Activity Report 2012

Team GRACE

Geometry, arithmetic, algorithms, codes and encryption

RESEARCH CENTER
Saclay - Île-de-France

THEME
Algorithms, Certification, and Cryptography

Table of contents

Team GRACE

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

Algorithmic number theory, and the computational issues related to algebraic curves over various fields and arithmetic rings, is a central theme in our research. This very rich area of mathematics and computer science has already shown its relevance in public key cryptography, with industrial successes including the RSA cryptosystem and elliptic curve cryptography. It is less well-known that very good codes for error correction can be built using the same areas of mathematics; this is also at the heart of the Grace proposal. We believe that geometric interpretation, unification, and transformation gives better insight into the nature and performance of this wide range of problems and algorithms in coding theory and cryptology.

Both of these application domains, cryptology and coding, deal with communication systems for securing high-level applications. Cryptography is seen as a part of computer science, while coding theory traditionally has an electical engineering flavour; but recent developments in computer science have shed new light on coding theory, with new applications more central to computer science. Grace aims to:

- *provide better cryptosystems,*
- *provide better security assessments for key sizes in cryptography and cryptanalysis, and*
- *build the best codes with algebraic curves.*

Creation of the Team: January 01, 2012 .

1. Members

Research Scientists

Daniel Augot [DR2 / Senior Researcher, Team Leader, HdR]
Alain Couvreur [CR1 / Junior Researcher]
Benjamin Smith [CR1 / Junior Researcher, Responsable Permanent]

Faculty Member

François Morain [Professor at École polytechnique, Former Team Leader, HdR]

PhD Students

Cécile Gonçalves [École polytechnique / DGA since 2011-10-1]
Guillaume Quintin [DGA since 2009-10-01, defended 2012-11-22]
Alexander Zeh [Universität Ulm, since 2010-05-1]

Post-Doctoral Fellows

Nicolas Delfosse [École polytechnique since 2012-10-1]
Julia Pieltant [since 2012-10-1]

Administrative Assistant

Évelyne Rayssac [École polytechnique]

2. Overall Objectives

2.1. Highlights of the Year

D. Augot co-edited a special issue of Designs, Codes and Cryptography, devoted to WCC 2011. Online versions of the articles are avalaible, while the issue will appear as volume number 66, issue 1-3, in January 2013.

2.2. Scientific foundations

Grace approaches its twin themes of coding theory and cryptology from the point of view of algebraic geometry and number theory. The foundations of Grace therefore lie in algorithmic number theory, the algorithmic theory of algebraic systems, the arithmetic geometry of curves, and the theory of algebraic codes.

Algorithmic Number Theory is concerned with effective number theory at large, with three main threads: fundamental algorithms (primality, factorization), number fields, and curves (over all kinds of fields). Algorithmic Number Theory is concerned with replacing special cases with algorithms. For example, Mersenne primes (which have the form $2^p - 1$) make nice and cute examples, but they lack generality: the primality of a Mersenne prie can be proven in deterministic polynomial time with a specific algorithm that cannot be used on all prime numbers. Now, there are several algorithms for this task.

Arithmetic Geometry is the meeting point of algebraic geometry and number theory: the study of geometric objects defined over arithmetic number systems. In our case, the most important objects are curves and their Jacobians over finite fields; these are fundamental to our applications in both coding theory and cryptology. Jacobians of curves are excellent candidates for cryptographic groups when constructing efficient instances of public-key cryptosystems, of which Diffie–Hellman key exchange is an instructive example.

Coding Theory studies originated with the idea of using redundancy in messages to protect them against noise and errors. While the last decade of the 20th century has seen the success of so-called iterative decoding methods, we see now many new ideas in the realm of algebraic coding, with the foremost example being list decoding.

3. Application Domains

3.1. Cryptology

We want to establish the security of practical proposals relying on computational problems, be they standardized (like RSA or Elliptic Curve Cryptography), or more exotic (like Hyperelliptic Curve Cryptography). We do not work with abstract cryptographic primitives. On the design side, building efficient near-optimal codes impacts directly on the security of basic operations in symmetric primitives. We also investigate other applications, such as secret sharing schemes, universal hash functions, and message authentication, revisiting them in the context of Algebraic Geometry codes.

3.2. Codes in Computer Science

We do not want to do basic forward error correction, dealing with bit error rates and signal-to-noise ratios. Rather, we aim to deal with higher models of communication and computation, including peer-to-peer systems and distributed storage. We also consider adversarial noise, or distributed computations with byzantine faults. List decoding deals precisely with these kinds of “difficult”, non-random errors. In a related spirit, one can deal with “computationally bounded channels”, where the errors are generated by an adversarial machine or algorithm that is computationally bounded.

4. Software

4.1. ECPP

F. Morain has been continually improving his primality proving algorithm called ECPP, originally developed in the early 1990s. Binaries for version 6.4.5 have been available since 2001 on his web page. Proving the primality of a 512 bit number requires less than a second on an average PC. His personal record is around $25,000$ decimal digits, using the fast version that he started developing in 2003. All of the code is written in C, and based on publicly available packages (GMP, mpfr, mpc, mpfrcx).

4.2. SEA

Together with E. Schost and L. DeFeo, F. Morain has developed a new implementation of the SEA algorithm that computes the cardinality of elliptic curves over finite fields (large prime case, case $p = 2$). It uses NTL and includes the most recent algorithms for solving all subtasks. The large prime case is relevant to cryptographical needs. The $p = 2$ case, though not directly useful, is a good testbed for the FAAST program of Luca De Feo. This program forms a `gforge` project.

4.3. TIFA

The TIFA library (short for Tools for Integer FActorization), initially developed in 2006, has been continuously improved during the last few years. TIFA is made up of a base library written in C99 using the GMP library, together with stand-alone factorization programs and a basic benchmarking framework to assess the performance of each algorithm.

It is now available online at http://www.lix.polytechnique.fr/Labo/Jerome.Milan/tifa/tifa.xhtml; it is distributed under the Lesser General Public License (version 2.1 or later).

4.4. Quintix

The Quintix library is a Mathemagix package, available at http://www.mathemagix.org/www/main/index.en.html. Quintix is a very efficient library for Galois rings, extensions of Galois rings and root-finding in Galois rings, developed in C++, within the Mathemagix computer algebra system. It implements basic arithmetic for Galois rings and their unramified extensions, basic functions for the manipulation of Reed–Solomon codes, and the complete Sudan list-decoding algorithm. It also implements the root-finding algorithms presented in [23]. The source code is distributed under the General Public License (version 2 or higher).

4.5. finitefieldz

G. Quintin wrote the finitefieldz package which provides arithmetic for finite fields (of any characteristic) and towers of finite fields. He wrote this package with the help of Grégoire Lecerf during the first year of his PhD thesis. The package uses univariate polynomials and multiprecision integers, and also provides univariate polynomial root finding and factorization over finite fields.

4.6. 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 of decoding algorithms (not necessarily list decoding algorithms) and their benchmarking.

For now (2012/12/13) you can use the library and have a working list decoding algorithm, but there is no unique decoding algorithm (though you can tell decoding to list decode up to half the minimum distance). The library is being further developedm and more algorithms will be added.

The library was presented at the 2012 International Symposium on Symbolic and Algebraic Computation.

5. New Results

5.1. Modular curves

F. Morain has been studying the theory and practice of modular curves associated with Weber's invariants. His paper ... is accepted for publication in *Acta Arithmetica*.

5.2. Computing discrete logarithms using codes

D. Augot and F. Morain have been working on the practical application of Reed–Solomon decoding to speed up discrete logarithm computations, following the work of Cheng and Wan. This work is available as a preprint [22], and a Magma implementation was written in support of the many experiments needed.

5.3. Interleaved codes and codes over rings

G. Quintin designed a decoding algorithm based on a lifting decoding scheme. He obtained a unique decoding algorithm with quasi-linear complexity in all parameters for Reed–Solomon codes over Galois rings. Using erasures, he improved the decoding radius with the same complexity. He then applied these techniques to interleaved linear codes over a finite field, and obtained a decoding algorithm that can recover more errors than half the minimum distance. This work has been presented at IEEE ISIT 2012 (Boston, USA).

5.4. Number fields codes

J.-F. Biasse and G. Quintin described an algorithm for list decoding algebraic number field codes in polynomial time in [24]. This is the first explicit procedure for decoding number field codes, whose construction were previously described by Lenstra [33] and Guruswami [32]. They rely on a new algorithm for computing the Hermite normal form of the basis of an $\mathcal{O}_K$-module due to Biasse and Fieker [31], where $\mathcal{O}_K$ is the ring of integers of a number field K. This work has been presented at IEEE ISIT 2012 (Boston, USA).

5.5. Point counting using p-adic methods

C. Gonçalvès designed a new algorithm to compute Zeta functions of cyclic covers of the projective line. This algorithm is a generalisation of the one for superelliptic curves provided by P. Gaudry and N. Gürel and has the same complexity. Moreover, optimal bounds for the precision have been proved. An alternative basis for computations has been studied and the resulting algorithm is faster, even if the asymptotic complexity is the same.

5.6. Codes and Cartier Operator

A. Couvreur proposed a new construction of codes from algebraic curves over a finite field in [25]. This class of codes is a natural geometric generalisation of classical Goppa codes. In particular, the nice equalities “$\Gamma(L, g^{q-1}) = \Gamma(L, g^q)$” satisfied by classical Goppa codes (for instance, see [30]) extend naturally to this larger class of codes. This article is to appear in *Proceeding of the American Mathematical Society*.

5.7. Quantum Codes

A. Couvreur, N. Delfosse and G. Zémor studied a construction of quantum LDPC codes proposed by McKay, Mitchison and Shokrollahi in a draft. This construction involves Cayley graphs of $GF(2)^n$. A general lower bound for the minimum distance of such codes has been found. In addition, a family of such codes whose parameters are proved to be $[[n, O(\sqrt{n}, O(\sqrt{N}))]]$ is exhibited. Notice that up to now, no construction of quantum LDPC codes is known to have a minimum distance better that $O(\sqrt{n})$. The obtained parameters beat many well–known constructions. This work has been presented at IEEE ISIT 2011 (St Petersburg, Russia), and a long version paper [26] has been submitted to an international journal.

5.8. Code-based McEliece like cryptology

A. Couvreur is working with P. Gaborit, V. Gauthier, A. Otmani, and J.-P. Tillich on distinguisher-based attacks on cryptosystems based on Generalised Reed–Solomon codes. Using the particular structure of the square of an evaluation code, they have been able to break some variants of McEliece's cryptosystem using Generalised Reed–Solomon codes, such as Wieschebrink's variant [34]. An article is in preparation.

5.9. Cyclic Codes

A. Zeh is working with A. Wachter-Zeh (University of Ulm and Institut de Recherche de Mathématique de Rennes) and Sergey Bezzateev (St. Petersburg State University of Aerospace Instrumentation) on a new bound for the minimum distance of q-ary cyclic codes [19], [18]. The connection to the BCH bound and the Hartmann–Tzeng (HT) bound was formulated explicitly. Furthermore, the bound was refined for several families of cyclic codes. We defined syndromes and formulated a Key Equation that allows an efficient decoding up to our bound with the Extended Euclidean Algorithm. It turned out that low-rate cyclic codes with small minimum distances are useful for our approach.

5.10. Iterative List Decoding

A. Zeh is working with J. S. R. Nielsen (Department of Mathematics, DTU) on an iterative list decoding algorithm for generalized Reed–Solomon codes. The method is parametrizable and allows variants of the usual list decoding approach. An article is in preparation.

6. Bilateral Contracts and Grants with Industry

6.1. Alcatel Lucent

In September, D. Augot and F. Levy-dit-Vehel submitted a proposal to fund a joint PhD thesis with Abdullatif Shikfa (Alcatel Lucent), on local codes for distributed storage and related cloud-like issues.

6.2. Cryptoexperts

A research agreement between Cryptoexperts and Grace has been made, to establish foundations for the DGA DIFMAT contract (see below). D. Augot is collaborating with M. Finiasz from Cryptoexperts.

7. Partnerships and Cooperations

7.1. National Initiatives

7.1.1. 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). The aim of this project is to make effective “attacks” on reduced-size discrete logarithm problem (DLP) instances. 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.

7.1.2. 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. G. Quintin has been hired as postdoctoral researcher using this funding.
- D. Augot is co-advising Gwezheneg Robert, with Pierre Loidreau (DGA, Rennes University).

7.2. European Initiatives

7.2.1. Collaborations in European Programs, except FP7

Program: PHC Hubert Curien PROCOPE

Project acronym: PowerList

Project title: PowerList

Duration: 01/01/2011 to 31/12/2012.

Coordinator: Daniel Augot

Other partners: Ulm Universität, TAIT group, Germany.

Abstract: Building a less powerful but faster probabilistic list decoding algorithm. This funded Alexander Zeh's visits.

7.3. International Initiatives

7.3.1. Inria International Partners

- DTU Lyngby.
- Ulm Universität.

7.4. International Research Visitors

7.4.1. Visits of International Scientists

7.4.1.1. Internships

- Johan Sebastian Nielsen, DTU Lyngby PhD student, visited us from September 1st to December 20th.

7.4.2. Visits to International Teams

- D. Augot, A. Couvreur, and B. Smith visited the University of Illinois at Urbana–Champaign. This visit included two talks given in the Number Theory seminar, and discussions with I. Duursma to prepare the second year of the DGA DIFMAT contract.
- A. Zeh visited the Institute of Information Transmission Problems (IITP), Moscow in December 2012. He gave a talk on low-rate small-minimum distance binary cyclic codes.

8. Dissemination

8.1. Scientific Animation

- D. Augot is editor for the journal "RAIRO - Theoretical Informatics and Applications"
- D. Augot was editor of a special issue of Designs, Codes and Cryptography.
- D. Augot is co-organizer, with P. Loidreau, of the French CCA (Coding, Cryptography and Algorithms) seminar, http://cca.saclay.inria.fr, held in Paris three times per year.
- D. Augot was in the program committee of YACC 2012, Porquerolles.
- D. Augot was a reviewer for IEEE Transactions on Information Theory, Designs, Codes and Cryptography, SIAM Journal on Discrete Mathematics, Journal of Symbolic Computation, AAECC.
- B. Smith was a reviewer for ANTS, Eurocrypt, Asiacrypt, PQCrypto, RAIRO ITA, ETRI Journal.
- B. Smith contributes to the American Mathematical Society's Mathematical Reviews (MathSciNet).
- A. Zeh was reviewer for Advances in Mathematics of Communications (AMC), IEEE Communications Letters and IEEE Transactions on Information Theory.

8.2. Teaching - Supervision - Juries

8.2.1. Teaching

Master MPRI : Daniel Augot, Error correcting codes and applications to cryptography, 24, M2, U. Paris Diderot, ENS Ulm, ENS Cachan, Polytechnique, U. Paris Sud, U. P. et M. Curie, France.

Master MPRI : F. Morain, arithmetic algorithms for cryptology, 9h, M2, U. Paris Diderot, ENS Ulm, ENS Cachan, Polytechnique, U. Paris Sud, U. P. et M. Curie, France.

Master MPRI: B. Smith, arithmetic algorithms for cryptology, 12h, M2, U. Paris Diderot, ENS Ulm, ENS Cachan, Polytechnique, U. ParisSud, U. P. et M. Curie, France

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

Master: B. Smith, 10 practical classes of 2h, 3rd year course “cryptology” at École polytechnique (M1).

Licence : F. Morain, 10 lectures of 1.5h, 1st year course “Introduction à l’informatique” (INF311) at École polytechnique (L2).

Licence: B. Smith, 20 TDs of 2h, 1st year course “Introduction à l’informatique” (INF311) at École polytechnique (L2).

Licence: A. Couvreur, 4 TP’s of 2h on Matlab Programming for 1st year students at École Polytechnique (L2).

8.2.2. Supervision

PhD: Guillaume QUINTIN, “Sur l’algorithme de d’ecodage en liste de Guruswami–Sudan sur les anneaux finis”, École polytechnique, defended 2012/11/22.

PhD in progress : Cécile GONÇALVES, Advanced cardinality algorithms for cryptographically interesting curves, 01/10/2011, F. Morain and B. Smith

8.2.3. Juries

- D. Augot was an examiner in the jury of Julia Pieltant, “Tours de corps de fonctions algébriques et rang de tenseur de la multiplication dans les corps finis”, Université d’Aix-Marseille, December 12 2012.
- D. Augot was an examiner in the jury of Guillaume Quintin, “Sur l’algorithme de décodage en liste de Guruswami-Sudan sur les anneaux finis”, école Polytechnique, November 22 2012.
- D. Augot was an examiner in the jury of Anja Becker, “La technique de représentation – Application à des problèmes difficiles en cryptographie”, UVSQ, October 26 2012.
- D. Augot was an examiner in the jury of Amar Siad, “Protocoles de génération des clés pour le chiffrement basé sur de l’identité”, Université Paris 8, December 21 2012.
- F. Morain was president of the jury of Stéphane Jacob, Mars 08 2012 (Protection cryptographique des bases de données: conception et cryptanalyse).
- B. Smith was an examiner in the jury of Jean-Pierre Flori, “Fonctions booléennes, courbes algébriques et multiplication complexe”, Télécom ParisTech, February 3 2012.

8.3. Popularization

- D. Augot made a presentation in the high school at Courcouronnes “Quand $1 \oplus 1 = 0$”.
- D. Augot was interviewed by French novelist François Bon.
- F. Morain gave a talk on “Turing et la cryptanalyse”, during the special days for the centenary of the birth of Turing, Nancy 2012/09/20.

9. Bibliography

Major publications by the team in recent years

[1] A. Basiri, A. Enge, J.-C. Faugère, N. Gürel. *The Arithmetic of Jacobian Groups of Superelliptic Cubics*, in "Math. Comp.", 2005, vol. 74, p. 389–410, http://hal.inria.fr/inria-00071967.

[2] J. BELDING, R. BRÖKER, A. ENGE, K. LAUTER. *Computing Hilbert class polynomials*, in "Algorithmic number theory", Berlin, Lecture Notes in Comput. Sci., Springer, 2008, vol. 5011, p. 282–295.

[3] A. BOSTAN, F. MORAIN, B. SALVY, É. SCHOST. *Fast algorithms for computing isogenies between elliptic curves*, in "Math. Comp.", 2008, vol. 77, n^o 263, p. 1755–1778, http://dx.doi.org/10.1090/S0025-5718-08-02066-8.

[4] L. DE FEO, É. SCHOST. *Fast Arithmetics in Artin-Schreier towers*, in "ISSAC 2009", 2009, p. 121-134.

[5] A. ENGE. *The complexity of class polynomial computation via floating point approximations*, in "Mathematics of Computation", 2008, vol. 78, p. 1089-1107, http://hal.inria.fr/inria-00001040/PDF/class.pdf.

[6] A. ENGE, P. GAUDRY. *A general framework for subexponential discrete logarithm algorithms*, in "Acta Arith.", 2002, vol. CII, n^o 1, p. 83–103.

[7] A. ENGE, P. GAUDRY. *An $L(1/3+\varepsilon)$ algorithm for the discrete logarithm problem for low degree curves*, in "Advances in Cryptology — Eurocrypt 2007", Berlin, M. NAOR (editor), Lecture Notes in Comput. Sci., Springer-Verlag, 2007, vol. 4515, p. 379–393, http://hal.inria.fr/inria-00135324.

[8] A. ENGE, F. MORAIN. *Comparing Invariants for Class Fields of Imaginary Quadratic Fields*, in "Algorithmic Number Theory", C. FIEKER, D. KOHEL (editors), Lecture Notes in Comput. Sci., Springer-Verlag, 2002, vol. 2369, p. 252–266, 5th International Symposium, ANTS-V, Sydney, Australia, July 2002, Proceedings.

[9] A. ENGE, R. SCHERTZ. *Constructing elliptic curves over finite fields using double eta-quotients*, in "Journal de Théorie des Nombres de Bordeaux", 2004, vol. 16, p. 555–568, http://jtnb.cedram.org/jtnb-bin/fitem?id=JTNB_2004__16_3_555_0.

[10] P. MIHĂILESCU, F. MORAIN, É. SCHOST. *Computing the eigenvalue in the Schoof-Elkies-Atkin algorithm using Abelian lifts*, in "ISSAC '07: Proceedings of the 2007 international symposium on Symbolic and algebraic computation", New York, NY, USA, ACM Press, 2007, p. 285–292, http://hal.inria.fr/inria-00130142.

[11] F. MORAIN. *La primalité en temps polynomial [d'après Adleman, Huang; Agrawal, Kayal, Saxena]*, in "Astérisque", 2004, n^o 294, p. Exp. No. 917, 205–230, Séminaire Bourbaki. Vol. 2002/2003.

[12] F. MORAIN. *Computing the cardinality of CM elliptic curves using torsion points*, in "Journal de Théorie des Nombres de Bordeaux", 2007, vol. 19, n^o 3, p. 663–681, http://arxiv.org/ps/math.NT/0210173.

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

[14] 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, p. 505-529.

Publications of the year

Doctoral Dissertations and Habilitation Theses

[15] G. QUINTIN. *Sur l'algorithme de décodage en liste de Guruswami-Sudan sur les anneaux finis*, Ecole Polytechnique X, November 2012, http://hal.inria.fr/pastel-00759820.

Articles in International Peer-Reviewed Journals

[16] A. COUVREUR. *The dual minimum distance of arbitrary-dimensional algebraic-geometric codes*, in "Journal of Algebra", January 2012, vol. 350, n^{o} 1, p. 84-107, Une partie de ce travail de recherche a été effectuée lorsque l'auteur de l'article était membre de l'institut de mathématiques de Luminy [*DOI :* 10.1016/J.JALGEBRA.2011.09.030], http://hal.inria.fr/inria-00540022.

[17] L. DE FEO, É. SCHOST. *Fast Arithmetics in Artin-Schreier Towers over Finite Fields*, in "Journal of Symbolic Computation", July 2012, vol. 47, n^{o} 7, p. 771-792 [*DOI :* 10.1016/J.JSC.2011.12.008], http://hal.inria.fr/hal-00505799.

[18] A. ZEH, S. BEZZATEEV. *A New Bound on the Minimum Distance of Cyclic Codes Using Small-Minimum-Distance Cyclic Codes*, in "Designs, Codes and Cryptography", June 2012, http://hal.inria.fr/hal-00710290.

[19] A. ZEH, A. WACHTER, S. BEZZATEEV. *Decoding Cyclic Codes up to a New Bound on the Minimum Distance*, in "IEEE Transactions on Information Theory", May 2012, http://hal.inria.fr/hal-00678646.

International Conferences with Proceedings

[20] A. ZEH, S. BEZZATEEV. *Describing A Cyclic Code by Another Cyclic Code*, in "ISIT 2012 - Internation Symposium on Information Theory", Boston, États-Unis, IEEE (editor), April 2012, http://hal.inria.fr/hal-00689746.

Books or Proceedings Editing

[21] D. AUGOT, A. CANTEAUT, G. KYUREGHYAN, F. SOLOV'EVA, Ø. YTREHUS. , D. AUGOT, A. CANTEAUT, G. KYUREGHYAN, F. SOLOV'EVA, Ø. YTREHUS (editors)*Editorial*, Designs, Codes and Cryptography, Springer, July 2012, 2 [*DOI :* 10.1007/S10623-012-9731-1], http://hal.inria.fr/hal-00741923.

Other Publications

[22] D. AUGOT, F. MORAIN. *Discrete logarithm computations over finite fields using Reed-Solomon codes*, 2012, http://hal.inria.fr/hal-00672050.

[23] J. BERTHOMIEU, G. LECERF, G. QUINTIN. *Polynomial root finding over local rings and application to error correcting codes*, 2012, This work has been partly supported by the French ANR-09-JCJC-0098-01 MaGiX project, and by the Digiteo 2009-36HD grant of the Région Île-de-France., http://hal.inria.fr/hal-00642075/en/.

[24] J.-F. BIASSE, G. QUINTIN. *An algorithm for list decoding number field codes*, 2012, http://hal.inria.fr/hal-00712441.

[25] A. COUVREUR. *Codes and the Cartier Operator*, 2012, http://hal.inria.fr/hal-00710451.

[26] A. COUVREUR, N. DELFOSSE, G. ZEMOR. *A construction of quantum LDPC codes from Cayley graphs*, 2012, http://hal.archives-ouvertes.fr/hal-00632257.

[27] G. QUINTIN, M. BARBIER, C. CHABOT. *On Generalized Reed-Solomon Codes Over Commutative and Noncommutative Rings*, 2012, http://hal.inria.fr/hal-00670004.

[28] G. QUINTIN. *A Lifting Decoding Scheme and its Application to Interleaved Linear Codes*, 2012, http://hal.inria.fr/hal-00673938.

[29] G. QUINTIN. *The decoding Library for List Decoding*, 2012, http://hal.inria.fr/hal-00700397.

References in notes

[30] D. J. BERNSTEIN, T. LANGE, C. PETERS. *Wild McEliece*, in "Selected areas in cryptography", Heidelberg, Lecture Notes in Comput. Sci., Springer, Heidelberg, 2011, vol. 6544, p. 143–158, http://dx.doi.org/10.1007/978-3-642-19574-7_10.

[31] J.-F. BIASSE, C. FIEKER. *A polynomial time algorithm for computing the HNF of a module over the integers of a number field*, 2012, Manuscript to appear in ISSAC 2012, http://www.lix.polytechnique.fr/~biasse/papers/HNF_pol.pdf.

[32] V. GURUSWAMI. *Constructions of codes from number fields*, in "IEEE Transactions on Information Theory", 2003, vol. 49, n^o 3, p. 594–603.

[33] H. W. LENSTRA, JR.. *Codes from algebraic number fields*, in "Mathematics and computer science II, Fundamental contributions in the Netherlands since 1945", North-Holland, Amsterdam, M. HAZEWINKEL, J. LENSTRA, L. L. MEERTENS (editors), CWI Monograph, 1986, vol. 4, p. 94–104.

[34] C. WIESCHEBRINK. *Two NP-complete Problems in Coding Theory with an Application in Code Based Cryptography*, in "Information Theory, 2006 IEEE International Symposium on", july 2006, p. 1733–1737, http://dx.doi.org/10.1109/ISIT.2006.261651.