

Attaque DPA contre l'algorithme de Miller

N. El Mrabet

ARITH-LIRMM, I3M, CNRS,
Université Montpellier II, France

C2 2008 Carcan
19 mars 2008

Couplage

Définition & Propriétés

Définition

Un couplage est une application qui à deux points d'une courbe elliptique associe un élément d'un corps fini.

Principaux couplages : Weil, Tate et Ate.

$$e_* : (G1 \subset E(\mathbb{F}_q)) \times (G2 \subset E(\mathbb{F}_{q^k})) \rightarrow (G3 \subset \mathbb{F}_{q^k})$$

Propriété

Un couplage est bilinéaire :

$$\forall P, P' \in G1, Q \in G2, e_*(P + P', Q) = e_*(P, Q)e_*(P', Q)$$

et non dégénéré : $\forall P \in S_1 - \{0\}, \exists Q \in G_2$ t.q. $e_*(P, Q) \neq 1$

Couplage

Utilisation en cryptographie

- Destructif : MOV et Frey Ruck attaque.
- Construction de nouveaux protocoles : Cryptographie Basée sur l'Identité (IBC).

Principe

La clé publique d'un utilisateur est son identité.

La clé privée lui est fournie par une autorité de confiance.

Exemple

Echange de clé sécurisée entre Alice et Bob.

IBC

Echange de clé secrète entre Alice et Bob

Autorité de confiance
(Trust Authority)



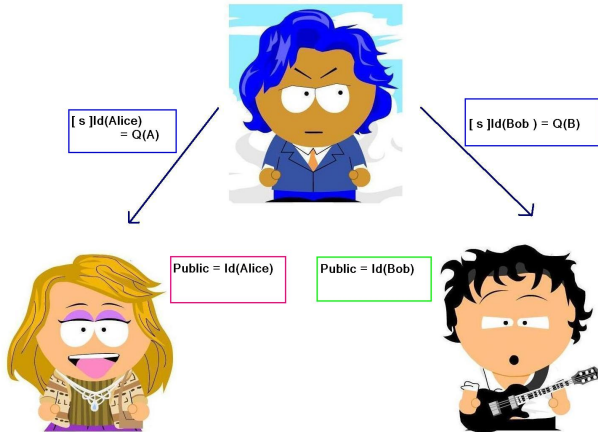
Alice



Bob

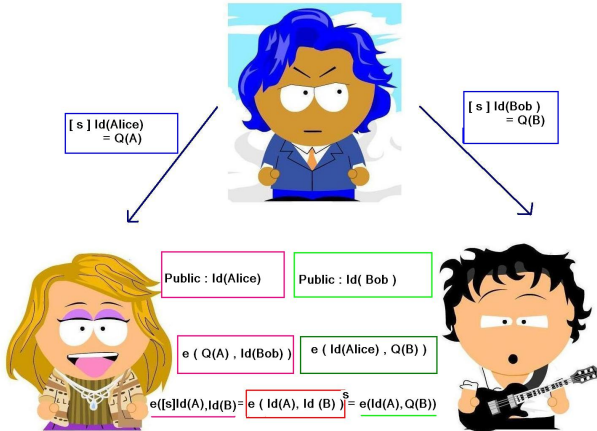
IBC

Echange de clé secrète entre Alice et Bob



IBC

Echange de clé secrète entre Alice et Bob



Calcul d'un couplage dans IBC

Les données

On considère :

- q nombre premier ou puissance d'un nombre premier
- E courbe elliptique d'équation : $y^2 = x^3 + ax + b$, a et $b \in \mathbb{F}_q$
- $P \in E(\mathbb{F}_q)$ l'entrée secrète lors des calculs : P est privé.
- $Q \in E(\mathbb{F}_{q^k})$ l'entrée connue lors des calculs : Q est public.

Calcul d'un couplage dans IBC

Les algorithmes

Les couplages de **Weil**, **Tate** et **Ate** sont tous basés sur l'algorithme du Miller.

Ils sont quotient ou puissance d'une fonction F_P appliquée à Q .

L'algorithme de Miller permet de construire la fonction F_P qui est l'étape centrale des calculs de couplage.

$$e_W(P, Q) = \frac{F_P(Q)}{F_Q(P)}$$

$$e_T(P, Q) = (F_P(Q))^\alpha$$

Algorithm de Miller

Data: $l = (l_n \dots l_0)$,

$P \in E(\mathbb{F}_q)$

and $Q \in E(\mathbb{F}_{q^k})$;

Result: $F_P(Q) \in \mathbb{F}_{q^k}^*$;

1 : $T \leftarrow P$, $f_1 \leftarrow 1$;

for $i = n - 1$ **to** 0 **do**

2 : $T \leftarrow [2]T$;

3 : $f_1 \leftarrow f_1^2 \times h_1(Q)$;

if $l_i = 1$ **then**

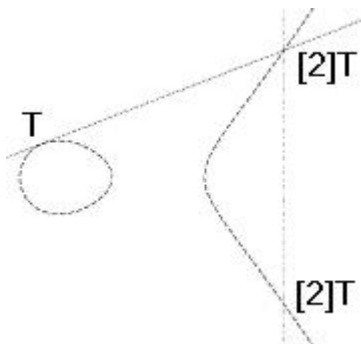
4 : $T \leftarrow T \oplus P$;

5 : $f_1 \leftarrow f_1 \times h_2(Q)$;

end

end

return f_1



Algorithme de Miller

Data: $l = (l_n \dots l_0)$,

$P \in E(\mathbb{F}_q)$

and $Q \in E(\mathbb{F}_{q^k})$;

Result: $F_P(Q) \in \mathbb{F}_{q^k}^*$;

1 : $T \leftarrow P$, $f_1 \leftarrow 1$;

for $i = n - 1$ **to** 0 **do**

2 : $T \leftarrow [2]T$;

3 : $f_1 \leftarrow f_1^2 \times h_1(Q)$;

if $l_i = 1$ **then**

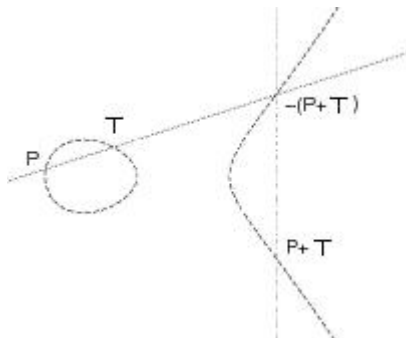
4 : $T \leftarrow T \oplus P$;

5 : $f_1 \leftarrow f_1 \times h_2(Q)$;

end

end

return f_1



Coordonnées affines

L'équation et la cible

L'équation de h_1 en coordonnées affines est :

$$h_1(x_Q, y_Q) = y_Q - \lambda(x_Q - x_T) - y_T$$

L'attaque porte sur la différence $(x_Q - x_T)$ à la première itération de l'algorithme de Miller.

Avec :

- $T = P = (x_P, y_P)$ que l'on cherche.
- Q public que l'on fait varier à volonté.

Illustration

$$\begin{array}{rcccccc} x_{Q_i} & & \dots & 0 & 1 & 0 \\ x_P & - & ? & 1 & 0 & 1 \\ \hline (x_{Q_i} - x_P) & & ? & 1 & 0 & 1 \end{array}$$

Coordonnées affines

Schéma d'attaque

- m point $Q_i \in G_2(\subset E(\mathbb{F}_{q^k}))$ sont choisis ($500 < m < 10000$)
 - Les $j - 1$ bits de poids faibles de x_P sont connus
1. Récupérer les courbes C_i pour $i = 0 \dots m$
 2. Supposer $(x_P)_j = 1$
 - Si $(x_{Q_i} - x_P)_j = 0$ mettre C_i dans S_0
 - Si $(x_{Q_i} - x_P)_j = 1$ mettre C_i dans S_1
 3. Calculer les moyennes $\overline{C_0}$ et $\overline{C_1}$ des paquets S_0 et S_1
 4. Calculer la différence $\Delta = \overline{C_1} - \overline{C_0}$
 - Si la courbe Δ présente un ou des pics de consommation, alors $(x_P)_j = 1$
 - Sinon $(x_P)_j = 0$
 5. on obtient ainsi le $j^{\text{ème}}$ bit de x_P .

Coordonnées affines

Schéma d'attaque

$$h_1(x_Q, y_Q) = y_Q - \lambda(x_Q - x_T) - y_T$$

- Une fois obtenue la valeur de x_P , on utilise l'équation de la courbe pour trouver y_P .
- L'équation de la courbe donne au plus deux valeurs de y_P .

$$y^2 = x^3 + ax + b$$

- En essayant les deux valeurs lors d'une exécution de l'algorithme de Miller, on peut déterminer la bonne.

Coordonnées projectives

L'équation et les cibles

L'équation de h_1 est :

$$h_1(x_Q, y_Q) = Z^2 y_Q - (3X^2 + aZ^2)(x_Q Z - X) - YZ$$

L'attaque porte en premier lieu sur le produit $x_Q Z$, puis sur la différence $(x_Q Z - X)$, toujours sur la première itération où :

- $T = P = (X_P, Y_P, Z_P)$ en coordonnées projectives
- $Q = (x_Q, y_Q)$ en coordonnées affines

Rappel

$T = (X_T, Y_T, Z_T)$ est équivalent à $T = (\frac{X_T}{Z_T}, \frac{Y_T}{Z_T}, 1)$ pour $Z_T \neq 0$

Coordonnées projectives

Schéma d'attaque

- m point $Q_i \in G_2(\subset E(\mathbb{F}_{q^k}))$ sont choisis
 - Les $j - 1$ bits de poids faibles de Z_P sont connus
1. Récupérer les courbes C_i pour $i = 0 \dots m$
 2. Supposer $(Z_P)_j = 1$
 - Si $Z_P \times x_{Q_i j} = 0$ mettre C_i dans S_0
 - Si $Z_P \times x_{Q_i j} = 1$ mettre C_i dans S_1
 3. Calculer les moyennes $\overline{C_0}$ et $\overline{C_1}$ des paquets S_0 et S_1
 4. Calculer la différence $\Delta = \overline{C_1} - \overline{C_0}$
 - Si la courbe Δ présente un ou des pics de consommation, alors $(Z_P)_j = 1$
 - Sinon $(Z_P)_j = 0$
 5. on obtient ainsi le $j^{\text{ème}}$ bit de Z_P .

Coordonnées projectives

Schéma d'attaque

$$h_1(x_Q, y_Q) = Z^2 y_Q - (3X^2 + aZ^2)(x_Q Z - X) - YZ$$

- Une fois obtenue la valeur de Z_P , on réitère le procédé pour retrouver la valeur de X_P via l'opération $(x_Q Z - X)$.
- L'équation de la courbe donne au plus deux valeurs de Y_P .

$$Y^2 = X^3 + aXZ^2 + bZ^3$$

- En essayant les deux valeurs lors d'une exécution de l'algorithme de Miller, on peut déterminer la bonne.

Coordonnées jacobiennes

L'équation et les cibles

L'équation de h_1 est :

$$h_1(Q) = Z_3 Z^2 y_Q - 2Y^2 - (3X^2 - aZ^4)(x_Q Z^2 - X)$$

L'attaque porte en premier lieu sur le produit $x_Q Z^2$, puis :

- soit sur la différence $(x_Q Z^2 - X)$
- soit sur le calcul de $Z_3 Z^2 y_Q = 2YZ \times Z^2 \times y_Q$

sachant que :

- $T = P = (X_P, Y_P, Z_P)$ en coordonnées jacobiennes, et $Z_3 = 2Y_T Z_T$.
- $Q = (x_Q, y_Q)$ en coordonnées affines

Rappel

$T = (X_T, Y_T, Z_T)$ est équivalent à $T = (\frac{X_T}{Z_T^2}, \frac{Y_T}{Z_T^3}, 1)$ pour $Z_T \neq 0$

Coordonnées jacobiniennes

Schéma d'attaque

Le schéma est le même qu'en coordonnées projectives :

$$h_1(Q) = Z_3 Z^2 y_Q - 2Y^2 - (3X^2 - aZ^4)(x_Q Z^2 - X)$$

- Il s'agit d'abord de retrouver Z_P^2 , ce qui nous donne deux possibilités pour Z_P .
- Ensuite, avec ces deux possibilités on réitère le procédé pour trouver les deux valeurs de Y_P associées.
- Enfin, pour trouver X_P , on se sert de l'équation de la courbe :

$$Y^2 = X^3 + aXZ^3 + Z^6$$

- ◊ Ou alors avec Z_P^2 on retrouve X_P via la différence $(x_Q Z^2 - X)$
- ◊ Puis retrouver Y_P à l'aide de l'équation de la courbe.

Coordonnées jacobiniennes

Schéma d'attaque

Le schéma est le même qu'en coordonnées projectives :

$$h_1(Q) = Z_3 Z^2 y_Q - 2Y^2 - (3X^2 - aZ^4)(x_Q Z^2 - X)$$

- Il s'agit d'abord de retrouver Z_P^2 , ce qui nous donne deux possibilités pour Z_P .
- Ensuite, avec ces deux possibilités on réitère le procédé pour trouver les deux valeurs de Y_P associées.
- Enfin, pour trouver X_P , on se sert de l'équation de la courbe :

$$Y^2 = X^3 + aXZ^3 + Z^6$$

- ◊ Ou alors avec Z_P^2 on retrouve X_P via la différence $(x_Q Z^2 - X)$
- ◊ Puis retrouver Y_P à l'aide de l'équation de la courbe.