Activity Report 2013

Project-Team GRACE

Geometry, arithmetic, algorithms, codes and encryption

RESEARCH CENTER
Saclay - Île-de-France

THEME
Algorithmics, Computer Algebra and Cryptology

Table of contents

Project-Team GRACE

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

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

1. Members

Research Scientists

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

Faculty Member

François Morain [Ecole Polytechnique, Professor, HdR]

External Collaborators

Françoise Levy-Dit-Vehel [ENSTA, Associate Professor, HdR]
Johan Nielsen [Ph.D. DTU Lyngby, until Oct 2013]
Guillaume Quintin [Univ. Limoges, from Oct 2013]

PhD Students

Cécile Goncalves [Ecole Polytechnique]
Pierre Karpman [Inria, from Nov 2013]
Gwezheneg Robert [Univ. Rennes I]
Alexander Zeh [Ph.D. Uni. Ulm, until Dec 2013]

Post-Doctoral Fellows

Nicolas Delfosse [Ecole Polytechnique, until Sep 2013]
Irene Marquez Corbella [Inria, from Oct 2013]
Julia Pieltant [Inria]

Administrative Assistant

Valerie Annie Lecomte [Inria]

Other

Charlotte Scribot [Min. de l'Education Nationale, enseignant, from Sep 2013]

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.

2.2. Highlights of the Year

- *Number-Theoretic Algorithms for Asymmetric Cryptology* Workshop. On June 20 and 21, 2013, GRACE hosted an international workshop on number-theoretic algorithms for asymmetric cryptology (with the support of Digicosme). Our invited speakers included Steven Galbraith (Auckland), Florian Hess (Oldenburg), Razvan Barbulescu (LORIA), Andreas Enge (Inria Bordeaux), Antoine Joux (UVSQ and Cryptoexperts), and Vadim Lyubashevsky (Inria Paris–Rocquencourt). Forty researchers attended over the two days. This workshop saw the first public announcement and presentation of what is undoubtedly the most remarkable new result in algorithmic number theory in 2013, if not the last decade: Barbulescu, Gaudry, Joux, and Thomé's quasi-polynomial time algorithm for discrete logarithms in a large class of finite fields.
- ISN-Privacy. In year 2013, N. Boujemaa's proposal for an *Institut de la société du numérique* (Digital Society Institute) was accepted within IDEX Paris-Saclay. This proposal aims to foster interdisciplinary research involving both computer scientists and researchers in the humanities. Daniel Augot joined researchers from project-teams COMETE (Saclay) and SMIS (Paris–Rocquencourt) in regular monthly discussions with economists and lawyers; a seminar will be held in Summer 2014. Funding was allocated from the IDEX to the PAIP (*Pour une Approche Interdisciplinaire de la Privacy*) project for all the partners of the privacy group.
- A special issue of *Designs, Codes and Cryptography* co-edited by Daniel Augot, devoted to the WCC2011 conference proceedings, was published in January 2013 [16].

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 number fields; and
- algorithms for algebraic curves (over all kinds of fields).

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

3.2. Arithmetic Geometry: Curves and their Jacobians

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

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

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

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

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

3.3. Curve-Based cryptology

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

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

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

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

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

3.4. Algebraic Coding Theory

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

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

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

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

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

4. Application Domains

4.1. Cryptography and Cryptanalysis

In the twenty-first century, cryptography plays two essential rôles: 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; and
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.

François Morain and Benjamin 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, Morain's elliptic curve point counting and primality proving algorithms are essential tools in the everyday construction of strong public-key cryptosystems, while Smith's recent work on elliptic curves aims to improve the speed of curve-based cryptosystems (such as Elliptic Curve Diffie–Hellman key exchange, a crucial step in establishing secure internet connections) without compromising their security.

Daniel Augot, Françoise Levy-dit-Vehel, and Alain 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, Couvreur's work on distinguishing codes has an important impact on the design of code-based systems built over algebraic geometry codes, and on the choice of parameter sizes for secure implementations. But coding theory also has important practical applications in the improvement of conventional symmetric cryptosystems. For example, Augot's recent work on MDS matrices via BCH codes gives a more efficient construction of optimal diffusion layers in block ciphers.

4.2. Privacy

While cryptography classically aims to provide confidentiality for messages during their transmission between a sender and a recipient, privacy is a broader, more subtle, and sometimes less technical issue.

Daniel Augot with other groups from Inria (Comete, SMIS) started discussions with lawyers and economists, fostered by IDEX Paris-Saclay's *Institut de la société du numérique*, to understand the privacy concerns of ordinary citizens. On a more technical side, privacy can be protected with cryptographic protocols other than encryption. In this direction, Grace is engaged since April 2013 in a collaboration with Alcatel–Lucent on private data storage and retrieval in the cloud.

5. Software and Platforms

5.1. ECPP

François Morain has been continually improving his primality proving algorithm, ECPP, originally developed in the early 1990s. Proving the primality of a 512-bit number requires less than a second on an average PC. Morain's personal record is around 25000 decimal digits, using the FASTECPP variant that he started developing in 2003. The code is written in C, and based on publicly available packages (GMP, MPFR, MPC, MPFRCX).

5.2. SEA

Together with E. Schost and L. De Feo, François Morain has developed a new implementation of the SEA algorithm for computing the cardinality of elliptic curves over large prime and binary finite fields. This program is a `gforge` project, based on the NTL library. The large prime case is relevant to cryptographic needs; the binary case, while not useful in contemporary cryptography, is a good testbed for De Feo's FAAST package.

5.3. TIFA

TIFA (Tools for Integer FActorization), initially developed in 2006, has been continuously improved during the last few years. TIFA includes a base library written in C99 using the GMP library, stand-alone factorization programs, and a basic benchmarking framework. Available online at http://www.lix.polytechnique.fr/Labo/Jerome.Milan/tifa/tifa.xhtml, TIFA is distributed under the Lesser General Public License (version 2.1 or later).

5.4. Quintix

Guillaume Quintin's Quintix library implements efficient arithmetic in Galois rings and their unramified extensions, the root-finding algorithms presented in [7], basic functions for the manipulation of Reed–Solomon codes, and the complete Sudan list-decoding algorithm. Part of the Mathemagix computer algebra system (http://www.mathemagix.org/), the source code is distributed under the General Public License (version 2 or higher).

5.5. finitefieldz

Within the Mathemagix CAS (http://www.mathemagix.org/), Guillaume Quintin wrote the finitefieldz package, which provides arithmetic for finite fields and towers of finite fields, as well as univariate polynomial root finding and factorization over finite fields.

5.6. Decoding

DECODING is a standalone C library licensed under the GPLv2. 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 and benchmarking of general decoding algorithms. As of 2012/12/13, DECODING provides a working list decoding algorithm, but there is no unique decoding algorithm (though this can be emulated by list-decoding up to half the minimum distance). The library is being still under development, and more algorithms will be added. DECODING was presented at the 2012 International Symposium on Symbolic and Algebraic Computation.

6. New Results

6.1. Diffusion layers for block ciphers

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

6.2. Rank metric codes over the rationals

Rank metric and Gabidulin codes over the rationals promise interesting applications to space-time coding. We have constructed optimal codes similar to Gabidulin codes but with complex coefficients, using number fields and Galois automorphisms. Using these codes we can completely bypass intermediate constructions using finite fields, which were the stumbling-block in classic constructions.

6.3. Cryptanalysis of McEliece cryptosystems based on Generalised Reed–Solomon codes

The McEliece encryption scheme based on binary Goppa codes was one of the first public-key encryption schemes [24]. Niederreiter [25] dramatically reduced the (huge) key size—a major problem with McEliece's original proposal—using Generalised Reed–Solomon (GRS) codes, but his modified scheme was broken by Sidelnikov and Shestakov [26] in 1992. There have been several attempts at repairing these smaller-key McEliece schemes. In collaboration with P. Gaborit, V. Gautier, A. Otmani and J.-P. Tillich, Alain Couvreur found polynomial time attacks on these schemes using the distinguishability of GRS codes from random codes.

6.4. New Identities relating Goppa codes

Goppa codes are strongly related to AG codes based on curves of genus 0. Among other applications, these codes are very famous for their cryptographic potential: they are one of the very few families of algebraic codes proposed for the McEliece encryption scheme which have not been broken up to now. At least for this reason, getting further knowledge on the structure of such codes is of interest. In [19], Alain Couvreur, A. Otmani and J.-P. Tillich proved a new identity yielding many improvements in the designed parameters of Goppa codes.

6.5. Root finding algorithms over local rings

Guillaume Quintin, in collaboration with J. Berthomieu and G. Lecerf, has developed new algorithms computing the roots of polynomials over complete local unramified rings [7]; this is important in the second stage of Guruswami–Sudan list decoding algorithms for codes over finite rings. Quintin has implemented these algorithms in MATHEMAGIX, using his FINITEFIELDZ and QUINTIX librairies.

6.6. Codes over rings

M. Barbier, C. Chabot and Guillaume Quintin proposed a new description for quasi–cyclic codes using the ring of matrices with polynomial entries, thus defining the new class of *quasi-BCH* codes. Guillaume Quintin proved that these codes can be regarded as interleaved subcodes of Reed–Solomon codes; this allowed them to define a polynomial-time decoding algorithm for quasi-BCH codes. Guillaume Quintin also generalized list decoding algorithms to codes over non commutative rings [8].

6.7. Quantum LDPC codes

For some time it was feared that quantum computers could not be built because of distortions of quantum states due to interaction with the environment. This issue could be addressed by the use of quantum codes. *Quantum LDPC codes* are very interesting candidates here, because their very fast decoding algorithm allows high error correction rates. But the design of good quantum LDPC codes is far more complicated than for their classical counterparts, and cannot be done by random generation. The best-known constructions come from algebraic topology and simplicial homology, but their limits were unknown. Nicolas Delfosse used Riemannian geometry theorems of Gromov to prove that an $[[n, k, d]]$-quantum code constructed from the homology of a simplicial surface satisfies $kd^2 \leq C(\log k)^2 n$ for some constant C [21].

Color codes are quantum LDPC codes constructed from 3–regular surface tilings whose set of faces is 3–colorable. Delfosse used morphisms of chain complexes to prove that the decoding of a color code can be reduced to the decoding of three associated surface codes; hence, every decoding algorithm for surface codes yields a decoding algorithm for color codes. From this result, Delfosse obtained theoretical lower bounds on the error threshold of a family of color codes [20].

6.8. New families of fast elliptic curves

Benjamin Smith has pioneered the use of mod-p reductions of Q-curves to produce elliptic curves with efficient scalar multiplication algorithms—which translates into faster encryption, decryption, signing, and signature verification operations on these curves. A theoretical article was presented at ASIACRYPT 2013 [9], and the Journal of Cryptology has invited the submission of a longer version. The theory was put into practice in collaboration with Craig Costello (Microsoft Research) and Huseyin Hisil (Yasar University). Their resulting publicly available implementation, which represents the state of the art in constant-time (side-channel conscious) elliptic curve scalar multiplication on 64-bit Intel platforms at the 128-bit security level, can carry out a constant-time scalar multiplication in 145k cycles on Ivy Bridge architectures. This work will appear in EUROCRYPT 2014 [17].

6.9. Tensor rank of multiplication over finite fields

Determining the tensor rank of multiplication over finite fields is a problem of great interest in algebraic complexity theory, but it also has practical importance: it allows us to obtain multiplication algorithms with a low bilinear complexity, which are of crucial significance in cryptography. In collaboration with S. Ballet and J. Chaumine [12], Julia Pieltant obtained new asymptotic bounds for the symmetric tensor rank of multiplication in finite extensions of finite fields $\mathbb{F}_q$. In the more general (not-necessarily-symmetric) case, Pieltant and H. Randriam obtained new uniform upper bounds for multiplication in extensions of $\mathbb{F}_q$. They also gave purely asymptotic bounds substantially improving those coming from uniform bounds, by using a family of Shimura curves defined over $\mathbb{F}_q$. This work will appear in Mathematics of Computation [22].

7. Bilateral Contracts and Grants with Industry

7.1. Bilateral Grants with Industry

- Within the framework of the joint lab Inria-ALU, Grace and Alcatel-Lucent collaborate on the topic of Private Information Retrieval: that is, retrieving 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, and is classically obtained through encryption, which prevents access to data in clear.) We are exploring applications of Locally Decodable Codes to Private Information Retrieval in the multi-cloud (multi-host) setting, to ensure both secure, reliable storage, and privacy of database queries. We will hire a PhD candidate in February 2014.

8. Partnerships and Cooperations

8.1. Regional Initiatives

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

  Daniel Augot engaged in monthly brainstorming meetings with researchers from Inria Paris–Rocquencourt (project-team SMIS), Université Jean Monnet's ADIS and CERDI labs (Alain Rallet, Alexandra Bensamoun), and Télécom ParisTech (Claire Levallois-Barth). Topics

under discussion include terms of service of various cloud storage providers, SMIS's *TrustedCell* secure token initiative for helding private and secure personnal data, privacy leaks, and measurements on smartphones.

A seminar will be held in Summer 2014. Within IDEX Paris-Saclay, the PAIP (Pour une Approche Interdisciplinaire de la Privacy) project was proposed and accepted in September 2013, with a small budget (30 keuros) for all the partners of the privacy group.

8.2. National Initiatives

8.2.1. ANR

- CATREL (accepted June 2012, Kickoff December 14, 2012, Starting January 1st, 2013): "Cribles: Améliorations Théoriques et Résolution Effective du Logarithme" (Sieve Algorithms: Theoretical Advances and Effective Resolution of the Discrete Logarithm Problem). This project aims to make effective "attacks" on reduced-size instances of the discrete logarithm problem (DLP). It is a key ingredient for the assessment of the security of cryptosystems relying on the hardness of the DLP in finite fields, and for deciding on relevant key sizes.

8.2.2. DGA

- DIFMAT: this two-year project aims to find matrices with good diffusion over small finite fields. These matrices are used in block ciphers and hash functions; coding theory helps to build and analyse them. Guillaume Quintin was hired as a postdoctoral researcher using this funding.
- Daniel Augot is co-advising Gwezheneg Robert with Pierre Loidreau (DGA, Rennes University).

8.2.3. PEPS ICQ (Projet Exploratoire de Premier Soutien - Information et Communication Quantique)

- ToCQ is a one-year project exploring the connections between algebraic topology, combinatorics, and Low Density Parity Check Quantum Codes. Alain Couvreur and Nicolas Delfosse are members of this project. The other partners are Inria Paris–Rocquencourt, Université Bordeaux I and Aix–Marseille Université.

8.3. European Initiatives

8.3.1. Collaborations in European Programs, except FP7

Program: COST

Project acronym: COST 4175/11

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

Duration: 04/2012 - 04/2016

Coordinator: Marcus Greferath

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

Abstract: Random network coding emerged through an award-winning paper by R. Koetter and F. Kschischang in 2008 and has since then opened a major research area in communication technology with widespread applications for communication networks like the internet, wireless communication systems, and cloud computing. It allows transmitting information through a network by disregarding any of its topological features. Worldwide, there exists a larger number of workgroups focusing on this topic, which includes several groups located in Europe. This COST Action will set up a European research network and establish network coding as a European core area in communication technology. Its aim is to bring together experts from pure and applied mathematics, computer science, and electrical engineering, who are working in the areas of discrete mathematics, coding theory, information theory, and related fields.

8.4. International Initiatives

8.4.1. Inria International Partners

8.4.1.1. Informal International Partners

- Martin Bossert, Institute of Communications Engineering, Ulm Universität.
- Steven Galbraith, Department of Mathematics, University of Auckland.

8.5. International Research Visitors

8.5.1. Visits of International Scientists

8.5.1.1. Internships

- Charlotte Scribot is spending the period September 2013 - February 2014 as an intern with GRACE as part of her professional masters program (Paris 7). She is working with Benjamin Smith and François Morain on parameter selection for efficient elliptic curve cryptosystems.

9. Dissemination

9.1. Scientific Committees

- Daniel Augot is member of the scientific committee of the French *CCA seminar*, held thrice a year in Institut Henry Poincaré.
- Daniel Augot was member of the programm committee of Fq11, the 11th International Conference on Finite Fields and their Applications, Magdeburg, July 22-26, 2013.

9.2. Administrative committees

- Alain Couvreur and Benjamin Smith are elected members of the *Commité de centre* of Inria Saclay.
- Alain Couvreur is *Jeune chercheur référent* for the *Commission de suivi doctoral* of Inria Saclay.
- Daniel Augot is member of the *Conseil de Laboratoire* of the LIX as a team leader.
- François Morain, Julia Pieltant and Benjamin Smith are elected members of the *Conseil de Laboratoire* of the LIX.
- Daniel Augot is head of the *Commission de suivi doctoral* of Inria Saclay.
- Daniel Augot is member of the *Bureau du comité des projets* de l'Inria Saclay–Île-de-France.
- Daniel Augot is member of the *commission scientifique* de l'Inria Saclay–Île-de-France.
- Daniel Augot is member of the *commission formation du labex Digicosme*
- Daniel Augot is member of the *comité de programme* of the Digiteo RTRA.
- Daniel Augot was member of the *comité de sélection pour un maître de conférence* at University of Versailles–Saint-Quentin.
- Benjamin Smith became the (scientific) international correspondent for Inria Saclay.
- Benjamin Smith became a member of Inria's Groupe de Travail "Relations Internationales" du Comité d'Orientation Scientifique et Technologique (COST-GTRI).
- Benjamin Smith is responsible for office assignments at LIX.
- Benjamin Smith was the chair of the LIX/Qualcomm/Carnot fellowship committee.
- François Morain is vice-head of the Département d'informatique of Ecole Polytechnique.
- François Morain represents École polytechnique in the committee in charge of *Mention HPC* in the *Master de l'université Paris Saclay*.

9.3. Teaching - Supervision - Juries

9.3.1. Teaching

Master: Daniel Augot, "Codes correcteurs d'erreurs et applications à la cryptographie" 13.5h (equiv TD), M2, Master Parisien de Recherche en Informatique (MPRI), France

Master: Benjamin Smith, Algorithmes arithmétiques pour la cryptologie, 13.5h (equiv TD), M2, Master Parisien de Recherche en Informatique (MPRI), France

Master: François Morain, Algorithmes arithmétiques pour la cryptologie, 9h (equiv TD), M2, Master Parisien de Recherche en Informatique (MPRI), France

Master: Benjamin Smith, Cryptologie, 18h (equiv TD), M1, École polytechnique, France

Licence: Benjamin Smith, Introduction à l'informatique, 40h (equiv TD), L3, École polytechnique, France

Master: Françoise Levy-dit-Vehel, Introduction à la crytopgraphie, 12h (equiv TD), Mastère spécialisé architecture et sécurité des systèmes d'information, ENSTA ParisTech.

Licence : F. Morain, 10 lectures of 1.5h, 1st year course "Introduction à l'informatique" (INF311) at École polytechnique (L2). Responsability of this module (350 students).

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

9.3.2. Supervision

- PhD in progress : Cécile Gonçalves, Algorithmes avancés de calcul de cardinalité pour des courbes intéressantes en cryptologie, 1/10/2011, Benjamin Smith and François Morain.
- PhD in progress: Gwezheneg Robert, Métrique rang et codes de Gabidulin en cacractéristique zéro, 1/10/12, Daniel Augot and P. Loidreau.
- PhD: Alexander Zeh, Algebraic Soft- and Hard-Decision Decoding of Generalized Reed–Solomon and Cyclic Codes, Ulm Universität, 2/09/2013, Daniel Augot and Martin Bossert.

9.3.3. Juries

- Alain Couvreur is member of the Jury of the *Agrégation de Mathématiques*, Options C (computer algebra) and D (computer science).
- Benjamin Smith was an examiner for the PhD of Louise Huot (UPMC, 13/12/2013)
- Benjamin Smith was an examiner for the PhD of Aurore Guillevic (ENS, 20/12/2013)
- Benjamin Smith was a member of the jury for the CNRS Concours IE63 (BAP E), 24-25/10/2013.
- Daniel Augot was examiner for the PhD of Mamdouh Abbara (X, 09/04/2013)
- Daniel Augot was reviewer of the PhD of Mila Tukumuli, (Aix-Marseille University, 13/09/2013)
- Daniel Augot was examiner for the PhD of Lin Sok (Télécom Paristech, 20/09/2013)
- Daniel Augot was examiner and reviewer of Johan Nielsen's PhD (DTU Lyngby, 30/09/2013)
- Daniel Augot was examiner and reviewer of Muhammad Foizul Islam Chowdhury's PhD (Western University Canada, London, Canada, 8/11/2013)
- Daniel Augot was reviewer of Stéphanie Dib's PhD (Aix-Marseille University, 11/12/2013)

9.4. Invitations to seminars and conferences

- Daniel Augot : 14/02/2014, GREYC, Caen. "Les connexions entre le logarithme discret sur les corps finis non premiers et le décodage des codes de Reed-Solomon".
- Daniel Augot was invited to participate to a session Cryptography and Number Theory at 2013 SIAM Conference on Applied Algebraic Geometry, 01-04/08/2013.
- Daniel Augot gave a talk at Dagstuhl Seminar 13351 on coding theory, 25-30/08/2013

- Alain Couvreur gave a talk at the Seminar on Coding Theory and Cryptography common to the universities of Neuchâtel and Zurich. 22/04/2013.
- Benjamin Smith was an invited speaker at the international Workshop on Number Theory at the American University of Beirut, Lebanon, 25-27/04/2013.
- Benjamin Smith gave a talk at AGCT-14, an invitational conference on Arithmetic, Geometry, Cryptography, and Coding Theory, 03-07/06/2013.
- Benjamin Smith gave two lectures on number-theoretic cryptography at the CryptoBG international summer school in Oriahovitsa, Bulgaria, 20-27/07/2013.
- Benjamin Smith gave an invited talk at the PIMS Workshop on Curves and Applications, Calgary, Canada, 19-21/08/2013.
- Benjamin Smith gave visited Microsoft Research, Redmond from 22/08/2013 to 04/09/2013, and gave a talk in their seminar.
- Benjamin Smith gave two lectures at the ECC 2013 summer school on Elliptic Curves for Cryptography in Leuven, Belgium, 11-13/09/2013.
- Benjamin Smith was an invited speaker at ECC 2013 (the 17th annual Elliptic Curve Cryptography workshop) in Leuven, Belgium, 16-18/09/2013.
- F. Morain gave three lectures in the summer school *Number theory for cryptography* in Warwick University, june 2013.

9.5. Popularization

- Alain Couvreur gave a talk at *UniThé ou Café*, a monthly science popularization event dedicated to all the employees of Inria Saclay.
- Daniel Augot presented bit operations, the Hamming code, the one-time pad and a bit of steganography to high school students in Courcouronnes, 10/04/2013.

10. Bibliography

Major publications by the team in recent years

[1] A. COUVREUR. , *Codes and the Cartier Operator*, 2012, To appear in Proc. Amer. Math. Soc., http://hal.inria.fr/hal-00710451

[2] J.-C. FAUGÈRE, F. LEVY-DIT-VEHEL, L. PERRET. *Cryptanalysis of MinRank*, in "Advances in Cryptology – CRYPTO 2008", D. WAGNER (editor), Lecture Notes in Computer Science, Springer Berlin Heidelberg, 2008, vol. 5157, pp. 280-296, http://dx.doi.org/10.1007/978-3-540-85174-5_16

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

[4] 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

[5] A. ZEH, C. GENTNER, D. AUGOT. *An Interpolation Procedure for List Decoding Reed-Solomon Codes Based on Generalized Key Equations*, in "IEEE Trans. Inform. Theory", September 2011, vol. 57, pp. 5946-5959, http://hal.inria.fr/hal-00645738

Publications of the year

Doctoral Dissertations and Habilitation Theses

[6] A. ZEH. , *Algebraic Soft- and Hard-Decision Decoding of Generalized Reed–Solomon and Cyclic Codes*, Ecole Polytechnique X, September 2013, http://hal.inria.fr/pastel-00866134

Articles in International Peer-Reviewed Journals

[7] J. BERTHOMIEU, G. LECERF, G. QUINTIN. *Polynomial root finding over local rings and application to error correcting codes*, in "Applicable Algebra in Engineering, Communication and Computing", December 2013, vol. 24, n° 6, pp. 413-443 [*DOI :* 10.1007/s00200-013-0200-5], http://hal.inria.fr/hal-00642075

[8] G. QUINTIN, M. BARBIER, C. CHABOT. *On Generalized Reed-Solomon Codes Over Commutative and Noncommutative Rings*, in "IEEE Transactions on Information Theory", September 2013, vol. 59, n° 9, pp. 5882-5897 [*DOI :* 10.1109/TIT.2013.2264797], http://hal.inria.fr/hal-00670004

[9] B. SMITH. *Families of fast elliptic curves from Q-curves*, in "Lecture notes in computer science", December 2013, vol. 8269, pp. 61-78 [*DOI :* 10.1007/978-3-642-42033-7_4], http://hal.inria.fr/hal-00825287

International Conferences with Proceedings

[10] D. AUGOT, M. FINIASZ. *Exhaustive Search for Small Dimension Recursive MDS Diffusion Layers for Block Ciphers and Hash Functions*, in "International Symposium on Information Theory (ISIT)", Istambul, Turkey, A. LAPIDOTH, I. SASON, J. SAYIR, E. TELATAR (editors), IEEE, 2013, http://hal.inria.fr/hal-00823082

[11] D. AUGOT, P. LOIDREAU, G. ROBERT. *Rank metric and Gabidulin codes in characteristic zero*, in "ISIT 2013 IEEE International Symposium on Information Theory", Istanbul, Turkey, A. LAPIDOTH, I. SASON, J. SAYIR, E. TELATAR (editors), July 2013, http://hal.inria.fr/hal-00823535

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

[13] A. COUVREUR, P. GABORIT, V. GAUTIER, A. OTMANI, J.-P. TILLICH. *Distinguisher-Based Attacks on Public-Key Cryptosystems Using Reed-Solomon Codes*, in "WCC 2013 - International Workshop on Coding and Cryptography", Bergen, Norway, Selmer Center at the University of Bergen, Norway and Inria, Rocquencourt, France, 2013, pp. 181-193, http://hal.inria.fr/hal-00830594

[14] J. S. R. NIELSEN, A. ZEH. *Multi-Trial Guruswami–Sudan Decoding for Generalised Reed–Solomon Codes*, in "International Workshop on Coding and Cryptography (WCC)", Bergen, Norway, April 2013, http://hal.inria.fr/hal-00781310

[15] A. ZEH, A. WACHTER-ZEH, M. GADOULEAU, S. BEZZATEEV. *Generalizing Bounds on the Minimum Distance of Cyclic Codes Using Cyclic Product Codes*, in "IEEE International Symposium on Information Theory (ISIT)", Istanbul, Turkey, A. LAPIDOTH, I. SASON, J. SAYIR, E. TELATAR (editors), IEEE, June 2013, pp. 1-6, accepted for ISIT2013, http://hal.inria.fr/hal-00828083

Books or Proceedings Editing

[16] D. AUGOT, A. CANTEAUT, G. KYUREGHYAN, F. SOLOV'EVA, Ø. YTREHUS (editors). , *Designs, Codes and Cryptography (Special Issue in Coding and Cryptography)*, Springer, January 2013, vol. 66, 399 p. , http://hal.inria.fr/hal-00931522

Other Publications

[17] C. COSTELLO, H. HISIL, B. SMITH. , *Faster Compact Diffie-Hellman: Endomorphisms on the x-line*, 2013, To appear in EUROCRYPT 2014, http://hal.inria.fr/hal-00932952

[18] A. COUVREUR, I. MÁRQUEZ-CORBELLA, R. PELLIKAAN. , *A Polynomial Time Attack against Algebraic Geometry Code Based Public Key Cryptosystems*, 2014, http://hal.inria.fr/hal-00937476

[19] A. COUVREUR, A. OTMANI, J.-P. TILLICH. , *New Identities Relating Wild Goppa Codes*, 2013, http://hal.inria.fr/hal-00880994

[20] N. DELFOSSE. , *Decoding color codes by projection onto surface codes*, 2013, http://hal.inria.fr/hal-00855003

[21] N. DELFOSSE. , *Tradeoffs for reliable quantum information storage in surface codes and color codes*, 2013, http://hal.inria.fr/hal-00798030

[22] J. PIELTANT, H. RANDRIAM. , *New uniform and asymptotic upper bounds on the tensor rank of multiplication in extensions of finite fields*, 2013, http://hal.inria.fr/hal-00828153

[23] B. SMITH. , *Easy scalar decompositions for efficient scalar multiplication on elliptic curves and genus 2 Jacobians*, October 2013, http://hal.inria.fr/hal-00874925

References in notes

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

[25] H. NIEDERREITER. *Knapsack-type cryptosystems and algebraic coding theory*, in "Problems of Control and Information Theory", 1986, vol. 15, n^{o} 2, pp. 159–166

[26] 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