

TP3 - Formes de Montgomery et de Edward

Exercice 1. On considère la courbe standard P192 $E: y^2 = x^3 - 3x + b$ sur $\mathbb{F}_p$ où b et p sont définis dans le fichier "P192.m" sur Moodle et le point $G = (G_x, G_y)$ défini sur le même fichier.

1. (a) Calculer le cardinal de $E(\mathbb{F}_p)$ et vérifier qu'il est premier.
(b) Vérifier que G est un point de E . Quel est son ordre ?
2. (a) Écrire un programme qui calcule la somme de deux points en coordonnées affines et le tester avec un point aléatoire P et G déjà défini.
(b) Comparer le temps de calcul avec magma.
3. Mêmes questions avec la duplication en coordonnées jacobienes.
4. Écrire un algorithme de fenêtre glissante pour implémenter la multiplication scalaire. Les duplications utiliseront le programme que vous avez écrit en question 3.

Exercice 2.

1. Trouver une courbe elliptique E_m sur $\mathbb{F}_p$ sous forme de Montgomery avec un niveau de sécurité correspondant à un nombre premier de plus de 180 bits.
2. Trouver un point sur cette courbe dont l'ordre est le plus grand facteur premier divisant $\#E_m(\mathbb{F}_p)$.
3. Programmer la multiplication scalaire de Montgomery.
4. Cela a-t-il un sens de comparer avec la multiplication scalaire de l'exercice précédent ?

Exercice 3.

1. Établir une stratégie pour générer une courbe d'Edwards bonne pour la cryptographie avec $c = 1$ et d petit et non-carré.
2. Générer une courbe de Edward E_d avec un niveau de sécurité correspondant à un nombre premier de plus de 180 bits..
3. Implémenter la fenêtre glissante sur cette courbe et comparer avec les exercices précédents.