

# Cours crypto

## Ouverture: Courbes elliptiques etc.

Laurent Fousse

December 1, 2008

# Outline

- 1 Courbes elliptiques
- 2 Off-The-Record
- 3 Anonymat
- 4 PIR

# Rappel Diffie-Hellman

## Rappel Diffie-Hellman

- Premier  $p$  et  $g$  générateur du groupe multiplicatif  $(\mathbb{Z}/p\mathbb{Z})^*$ .

## Rappel Diffie-Hellman

- Premier  $p$  et  $g$  générateur du groupe multiplicatif  $(\mathbb{Z}/p\mathbb{Z})^*$ .
- Alice choisit  $a$  entier au hasard,  $0 \leq a \leq p - 1$ .

## Rappel Diffie-Hellman

- Premier  $p$  et  $g$  générateur du groupe multiplicatif  $(\mathbb{Z}/p\mathbb{Z})^*$ .
- Alice choisit  $a$  entier au hasard,  $0 \leq a \leq p - 1$ .
- Bob choisit  $b$  entier au hasard,  $0 \leq b \leq p - 1$ .

## Rappel Diffie-Hellman

- Premier  $p$  et  $g$  générateur du groupe multiplicatif  $(\mathbb{Z}/p\mathbb{Z})^*$ .
- Alice choisit  $a$  entier au hasard,  $0 \leq a \leq p - 1$ .
- Bob choisit  $b$  entier au hasard,  $0 \leq b \leq p - 1$ .
- Alice transmet  $g^a \bmod p$  à Bob.

## Rappel Diffie-Hellman

- Premier  $p$  et  $g$  générateur du groupe multiplicatif  $(\mathbb{Z}/p\mathbb{Z})^*$ .
- Alice choisit  $a$  entier au hasard,  $0 \leq a \leq p - 1$ .
- Bob choisit  $b$  entier au hasard,  $0 \leq b \leq p - 1$ .
- Alice transmet  $g^a \bmod p$  à Bob.
- Bob transmet  $g^b \bmod p$  à Alice.

## Rappel Diffie-Hellman

- Premier  $p$  et  $g$  générateur du groupe multiplicatif  $(\mathbb{Z}/p\mathbb{Z})^*$ .
- Alice choisit  $a$  entier au hasard,  $0 \leq a \leq p - 1$ .
- Bob choisit  $b$  entier au hasard,  $0 \leq b \leq p - 1$ .
- Alice transmet  $g^a \bmod p$  à Bob.
- Bob transmet  $g^b \bmod p$  à Alice.
- Alice calcule  $(g^b)^a = g^{ab}$ .

## Rappel Diffie-Hellman

- Premier  $p$  et  $g$  générateur du groupe multiplicatif  $(\mathbb{Z}/p\mathbb{Z})^*$ .
- Alice choisit  $a$  entier au hasard,  $0 \leq a \leq p - 1$ .
- Bob choisit  $b$  entier au hasard,  $0 \leq b \leq p - 1$ .
- Alice transmet  $g^a \bmod p$  à Bob.
- Bob transmet  $g^b \bmod p$  à Alice.
- Alice calcule  $(g^b)^a = g^{ab}$ .
- Bob calcule  $(g^a)^b = g^{ab}$ .

## Rappel Diffie-Hellman

- Premier  $p$  et  $g$  générateur du groupe multiplicatif  $(\mathbb{Z}/p\mathbb{Z})^*$ .
- Alice choisit  $a$  entier au hasard,  $0 \leq a \leq p - 1$ .
- Bob choisit  $b$  entier au hasard,  $0 \leq b \leq p - 1$ .
- Alice transmet  $g^a \bmod p$  à Bob.
- Bob transmet  $g^b \bmod p$  à Alice.
- Alice calcule  $(g^b)^a = g^{ab}$ .
- Bob calcule  $(g^a)^b = g^{ab}$ .

Sécurité:

- Connaissant  $g$  et  $g^a$  il est dur de trouver  $a$ .

# Rappel Diffie-Hellman

- Premier  $p$  et  $g$  générateur du groupe multiplicatif  $(\mathbb{Z}/p\mathbb{Z})^*$ .
- Alice choisit  $a$  entier au hasard,  $0 \leq a \leq p - 1$ .
- Bob choisit  $b$  entier au hasard,  $0 \leq b \leq p - 1$ .
- Alice transmet  $g^a \bmod p$  à Bob.
- Bob transmet  $g^b \bmod p$  à Alice.
- Alice calcule  $(g^b)^a = g^{ab}$ .
- Bob calcule  $(g^a)^b = g^{ab}$ .

## Sécurité:

- Connaissant  $g$  et  $g^a$  il est dur de trouver  $a$ .
- Connaissant  $g$  et  $g^b$  il est dur de trouver  $b$ .

## Rappel Diffie-Hellman

- Premier  $p$  et  $g$  générateur du groupe multiplicatif  $(\mathbb{Z}/p\mathbb{Z})^*$ .
- Alice choisit  $a$  entier au hasard,  $0 \leq a \leq p - 1$ .
- Bob choisit  $b$  entier au hasard,  $0 \leq b \leq p - 1$ .
- Alice transmet  $g^a \bmod p$  à Bob.
- Bob transmet  $g^b \bmod p$  à Alice.
- Alice calcule  $(g^b)^a = g^{ab}$ .
- Bob calcule  $(g^a)^b = g^{ab}$ .

### Sécurité:

- Connaissant  $g$  et  $g^a$  il est dur de trouver  $a$ .
- Connaissant  $g$  et  $g^b$  il est dur de trouver  $b$ .
- Connaissant  $g$ ,  $g^a$  et  $g^b$  il est dur de trouver  $g^{ab}$ .

## Diffie-Hellman: dans un groupe «générique»

- Groupe  $G$  de générateur  $g$  et d'ordre  $n$ .

## Diffie-Hellman: dans un groupe «générique»

- Groupe  $G$  de générateur  $g$  et d'ordre  $n$ .
- Alice choisit  $a$  entier au hasard,  $0 \leq a \leq n - 1$ .

## Diffie-Hellman: dans un groupe «générique»

- Groupe  $G$  de générateur  $g$  et d'ordre  $n$ .
- Alice choisit  $a$  entier au hasard,  $0 \leq a \leq n - 1$ .
- Bob choisit  $b$  entier au hasard,  $0 \leq b \leq n - 1$ .

## Diffie-Hellman: dans un groupe «générique»

- Groupe  $G$  de générateur  $g$  et d'ordre  $n$ .
- Alice choisit  $a$  entier au hasard,  $0 \leq a \leq n - 1$ .
- Bob choisit  $b$  entier au hasard,  $0 \leq b \leq n - 1$ .
- Alice transmet  $g^a$  à Bob.

## Diffie-Hellman: dans un groupe «générique»

- Groupe  $G$  de générateur  $g$  et d'ordre  $n$ .
- Alice choisit  $a$  entier au hasard,  $0 \leq a \leq n - 1$ .
- Bob choisit  $b$  entier au hasard,  $0 \leq b \leq n - 1$ .
- Alice transmet  $g^a$  à Bob.
- Bob transmet  $g^b$  à Alice.

## Diffie-Hellman: dans un groupe «générique»

- Groupe  $G$  de générateur  $g$  et d'ordre  $n$ .
- Alice choisit  $a$  entier au hasard,  $0 \leq a \leq n - 1$ .
- Bob choisit  $b$  entier au hasard,  $0 \leq b \leq n - 1$ .
- Alice transmet  $g^a$  à Bob.
- Bob transmet  $g^b$  à Alice.
- Alice calcule  $(g^b)^a = g^{ab}$ .

## Diffie-Hellman: dans un groupe «générique»

- Groupe  $G$  de générateur  $g$  et d'ordre  $n$ .
- Alice choisit  $a$  entier au hasard,  $0 \leq a \leq n - 1$ .
- Bob choisit  $b$  entier au hasard,  $0 \leq b \leq n - 1$ .
- Alice transmet  $g^a$  à Bob.
- Bob transmet  $g^b$  à Alice.
- Alice calcule  $(g^b)^a = g^{ab}$ .
- Bob calcule  $(g^a)^b = g^{ab}$ .

## Diffie-Hellman: dans un groupe «générique»

- Groupe  $G$  de générateur  $g$  et d'ordre  $n$ .
- Alice choisit  $a$  entier au hasard,  $0 \leq a \leq n - 1$ .
- Bob choisit  $b$  entier au hasard,  $0 \leq b \leq n - 1$ .
- Alice transmet  $g^a$  à Bob.
- Bob transmet  $g^b$  à Alice.
- Alice calcule  $(g^b)^a = g^{ab}$ .
- Bob calcule  $(g^a)^b = g^{ab}$ .

Sécurité:

- Connaissant  $g$  et  $g^a$  il est dur de trouver  $a$ .

## Diffie-Hellman: dans un groupe «générique»

- Groupe  $G$  de générateur  $g$  et d'ordre  $n$ .
- Alice choisit  $a$  entier au hasard,  $0 \leq a \leq n - 1$ .
- Bob choisit  $b$  entier au hasard,  $0 \leq b \leq n - 1$ .
- Alice transmet  $g^a$  à Bob.
- Bob transmet  $g^b$  à Alice.
- Alice calcule  $(g^b)^a = g^{ab}$ .
- Bob calcule  $(g^a)^b = g^{ab}$ .

Sécurité:

- Connaissant  $g$  et  $g^a$  il est dur de trouver  $a$ .
- Connaissant  $g$  et  $g^b$  il est dur de trouver  $b$ .

## Diffie-Hellman: dans un groupe «générique»

- Groupe  $G$  de générateur  $g$  et d'ordre  $n$ .
- Alice choisit  $a$  entier au hasard,  $0 \leq a \leq n - 1$ .
- Bob choisit  $b$  entier au hasard,  $0 \leq b \leq n - 1$ .
- Alice transmet  $g^a$  à Bob.
- Bob transmet  $g^b$  à Alice.
- Alice calcule  $(g^b)^a = g^{ab}$ .
- Bob calcule  $(g^a)^b = g^{ab}$ .

### Sécurité:

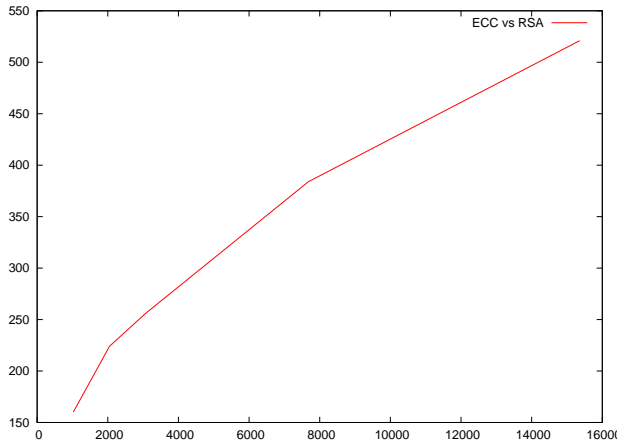
- Connaissant  $g$  et  $g^a$  il est dur de trouver  $a$ .
- Connaissant  $g$  et  $g^b$  il est dur de trouver  $b$ .
- Connaissant  $g$ ,  $g^a$  et  $g^b$  il est dur de trouver  $g^{ab}$ .

# Sécurité des courbes elliptiques

Taille recommandée des clefs:

Symmetric	RSA and Diffie-Hellman	Elliptic Curve
80	1024	160
112	2048	224
128	3072	256
192	7680	384
256	15360	521

# Sécurité des courbes elliptiques



# Sécurité des courbes elliptiques

Meilleure attaque contre les courbes par "Baby steps/Giant steps".

Exemple de problème du logarithme discret

$$g = 3, p = 17$$

Trouver  $a$  tel que  $g^a = 5$ .

# Présentation des courbes elliptiques

Sur un corps fini  $K$  de caractéristique  $> 3$ :

$$E_{a,b} = \{(x, y) \in K^2; y^2 = x^3 + ax + b\}$$

où  $4a^3 + 27b^2 \neq 0$ .

# Présentation des courbes elliptiques

Sur un corps fini  $K$  de caractéristique  $> 3$ :

$$E_{a,b} = \{(x, y) \in K^2; y^2 = x^3 + ax + b\}$$

où  $4a^3 + 27b^2 \neq 0$ .

$$P = (x, y) \in E_{a,b} \iff y^2 = x^3 + ax + b$$

Exemple:  $P = (8, 26)$  et  $E_{1,1}$  et  $K = \mathbb{F}_{31}$ .

# Présentation des courbes elliptiques

Sur un corps fini  $K$  de caractéristique  $> 3$ :

$$E_{a,b} = \{(x, y) \in K^2; y^2 = x^3 + ax + b\}$$

où  $4a^3 + 27b^2 \neq 0$ .

$$P = (x, y) \in E_{a,b} \iff y^2 = x^3 + ax + b$$

Exemple:  $P = (8, 26)$  et  $E_{1,1}$  et  $K = \mathbb{F}_{31}$ .

$$y^2 = 26^2 = 676 = 25$$

# Présentation des courbes elliptiques

Sur un corps fini  $K$  de caractéristique  $> 3$ :

$$E_{a,b} = \{(x, y) \in K^2; y^2 = x^3 + ax + b\}$$

où  $4a^3 + 27b^2 \neq 0$ .

$$P = (x, y) \in E_{a,b} \iff y^2 = x^3 + ax + b$$

Exemple:  $P = (8, 26)$  et  $E_{1,1}$  et  $K = \mathbb{F}_{31}$ .

$$\begin{aligned} y^2 = 26^2 &= 676 = 25 \\ x^3 + x + 1 = 8^3 + 8 + 1 &= 521 = 25 \end{aligned}$$

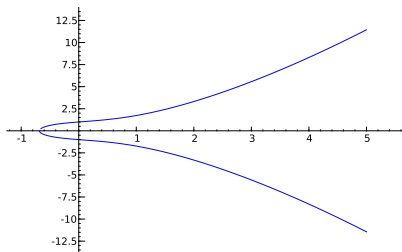
# Présentation des courbes elliptiques

## Cardinal d'une courbe (Hasse)

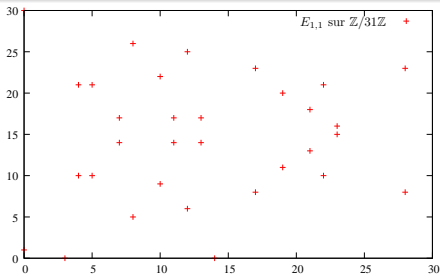
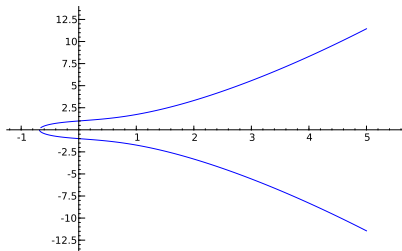
Une courbe  $E$  définie sur un corps fini  $\mathbb{F}_q$  vérifie:

$$|\#E - q - 1| \leq 2\sqrt{q}$$

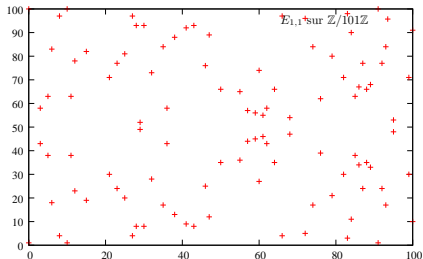
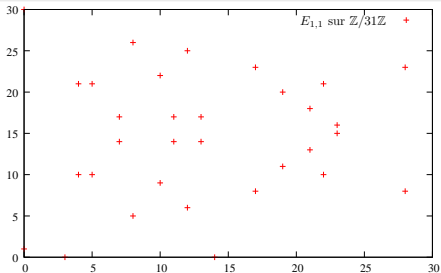
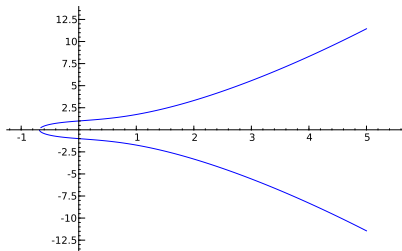
# Présentation des courbes elliptiques: $y^2 = x^3 + x + 1$



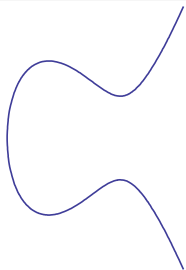
# Présentation des courbes elliptiques: $y^2 = x^3 + x + 1$



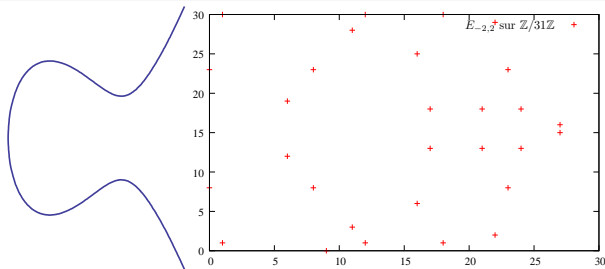
# Présentation des courbes elliptiques: $y^2 = x^3 + x + 1$



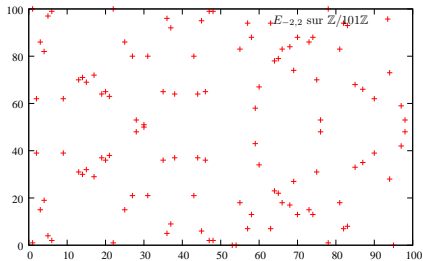
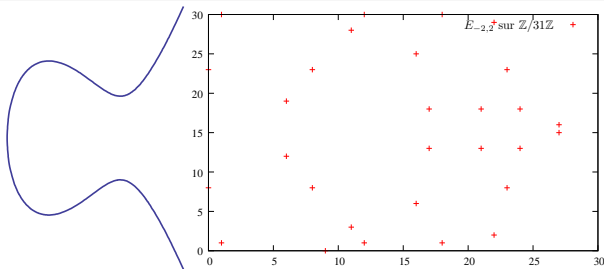
# Présentation des courbes elliptiques: $y^2 = x^3 - 2x + 2$



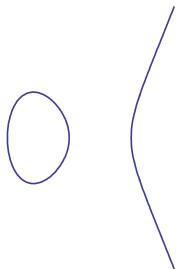
# Présentation des courbes elliptiques: $y^2 = x^3 - 2x + 2$



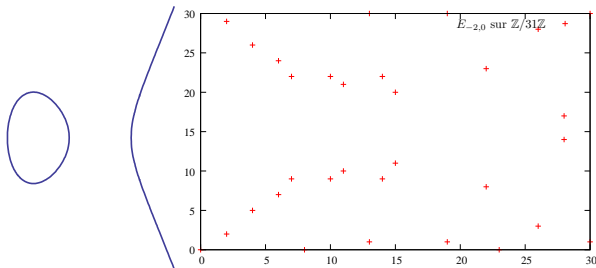
# Présentation des courbes elliptiques: $y^2 = x^3 - 2x + 2$



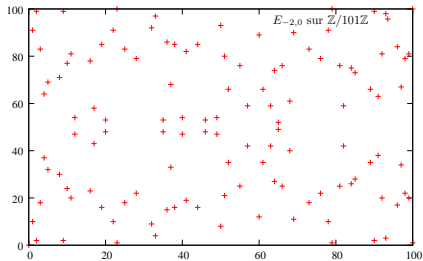
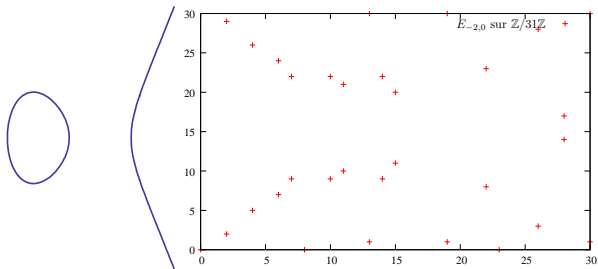
# Présentation des courbes elliptiques: $y^2 = x^3 - 2x$



# Présentation des courbes elliptiques: $y^2 = x^3 - 2x$

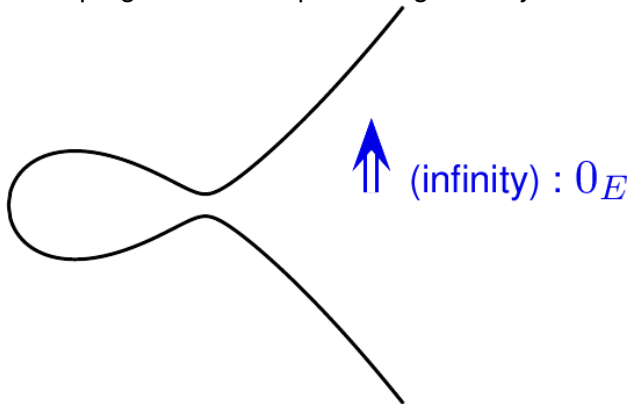


# Présentation des courbes elliptiques: $y^2 = x^3 - 2x$



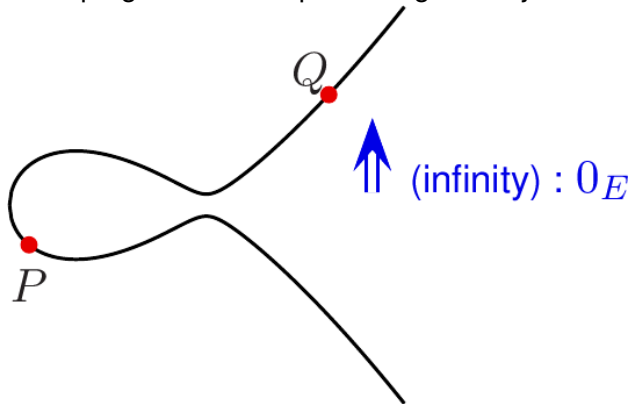
# Opérations sur les courbes

Principe général: trois points alignés s'ajoutent à zéro.



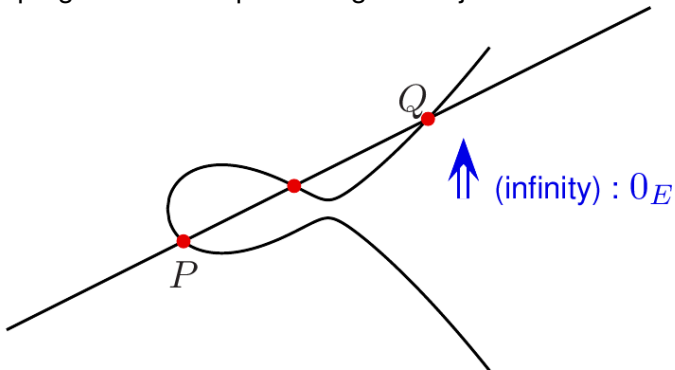
# Opérations sur les courbes

Principe général: trois points alignés s'ajoutent à zéro.



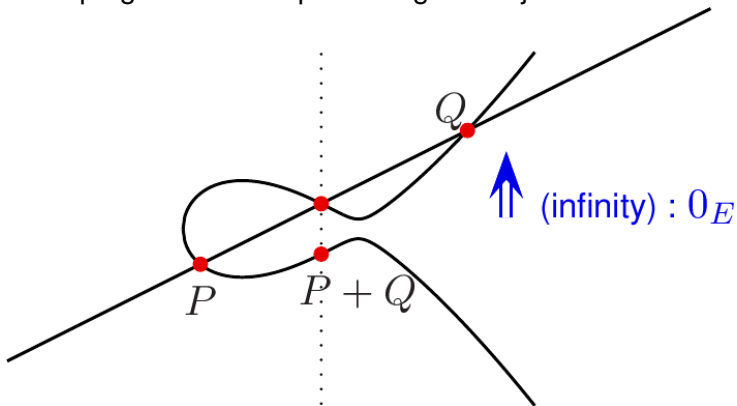
# Opérations sur les courbes

Principe général: trois points alignés s'ajoutent à zéro.



# Opérations sur les courbes

Principe général: trois points alignés s'ajoutent à zéro.



## Opérations sur les courbes: les formules

Soient  $P = (x_1, y_1)$  et  $Q = (x_2, y_2)$  deux points sur la courbe.

## Opérations sur les courbes: les formules

Soient  $P = (x_1, y_1)$  et  $Q = (x_2, y_2)$  deux points sur la courbe.

$$-P = (x_1, -y_1)$$

## Opérations sur les courbes: les formules

Soient  $P = (x_1, y_1)$  et  $Q = (x_2, y_2)$  deux points sur la courbe.

$$-P = (x_1, -y_1)$$

$$\lambda = \frac{y_2 - y_1}{x_2 - x_1} \text{ si } x_1 \neq x_2$$

$$\lambda = \frac{3x_1^2 + a}{2y_1} \text{ sinon}$$

## Opérations sur les courbes: les formules

Soient  $P = (x_1, y_1)$  et  $Q = (x_2, y_2)$  deux points sur la courbe.

$$-P = (x_1, -y_1)$$

$$\lambda = \frac{y_2 - y_1}{x_2 - x_1} \text{ si } x_1 \neq x_2$$

$$\lambda = \frac{3x_1^2 + a}{2y_1} \text{ sinon}$$

$$x_3 = \lambda^2 - x_1 - x_2$$

## Opérations sur les courbes: les formules

Soient  $P = (x_1, y_1)$  et  $Q = (x_2, y_2)$  deux points sur la courbe.

$$-P = (x_1, -y_1)$$

$$\lambda = \frac{y_2 - y_1}{x_2 - x_1} \text{ si } x_1 \neq x_2$$

$$\lambda = \frac{3x_1^2 + a}{2y_1} \text{ sinon}$$

$$x_3 = \lambda^2 - x_1 - x_2$$

$$y_3 = (x_1 - x_3)\lambda - y_1$$

## Opérations sur les courbes: les formules

Soient  $P = (x_1, y_1)$  et  $Q = (x_2, y_2)$  deux points sur la courbe.

$$-P = (x_1, -y_1)$$

$$\lambda = \frac{y_2 - y_1}{x_2 - x_1} \text{ si } x_1 \neq x_2$$

$$\lambda = \frac{3x_1^2 + a}{2y_1} \text{ sinon}$$

$$x_3 = \lambda^2 - x_1 - x_2$$

$$y_3 = (x_1 - x_3)\lambda - y_1$$

### Theorem

*La courbe  $E$  munie de l'addition de points ainsi définie forme un groupe abélien.*

# Utilisation des courbes en cryptologie

- En cryptographie, pour tous les schémas pouvant s'exprimer dans un groupe générique:

# Utilisation des courbes en cryptologie

- En cryptographie, pour tous les schémas pouvant s'exprimer dans un groupe générique:
  - échange de clef Diffie-Hellman;

# Utilisation des courbes en cryptologie

- En cryptographie, pour tous les schémas pouvant s'exprimer dans un groupe générique:
  - échange de clef Diffie-Hellman;
  - signature à la DSA;

# Utilisation des courbes en cryptologie

- En cryptographie, pour tous les schémas pouvant s'exprimer dans un groupe générique:
  - échange de clef Diffie-Hellman;
  - signature à la DSA;
  - chiffrement à la Elgamal.

# Utilisation des courbes en cryptologie

- En cryptographie, pour tous les schémas pouvant s'exprimer dans un groupe générique:
  - échange de clef Diffie-Hellman;
  - signature à la DSA;
  - chiffrement à la Elgamal.
- En cryptographie, à l'aide de couplages (*pairings*) de nouveaux cryptosystèmes sont possibles.

# Utilisation des courbes en cryptologie

- En cryptographie, pour tous les schémas pouvant s'exprimer dans un groupe générique:
  - échange de clef Diffie-Hellman;
  - signature à la DSA;
  - chiffrement à la Elgamal.
- En cryptographie, à l'aide de couplages (*pairings*) de nouveaux cryptosystèmes sont possibles.
- Pour factoriser des entiers (pas directement applicable à RSA cependant).

# Diffie-Hellman sur des courbes

- Courbe elliptique  $E$  et  $P$  point sur la courbe de grand ordre  $n$ .

## Diffie-Hellman sur des courbes

- Courbe elliptique  $E$  et  $P$  point sur la courbe de grand ordre  $n$ .
- Alice choisit  $a$  entier au hasard,  $0 \leq a \leq n - 1$ .

## Diffie-Hellman sur des courbes

- Courbe elliptique  $E$  et  $P$  point sur la courbe de grand ordre  $n$ .
- Alice choisit  $a$  entier au hasard,  $0 \leq a \leq n - 1$ .
- Bob choisit  $b$  entier au hasard,  $0 \leq b \leq n - 1$ .

## Diffie-Hellman sur des courbes

- Courbe elliptique  $E$  et  $P$  point sur la courbe de grand ordre  $n$ .
- Alice choisit  $a$  entier au hasard,  $0 \leq a \leq n - 1$ .
- Bob choisit  $b$  entier au hasard,  $0 \leq b \leq n - 1$ .
- Alice transmet  $a \cdot P$  à Bob.

## Diffie-Hellman sur des courbes

- Courbe elliptique  $E$  et  $P$  point sur la courbe de grand ordre  $n$ .
- Alice choisit  $a$  entier au hasard,  $0 \leq a \leq n - 1$ .
- Bob choisit  $b$  entier au hasard,  $0 \leq b \leq n - 1$ .
- Alice transmet  $a \cdot P$  à Bob.
- Bob transmet  $b \cdot P$  à Alice.

## Diffie-Hellman sur des courbes

- Courbe elliptique  $E$  et  $P$  point sur la courbe de grand ordre  $n$ .
- Alice choisit  $a$  entier au hasard,  $0 \leq a \leq n - 1$ .
- Bob choisit  $b$  entier au hasard,  $0 \leq b \leq n - 1$ .
- Alice transmet  $a \cdot P$  à Bob.
- Bob transmet  $b \cdot P$  à Alice.
- Alice calcule  $a \cdot (b \cdot P) = (ab) \cdot P$ .

## Diffie-Hellman sur des courbes

- Courbe elliptique  $E$  et  $P$  point sur la courbe de grand ordre  $n$ .
- Alice choisit  $a$  entier au hasard,  $0 \leq a \leq n - 1$ .
- Bob choisit  $b$  entier au hasard,  $0 \leq b \leq n - 1$ .
- Alice transmet  $a \cdot P$  à Bob.
- Bob transmet  $b \cdot P$  à Alice.
- Alice calcule  $a \cdot (b \cdot P) = (ab) \cdot P$ .
- Bob calcule  $b \cdot (a \cdot P) = (ab) \cdot P$ .

## Diffie-Hellman sur des courbes

- Courbe elliptique  $E$  et  $P$  point sur la courbe de grand ordre  $n$ .
- Alice choisit  $a$  entier au hasard,  $0 \leq a \leq n - 1$ .
- Bob choisit  $b$  entier au hasard,  $0 \leq b \leq n - 1$ .
- Alice transmet  $a \cdot P$  à Bob.
- Bob transmet  $b \cdot P$  à Alice.
- Alice calcule  $a \cdot (b \cdot P) = (ab) \cdot P$ .
- Bob calcule  $b \cdot (a \cdot P) = (ab) \cdot P$ .

Sécurité:

- Connaissant  $P$  et  $a \cdot P$  il est dur de trouver  $a$ .

## Diffie-Hellman sur des courbes

- Courbe elliptique  $E$  et  $P$  point sur la courbe de grand ordre  $n$ .
- Alice choisit  $a$  entier au hasard,  $0 \leq a \leq n - 1$ .
- Bob choisit  $b$  entier au hasard,  $0 \leq b \leq n - 1$ .
- Alice transmet  $a \cdot P$  à Bob.
- Bob transmet  $b \cdot P$  à Alice.
- Alice calcule  $a \cdot (b \cdot P) = (ab) \cdot P$ .
- Bob calcule  $b \cdot (a \cdot P) = (ab) \cdot P$ .

### Sécurité:

- Connaissant  $P$  et  $a \cdot P$  il est dur de trouver  $a$ .
- Connaissant  $P$  et  $b \cdot P$  il est dur de trouver  $b$ .

## Diffie-Hellman sur des courbes

- Courbe elliptique  $E$  et  $P$  point sur la courbe de grand ordre  $n$ .
- Alice choisit  $a$  entier au hasard,  $0 \leq a \leq n - 1$ .
- Bob choisit  $b$  entier au hasard,  $0 \leq b \leq n - 1$ .
- Alice transmet  $a \cdot P$  à Bob.
- Bob transmet  $b \cdot P$  à Alice.
- Alice calcule  $a \cdot (b \cdot P) = (ab) \cdot P$ .
- Bob calcule  $b \cdot (a \cdot P) = (ab) \cdot P$ .

### Sécurité:

- Connaissant  $P$  et  $a \cdot P$  il est dur de trouver  $a$ .
- Connaissant  $P$  et  $b \cdot P$  il est dur de trouver  $b$ .
- Connaissant  $P$ ,  $a \cdot P$  et  $b \cdot P$  il est dur de trouver  $(ab) \cdot P$ .

# Elgamal sur les courbes elliptiques

- Courbe elliptique  $E$  et  $P$  point sur la courbe de grand ordre  $n$ .

# Elgamal sur les courbes elliptiques

- Courbe elliptique  $E$  et  $P$  point sur la courbe de grand ordre  $n$ .
- Bob choisit  $x$  entier,  $0 \leq x \leq n - 1$ :

# Elgamal sur les courbes elliptiques

- Courbe elliptique  $E$  et  $P$  point sur la courbe de grand ordre  $n$ .
- Bob choisit  $x$  entier,  $0 \leq x \leq n - 1$ :
  - $x$  est la clef privée de Bob.

# Elgamal sur les courbes elliptiques

- Courbe elliptique  $E$  et  $P$  point sur la courbe de grand ordre  $n$ .
- Bob choisit  $x$  entier,  $0 \leq x \leq n - 1$ :
  - $x$  est la clef privée de Bob.
  - $H = x \cdot P$  est la clef publique de Bob.

# Elgamal sur les courbes elliptiques

- Courbe elliptique  $E$  et  $P$  point sur la courbe de grand ordre  $n$ .
- Bob choisit  $x$  entier,  $0 \leq x \leq n - 1$ :
  - $x$  est la clef privée de Bob.
  - $H = x \cdot P$  est la clef publique de Bob.
- Alice transmet le message  $m \in E$ :

# Elgamal sur les courbes elliptiques

- Courbe elliptique  $E$  et  $P$  point sur la courbe de grand ordre  $n$ .
- Bob choisit  $x$  entier,  $0 \leq x \leq n - 1$ :
  - $x$  est la clef privée de Bob.
  - $H = x \cdot P$  est la clef publique de Bob.
- Alice transmet le message  $m \in E$ :
  - Elle choisit  $k$  entier au hasard.

# Elgamal sur les courbes elliptiques

- Courbe elliptique  $E$  et  $P$  point sur la courbe de grand ordre  $n$ .
- Bob choisit  $x$  entier,  $0 \leq x \leq n - 1$ :
  - $x$  est la clef privée de Bob.
  - $H = x \cdot P$  est la clef publique de Bob.
- Alice transmet le message  $m \in E$ :
  - Elle choisit  $k$  entier au hasard.
  - Elle calcule  $a = k \cdot H$ .

# Elgamal sur les courbes elliptiques

- Courbe elliptique  $E$  et  $P$  point sur la courbe de grand ordre  $n$ .
- Bob choisit  $x$  entier,  $0 \leq x \leq n - 1$ :
  - $x$  est la clef privée de Bob.
  - $H = x \cdot P$  est la clef publique de Bob.
- Alice transmet le message  $m \in E$ :
  - Elle choisit  $k$  entier au hasard.
  - Elle calcule  $a = k \cdot H$ .
  - Elle calcule  $b = m + a$ .

# Elgamal sur les courbes elliptiques

- Courbe elliptique  $E$  et  $P$  point sur la courbe de grand ordre  $n$ .
- Bob choisit  $x$  entier,  $0 \leq x \leq n - 1$ :
  - $x$  est la clef privée de Bob.
  - $H = x \cdot P$  est la clef publique de Bob.
- Alice transmet le message  $m \in E$ :
  - Elle choisit  $k$  entier au hasard.
  - Elle calcule  $a = k \cdot H$ .
  - Elle calcule  $b = m + a$ .
  - Elle transmet  $(a, b)$  à Bob.

# Elgamal sur les courbes elliptiques

- Courbe elliptique  $E$  et  $P$  point sur la courbe de grand ordre  $n$ .
- Bob choisit  $x$  entier,  $0 \leq x \leq n - 1$ :
  - $x$  est la clef privée de Bob.
  - $H = x \cdot P$  est la clef publique de Bob.
- Alice transmet le message  $m \in E$ :
  - Elle choisit  $k$  entier au hasard.
  - Elle calcule  $a = k \cdot H$ .
  - Elle calcule  $b = m + a$ .
  - Elle transmet  $(a, b)$  à Bob.
- Bob déchiffre:

# Elgamal sur les courbes elliptiques

- Courbe elliptique  $E$  et  $P$  point sur la courbe de grand ordre  $n$ .
- Bob choisit  $x$  entier,  $0 \leq x \leq n - 1$ :
  - $x$  est la clef privée de Bob.
  - $H = x \cdot P$  est la clef publique de Bob.
- Alice transmet le message  $m \in E$ :
  - Elle choisit  $k$  entier au hasard.
  - Elle calcule  $a = k \cdot H$ .
  - Elle calcule  $b = m + a$ .
  - Elle transmet  $(a, b)$  à Bob.
- Bob déchiffre:
  - Bob calcule  $c = x \cdot a = x \cdot (k \cdot P) = (xk) \cdot P$ .

# Elgamal sur les courbes elliptiques

- Courbe elliptique  $E$  et  $P$  point sur la courbe de grand ordre  $n$ .
- Bob choisit  $x$  entier,  $0 \leq x \leq n - 1$ :
  - $x$  est la clef privée de Bob.
  - $H = x \cdot P$  est la clef publique de Bob.
- Alice transmet le message  $m \in E$ :
  - Elle choisit  $k$  entier au hasard.
  - Elle calcule  $a = k \cdot H$ .
  - Elle calcule  $b = m + a$ .
  - Elle transmet  $(a, b)$  à Bob.
- Bob déchiffre:
  - Bob calcule  $c = x \cdot a = x \cdot (k \cdot P) = (xk) \cdot P$ .
  - Bob retrouve le message par

$$m' = b - c$$

## Factorization method principle

Let  $n$  be the number to be factored, and  $p$  an unknown prime factor of  $n$ .

## Factorization method principle

Let  $n$  be the number to be factored, and  $p$  an unknown prime factor of  $n$ .

- 1 Pick an abelian group  $G_p$  where operations are compatible with modular arithmetics.

## Factorization method principle

Let  $n$  be the number to be factored, and  $p$  an unknown prime factor of  $n$ .

- 1 Pick an abelian group  $G_p$  where operations are compatible with modular arithmetics.
- 2 Perform all operations mod  $n$  in the structure  $G_n$ .

## Factorization method principle

Let  $n$  be the number to be factored, and  $p$  an unknown prime factor of  $n$ .

- 1 Pick an abelian group  $G_p$  where operations are compatible with modular arithmetics.
- 2 Perform all operations mod  $n$  in the structure  $G_n$ .
- 3 Operations done mod  $n$  reduce naturally to  $G_p$ .

## Factorization method principle

Let  $n$  be the number to be factored, and  $p$  an unknown prime factor of  $n$ .

- 1 Pick an abelian group  $G_p$  where operations are compatible with modular arithmetics.
- 2 Perform all operations mod  $n$  in the structure  $G_n$ .
- 3 Operations done mod  $n$  reduce naturally to  $G_p$ .
- 4 Pick an element  $P_0 \in G_n$ , a positive integer  $x$  and compute  $x \cdot P$ .

## Factorization method principle

Let  $n$  be the number to be factored, and  $p$  an unknown prime factor of  $n$ .

- 1 Pick an abelian group  $G_p$  where operations are compatible with modular arithmetics.
- 2 Perform all operations mod  $n$  in the structure  $G_n$ .
- 3 Operations done mod  $n$  reduce naturally to  $G_p$ .
- 4 Pick an element  $P_0 \in G_n$ , a positive integer  $x$  and compute  $x \cdot P_0$ .
- 5 If  $o_{G_p}(P_0) \mid x$  the computation of  $x \cdot P_0$  will give a factor of  $n$  (probably).

# Factorization method principle

Example:

# Factorization method principle

Example:

- For the P-1 factorization method, we have  $G_p = (\mathbb{Z}/p\mathbb{Z})^*$ .

## Factorization method principle

Example:

- For the P-1 factorization method, we have  $G_p = (\mathbb{Z}/p\mathbb{Z})^*$ .
- For the P+1 factorization method, we have  $G_p = GF(p^2)^*$

# Factorization method principle

Example:

- For the P-1 factorization method, we have  $G_p = (\mathbb{Z}/p\mathbb{Z})^*$ .
- For the P+1 factorization method, we have  $G_p = GF(p^2)^*$   
(more correctly  $GF(p^2)^*/GF(p)^*$ ).

## Factorization method principle

Example:

- For the P-1 factorization method, we have  $G_p = (\mathbb{Z}/p\mathbb{Z})^*$ .
- For the P+1 factorization method, we have  $G_p = GF(p^2)^*$   
(more correctly  $GF(p^2)^*/GF(p)^*$ ).
- For ECM, we chose an elliptic curve  $E_{a,b}$ .

## A simple P-1 example

Take  $n = 10090019171$ ,  $P_0 = 42$  and  $x = 42$ .

## A simple P-1 example

Take  $n = 10090019171$ ,  $P_0 = 42$  and  $x = 42$ .

We notice that

$$\gcd(P_0^x - 1, n) = 1009$$

so we found a non trivial factor  $p = 1009$  of  $n$ .

## A simple P-1 example

Take  $n = 10090019171$ ,  $P_0 = 42$  and  $x = 42$ .

We notice that

$$\gcd(P_0^x - 1, n) = 1009$$

so we found a non trivial factor  $p = 1009$  of  $n$ .

The order of 42 in  $(\mathbb{Z}/p\mathbb{Z})^*$  is 21 and  $21|42$ .

## A simple P-1 example

Take  $n = 10090019171$ ,  $P_0 = 42$  and  $x = 42$ .

We notice that

$$\gcd(P_0^x - 1, n) = 1009$$

so we found a non trivial factor  $p = 1009$  of  $n$ .

The order of 42 in  $(\mathbb{Z}/p\mathbb{Z})^*$  is 21 and  $21|42$ .

Moreover  $p - 1 = 2^4 \cdot 3^2 \cdot 7$

## A simple P-1 example

Take  $n = 10090019171$ ,  $P_0 = 42$  and  $x = 42$ .

We notice that

$$\gcd(P_0^x - 1, n) = 1009$$

so we found a non trivial factor  $p = 1009$  of  $n$ .

The order of 42 in  $(\mathbb{Z}/p\mathbb{Z})^*$  is 21 and  $21|42$ .

Moreover  $p - 1 = 2^4 \cdot 3^2 \cdot 7$

$n = p \cdot q$  where  $q$  is prime and  $q - 1 = 2 \cdot 7^2 \cdot 67 \cdot 1523$

## A simple P-1 example

Take  $n = 10090019171$ ,  $P_0 = 42$  and  $x = 42$ .

We notice that

$$\gcd(P_0^x - 1, n) = 1009$$

so we found a non trivial factor  $p = 1009$  of  $n$ .

The order of 42 in  $(\mathbb{Z}/p\mathbb{Z})^*$  is 21 and  $21|42$ .

Moreover  $p - 1 = 2^4 \cdot 3^2 \cdot 7$

$n = p \cdot q$  where  $q$  is prime and  $q - 1 = 2 \cdot 7^2 \cdot 67 \cdot 1523$

and the order of 42 in  $(\mathbb{Z}/q\mathbb{Z})^*$  is  $102041 > 42$ .

## A simple P-1 example

Take  $n = 10090019171$ ,  $P_0 = 42$  and  $x = 42$ .

We notice that

$$\gcd(P_0^x - 1, n) = 1009$$

so we found a non trivial factor  $p = 1009$  of  $n$ .

The order of 42 in  $(\mathbb{Z}/p\mathbb{Z})^*$  is 21 and  $21|42$ .

Moreover  $p - 1 = 2^4 \cdot 3^2 \cdot 7$

$n = p \cdot q$  where  $q$  is prime and  $q - 1 = 2 \cdot 7^2 \cdot 67 \cdot 1523$

and the order of 42 in  $(\mathbb{Z}/q\mathbb{Z})^*$  is  $102041 > 42$ .

So we were able to factorize  $n$ .

## Comparison of ECM with other methods

Group	Order
$\mathbb{Z}/p\mathbb{Z}$	$p - 1 = \Pi_1(p)$
$GF(p^2)$	$p + 1 = \Pi_2(p)$
“Generic cyclotomic”	$\Pi_d(p)$
$E_{a,b} \bmod p$	$ o - (p + 1)  < 2\sqrt{p}$

# Complexity of ECM

Let  $L_{\alpha,c}(p) = e^{c(\log p)^\alpha (\log \log p)^{1-\alpha}}$ . Then the expected time complexity of ECM to find a factor  $p$  of  $n$  is

$$O(L_{\frac{1}{2},\sqrt{2}}(p)M(\log n))$$

where  $M(\log n)$  is the complexity of multiplication mod  $n$ .

# Complexity of ECM

Let  $L_{\alpha,c}(p) = e^{c(\log p)^\alpha (\log \log p)^{1-\alpha}}$ . Then the expected time complexity of ECM to find a factor  $p$  of  $n$  is

$$O(L_{\frac{1}{2},\sqrt{2}}(p)M(\log n))$$

where  $M(\log n)$  is the complexity of multiplication mod  $n$ .

- for NFS  $O(L_{\frac{1}{3},c}(n))$  (where  $c < 2$ ).

# Complexity of ECM

Let  $L_{\alpha,c}(p) = e^{c(\log p)^\alpha (\log \log p)^{1-\alpha}}$ . Then the expected time complexity of ECM to find a factor  $p$  of  $n$  is

$$O(L_{\frac{1}{2},\sqrt{2}}(p)M(\log n))$$

where  $M(\log n)$  is the complexity of multiplication mod  $n$ .

- for NFS  $O(L_{\frac{1}{3},c}(n))$  (where  $c < 2$ ).
- ECM won't break RSA any time soon.

## Complexity of ECM

Let  $L_{\alpha,c}(p) = e^{c(\log p)^\alpha (\log \log p)^{1-\alpha}}$ . Then the expected time complexity of ECM to find a factor  $p$  of  $n$  is

$$O(L_{\frac{1}{2},\sqrt{2}}(p)M(\log n))$$

where  $M(\log n)$  is the complexity of multiplication mod  $n$ .

- for NFS  $O(L_{\frac{1}{3},c}(n))$  (where  $c < 2$ ).
- ECM won't break RSA any time soon.
- huge numbers with expected relatively small factors are out of reach for NSF: ECM can be used there.

## How to chose $x$

The hope is to pick  $P_0$  and  $x$  such that  $x|o_{G_p}(P_0)$ .  
Use two bounds  $B1, B2$ :

## How to chose $x$

The hope is to pick  $P_0$  and  $x$  such that  $x | o_{G_p}(P_0)$ .

Use two bounds  $B_1, B_2$ :

- “cover” all primes up to  $B_1$ ,

## How to chose $x$

The hope is to pick  $P_0$  and  $x$  such that  $x | o_{G_p}(P_0)$ .

Use two bounds  $B_1, B_2$ :

- “cover” all primes up to  $B_1$ ,
- permit an additional prime factor in  $[B_1, B_2]$ .

This explains naturally the two stages method used in GMP-ECM.

## High level algorithm description

INPUT: a number  $n$ , integer bounds  $B_1 \leq B_2$ .

OUTPUT: a factor  $p$  of  $n$  or FAIL.

- 1: Choose a random elliptic curve  $E_{a,b} \bmod n$  and a point  $P_0 = (x_0 : y_0 : z_0)$  on it.
- 2: Compute  $Q = \prod_{\pi \leq B_1} \pi^{\lfloor \log B_1 / \log \pi \rfloor} P_0$ .
- 3: **for**  $\pi$  prime,  $B_1 < \pi \leq B_2$  **do**
- 4:      $(x_\pi : y_\pi : z_\pi) \leftarrow \pi Q$
- 5:      $g \leftarrow \gcd(n, z_\pi)$
- 6:     **if**  $g \neq 1$  **then**
- 7:         **return**  $g$
- 8:     **end if**
- 9: **end for**
- 10: **return** FAIL

# Algorithmic challenges

An implementation of ECM is faced with the following algorithmic challenges:

# Algorithmic challenges

An implementation of ECM is faced with the following algorithmic challenges:

- fast modular arithmetic

# Algorithmic challenges

An implementation of ECM is faced with the following algorithmic challenges:

- fast modular arithmetic
- efficient curve operations

# Algorithmic challenges

An implementation of ECM is faced with the following algorithmic challenges:

- fast modular arithmetic
- efficient curve operations
- fast polynomial evaluation (stage 2)

# Algorithmic challenges

An implementation of ECM is faced with the following algorithmic challenges:

- fast modular arithmetic
- efficient curve operations
- fast polynomial evaluation (stage 2)

In order to be fast, we use algorithmic improvements tailored to the size of the numbers used (with thresholds) as well as assembly code.

## An example ECM factorization with GMP-ECM

Let

$$N = 14421499473850156964908748714733530694523632245$$
$$48199639497786788488662355550896284406444518825$$
$$58206114371958127980496626323628808250533258921$$
$$4668868374102124472638792350353190035972075401$$

of 187 digits. We chose  $B_1 = 433993$ , the curve parameterized by  $\sigma = 550048451$  (Suyama).

# An example ECM factorization with GMP-ECM

```
$ ecm -v -v -sigma 550048451 433993 < composite
GMP-ECM 6.1.1 [powered by GMP 4.2.1] [ECM]
Input number is [...] (187 digits)
Using MODMULN
Using B1=433993, B2=347971482, polynomial Dickson(3), sigma=550048451
Expected number of curves to find a factor of n digits:
20      25      30      35      40      45      50      55      60      65
6        33      241     2322    27856   401319  6767926  1.3e+08  2.9e+09  7.1e+10
Step 1 took 39656ms
Step 2 took 12204ms
***** Factor found in step 2: 344518986834068356794510012742065462371
Found probable prime factor of 39 digits: 344518986834068356794510012742065462371
Composite cofactor 41...1 has 148 digits
```

# Problématique

Tiens, regarde ce qu'Alice m'a confié :

$M = \langle \dots \rangle, \text{Sign}(\text{Alice}, M)$

Charlie



Bob



Alice



canal sûr



$M = \langle \text{Ce Noël j'offre une Wii à Charlie} \rangle, \text{Sign}(\text{Alice}, M)$

# Problématique

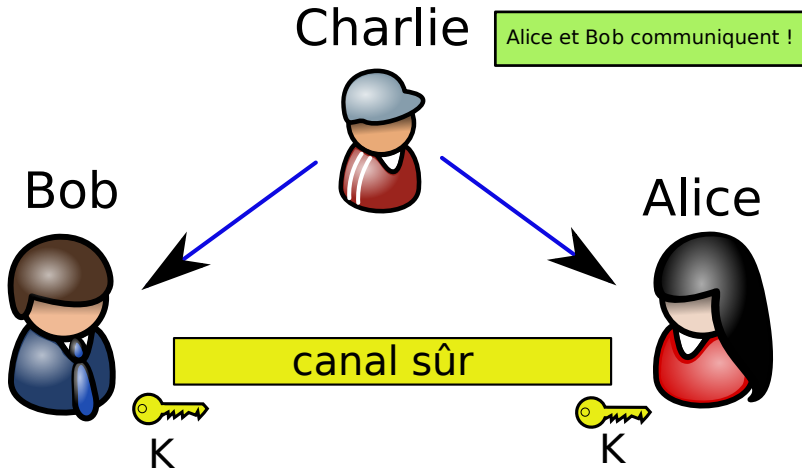
- Une signature classique (RSA, DSA) d'un message échangé entre Alice et Bob est vérifiable par toute personne ayant la clef publique du signataire.
- Toutes les communications ne nécessitent pas ce niveau d'engagement.

# Problématique

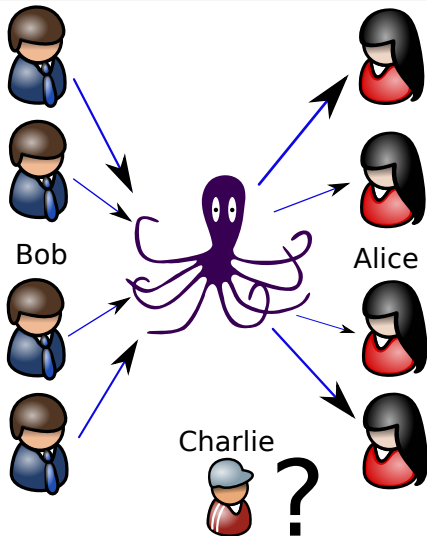
- Une signature classique (RSA, DSA) d'un message échangé entre Alice et Bob est vérifiable par toute personne ayant la clef publique du signataire.
- Toutes les communications ne nécessitent pas ce niveau d'engagement.

Cf. exposé OTR.

# Problématique



# Solution !



# Une solution basée sur PGP

- Alice veut envoyer le message  $m$  à Bob en masquant son identité;
- Elle choisit une chaîne de *remailers* anonymes  $C_1, C_2, \dots, C_n$ ;

# Problématique

Cf. exposé Carlos Aguilar Melchor.