Optimisation des couplages

Nadia El Mrabet

GREYC−LMNO−Université de Caen, France

Ecole « Code et Cryptographie », ENSIAS de Rabat−MAROC,
Semaine du 8 au 14 mars 2010.

Plan de la présentation

Outline

Suite des festivités

Les couplages dans tout leur état

Dans la suite, nous allons commencer à entrer dans le vif du sujet

- Définition mathématiques des couplages (Ca c'est fait !)
- Exemple et calcul de couplages (Fait !)
- Optimisation des couplages Mathématiques et Arithmétique
- Attaques par canaux cachés : SPA, attaque par faute, DPA
- Application au couplage
- Perspective de la recherche à base de couplage.

Suite des festivités

Optimisation des couplages

Nous allons voir qu'il existe deux types d'optimisation des couplages

- des optimisations mathématiques, liées à la structure des groupes que nous utilisons
- des optimisations arithmétiques, liées aux algorithmes de multiplication

Outline

Aspect Arithmétique du calcul des couplages

Rappel : représentation Jacobienne

Afin de mieux comprendre à quel niveau interviennent les différentes optimisations, nous analysons les étapes de l'algorithme de Miller.

- Soit P un point de $E(\mathbb{F}_p)[r]$ donné en coordonnées affines (X_P, Y_P) (ou Jacobiennes avec $Z_P = 1$),
- le point Q d'ordre r dans $E(\mathbb{F}_{p^k})$, donné lui aussi en coordonnées affines (x_Q, y_Q),

- $\mathbb{G}_1 =< P >$ le sous groupe d'ordre r de $E(\mathbb{F}_p)$ engendré par le point P et $\mathbb{G}_2 =< Q >$. Les groupes $\mathbb{G}_1$ et $\mathbb{G}_2$ seront ceux dans lesquels nous souhaitons calculer un couplage, sous la condition $\mathbb{G}_1 \neq \mathbb{G}_2$. Le groupe $\mathbb{G}_3$ est un sous groupe de $\mathbb{F}^{\star}_{p^k}$ de même ordre r.

- Soit T un point de $E(\mathbb{F}_{p^k})$ en coordonnées Jacobiennes (X_T, Y_T, Z_T).

$\Rightarrow$ Les coordonnées Jacobiennes présentent l'avantage de ne pas nécessiter d'inversion lors des opérations arithmétiques sur la courbe elliptique.

Outline

Aspect Arithmétique du calcul des couplages

Rappel : l'algorithme de Miller

Données: $r = (r_n \dots r_0)$(représentation binaire), $P \in \mathbb{G}_1 (\subset E(\mathbb{F}_p))$ et $Q \in \mathbb{G}_2 (\subset E(\mathbb{F}_{p^k}))$;

Résultat: $f_{r,P}(Q) \in G_3 (\subset \mathbb{F}^{\star}_{p^k})$;

1. $T \leftarrow P$, $f_1 \leftarrow 1$, $f_2 \leftarrow 1$

pour $i = n - 1$ **to** 0 **faire**

1 $T \leftarrow [2]T$

$f_1 \longleftarrow {f_1}^2 \times l_d(Q)$, l_d est la tangente à la courbe en T.

$f_2 \longleftarrow {f_2}^2 \times v_d(Q)$, v_d est la droite verticale en $[2]T$.

2 **si** $n_i = 1$ **alors**

$T \leftarrow T + P$

$f_1 \longleftarrow f_1 \times l_a(Q)$, l_a est la droite (PT)

$f_2 \longleftarrow f_2 \times v_a(Q)$, v_a est la verticale au point $P + T$

fin

retourner $\frac{f_1}{f_2}$

fin

Algorithm 1: Miller(P, Q, r)

Arithmétique des couplages

Complexité des couplages

- Les fonctions $l_d(Q)$, $l_a(Q)$, $v_d(Q)$ et $v_a(Q)$ intervenant dans le calcul d'un couplage via l'algorithme de Miller ont pour espace d'arrivée $\mathbb{F}^{\star}_{p^k}$. Les paramètres f_1 et f_2 sont donc des éléments de $\mathbb{F}^{\star}_{p^k}$.

- Le choix de l'ordre r du sous groupe de la courbe elliptique dans lequel nous travaillons est très important, il est choisi de manière à avoir une représentation binaire creuse.

$\Rightarrow$ L'étape d'addition n'est alors pas souvent effectuée.

$\Rightarrow$ La complexité de l'algorithme de Miller est presque celle de l'étape de doublement.

Ainsi, l'opération effectuée à chaque itération est l'étape de doublement.

Arithmétique des couplages

Complexité des couplages

L'équation de la courbe elliptique E est de la forme $Y^2 = X^3 + aXZ^4 + bZ^6$, avec a et b éléments de $\mathbb{F}_p$.
Nous noterons $P = (X_P, Y_P)$, $T = (X_T, Y_T, Z_T)$ le point courant durant l'algorithme de Miller et $2T = (X_{2T}, Y_{2T}, Z_{2T})$ le doublement de ce point.
Les formules de doublement en coordonnées Jacobiennes sont les suivantes :

$$C = 2Y_T^2, \quad D = Z_T^2, \quad A = 4X_T Y_T^2 = 2X_T C, \quad B = (3X_T^2 + aZ_T^4)$$

$$X_{2T} = B^2 - 2A, \quad Y_{2T} = B(A - X_{2T}) - 2C^2, \quad Z_{2T} = 2Y_T Z_T.$$

Arithmétique des couplages

Complexité des couplages

En coordonnées Jacobiennes, les expressions de l_d, et v_d, avec $Q = (x_Q, y_Q) \in E(\mathbb{F}_{p^k})$, sont données par les formules :

$$l_d(x_Q, y_Q) = Z_P^2(Z_{2T} D y_Q - B(D x_Q - X_T) - 2Y_T)$$

$$v_d(x_Q, y_Q) = Z_{2T}^2 Z_P x_Q + 4Y_P^2(X_P D + X_T Z_P^2) - Z_P^2 B^2$$

Implantation des couplages sur courbes elliptiques

Soit M_p (resp. S_p) le coût d'une multiplication (resp. un carré) dans $\mathbb{F}_p$, S_{p^k} celui d'un carré et M_{p^k} celui d'une multiplication dans $\mathbb{F}_{p^k}$.

L'algorithme de Miller nécessite

- $N = [\log_2(r)] + 1$ itérations
- la complexité de l'étape de doublement est $11A_p + 9S_p + (4k + 9)M_p$
- la complexité de l'étape d'addition est $6S_p + (20 + 3k)M_p + 2S_{p^k} + 2M_{p^k}$

Implantation des couplages sur courbes elliptiques

Soit M_p (resp. S_p) le coût d'une multiplication (resp. un carré) dans $\mathbb{F}_p$, S_{p^k} celui d'un carré et M_{p^k} celui d'une multiplication dans $\mathbb{F}_{p^k}$.

L'algorithme de Miller nécessite

- $N = [\log_2(r)] + 1$ itérations
- la complexité de l'étape de doublement est $11A_p + 9S_p + (4k + 9)M_p$
- la complexité de l'étape d'addition est $6S_p + (20 + 3k)M_p + 2S_{p^k} + 2M_{p^k}$

Afin d'améliorer l'efficacité du calcul du couplage, nous pouvons :

- réduire le nombre d'additions et de multiplications dans $\mathbb{F}_{p^k}$.
- améliorer l'arithmétique dans $\mathbb{F}_{p^k}$.

Outline

Optimisation des couplages

Les optimisations mathématiques

- Utilisation d'une courbe twistée
- Elimination du calcul des dénominateurs
- Les couplages Ate et Twisted Ate

Optimisation des couplages

Les optimisations mathématiques

- Utilisation d'une courbe twistée
- Elimination du calcul des dénominateurs
- Les couplages Ate et Twisted Ate

Les optimisations arithmétiques

- Utilisation des corps amis
- Amélioration de l'exponentiation
- Amélioration de l'arithmétique de $\mathbb{F}_{p^5}$

Outline

Utilisation d'une courbe twistée

Définition

Terminologie

Nous définissons la notion de twist ou tordue d'une courbe elliptique qui est une courbe elliptique telle que nous pouvons construire un isomorphisme entre ces deux courbes.

Définition

Soient E et $\widetilde{E}$ deux courbes elliptiques définies sur $\mathbb{F}_q$.
Alors, la courbe $\widetilde{E}$ est **un twist de degré d de la courbe E** s'il existe un isomorphisme Ψ_d défini sur $\mathbb{F}_{q^d}$ de $\widetilde{E}$ dans E et tel que d soit minimal.
Nous noterons :

$$\Psi_d : \widetilde{E}(\mathbb{F}_q) \rightarrow E(\mathbb{F}_{q^d})$$

Utilisation d'une courbe twistée

Définition

Le nombre de twists de courbe elliptique possible est limité, il dépend du groupe formé par les morphismes de la courbe elliptique E dans elle même. Le Théorème suivant donne la classification des différents twists possibles. Ce théorème est un résultat important de la théorie des twists de courbes elliptiques.

Théorème

Soit E une courbe elliptique d'équation $y^2 = x^3 + ax + b$ définie sur une extension $\mathbb{F}_{p^k}$ d'un corps fini $\mathbb{F}_p$. Suivant les valeurs de k, les degrés possibles de twists d sont 2, 3, 4 et 6.

Utilisation d'une courbe twistée

Exemple

- En pratique, nous considérons que E est définie sur $\mathbb{F}_{p^k}$.
- Nous notons $\widetilde{E}$ la courbe tordue de E définie sur $\mathbb{F}_{p^{k/d}}$ un sous-corps de $\mathbb{F}_{p^k}$, pour d un diviseur de k.
- Les équations des différents twists possibles existent.
- Nous allons voir l'expression d'un twist de degré 2.
- Nous construisons explicitement le morphisme $\Psi_d : \widetilde{E} \longrightarrow E$.

Utilisation d'une courbe twistée

Exemple

- $d = 2$, Soit $\nu \in \mathbb{F}_{p^{k/2}}$ tel que le polynôme $X^2 - \nu$ soit irréductible dans $\mathbb{F}_{p^{k/2}}$.
- L'équation de la courbe $\widetilde{E}$ définie sur $\mathbb{F}_{p^{k/2}}$ est

$$\widetilde{E} : \nu y^2 = x^3 + ax + b.$$

- Le morphisme Ψ_2 est défini par :

$$\begin{array}{rccc} \Psi_2 : & \widetilde{E}(\mathbb{F}_{p^{k/2}}) & \rightarrow & E(\mathbb{F}_{p^k}) \\ & (x, y) & \rightarrow & (x, y\nu^{1/2}). \end{array}$$

Utilisation d'une courbe twistée

Conséquence sur le coût des calculs

Rappel : équation de l_d

$$l_d(x_Q, y_Q) = Z_P^2(Z_{2T}Dy_Q - B(Dx_Q - X_T) - 2Y_T)$$

Au tableau : détaillé la complexité sans utiliser de twist.
Au tableau : détaillé la complexité en utilisant un twist.

Utilisation d'une courbe twistée

Conséquence sur le coût des calculs

Doublement point sur E	$4S_p + 4M_p$
Évaluation fonction l_d seule	$(3 + 2k/d)M_P$
Étape de doublement	$4S_p + (12 + 4k/d)M_p + 2S_{p^k} + 2M_{p^k}$

Table: Coût de l'étape de doublement de l'algorithme de Miller

Outline

Elimination des dénominateurs

Principe

Repose sur les courbes twistées

L'utilisation des courbes twistées permet d'effectuer la majorité des calculs durant l'algorithme de Miller dans les corps $\mathbb{F}_p$ et $\mathbb{F}_{p^{k/2}}$ plutôt que dans $\mathbb{F}_{p^k}$. De plus, elle simplifie les calculs en permettant l'élimination des

dénominateurs dans l'algorithme de Miller.

Elimination des dénominateurs

Mise en oeuvre

Représentation de Q

$Q \in E(F_{p^k})$ s'écrit $(x, y\sqrt{\nu})$
avec $x,\ y,\ \nu \in F_{p^{k/2}}$, et $\sqrt{\nu} \in F_{p^k}$

Coordonnées de T

Les coordonnées (X_T, Y_T, Z_T) sont dans $\mathbb{F}_p$.

Elimination des dénominateurs

Mise en oeuvre

Conséquence

Rappelons l'équation de la vertical :

$$v_d(x_Q, y_Q) = Z_{2T}^2 Z_P x_Q + 4 Y_P^2 (X_P D + X_T Z_P^2) - Z_P^2 B^2$$

sachant dans quel sous groupe vivent les coordonnées des points, on a le fait suivant

$$v_d \in \mathbb{F}_{p^{k/d}}.$$

Elimination des dénominateurs

Théorème de Fermat

Petit théorème de Fermat

Soit p un nombre premier et x un entier non nul dans $\mathbb{F}_p$. Alors les égalités suivantes sont vraies :

$$\begin{aligned} x^p &\equiv x \bmod p, \\ \text{si } x \neq 0 \bmod p,\ x^{(p-1)} &\equiv 1 \bmod p. \end{aligned}$$

Elimination des dénominateurs

Regroupement des informations

Nous savons que le couplage de Tate est

$$(f_{r,P}(Q))^{\frac{p^k-1}{r}}.$$

Sachant que :

- $f_{r,P}(Q) = \frac{f_1}{f_2}$, avec $f_2 = \prod v_d(Q)$
- $v_d \in \mathbb{F}_{p^{k/d}}$

$\Rightarrow$ Comment simplifier les calculs ?

Elimination des dénominateurs

L'astuce qui tue ! !

L'astuce permettant d'éliminer les dénominateurs est une réécriture de l'exposant.

Récriture de l'exposant

$$p^k - 1 = (p^{k/d} - 1)\left((p^{k/d})^{d-1} + (p^{k/d})^{d-2} + \ldots + (p^{k/d}) + 1\right)$$

Elimination des dénominateurs

L'astuce qui tue ! !

L'astuce permettant d'éliminer les dénominateurs est une réécriture de l'exposant.

Récriture de l'exposant

$$p^k - 1 = (p^{k/d} - 1)\left((p^{k/d})^{d-1} + (p^{k/d})^{d-2} + \ldots + (p^{k/d}) + 1\right)$$

Conséquences

$v_d \in \mathbb{F}_{p^{k/d}}$, donc $v_d^{p^{k/d}-1} = 1$
et ainsi $v_d^{(p^k-1)} = 1$.
Nous pouvons alors simplifier l'algorithme de Miller en oubliant de calculer les dénominateurs.

Optimisation des couplages

Les optimisations mathématiques

- Utilisation d'une courbe twistée
- Elimination du calcul des dénominateurs
- Les couplages Ate et Twisted Ate

Les optimisations arithmétiques

- Utilisation des corps amis
- Amélioration de l'exponentiation
- Amélioration de l'arithmétique de $\mathbb{F}_{p^k}$

Suite des festivités

Les couplages dans tout leur état

Dans la suite, nous allons commencer à entrer dans le vif du sujet

- Définition mathématiques des couplages (Ca c'est fait !)
- Exemple et calcul de couplages (Ca c'est fait !)
- Optimisation des couplages Mathématiques et Arithmétique (Ca c'est presque fait !)
- Attaques par canaux cachés : SPA, attaque par faute, DPA
- Application au couplage
- Perspective de la recherche à base de couplage.