Activity Report 2016

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

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
- 4.3.3. - Cryptographic protocols
- 4.8. - Privacy-enhancing technologies
- 7.6. - Computer Algebra
- 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

Luca de Feo [Univ. Versailles, Associate Professor]
Françoise Levy-Dit-Vehel [ENSTA, Associate Professor, HDR]
François Morain [Ecole Polytechnique, Professor, HDR]

Engineers

Nicholas Coxon [Inria]
David Lucas [Inria, until Sep 2016]

PhD Students

Elise Barelli [Inria]
Hanna-Mae Bisserier [Inst. de Recherche Technologique SystemX, from Nov 2016]
Nicolas Duhamel [ENS Cachan]
Pierre Karpman [Inria, until October 2016]
Julien Lavauzelle [Ecole Polytechnique]

Post-Doctoral Fellow

Virgile Ducet [Inria, until Oct 2016]

Visiting Scientists

Philippe Lebacque [Univ. Franche-Comté, Faculty Member]
François-Régis Blache [Université des Antilles, Faculty Member, Nov 2016]

Administrative Assistants

Helene Bessin Rousseau [Inria]
Jessica Gameiro [Inria]
Emmanuelle Perrot [Inria]

Others

Christopher Barbin [Inria, Master intern, from Apr 2016 until Jul 2016]

Nagarjun Chinthamani Dwarakanath [Inria, Master intern, from Apr 2016 until Jul 2016]
Eleonora Palazzolo [Inria, Master intern, until Apr 2016]
Evrim Petek [Inria, Master intern, from May 2016 until Sep 2016]

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 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 $\mathcal{X}$.

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.

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 and genus 2 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

5.1.1. Events organization

- A. Couvreur, D. Augot and D. Lucas organized with L. De Feo and Hugues Randriambololona (ENST ParisTech) a spring school on coding and cryptology in la Chapelle Gauthier (Seine et Marne).
- A. Couvreur and D. Augot organized 4 days workshop in november 2016 for the ANR MANTA. The topics were: "Decoding" and "Codes from surfaces".
- SageDays75. To conclude the ACTIS projet, we organized a one-week SageDays in August 2016. The day was spent at Inria Saclay, and people were staying at night in a cottage in Vallée de Chevreuse.

  The overall theme of this Sage Days was coding theory and exact linear algebra related to it, but there was be lots of general hacking. The aim of this Sage Days was to Introduce Sage to coding theorists;

have presentations about the enhancements we made to Sage's coding theory library during Inria's ACTIS project; Help people to work on their own projects.

We had a few talks on the mornings, and coding sprints on the afternoons. The first days' talks were focused on basic functionalities of our library, the last 2 days on advanced functionalities, with an emphasis on Sage development.

We were glad to attract several core sage developpers, who recognized the quality of the work done by D. Lucas.

6. New Software and Platforms

6.1. ACTIS

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 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.

- Contact: David Lucas
- https://bil.inria.fr/fr/software/view/2114/tab

During the project, D. Lucas and J. Nielsen proposed a google summer of code project on rank-metric codes under our ACTIS framework. The intern was Arpit Merchant, who visited us for SageDays75.

6.2. muKummer

KEYWORD: Cryptography
FUNCTIONAL DESCRIPTION

A competitive, high-speed, open implementation of the Diffie–Hellman key exchange protocol and a Schnorr-type digital signature scheme, targeting the 128-bit security level on two microcontroller platforms: the classic AVR ATMega 8-bit platform and the more modern ARM Cortex M0 32-bit platform. These downloads contain mixed C and assembly sources for the implementations described in [16].

- Participant: Benjamin Smith
- Contact: Benjamin Smith
- ATMega implementation URL: http://www.cs.ru.nl/~jrenes/software/mukummer-avr.tar.gz
- Cortex M0 implementation URL: http://www.cs.ru.nl/~jrenes/software/mukummer-arm.tar.gz

7. New Results

7.1. 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 2016. In joint work 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; this was presented at SAC 2016. The theory in this article was the basis of a highly competitive implementation of key exchange and signatures for microcontroller platforms, in joint work with J. Renes, P. Schwabe, and L. Batina, presented at CHES 2016.

7.2. 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 [22].

7.3. Advances in point counting

Determining the number of points on an elliptic curve, or more generally on the Jacobian of an algebraic curve, is a classic problem in algorithmic number theory that is now crucial for efficiently generating secure cryptographic parameters. Together with C. Scribot, F. Morain and B. Smith developed an improved version of the state-of-the-art SEA algorithm for certain families of elliptic curves with special endomorphisms; this was presented at ANTS-XII [10]. B. Smith also led a project group on special genus-2 point counting algorithms at the "Algebraic Geometry for Coding Theory and Cryptography" workshop at IPAM, UCLA, in 2016.

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 [31]. 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 [32], 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 [26], 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 [3]. A detailed long version has been written and recently published [9]. A. Couvreur, Irene Márquez–Corbella, and R. Pellikaan broke McEliece based on algebraic geometry codes from curves of arbitrary genus [2], [27] by reconstructing optimal polynomial time decoding algorithms decoding up to the half minimum distance minus half the genus. This can be computed from the raw data of a generator matrix. In a recently submitted long version [21] the algorithm has been improved and permits to reconstruct a decoding algorithm up to the half minimum distance.

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 [24], 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.

A. Guillevic and F. Morain have written a chapter [18] on discrete logarithm computations for a book on pairings.

7.6.1. Breaking a MNT curve using DL computations

There is a reduction between an elliptic curve E defined over $\mathbf{F}_p$ and a finite extension of degree k (aka *embedding degree*) of the base field, using pairing computations. In brief, one can transport the discrete logarithm problem from E to $\mathbf{F}_{p^k}$. If k is relatively small, this yields a DLP much easier to solve than directly on E. To give some highlight on current easyness, A. Guillevic, F. Morain and E. Thomé (from CARAMBA EPC in LORIA) computed a discrete log on a curve of embedding degree 3 and cryptographic size. This clearly showed that curves with small embedding degrees are indeed weak. The article [14] was presented by A. Guillevic during the SAC 2016 conference in New Foundland.

7.7. 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.

7.8. 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.
- 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. 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 was accepted at EUROCRYPT 2016 [17].

7.9. 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.

In 2015, we helped to improve the state of the art in block cipher research in several ways:

- 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 [23].

In 2016, together with P.-A. Fouque, P. Kirchner and B. Minaud, P. Karpman designed a family of efficient provably incompressible symmetric primitives, which corresponds to a weak notion of white-box cryptography. The objective of such algorithms is that given an implementation of a certain target size, an adversary shouldn't be able to efficiently find a smaller implementation with comparable functionality. We introduced a security model that captures the behaviour of realistic adversaries and used this model to prove the security of a family of block cipher and a family of key generating functions. The corresponding paper was published at ASIACRYPT 2016 [13].

7.10. 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.

7.11. Update on the Chor-Rivest cryptosystem

The Chor-Rivest cryptosystem from the 90's was "broken" by Vaudenay. However, Vaudenay's attack applies only for the range of parameters originally proposed. The major recent breakthrough in discrete logarithm computations enable to redesign the system with a completly different range of paramaters, possibly thwarting Vaudenay's attack. D. Augot and C. Barbin tried to find a new attack against this discrete log and knapsack-based cryptosystem, using the Sidelnikov-Shestakov algorithm for recovering a Reed-Solomon code. Apparently, our new attack does not outperform S. Vaudenay's original attack, and it may be possible that the Chor-Rivest could be redesigned in a secure way.

7.12. Proofs or Retrievability

A Proof of Retrievability (PoR) is a cryptographic protocol which aims at ensuring a user that he can retrieve files he previously stored on a server. J. Lavauzelle and F. Levy-dit-Vehel studied a new approach for the construction of PoRs. The idea is to encode the file so that the user can check with low communication whether its file has been damaged. Such an encoding can be efficiently done with locally decodable and testable codes, and especially with the family of lifted codes introduced by Guo, Kopparty and Sudan [30]. In practice, PoRs thus defined achieve very efficient storage overhead and acceptable communication, compared to the existing litterature. This new construction [15] has been presented during the ISIT2016 conference in Barcelona.

7.13. Fast Encoding of Multiplicity Codes

N. Coxon has produced a fast implementation which demonstrates that the multiplicity codes from Kopparty, Saraf and Yehkanin are indeed practical for very large databases (when used in the Private Information Retrieval setting). For instance, we can encode a 10^8 bit longs message in two seconds on a regular laptop, and 10^9 in thirty seconds. We envisioned a scenario where DNA sequences are encoded using these multiplicity codes: 10^8 bits is the size of Drosophila melanogaster (flies), and 10^9 bits is the order of magnitude of the human genome.

7.14. Private Information Retrieval

Imagine the following scenario, in which a researcher wants to access many sustrings a DNA sequences, while maintaining the privacy of the request. The privacy or the secrecy of the database is not a concern here: for instance, this researcher wants to access many DNA subsequences of drosophila melanogaster, hosted on a remote data broker, and clearly the concern is not to protect the private life of flies. But the information leaked about the queries may endanger the novel aspect of the discovery the researcher is about to make, by revealing which DNA sequences he is studying.

Private Information Retrieval (PIR) schemes are designed to achieve this goal: a user queries a database T hosted on a remote server, and wants the i-th entry, i.e. $T[i]$. A cryptographic protocol is then run, and at the end of the protocol, the server must not know i, neither the $T[i]$ he answered, yet the user gets $T[i]$.

These PIR schemes can be achieved in an unconditionally secure way using the above Multiplicity codes, which N. Coxon made practical. In September, we explained this scenario and demoed our software at Nokia Bell Lab's Future X days a use case of Multiplicity codes for private access to DNA sequences.

7.15. Compact McEliece Keys from Algebraic-geometry codes

In 1978, McEliece [31], introduced a public key cryptosystem based on linear codes and suggested to use classical Goppa codes which belong to the family of alternant codes. This proposition remains secure but leads to very large public keys compared to other public-key cryptosystems. Many proposals have been made in order to reduce the key size, in particular quasi-cyclic alternant codes. Quasi-cyclic alternant codes refer to alternant codes admitting a generator matrix made of severals cyclic bloks. These alternant codes contains weakness because they have a non-trivial automorphism group. Thanks to this property we can build, from a quasi-cyclic alternant code, an alternant code with smaller parameters which has almost same private elements than the original code. Faugère, Otmani, Tillich, Perret and Portzamparc [29] showed this fact for alternant codes obtained by using supports $x \in \mathbb{F}_{q^m}^n$ globally stable by an affine map $\phi : z \mapsto az + b$, with $a, b \in \mathbb{F}_{q^m}^n$. E. Barelli has extended this proof to the non-affine case: for all codes obtained by using supports $x \in \mathbb{F}_{q^m}^n$ globally stable by a map $\phi : z \mapsto \frac{az+b}{cz+d}$, with $a, b, c, d \in \mathbb{F}_{q^m}^n$.

In order to suggest compact keys for the McEliece cryptosystem E. Barelli and A. Couvreur studied quasi-cyclic alternant gemeotric codes. Alternant geometric codes means a subfield subcode of an algebraic-geometry codes. To build these codes, we need curves with automorphisms. In particular, we studied Kummer cover of plane curves.

8. Bilateral Contracts and Grants with Industry

8.1. Bilateral Grants with Industry

8.1.1. Nokia (ex 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.

N. Coxon made the first implementation of these codes, who are indeed very practical. On a laptop, we can encode an ADN of a drosophilia in two seconds, and a 10^9 bit data base in 30 seconds. We have a few real-life scenario in mind (DNA, geolocalisation, streaming), and we will check how realistic they are.

8.1.2. Safran Identity and Security (ex-Morpho)

A contract has been signed in November 2016 between Safran Identity and Security and École polytechnique, for one year post-doc position. A candidate has been found, and will arrive early 2017 (January).

The topic is the research is to use bitcoin's blockchain to issue and manipulate certification of identities, which is very close to the (trendy) topic of diplomation with blockchains.

Safran had a preliminary construction for doing that, and a preliminary version has been submitted to the IEEE Security and Privacy on the Blockchain Workshop.

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 economique de Bitcoin) was accepted as interdisciplinary research for a PEPS (Projet exploratoire Premier Soutien) cofunded by the CNRS and Universite 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.

One M2 intern, E. Palazzollo, was intern in Sceaux, with aim to qualify the nature of bitcoin, as an asset, curency, etc.

This project ended in March 2016

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 [25], 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.

The last year of the 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 [28].

9.1.3. IRT System-X

D. Augot is co-advising a PhD candidate, H.-M. Bisserier, on "les relations contractuelles de droit privé à l'épreuve de la technologie des blockchains", i.e. on (French) law and so-called "smart contracts". D. Augot will mainly help H.-M. Bisserier to clarify the essential computer science topics and issues relevant to the most important blockchains (bitcoin, ethereum). Then H.-M. Bisserier will be advised by C. Zolynksi for remaining two years, fixing research directions.

9.2. National Initiatives

9.2.1. ANR

MANTA (accepted July 2015, starting March 2016): "Curves, surfaces, codes and cryptography". This project deals with applications of coding theory error correcting codes to in cryptography, multi-party computation, and complexity theory, using advanced topics in algebraic geometry and number theory. The kickoff was a one week-retreat in Dordogne (20 participants), and we had another four day meeting in Saclay in November 17. See http://anr-manta.inria.fr/.

9.2.2. DGA

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.

Our team is engaged in WP3.3 “advanced applications for the cloud”. We envision to focus essentially on secure multiparty computation, essentially the information theoretically secure constructions, who are naturally secure against a quantum computer invoked on classical queries. We will study whether these protocols still resist quantum queries. This work sub package started March 2015, and is dealt with by D. Augot.

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.

10.1.2. Scientific Events Selection

10.1.2.1. Reviewer

- D. Augot was reviewer for International Symposium on Information Theory

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.
- F. Morain is member of the editorial board of the *Applicable Algebra in Engineering, Communication and Computing*, Springer.
- A. Couvreur was editor with Alp Bassa (Bogazici University, Turkey) and David Kohel (Aix-Marseille University) of a number of *AMS Contemporary Mathematics* for the proceedings of the conference AGCT (*Arithmetic Geometry Cryptography and Coding Theory*) 2015.

10.1.3.2. Reviewer - Reviewing Activities

- D. Augot was reviewer for
  - Discrete Mathematics
  - Designs, Codes and Cryptography
  - Linear and Multilinear Algebra
  - Finite Fields and their applications
- A. Couvreur was reviewer for
  - Discrete Mathematics
  - Designs, Codes and Cryptography
  - Journal of Algebra

10.1.4. Invited Talks

- D. Augot was invited speaker at Yet Another Cryptography Conference (YACC), Porquerolles, June 2016.
- B. Smith was an invited speaker at the 20th international Workshop on Elliptic Curve Cryptography (ECC), Izmir, Turkey, September 2016.
- A. Couvreur gave a talk to represent the group *Codes et Cryptographie* of the GdR *Informatique Mathématiques* (GdR IM) at the *Journées nationales du GdR IM* at University Paris 13 (January 13).

10.1.5. Scientific Expertise

- D. Augot participated in a round table at a workshop organized by French National Assembly (lower house) at, on blockchains (March 24th).
- D. Augot participated in a round table at Paris Dauphine on blockchains, organized by the chair “Chaire Gouvernance & Régulation” (November 1).
- D. Augot made a talk on hashing and blockchain at a workshop on blockchains held at Institut Poincaré (November 16).

10.1.6. Teaching in international postgraduate summer schools

- B. Smith gave lectures on *Basic public-key constructions with elliptic curves* and *Advanced constructions in curve-based cryptography* at the *Summer school on real-world crypto and privacy*, Sibenik, Croatia, June 2016.

- B. Smith gave a course on *asymmetric cryptography and elliptic curves* at the *Crypto-CO summer school on cryptography and security*, Bogota, Colombia, July 2016.
- B. Smith gave lectures on elliptic curves at the *ECC2016 Computational Algebraic Number Theory School*, Izmir, Turkey, September 2016.

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 *assemblée des chefs d'équipe*
- D. Augot is elected member of the *conseil académique consultatif* of Paris-Saclay University.
- F. Levy-dit-Vehelis a representative of "enseignants-chercheurs" of LIX.
- F. Morain, B. Smith and A. Couvreur 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.
- B. Smith is the academic coordinator for Computer Science in the new *Bachelor* program at École polytechnique.

Committees

- D. Augot was in the committee assessing candidates for Univ. Paris 8.

10.2. Teaching - Supervision - Juries

10.2.1. Teaching

Licence :

- D. Augot was mentoring a group of polytechnique students on a L3 projet on homomorphic encryption and voting (6 students)
- D. Augot was mentoring a group of polytechnique students on a L3 projet on blockchains and hyperledger, in collaboration with Orange (5 students)
- F. Levy-dit-Vehel, "Mathématiques discrètes pour la protection de l'information", 24h (equiv TD), 2nd year (L3), ENSTA ParisTech, France.
- J. Lavauzelle, 1I002, "Introduction à la programmation en C", tutorial class (38.5h), L1, Université Pierre et Marie Curie, France
- J. Lavauzelle, 2I011, "Méthodes numériques", tutorial class (21h), L2, Université Pierre et Marie Curie, France

- J. Lavauzelle, 1I001, “Éléments de programmation”, tutorial class (38.5h), L1, Université Pierre et Marie Curie, France
- J. Lavauzelle, 2I003, “Initiation à l’algorithmique”, tutorial class (21.25h), L2, Université Pierre et Marie Curie, France
- A. Couvreur and E. Barelli, INF311, ”Introduction à l’informatique“, 26.7h(equiv TD), 1st year, Ecole Polytechnique, France.
- E. Barelli, INF411, "Les bases de la programmation et de l’algorithmique", 21.3h (equiv TD), 2nd year (L3), Ecole Polytechnique, France.
- B. Smith, INF442, "Traitement des données massives", 32h TD, 2nd year, École polytechnique
- A. Couvreur and B. Smith, INF411, "Les bases de la programmation et de l’algorithmique", 32h TD, 2nd year, École polytechnique

Master :

- D. Augot was mentoring François Bonnal, on a M1 research training projet, “bitcoin malleability”
- D. Augot was mentoring Édouard Dufour-Sans, on a M1 research training projet, “symmetric information theoretically secure private information retrieval schemes and applications”
- F. Levy-dit-Vehel, “Cours de Cryptographie”, 30h. (equiv TD), 3rd year (M1), ENSTA ParisTech, France.
- B. Smith, “Algorithmes arithmétiques pour la cryptologie”, 15h, MPRI (M2), Paris
- A. Couvreur, INF558a, “Introduction to cryptology”, 25h, Ecole Polytechnique (M1).
- A. Couvreur, “Introduction to coding theory and cryptology”, 10h, MPRI (M2), Paris.
- B. Smith supervised Nagarjun Chinthamani Dwarakanath for a 3A project and an M1 project on efficient curve-based cryptosystems at École polytechnique
- A. Couvreur supervised Evrim Petek’s M2 internship on the power decoding algorithm.
- A. Couvreur supervised Anas Aarab’s M1 TRE (*Travail de Recherche Encadré*) on the decoding of Reed Solomon codes.

Doctorat :

- Ben Smith made a lecture at the spring school on coding and cryptology at La Chapelle-Gauthier.

10.2.2. Supervision

- 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.
- Completed PhD. P. Karpman, starting in 2013, defended in November 2016 his PhD on security of symmetric crytographic primitives.

10.2.3. Juries

- D. Augot was examiner in the jury of Fanny Jardel, who defended her thesis “Calcul et Stockage Distribués pour les Réseaux de Communication”, January 11, Télécom-ParisTech
- D. Augot was examiner in the jury of Cécile Pierrot, who defended her thesis “Le logarithme discret dans les corps finis”, November 25, Pierre and Marie Curie University.

- F. Morain was referee and examiner in the jury of Alexandre WALLET, who defended his thesis “Le problème de décomposition de points dans les variétés jacobiennes”, December 14, Pierre and Marie Curie University.
- A. Couvreur is member of the jury of the agrégation de mathématiques and coordinator of option C (“algèbre et calcul formel).

10.3. Popularization

- At the occasion of Nokia Bell Labs Future X-Days, September 2016, D. Augot, N. Coxon and F. Levy-dit-Vehel demoed N. Coxon’s implementation of a code based *private information retrieval scheme*
- D. Augot made a two hours lecture on bitcoin to the French *institut des actuaires*.

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, 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

[3] 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

[4] 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

[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^{o} 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] A. COUVREUR. *An upper bound on the number of rational points of arbitrary projective varieties over finite fields*, in "Proceedings of the American Mathematical Society", 2016, vol. 144, pp. 3671-3685, https://hal.archives-ouvertes.fr/hal-01069510

[9] A. COUVREUR, A. OTMANI, J.-P. TILLICH. *Polynomial Time Attack on Wild McEliece Over Quadratic Extensions*, in "IEEE Transactions on Information Theory", 2017, vol. 63, n° 1, pp. 404 - 427 [*DOI :* 10.1109/TIT.2016.2574841], https://hal.archives-ouvertes.fr/hal-01426775

[10] F. MORAIN, C. SCRIBOT, B. SMITH. *Computing cardinalities of Q-curve reductions over finite fields*, in "LMS Journal of Computation and Mathematics", August 2016, vol. 19, n° A, 15 p. [*DOI :* 10.1112/S1461157016000267], https://hal.inria.fr/hal-01320388

[11] B. SMITH. *The Q-curve construction for endomorphism-accelerated elliptic curves*, in "Journal of Cryptology", October 2016, vol. 29, n° 4, 27 p. [*DOI :* 10.1007/s00145-015-9210-8], https://hal.inria.fr/hal-01064255

International Conferences with Proceedings

[12] P. FOUQUE, P. KARPMAN, P. KIRCHNER, B. MINAUD. *Efficient and Provable White-Box Primitives*, in "ASIACRYPT 2016", HANOI, Vietnam, Advances in Cryptology - ASIACRYPT 2016 - 22nd International Conference on the Theory and Application of Cryptology and Information Security, December 2016, vol. LNCS 10031, pp. 159 - 188 [*DOI :* 10.1007/978-3-662-53887-6_6], https://hal.archives-ouvertes.fr/hal-01427810

[13] P.-A. FOUQUE, P. KARPMAN, P. KIRCHNER, B. MINAUD. *Efficient and Provable White-Box Primitives*, in "ASIACRYPT", Hanoï, Vietnam, Springer, December 2016 [*DOI :* 10.1007/978-3-662-53887-6_6], https://hal.inria.fr/hal-01421044

[14] A. GUILLEVIC, F. MORAIN, E. THOMÉ. *Solving discrete logarithms on a 170-bit MNT curve by pairing reduction*, in "Selected Areas in Cryptography 2016", St. John's, Canada, R. AVANZI, H. HEYS (editors), Selected Areas in Cryptography 2016, Springer, August 2016, to appear in the Lecture Notes in Computer Science (LNCS), https://hal.inria.fr/hal-01320496

[15] J. LAVAUZELLE, F. LEVY-DIT-VEHEL. *New proofs of retrievability using locally decodable codes*, in "International Symposium on Information Theory ISIT 2016", Barcelona, Spain, July 2016, pp. 1809 - 1813 [*DOI :* 10.1109/ISIT.2016.7541611], https://hal.archives-ouvertes.fr/hal-01413159

[16] J. RENES, P. SCHWABE, B. SMITH, L. BATINA. *μKummer: efficient hyperelliptic signatures and key exchange on microcontrollers*, in "Cryptographic Hardware and Embedded Systems – CHES 2016", Santa Barbara, United States, Cryptographic Hardware and Embedded Systems – CHES 2016, Springer-Verlag, August 2016, vol. 9813, 20 p. [*DOI :* 10.1007/978-3-662-53140-2_15], https://hal.inria.fr/hal-01300727

[17] M. STEVENS, P. KARPMAN, T. PEYRIN. *Freestart Collision for Full SHA-1*, in "EUROCRYPT 2016", Vienne, Austria, IACR, May 2016 [*DOI :* 10.1007/978-3-662-49890-3_18], https://hal.inria.fr/hal-01251023

Scientific Books (or Scientific Book chapters)

[18] A. GUILLEVIC, F. MORAIN. *Discrete Logarithms*, in "Guide to pairing-based cryptography", N. E. MRABET, M. JOYE (editors), CRC Press - Taylor and Francis Group, December 2016, 42 p. , https://hal.inria.fr/hal-01420485

Other Publications

[19] S. BALLENTINE, A. GUILLEVIC, E. LORENZO GARCÍA, C. MARTINDALE, M. MASSIERER, B. SMITH, J. TOP. *Isogenies for point counting on genus two hyperelliptic curves with maximal real multiplication*, December 2016, working paper or preprint, https://hal.inria.fr/hal-01421031

[20] P. N. CHUNG, C. COSTELLO, B. SMITH. *Fast, uniform scalar multiplication for genus 2 Jacobians with fast Kummers*, 2016, working paper or preprint, https://hal.inria.fr/hal-01353480

[21] A. COUVREUR, I. MÁRQUEZ-CORBELLA, R. PELLIKAAN. *Cryptanalysis of McEliece Cryptosystem Based on Algebraic Geometry Codes and their subcodes*, March 2016, working paper or preprint, https://hal.archives-ouvertes.fr/hal-01280927

[22] F. GROSSHANS, T. LAWSON, B. SMITH, F. MORAIN. *Factoring Safe Semiprimes with a Single Quantum Query*, September 2016, working paper or preprint, https://hal.inria.fr/hal-01229587

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

References in notes

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

[25] 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

[26] 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

[27] 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

[28] 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

[29] J.-C. FAUGERE, A. OTMANI, L. PERRET, F. DE PORTZAMPARC, J.-P. TILLICH. *Folding alternant and Goppa codes with non-trivial automorphism groups*, in "IEEE Transactions on Information Theory", 2016, vol. 62, n^{o} 1, pp. 184–198

[30] A. GUO, S. KOPPARTY, M. SUDAN. *New Affine-invariant Codes from Lifting*, in "Proceedings of the 4th Conference on Innovations in Theoretical Computer Science", New York, NY, USA, ITCS '13, ACM, 2013, pp. 529–540, http://doi.acm.org/10.1145/2422436.2422494

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

[32] 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