La méthode RSA et la cryptographie fondée sur les courbes elliptiques

Andreas Enge

Centre d'Alembert

Orsay, 1er mars 2006

enge@lix.polytechnique.fr

http://www.lix.polytechnique.fr/Labo/Andreas.Enge

INRIA Futurs & Laboratoire d'Informatique (LIX)
École polytechnique
France

RSA et ECC

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

Papier et crayon — substitutions

- 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	l	i	e
+	c	l	e	f	c	l	e	f	c	l	e	f	c	l	e	f
	L	P	X	F	K	X	H	F	N	L	I	T	N	W	M	I

Papier et crayon — Transpositions

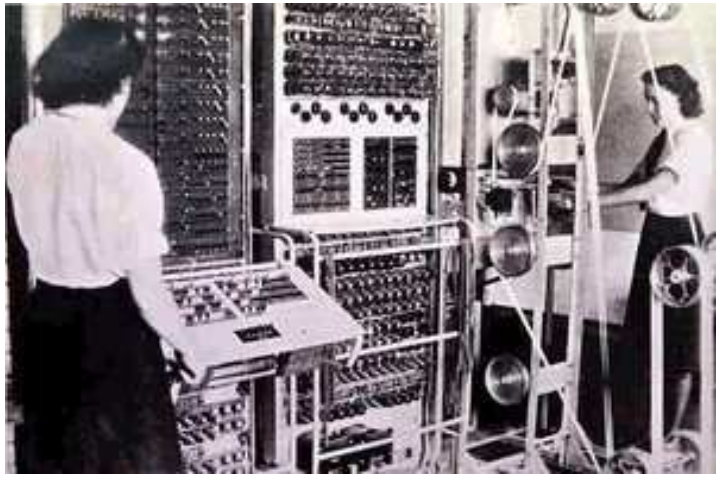
3	2	5	1	4
c	e	c	i	e
s	t	u	n	m
e	s	s	a	g
e	a	r	c	h
i	s	e	c	r
e	t			

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



RSA et ECC

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

Échange de clefs à la Diffie–Hellman (1976)

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

Chiffrement ElGamal (1985)

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

	Alice	Bob
clef privée		$b \in_R [0, n-1]$
clef publique		g^b
"clef privée" éphémère	$r \in_R [0, n-1]$	
"clef publique" éph.	g^r	
chiffrement	$c = (c', c'') = (g^r, m(g^b)^r)$	
	$\longrightarrow$	
déchiffrement		$m = c''/(c')^b$

Problèmes calculatoires sous-jacentes à la sécurité

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

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	$(g^e)^a$	$=$	$(g^a)^e$		
			$(g^b)^e$	$=$	$(g^e)^b$

RSA et ECC

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

Petit théorème de Fermat

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

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

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

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

$$a^m = 1 \bmod p$$

- Preuve rapide:

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

- Preuve lente:

$$\begin{aligned} a^{p-1} &= 1 + \ell p \\ (a^{p-1})^k &= (1+\ell p)^k = 1 + k\,\ell p + \binom{k}{2} (\ell p)^2 + \cdots + (\ell p)^k = 1 \bmod p \end{aligned}$$

Fermat chinois

- Généralisation pour des modules composés
  - p et q premiers, $N = pq$
  - $\lambda = \mathrm{ppcm}(p-1, q-1)$
  - a un entier (non divisible par p et q)

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

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

- Corollaire: Pour λ qui divise m, on a

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

Chiffrement RSA (1978)

	Alice	Bob
clef publique		N, e premier avec N
clef privée		$N = pq$, $d = e^{-1} \bmod \lambda$
chiffrement	$c = m^e \bmod N$	
	$\longrightarrow$	
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 $\Longrightarrow$ clefs privées
- Problème RSA (RSAP) = calcul de racines modulo N composé:
  Étant donnés N, e et m^e, trouver m
- Solution à RSAP $\Longrightarrow$
  - déchiffrement de textes un à un
  - forgeage de signatures une à une
- FP $\Longrightarrow$ RSAP
  $\Longleftarrow$ probablement faux pour petits exposants (LE-RSAP)

Boneh–Venkatesan 1998

Un algorithme algébrique pour factoriser en résolvant quelques RSAP avec petit e

peut être transformé de façon polynomiale en un algorithme pour factoriser sans résoudre des LE-RSAP.

Modulo quelques restrictions:

- Si LE-RSAP et FP sont polynomialement équivalentes,
- alors il y a un algorithme polynomial pour la factorisation utilisant un nombre polynomial de solutions à LE-RSA,
- alors FP peut être résolu en temps polynomial.

Modèles de sécurité

- Buts d'un attaquant
  - déchiffrer un texte clair inconnu (sécurité élémentaire)
  - dinstinguer 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 distingable (non IND-CPA):

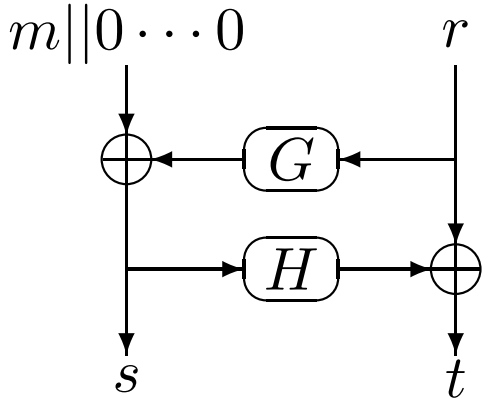
$$c(\text{oui}), c(\text{non})$$

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

RSA-OAEP — une version sûre de RSA

- Entrée
  - $n > 2^{k+1}$, pour chiffrer jusqu'à k bits; exposant public e
  - $k' = k - k_0 - k_1 > 0$
  - $G : \{0,1\}^{k_0} \to \{0,1\}^{k-k_0}$
  - $H : \{0,1\}^{k-k_0} \to \{0,1\}^{k_0}$
  - $m \in \{0,1\}^{k'}$
- Sortie: chiffré $c \in \{0,1\}^k$
- tirer aléatoirement $r \in \{0,1\}^{k_0}$, puis calculer

$$\begin{aligned} s &= (m||0^{k_1}) \oplus G(r) \\ t &= r \oplus H(s) \\ w &= s||t \\ c &= w^e \end{aligned}$$



RSA-OAEP — une version sûre de RSA!

- OAEP proposé en 1994 par Bellare et Rogaway non seulement pour RSA, mais toute fonction à sens unique avec trappe
avec preuve de IND-CCA (1 ou 2?)
- Problèmes avec la preuve sont découvertes, par ex. par Shoup en 2001
- Fujisaki, Okamoto, Pointcheval et Stern montrent IND-CCA2 pour RSA-OAEP in 2001:

> Une attaque IND-CCA2 est polynomialement équivalente à résoudre le problème RSA.

RSA et ECC

1. Petite histoire de la cryptologie,
   ou Les bons vieux temps
2. Diffie–Hellman,
   ou Le début de l'âge moderne
3. RSA,
   ou Le système d'aujourd'hui
4. Logarithmes discrets et factorisation,
   ou Un peu de cryptanalyse
5. ECC,
   ou 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

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

  - 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.

Grand comment?

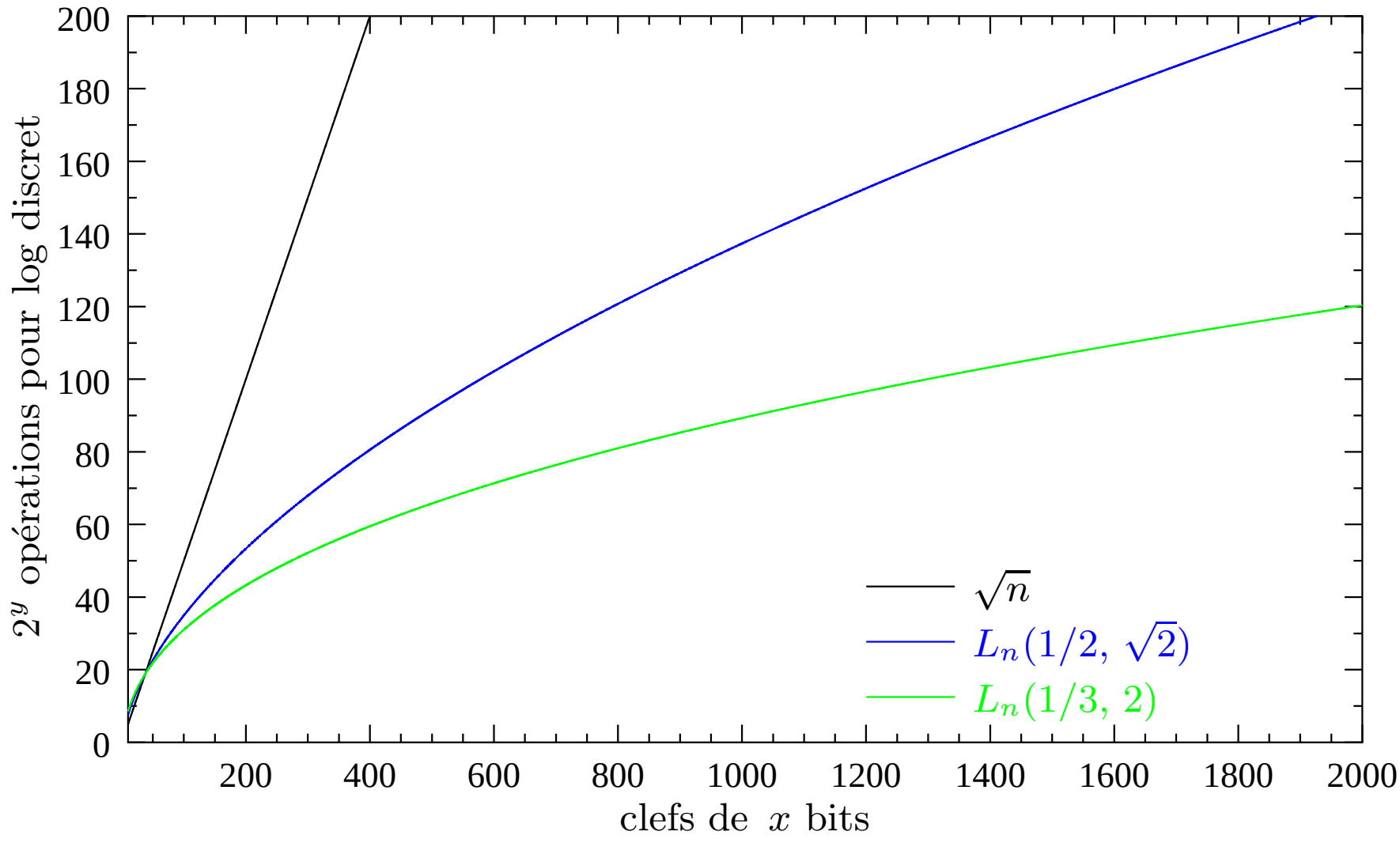
- chiffre symétrique RC5-64 cassé par recherche exhaustive, distribué sur Internet, en testant 2^{64} clefs
  $\longrightarrow$ 2^{64} “opérations” faisables
- 2^{80} opérations considérées comme infaisables
- 2^{100} pour les paranos

$p \approx 2^{160}$ à 2^{200}

Records

- Factorisation
  RSA-663 (Bar, Böhm, Franke, Kleinjung 2005)
- DLP dans $\mathbb{F}_p$
  397 bits (Joux–Lercier 2001)
- DLP dans $\mathbb{F}_{2^m}$
  $m = 607$ (Thomé 2002)
- DLP dans une courbe elliptique
  courbe de Koblitz sur $\mathbb{F}_{2^{108}}$ (Harley et al. 2000)
  courbe sur $\mathbb{F}_p$: 97 bits (1998)

Tailles de clefs

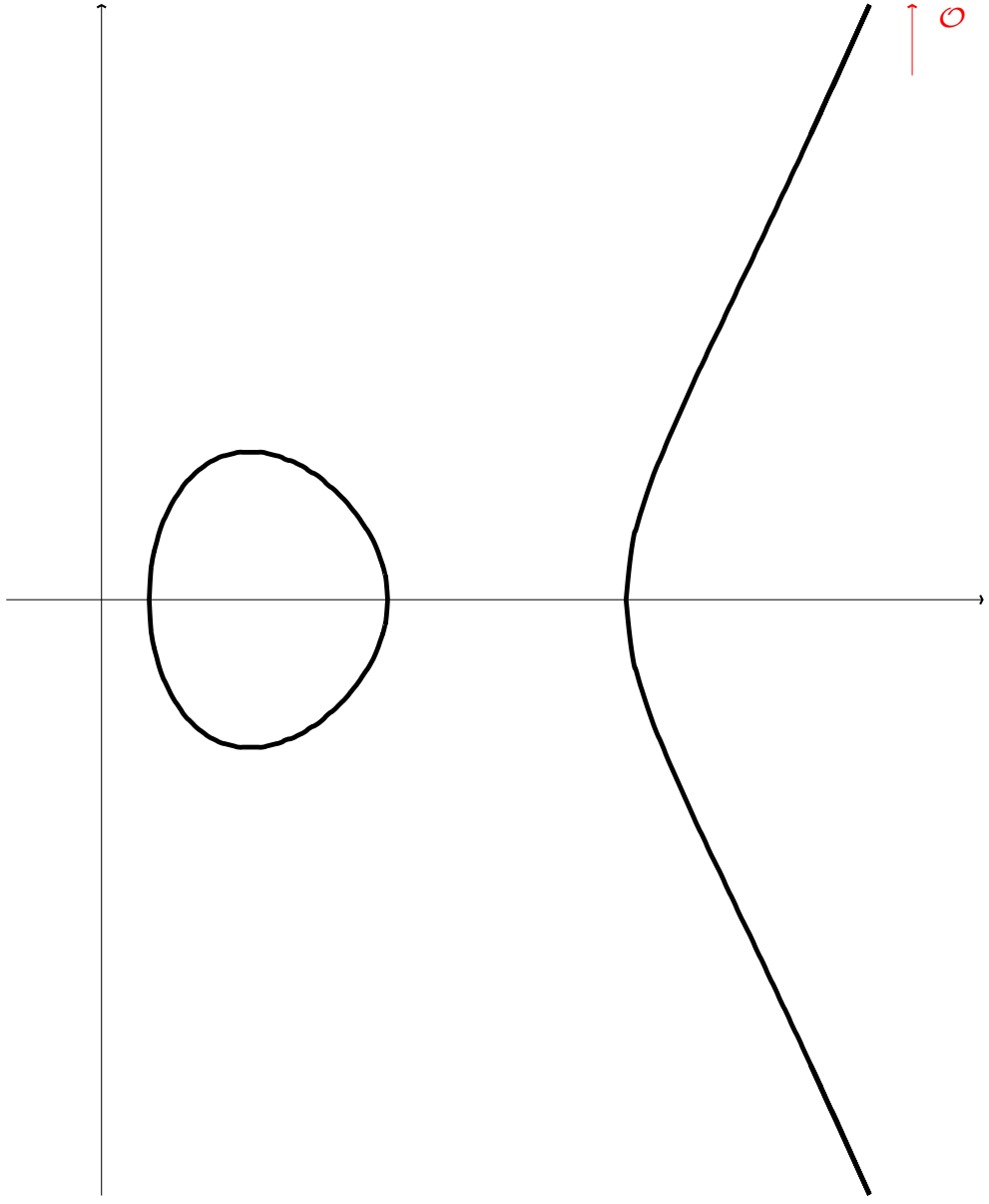


RSA et ECC

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

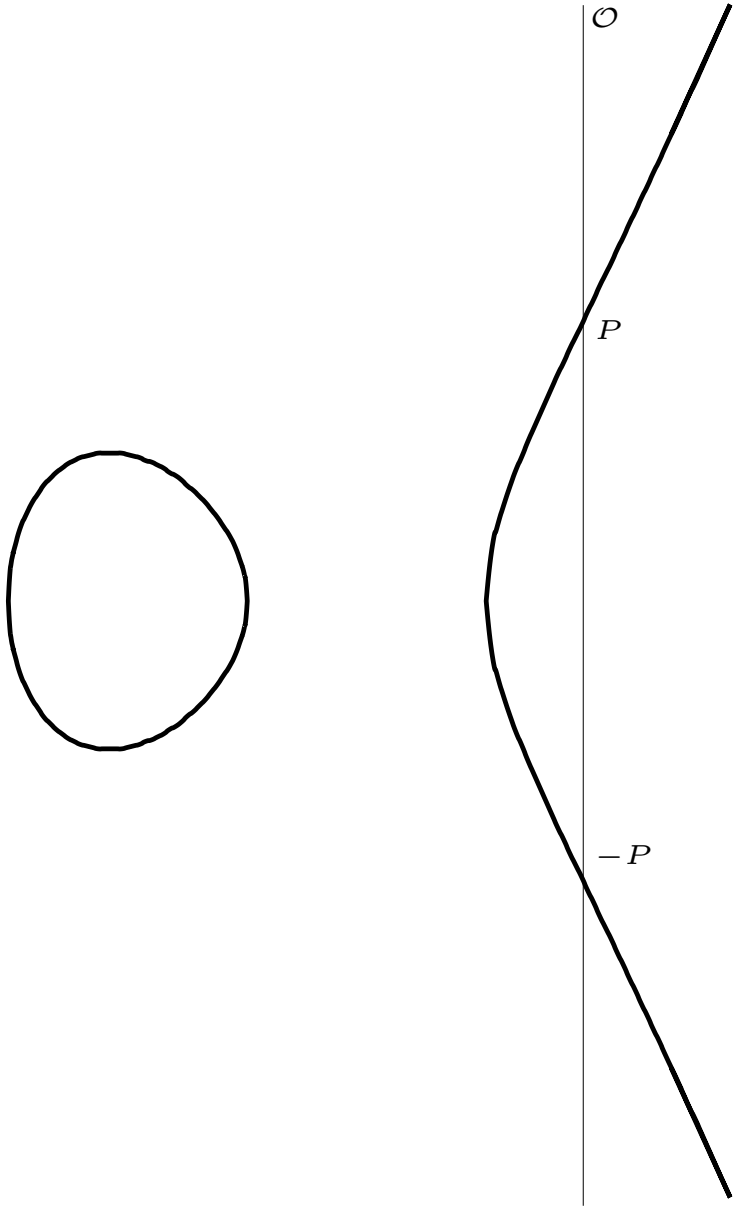
Courbes elliptiques

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

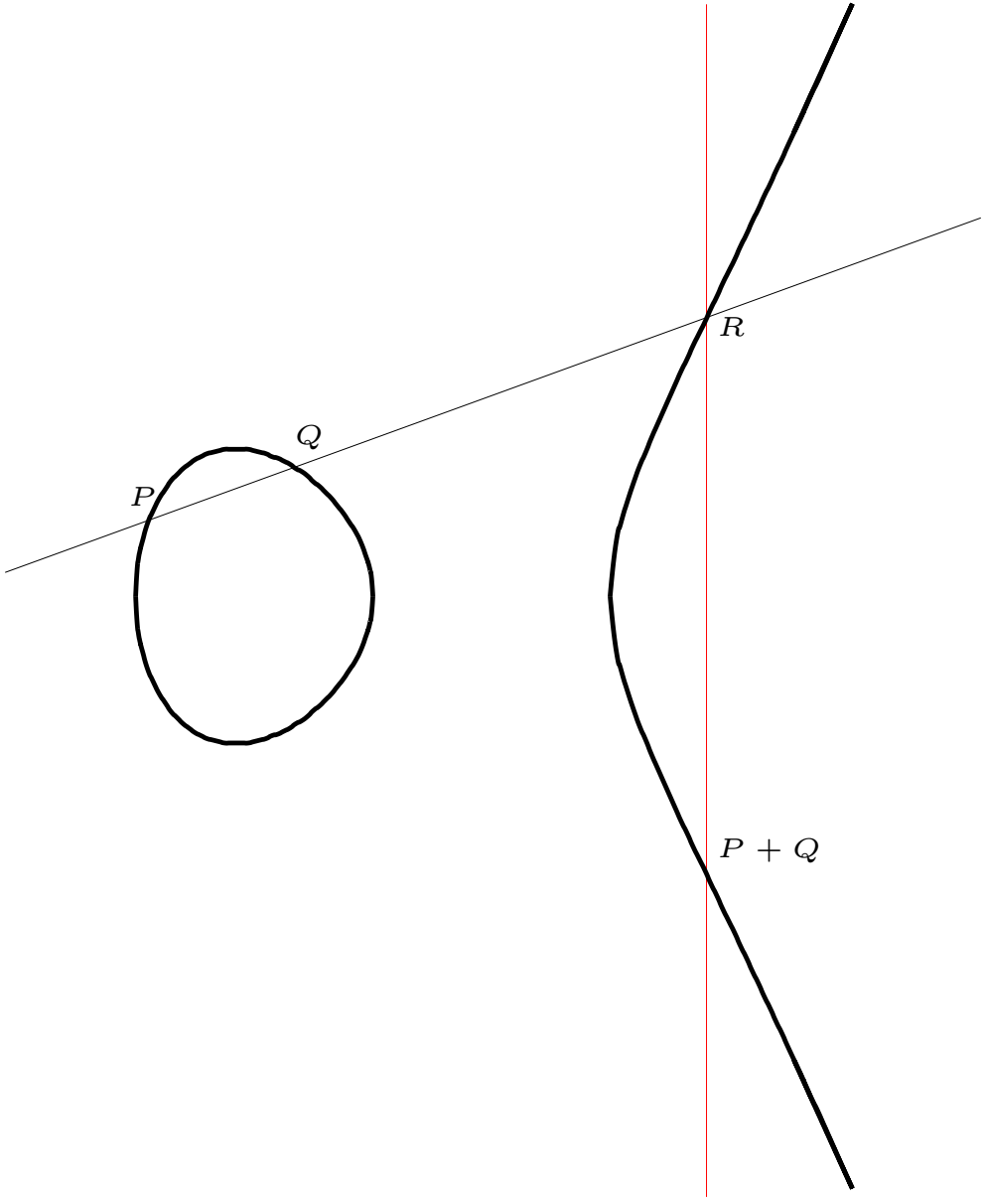


Inverse

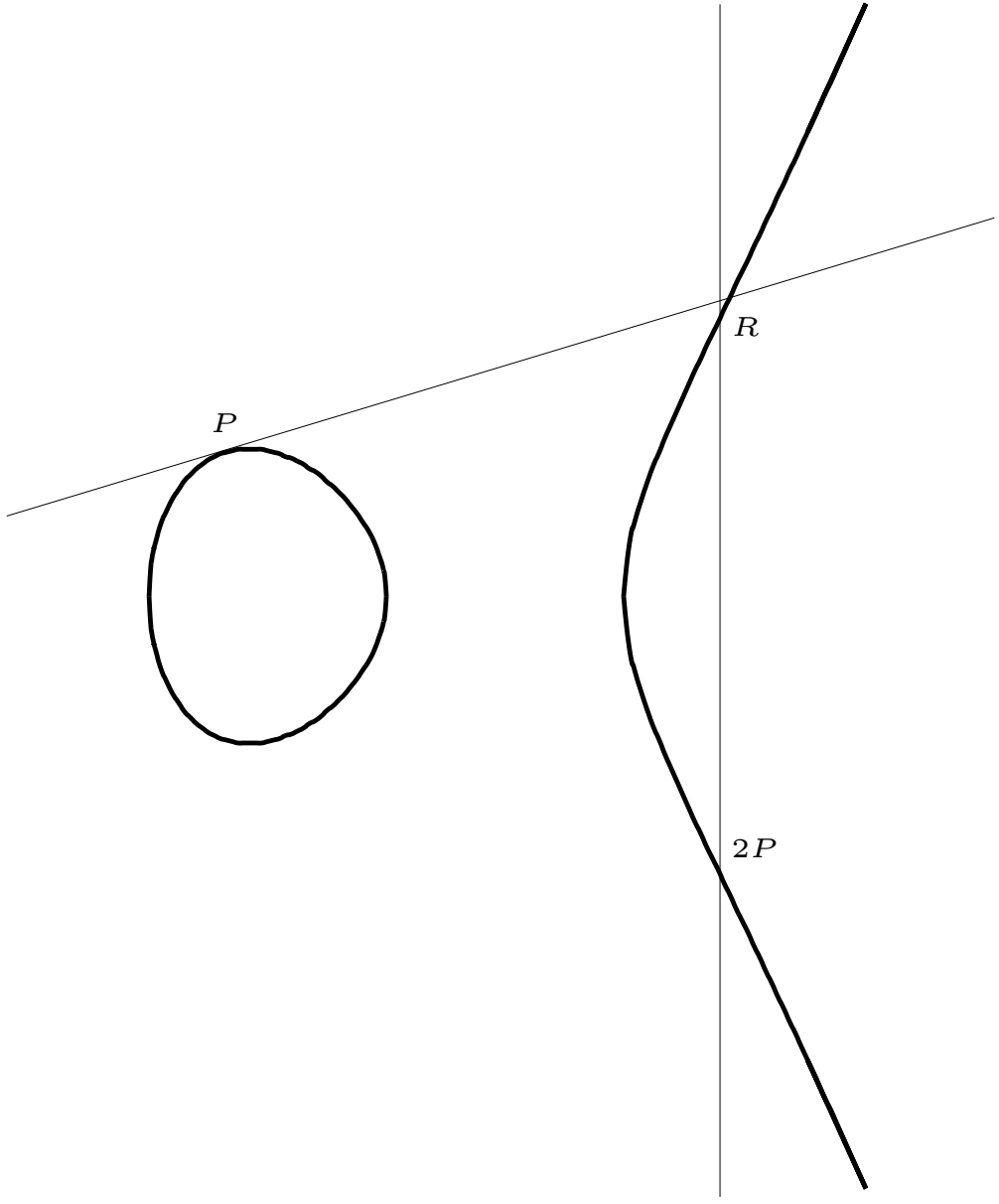
La somme de trois points sur une droite est $\mathcal{O}$.



Addition



Doublement



Formule d'inversion

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

Formules d'addition

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

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

Courbes elliptiques sur les corps finis

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

Algorithmique

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

Utilisations

- 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)