TP13 : Courbes elliptiques

Résumé du TP

Bertrand Meyer

8 juin 2020

Les base pratiques des courbes elliptiques

Equation de Weierstraß

Définition
Soient a et $b \in \mathbb{F}_q$, corps de caractéristique $\neq 2, 3$. On suppose que

$$\Delta = -16(4a^3 + 27b^2) \neq 0.$$

Equation de Weierstraß

Définition
Soient a et $b \in \mathbb{F}_q$, corps de caractéristique $\neq 2, 3$. On suppose que

$$\Delta = -16(4a^3 + 27b^2) \neq 0.$$

La courbe elliptique $\mathcal{E}_{a,b}$ est la réunion du point à l'infini $(0:1:0)$ et de l'ensemble des points affines $(x, y) \in \mathbb{F}_q^2$ tels que

$$\mathcal{E}_{a,b}: \quad y^2 = x^3 + ax + b.$$

Equation de Weierstraß

Définition
Soient a et $b \in \mathbb{F}_q$, corps de caractéristique $\neq 2, 3$. On suppose que

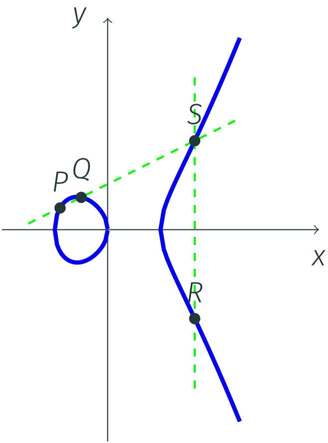
$$\Delta = -16(4a^3 + 27b^2) \neq 0.$$

La courbe elliptique $\mathcal{E}_{a,b}$ est la réunion du point à l'infini $(0 : 1 : 0)$ et de l'ensemble des points affines $(x, y) \in \mathbb{F}_q^2$ tels que

$$\mathcal{E}_{a,b} : \quad y^2 = x^3 + ax + b.$$

Géométriquement, une courbe elliptique est une courbe algébrique projective lisse de genre 1.

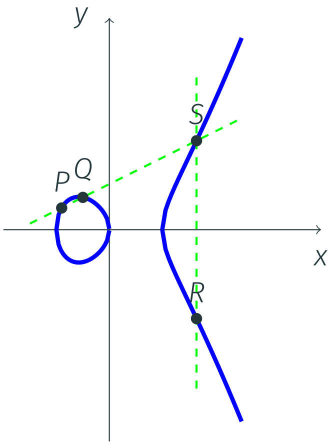
Loi d'addition



Somme des points $R = P + Q$:

$$
\begin{aligned}
x_R &= \lambda^2 - x_P - x_Q \\
y_R &= -y_P + \lambda(x_P - x_R) \\
\lambda &= \text{pente } (PQ) \\
&= \begin{cases} \dfrac{y_Q - y_P}{x_Q - x_P} & \text{si } P \neq Q \\ \text{ou} & \\ \dfrac{3x_P^2 + a}{2y_P} & \text{si } P = Q \end{cases}
\end{aligned}
$$

Loi d'addition



Somme des points $R = P + Q$:

$$
\begin{aligned}
x_R &= \lambda^2 - x_P - x_Q \\
y_R &= -y_P + \lambda(x_P - x_R) \\
\lambda &= \text{pente } (PQ) \\
&= \begin{cases} \dfrac{y_Q - y_P}{x_Q - x_P} & \text{si } P \neq Q \\ \quad\text{ou} & \\ \dfrac{3x_P^2 + a}{2y_P} & \text{si } P = Q \end{cases}
\end{aligned}
$$

Attention aux cas particuliers : points de 2-torsion, point $0_{\mathcal{E}}$, etc.

Les courbes elliptiques en cryptographie

Aspects cryptographiques

Le groupe abélien $\mathcal{E}_{a,b}(\mathbb{F}_q)$ remplace avantageusement le groupe $(\mathbb{Z}/N\mathbb{Z})^\times$ dans de nombreux protocoles cryptographiques (par exemple Diffie-Hellman, El-Gamal, etc).

Aspects cryptographiques

Le groupe abélien $\mathcal{E}_{a,b}(\mathbb{F}_q)$ remplace avantageusement le groupe $(\mathbb{Z}/N\mathbb{Z})^\times$ dans de nombreux protocoles cryptographiques (par exemple Diffie-Hellman, El-Gamal, etc).

Le groupe $\mathcal{E}_{a,b}(\mathbb{F}_q)$ possède $q+1+O(\sqrt{q})$ points (borne de Hasse).

Aspects cryptographiques

Le groupe abélien $\mathcal{E}_{a,b}(\mathbb{F}_q)$ remplace avantageusement le groupe $(\mathbb{Z}/N\mathbb{Z})^\times$ dans de nombreux protocoles cryptographiques (par exemple Diffie-Hellman, El-Gamal, etc).

Le groupe $\mathcal{E}_{a,b}(\mathbb{F}_q)$ possède $q+1+O(\sqrt{q})$ points (borne de Hasse).

En général, on stocke seulement l'abscisse d'un point : avec $n = \log_2 q$ bits, on a accès à un groupe contenant $\simeq 2^n + O(2^{n/2})$ points.

Aspects cryptographiques

Le groupe abélien $\mathcal{E}_{a,b}(\mathbb{F}_q)$ remplace avantageusement le groupe $(\mathbb{Z}/N\mathbb{Z})^\times$ dans de nombreux protocoles cryptographiques (par exemple Diffie-Hellman, El-Gamal, etc).

Le groupe $\mathcal{E}_{a,b}(\mathbb{F}_q)$ possède $q+1+O(\sqrt{q})$ points (borne de Hasse).

En général, on stocke seulement l'abscisse d'un point : avec $n = \log_2 q$ bits, on a accès à un groupe contenant $\simeq 2^n + O(2^{n/2})$ points.

Dans les applications cryptographiques, on utilise des courbes telles que $|\mathcal{E}_{a,b}(\mathbb{F}_q)|$ est proche d'un nombre premier. L'algorithme de Schoof-Elkies-Atkin calcule le cardinal d'une courbe en $O(n^{4+o(1)})$.

Une courbe fréquente : P_{256} du NIST

La courbe

$$y^2 = x^3 - 3x + b \in \mathbb{F}_p[x, y]$$

avec

$$\begin{aligned} b &= \texttt{0x5ac635d8aa3a93e7b3ebbd55769886bc651d06b0cc53b0f63bce3c3e27d2604b} \\ p &= \texttt{0xffffffff00000001000000000000000000000000ffffffffffffffffffffffff} \end{aligned}$$

est isomorphe à $\mathbb{Z}/m\mathbb{Z}$ avec

$$m = \texttt{0xffffffff00000000ffffffffffffffffbce6faada7179e84f3b9cac2fc632551}$$

points. Elle est classique pour la cryptographie par courbe elliptique (ECC) en 256 bits.

La factorisation par la méthode de Lenstra

Comparaison entre ρ de Pollard et ECM

But :
Factoriser n. On suppose $n = p \cdot q$ pour simplifier.

Méthode ρ de Pollard	ECM de Lenstra
$a \in \mathcal{G} = (\mathbb{Z}/n\mathbb{Z})^\times \simeq (\mathbb{Z}/p\mathbb{Z})^\times \oplus (\mathbb{Z}/q\mathbb{Z})^\times$	$A \in \mathcal{G} = \mathcal{E}_{a,b}(\mathbb{Z}/n\mathbb{Z}) \simeq \mathcal{E}_{a,b}(\mathbb{Z}/p\mathbb{Z}) \times \mathcal{E}_{a,b}(\mathbb{Z}/q\mathbb{Z})$
Trouver m tel que	Trouver m tel que
$a^m \mapsto (1, x \neq 1) \mod p, q$	$m \cdot A \mapsto (0_\mathcal{E}, X \neq 0_\mathcal{E}) \mod p, q$
Conséquence : $a^m - 1 \wedge n = p$	**Conséquence :** mA est ET n'est pas $0_{\mathcal{E}(\mathbb{Z}/n\mathbb{Z})}$. Le calcul échoue lors d'une division mod n ($\rightarrow$ pgcd non trivial).

Méthode ECM

On calcule $m \cdot A$ dans $\mathcal{G} = \mathcal{E}_{a,b}(\mathbb{Z}/n\mathbb{Z})$.
Si m est multiple de l'ordre de A dans $\mathcal{E}_{a,b}(\mathbb{Z}/p\mathbb{Z})$ et non dans $\mathcal{E}_{a,b}(\mathbb{Z}/q\mathbb{Z})$, l'algorithme réussit.

On utilise

$$m = \mathrm{ppcm}\{1, 2, 3, \ldots, b\}.$$

On peut faire varier le groupe $\mathcal{G}$: plus de chances de succès en itérant.

Les dangers de l'exponentiation usuelle

La situation

Dans la plupart des protocoles cryptographiques, un point de la courbe G est fixé et il est nécessaire de calculer

$$s \cdot G$$

où s doit rester secret pour l'intégrité du protocole.

Exemple (Diffie-Hellman)
Alice et Bob choisissent a et $b \in \mathbb{Z}$ respectivement, calculent et s'échangent $a \cdot G$ et $b \cdot G$ et disposent de $ab \cdot G$ comme secret commun.

L'exponentiation rapide

Il est classique de calculer $s \cdot G$ par exponentiation rapide :

$$s \cdot G = \begin{cases} \lfloor \frac{s}{2} \rfloor \cdot (2 \cdot G) & \text{si } s > 1 \text{ est pair} \\ \lfloor \frac{s}{2} \rfloor \cdot (2 \cdot G) + G & \text{si } s > 1 \text{ est impair} \\ 0_{\mathcal{E}} & \text{si s=0} \\ G & \text{si } s = 1 \end{cases}$$

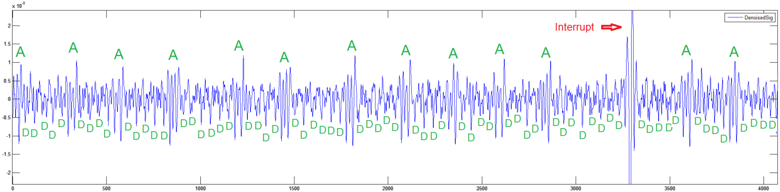
L'exponentiation rapide

Il est classique de calculer $s \cdot G$ par exponentiation rapide :

$$s \cdot G = \begin{cases} \lfloor \frac{s}{2} \rfloor \cdot (2 \cdot G) & \text{si } s > 1 \text{ est pair} \\ \lfloor \frac{s}{2} \rfloor \cdot (2 \cdot G) + G & \text{si } s > 1 \text{ est impair} \\ 0_{\mathcal{E}} & \text{si s=0} \\ G & \text{si } s = 1 \end{cases}$$

Comme dupliquer et additionner sont deux opérations différentes, le bruit du calcul de $s \cdot G$ révèle les bits successifs de s.

Une attaque par canaux cachés



Équation alternative à l'équation de Weierstraß :

$$x^2 + y^2 = 1 + dx^2y^2.$$

- formule unifiée de l'addition et de la dupplication,
- ne représente pas toutes les courbes,
- présente d'autres faiblesses.

Aperçu de la seconde partie sur les courbes elliptiques

Dans le prochain épisode (TP 14)

- Alice, Bob et Charlie tiennent une partie à trois grâce au protocole de Diffie-Hellman triparti.
- Ève surprend le terrible secret entre Alice et Bob grâce à une attaque par couplage (M.O.V.).
- Et d'autres aventures encore.

Retrouvez vos héros la semaine prochaine pour le grand final de la saison.