D34: Méthodes de calcul efficaces
Courbes elliptiques

1 Exercices

Exercice 1. Bases Doubles

1. Convertir l'entier 247 en base double chaînées.
2. Décrire les étapes de l'algorithme de multiplication de point `cBDNS` pour le calcul de $[247]P$.
3. On admet que $3141592653589 = 2^{32}3^6+3^{21}+2^{25}3^1+2^33^{10}+2^32^6+2^03^4+2^02^0$. Proposer un schéma de multiplication de point calculant $[3141592653589]P$ en 32 doublements, 21 triplements et 6 additions de points.
4. Proposer un algorithme de multiplication de points `DBNS` sur le modèle de l'algorithme de Yao calculant $[k]P$. Quel est son cout de calcul?

Exercice 2. Algorithme de Montgomery

1. Décrire les étapes de l'algorithme de Montgomery pour le calcul de $[132]P$, où P est un point sur une courbe elliptique quelconque.

On souhaite adapter l'algorithme de Montgomery au cas de la base 3.

2. On rappelle que l'algorihme calcule simultanément $[k']P$ et $[k'+1]P$, où k correspond aux bits de poids fort du scalaire k. Décrire les calculs que doit effectuer l'algorithme selon que le bit courant est égal à 0,1 ou 2.
3. Quel est le cout (en termes d'addition et doublement de points) par bit de scalaire cet algorithme? Comparer à la version binaire.
4. Proposer un algorithme adapté au cas des doubles bases chaînées.

Exercice 3. Addition Co-Z sur $E(\mathbb{F}_p)$

On rappelle les formules d'additions de points en coordonnées jacobiennes:

- Soient $P_1 = (X_1 : Y_1 : Z_1)$, $P_2 = (X_2 : Y_2 : Z_2)$ et $P_3 = P_1 + P_2 = (X_3 : Y_3 : Z_3)$:

$$A = X_1Z_1^2, \quad B = X_2Z_1^2, \quad C = Y_1Z_2^3, \quad D = Y_2Z_1^3, \quad E = B - A,$$
$$F = 2(D - C), \quad G = (2E)^2, \quad H = EG, \quad I = AG \quad .$$

$$X_3 = F^2 - H - 2I \quad Y_3 = F(F - X_3) - 2CH, \quad Z_3 = ((Z_1 + Z_2)^2 - Z_1^2 - Z_2^2)E$$

1. En supposant que $Z_1 = Z_2 = Z$, montrer que l'addition de points peut s'effectuer en seulement $5\mathtt{M} + 2\mathtt{S}$.

2. Montrer que l'on obtient, lors de l'addition de points, la mise à jour d'un des points P_1 ou P_2 de sorte qu'il partage la même coordonnée z que le point $P_1 + P_2$.
3. En remarquant que l'on peut faire la même observation pour le doublement, proposer une méthode efficace pour caculer $P, [2]P, [3]P, [5]P$ etc. Quel est le cout de cette méthode?
4. Établir une relation de récurrence simple entre les coordonnées z des points ainsi calculé.
5. En déduire un schéma de précalcul dont les points sont tous en coordonnées affines et ne faisant appel qu'a une seule inversion modulaire.

Exercice 4. Division de point

1. Décrire les différentes étapes du calcul de $[99]P$ en utilisant l'algorithme de division de point (`halving-add-add`).

On considère maintenant un point P d'une courbe elliptique $E(\mathbb{F}_2$ d'ordre impair s.

2. Soient k un entier de n bits et $d < n$. Montrer qu'il existe un nombre k' de la forme $\sum_{i=0}^{n-1-d} k_i 2^i + \sum_{i=1}^{d} k_{-i} 2^{-i}$ tel que $[k]P = [k']P$.
3. En déduire un algorithme de multiplication de point parallèle (sur deux threads) utilisant les algorithmes `double-and-add` et `halving-add-add`. Discuter l'efficacité de cet algorithme en fonction de d.

Exercice 5. Courbes Koblitz

On considèrel la courbe de Koblitz $E_1 : y^2 + xy = x^3 + x^2 + 1$.

1. Calculer la τ-représentation de 12. Détailler les étapes du calcul de $[12]P$ en utilisant l'algorithme τ-`and-add`.
2. On suppose le point P fixé. Proposer un algorithme de multiplication de point de type méthode combinée et expliciter son cout de calcul.
3. Soient maintenant deux points P et Q ainsi que deux scalaires r et s. Écrire un algorithme de multiplication de points multiples permettant le calcul de $[r]P + [s]Q$ et exploitant la τ représentation de r et s.

2 Programmation

Exercice 1. Optimisation de la méthode w`NAF`

Le but de l'exercice est de mener une expérience numérique afin de trouver la taille de fenêtre idéale pour l'algorithme de multiplication de point utilisant la méthode w`NAF` en coordonnées jacobiennes. Tous les calculs sur les grands nombres se feront à l'aide de `gmp`. Les expérience numériques se feront à partir des paramètres contenus dans le fichier `ecc_param.h`.

1. Implanter les fonctions de bases de l'arithmique des courbes elliptiques: addition, doublement, mise à jour, test d'appartenance.
2. Implanter une fonction de conversion d'un entier k en représentation w`NAF`.

3. Implanter une fonction permettant de précalculer tous les points $[3]P, [5]P, \ldots, [2^{w-1}-1]P$, où w et P sont des paramètres.
4. Implanter la multiplication scalaire w`NAF` permettant le calcul de $[k]P$.
5. Effectuer une expérience numérique montrant l'efficacité de l'algirthme pour différentes valeurs de w.