D31: Protocoles Cryptographiques

Cryptosystèmes basés sur le problème du logarithme discret

Nicolas Méloni

Master 2: 1er semestre
(2014/2015)

Introduction

- Introduit dès 1976 par Diffie et Hellman comme base pour leur protocole d'échange de clé
- Utilisé par ElGamal en 1984 pour construire un schéma de chiffrement à clé publique ainsi qu'un protocole de signature
- Problème difficile sur lequel repose la cryptographie basée sur les courbes elliptiques

Définition

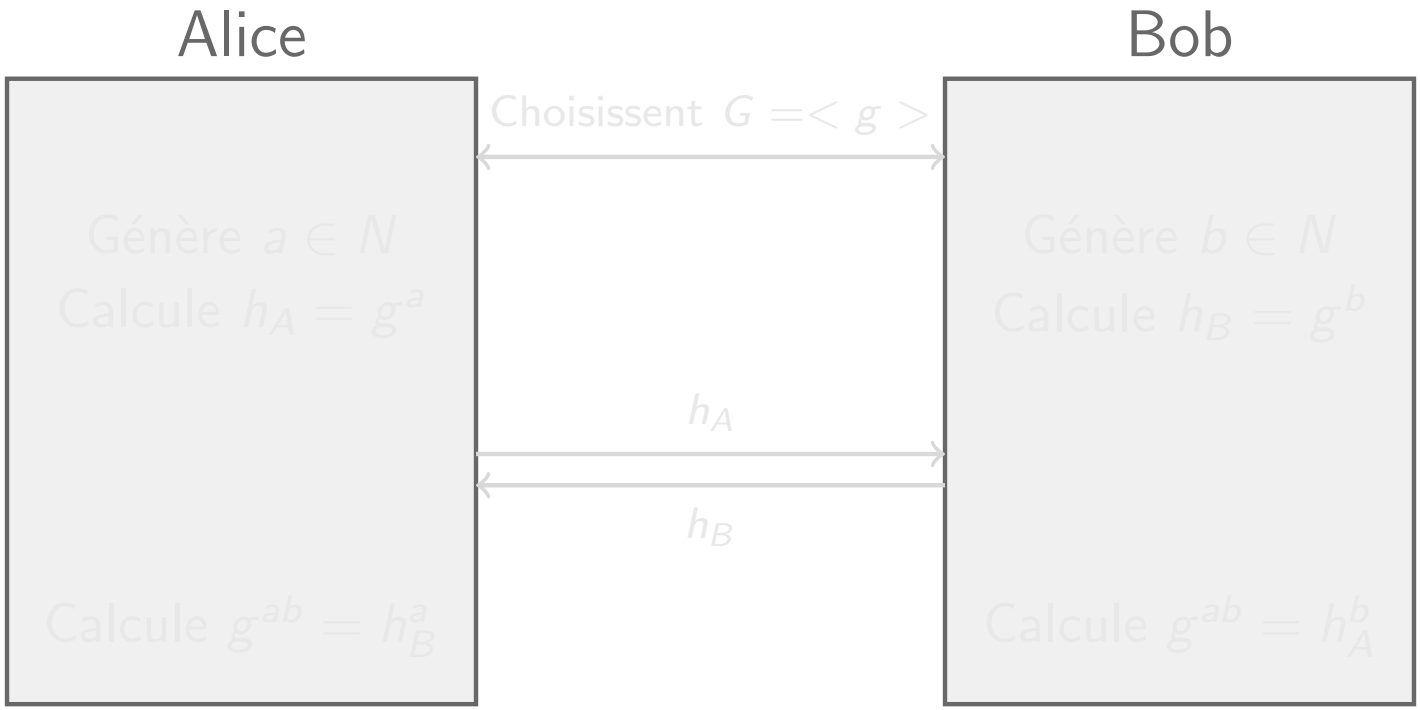
Soit G un groupe cyclique d'ordre n. $G = \{g^i : 0 \leq i \leq n-1\}$ pour un certain $g \in G$. Pour tout $h \in G$, il existe un unique entier $k \in \{0, \ldots, n-1\}$ tel que $h = g^k$ que l'on appelle logarithme discret de h (en base g). Résoudre le problème du logarithme discret (PLD) c'est résoudre l'équation en k:

$$k \in \{0, \ldots, n-1\}, h = g^k.$$

Remarque

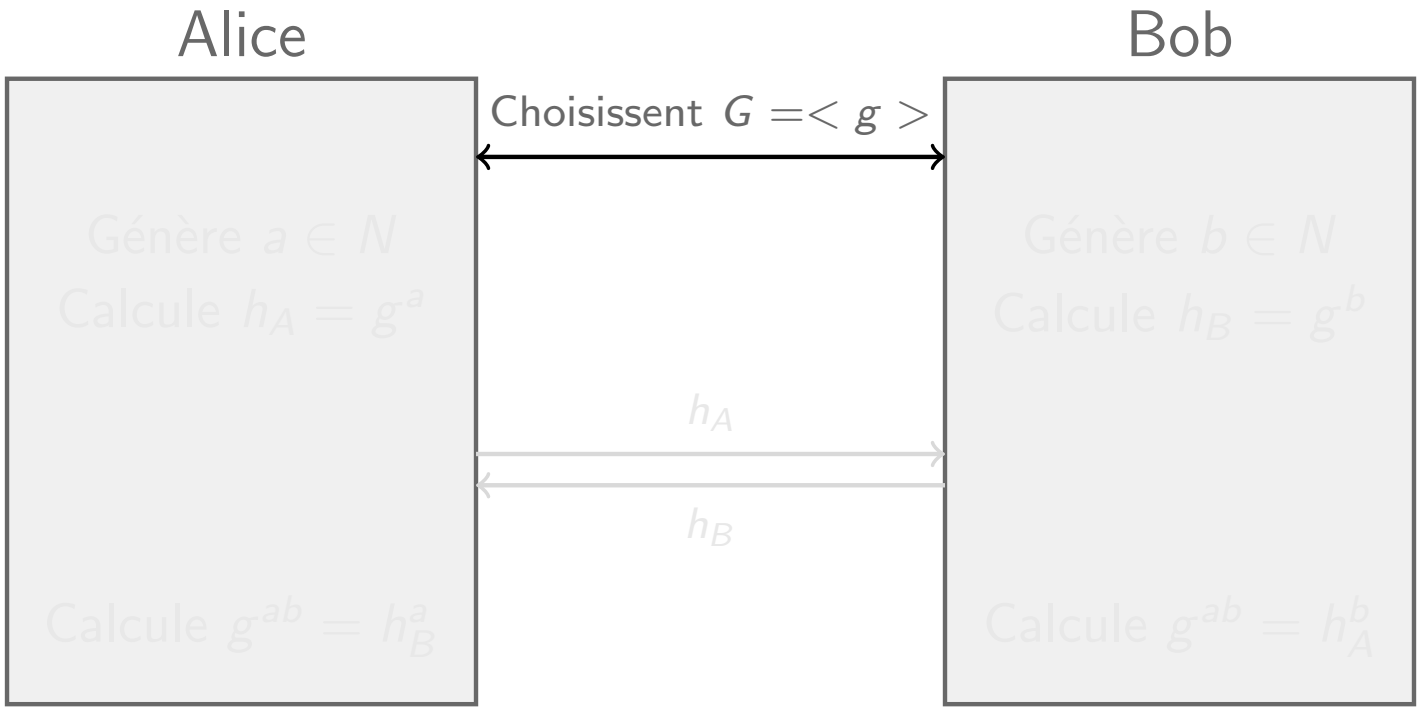
La fonction $f : g \mapsto g^k$ est une fonction à sens unique mais pas une fonction à trappe!

Protocole de Diffie-Hellman



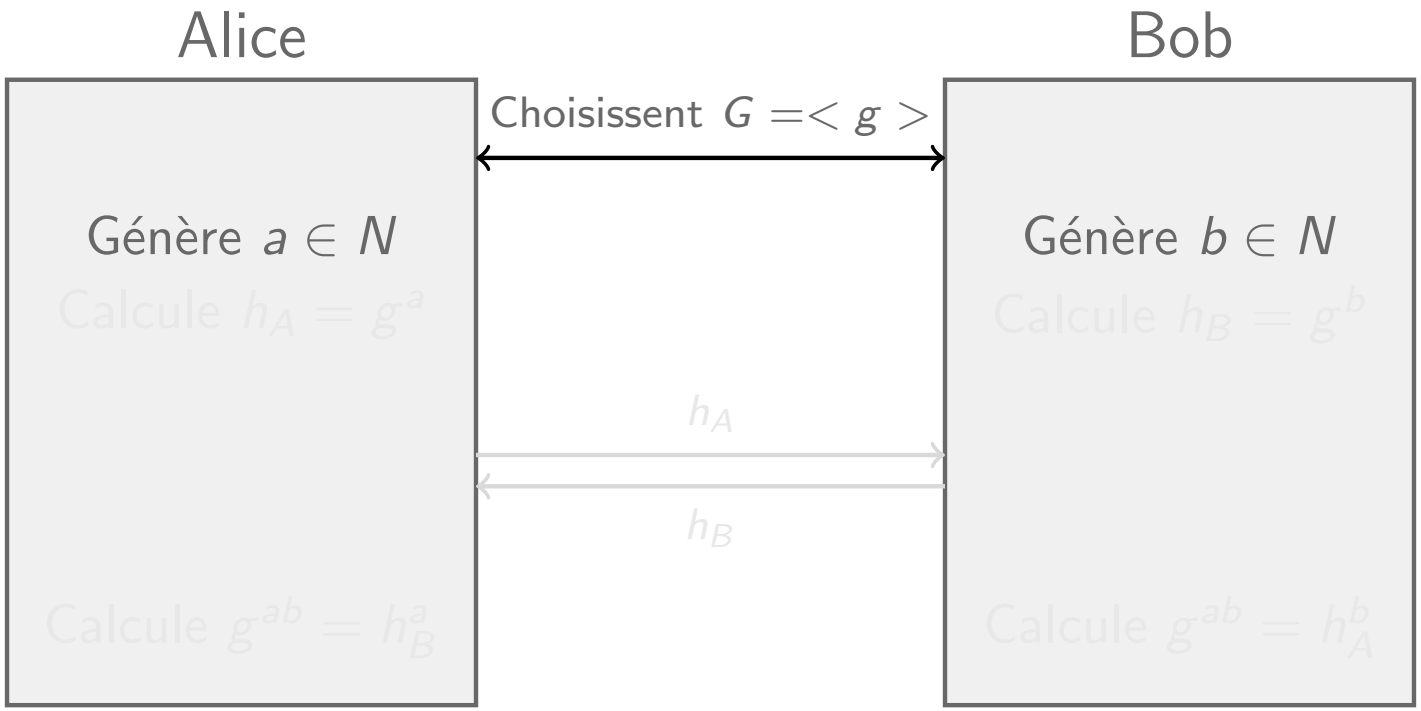
- Alice et Bob partage le secret g^{ab}

Protocole de Diffie-Hellman



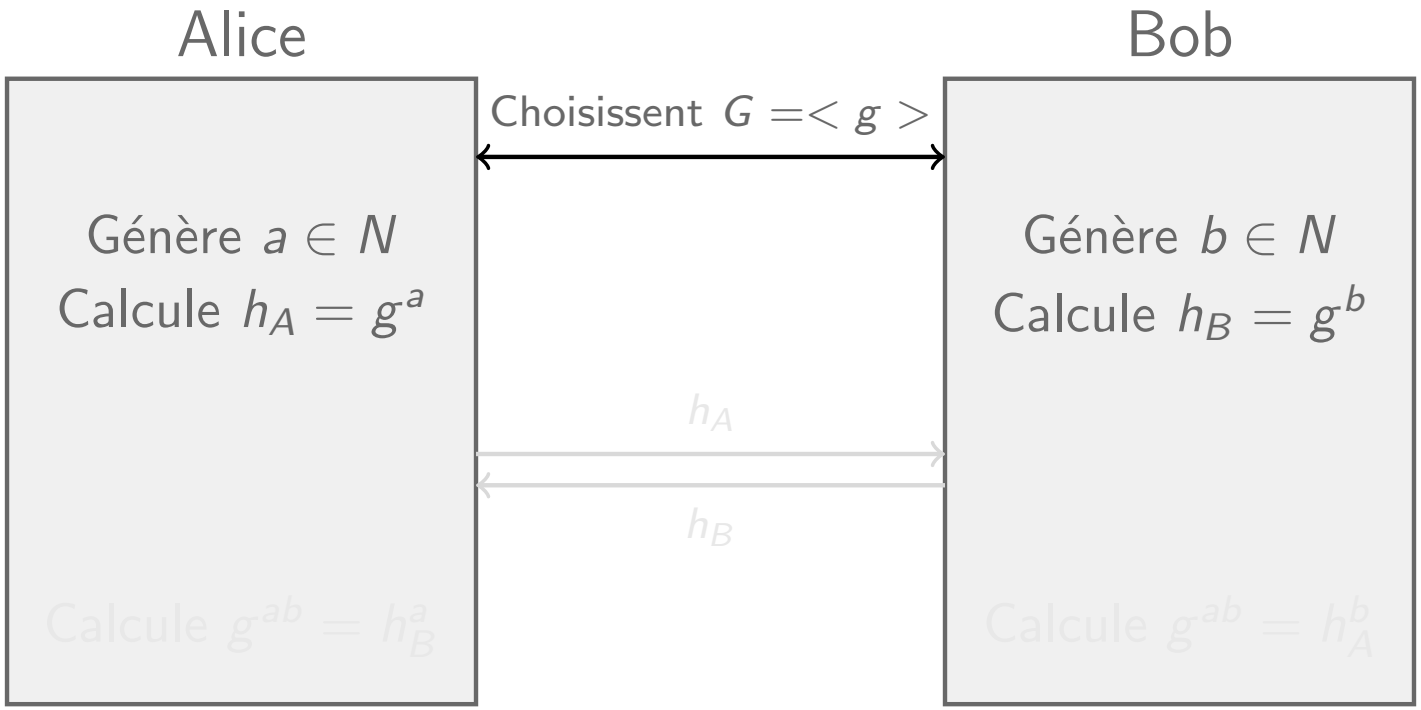
- Alice et Bob partage le secret g^{ab}

Protocole de Diffie-Hellman



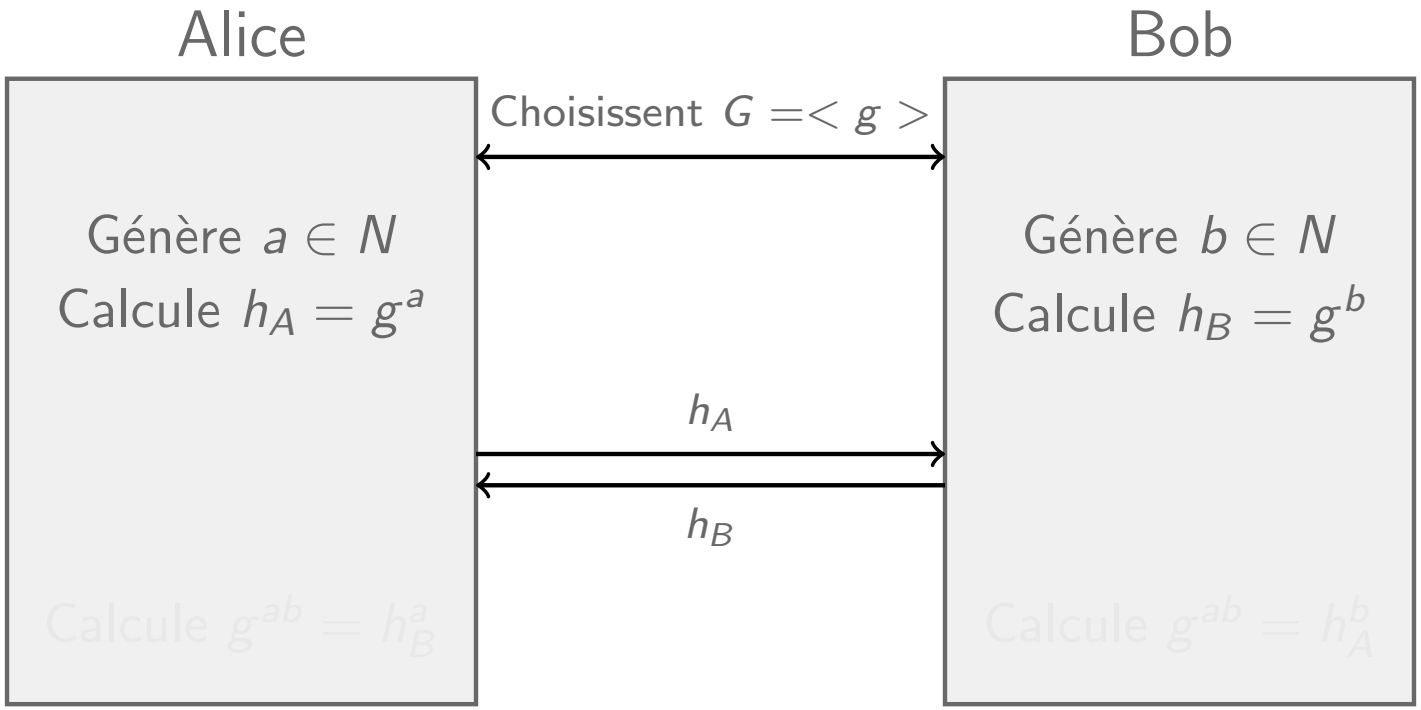
- Alice et Bob partage le secret g^{ab}

Protocole de Diffie-Hellman



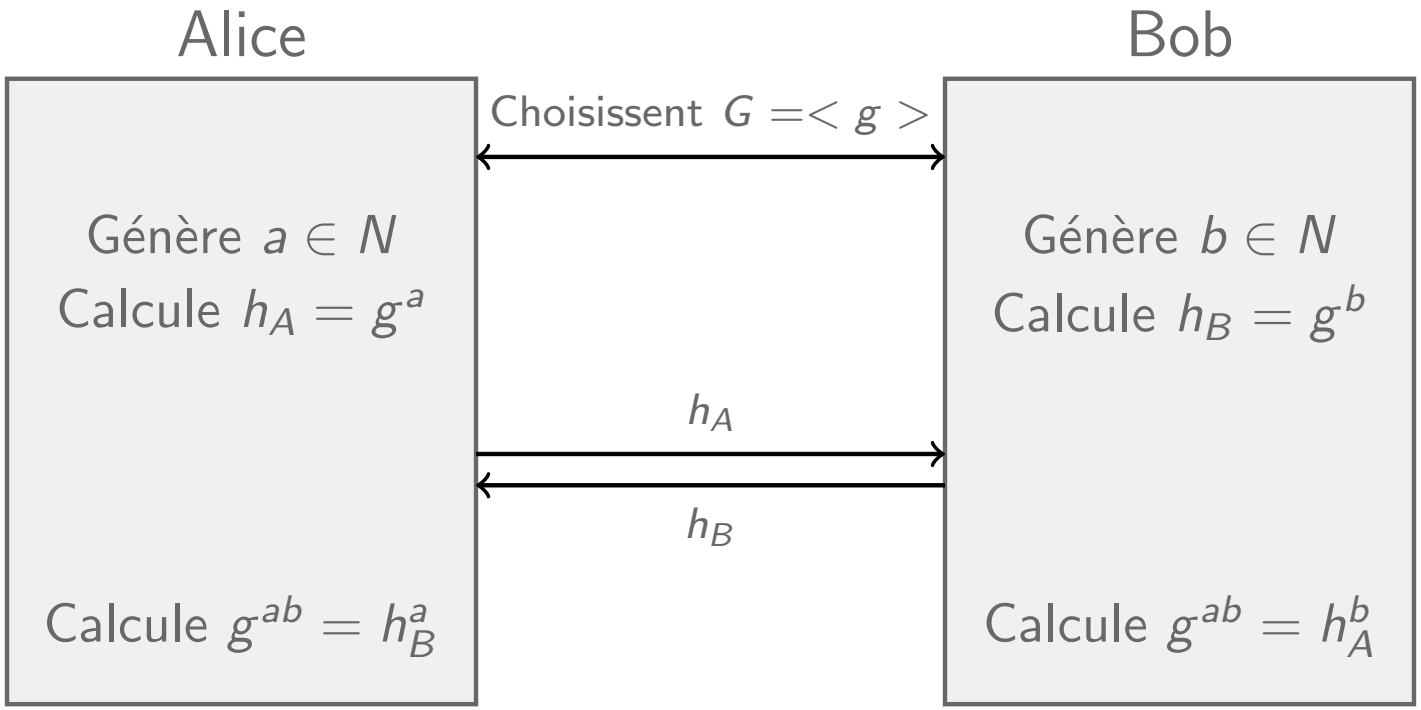
- Alice et Bob partage le secret g^{ab}

Protocole de Diffie-Hellman



- Alice et Bob partage le secret g^{ab}

Protocole de Diffie-Hellman



- Alice et Bob partage le secret g^{ab}

Protocole de Diffie-Hellman

Sécurité du protocole

- Un adversaire voit passer sur le réseau g, h_A, h_B
- Il doit calculer g^{ab} à partir de g, g^a, g^b, c'est ce qu'on appelle le problème de Diffie-Hellman calculatoire (PDHC).
- Un sous probème est également considérer parfois, le problème de Diffie-Hellman décisionel (PDHD): à partir de g, g^a, g^b et $h \in G$ a-t'on $h = g^{ab}$?

Protocole de Diffie-Hellman

- Si un adersaire peut résoure le PLD sur G il peut simplement résoudre le PDHC
- De même, s'il peut résoudre le PDHC il peut résoudre le PDHD
- Il existe cependant des groupes pour lesquels le PDHD est facile alors que le PDHC reste dur
- Le PLD et le PDHC ne sont pas prouvés équivalents, la sécurité des systèmes à base de logarithme discret repose en général sur la difficulté du PDHC et non directement du PLD

Le cryptosystème El Gamal

Le cryptosystème

Soit p un nombre premier, on note $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ le corps à p éléments. Soit α un élément primitif de $\mathbb{F}_p^*$. Soient enfin k un entier et $\beta = \alpha^k$. On définit:

$$\begin{aligned} \mathcal{P} &= \mathbb{F}_p^* \\ \mathcal{C} &= \mathbb{F}_p^* \times \mathbb{F}_p^* \\ K_{pub} &= (p, \alpha, \beta) \\ K_{sec} &= k \end{aligned}$$

Le cryptosystème El Gamal

Chiffrement

Soit $m \in \mathcal{P}$,

$$E(K_{pub}, m) = (y_1, y_2)$$

où $y_1 = \alpha^r \mod p, y_2 = m\beta^r \mod p$ et r est un entier généré aléatoirement.

Déchiffrement

Le chiffré est $c = (y_1, y_2)$,

$$D(K_{sec}, c) = y_2(y_1^k)^{-1} \mod p.$$

Sécurité du système El Gamal

Le niveau de sécurité est directement lié au problème de Diffie-Hellman:

- la fonction de chiffrement est bien à sens unique si le PDHC est difficile,
- le système est sémantiquement sûr si le PDHD est diffcile,
- le système doit être modifié pour devenir résistant aux attaques à chiffrés choisis.

Résolution du PLD

- $G =< g >$ est un groupe d'ordre $p-1$, on cherche à calculer l'entier k tel que $h = g^k$ pour un certain $h \in G$ donné.

Algorithme naïf

Il "suffit" donc d'énumérer les puissances de g jusqu'à obtenir h.
Compléxité: $O(p)$

Algorithme de Shanks (pas de bébé, pas de géant)

Il consiste à choisir un entier $m < k$ et à écrire k sous la forme $k = qm + r$ où q et r sont, respectivement, le quotient et le reste de la division de k par m.

- On calcule les g^{mj}
- On calcule les hg^{i}
- lorsqu'on obtient une collision on a bien

$$g^{mj} = hg^{i} \Leftrightarrow g^{mj+i} = h.$$

La compléxité est optimale en choisissant $m = \lceil \sqrt{p} \rceil$. On alors un algorithme en $O(\sqrt{p})$.

Algorithme Rho de Pollard

Repose sur le paradoxe des anniversaires.

- Génère aléatoirement des éléments de la forme $g^{a_i} h^{b_i}$
- lorsqu'on obtient une collision on a:

$$g^{a_i} h^{b_i} = g^{a_j} h^{b_j} \Rightarrow k \equiv \frac{a_i - a_j}{b_j - b_i} \mod p$$

En moyenne, il faut $\sqrt{p}$ étapes pour obtenir une collision. On a donc un algorithme en $O(\sqrt{p})$ en moyenne.

Algorithme de Pohlig-Hellman

Permet d'accélérer le calcul lorsque l'ordre du groupe n ($n = p - 1$ dans le cas d'ElGamal)peut être factorisé, i.e.

$$n = \prod_{i=1}^{r} p_i^{c_i},$$

grâce au théorème des restes chinois.
Compléxité: $O(c\sqrt{q})$ où q^c est la plus grande puissance première divisant n.

Courbe elliptique sur un corps $\mathbb{K}$ (car(K) >3)

Soient $a, b \in \mathbb{K}$ deux tels que $4a^3 + 27b^3 \neq 0$. Une courbe elliptique est l'ensemble des solutions $(x, y) \in \mathbb{K} \times \mathbb{K}$ de l'équation

$$E : y^2 = x^3 + ax + b,$$

plus un point à l'infini noté $\mathcal{O}$. On note généralement $E(\mathbb{K})$ cet ensemble de points.

Loi de groupe d'un courbe elliptique

Propriété

Une courbe elliptique peut être munie d'un structure de groupe commutatif. La somme $R = (x_3, y_3)$ de deux points $P = (x_1, y_1), Q = (x_2, y_2)$ s'obtient comme suit:

- $-P = (x_1, -y_1)$
- $x_3 = \lambda^2 - x_1 - x_2, y_3 = \lambda(x_1 - x_3) - y_1$ où
  $$\lambda = \begin{cases} \frac{y_2 - y_1}{x_2 - x_1} \text{ si } P \neq \pm Q \\ \frac{3x_1^2 + a}{2y_1} \text{si} P = Q \end{cases}$$
- $R = \mathcal{O}$ si $P = -Q$
- $P + \mathcal{O} = \mathcal{O} + P = P$

Loi de groupe sur $\mathbb{R}$

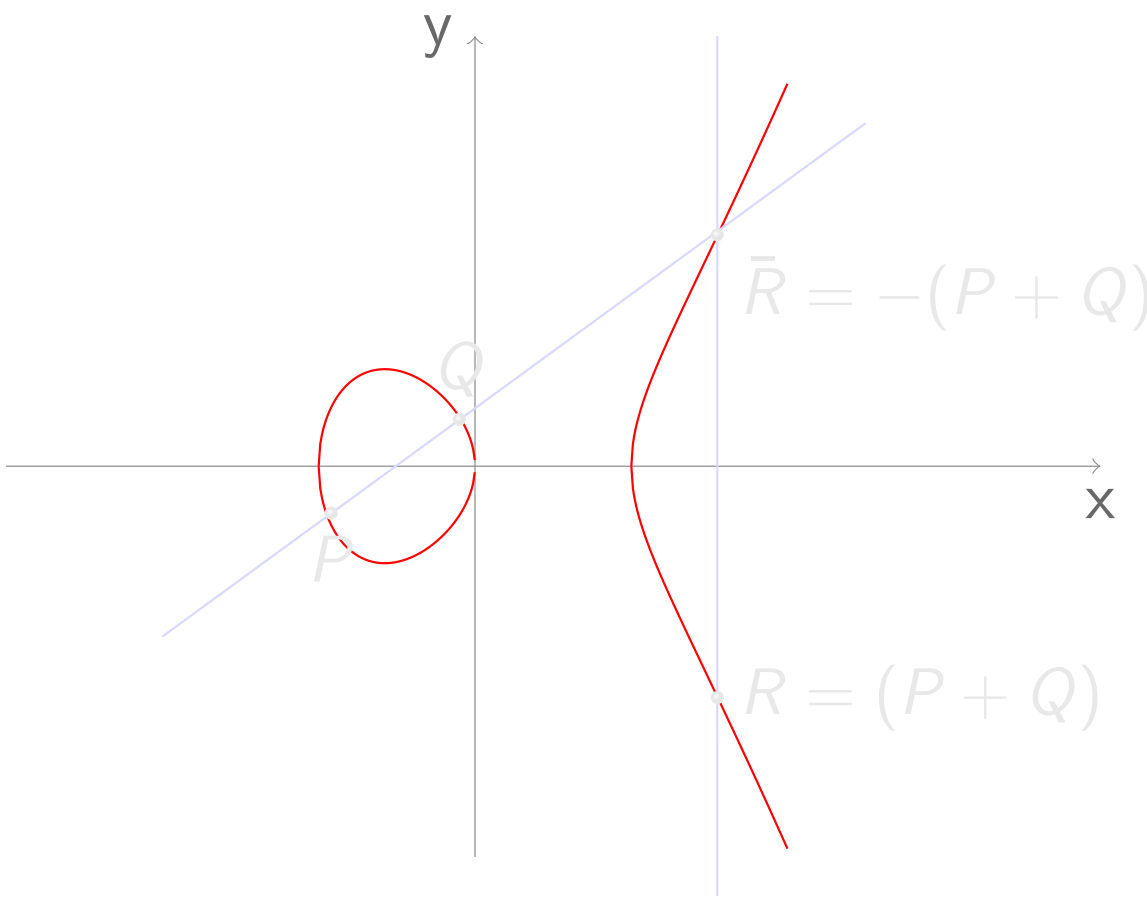


Figure : Courbe $y^2 = x^3 - x$ sur $\mathbb{R}$

Loi de groupe sur $\mathbb{R}$

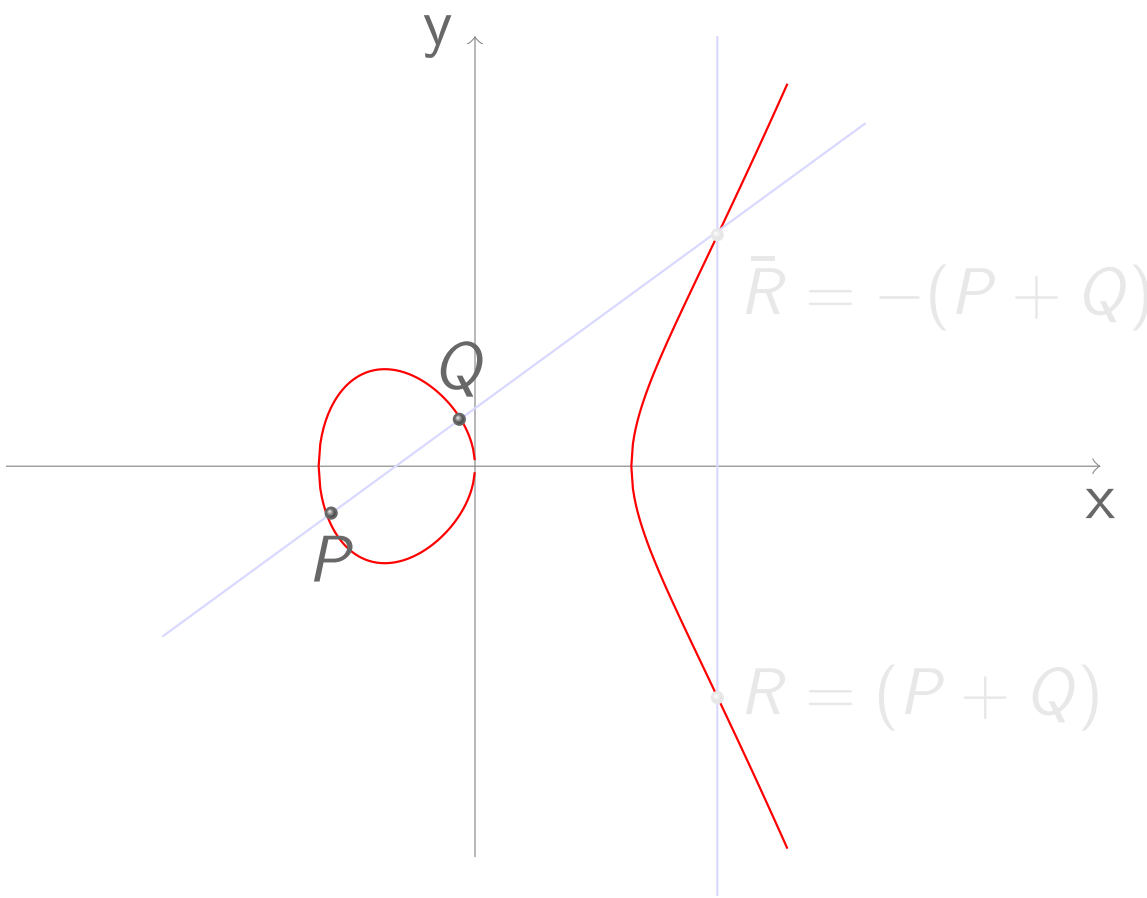


Figure : Courbe $y^2 = x^3 - x$ sur $\mathbb{R}$

Loi de groupe sur $\mathbb{R}$

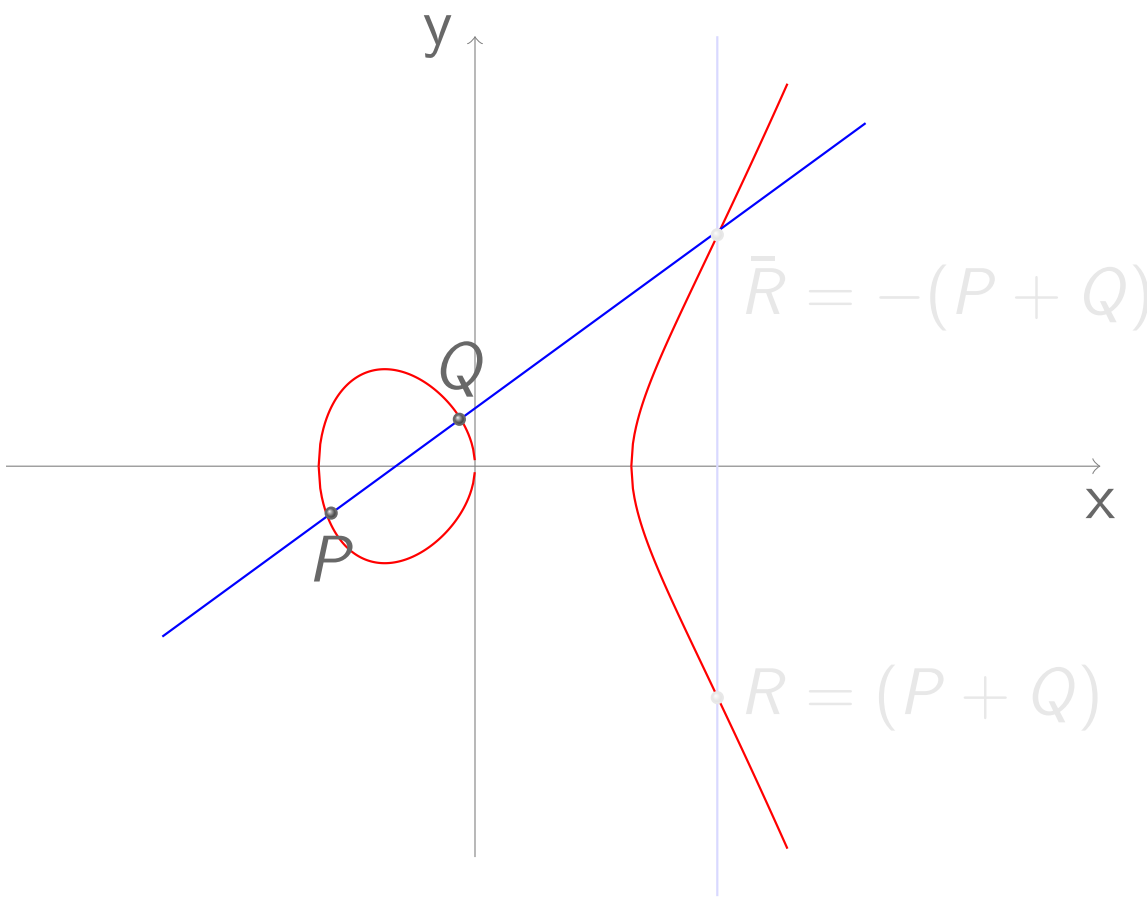


Figure : Courbe $y^2 = x^3 - x$ sur $\mathbb{R}$

Loi de groupe sur $\mathbb{R}$

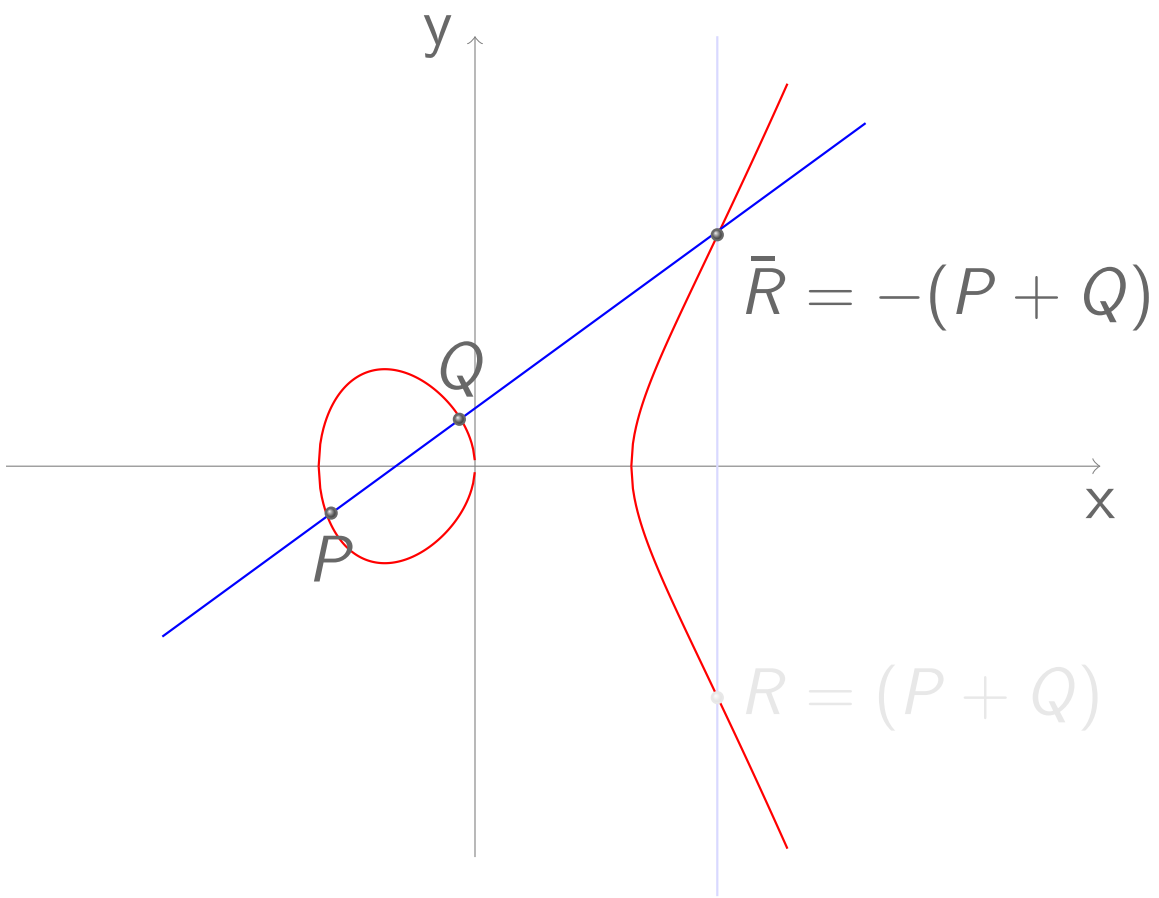


Figure : Courbe $y^2 = x^3 - x$ sur $\mathbb{R}$

Loi de groupe sur $\mathbb{R}$

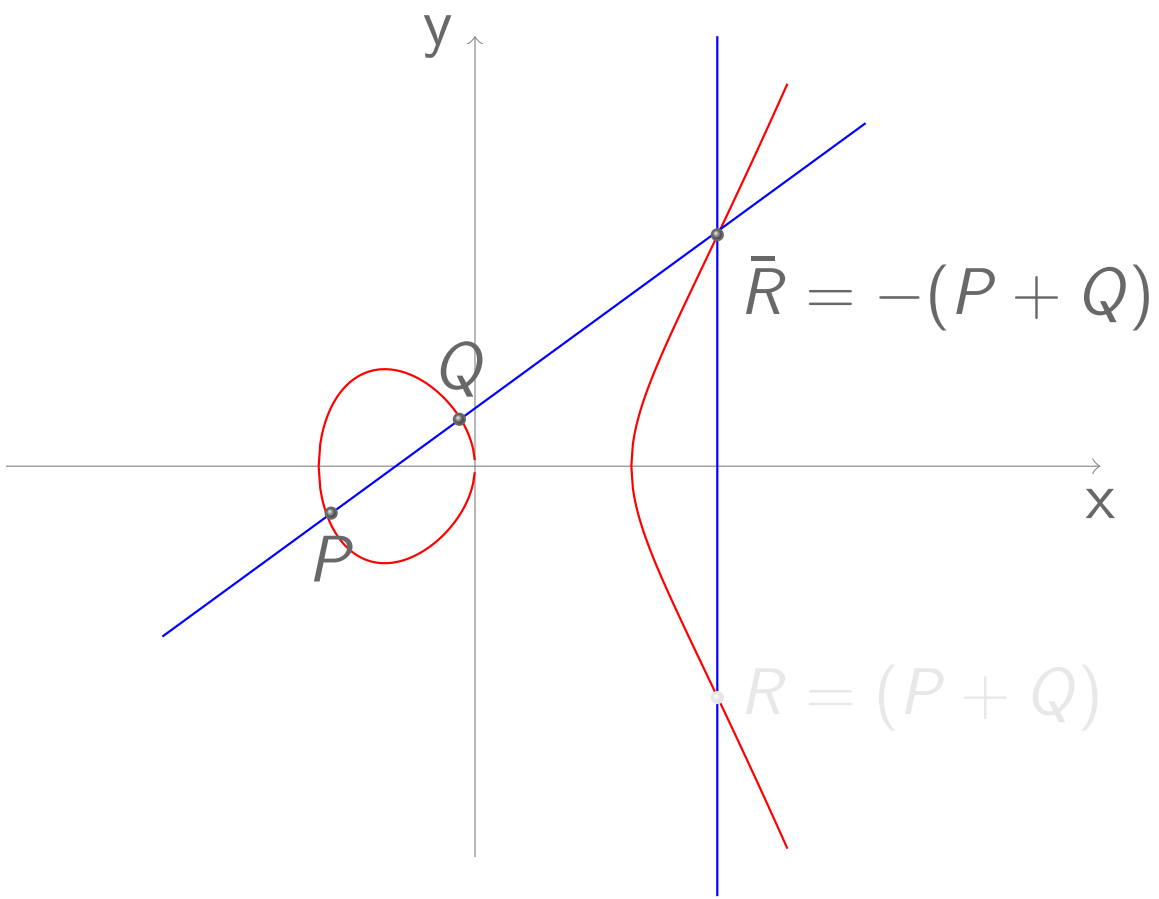


Figure : Courbe $y^2 = x^3 - x$ sur $\mathbb{R}$

Loi de groupe sur $\mathbb{R}$

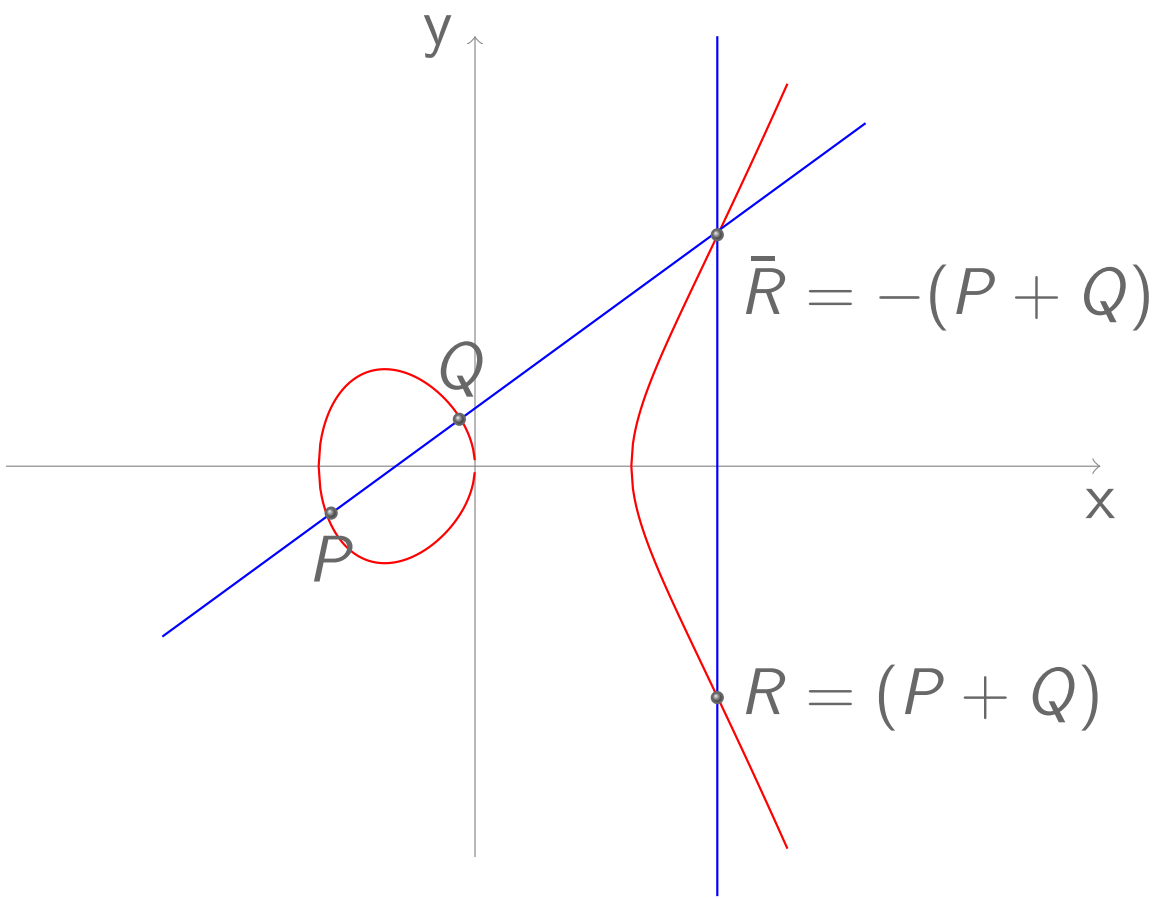


Figure : Courbe $y^2 = x^3 - x$ sur $\mathbb{R}$

Loi de groupe sur $\mathbb{R}$

Les courbes sur $\mathbb{R}$ ne sont pas utilisées dans la pratique:

- impossible de représenter les réels en machine,
- le PLD est "facile" à résoudre sur $\mathbb{Q}$.

C'est pour cela qu'on utilise des courbes définies sur un corps fini, en général $\mathbb{F}_p$ ou $\mathbb{F}_{2^n}$.

Un exemple de courbe sur $\mathbb{F}_{11}$

Considérons la courbe $E : y^2 = x^3 + x + 6$ définie sur le corps $\mathbb{F}_{11}$.

x	0	1	2	3	4	5	6	7	8	9	10
y	0	1	2	3	4	5	6	7	8	9	10
$x^3 + x + 6$	6	8	5	3	8	4	8	4	9	7	4
y^2	0	1	4	9	5	3	3	5	9	4	1

$$E(\mathbb{F}_{11}) = \{ \quad (2,4),(2,7),(3,5),(3,6),(5,2),(5,9),\\ (7,2),(7,9),(8,3),(8,8),(10,2),(10,9)\}$$

Un exemple de courbe sur $\mathbb{F}_{11}$

Considérons la courbe $E : y^2 = x^3 + x + 6$ définie sur le corps $\mathbb{F}_{11}$.

x	0	1	2	3	4	5	6	7	8	9	10
y	0	1	2	3	4	5	6	7	8	9	10
$x^3 + x + 6$	6	8	5	3	8	4	8	4	9	7	4
y^2	0	1	4	9	5	3	3	5	9	4	1

$$E(\mathbb{F}_{11}) = \{ (2,4),(2,7),(3,5),(3,6),(5,2),(5,9), (7,2),(7,9),(8,3),(8,8),(10,2),(10,9)\}$$

Un exemple de courbe sur $\mathbb{F}_{11}$

Considérons la courbe $E : y^2 = x^3 + x + 6$ définie sur le corps $\mathbb{F}_{11}$.

x	0	1	2	3	4	5	6	7	8	9	10
y	0	1	2	3	4	5	6	7	8	9	10
$x^3 + x + 6$	6	8	5	3	8	4	8	4	9	7	4
y^2	0	1	4	9	5	3	3	5	9	4	1

$$E(\mathbb{F}_{11}) = \{ (2,4),(2,7),(3,5),(3,6),(5,2),(5,9), (7,2),(7,9),(8,3),(8,8),(10,2),(10,9)\}$$

Un exemple de courbe sur $\mathbb{F}_{11}$

Considérons la courbe $E : y^2 = x^3 + x + 6$ définie sur le corps $\mathbb{F}_{11}$.

x	0	1	2	3	4	5	6	7	8	9	10
y	0	1	2	3	4	5	6	7	8	9	10
$x^3 + x + 6$	6	8	5	3	8	4	8	4	9	7	4
y^2	0	1	4	9	5	3	3	5	9	4	1

$$E(\mathbb{F}_{11}) = \{ \quad (2,4),(2,7),(3,5),(3,6),(5,2),(5,9),$$
$$(7,2),(7,9),(8,3),(8,8),(10,2),(10,9)\}$$

Un exemple de courbe sur $\mathbb{F}_{11}$

Considérons la courbe $E : y^2 = x^3 + x + 6$ définie sur le corps $\mathbb{F}_{11}$.

x	0	1	2	3	4	5	6	7	8	9	10
y	0	1	2	3	4	5	6	7	8	9	10
$x^3 + x + 6$	6	8	5	3	8	4	8	4	9	7	4
y^2	0	1	4	9	5	3	3	5	9	4	1

$$E(\mathbb{F}_{11}) = \{ \quad (2,4),(2,7),(3,5),(3,6),(5,2),(5,9),$$
$$(7,2),(7,9),(8,3),(8,8),(10,2),(10,9)\}$$

Un exemple de courbe sur $\mathbb{F}_{11}$

Considérons la courbe $E : y^2 = x^3 + x + 6$ définie sur le corps $\mathbb{F}_{11}$.

x	0	1	2	3	4	5	6	7	8	9	10
y	0	1	2	3	4	5	6	7	8	9	10
$x^3 + x + 6$	6	8	5	3	8	4	8	4	9	7	4
y^2	0	1	4	9	5	3	3	5	9	4	1

$$E(\mathbb{F}_{11}) = \{ \quad (2,4),(2,7),(3,5),(3,6),(5,2),(5,9),$$
$$(7,2),(7,9),(8,3),(8,8),(10,2),(10,9)\}$$

Un exemple de courbe sur $\mathbb{F}_{11}$

Considérons la courbe $E : y^2 = x^3 + x + 6$ définie sur le corps $\mathbb{F}_{11}$.

x	0	1	2	3	4	5	6	7	8	9	10
y	0	1	2	3	4	5	6	7	8	9	10
$x^3 + x + 6$	6	8	5	3	8	4	8	4	9	7	4
y^2	0	1	4	9	5	3	3	5	9	4	1

$$E(\mathbb{F}_{11}) = \{ \quad (2,4),(2,7),(3,5),(3,6),(5,2),(5,9),$$
$$(7,2),(7,9),(8,3),(8,8),(10,2),(10,9)\}$$

Un exemple de courbe sur $\mathbb{F}_{11}$

Considérons la courbe $E : y^2 = x^3 + x + 6$ définie sur le corps $\mathbb{F}_{11}$.

x	0	1	2	3	4	5	6	7	8	9	10
y	0	1	2	3	4	5	6	7	8	9	10
$x^3 + x + 6$	6	8	5	3	8	4	8	4	9	7	4
y^2	0	1	4	9	5	3	3	5	9	4	1

$$E(\mathbb{F}_{11}) = \{ \quad (2,4),(2,7),(3,5),(3,6),(5,2),(5,9),\\ (7,2),(7,9),(8,3),(8,8),(10,2),(10,9)\}$$

Addition de deux points sur $E(\mathbb{F}_{11})$

Considérons les points $P = (3, 6)$ et $Q = (7, 9)$. Pour obtenir le point $R = P + Q$ on calcule:

- $\lambda = (y_1 - y_2)(x_1 - x_2)^{-1} \equiv (-3) \times (-4)^{-1} \equiv 9 \mod 11$
- $x_3 = \lambda^2 - x_1 - x_2 \equiv 9^2 - 3 - 7 \equiv 5 \mod 11$
- $y_3 = \lambda(x_1 - x_3) - y_1 \equiv 9(3 - 5) - 6 \equiv 9 \mod 11$

Ainsi $P + Q = (5, 9)$.

Loi de groupe sur $\mathbb{F}_p$

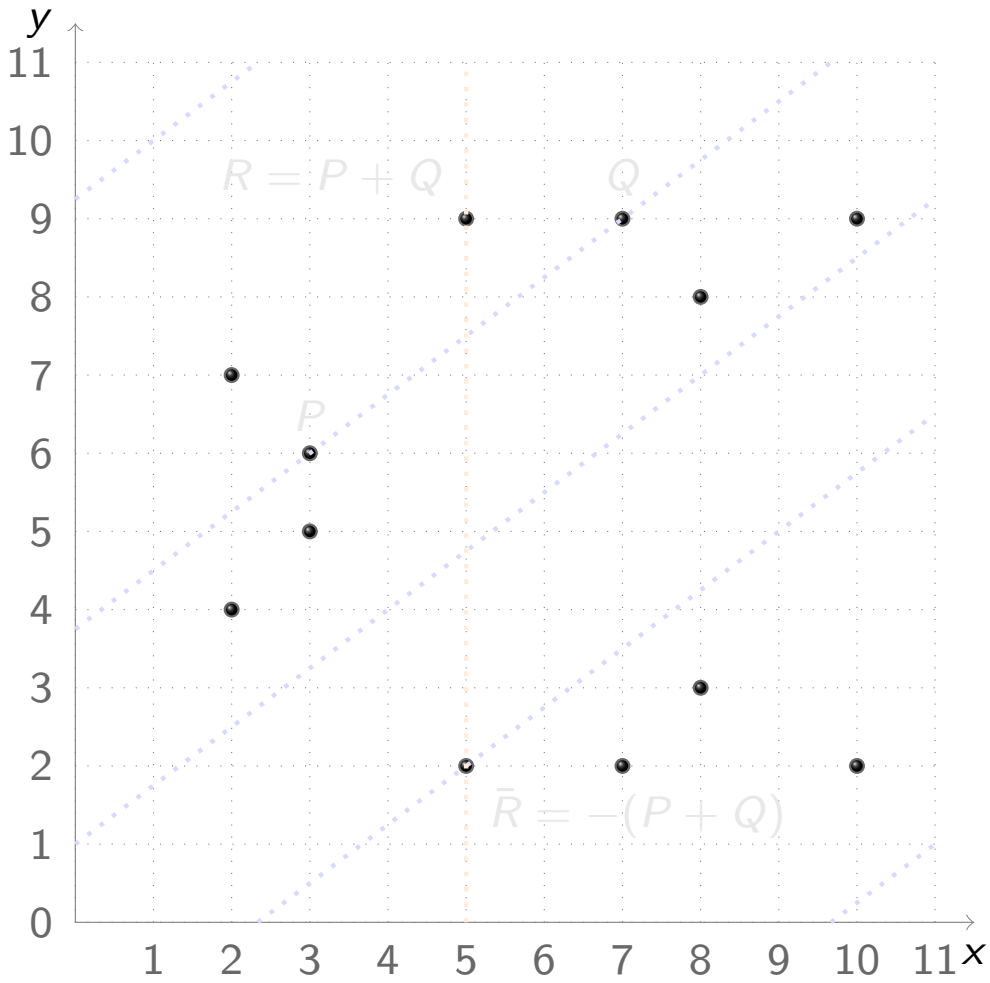


Figure : Courbe $y^2 = x^3 + x + 6$ sur $\mathbb{F}_{11}$

Loi de groupe sur $\mathbb{F}_p$

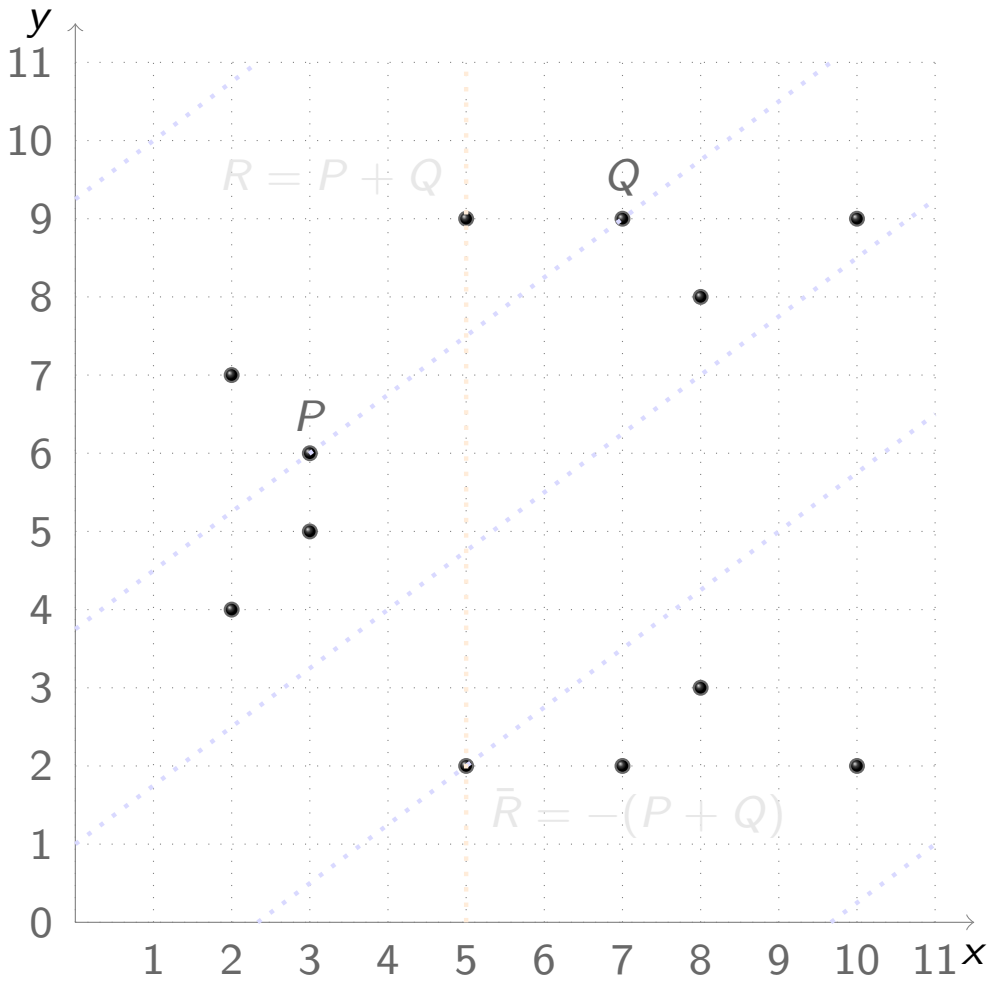


Figure : Courbe $y^2 = x^3 + x + 6$ sur $\mathbb{F}_{11}$

Loi de groupe sur $\mathbb{F}_p$

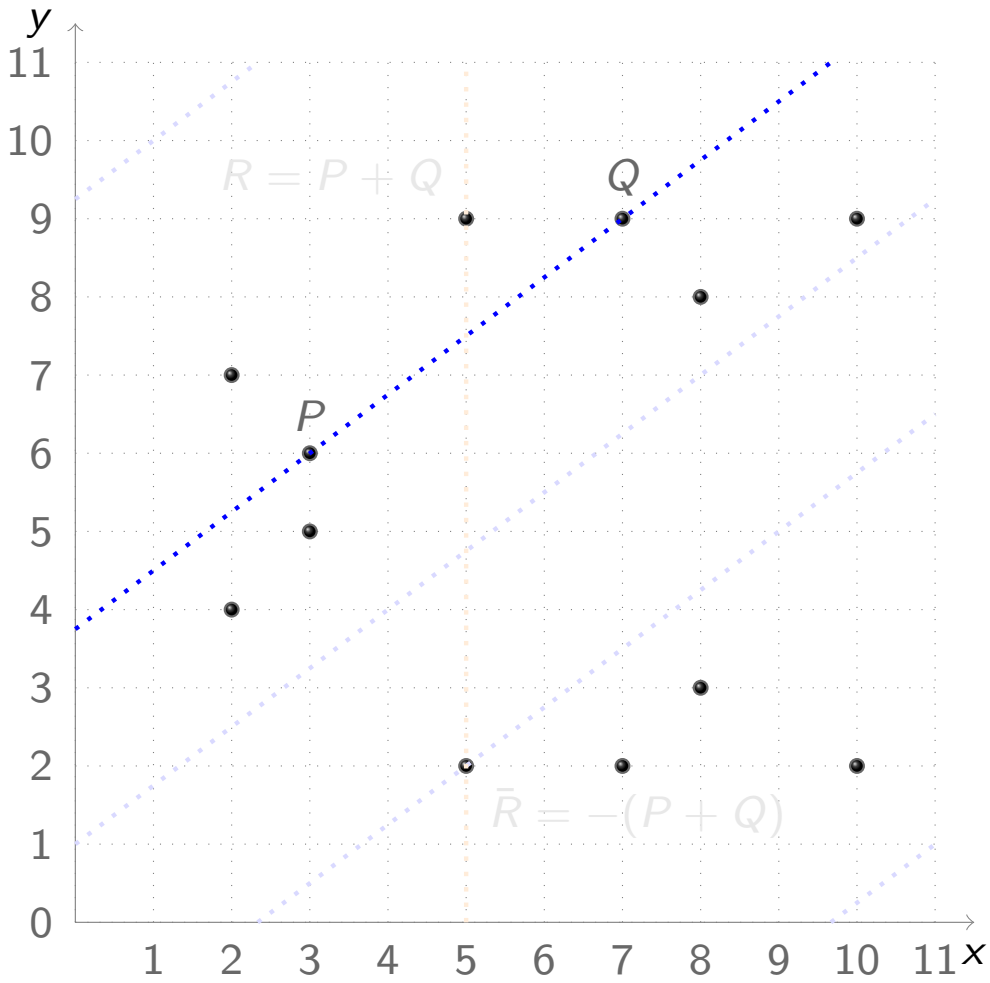


Figure : Courbe $y^2 = x^3 + x + 6$ sur $\mathbb{F}_{11}$

Loi de groupe sur $\mathbb{F}_p$

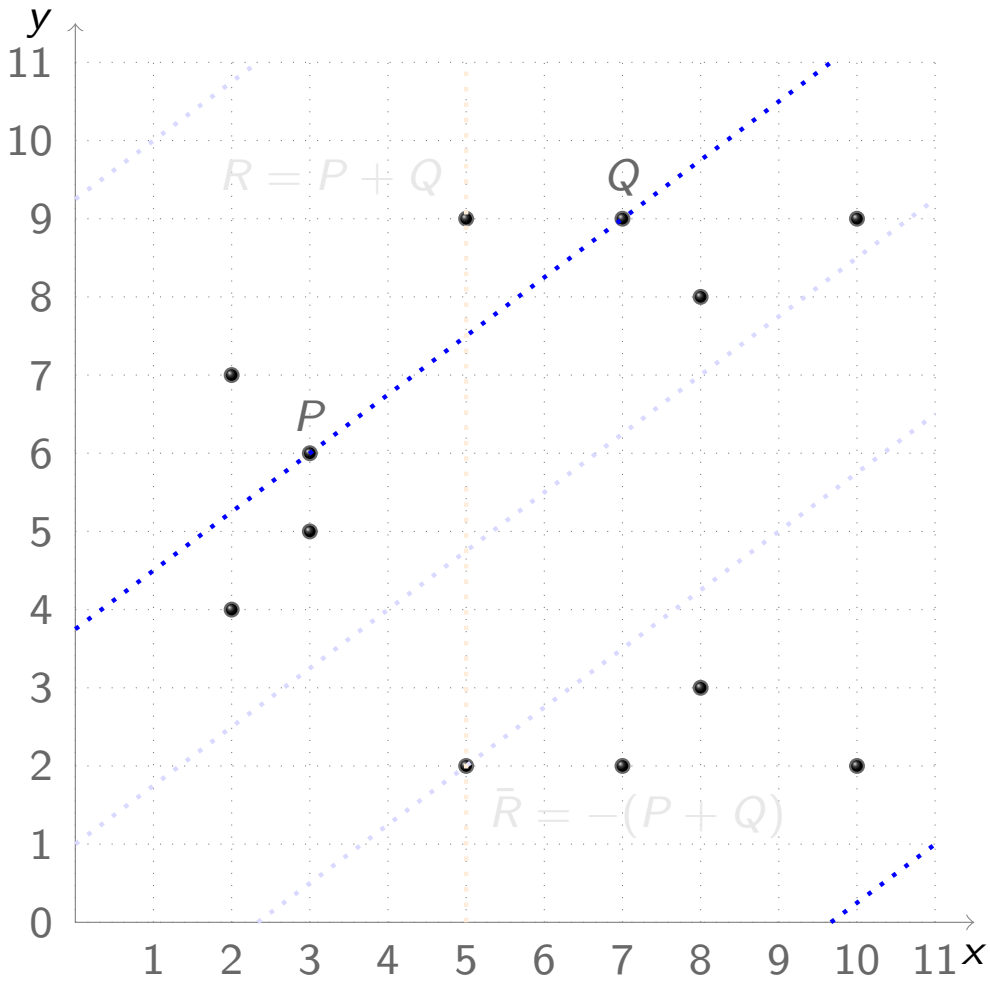


Figure : Courbe $y^2 = x^3 + x + 6$ sur $\mathbb{F}_{11}$

Loi de groupe sur $\mathbb{F}_p$

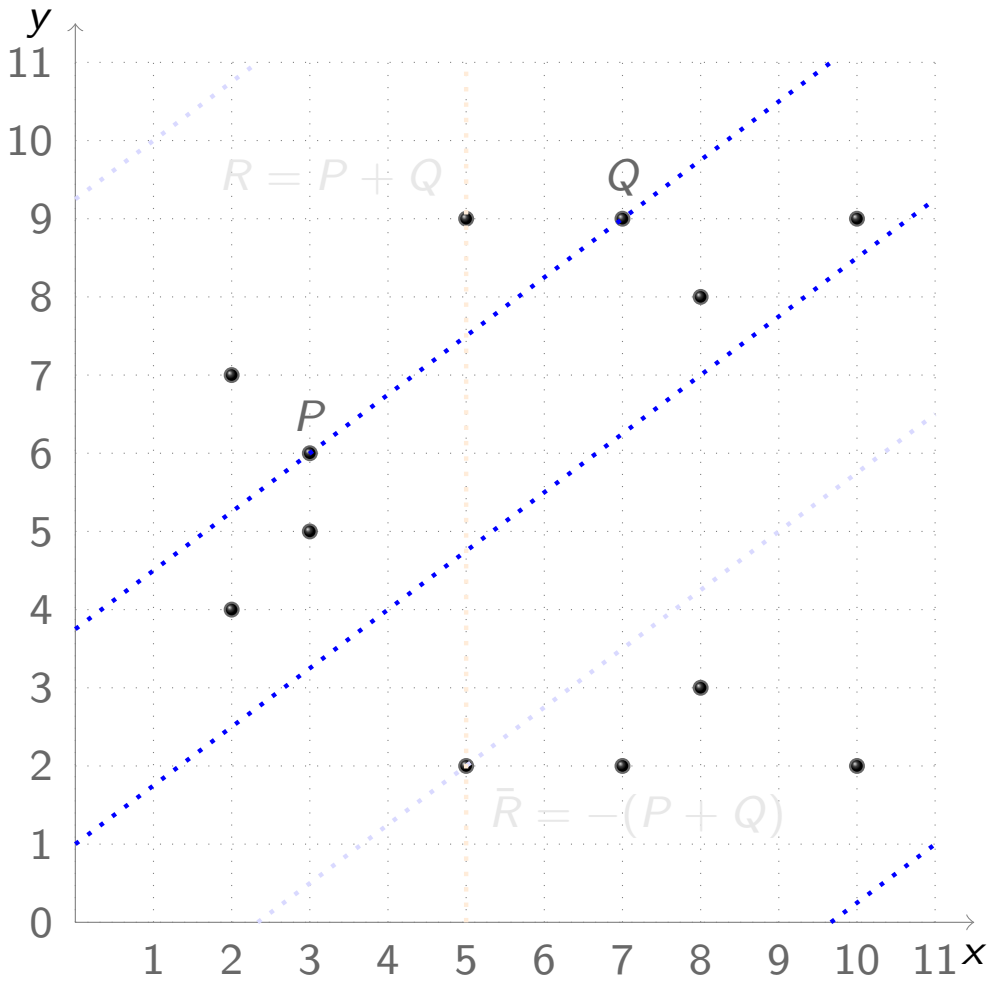


Figure : Courbe $y^2 = x^3 + x + 6$ sur $\mathbb{F}_{11}$

Loi de groupe sur $\mathbb{F}_p$

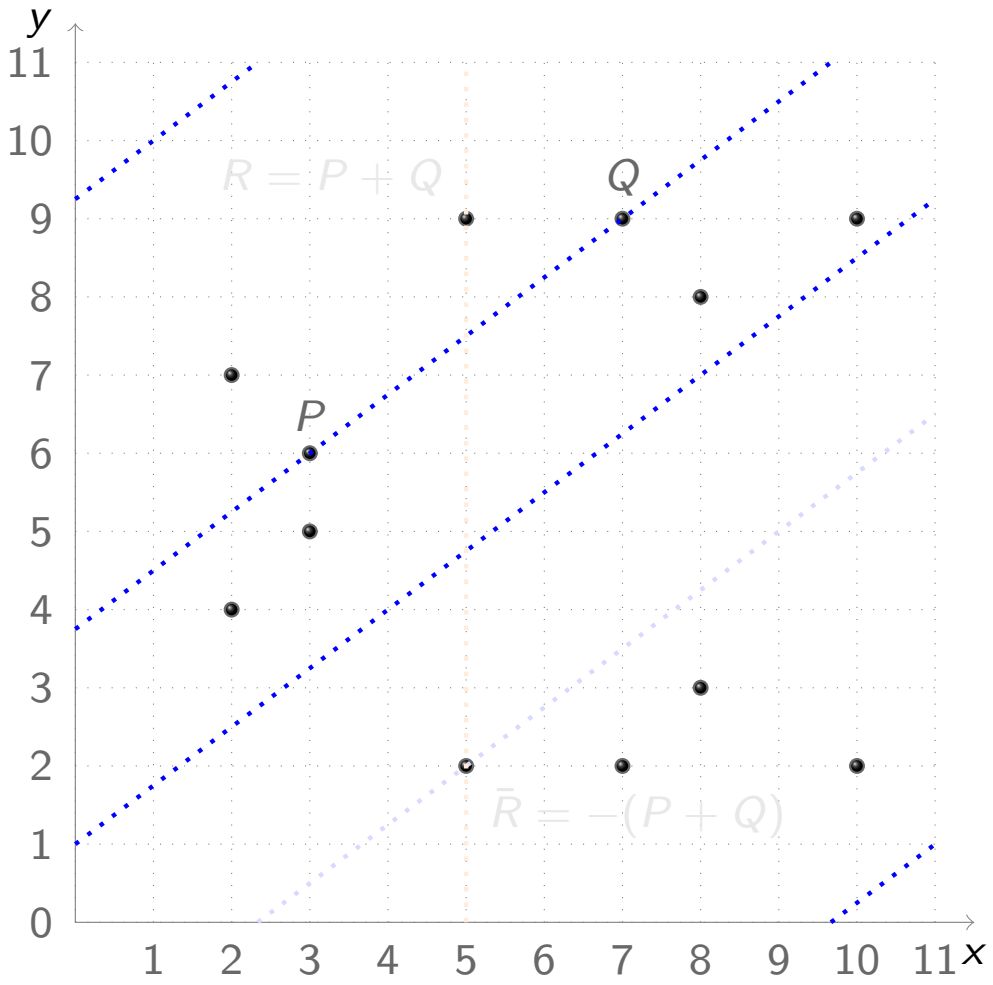


Figure : Courbe $y^2 = x^3 + x + 6$ sur $\mathbb{F}_{11}$

Loi de groupe sur $\mathbb{F}_p$

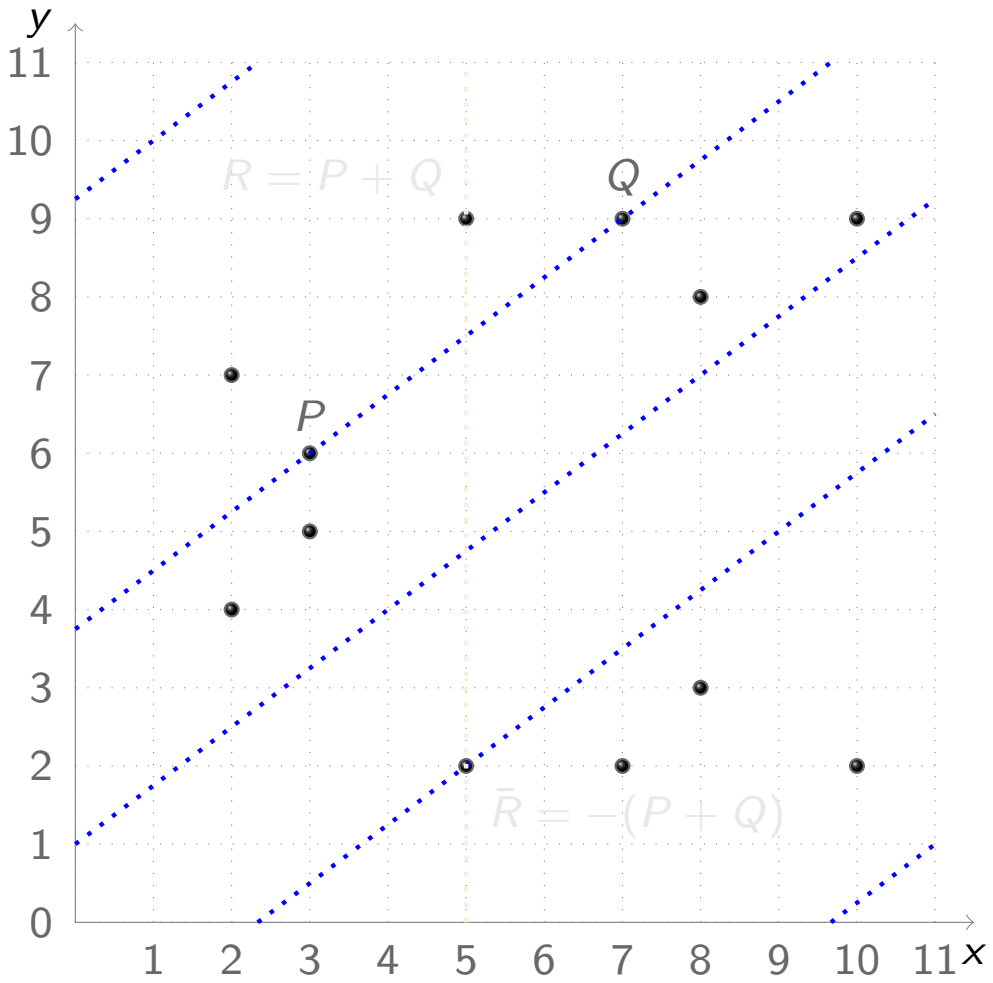


Figure : Courbe $y^2 = x^3 + x + 6$ sur $\mathbb{F}_{11}$

Loi de groupe sur $\mathbb{F}_p$

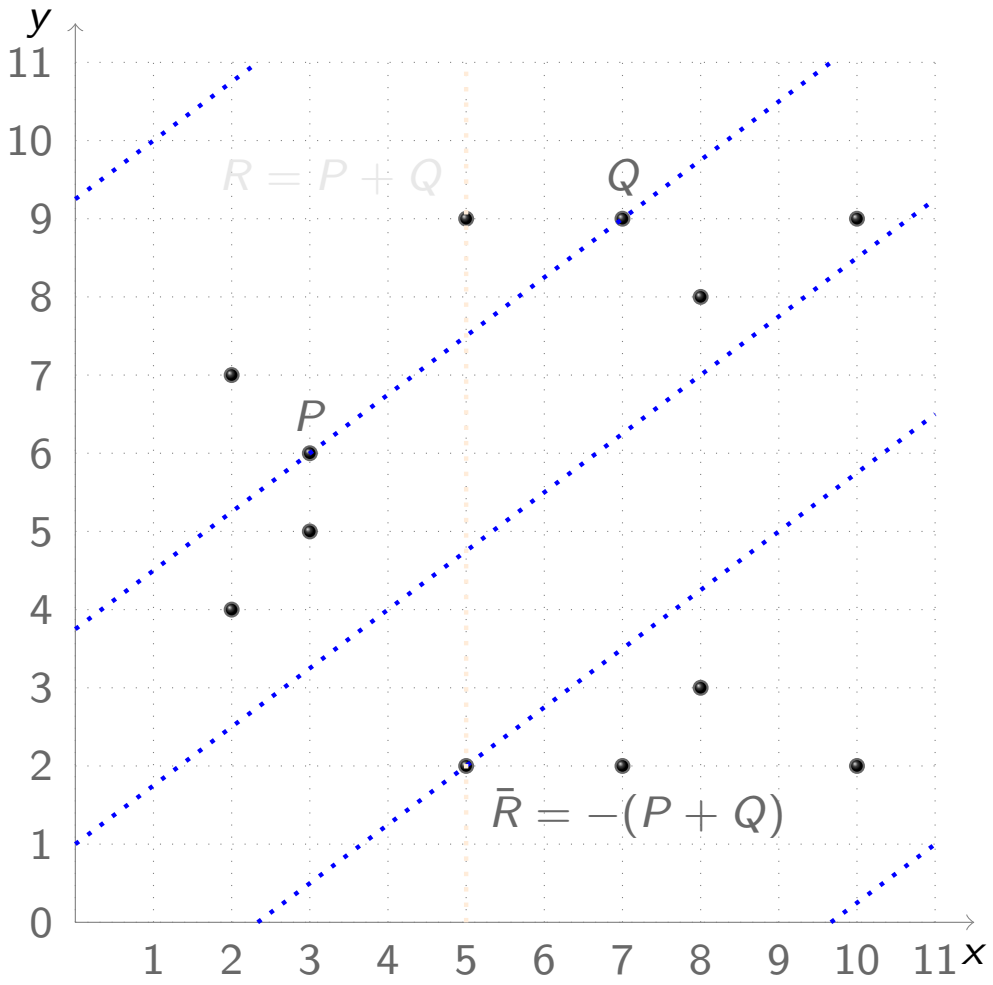


Figure : Courbe $y^2 = x^3 + x + 6$ sur $\mathbb{F}_{11}$

Loi de groupe sur $\mathbb{F}_p$

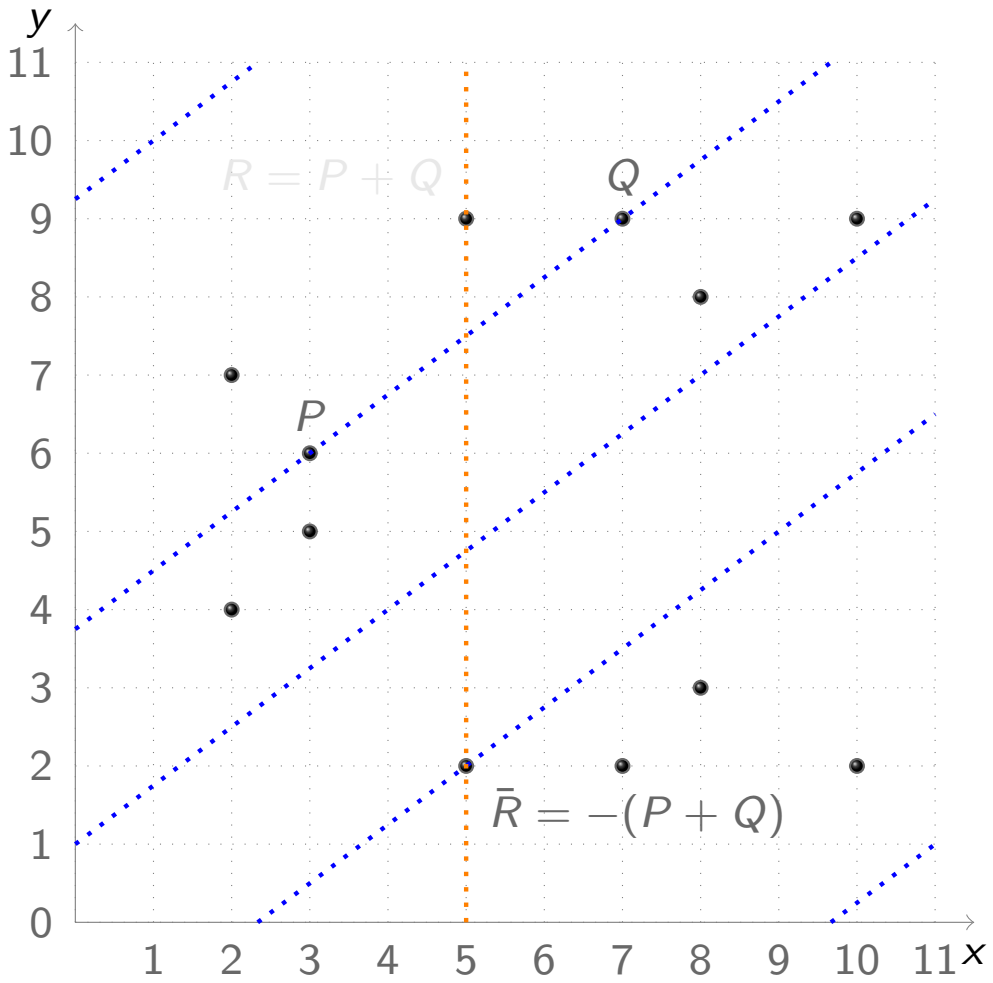


Figure : Courbe $y^2 = x^3 + x + 6$ sur $\mathbb{F}_{11}$

Loi de groupe sur $\mathbb{F}_p$

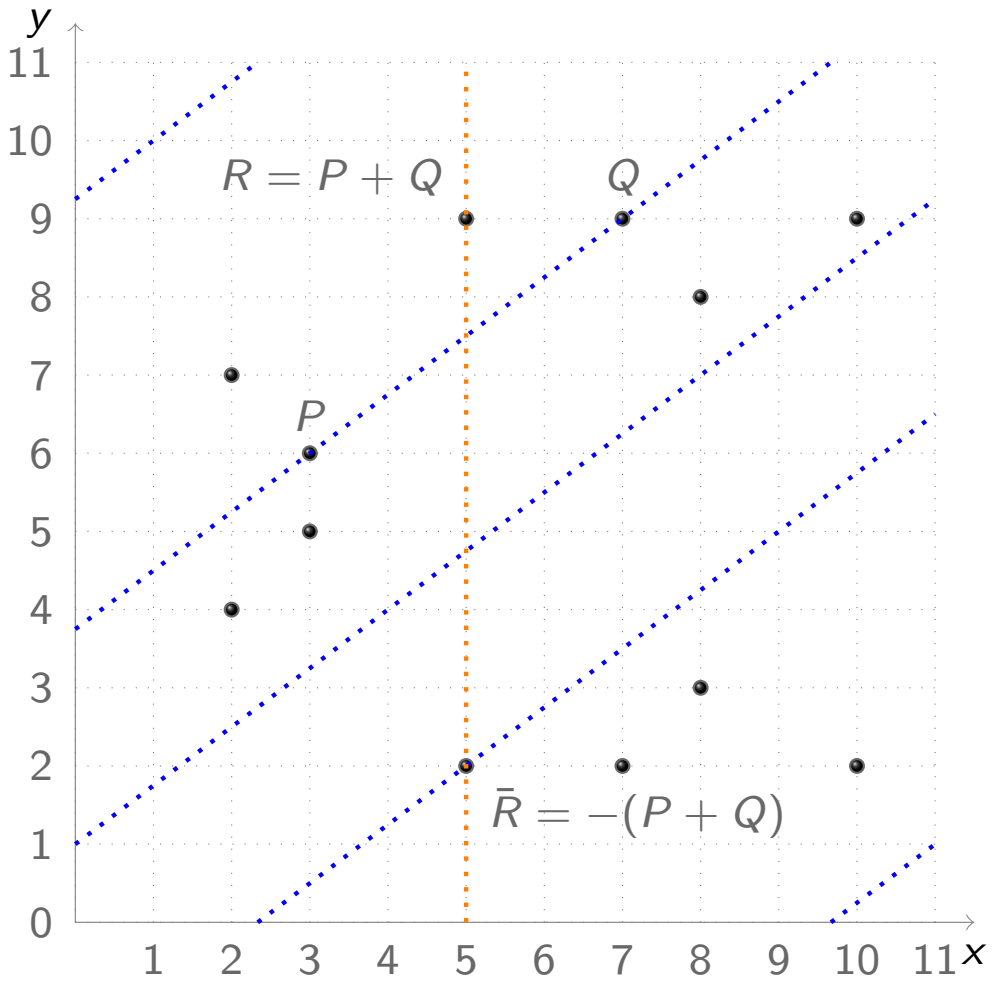


Figure : Courbe $y^2 = x^3 + x + 6$ sur $\mathbb{F}_{11}$

Le groupe $E(\mathbb{F}_{11})$

- En rajoutant le point à l'infini $\mathcal{O}$ on obtient 13 points sur la courbe E
- Le groupe est d'ordre premier et donc est engendré par n'importe quel élément non nul
- Par exemple prenons $P = (2, 7)$ comme générateur on a

$$E(\mathbb{F}_{11}) = \{[i]P : i = 0 \dots 12\}.$$

Notation

Le groupe $(\mathbb{F}_p^*, \times)$ est noté multiplicativement $(G = \{\alpha^i\})$ alors que le groupe des points d'une courbe elliptique est noté, par convention, additivement.

Le groupe $E(\mathbb{F}_{11})$

- En rajoutant le point à l'infini $\mathcal{O}$ on obtient 13 points sur la courbe E
- Le groupe est d'ordre premier et donc est engendré par n'importe quel élément non nul
- Par exemple prenons $P = (2, 7)$ comme générateur on a

$$E(\mathbb{F}_{11}) = \{[i]P : i = 0 \dots 12\}.$$

Notation

Le groupe $(\mathbb{F}_p^*, \times)$ est noté multiplicativement $(G = \{\alpha^i\})$ alors que le groupe des points d'une courbe elliptique est noté, par convention, additivement.

Nombre de points d'un courbe elliptique

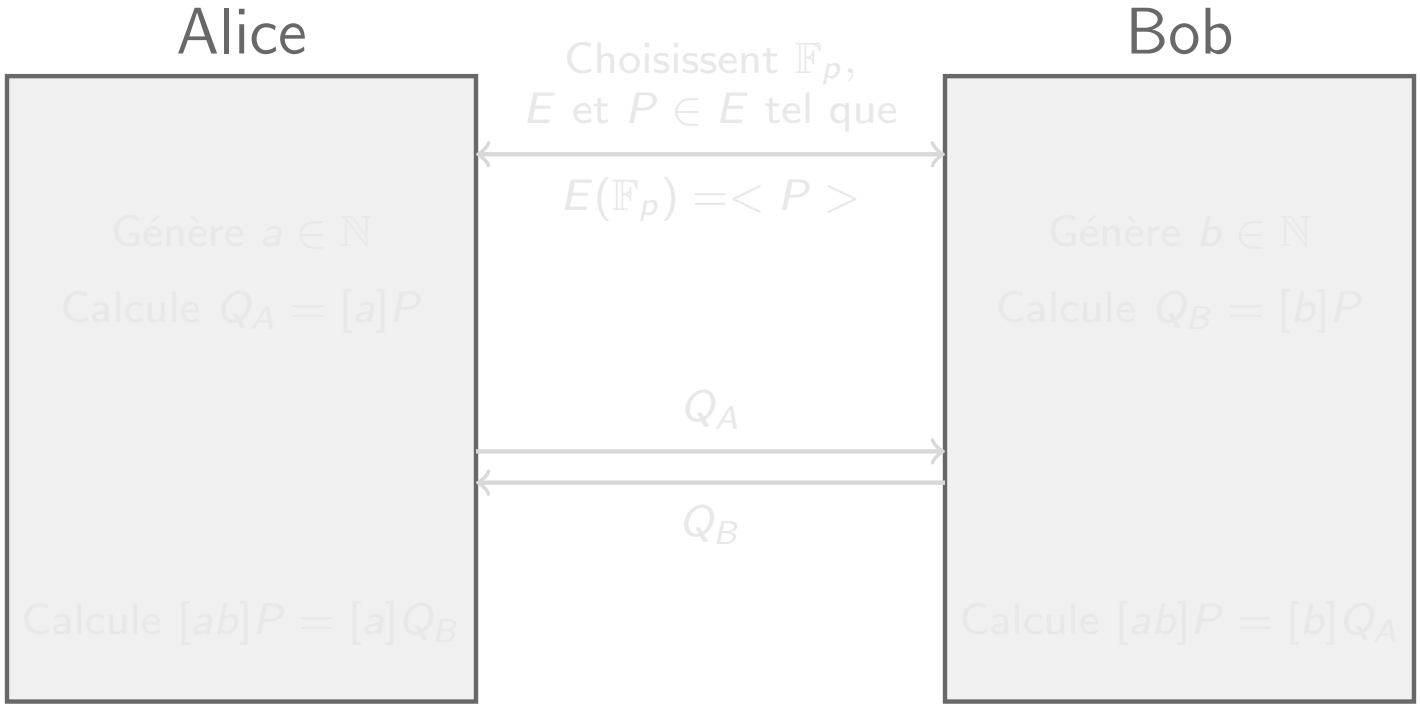
Théorème

Soit E une courbe elliptique définie sur un corps fini $\mathbb{F}_q$. L'ordre du groupe $E(\mathbb{F}_q)$, noté $\#E(\mathbb{F}_q)$, vérifie:

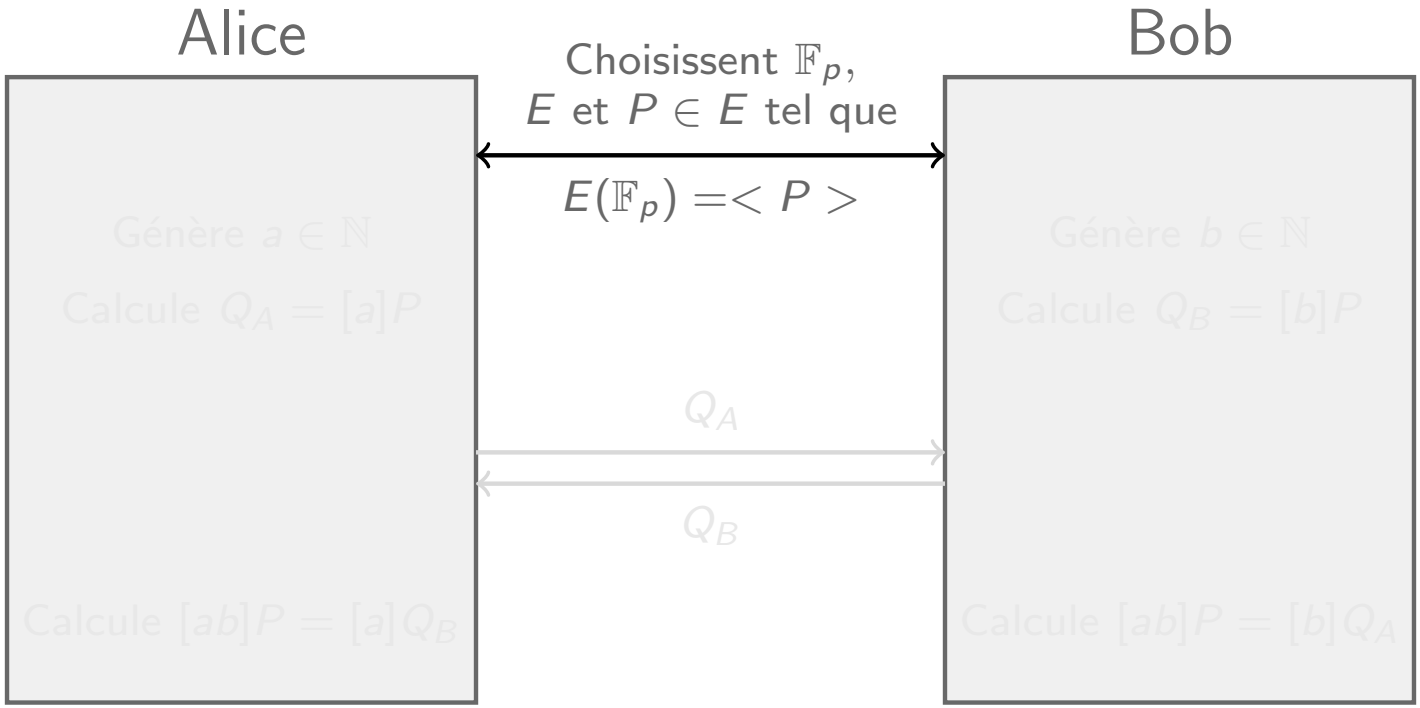
$$q + 1 - 2\sqrt{q} \leq \#E(\mathbb{F}_q) \leq q + 1 + 2\sqrt{q}.$$

- Une courbe sur $\mathbb{F}_q$ possède, environ, q points
- Il n'existe pas d'algorithme sous exponentiel pour résoudre le PLD sur une courbe bien choisie
- C'est donc un objet particulièrement intéressant pour la cryptographie

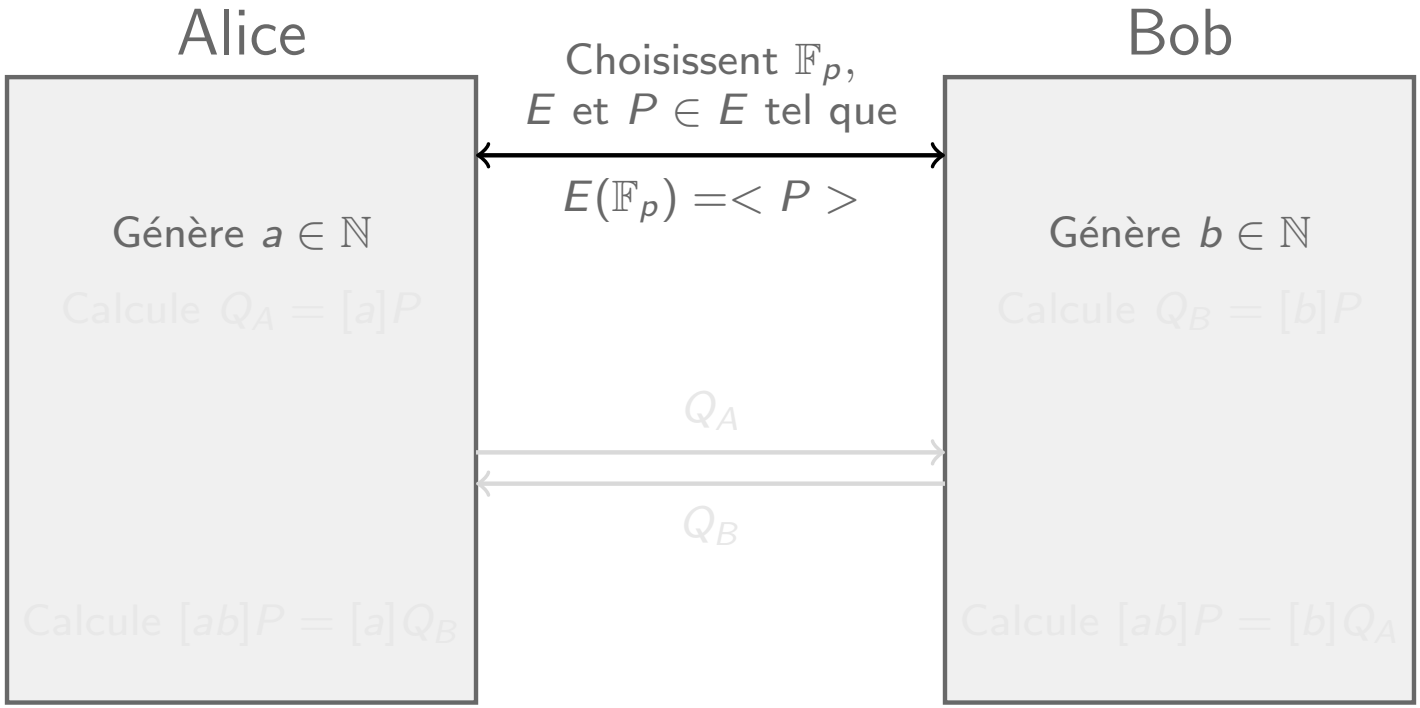
Protocole de Diffie-Hellman avec ECC



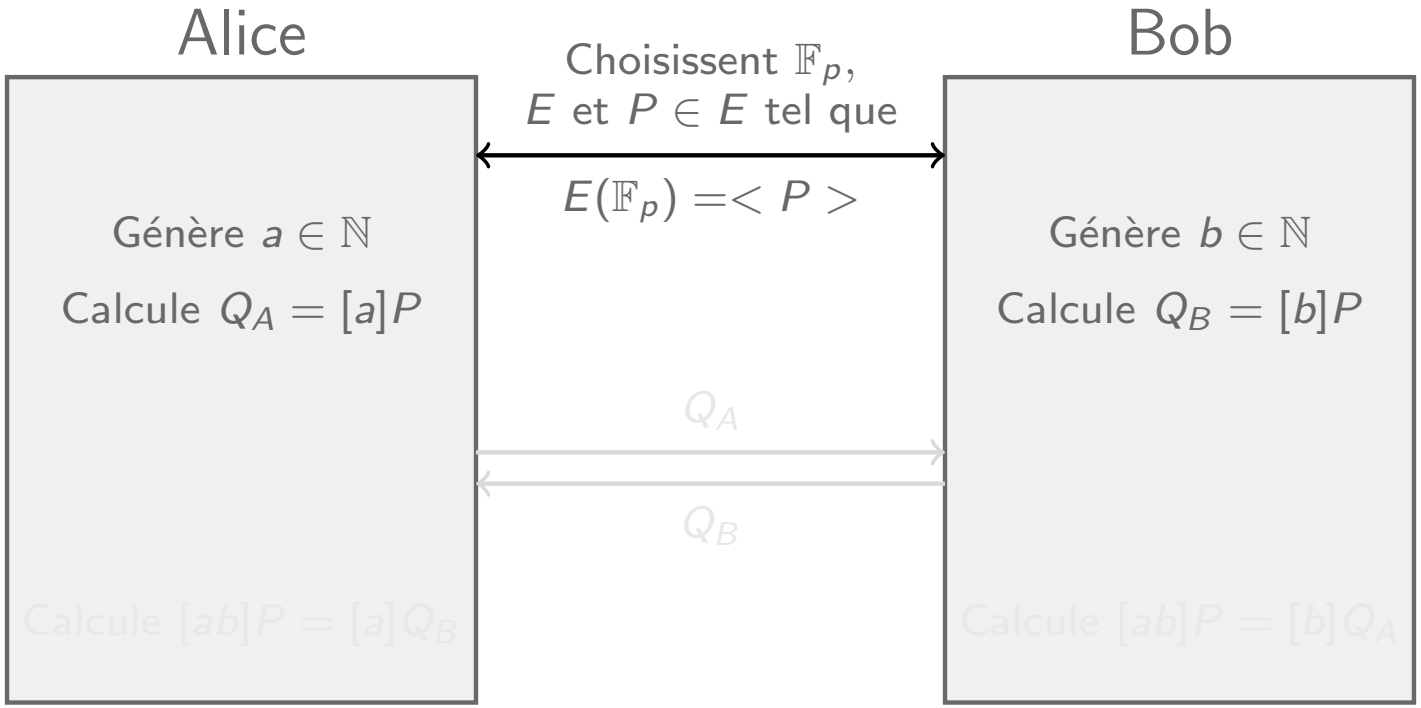
Protocole de Diffie-Hellman avec ECC



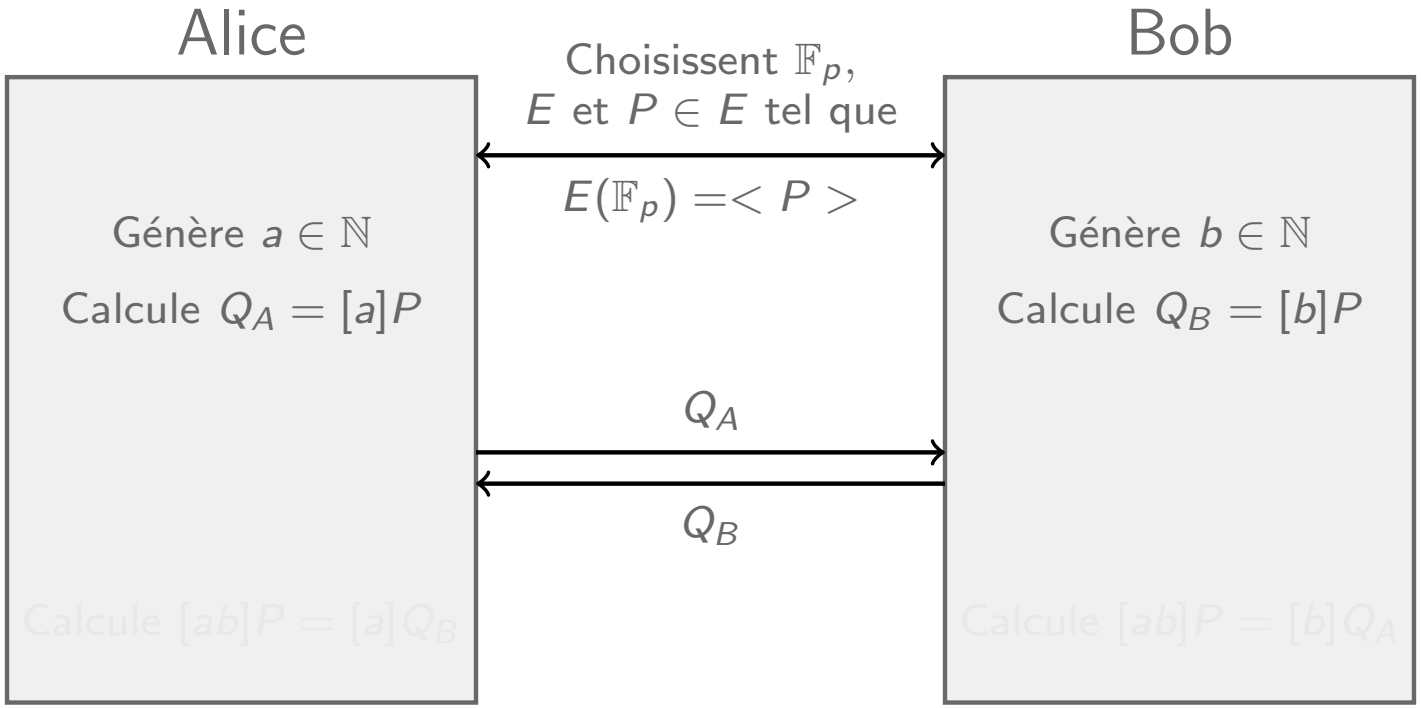
Protocole de Diffie-Hellman avec ECC



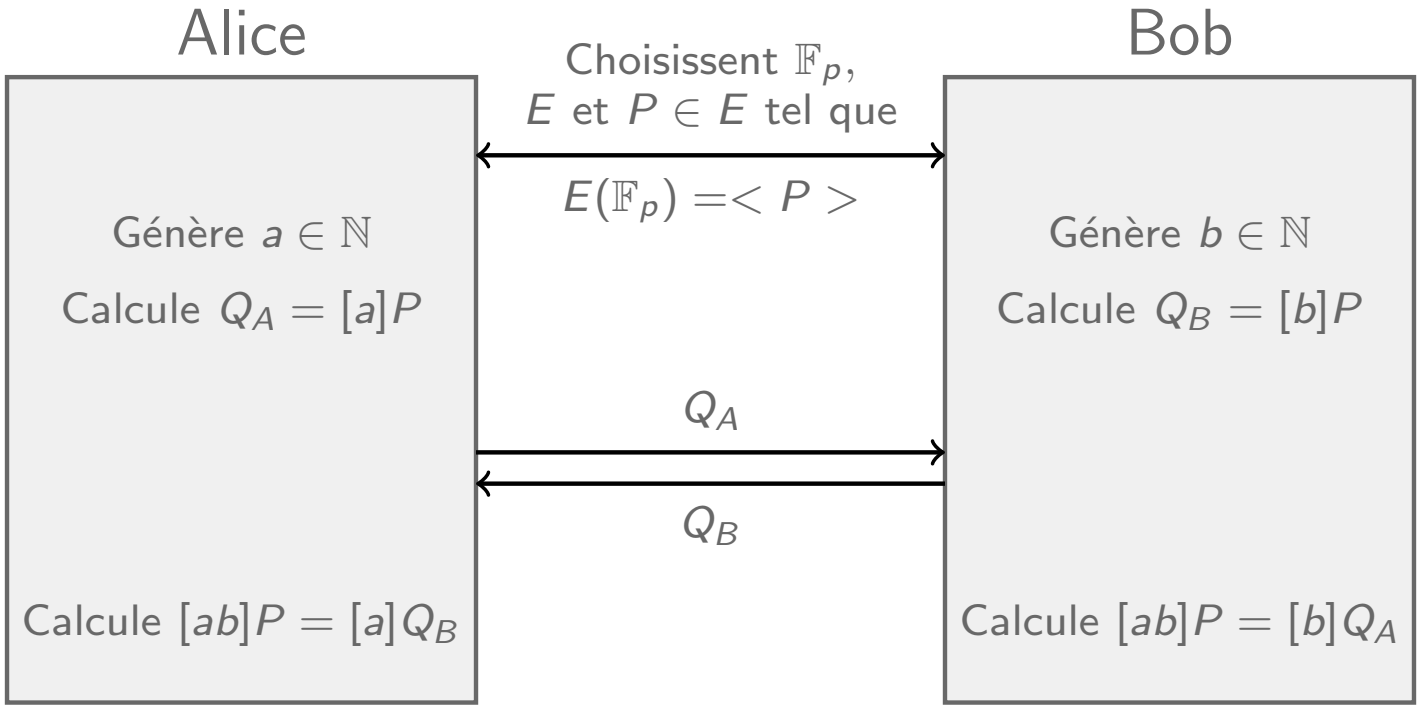
Protocole de Diffie-Hellman avec ECC



Protocole de Diffie-Hellman avec ECC



Protocole de Diffie-Hellman avec ECC



Le cryptosystème

Soit $E(\mathbb{F}_p)$ une courbe elliptique d'ordre premier n. Soient $P, Q \in E(\mathbb{F}_p)$ deux points tels que $Q = [k]P$. On définit:

$$\begin{aligned} \mathcal{P} &= E(\mathbb{F}_p) \\ \mathcal{C} &= E(\mathbb{F}_p) \times E(\mathbb{F}_p) \\ K_{pub} &= (E(\mathbb{F}_p), P, Q) \\ K_{sec} &= k \end{aligned}$$

Le cryptosystème El Gamal

Chiffrement

So it $M \in E(\mathbb{F}_p)$,

$$E(K_{pub}, M) = (P_1, P_2)$$

où $P_1 = [r]P, P_2 = M + [r]Q$ et r est un entier généré aléatoirement.

Déchiffrement

Le chiffré est $C = (P_1, P_2)$,

$$D(K_{sec}, C) = P_2 - [k]P1.$$

Compression de point

- Un chiffré contient deux points soit 4 coordonnées, on utilise l'équation de la courbe pour limiter la bande passante

Compression

$\texttt{Compress}(P = (x, y)) = (x, y \mod 2)$

Décompression

$\texttt{Decompress}(x, i)$:

- $z \leftarrow x^3 + ax + b$
- $y \leftarrow \sqrt{z} \mod p$
- si $y \equiv i \mod p$ on retourne (x, y) et $(x, p - y)$ sinon

Paramètres

- Message: $m \in \mathbb{F}_p^*$
- Clé publique: $E(\mathbb{F}_p)$ d'ordre n, $P, Q \in E(\mathbb{F}_p)$
- Clé privée: k tel que $P = [k]Q$

Chiffrement

- r généré aléatoirement
- $E(K_{pub}, m) = (\texttt{Compress}([r]P), x_q m \mod p))$ où $[r]Q = (x_q, y_q)$ et $x_q \neq 0$

Déchiffrement

- Chiffré $C = (c_1, c_2)$
- $D(K_{pri}, C) = c_2(x_q)^{-1} \mod p$ où $(x_q, y_q) = [k]\texttt{Decompress}(c_1)$

Sécurité des primitives à clé publique

Compléxité des meilleures attaques

- AES-n: $O(n)$
- ECC sur $\mathbb{F}_p$: $O(\sqrt{p})$
- DLP sur $\mathbb{F}_p^*$: $O(L_p[1/2, 1])$
- RSA-n: $O(L_n[1/3, 1.92])$

Niveau de sécurité

Sécurité (bits)	AES	ECC	RSA	$\mathbb{F}_p^*$
80	80	160	1024	1024
128	128	256	3072	3072
256	256	512	15360	15360