Constructions génériques de cryptosystèmes probabilistes et ses applications

Guilhem Castagnos

Département Mathématiques Informatique – Xlim
Université de Limoges

Jeudi 19 Avril

Cadre

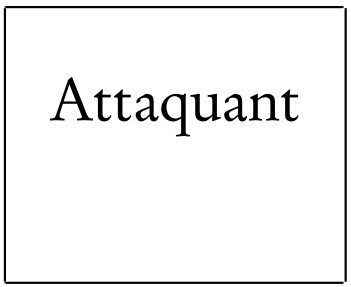
- Cryptographie probabiliste : un message m a plusieurs chiffrés possibles, l'algorithme de chiffrement est probabiliste.
- Expansion :
$$\frac{\text{taille du chiffré}}{\text{taille du clair}}.$$
- Chiffrement homomorphique : Si c_1 est un chiffré de m_1, et c_2 est un chiffré de m_2, c_1c_2 est un chiffré de $m_1 + m_2$.
- Fonctions trappe : fonctions facilement évaluables mais difficiles à inverser à moins de connaître une trappe.

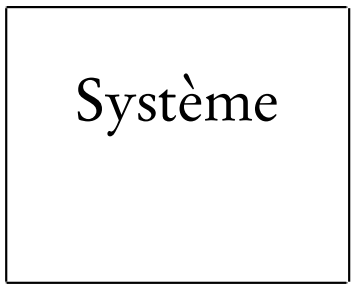
Sécurité

- Moyens de l'attaquant :
  - Attaques à messages clairs choisis (CPA).
  - Attaques adaptatives à messages chiffrés choisis (CCA2).

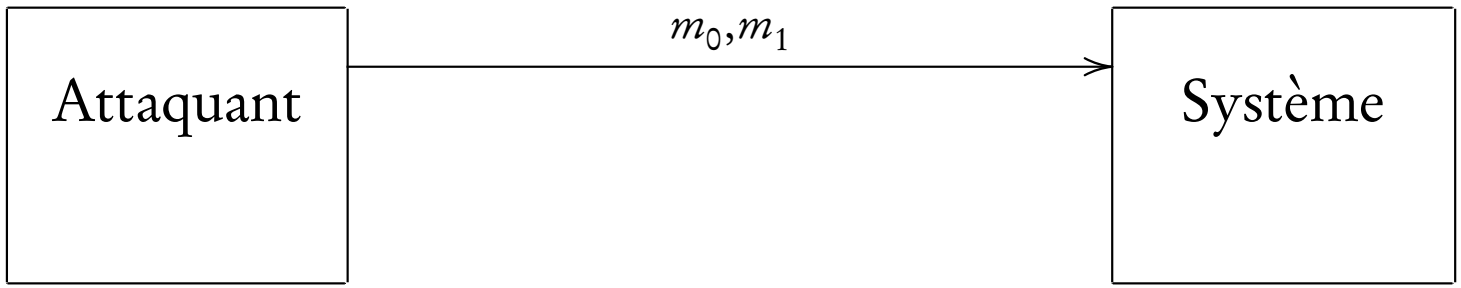
- Buts de l'attaquant :
  - Sécurité : Étant donné un chiffré, un attaquant ne peut retrouver le message correspondant (sens-unique).
  - Sécurité sémantique : Un attaquant ne peut extraire aucune information en temps polynomial sur un message à partir de l'un de ces chiffrés, en dehors de celles qu'il aurait pu obtenir sans ce chiffré.
  - Équivalent à la notion d'indistinguabilité (IND) : Un attaquant ne peut reconnaître lequel des deux messages, qu'il a préalablement choisi, a été chiffré.

Sécurité sémantique

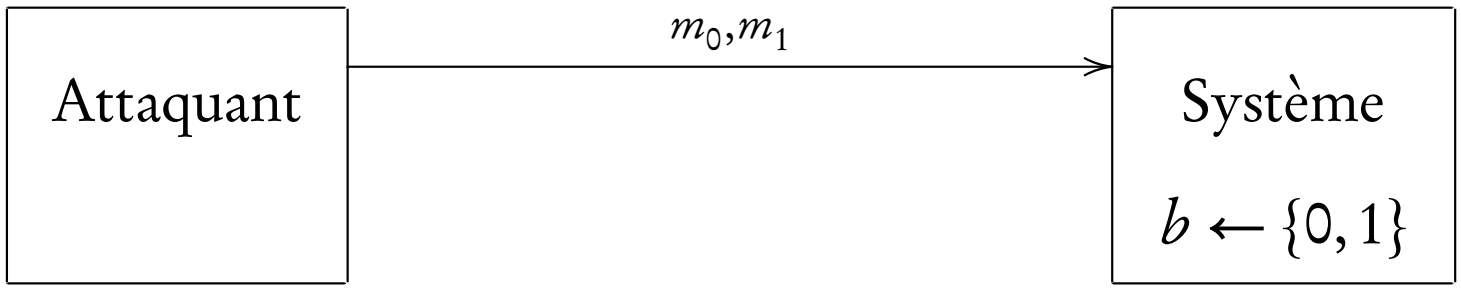




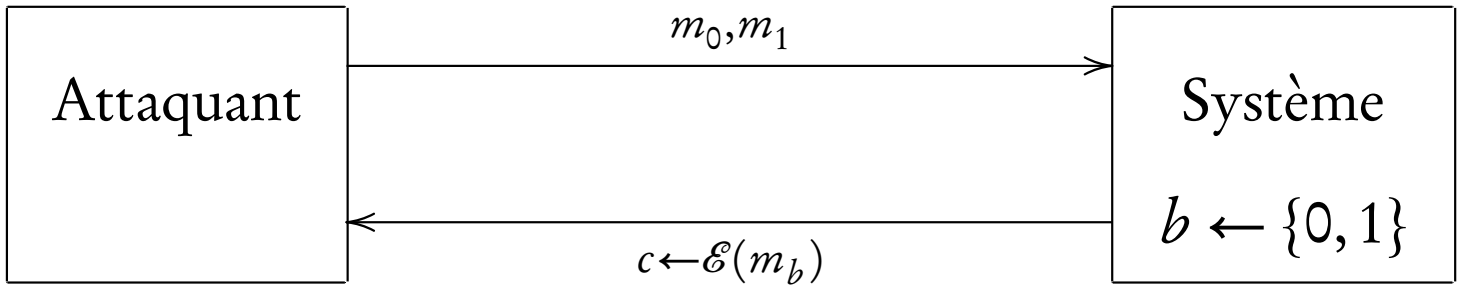
Sécurité sémantique



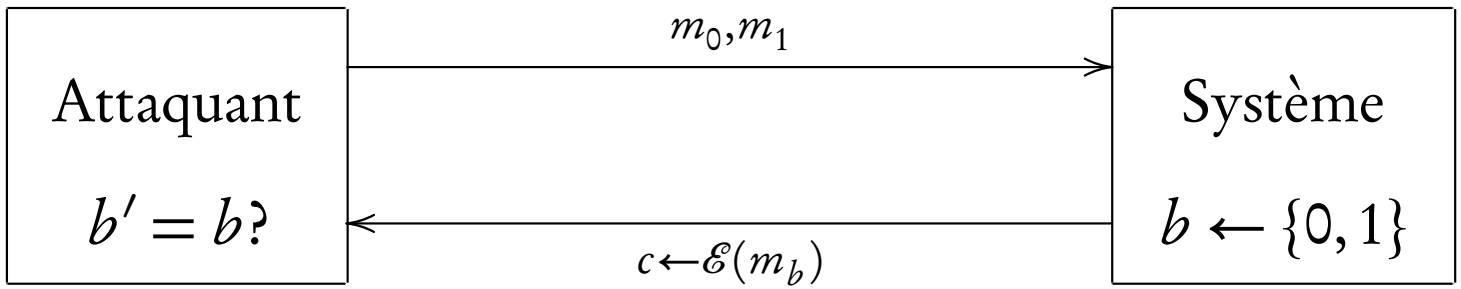
Sécurité sémantique



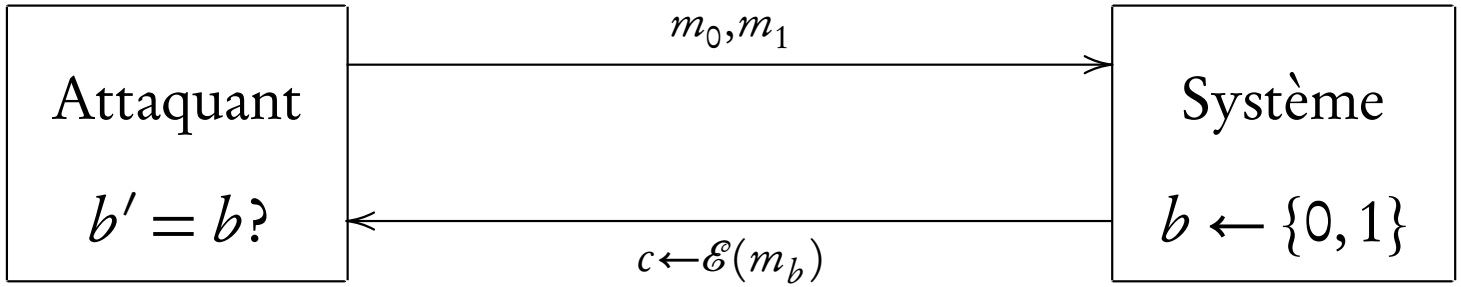
Sécurité sémantique



Sécurité sémantique



Sécurité sémantique



$$\mathrm{Adv}^{\mathrm{IND}}_{\Pi,\mathcal{A}} = \left| 2 \times \mathrm{P}\left[b' = b\right] - 1 \right|$$

$$= \left| \mathrm{P}\left[b' = 1 | b = 1\right] - \mathrm{P}\left[b' = 1 | b = 0\right] \right|$$

$$\mathrm{P}\left[b' = b\right] = \frac{1}{2} \pm \frac{\mathrm{Adv}^{\mathrm{IND}}_{\Pi,\mathcal{A}}}{2}$$

Plan

Plan

Cadre

- G groupe abélien fini multiplicatif.
- On suppose $|\mathrm{G}| = \lambda k$ avec $\mathrm{pgcd}(\lambda, k) = 1$.
- On note

$$\mathrm{G}^k := \left\{x \in \mathrm{G}, \exists y \in \mathrm{G},\ x = y^k\right\} = \left\{x \in \mathrm{G},\ x^\lambda = 1\right\}, \text{ d'ordre } \lambda.$$

$$\mathrm{G}^\lambda := \left\{x \in \mathrm{G}, \exists y \in \mathrm{G},\ x = y^\lambda\right\} = \left\{x \in \mathrm{G},\ x^k = 1\right\}, \text{ d'ordre } k.$$

- On a alors

$$\mathrm{G}^\lambda \times \mathrm{G}^k \xrightarrow{\sim} \mathrm{G}.$$

- On suppose que $\mathrm{G}^\lambda = \langle g \rangle$, *i.e.*,

$$\mathbf{Z}/k\mathbf{Z} \times \mathrm{G}^k \xrightarrow{\sim} \mathrm{G}.$$

Chiffrement

- Données publiques : G, k et g.
- Prototype de l'algorithme de chiffrement :

$$\mathcal{E}_{G,k,g} : \begin{cases} \mathbf{Z}/k\mathbf{Z} & \longrightarrow & G \\ m & \longmapsto & g^m \rho \end{cases}$$

où ρ est un élément aléatoire de G^k.
- Le quotient G/G^k est cyclique d'ordre k engendré par $\overline{g}$.
- Si $c \leftarrow \mathcal{E}_{G,k,g}(m)$,

$$m = \log_{\overline{g}}(\overline{c}).$$

- Le cryptosystème est donc homomorphique.

Déchiffrement

- Clef secrète : λ.
- On a
$$\rho \in G^k \iff \rho^\lambda = 1.$$
- Pour déchiffrer $c \in G$ ($c = g^m \rho$, $m \in \mathbf{Z}/k\mathbf{Z}$ et $\rho \in G^k$), on calcule
$$c^\lambda = g^{m\lambda}.$$
- On est donc ramené à un calcul de log discret dans $< g >$.
- Il faut donc un algorithme efficace pour ce calcul.

Caractéristiques du système

Sécurité :

- Repose sur la difficulté du calcul de $\log_{\overline{g}}(\overline{c})$.
- Se réduit à l'inversion de

$$G/\langle g\rangle \xrightarrow{\sim} G/\langle g\rangle, x \mapsto x^k.$$

- Se réduit à retrouver λ, *i.e.*, l'ordre de G.

Caractéristiques du système

Sécurité sémantique (IND-CPA) :

- Problème décisionnel : étant donné m et c, décider si

$$m = \log_{\overline{g}}(\overline{c}).$$

- Équivalent à $\text{Rés}_{G,k}$: reconnaître les éléments de G^k dans G.
- Système sémantiquement sûr $\Longrightarrow$ $\text{Rés}_{G,k}$ dur.

Caractéristiques du système

Sécurité sémantique (IND-CPA) :

- Système sémantiquement sûr $\Longleftarrow$ $\text{Rés}_{G,k}$ dur :

$\mathcal{D}(z)$ $\qquad$ $z \in G^k$?

$(m_0, m_1, s) \leftarrow \mathcal{A}_1(G, k, g)$
$b \leftarrow \{0, 1\}$,
$c \leftarrow (g^{m_b} z)$
$b' \leftarrow \mathcal{A}_2(m_0, m_1, s, c)$
si $b = b'$ **alors**
  retourner : 1
sinon
  retourner : 0

$$\mathrm{P}\left(\mathcal{D}(z) = 1 \mid z \in G^k\right) = \frac{1 \pm \mathrm{Adv}(\mathcal{A})}{2},$$

$$\mathrm{P}\left(\mathcal{D}(z) = 1 \mid z \notin G^k\right) = \frac{1}{2},$$

$$\mathrm{Adv}(\mathcal{D}) = \frac{\mathrm{Adv}(\mathcal{A})}{2}.$$

Caractéristiques du système

Coût :

- Chiffrement : calcul de g^m (rapide), création de la puissance k–ième par l'isomorphisme :

$$G/\langle g\rangle \xrightarrow{\sim} G^k,\ x \longmapsto x^k$$

- Déchiffrement : Exponentiation à la puissance λ, calcul du logarithme discret dans $\langle g\rangle$ (rapide)

Expansion :

$$1+\frac{|\lambda|_2}{|k|_2}.$$

Quelques cryptosystèmes suivant ce schéma

Messages dans $\mathbf{Z}/k\mathbf{Z}$, chiffrés dans G, aléas : puissances k–ièmes de G.

Soit $n = pq$ un entier RSA.

- **Goldwasser-Micali (1984).** G : sous-groupe des éléments de symbole de Jacobi positif de $\mathbf{Z}/n\mathbf{Z}$, $k = 2$, aléa : carrés, $\mathrm{E} = |n|_2$.
- **Benaloh (1988).** $\mathrm{G} = (\mathbf{Z}/n\mathbf{Z})^\times$ et ses puissances k–ièmes, $\mathrm{E} = |n|_2 / |k|_2$, amélioré par **Naccache et Stern (1998)** : $\mathrm{E} \approx 4$.
- **Paillier (1999).** $\mathrm{G} = (\mathbf{Z}/n^2\mathbf{Z})^\times$ et ses puissances n–ièmes : $k = n$, $\mathrm{E} = 2$.
- **Galbraith (2002).** G : courbe elliptique sur $\mathbf{Z}/n^2\mathbf{Z}$ et ses « puissances » n–ièmes.

Idée générale : travailler modulo n^2

- But : trouver un groupe G avec une décomposition $G^\lambda \times G^k$, tel que $G^\lambda = \langle g \rangle$ ait une expression « simple », et $|G|$ caché.
- Exemple : le système de Paillier : n un entier RSA, $G = (\mathbf{Z}/n^2\mathbf{Z})^\times$, $|G| = n\varphi(n)$ avec ($k = n$ et $\lambda = \varphi(n)$). On considère
$$\pi : (\mathbf{Z}/n^2\mathbf{Z})^\times \to (\mathbf{Z}/n\mathbf{Z})^\times .$$
- On a $G^\lambda = \ker \pi \cong \mathbf{Z}/n\mathbf{Z}$ est cyclique d'ordre n engendré par $1+n$, et $(1+n)^i = 1 + ni \mod n^2$.
- Fonction de chiffrement :
$$\begin{array}{ccccc} \mathbf{Z}/n\mathbf{Z} & \times & (\mathbf{Z}/n\mathbf{Z})^\times & \xrightarrow{\sim} & (\mathbf{Z}/n^2\mathbf{Z})^\times \\ (m & , & r) & \longmapsto & (1+n)^m r^n \end{array}$$

Plan

Principe

- Fonction trappe précédente :

$$\begin{array}{ccccc} \mathbf{Z}/k\mathbf{Z} & \times & \mathrm{G}/\langle g\rangle & \longrightarrow & \mathrm{G} \\ (m & , & \rho) & \longmapsto & g^m\rho^k \end{array}$$

en utilisant : $\mathrm{G}/\langle g\rangle \to \mathrm{G}/\langle g\rangle$, $\rho \mapsto \rho^k$.

Par exemple : $(\mathbf{Z}/n\mathbf{Z})^\times \to (\mathbf{Z}/n\mathbf{Z})^\times : r \mapsto r^n$.

- On remplace par

$$\overline{\Lambda} \xrightarrow[\overline{f}]{\sim} \overline{\Lambda} \hookrightarrow \mathrm{G}/\langle g\rangle,$$

où $\overline{f}$ est une fonction trappe déterministe.

Par exemple : $(\mathbf{Z}/n\mathbf{Z})^\times \to (\mathbf{Z}/n\mathbf{Z})^\times : r \mapsto r^e$.

Chiffrement

- On « relève » $\overline{f}$ en $f : \Lambda \longrightarrow \Omega$, avec $\Lambda \subset \mathrm{G}$ et $\Omega \subset \mathrm{G}$

- Données publiques : G, k, g d'ordre k, Λ et Ω et $f : \Lambda \longrightarrow \Omega$.
- Prototype de l'algorithme de chiffrement :

$$\mathscr{E}_{\mathrm{G},f,g} : \left\{ \begin{array}{ccccc} \mathbf{Z}/k\mathbf{Z} & \times & \Lambda & \longrightarrow & \Omega \\ (m & , & \rho) & \longmapsto & g^m f(\rho) \end{array} \right.$$

- $\mathscr{E}_{\mathrm{G},f,g}$ est bijective.
- Cryptosystème est non homomorphique.

Déchiffrement

- Soit $\pi : G \to G/\langle g \rangle$.
- f construite telle que $\pi \circ f = \overline{f} \circ \pi$.

- Clef secrète : trappe permettant d'inverser $\overline{f}$.
- Soit $c \in \Omega$ à déchiffrer ($c = g^m f(\rho)$ avec $m \in \mathbf{Z}/k\mathbf{Z}$ et $\rho \in \Lambda$)
- On calcule $\pi(c)$ ($= \pi \circ f(\rho) = \overline{f} \circ \pi(\rho)$) puis

$$\left(\overline{f}\right)^{-1}(\pi(c)) = \pi(\rho).$$

- On a alors

$$g^m = c/f(\rho).$$

Caractéristiques du système

Sécurité :

- Repose sur le problème : Étant donné c un élément de Ω, trouver m dans $\mathbf{Z}/k\mathbf{Z}$ tel que $c = g^m f(\rho)$ avec $\rho \in \Lambda$.
- Équivalent au problème de relèvement : Étant donné $\overline{c} \in \overline{\Lambda}$ $(\overline{c} = \overline{f}(\overline{\rho}))$, trouver $f(\rho)$.
- Se réduit à l'inversion de $\overline{f}$.

Sécurité sémantique (IND-CPA) :

- Repose sur le problème de reconnaissance des éléments de $f(\Lambda)$ dans Ω. ($\text{Rés}_{G,f,g}$).

Cryptosystèmes suivant ce schéma

Soit $n = pq$ un entier RSA.

- **Catalano, Gennaro *et al.* (2001)** : $(\mathbf{Z}/n^2\mathbf{Z})^\times$ et $\mathrm{RSA}_{n,e}$ automorphisme de $(\mathbf{Z}/n\mathbf{Z})^\times$. Sécurité équivalente à RSA.
- **Galindo, Martin *et al.* (2002)** : courbes elliptiques sur $\mathbf{Z}/n^2\mathbf{Z}$ et la fonction trappe $\mathrm{KMOV}_{n,e}$ associée à des courbes elliptiques sur $\mathbf{Z}/n\mathbf{Z}$.

Variante IND-CCA2 dans le ROM

- Primitive de chiffrement :

$$\mathcal{E}'_{G,f,g} : \left\{ \begin{array}{ccccccc} \mathbf{Z}/k\mathbf{Z} & \times & \Lambda & \longrightarrow & \Omega & \times & \{0,1\}^\ell \\ (m & , & \rho) & \longmapsto & (g^m f(\rho) & , & h(m,\rho)) \end{array} \right.$$

- $h : \mathbf{Z}/k\mathbf{Z} \times \Lambda \to \{0,1\}^\ell$, fonction de hachage vue comme un oracle aléatoire.

- Déchiffrement : on récupère ρ et m puis vérifie que le haché convient.
  - haché OK : retourne m
  - Sinon : retourne $\perp$.
- Dans le modèle de l'oracle aléatoire : système sémantiquement sûr (IND-CCA2) $\Longleftarrow$ $\text{Rés}_{G,f,g}$ dur.

Plan

Définitions

- Soit $\mathcal{O}_\Delta$ l'anneau des entiers de $\mathbf{Q}(\sqrt{\Delta})$, avec Δ un entier non carré. Soit n un entier impair premier avec Δ.
- $\mathcal{O}_\Delta/n\mathcal{O}_\Delta$ module libre de rang 2 sur $\mathbf{Z}/n\mathbf{Z}$.
- On note $(\mathcal{O}_\Delta/n\mathcal{O}_\Delta)^\wedge$ le groupe constitué par les éléments de norme 1 :

$$(\mathcal{O}_\Delta/n\mathcal{O}_\Delta)^\wedge = \left\{x + y\sqrt{\Delta}, (x,y) \in (\mathbf{Z}/n\mathbf{Z})^2, x^2 - \Delta y^2 = 1\right\}$$

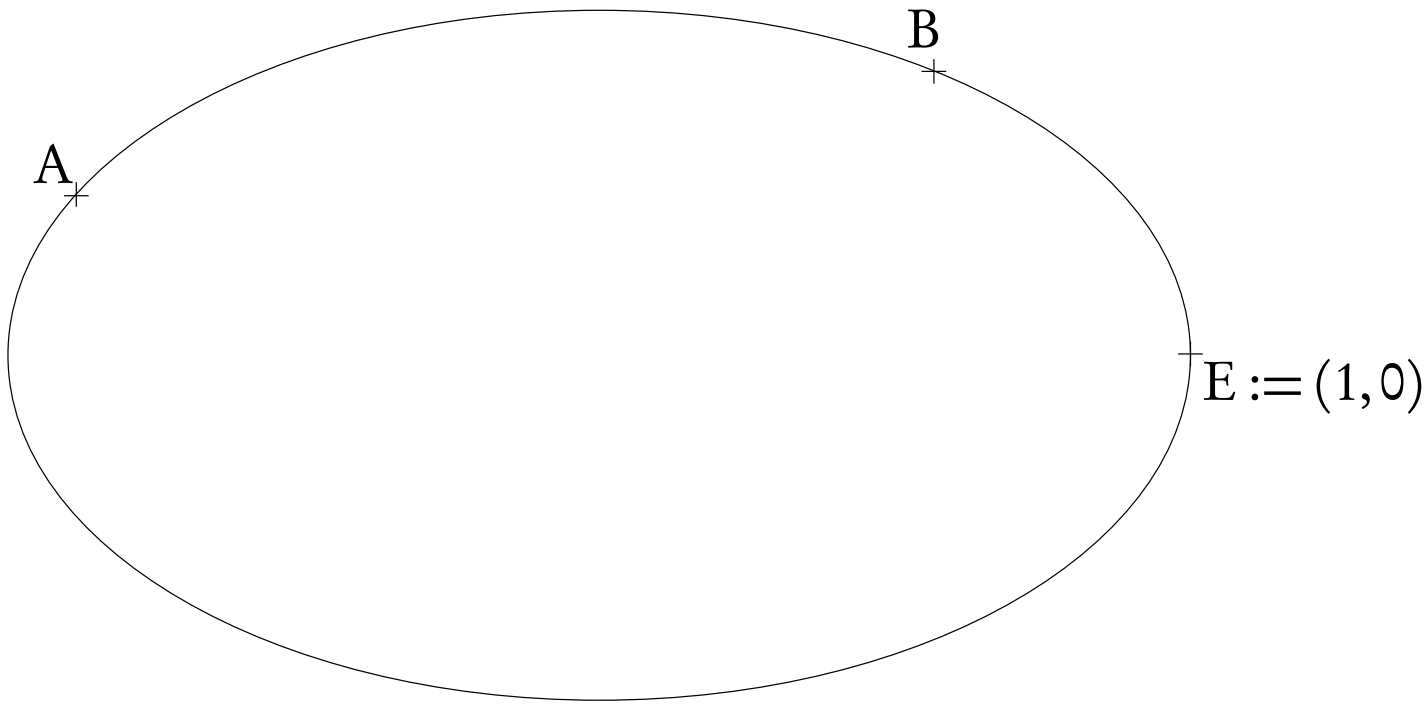
$$\left(x_1 + y_1\sqrt{\Delta}\right)\left(x_2 + y_2\sqrt{\Delta}\right) = x_1x_2 + \Delta y_1y_2 + (x_2y_1 + x_1y_2)\sqrt{\Delta}$$

- Groupe des points de la conique d'équation affine

$$X^2 - \Delta Y^2 = 1,$$

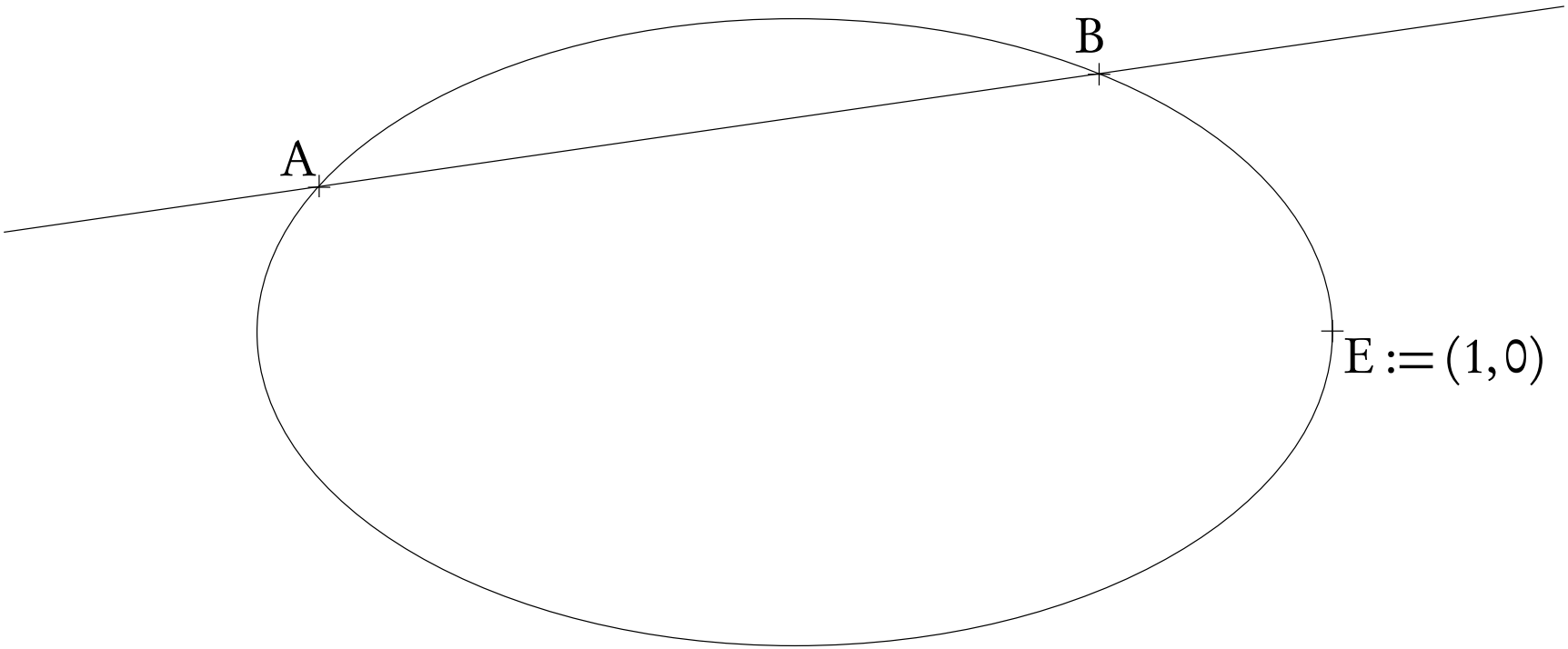
sur $\mathbf{Z}/n\mathbf{Z}$.

Addition dans une conique



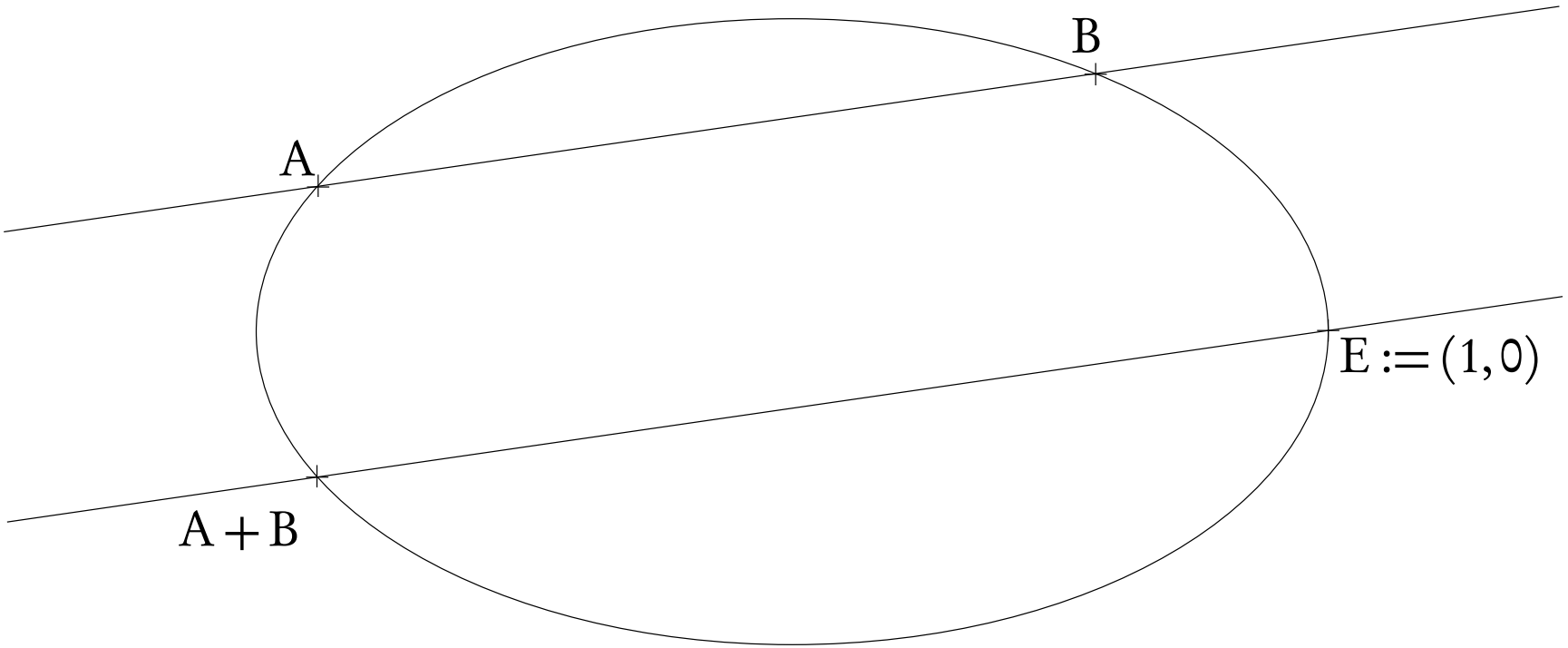
$\mathscr{C}$ d'équation affine $X^2 - \Delta Y^2 = 1$

Addition dans une conique



$\mathscr{C}$ d'équation affine $X^2 - \Delta Y^2 = 1$

Addition dans une conique



$\mathscr{C}$ d'équation affine $X^2 - \Delta Y^2 = 1$

Structure de $(\mathcal{O}_\Delta/n\mathcal{O}_\Delta)^\wedge$

- On note $\varphi_\Delta(n)$ l'ordre de $(\mathcal{O}_\Delta/n\mathcal{O}_\Delta)^\wedge$.
- Si $n = \prod p_i^{r_i}$, avec les p_i premiers distincts, on a

$$\varphi_\Delta(n) = \prod \varphi_\Delta(p_i^{r_i}).$$

- Pour les puissances de nombres premiers, on a :

Théorème

Pour p premier impair ne divisant pas Δ et $r \in \mathbf{N}^*$,

$$\varphi_\Delta(p^r) = p^{r-1}\left(p - \left(\frac{\Delta}{p}\right)\right),$$

et $(\mathcal{O}_\Delta/p^r\mathcal{O}_\Delta)^\wedge$ est cyclique.

Plan

Suites de Lucas

- Pour tout entier $k \geqslant 1$,

$$\begin{aligned} U_{k+1}(P,Q) &= PU_k(P,Q) - QU_{k-1}(P,Q), \\ V_{k+1}(P,Q) &= PV_k(P,Q) - QV_{k-1}(P,Q), \end{aligned}$$

et $U_1(P,Q) = 1$, $U_0(P,Q) = 0$, $V_1(P,Q) = P$, $V_0(P,Q) = 2$.

- Soit α un élément de $\mathcal{O}_\Delta$ et x, y deux entiers tels que $\alpha \equiv x + y\sqrt{\Delta} \pmod{n\mathcal{O}_\Delta}$. Pour tout entier naturel k, on a

$$\begin{aligned} \alpha^k &\equiv \frac{V_k\left(2x, N(\alpha)\right)}{2} + yU_k\left(2x, N(\alpha)\right)\sqrt{\Delta} \pmod{n\mathcal{O}_\Delta}, \\ Tr(\alpha^k) &\equiv V_k\left(2x, N(\alpha)\right) \pmod{n}. \end{aligned}$$

Calcul dans $(\mathcal{O}_\Delta/n\mathcal{O}_\Delta)^\wedge$

Calcul	Termes utilisés	Coût
$\mathrm{Tr}(\alpha^k)$	$V_k(P,1)$	$2\lvert k\rvert_2 M$
α^k	$V_k(P,1)$ et $U_k(P,1)$	$3\lvert k\rvert_2 M$

- M : multiplication modulo n.
- Exponentiation deux fois plus rapide qu'en utilisant la base $(1, \sqrt{\Delta})$.

Plan

Chiffrement

- On prend $n = pq$ et $\mathrm{G} := \left(\mathcal{O}_\Delta/n^2\mathcal{O}_\Delta\right)^\wedge$, avec Δ premier avec n.
- $|\mathrm{G}| = n\varphi_\Delta(n)$, on suppose que $\mathrm{pgcd}\left(n, \varphi_\Delta(n)\right) = 1$ ($k = n$ et $\lambda = \varphi_\Delta(n)$)
- On a
$$\mathrm{G}^\lambda = \ker\left(\left(\mathcal{O}_\Delta/n^2\mathcal{O}_\Delta\right)^\wedge \to (\mathcal{O}_\Delta/n\mathcal{O}_\Delta)^\wedge\right).$$
cyclique d'ordre n, engendré par $g = 1 + n\sqrt{\Delta}$. De plus, $g^i = 1 + in\sqrt{\Delta}$.
- La fonction de chiffrement est
$$\mathcal{E} : \left\{ \begin{array}{ccc} \mathbf{Z}/n\mathbf{Z} & \to & \left(\mathcal{O}_\Delta/n^2\mathcal{O}_\Delta\right)^\wedge \\ m & \mapsto & (1 + mn\sqrt{\Delta})\rho \end{array} \right.$$
avec $\rho \in \mathrm{G}^n$.

Les puissances n–ièmes

- Générer un élément de $(\mathcal{O}_\Delta/n\mathcal{O}_\Delta)^\wedge$: résoudre $x^2 - \Delta y^2 = 1$ dans $\mathbf{Z}/n\mathbf{Z} \times \mathbf{Z}/n\mathbf{Z}$.
- Comment générer $\rho \in \mathrm{G}^n$:
  - Travailler avec Δ non fixé : système non homomorphique.
  - Utiliser la fonction : $r \mapsto \left(\frac{r+\sqrt{\Delta}}{r-\sqrt{\Delta}}\right)^n$ de $(\mathbf{Z}/n\mathbf{Z})^\times$ dans G^n.
  - Publier une puissance n–ième β d'ordre grand et calculer $\rho := \beta^r$ avec $r < n$ aléatoire.

Déchiffrement

- Si c est un chiffré de m on a $c = g^m \rho$, avec $\rho \in G^n$.
- La clef secrète est

$$\varphi_\Delta(n) = \left(p - \left(\frac{\Delta}{p}\right)\right)\left(q - \left(\frac{\Delta}{q}\right)\right).$$

- Pour déchiffrer $c \in G$, on calcule

$$c^{\varphi_\Delta} = g^{\varphi_\Delta m} = 1 + \varphi_\Delta m n \sqrt{\Delta}.$$

- La sécurité du système est liée à la factorisation.
- La sécurité sémantique est équivalente à la reconnaissance des puissances n–ièmes de G.

Comparaison des cryptosystèmes

Cryptosystème	Paillier	Galbraith	Paillier quad.
Cadre	$(\mathbf{Z}/n^2\mathbf{Z})^\times$	E_{n^2}	$\left(\mathcal{O}_\Delta/n^2\mathcal{O}_\Delta\right)^\wedge$
Chiffrement	$(\frac{9}{2}\lvert n\rvert+1)\mathrm{M}$	$(35\lvert n\rvert+3)\mathrm{M}$	$(9\lvert n\rvert+7)\mathrm{M}$
Déchiffrement	$\left(\frac{3}{2}\lvert n\rvert+\frac{5}{3}\right)\mathrm{M}$	$(21\lvert n\rvert+\frac{5}{3})\mathrm{M}$	$\left(3\lvert n\rvert+\frac{4}{3}\right)\mathrm{M}$

- M : multiplication modulo n.
- Système homomorphique fonctionnel, basé sur un problème différent que Paillier : diversité.

Plan

Principe

- On prend $n = pq$, un entier RSA.
- $(\mathcal{O}_\Delta/n\mathcal{O}_\Delta)^\wedge$ est d'ordre $\varphi_\Delta(n) = \left(p - \left(\frac{\Delta}{p}\right)\right)\left(q - \left(\frac{\Delta}{q}\right)\right)$.
- Soit e premier avec $(p^2-1)(q^2-1)$, le morphisme

$$\alpha \mapsto \alpha^e,$$

est un automorphisme de $(\mathcal{O}_\Delta/n\mathcal{O}_\Delta)^\wedge$ d'inverse

$$\alpha \mapsto \alpha^d,$$

avec $d \equiv e^{-1} \pmod{(p^2-1)(q^2-1)}$.
- Si $\alpha = \frac{m+\sqrt{\Delta}}{2}$, $\mathrm{Tr}(\alpha^e) = V_e(m,1)$ avec $\Delta = m^2 - 4$.

Cryptosystème LUC (Smith et Lennon 1993)

- Soit $\Lambda := \{x \in \mathbf{N},\, x < n, \mathrm{pgcd}(x^2-4, n) = 1\}$.
- On définit la fonction $\mathrm{LUC}_{n,e}$:

$$\mathrm{LUC}_{n,e} : \begin{cases} \Lambda & \longrightarrow & \Lambda \\ m & \longmapsto & \mathrm{V}_e(m) := \mathrm{V}_e(m,1) \bmod n \end{cases}$$

- $\mathrm{LUC}_{n,e}$ est une permutation de Λ d'inverse $\mathrm{LUC}_{n,d}$.
- Complexité similaire à celle de RSA, en moyenne 1/3 de multiplications en plus.
- La sécurité de LUC repose sur la factorisation de n.

Plan

Comparaison

- On construit un système probabiliste avec la fonction LUC en utilisant la deuxième construction.
- Comparaison avec d'autres cryptosystèmes probabilistes :
  - ElGamal EC : courbe elliptique sur $\mathbf{F}_p$, avec p de 192 bits, autres systèmes module RSA, n, de 1024 bits.
  - Unité : Multiplication modulo n par kilo bits chiffrés.

Système	Catalano	Galindo	El Gamal EC	LUC proba
Chiffrement	52	125	600	97
Déchiffrement	565	6952	301	765

- LUC proba légèrement plus lent que Catalano *et al.*
- Systèmes non basés sur RSA : LUC proba concurrence sérieusement El Gamal elliptique.