Théorie algorithmique des nombres et cryptologie publique

F. Morain, P. Gaudry, A. Enge, R. Dupont, T. Houtmann

`http://www.lix.polytechnique.fr`
LIX, École Polytechnique, Palaiseau Cedex 91128, FRANCE

Qu'est-ce que la cryptologie ?

But : protéger les communications, les fichiers, etc. d'ennemis de toute sorte.
Alliance de la cryptographie (**je construis**) et de la cryptanalyse (**je casse**).

Le CREDO de l'équipe : la cryptologie du troisième millénaire ne peut se passer d'un mélange en parts égales de mathématiques non triviales et d'informatique de pointe.

Rivest–Shamir–Adleman, 1976

Principe : la factorisation d'entiers est beaucoup plus difficile que la multiplication.
Fonctionnement :

$$N = p\,q$$

$$\mathrm{pgcd}(e,\,\varphi(N)) = 1 \;\Rightarrow\; \exists\, d,\; e\,d = 1 + k\varphi(N)$$

$$\begin{array}{lcccl} \textbf{clair} & : & x & & \\ \textbf{chiffrement} & : & y & \equiv & x^e \bmod N \\ \textbf{déchiffrement} & : & y^d & \equiv & x^{ed} \bmod N \\ & & & \equiv & x(x^{\varphi(N)})^k \\ & & & \equiv & x \end{array}$$

Deux problèmes :

- fabriquer p et q ;
- sûreté $\Leftarrow$ factorisation d'entiers.

Diffie et Hellman, 1976

Logarithme discret :
p nombre premier, g donnés

$$A \overset{g^x \bmod p}{\longrightarrow} B$$

$$A \overset{g^y \bmod p}{\longleftarrow} B$$

$$A : K_{AB} = (g^y)^x \equiv g^{xy} \bmod p$$

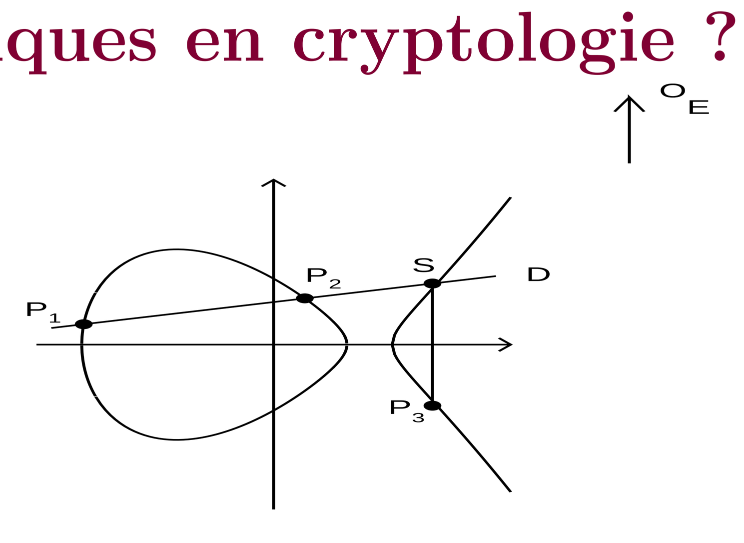
$$B : K_{BA} = (g^x)^y \equiv g^{xy} \bmod p$$

Le principe se généralise à un groupe G quelconque pour lequel $\#G$ est connu.

Problème :

- Sûreté $\Leftarrow$ calcul de x à partir de (g, g^x) ?
- Meilleur algorithme $O(\exp(c(\log p)^{1/3}(\log\log p)^{2/3}))$.

Pourquoi des courbes algébriques en cryptologie ?



- Point de vue théorique : beaucoup de groupes possibles, fournissant des algorithmes rapides pour de nombreux problèmes (primalité en temps polynomial, factorisation rapide).

- Point de vue pratique : à sécurité égale, la taille des clefs est de 6 à 10 fois plus petite que dans le cas classique.

Les axes de recherche

A) Arithmétique effective

- prouver la primalité d'un entier quelconque (courbes elliptiques) ;

- factoriser les entiers

- résoudre des logarithmes discrets sur des corps finis.

B) Multiplication complexe

- prouver la primalité d'un entier quelconque (courbes elliptiques) ;

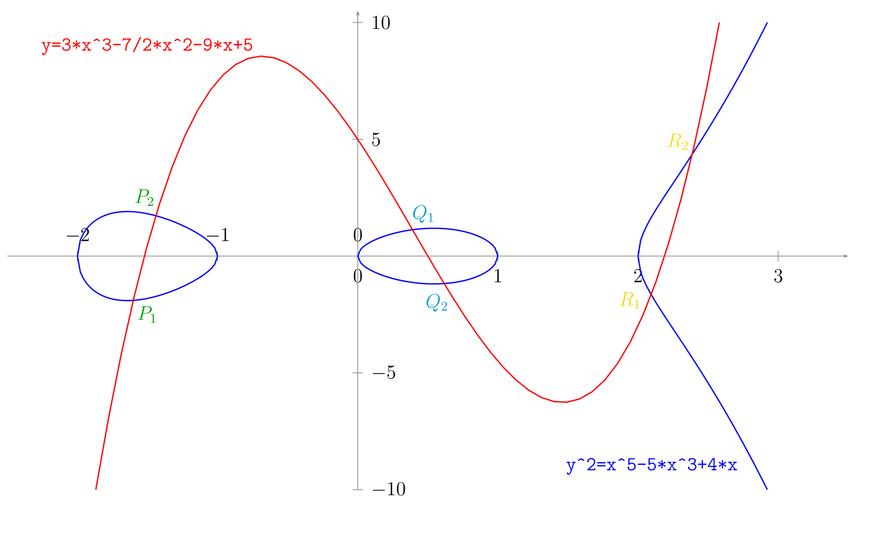
- construire des courbes algébriques (elliptiques, hyperelliptiques) sures ;

C) Courbes algébriques sur des corps finis

- calculer la loi de groupe sur la Jacobienne d'une courbe ;

- calculer le cardinal de la Jacobienne d'une courbe ;

- étudier la sécurité du logarithme discret dans la Jacobienne d'une courbe.



Les domaines mathématiques abordés

- corps finis : théorie, algorithmique ;
- corps de nombres : corps quadratiques imaginaires, réels, etc.
- nombres p-adiques : théorie, algorithmique, extensions non ramifiées ;
- théorie de Galois : résolution par radicaux ;
- courbes (hyper)elliptiques : réseaux, multiplication complexe, corps de classes ;
- géométrie algébrique effective ;
- systèmes polynomiaux : résultants, bases de Gröbner.

Les outils informatiques

- librairies de calcul en multiprécision : GMP, NTL, MPFR, MPC, Mploc ;
- systèmes de calcul formel : Maple, Magma ;
- calculs distribués : réseaux de stations de travail.

Quelques résultats

- Primalité : preuve de primalité du nombre premier de 15071 décimales : $4405^{2638} + 2638^{4405}$.
Calcul : fastECPP, 720 jours sur un Xeon 2.6 GHz (07/2004).

- Factorisation : RSA155 (1999).

- Construction de courbes elliptiques sures : tous les records mondiaux (500 chiffres décimaux).

Qui?	Méthode	Date	Taille	Temps
Lercier-Morain	SEA	1997	2^{1307}	103 j DEC alpha 250 (266MHz)
Joux-Lercier	SEA	06/1998	2^{1663}	330 j DEC alpha 250 (266MHz)
Vercauteren	SEA	10/1999	2^{1999}	65 j PC, 400MHz
FGHM	Satoh -FGH	05/2000	2^{2003}	14 h Alpha EV6 (500MHz)
FGHM	Satoh -FGH	08/2000	2^{6007}	9 j Alpha EV6 (750MHz)
Harley	AGM	08/2002	2^{32003}	27 h Alpha EV6 (750MHz)

- Cassage de cryptosystèmes basés sur les courbes hyperelliptiques :
  $\ast$ amélioration des algorithmes théoriques et pratiques pour les courbes hyperelliptiques de genre grand ;
  $\ast$ nouvel algorithme pour les courbes de genre 3 et 4 ;
  $\Rightarrow$ Ne pas utiliser les courbes de genre $\geqslant 4$, et attention au genre 3.
  $\ast$ attaque générale des courbes elliptiques sur $\mathbb{F}_{p^3}$ et $\mathbb{F}_{p^4}$.
  $\Rightarrow$ Ne pas utiliser ces courbes !

Calcul de cardinalité de Jacobiennes de courbes algébriques

A) Algorithmes en petite caractéristique

- Extension de l'algorithme de Kedlaya des courbes plus générales ;

- extension à des courbes de caractéristique moyenne.

B) Algorithmes en grande caractéristique

- Améliorations multiples de l'algorithme de Schoof en genre 2 ;

- Première construction de courbes aléatoires cryptographiquement sures.
Fabrication d'une courbe de genre 2 d'ordre premier sur $\mathbb{F}_p$ avec $p \approx 5 \times 10^{24}$.
Environ 45 jours de calculs sur un Pentium 2 GHz.

$\Rightarrow$ De nouvelles courbes utilisables en cryptographie !