Calculer des couplages sur les courbes de degré de plongement $k = 15$

Nadia El Mrabet[(1)], Sorina Ionica[(2)] et Nicolas Guillermin[(3)]

(1) Equipe Algorithmique/GREYC, Université de Caen

(2) Equipe Prism, Université de Versailles

(3) Laboratoire IRMAR Université de Rennes 2

GREYC, 21 octobre 2009

Outline

Outline

Qu'est ce qu'un couplage ?

Propriétés

Soient G_1, G_2 et G_3 trois groupes finis du même ordre r. Un couplage est une application :

$$e : G_1 \times G_2 \longrightarrow G_3$$

Qu'est ce qu'un couplage ?

Propriétés

Soient G_1, G_2 et G_3 trois groupes finis du même ordre r. Un couplage est une application :

$$e : G_1 \times G_2 \longrightarrow G_3$$

vérifiant les propriétés suivantes :

Qu'est ce qu'un couplage ?

Propriétés

Soient G_1, G_2 et G_3 trois groupes finis du même ordre r. Un couplage est une application :

$$e : G_1 \times G_2 \rightarrow G_3$$

vérifiant les propriétés suivantes :

- *Non dégénérescence ;*
  - $\forall P \in G_1 \setminus \{0\}, \exists Q \in G_2$ t.q. $e(P, Q) \neq 1$

Qu'est ce qu'un couplage ?

Propriétés

Soient G_1, G_2 et G_3 trois groupes finis du même ordre r. Un couplage est une application :

$$e : G_1 \times G_2 \rightarrow G_3$$

vérifiant les propriétés suivantes :

- *Non dégénérescence ;*
  - $\forall P \in G_1 \ \{0\}, \exists Q \in G_2$ t.q. $e(P, Q) \neq 1$
  - $\forall Q \in G_2 \ \{0\} \exists P \in G_1$ t.q. $e(P, Q) \neq 1$

Qu'est ce qu'un couplage ?

Propriétés

Soient G_1, G_2 et G_3 trois groupes finis du même ordre r. Un couplage est une application :

$$e : G_1 \times G_2 \longrightarrow G_3$$

vérifiant les propriétés suivantes :

- *Non dégénérescence ;*
- *Bilinéarité :* $\forall P, P' \in G_1, \forall Q, Q' \in G_2$

Qu'est ce qu'un couplage ?

Propriétés

Soient G_1, G_2 et G_3 trois groupes finis du même ordre r. Un couplage est une application :

$$e : G_1 \times G_2 \rightarrow G_3$$

vérifiant les propriétés suivantes :

- *Non dégénérescence ;*
- *Bilinéarité :* $\forall P, P' \in G_1, \forall Q, Q' \in G_2$
  - $e(P + P', Q) = e(P, Q).e(P', Q)$

Qu'est ce qu'un couplage ?

Propriétés

Soient G_1, G_2 et G_3 trois groupes finis du même ordre r. Un couplage est une application :

$$e : G_1 \times G_2 \rightarrow G_3$$

vérifiant les propriétés suivantes :

- *Non dégénérescence ;*
- *Bilinéarité :* $\forall P, P' \in G_1, \forall Q, Q' \in G_2$
  - $e(P + P', Q) = e(P, Q).e(P', Q)$
  - $e(P, Q + Q') = e(P, Q).e(P, Q')$

Qu'est ce qu'un couplage ?

Propriétés

Soient G_1, G_2 et G_3 trois groupes finis du même ordre r. Un couplage est une application :

$$e : G_1 \times G_2 \longrightarrow G_3$$

vérifiant les propriétés suivantes :

- *Non degenerate ;*
- *Bilinearity ;*

Conséquences

$$\forall j \in \mathbb{N}, e([j]P, Q) = e(P, Q)^j = e(P, [j]Q)$$

Cryptographie à base de couplages

Cryptanalyse

La propriété de bilinéarité des couplages a permis de transférer le problème du logarithme discret depuis une courbe elliptique en un problème de logarithme discret sur un corps fini.

Cryptographie à base de couplages

Cryptanalyse

La propriété de bilinéarité des couplages a permis de transférer le problème du logarithme discret depuis une courbe elliptique en un problème de logarithme discret sur un corps fini.

Cryptographie

les couplages ont permis la construction de protocols originaux et la simplification de protocoles cryptographiques existants.

- L'échange de clé tripartite à la Diffie Hellman (Joux 2001)
- La cryptographie basée sur l'identité (Boneh et Franklin 2001)
- Les schémas de signature courte (Boneh, Lynn, Schackamm 2001)
- Les schémas de signature de groupe (Boneh, Schackamm, 2004)

Les couplages existants

Quatre couplages sont principalement utilisés en cryptographie :

- le couplage de Weil,
- le couplage de Tate,
- le η couplage,
- le couplage Ate et Twisted Ate.

Leurs calculs nécessitent des opérations dans des corps finis $\mathbb{F}_p$ et des extensions $\mathbb{F}_{p^k}$ de ces corps.
Nous cherchons à utiliser le couplage minimisant ces opérations.

Construction des couplages

Données

Afin de calculer un couplage, nous avons besoin des éléments suivants :

- E une courbe elliptique sur un corps fini premier $\mathbb{F}_p$:
  $E : y^2 = x^3 + ax + b$, avec a, $b \in \mathbb{F}_p$.

Construction des couplages

Données

Afin de calculer un couplage, nous avons besoin des éléments suivants :

- E une courbe elliptique sur un corps fini premier $\mathbb{F}_p$:
  $E : y^2 = x^3 + ax + b$, avec a, $b \in \mathbb{F}_p$.
- r un nombre premier divisant $\text{card}(E(\mathbb{F}_p))$,
  ainsi que l'ensemble $E[r]$: $E[r] = \{P \in E(\overline{\mathbb{F}_p}), [r]P = P_\infty\}$.

Construction des couplages

Données

Afin de calculer un couplage, nous avons besoin des éléments suivants :

- E une courbe elliptique sur un corps fini premier $\mathbb{F}_p$:
  $E : y^2 = x^3 + ax + b$, avec a, $b \in \mathbb{F}_p$.
- r un nombre premier divisant $\text{card}(E(\mathbb{F}_p))$,
  ainsi que l'ensemble $E[r]$: $E[r] = \{P \in E(\overline{\mathbb{F}_p}), [r]P = P_\infty\}$.
- Le degré de plongement k : le plus petit entier tel que $r|(q^k - 1)$:

Construction des couplages

Données

Afin de calculer un couplage, nous avons besoin des éléments suivants :

- E une courbe elliptique sur un corps fini premier $\mathbb{F}_p$:
  $E : y^2 = x^3 + ax + b$, avec a, $b \in \mathbb{F}_p$.
- r un nombre premier divisant $\text{card}(E(\mathbb{F}_p))$,
  ainsi que l'ensemble $E[r]$: $E[r] = \{P \in E(\overline{\mathbb{F}_p}), [r]P = P_\infty\}$.
- Le degré de plongement k : le plus petit entier tel que $r|(q^k - 1)$:
  Si $pgcd(r, q) = 1$, alors $E[r] \cong \mathbb{Z}/r\mathbb{Z} \times \mathbb{Z}/r\mathbb{Z}$,
  Si $k > 1$ alors $E[r] = E(\mathbb{F}_{p^k})[r]$.

Construction des couplages

Données

Afin de calculer un couplage, nous avons besoin des éléments suivants :

- E une courbe elliptique sur un corps fini premier $\mathbb{F}_p$:
  $E : y^2 = x^3 + ax + b$, avec a, $b \in \mathbb{F}_p$.
- r un nombre premier divisant $\text{card}(E(\mathbb{F}_p))$,
  ainsi que l'ensemble $E[r]$: $E[r] = \{P \in E(\overline{\mathbb{F}_p}), [r]P = P_\infty\}$.
- Le degré de plongement k : le plus petit entier tel que $r|(q^k - 1)$:
  Si $pgcd(r, q) = 1$, alors $E[r] \cong \mathbb{Z}/r\mathbb{Z} \times \mathbb{Z}/r\mathbb{Z}$,
  Si $k > 1$ alors $E[r] = E(\mathbb{F}_{p^k})[r]$.
- Une fonction $f_{r,P}$ décrite plus loin.

Construction des couplages

Le couplage de Tate

Soit $P \in E(\mathbb{F}_p)[r]$, $Q \in E(\mathbb{F}_{p^k})/rE(\mathbb{F}_{p^k})$ et k le degré de plongement de la courbe relativement à r.

Construction des couplages

Le couplage de Tate

Soit $P \in E(\mathbb{F}_p)[r]$, $Q \in E(\mathbb{F}_{p^k})/rE(\mathbb{F}_{p^k})$ et k le degré de plongement de la courbe relativement à r.

Le couplage de Tate est l'application :

$$e_T : E(\mathbb{F}_p)[r] \times E(\mathbb{F}_{p^k})/rE(\mathbb{F}_{p^k}) \longrightarrow \mathbb{F}_{p^k}^*$$

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

Construction des couplages

Le couplage Ate

Le couplage Ate est la dernière optimisation calculatoire des couplages. Il est construit de la même façon que le couplage de Tate.

Construction des couplages

Le couplage Ate

Le couplage Ate est la dernière optimisation calculatoire des couplages. Il est construit de la même façon que le couplage de Tate.

Soit π_p l'application Frobenius sur la courbe elliptique :

$$\pi_p([x, y]) = [x^q, y^q].$$

Nous notons t la trace du Frobenius sur $E(\mathbb{F}_p)$ et $T = t - 1$.
Nous allons utiliser les espaces propres du Frobenius.

Construction des couplages

Le couplage Ate

Soit $P \in E[r] \cap \mathrm{Ker}(\pi_p - [1])$ et $Q \in E[r] \cap \mathrm{Ker}(\pi_p - [q])$, i.e. Q vérifie que $\pi_p(Q) = [q]Q$.

Construction des couplages

Le couplage Ate

Soit $P \in E[r] \cap \mathrm{Ker}(\pi_p - [1])$ et $Q \in E[r] \cap \mathrm{Ker}(\pi_p - [q])$, i.e. Q vérifie que $\pi_p(Q) = [q]Q$.
Le couplage Ate est l'application :

$$e_A : E[r] \cap \mathrm{Ker}(\pi_p - [1]) \times E[r] \cap \mathrm{Ker}(\pi_p - [q]) \longrightarrow \mathbb{F}^*_{p^k}$$

$$(P, Q) \longrightarrow f_{T,P}(Q)^{\frac{q^k-1}{r}}$$

Outline

L'égalité de Miller

La fonction $f_{s,P}$

Le calcul des couplages décrits nécessite la construction d'une fonction $f_{s,P}$ pour s un entier naturel.
La propriété principale de cette fonction est la suivante :

L'égalité de Miller

La fonction $f_{s,P}$

Le calcul des couplages décrits nécessite la construction d'une fonction $f_{s,P}$ pour s un entier naturel.
La propriété principale de cette fonction est la suivante :

$$Div(f_{s,P}) = sDiv(P) - sDiv(P_\infty)$$

L'égalité de Miller

La fonction $f_{s,P}$

Le calcul des couplages décrits nécessite la construction d'une fonction $f_{s,P}$ pour s un entier naturel.
La propriété principale de cette fonction est la suivante :

$$Div(f_{s,P}) = sDiv(P) - sDiv(P_\infty)$$

Victor Miller a établit l'équation homonyme :

$$f_{i+j,P} = f_{i,P} \times f_{j,P} \times \frac{l_{[i]P,[j]P}}{v_{[i+j]P}}$$

L'égalité de Miller

La fonction $f_{s,P}$

Le calcul des couplages décrits nécessite la construction d'une fonction $f_{s,P}$ pour s un entier naturel.
La propriété principale de cette fonction est la suivante :

$$Div(f_{s,P}) = sDiv(P) - sDiv(P_\infty)$$

Victor Miller a établit l'équation homonyme :

$$f_{i+j,P} = f_{i,P} \times f_{j,P} \times \frac{l_{[i]P,[j]P}}{v_{[i+j]P}}$$

où $l_{[i]P+[j]P}$ est la droite passant pas les points $[i]P$ et $[j]P$,

L'égalité de Miller

La fonction $f_{s,P}$

Le calcul des couplages décrits nécessite la construction d'une fonction $f_{s,P}$ pour s un entier naturel.
La propriété principale de cette fonction est la suivante :

$$Div(f_{s,P}) = sDiv(P) - sDiv(P_\infty)$$

Victor Miller a établit l'équation homonyme :

$$f_{i+j,P} = f_{i,P} \times f_{j,P} \times \frac{l_{[i]P,[j]P}}{v_{[i+j]P}}$$

où $l_{[i]P+[j]P}$ est la droite passant pas les points $[i]P$ et $[j]P$,
et $v_{[i+j]P}$ est la droite vertical au point $[i+j]P$.

L'égalité de Miller

Exemple

Nous voulons calculer $f_{7,P}$:

L'égalité de Miller

Exemple

Nous voulons calculer $f_{7,P}$:

- $7 = 6 + 1$

L'égalité de Miller

Exemple

Nous voulons calculer $f_{7,P}$:

- $7 = 6 + 1$
- $f_{7,P} = f_{6,P} \times f_{1,P} \times \frac{l_{[6]P,P}}{v_{[7]P}}$

L'égalité de Miller

Exemple

Nous voulons calculer $f_{7,P}$:

- $7 = 6 + 1$
- $f_{7,P} = f_{6,P} \times f_{1,P} \times \frac{l_{[6]P,P}}{v_{[7]P}}$

  $f_{1,P} = 1$

  $f_{7,P} = f_{6,P} \times \frac{l_{[6]P,P}}{v_{[7]P}}$

L'égalité de Miller

Exemple

Nous voulons calculer $f_{7,P}$:

- $7 = 6 + 1$
- $f_{7,P} = f_{6,P} \times f_{1,P} \times \frac{l_{[6]P,P}}{v_{[7]P}}$

  $f_{1,P} = 1$

  $f_{7,P} = f_{6,P} \times \frac{l_{[6]P,P}}{v_{[7]P}}$
- $f_{6,P} = f_{3,P} \times f_{3,P} \times \frac{l_{[3]P,[3]P}}{v_{[6]P}}$

  lorsque $i = j$, la droite l est la tangente au point $[i]P$

L'égalité de Miller

Exemple

Nous voulons calculer $f_{7,P}$:

- $7 = 6 + 1$
- $f_{7,P} = f_{6,P} \times f_{1,P} \times \frac{l_{[6]P,P}}{v_{[7]P}}$

  $f_{1,P} = 1$

  $f_{7,P} = f_{6,P} \times \frac{l_{[6]P,P}}{v_{[7]P}}$
- $f_{6,P} = f_{3,P} \times f_{3,P} \times \frac{l_{[3]P,[3]P}}{v_{[6]P}}$

  lorsque $i = j$, la droite l est la tangente au point $[i]P$
- $f_{6,P} = f_{3,P}^2 \times \frac{l_{[3]P,[3]P}}{v_{[6]P}}$

  $f_{7,P} = f_{3,P}^2 \times \frac{l_{[3]P,[3]P}}{v_{[6]P}} \times \frac{l_{[6]P,P}}{v_{[7]P}}$

L'égalité de Miller

Exemple

Nous voulons calculer $f_{7,P}$:

- $f_{7,P} = f_{3,P}^2 \times \frac{l_{[3]P,[3]P}}{v_{[6]P}} \times \frac{l_{[6]P,P}}{v_{[7]P}}$

L'égalité de Miller

Exemple

Nous voulons calculer $f_{7,P}$:

- $f_{7,P} = f_{3,P}^2 \times \frac{l_{[3]P,[3]P}}{v_{[6]P}} \times \frac{l_{[6]P,P}}{v_{[7]P}}$
- $f_{3,P} = f_{2,P} \times f_{1,P} \times \frac{l_{[2]P,P}}{v_{[3]P}}$

  $f_{3,P} = f_{2,P} \times \frac{l_{[2]P,P}}{v_{[3]P}}$

L'égalité de Miller

Exemple

Nous voulons calculer $f_{7,P}$:

- $f_{7,P} = f_{3,P}^2 \times \frac{l_{[3]P,[3]P}}{v_{[6]P}} \times \frac{l_{[6]P,P}}{v_{[7]P}}$
- $f_{3,P} = f_{2,P} \times f_{1,P} \times \frac{l_{[2]P,P}}{v_{[3]P}}$

  $f_{3,P} = f_{2,P} \times \frac{l_{[2]P,P}}{v_{[3]P}}$

L'égalité de Miller

Exemple

Nous voulons calculer $f_{7,P}$:

- $f_{7,P} = f_{3,P}^2 \times \frac{l_{[3]P,[3]P}}{v_{[6]P}} \times \frac{l_{[6]P,P}}{v_{[7]P}}$
- $f_{3,P} = f_{2,P} \times f_{1,P} \times \frac{l_{[2]P,P}}{v_{[3]P}}$

  $f_{3,P} = f_{2,P} \times \frac{l_{[2]P,P}}{v_{[3]P}}$
- $f_{2,P} = f_{1,P} \times f_{1,P} \times \frac{l_{P,P}}{v_{[2]P}}$

L'égalité de Miller

Exemple

Nous voulons calculer $f_{7,P}$:

- $f_{7,P} = f_{3,P}^2 \times \frac{l_{[3]P,[3]P}}{v_{[6]P}} \times \frac{l_{[6]P,P}}{v_{[7]P}}$
- $f_{3,P} = f_{2,P} \times f_{1,P} \times \frac{l_{[2]P,P}}{v_{[3]P}}$

  $f_{3,P} = f_{2,P} \times \frac{l_{[2]P,P}}{v_{[3]P}}$
- $f_{2,P} = f_{1,P} \times f_{1,P} \times \frac{l_{P,P}}{v_{[2]P}}$
- $f_{7,P} = \left(\frac{l_{P,P}}{v_{[2]P}} \times \frac{l_{[2]P,P}}{v_{[3]P}} \right)^2 \times \frac{l_{[3]P,[3]P}}{v_{[6]P}} \times \frac{l_{[6]P,P}}{v_{[7]P}}$

Calcul des couplages

L'algorithme de Miller renvoie $f_{r,P}(Q)$

Data: $r = (r_n \dots r_0)_2$,
$P \in E(\mathbb{F}_p)$ et Q
$\in E(\mathbb{F}_{p^k})$;
Result: $f_{r,P}(Q) \in \mathbb{F}^*_{p^k}$;
$1 : T \leftarrow P$, $f_1 \leftarrow 1$, $f_2 \leftarrow 1$;
for $i = n - 1$ **to** 0 **do**
    ;
        ;
            ;
    if $r_i = 1$ **then**
        ;
        ;
        ;
    end
end
return

Calcul des couplages

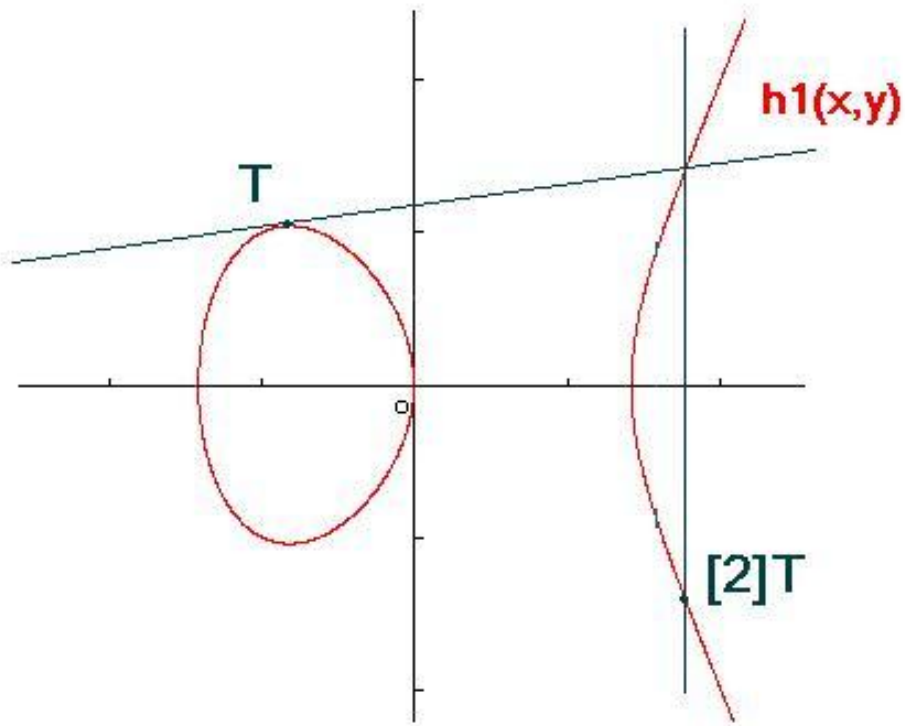
L'algorithme de Miller renvoie $f_{r,P}(Q)$

Data: $r = (r_n \dots r_0)_2$,
$P \in E(\mathbb{F}_p)$ et Q
$\in E(\mathbb{F}_{p^k})$;
Result: $f_{r,P}(Q) \in \mathbb{F}^*_{p^k}$;
$1 : T \leftarrow P$, $f_1 \leftarrow 1$, $f_2 \leftarrow 1$;
for $i = n - 1$ **to** 0 **do**
  $2 : T \leftarrow [2]T$;
  ;
  ;
  if $r_i = 1$ **then**
    $5 : T \leftarrow T + P$;
    ;
    ;
  end
end
return

Calcul des couplages

L'algorithme de Miller renvoie $f_{r,P}(Q)$

Data: $r = (r_n \dots r_0)_2$,
$P \in E(\mathbb{F}_p)$ et Q
$\in E(\mathbb{F}_{p^k})$;
Result: $f_{r,P}(Q) \in \mathbb{F}^*_{p^k}$;
$1 : T \leftarrow P$, $f_1 \leftarrow 1$, $f_2 \leftarrow 1$;
for $i = n - 1$ **to** 0 **do**
  $2 : T \leftarrow [2]T$;
  $3 : f_1 \longleftarrow {f_1}^2 \times l_1(Q)$;
  $4 : f_2 \longleftarrow {f_2}^2 \times v_2(Q)$;
  if $r_i = 1$ **then**
    $5 : T \leftarrow T + P$;
    ;
    ;
  end
end
return

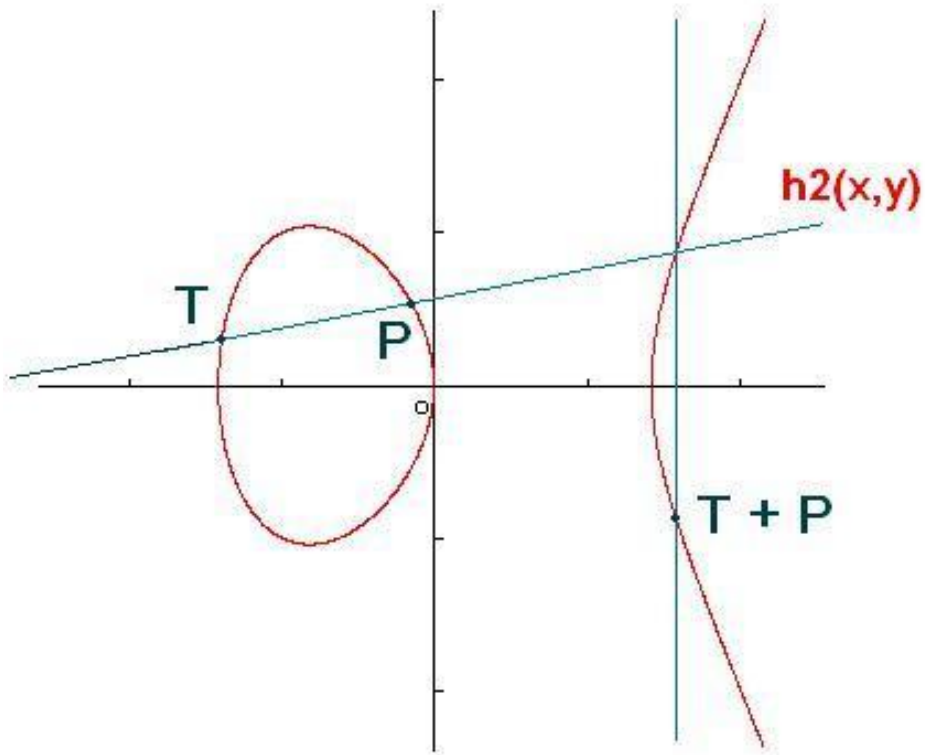


Doubling on an elliptic curve

Calcul des couplages

L'algorithme de Miller renvoie $f_{r,P}(Q)$

Data: $r = (r_n \dots l_0)_2$,
$P \in E(\mathbb{F}_p)$ et Q
$\in E(\mathbb{F}_{p^k})$;
Result: $f_{r,P}(Q) \in \mathbb{F}^*_{p^k}$;
$1 : T \leftarrow P$, $f_1 \leftarrow 1$, $f_2 \leftarrow 1$;
for $i = n - 1$ **to** 0 **do**
  $2 : T \leftarrow [2]T$,;
  $3 : f_1 \longleftarrow {f_1}^2 \times l_d(Q)$;
  $4 : f_2 \longleftarrow {f_2}^2 \times v_d(Q)$;
  if $r_i = 1$ **then**
    $5 : T \leftarrow T + P$;
    $6 : f_1 \longleftarrow f_1 \times l_a(Q)$;
    $7 : f_2 \longleftarrow f_2 \times v_a(Q)$;
  end
end
return



Addition on an elliptic curve

Calcul des couplages

L'algorithme de Miller renvoie $f_{r,P}(Q)$

Data: $r = (r_n \dots l_0)_2$, $P \in E(\mathbb{F}_p)$ et $Q \in E(\mathbb{F}_{p^k})$;
Result: $f_{r,P}(Q) \in \mathbb{F}^*_{p^k}$;
$1 : T \leftarrow P$, $f_1 \leftarrow 1$, $f_2 \leftarrow 1$;
for $i = n - 1$ **to** 0 **do**
  $2 : T \leftarrow [2]T$;
  $3 : f_1 \longleftarrow {f_1}^2 \times l_d(Q)$;
  $4 : f_2 \longleftarrow {f_2}^2 \times v_d(Q)$;
  if $r_i = 1$ **then**
    $5 : T \leftarrow T + P$;
    $6 : f_1 \longleftarrow f_1 \times l_a(Q)$;
    $7 : f_2 \longleftarrow f_2 \times v_a(Q)$;
  end
end
return $\frac{f_1}{f_2}$

L'implémentation des couplages sur courbes elliptiques.

- La complexité d'une étape de l'algorithme de Miller est :
  $2kM_p + 6S_{p^k} + 7M_{p^k}$.

- Afin d'optimiser et améliorer le calcul des couplages, il existe deux solutions :
  - réduire le nombre d'opérations dans $\mathbb{F}_{p^k}$.
  - améliorer la complexité des opérations dans $\mathbb{F}_{p^k}$.

Outline

Corps finis utilisés pour le calcul des couplages

- Le corps fini $\mathbb{F}_p$
  - est l'ensemble des entiers modulo un nombre premier $p \geq 2^{160}$.
  - Les courbes de degré de plongement k sont construites par la méthode de multiplication complexe.
  - Une conséquence est que le nombre premier p est de forme quelconque, l'arithmétique sur $\mathbb{F}_p$ est construite à l'aide d'algorithmes génériques (Montgomery, Barett).
- L'extension $\mathbb{F}_{p^k}$
  - est l'ensemble des polynômes $\mathbb{F}_p[X]$ modulo un polynôme irréductible P de degré k.
  - k est choisit tel que $p^k \geq 2^{1024}$.
  - $P = X^k - \mu$ avec μ un petit entier et/ou si possible une puissance de 2.

Les corps amis

Définition

Définition

- $\mathbb{F}_{p^k}$ est un corps ami si $p \equiv 1\ mod(12)$ & $k = 2^i.3^j$.

Théorème

- Soit $\mathbb{F}_{p^k}$ un corps ami, et β qui ne soit ni un carré, ni un cube dans $\mathbb{F}_p$.

  Alors $X^k - \beta$ est irréductible sur $\mathbb{F}_p$.

Conséquences

- $\mathbb{F}_{p^k}$ est construit par une tour d'extension quadratique et cubique.

  $\Rightarrow$ une amélioration perceptoble de la complexité de la multiplication dans $\mathbb{F}_{p^k}$.
- Une multiplication dans $\mathbb{F}_{p^k}$ s'effectue en 3^i5^j multiplications in $\mathbb{F}_p$.

Les corps amis

Optimisations des calculs

Les corps amis permettent de simplifier les coûts de calcul de l'algorithme de Miller, à travers :

- l'utilisation des multiplications de Karatsuba et Toom Cook ;
- l'utilisation d'un twist de degré pair
  $\phi : \widetilde{Q} = (x, y) \in E(\mathbb{F}_{p^{k/2}}) \to Q = (x, y\sqrt{\nu}) \in E(\mathbb{F}_{p^k})$ qui permet :
- ◊ de réduire le nombre global d'opérations dans $\mathbb{F}_p$;
- ◊ d'éliminer le calcul de la fonction f_2 dans l'algorithme de Miller.

Les corps amis sont donc privilégiés dans la littérature.
Que se passe-t-il pour un degré de plongement moins « amical » ?

Outline

Les courbes de degré de plongement $k = 15$

L'équation d'une courbe elliptique admettant un degré de plongement $k = 15$ est $E : y^2 = x^3 + b$.
La paramétrisation de Duan and all de 2005 est un exemple d'une telle famille de courbe :

$$\begin{aligned} p &= 1/3x^{12} - 2/3x^{11} + 1/3x^{10} + 1/3x^7 - 2/3x^6 + 1/3x^5 + 1/3x^2 + 1/3x \\ r &= x^8 - x^7 + x^5 - x^4 + x^3 - x + 1 \\ t &= x + 1. \end{aligned}$$

Définition d'un twist

Soit E une courbe définie sur $\mathbb{F}_p$ est d'équation $y^2 = x^3 + b$, avec $b \in \mathbb{F}_p$.
Soit D un élément de $\mathbb{F}_{p^{k/3}}$ qui ne soit pas un cube.
Alors, il existe un morphisme envoyant tout point de la courbe E' d'équation $y^2 = x^3 + \frac{b}{D}$ sur $\mathbb{F}_{p^{k/3}}$, sur un point de la courbe $E(\mathbb{F}_{p^k})$:

$$\begin{aligned} \Phi_3 : E'(\mathbb{F}_{p^{k/3}}) &\rightarrow E(\mathbb{F}_{p^k}) \\ (x, y) &\rightarrow (x\nu^{1/3}, y\nu^{1/2}) \end{aligned}$$

Ainsi, tout élément Q de G_2 peut être vu comme l'image d'un point de E' par Φ_3, et donc s'écrire $Q = (D^{1/3}x, D^{1/2}y)$, avec x, y, et $D^{1/2} \in \mathbb{F}_{p^{k/3}}$ et $D^{1/3} \in \mathbb{F}_{p^k}$.
Ceci permet de ramener certaines opérations durant le calcul des couplages dans $\mathbb{F}_{p^5}$.

Elimination des dénominateurs

L'élimination des dénominateur repose sur l'exponentiation finale des couplages de Tate et Ate.
En effet élever le résultat du couplage à la puissance $\frac{p^k-1}{r}$ tue tout facteur qiu soit dans un sous corps propre de $\mathbb{F}_{p^k}$.
Le dénominateur dans l'algorithme de Miller est l'élément f_2 mis à jour à chaque étape de l'algorithme.
L'équation de cette mise à jour est de la forme $f_2 \leftarrow (f_2) \times (x_T - x_Q)$, ou encore avec l'utilisation d'un twist de degré 3 de la forme $x_T - xD^{1/3}$, avec x_T et x dans un sous corps propre de $\mathbb{F}_{p^k}$ et $D^{1/3} \in \mathbb{F}_{p^k}$.
Ecrit ainsi, l'élément f_2 appartient à $\mathbb{F}_{p^k}$.
Nous allons le transformer pour en extraire un facteur appartenant à $\mathbb{F}_{p^{k/3}}$.

Elimination des dénominateurs

Utilisant l'équation de la courbe elliptique $y^2 = x^3 + b$, nous pouvons écire

$$x_T - x_Q = \frac{x_T^3 - x_Q^3}{x_T^2 + x_T x_Q + x_Q^2} = \frac{y_T^2 - y_Q^2}{x_T^2 + x_T x_Q + x_Q^2}.$$

Cette fois ci le terme $y_T^2 - y_Q^2$ appartient à $\mathbb{F}_{p^{k/3}}$ il sera éliminé par l'exponentiation finale.

We use an idea given in [**?**]. We observe that the expression of line h_2 in Equation (**??**) can be written as :

$x_T - x_Q = \frac{x_T^3 - x_Q^3}{x_T^2 + x_T x_Q + x_Q^2} = \frac{y_T^2 - y_Q^2}{x_T^2 + x_T x_Q + x_Q^2}$. The element $(y_Q^2 - y_T^2)$ is in $\mathbb{F}_{p^5}$ and can be forgotten during the computation of the pairing, because of the final exponentiation. Indeed, $p^5 - 1$ is a divisor of $\frac{p^{15}-1}{r}$ so multiplication by this term can be omitted. Consequently at each iteration in Miller's algorithm loop it suffices to multiply by $x_T^2 + x_T x_Q + x_Q^2$, instead of dividing by h_2. This saves operations, as we no longer need to compute denominators at each step and also avoids the final inversion, which is important on restricted devices.

L'élimination des dénominateurs est donc réalisable pour les twists de degré 3, moyennant une multiplication supplémentaire par le terme

We begin with the following definition.

Definition

Let E, E' be elliptic curves over F_p. Then E' is called a twist of degree d if there exists an isomorphism $\phi_d : E' \to E$ defined over $\mathbb{F}_{p^d}$ and d is minimal.

Suppose now that E admits a twist E' defined over $\mathbb{F}_{p^{k/d}}$ of degree d, with $d \mid k$. We set $m = \gcd(k, d)$ and $e = k/m$. We consider G_1 and G_2 as above. Then for $P \in G_1, Q \in G_2$ we get [**?**] :

$$e_{twisted}(P, Q) = f_{T^e,P}(Q)^{(p^k-1)/r},$$

The twisted Ate pairing is also a power of the reduced Tate pairing.

Côut des couplages

Pairing computation on elliptic curves in Weierstrass form is usually performed in Jacobian coordinates , but we find that homogenous coordinates will give better results in our case. Our starting point is a suggestion for pairing computation in homogenous coordinates given in [**?**]. The point $T = (X, Y, Z)$ in homogenous coordinates represents the affine point $(X/Z, Y/Z)$ on the elliptic curve. Due to the denominator elimination, the doubling step of the Miller loop becomes :

$$\begin{aligned} (2i)P &\leftarrow 2 \cdot (iP) \\ f_{2i,P} &\leftarrow f_{i,P}^2 h_1(Q) S_T(Q) \end{aligned}$$

where $h_1(Q) = 2YZy_Q - 3X^2x_Q + Y^2 - 3cZ^2$ and $S_T(Q) = Z^2x_Q^2 + XZx_Q + X^2$. We compute $(2i)P = (X_3, Y_3, Z_3)$ as

$$\begin{aligned} X_3 &= 2XY(Y^2 - 9Z^2), \\ Y_3 &= (Y - Z)(Y + 3Z)^3 - 8Y^3Z, \\ Z_3 &= 2Y^3Z. \end{aligned}$$

We denote by S_{p^n} and M_{p^n} the cost of a squaring and a multiplication, respectively, in the extension field of degree n of $\mathbb{F}_p$. We assume that the

La sécurité des couplages

The security of a pairing based cryptosystem relies on two parameters : the bit length of r, $\log_2 r$ and the bit size of the extension field $k\log_2 p$. These parameters have to be chosen large enough to ensure that the discrete logarithm problem will be hard in both the subgroup of points of order r of the curve and the multiplicative group of the finite field $\mathbb{F}_{p^k}$. The fastest known attack on finite field is the index calculus method, whose complexity is $\mathcal{O}(L_r(\frac{1}{3}))$, where $L_r(\frac{1}{3}) = \exp\left((32/9)^{(1/3)}(\log r)^{\frac{1}{3}}\log(\log(r))^{\frac{2}{3}}\right)$ and c is a constant depending on the characteristic of the finite field [**?**]. Meanwhile the best attack known on elliptic curves DLP is the Pollard-ρ method, whose complexity is $\mathcal{O}(\sqrt{r})$ [**?**, Chap. 17]. As a consequence, while the security level will increase, the bound on $k\log_2(p)$ is expected to grow faster than the bound on $\log_2(r)$. Following NIST recommendations [**?**], Table 1 gives optimal bit sizes of r and p^k for different security levels.

TAB.: Level of security in bit

AES security	size of r	size of p^k	Most adapted embedding degree
80	160	1024	$k = 6$ and $\rho \approx 1$

Comparaison des coûts des couplages

TAB.: Arithmetic of finite fields

M_{p^2}	M_{p^3}	M_{p^4}	M_{p^5}	M_{p^6}
$3M_p + 4A_p$	$5M_p + 20A_p$	$9M_p + 20A_p$	$13M_p + 58A_p$	$15M_p + 72A_p$

Mettre la comparaison entre k=15, 16 et 18 au niveau de sécurité 192 bits. Avec arithmétique pas optimisée

TAB.: A security evaluation : curves with embedding degree 15 versus Barreto-Naehrig curves

AES security	recommended group sizes		group sizes $k = 15$		group s ($k =$	
	bit length of r	bit length of p^k	r	p	r	
128	256	3072	256	384	256	256 (
192	384	7680	384	576	384	480 (

Outline

Optimisation de l'arithmétique dans $\mathbb{F}_{p^5}$

En utilisant les multiplications de Karatsuba et Toom Cook une multiplication dans $\mathbb{F}_{p^5}$ s'effectue en $13M_p + 60A_p$ l'article de Montgmory la propose en $13M_p + 22A_p$. Nous proposons d'effectuer cette multiplication en $9M_p + 107A_p$ en utilisant l'interpolation de Newton.

1. l'évaluation en les valeurs d'interpolation α_i des polynômes $A(X)$ et $B(X)$, pour $i = 0, 1, 2, \ldots, 8$;
2. les neuf multiplications dans $\mathbb{F}_p$ ($A(\alpha_i) \times B(\alpha_i)$) ;
3. le calcul des c'_i dont les formules sont données dans la partie **??**, pour $i = 0, 1, 2, \ldots, 8$;
4. la construction du polynôme de degré 8 $C(X) = A(X) \times B(X)$, via le schéma de Horner.

Les quatre multiplications dans $\mathbb{F}_p$ ont une complexité de

$$4(5N^{1,6}(1+m))A_w.$$

Les 43 additions dans $\mathbb{F}_p$ ont une complexité de $43NA_w$.
Nous cherchons m telle que l'inégalité suivante soit vraie :

$$4(5N^{\log_2(3)}(1+m))A_w > 43NA_w$$