IN PARTNERSHIP WITH:
CNRS

Ecole Polytechnique

Activity Report 2018

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
A4.3.4. - Quantum Cryptography
A4.8. - Privacy-enhancing technologies
A8.1. - Discrete mathematics, combinatorics
A8.4. - Computer Algebra
A8.5. - Number theory

Other Research Topics and Application Domains:

B9.5.1. - Computer science
B9.5.2. - Mathematics
B9.10. - Privacy

1. Team, Visitors, External Collaborators

Research Scientists

Daniel Augot [Team leader, Inria, Senior Researcher, HDR]
Alain Couvreur [Inria, Researcher]
Benjamin Smith [Inria, Researcher]
Matthieu Rambaud [Inria, Researcher, en détachement depuis le corps Mines-Télécom, until Sep 2018]

Faculty Members

Luca de Feo [Université de Versailles Saint-Quentin-en-Yvelines, Associate Professor, en délégation depuis l'Université de Versailles Saint-Quentin, until Aug 2018]
Françoise Levy-Dit-Vehel [École Nationale Supérieure de Techniques Avancées, Professor, HDR]
François Morain [Ecole polytechnique, Professor, HDR]

Post-Doctoral Fellow

William George [Ecole polytechnique, until Jan 2018]

PhD Students

Elise Barelli [Inria, until Aug 2018]
Lucas Benmouffok [Institut de recherche technologique System X, from Oct 2018]
Hanna-Mae Bisserier [Institut de recherche technologique System X]
Sarah Bordage [Ecole polytechnique, from Oct 2018]
Mathilde Chenu de La Morinerie [Ecole polytechnique, from Oct 2018]
Hussein Khazaie [Inria, until May 2018]
Julien Lavauzelle [Ecole polytechnique until Sep 2018, Inria from Oct 2018]
Isabella Panaccione [Inria, from Oct 2018]

Technical staff

Nicholas Coxon [Inria, until nov 2018]

Interns

Lucas Benmouffok [Inria, from Mar 2018 until Jul 2018]
Sarah Bordage [Inria, from Apr 2018 until Aug 2018]
Christophe Levrat [Inria, from Apr 2018 until Jul 2018]
Isabella Panaccione [Inria, from Mar 2018 until Jul 2018]
Mattia Veroni [Inria, from Mar 2018 until Jun 2018]

Administrative Assistants

Jessica Gameiro [Inria, until Apr 2018]
Maria Agustina Ronco [Inria, from May 2018]

External Collaborators

Luca de Feo [Université de Versailles Saint-Quentin-en-Yvelines, from Sep 2018]
Elise Barelli [Univ de Versailles Saint-Quentin-en-Yvelines, from Sep 2018]

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. Internet of Things

The *Internet of Things* (IoT) is the network and application space formed by the millions of small, connected devices that are increasingly present in our daily lives, and by the servers, clouds, and apps that they communicate with. This includes not only consumer devices such as smartphones, household devices, and wearable technology, but also an increasinly large proportion of our fundamental civic infrastructure (as is reflected by the increasing attention given to *Smart Cities*).

The IoT is therefore a massive, pervasive, and highly heterogeneous distributed computing system; a system that is mostly unprotected and insecure. Many of the devices are simply too small and underpowered to run the conventional cryptosystems that are standard for internet communications: even a minimalist TLS stack will often overwhelm the resources available on some small platforms. These limitations include small memory size, limited battery power, and low computational capacity. Not only are these devices harder to defend, but they are also much easier to attack: for example, these devices are generally extremely physically accessible (they must be, to fulfil their purpose), but this makes them extremely vulnerable to side-channel attacks.

Nevertheless, strong cryptography is essential to the future of IoT, precisely because these systems are so pervasive in our everyday lives, both individually (in our homes) and collectively (in our cities, industries, and urban infrastructure). We need strong cryptography to protect the personal and industrial data that these devices collect, process, and transmit; but we also need strong cryptography to ensure that devices and services can identify and authenticate themselves and each other with confidence. It is not enough to simply put secure systems in place; we must also develop reliable software update mechanisms, tailored to the needs and challenges of the IoT space.

While these technical challenges have been met, to some extent, for symmetric cryptosystems (which means that we have reasonable means of encrypting data and ensuring its integrity), they pose a massive problem for implementers of asymmetric cryptosystems (including key exchange, signatures, identification, and authentication). Efficient asymmetric cryptosystems have long been a research focus for GRACE, and our expertise in elliptic curve cryptosystems is of particular relevance for IoT, since these cryptosystems typically require the fewest memory and bandwidth resources.

Looking towards the future, the massive contemporary research effort in postquantum cryptosystems has so far mostly yielded systems even less-suited to IoT than conventional asymmetric systems are. Nevertheless, there is some hope that postquantum security can be brought to some IoT devices, and we are hopeful that GRACE's strength in isogeny-based cryptography will have an impact here.

4.2. Cloud storage

The team is concerned with several aspect of reliability and security of cloud storage, obtained mainly with tools from coding theory. On the privacy side, we build protocols for so-called Private Information Retrieval which enable a user to query a remote database for an entry, while not revealing his query. For instance, a user could query a service for stock quotes without revealing with company he is interested in. On the availability side, we study protocols for proofs of retrievability, which enable a user to get assurance that a huge file is still available on a remote server, with a low bandwith protocol which does not require to download the whole file. For instance, in a peer-to-peer distributed storage system, where nodes could be rewarded for storing data, they can be audited with proof of retrievability protocols to make sure they indeed hold the data.

We investigate these problems with algebraic coding theory, mainly codes with locality (locally decodable codes, locally recoverable codes, and so on).

4.3. Blockchains

The huge interest shown by companies for blockchains and cryptocurrencies have attracted the attention of mainstream industries for new, advanced uses of cryptographic, beyond confidentiality, integrity and authentication. In particular, zero-knowledge proofs, computation with encrypted data, etc, are now revealing their potential in the blockchain context. Team Grace is investigating two topics in these areas: secure multiparty computation and so-called "STARKS".

Secure multiparty computation enables several participants to compute a common function of data they each secretly own, without each participant revealing his data to the other participants. This area has seen great progress in recent years, and the cryptogaphic protocols are now mature enough for practical use. This topic is new to project-team Grace, and we will investigate it in the context of blockchains, through the lenses of use for private "smart contracts". A PhD student has been hired since October, funded by IRT System-X.

(ZK-)STARKS stands for "(Zero-Knowledge) Scalable Transparent ARguments of Knowledge", which can be zero knowledge or not. These techniques enable to have short probabilistic proof of correctness of program execution, which can be quicly checked by a verifier, without requiring the verifier to redo the computation again. This topic is close to the problem of computational integrity, and its theoretical foundations originate back to the 90's, which saw the formulation and proof of the celebrated PCP theorem. A protocol family equivalent of STARKS, "SNARKS", are well established, performant and promoted by the zerocash protocol for anomymous cryptocurrency (and also available in Ethereum), and STARKS are seen as a future replacement for SNARKS, overcoming the SNARKS problem of trusted setup. At the core of STARKS lie algebraic codes, mainly basic Reed-Solomon codes, and we will investigate replacement for the Reed-Solomon codes, to allow more performant (shorter) STARKS.

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.
NEWS OF THE YEAR: The main program for relation collection now supports composite "special-q", and also parallelizes better. The memory footprint of the central step of linear algebra has been reduced, and the parallelism of this step has been improved.

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

6. New Results

6.1. Fast transforms over fields of characteristic 2

Participant: Nicholas Coxon.

With the aim of reaching fast, linear time, algorithms for encoding multiplicity codes, which have good local properties, N. Coxon had to develop subalgorithms for dealing with the Hermite interpolation [13], which in turn relies on computer algebra for fast transforms over fields of characteritic two [14]. Locally decodable codes are used for private information retrieval, where a database can be privately queried by a user, in such a way that the user does not reveal his query. Using codes with locality for private information retrieval, the database is first encoded, then queried using the local property of the code. Since the databases in question can be large, only linear time algorithms can be used. Our results achieve linear-time complexity, and even with a non agressively optimized implementation, can encode as much as 10^9 bits in thirty seconds on a laptop.

6.2. Private information retrieval

Participants: Daniel Augot, Nicholas Coxon, Julien Lavauzelle, Françoise Levy-Dit-Vehel.

J. Lavauzelle continued his study on private information retrieval (PIR) protocols. First, he completed the construction of PIR protocols from transversal designs [8], initiated in 2017. Compared to existing protocols, the main benefit of the construction is to feature an optimal computation complexity for the servers. Sublinear communication complexity and negligeable storage overhead can also be achieved for some particular instances.

Second, in a joint work with R. Tajeddine, R. Freij-Hollanti and C. Hollanti from the University of Aalto (Finland), J. Lavauzelle considered the setting in which the database is encoded with an optimal regenerating code [16]. Quantitatively, their construction of PIR protocols improves upon a recent work of Dorkson and Ng, for every non-trivial set of parameters.

6.3. Locally correctable codes

Participant: Julien Lavauzelle.

In 2013, Guo, Kopparty and Sudan built a new family of locally correctable codes from lifting, achieving an arbitrarily high information rate for sublinear locality. J. Lavauzelle proposed an analogue of this construction in projective spaces [7]. The parameters of this construction are similar to the original work of Guo *et al.* Intertwined relations between the two families of codes were proven thanks to a careful analysis of their monomial bases. The practicality of the construction was also established through an implementation and a study of information sets and automorphisms of the code.

6.4. Cryptanalysis in code based cryptography

Participant: Alain Couvreur.

Following NIST call for post quantum cryptography, A. Couvreur and E. Barelli designed a key recovery attack against a McEliece–like encryption scheme called DAGS [9].

In addition, in collaboration with Matthieu Lequesne and Jean-Pierre Tillich (Inria Paris, SECRET team), A. Couvreur designed an attack against another proposal called RLCE (Random Linear Code Encryption) [12].

6.5. Commutative isogeny-based cryptography

Participants: Luca de Feo, Benjamin Smith.

Despite the many advances in post-quantum cryptography in recent years, efficient drop-in replacements for the classic Diffie–Hellman key exchange algorithm have proven elusive. L. De Feo, J. Kieffer, and B. Smith laid the algorithmic groundwork for *commutative isogeny-based key exchange* in [10]; this work became the basis of the exciting new CSIDH proposal [19].

6.6. Factoring oracles

Participants: François Morain, Benjamin Smith.

Integer factoring is an old topic, and the situation is as follows: in the classical world, we think integer factoring is hard and the algorithms we have are quite powerful though of subexponential complexity and factoring numbers with several hundred bits; whereas in the quantum world, it is assumed to be easy (i.e., there exists a quantum polynomial time algorithm) but never experienced and the record is something like a few bits. F. Morain, helped by B. Smith and G. Renault (ANSSI) studied the theoretical problem of factoring integers given access to classical oracles, like the Euler totient function. They were able to give some interesting classes of numbers that could tackled, see [17].

7. Bilateral Contracts and Grants with Industry

7.1. Bilateral Contracts with Industry

7.1.1. Nokia

Participants: Daniel Augot, Nicholas Coxon, Françoise Levy-Dit-Vehel.

Phase 2 has been finished, while a new phase, phase 3, has been negociated between Inria and Nokia. Grace finished his work on fast algorithms for polynomials over fields of small caracteristic, wth application to coding theory, multiplicity codes and private information retrieval. The new phase will fund a project on rank-metric codes for security and privacy in cloud storage (in collaboration with Gilles Zémor, Uni. Bordeaux).

8. Partnerships and Cooperations

8.1. Regional Initiatives

Participants: Daniel Augot, Matthieu Rambaud.

A “research initiative” “BART” (Blockchain advanced research and technologies) has been launched with three partners: Inria, Institut Mines-Télécom, and System-X. This is funded by *Institut de recherche* System-X, located in Paris-Saclay area, whose objective is to connect industry and academia. A new PhD has been started, with L. Benmouffok, hired in October 2018, whose topic is the use of secure multiparty computation in blockchains.

8.2. National Initiatives

8.2.1. ANR

Participants: Daniel Augot, Alain Couvreur, Matthieu Rambaud.

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/.

8.3. European Initiatives

8.3.1. SPARTA

- Program: H2020
- Project acronym: SPARTA
- Project title: SPARTA
- Duration: three years
- Coordinator: CEA
- Other partners: IMT, Inria, ANSSI
- Abstract: Propose, test, validate and exploit the possible organizational, technological and operational setup of a cybersecurity competence network; Produce a roadmap that include targets to be achieved by the end of the project, as well as priorities to be addressed in the future by the Cybersecurity Competence Network; Serve to align research, education and certification; Build on and align existing roadmap efforts.
  Participant: Benjamin Smith.

8.3.2. 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. 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.

These systems are all broken as soon as large quantum computers are built. 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: 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, ended in March 2018.
Participants: Daniel Augot, Matthieu Rambaud.

9. Dissemination

9.1. Promoting Scientific Activities

9.1.1. Scientific Events Selection

9.1.1.1. Member of the Conference Program Committees

- D. Augot was in the program committee of FAB 2018, Foundations and Applications of Blockchain, Los Angeles.
- D. Augot was in the program committee of WTSC 2018, Workshop on Trusted Smart Contracts, Curaçao.
- D. Augot was in the program committee of WAIFI 2018, Workshop on the Arithmetic of Finite Fields, Bergen, Norway.
- D. Augot was in the program committee of BCT 2018, International Workshop on Cryptocurrencies and Blockchain Technology, in conjunction with ESORICS 2018, Barcelona.
- A. Couvreur was in the program committee of the *Journées codes et cryptographie (C2) 2018.*

9.1.1.2. Reviewer

- D. Augot: ISIT 2018 (International Symposium on Information Theory)
- B. Smith: ANTS 2018, Indocrypt 2018, PKC 2019

9.1.2. Journal

9.1.2.1. Member of the Editorial Boards

- F. Morain is member of the editorial board of the *Applicable Algebra in Engineering, Communication and Computing*, Springer.
- With Thomas Johansson, Marine Minier, Faina Soloveva, Victor Zinonviev, D. Augot is guest editor for a special issue of *Designs, Codes and Cryptography*, devoted to WCC2017, Workshop on Coding and Cryptography, St Petersburg, Russia.

9.1.2.2. Reviewer - Reviewing Activities

- A. Couvreur: Designs, Codes and Cryptography, Asiacrypt 2018, IEEE Transactions on information theory, Advances in Mathematics of communication, etc...
- J. Lavauzelle: Designs, Codes and Cryptography (special issue WCC 2017)
- B. Smith: Designs, Codes, and Cryptography, Finite Fields and their Applications, Journal of the London Mathematical Society, Mathematics of Computation,

9.1.3. Invited Talks

- D. Augot was an invited speaker of the Munich Workshop on Coding and Cryptography (MWCC) 2018
- D. Augot was an invited speaker at ACA 2018, Application of Computer Algebra, Santiago de Compostela
- D. Augot was invited at Dasgsthul Seminar 18511, Algebraic Coding Theory for Networks, Storage, and Security, and gave here a talk.
- B. Smith was an invited speaker at the *International Workshop on the Arithmetic of Finite Fields (WAIFI 2018)* (Bergen, Norway).
- B. Smith was an invited speaker at the *Journées Codage et Cryptographie 2018* (Aussois, France).

9.1.4. Industrial Show

- F. Levy-dit-Vehel demoed our Private Information Retrieval protocol at "FIC", International Security Forum, Lille, January 2018.

9.1.5. Leadership within the Scientific Community

- D. Augot is member of the scientific committee of the C2-CCA seminar, held three or four times a year, with a France wide audience, and which is the seminar of "groupe de travail" C2 "codage et cryptographie" of the GDR IM "groupement de recherche informatique mathématique".
- D. Augot is leading the scientific committee of the blocksem seminar of Plateau de Saclay.

9.1.6. Scientific Expertise

- A. Couvreur was evaluator for research grants attribution by university of Crete.

9.1.7. Research Administration

- F. Morain is vice-head of the Département d'informatique of Ecole Polytechnique; in charge of years 1 and 2 for Computer Science courses.
- F. Morain is member of the Board of Master Parisien de Recherche en Informatique (MPRI).
- A. Couvreur is member of Inria Saclay *Commission Scientifique*.
- D. Augot was member of the jury for two Inria Grenoble Rhône-Alpes positions
- D. Augot was member of the jury for a position at Institut Mines-Télécom.

9.2. Teaching - Supervision - Juries

9.2.1. Teaching

Licence :

- F. Morain, Lectures for INF311: "Introduction à l'informatique", 15h (equiv TD), 1st year (L3), École polytechnique. Coordinator of this module (350 students).
- J. Lavauzelle, *Éléments de programmation* (1I002), 13.5h, L1, Université Pierre et Marie Curie, France
- A. Couvreur, INF411 *Introduction à la programmation et à l'algorithmique*, 40h, L3, École Polytechnique, France

- B. Smith, CSE101 *Introduction to Computer Programming*, 36h, L1, École polytechnique, France

Master :

- F. Morain is the scientific leader of the Graduate Degree *Cybersecurity: Threats and Defense* of École Polytechnique.
- A. Couvreur, *Coding theory and application to cryptography*, 20h, M2, MPRI (Université Paris VII, ENS Paris, ENS Cachan, École Polytechnique), France
- F. Morain and A. Couvreur, INF558, *Introduction to cryptology*, 36h, M1, École Polytechnique.
- B. Smith, INF568 *Advanced Cryptography*, 36h, M1, École polytechnique
- B. Smith and F. Morain, *Algorithmes arithmétiques pour la cryptologie*, 20h, M2, MPRI (Université Paris VII, ENS Paris, ENS Cachan, École Polytechnique), France
- F. Levy-dit-Vehel, discrete maths, 21h, M1, ENSTA.
- F. Levy-dit-Vehel, cryptography, 24h, M2, ENSTA.

Doctorat :

- A. Couvreur, *Introduction to code based cryptography*, 6 hours. Spring school *Post Scryptum*

9.2.2. Supervision

- PhD : J. Lavauzelle, *Codes à propriétés locales : constructions et applications à des protocoles cryptographiques*, Université Paris Saclay.
- PhD : E. Barelli, *Étude de la sécurité de certaines clés compactes pour le schéma de McEliece utilisant des codes géométriques*, Université Paris Saclay.

9.2.3. Juries

- D. Augot, A. Couvreur, and F. Levy-dit-Vehelwere in the jury of J. Lavauzelle's PhD defense, le 30 novembre 2018, à Palaiseau: *Codes à propriétés locales : constructions et applications à des protocoles cryptographiques*
- D. Augot and A. Couvreur were in the jury of E. Barelli's PhD defense, le 10 décembre 2018 à Palaiseau: *Étude de la sécurité de certaines clés compactes pour le schéma de McEliece utilisant des codes géométriques*
- D. Augot was in in the committee of
  - Victor Cauchois, le jeudi 13 Décembre 2018 à Rennes: *Couches de diffusion linéaires à partir de matrices MDS*
  - Sviat Covanov, le 5 juin 2018 à Nancy: *Multiplication algorithms: algebraic complexity and fast asymptotic methods*
  - Jonathan Detchart, le 5 décembre 2018, à Toulouse: *Optimisation de codes correcteurs d'effacements par application de transformées polynomiales*

9.3. Popularization

9.3.1. Internal or external Inria responsibilities

- D. Augot is member of the "comité de pilotage" the "BART" (Blockchain advanced research and technologies) research initiative, with Institut Mines Télécom and System-X.

9.3.2. Interventions

- D. Augot was interviewed on blockchains by three representatives of the French National Assembly.

- D. Augot was interviewed by “France Stratégie”, an institution attached to the Prime Minister to support forward thinking of the French government.
- F. Levy-dit-Vehel demoed our Private Information Retrieval protocol with partitionned locally decodable codes

10. Bibliography

Publications of the year

Doctoral Dissertations and Habilitation Theses

[1] E. BARELLI. *Étude de la sécurité de certaines clés compactes pour le schéma de McEliece utilisant des codes géométriques*, Université Paris-Saclay, December 2018, https://pastel.archives-ouvertes.fr/tel-01982502

[2] J. LAVAUZELLE. *Codes with locality : constructions and applications to cryptographic protocols*, Université Paris-Saclay, November 2018, https://pastel.archives-ouvertes.fr/tel-01951078

Articles in International Peer-Reviewed Journals

[3] B. AUDOUX, A. COUVREUR. *On tensor products of CSS Codes*, in "Annales de l’Institut Henri Poincaré (D) Combinatorics, Physics and their Interactions", 2018, https://arxiv.org/abs/1512.07081 , https://hal.archives-ouvertes.fr/hal-01248760

[4] D. AUGOT, P. LOIDREAU, G. ROBERT. *Generalized Gabidulin codes over fields of any characteristic*, in "Designs, Codes and Cryptography", 2018, vol. 86, n^{o} 8, pp. 1807-1848, https://arxiv.org/abs/1703.09125 [*DOI :* 10.1007/S10623-017-0425-6], https://hal.archives-ouvertes.fr/hal-01503212

[5] C. BACHOC, A. COUVREUR, G. ZÉMOR. *Towards a function field version of Freiman’s Theorem*, in "Algebraic Combinatorics", 2018, vol. 1, n^{o} 4, pp. 501-521, https://arxiv.org/abs/1709.00087 [*DOI :* 10.5802/ALCO.19], https://hal.archives-ouvertes.fr/hal-01584034

[6] E. BARELLI, P. BEELEN, M. DATTA, V. NEIGER, J. ROSENKILDE. *Two-Point Codes for the Generalized GK Curve*, in "IEEE Transactions on Information Theory", 2018 [*DOI :* 10.1109/TIT.2017.2763165], https://hal.archives-ouvertes.fr/hal-01535513

[7] J. LAVAUZELLE. *Lifted projective Reed–Solomon codes*, in "Designs, Codes and Cryptography", 2018, https://arxiv.org/abs/1809.00931 [*DOI :* 10.1007/S10623-018-0552-8], https://hal.archives-ouvertes.fr/hal-01901147

[8] J. LAVAUZELLE. *Private Information Retrieval from Transversal Designs*, in "IEEE Transactions on Information Theory", 2018, 1 p. , https://arxiv.org/abs/1709.07952 [*DOI :* 10.1109/TIT.2018.2861747], https://hal.archives-ouvertes.fr/hal-01901014

International Conferences with Proceedings

[9] E. BARELLI, A. COUVREUR. *An efficient structural attack on NIST submission DAGS*, in "ASIACRYPT 2018", Brisbane, Australia, Advances in Cryptology – ASIACRYPT 2018, December 2018, vol. 11272, https://arxiv.org/abs/1805.05429 [*DOI :* 10.1007/978-3-030-03326-2_4], https://hal.archives-ouvertes.fr/hal-01796338

[10] L. De Feo, J. Kieffer, B. Smith. *Towards practical key exchange from ordinary isogeny graphs*, in "ASIACRYPT 2018", Brisbane, Australia, December 2018, https://arxiv.org/abs/1809.07543 , https://hal.inria.fr/hal-01872817

Other Publications

[11] A. Couvreur, M. Lequesne, J.-P. Tillich. *Recovering short secret keys of RLCE encryption scheme in polynomial time*, October 2018, JC2 2018 - Journées Codage et Cryptographie, https://hal.inria.fr/hal-01959617

[12] A. Couvreur, M. Lequesne, J.-P. Tillich. *Recovering short secret keys of RLCE in polynomial time*, May 2018, https://arxiv.org/abs/1805.11489 - working paper or preprint, https://hal.archives-ouvertes.fr/hal-01803440

[13] N. Coxon. *Fast Hermite interpolation and evaluation over finite fields of characteristic two*, July 2018, https://arxiv.org/abs/1807.00645 - working paper or preprint, https://hal.archives-ouvertes.fr/hal-01827583

[14] N. Coxon. *Fast transforms over finite fields of characteristic two*, July 2018, https://arxiv.org/abs/1807.07785 - working paper or preprint, https://hal.archives-ouvertes.fr/hal-01845238

[15] S. Galbraith, L. Panny, B. Smith, F. Vercauteren. *Quantum Equivalence of the DLP and CDHP for Group Actions*, December 2018, https://arxiv.org/abs/1812.09116 - working paper or preprint, https://hal.inria.fr/hal-01963660

[16] J. Lavauzelle, R. Tajeddine, R. Freij-Hollanti, C. Hollanti. *Private Information Retrieval Schemes with Regenerating Codes*, November 2018, https://arxiv.org/abs/1811.02898 - working paper or preprint, https://hal.archives-ouvertes.fr/hal-01951956

[17] F. Morain, G. Renault, B. Smith. *Deterministic factoring with oracles*, February 2018, https://arxiv.org/abs/1802.08444 - working paper or preprint, https://hal.inria.fr/hal-01715832

[18] B. Smith. *Pre- and post-quantum Diffie-Hellman from groups, actions, and isogenies*, September 2018, https://arxiv.org/abs/1809.04803 - working paper or preprint, https://hal.inria.fr/hal-01872825

References in notes

[19] W. Castryck, T. Lange, C. Martindale, L. Panny, J. Renes. *CSIDH: An Efficient Post-Quantum Commutative Group Action*, in "Advances in Cryptology - ASIACRYPT 2018 - 24th International Conference on the Theory and Application of Cryptology and Information Security, Brisbane, QLD, Australia, December 2-6, 2018, Proceedings, Part III", T. Peyrin, S. D. Galbraith (editors), Lecture Notes in Computer Science, Springer, 2018, vol. 11274, pp. 395–427, https://doi.org/10.1007/978-3-030-03332-3_15