MACISA — Mathematics applied to cryptology and information security in Africa

2013/09/17 — EMI, Rabat

Damien Robert

Équipe LFANT, Inria Bordeaux Sud-Ouest

Contenu

Contexte actuel

- http://en.wikipedia.org/wiki/PRISM_(surveillance_program) :
  « The Prism program collects stored Internet communications based on demands made to Internet companies » (Microsoft, Yahoo !, Google, Facebook, Paltalk, YouTube, AOL, Skype, Apple...)
- Officiellement pour lutter contre le terrorisme ;
- Mais aussi utilisé pour l'espionnage économique :
  http://www.theguardian.com/world/2013/jun/09/edward-snowden-nsa-whistleblower-surveillance
- Les Étas-Unis ne sont pas les seuls à avoir des systèmes de surveillance...
  http://www.theguardian.com/world/2013/jul/04/france-electronic-spying-operation-nsa

$\Rightarrow$ L'utilisation de la cryptographie est un enjeu de souveraineté nationale !

Quelle cryptographie ?

- Tout système ad-hoc, non basé sur des standards a été cassé (DECSS, GSM, WEP...)
- Utiliser un standard suffit-il ?

Quelle cryptographie ?

http://blog.cryptographyengineering.com/2013/09/on-nsa.html

Matthew Green — « The NSA has been :

- Tampering with national standards (NIST is specifically mentioned) to promote weak, or otherwise vulnerable cryptography.
- Influencing standards committees to weaken protocols.
- Working with hardware and software vendors to weaken encryption and random number generators.
- Attacking the encryption used by “the next generation of 4G phones”.
- Obtaining cleartext access to “a major internet peer-to-peer voice and text communications system”
- Identifying and cracking vulnerable keys.
- Establishing a Human Intelligence division to infiltrate the global telecommunications industry.
- decrypting SSL connections.

»

Quelle cryptographie ?

- Tout système ad-hoc, non basé sur des standards a été cassé (DECSS, GSM, WEP...)
- Utiliser un standard suffit-il ?

⇒ On a besoin d'une cryptographie issue de la recherche publique, conduite par des experts universitaires, en lien avec le milieu économique local.

MACISA

- MACISA : Mathematics applied to cryptology and information security in Africa ;
- Cryptologie à clés publiques, via des constructions provenant de l'algèbre et de la géométrie ;
- Authentification, chiffrement asymétrique, signature, preuves zero-knowledge ;
- Étude des aspects théoriques et algorithmiques.
- Nouvellement crée. Réunion de lancement à Rennes en Décembre 2013.

Deux thèmes :

1. Anneaux, primalité, factorisation et logarithme discret ;
2. Cryptographie elliptique et hyperelliptique.

Organisateurs

- **Guy Martial Nkiet** (Franceville), coordinateur ;
- **Jean-Marc Couveignes** (Bordeaux), vice-coordinateur ;
- **Andreas Enge** (Bordeaux) ;
- **Tony Ezome** (Franceville), responsable scientifique du thème algèbre ;
- **Damien Robert** (Bordeaux), responsable scientifique du thème géométrie.

Participants

- École Normale Supérieure de Bambili, Bamenda, Cameroun : **Émmanuel Fouotsa** ;
- Inria Bordeaux et Université de Bordeaux, France : **Jean-Marc Couveignes, Andreas Enge, Damien Robert** ;
- Université Cheikh Anta Diop, Dakar, Sénégal : **Abdoul Aziz Ciss, Djiby Sow** ;
- Université des Sciences et Techniques de Masuku, Franceville, Gabon : **Guy Martial Nkiet, Tony Ezome** ;
- Université de Ngaoundéré, Cameroun : **Daniel Tieudjo** ;
- Université de Rennes, France : **Sylvain Duquesne, Reynald Lercier, David Lubicz, Julien Sebag** ;
- Université des Sciences, Yaoundé, Cameroun : **Marcel Tonga** ;

Thésards

- **Hortense Boudjou Tchapgnouo** (Maroua) ;
- **Émmanuel Fouotsa** (Rennes et Yaoundé) ;
- **Kodjo Kpognon Egadédé** (Rennes) ;
- **Nicolas Mascot** (Bordeaux) ;
- **Régis Maurin Obiang Mba** (Montpellier) ;
- **Christophe Tran** (Rennes).

Anneaux, primalité, factorisation, logarithme discret

Participants : **Ezome, Boudjou, Ciss, Couveignes, Duquesne, Enge, Lercier, Nkiet, Mascot, Tieudjo, Tonga.**

- Bases normales ;
- Residue number system ;
- Tests de primalité ;
- Calcul d'index.

Bases normales

Définition

Une extension Galoisienne de corps L/K est représentée par une base normale B si B est un torseur sous l'action de $\mathrm{Gal}(L/K)$.

- Sur un corps fini $L = \mathbb{F}_{p^e}$, une base normale est générée par un élément primitif x. La base est alors donnée par

$$B = (x, x^p, x^{p^2}, \ldots, x^{p^{e-1}}).$$

- Calcul très efficace du Frobenius ;
- Multiplication rapide.

Remarque

On peut utiliser les courbes elliptiques pour générer des bases normales (ou pseudo-normales) de corps finis.

Residue number system (RNS)

Théorème (Théorème des restes Chinois)

Si $N = \prod p_i^{e_i}$*, alors*

$$\mathbb{Z}/N\mathbb{Z} \simeq \prod \mathbb{Z}/p_i^{e_i}$$

- Représentation d'un nombre via son système de résidus ;
- Arithmétique rapide ;
- Implémentation hardware efficace.

Tests de primalité

- Soit n un entier naturel, $n-1=2^s d$ (d impair). Supposons n premier.
- Soit $x \in (\mathbb{Z}/n\mathbb{Z})^*$;
- Par le petit théorème de Fermat, $x^{n-1}=1$;
- Les seules racines carrées de l'unité sont $\{1,-1\}$ donc soit $x^d=1$, soit il existe $0 \leqslant r < s$ tel que $x^{2^r d}=-1$;
- Si on trouve x tel que cette alternative n'est pas vérifiée, alors n est en fait un nombre composé ;
- C'est le test probabiliste de Miller Rabin.

Remarque

On peut améliorer l'efficacité du test de Miller Rabin en utilisant la théorie Galoisienne des anneaux étales.

Cryptographie elliptique et hyperelliptique

Participants : **Robert, Ciss, Couveignes, Diao, Duquesne, Enge, Ezome, Fouotsa, Kpognon, Lubicz, Mascot, Sebag, Sow, Tran.**

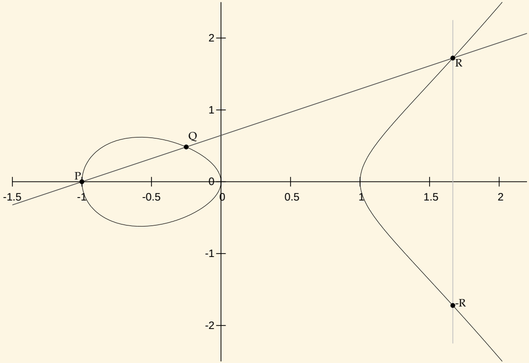
- Modèles de courbes, lois d'addition ;
- Sécurité : Comptage de points ;
- Couplages.

Les courbes elliptiques

Définition (char $k \neq 2, 3$)

Une courbe elliptique est une courbe plane d'équation

$$y^2 = x^3 + ax + b \qquad 4a^3 + 27b^2 \neq 0.$$



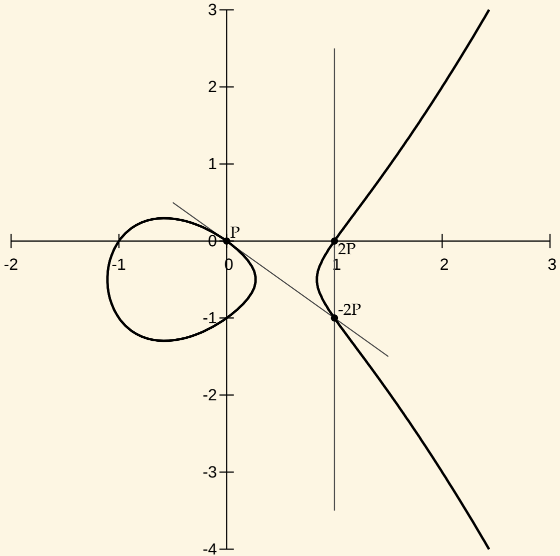
Exponentiation :

$$(\ell, P) \mapsto \ell P$$

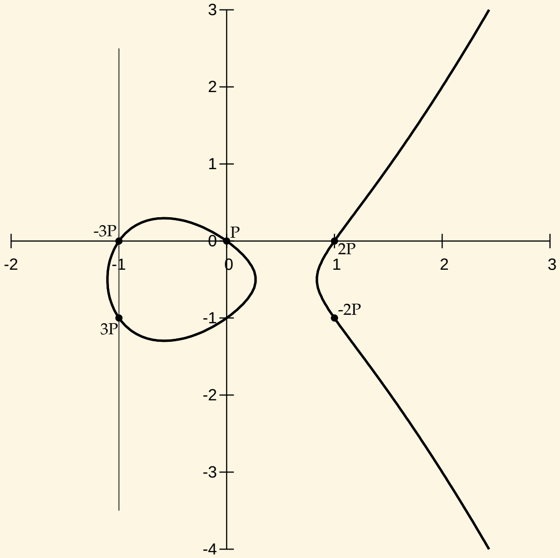
Logarithme discret :

$$(P, \ell P) \mapsto \ell$$

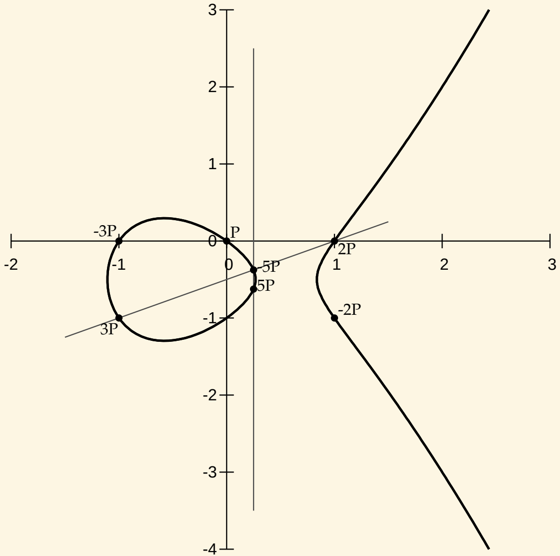
Exponentiation sur une courbe elliptique



Exponentiation sur une courbe elliptique



Exponentiation sur une courbe elliptique



Utilisation des courbes elliptiques

Exemple (ECC 160 bits)

- E courbe elliptique $y^2 = x^3 + x + 333$ sur $\mathbb{F}_{1461501637330902918203684832716283019655932542983}$
- Clé publique :

$$P = (1369962487580788774992199588498961558341362086296,$$
$$4071602035929820962999050316307984909420439350 21);$$
$$Q = (695697562436343265984113032286189105569389589 80,$$
$$1126203611660190221708449639677667925024412968395);$$

- Clé secrète : ℓ tel que $Q = \ell P$.

- Recommandées par la NSA ;
- Utilisées dans les passeports biométriques Européens.

Avantage des courbes elliptiques

À niveau de sécurité égale, les cryptosystèmes basés sur les courbes elliptiques, par rapport à RSA sont

- plus rapides ;
- plus compacts ;
- plus puissants.

Exemple (Couplages)

- Un couplage est une application bilinéaire non dégénérée.
- Sur une courbe elliptique, à partir d'une clé publique on peut générer d'autres clé publiques. De même pour la clé secrète.

$\Rightarrow$ Certificats anonymes, cryptographie fondée sur l'identité, signatures courtes, diffusion multicanaux ...

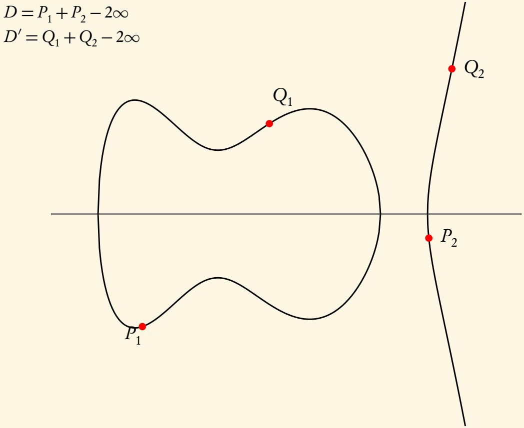
Exemple (Fonctions de hachage)

Les graphes d'isogénies de courbes elliptiques supersingulières fournissent des fonctions de hachage cryptographiquement sûres.

Dimension supérieure

Dimension 2 : Loi d'addition sur la Jacobienne d'une courbe hyperelliptique de genre 2 :

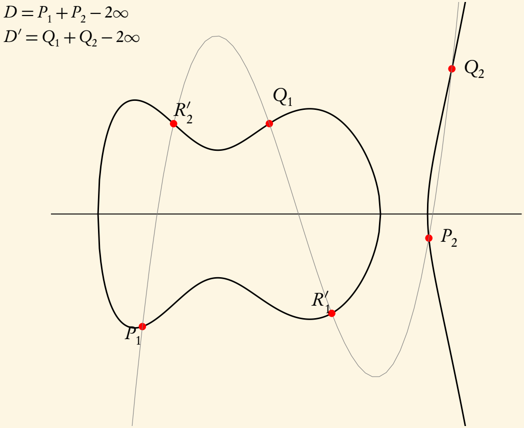
$$y^2 = f(x),\ \deg f = 5.$$



Dimension supérieure

Dimension 2 : Loi d'addition sur la Jacobienne d'une courbe hyperelliptique de genre 2 :

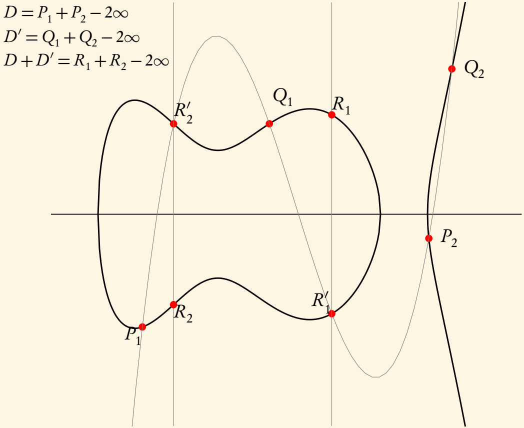
$$y^2 = f(x),\ \deg f = 5.$$



Dimension supérieure

Dimension 2 : Loi d'addition sur la Jacobienne d'une courbe hyperelliptique de genre 2 :

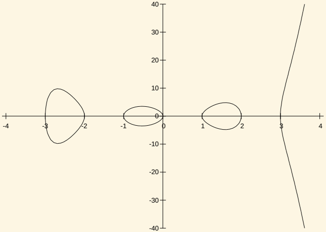
$$y^2 = f(x), \deg f = 5.$$



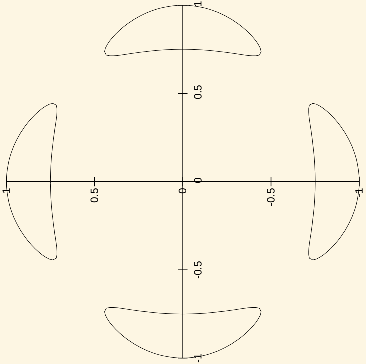
Dimension supérieure

Dimension 3

Jacobiennes de courbes hyperelliptiques de genre 3.



Jacobiennes de quartiques.



Graphe d'isogénies sur les courbes elliptiques

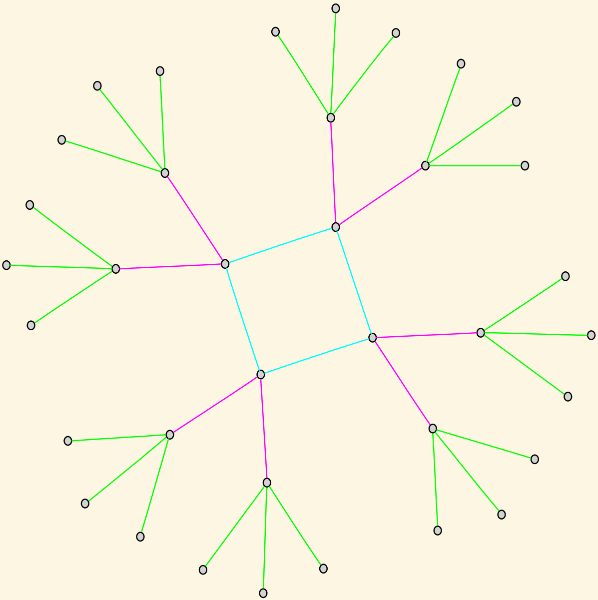
Définition

Les isogénies sont les morphismes de courbes elliptiques.

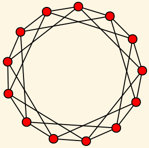
Les isogénies font le lien entre

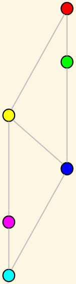
- arithmétique ;
- anneaux d'endomorphismes ;
- polynômes de classes ;
- polynômes modulaires ;
- comptage de points ;
- relèvements canoniques ;
- espaces de modules ;
- transfert du logarithme discret.

Graphe d'isogénies sur les courbes elliptiques

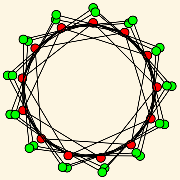


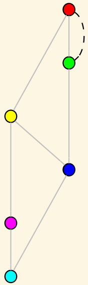
Graphe d'isogénies en dimension 2



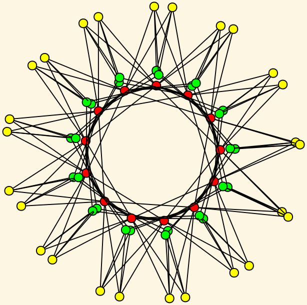


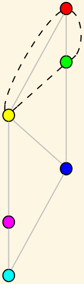
Graphe d'isogénies en dimension 2



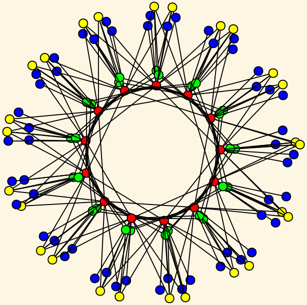


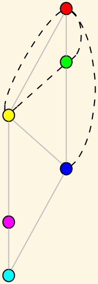
Graphe d'isogénies en dimension 2



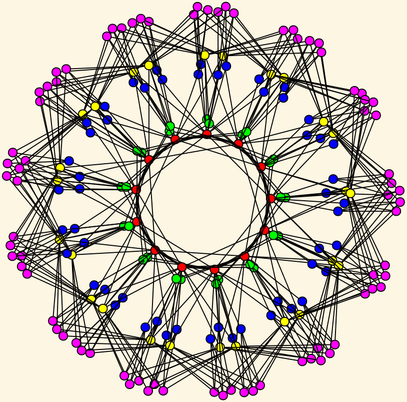


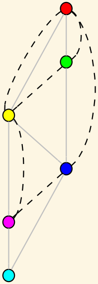
Graphe d'isogénies en dimension 2





Graphe d'isogénies en dimension 2





Graphe d'isogénies en dimension 2