Couplages sur courbes elliptiques et applications en cryptographie
Sous la direction de Louis Goubin
Soutenance de stage du Master Algèbre Appliquée

V. Vitse

Université Versailles Saint-Quentin - Laboratoire PRISM

10 septembre 2008

Plan

Petit aperçu historique - Rappels présoutenance

- *DL (Problème du Logarithme discret)* : $(g, g^a) \dashrightarrow a$
  algorithme sous-exp. sur $\mathbf{F}_q^*$, en général exp. sur $E(\mathbf{F}_q)$
- Miller & Koblitz (1985) : transformer les protocoles crypto dont la sécurité repose sur DL en leur analogue elliptique $\Rightarrow$ à sécurité égale, des clés et des signatures plus courtes
- 1ère difficulté : calcul de $\#E(\mathbf{F}_q)$
  solution envisagée : utilisation des courbes supersingulière (calcul de cardinalité facile)
- attaque MOV (1993) : réduction de DL à $\mathbf{F}_{q^k}^*$, $k \leq 6$ grâce au couplage de Weil
- à partir de 2000 : échange tripartite de A. Joux, IBE de Boneh-Franklin... révélation des couplages dans le milieu cryptographique

Petit aperçu historique - Rappels présoutenance

- *DL (Problème du Logarithme discret)* : $(g, g^a) \dashrightarrow a$
  algorithme sous-exp. sur $\mathbf{F}_q^*$, en général exp. sur $E(\mathbf{F}_q)$
- Miller & Koblitz (1985) : transformer les protocoles crypto dont la sécurité repose sur DL en leur analogue elliptique $\Rightarrow$ à sécurité égale, des clés et des signatures plus courtes
- 1ère difficulté : calcul de $\#E(\mathbf{F}_q)$
  solution envisagée : utilisation des courbes supersingulière (calcul de cardinalité facile)
- attaque MOV (1993) : réduction de DL à $\mathbf{F}_{q^k}^*$, $k \leq 6$ grâce au couplage de Weil
- à partir de 2000 : échange tripartite de A. Joux, IBE de Boneh-Franklin... révélation des couplages dans le milieu cryptographique

Petit aperçu historique - Rappels présoutenance

- *DL (Problème du Logarithme discret)* : $(g, g^a) \dashrightarrow a$
  algorithme sous-exp. sur $\mathbf{F}_q^*$, en général exp. sur $E(\mathbf{F}_q)$
- Miller & Koblitz (1985) : transformer les protocoles crypto dont la sécurité repose sur DL en leur analogue elliptique $\Rightarrow$ à sécurité égale, des clés et des signatures plus courtes
- 1ère difficulté : calcul de $\#E(\mathbf{F}_q)$
  solution envisagée : utilisation des courbes supersingulière (calcul de cardinalité facile)
- attaque MOV (1993) : réduction de DL à $\mathbf{F}_{q^k}^*$, $k \leq 6$ grâce au couplage de Weil
- à partir de 2000 : échange tripartite de A. Joux, IBE de Boneh-Franklin... révélation des couplages dans le milieu cryptographique

Petit aperçu historique - Rappels présoutenance

- *DL (Problème du Logarithme discret)* : $(g, g^a) \dashrightarrow a$
  algorithme sous-exp. sur $\mathbf{F}_q^*$, en général exp. sur $E(\mathbf{F}_q)$
- Miller & Koblitz (1985) : transformer les protocoles crypto dont la sécurité repose sur DL en leur analogue elliptique $\Rightarrow$ à sécurité égale, des clés et des signatures plus courtes
- 1ère difficulté : calcul de $\#E(\mathbf{F}_q)$
  solution envisagée : utilisation des courbes supersingulière (calcul de cardinalité facile)
- attaque MOV (1993) : réduction de DL à $\mathbf{F}_{q^k}^*$, $k \leq 6$ grâce au couplage de Weil
- à partir de 2000 : échange tripartite de A. Joux, IBE de Boneh-Franklin... révélation des couplages dans le milieu cryptographique

Petit aperçu historique - Rappels présoutenance

- *DL (Problème du Logarithme discret)* : $(g, g^a) \dashrightarrow a$
  algorithme sous-exp. sur $\mathbf{F}_q^*$, en général exp. sur $E(\mathbf{F}_q)$
- Miller & Koblitz (1985) : transformer les protocoles crypto dont la sécurité repose sur DL en leur analogue elliptique $\Rightarrow$ à sécurité égale, des clés et des signatures plus courtes
- 1ère difficulté : calcul de $\#E(\mathbf{F}_q)$
  solution envisagée : utilisation des courbes supersingulière (calcul de cardinalité facile)
- attaque MOV (1993) : réduction de DL à $\mathbf{F}_{q^k}^*$, $k \leq 6$ grâce au couplage de Weil
- à partir de 2000 : échange tripartite de A. Joux, IBE de Boneh-Franklin... révélation des couplages dans le milieu cryptographique

Plan

Couplages en cryptographie

Soient $G_1 = \langle P \rangle$, $G_2 = \langle Q \rangle$ et G_3 des groupes cycliques d'ordre r premier. Deux types de couplages (= application bilinéaire, non dégénérée, efficacement calculable) :

- *"self-pairings"* : $\hat{e} : G_1 \times G_1 \longrightarrow G_3$
- *couplages asymétriques* : $e : G_1 \times G_2 \longrightarrow G_3$

Couplages en cryptographie

Soient $G_1 = \langle P \rangle$, $G_2 = \langle Q \rangle$ et G_3 des groupes cycliques d'ordre r premier. Deux types de couplages (= application bilinéaire, non dégénérée, efficacement calculable) :

- *"self-pairings"* : $\hat{e} : G_1 \times G_1 \longrightarrow G_3$
- *couplages asymétriques* : $e : G_1 \times G_2 \longrightarrow G_3$

Quelques hypothèses de sécurité sous-jacentes

- *DBDH* : $[a]P, [b]P, [c]P, \hat{e}(P,P)^d \dashrightarrow d =^? abc$
- *BDH* : $[a]P, [b]P, [c]P \dashrightarrow \hat{e}(P,P)^{abc}$
- *Co-BDH* : $[a]P, [b]P, [a]Q, [c]Q \dashrightarrow e(P,Q)^{abc}$
- *Inversion problem* : $e([a]P, Q) \dashrightarrow [a]P$

Schéma de chiffrement Identity-Based (IBE)

Shamir (1984) : concept de cryptosystèmes à clefs publiques "ID-based" pour simplifier la gestion basée sur PKI et certificats

IBE = `setup` + `extract` + `encrypt` + `decrypt`

Schéma de chiffrement Identity-Based (IBE)

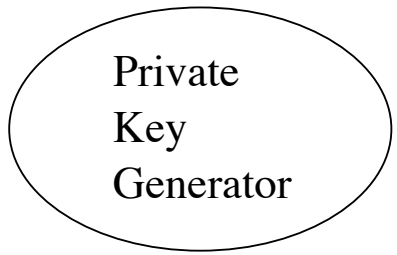


Schéma de chiffrement Identity-Based (IBE)

setup

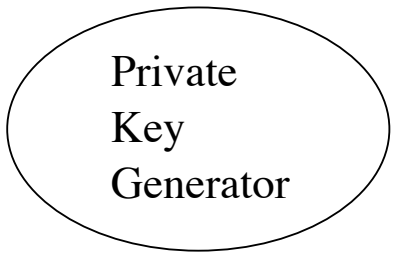


Schéma de chiffrement Identity-Based (IBE)

setup

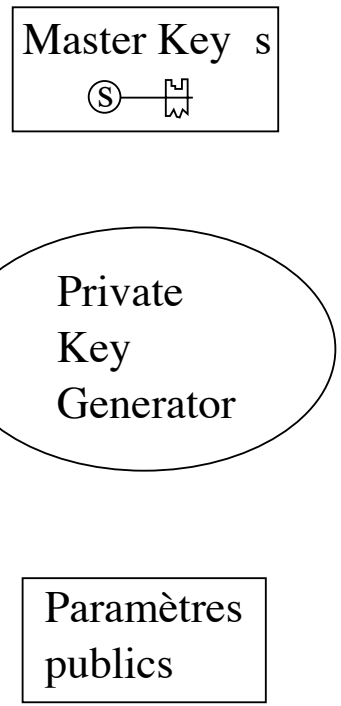
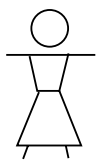
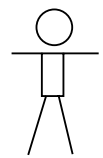


Schéma de chiffrement Identity-Based (IBE)

setup



Alice



Bob

Schéma de chiffrement Identity-Based (IBE)

setup

encrypt

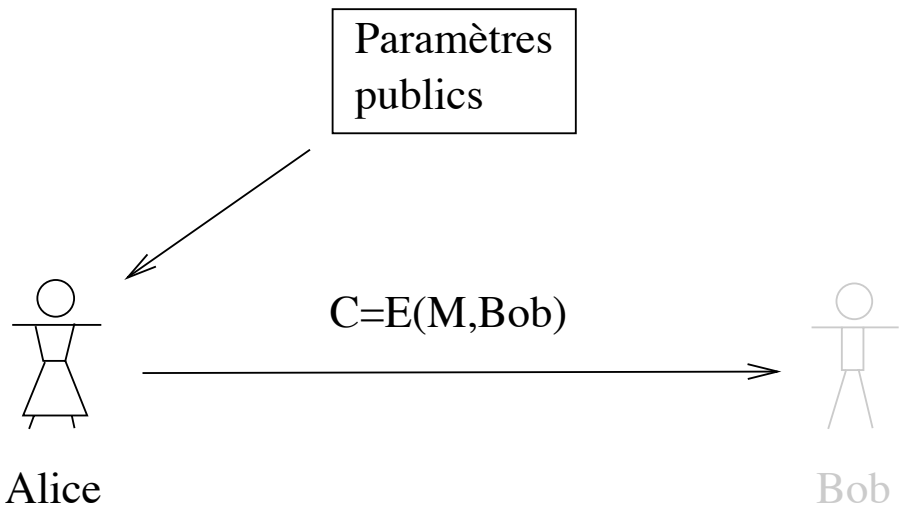


Schéma de chiffrement Identity-Based (IBE)

setup

encrypt

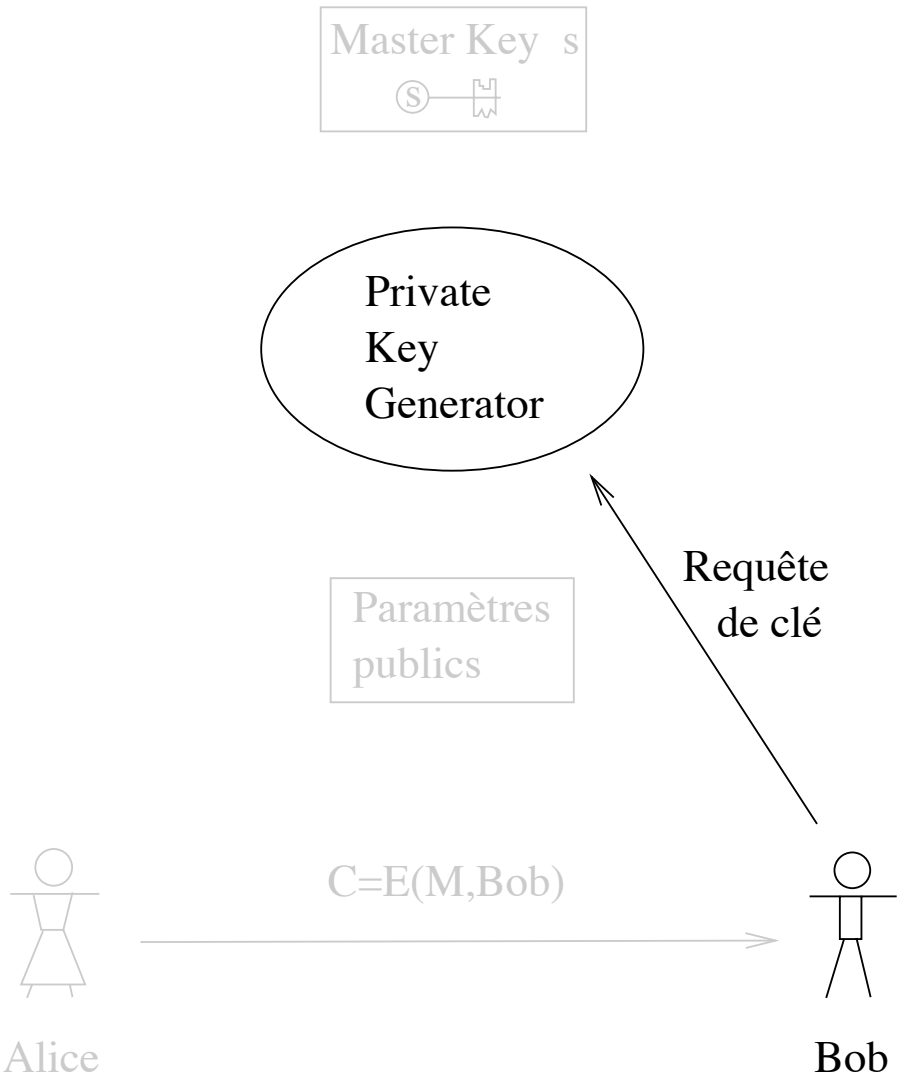


Schéma de chiffrement Identity-Based (IBE)

setup

encrypt

extract

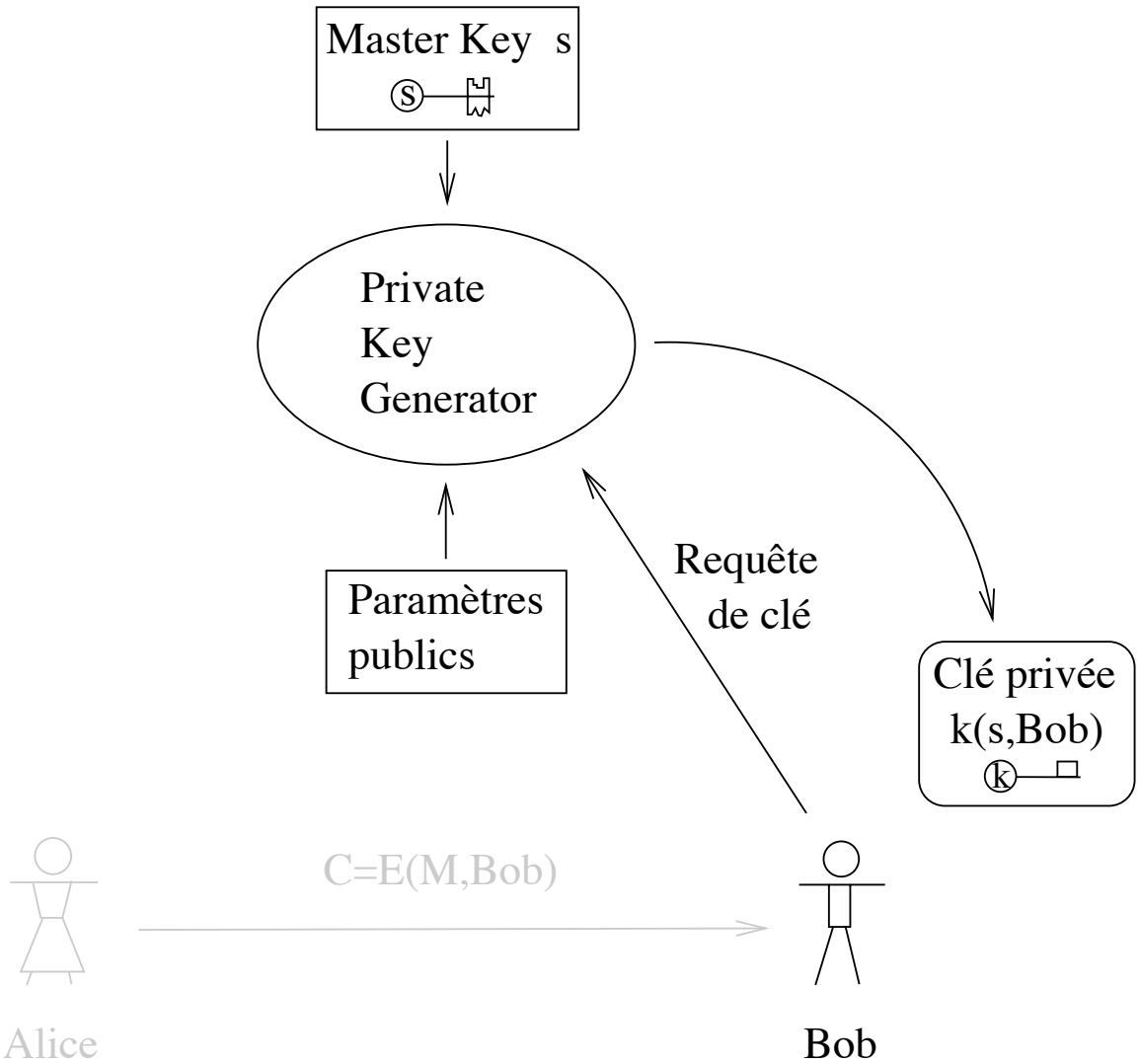


Schéma de chiffrement Identity-Based (IBE)

setup
encrypt
extract
decrypt

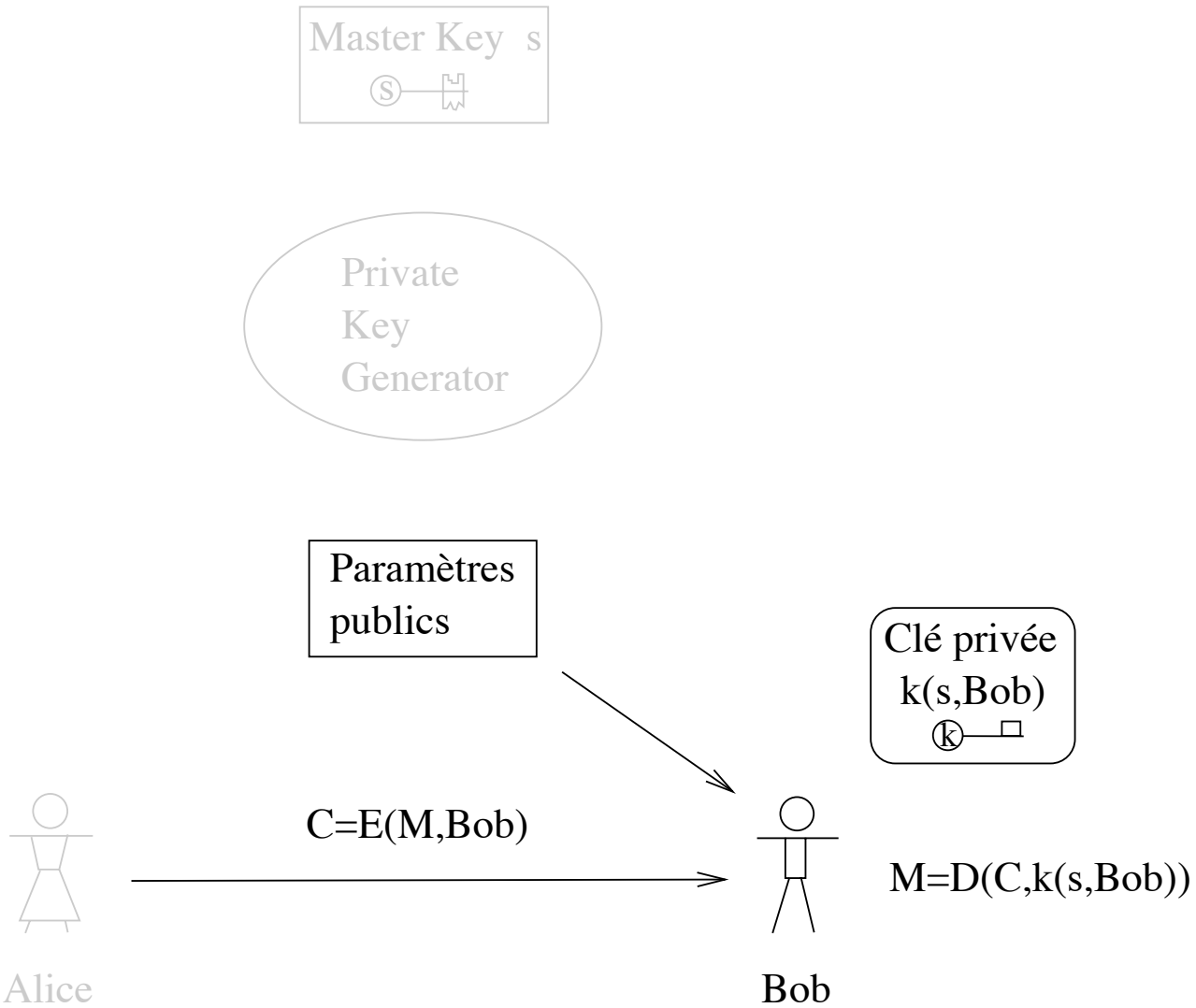


Schéma de chiffrement Identity-Based (IBE)

setup
encrypt
extract
decrypt

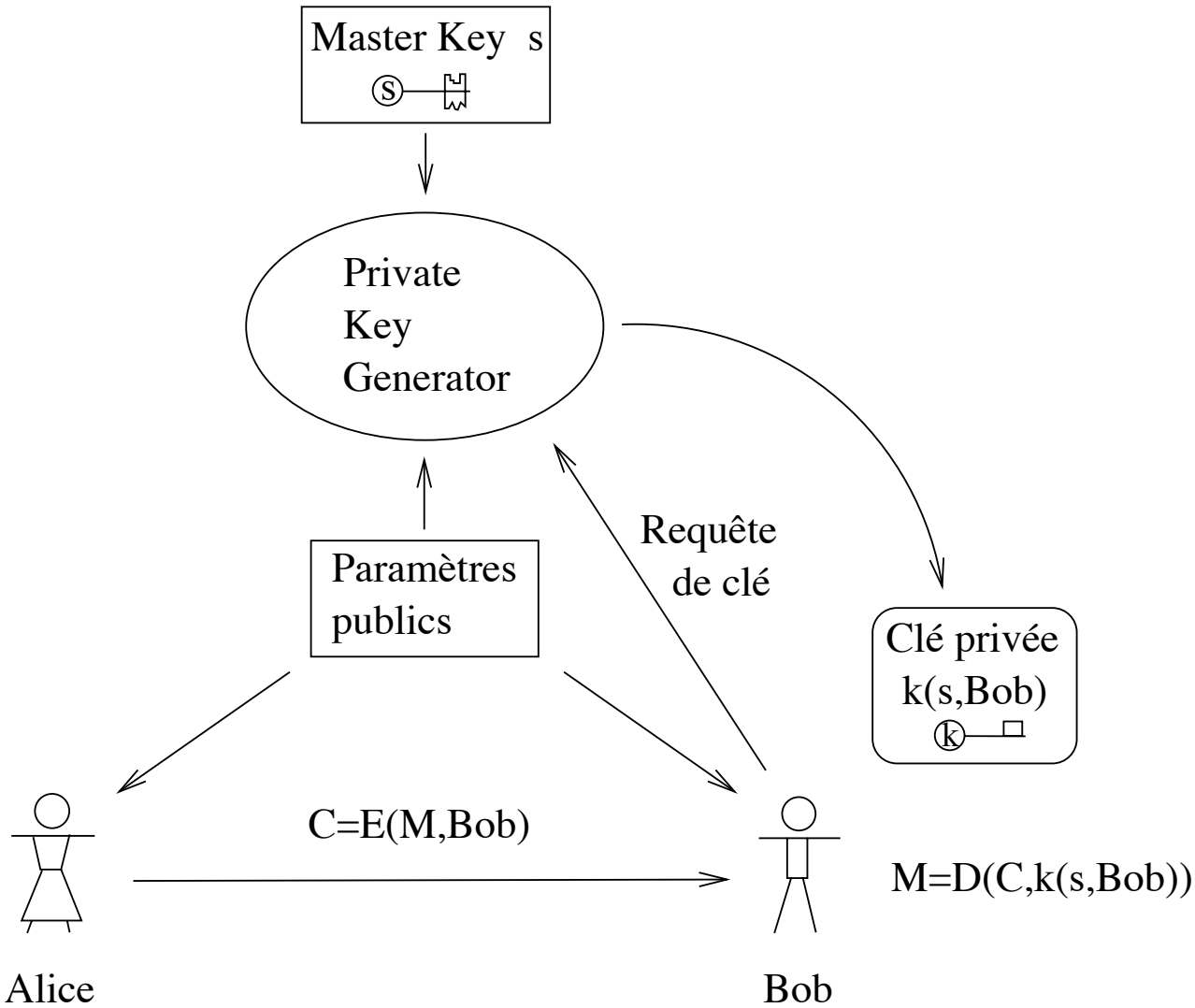


Schéma IBE de Boneh-Franklin avec couplage asymétrique

Soient $G_1 = \langle P \rangle$, $G_2 = \langle Q \rangle$, G_3 cycliques d'ordre r premier,
et $e : G_1 \times G_2 \longrightarrow G_3$ tels que *Co-BDH* est difficile.

Schéma IBE de Boneh-Franklin avec couplage asymétrique

Soient $G_1 = \langle P \rangle$, $G_2 = \langle Q \rangle$, G_3 cycliques d'ordre r premier, et $e : G_1 \times G_2 \longrightarrow G_3$ tels que *Co-BDH* est difficile.

On présente le schéma de chiffrement `BasicIdent` décomposé en 4 algorithmes : `setup`, `extract`, `encrypt` et `decrypt`

- `setup`
  - choisir $s \in \mathbf{Z}_r^*$ et calculer $P_{pub} = [s]P$
  - prendre $H_1 : \{0;1\}^* \longrightarrow G_2$ et $H_2 : G_3 \longrightarrow \{0;1\}^n$ (n =taille des blocs)
  - prendre $\mathcal{M} = \{0;1\}^n$ et $\mathcal{C} = G_1 \times \{0;1\}^n$
  - paramètres publics : $\langle G_1, G_2, G_3, e, P, P_{pub}, Q, H_1, H_2 \rangle$
  - "master-key" : $s \in \mathbf{Z}_r^*$

Schéma IBE de Boneh-Franklin avec couplage asymétrique

Soient $G_1 = \langle P \rangle$, $G_2 = \langle Q \rangle$, G_3 cycliques d'ordre r premier,
et $e : G_1 \times G_2 \longrightarrow G_3$ tels que *Co-BDH* est difficile.

On présente le schéma de chiffrement `BasicIdent` décomposé en 4 algorithmes : `setup`, `extract`, `encrypt` et `decrypt`

- `setup`
  - choisir $s \in \mathbf{Z}_r^*$ et calculer $P_{pub} = [s]P$
  - prendre $H_1 : \{0;1\}^* \longrightarrow G_2$ et $H_2 : G_3 \longrightarrow \{0;1\}^n$ (n =taille des blocs)
  - prendre $\mathcal{M} = \{0;1\}^n$ et $\mathcal{C} = G_1 \times \{0;1\}^n$
  - paramètres publics : $\langle G_1, G_2, G_3, e, P, P_{pub}, Q, H_1, H_2 \rangle$
  - "master-key" : $s \in \mathbf{Z}_r^*$

Schéma IBE de Boneh-Franklin avec couplage asymétrique

Chiffrement `BasicIdent` :

- `encrypt` : calcule le chiffré de $M \in \mathcal{M}$ destiné à un utilisateur à partir de son identité Id :
  - calculer $Q_{Id} = H_1(Id) \in G_2$, choisir $t \in_R \mathbf{Z}_r^*$
  - envoyer $C = \langle [t]P, M \oplus H_2(e(P_{pub}, Q_{Id})^t) \rangle$
- `extract` : calcule à partir de Id la clé privée $S_{Id} = [s]Q_{Id} \in G_2$
- `decrypt` : déchiffre $C = \langle C_1, C_2 \rangle$ avec la clé privée S_{Id} en calculant

$$M' = C_2 \oplus H_2(e(C_1, S_{Id}))$$

Schéma IBE de Boneh-Franklin avec couplage asymétrique

Chiffrement `BasicIdent` :

- `encrypt` : calcule le chiffré de $M \in \mathcal{M}$ destiné à un utilisateur à partir de son identité Id :
  - calculer $Q_{Id} = H_1(Id) \in G_2$, choisir $t \in_R \mathbf{Z}_r^*$
  - envoyer $C = \langle [t]P, M \oplus H_2(e(P_{pub}, Q_{Id})^t) \rangle$
- `extract` : calcule à partir de Id la clé privée $S_{Id} = [s]Q_{Id} \in G_2$
- `decrypt` : déchiffre $C = \langle C_1, C_2 \rangle$ avec la clé privée S_{Id} en calculant

$$M' = C_2 \oplus H_2(e(C_1, S_{Id}))$$

Schéma IBE de Boneh-Franklin avec couplage asymétrique

Chiffrement `BasicIdent` :

- `encrypt` : calcule le chiffré de $M \in \mathcal{M}$ destiné à un utilisateur à partir de son identité Id :
  - calculer $Q_{Id} = H_1(Id) \in G_2$, choisir $t \in_R \mathbf{Z}_r^*$
  - envoyer $C = \langle [t]P, M \oplus H_2(e(P_{pub}, Q_{Id})^t) \rangle$
- `extract` : calcule à partir de Id la clé privée $S_{Id} = [s]Q_{Id} \in G_2$
- `decrypt` : déchiffre $C = \langle C_1, C_2 \rangle$ avec la clé privée S_{Id} en calculant

$$M' = C_2 \oplus H_2(e(C_1, S_{Id}))$$

Schéma IBE de Boneh-Franklin avec couplage asymétrique

Chiffrement `BasicIdent` :

- `encrypt` : calcule le chiffré de $M \in \mathcal{M}$ destiné à un utilisateur à partir de son identité Id :
  - calculer $Q_{Id} = H_1(Id) \in G_2$, choisir $t \in_R \mathbf{Z}_r^*$
  - envoyer $C = \langle [t]P, M \oplus H_2(e(P_{pub}, Q_{Id})^t) \rangle$
- `extract` : calcule à partir de Id la clé privée $S_{Id} = [s]Q_{Id} \in G_2$
- `decrypt` : déchiffre $C = \langle C_1, C_2 \rangle$ avec la clé privée S_{Id} en calculant

$$M' = C_2 \oplus H_2(e(C_1, S_{Id}))$$

- **Consistance du schéma :**

$$e(P_{pub}, Q_{Id})^t = e(P, Q_{Id})^{st} = e([t]P, [s]Q_{Id}) = e(C_1, S_{Id})$$

Schéma IBE de Boneh-Franklin avec couplage asymétrique

Chiffrement `BasicIdent` :

- `encrypt` : calcule le chiffré de $M \in \mathcal{M}$ destiné à un utilisateur à partir de son identité Id :
  - calculer $Q_{Id} = H_1(Id) \in G_2$, choisir $t \in_R \mathbf{Z}_r^*$
  - envoyer $C = \langle [t]P, M \oplus H_2(e(P_{pub}, Q_{Id})^t) \rangle$
- `extract` : calcule à partir de Id la clé privée $S_{Id} = [s]Q_{Id} \in G_2$
- `decrypt` : déchiffre $C = \langle C_1, C_2 \rangle$ avec la clé privée S_{Id} en calculant

$$M' = C_2 \oplus H_2(e(C_1, S_{Id}))$$

- **Consistance du schéma :**

$$e(P_{pub}, Q_{Id})^t = e(P, Q_{Id})^{st} = e([t]P, [s]Q_{Id}) = e(C_1, S_{Id})$$

Sémantiquement sûr si *Co-BDH* supposé difficile.

Plan

En pratique : quelle courbe ? quel couplage ?

(E, O) courbe elliptique définie sur $\mathbf{F}_q$.

Notations :

- *r-torsion* : $E[r] = \{P \in E : [r]P = O\}$ (ici $r | \#E(\mathbf{F}_q)$ premier, $r \neq p$)
- *degré de plongement* : $k = \min\{e : r | (q^e - 1)\}$
- μ_r : racines r-èmes de l'unité dans $\mathbf{F}_{q^k}$

En pratique : quelle courbe ? quel couplage ?

(E, O) courbe elliptique définie sur $\mathbf{F}_q$.

Notations :

- *r-torsion* : $E[r] = \{P \in E : [r]P = O\}$ (ici $r | \#E(\mathbf{F}_q)$ premier, $r \neq p$)
- *degré de plongement* : $k = \min\{e : r|(q^e - 1)\}$
- μ_r : racines r-èmes de l'unité dans $\mathbf{F}_{q^k}$

Couplages connus :

- *Weil* (bilinéaire, non dégénéré et alterné)

$$\begin{array}{rcl} E[r] \times E[r] & \rightarrow & \mu_r \subset \mathbf{F}_{q^k}^* \\ (P, Q) & \mapsto & e(P, Q)_r = (-1)^r \frac{f_P(Q)}{f_Q(P)} \end{array}$$

- *Tate* (bilinéaire et non dégénéré)

$$\begin{array}{rcl} E(\mathbf{F}_{q^k})[r] \times E(\mathbf{F}_{q^k})/(rE(\mathbf{F}_{q^k})) & \rightarrow & \mu_r \subset \mathbf{F}_{q^k}^* \\ (P, Q) & \mapsto & \langle P, Q \rangle_r = f_P(Q)^{\frac{q^k - 1}{r}} \end{array}$$

Des couplages efficacement calculables

- En général, Tate non dégénéré sur $E(\mathbf{F}_{q^k})[r] \times E(\mathbf{F}_{q^k})[r]$, car

$$E(\mathbf{F}_{q^k})[r] \simeq E(\mathbf{F}_{q^k})/(rE(\mathbf{F}_{q^k})) \Leftrightarrow E(\mathbf{F}_{q^k})[r^2] = E(\mathbf{F}_{q^k})[r]$$

- **Algorithme de Miller** : permet un calcul efficace de $f_P(Q)$, si $P \in E(\mathbf{F}_q)[r]$ et $Q \in E(\mathbf{F}_{q^k})$, complexité en

$$O\left((\log q)^{\mu+1}(\log r + k^{\mu+1})\right)$$

$\Rightarrow$ pour un calcul rapide, le degré de plongement k ne doit pas être trop grand...

- **Problème :** Pour une courbe aléatoire, k est grand de l'ordre de r [Balasubramanian-Koblitz]

Des couplages efficacement calculables

- En général, Tate non dégénéré sur $E(\mathbf{F}_{q^k})[r] \times E(\mathbf{F}_{q^k})[r]$, car

$$E(\mathbf{F}_{q^k})[r] \simeq E(\mathbf{F}_{q^k})/(rE(\mathbf{F}_{q^k})) \Leftrightarrow E(\mathbf{F}_{q^k})[r^2] = E(\mathbf{F}_{q^k})[r]$$

- **Algorithme de Miller** : permet un calcul efficace de $f_P(Q)$, si $P \in E(\mathbf{F}_q)[r]$ et $Q \in E(\mathbf{F}_{q^k})$, complexité en

$$O\left((\log q)^{\mu+1}(\log r + k^{\mu+1})\right)$$

$\Rightarrow$ pour un calcul rapide, le degré de plongement k ne doit pas être trop grand...

- **Problème :** Pour une courbe aléatoire, k est grand de l'ordre de r [Balasubramanian-Koblitz]

Des couplages efficacement calculables

- En général, Tate non dégénéré sur $E(\mathbf{F}_{q^k})[r] \times E(\mathbf{F}_{q^k})[r]$, car

$$E(\mathbf{F}_{q^k})[r] \simeq E(\mathbf{F}_{q^k})/(rE(\mathbf{F}_{q^k})) \Leftrightarrow E(\mathbf{F}_{q^k})[r^2] = E(\mathbf{F}_{q^k})[r]$$

- **Algorithme de Miller** : permet un calcul efficace de $f_P(Q)$, si $P \in E(\mathbf{F}_q)[r]$ et $Q \in E(\mathbf{F}_{q^k})$, complexité en

$$O\left((\log q)^{\mu+1}(\log r + k^{\mu+1})\right)$$

$\Rightarrow$ pour un calcul rapide, le degré de plongement k ne doit pas être trop grand...

- **Problème :** Pour une courbe aléatoire, k est grand de l'ordre de r [Balasubramanian-Koblitz]

Courbes "pairing-friendly"

Solution n°1 : utiliser des courbes supersingulières ($k \leq 6$)

MAIS Tate est alterné sur ces courbes donc mauvais candidat tel quel pour "self-pairing" $\rightsquigarrow$ utiliser des *applications de distorsion* (Verheul)

Définition

Soit $P \in E[r]$, $\varphi \in End(E)$ est une application de distorsion si

$$Q \in \langle P \rangle, Q \neq O \Rightarrow \varphi(Q) \notin \langle P \rangle$$

Théorème

Si E est supersingulière, il existe des applications de distorsion et si $k > 1$

$$\begin{array}{rcl} E(\mathbf{F}_q)[r] \times E(\mathbf{F}_q)[r] & \longrightarrow & \mu_r \subset \mathbf{F}_{q^k}^* \\ (P, Q) & \mapsto & \hat{e}(P, Q) = \langle P, \varphi(Q) \rangle_r \end{array} \quad \textit{est un self-pairing.}$$

Courbes "pairing-friendly"

Solution n°1 : utiliser des courbes supersingulières ($k \leq 6$)
MAIS Tate est alterné sur ces courbes donc mauvais candidat tel quel pour "self-pairing" $\rightsquigarrow$ utiliser des *applications de distorsion* (Verheul)

Définition

Soit $P \in E[r]$, $\varphi \in End(E)$ est une application de distorsion si

$$Q \in \langle P \rangle, Q \neq O \Rightarrow \varphi(Q) \notin \langle P \rangle$$

Théorème

Si E est supersingulière, il existe des applications de distorsion et si $k > 1$

$$\begin{array}{rcl} E(\mathbf{F}_q)[r] \times E(\mathbf{F}_q)[r] & \rightarrow & \mu_r \subset \mathbf{F}_{q^k}^* \\ (P, Q) & \mapsto & \hat{e}(P, Q) = \langle P, \varphi(Q) \rangle_r \end{array}$$

est un self-pairing.

Méthode de multiplication complexe

Solution n°2 : trouver des courbes ordinaires avec un degré de plongement petit en utilisant la méthode de multiplication complexe (CM)

- Idée d'Atkin et Morain : adapter au cas des corps finis la théorie de la CM pour les courbes elliptiques définies sur $\mathbf{C}$
- En pratique : étant donnés q premier, t tel que $|t| \leq 2\sqrt{q}$ et D (*discriminant fondamental*) tels que

$$4q - t^2 = Dy^2$$

  la méthode CM construit une courbe elliptique sur $\mathbf{F}_q$ de cardinal $q + 1 \pm t$
- la méthode est efficace si D petit

Méthode de multiplication complexe

Solution n°2 : trouver des courbes ordinaires avec un degré de plongement petit en utilisant la méthode de multiplication complexe (CM)

- Idée d'Atkin et Morain : adapter au cas des corps finis la théorie de la CM pour les courbes elliptiques définies sur $\mathbf{C}$
- En pratique : étant donnés q premier, t tel que $|t| \leq 2\sqrt{q}$ et D (*discriminant fondamental*) tels que

$$4q - t^2 = Dy^2$$

  la méthode CM construit une courbe elliptique sur $\mathbf{F}_q$ de cardinal $q + 1 \pm t$
- la méthode est efficace si D petit

Courbes MNT

- Comment choisir q et t pour avoir un degré k de plongement petit ?
- Idée de Miyaji, Nakabayashi et Takano : paramétrer q et t quadratiquement

Théorème (MNT)

Si E courbe elliptique ordinaire définie sur $\mathbf{F}_q$ telle que $\#E(\mathbf{F}_q) = q + 1 - t$ premier et $k = 6$, alors $q = 4l^2 + 1$ et $t = \pm 2l$.

$\rightsquigarrow$ le problème se ramène à la résolution l'équation de Pell

$$x^2 - 3Dy^2 = -8$$

- D'autres familles de courbes peuvent être obtenues avec des méthodes type Cocks-Pinch, Brezing-Weng...

Courbes MNT

- Comment choisir q et t pour avoir un degré k de plongement petit ?
- Idée de Miyaji, Nakabayashi et Takano : paramétrer q et t quadratiquement

Théorème (MNT)

Si E courbe elliptique ordinaire définie sur $\mathbf{F}_q$ telle que $\#E(\mathbf{F}_q) = q + 1 - t$ premier et $k = 6$, alors $q = 4l^2 + 1$ et $t = \pm 2l$.

$\rightsquigarrow$ le problème se ramène à la résolution l'équation de Pell

$$x^2 - 3Dy^2 = -8$$

- D'autres familles de courbes peuvent être obtenues avec des méthodes type Cocks-Pinch, Brezing-Weng...

Courbes MNT

- Comment choisir q et t pour avoir un degré k de plongement petit ?
- Idée de Miyaji, Nakabayashi et Takano : paramétrer q et t quadratiquement

Théorème (MNT)

Si E courbe elliptique ordinaire définie sur $\mathbf{F}_q$ telle que $\#E(\mathbf{F}_q) = q + 1 - t$ premier et $k = 6$, alors $q = 4l^2 + 1$ et $t = \pm 2l$.

$\rightsquigarrow$ le problème se ramène à la résolution l'équation de Pell

$$x^2 - 3Dy^2 = -8$$

- D'autres familles de courbes peuvent être obtenues avec des méthodes type Cocks-Pinch, Brezing-Weng...

Courbes "pairing-friendly" ordinaires ?

Tate est-il un bon candidat sur les courbes ordinaires ?

- Si $k = 1$, et si $r^2 \nmid \#E(\mathbf{F}_q)$, Tate est un self-pairing.
  MAIS ce sont des courbes difficiles à trouver en pratique...
- Si $k > 1$, Tate est toujours dégénéré sur $E(\mathbf{F}_q)[r] \times E(\mathbf{F}_q)[r]$...

Pire :

Théorème (Verheul)

Sur les courbes ordinaires, il n'y a pas d'applications de distorsion.

Par contre, si $k > 1$, on a (Balasubramanian-Koblitz)

$$E(\mathbf{F}_{q^k})[r] = E[r] \simeq \mathbf{Z}/r\mathbf{Z} \times \mathbf{Z}/r\mathbf{Z}$$

Conséquence :
si $G_1 = \langle P \rangle$ et $G_2 = \langle Q \rangle$ où $P \in E(\mathbf{F}_q)[r]$ et $Q \in E(\mathbf{F}_q^k)[r] \setminus G_1$,
alors $\langle ., . \rangle : G_1 \times G_2 \longrightarrow \mathbf{F}_{q^k}^*$ est un couplage asymétrique non dégénéré.

Courbes "pairing-friendly" ordinaires ?

Tate est-il un bon candidat sur les courbes ordinaires ?

- Si $k = 1$, et si $r^2 \nmid \#E(\mathbf{F}_q)$, Tate est un self-pairing.
  MAIS ce sont des courbes difficiles à trouver en pratique...
- Si $k > 1$, Tate est toujours dégénéré sur $E(\mathbf{F}_q)[r] \times E(\mathbf{F}_q)[r]$...

Pire :

Théorème (Verheul)

Sur les courbes ordinaires, il n'y a pas d'applications de distorsion.

Par contre, si $k > 1$, on a (Balasubramanian-Koblitz)

$$E(\mathbf{F}_{q^k})[r] = E[r] \simeq \mathbf{Z}/r\mathbf{Z} \times \mathbf{Z}/r\mathbf{Z}$$

Conséquence :
si $G_1 = \langle P \rangle$ et $G_2 = \langle Q \rangle$ où $P \in E(\mathbf{F}_q)[r]$ et $Q \in E(\mathbf{F}_q^k)[r] \setminus G_1$,
alors $\langle ., . \rangle : G_1 \times G_2 \longrightarrow \mathbf{F}_{q^k}^*$ est un couplage asymétrique non dégénéré.

Courbes "pairing-friendly" ordinaires ?

Tate est-il un bon candidat sur les courbes ordinaires ?

- Si $k = 1$, et si $r^2 \nmid \#E(\mathbf{F}_q)$, Tate est un self-pairing.
  MAIS ce sont des courbes difficiles à trouver en pratique...
- Si $k > 1$, Tate est toujours dégénéré sur $E(\mathbf{F}_q)[r] \times E(\mathbf{F}_q)[r]$...

Pire :

Théorème (Verheul)

Sur les courbes ordinaires, il n'y a pas d'applications de distorsion.

Par contre, si $k > 1$, on a (Balasubramanian-Koblitz)

$$E(\mathbf{F}_{q^k})[r] = E[r] \simeq \mathbf{Z}/r\mathbf{Z} \times \mathbf{Z}/r\mathbf{Z}$$

Conséquence :
si $G_1 = \langle P \rangle$ et $G_2 = \langle Q \rangle$ où $P \in E(\mathbf{F}_q)[r]$ et $Q \in E(\mathbf{F}_q^k)[r] \setminus G_1$,
alors $\langle ., . \rangle : G_1 \times G_2 \longrightarrow \mathbf{F}_{q^k}^*$ est un couplage asymétrique non dégénéré.

Plan

Implémentation