TP - ECC et ECDSA

3 octobre 2022

Le TP d'aujourd'hui est un examen. Un rendu est attendu : une archive contenant tout votre code. N'oubliez pas de commenter votre code.

Le rendu est à envoyer par mail pour le **vendredi 7 0ctobre, 23h59**, en incluant "[BCS]" dans l'objet, à l'adresse `andrea.lesavourey@irisa.fr`.

> L'objectif est d'implanter **en C** les opérations sur les courbes elliptiques nécessaires à la cryptographie.

Exercice 1 : Manipulation de points sur une courbe elliptique

Implantez les opérations nécessaires à la cryptographie basée sur les courbes elliptiques. Vous pouvez par exemple utiliser la librairie GMP pour manipuler des entiers de taille arbitraire.

Afin de rendre des étapes d'exponentiation plus efficaces, plusieurs méthodes ont été développées [1] [2]. L'objectif des exercices suivants est d'en explorer deux d'entre elles.

Exercice 2 : Fenêtre fixe ou méthode 2^k-aire

La méthode de la fenêtre fixe ou 2^k-aire consiste à calculer à l'avance certaines puissances de l'élément de base g qu'on pourra réutiliser durant le calcul d'éléments de la forme g^e. Adaptez cette méthode à la multiplication d'un point P d'une courbe elliptique par un scalaire.

Bonus : Implantez la version améliorée de cette méthode qu'est la fenêtre glissante.

Exercice 3 : Forme non adjacente

La forme non adjacente (NAF) d'un entier k est une représentation signée équivalente à la décomposition binaire. Elle permet notamment de remplacer des additions par des soustractions lors de la multiplication d'un point P par le scalaire k.

1. Codez des fonctions permettant de passer d'une décomposition binaire d'un entier à sa NAF et vice-versa.
2. Implantez un algorithme de multiplication d'un point par un scalaire qui utilise la NAF.

1. `https://en.wikipedia.org/wiki/Exponentiation_by_squaring`
2. `http://koclab.cs.ucsb.edu/teaching/ecc/eccPapers/Doche-ch09.pdf`