Elliptic-Curve Diffie-Hellman

BEHAGUE Quentin, LECORNU Adrien
Sous la direction de CASTANHEIRA Stéphane
École normale supérieure de Rennes

Table des matières

1 Introduction

Dans leur article "New Directions in Cryptography" paru en 1976 pour lequel ils recevront le prix Turing en 2015, Whitfield Diffie et Martin Hellman introduisent un nouvel algorithme révolutionnaire. Celui-ci permet à deux interlocuteurs de générer à distance une même clé secrète de manière sécurisée.

Dans ce rapport, nous présenterons le vocabulaire de la cryptographie avant de formuler le protocole d'échange de clés Diffie-Hellman (sur le groupe $\mathbb{Z}/p\mathbb{Z}$). Par la suite, nous introduirons le concept de courbes elliptiques et leur structure de groupe, utilisé dans une version plus moderne de Diffie-Hellman : le protocole Elliptic-Curve-Diffie-Hellman (ECDH). Enfin, nous donnerons des résultats expérimentaux, obtenus en implémentant ECDH avec le language `Python`, sur la sécurité du protocole et nous donnerons des méthodes pour trouver des générateurs convenables dans l'algorithme.

2 Cryptographie : Chiffrement, Sinature et Authentification

2.1 Généralités :

La cryptographie est un champ de la cryptologie dont l'objectif est de garantir la confidentialité des communications et des données. Elle repose sur des techniques de chiffrement permettant de sécuriser l'échange d'informations, des mécanismes de signature assurant l'authenticité des messages, ainsi que des protocoles d'authentification garantissant l'identité des utilisateurs.

La cryptographie se divise en deux catégories, la cryptographie symétrique et asymétrique.

2.1.1 Cryptographie symétrique

La cryptographie symétrique repose sur l'utilisation d'une seule clé secrète partagée (dans certain cas deux clés, dont l'une peut être facilement déduite de l'autre) entre les parties communicantes. Cette clé est utilisée aussi bien pour chiffrer que pour déchiffrer les messages, ce qui garantit la confidentialité des échanges.

2.1.2 Cryptographie asymétrique

La cryptographie asymétrique repose quant à elle sur l'utilisation d'un couple de clés : une clé publique, accessible à tous, et une clé privée, connue uniquement par une des parties. Cette approche permet de résoudre le problème de distribution des clés. Cependant, elle demande plus de ressources (temps de calcul).

2.1.3 Échange de clé

Le problème principal de la cryptographie symétrique réside dans la gestion et la distribution sécurisée de la clé secrète. La meilleure solution consiste à utiliser un protocole d'échange de clé sécurisé tel que Diffie-Hellman. Avant la découverte de tels protocoles, tous les échanges de clés devaient s'effectuer de manière physique. C'était notamment la méthode utilisée pour sécuriser les échanges directs entre les Etats-Unis et l'Union soviétique durant la guerre froide. L'échange physique de clé sur de si longue distance soulevait alors de nombreux problème de sécurité.

3 Diffie-Hellman

Dans le but d'échanger de manière sécurisée via un système reposant sur la cryptographie symétrique, deux agents doivent s'accorder sur le choix d'une clé de chiffrement. Pour de nombreuses raisons pratiques, on souhaite pouvoir échanger cette clé de chiffrement à distance : risque d'interception physique de la clé, multiplication des intermédiaires, ressources pour organiser un transport sécurisé.
L'objectif du protocole Diffie-Hellman est d'effectuer cet échange de clé sur un canal non nécessairement sécurisé, c'est-à-dire qu'un attaquant peut accéder aux données échangées sans pour autant en déduire la clé commune choisie par les deux agents.

3.1 Paramètres publics

Les deux agents (appelées traditionnellement Alice et Bob) s'accordent sur :

- Un grand nombre premier $p \in \mathbb{P}$.
- Un élément g, qui est, pour la version classique de Diffie-Hellman, un élément de $\mathbb{Z}/p\mathbb{Z}$.

Ces données sont communiquées sur un canal qui n'est a priori pas sécurisé. On considère que tout attaquant y a accès

3.2 Génération des clés

Les deux parties, Alice et Bob, choisissent les entiers $1 \leq a, b \leq p$, puis communiquent uniquement les valeurs $A = g^a \bmod p$ et $B = g^b \bmod p$. Alice et Bob sont alors en capacité de calculer la clé commune :

$$K = B^a \mod p = A^b \mod p = g^{ab} \mod p$$

Dans la suite, on désignera l'attaquant, par le nom Charlie. Les valeurs auxquelles Charlie a accès sont les suivantes : p, $g^a \bmod p$, $g^b \bmod p$ et g.

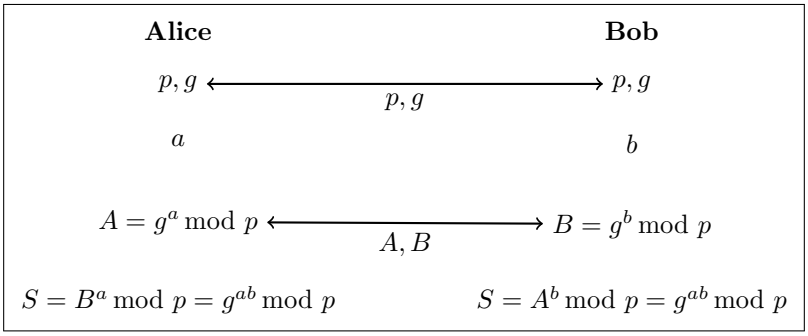


FIGURE 1 – Échange de clé Diffie-Hellman

3.3 Sécurité du protocole

Le protocole Diffie-Hellman repose sur le problème du même nom, qui est en pratique difficile à résoudre dans des corps finis.

Définition : (Problème Diffie-Hellman)
Soit $(G, \cdot)$ un groupe cyclique, g un générateur de G. En ayant connaissance de $A = g^a \mod p$ et $B = g^b \mod p$, déterminer $g^{ab} \mod p$.

Bien qu'on ne dispose pas de résultat théorique sur la difficulté informatique de ce problème, la seule façon connue de résoudre ce problème est de résoudre le problème du logarithme discret.

Définition : (Problème du logarithme discret)
Soit $(G, \cdot)$ un groupe cyclique, g un générateur de G et $h \in G$ quelconque. Trouver un entier k tel que $g^k = h$. Cet entier k est noté $\log_g(h)$.

3.4 Attaque Man in the Middle

L'attaque Man in the Middle sur le protocole de Diffie-Hellman exploite l'absence d'authentification lors de l'échange des clés publiques de la version rudimentaire de DH. Charlie peut intercepter les messages envoyés à Bob par Alice, récupérer g^a, choisir $1 \leq \tilde{c} \leq p$, puis envoyer $g^{\tilde{c}}$ à Bob, qui pense alors communiquer directement avec Alice.
De même, il intercepte la réponse de Bob, g^b, choisi $1 \leq c \leq p$, puis envoie g^c à Alice.
Ainsi, il crée deux clés $S_A = g^{ca}$ et $S_B = g^{b\tilde{c}}$ qui lui permettent de lire et modifier les échanges entre Alice et Bob sans être remarqué.

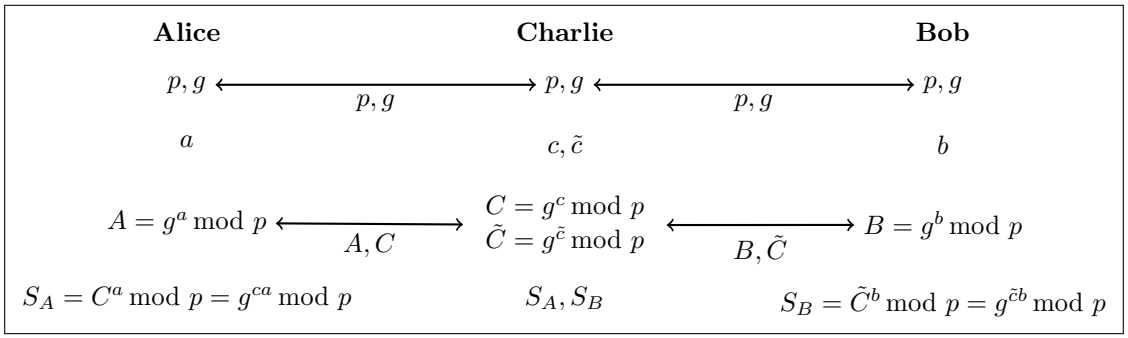


FIGURE 2 – Attaque Man in the Middle sur l'échange de clé Diffie-Hellman

3.5 Attaque brute force

Algorithme 1 : Attaque brute force (Diffie-Hellman)

Input : $p \in \mathbb{P}$, $A, B \in [\![1, p-1]\!]$, $g \in p$
Output : La clé secrète A^b ou B^a
$r \leftarrow g$
pour $k \in [\![1, p-1]\!]$ **faire**
  si $r = A$ **alors**
    retourner $B^k \mod p$
  fin
  si $r = B$ **alors**
    retourner $A^k \mod p$
  fin
  $r \leftarrow (r \times g) \bmod p$
fin

L'algorithme 1 vérifie pour tout $k \in [\![1, p-1]\!]$ si k est le logarithme discret de A ou de B en base g. Il détermine ainsi la clé secrète de Alice ou Bob respectivement. L'algorithme fait donc en moyenne $O(p)$, soit $O(p^3)$ opération avec la méthode naive (voire $O(p^{2,585})$ en effectuant des multiplication par l'algorithme de Karatsuba par exemple).

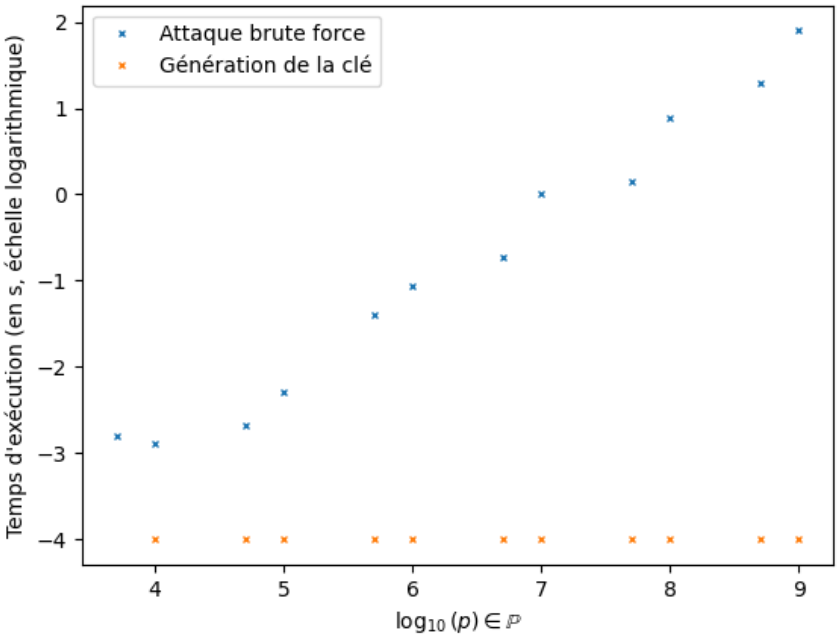


FIGURE 3 – Temps d'éxecution moyen de l'algorithme 1 (sur 1000 échantillons (a, b, g) aléatoires)

En pratique, pour s'assurer que le protocole Diffie-Hellman soit résistant à une attaque brute force, il faut choisir un entier p premier très grand, supérieur à 2^{10} bits, soit une écriture décimale de 600 chiffres environ.

En effectuant une simulation d'attaque pour quelques nombres premiers dans $[\![10^4, 10^9]\!]$ (figure 3), on s'apperçoit que si le temps d'exécution poursuit sa tendance pour les grands nombres premiers - de l'ordre de 10^{600} - le temps de calcul d'une méthode naïve avoisinerait les 10^{500} secondes. Ce qui est innateignable en pratique, même en disposant d'une machine ayant une grande puissance de calcul.

Bien qu'importante pour garantir la sécurité du protocole, la taille de l'entier p pose plusieurs problème : il faut générer un grand nombre premier, de plus, il faut des clés de grandes taille. On peut diminuer la quantité de calcul à effectuer en changeant le groupe dans lequel on applique Diffie-Hellman. Le choix le plus courant est celui des groupes sur les courbes elliptiques.

4 Courbes elliptiques

Le protocole Diffie-Hellman, bien qu'initialement formulé pour le groupe $\mathbb{Z}/p\mathbb{Z}$ peut être appliqué dans d'autre groupe. Il faut toutefois s'assurer que le problème du logarithme discret dans ces groupes reste difficile à résoudre en pratique. Nous introduisons dans cette section le concept de courbes elliptiques, qui sont utilisées pour générer des groupes finis dans lesquels la génération des clés est plus rapide tout en conservant le même niveau de sécurité.

Dans toute cette section, K désigne un corps quelconque.

4.1 Variétés algébriques

4.1.1 Cadre général

Définition : (Ensemble algébrique)
Soit $(P_i)_{i\in I} \in K[X_1, ..., X_n]$, alors, on définit l'ensemble algébrique de I par :

$$V((P_i)_{i\in I}) := \{(x_1, \cdots, x_n) \in K^n \mid \forall\, i \in I, P_i(x_1, \cdots, x_n) = 0\}$$

Définition : (Idéal d'un ensemble algébrique)
Si V est un ensemble algébrique, on note :

$$I(V) := \{P \in K[X_1, ..., X_n] \mid \forall\, (x_1, \cdots, x_n) \in V, P(x_1, \cdots, x_n) = 0\}\,.$$

Définition : (Variété algébrique)
Une variété algébrique est un ensemble algébrique V dont l'idéal $I(V)$ est premier dans $K[X_1, \cdots, X_n]$. C'est-à-dire :

$$\forall\, P, Q \in K[X_1, \cdots, X_n], (PQ \in I(V)) \Longrightarrow (P \in I(V) \text{ ou } Q \in I(V))$$

4.1.2 Cadre des courbes elliptiques

Dans le cadre des équations de Weierstrass, nous étudierons uniquement des ensembles algébriques engendrés par un unique polynôme $P \in K[X, Y]$ (Après changement de variable dans une équation de Weirstrass sous la forme (1)). On définit alors naturellement la courbe associée à un tel ensemble algébrique.

Définition : (Courbe plane affine)
Soit $P \in K[X_1, \cdots, X_n]$, on appelle courbe plane affine sur K associée à P et on note C_P l'ensemble algébrique :

$$C_P := V(P)$$

Pour une courbe elliptique $P \in K[X, Y, Z]$.

Définition : (Point singulier)
Dans le cadre d'une variété algébrique définie par un unique polynôme $P \in K[X_1, \cdots, X_n]$, on dit que $(x_1, \cdots, x_n) \in K^n$ est singulier si :

$$\frac{\partial P}{\partial X_1}(x_1, \cdots, x_n) = \cdots = \frac{\partial P}{\partial X_n}(x_1, \cdots, x_n) = 0$$

Si un point est non singulier, il est lisse

Pour garantir la structure de groupe abélien sur les courbes elliptiques dans la suite, il faut vérifier que la variété algébrique est lisse, ou non singulière.

Définition : (Variété lisse/non singulière)
Une variété algébrique est dite lisse, ou non singulière si elle n'admet aucun point singulier.

4.2 Espace projectif

Définition : (Espace projectif)
On appelle espace projectif de dimension n, et on note $\mathbb{P}^n$ l'ensemble :

$$\mathbb{P}^n = \left(K^{n+1}\right)^* / \sim .$$

Où $\sim$ est la relation d'équivalence définie par, pour tout $(x_0, \cdots, x_n), (y_0, \cdots, y_n) \in \left(K^{n+1}\right)^*$:

$$(x_0, \cdots, x_n) \sim (y_0, \cdots, y_n) \iff \exists\, \lambda \in K^*, \forall\, i \in [\![0, n]\!], x_i = \lambda y_i.$$

Définition : (Point fini, à l'infini)
Soit $u = (x_0, \ldots, x_n) \in K^{n+1}$,

- Si $x_n \neq 0$, il existe un représentant de u de la forme $[\frac{x_0}{x_n} : \ldots : \frac{x_{n-1}}{x_n} : 1]$. On dit que c'est un point fini de l'espace projectif.
- Si $x_n = 0$, il existe un représentant de u de la forme $[x_0 : \ldots : x_{n-1} : 0]$. On dit que c'est un point à l'infini de l'espace projectif. Ces points forment un hyperplan de $\mathbb{P}^n$.

Dans la suite, on se contente d'introduire les différents outils dans $\mathbb{P}^2$ qui sera notre cadre d'étude. Ces définitions sont cependant toujours valables pour $\mathbb{P}^n$.

Définition : (Droite projective dans $\mathbb{P}^2$)
Une droite de $\mathbb{P}^2$ d'équation $ux + vy + wz = 0$ avec $u, v, w \in \overline{K}$ non tous nuls est l'ensemble :

$$\left\{[x : y : z] \in \mathbb{P}^2 \;\middle|\; ux + vy + wz = 0\right\}$$

.

Propriété 4.2.1 :
Soient $P = [x_P : y_P : z_P]$ et $Q = [x_Q : y_Q : y_Q]$ deux points distincts de $\mathbb{P}^2$. Il existe une unique droite de $\mathbb{P}^2$ passant par P et Q. C'est l'ensemble

$$D = \left\{ [x : y : z] \in \mathbb{P}^2 \;\middle|\; \det \begin{pmatrix} x_P & x_Q & x \\ y_P & y_Q & y \\ z_P & z_Q & z \end{pmatrix} = 0 \right\}.$$

Autrement dit, c'est la droite d'équation $ux+vy+wz = 0$, avec $u = y_P z_Q - z_P y_Q$, $v = z_P x_Q - x_P z_Q$, $w = x_P y_Q - y_P x_Q$.

Démonstration :
$(u, v, w) \neq (0, 0, 0)$ car P et Q sont distincts, c'est donc une équation de droite et elle contient P et Q par définition du déterminant.
Soit D' une droite d'équation $u'x + v'y + w'z = 0$ contenant P et Q. En notant pour $(x, y, z) \in \overline{K}^3$ $f(x, y, z) = ux + vy + wz$ et $g(x, y, z) = u'x + v'y + w'z$, f et g sont des formes linéaires. Comme P et Q sont distincts, $\mathrm{Vect}((a_1, a_2, a_3), (b_1, b_2, b_3))$ est de dimension 2. Donc $\mathrm{Ker}(f) = D = \mathrm{Ker}(g) = D'$. De plus, f et g sont alors proportionnelles donc $[u : v : w] = [u' : v' : w']$.

□

Définition : (Tangente à un point lisse d'une courbe)
Soit E une courbe plane affine de polynôme $F \in K[X,Y,Z]$ et P un point lisse de la courbe, la tangente à E en $P \in E$ est la droite d'équation :

$$\frac{\partial F}{\partial X}(P)x + \frac{\partial F}{\partial Y}(P)y + \frac{\partial F}{\partial Z}(P)z = 0.$$

Remarque : Le fait que P soit lisse assure la bonne définition de la droite (coefficients non tous nuls).

4.3 Équations de Weierstrass

Définition : (Équations de Weierstrass)
On appelle équation de Weierstrass une équation de la forme :

$$Y^2Z + a_1XYZ + a_3YZ^2 = X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3. \tag{1}$$

On note $F(X,Y,Z) = Y^2Z + a_1XYZ + a_3YZ^2 - (X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3)$ le polynôme associé.

Propriété 4.3.1 :
Une courbe de Weierstrass a un seul point à l'infini. C'est le point $[0:1:0]$. Il est lisse (non singulier) et la tangente à la courbe en ce point a pour équation $z = 0$.

Démonstration : En effet, on a $F(X,Y,0) = 0 \iff X^3 = 0 \iff X = 0$, donc dans $\mathbb{P}^2$, la droite d'équation $z = 0$ et la courbe d'équation $F(X,Y,Z) = 0$ se coupent au seul point :

$$P_\infty = [0:Y:0] = [0:1:0].$$

Et, $\frac{\partial F}{\partial Z}(P_\infty) = 1$ donc P_∞ est un point lisse. De plus :

$$\frac{\partial F}{\partial X}(P_\infty) = 0 \quad \text{et} \quad \frac{\partial F}{\partial Y}(P_\infty) = 0.$$

Ainsi, la tangente à la courbe au point P_∞ a pour équation $z = 0$.

□

Propriété 4.3.2 :
Pour un corps K de caractéristique différente de 2 ou 3, on peut se ramener à une équation de la forme :

$$y^2 = x^3 + ax + b \tag{2}$$

pour les points finis de $\mathbb{P}^2$: (les $[x,y,1] \in \mathbb{P}^2$) ou bien en toute généralité :

$$y^2z = x^3 + axz^2 + bz^3 \tag{3}$$

Démonstration :
En annexe : 8.2

□

Dans toute la suite, on suppose la caractéristique de K différente de 2 et 3.
Notation : Pour une équation de Weierstrass sous la forme (2), on notera Δ et j les quantités suivantes :

$$\Delta := -16(4a^3 + 27b^2) \quad \text{et} \quad j := -1728\frac{(4a)^3}{\Delta} \quad \text{lorsque } \Delta \neq 0$$

On peut remarquer que Δ est 16 fois le discriminant de l'équation $x^3 + ax + b$. On posera aussi :

$$P_W(X,Y) = Y^2 - X^3 - aX - b$$

Ainsi, $\mathcal{C}_{P_W}$ désignera dans la suite l'ensemble algébrique défini par l'équation de Weierstrass (2).

Remarque : On sait qu'un point singulier $(x_0, y_0) \in \mathcal{C}_{P_W}$ vérifie :

$$\frac{\partial P_W}{\partial X}(x_0, y_0) = \frac{\partial P_W}{\partial Y}(x_0, y_0) = 0$$

En particulier, on peut effectuer un développement de Taylor (pour les polynômes) en (x_0, y_0), il existe pour tout $(x, y) \in \mathcal{C}_{P_W}$:

$$P_W(x, y) - P_W(x_0, y_0) = ((y - y_0) - \alpha(x - x_0))((y - y_0) - \beta(x - x_0)) - (x - x_0)^3 \tag{4}$$

Définition : (Nœud, point de rebroussement)
Soit (x, y) un point singulier de $\mathcal{C}_{P_W}$, avec les notations de (4), on dit que :

- (x, y) est un noeud si $\alpha \neq \beta$,
- (x, y) est un point de rebroussement si $\alpha = \beta$.

Propriété 4.3.3 :

- $\mathcal{C}_{P_W}$ est lisse $\iff \Delta \neq 0$
- $\mathcal{C}_{P_W}$ admet un nœud $\iff \Delta = 0$ et $a \neq 0$
- $\mathcal{C}_{P_W}$ admet un point de rebroussement $\iff \Delta = 0$ et $a = 0$

Démonstration : On ne montre que la première équivalence.

Si $\mathcal{C}_{P_W}$ n'est pas lisse, comme l'unique point à l'infini de $\mathcal{C}_{P_W}$ est lisse (propriété 4.3.1), il existe $M = [x_M : y_M : 1]$ un point fini singulier de $\mathcal{C}_{P_W}$. Ainsi :

$$\frac{\partial P_W}{\partial X}(M) = -3{x_M}^2 - a = 0 \quad \text{et} \quad \frac{\partial P_W}{\partial Y}(M) = 2y_M = 0.$$

Comme car(K) est différente de 2 et 3, ${y_M}^2 = {x_M}^3 + ax_M + b = 0$. Donc, x_m est racine de $X^3 + aX + b$ et de sa dérivée $3X^2 + a$, c'est une racine multiple de $X^3 + aX + b$.

Or, d'après les formules de Cardan dans un corps commutatif de caractéristique différente de 2 et 3, le discriminant de $X^3 + aX + b$ est nul, donc $\Delta = 0$.

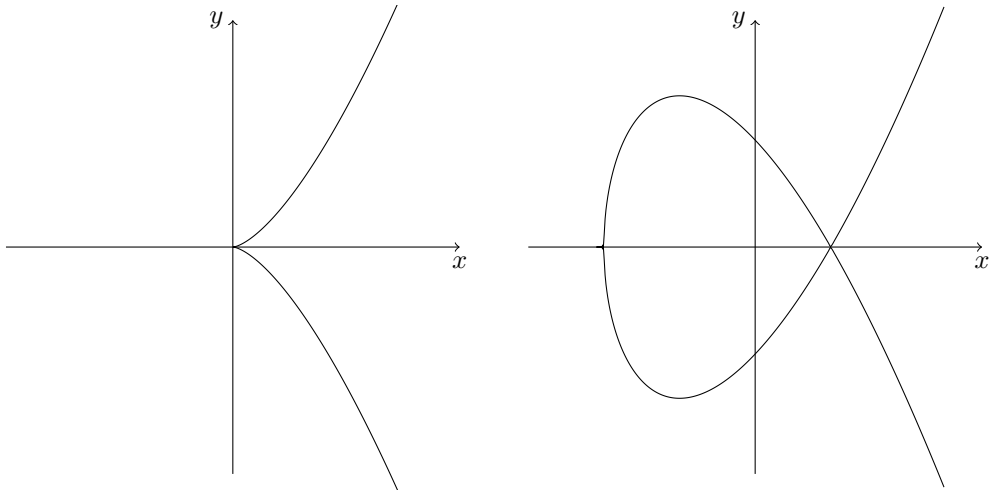
Réciproquement, si $\Delta = 0$, il existe $x_M \in K$ une racine multiple de $X^3 + aX + b$ d'après les formules de Cardan dans K. On note $y_M = 0 = {y_M}^2 = {x_M}^3 + ax_M + b \in K$. Donc $M = [x_M : y_M : 1] \in E$.

Et

$$\frac{\partial P_W}{\partial X}(M) = -3{x_M}^2 - a = 0 \quad \text{et} \quad \frac{\partial P_W}{\partial Y}(M) = 2y_M = 0.$$

Donc, $\mathcal{C}_{P_W}$ n'est pas lisse.

□



Point de rebroussement ($y^2 = x^3$). Noeud ($y^2 = x^3 - 3x + 2$).

FIGURE 4 – Courbes possédant des points singuliers

4.4 Courbe elliptique et structure de groupe

Définition : (Courbe elliptique)
Une courbe elliptique sur K est un couple $(E, \mathcal{O})$ où :

- E est une courbe plane affine lisse associée à un polynôme de $K[X, Y, Z]$.
- $\mathcal{O}$ désigne l'origine.

On se donne dans cette section $(E, \mathcal{O})$ une courbe elliptique vérifiant une équation de Weierstrass sous la forme (1), c'est-à-dire, sous la forme $E = V(Y^2Z + a_1XYZ + a_3YZ^2 - (X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3)) \subset \mathbb{P}^2$. Dans ce cadre, $\mathcal{O}$ est l'unique point à l'infini dans E.

Remarque : Pour E une courbe elliptique d'équation $y^2 = x^3 + ax + b$, l'équation de la tangente à E au point $P = (x_P, y_P) \in E$ est donnée par : $y = \frac{3x_P^2 + a}{2y_P}(x - x_P) + y_P$ si $y_P \neq 0$, $x = x_P$ sinon.

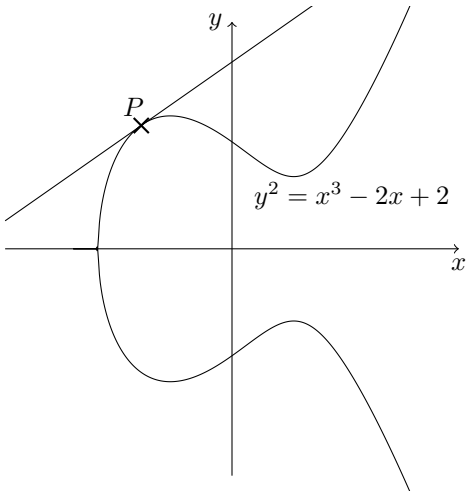


FIGURE 5 – Tangente au point $P = (-1.2, 1.63)$

4.5 Loi de groupe

Théorème 4.5.1 :
Soient P et Q des points de E. Soit D la droite de $\mathbb{P}^2$ passant par P et Q si $P \neq Q$, ou bien la tangente à E en P si $P = Q$. On a :

$$D \cap E = \{P, Q, f(P,Q)\}$$

où $f(P,Q)$ désigne le point de E défini par les conditions suivantes :

- 1. Supposons $P \neq Q$, $P \neq \mathcal{O}$ et $Q \neq \mathcal{O}$.
  - 1.1) Supposons $x_P \neq x_Q$. Posons

$$\lambda = \frac{y_P - y_Q}{x_P - x_Q} \quad \text{et} \quad \nu = \frac{x_P y_Q - x_Q y_P}{x_P - x_Q}.$$

    On a

$$f(P,Q) = \left[\lambda^2 - x_P - x_Q : \lambda(\lambda^2 - x_P - x_Q) + \nu : 1\right]. \tag{5}$$

  - 1.2) Si $x_P = x_Q$, on a $f(P,Q) = \mathcal{O}$.
- 2) Supposons $P \neq \mathcal{O}$ et $Q = \mathcal{O}$.

$$f(P,\mathcal{O}) = [x_P : -y_P : 1]. \tag{6}$$

  De même, si $P = \mathcal{O}$ et $Q \neq \mathcal{O}$, on a $f(\mathcal{O},Q) = [x_Q, -y_Q, 1]$.
- 3) Si $P = Q = \mathcal{O}$, on a $f(\mathcal{O},\mathcal{O}) = \mathcal{O}$.
- 4) Supposons $P = Q$ et $P \neq \mathcal{O}$.
  - 4.1) Si $y_P = 0$, on a $f(P,P) = \mathcal{O}$.
  - 4.2) Supposons $y_P \neq 0$. Posons

$$\lambda = \frac{3x_P^2 + a}{2y_P} \quad \text{et} \quad \nu = \frac{-x_P^3 + ax_P + 2b}{2y_P}.$$

    On a

$$f(P,P) = [\lambda^2 - 2x_P : \lambda(\lambda^2 - 2x_P) + \nu : 1].$$

Démonstration :

- – 1.1) Supposons $x_P \neq x_Q$.
  L'équation de D est celle de la droite entre deux points distincts (propriété 4.2.1). Ici : $(y_P - y_Q)x + (x_Q - x_P)y + (x_P y_Q - y_P x_Q) = 0$ ce qui donne $y = \lambda x + \nu$.
  Soit M un point de $D \cap E$. Puisque $\mathcal{O}$ n'est pas sur D, $M = [x_M : y_M : 1]$ avec $x_M, y_M \in K$.
  On a donc :

$$y_M^2 = x_M^3 + ax_M + b \quad \text{et} \quad y_M = \lambda x_M + \nu.$$

  Ainsi, x_M est une racine du polynôme :

$$\begin{aligned} H &= X^3 - \lambda X^2 + (a - 2\nu)X + b - \nu^2. \\ H &= (X - x_P)(X - x_Q)(X - (\lambda^2 - x_P - x_Q)) \end{aligned}$$

  Réciproquement, $f(P,Q)$ est un point de $D \cap E$. Ainsi $D \cap E = \{P, Q, f(P,Q)\}$.
  – 1.2) Supposons $x_P = x_Q$.
  On a alors ${y_P}^2 = {y_Q}^2$ et puisque P et Q sont distincts, $y_P = -y_Q \neq 0$. L'équation de D est donc $2y_P x - 2y_P x_P = 0$, ce qui donne $x = x_P$.
  Donc, $\mathcal{O} \in D \cap E$.
  Réciproquement, si $M = [x_M : y_M : 1] \in (D \cap E) \setminus \{\mathcal{O}\}$, alors $x_M = x_P$ et donc $y_M^2 = y_P$.
  On a donc $M = P$ ou $M = Q$. On en déduit que $D \cap E = \{P, \mathcal{O}, Q\}$.

- 2) Supposons $P \neq O$.

  La droite D passant par P et $\mathcal{O}$ a pour équation $-x + x_P = 0$, ce qui donne $x = x_P$ Si $M = [x_M, y_M, 1]$ est un point fini de$D \cap E$, on a $x_0 = x_P$ d'où $y_0 = y_P$ ou $y_0 = -y_P$. Réciproquement, $[x_P, -y_P, 1] \in D \cap E$. On a ainsi $D \cap E = \{P, \mathcal{O}, f(P, \mathcal{O})\}$.

- 3) La tangente à E en $\mathcal{O}$ a pour équation $z = 0$. Ainsi, $\mathcal{O}$ est le seul point de $D \cap E$, d'où $f(\mathcal{O}, \mathcal{O}) = \mathcal{O}$.

- 4) Supposons $P = Q$ et $P \neq \mathcal{O}$. L'équation de la tangente D à E en P a donc pour équation $\frac{\partial F}{\partial X}(P)x + \frac{\partial F}{\partial Y}(P)y + \frac{\partial F}{\partial Z}(P)z = 0$.

  Or,

$$\frac{\partial F}{\partial X}(P) = -3{x_P}^2 \quad \text{et} \quad \frac{\partial F}{\partial Y}(P) = 2y_P \quad \text{et} \quad \frac{\partial F}{\partial Z}(P) = {y_P}^2 - 2ax_P + 3b$$

  Ainsi,

$$\begin{array}{rcl} \frac{\partial F}{\partial X}(P)(x - x_P z) + \frac{\partial F}{\partial Y}(P)(y - y_P z) & = & \frac{\partial F}{\partial X}(P)x + 3{x_p}^3 z + \frac{\partial F}{\partial Y}(P)y - 2{y_P}^2 z \\ & = & \frac{\partial F}{\partial X}(P)x + \frac{\partial F}{\partial Y}(P)y + \frac{\partial F}{\partial Z}(P)z \end{array}$$

  car ${y_P}^2 = {x_P}^3 + ax_P + b$

  - 4.1) Si $y_P = 0$, alors $\frac{\partial F}{\partial Y}(P) = 0$.
    Donc, on a comme équation $-3{x_P}^2(x - x_P z) = 0$, avec $x_P \neq 0$ car la courbe est lisse.
    On obtient donc $D \cap E = \{P, \mathcal{O}\}$
  - 4.2) Si $y_P \neq 0$, alors $\mathcal{O}$ n'appartient pas à la tangente D.

$$\frac{\partial F}{\partial X}(P)x + \frac{\partial F}{\partial Y}(P)y + \frac{\partial F}{\partial Z}(P)z = -3{x_P}^2 x + 2y_P y + ({y_P}^2 - 2ax_P + b)z$$

    L'équation de D (sur les points finis car $\mathcal{O} \notin D$ est donc est donc : $y = \lambda x + \nu$. Et, si $M = [x_M : y_M : 1] \in (D \cap E) \setminus \{\mathcal{O}\}$, On a donc :

$$y_M^2 = x_M^3 + ax_M + b \quad \text{et} \quad y_M = \lambda x_M + \nu.$$

    Ainsi, x_M est une racine du polynôme :

$$\begin{array}{rcl} H & = & X^3 - \lambda X^2 + (a - 2\nu)X + b - \nu^2. \\ H & = & (X - x_P)^2(X - (\lambda^2 - 2x_P)) \end{array}$$

    Réciproquement, $f(P, Q)$ est un point de $D \cap E$. Ainsi $D \cap E = \{P, Q, f(P, Q)\}$.

□

Remarque : Il y a au plus 3 points d'une courbe elliptique alignés sur une même droite, il y en a exactement 3 en comptant les multiplicités.
Cette propriété justifie la définition suivante :

Définition : (Somme sur les courbes elliptiques)
Soit $P, Q \in E$, on note $P \oplus Q = f(f(P, Q), \mathcal{O})$. Si $f(P, Q) \neq \mathcal{O}$, $P \oplus Q$ est le symétrique de $f(P, Q)$ par rapport à l'axe des abscisses.

Théorème 4.5.2 : Soit $(E, \mathcal{O})$ une courbe elliptique. La loi $\oplus$ munit E d'une structure de groupe commutatif d'élément neutre $\mathcal{O}$ tel pour tout P, Q et $R \in E$ alignés, $(P \oplus Q) \oplus R = \mathcal{O}$.

Démonstration : On admet l'associativité. Pour $P, Q \in E$,

$$f(P, Q) = f(Q, P) \quad \text{donc} \quad P \oplus Q = Q \oplus P$$

Et,

$$P \oplus \mathcal{O} = f(f(P, \mathcal{O}), \mathcal{O}) = P \quad \text{et} \quad P \oplus f(P, \mathcal{O}) = \mathcal{O}$$

Enfin,

$$(P \oplus Q) \oplus f(P, Q) = P \oplus Q \oplus f(P, Q) = f(f(P, Q), \mathcal{O}) \oplus f(P, Q) = \mathcal{O}$$

D'où le résultat.

□

Propriété 4.5.1 :
Soit $P, Q \in (E, \mathcal{O})$, avec E d'équation $y^2 = x^3 + ax + b$, $P = (x_P, y_P), Q = (x_Q, y_Q)$, alors, en notant :

$$\begin{cases} s = \frac{y_P - y_Q}{x_P - x_Q} & \text{si } x_P \neq x_Q \text{ et } y_P \neq y_Q \\ s = \frac{3x_P^2 + a}{2y_P} & \text{si } x_P = x_Q \neq 0 \text{ et } y_P = y_Q \end{cases}$$

Les coordonnées de $R = P \oplus Q$ sont données par :

$$\begin{cases} x_R = s^2 - (x_P + x_Q) \\ y_R = s(x_P - x_R) - y_P \end{cases}$$

Enfin, si $y_P \neq y_Q$ et $x_P \neq x_Q$, on a $R = \mathcal{O}$

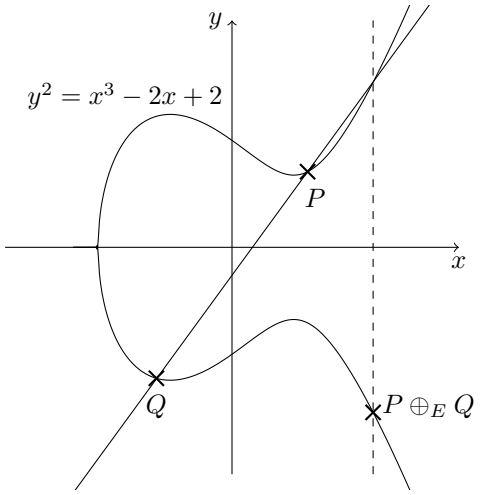


FIGURE 6 – Représentation géométrique de la somme de $P = (1, 1)$ et $Q = (-1, -1.732) \in E$

Nous souhaitons à présent définir le protocole d'échange de clé ECDH. Travaillant sur machine, nous ne pouvons pas considérer des courbes elliptiques sur $\mathbb{R}$. Cependant, travailler dans un corps fini, par exemple $\mathbb{Z}/p\mathbb{Z}$, comme on le fait souvent en cryptographie, permet de contourner ce problème : le nombre de points sur la courbe est fini, leurs coordonées sont bornées (et la borne ne dépend pas de la courbe), de plus les calculs sont exacts.

5 Elliptic-Curve-Diffie-Hellman

5.1 Motivation

L'utilisation des courbes elliptiques permet de réduire la taille des clés tout en conservant le même niveau de sécurité. La réduction de la taille des clés permet de faciliter les calculs, rendant ainsi le processus plus rapide, et moins coûteux en CPU.

5.2 Principe du protocole

Dans la suite, p est un nombre premier différent de 2 et 3. $\mathbb{Z}/p\mathbb{Z}$ est alors un corps de caractéristique p, différente de 2 et 3.

Définition : (Ensemble $E(\mathbb{Z}/p\mathbb{Z})$)
Soit $(E, \mathcal{O})$ une courbe elliptique d'équation $y^2 = x^3 + ax + b$. On définit l'ensemble $E(\mathbb{Z}/p\mathbb{Z})$ par :

$$E(\mathbb{Z}/p\mathbb{Z}) := \left\{(x, y) \in (\mathbb{Z}/p\mathbb{Z})^2 \;\middle|\; y^2 \equiv x^3 + ax + b \mod p\right\} \cup \{\mathcal{O}\}$$

On se donne une courbe elliptique $(E, \mathcal{O})$ définie sur un ensemble $\mathbb{Z}/p\mathbb{Z}$, avec $p \in \mathbb{P}$.

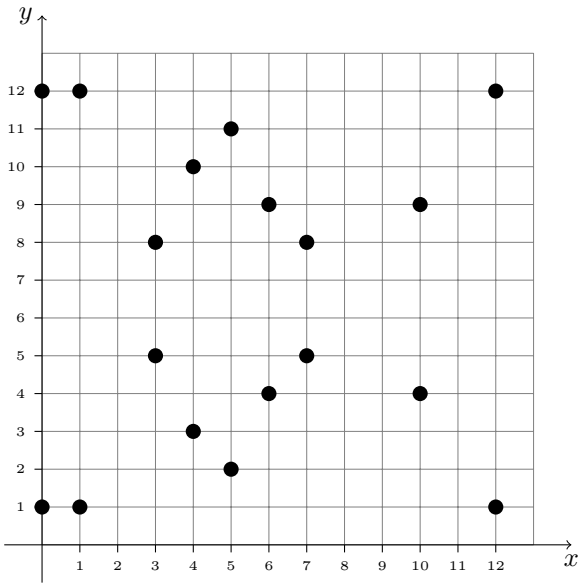


FIGURE 7 – Courbe elliptique $y^2 = x^3 - x + 1$ dans $\mathbb{Z}/13\mathbb{Z}$

On se donne dans la suite G un générateur d'un sous-groupe de $\mathbb{Z}/p\mathbb{Z}$ pour la loi $\oplus_E$.
Pour que la loi $\oplus_E$ reste une loi de composition interne sur $E(\mathbb{Z}/p\mathbb{Z})$, il faut modifier légèrement la définition. Introduisons la notion d'inverse modulaire.

Définition : (Inverse modulaire)
Soit $p, q, n \in \mathbb{Z}^2 \times \mathbb{N}^*$. On dit que q est l'inverse modulaire de p modulo n, noté p^{-1} si :

$$pq \equiv 1 \mod n$$

Remarque : L'inverse modulaire de p modulo n existe si et seulement si $p \wedge n = 1$ d'après le théorème de Bézout. On peut alors obtenir facilement l'inverse modulaire via l'algorithme d'Euclide étendu (5.3.1). Enfin, l'inverse modulaire est bien unique car si $pq \equiv 1 \equiv pq' \mod n$, comme $p \wedge n = 1$, on a $q \equiv q' \mod n$.

Définition : (Somme dans $E(\mathbb{Z}/p\mathbb{Z})$)
Soit $P = (x_P, y_P)$, $Q = (x_Q, y_Q) \in E(\mathbb{Z}/p\mathbb{Z})$, avec E d'équation $y^2 = x^3 + ax + b$.

- On a $\mathcal{O} \oplus_E \mathcal{O} = \mathcal{O}$ et $P \oplus_E \mathcal{O} = P$.
- Si $x_P = x_Q$ et $y_P \neq y_Q$, $P \oplus_E Q = \mathcal{O}$
- Si $x_P = x_Q$ et $y_P = y_Q = 0$, $P \oplus_E Q = \mathcal{O}$
- Si $x_P = x_Q$ et $y_P = y_Q \neq 0$, alors on note :

$$s = (3x_P^2 + a) \times (2y_p)^{-1}$$

- Si $x_P \neq x_Q$, alors on note :

$$s = (y_P - y_Q) \times (x_P - x_Q)^{-1}$$

Et enfin $P \oplus_E Q = R$ avec :

$$\begin{cases} x_R = s^2 - (x_P + x_Q) \mod p \\ y_R = s(x_P - x_R) - y_P \mod p \end{cases}$$

(Ici $^{-1}$ désigne l'inverse modulo p)

On peut toujours représenter la somme de deux points sur $E(\mathbb{Z}/p\mathbb{Z})$ de manière géométrique.

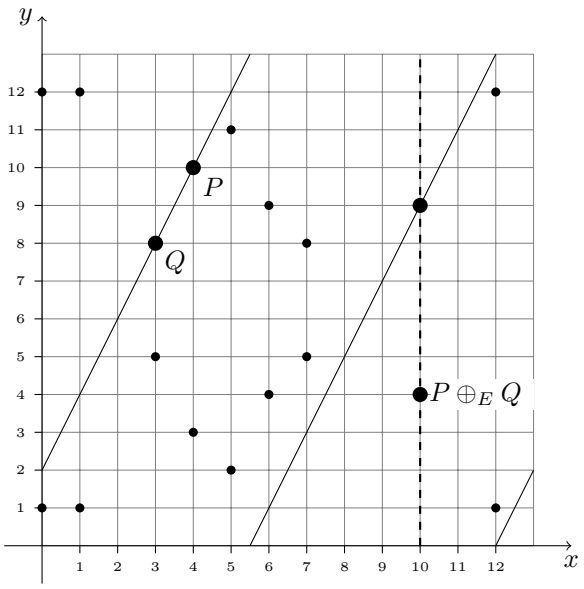


FIGURE 8 – Représentation géométrique de la somme $(4, 10) \oplus_E (3, 8)$ sur la courbe de fig. 6

Le protocole ECDH fonctionne de la même manière que DH, seul le groupe change, c'est désormais un groupe pour la somme (loi $\oplus_E$).

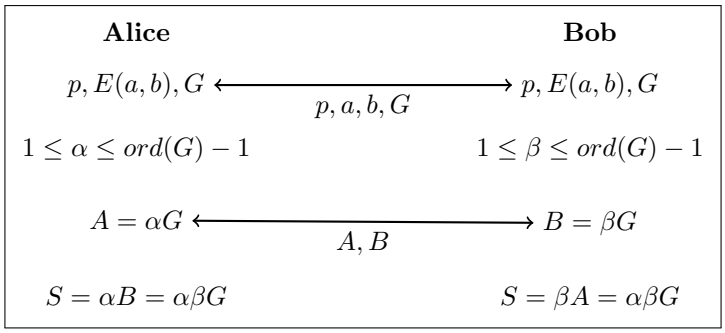


FIGURE 9 – Échange de clé Diffie-Hellman

5.3 Implémentation

5.3.1 Algorithme d'Euclide étendu pour le calcul de l'inverse modulaire

L'algorithme 1 est basé sur l'algorithme d'Euclide étendu et utilise la remontée des coefficients de Bézout pour calculer l'inverse. Plus précisément, on applique l'algorithme d'Euclide étendu à $a = k$ et $b = p$, car connaitre u et v tel que : $ku + pv = pgcd(k, p) = 1$ fournit en particulier $u = k^{-1}$.

Algorithme 2 : Calcul de l'inverse modulaire

Input : $k \in \mathbb{Z}, p \in \mathbb{N}$ avec $p > 0$
Output : L'inverse modulaire $k^{-1} \mod p$ si celui-ci existe, sinon lève une erreur
$a \leftarrow k$, $b \leftarrow p$
$x_0 \leftarrow 1$, $x_1 \leftarrow 0$
tant que $b \neq 0$ **faire**
  $q \leftarrow \lfloor a/b \rfloor$
  $(a, b) \leftarrow (b, a \mod b)$
  $(x_0, x_1) \leftarrow (x_1, x_0 - q \times x_1)$
fin
si $a \neq 1$ **alors**
  lever erreur
fin
retourner $x_0 \mod p$

Propriété 5.3.1 :
L'algorithme d'Euclide étendu permet de déterminer l'inverse modulaire avec une complexité $O(\log_2(p))$

5.3.2 Algorithme double-and-add

La seule opération utilisée par le protocole ECDH est la multiplication d'un point $P \in E(\mathbb{Z}/p\mathbb{Z})$. On peut implémenter une méthode de calcul rapide de la multiplication scalaire sur les courbes elliptiques à l'aide de l'algorithme double-and-add. Son principe est le même que celui de l'exponentiation rapide, pour calculer $n \cdot P$, on remarque que :

$$n \cdot P = \begin{cases} \frac{n}{2} \cdot (2 \cdot P) & \text{si } n \mod 2 = 0 \\ \frac{n-1}{2} \cdot (2 \cdot P) \oplus_E P & \text{sinon.} \end{cases}$$

Algorithme 3 : Algorithme double-and-add

Input : $k \in \mathbb{N}, P \in E(\mathbb{Z}/p\mathbb{Z})$
Output : kP
si $k = 0$ **alors**
  retourner $\mathcal{O}$
fin
$R \leftarrow \mathcal{O}$
$P_0 = P$ **tant que** $k > 0$ **faire**
  si $k \mod 2 = 1$ **alors**
    $R \leftarrow R \oplus_E P_0$
  fin
  $P_0 \leftarrow P_0 \oplus_E P_0$
  $k \leftarrow \lfloor k/2 \rfloor$
fin
retourner R

.

Remarque : L'algorithme double-and-add utilise $\log_2(k)$ addition de P_0 à lui-même, de plus si on note $\omega(n)$ le nombre de 1 dans l'écriture en base 2 de n, on effectue $\omega(k)$ opération d'addition $R + P_0$. Finalement, l'algorithme à une complexité $O((\log_2(k) + w(k)) \times \log_2(\|P\|)) = O((\log_2(k) \log_2(\|P\|))$

En effet, le calcul d'une somme nécessite le calcul d'un inverse modulaire d'une expression dépendant des coordonnées de P.

5.4 Sécurité de ECDH

Le problème qui rend ECDH résistant aux attaques est le même que pour DH, en voici la formulation dans le cadre des courbes elliptiques :

Définition : (Problème du logarithme discret sur les courbes elliptiques)
Soient $P \in E(\mathbb{Z}/p\mathbb{Z})$ et $Q \in \langle P \rangle$. Trouver un entier k tel que $k \cdot Q = P$.

Ce problème est difficile à résoudre en pratique pour des grandes valeurs de $\text{Card}(\langle P \rangle)$. Ainsi, il est important de choisir correctement p et P pour garantir la sécurité du protocole ECDH.

On peut adapter l'algorithme 1 pour qu'il trouve la clé secrète de la manière illustrée ci-dessous.

Algorithme 4 : Attaque brute force (Elliptic-Curve-Diffie-Hellman)

Input : $p \in \mathbb{P}$, $A, B \in E(\mathbb{Z}/p\mathbb{Z})$, $G \in E(\mathbb{Z}/p\mathbb{Z})$
Output : La clé secrète αB ou βA
$R \leftarrow G$
pour $k \in Card(E(\mathbb{Z}/p\mathbb{Z})$ **faire**
  si $R = A$ **alors**
    retourner $k \cdot B$
  fin
  si $R = B$ **alors**
    retourner $k \cdot A$
  fin
  $R \leftarrow R \oplus_E G$;
fin

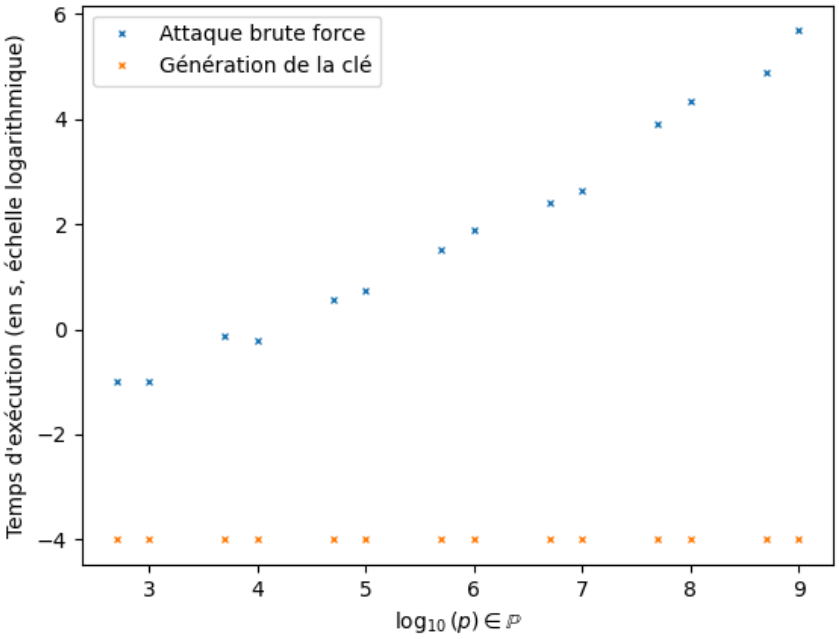


FIGURE 10 – Temps d'éxécution moyen de l'algorithme 4 (sur 100 échantillons (a, b, g) aléatoires).

On constate, à l'aide de la figure 10, que le temps de calcul pour la récupération de la clé (par la méthode brute force) est plus long pour le protocole ECDH que pour DH. Cela est notamment dû au calcul de l'inverse modulaire nécessaire à chaque addition de points sur la courbe elliptique.
Tout comme pour le protocole Diffie-Hellman, il faut s'assurer de bien choisir un nombre premier p ainsi qu'un générateur P, tels que l'ordre du groupe soit grand pour rendre difficile le problème du logarithme discret. Cependant, il ne suffit pas de prendre p grand a priori, car on ne connait pas à l'avance l'ordre de $E(\mathbb{Z}/p\mathbb{Z})$.

6 Choix du générateur

6.1 Isogénie

Définition : (Isogénie)
Soient $(E_1, \mathcal{O}_1), (E_2, \mathcal{O}_2)$ deux courbes elliptiques. On appelle isogénie un morphisme φ entre E_1, et E_2 vérifiant $\varphi(\mathcal{O}_1) = \mathcal{O}_2$.

Propriété 6.1.1 :
Si φ est un morphisme entre deux courbes C_1 et C_2, alors φ est constante ou surjective.

En particulier, toute isogénie φ vérifie :

$$\varphi(E_1) = \{\mathcal{O}_2\} \text{ ou } E_2.$$

Définition : ($\mathrm{Hom}(E_1, E_2)$)
On note $\mathrm{Hom}(E_1, E_2)$ l'ensemble des isogénies de E_1 vers E_2 et $\mathrm{End}(E) := \mathrm{Hom}(E, E)$.

Définition : ($[n]$)
Soit $n \in \mathbb{N}$, on note $[n]$ l'endomorphisme :

$$\begin{array}{rccl} [n] : & E & \longrightarrow & E \\ & P & \longrightarrow & n \cdot P \quad := \underbrace{P \oplus_E \cdots \oplus_E P}_{n \text{ fois}} \end{array}$$

6.2 Théorème de Hasse et choix de p

Plus le cardinal du sous-groupe engendré est élevée, meilleure est la sécurité du protocole. On cherche donc dans un premier temps à maximiser la quantité $\mathrm{Card}(E(\mathbb{Z}/p\mathbb{Z}))$. Or, nous disposons du théorème de Hasse qui nous fournit un encadrement de cette quantité. Nous démontrons ce théorème, et expliquons ces conséquences sur le choix de p.

Lemme 6.2.1 : (Inégalité de Cauchy-Schwartz)
Soit G un groupe. Soit $d : G \longrightarrow \mathbb{Z}$ une forme quadratique définie positive, alors, en notant :

$$\forall g, h \in G, \langle h, g \rangle_d := d(g + h) - d(g) - d(h).$$

On a :

$$\forall g, h \in G, |\langle h, g \rangle_d| \leq \sqrt{2d(h)d(g)}.$$

Démonstration : Puisque d est définie positive, on a, pour tout $g, h \in G$, pour tout :

$$0 \leq d(mg + nh) = m^2 d(g) + mn\langle g, h \rangle_d + n^2 d(h).$$

En prenant cette inégalité pour $m = -\langle g, h \rangle_d$ et $n = 2d(g)$ on trouve :

$$0 \leq \langle g, h \rangle_d^2 d(g) - 2d(g)\langle g, h \rangle_d^2 + 4d(g)2d(h) = d(g)(-\langle g, h \rangle_d^2 + 4d(g)d(h)).$$

D'où le résultat.

□

Théorème 6.2.1 : Soit $\varphi : E_1 \longrightarrow E_2$ une isogénie séparable. Alors :

$$\mathrm{Card}(\ker(\varphi)) = \deg(\varphi).$$

Remarque : Propriété admise (Voir [1], III.4.10c).

Définition : (Endomorphisme de Frobenius)
Soit $p \in \mathbb{P}$. On appelle endomorphisme de Frobenius l'endomorphisme :

$$\pi_p : \begin{array}{ccc} E & \longrightarrow & E^{(r)} \\ (x,y) & \longmapsto & (x^p, y^p) \end{array}$$

où $E^{(r)}$ désigne la courbe elliptique d'équation $x^3 = a^r x^2 + b^r$.

Propriété 6.2.1 :
L'endomorphisme de Frobenius π_p est de degré p et $[1] - \pi_p$ est séparable.

Remarque : Propriété admise (Voir [1], II.2.11).

Théorème 6.2.2 : (Hasse) Soit $p \in \mathbb{P}$, on a :

$$|\mathrm{Card}(E(\mathbb{Z}/p\mathbb{Z})) - (p+1)| \leq 2\sqrt{p}.$$

Démonstration : Tout d'abord, remarquons que :

$$\ker(\pi_p - [1]) = \{P \in E(\mathbb{Z}/p\mathbb{Z}) \mid \pi_p(P) = P\} = E(\mathbb{Z}/p\mathbb{Z}).$$

En effet, cela découle directement du petit théorème de Fermat. De plus, comme $[1] - \pi_p$ est séparable, on a :

$$\mathrm{Card}(\ker(\pi_p - [1])) = \mathrm{Card}(E(\mathbb{Z}/p\mathbb{Z})) = \deg(\pi_p - [1]).$$

Comme deg : $End(E) \longrightarrow \mathbb{Z}$ est une forme quadratique définie positive (Admis, [1] III.6.3), on peut lui appliquer l'inégalité de Cauchy-Schwartz :

$$\forall \psi, \varphi \in \mathrm{End}(E), |\deg(\varphi + \psi) - \deg(\varphi) - \deg(\psi)| \leq 2\sqrt{\deg(\varphi)\deg(\psi)}$$

En posant $\varphi = [1]$ et $\psi = -\pi_p$, comme $\deg(1 - \pi_p) = \mathrm{Card}(E(\mathbb{Z}/p\mathbb{Z}))$, il vient :

$$|\mathrm{Card}(E(\mathbb{Z}/p\mathbb{Z})) - \deg[1] - \deg(-\pi_p)| \leq 2\sqrt{\deg[1]\deg(-\pi_p)}.$$

Or $\deg[1] = \deg\left(\frac{K(E)}{K(E)}\right) = 1$ et $\deg(-\pi_p) = p$. On en déduit le résultat voulu.

□

Remarque : On obtient donc l'encadrement suivant pour $p \in \mathbb{P}$:

$$(\sqrt{p} - 1)^2 \leq \mathrm{Card}(E(\mathbb{Z}/p\mathbb{Z})) \leq (\sqrt{p} + 1)^2.$$

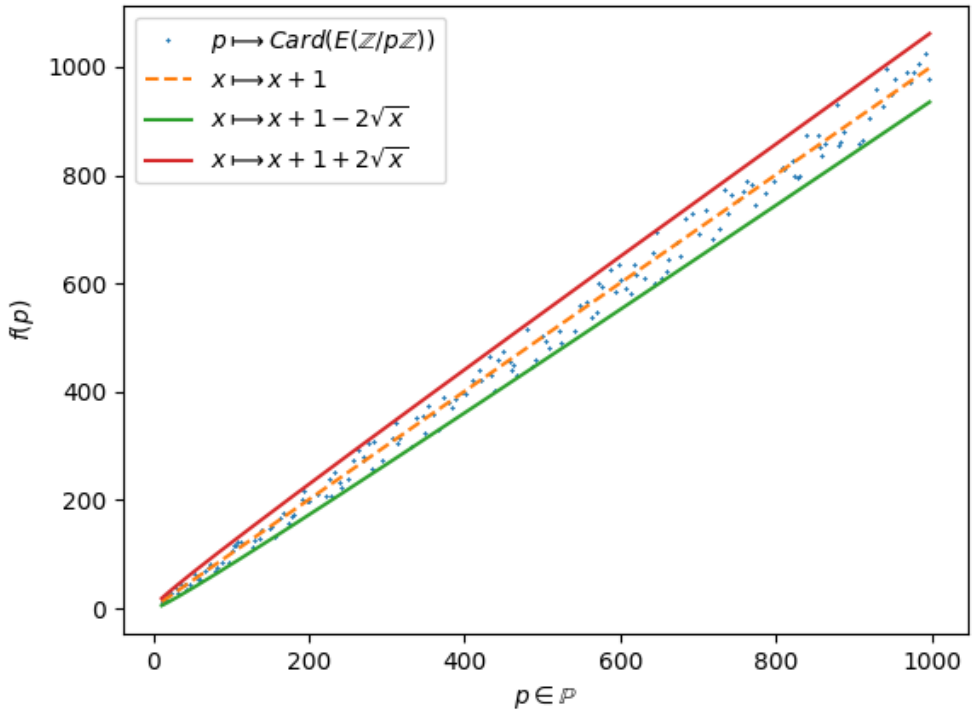


FIGURE 11 – $\text{Card}(E(\mathbb{Z}/p\mathbb{Z}))$ pour $p \in \mathbb{P} \cap [\![10, 1000]\!]$ et pour E d'équation $y^2 = x^3 - 2x + 3$.

Le théorème de Hasse garantit donc qu'on peut choisir aléatoirement un entier $p \in \mathbb{P}$ sans diminuer significativement $\text{Card}(E(\mathbb{Z}/p\mathbb{Z}))$. Il reste à faire le choix d'un générateur $G \in E(\mathbb{Z}/p\mathbb{Z})$.

6.3 Observation sur le cofacteur

Définition : (Ordre)
On note $\text{ord}(G) = \text{Card}(\langle G \rangle)$ l'ordre de $G \in E(\mathbb{Z}/p\mathbb{Z})$.

Remarque : $\text{ord}(G)$ est le plus petit $k \in \mathbb{N}^*$ tel que $[k]G = \mathcal{O}$.

Définition : (Cofacteur)
On appelle cofacteur, et on note h la quantité :

$$h(G) = \frac{\text{Card}(E(\mathbb{Z}/p\mathbb{Z}))}{\text{ord}(G)}.$$

Plus le cofacteur est proche de 1, meilleur est le choix du générateur. En effet, si le cofacteur est trop élevé, le problème du logarithme discret est plus facile à résoudre car G engendre un petit sous groupe de $E(\mathbb{Z}/p\mathbb{Z})$.

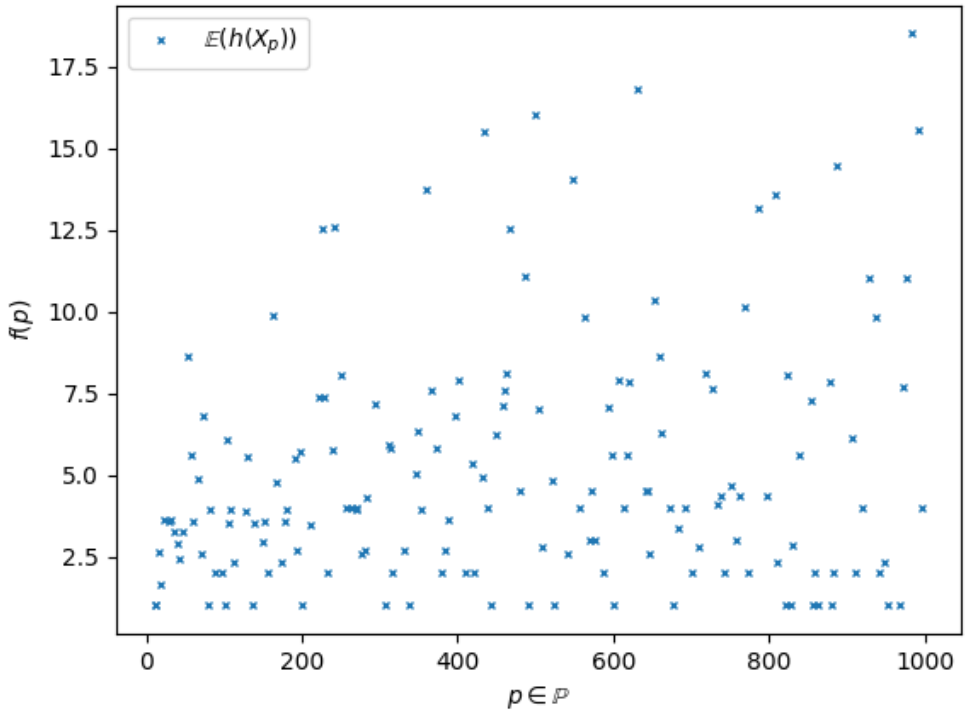


FIGURE 12 – $\mathbb{E}(h(X_p))$ pour X_p suivant une loi uniforme sur $E(\mathbb{Z}/p\mathbb{Z})$ avec $p \in \mathbb{P} \cap [\![10, 1000]\!]$ et pour E d'équation $y^2 = x^3 - 2x + 3$.

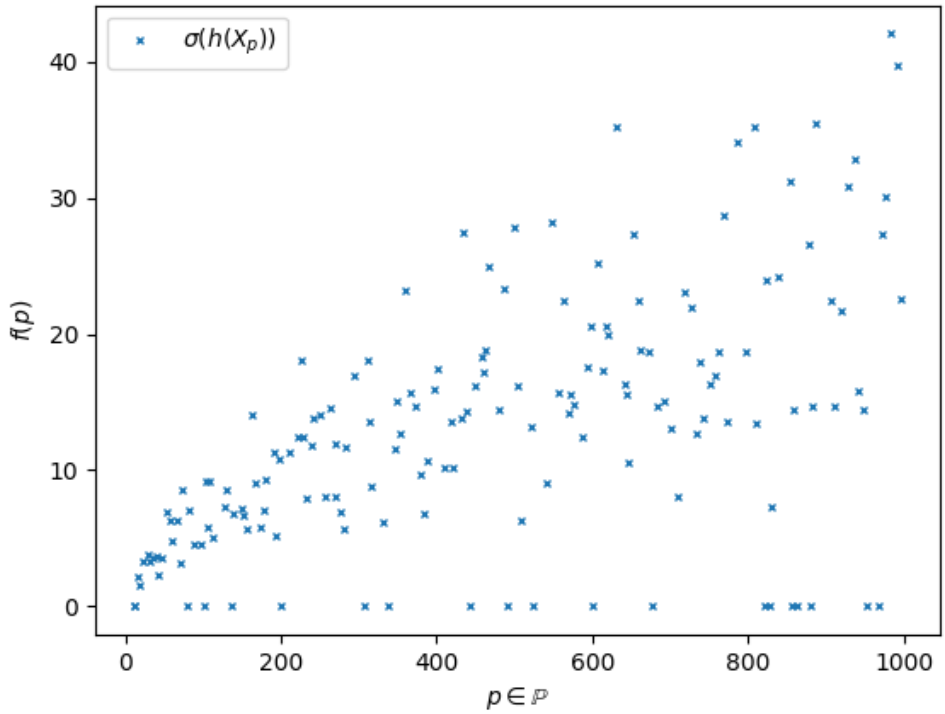


FIGURE 13 – $\sigma(h(X_p))$ pour les conditions de fig. 10.

On souhaiterait déterminer $G \in E(\mathbb{Z}/p\mathbb{Z})$ de sorte à minimiser le cofacteur $h(G)$. Cependant, il n'est en général pas facile de déterminer un tel G.

Considérons E d'équation $y^2 = x^3 - 2x + 3$, et en notant $Y_p = h(X_p)$ avec $X_p \sim \mathbb{U}_{E(\mathbb{Z}/p\mathbb{Z})}$. C'est à dire que la variable aléatoire X_p correspond à un point aléatoire de $E(\mathbb{Z}/p\mathbb{Z})$ choisit uniformément. On peut alors déterminer algorithmiquement l'espérance et l'écart-type de Y_p en fonction de p (figure 10 et 11 respectivement).

On constate que l'espérance de $h(X)$ est globalement proche de 1, ce qui correspond à un sous-groupe engendré de taille optimale. Cependant, bien que l'espérance de Y_p reste faible, on observe que l'écart-type peut prendre des valeurs relativement élevées. Contrairement au choix de p qui influence $\mathrm{Card}(E(\mathbb{Z}/p\mathbb{Z}))$ (qui est une quantité encadrée par le théorème de Hasse), on ne dispose pas de majoration théorique de h. Ainsi, le choix aléatoire d'un générateur ne garanti pas une sécurité du protocole suffisante. Il faut donc trouver un moyen de déterminer un tel générateur.

6.4 Ordre d'un point

Soit $p \in \mathbb{P}$, notons :

$$N := \mathrm{Card}(E(\mathbb{Z}/p\mathbb{Z})) = \prod_{k=1}^{n} p_k^{a_k}.$$

Soit $G \in E(\mathbb{Z}/p\mathbb{Z})$. On a $\mathrm{ord}(G)|N$. Posons désormais, pour tout $k \in [\![1, n]\!]$, $G_k := \dfrac{N}{p_k^{a_k}} \cdot G$.

Propriété 6.4.1 :
Pour tout $k \in [\![1, n]\!]$:

$$\mathrm{ord}(G_k) = \min\left\{p_k^i \;\middle|\; i \in [\![1, a_k]\!],\ p_k^i \cdot G_k = \mathcal{O}\right\}.$$

Démonstration : Soit $k \in [\![1, n]\!]$, tout d'abord, $N \cdot G = \mathcal{O}$. Donc :

$$p_k^{a_k} \cdot G_k = p_k^{a_k} \frac{N}{p_k^{a_k}} \cdot G = N \cdot G = \mathcal{O}.$$

Donc $\mathrm{ord}(G_k) \,|\, p_k^{a_k}$. Ainsi :

$$\forall k \in [\![1, n]\!],\ \mathrm{ord}(G_k) \in \left\{p_k^i \;\middle|\; i \in [\![1, a_k]\!]\right\}$$

$$\iff \forall k \in [\![1, n]\!],\ \mathrm{ord}(G_k) = \min\left\{p_k^i \;\middle|\; i \in [\![1, a_k]\!],\ p_k^i G_k = \mathcal{O}\right\}.$$

□

Remarque : Pour trouver l'ordre de G, il suffit de connaitre l'ordre de G_k, pour tout k. En effet, on a :

Propriété 6.4.2 :

$$\mathrm{ord}(G) = \prod_{k=1}^{n} \mathrm{ord}(G_k)$$

Démonstration :

- D'une part :

$$\forall k \in [\![1, n]\!], \mathrm{ord}(G) \cdot G_k = \frac{N}{p_k^{a_k}} \mathrm{ord}(G) \cdot G = \frac{N}{p_k^{a_k}} \cdot \mathcal{O} \Longrightarrow \forall k \in [\![1, n]\!], \mathrm{ord}(G_k) | \mathrm{ord}(G).$$

De plus, pour tout $k \neq l \in [\![1, n]\!], \mathrm{ord}(G_k) \wedge \mathrm{ord}(G_l) = 1$ (car pour tout k, $\mathrm{ord}(G_k) \mid p_k^{a_k}$). Donc :

$$\left(\prod_{k=1}^{n} \mathrm{ord}(G_k)\right) | \ \mathrm{ord}(G).$$

- D'autre part, si on note :

$$\mathrm{ord}(G) = \prod_{k=1}^{n} p_k^{\sigma_k} \quad \text{et} \quad \forall k \in [\![1,n]\!], \mathrm{ord}(G_k) = p_k^{o_k}.$$

Alors, par définition :

$$\forall j \in [\![1,n]\!],\ p_j^{o_j} \cdot G_j = p_j^{o_j} \frac{N}{p_j^{a_j}} \cdot G = \frac{N}{p_j^{a_j - o_j}} \cdot G = \mathcal{O}.$$

Ainsi, pour tout $j \in [\![1,n]\!]$:

$$\mathrm{ord}(G) \mid \frac{N}{p_j^{a_j-o_j}} \Longrightarrow \prod_{k=1}^{n} p_k^{\sigma_k} \mid \frac{1}{p_j^{a_j-o_j}} \prod_{k=1}^{n} p_k^{a_k} \Longrightarrow \prod_{k=1}^{n} p_k^{\sigma_k} \mid \prod_{\substack{k=1 \\ k\neq j}}^{n} p_k^{a_k} \times p_j^{o_k}.$$

En particulier :

$$\forall j \in [\![1,n]\!],\ p_j^{\sigma_j} \mid p_j^{o_j} \Longrightarrow \mathrm{ord}(G) \mid \left(\prod_{k=1}^{n} \mathrm{ord}(G_k) \right).$$

Enfin :

$$\mathrm{ord}(G) = \left(\prod_{k=1}^{n} \mathrm{ord}(G_k) \right).$$

□

Ces résultats nous permettent d'établir un premier algorithme calculant l'ordre d'un point quelconque de $E(\mathbb{Z}/p\mathbb{Z})$. Il suffit d'effectuer la décomposition en facteur premier de N, puis de calculer $\mathrm{ord}(G_k)$ pour $k \in [\![1,n]\!]$ et de renvoyer le produit des résultats obtenus.

Algorithme 5 : Calcul de l'ordre de G_k

Input : $G_k \in E(\mathbb{Z}/p\mathbb{Z}), p_k \in \mathbb{P}$
Output : $\mathrm{ord}(G_k) = \min\left\{p_k^i \mid i \in [\![1,a_k]\!],\ p_k^i \cdot G_k = \mathcal{O}\right\}$
$P \leftarrow G_k$
$i \leftarrow 0$
tant que $P \neq \mathcal{O}$ **faire**
  $i \leftarrow i+1$
  $P \leftarrow p_k \cdot P$ (Algorithme 3)
fin
retourner p^i

Algorithme 6 : Calcul de l'ordre de G

Input : $G \in E(\mathbb{Z}/p\mathbb{Z}), p \in \mathbb{P}$
Output : $\mathrm{ord}(G)$
$N \leftarrow \mathrm{Card}(E(\mathbb{Z}/p\mathbb{Z}))$ (Algorithme de Schoof [4])
$P, A \leftarrow [p_1, \cdots, p_n], [a_1, \cdots, a_n]$ (Décomposition en facteurs premiers)
$O_G = 1$
pour $k \in [\![1,n]\!]$ **faire**
  $G_k \leftarrow (N/P[k]^{A[k]}) \cdot G$
  $O_{G_k} \leftarrow \mathrm{ord}(G_k)$ (Algorithme 5)
  $O_G = O_G \times O_{G_k}$
fin
retourner O_G

Cependant, il est possible d'améliorer la complexité de l'algorithme précédent en employant une méthode diviser pour régner. On procède de la manière suivante :

- Si $n = 1$, il suffit de trouver $\mathrm{ord}(G) = \mathrm{ord}(G_1)$.
- Sinon, on pose :
$$R = \left(\prod_{k=1}^{\lfloor n/2 \rfloor} p_k^{a_k} \right) \cdot G.$$
- On trouve $\mathrm{ord}(R)$ récursivement.
- On pose :
$$T = \mathrm{ord}(R) \cdot G.$$
- On trouve $\mathrm{ord}(T)$ récursivement.
- On renvoie $\mathrm{ord}(Q) = \mathrm{ord}(R) \cdot \mathrm{ord}(T)$.

Ayant désormais connaissance d'une méthode fournissant l'ordre d'un point, on peut tirer uniformément P dans $E(\mathbb{Z}/p\mathbb{Z})$, puis vérifier si $h(P)$ est suffisamment proche de 1. Si c'est le cas P est un générateur convenable. Sinon, on répète le procédé pour un nouveau point $\tilde{P}$.

7 Bilbiographie

[1] Joseph H. Silverman, *The Arithmetic of Elliptic Curves*, Second edition, Springer, 2009, ISBN 978-0-387-09493-9.

[2] Johannes A. Buchmann, *Introduction to cryptography*, Springer, 2001, ISBN 978-0-387-95034-1.

[3] A van Tuyl, *The field of N-torsion points of an elliptic curve over a finite field*, PhD thesis, M. Sc. Thesis, McMaster University, 1997.

[4] Rene Schoof, *Elliptic Curves over Finite Fields and the Computation of Square Roots mod p*, Mathematics of Computation, Vol. 44, No. 170, 1985.

8 Annexes

8.1 Annexe 1 : Cryptosystème

Définition : (O)
n définit un cryptosystème par un tuple $(\mathcal{P}, \mathcal{C}, \mathcal{K}, \mathcal{E}, \mathcal{D})$ où :

- $\mathcal{P}$ désigne l'ensemble des textes en clair (plaintext)
- $\mathcal{C}$ désigne l'ensemble des textes chiffrés (ciphertext)
- $\mathcal{K}$ désigne l'ensemble des clés (key)
- $\mathcal{E} := \{E_k : \mathcal{P} \longrightarrow \mathcal{C} \mid k \in \mathcal{K}\}$ désigne l'ensemble des fonctions de chiffrement (encryption function)
- $\mathcal{E} := \{E_k : \mathcal{C} \longrightarrow \mathcal{D} \mid k \in \mathcal{K}\}$ désigne l'ensemble des fonctions de déchiffrement (decryption function)

Vérifiant la propriété :

$$\forall k \in \mathcal{K}, \exists \kappa \in \mathcal{K}, \forall p \in \mathcal{P}, D_\kappa(E_k(p)) = p$$

Autrement dit, pour tout chiffrement à partir d'une clé k, on peut trouver une clé κ qui permet de décrypter le message.

8.2 Annexe 2 : Changements de variables

Définition : (Equation de Weierstrass sur les points finis)
Une équation sur les points finis de Weierstrass d'une courbe de Weierstrass s'obtient en prenant $Z = 1$. C'est donc l'équation :

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

Pour simplifier les équations, on cherche à faire des changements de variables. Il faut dons définir le cadre des changements de variables légaux :

Propriété 8.2.1 :
Un changement de variables dans $\mathbb{P}^2$ transforme un polynôme homogène de Weierstrass en un autre un polynôme homogène de Weierstrass (à une constante multiplicative près) si et seulement si il est de la forme :

$$\begin{cases} X' = u^2X + rZ \\ Y' = u^3Y + u^2sX + tZ \\ Z' = Z \end{cases} \qquad \text{avec } u, r, s, t \in K \text{ et } u \neq 0$$

Remarque : En particulier, pour les points finis ces changements de variables sont :

$$\begin{cases} x = u^2x' + r \\ y = u^3y' + u^2sx' + t \end{cases} \qquad \text{avec } u, r, s, t \in \mathbb{K} \text{ et } u \neq 0$$

Démonstration :
La droite projective d'équation $z = 0$ doit être conservée ainsi que le point $[0 : 1 : 0]$ (propriété 4.3.1). On a donc nécessairement $z' = z$. Pour raison de degrés en x et y, le changement de variables est affine et vu l'absence de terme en y^3, il est forcément de la forme

$$\begin{cases} x = ax' + r \\ y = by' + cx' + t \end{cases} \qquad \text{avec } ab \neq 0$$

Mais (x, y) et (x', y') vérifient des équations de Weierstrass dont les coefficients de y^2 et de x^3

sont égaux à 1. Or le coefficient de y'^2 est b^2 et celui de x^3 est a^3. On doit donc avoir $b^2 = a^3$. Réciproquement, ces changements de variables conserve la forme de polynôme homogène de Weierstrass.

□

Supposons car(K) différente de 2 et 3.
On considère une courbe de Weierstrass E d'équation sur les points finis :

$$(E) : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

On a :

$$\begin{aligned}(2y + a_1x + a_3)^2 &= 4y^2 + a_1^2x^2 + a_3^2 + 4a_1xy + 4a_3y + 2a_1a_3x \\ &= 4(y^2 + a_1xy + a_3y) + (a_1^2x^2 + 2a_1a_3x + a_3^2)\end{aligned}$$

Comme Caract$(K) \neq 2$, 2 est inversible et on a :

$$\begin{aligned}(E) &\iff \tfrac{1}{4}(2y + a_1x + a_3)^2 - \tfrac{1}{4}(a_1^2x^2 + 2a_1a_3x + a_3^2) = x^3 + a_2x^2 + a_4x + a_6 \\ &\iff \left(y + \tfrac{a_1}{2}x + \tfrac{a_3}{2}\right)^2 = x^3 + \tfrac{b_2}{4}x^2 + \tfrac{b_4}{2}x + \tfrac{b_6}{4}\end{aligned}$$

avec

$$\begin{cases} b_2 = a_1^2 + 4a_2 \\ b_4 = a_1a_3 + 2a_4 \\ b_6 = a_3^2 + 4a_6 \end{cases}$$

En posant $y' = y + \frac{a_1}{2}x + \frac{a_3}{2}$ on obtient :

$$(E) \iff (y')^2 = x^3 + \frac{b_2}{4}x^2 + \frac{b_4}{2}x + \frac{b_6}{4}.$$

Comme Caract$(K) \neq 3$, 3 est aussi inversible et on a :

$$\begin{aligned}(E) &\iff (y')^2 = (x + \tfrac{b_2}{12})^3 - 3\tfrac{b_2}{12}(x + \tfrac{b_2}{12})^2 + \tfrac{b_3}{123} + \tfrac{b_6}{4} \\ &\iff (y')^2 = (x + \tfrac{b_2}{12})^3 - \tfrac{b_2^2 - 24b_4}{12}(x + \tfrac{b_2}{12}) - \tfrac{b_3}{3} + \tfrac{36b_2b_4 - 216b_6}{864}\end{aligned}$$

avec

$$\begin{cases} c_4 = b_2^2 - 24b_4 \\ c_6 = -b_2^3 + 36b_2b_4 - 216b_6 \end{cases}$$

En posant $x' = x + \frac{b_2}{12} = x + \frac{a_1^2 + 4a_2}{12}$, on obtient :

$$(E) \iff (y')^2 = x'^3 - \frac{c_4}{48}x' - \frac{c_6}{864}.$$

$K = B^a \bmod p$ $K = A^b \bmod p$