbulescu and P. Gaudry) broke the discrete logarithm world record for finite fields of the form $GF(p^2)$ with a prime p of 80 decimal digits. The new techniques form the preprint [31].
- D. Augot and M. Finiasz received the best paper award at FSE 2014 [17]. FSE is the most important conference devoted to symmetric cryptography. Grace contribution is to propose a mathematical construction which enables direct construction of so-called diffusion layers in block ciphers.
- A. Zeh, former Grace PhD student, received the special Prize of the Université Franco-Allemande (UFA) Jury 2014 at the French Ambassy in Berlin, on November 21st.

BEST PAPER AWARD :
[17] **Direct Construction of Recursive MDS Diffusion Layers using Shortened BCH Codes in 21st International Workshop on Fast Software Encryption, FSE 2014**. D. AUGOT, M. FINIASZ.

6.2. Diffusion layers for block ciphers

MDS matrices allow the construction of optimal linear diffusion layers in block ciphers. However, MDS matrices usually have a large description (for example, they can never be sparse), and this results in costly software/hardware implementations. We can solve this problem using *recursive MDS matrices*, which can be computed as a power of a simple companion matrix—and thus have a compact description suitable for constrained environments. Until now, finding recursive MDS matrices required an exhaustive search on families of companion matrices; this clearly limited the size of MDS matrices that one could look for. We have found a new direct construction, based on shortened BCH codes, which allows us to efficiently construct these matrices for arbitrary parameter sizes [17]. D. Augot and M. Finiasz received the best paper award at FSE 2014, and were invited to submit an extended journal version to *Journal of Cryptology*.

P. Karpman started to study sub-optimal diffusion layers, which can be built using algebraic geometry codes with a large automorphism group. Preliminary work has been done, leading to promising results [18]. To properly assert the cryptanalytic properties of these codes, V. Ducet is starting to implement a method for computing efficiently the weight distribution of AG codes.

6.3. 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 [25].

6.4. Tensor rank of multiplication over finite fields

Determining the tensor rank of multiplication over finite fields is a problem of great interest in algebraic complexity theory, but it also has practical importance: it allows us to obtain multiplication algorithms with a low bilinear complexity, which are of crucial significance in cryptography. In collaboration with S. Ballet and J. Chaumine [35], J. Pieltant obtained new asymptotic bounds for the symmetric tensor rank of multiplication in finite extensions of finite fields $\mathbb{F}_q$. In the more general (not-necessarily-symmetric) case, J. Pieltant and H. Randriam obtained new uniform upper bounds for multiplication in extensions of $\mathbb{F}_q$. They also gave purely asymptotic bounds substantially improving those coming from uniform bounds, by using a family of Shimura curves defined over $\mathbb{F}_q$. This work will appear in Mathematics of Computation [15].

6.5. Filtration Attacks against McEliece Cryptosystem

The McEliece encryption scheme based on binary Goppa codes was one of the first public-key encryption schemes [39]. 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 [40], 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 [10], 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 [23]; and A. Couvreur, I. Márquez-Corbella, and R. Pellikaan to break McEliece based on algebraic geometry codes from curves of arbitrary genus [22], [26].

6.6. A new bound on the number of rational points of arbitrary projective varieties

In [38], the authors asked for a general upper bound on the number of rational points of a (possibly reducible) equidimensional variety $X \subseteq \mathbf{P}^n$ of dimension d and degree δ. They conjectured that

$$|X(\mathbf{F}_q)| \leq \delta(\pi_d - \pi_{2d-n}) + \pi_{2d_n}, \tag{1}$$

where for all positive integer ℓ, π_ℓ is defined as the number of rational points of the projective space of dimension ℓ over $\mathbf{F}_q$. That is to say, $\pi_\ell = \frac{q^{\ell+1}-1}{q-1}$.

By combining algebraic geometric methods with a combinatorial method of double counting, A. Couvreur proved this conjecture [32] and got a more general upper bound on the number of rational points of arbitrary varieties (possibly non-equidimensional). In addition, he proved that (1) is sharp by providing examples of varieties reaching this bound.

6.7. New families of fast elliptic curves

B. Smith has pioneered the use of mod-p reductions of Q-curves to produce elliptic curves with efficient scalar multiplication algorithms—which translates into faster encryption, decryption, signing, and signature verification operations on these curves. A theoretical article was presented at ASIACRYPT 2013 [7], and a longer version was submitted (upon invitation) to the Journal of Cryptology. The theory was put into practice in collaboration with Craig Costello (Microsoft Research) and Huseyin Hisil (Yasar University). Their resulting publicly available implementation, which represents the state of the art in constant-time (side-channel conscious) elliptic curve scalar multiplication on 64-bit Intel platforms at the 128-bit security level, can carry out a constant-time scalar multiplication in 145k cycles on Ivy Bridge architectures. This work appeared in EUROCRYPT 2014 [21].

6.8. New results for solving the discrete logarithm problem

Recent results of R. Barbulescu, P. Gaudry, A. Joux, and E. Thomé seem to indicate that solving the discrete logarithm problem over finite fields of small characteristic is easier than was precedently thought. F. Morain and A. Guillevic, joined by R. Barbulescu and P. Gaudry, embarked on an attempt to assess the security of the discrete logarithm problem in a closely related context: that of finite fields with large characteristic and small degree. Improving on the methods of A. Joux, R. Lercier and others, they found new algorithms to select polynomials for the Number Field Sieve – the algorithm of choice in this setting. Moreover, a clever study of the algebraic properties of the fields used (e.g., algebraic units), enabled them to break the world record for the case of $GF(p^2)$, soon to be followed by new cases. This work is described in [31], and part of it is currently submitted.

6.9. Quantum Integer Factorization

Together with two researchers in quantum physics (F. Grosshans and T. Lawson), F. Morain and B. Smith have been working on the number theoretical postprocessing in Shor's algorithm. A preprint is being written.

7. Bilateral Contracts and Grants with Industry

7.1. Bilateral Contracts with Industry

7.1.1. 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.

We hired Man-Cuong Ngo as a PhD student, in February 2014. We proposed a much better way of using LDC codes in PIR protocols, allowing less storage and a very small number of servers. This idea was at the heart of a European patent (EP14305549.9), co-submitted by Inria and Alcatel-Lucent. A preliminary presentation was made at CANS [19].

8. Partnerships and Cooperations

8.1. Regional Initiatives

8.1.1. PEPS PAIP

From late 2012 through 2013, D. Augot was heavily involved in the preparation of the *Institut de la société du numérique* (Digital Society Institute) proposal within IDEX Paris-Saclay. Led by N. Boujemaa, this proposal aims to be a catalyst for interdisciplinary research (involving computer scientists and researchers from the humanities) on societal challenges inherent to eLife/life digitization. The proposal has initial funding from the IDEX, and will hopefully be self-funding within three years. Two kick-off projects were defined: joint human & machine interaction, and privacy and digital identity.

Within IDEX Paris-Saclay, the PAIP (Pour une Approche Interdisciplinaire de la Privacy) project was proposed and accepted in September 2013, with a small budget (30 keuros) for all the partners of the privacy group.

D. Augot engaged in monthly brainstorming meetings with researchers from Inria Paris–Rocquencourt (project-team SMIS), Université Jean Monnet's ADIS and CERDI labs (A. Rallet, A. Bensamoun), and Télécom ParisTech (C. Levallois-Barth). Topics under discussion include terms of service of various cloud storage providers; SMIS's *TrustedCell* secure token initiative for helding private and secure personal data; privacy leaks; and measurements on smartphones.

A one-day conference was held in Paris in December 2014.

8.1.2. 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.

8.1.3. 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). It funds one two-year post-doc, J. Nielsen, 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 [36], 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.

8.2. National Initiatives

8.2.1. ANR

- CATREL (accepted June 2012, Kickoff December 14, 2012, Starting January 1st, 2013): "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.

8.2.2. DGA

- DIFMAT-3: this one-year project aims to find matrices with good diffusion properties over small finite fields, in the spirit of [17]. 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 [37].
- 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 de Rennes), and D. Augot.

8.3. European Initiatives

8.3.1. FP7 & H2020 Projects

PQCRYPTO (Post-Quantum Cryptography) is a proposal which was submitted in 2014 by Tanja Langa (Tu/E), with Inria as a partner. We received in September 2014 the notification that it was accepted. Inria's Secret and Grace project-teams are part of this proposal, whose starting date is March 2015.

8.3.2. Collaborations in European Programs, except FP7 & H2020

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.

8.4. International Initiatives

8.4.1. Informal International Partners

- M. Bossert, Institute of Communications Engineering, Ulm Universität.
- S. Galbraith, Department of Mathematics, University of Auckland.

8.5. International Research Visitors

8.5.1. Visits of International Scientists

Ruud Pellikaan (Department of Mathematics and Computing Science Eindhoven University of Technology) visited us from April 24th to May 21st.

9. Dissemination

9.1. Promoting Scientific Activities

9.1.1. Scientific events organisation

9.1.1.1. member of the organizing committee

- D. Augot is member of the committee of the CCA seminar on coding and cryptology. This seminar regularly attracts around 30 participants.
- J. Nielsen, with L. de Feo, organized a Digiteo event CLIC related to J. Nielsen's Ditigeo funding IDEALCODES. This non-recurrent event attracted 30 participants.

9.1.2. Scientific events selection

9.1.2.1. member of the conference program committee

- D. Augot was a member of the WAIFI 2014 programm committee (International Workshop on the Arithmetic of Finite Fields, Gebze, Turkey)

9.1.3. Reviewer

- D. Augot was a reviewer for ITW (Information Theory Workshop) 2015.
- B. Smith was a reviewer for Eurocrypt 2014, CRYPTO 2014, PKC (Public Key Cryptography) 2014, and ANTS (Algorithmic Number Theory Symposium) 2014.

9.1.4. Journal

9.1.4.1. member of the editorial board

- 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.

9.1.4.2. reviewer

- D. Augot was reviewer for
  - *Designs, Codes and Cryptography*;
  - *Discrete Mathematics*.
  - *IEEE Transactions in Information Theory*;
- A. Couvreur was reviewer for
  - *Design, Codes and Cryptography*;
  - *Finite Fields and Their Applications*;

  - *IEEE Transactions on Communication*;
  - *Journal of Symbolic Computation*.
- B. Smith was a reviewer for
  - *Designs, Codes and Cryptography*
  - *Mathematics of Computation*
  - *ETRI Journal*

9.2. Teaching - Supervision - Juries

9.2.1. Teaching

Master

D. Augot, Error-correcting codes and applications to cryptography, 6h00, level M2, MPRI, France.

A. Couvreur, Error-correcting codes and applications to cryptography, 12h, level M2, MPRI, France.

A. Couvreur is *Chargé d'enseignement* at the École Polytechnique for the academic year 2014-2015.

A. Couvreur gave a one-week crash course in cryptology at the university of Masuku (Franceville, Gabon). Level M1.

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

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

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

F. Morain, 9 lectures of 1.5h, 3rd year (M1) course "cryptology" at École polytechnique.

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

Licence

F. Morain 10 lectures of 1.5h, 1st year course "Introduction à l'informatique" (INF311) at École polytechnique (L3). Responsability of this module (350 students).

B. Smith Introduction à l'informatique, 40h (equiv TD), L3, École polytechnique, France course "Introduction à l'informatique" (INF311) at École polytechnique (L3).

A. Couvreur Introduction à l'informatique, 40h (equiv TD), L3, École polytechnique, France course "Introduction à l'informatique" (INF311) at École polytechnique (L3).

A. Couvreur Les bases de la programmation et de l'algorithmique, 32h (equiv TD), M1, École polytechnique, France course (INF411) at École polytechnique (M1).

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

E-learning

I. Márquez-Corbella, with D. Augot's help, is currently preparing a MOOC on *code-based cryptology*. This MOOC is intended for an audience of M2 or PhD students who are interested in this sub-branch of cryptology. This can bring in students from coding theory, cryptology, or even physicists interested in post-quantum cryptography. N. Sendrier and M. Finiasz will complement and bring scientific authority to these lectures, by addressing more advanced topics. This bilingual MOOC (Spanish and English) is planned to be open in March, with a five week duration. It is supported by the Inria MOOC Lab, and will be hosted on the platform FUN.

9.2.2. Supervision

- D. Augot, advised two students, Gaspard Ferey and Sylvain Colin, for a "Projet personnel en laboratoire", whose object of study was attacks on code-based cryptosystems and their relation to the Chor-Rivest cryptosystem. 12h, level M1, Polytechnique, France.
- A. Couvreur advised one student, Alexander Schaub, for a "Projet personnel en laboratoire" on an oblivious transfer protocol using a noisy channel. 12h, level M1, Polytechnique, France.
- A. Couvreur advised the Masters thesis of Elise Barelli (Master Cryptis, University of Limoges). 6 month internship, level M2.
- B. Smith supervised Charlotte Scribot's Masters thesis (Master P7). 6 month internship, level M2.
- B. Smith co-supervised the third year of Cécile Gonçalves' PhD project.
- F. Levy-dit-Vehel supervised Julien Lavauzelle's end of ENSTA studies internship (level M2), 5 months.

9.2.3. Juries

- D. Augot was a member of Maurice Denise's PhD committee, for her defense "Codes correcteurs quantiques pouvant se décoder itérativement", June 26th.
- D. Augot was a member of Nicolás Bordenabe's PhD committee, for his defense "Measuring Privacy with Distinguishability Metrics: Definitions, Mechanisms and Application to Location Privacy", September 12th.
- D. Augot was a reviewer of Clément Pernet's HDR thesis "High Performance and Reliable Algebraic Computing", and member of his defense committee, November 21st.
- A. Couvreur is a member of the jury of the *agrégation de mathématiques*.
- B. Smith was a member of Ivan Boyer's PhD jury, for his defense "Variétés abéliennes et jacobiennes de courbes hyperelliptiques, en particulier à multiplication réelle ou complexe", January 24th.
- B. Smith was a member of Jean-Christophe Zapalowicz's PhD jury for his defense "Sécurité des générateurs pseudo-aléatoires et des implémentations de schémas de signature à clé publique", November 21st.

9.3. Invitations to seminars and conferences

- D. Augot made a presentation, "Décodage des codes de Reed-Solomon et logarithme discret dans les corps finis", at the Cryptography Seminar of Université de Rennes I, March 21st
- D. Augot made a presentation for the Secret project-team at Inria Rocquencourt "Bitcoin hors-sol", November 13th.
- A. Couvreur was an invited speaker at *Journées Codage et Cryptographie*, Grenoble in march 2014.
- A. Couvreur has been invited to give a talk at regular seminars in Rennes, Caen, University Paris 6, University Paris 8 and Bordeaux.
- B. Smith was an invited speaker at *YACC 2014*, Porquerolles, June 2014.
- B. Smith was an invited speaker in the *Computational Number Theory* workshop at *FOCM 2014*, Montevideo, Uruguay, December 2014.
- B. Smith was an invited speaker at the inaugural *MCrypt Workshop*, Les Deux Alpes, August 2014.
- B. Smith was an invited speaker at *DLP2014* (Theoretical and Practical Aspects of the Discrete Logarithm Problem), Ascona, Switzerland, May 2014.
- B. Smith gave a talk in the regular *PolSys* seminar at UPMC, March 2014.

9.4. Popularization

- D. Augot made a presentation “Quand $1 \oplus 1$ égal 0” at Lycée Albert Einstein, Sainte-Geneviève-des-Bois, May 19th.
- J. Pieltant was one of the presenters for Inria’s stand at « Bouge la Science » at Supélec.
- A. Couvreur gave a conference “Les mathématiques pour protéger l’information” for the pupils of Collège Moreau in Monthléry (91).

9.5. Institutional commitment

- A. Couvreur is an elected member of Saclay’s *commité de centre*.
- A. Couvreur was a member of the commission for the recruitment of post-doc researchers in 2014 at LIX in the programm Qualcomm-Carnot.
- A. Couvreur is the *jeune chercheur référent* for the *commission de suivi doctoral* of Inria Saclay.
- D. Augot was a member of RTRA Digiteo program committee.
- D. Augot is a member of LIX’s *conseil de direction*.
- D. Augot is a member of the *conseil de l’école doctorale en informatique de Paris-Sud*
- 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 and B. Smith were reviewers for ANRT CIFRE fundings.
- F. Morain, J. Pieltant 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*.
- 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.

10. 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. 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

[4] 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

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

[6] B. SMITH. *Isogenies and the discrete logarithm problem in Jacobians of genus 3 hyperelliptic curves*, in "J. of Cryptology", 2009, vol. 22, n° 4, pp. 505-529

[7] 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

Articles in International Peer-Reviewed Journals

[8] M. BORGES-QUINTANA, M. A. BORGES-TRENARD, I. MÁRQUEZ-CORBELLA, E. MARTINEZ-MORO. *Computing coset leaders and leader codewords of binary codes*, in "Journal of Algebra and Its Applications", November 2014, 19 p. [*DOI :* 10.1142/S0219498815501285], https://hal.archives-ouvertes.fr/hal-01088431

[9] A. COUVREUR. *Codes and the Cartier Operator*, in "Proceedings of the American Mathematical Society", March 2014, vol. 142, pp. 1983-1996, A part of this work has been done when the author was a Post Doc researcher supported by the French ANR Defis program under contract ANR-08-EMER-003 (COCQ project), https://hal.inria.fr/hal-00710451

[10] 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° 2, pp. 641-666 [*DOI :* 10.1007/s10623-014-9967-z], https://hal.archives-ouvertes.fr/hal-01096172

[11] A. COUVREUR, A. OTMANI, J.-P. TILLICH. *New identities relating wild Goppa codes*, in "Finite Fields and Their Applications", September 2014, vol. 29, pp. 178-197 [*DOI :* 10.1016/j.ffa.2014.04.007], https://hal.archives-ouvertes.fr/hal-00880994

[12] A. ENGE, F. MORAIN. *Generalised Weber Functions*, in "Acta Arithmetica", 2014, vol. 164, n° 4, pp. 309-341 [*DOI :* 10.4064/aa164-4-1], https://hal.inria.fr/inria-00385608

[13] I. MÁRQUEZ-CORBELLA, E. MARTINEZ-MORO, R. PELLIKAAN, R. DIEGO. *Computational aspects of retrieving a representation of an algebraic geometry code*, in "Journal of Symbolic Computation", August 2014, vol. 64, pp. 67-87 [*DOI :* 10.1016/j.jsc.2013.12.007], https://hal.archives-ouvertes.fr/hal-01088430

[14] J. S. R. NIELSEN, A. ZEH. *Multi-Trial Guruswami–Sudan Decoding for Generalised Reed–Solomon Codes*, in "Design Codes and Cryptography", March 2014, pp. 1-21 [*DOI :* 10.1007/s10623-014-9951-7], https://hal.inria.fr/hal-00975927

[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", 2015, pp. S 0025-5718(2015)02921-4 [*DOI :* 10.1090/S0025-5718-2015-02921-4], https://hal.archives-ouvertes.fr/hal-00828153

[16] A. WACHTER-ZEH, A. ZEH, M. BOSSERT. *Decoding interleaved Reed-Solomon codes beyond their joint error-correcting capability*, in "Designs, Codes and Cryptography", 2014, vol. 71, n° 2, pp. 261-281 [*DOI :* 10.1007/s10623-012-9728-9], https://hal.archives-ouvertes.fr/hal-00957810

International Conferences with Proceedings

[17] *Best Paper*
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), Lecture Notes in Computer Science, Springer, March 2014, Best paper award, https://hal.inria.fr/hal-01044597.

[18] D. AUGOT, P.-A. FOUQUE, P. KARPMAN. *Diffusion Matrices from Algebraic-Geometry Codes with Efficient SIMD Implementation*, in "Selected Areas in Cryptology - SAC 2014", Montreal, Canada, A. JOUX, A. YOUSSEF (editors), Lecture Notes in Computer Science, Springer, August 2014, vol. 8781, pp. 243-260 [*DOI :* 10.1007/978-3-319-13051-4_15], https://hal.inria.fr/hal-01094085

[19] D. AUGOT, F. LEVY-DIT-VEHEL, A. SHIKFA. *A Storage-Efficient and Robust Private Information Retrieval Scheme Allowing Few Servers*, in "13th International Conference, Cryptology and Network Security (CANS 2014) Proceedings", Heraklion, Greece, D. GRITZALIS, A. KIAYIAS, I. ASKOXYLAKIS (editors), Lecture notes in computer science, Springer, October 2014, vol. 8813, pp. 222 - 239 [*DOI :* 10.1007/978-3-319-12280-9_15], https://hal.inria.fr/hal-01094807

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

[21] C. COSTELLO, H. HISIL, B. SMITH. *Faster Compact Diffie-Hellman: Endomorphisms on the x-line*, in "EUROCRYPT 2014", Copenhagen, Denmark, P. Q. NGUYEN, E. OSWALD (editors), Lecture Notes in Computer Science, Springer, May 2014, vol. 8441, pp. 183-200 [*DOI :* 10.1007/978-3-642-55220-5_11], https://hal.inria.fr/hal-00932952

[22] A. COUVREUR, I. MÁRQUEZ-CORBELLA, R. PELLIKAAN. *A Polynomial Time Attack against Algebraic Geometry Code Based Public Key Cryptosystems*, in "IEEE International Symposium onInformation Theory (ISIT)", Honolulu, United States, IEEE, June 2014, pp. 1446-1450 [*DOI :* 10.1109/ISIT.2014.6875072], https://hal.archives-ouvertes.fr/hal-00937476

[23] A. COUVREUR, A. OTMANI, J.-P. TILLICH. *Polynomial Time Attack on Wild McEliece Over Quadratic Extensions*, in "Advances in Cryptology - Eurocrypt 2014", Copenhagen, Denmark, P. Q. NGUYEN, E. OSWALD (editors), LNCS, Springer, May 2014, vol. 8441, pp. 17-39 [*DOI :* 10.1007/978-3-642-55220-5_2], https://hal.archives-ouvertes.fr/hal-00931774

[24] 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

Conferences without Proceedings

[25] D. AUGOT. *Generalization of Gabidulin Codes over Fields of Rational Functions*, in "21st International Symposium on Mathematical Theory of Networks and Systems (MTNS 2014)", Groningen, Netherlands, July 2014, https://hal.inria.fr/hal-01094843

[26] 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

[27] N. DÜCK, I. MÁRQUEZ-CORBELLA, E. MARTÍNEZ-MORO. *On the fan associated to a linear code **, in "4th ICMCTA - Fourth International Castle Meeting on Coding Theory and Applications", Palmela, Portugal, September 2014, forthcoming, https://hal.archives-ouvertes.fr/hal-01088432

[28] I. MÁRQUEZ-CORBELLA, R. PELLIKAAN. *Error-correcting pairs: a new approach to code-based cryptography*, in "20th Conference on Applications of Computer Algebra (ACA 2014)", New York, United States, July 2014, https://hal.archives-ouvertes.fr/hal-01088433

Patents and standards

[29] D. AUGOT, F. LEVY-DIT-VEHEL, A. SHIKFA. *Storage efficient and unconditionnally secure private information retrieval*, September 2014, n^{o} 14305549.9, https://hal.inria.fr/hal-01111694

Other Publications

[30] S. BALLET, J. PIELTANT. *Tower of algebraic function fields with maximal Hasse-Witt invariant and tensor rank of multiplication in any extension of $\mathbb{F}_2$ and $\mathbb{F}_3$*, September 2014, https://hal.archives-ouvertes.fr/hal-01063511

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

[32] A. COUVREUR. *An upper bound on the number of rational points of arbitrary projective varieties over finite fields*, September 2014, https://hal.archives-ouvertes.fr/hal-01069510

[33] C. GONÇALVES. *A Point Counting Algorithm for Cyclic Covers of the Projective Line*, August 2014, https://hal.archives-ouvertes.fr/hal-01054645

[34] B. SMITH. *The Q-curve construction for endomorphism-accelerated elliptic curves*, September 2014, https://hal.inria.fr/hal-01064255

References in notes

[35] S. BALLET, J. CHAUMINE, J. PIELTANT. *Shimura modular curves and asymptotic symmetric tensor rank of multiplication in any finite field*, in "Conference on Algebraic Informatics", Porquerolles Island, France, T. MUNTEAN, D. POULAKIS, R. ROLLAND (editors), Lecture notes in computer science / Theoretical Computer Science and General Issues, Springer-Verlag Berlin Heidelberg, September 2013, vol. 8080, pp. 160-172 [*DOI :* 10.1007/978-3-642-40663-8_16], https://hal.archives-ouvertes.fr/hal-00828070

[36] 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

[37] 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

[38] S. R. GHORPADE, G. LACHAUD. *Étale Cohomology, Lefschetz Theorems and number of points of singular varieties over finite fields*, in "Mosc. Math. J.", 2002, vol. 2, n^{o} 3, pp. 589–631

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

[40] 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