IN PARTNERSHIP WITH:
CNRS

Ecole Polytechnique

Activity Report 2017

Project-Team GRACE

Geometry, arithmetic, algorithms, codes and encryption

IN COLLABORATION WITH: Laboratoire d'informatique de l'école polytechnique (LIX)

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:

A4.2. - Correcting codes
A4.3. - Cryptography
A4.3.1. - Public key cryptography
A4.3.3. - Cryptographic protocols
A4.8. - Privacy-enhancing technologies
A8.4. - Computer Algebra
A8.5. - Number theory

Other Research Topics and Application Domains:

B9.4.2. - Mathematics
B9.8. - Privacy

1. Personnel

Research Scientists

Daniel Augot [Team leader, Inria, Senior Researcher, HDR]
Alain Couvreur [Inria, Researcher]
William George [Laboratoire d'informatique de l'école polytechnique (LIX), Starting Research Position]
Matthieu Rambaud [Inria, Researcher, from Oct 2017]
Benjamin Smith [Inria, Researcher]

Faculty Members

Luca de Feo [Univ de Versailles Saint-Quentin-en-Yvelines, Associate Professor]
Francoise Levy-Dit-Vehel [École Nationale Supérieure de Techniques Avancées, Associate Professor, HDR]
François Morain [Ecole polytechnique, Professor, HDR]

PhD Students

Elise Barelli [Inria]
Hanna-Mae Bisserier [Institut de recherche technologique System X]
Nicolas Duhamel [Ecole Polytechnique, until Jul 2017]
Hussein Khazaie [Inria, from Oct 2017]
Julien Lavauzelle [Ecole polytechnique]
Edouard Rousseau [Institut Telecom ex GET Groupe des Ecoles des Télécommunications , from Oct 2017]

Technical staff

Nicholas Coxon [Inria]

Interns

Benoît Billaudel [Inria, from Mar 2017 until Aug 2017]
Rémi Clarisse [Inria, from May 2017 until Aug 2017]
Jean Kieffer [Ecole Normale Supérieure Paris, from Mar 2017 until Aug 2017]

Administrative Assistant

Jessica Gameiro [Inria]

Visiting Scientist

Elisabeth Malmskog [Colorado College, USA, from Nov 2017]

External Collaborators

Christian Berghoff [Bonn International Graduate School - BIGS, until Feb 2017]
Pierre Karpman [Centrum Wiskunde and Informatica, Amsterdam, until Nov 2017]
David Kohel [Aix–Marseille Université,from Jul 2017]
Philippe Lebacque [Univ de Franche-Comté]

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. Highlights of the Year

4.1. Highlights of the Year

4.1.1. Presentation at Inria@SiliconValley

D. Augot made a presentation at a one day workshop "Blockchain Technology for Cybersecurity and Social Impact" at Berkeley's CITRIS https://project.inria.fr/siliconvalley/bis2017-day1-conference-blockchain

4.1.2. Workshop on Coding theory and Cryptography (WCC)

D. Augot was co-chair of the Program Commitee of WCC 2017 (St Petersburg, Russia).

4.1.3. NIST Call for post quantum cryptography

In the context of NIST's call for post quantum cryptography:

https://csrc.nist.gov/Projects/Post-Quantum-Cryptography

members of the team participated to two sumbissions:

- A. Couvreur and E. Barelli participated to the submission of **BIG QUAKE** proposal [19]:
  https://bigquake.inria.fr/
- L. De Feo participated to the submission of **SIKE** proposal:
  https://rwc.iacr.org/2018//Slides/Longa.pdf

5. New Software and Platforms

5.1. ACTIS

Algorithmic Coding Theory in Sage
FUNCTIONAL DESCRIPTION: The aim of this project is to vastly improve the state of the error correcting library in Sage. The existing library does not present a good and usable API, and the provided algorithms are very basic, irrelevant, and outdated. We thus 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.

- Partner: Technical University Denmark
- Contact: Daniel Augot

5.2. DECODING

KEYWORD: Algebraic decoding
FUNCTIONAL DESCRIPTION: Decoding is a standalone C library. Its primary goal is to implement Guruswami–Sudan list decoding-related algorithms, as efficiently as possible. Its secondary goal is to give an efficient tool for the implementation of decoding algorithms (not necessarily list decoding algorithms) and their benchmarking.

- Participant: Guillaume Quintin
- Contact: Daniel Augot

5.3. Fast Compact Diffie-Hellman

KEYWORD: Cryptography

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

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

5.4. CADO-NFS

Crible Algébrique: Distribution, Optimisation - Number Field Sieve
KEYWORDS: Cryptography - Number theory
FUNCTIONAL DESCRIPTION: CADO-NFS is a complete implementation in C/C++ of the Number Field Sieve (NFS) algorithm for factoring integers and computing discrete logarithms in finite fields. It consists in various programs corresponding to all the phases of the algorithm, and a general script that runs them, possibly in parallel over a network of computers.

- Participants: Pierrick Gaudry, Emmanuel Thomé and Paul Zimmermann
- Contact: Emmanuel Thomé
- URL: http://cado-nfs.gforge.inria.fr/

6. New Results

6.1. qDSA: Compact signatures for IoT

B. Smith and Joost Renes (Radboud University, NL) developed **qDSA**, a new digital signature scheme targeting constrained devices, typically microcontrollers with extremely limited memory. An article describing qDSA was presented at ASIACRYPT 2017, and a reference implementation software package has been placed into the public domain.

6.2. PIR based on transversal designs

J. Lavauzelle presented a construction of Private Information Retrieval (PIR) protocols from combinatorial structures called transversal designs. The construction features low computation and low storage overhead for the servers. For some instances, adequate communication between servers and user is achieved. The PIR scheme also generalizes to colluding servers. The construction has been presented during WCC 2017 [17], and in a poster session in the Munich Workshop in Coding and Applications.

6.3. On the security of compact McEliece keys

E. Barelli presented at WCC 2017 (Workshop on Coding and Cryptography, St Petersburg, Russia) her recent results on the analysis of McEliece scheme based on alternant codes with a non trivial automorphism group [16]. These codes were suggested for public key encryption since, compared to codes with trivial automorphism group, they could provide shorter keys.

If the security with respect to generic decoding attacks is almost unchanged when considering codes with non trivial automorphisms, E. Barelli proved that the security with respect to key recovery attacks is highly reduced since, it reduces to recover the structure of the subcode of fixed elements by the automorphism group.

6.4. Two-points codes on the generalized Giuletti Korchmaros curve

In a collaboration with Peter Beelen, Mrinmoy Datta, Vincent Neiger and Johan Rosenkilde (DTU Copenhagen), E. Barelli obtained improved lower bounds for the minimum distance of some algebraic geometry codes from Giulietti Korchmaros curves [20].

6.5. Towards a function field version of Freiman's theorem

In a collaboration with Christine Bachoc and Gilles Zémor (University of Bordeaux), A. Couvreur obtained a characterisation of subspaces S of a function field F over an algebraically closed field satisfiying

$$\dim S^2 = 2 \dim S$$

where S^2 denotes the space spanned by all the products of two elements of S. They obtained the following result [18]:

Theorem. *Let F be a function field over an algebraically closed field, and S be a finite dimensional subspace of F which spans F as an algebra and such that*

$$\dim S^2 = 2 \dim S.$$

Then F is a function field of transcendence degree 1 and

- *either F has genus 1 and S is a Riemann Roch space*
- *or F has genus 0 and S is a subspace of codimension 1 in a Riemann Roch space.*

6.6. BIG QUAKE

In the context of NIST's call for post quantum cryptosystems:

https://csrc.nist.gov/Projects/Post-Quantum-Cryptography

A. Couvreur and E. Barelli participated to the submission BIG QUAKE [19] (BInary Goppa QUAsi–cyclic Key Encapsulation). The proposal consists in a public key encryption scheme (with a conversion to a Key Encapsulation Mechanism) using binary quasi–cyclic Goppa codes.

The details on the proposal are on the following website.

https://bigquake.inria.fr/

6.7. 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.

6.7.1. Computing discrete logarithms in $GF(p^6)$

A. Guillevic, L. Grémy, F. Morain and E. Thomé (from CARAMBA EPC in LORIA) computed a discrete log on a curve of embedding degree 6 and cryptographic size. This clearly showed that curves with small embedding degrees are indeed weak. The article [23] was presented by L. Grémy during the SAC 2017 conference in Ottawa.

6.7.2. Identity management on Bitcoin's blockchain

D. Augot and W. George in collaboration with Hervé Chabanne (Safran Identity and Security, ex Morpho, now Idemia) designed two schemes to allow users to authenticate using so-called anonymous credentials, issues by an identity provider. We used Brands anonymous credentials with selective disclosure each time, first for a finely tuned, user managed, identity scheme [12], second for a more classical high throughput scheme [13], inspired by CONIKS https://coniks.cs.princeton.edu.

6.7.3. Law and Blokchain smart contracts

D. Augot, with Célia Zolynski, is co-advising Hanna-Mae Bisserier, a PhD student law, on the impact of blockchains on legal systems. The PhD is in law, and D. Augot only gives scientific and technological explanations, while the direction of the thesis is done by Célia Zolynski.

7. Bilateral Contracts and Grants with Industry

7.1. Bilateral Contracts with Industry

- **NOKIA BELL LABS**
  - New PhD student H. Khazaie is funded by ADR with NOKIA BELL LABS. The PhD topic is the security of distributed storage systems.
  - Post doctoral researcher N. Coxon is funded by ADR with NOKIA BELL LABS. The post doc topic is an information theoretically secure private information retrieval scheme.
- **SAFRAN Identity and Security (Ex Morpho and now Idemia)**
  - Post doctoral researcher W. George is funded by Idemia to design an identity management scheme based on Bitcoin's blockchain.

8. Partnerships and Cooperations

8.1. National Initiatives

8.1.1. 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/.

8.2. European Initiatives

8.2.1. FP7 & H2020 Projects

8.2.1.1. 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.

8.3. International Initiatives

8.3.1. Inria International Partners

8.3.1.1. Informal International Partners

B. Smith has continued our successful informal partnership with the cryptography research group at Radboud University, Nijmegen (NL). 2017 has seen visits from researchers in both directions, and the production of the **qDSA** signature scheme package.

8.4. International Research Visitors

8.4.1. Visits of International Scientists

Beth Malmskog (Colorado College) visited the team from November 27 to December 1 2017 and gave a talk on locally recoverable codes based on fibre products of algebraic curves.

8.4.2. Visits to International Teams

8.4.2.1. Research Stays Abroad

B. Smith was an invited researcher in the Computer Science department at CINVESTAV (Mexico City, Mexico) for the month of August 2017, hosted by Professor Francisco Rodríguez Henríquez.

J. Lavauzelle visited Incidence Geometry team at Gent University (Belgium) for the month of April 2017, hosted by Professor Leo Storme.

E. Barelli visited the COMPUTE team in the DTU University at Lyngby (Danemark) during one month in february-march 2017, hosted by Professor Peter Beelen.

9. Dissemination

9.1. Promoting Scientific Activities

9.1.1. Scientific Events Organisation

9.1.1.1. Member of the Organizing Committees

B. Smith was a member of the organizing committee and Short Talk Chair for IEEE EuroS&P 2017 (Paris, April 2017)

9.1.2. Scientific Events Selection

9.1.2.1. Chair of Conference Program Committees

- D. Augot was co-chair of Workshop on Coding and Cryptography (WCC) 2017 at St Petersburg (Russia).

9.1.2.2. Member of the Conference Program Committees

B. Smith: Latincrypt 2017, ECC (International Workshop on Elliptic Curve Cryptography) 2017.

D. Augot and A. Couvreur : Fifth Code-based Cryptography Workshop 2017, Tenerife, Spain.

A. Couvreur: WCC 2017 (Workshop on Coding and Cryptography 2017, St Petersbug, Russia).

A. Couvreur : AGC^{2}T 2017 (Arithmetic Geometry Cryptography and Coding Theory 2017, Marseille, France).

D. Augot: International Conference on Mathematical Aspects of Computer and Information Sciences https://macis2017.sba-research.org/

9.1.2.3. Reviewer

B. Smith: IFIPSEC2017, Africacrypt 2017, WCC 2017, Asiacrypt 2017, Eurocrypt 2017, MACIS 2017, PKC 2018

J. Lavauzelle: MACIS 2017

A. Couvreur: Crypto 2017, Eurocrypt 2017, ISIT 2017.

9.1.3. Journal

9.1.3.1. Member of the Editorial Boards

F. Morain is member of the editorial board of the *Applicable Algebra in Engineering, Communication and Computing*, Springer.

9.1.3.2. Reviewer - Reviewing Activities

B. Smith: Theory of Computing Systems, Springer Women in Mathematics, Research in Number Theory, IEEE Transactions on Information Theory, Journal of Cryptographic Engineering.

A. Couvreur: IEEE Transactions on Information Theory, IEEE Transactions on Communication, Journal of Number Theory, SIAM Journal on Applied Algebra and Geometry.

9.1.4. Invited Talks

B. Smith was an invited speaker at the annual FMF Symposium, a public science event at Universiteit Groningen (Groningen, NL, November 2017)

B. Smith was an invited speaker in the SIAM Applied Algebraic Geometry minisymposium on Applications of Computational Algebraic Geometry to Cryptology (Atlanta, USA, August 2017).

B. Smith was an invited speaker at the FoCM workshop on Computational Number Theory (Barcelona, ES, July 2017)

B. Smith was an invited speaker at the Summer School on Real-World Crypto and Privacy (Sibenik, HR, June 2017)

B. Smith was an invited speaker at JeudiX, a public science outreach event of École polytechnique (Paris, January 2017)

9.1.5. Animation of Seminars

- D. Augot is member of the scientific committee of the CCA seminar, "Codage, Cryptographie et Algorithms", https://cca.inria.fr
- D. Augot, with Bernadette Charron-Bost, is heading the scientific committee of the Blocksem seminar at Polytechnique, on blockchains, http://www.lix.polytechnique.fr/blocksem
- D. Augot, with Fabrice Le Fessant, organised the Open Source Spring on blockchains http://www.open-source-innovation-spring.org/

9.1.6. Research Administration

F. Morain is vice-head of the Département d'informatique of Ecole Polytechnique.

F. Morain is member of the Board of Master Parisien de Recherche en Informatique (MPRI).

A. Couvreur is member of LIX's *Conseil de laboratoire*.

B. Smith was the International Correspondant for CRI Saclay.

B. Smith was a member of the COST-GTRI.

D. Augot is elected member of the "conseil académique consultatif" de Paris-Saclay.

D. Augot was in the "comité de sélection" for a "maître de conférences" position in Grenoble

D. Augot was heading the "comité de sélection" for a "maître de conférences" position in Rouen

9.2. Teaching - Supervision - Juries

9.2.1. Teaching

Licence:

B. Smith, Computer Programming (CSE101), 23h EqTD, L1, École polytechnique, France

J. Lavauzelle, 1I001, *Éléments de programmation*, tutorial class (17.5h equiv TD), L1, Université Pierre et Marie Curie

J. Lavauzelle, 2I003, *Initiation à l'algorithmique*, tutorial class (47.5h equiv TD), L2, Université Pierre et Marie Curie

A. Couvreur and E. Barelli, INF411, "Les bases de la programmation et de l'algorithmique", 21.3h (equiv TD), 2nd year (L3), Ecole Polytechnique, France.

E. Barelli, INF311, "Introduction à l'informatique", 26.7h(equiv TD), 1st year, Ecole Polytechnique, France.

Master:

B. Smith, Advanced Cryptology (INF568), 55h EqTD, M1, École polytechnique, France

B. Smith and F. Morain, Algorithmes Arithmétiques pour la Cryptologie (2-12-2), 20h EqTD, M2, Master Parisien de Recherche en Informatique (MPRI), France

A. Couvreur and F. Morain, Introduction to Cryptology (INF558), 40h, M1, École polytechnique, France

A. Couvreur, Error Correcting Codes and Applications to Cryptography, (2-13-2), 15h, M2, MPRI, FRANCE

Master 2 intern

- D. Augot was the director of Rémi Clarisse internship on the Chor-Rivest cryptosystem

Students project

- D. Augot was managing two groups of polytechniques students on their own project: one about a voting system based on homomorphic encryption (with CEA List), the second about a medical kidney exchange scheme secured and enforced by the Hyperledger/fabric blockchain (with Orange)

9.2.2. Supervision

PhD : Cyril Hugounenq, Volcans et calcul d'isogénies, Université Paris Saclay, 25/09/2017, F. Morain& L. Goubin & L. De Feo.

9.2.3. Juries

- D. Augot
  - examinator of the PhD defense of Sarah Kamel, "Sécurité pour les réseaux sans fil", le 10 mars 2017 (Télécom Paris Tech)
  - examinator of the PhD defense of Francisco Vial-Prado, "Contributions to the design and analysis of fully homomorphic encryption schemes, le 12 juin 2017 (Université Versailles Saint-Quentin)
  - examinator of the PhD defense of Vlad Dragoi "Approche algébrique pour l'étude et la résolution de problèmes algorithmiques issus de la cryptographie et de la théorie des codes", le 6 juillet 2017 (University of Rouen).
  - examinator of the PhD defense of Mohamed A. M. Saeed Taha "Algebraic Approach for Code Equivalence", le 18 décembre 2017 (University of Rouen).
- A. Couvreur
  - PhD : Hervé Talé Kalachi (University of Rouen).
  - Agrégation de Mathématiques.

9.3. Popularization

- A. Couvreur gave the *Conférence inaugurale* of the *Semaine des mathématiques* in the accadémie de Créteil: *Cryptographie, le langage des secrets*.

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, 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] D. AUGOT, P. LOIDREAU, G. ROBERT. *Generalized Gabidulin codes over fields of any characteristic*, in "Designs, Codes and Cryptography", 2017, https://arxiv.org/abs/1703.09125 , forthcoming [*DOI :* 10.1007/s10623-017-0425-6], https://hal.archives-ouvertes.fr/hal-01503212

[9] C. COSTELLO, B. SMITH. *Montgomery curves and their arithmetic: The case of large characteristic fields*, in "Journal of Cryptographic Engineering", 2017, https://arxiv.org/abs/1703.01863 [*DOI :* 10.1007/s13389-017-0157-6], https://hal.inria.fr/hal-01483768

[10] A. COUVREUR, A. OTMANI, J.-P. TILLICH. *Polynomial Time Attack on Wild McEliece Over Quadratic Extensions*, in "IEEE Transactions on Information Theory", January 2017, vol. 63, n^{o} 1, pp. 404–427 [*DOI :* 10.1109/TIT.2016.2574841], https://hal.inria.fr/hal-01661935

[11] C. RITZENTHALER, R. LERCIER, F. ROVETTA, J. SIJSLING, B. SMITH. *Distributions of traces of Frobenius for smooth plane curves over finite fields*, in "Experimental Mathematics", 2017, https://arxiv.org/abs/1510.05601 [*DOI :* 10.1080/10586458.2017.1328321], https://hal.inria.fr/hal-01217995

International Conferences with Proceedings

[12] D. AUGOT, H. CHABANNE, T. CHENEVIER, W. GEORGE, L. LAMBER. *A User-Centric System for Verified Identities on the Bitcoin Blockchain*, in "International Workshop on Cryptocurrencies and Blockchain Technology - CBT'17", Oslo, Norway, September 2017, https://arxiv.org/abs/1710.02019 , https://hal.inria.fr/hal-01611251

[13] D. AUGOT, H. CHABANNE, O. CLÉMOT, W. GEORGE. *Transforming face-to-face identity proofing into anonymous digital identity using the Bitcoin blockchain*, in "PST2017 - International Conference on Privacy, Security and Trust", Calgary, Canada, August 2017, 10 p. , https://arxiv.org/abs/1710.02951 , https://hal.inria.fr/hal-01611297

[14] L. GRÉMY, A. GUILLEVIC, F. MORAIN, E. THOMÉ. *Computing discrete logarithms in $GF(p^6)$*, in "24th Annual Conference on Selected Areas in Cryptography", Ottawa, Canada, August 2017, https://hal.inria.fr/hal-01624662

[15] J. RENES, B. SMITH. *qDSA: Small and Secure Digital Signatures with Curve-based Diffie–Hellman Key Pairs*, in "ASIACRYPT 2017", Hong Kong, China, IACR, December 2017, https://arxiv.org/abs/1709.03358 , https://hal.inria.fr/hal-01585322

Conferences without Proceedings

[16] E. BARELLI. *On the security of Some Compact Keys for McEliece Scheme*, in "WCC 2017 - The Tenth International Workshop on Coding and Cryptography", St Petersbourg, Russia, September 2017, pp. 1-9, https://hal.inria.fr/hal-01674546

[17] J. LAVAUZELLE. *Constructions for efficient Private Information Retrieval protocols*, in "WCC 2017 - The Tenth International Workshop on Coding and Cryptography", Saint-Petersbourg, Russia, Inria and SUAI and Skoltech, September 2017, pp. 1-12, https://hal.inria.fr/hal-01633469

Other Publications

[18] C. BACHOC, A. COUVREUR, G. ZÉMOR. *Towards a function field version of Freiman's Theorem*, September 2017, https://arxiv.org/abs/1709.00087 - working paper or preprint, https://hal.archives-ouvertes.fr/hal-01584034

[19] M. BARDET, E. BARELLI, O. BLAZY, R. CANTO TORRES, A. COUVREUR, P. GABORIT, A. OTMANI, N. SENDRIER, J.-P. TILLICH. *BIG QUAKE BInary Goppa QUAsi–cyclic Key Encapsulation*, December 2017, submission to the NIST post quantum cryptography standardization process, https://hal.archives-ouvertes.fr/hal-01671866

[20] E. BARELLI, P. BEELEN, M. DATTA, V. NEIGER, J. ROSENKILDE. *Two-Point Codes for the Generalized GK Curve*, October 2017, working paper or preprint, https://hal.archives-ouvertes.fr/hal-01535513

[21] N. COXON. *Fast systematic encoding of multiplicity codes*, April 2017, https://arxiv.org/abs/1704.07083 - working paper or preprint, https://hal.archives-ouvertes.fr/hal-01512372

[22] L. GRÉMY, A. GUILLEVIC, F. MORAIN. *Breaking DLP in $GF(p^5)$ using 3-dimensional sieving*, July 2017, working paper or preprint, https://hal.inria.fr/hal-01568373

References in notes

[23] 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