Définition mathématique des couplages

Nadia El Mrabet

GREYC−LMNO−Université de Caen, France

Ecole « Code et Cryptographie », ENSIAS de Rabat−MAROC,
Semaine du 8 au 14 mars 2010.

Plan de la présentation

Outline

Qu'est ce qu'un couplage ?

Propriétés

Soit G_1, G_2 et G_3 trois groupes de même ordre r, et un couplage

$$e : G_1 \times G_2 \longrightarrow G_3$$

vérifiant les propriétés de

- *non dégénérescence ;*
- *bilinéarité.*

Conséquences

$$\forall j \in \mathbb{N}, e([j]P, Q) = e(P, Q)^j = e(P, [j]Q)$$

Suite des festivités

Les couplages dans tout leur état

Dans la suite, nous allons commencer à entrer dans le vif du sujet

- Définition mathématiques des couplages
- Exemple et calcul de couplages
- Optimisation des couplages Mathématiques et Arithmétique
- Attaques par canaux cachés : SPA, attaque par faute, DPA
- Application au couplage
- Perspective de la recherche à base de couplage.

Suite des festivités

Les couplages dans tout leur état

Dans la suite, nous allons commencer à entrer dans le vif du sujet

- Définition mathématiques des couplages

Références

- Finite Fields de R. Lidl and H. Niederreiter,
- The arithmetic of elliptic curves deJ. H. Silverman.

Outline

Les corps finis

Introduction

- Soit p un nombre premier, nous noterons $\mathbb{F}_p$ le **corps fini** à p éléments.
- Il est isomorphe à $\mathbb{Z}/p\mathbb{Z} = \{0, 1, 2, \ldots, p-2, p-1\}$.
- $\mathbb{F}_p$ est un corps premier de caractéristique p.
- Nous notons $\mathbb{F}_p^\star$ le sous ensemble de $\mathbb{F}_p$ composé des éléments inversibles pour la loi $\times$ dans $\mathbb{F}_p$, il s'agit du sous groupe multiplicatif de $\mathbb{F}_p$.

Propriété

Le sous groupe $\mathbb{F}_p^\star$ est cyclique, il admet donc un élément g tel que n'importe lequel des éléments de $\mathbb{F}_p^\star$ soit une puissance de g ; g est appelé un générateur de $\mathbb{F}_p^\star$.

Les corps finis

Introduction

Le calcul des couplages repose sur l'arithmétique des corps finis. En particulier, de nombreuses démonstrations de théorèmes reposent sur le petit théorème de Fermat :

Petit théorème de Fermat

Soit p un nombre premier et x un entier non nul dans $\mathbb{F}_p$. Alors les égalités suivantes sont vraies :

$$\begin{aligned} x^p &\equiv x \bmod p, \\ \text{si } x \neq 0 \bmod p,\ x^{(p-1)} &\equiv 1 \bmod p. \end{aligned}$$

L'**ordre d'un élément** x est le plus petit entier α tel que $x^\alpha \equiv 1 \bmod(p)$. Les générateurs de $\mathbb{F}_p^\star$ sont les éléments de $\mathbb{F}_p$ d'ordre $p-1$.

Les corps finis

Polynôme irréductible

Nous notons $\mathbb{F}_p[X]$ l'ensemble des polynômes à coefficients dans $\mathbb{F}_p$; nous aurons en particulier besoin de la notion de polynômes irréductibles :

Définition

Un **polynôme** $P(X)$ de degré n est dit **irréductible** sur $\mathbb{F}_p$ si $P(X)$ n'est divisible par aucun polynôme $Q(X)$ de degré compris entre 1 et $(n-1)$.

Exemple

Soit $p = 257$, le corps fini $\mathbb{F}_{257}$ est défini comme étant l'ensemble des entiers compris entre 0 et 256. Le polynôme $P(X) = X^4 - 3$ est un polynôme irréductible sur $\mathbb{F}_{257}$. En effet, P est de degré 4. Donc si P était réductible, P s'écrirait soit comme le produit d'un polynôme de degré 1 et d'un polynôme de degré 3 soit comme le produit de deux polynômes de degré 2. La suite en exercice.

Les corps finis

Extension de corps

L'arithmétique des couplages nécessite de construire des extensions de $\mathbb{F}_p$. Une extension de $\mathbb{F}_p$ peut être vue comme un corps plus gros englobant $\mathbb{F}_p$, la définition suivante donne une représentation classique d'une telle extension de corps.

Définition

Une **extension de degré k du corps fini** $\mathbb{F}_p$, notée $\mathbb{F}_{p^k}$, est un corps fini que nous pouvons construire par le quotient $\mathbb{F}_p[X]/(P(X)\mathbb{F}_p[X])$ où $\mathbb{F}_p[X]$ est l'ensemble des polynômes à coefficients dans $\mathbb{F}_p$, $P(X)$ est un polynôme irréductible sur $\mathbb{F}_p$ de degré k et $P(X)\mathbb{F}_p[X]$ est l'ensemble des polynômes admettant $P(X)$ comme facteur (ou divisible par $P(X)$).

Une extension de degré k de $\mathbb{F}_p$ peut donc être décrite comme l'ensemble des polynômes à coefficients dans $\mathbb{F}_p$ et de degré strictement inférieur à k.

$$\mathbb{F}_{p^k} = \{R(X) \in \mathbb{F}_p[X], \text{ tel que } \deg(R) < k\}.$$

Les corps finis

Extension de corps

Il est possible de construire une **base** de $\mathbb{F}_{p^k}$. Notons γ une racine dans $\mathbb{F}_{p^k}$ de $P(X)$, polynôme irréductible de degré k, γ est une classe de X dans $\mathbb{F}_{p^k}$. Alors une base de $\mathbb{F}_{p^k}$ est composée des puissances de γ inférieures à k : $\{1, \gamma, \gamma^2, \ldots, \gamma^{k-1}\}$. Cette représentation permet de déduire directement le cardinal d'une extension de degré k du corps $\mathbb{F}_p$:

Propriété

Le cardinal de $\mathbb{F}_{p^k}$, noté $\#\mathbb{F}_{p^k}$, est p^k.

Les corps finis

Extension de corps

Les racines des polynômes de $\mathbb{F}_p[X]$ ne sont pas toutes contenues dans $\mathbb{F}_p$. Afin de décrire l'espace dans lequel elles évoluent nous devons introduire la notion de clôture algébrique d'un corps :

Définition

La clôture algébrique d'un corps fini $\mathbb{F}_p$ est l'extension de ce corps qui contient les racines de tous les polynômes de $\mathbb{F}_p[X]$. Nous la noterons $\overline{\mathbb{F}_p}$.

Remarque

Il n'y pas unicité de la clôture algébrique associée à un corps, mais elles sont toutes isomorphes.

Exemple

Le polynôme $P(X) = X^4 - 3$ est un polynôme irréductible sur $\mathbb{F}_{257}$.
Comme il s'agit d'un polynôme de degré 4 il nous permet de construire une extension $\mathbb{F}_{257^4}$ de degré 4 du corps fini $\mathbb{F}_{257}$.
Notons γ une racine dans $\mathbb{F}_{257^4}$ du polynôme $P(X) = X^4 - 3$. Nous pouvons alors décrire les éléments de $\mathbb{F}_{257^4}$ comme des polynômes en γ à coefficient dans $\mathbb{F}_{257^4}$:

$$\mathbb{F}_{257^4} \cong \left\{ a_0 + a_1\gamma + a_2\gamma^2 + a_3\gamma^3, \quad a_i \in \mathbb{F}_{257} \right\}.$$

Outline

Les courbes elliptiques

Définition

Une **courbe elliptique** E sur le corps $\mathbb{K}$ (notée $E(\mathbb{K})$) est définie par une équation de Weierstrass du type

$$y^2 + a_1xy + a_3y \quad = \quad x^3 + a_2x^2 + a_4x + a_6, \text{ pour } a_i \in \mathbb{K}. \qquad (1)$$

Une équation de Weierstrass définit bien une courbe elliptique s'il n'existe pas de point de $E(\overline{\mathbb{K}})$ pour lequel les dérivées partielles $(2y + a_1x + a_3)$ et $(3x^2 + 2a_2x + a_4 - a_1y)$ s'annulent simultanément. Les coordonnées (x, y) sont appelées **coordonnées affines** sur E.

Il est possible de décrire plus simplement une courbe elliptique, en utilisant une équation de Weierstrass réduite comme nous le montre le théorème suivant de :

Théorème

Soit $\mathbb{K}$ un corps fini de caractéristique différente de 2 et 3. Alors pour toute courbe elliptique $E(\mathbb{K})$ il existe un changement de variables tel que $E(\mathbb{K})$ admette une équation de Weierstrass réduite

$$y^2 = x^3 + ax + b.$$

Les courbes elliptiques

Loi de groupe

Soit $E(\mathbb{K})$ une courbe elliptique sur un corps $\mathbb{K}$.
Il existe une loi de groupe notée $+$ sur $E(\mathbb{K})$. Cette loi existe en toute caractéristique, mais nous ne considérons que les courbes elliptiques définies sur un corps de caractéristique différente de 2 et 3 et données par une équation réduite de Weierstrass. La loi de groupe repose sur le théorème suivant :

Théorème

Soit E un courbe elliptique et D une droite du plan. Si D est tangente en un point à la courbe E ou bien si D coupe E en deux points distincts ; alors D coupe E en un unique autre point.

La loi de groupe se décrit très bien de manière graphique.

Courbe elliptique

Représentation graphique

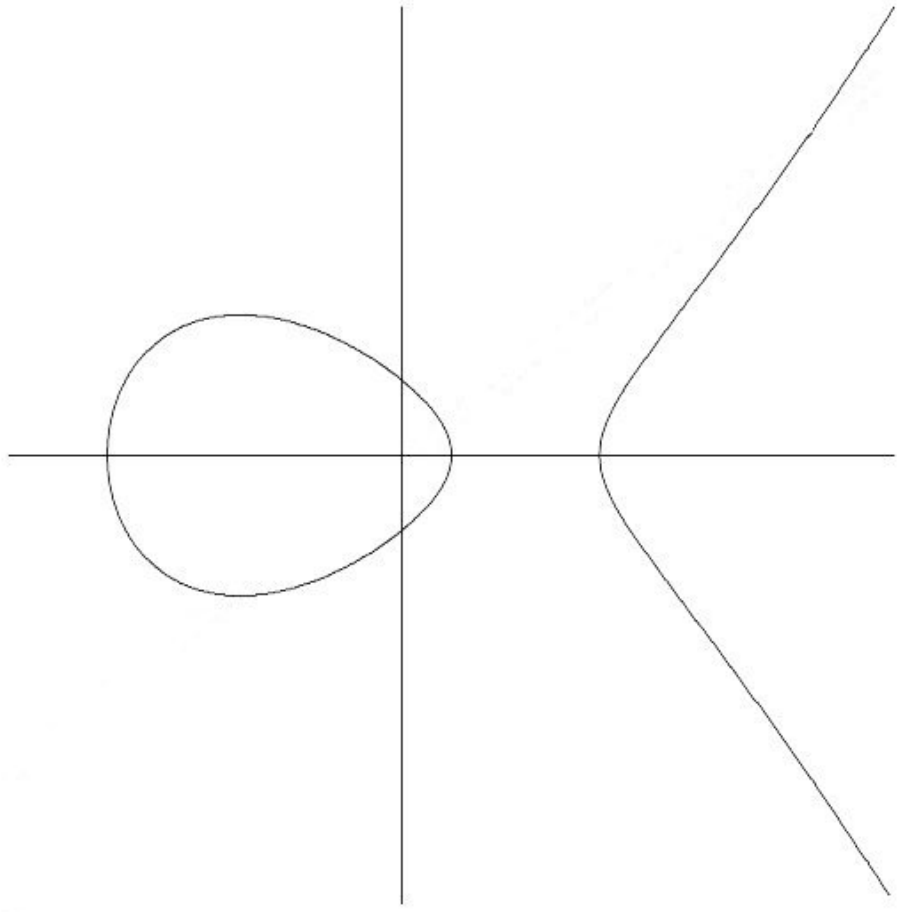
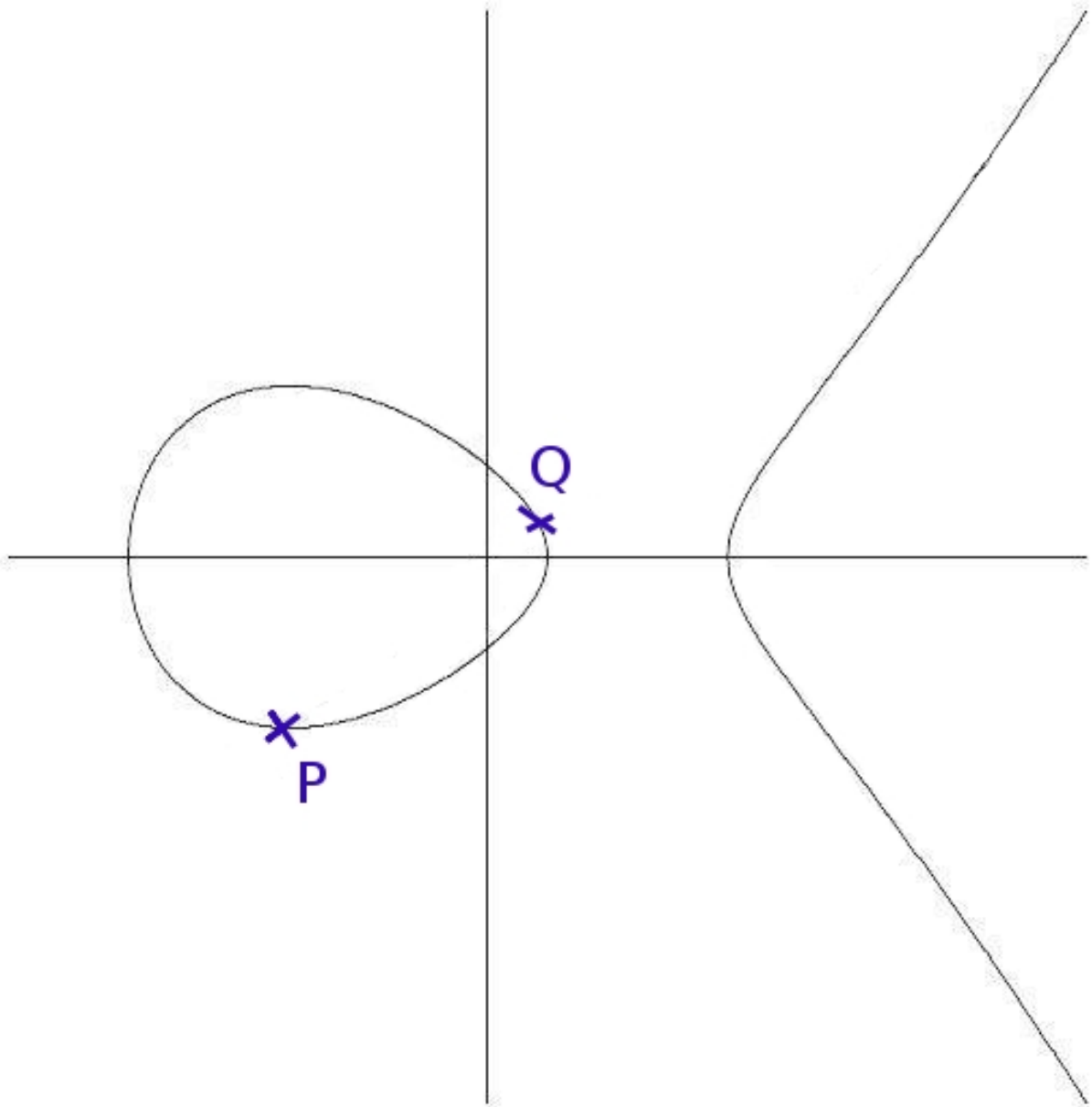


Figure: Courbe elliptique dans le plan réel

La courbe elliptique est munie d'une loi d'addition.

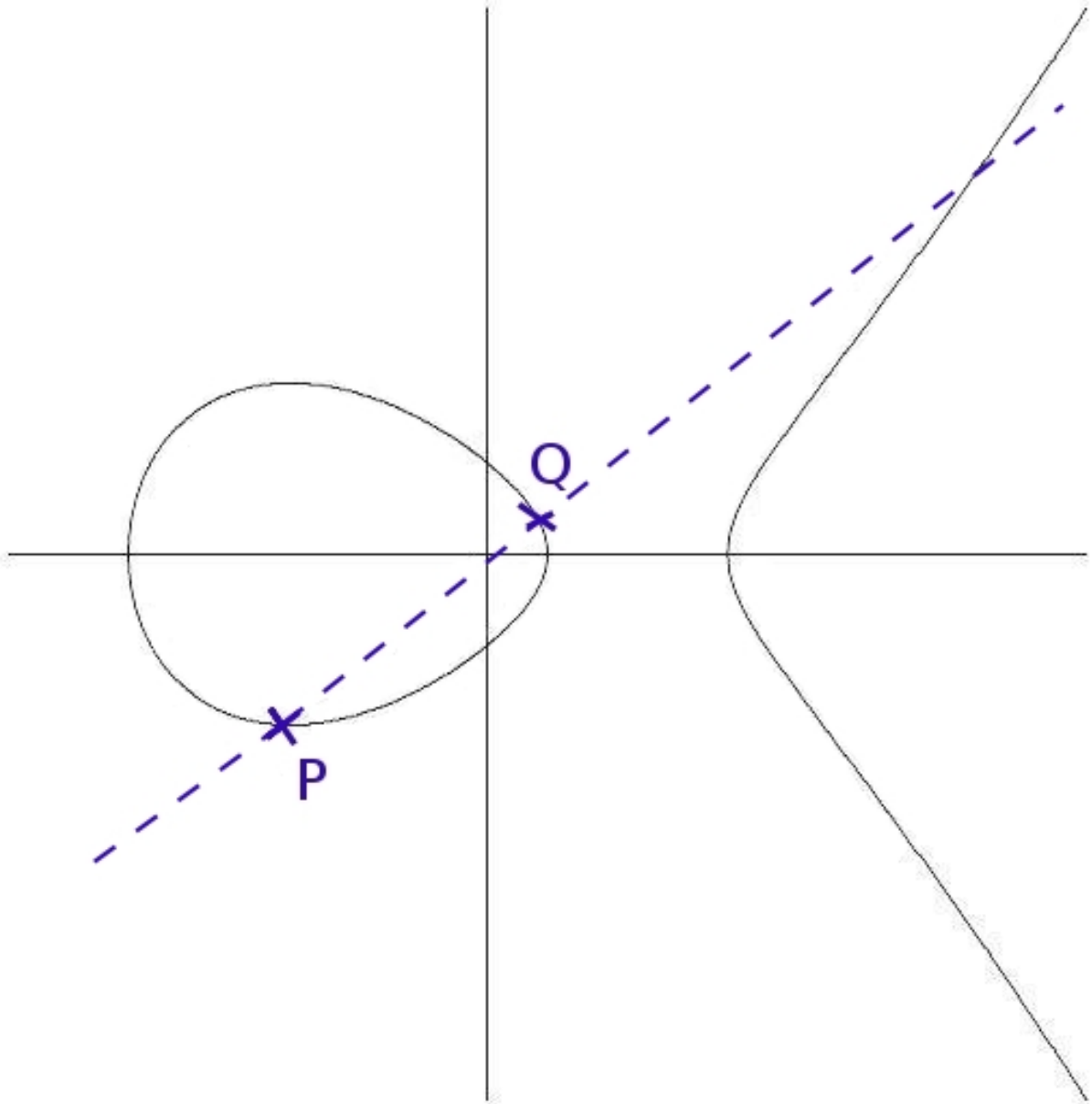
Courbe elliptique

Loi de groupe - Addition



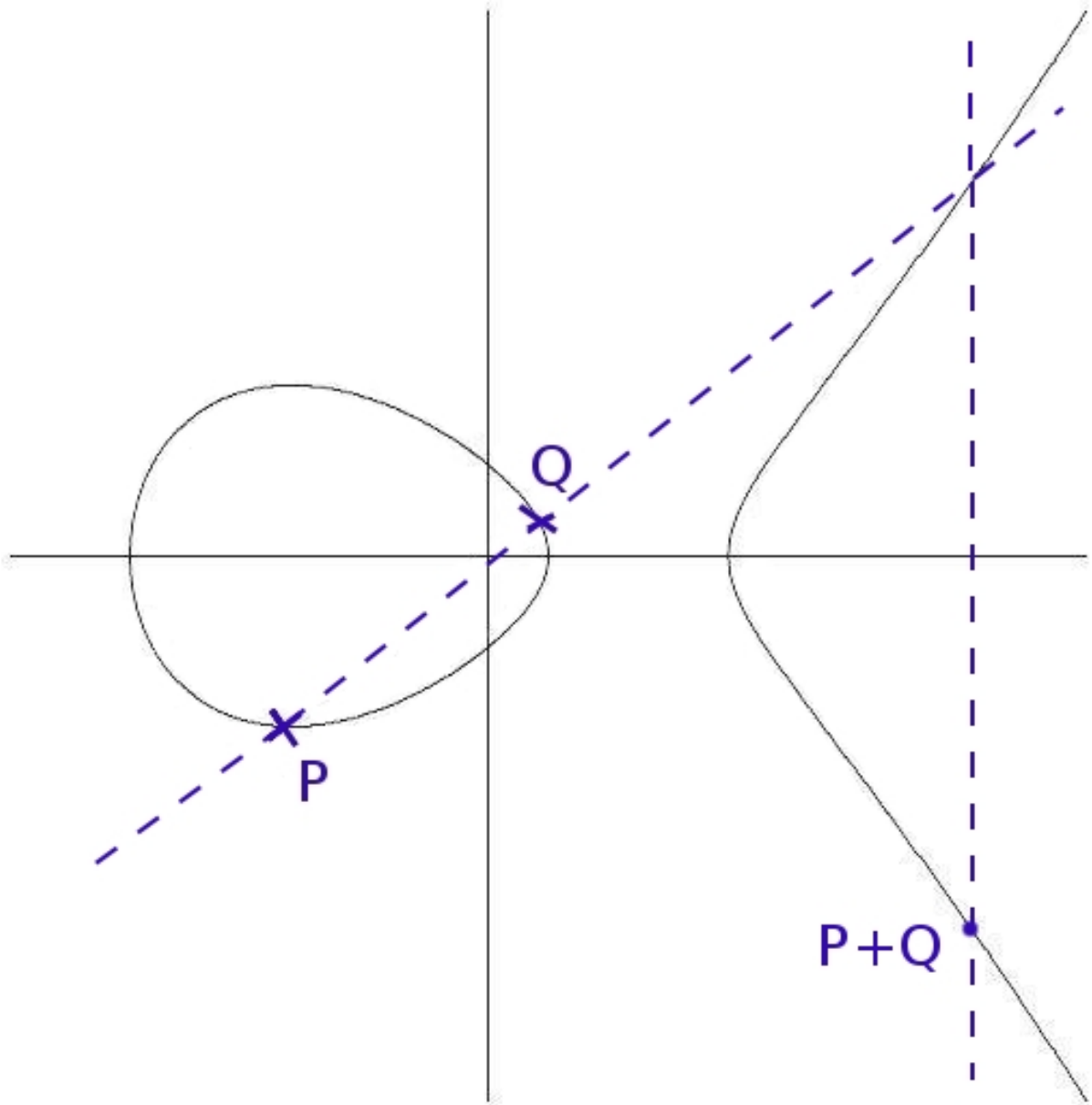
Courbe elliptique

Loi de groupe - Addition



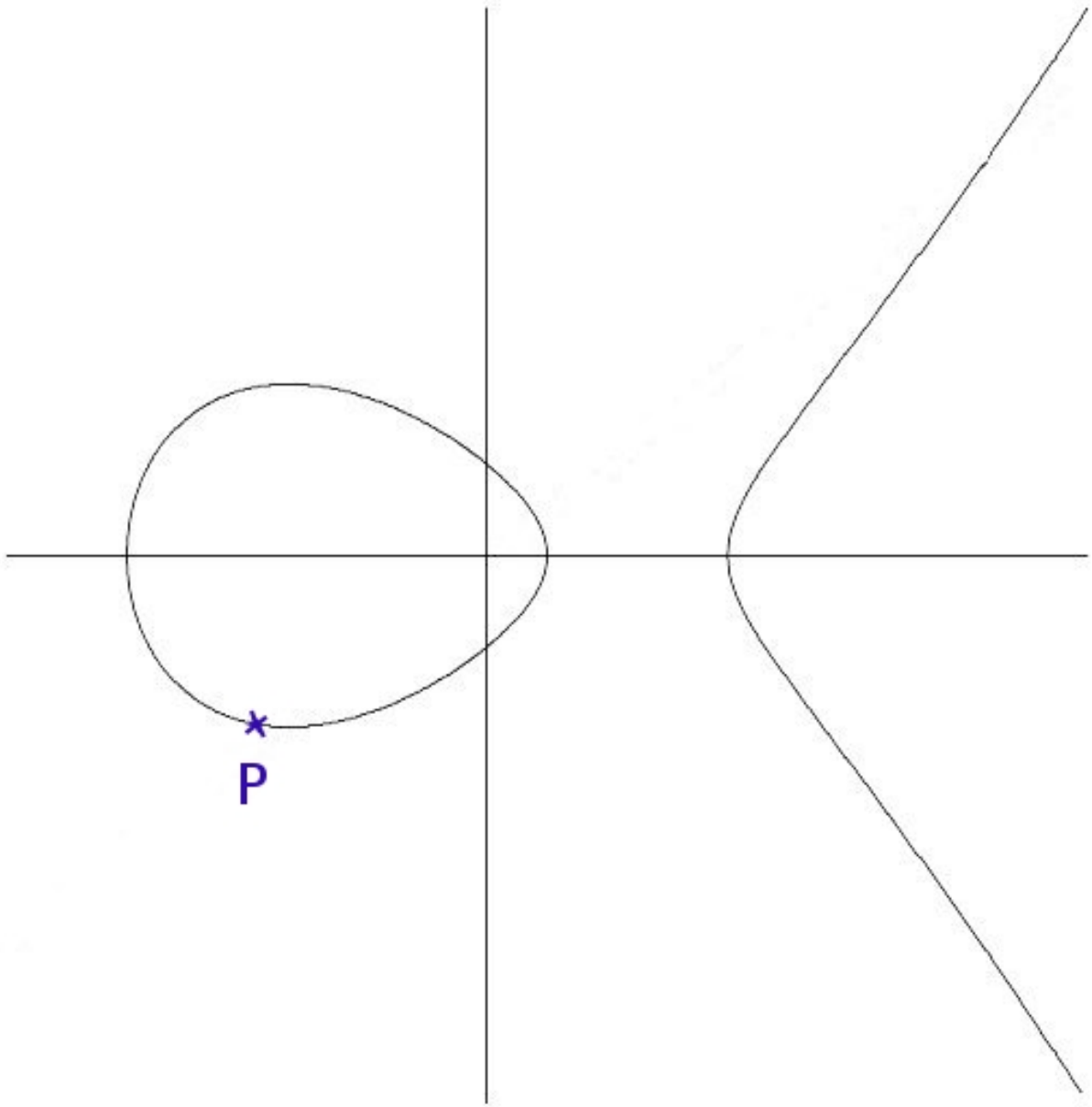
Courbe elliptique

Loi de groupe - Addition



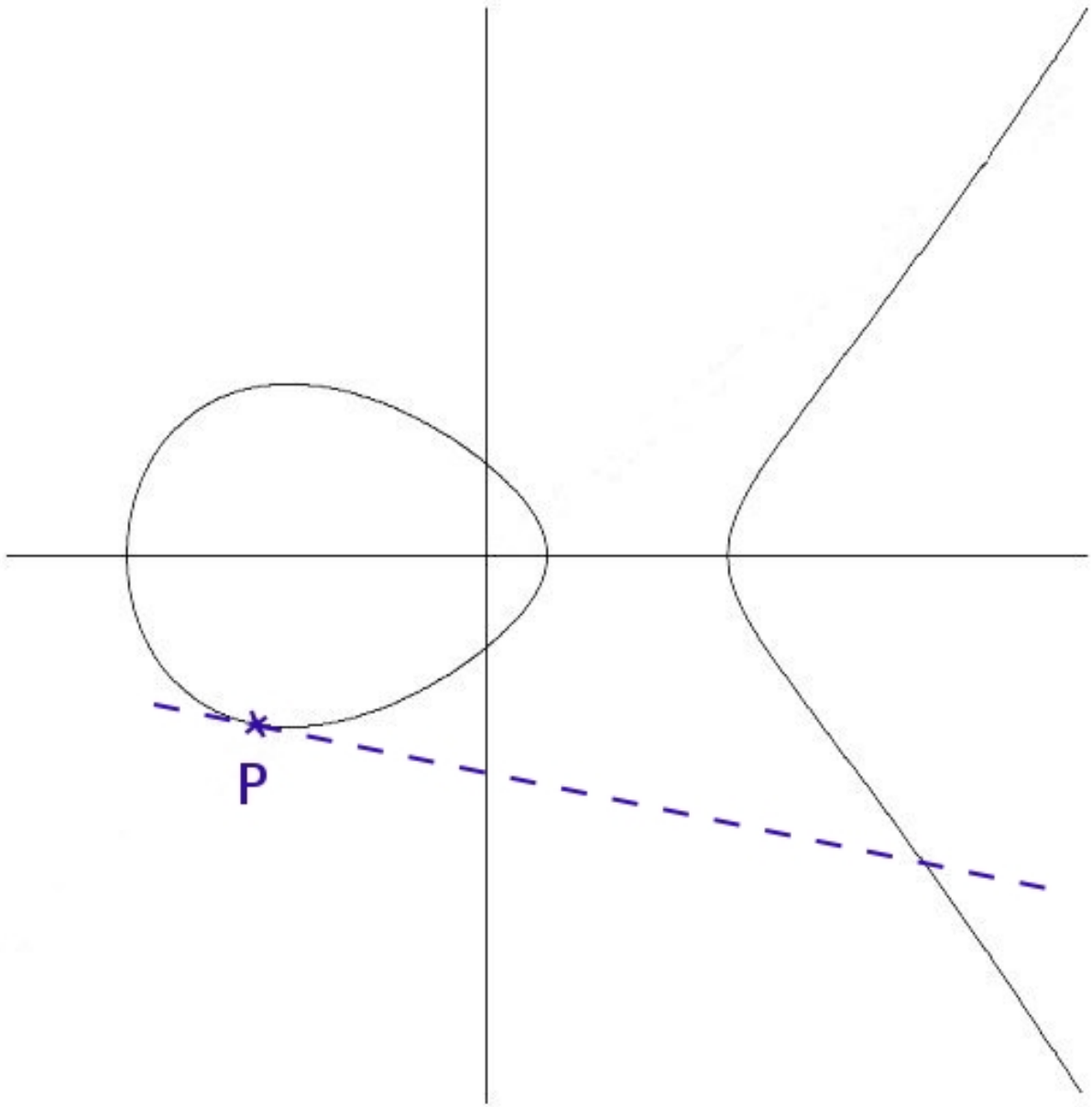
Courbe elliptique

Loi de groupe - Doublement



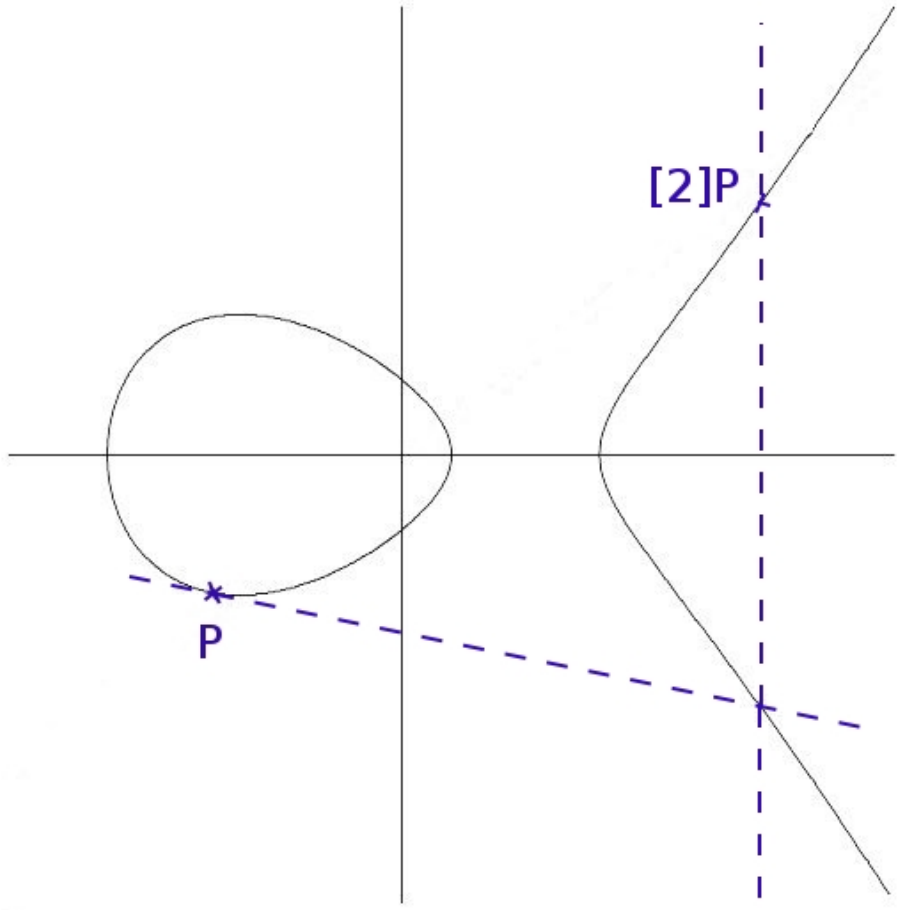
Courbe elliptique

Loi de groupe - Doublement



Courbe elliptique

Loi de groupe - Doublement



Par convention nous noterons $[r]P = \underbrace{P + P + \ldots + P}_{r \text{ fois}}$.

Cette construction nous permet d'assurer que le théorème suivant est vrai.

Théorème

L'ensemble des points d'une courbe elliptique E muni de la loi $+$ vérifie les propriétés suivantes :

(i) La loi $+$ est interne : $\forall P, Q \in E, P + Q \in E$.

(ii) Existence d'un élément neutre : $\forall P \in E,\ P + P_\infty = P$.

(iii) Commutativité de la loi $+$: $\forall P, Q \in E, P + Q = Q + P$.

(iv) La loi $+$ est associative :
$\forall P, Q, R \in E, (P + Q) + R = P + (Q + R)$.

(v) La loi $+$ est symétrique : $\forall P \in E$, il existe un point noté $-P$ tel que $P + (-P) = P_\infty$.

$(E(\mathbb{K}), +)$ est donc un groupe abélien additif d'élément neutre P_∞.

Les courbes elliptiques

Loi de groupe - Aspect algébrique

Nous pouvons décrire algébriquement la loi de groupe que nous venons de présenter graphiquement.
Soient P et Q deux points d'une même courbe elliptique.
Nous nous plaçons dans le plan affine sur $\mathbb{K} = \mathbb{R}$ pour écrire les équations de droites intervenant dans les constructions des points $P + Q$ et $[2]P$.
Ces équations de droites vont nous permettre de décrire par des formules explicites la loi de groupe d'une courbe elliptique.

Opposé d'un point

Soit E une courbe d'équation $y^2 = x^3 + ax + b$, $P = (x_P, y_P)$ et $Q = (x_Q, y_Q)$ deux éléments de $E(\mathbb{K})$. Les coordonnées du point $-P$ l'inverse du point P pour la loi $+$ peuvent s'exprimer en fonction des coordonnées de P.
L'opposé du point P, noté $-P$, admet pour coordonnées $(x_P, -y_P)$.

Cette propriété est une conséquence directe du fait que la droite $(P(-P))$ est une droite verticale. Le troisième point d'intersection de la courbe elliptique et de cette droite ne peut être que le point à l'infini. Ainsi, $P + (-P) = P_\infty$.

Les courbes elliptiques

Loi de groupe - Aspect algébrique

Soient $P = (x_P, y_P)$ et $Q = (x_Q, y_Q)$ deux points distincts d'une courbe elliptique $E(\mathbb{K})$ tels que $P \neq -Q$.
Pour trouver les formules donnant les coordonnées du point $R = P + Q$ avec $R = (x_R, y_R)$, nous cherchons à résoudre le système de deux équations formé par l'équation de la droite (PQ) et l'équation de la courbe elliptique. Ce système traduit exactement le fait que $-(P + Q)$ est le troisième point d'intersection de la courbe elliptique et de la droite (PQ). Nous obtenons les formules 2, où λ représente la pente de la droite (PQ) :

$$\begin{cases} \lambda &= \frac{y_P - y_Q}{x_P - x_Q} \\ x_R &= \lambda^2 - x_P - x_Q \\ y_R &= \lambda(x_P - x_R) - y_P \end{cases} \tag{2}$$

Les courbes elliptiques

Loi de groupe - Aspect algébrique

Pour trouver les formules donnant les coordonnées du point $R = [2]P$, nous utilisons le fait que $-[2]P$ est le second point d'intersection de la courbe E et de la tangente en E au point P. L'équation de la tangente et celle de la courbe elliptique forment un système dont la résolution nous donne les formules pour obtenir les coordonnées de point $R = [2]P$. Nous obtenons les formules 3, où λ représente la pente de la tangente au point P de la courbe elliptique :

$$\begin{cases} \lambda &= \frac{3x_P^2+a}{2y_P} \\ x_R &= \lambda^2 - 2x_P \\ y_R &= \lambda(x_P - x_R) - y_P \end{cases} \tag{3}$$

Les courbes elliptiques

Différents systèmes de coordonnées

Soit $P = (x_P, y_P)$ un point de la courbe elliptique $E : y^2 = x^3 + ax + b$.
Nous avons donné dans les parties précédentes les formules d'addition et de doublement de points en coordonnées affines.
Il existe d'autre types de coordonnées :

- projectives
- Jacobiennes,....

Les équations pour l'addition et le doublement s'adaptent à ces coordonnées.

Les courbes elliptiques

Différents systèmes de coordonnées

- Les **coordonnées projectives** du point P sont notées $(X_P : Y_P : Z_P)$,
  - $E : Y^2Z = X^3 + aXZ^2 + bZ^3$ Le point à l'infini est le point $(0 : 1 : 0)$.
  - pour α non nul le point $(X_P : Y_P : Z_P) \equiv (\alpha \times X_P : \alpha \times Y_P : \alpha \times Z_P)$.
  - Relation entre coordonnées affines et projectives
    $(X_P : Y_P : Z_P) \equiv (\frac{X_P}{Z_P}, \frac{Y_P}{Z_P})$, si $Z_P \neq 0$ et au point à l'infini sinon.
  - L'opposé du point $(X_P : Y_P : Z_P)$ est le point $(X_P : -Y_P : Z_P)$.

Les courbes elliptiques

Différents systèmes de coordonnées

- Les **coordonnées Jacobiennes** du point P sont notées $(X_P; Y_P; Z_P)$,
  - $E : Y^2 = X^3 + aXZ^4 + bZ^6$ Le point à l'infini est le point $(1 : 1 : 0)$.
  - pour α non nul le point $(X_P; Y_P; Z_P) \equiv (\alpha^2 \times X_P; \alpha^3 \times Y_P; \alpha \times Z_P)$
  - Relation entre coordonnées affines et jacobiennes
    $(X_P; Y_P; Z_P) \equiv (\frac{X_P}{Z_P^2}, \frac{Y_P}{Z_P^3})$, si $Z_P \neq 0$ et au point à l'infini sinon.
  - L'opposé du point $(X_P : Y_P : Z_P)$ est le point $(X_P : -Y_P : Z_P)$.

Les courbes elliptiques

Cardinalité et torsion

Le premier résultat intéressant concernant le cardinal d'une courbe elliptique est le théorème de Hasse.
Ce théorème donne un intervalle dans lequel se trouvent toutes les valeurs possibles du cardinal d'une courbe elliptique définie sur $\mathbb{F}_q$, pour $q = p^m$ avec p premier strictement supérieur à 3 et $m \in \mathbb{N}^\star$.
Nous noterons $\#E(\mathbb{F}_q)$ le cardinal de la courbe elliptique $E(\mathbb{F}_q)$.

Théorème de Hasse

Soit E une courbe elliptique définie sur un corps $\mathbb{F}_q$ alors

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

Il existe des algorithmes permettant de calculer le cardinal d'une courbe elliptique donnée, par exemple : l'algorithme de Schoof-Elkies-Atkin de complexité en $O((\log(q))^4)$ opérations. L'algorithme est implémenté dans les logiciels de calculs formels Magma et PariGP.

Les courbes elliptiques

Cardinalité et torsion

Soient E une courbe elliptique définie sur un corps $\mathbb{F}_q$ et r un entier. Nous définissons la notion de points de r-torsion de la courbe elliptique $E(\overline{\mathbb{F}_q})$ comme suit :

Définition

Un point P de la courbe elliptique $E(\overline{\mathbb{F}_q})$ est un **point de r-torsion** s'il vérifie la condition $[r]P = P_\infty$.

Exemple

Soit E la courbe elliptique d'équation $y^2 = x^3 + 1$ sur $\mathbb{F}_{257}$. Le cardinal de cette courbe est $258 = 2 \times 129$. La courbe admet donc deux sous groupes de torsion non triviaux, un d'ordre 2 et un d'ordre 129. Le point $P = (8, 16)$ est un point de E de 129-torsion. Le point $Q = (-1, 0)$ est un point de E de 2-torsion.

Afin de décrire tous les points de r-torsion, nous devons donc considérer la courbe elliptique définie sur la clôture algébrique de $\mathbb{F}_q$, notée $\overline{\mathbb{F}_q}$.

Remarque

Soit $E(\mathbb{F}_q)$ une courbe elliptique sur un corps fini $\mathbb{F}_q$, et r un entier.

- L'ensemble des points r-torsion appartient à $E(\overline{\mathbb{F}_q})$.
- L'ensemble des points de $E(\overline{\mathbb{F}_q})$ de r-torsion est le noyau de l'application $[r] : P \longrightarrow [r]P$:

$$E[r] = \left\{ P \in E(\overline{\mathbb{F}_q}), \text{ tel que } [r]P = P_\infty \right\}.$$

Les courbes elliptiques

Cardinalité et torsion

Nous connaissons la structure de l'ensemble des points de r-torsion :

Théorème

Soit r un entier premier avec p la caractéristique de $\mathbb{F}_q$. Alors

$$E[r] \cong \mathbb{Z}/r\mathbb{Z} \times \mathbb{Z}/r\mathbb{Z}.$$

Si p divise r alors r peut s'écrire sous la forme $r = p^\alpha n$, où p ne divise pas n et alors

$$E[r] \cong \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} \text{ ou } \mathbb{Z}/r\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}.$$

Corollaire

Pour r premier avec p et divisant $\#E(\mathbb{F}_q)$, nous déduisons du Théorème **??** que $\#E[r] = r^2$.

Pour décrire les points de $E[r]$ nous introduisons le degré de plongement de la courbe.

Les courbes elliptiques

Degré de plongement de la courbe

Définition

Soit $E(\mathbb{F}_q)$ une courbe elliptique, et r un diviseur premier de $\#E(\mathbb{F}_q)$. Le **degré de plongement** de la courbe elliptique E relativement à r est le plus petit entier k pour lequel r divise $(q^k - 1)$. Autrement dit, k est l'ordre de q dans $\mathbb{F}_r$.

Ce paramètre de la courbe permet de savoir dans quel groupe vivent les points de r-torsion comme le montre le théorème de Balasubramanian et Koblitz :

Théroème

Soit $E(\mathbb{F}_q)$ une courbe elliptique définie sur un corps fini $\mathbb{F}_q$, et r un diviseur de $\#E(\mathbb{F}_q)$. Si r est premier avec q et r ne divise pas $(q-1)$, alors $E[r] \subset E(\mathbb{F}_{q^n})$ pour n un entier positif si et seulement si r divise $(q^n - 1)$.

Les courbes elliptiques

Degré de plongement de la courbe

Structure des points de r-torsion

Le degré de plongement k est le degré de l'extension minimale du corps $\mathbb{F}_q$ telle que $E[r] \subset E(\mathbb{F}_{q^k})$. Si $k > 1$, nous savons donc que $E[r] \subset E(\mathbb{F}_{q^k})$. De plus, la structure des points de r-torsion est connue, il existe $P \in E(\mathbb{F}_q)$ et $Q \in E(\mathbb{F}_{q^k})$ tels que

$$E[r] = \left\{ iP + jQ, (i,j) \in \mathbb{Z}^2 \right\}.$$

Exemple

- Le sous groupe de 2-torsion de la courbe E d'équation $y^2 = x^3 + 1$ sur $\mathbb{F}_{257}$ admet un degré de plongement égal à 1. Il suffit de remarquer que 2 divise $257 - 1 = 256$.
- Le sous groupe de 129-torsion de la courbe E d'équation $y^2 = x^3 + 1$ sur $\mathbb{F}_{257}$ admet un degré de plongement égal à 2. En effet, 129 divise $(257^2 - 1)$ mais pas $257 - 1$.

Outline

Construction des couplages

Données

Afin de calculer un couplage, nous avons besoin de :

- Soit E une courbe elliptique sur un corps $\mathbb{K} \supset \mathbb{F}_p$, a et $b \in \mathbb{F}_p$:
  $E(\mathbb{K}) := \left\{(x, y) \in \mathbb{K} \times \mathbb{K},\ y^2 = x^3 + ax + b\right\} \cup \{P_\infty\}$.

Construction des couplages

Données

Afin de calculer un couplage, nous avons besoin de :

- Soit E une courbe elliptique sur un corps $\mathbb{K} \supset \mathbb{F}_p$, a et $b \in \mathbb{F}_p$:
  $E(\mathbb{K}) := \left\{(x, y) \in \mathbb{K} \times \mathbb{K},\ y^2 = x^3 + ax + b\right\} \cup \{P_\infty\}$.

- r un nombre premier divisant $\text{card}(E(\mathbb{F}_p))$,
  ainsi que l'ensemble : $E[r] = \left\{P \in E(\overline{\mathbb{F}_p}), [r]P = P_\infty\right\}$.

Construction des couplages

Données

Afin de calculer un couplage, nous avons besoin de :

- Soit E une courbe elliptique sur un corps $\mathbb{K} \supset \mathbb{F}_p$, a et $b \in \mathbb{F}_p$:
  $E(\mathbb{K}) := \left\{(x, y) \in \mathbb{K} \times \mathbb{K},\ y^2 = x^3 + ax + b\right\} \cup \{P_\infty\}$.

- r un nombre premier divisant $\mathrm{card}(E(\mathbb{F}_p))$,
  ainsi que l'ensemble : $E[r] = \left\{P \in E(\overline{\mathbb{F}_p}), [r]P = P_\infty\right\}$.

- Le degré de plongement k : le plus petit entier tel que $r | (p^k - 1)$;
  Si $k > 1$ alors $E[r] \subset E(\mathbb{F}_{p^k})$.

Construction des couplages

Données

Afin de calculer un couplage, nous avons besoin de :

- Soit E une courbe elliptique sur un corps $\mathbb{K} \supset \mathbb{F}_p$, a et $b \in \mathbb{F}_p$:
  $E(\mathbb{K}) := \left\{(x, y) \in \mathbb{K} \times \mathbb{K},\ y^2 = x^3 + ax + b\right\} \cup \{P_\infty\}$.

- r un nombre premier divisant $\text{card}(E(\mathbb{F}_p))$,
  ainsi que l'ensemble : $E[r] = \left\{P \in E(\overline{\mathbb{F}_p}), [r]P = P_\infty\right\}$.

- Le degré de plongement k : le plus petit entier tel que $r|(p^k - 1)$;
  Si $k > 1$ alors $E[r] \subset E(\mathbb{F}_{p^k})$.

- La fonction de Miller notée $f_{r,P}$ qui admet :
  le point P comme zéro d'ordre r
  le point $[r]P$ comme pôle.

Construction des couplages

Données

- Soient $E : y^2 = x^3 + ax + b$ une courbe elliptique définie sur $\mathbb{F}_p$ et r un facteur premier du cardinal de $E(\mathbb{F}_p)$.

- Afin d'éviter que toute la r-torsion soit dans $E(\mathbb{F}_p)$, nous demandons de plus que r^2 ne divise pas le cardinal de $E(\mathbb{F}_p)$, noté $\#E(\mathbb{F}_p)$. Cette condition est facilement réalisable en pratique. Nous savons que les points de r-torsion de la courbe elliptique vérifient que $E[r] \subset E(\mathbb{F}_{p^k})$, où k est le degré de plongement de la courbe relativement au facteur r.

- Nous noterons $\mathbb{G}_1 = E(\mathbb{F}_p)[r]$,
- $\mathbb{G}_2 \subset E(\mathbb{F}_{p^k})[r]$ et
- $\mathbb{G}_3 = \left\{\mu \in \mathbb{F}_{p^k} \text{ tel que } \mu^r = 1 \text{ dans } \mathbb{F}_{p^k}\right\}$, il s'agit du sous-groupe des racines r-ième de l'unité.

Construction des couplages

Le couplage de Weil

Soit $P \in E(\mathbb{F}_p)[r]$, $Q \in E(\mathbb{F}_{p^k})/rE(\mathbb{F}_{p^k})$ et k le degré de plongement de la courbe relativement à r.

$$\begin{array}{rcl} e_W : \mathbb{G}_1 \times \mathbb{G}_2 & \longrightarrow & \mathbb{G}_3, \\ (P, Q) & \longrightarrow & (-1)^r \frac{f_{r,P}(Q)}{f_{r,Q}(P)} \end{array}$$

Construction des couplages

Le couplage de Tate

Soit $P \in E(\mathbb{F}_p)[r]$, $Q \in E(\mathbb{F}_{p^k})/rE(\mathbb{F}_{p^k})$ et k le degré de plongement de la courbe relativement à r.

Construction des couplages

Le couplage de Tate

Soit $P \in E(\mathbb{F}_p)[r]$, $Q \in E(\mathbb{F}_{p^k})/rE(\mathbb{F}_{p^k})$ et k le degré de plongement de la courbe relativement à r.

Le couplage de Tate est l'application :

$$e_T : E(\mathbb{F}_p)[r] \times E(\mathbb{F}_{p^k})/rE(\mathbb{F}_{p^k}) \longrightarrow \mathbb{F}_{p^k}^*$$

$$(P, Q) \longrightarrow f_{r,P}(Q)^{\frac{p^k-1}{r}}$$

L'égalité de Miller

La fonction $f_{r,P}$

Le calcul des couplages nécessite la construction d'une fonction rationnelle $f_{r,P}$ pour r un entier naturel.
Cette fonction admet le point P comme zéro d'ordre r et le point $[r]P$ comme pôle.

Victor Miller a établi l'égalité :

$$f_{i+j,P} = f_{i,P} \times f_{j,P} \times \frac{l_{[i]P,[j]P}}{v_{[i+j]P}}$$

Cette égalité nous permet de construire une suite de fonction admettant le point $[i]P$ comme pôle pour i allant de 1 à r.

L'égalité de Miller

Exemple

Nous voulons calculer $f_{5,P}$ en utilisant sa décomposition binaire :
$5 = (101)_2$

et un algorithme de doublement et addition :

L'égalité de Miller

Exemple

Nous voulons calculer $f_{5,P}$ en utilisant sa décomposition binaire :
$5 = (101)_2$

et un algorithme de doublement et addition :

- Nous partons de $i = 1$,
- Le deuxième bit de 5 est 0 :

  $i := 2 \times i \qquad \Rightarrow \qquad i = 2$

L'égalité de Miller

Exemple

Nous voulons calculer $f_{5,P}$ en utilisant sa décomposition binaire :
$5 = (101)_2$

et un algorithme de doublement et addition :

- Nous partons de $i = 1$,
- Le deuxième bit de 5 est 0 :

  $i := 2 \times i \qquad \Rightarrow \qquad i = 2$
- Le troisième bit de 5 est 1 :

  $i := 2 \times i \qquad \Rightarrow \qquad i = 4$

  $i := i + 1 \qquad \Rightarrow \qquad i = 5$

Sur ce modèle, nous allons calculer $f_{5,P}$ en utilisant l'égalité de Miller et la décomposition binaire de 5.

L'égalité de Miller

Exemple

Soit $f_{1,P}$ qui vaut 1 par construction des fonctions $f_{i,P}$ et $i = 1$.

- $i := 2i \quad (i = 2)$
- $f_{2,P} = f_{1,P} \times f_{1,P} \times \frac{l_{P,P}}{v_{[2]P}}$
- $f_{2,P} = \frac{l_{P,P}}{v_{[2]P}}$

L'égalité de Miller

Exemple

Soit $f_{1,P}$ qui vaut 1 par construction des fonctions $f_{i,P}$ et $i = 1$.

- $i := 2i \quad (i = 2)$
- $f_{2,P} = f_{1,P} \times f_{1,P} \times \frac{l_{P,P}}{v_{[2]P}}$
- $f_{2,P} = \frac{l_{P,P}}{v_{[2]P}}$

- $i := 2i \quad (i = 4)$
- $f_{4,P} = f_{2,P} \times f_{2,P} \times \frac{l_{[2]P,[2]P}}{v_{[4]P}}$
- $f_{4,P} = f_{2,P}^2 \times \frac{l_{[2]P,[2]P}}{v_{[4]P}}$

- $i := i + 1 \quad (i = 5)$
- $f_{5,P} = f_{4,P} \times \frac{l_{[4]P,P}}{v_{[5]P}}$

L'égalité de Miller

Exemple

Soit $f_{1,P}$ qui vaut 1 par construction des fonctions $f_{i,P}$ et $i = 1$.

- $i := 2i \quad (i = 2)$
- $f_{2,P} = f_{1,P} \times f_{1,P} \times \frac{l_{P,P}}{v_{[2]P}}$
- $f_{2,P} = \frac{l_{P,P}}{v_{[2]P}}$

- $i := 2i \quad (i = 4)$
- $f_{4,P} = f_{2,P} \times f_{2,P} \times \frac{l_{[2]P,[2]P}}{v_{[4]P}}$
- $f_{4,P} = f_{2,P}^2 \times \frac{l_{[2]P,[2]P}}{v_{[4]P}}$

- $i := i + 1 \quad (i = 5)$
- $f_{5,P} = f_{4,P} \times \frac{l_{[4]P,P}}{v_{[5]P}}$

$$f_{5,P} = \left(\left(\frac{l_{P,P}}{v_{[2]P}} \right)^2 \times \frac{l_{[2]P,[2]P}}{v_{[4]P}} \right) \times \frac{l_{[4]P,P}}{v_{[5]P}}$$

Calcul des couplages

L'algorithme de Miller renvoie $f_{r,P}(Q)$

Data: $r = (r_N \dots r_0)_2$,
$P \in \mathbb{G}_1 \subset E(\mathbb{F}_p)[r]$

Result: $[r]P$

$T \leftarrow P$

for $i = N - 1$ **to** 0 **do**

  $T \leftarrow [2]T$

  if $r_i = 1$ **then**

    $T \leftarrow T + P$

  end

end

return $T = [r]P$

Calcul des couplages

L'algorithme de Miller renvoie $f_{r,P}(Q)$

Data: $r = (r_N \dots r_0)_2$,
$P \in \mathbb{G}_1 \subset E(\mathbb{F}_p)[r]$ et
$Q \in \mathbb{G}_2 \subset E(\mathbb{F}_{p^k})[r]$
Result: $f_{r,P}(Q) \in \mathbb{G}_3 \subset \mathbb{F}^*_{p^k}$
$T \leftarrow P$, $f_1 \leftarrow 1$, $f_2 \leftarrow 1$
for $i = N - 1$ **to** 0 **do**
  $T \leftarrow [2]T$
  if $r_i = 1$ **then**
    $T \leftarrow T + P$
  end
end
return $\frac{f_1}{f_2}$

Calcul des couplages

L'algorithme de Miller renvoie $f_{r,P}(Q)$

Data: $r = (r_N \dots r_0)_2$,
$P \in \mathbb{G}_1 \subset E(\mathbb{F}_p)[r]$ et
$Q \in \mathbb{G}_2 \subset E(\mathbb{F}_{p^k})[r]$

Result: $f_{r,P}(Q) \in \mathbb{G}_3 \subset \mathbb{F}^*_{p^k}$

$T \leftarrow P$, $f_1 \leftarrow 1$, $f_2 \leftarrow 1$

for $i = N - 1$ **to** 0 **do**

  $T \leftarrow [2]T$

  $f_1 \longleftarrow {f_1}^2 \times l_d(Q)$

  $f_2 \longleftarrow {f_2}^2 \times v_d(Q)$

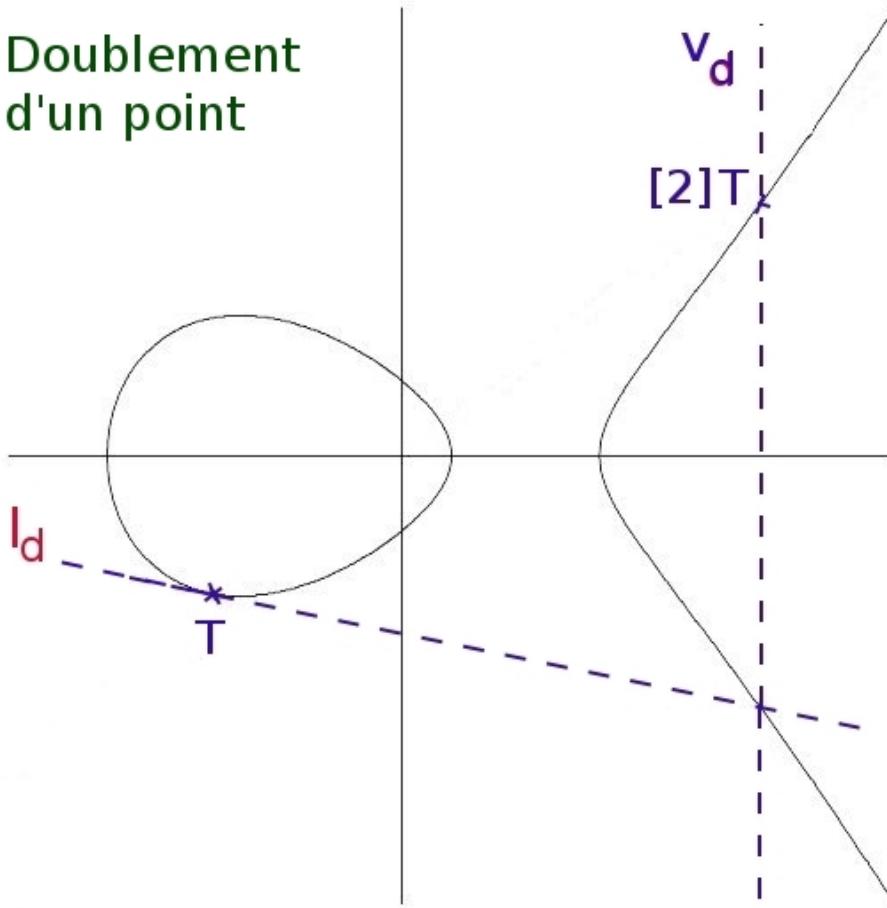
  if $r_i = 1$ **then**

    $T \leftarrow T + P$

  end

end

return $\frac{f_1}{f_2}$



Calcul des couplages

L'algorithme de Miller renvoie $f_{r,P}(Q)$

Data: $r = (r_N \dots r_0)_2$,
$P \in \mathbb{G}_1 \subset E(\mathbb{F}_p)[r]$ et
$Q \in \mathbb{G}_2 \subset E(\mathbb{F}_{p^k})[r]$

Result: $f_{r,P}(Q) \in \mathbb{G}_3 \subset \mathbb{F}^*_{p^k}$

$T \leftarrow P$, $f_1 \leftarrow 1$, $f_2 \leftarrow 1$

for $i = N - 1$ **to** 0 **do**

  $T \leftarrow [2]T$

  $f_1 \longleftarrow {f_1}^2 \times l_d(Q)$

  $f_2 \longleftarrow {f_2}^2 \times v_d(Q)$

  if $r_i = 1$ **then**

    $T \leftarrow T + P$

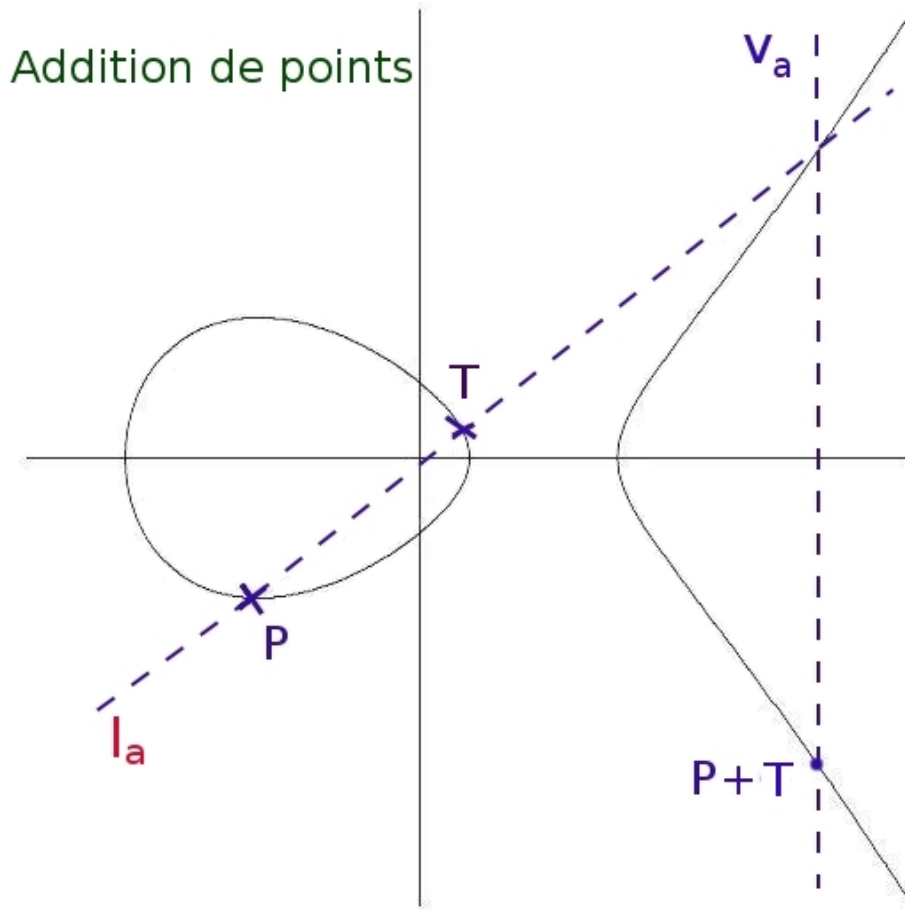
    $f_1 \longleftarrow f_1 \times l_a(Q)$

    $f_2 \longleftarrow f_2 \times v_a(Q)$

  end

end

return $\frac{f_1}{f_2}$



Calcul des couplages

L'algorithme de Miller renvoie $f_{r,P}(Q)$

Data: $r = (r_N \dots r_0)_2$,
$P \in \mathbb{G}_1 \subset E(\mathbb{F}_p)[r]$ et
$Q \in \mathbb{G}_2 \subset E(\mathbb{F}_{p^k})[r]$
Result: $f_{r,P}(Q) \in \mathbb{G}_3 \subset \mathbb{F}^*_{p^k}$
$T \leftarrow P$, $f_1 \leftarrow 1$, $f_2 \leftarrow 1$
for $i = N - 1$ **to** 0 **do**
  $T \leftarrow [2]T$
  $f_1 \longleftarrow {f_1}^2 \times l_d(Q)$
  $f_2 \longleftarrow {f_2}^2 \times v_d(Q)$
  if $r_i = 1$ **then**
    $T \leftarrow T + P$
    $f_1 \longleftarrow f_1 \times l_a(Q)$
    $f_2 \longleftarrow f_2 \times v_a(Q)$
  end
end
return $\frac{f_1}{f_2}$

Calcul des couplages

La sécurité des couplages

Niveau de sécurité en bits	80	128	192	256
Nombre minimal de bits de r	160	256	384	512
Nombre minimal de bits de p^k	1 024	3 072	7 680	15 360

Table: Niveau de sécurité

Suite des festivités

Les couplages dans tout leur état

Dans la suite, nous allons commencer à entrer dans le vif du sujet

- Définition mathématiques des couplages (Fait !)
- Exemple et calcul de couplages (Fait !)
- Optimisation des couplages Mathématiques et Arithmétique
- Attaques par canaux cachés : SPA, attaque par faute, DPA
- Application au couplage
- Perspective de la recherche à base de couplage.