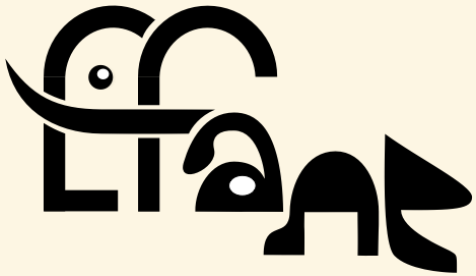
MACISA — Mathematics applied to cryptology and information security in Africa

2015/05/20 — LIRIMA Meeting, Saint-Louis, Sénégal

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;
- Equation, Stuxnet: High level viruses to compromise state level facilities (Iran nuclear centrifugal cuves);
- Heartbleed software bug in openssl...

Standards:

- NIST workshop to standardize new elliptic curves;
- IETF CFRG workgroup (Crypto Forum Research Group).

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: Université de Bamenda, Université de Maroua, 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.

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.

Collaborations:

- PRMASI/PRMAIS Project (Pole of Research in Mathematics and their Applications in Information Security): Cameroun, Gabon, Madagascar, Sénégal along with members in Cote d'Ivoire, Maroc, South Africa and international collaborators in Canada, France, the Netherlands, Singapore;
- ICPAM/CIMPA (Centre International de Mathématiques Pures et Appliquées) for the École Mathématiques Africaines;

Objectives

- Bolster collaborations in Africa about Cryptography;
- ☺ Several meetings and collaborations between members of the Macisa team;
- ☹ No industrial partners in Africa yet;
- Open master level formations in this subject;
- ☹ No master cursus in cryptography in Cameroun and Gabon;
- ☺ Several international course and École Mathématiques Africaines in cryptography given by Macisa's members;
- Aims for an internationally recognized scientific activity;
- ☺ Emmanuel Fouotsa recruited for a one year postdoc to work for the industrial ANR Simpatic (SIM and PAiring Theory for Information and Communications security);
- Develop open source softwares;
- ☺ Abdoul Aziz Ciss work in progress on the arithmetic in Mumford coordinates for Jacobian of genus 2 hyperelliptic curves in Pari/GP.

Scientific content

Rings, primality, factoring and discrete logarithms

1. Prime detection: [EL13], [Ezo13];
2. Fast arithmetic (RNS): [DBE13];
3. Normal Bases;
4. Index Calculus;
5. Randomness extractor: [CS13], [Cis14], [TC15].

Elliptic and hyperelliptic curve cryptography

1. Group law and models: [DF13a];
2. Isogenies and point counting: [CE14];
3. Pairings: [CS12], [CDF+11], [DF13b], [DEFre], [EF15];
4. Protocols: [CCS13], [MCN14], [OK15].

PhD Thesis

- E. Fouotsa. “Calcul des couplages et arithmétique des courbes elliptiques pour la cryptographie”. PhD thesis. Université de Rennes, 2013
- Defense of the PhD Thesis of Kodjo Egadédé (supervised by Julien Sebag) in December 2014.

- Hortense Hardy-Boudjou, Assistant Professor, PhD Student (Université de Maroua, Cameroun);
- Thierry Mefenza, PhD in co-management between the University of Yaounde 1 in Cameroon under the direction of Professor Marcel Tonga, and the École Normale Supérieure (ENS) in Paris, France under the direction of Professor Damien Vergnaud on Étude de l’aléatoire en cryptographie mathématique.

Scientific activities for the year 2015

- Summer school in Franceville (Gabon) with the International Center for Pure and Applied Mathematics (ICPAM/CIMPA), March 2014: one week cryptography course by Jean-Marc Couveignes and Damien Robert along with short presentations by some members of the team;
- Courses in Yaounde and Bamenda (Cameroun) by members of the team (the local members, Ciss, Ezome) to prepare a master in cryptography cursus;

- Visit of Thierry Mefenza in Paris for the ANR ROMAnTIC (Randomness in Mathematical Cryptography).
- Visit of Abdoul Aziz Ciss and Emmanuel Fouotsa for ECC 2015 in September in Bordeaux;
- Visit of Tony Ezome in Bordeaux in October following a workshop in Italy;

Scientific highlight

- J.-M. Couveignes and T. Ezome. “Computing functions on Jacobians and their quotients”. Accepted for publication in LMS Journal of Computation and Mathematics. Nov. 2014. URL: https://hal.archives-ouvertes.fr/hal-01088933;
- Efficient way to evaluate functions on Jacobians (following Weil);
- Combine eta functions and a deformation trick;
- Geometric way to compute isogenies;
- Key idea: compute the regular action of the theta group rather than the irreducible action;
- System of differential equation allow to recover the equations of the isogenous curve from the image of only one thick point.

- Let $p > 2$ be a prime. $(\mathbb{Z}/p\mathbb{Z}^*, \times)$ is a cyclic group of order $p-1$;
- There are $(p-1)/2$ squares and $(p-1)/2$ non squares;
- If $x \in \mathbb{Z}/p\mathbb{Z}^*$ then x is a square if and only if $x^{\frac{p-1}{2}} = 1$ (by Fermat $x^{p-1} = 1$ for all $x \in \mathbb{Z}/p\mathbb{Z}^*$);
- Legendre symbol:

$$\left(\frac{x}{p}\right) = \begin{cases} 1 & x \text{ is a square} \\ -1 & x \text{ is not a square} \\ 0 & x = 0 \bmod p; \end{cases}$$

- $\left(\frac{x}{p}\right) = x^{\frac{p-1}{2}} \pmod p$;
- Multiplicativity: $\left(\frac{xy}{p}\right) = \left(\frac{x}{p}\right)\left(\frac{x}{q}\right)$;
- Quadratic reciprocity: p, q primes > 2:

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\,\frac{q-1}{2}}.$$

- Jacobi symbol: if n is odd, define the Jacobi symbol by extending the Legendre symbol multiplicatively on the bottom argument:

$$\left(\frac{x}{n_1 n_2}\right) = \left(\frac{x}{n_1}\right)\left(\frac{x}{n_2}\right);$$

- Extension of quadratic reciprocity:

$$\left(\frac{m}{n}\right) = (-1)^{\frac{m-1}{2}\frac{n-1}{2}}\left(\frac{n}{m}\right) \quad (m \text{ and } n \text{ odd and coprime})$$

with the extra relations $\left(\frac{-1}{n}\right) = (-1)^{\frac{n-1}{2}}$, $\left(\frac{2}{n}\right) = (-1)^{\frac{n^2-1}{8}}$;

$\Rightarrow$ The Jacobi symbol can be computed in polynomial time;

- Primality test: if $\left(\frac{x}{n}\right) \neq x^{\frac{n-1}{2}}$ then n is not prime (and if n is not prime at least half the x coprime to n will be witnesses).

An introduction to public key cryptography: Heads or tails

- Let $n = pq$ be an RSA number, by the CRT $(\mathbb{Z}/n\mathbb{Z}^*, \times) = (\mathbb{Z}/p\mathbb{Z}^* \times \mathbb{Z}/q\mathbb{Z}^*, \times)$;
- $\left(\frac{x}{n}\right) = \left(\frac{x}{p}\right)\left(\frac{x}{q}\right)$ so if x is prime to n, $\left(\frac{x}{n}\right) = 1$ when x is a square modulo n (=square modulo p and square modulo q) or when x is neither a square modulo p and q;
- Computing $\left(\frac{x}{n}\right)$: polynomial time;
- Deciding if x is a real square (and computing the square root) or false square: factorisation of n
- $x \mapsto x^2$ is a one way trapdoor function!

Heads or tails:

- Bob choose $n = pq$ and sends x such that $\left(\frac{x}{n}\right) = 1$;
- Alice answers “real square” or “false square”;
- Bob sends p and q so Alice can verify if she was right or not.

An introduction to public key cryptography: Zero Knowledge identification

- Secret key of Alice: p, q, s mod $n = pq$;
- Public key of Alice: $n = pq$, $r = s^2$;

Zero Knowledge identification:

- Alice chooses a random u mod n, computes $z = u^2$ and sends $t = zr = u^2 s^2$ to Bob;
- Bob either chooses
  - To check z: he asks u to Alice and checks that $z = u^2$;
  - To check t: he asks us to Alice and checks that $t = (us)^2$.
- A liar will either produce a false u or a false t and has $1/2$ chances to be catched, Bob will ask for several rounds (30);
- To always give the correct answer mean that Alice knows the secret s or is very lucky (probability $1/2^{30}$).

Bibliography

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 (cit. on p. 7).

A. A. Ciss. "Two-sources Randomness Extractors for Elliptic Curves". In: *arXiv preprint arXiv:1404.2226* (2014) (cit. on p. 7).

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 (cit. on p. 7).

A. A. Ciss and D. Sow. "Pairings on Generalized Huff Curves". 2012 (cit. on p. 7).

A. A. Ciss and D. Sow. "Randomness Extraction in finite fields Fpn". In: *International Journal of Algebra* 7.9 (2013), pp. 409–420 (cit. on p. 7).

J.-M. Couveignes and T. Ezome. “Computing functions on Jacobians and their quotients”. Accepted for publication in LMS Journal of Computation and Mathematics. Nov. 2014. URL: https://hal.archives-ouvertes.fr/hal-01088933 (cit. on pp. 7, 10).

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 (cit. on p. 7).

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 (cit. on p. 7).

S. Duquesne, N. El Mrabet, and E. Fouotsa. “Efficient Pairing Computation on Jacobi Quartic Elliptic Curves”. In: *Journal of Mathematical Cryptology* (à paraitre) (cit. on p. 7).

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 (cit. on p. 7).

N. El Mrabet and E. Fouotsa. "Failure of the Point Blinding Countermeasure Against Fault Attack in Pairing-Based Cryptography". In: *Codes, Cryptology, and Information Security*. Springer, 2015, pp. 259–273 (cit. on p. 7).

T. Ezome. "Tests de primalité et de pseudo-primalité". In: *Publications Mathématiques de Besancon* (2013), pp. 89–106 (cit. on p. 7).

T. Ezome and R. Lercier. "Elliptic periods and primality proving". In: *Journal of Number Theory* 133.1 (2013), pp. 343–368 (cit. on p. 7).

E. Fouotsa. "Calcul des couplages et arithmétique des courbes elliptiques pour la cryptographie". PhD thesis. Université de Rennes, 2013 (cit. on p. 8).

A. Mbaye, A. A. Ciss, and O. Nian. "A Lightweight Identification Protocol for Embedded Devices". In: *arXiv preprint arXiv:1408.5945* (2014) (cit. on p. 7).

A. Otmani and H. T. Kalachi. “Square Code Attack on a Modified Sidelnikov Cryptosystem”. In: *Codes, Cryptology, and Information Security*. Springer, 2015, pp. 173–183 (cit. on p. 7).

H. B. Tchapgnouo and A. A. Ciss. “Multi-sources Randomness Extraction over Finite Fields and Elliptic Curve”. In: *arXiv preprint arXiv:1502.00433* (2015) (cit. on p. 7).