Attaque DPA contre l'algorithme de Miller

Nadia El Mrabet

Arith'-LIRMM, I3M, CNRS,
Université Montpellier 2, France

C2 2008 Carcan
19 mars 2008

Plan

1. Couplage : définition & propriétés.
2. Calcul des couplages.
3. Utilisation des couplages en cryptographie.
4. Attaque DPA contre l'algorithme de Miller.

Couplage
Définition & Propriétés

Définition

Un couplage est une application qui a deux points d'une courbe elliptique associe un élément d'un corps fini.
Principaux couplages : Weil, Tate et Ate.

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

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
Définition & Propriétés

Définition

Un couplage est une application qui a deux points d'une courbe elliptique associe un élément d'un corps fini.
Principaux couplages : Weil, Tate et Ate.

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

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
Définition & Propriétés

Définition

Un couplage est une application qui a 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

Des exemples

Les couplages de Weil, Tate et Ate sont tous basés sur l'algorithme de Miller :
soit quotient, soit puissance d'une function F_P appliquée à Q.
L'algorithme de Miller construit la fonction F_P et l'évalue en Q.
L'algorithme de Miller est l'étape centrale des calculs de couplage :

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

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

Calcul d'un couplage

Les données

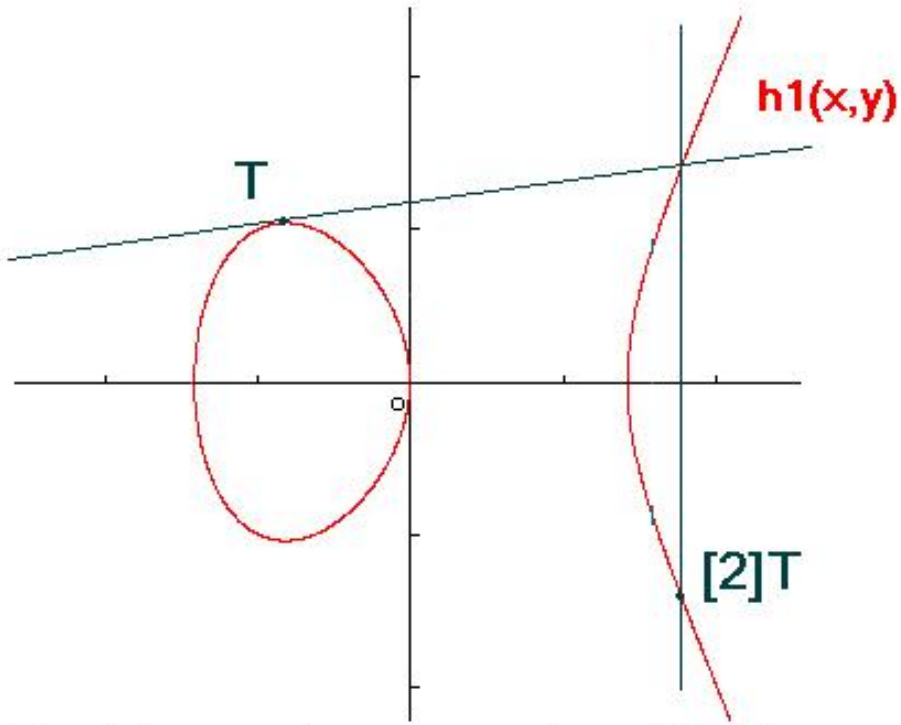
On considère :

- q 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 l'ordre de P
- $Q \in E(\mathbb{F}_{q^k})$

Calcul des couplages

Algorithme de Miller : renvoie $F_P(Q)$

Data: $l = (l_n \dots l_0)_2$,
$P \in E(\mathbb{F}_q)$ 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**
  $2 : T \leftarrow [2]T$, ;
  $3 : f_1 \longleftarrow {f_1}^2 \times h_1(Q)$;
  if $l_i = 1$ **then**
    $4 : T \leftarrow T \oplus P$;
    $5 : f_1 \longleftarrow f_1 \times h_2(Q)$;
  end
end
return f_1

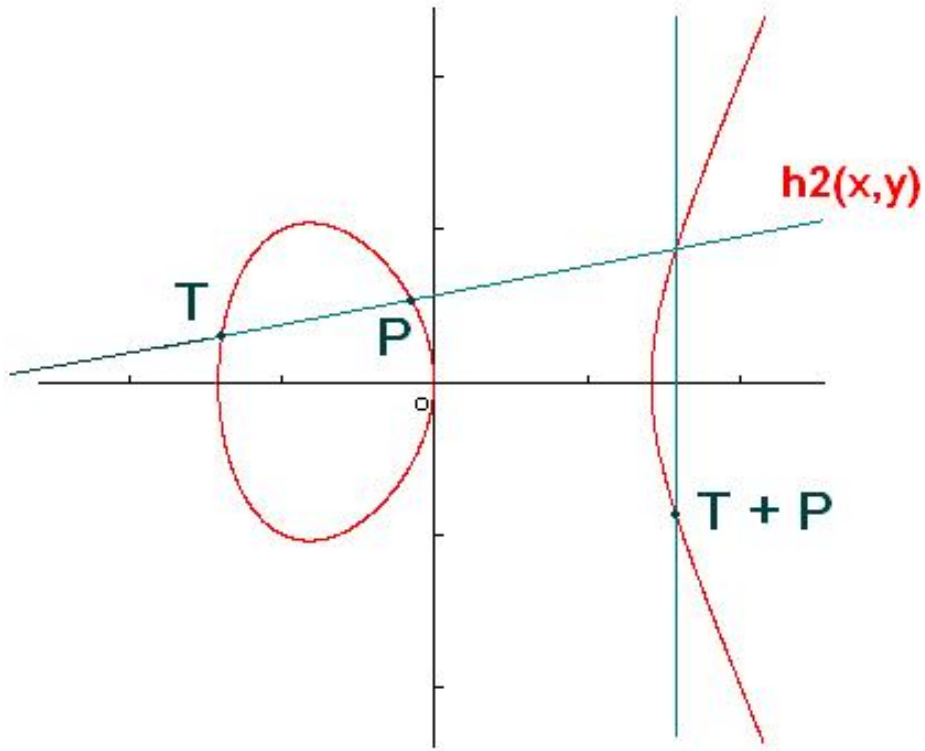


Doublement sur courbe elliptique

Calcul des couplages

Algorithme de Miller : renvoie $F_P(Q)$

Data: $l = (l_n \dots l_0)_2$,
$P \in E(\mathbb{F}_q)$ 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**
  $2 : T \leftarrow [2]T$, ;
  $3 : f_1 \longleftarrow {f_1}^2 \times h_1(Q)$;
  if $l_i = 1$ **then**
    $4 : T \leftarrow T \oplus P$;
    $5 : f_1 \longleftarrow f_1 \times h_2(Q)$;
  end
end
return f_1



Addition sur courbe elliptique

Couplage
Utilisation en cryptographie

- Destructive : attaques de MOV et Frey Ruck.
- Constructive : Cryptographie Basée sur l'Identité.

Principe

La clé publique d'un utilisateur est son identité.
La clé privée lui est fournie par une autorité de confiance.

Déchiffrement

Le déchiffrement implique un calcul de couplage entre une entrée secrète notée P, et une entrée connue Q.

Attaque DPA

Principe de l'attaque DPA

Faire une corrélation entre les bits du secret utilisé et la consommation de courant lors des calculs faisant intervenir ce secret.

Hypothèses

1. On considère un calcul de couplage entre :
   - P secret que l'on cherche à découvrir
   - Q public que l'on peut faire varier à volonté.
2. On peut mesurer la consommation de courant lors des calculs de $F_P(Q)$.

Attaque DPA

Algorithme de Miller

Data: $l = (l_n \dots l_0)_2$, $P \in E(\mathbb{F}_q)$ 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**
  $2 : T \leftarrow [2]T$, ;
  $3 : f_1 \longleftarrow {f_1}^2 \times h_1(Q)$;
  if $l_i = 1$ **then**
    $4 : T \leftarrow T \oplus P$;
    $5 : f_1 \longleftarrow f_1 \times h_2(Q)$;
  end
end
return f_1

Attaque DPA

Coordonées affines

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.

Hypothèse

Coût de la multiplication $\lambda \times (x_Q - x_T)$ lié au poids de Hamming de $(x_Q - x_P)$.

Attaque DPA

Schéma d'attaque

Principe

- On a trouvé les $(j-1)$ octet de poids faible de x_P.
- Faire des hypothèses sur le $j^{ème}$ octet de x_P.
- Connaissant x_Q on peut calculer le $j^{ème}$ octet de $x_Q - x_P$.

Illustration : premier octet

x_{Q_μ}	...	1	1	0	0	1	0	0	1	1	poids de
$-x_P$	$-$	?	0	1	0	1	0	1	1	0	Hamming :
$(x_{Q_\mu} - x_P)$		?	1	0	1	1	0	1	0	1	5

Attaque DPA

Coordonnées affines : algorithme d'attaque (1)

- m point $Q_\mu \in G_2(\subset E(\mathbb{F}_{q^k}))$ sont choisis $(500 < m < 10000)$
- Pour j allant de 0 à n (nombre d'octet de x_P)
- Pour r allant de 1 à 2^8

Attaque DPA

Coordonnées affines : algorithme d'attaque (2)

1. Récupérer les courbes C_μ pour $\mu = 0 \dots m$
2. Construire le $\mathbf{j^{eme}}$ **octet** de x_P : $(\mathbf{x_P})_\mathbf{r} = (\mathbf{x_P})_{(\mathbf{8j-1})\dots(\mathbf{8(j-1)-1})}$
3. Les $(j-1)$ octet de poids faibles de x_P ont été trouvés
4. Calcul de la **différence** $(\mathbf{x_{Q_\mu}} - \mathbf{x_P})$
   - Si $\mathbf{HW}((\mathbf{x_{Q_\mu}} - \mathbf{x_P})_{(\mathbf{8j-1})\dots\mathbf{0}}) < \mathbf{4j}$ mettre C_μ dans S_0
   - Si $\mathbf{HW}((\mathbf{x_{Q_\mu}} - \mathbf{x_P})_{(\mathbf{8j-1})\dots\mathbf{0}}) > \mathbf{4j}$ mettre C_μ dans S_1
5. Calculer les courbes moyennes $\overline{C_0}$ & $\overline{C_1}$ des ensembles S_0 & S_1
6. Calculer le biais $\Delta_r = \overline{C_1} - \overline{C_0}$ correspondant à l'hypothèse $(x_P)_r$

Attaque DPA

Coordonnées affines : algorithme d'attaque (3)

- Pour chaque hypothèse r on a une courbe Δ_r.
- Toutes ses courbes présentent un pic de consommation correspondant à la multiplication.
- La courbe avec le pic de plus grande amplitude donne l'hypothèse correcte.

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.

Merci de votre attention.

Des questions ?

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 $Q_\mu \in G_2(\subset E(\mathbb{F}_{q^k}))$ sont choisis
- Les $j-1$ bits de poids faibles de Z_P sont connus

1. Récupérer les courbes C_μ pour $i = 0 \ldots m$
2. Supposer $(Z_P)_j = 1$
   - Si $Z_P \times x_{Q_\mu j} = 0$ mettre C_μ dans S_0
   - Si $Z_P \times x_{Q_\mu j} = 1$ mettre C_μ 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 $j^{ème}$ 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 jacobiennes

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 possiblités pour Z_P.
- Ensuite, avec ces deux possiblités 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 jacobiennes

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 possiblités pour Z_P.
- Ensuite, avec ces deux possiblités 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.

Contre mesures

- Affine : faire multiplication dont consommation indépendante du poids de hamming des facteurs.
- Projective et Jacobienne : utiliser l'homogénéité.

- Nombre de courbe : lié à l'implémentation et taille des données.
- Implémentation : travaux en cours.