Multiplication scalaire de Montgomery pour les courbes de genre 2 en caractéristique 2

Sylvain Duquesne

Université Montpellier 2

Journées C2

Carcans, 20 mars 2008

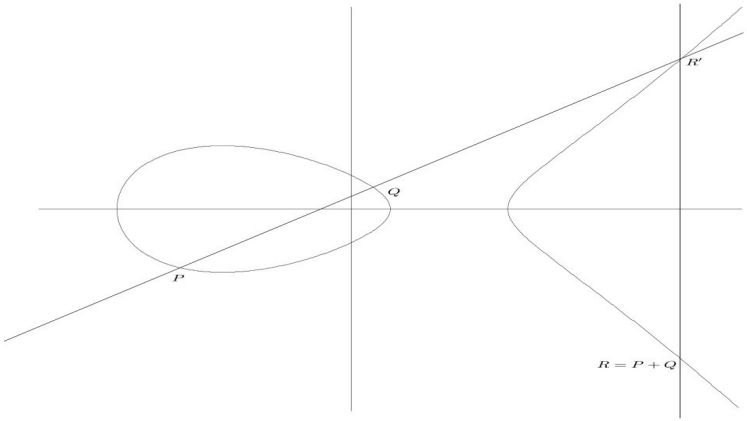
Institut de Mathématiques et de
Modélisation de Montpellier
et
Laboratoire d'Informatique de Robotique
et de Microélectronique de Montpellier

Rapides rappels sur la cryptographie (hyper)elliptique

Une courbe elliptique

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

est un groupe



$\Rightarrow$ Cryptographie à clé publique utilisant le logarithme discret

Opération centrale : multiplication scalaire $(n, P) \longrightarrow nP$

Algorithme standard

- Initialiser T à $\mathcal{O}$
- Pour chaque bit n_i de n, faire
  - $T \leftarrow 2T$
  - et $T \leftarrow T + P$ si $n_i = 1$

Plein d'améliorations possibles

Multiplication scalaire de Montgomery pour les courbes elliptiques

But : algorithme efficace de multiplication scalaire (nP)

Idée : on considère seulement l'abscisse du point

Incovénient

On ne distingue plus un point P et son opposé $-P$

- Gênant pour l'addition $(\pm P \pm Q = \pm(P+Q)$ ou $\pm(P-Q))$
- Pas gênant pour le doublement $(\pm P \pm P = \pm 2P$ ou $\mathcal{O})$

Pour le calcul de nP on utilise comme variable temporaire un couple $(kP, (k+1)P)$ dont la différence est toujours connue.

Multiplication scalaire de Montgomery pour les courbes elliptiques

But : algorithme efficace de multiplication scalaire (nP)

Idée : on considère seulement l'abscisse du point

- formules d'addition et doublement plus efficaces
- nouvel algorithme de multiplication scalaire
- efficace seulement (en caractéristique impaire) pour les courbes données par

$$By^2 = x^3 + Ax^2 + x$$

- résistance aux attaques par canaux cachés

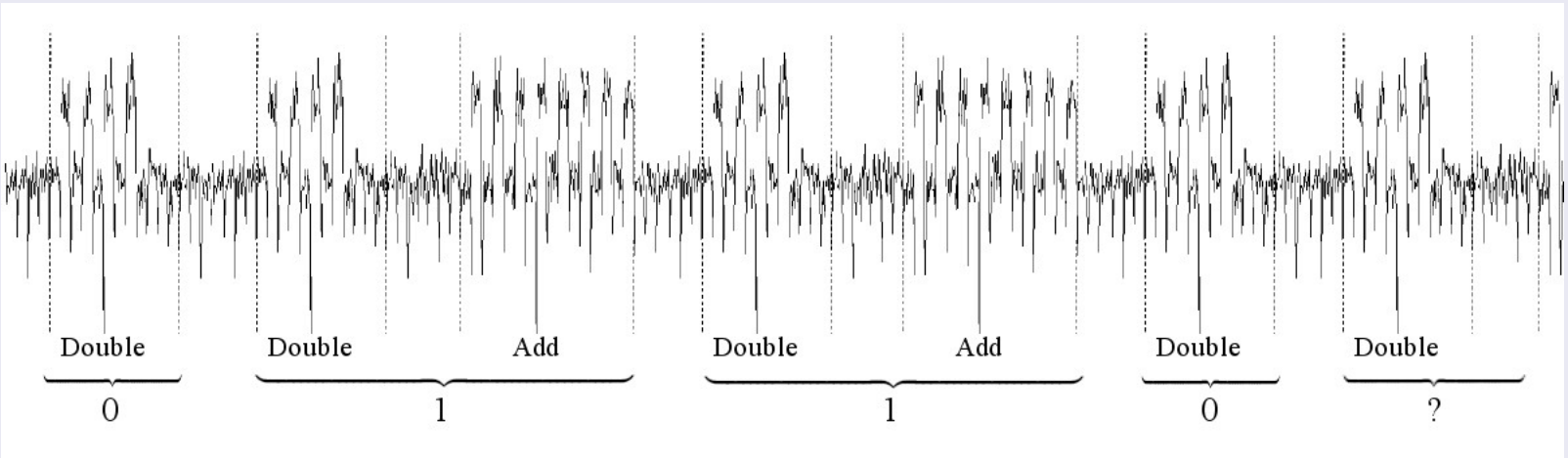
Meilleure multiplication scalaire sur les courbes elliptiques

Les attaques par canaux cachés

Faiblesse : les opérations effectuées dépendent des bits de la clé

Exemple

Un double-and-add effectue un doublement si le bit de n vaut 0 et un doublement et une addition si le bit vaut 1



Possibilité d'analyser d'autres fuites

Courbes hyperelliptiques

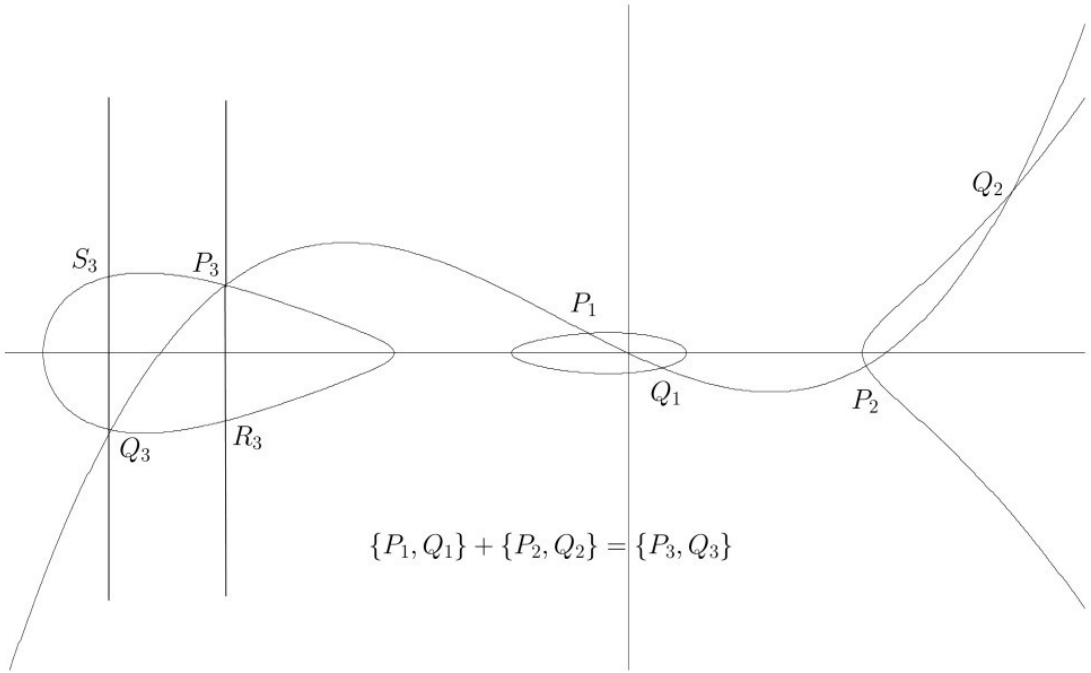
Une courbe hyperelliptique sur $\mathbf{K}$ de genre $\mathbf{g}$ est donnée par une équation

$$\mathbf{y^2 + h(x)y = f(x)}$$

avec $\mathbf{h, f} \in \mathbf{K[x]}$ de degrés $\mathbf{g}$ et $2\mathbf{g}+1$ ou $2\mathbf{g}+2$.

On donne aux $\mathbf{g}$-uplets de points une structure de groupe : la **Jacobienne**

Loi de groupe en genre 2 :



La variété de Kummer

Motivations

- Arithmétique compliquée sur la Jacobienne
- Trop d'information

La variété de Kummer est le quotient de la Jacobienne par l'involution hyperelliptique : on identifie un élément et son opposé

En genres 1 et 3

- Pour les courbes elliptiques : prendre juste l'abscisse
  $\longrightarrow$ "simple" et connu
- Pour les courbes de genre 3 : variété de $\mathbb{P}^7(\mathbf{K})$ définie par 27 équations
  $\longrightarrow$ compliqué

Surface de Kummer en genre 2 et caractéristique impaire

$$\begin{array}{rccc} \kappa : & \mathcal{J}_{\mathbf{K}}(\mathcal{C}) & \longrightarrow & \mathbb{P}^3(\mathbf{K}) \\ & \{(\mathbf{x}_1, \mathbf{y}_1), (\mathbf{x}_2, \mathbf{y}_2)\} & \longmapsto & [1, \mathbf{x}_1 + \mathbf{x}_2, \mathbf{x}_1\mathbf{x}_2, \beta_0] \end{array}$$

avec $\beta_0 = \frac{2\mathbf{f}_0+\mathbf{f}_1(\mathbf{x}_1+\mathbf{x}_2)+2\mathbf{f}_2\mathbf{x}_1\mathbf{x}_2+\mathbf{f}_3\mathbf{x}_1\mathbf{x}_2(\mathbf{x}_1+\mathbf{x}_2)+2\mathbf{f}_4\mathbf{x}_1^2\mathbf{x}_2^2+\mathbf{f}_5\mathbf{x}_1^2\mathbf{x}_2^2(\mathbf{x}_1+\mathbf{x}_2)^2+2\mathbf{f}_6\mathbf{x}_1^3\mathbf{x}_2^3-2\mathbf{y}_1\mathbf{y}_2}{(\mathbf{x}_1-\mathbf{x}_2)^2}$

La loi de groupe sur la Jacobienne est perdue sur la surface de Kummer.

Toutefois :

- **Addition d'un élément de 2-torsion**
  matrice 4×4 obtenue par la loi de groupe
- **Formes biquadratiques**

$$\mathbf{k_i}(\mathcal{A}+\mathcal{B})\mathbf{k_j}(\mathcal{A}-\mathcal{B}) + \mathbf{k_i}(\mathcal{A}-\mathcal{B})\mathbf{k_j}(\mathcal{A}+\mathcal{B})$$

  déduites du cas $\mathcal{B}$ de 2 torsion
- **Doublement**
  cas particulier des formes biquadratiques

Multiplication scalaire de Montgomery en genre 2 et caractéristique impaire

Entrée : $\mathcal{C}$ une courbe de genre 2 sous forme de Montgomery
$\mathcal{D} \in \mathcal{J}_{\mathcal{C}}(\mathbf{K})$ et $\mathbf{n} \in \mathbb{Z}$

Sortie : $\kappa(\mathbf{n}\mathcal{D})$, l'image de $\mathbf{n}\mathcal{D}$ dans la surface de Kummer

- Initialisation $(\kappa(\mathcal{A}), \kappa(\mathcal{B})) = ([0,0,0,1], \kappa(\mathcal{D}))$
- Si le bit de $\mathbf{n}$ vaut 0, $(\kappa(\mathcal{A}), \kappa(\mathcal{B})) = (\kappa(2\mathcal{A}), \kappa(\mathcal{A}+\mathcal{B}))$
- Si le bit de $\mathbf{n}$ vaut 1, $(\kappa(\mathcal{A}), \kappa(\mathcal{B})) = (\kappa(\mathcal{A}+\mathcal{B}), \kappa(2\mathcal{B}))$
- Après avoir fait ça pour chaque bit de $\mathbf{n}$, return $\kappa(\mathcal{A})$

Remarques

- A chaque étape, on a toujours $\kappa(\mathcal{B}-\mathcal{A}) = \kappa(\mathcal{D})$ et l'addition de $\mathcal{A}$ et $\mathcal{B}$ est donc possible
- On fait un doublement et une addition pour chaque bit de l'exposant

La surface de Kummer en caractéristique 2

Les coordonnées sont données par

$$\begin{aligned} k_1 &= 1 \\ k_2 &= x_1 + x_2 \\ k_3 &= x_1 x_2 \\ k_4 &= \frac{(x_1+x_2)\left(x_1^2x_2^2+f_3x_1x_2+f_1\right)+h(x_2)y_1+h(x_1)y_2}{(x_1+x_2)^2} \end{aligned}$$

Formes biquadratiques

Il existe des formes biquadratiques φ_{ij} telles que, projectivement

$$k_i(\mathcal{A}+\mathcal{B})k_j(\mathcal{A}-\mathcal{B}) + \varepsilon_{ij}k_i(\mathcal{A}-\mathcal{B})k_j(\mathcal{A}+\mathcal{B}) = \varphi_{ij}(\mathcal{A},\mathcal{B})$$

avec $\varepsilon_{ij} = 1$ si $i \neq j$ et 0 si $i = j$

$\longrightarrow$ formules pour le doublement et l'addition

Comment calcule t'on ces formes biquadratiques ?

- Les astuces de la caractéristique impaire ne s'appliquent pas
- Le calcul brutal est irréalisable

Principe de la méthode utilisée

On réitère le procédé suivant

- Effectuer le calcul brutal sur des cas particuliers ou en spécialisant des variables
- En déduire des propriétés du résultat dans le cas général
- Utiliser ces propriétés pour imposer des contraintes sur le calcul brutal qui en diminuent la complexité

Classification des courbes de genre 2 en caractéristique 2

On s'interesse, en cryptographie, aux courbes définies sur $\mathbb{F}_{2^d}$ par

$$y^2 + (h_2x^2 + h_1x + h_0)y = x^5 + f_4x^4 + f_3x^3 + f_2x^2 + f_1x + f_0$$

Type de courbes

- Type I : $h_2 \neq 0$
- Type II : $h_2 = 0$, $h_1 \neq 0$
- Type III : $h_2 = h_1 = 0$, $h_0 \neq 0$

On peut représenter ces courbes par les équations

$$\begin{aligned}
\text{Type Ia} &: y^2 + (x^2 + h_1x + h_1^2)y = x^5 + \varepsilon x^4 + f_2x^2 + f_0 \\
\text{Type Ib} &: y^2 + (x^2 + h_1x)y = x^5 + \varepsilon x^4 + f_2x^2 + f_0 \\
\text{Type II} &: y^2 + xy = x^5 + f_3x^3 + \varepsilon x^2 + f_0
\end{aligned}$$

Formules d'addition pour les courbes de type II

$$
\begin{aligned}
\mathbf{k}_1(\mathcal{A}+\mathcal{B}) &= \varphi_{11}(\mathcal{A},\mathcal{B}) \\
\mathbf{k}_2(\mathcal{A}+\mathcal{B}) &= \varphi_{12}(\mathcal{A},\mathcal{B}) + \mathbf{k}_1(\mathcal{A}+\mathcal{B})\mathbf{k}_2(\mathcal{A}-\mathcal{B}) \\
\mathbf{k}_3(\mathcal{A}+\mathcal{B}) &= \varphi_{13}(\mathcal{A},\mathcal{B}) + \mathbf{k}_1(\mathcal{A}+\mathcal{B})\mathbf{k}_3(\mathcal{A}-\mathcal{B}) \\
\mathbf{k}_4(\mathcal{A}+\mathcal{B}) &= \varphi_{14}(\mathcal{A},\mathcal{B}) + \mathbf{k}_1(\mathcal{A}+\mathcal{B})\mathbf{k}_4(\mathcal{A}-\mathcal{B})
\end{aligned}
$$

avec

$$
\begin{aligned}
\varphi_{11}(\mathcal{A},\mathcal{B}) &= (\mathbf{k}_1\mathbf{l}_4 + \mathbf{k}_2\mathbf{l}_3 + \mathbf{k}_4\mathbf{l}_1 + \mathbf{k}_3\mathbf{l}_2)^2 \\
\varphi_{12}(\mathcal{A},\mathcal{B}) &= (\mathbf{k}_1\mathbf{l}_3 + \mathbf{k}_3\mathbf{l}_1)^2 \\
\varphi_{13}(\mathcal{A},\mathcal{B}) &= \mathbf{k}_3\mathbf{l}_1(\mathbf{k}_1\mathbf{l}_4 + \mathbf{k}_2\mathbf{l}_3) + \mathbf{k}_1\mathbf{l}_3(\mathbf{k}_4\mathbf{l}_1 + \mathbf{k}_3\mathbf{l}_2) \\
\varphi_{14}(\mathcal{A},\mathcal{B}) &= (\mathbf{k}_4\mathbf{l}_1 + \mathbf{k}_3\mathbf{l}_2)(\mathbf{k}_1\mathbf{l}_4 + \mathbf{k}_2\mathbf{l}_3)
\end{aligned}
$$

Formules particulièrement simple (11M+2S)

$\longrightarrow$ multiplication scalaire très rapide

Complexités et comparaisons de performances

Type	Ia	Ia (h_1=1)	Ib	Ib (h_1=1)	II
Formules de Lange					
Doublement	38M+7S	33M+6S	37M+6S	33M+6S	20M+8S
Addition	38M+4S	35M+5S	37M+4S	35M+4S	42M+7S
Fenêtre glissante	46M+8S	40M+7S	44M+8S	42M+8S	28M+9S
avec S=0.3M	48M	42M	47M	44M	31M
avec S=0	46M	40M	44M	42M	28M
Surface de Kummer					
Doublement	22M+5S	14M+6S	17M+6S	10M+6S	6M+6S
Addition	36M+S	26M+S	17M+S	13M+S	11M+2S
Montgomery	58M+6S	40M+7S	34M+7S	23M+7S	17M+8S
avec S=0.3M	60M	42M	36M	25M	19M
avec S=0	58M	40M	34M	23M	17M
gain avec S=0.3M	-25%	0%	22%	40%	39%
gain avec S=0	-26%	0%	23%	42%	39%

Approche de Gaudry et Lubicz

Utilisation des fonctions Θ pour définir la surface de Kummer

Nécessite que tous les points de 2-torsion soient rationnels

En caractéristique 2

- Seulement le type Ib avec $h_1 = 1$
- 16 à 18M par bit dans ce cas

gain de 25%

Unification des 2 approches ?

Comparaison avec les courbes elliptiques

Pourquoi le genre 2 ?

$\#\mathcal{J}_{\mathbb{F}_q}(\mathcal{C}) \simeq q^2$ contre q pour les courbes elliptiques

Corps de base 2 fois plus petit pour la même sécurité
$\Rightarrow$ Arithmétique de base plus efficace (3 à 4 fois)

Meilleur algorithme en caractéristique 2 : Montgomery (6M et 4S par bit)

Montgomery en genre 2 (type II) : 17M et 8S par bit

Gain de 5 à 10 % dans le pire des cas