

Petit théorème de Fermat et courbes elliptiques, les mathématiques au service du secret

Andreas Enge

LFANT project-team
INRIA Bordeaux-Sud-Ouest
andreas.enge@inria.fr
<http://www.math.u-bordeaux1.fr/~enge>

Bordeaux, 28/01/2011





- 1 Petite histoire de la cryptologie: Les bons vieux temps
- 2 Diffie–Hellman: Le début des temps modernes
- 3 RSA: Le système d'aujourd'hui
- 4 Logarithmes discrets et factorisation: Un peu de cryptanalyse
- 5 ECC: Les systèmes de l'avenir

- **ATBASH** — substitution utilisée dans la bible
A = T, B = SH, ...
Babylon = Sheshach
- 1412: encyclopédie arabe contenant une section sur la cryptologie, fréquence des mots dans le coran



- substitution monoalphabétique avec homophones
- substitution polyalphabétique
 - ▶ inventée par Trithemius en 1518
 - ▶ attaquée par Kasiski en 1863

j e t a i m e a l a f o l i e
+ c l e f c l e f c l e f c l e
LPXFKXHFNLITNWI

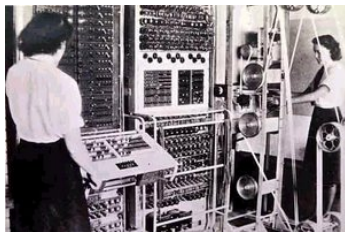
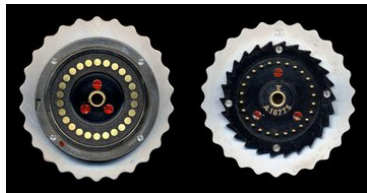
r	e	v	a	s
3	2	5	1	4
c	e	c	i	e
s	t	u	n	m
e	s	s	a	g
e	a	r	c	h
i	s	e	c	r
e	t			

INAC CETS ASTC SEEI EEMG HRCU SRE

Lois de Kerckhoffs (1883)

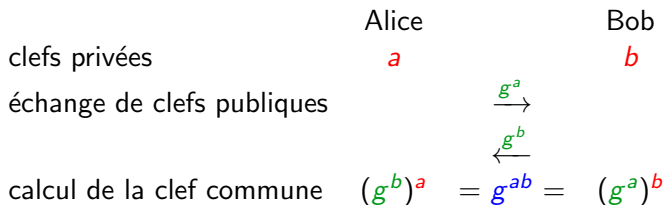
- Le système doit être matériellement, sinon **mathématiquement**, indéchiffrable.
- Il faut qu'il n'exige pas le secret, et qu'il puisse sans inconvénient tomber entre les mains de l'ennemi.
- La clef doit pouvoir en être communiquée et retenue sans le secours de notes écrites, et être changée ou modifiée au gré des correspondants.
- Il faut qu'il soit applicable à la correspondance télégraphique.
- Il faut qu'il soit portatif, et que son maniement ou son fonctionnement n'exige pas le concours de plusieurs personnes.
- Enfin, il est nécessaire, vu les circonstances qui en commandent l'application, que le système soit d'un usage facile, ne demandant ni tension d'esprit, ni la connaissance d'une longue série de règles à observer.

Enigma



- 1 Petite histoire de la cryptologie: Les bons vieux temps
- 2 Diffie–Hellman: Le début des temps modernes
- 3 RSA: Le système d'aujourd'hui
- 4 Logarithmes discrets et factorisation: Un peu de cryptanalyse
- 5 ECC: Les systèmes de l'avenir

Échange de clefs à la Diffie–Hellman (1976)



Chiffrement ElGamal (1985)

- $G = \langle g \rangle$ groupe cyclique fini d'ordre n
(entiers modulo p premier sans 0, $n = p - 1$)
- $m \in G$ texte clair

Alice

clef privée

clef publique

“clef privée” éphémère

“clef publique” éph.

chiffrement

déchiffrement

$$r \in_R [0, n - 1]$$

$$c = (c', c'') = (g^r, m(g^b)^r)$$

→

Bob

$$b \in_R [0, n - 1]$$

$$g^b$$

$$m = c'' / (c')^b$$

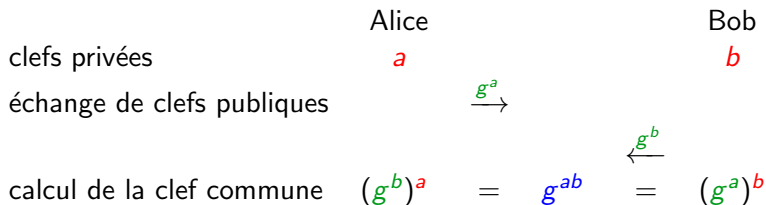
- Problème du logarithme discret (DLP):
Étant donné h , trouver x t.q. $h = g^x$
- Solution du DLP \implies clefs privées

- Problème du logarithme discret (DLP):
Étant donné h , trouver x t.q. $h = g^x$
- Solution du DLP \implies clefs privées
- Problème de Diffie–Hellman (CDH):
Étant donnés g, g^x, g^y , trouver g^{xy}
- Solution de CDH \implies
 - ▶ secrets partagés
 - ▶ décryptage de textes chiffrés au coup par coup
 - ▶ forgeage de signatures

- Problème du logarithme discret (**DLP**):
Étant donné h , trouver x t.q. $h = g^x$
- Solution du DLP \implies clefs privées
- Problème de Diffie–Hellman (**CDH**):
Étant donnés g, g^x, g^y , trouver g^{xy}
- Solution de CDH \implies
 - ▶ secrets partagés
 - ▶ décryptage de textes chiffrés au coup par coup
 - ▶ forgeage de signatures
- DLP \implies CDH

- Problème du logarithme discret (DLP):
Étant donné h , trouver x t.q. $h = g^x$
- Solution du DLP \implies clefs privées
- Problème de Diffie–Hellman (CDH):
Étant donnés g, g^x, g^y , trouver g^{xy}
- Solution de CDH \implies
 - ▶ secrets partagés
 - ▶ décryptage de textes chiffrés au coup par coup
 - ▶ forgeage de signatures
- DLP \implies CDH
 \longleftarrow moralement vrai
(Maurer–Wolf 1999; preuve avec les courbes elliptiques!)

Échange de clefs à la Diffie–Hellman



Attaque de la femme au milieu

	Alice		Ève		Bob
clefs privées	a		e		b
échange de clefs publiques		$\xrightarrow{g^a}$		$\xrightarrow{g^e}$	
		$\xleftarrow{g^e}$		$\xleftarrow{g^b}$	
calcul de la clef commune	$(g^e)^a$	=	$(g^a)^e$ $(g^b)^e$	=	$(g^e)^b$

- 1 Petite histoire de la cryptologie: Les bons vieux temps
- 2 Diffie–Hellman: Le début des temps modernes
- 3 RSA: Le système d'aujourd'hui**
- 4 Logarithmes discrets et factorisation: Un peu de cryptanalyse
- 5 ECC: Les systèmes de l'avenir

Petit théorème de Fermat

- Pour p premier et a un entier (non divisible par p), on a

$$p \text{ divise } a^{p-1} - 1$$

$$a^{p-1} = 1 \pmod{p}$$

- Exemple

Petit théorème de Fermat

- Pour p premier et a un entier (non divisible par p), on a

$$p \text{ divise } a^{p-1} - 1$$

$$a^{p-1} = 1 \pmod{p}$$

- Exemple
- Corollaire: Pour $p - 1$ qui divise m , on a

$$a^m = 1 \pmod{p}$$

- Preuve rapide:

$$a^m = a^{k(p-1)} = (a^{p-1})^k = 1^k = 1 \pmod{p}$$

- Généralisation pour des modules composés

- ▶ p et q premiers, $N = pq$

- ▶ $\lambda = \text{ppcm}(p - 1, q - 1)$

- ▶ a un entier (non divisible par p et q)

N divise $a^\lambda - 1$

$a^\lambda = 1 \pmod N$

- Généralisation pour des modules composés

- ▶ p et q premiers, $N = pq$

- ▶ $\lambda = \text{ppcm}(p - 1, q - 1)$

- ▶ a un entier (non divisible par p et q)

$$N \text{ divise } a^\lambda - 1$$

$$a^\lambda = 1 \pmod{N}$$

- Corollaire: Pour λ qui divise m , on a

$$a^m = 1 \pmod{N}$$

Chiffrement RSA (1978)

Alice

clef publique

clef privée

chiffrement

$$c = m^e \bmod N$$

déchiffrement

→

Bob

N, e premier avec N
 $N = pq, d = e^{-1} \bmod \lambda$

$$m = c^d = m^{ed} \bmod N$$

Chiffrement RSA (1978)

Alice

clef publique

clef privée

chiffrement

$$c = m^e \bmod N$$

Bob

N , e premier avec N

$$N = pq, d = e^{-1} \bmod \lambda$$

déchiffrement

→

$$m = c^d = m^{ed} \bmod N$$

- $ed = 1 + k\lambda$
- $m^{ed} = m^{1+k\lambda} = (m^\lambda)^k \cdot m = 1^k \cdot m = m$

Problèmes calculatoires sous-jacentes à la sécurité

- Factorisation (FP):
Étant donné N , trouver p, q t.q. $N = pq$
- Solution à FP \implies clefs privées

- Factorisation (FP):
Étant donné N , trouver p, q t.q. $N = pq$
- Solution à FP \implies clefs privées
- Problème RSA (RSAP) = calcul de racines modulo N composé:
Étant donnés N, e et m^e , trouver m
- Solution à RSAP \implies
 - ▶ déchiffrement de textes un à un
 - ▶ forgeage de signatures une à une

- Factorisation (FP):
Étant donné N , trouver p, q t.q. $N = pq$
- Solution à FP \implies clefs privées
- Problème RSA (RSAP) = calcul de racines modulo N composé:
Étant donnés N, e et m^e , trouver m
- Solution à RSAP \implies
 - ▶ déchiffrement de textes un à un
 - ▶ forgeage de signatures une à une
- FP \implies RSAP

- Factorisation (FP):
Étant donné N , trouver p, q t.q. $N = pq$
- Solution à FP \implies clefs privées
- Problème RSA (RSAP) = calcul de racines modulo N composé:
Étant donnés N, e et m^e , trouver m
- Solution à RSAP \implies
 - ▶ déchiffrement de textes un à un
 - ▶ forgeage de signatures une à une
- FP \implies RSAP
 \longleftarrow peut-être faux pour petits exposants (LE-RSAP)

- Buts d'un attaquant
 - ▶ **déchiffrer** un texte clair inconnu (**sécurité élémentaire**)
 - ▶ **distinguer** entre deux messages candidats (**indistingabilité, IND**)

- Buts d'un attaquant
 - ▶ **déchiffrer** un texte clair inconnu (**sécurité élémentaire**)
 - ▶ **distinguer** entre deux messages candidats (**indistingabilité, IND**)
- Capacités de l'attaquant
 - ▶ **Ciphertext only attack**
 - ▶ **CPA (chosen plaintext attack)**:
chiffrer des textes clairs arbitraires
possibles en crypto à clef publique!
 - ▶ **CCA1 (chosen ciphertext attack, non adaptative)**:
accès à un oracle de déchiffrement avant l'attaque
 - ▶ **CCA2 (chosen ciphertext attack, adaptative)**:
accès à un oracle de déchiffrement tout le temps

Quelques attaques sans factoriser

- RSA est déterministe, donc **distinguishable** (non IND-CPA):

$c(\text{oui}), c(\text{non})$

Quelques attaques sans factoriser

- RSA est déterministe, donc **distingable** (non **IND-CPA**):

$c(\text{oui}), c(\text{non})$

- Attaque **CCA2** sur la sécurité élémentaire
- Attaque pour e petit et plusieurs destinataires

• Entrée

- ▶ $n > 2^{k+1}$, pour chiffrer jusqu'à k bits; exposant public e
- ▶ $k' = k - k_0 - k_1 > 0$
- ▶ $G : \{0, 1\}^{k_0} \rightarrow \{0, 1\}^{k-k_0}$
- ▶ $H : \{0, 1\}^{k-k_0} \rightarrow \{0, 1\}^{k_0}$
- ▶ $m \in \{0, 1\}^{k'}$

• Sortie: chiffré $c \in \{0, 1\}^k$

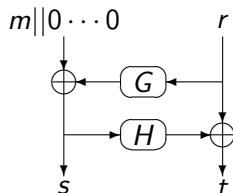
• Tirer aléatoirement $r \in \{0, 1\}^{k_0}$, puis calculer

$$s = (m || 0^{k_1}) \oplus G(r)$$

$$t = r \oplus H(s)$$

$$w = s || t$$

$$c = w^e$$



- 1 Petite histoire de la cryptologie: Les bons vieux temps
- 2 Diffie–Hellman: Le début des temps modernes
- 3 RSA: Le système d'aujourd'hui
- 4 Logarithmes discrets et factorisation: Un peu de cryptanalyse
- 5 ECC: Les systèmes de l'avenir

Paradoxe des anniversaires

- DLP: Étant donné $G = \langle g \rangle$ d'ordre n et $h \in G$, trouver x t.q. $h = g^x$
- Idée de l'algorithme (Pollard 1974)
 - ▶ calculer des $g^{a_i} h^{b_i}$
 - ▶ quand il y a une collision

$$\begin{aligned}g^{a_i} h^{b_i} &= g^{a_j} h^{b_j} \\g^{a_i - a_j} &= h^{b_j - b_i} \\&= g^{x(b_j - b_i)} \\x &= \frac{a_i - a_j}{b_j - b_i} \pmod{n}\end{aligned}$$

Paradoxe des anniversaires

- DLP: Étant donné $G = \langle g \rangle$ d'ordre n et $h \in G$, trouver x t.q. $h = g^x$
- Idée de l'algorithme (Pollard 1974)
 - ▶ calculer des $g^{a_i} h^{b_i}$
 - ▶ quand il y a une collision

$$\begin{aligned}g^{a_i} h^{b_i} &= g^{a_j} h^{b_j} \\g^{a_i - a_j} &= h^{b_j - b_i} \\&= g^{x(b_j - b_i)} \\x &= \frac{a_i - a_j}{b_j - b_i} \pmod{n}\end{aligned}$$

- ▶ Il y a une bonne chance de succès avec $O(\sqrt{n})$ éléments.

Paradoxe des anniversaires

- DLP: Étant donné $G = \langle g \rangle$ d'ordre n et $h \in G$, trouver x t.q. $h = g^x$
- Idée de l'algorithme (Pollard 1974)
 - ▶ calculer des $g^{a_i} h^{b_i}$
 - ▶ quand il y a une collision

$$\begin{aligned}g^{a_i} h^{b_i} &= g^{a_j} h^{b_j} \\g^{a_i - a_j} &= h^{b_j - b_i} \\&= g^{x(b_j - b_i)} \\x &= \frac{a_i - a_j}{b_j - b_i} \pmod{n}\end{aligned}$$

- ▶ Il y a une bonne chance de succès avec $O(\sqrt{n})$ éléments.
- astuces pratiques: parallélisable, sans mémoire

Restes chinois (Pohlig–Hellman 1978)

- DLP: Étant donné $G = \langle g \rangle$ d'ordre n et $h \in G$, trouver x t.q. $h = g^x$
- Idée pour n composé:

$$n = \prod p_i^{e_i}$$

Calculer des logs discrets dans des (sous-)groupes d'ordre p_i .

▶ Restes chinois

permettent de recoller les logs discrets dans les sous-groupes d'ordre $p_i^{e_i}$

▶ Argument à la relèvement de Hensel

permet de passer de p_i^{k-1} à p_i^k par un log discret dans le sous-groupe d'ordre p_i

▶ complexité totale: $\sim O(\sqrt{\max p_i})$

Condition nécessaire pour DLP difficile

n a un grand facteur premier p .

n a un grand facteur premier p .

Grand comment?

- chiffre symétrique RC5-64 cassé par recherche exhaustive, distribué sur Internet, en testant 2^{64} clefs
→ 2^{64} “opérations” faisables
- 2^{80} opérations considérées comme infaisables
- 2^{100} pour les paranos

$$p \approx 2^{160} \text{ à } 2^{200}$$

- Factorisation

RSA-768 (EPFL, NTT, Bonn Univ., INRIA, MSR, CWI 2010)

- DLP dans \mathbb{F}_p

530 bits (Kleinjung 2007)

- DLP dans \mathbb{F}_{2^m}

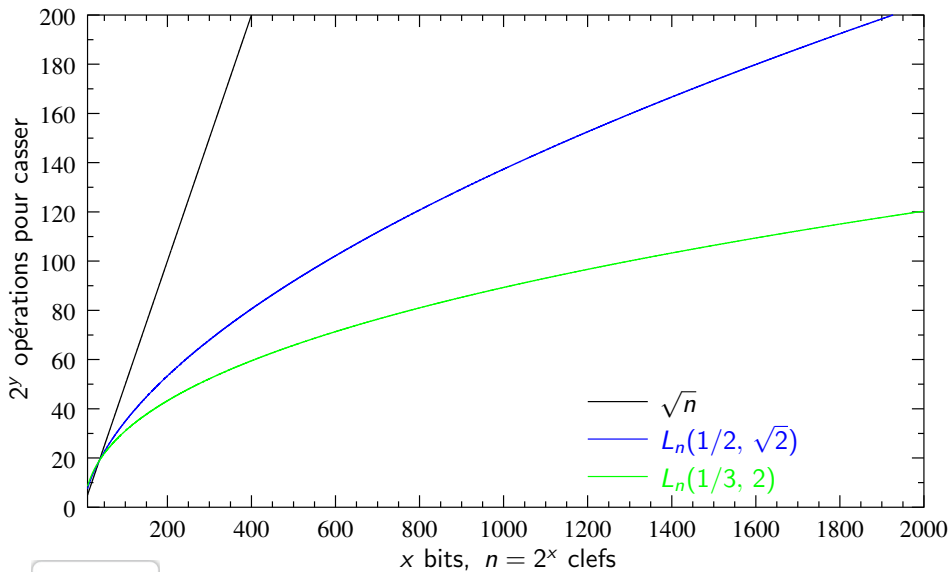
$m = 613$ (Joux–Lercier 2005)

- DLP dans une courbe elliptique

courbe sur \mathbb{F}_p : 109 bits (Monico et al. 2002)

courbe sur $\mathbb{F}_{2^{109}}$ (Monico et al. 2004)

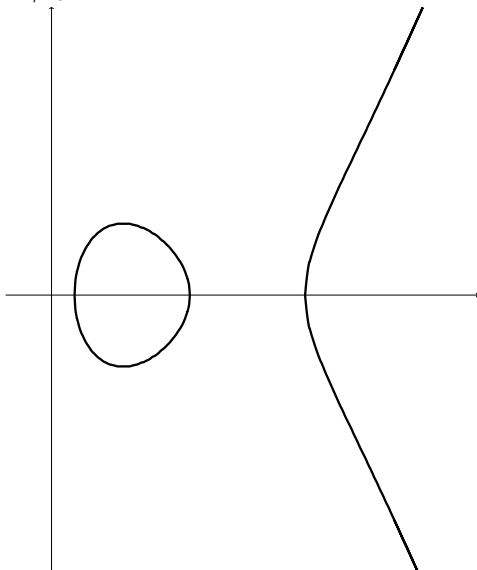
Tailles de clefs



- 1 Petite histoire de la cryptologie: Les bons vieux temps
- 2 Diffie–Hellman: Le début des temps modernes
- 3 RSA: Le système d'aujourd'hui
- 4 Logarithmes discrets et factorisation: Un peu de cryptanalyse
- 5 ECC: Les systèmes de l'avenir

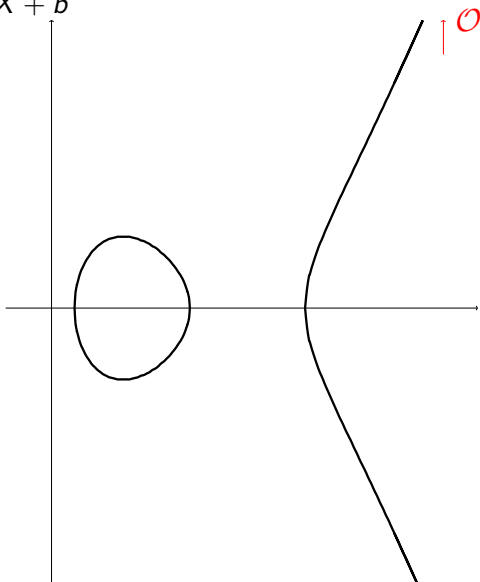
Courbes elliptiques

$$E : Y^2 = X^3 + aX + b$$

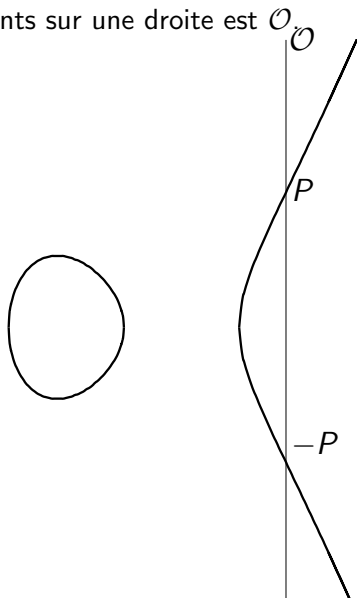


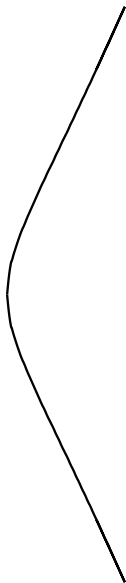
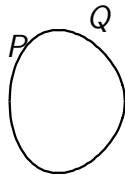
Courbes elliptiques

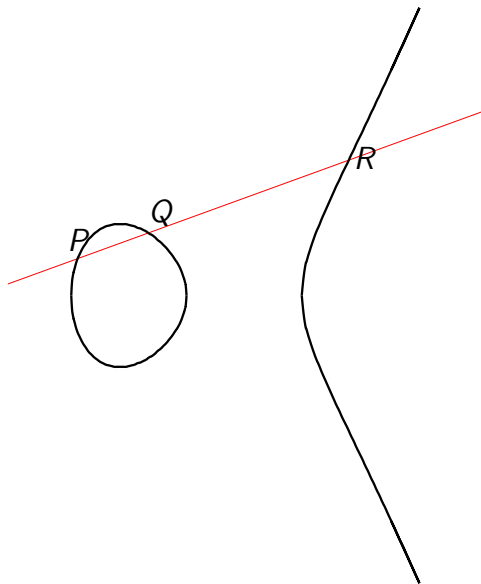
$$E : Y^2 = X^3 + aX + b$$

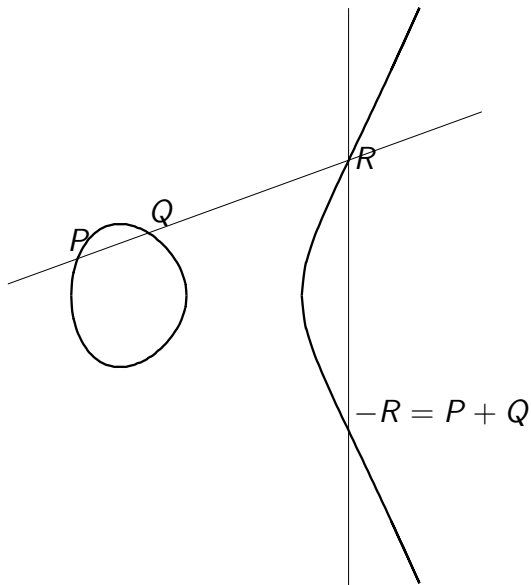


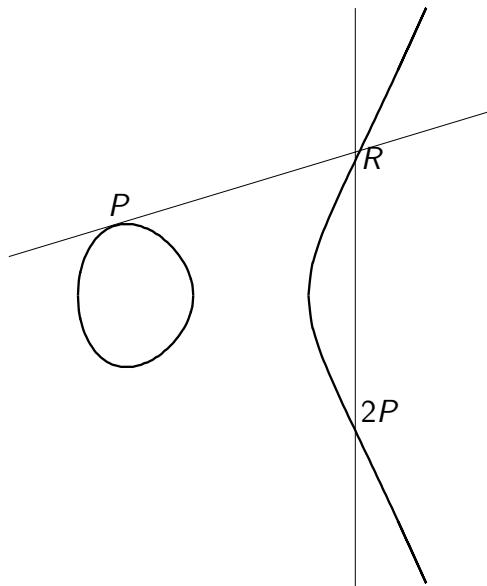
La somme de trois points sur une droite est \mathcal{O}











$$P = (x, y) \Rightarrow -P = (x, -y)$$

$$x_3 = \begin{cases} \left(\frac{y_2 - y_1}{x_2 - x_1} \right)^2 - x_1 - x_2 & \text{si } P_1 \neq P_2 \\ \left(\frac{3x_1^2 + a}{2y_1} \right)^2 - 2x_1 & \text{si } P_1 = P_2 \end{cases}$$

$$y_3 = \begin{cases} \frac{y_2 - y_1}{x_2 - x_1} (x_1 - x_3) - y_1 & \text{si } P_1 \neq P_2 \\ \frac{3x_1^2 + a}{2y_1} (x_1 - x_3) - y_1 & \text{si } P_1 = P_2 \end{cases}$$

Courbes elliptiques sur les corps finis

- Les points sur E/\mathbb{F}_q forment un groupe abélien fini.

Courbes elliptiques sur les corps finis

- Les points sur E/\mathbb{F}_q forment un groupe abélien fini.
- Théorème de Hasse

$$q + 1 - 2\sqrt{q} \leq \#E(\mathbb{F}_q) \leq q + 1 + 2\sqrt{q}$$

- Les points sur E/\mathbb{F}_q forment un groupe abélien fini.
- Théorème de Hasse

$$q + 1 - 2\sqrt{q} \leq \#E(\mathbb{F}_q) \leq q + 1 + 2\sqrt{q}$$

- Points sont représentés par $\lceil \log_2 q \rceil + 1$ bits:
 - ▶ coordonnée X
 - ▶ un bit pour choisir la bonne racine de $X^3 + aX + b$ comme Y

- loi de groupe
- trouver des courbes à cardinal (presque) premier
- calculer des logarithmes discrets

- Blackberry (Research in Motion; source: H. Little)

	ECC 256	RSA 3072	DH 3072
génération de clefs	166 ms	trop long	38 s
chiffrement	150 ms	52 ms	74 s
déchiffrement	168 ms	8 s	74 s



- Timbres numériques



- OpenSSL
- Digital Rights Management (Windows Media Player 7.0)