MACISA — Mathematics applied to cryptology and information security in Africa

2014/09/24 — LIRIMA Evaluation Seminar, Paris

Tony Ezome, **Damien Robert**

Équipe LFANT, Inria Bordeaux Sud-Ouest

Context

High need for secure communications

Security:

- Adversaries include other countries with high ressources available (NSA).
- The Prism program collects stored Internet communications based on demands made to Internet companies (Microsoft, Yahoo!, Google, Facebook, Paltalk, YouTube, AOL, Skype, Apple...)
- Bullrun to weaken cryptographic standards and implementations;
- Heartbleed software bug in openssl...

Context

Cryptology:

- Encryption;
- Authenticity;
- Integrity.

Public key cryptology is based on a one way (trapdoor) function ⇒ asymmetric encryption, signatures, zero-knowledge proofs...

Applications:

- Military;
- Privacy;
- Communications (internet, mobile phones...)
- E-commerce...

Macisa: Mathematics applied to cryptology and information security in Africa

Focus:

Public key cryptology and more specifically the role played by algebraic maps in this context.

Two themes:

1. Dimension zero: Rings, Primality, Factorisation and Discrte Logarithm;
2. Dimension one and higher: Elliptic and hyperelliptic curve cryptography.

Organisation:

- Cameroun: École Normale Supérieure de Bambili, Université de Ngaoundéré, Université de Yaoundé I;
- France: Inria Bordeaux et Université de Bordeaux, Université de Rennes;
- Gabon: Université des Sciences et Techniques de Masuku, Franceville;
- Senegal: Université Cheikh Anta Diop, Dakar.

Objectives

- Bolster collaborations in Africa about Cryptography;
- Open master level formations in this subject;
- Aims for an internationally recognized scientific activity;
- Develop open source softwares.

Scientific content

Rings, primality, factoring and discrete logarithms

1. Prime detection;
2. Fast arithmetic (RNS);
3. Normal Bases;
4. Index Calculus.

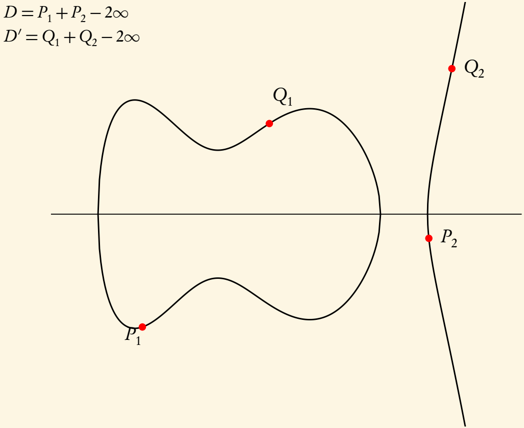
Elliptic and hyperelliptic curve cryptography

1. Group law and models;
2. Isogenies and point counting;
3. Pairings.

Jacobian of a genus 2 curve

Dimension 2: Addition law on the Jacobian of an hyperelliptic curve of genus 2:

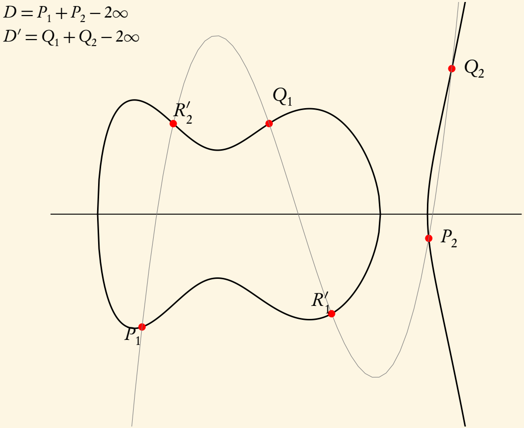
$$y^2 = f(x),\ \deg f = 5.$$



Jacobian of a genus 2 curve

Dimension 2: Addition law on the Jacobian of an hyperelliptic curve of genus 2:

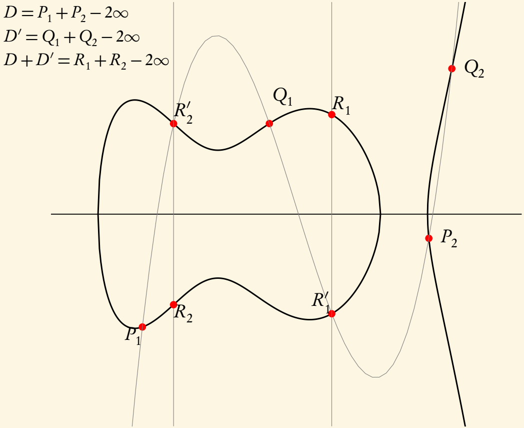
$$y^2 = f(x),\ \deg f = 5.$$



Jacobian of a genus 2 curve

Dimension 2: Addition law on the Jacobian of an hyperelliptic curve of genus 2:

$$y^2 = f(x), \deg f = 5.$$


$D = P_1 + P_2 - 2\infty$
$D' = Q_1 + Q_2 - 2\infty$
$D + D' = R_1 + R_2 - 2\infty$
Q_2
Q_1
R_1
R'_2
P_2
R'_1
R_2
P_1

Scientific activities for the year 2013

PhD Thesis

- E. Fouotsa. “Calcul des couplages et arithmétique des courbes elliptiques pour la cryptographie”. PhD thesis. Université de Rennes, 2013
- The PhD Thesis of Kodjo Egadédé (supervised by Julien Sebag) is planned for the end of November 2014.

Book

- A. Enge. “Elliptic curve cryptographic systems”. In: *Handbook of Finite Fields*. Ed. by G. L. Mullen and D. Panario. Discrete Mathematics and Its Applications. Chapman and Hall/CRC, 2013, pp. 784–796. URL: `http://hal.inria.fr/hal-00764963`

Scientific activities for the year 2013

Journals

- A. A. Ciss and D. Sow. “Randomness Extraction in finite fields Fpn”. In: *International Journal of Algebra* 7.9 (2013), pp. 409–420
- A. A. Ciss, A. Cheikh, and D. Sow. “A Factoring and Discrete Logarithm based Cryptosystem”. In: *International Journal of Contemporary Mathematical Sciences* 8.11 (2013), pp. 511–517
- J.-M. Couveignes and R. Lercier. “Fast construction of irreducible polynomials over finite fields”. In: *Israël Journal of Mathematics* 194.1 (2013). This text reports on a talk given at Lorentz center in Leiden during the recent workshop on it Counting points on varieties, pp. 77–105. DOI: 10.1007/s11856-012-0070-8. URL: http://hal.inria.fr/hal-00456456
- O. Diao and E. Fouotsa. “Arithmetic of the Level four theta model of elliptic curves”. In: *Afrika Mathematika* (2013). ISSN: 1012-9405. DOI: 10.1007/s13370-013-0203-1. URL: http://dx.doi.org/10.1007/s13370-013-0203-1
- S. Duquesne, J.-C. Bajard, and M. Ercegovac. “Combining leak-resistant arithmetic for elliptic curves defined over Fp and RNS representation”. In: *Publications Mathématiques de Besancon* 1 (2013), pp. 67–87

Scientific activities for the year 2013

Journals

- S. Duquesne, N. El Mrabet, and E. Fouotsa. “Efficient Pairing Computation on Jacobi Quartic Elliptic Curves”. In: *Journal of Mathematical Cryptology* (à paraitre)
- A. Enge and R. Schertz. “Singular values of multiple eta-quotients for ramified primes”. In: *LMS Journal of Computation and Mathematics* 16 (2013), pp. 407–418. DOI: 10.1112/S146115701300020X. URL: http://hal.inria.fr/hal-00768375
- A. Enge and E. Thomé. “Computing class polynomials for abelian surfaces”. In: *Experimental Mathematics* (2014). Accepted for publication. URL: http://hal.inria.fr/hal-00823745
- A. Enge. “Bilinear pairings on elliptic curves”. To appear in L’Enseignement Mathématique. Jan. 2013. URL: http://hal.inria.fr/hal-00767404
- T. Ezome and R. Lercier. “Elliptic periods and primality proving”. In: *Journal of Number Theory* 133.1 (2013), pp. 343–368
- T. Ezome. “Tests de primalité et de pseudo-primalité”. In: *Publications Mathématiques de Besancon* (2013), pp. 89–106

Scientific activities for the year 2013

Journals

- N. Mascot. “Computing modular Galois representations”. In: *Rendiconti del Circolo Matematico di Palermo* 62.3 (Dec. 2013), pp. 451–476. DOI: 10.1007/s12215-013-0136-4. URL: http://hal.inria.fr/hal-00776606
- R. Cosset and D. Robert. “Computing (l,l)-isogenies in polynomial time on Jacobians of genus 2 curves”. Accepté pour publication à Mathematics of Computations. 2013. URL: http://hal.inria.fr/hal-00578991
- D. Lubicz and D. Robert. “Computing separable isogenies in quasi-optimal time”. Accepted for publication at LMS Journal of Computation and Mathematics. Feb. 2014. URL: http://hal.archives-ouvertes.fr/hal-00954895

Scientific activities for the year 2013

Conferences

- R. C. Cheung, S. Duquesne, J. Fan, N. Guillermin, I. Verbauwhede, and G. Yao. “FPGA Implementation of Pairings Using Residue Number System and Lazy Reduction”. In: *Cryptographic Hardware and Embedded Systems, CHES 2011*. Ed. by B. Preneel and T. Takagi. Vol. 6917. Lecture Notes in Computer Science. Springer Berlin Heidelberg, 2011, pp. 421–441. ISBN: 978-3-642-23950-2. DOI: 10.1007/978-3-642-23951-9_28. URL: http://dx.doi.org/10.1007/978-3-642-23951-9_28
- S. Duquesne and E. Fouotsa. “Tate Pairing Computation on Jacobi’s Elliptic Curves”. In: *Pairing-Based Cryptography Pairing 2012*. Ed. by M. Abdalla and T. Lange. Vol. 7708. Lecture Notes in Computer Science. Springer Berlin Heidelberg, 2013, pp. 254–269. ISBN: 978-3-642-36333-7. DOI: 10.1007/978-3-642-36334-4_17. URL: http://dx.doi.org/10.1007/978-3-642-36334-4_17
- K. Lauter and D. Robert. “Improved CRT Algorithm for Class Polynomials in Genus 2”. In: *ANTS X - Algorithmic Number Theory 2012*. Ed. by E. W. Howe and K. S. Kedlaya. Vol. 1. The Open Book Series. San Diego, États-Unis: Mathematical Sciences Publisher, Nov. 2013, pp. 437–461. DOI: 10.2140/obs.2013.1.437. URL: http://hal.inria.fr/hal-00734450

Scientific activities for the year 2013

Preprints

- A. Mbaye, A. A. Ciss, and O. Nian. "A Lightweight Identification Protocol for Embedded Devices". In: *arXiv preprint arXiv:1408.5945* (2014)
- A. A. Ciss. "Two-sources Randomness Extractors for Elliptic Curves". In: *arXiv preprint arXiv:1404.2226* (2014)
- J.-M. Couveignes and R. Lercier. "The geometry of some parameterizations and encodings". 2013. URL: `http://hal.inria.fr/hal-00870112`

Software

- PARI/GP (via the LFANT INRIA project-team) designed for fast computations in number theory (factorisations, algebraic number theory, elliptic curves, ..., but also matrices, polynomials, power series, algebraic numbers, transcendental functions...). Used by SAGE. See `http://pari.math.u-bordeaux.fr/`.
- GNU MPC, a C library for the arithmetic of complex numbers with arbitrarily high precision and correct rounding of the result. Used by GCC. See `http://mpc.multiprecision.org/`
- Cmh, a library to compute Igusa class polynomials, parametrising two-dimensional abelian varieties with given complex multiplication. See `http://cmh.gforge.inria.fr/`
- AVIsogenies (Abelian Varieties and Isogenies), a magma package for computation on abelian varieties, with a particular emphasis on explicit isogeny computation. See `http://avisogenies.gforge.inria.fr/`.
- Magma packages for pseudo-primality testing and computation of elliptic normal basis are available here `http://perso.univ-rennes1.fr/reynald.lercier/`.

Meetings and Teaching

Meetings:

- Workshop at the Rennes Mathematical Research Institute to kickstart the project, November 2013;
- Summer school in M'Bour in Senegal with the International Center for Pure and Applied Mathematics (ICPAM/CIMPA), June 2014;
- Conference *Théorie des nombres et Applications* at CIRM, Marseille, March 2014;
- Annual Cameroonian workshop on Cryptography, Algebra and Geometry (CRAG), July 2014;
- African Mathematical School (AMS) in Franceville (Gabon), planned for March 2015.

Visits:

- Thierry Mefenza (Cameroun), to École Normale Supérieure de Paris for a PhD Thesis with Damien Vergnault, November 2013 and September–November 2014;
- Hortense Boudjou (Maroua) to visit Abdoul Aziz Ciss (École Polytechnique de Thièse, Sénégal), May – July 2014;
- Visit of Abdoul Aziz Ciss (Dakar) and Tony Ezome (Franceville) to Bordeaux, September 2014.