Génération de courbes elliptiques sécurisées

Les courbes elliptiques

On considère un corps fini $\mathbb{F}_p$ de caractéristique p > 3.

Définition: une courbe elliptique E sur K est définie par une équation de Weierstrass de la forme

$$E/\mathbb{F}_p : y^2 = x^3 + ax + b,\ (a, b) \in \mathbb{F}_p^2$$

lorsque les dérivées partielles par rapport à x et y ne s’annulent jamais simultanément.

Une courbe elliptique possède une structure de groupe, que l’on définit par la suite.

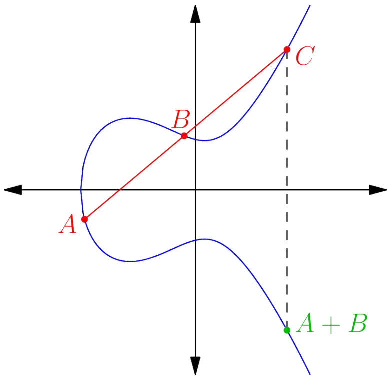
La loi de groupe

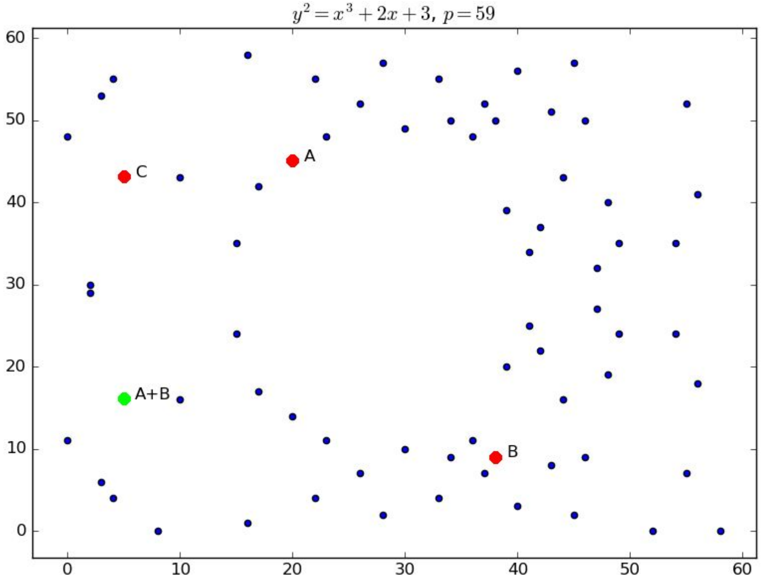
- Définition graphique simple dans le cas où K = R.
- Définition algébrique: pour 2 points A et B distincts,

$$x_{A+B} = \left(\frac{y_A - y_B}{x_A - x_B} \right)^2 - x_A - x_B$$

$$y_{A+B} = y_A + \frac{y_A - y_B}{x_A - x_B} \cdot (x_{A+B} - x_A)$$

- Formules semblables pour le doublage de point.
- Intérêt en cryptographie: Diffie-Hellman





Quelques outils théoriques

- Les endomorphismes de E admettent un degré, $\deg\ \psi$
- Il existe un morphisme $H : End(E) \to End(T_l(E)),\ \psi \mapsto \psi_l$
- ψ_l est représenté par une matrice d'ordre 2
- $\deg\ \psi = \det\ \psi_l$
- $\#\mathrm{Ker}\ \psi = \deg\ \psi$ pour ψ dite "séparable"
- Le morphisme de Frobenius, $\phi : E \to E,\ (x, y) \mapsto (x^p, y^p)$ vérifie $\deg\ \phi = p$

Quelques résultats

- Les éléments de $\mathbb{F}_p$ vérifient $x^p = x$, donc $E = \mathrm{Ker}(id - \phi)$
- $id - \phi$ est séparable, donc $\#\mathrm{Ker}(id - \phi) = \#E = \deg(id - \phi)$
- On a $\mathrm{tr}\ f = 1 + \det\ f - \det(id - f)$ en dimension 2, donc

$$\mathrm{tr}\ \phi_l = 1 + \deg\ \phi - \deg(id - \phi) \Rightarrow \#E = p + 1 - t$$

- $P = X^2 - tX + p$ est le polynôme caractéristique de ϕ_l, et on a

$$\deg(\phi^2 - t\phi + pid) = \det(\phi_l^2 - t\phi_l + pid) = 0$$

- Pour P tel que $[l]P = \mathcal{O},\ \phi^2(P) - [t\ mod\ l]\phi(P) + [p]P = \mathcal{O}$. Les points de la l-torsion permettent donc d'accéder à $t\ (mod\ l)$

L'algorithme de Schoof

Entrée: a, b et p définissant E.

Sortie: $\#E$

Complexité: $\mathcal{O}(\log^8 p)$

- Théorème de Hasse:

$$|\#E - (p+1)| \leq 2\sqrt{p}$$

- $$\#E = p + 1 - t$$

A ← 1
l ← 3
tant que A < 4√p:
    pour n ← 0, …,l-1:
        en calculant dans $\dfrac{F_p[x,y]}{(\psi_l, y^2 - f)}$
        si $(x^{p^2}, y^{p^2}) + [p](x,y) = [n](x^p, y^p)$:
            A ← lA
            n_l ← n
            p_l ← l
            sortir de la boucle
    l ← le prochain premier supérieur à l
t ← l'unique x dans 0, …, A vérifiant $x \equiv n_l \ [p_l]$
si t > 2√p:
    t ← t - A
renvoyer p+1 - t

Les caractéristiques d’une courbe sécurisée

Critères:

- p grand: $p > 2^{256}$ (256 bits dans sa représentation binaire)
- L’ordre du groupe est soit premier soit se factorise en $\#E = kr$ avec k petit et r premier
- $r \neq p$: cela exclu les courbes dites “anormales”, vulnérables
- L’ordre multiplicatif de p dans $\mathbb{F}_r$ est suffisamment grand (on le prendra supérieur à 20)

On dispose donc d’une fonction indiquant si une courbe est sécurisée ou non, selon #E, r_0 et k_0.

Utilisation dans la génération de courbes

Entrée: r_0, k_0

Sortie: a, b, p, $\#E$

p ← un nombre premier aléatoire supérieur à r

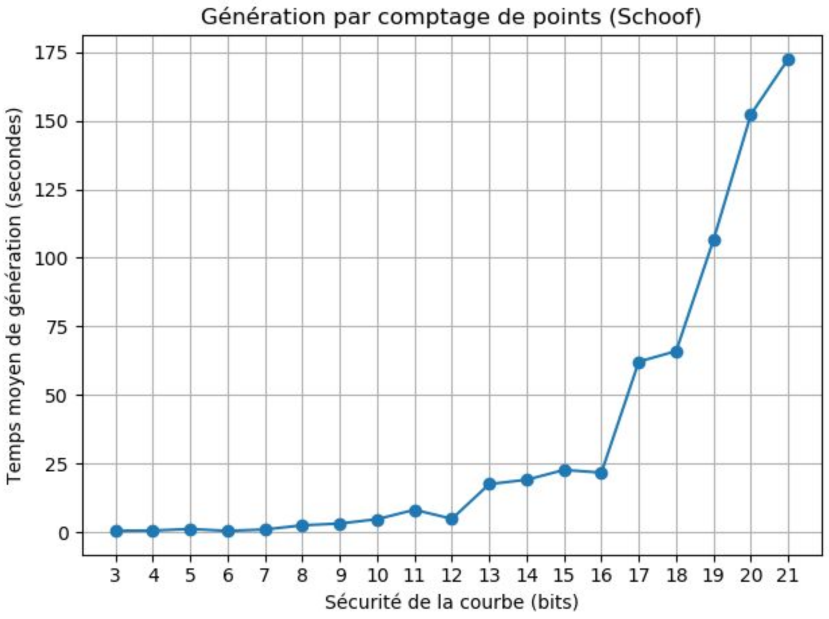
faire:

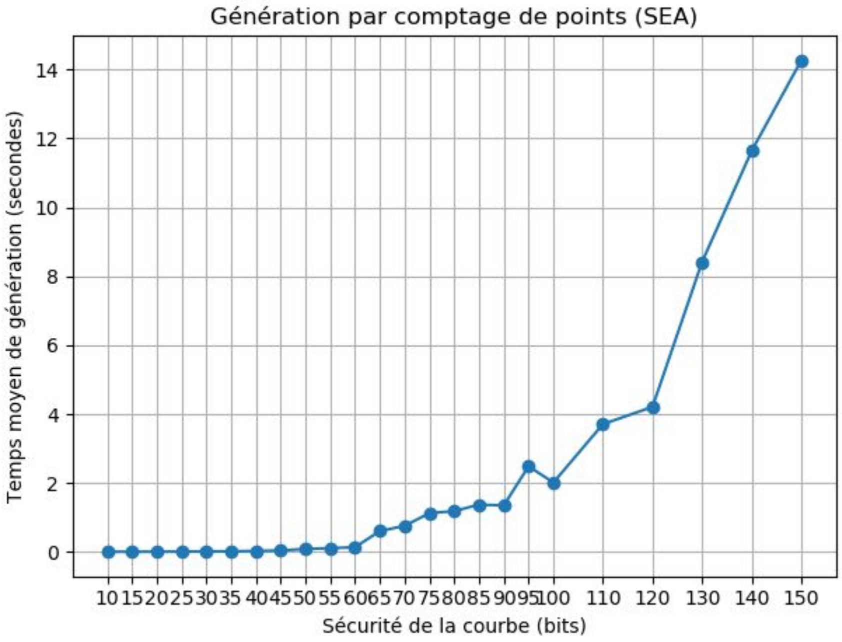
    a, b ← deux éléments aléatoires de $\mathbb{F}_p$

tant que schoof(a, b, p) ne vérifie pas les critères de sécurité;

renvoyer a, b, p, schoof(a, b, p)

Approche aléatoire: performance





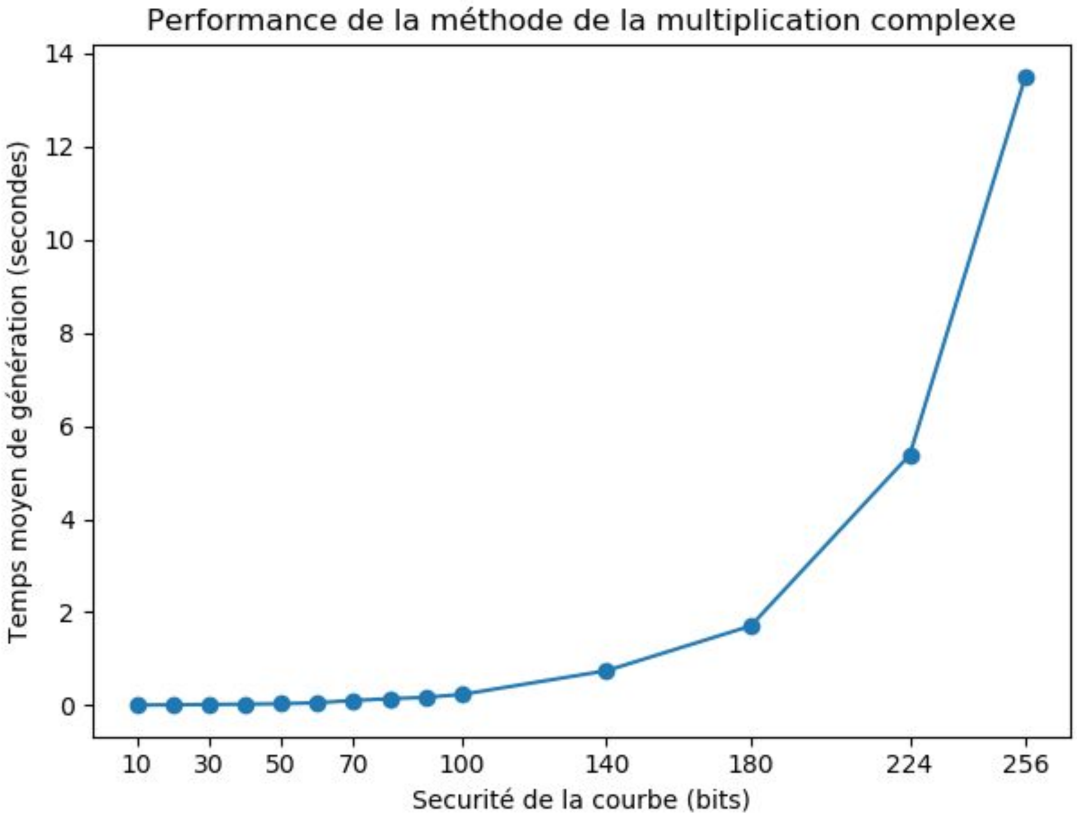
La méthode de la multiplication complexe

Entrée: r_0, k_0

Sortie: a, b, p, $\#E$

N ← 0
faire:
    d ← entier sans carré aléatoire tel que -d ≡ 0 ou 1 [4]
    m, s ← (4, 1) si d ≡ 3 [4], sinon (1, 2)
    u, v, p ← p > r premier, u et v tels que $mp = u^2+dv^2$
    si l'un de {p+1 - su, p+1 + su} vérifie les critères de sécurité:
        N ← p+1 ± su
tant que N = 0;
H ← le polynôme de classe de Hilbert de -d
j ← une racine de H dans $\mathbb{F}_p$
a ← -27j/(4(j - 1728))
b ← -a
E ← la courbe elliptique définie par (a, b, p)
P ← un point aléatoire de E
si l'ordre de P divise N:
    renvoyer a, b, p, N
sinon:
    a, b ← coefficients du tordu de E
    renvoyer a, b, p, N

Multiplication complexe: performance



Comparaison des méthodes