N° d'ordre: 05/2012-M/MT

REPUBLIQUE ALGÉRIENNE DEMOCRATIQUE ET POPULAIRE
MINISTERE DE L'ENSEIGNEMENT SUPÉRIEURE ET
DE LA RECHERCHE SCIENTIFIQUE

UNIVERSITE DES SCIENCES ET DE LA TECHNOLOGIE
HOUARI BOUMEDIENE
Faculté de Mathématiques

Mémoire

Présenté pour l'obtention du diplôme de MAGISTER
EN : MATHÉMATIQUES
Spécialité : Algèbre et Théorie des Nombres

Par : Ourida BELKADI

Sujet :

Cryptographie basée sur les Couplages des Courbes Elliptiques

Soutenu publiquement le : 30 septembre 2012 , devant le Jury proposé de :

M Meziane AIDER	Professeur à l'U.S.T.H.B	Président
M M S HACHAICHI	Maitre de Conférences à l'U.S.T.H.B	directeur de la Mémoire
M Mohamed ZITOUNI	Professeur à l'U.S.T.H.B	Examinateur
M Mohand Ouamer HERNANE	Professeur à l'U.S.T.H.B	Examinateur

Remerciements

Je remercie profondément M Hachaichi, Maitre de conférence au Département de Mathématique à l'USTHB, pour son soutien, ses encouragements, ses conseils, sa patience et son aide précieuse durant ces années de thèse.

Mes sincères remerciements a M. Meziane AIDER , Professeur au départementde Mathématique à l'USTHB pour avoir accepté de présider le jury de soutenance

j'exprime ma gratitude à M . Mohamed ZITOUNI , professeur à l'USTHB a M . Mohand O. hernane professeur à l'USTHB pour avoir accepté de participer dans le jury de soutenance.

Merci a tous ceux qui m'ont apporté de l'aide, chacun a sa manière tout au long de ma thèse.

Mes remerciements sont également adressés à mes parents et aux membres de ma famille a ma tante d'Alger qui ont toujours été la pour m'encourager et soutenir. Un grand merci a mon fiancé pour ses encouragements et sa compréhension.

Sommaire

Sommaire

Introduction

Les courbes elliptiques sont nées de l'étude au début du 19ème siècle des intégrales elliptiques du type $\int \frac{dx}{\sqrt{P(x)}}$, où **P** est un polynôme de degré 3 ou 4 à racines simples.
La courbe plane $C = \{(x, y); y^2 = P(x)\}$ est une courbe elliptique et l'intégrale se ramène alors à celle de la forme différentielle régulière $\frac{dx}{y}$ sur **C**. Cependant, ce n'est qu'au début du 20eme siècle que la théorie des courbes elliptiques est formalisée et développée avec les travaux de Mordel, ce qui leur a ouvert un vaste champ d'applications, notamment en cryptographieà clé publique sous l'instigation de $N. Koblitz$ et de $V. Miller$ en 1985.
Une des propriétés importantes des points K − rationnels d'une courbe elliptiquesur un corps commutatif **K** est l'existence d'une structure de groupe abélien sous jacente.
Sur une courbe elliptique, la loi de groupe est relativement facile à calculer, mais le problème du logarithme discret est difficile, faute d'algorithme effectif en complexité polynomiale .
La cryptographie à clé publique est une invention de $Diffie - Hellman$ en 1975, mais ce n'est que trois ans plus tard qu'on a un exemple concret avec le chiffrement **RSA** du nom de ses inventeurs $Rivest, Shamir$ et $Adelman$. L'utilisation des courbes elliptiques est l'initiative de $H. W. Lenstra$ en 1985 qui les a utilisées pour la factorisation de grands nombres entiers.

Une des directions prise à l'heure actuelle est la cryptographie utilisant les couplages. Un couplage est une application bilinéaire qui prend deux points sur une courbe elliptique et donne un élément du groupe multiplicatif d'un corps fini, comme les couplages de $Weil$ et $Tate$. Le calcul des couplages a été considéré inefficace jusqu'a l'invention de l'algorithme de $Miller$ en 1986. Cependant, à l'époque les couplages n'avaient pas encore trouvé d'applications concrètes.

Les premières applications des couplages en cryptologie sont de nature cryptanalytiques. En 1993 $Menezes$ et al. utilise le couplage de $Weil$ pour réduire le problème du logarithme discret sur une courbe elliptique à celui dans un corps fini. Un an plus tard, Frey − Rück propose une attaque similaire avec le couplage de $Tate$

Les couplages ont trouvé les premières applications constructives en 2000 avec le

protocole de $Diffie\ Hellman$ pour trois parties proposé par $Joux$ et ensuite $Sakai$, $Ohgishi$ & $Kasahara$. L'application la plus significative des couplages est le chiffrement

à base d'identité : $Boneh\ et\ Franklin$ proposent en 2001 un schéma réalisable fondé sur les couplages, résolvant ainsi le problème posé par $Shamir$ en 1984.

Les couplages ont trouvé par la suite de nombreuses applications: signature à base d'identité, signature courte, etc … . A l'heure actuelle, les couplages sont un sujet de recherche très actif en cryptographie à base des courbes elliptiques.

Notre travail est constitué de 4 chapitres ainsi précisés :

Dans le chapitre 1, nous étudions l'arithmétique des courbes elliptiques, et notamment les concepts d'isogénie de courbes elliptiques, d'endomorphismes et de points de torsion.

Dans le chapitre 2, Nous définissons les couplages de $Tate$ et de $Weil$ et nous rappelons leurs propriétés principales. Nous effectuons ensuite la comparaison des deux couplages ainsi que l'étude du groupe cyclique avec couplage.

Dans le chapitre 3, Nous précisons la construction de courbes elliptiques bien couplées.

Le chapitre 4 est consacré aux applications des couplages en cryptologie, y compris l'attaque $MOV/FREY - Ruc\ddot{k}$, le protocole de $Diffie - Hellman$ pour trois parties et le chiffrement à base d'identité de $Boneh - Franklin$

1. **Arithmétique des Courbes Elliptiques** :

Cette partie est une présentation sommaire des éléments de base nécessaires à la compréhension de l'arithmétique des courbes elliptiques. Nous n'en donnerons pas les démonstrations dont on peut trouver le détail dans [Sil86], ou [HMV04].

Dans la suite, on notera par $\mathbf{K}$ un corps commutatif, local, global ou fini, $\overline{\boldsymbol{K}}$ sa clôture algébrique et $\mathbf{K}^* = \mathbf{K} \setminus \{\mathbf{0}\}$

1.1 Généralités

Dans cette partie, $(\mathbf{K})$désigne l'ensemble des points$(\mathbf{x}, \mathbf{y})$ à coordonnées dans $\mathbf{K}$, et $IP^2(K)$ désigne l'ensemble des triplets $(\mathbf{X}, \mathbf{Y}, \mathbf{Z}) \neq (\mathbf{0}, \mathbf{0}, \mathbf{0})$des éléments de $\mathbf{K}$ muni dela relation d'équivalence :

$$\forall \boldsymbol{\lambda} \in \boldsymbol{K}^* : (\mathbf{X}, \mathbf{Y}, \mathbf{Z}) \sim (\boldsymbol{\lambda}\mathbf{X}, \boldsymbol{\lambda}\mathbf{Y}, \boldsymbol{\lambda}\mathbf{Z}) \qquad \textbf{(1.1)}$$

Définition 1 : *Une courbe elliptique* $\boldsymbol{E} \setminus \boldsymbol{K}$, *est l'ensemble des solutions* $(\boldsymbol{X}, \boldsymbol{Y})$ *dans* $IP^2(\boldsymbol{K})$ *d'une équation homogène de la forme* :

$$F(X,Y,Z) = Y^2Z + a_1XYZ + a_3YZ^2 - X^3 - a_2X^2Z - a_4XZ^2 - a_6Z^3 = 0\,,\ a_i \in \overline{\boldsymbol{K}}\,, \qquad \textbf{(1.2)}$$

telle que $\boldsymbol{\partial F/\partial X}$, $\boldsymbol{\partial F/\partial Y}$ et $\boldsymbol{\partial F/\partial Z}$ ne soient pas tous nuls en tout point $\mathbf{P}$ de cette courbes : on exprime ce fait en disant que la courbe est « lisse » ou non singulière.
Il y a un seul point noté $\boldsymbol{O} \in \boldsymbol{E}$ avec $\mathbf{Z} = \mathbf{0}$ qui est le point de coordonnées $(\mathbf{0}, \mathbf{1}, \mathbf{0})$, appelé le point à l'infini.

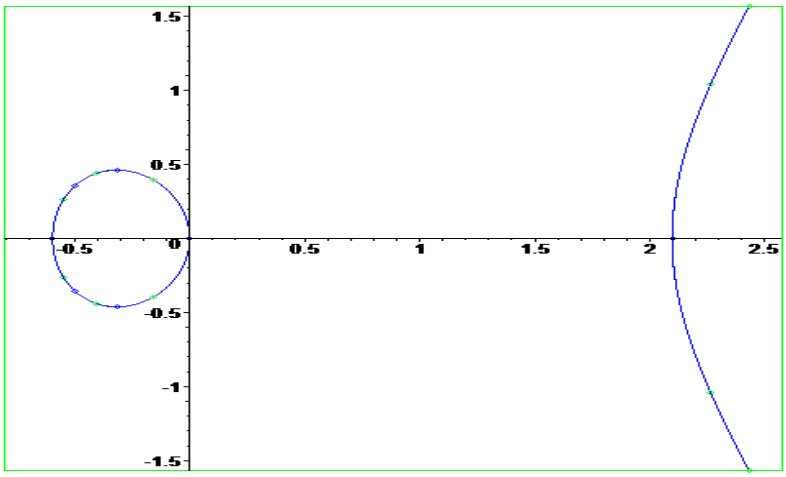
On utilise dans la pratique les coordonnées affines $\mathbf{x} = \frac{\mathbf{X}}{\mathbf{Z}}$ et $\mathbf{y} = \frac{\mathbf{Y}}{\mathbf{Z}}$, en sorte que l'équation de la courbe elliptique prend la forme, dite affine :

$$f(x,y) = \mathbf{y^2} + \mathbf{a_1xy} + \mathbf{a_3y} - \mathbf{x^3} - \mathbf{a_2x^2} - \mathbf{a_4x} - \mathbf{a_6} = \mathbf{0} \in \mathbf{K}[\mathbf{x}, \mathbf{y}] \qquad (\mathbf{1.3})$$

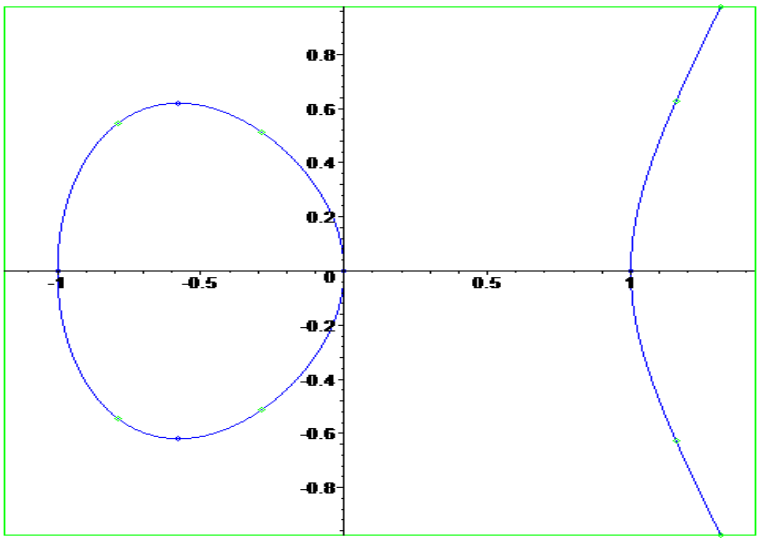
et on peut traduire la définition générale en disant qu'une courbe elliptique est l'ensemble des point $(\mathbf{x}, \mathbf{y}) \in \mathbf{A^2}(\overline{\mathbf{K}}) = \overline{\mathbf{K}} \times \overline{\mathbf{K}}$ satisfaisant l'équation $(\mathbf{1.3})$, muni du point à l'infini $\mathbf{O}$.

Nous présentons quelques exemples de courbes elliptiques :

1 – sur le corps des nombres réels $\mathbb{R}$:



$$(a)\ E_1 : y^2 = x^3 - \frac{3}{2}x^2 - \frac{5}{4}x$$



$$(b)\ E_2 : y^2 = x^3 - x$$

***fig*1.1 *Courbes Elliptiques sur* $\mathbb{R}$**

2 - Sur le corps fini à 17 éléments $\mathbf{IF_{17}}$

Soit $\mathbf{E : y^2 = x^3 + x}$ une courbe elliptique sur $\mathbf{IF_{17}}$

Montrons que $\mathbf{E(IF_{17})} = \{(\mathbf{x},\mathbf{y}) \in \mathbf{IF_{17}} \times \mathbf{IF_{17}} : \boldsymbol{f}(\boldsymbol{x},\boldsymbol{y}) = \boldsymbol{y}^2 - \boldsymbol{x}^3 - \boldsymbol{x} = 0\}$

est une courbe elliptique sur $\mathbf{IF_{17}}$, en calculant $\partial \boldsymbol{f}/\partial \boldsymbol{x}$ et $\partial \boldsymbol{f}/\partial \boldsymbol{y}$ qui doivent être non nulles

en tout point de $\mathbf{E}$

En effet : $\frac{\partial \boldsymbol{f}}{\partial \boldsymbol{x}}(\boldsymbol{x},\boldsymbol{y}) = -3\boldsymbol{x}^2 - 1$ qui ne s'annule en aucun point $(\boldsymbol{x},\boldsymbol{y}) \in \mathbf{IF_{17}}$ x $\mathbf{IF_{17}}$;

de même : $\frac{\partial \boldsymbol{f}}{\partial \boldsymbol{y}}(\boldsymbol{x},\boldsymbol{y}) = 2\boldsymbol{y}$ qui est nulle seulement pour $\mathbf{y = 0}$

Ainsi $(\frac{\partial \boldsymbol{f}}{\partial \boldsymbol{x}}(\boldsymbol{x},\boldsymbol{y}), \frac{\partial \boldsymbol{f}}{\partial \boldsymbol{y}}(\boldsymbol{x},\boldsymbol{y})) \neq (0,0)$ pour tout point $(\boldsymbol{x},\boldsymbol{y}) \in \mathbf{IF_{17}}$ x $\mathbf{IF_{17}}$ et donc $\mathbf{E}$

est une courbe non singulière, c'est − à − dire elliptique sur $\mathbf{IF_{17}}$.

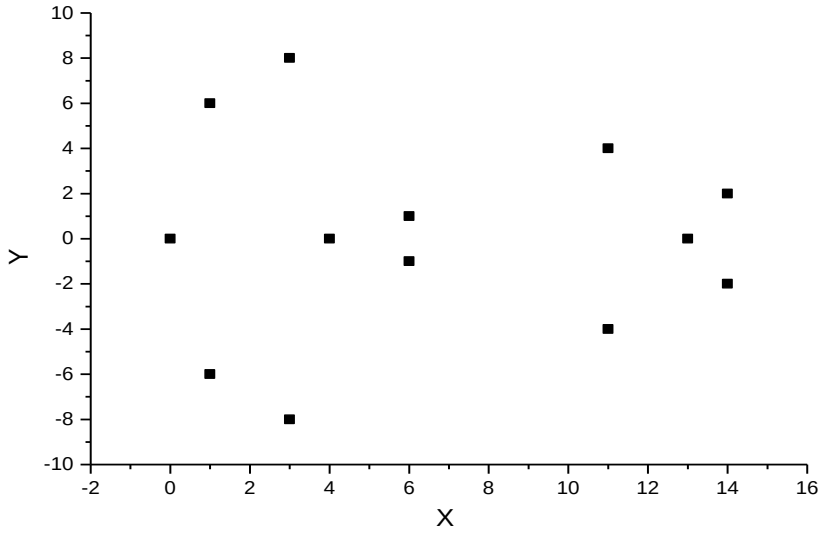
Les valeurs possibles de $\mathbf{y}$ en fonction de $\boldsymbol{x} \in \mathbf{IF_{17}}$ sont données dans le tableau suivant :

$\boldsymbol{x}$	**0**	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**13**	**14**	**15**	**16**
$\boldsymbol{y}$	**0**	$\pm\mathbf{6}$	−	$\pm\mathbf{8}$	**0**	−	$\pm\mathbf{1}$	−	−	−	−	$\pm\mathbf{4}$	−	**0**	$\pm\mathbf{2}$	−	$\pm\mathbf{7}$

Donc :

$$\boldsymbol{E}(\boldsymbol{IF_{17}}) = \left\{ \begin{matrix} (0,0)\ ;\ (1,\pm 6)\ ;\ (3,\pm 8)\ ;\ (4,0)\ ;\ (6,\pm 1)\ ;\ (11,\pm 4)\ ;\ (13,0); \\ (14,\pm 2);\ (16,\pm 7) \end{matrix} \right\} \cup (\infty)$$

Illustration graphique de cette courbe



$$\mathbf{E : } y^2 = x^3 + x \textbf{ dans } \mathbf{IF_{17}}$$

Remarque 1 : Selon la caractéristique du corps de base, l'équation d'une courbe elliptique peut être simplifiée. On peut distinguer les cas suivants :

- Si *car* $\left(\overline{K} \right) \neq 2$ $\left(\begin{matrix} \text{en pratique } \mathbf{K} = \mathbf{IF_N} \text{ corps fini avec } \mathbf{N} \text{ un grand nombre} \\ \text{premier} \end{matrix} \right)$,

  on élimine les monômes en **xy** et en **y** par le changement de variables $(\mathbf{x}, \mathbf{y})$ par $(\mathbf{x}, \frac{1}{2}(y - a_1 x - a_3))$ on obtient l'équation de la courbe sous la forme suivante :

$$\boldsymbol{E} : \boldsymbol{y}^2 = 4\boldsymbol{x}^3 + \boldsymbol{b}_2\boldsymbol{x}^2 + 2\boldsymbol{b}_4\boldsymbol{x} + \boldsymbol{b}_6$$

avec :

$$\mathbf{b_2} = \mathbf{a_1^2} + \mathbf{4a_2}$$

$$\mathbf{b_4} = \mathbf{2a_4} + \mathbf{a_1 a_3}$$

$$\mathbf{b_6} = \mathbf{a_3^2} + \mathbf{4a_6}$$

Posons en suite:

$$\boldsymbol{b}_8 = \boldsymbol{a}_1^2\boldsymbol{a}_6 + 4\boldsymbol{a}_2\boldsymbol{a}_6 - \boldsymbol{a}_1\boldsymbol{a}_3\boldsymbol{a}_4 + \boldsymbol{a}_2\boldsymbol{a}_3^2 - \boldsymbol{a}_4^2 \quad \text{et} \quad \mathbf{c_4 = b_2^2 - 24b_4}$$

$$\mathbf{c_6 = b_2^3 + 36\, b_2 b_4 - 216\, b_6}$$

Invariants des courbes elliptiques :

Toute courbe elliptique $\mathbf{E\backslash K}$ possède plusieurs invariants : le discriminant, l'invariant modulaire, l'invariant différentiel, le conducteur, etc. … … … … ….

Définition 2 : *le discriminant d'une courbe elliptique* $\boldsymbol{E\backslash K}$, *est le polynôme "homogène" de degré* 12 *de l'anneau* $\mathbb{Z}[b_2, b_4, b_6, b_8]$ *égal* à :

$$\Delta(\boldsymbol{E}) = \mathbf{9}\boldsymbol{b_2 b_4 b_6} - \mathbf{8}\boldsymbol{b_4^3} - \mathbf{27}\,\boldsymbol{b_6^2} - \boldsymbol{b_2^2\, b_8}$$

Définition 3: *Soit* $\boldsymbol{K}$ *un corps de caractéristique* $\boldsymbol{car}(\boldsymbol{K}) \neq \mathbf{2}, \mathbf{3}$ *On définit l'invariant modulaire* $\boldsymbol{j}(\boldsymbol{E})$ *d'une courbe elliptique* $\boldsymbol{E\backslash K}$ *d'équation de Weierstrass* $\boldsymbol{E\backslash K}$: $y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$ *par* : $j(E) = c_4^3/\Delta(E)$,

ce qui a un sens car $\Delta(\boldsymbol{E}) \neq \mathbf{0}$ *puisque* $\boldsymbol{E\backslash K}$ *est elliptique* (*et donc lisse*)

Remarque 2 :

Un simple calcul fournit que :

$$\mathbf{4b_8 = b_2b_6 - b_4^2} \qquad \text{et} \qquad 1728\Delta = c_4^3 - c_6^2$$

Par ailleurs, dans le cas où $\mathbf{car}\left(\overline{\boldsymbol{K}}\right) \neq 2, 3$, on peut simplifier davantage l'équation de la courbe elliptique en utilisant le changement de variable suivant :

$(\mathbf{x}, \mathbf{y}) = ((\boldsymbol{x} - 3\boldsymbol{b}_2)/36,\ \boldsymbol{y}/108)$, en sorte que l'équation ce simplifie :

$$\mathbf{E\backslash K : y^2 = x^3 - 27c_4\, x - 54c_6}$$

On a alors le résultat important suivant :

Théorème 1:

Soient $\boldsymbol{K}$ *un corps de caractéristique* $\boldsymbol{car}(\boldsymbol{K}) \neq 2,3.$ *et* $\boldsymbol{E}\backslash\boldsymbol{K}$ *une courbe elliptique*

(a) *La courbe elliptique* $\boldsymbol{E}\backslash\boldsymbol{K}$ *donnée par son équation de Weierstrass peut*

Etre classée de la manière suivante :

(i) $\boldsymbol{E}\backslash\boldsymbol{K}$ *est non singulière si et seulement si* $\boldsymbol{\Delta}(\boldsymbol{E}) \neq \boldsymbol{0}$

(ii) $\boldsymbol{E}\backslash\boldsymbol{K}$ *possède un nœud si et seulement si* $\Delta(\boldsymbol{E}) = \boldsymbol{0}$ *et* $\boldsymbol{c_4} \neq \boldsymbol{0}$

(iii) $\boldsymbol{E}\backslash\boldsymbol{K}$ *a un point de rebroussement si et seulement si* $\Delta(\boldsymbol{E}) = \boldsymbol{c_4} = \boldsymbol{0}$

Dans les cas (ii) *et* (iii), *on dit que le point est singulier*.

(b) *Deux courbes elliptiques sont isomorphes* $(sur\overline{\boldsymbol{K}})$ *si et seulement si elles ont le même* $\boldsymbol{j} - invariant$.

(c) *Soit* $\boldsymbol{j}_0 \in \overline{\boldsymbol{K}}$. *alors il existe une courbe elliptique* $\left(définie\ sur\ \boldsymbol{K}(\boldsymbol{j_0})\right)$ *ayant* $\boldsymbol{j_0}$ *comme* $\boldsymbol{j} - invariant$

Preuve : [**Sil86**]

Remarque 3 : Concernant les caractéristiques 2 et 3, les conditions $a_1^2 \neq -a_2$ et $a_1 \neq 0$ assurent que les courbes ne sont pas supersinguliére dont il est connu qu'elles sont sensibles à l'attaque MOV de $Menezes - Okamoto - Vanstone$ et $Frey - Rück$

L'ensemble des points d'une courbe elliptique peut être muni d'une structure de groupe abélien dont l'élément neutre est le point à l'infini O. La loi de groupe peut être interprétée géométriquement, dans le cas réel, grâce à la méthode dite de la « sécante /tangente» (voir figure 1.2).
La somme de deux points $\mathbf{P} \in \mathbf{E}(\mathbb{R})$ et $\mathbf{Q} \in \mathbf{E}(\mathbb{R})$, est obtenue de la manière suivante : on commence par tracer la droite passant par ces deux points. Cette droite coupe la courbe nécessairement en un troisième point noté $R = -(P + Q)$. La somme des points P et Q $(P \neq Q)$ est alors le symétrique de R par rapport à l'axe de symétrie de la courbe.

Cette construction permet alors de préciser la loi de groupe de $\mathbf{E}(\mathbb{R})$:

Proposition 1 : *Soit* $\boldsymbol{E}(\mathbb{R})$: $y^2 = x^3 + ax + b$ *une courbe elliptique sur* $\mathbb{R}$, *alors* $\boldsymbol{E}(\mathbb{R})$ *est un groupe abélien pour la loi de composition suivante* :

1. $\boldsymbol{P + 0 = 0 + P = P}$ *pour tout* $\boldsymbol{P} \in \boldsymbol{E}(\mathbb{R})$.
2. *Soit* $\boldsymbol{P = (x, y)} \in \boldsymbol{E}(\mathbb{R})$. *on définit* $\boldsymbol{-P}$ *par*: $\boldsymbol{-P = (x, -y)}$
3. *Soient* $\boldsymbol{P_1 = (x_1, y_1)}$ *et* $\boldsymbol{P_2 = (x_2, y_2)}$ *deux points sur la courbe tels que* $\boldsymbol{P_1 \neq -P_2}$.

Alors

$$\boldsymbol{P_1 + P_2 = (x_3, y_3)}$$

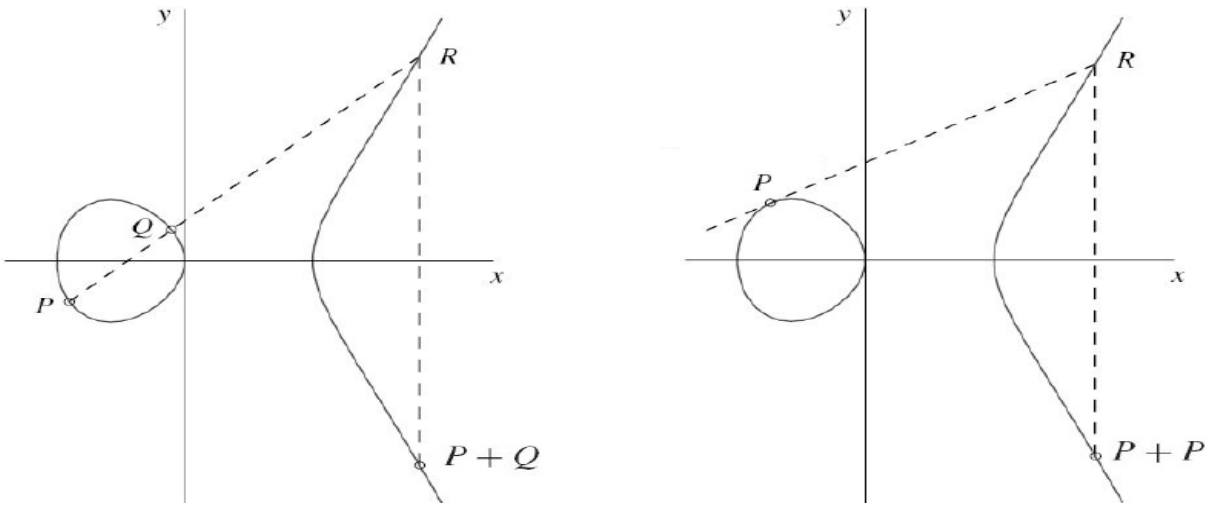
avec :

$$x^3 = \lambda^2 - x_1 - x_2$$

$$y^3 = \lambda(x_1 - x_3) - y_1$$

Où $\lambda = \dfrac{y_2 - y_1}{x_2 - x_1}$ *si* $P_1 \neq P_2$, *et* $\lambda = \dfrac{3x_1^2 + a}{2y_1}$ *sinon*

Illustration de cette loi sur des courbes elliptiques sur $\mathbb{R}$



$(\boldsymbol{a})$ ***Addition de deux points*** $(\boldsymbol{b})$ ***Doublement de point***

Fig*. 1. 2 – *lois de groupe sur $\boldsymbol{E_2}(\mathbb{R})$

Dans le cas où $\mathbf{Car}(\mathbf{K}) = \mathbf{5}$, on obtient les résultats suivants :

Proposition 2 : *Soit* $E\backslash K$: $y^2 = x^3 + ax^2 + b$ *une courbe elliptique avec* $\boldsymbol{Car(K) = 5}$, *alors* $E\backslash K$ *est un groupe pour la loi de composition suivante* :

1. $\boldsymbol{P + 0 = 0 + P = P}$ *pour tout* $\boldsymbol{P \in E(K)}$.

2. *Soit* $\boldsymbol{P = (x, y) \in E(K)}$. *on définit* $\boldsymbol{-P}$ *par:* $\boldsymbol{-P = (x, -y)}$

3. *Soient* $\boldsymbol{P_1 = (x_1, y_1)}$ *et* $\boldsymbol{P_2 = (x_2, y_2)}$ *deux points sur la courbe tels que* $\boldsymbol{P_1 \neq -P_2}$

Alors

$$\boldsymbol{P_1 + P_2 = (x_3, y_3)}$$

avec

$$x_3 = \lambda - a - x_1 - x_2$$

$$y_3 = \lambda(x_1 - x_3) - y_1$$

où $\lambda = \dfrac{y_2 - y_1}{x_2 - x_1}$ *si* $p_2 \neq p_1$, *et* $\lambda = \dfrac{ax_1}{y_1}$ *sinon*

Remarque 4 : Les équations précédentes permettent de définir une loi de groupe analogue pour une courbe elliptique sur n'importe quel corps K de caractéristique $\text{Car(K)} \neq 2,3$

Dans le cas où $\text{Car(K)} = 2$ on obtient le résultat suivant:

Proposition 3 : *Soit* $\boldsymbol{E\backslash K : y^2 + xy = x^3 + ax^2 + b}$ *une courbe elliptique avec* $\boldsymbol{Car(K) = 2}$, *alors* $\boldsymbol{E\backslash K}$ *est un groupe pour la loi de composition suivante* :

1. $\boldsymbol{P + 0 = 0 + P = P}$ *pour tout* $\boldsymbol{P \in E\backslash K}$.

2. *Soit* $\boldsymbol{P = (x, y) \in E\backslash k}$. *on définit* $\boldsymbol{-P}$ *par:* $\boldsymbol{-P = (x, x + y)}$

3. *Soient* $\boldsymbol{P_1 = (x_1, y_1)}$ *et* $\boldsymbol{P_2 = (x_2, y_2)}$ *deux points sur la courbe tels que* $\boldsymbol{P_1 \neq -P_2}$, *alors*

$$\boldsymbol{P_1 + P_2 = (x_3, y_3)}$$

avec :

$$x_3 = \lambda^2 + \lambda + x_1 + x_2 + a$$

$$y_3 = \lambda(x_1 - x_3) + x_3 + y_1$$

où $\lambda = \frac{y_2 + y_1}{x_2 + x_1}$ *si* $p_1 \neq p_2$ *, et* $\lambda = x_1 + \frac{y_1}{x_1}$ *sinon*

Définitions 4 : **multiplication par un scalaire** :

- *On définit, pour tout entier* $\boldsymbol{k} \in \mathbb{Z}$*, et pour tout* $\boldsymbol{P} \in \boldsymbol{E}$ *le morphisme de multiplication scalaire*:

  $[\boldsymbol{k}]\boldsymbol{P} = \boldsymbol{P} + \cdots \ldots \ldots \ldots \ldots \ldots \ldots ; + \boldsymbol{P}$ $(\boldsymbol{k} - \ termes)$, *si* $\boldsymbol{k} > 0$

  $[\boldsymbol{0}]\boldsymbol{P} = \boldsymbol{0_E}$ *et* , $[-\boldsymbol{k}]\,\boldsymbol{P} = [\boldsymbol{k}](-\boldsymbol{P})$

- *On définit alors l'ordre d'un point* $\boldsymbol{P} \in \boldsymbol{E}$ *comme étant le plus petit entier positif* $\boldsymbol{k}$ *tel que* $[\boldsymbol{k}]\,\boldsymbol{P} = \boldsymbol{0_E}$

  Si $[\boldsymbol{n}]\boldsymbol{P} = \boldsymbol{O_E}$ *pour un certain* $\boldsymbol{P} \in \boldsymbol{E}$ *, on dit que* $\boldsymbol{P}$ *est un point de* $n -$ *torsion*

- *On note* $\boldsymbol{E}[\boldsymbol{n}] = \{\boldsymbol{P} \in \boldsymbol{E} : [\boldsymbol{n}]\boldsymbol{P} = \boldsymbol{O_E}\}$ *le sous − groupe des points de* $n -$ *torsion de la courbe elliptique* $\boldsymbol{E}\backslash\boldsymbol{K}$

- *On note enfin :* $\boldsymbol{E}(\boldsymbol{K})[\boldsymbol{n}] = \{\boldsymbol{P} \in \boldsymbol{E}(\boldsymbol{K}) : [\boldsymbol{n}]\boldsymbol{P} = \boldsymbol{O_E}\}$ *le sous − groupe des points de* $\boldsymbol{n} -$ *torsion de* $\boldsymbol{E}\backslash\boldsymbol{K}$ *qui est l'ensemble des points* $\boldsymbol{K} -$ *rationnel de* $\boldsymbol{E}$.

***Définition* 5**: *Soit* $\boldsymbol{E}$ *une courbe elliptique définit sur un corps fini* $\boldsymbol{IF_q}$.

- *On note* $\#\,\boldsymbol{E}(\boldsymbol{IF_q})$ *le nombre de points de* $\boldsymbol{E}(\boldsymbol{IF_q})$ *que l'on appelle aussi l'ordre de la courbe elliptique*
- *On appel trace d'une courbe elliptique (ou trace du Frobenius) le scalaire* $\boldsymbol{t}$ *vérifiant la relation :* $\#\,\boldsymbol{E}(\boldsymbol{IF_q}) = \boldsymbol{q} + \boldsymbol{1} - \boldsymbol{t}$

On a alors le résultat suivant

Théorème 2 (**Hasse**) :

La trace $\boldsymbol{t}$ *d'une courbe elliptique vérifie l'inégalité :* $|\boldsymbol{t}| \leq \boldsymbol{2}\sqrt{\boldsymbol{q}}$

Preuve : [sil 86, théoréme 5.3.1]

1. 2. Isogénie de courbes elliptiques :

Définition 6 : *Soient* E_1 *et* E_2 *deux courbes elliptiques . une isogénie entre* E_1 *et* E_2 *est un morphisme :* $\phi : E_1 \longrightarrow E_2$ Satisfaisant a la condition $\phi(0_{E_1}) = 0_{E_2}$

E_1 et E_2 sont dites isogènes s'il existe une isogénie ϕ entre elles avec $\phi(0_{E_1}) \neq \{0\}$

Puisque les courbes elliptiques sont des groupes les applications entre elle possède une structure de groupe. Posons alors :

$$\text{Hom}\{E_1, E_2\} = \{\text{isogénies } \phi : E_1 \longrightarrow E_2\}$$

Alors Hom $\{E_1, E_2\}$est un groupe pour la loi d'addition suivante:

$$(\varphi + \phi)(P) = \varphi(P) + \phi(P)$$

Si E est une courbe elliptique . on note : $\text{End}(E) = \text{Hom}(E, E)$, l'anneau muni de l'addition précédente et de la multiplication donnée par la composition des applications suivantes :

$$(\phi \circ \psi)(P) = \phi\big(\psi(P)\big)$$

Soit $M \in \mathbb{Z}$ on considère l'isogénie : $[m]: E \longrightarrow E$ défini par :

$[\mathbf{m}]\ (\mathbf{P}) = \mathbf{P} + \mathbf{P} + \cdots \ldots \ldots + \mathbf{P}$ ($\mathbf{m}$ **fois**) **si** $\mathbf{m} > 0$

Si $\mathbf{m} < 0$: $[\mathbf{m}]\ \mathbf{P} = [-\mathbf{m}](-\mathbf{P})$, étant entendu que $[\mathbf{0}]\ \mathbf{P} = \mathbf{O}$. On a alors Une courbes elliptique E est une variété abélienne de dimension 1 ; donc elle est projective, non singulière, avec une structure de groupe algébrique, de point neutre à l'infini $O_E = (\infty, \infty)$,de groupe de Mordell − Weil E(K)Soit **K** un corps commutatif . Il y a des morphismes particulier $E(K) \longrightarrow E'(K)$ classés dans la classe des isogénies de Courbes Elliptiques.

Définition 7 : *Soient deux Courbes Elliptiques E et È sur le même corps K, d'éléments neutres* respectifs 0_E et $0_{E'}$, *de groupes de Mordell − Weil* $E(K)$ *et* $E'(K)$ *une isogénie de E sur E′ est un homomorphisme* $\lambda : E(K) \longrightarrow E`(K)$ *qui satisfait les conditions* :

1. $\boldsymbol{\lambda}$ n'est pas l'homomorphisme nul

2. le noyau de λ est un sous groupe d'ordre fini de E(K)

3. $\boldsymbol{\lambda}$ est un homomorphisme surjectif

4. $\boldsymbol{\lambda(O_E) = 0_{E'}}$ pour les points à l'infini O_E de E, $0_{E'}$ de E'

5. $\lambda\ (\mathbf{P} + \mathbf{R}) = \lambda\ (\mathbf{P}) + \lambda\ (\mathbf{R})$ pour touts points P et R de E.

L'homomorphisme nul est l'homomorphisme f : A ⟶ B de valeur $f(a) = 0_{E'}$.

Le noyau de λ est l'image réciproque du point $\mathbf{0_{\grave{E}}} = (\infty, \infty)$.

$$\text{Ker } \lambda = \{P \in E(K) ;\ \lambda(p) = 0_{E'}\}.$$

Un homomorphisme f : A ⟶ B est surjectif si l'équation f(a) = b admet une solution a au moins pour tout élément $b \in B$.

Les deux Courbes Elliptiques E et E′ sont isogènes par l'isogénie $\lambda : E(K) \longrightarrow E'(K)$.

Les isogénies sont caractérisées par un invariant.

Définition 8 : *Le degré d'une isogénie λ est égal à l'ordre de son noyau.*

Exemple 1 : Une isogénie $\lambda : E(k) \to E'(k)$ de degré 6 admet un noyau F, sous groupe de E(k) d'ordre 6 :

$$F = \{P, 2P, 3P, 4P, 5P, 6P = o_E\} = \{P, 2P, 3P, -2P, -P, o_E\}.$$

Exemple 2: (**exemple 4 − 5 dans *Shimura Goro***):

Soient deux Courbes Elliptiques E/Q et E′/Q.

$$E: y^2 = x^3 + ax^2 + bx \in Q[X, Y]$$

$$È: y^2 = x^3 - 2ax^2 + (a^2 - 4b)x \in Q[X, Y]$$

Vérifions que E et E′ sont des Courbes Elliptiques en calculant leurs discriminants.

Nous trouvons

$$\Delta(E) = 16\, b^2(a^2 - 4b) \neq 0 \quad \text{pour} \quad b \neq 0 \text{ et } 4b \neq a^2$$

$$\Delta(E') = 512\, b(a^2 - 4b)(a - 2b) \neq 0 \quad \text{pour } a \neq 2b \text{ et } b \neq 0$$

Il en résulte les conditions. $a \neq 2b, b \neq 0$ et $b \neq a^2$

Soit les deux homomorphismes

$$\lambda : E(K) \longrightarrow E'(K) \quad \text{de valeur.} \quad \lambda(x, y) = \left(\frac{y^2}{x^2}, \frac{y(b - x^2)}{x^2} \right)$$

$$\lambda' : E'(K) \longrightarrow E(K) \text{ de valeur. } \lambda'(x, y) = \left(\frac{y^2}{4x^2}, \frac{y(a^2 - 4b - x)}{8x^2} \right)$$

Le noyau de λ est le sous groupe F de E(Q) égal à :

$$F = \ker(\lambda) = \{P \in E(Q) ; \lambda(P) = o_E\}.$$

Le point $P = (0, 0)$ satisfait $2P = (\infty, \infty) = 0_E$

Donc λ est une isogénie de degré 2.

Le point $P' = (0, 0)$ satisfait $2P' = (\infty, \infty) = 0_{E'}$

Donc λ' est une isogénie de degré 2. Il en résulte que leurs composées.

$$\lambda \circ \lambda' : E' \longrightarrow E' \quad \text{et} \quad \lambda' \circ \lambda : E \longrightarrow E.$$

Sont des isogénies de degré 2.

Cet exemple implique une méthode de détermination des isogénies des Courbes elliptiques.

***Proposition* 4** : *Soit une Courbe Elliptique $E\backslash K$ sur un corps commutatif K.*

A chaque sous groupe fini IF du groupe $E(K)$de Mordell – Weil de E il correspond une isogénie

$$\lambda : E(K)/IF \longrightarrow E(K)$$

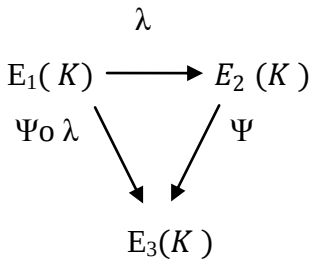
de noyau F.

Preuve : Le groupe quotient E (K)\IF est additif abélien; le sous groupe IF est dans la classe neutre. Alors $\lambda\left(\mathrm{cl(F)}\right) = 0_E$ et $\lambda\,(P + R) = \lambda(P) + \lambda(R)$ pour tous points P et R tels que : $\mathrm{cl}\,(P) \neq IF$ et $\mathrm{cl}(R) \neq IF$.

Proposition 5 : *Soient deux isogénies de Courbes Elliptiques*

$$\lambda : E_1(K) \longrightarrow E_2(K) \;et\; \Psi : E_2(K) \longrightarrow E_3\,(K).$$

Alors la composée Ψ o $\lambda : E_1\,(K) \longrightarrow E_3\,(K)$ est une isogénie



Preuve : Pour les points à l'infini des 3 Courbes Elliptiques.

$$\psi\,\lambda\left(0_{E_1}\right) = \psi\left(0_{E_2}\right) = 0_{E_3}$$

Pour tous points P et R de E_1

$$\Psi\,\lambda\,(P + R) = \Psi(\lambda(P) + \lambda(R)) = \Psi(\lambda(P)) + \Psi(\lambda(R))$$

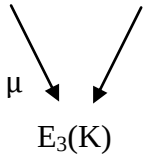
Proposition 6 : *Soient deux isogénies de Courbes Elliptiques*

$$\lambda : E_1(K) \longrightarrow E_2\,(K)\; et\;\; \mu : E_1(K) \longrightarrow E_3\,(K).$$

si $Ker\,(\lambda) \subset Ker\,(\mu)$, alors il existe une isogénie unique $f : E_2(K) \longrightarrow E_3\,(K)$.

Preuve : Soient deux isogénies λ et μ et le diagramme commutatif.

$$E_1(K) \xrightarrow{\ \lambda\ } E_2\,(K)$$



$\text{Ker}(\lambda) \subset \text{Ker}(\mu)$

Relations entre les points à l'infini

$$\lambda(0_{E_1}) = 0_{E_2} \text{ et } \mu(0_{E_1}) = 0_{E_3} \text{ cela implique } f(0_{E_2}) = 0_{E_3}$$

Les formules d'homomorphismes

$$\lambda(P_1 + R_1) = \lambda(P_1) + \lambda(R_1)$$

$$\mu(S_1 + T_1) = \mu(S_1) + \mu(T_1)$$

et l'inclusion des noyaux $\text{Ker}(\lambda) \subset \text{Ker}(\mu)$ impliquent les homomorphisme

$E_1(K) \setminus Ker(\lambda) \longrightarrow E_2(K)$

$E_1(K) \setminus \text{Ker}(\mu) \longrightarrow E_3(K)$

et $E_1(K) \setminus \text{Ker}(\lambda) \longrightarrow E_2(K) \longrightarrow E_3(K)$

Soit $f : E_2(K) \longrightarrow E_3(K)$.

1.2.1 – Multiplication par des entiers rationnels :

Ce sont des isogénies particulières de Courbe Elliptique.

Pour tout entier rationnel $m \in \mathbb{Z}, m \neq 0$, le symbole $mP, P \in E(K)$ représente les points :

$mP = P + P + \cdots + P$, m fois P si $m > 0$

$mP = (-P) + (-P) + \cdots + (-P)$, $(-m)$ fois $-P$ si $m < 0$,

$0P = 0_E$ si $m = 0$.

Considérons l'homomorphisme $t_m : E(K) \longrightarrow E(K)$,

de valeur $t_m(P) = mP$.

Proposition 7: *Les multiplications t_m sur les Courbes Elliptiques $E\setminus\mathbb{Q}$ sont des isogénies de degré m^2 pour $m \neq 0$.*

Preuve : Vérifions les propriétés des isogénies des Courbes Elliptiques, l'hypothèse $m \neq 0$ implique :

$t_m(P) \neq 0_E$, donc t_m n'est pas l'homomorphisme nul.

$t_m(0_E) = m_{o_E} = 0_E$:

$t_m(P + R) = m(P + R) = mP + mR = t_m(P) + t_m(R)$

Pour tous points P et R du groupe de MORDELL − WEIL E(ℚ) Le noyau de t_m est le sous groupe F de E(ℚ) égal à :

$$F = \{P \in E(Q) , mp = 0_E\}$$

F est donc le sous groupe de m − torsion E[m] de E

Cette multiplication t_m est donc un endomorphisme surjectif du groupe E(ℚ). Avec un argument d'endomorphisme " dual ", on obtient le résultat :

Ord(F) = m^2 = degré de la multiplication $t_m : E(K) \longrightarrow E(K)$.

A chaque isogénie $\lambda : E(K) \longrightarrow E'(K)$ est associée une isogénie duale.

Définition 9: *Lorsqu'une courbe E est isogéne* à *une courbe* E' *la courbe* E' *est isogéne* à E, *le noyau de cette isogénie est un sous groupe fini du groupe* $E(K)$
L'ordre de λ *ce sous groupe est égal au degré de l'isogénie* λ.
A chaque isogénie est associer une isogénie dual par la.

Définition 10: *l'isogénie duale d'une isogénie de degré d* :
$\lambda: E(K) \longrightarrow E'(K)$ *est le morphisme de groupes* $\hat{\lambda}: E'(K) \longrightarrow E(K)$
qui satisfait les deux composées $\lambda\hat{\lambda}$ *est la multiplication par d sur* $E'(K)$ *et* $\hat{\lambda}\ \lambda$ *est la multiplication par d sur* $E(K)$

les isogénies de courbes elliptiques, étant des morphismes de variétés abéliennes, sont soumises à l'opération de composition des applications.

Proposition 8 : *Soit deux isogénies* $\lambda : E(K) \longrightarrow E'(K)$ *et* $\mu : E'(K) \longrightarrow E_1(K)$

1. *la composée* $\mu \circ \lambda: E(K) \longrightarrow E_1(K)$ *est une isogénie de courbes elliptiques*
2. *les isogénies duales* $\hat{\lambda}$, $\hat{\mu}$ *et* $\widehat{(\lambda\mu)}$ *satisfait la relation* : $\widehat{(\mu\lambda)} = \hat{\lambda}\,\hat{\mu}$
3. *les degrés des isogénies satisfont les relations* :

$$\deg(\lambda) = \deg\left(\hat{\lambda}\right) \quad et \quad deg(\mu) = deg(\hat{\mu})$$

Proposition 9: *Pour une courbe elliptique E, sur un corps K, il y a seulement un nombre fini de courbe elliptiques isogènes* à E .

1. 2. 2. Technique de Velu :

Soit une Courbe Elliptique E d'équation de Weierstrass:

$$E: \mathbf{y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6} \in \mathbf{K[x, y]} \quad (1)$$

Sur le corps $K(E) = K(x, y)$ des fonctions rationnelles définies sur K, nous associons à tout point $p \neq o_E$,une valuation v_P de valeur :

$$v_P(x) \geq 0 \; ; \; v_P(y) \geq 0. \quad (2)$$

Au point à l'infini o_E , nous associons la valuation v_P de valeur :

$$v_0(x) = -2 \; ; \; v_0(y) = -3 \quad (3)$$

Mettons l'équation de E sous la forme :

$$g(x, y) = y^2 + a_1xy + a_3y - x^3 - a_2x^2 - a_4x - a_6 = 0 \quad (4)$$

L'invariant différentiel de E est égal à : $W(E) = \frac{dx}{-g'_y} = \frac{dy}{g'_x}$

Ou les dérivées partielles de la fonction $g(x, y)$ sont égales à :

$$g'_x = 3x^2 + 2a_2x + a_4 - a_1y \text{ et } g'_y = -(2y + a_1x + a_3). \quad (5)$$

En posant $z = -x / y$, nous obtenons les développements de x et de y en z :

$$x = z^{-2} - d_1z - 1 - d_2 - d_3z - d_4z^2 - d_5z^3 \ldots\ldots\ldots ;$$
$$y = -x/z = - z^{-3} + d_1z^{-2} + d_2z^{-1} + d_3z + d_4z + d_5z^2 + \ldots \quad (6)$$

les relations entre les coefficients d_i et a_i sont :

$$d_1 = a_1 \; ; \quad d_2 = a_2 \; ; \quad d_3 = a_3 \; ;$$
$$d_4 = a_4 + a_1a_3 \quad (7)$$
$$d_5 = a_1a_4 + a_2a_3 + a_1^2a_3;$$
$$d_6 = a_6 + a_1^2a_4 + a_1^3a_3 + a_2a_4 + 2a_1a_2a_3 \; ; \ldots\ldots$$

L'invariant différentiel de E est une fonction de z :

$$W(E) = dz\{1 + a_1z + (a_1^2 + a_4)z^2 + (a_1^3 + 2a_1a_2 + a_3) + \cdots\} \quad (8)$$

Soit un point (X, Y) de la courbe isogéne à E .

A chaque point P = (x, y) de E, nous associons le point (X, Y) par les relations :

$$X = x + \sum_{T \in F - O_E} \big(x(P+T) - x(T)\big) \qquad (9)$$
$$Y = y + \sum_{T \in F - O_E} \big(y(P+T) - y(T)\big)$$

Nous obtenons les développements de x et y en z :

$$X = z^{-2} - a_1 z - a_2 - a_3 z - \ldots ;$$
$$Y = -z^{-3} + a_1 z^{-2} + a_2 z^{-1} + \ldots \qquad (10)$$

La formule $Z = -X/Y$ implique le développement de Z en série :

$$Z = z + 2tz^3 + 3a_1 tz^6 + \cdots. \qquad (11)$$

Nous en déduisons une relation entre X et Y indépendante de z :

$$Y^2 + A_1 XY + A_3 Y = X^3 + A_2 X^2 + A_4 X + A_6; \qquad (12)$$

avec $A_1 = a_1$; $A_2 = a_2$; $A_3 = a_3$;

$A_4 = a_4 - 5t$ et $A_6 = a_6 - b_2 - 7w$; t et w de la formule (14)ci – dessous et b_2 se trouve dans l'équation de E :

$$y^2 = 4x^3 + b_2 x^2 + 2b_4 x + b_6 \quad \text{avec } b_2 = a_1^2 + 4a_2.$$

1. 2. 3. Algorithme de calcul des Courbes Elliptiques E\ℚ :

1) Soit une Courbe Elliptique E d'équation de Weierstrass (1) :
2) Choix d'un sous groupe fini F du groupe E(ℚ).
3) Prendre $F_2 = \{P \in F, \text{d'ordre } 2\}$.
4) l'ensemble R des points de $F - F_2 - \{O_E\}$, et $-R = \{-P ; P \in R\}$, tel que :

   $R \cup -R = F - F_2 - o_E$ et $R \cap -R = \{\emptyset\}$.
5) Prendre la partie $S = F_2 \cup R$.
6) Calculer les dérivées partielles g'_x et g'_y avec la formule (4).
7) les coordonnées X et Y d'un point de la courbe isogènes sont :

(VELU-1) $$X = x + \sum_{p \in s} \left(\frac{t_p}{x - x(p)} + \frac{u_p}{(x - x(p))^2} \right)$$

(VELU-2) (13)

$$Y = y - \sum_{p \in s}\left(u_p \frac{2y + a_1 x + a_3}{(x - x(p))^3} + t_p \frac{a_1(x - x(p)) + y - y(p)}{(x - x(p))^2} + \frac{a_1 u_p - g'_x(p) g'_y(p)}{(x - x(p))^2} \right)$$

est une isogénie de Courbes Elliptiques.

8) Calculer les nombres :

$g'_x(P)$; $g'_y(P)$ si $P \in F_2$ (sont les dérivées partielle); $t_P = g'_x(P)$ si $P \notin F_2$;

$$t_P = 6X^2 + b_2X + b_4 \qquad \text{si} \quad P \notin F_2. \tag{14}$$

$$u_P = 4X^3 + b_2X^2 + 2b_4X + b_6$$

$$t = \sum_{P \in S} t_P \quad ; W = \sum_{P \in S} \left(u_P + t_P\, X(P)\right)$$

9) L'équation de Weierstrass de la Courbe isogéne $E' = E \setminus F$ est

$$E' = E / F : Y^2 + a_1XY + a_3Y = X^3 + a_2X^2 + (a_4 - 5t)X + a_6 - b_2 t - 7\omega ;$$

Exemple : Application de l'algorithme à la Courbe Elliptique E_1 d'équation de Weierstrass :

$$E_1 : y^2 = x^3 + 5 ; \tag{1}$$

Le calcul implique les invariants

$$\Delta(E_1) = -10800 = -2^4 \times 3^3 \times 5^2 \text{ et } j(E_1) = 0. \tag{2}$$

Le groupe $E_1(K)$ a un sous groupe F d'ordre 3, formé des points :

$$F = \left\{ P = (0, \sqrt{5}), 2P = (0, -\sqrt{5}), 3P = O_E = (\infty, \infty) \right\}; \tag{3}$$

En utilisant la méthode de VELU, nous obtenons les ensembles :

$$F_2 = \{Ø\} \quad , \quad R = \{P\} = S. \tag{4}$$

Avec le calcul nous obtenons les coordonnées du point (X, Y) :

$$(x, y) \longrightarrow \left[X = x + \frac{20}{x^2} \ , Y = y - \frac{40y}{x^3} \right] \tag{5}$$

Par le calcul nous obtenons les nombres de l'étape (8)

$$t = 0,\ \omega = 20\ ; \qquad (6)$$

Nous en déduisons l'équation de Weierstrass de la Courbe Elliptique isogéne E_2 :

$$E_2 = E_1 / F : Y^2 = X^3 - 135. \qquad (7)$$

Le calcul implique les invariants :

$$\Delta(E_2) = -7873200 = -2^4 \times 3^9 \times 5^2 \quad \text{et} \quad j(E_2) = 0. \qquad (8)$$

La proposition 5 et la relation $j(E_1) = j(E_2) = 0$ impliquent que les Courbes isogènes E_1 et E_2 sont isomorphes.

1.3. Isogénies, endomorphismes et points de torsion :

1.3.1. Isogénie, isogénie duale :

Soient E_1, E_2 deux courbes elliptiques rationnelle φ: $E_1 \longrightarrow E_2$ définies sur un corps k et O_1,O_2 leurs points à l'infini, une fonction tel que $\varphi(O_1) = O_2$ est appelé isogénie Comme tout morphisme de courbes, une isogénie est soit surjective, soit constante.

Les isogénies vérifient par ailleurs la propriété remarquable d'être aussides morphismes de groupes ([Sil86] III. 4).

A toute isogénie non constante $\varphi: E_1 \rightarrow E_2$, on associe le morphisme de corps injectif

$$\varphi^* : \bar{k}(E_2) \longrightarrow \bar{k}(E_1)$$

On dit que $\varphi : E_1 \longrightarrow E_2$ est séparable, inséparable ou purement inséparable si l'extension de corps correspondante $\bar{k}(E_1)/\varphi^* \bar{k}(E_2)$ est respectivement séparable, inséparable ou purement inséparable.

On définit le degré de φ noté $\deg\varphi$, comme étant le degré de l'extension correspondante $\bar{k}(E_1)/\varphi^* \bar{k}(E_2)$;de même pour le degré de séparabilité $\deg_s$ et le degré d'inséparabilité $\deg_i$.

En particulier

$$\deg\varphi = \deg_s \varphi \ \deg_i \varphi$$

Proposition 10: ([$Sil86$] $p.76$)

Soit $\varphi: E_1 \longrightarrow E_2$ *une isogénie non constante.*

Le degré de séparabilité de φ *est égal au nombre de points du noyau de* φ:

$$\#(\ker\varphi) = \deg_s \varphi$$

Le degré d'inséparabilité est égal au degré de ramification de φ au dessus de chaque point de E_2.

L'ensemble des isogénies d'une courbe E dans elle même forme un anneau, appelé anneau des endomorphismes de E et noté End (E)

Exemple :

1. Etant donnée la loi de groupe commutative sur E , on peut définir l'endomorphisme multiplication par m, $[m] \in End(E)$ qui consiste à additionner un point m fois à lui même. Pour tout $m \in \mathbb{Z}$, $\deg[m] = m^2$

2.Soient E une courbe elliptique définie sur IF_q et $\sigma \in Gal\left(IF_q/IF_p\right)$ tel que $\sigma(X) = X^p$.

On note E la courbe obtenue en appliquant σ aux coefficients de E. Le $P-$ iém Morphisme de Frobenius ϕ_P défini par $\phi_P(X, Y) = (X^P, Y^P)$ est une isogénie purement inséparable de E dans E^{σ} et $\deg \Phi_p = \deg_i \Phi_p = p$.

3. De façon similaire, pour E une courbe elliptique définie sur IF_P ,on définit le $q-$ iéme morphisme de Frobenius $\phi_q \in End(E)$, tel que $(X, Y) = (X^q, Y^q)$.Cet endomorphisme est purement inséparable de degré q.

A chaque isogénie non constante $\varphi: E_1 \longrightarrow E_2$ correspond une unique isogénie $\hat{\varphi}: E_2 \longrightarrow E_1$, appelée isogénie duale, telle que $\hat{\varphi} \circ \varphi = [\deg\varphi] \in End(E_1)$ et $\varphi \circ \hat{\varphi} = [\deg\varphi] \in End(E_2)$.

Les propriétés remarquables de ces Isogénies sont données dans [Sil86](section III. 6). Elles permettent en particulier de donner une bonne description des points de m $-$ torsion, et pourront s'avérer utiles dans la construction de couplages, dits symétriques ou self $-$ pairings.

1.3.2 Groupes de torsion :

On note $E[m] = \ker([m])$le sous $-$ groupe des points de m $-$ torsion. De la même façon, on définit pour K extension quelconque du corps K , le sous $-$ groupe $E(K)[m]$ des points K $-$ rationnels de m $-$ torsion.

La structure des groupes de torsion est détaillée dans le théorème suivant :

Théorème 3 : ([$Sil86$] $p.89$).

Soit E une courbe elliptique sur un corps K et $m \in \mathbb{Z}^*$

- *Si* $car(k) = 0$ ou $car(k) \wedge m = 1$, alors : $E[m] \simeq (\mathbb{Z}/m\mathbb{Z}) \times (\mathbb{Z}/m\mathbb{Z})$.
- *Si* $car(k) = p$, alors

  ou bien $E[\pi^e] \simeq \{O\}$ *pour tout* $e \in \mathbb{N}^*$

  ou bien $E[P^e] = \mathbb{Z}/P^e\mathbb{Z}$ *pour tout* $e \in \mathbb{N}^*$

De ce théorème, on peut déduire facilement la structure de groupe des points IF_q rationnels d'une courbe E définie sur IF_q :

***Corollaire* 1** : *Soit E une courbe elliptique définie sur* IF_q, *alors*

$$E(IF_q) \simeq \mathbb{Z}/n_1\mathbb{Z} \times \mathbb{Z}/n_2\mathbb{Z} \text{ avec } n_1/n_2 \text{ et } n_1/q-1$$

preuve : $E(IF_q)$étant un groupe commutatif, il est de la forme $\mathbb{Z}/n_1\mathbb{Z} \times \ldots\ldots\ldots \times \mathbb{Z}/n_k\mathbb{Z}$, où $n_1/\ldots\ldots/n_k$.S'il existe $m \in \mathbb{Z}^*$ premier à la caractéristique P de IF_q,tel que m/n_1, on compte Alors m^kpoints de $m-$torsion, ce qui impose d'après le théorème que $k \leq 2$. De même, si p/n_1 , avec le théorème, on a nécessairement $k \leq 1$. Dans tous les cas, $E(IF_q)$ est de la forme $\mathbb{Z}/n_1\mathbb{Z} \times \mathbb{Z}/n_2\mathbb{Z}$, où n_1/n_2.on utilisant le couplage de Weil on montre que $n_1/q-1$

***Lemme* 1** : *Soit E une courbe elliptique définie sur* $IF_q.(q = p^d)$,$e \geq 1$ *un entier quelconque, et m un entier premier* à p. *Alors* :

$E[m] \subset E(F_{q^e})$, $\mu_m \subset IF^*{}_{q^e}$

Où μ_m désigne l'ensemble des racines $m-$iéme de l'unité de IF_q.

En particulier, comme $E[n_1] \subset E(IF_q)$, on a $n_1/q-1$.

1.3.3 ***Structure de l'anneau des endomorphismes*** :

Il est intéressant pour la construction de certains couplages dits "self − pairing" de bien connaître la structure de End(E). Avec les exemples donnés ci − dessous (voir 1.3.1), il est clair que celuici contient au moins un sous anneau isomorphe à $\mathbb{Z}$ (pour tout $m \in \mathbb{Z}$, $[m] \in$ End(E) et que cette inclusion est stricte pour les corps finis (si E définie sur IF_q,

$\phi_q \in \mathrm{End}(E)$

Le théorème qui suit résume les différentes possibilités pour la structure de End(E)

Théorème 4 : ([*Sil*86] $p.102$).

L'anneau des endomorphismes d'une courbe elliptique est soit $\mathbb{Z}$*,soit un ordre dans un corps quadratique imaginaire, soit un ordre dans une algèbre de quaternions. Lorsque* $\mathbb{Z} \subset End(E)$*, on dit que la courbe E est* à *multiplication complexe.*

En particulier, si la courbe est définie sur un corps fini, End(E) contient également l'endomorphisme de *Frobenius*[1] et donc la courbe est toujours à multiplication complexe.

[1] *il est possible que l'endomorphisme de Frobinus soit égal* à *l'endomorphisme de multiplication par un entier* $m \in \mathbb{Z}$,mais dans ce cas, E est supersinguliére et $\mathbb{Z} \subsetneq \mathrm{End}(E)$.

Couplages:

Un couplage est une application bilinéaire de groupes, c'est-à- dire une application $e: G_1 \times G_2 \to G_3$

où G_1, G_2 sont des groupes additifs et G_3 un groupe multiplicatif tels que :

$$e(S_1 + S_2, T) = e(S_1, T)e(S_2, T) \text{ et } e(S, T_1 + T_2) = e(S, T_1)e(S, T_2)$$

un exemple est donné par l'application suivante :

$$f: M_k(\mathbb{Z}/n\mathbb{Z}) \times M_k(\mathbb{Z}/n\mathbb{Z}) \longrightarrow F_p$$
$$(A, B) \longrightarrow a^{tr(AB)}$$

Où $a \in IF_p$ est d'ordre n cependant ce couplage ne connaîtrait pas d'application cryptographique car le problème de logarithme discret est trivial dans le groupe de départ $M_k(\mathbb{Z}/n\mathbb{Z})$.

A ce jour les couplages connus en cryptographie sont les couplages de *Tate* et de *Weil*

2. 1. Couplage de Weil.

Soit E une courbe elliptique définie sur IF_q .on rappelle que si $D = \sum n_p P$ un diviseur et f une fonction rationnelle tels que $SUPP(D)$ et $SUPP(div(f))$ sont disjoints, on peut définir

$$f(D) = \prod f(P)^{n_P}$$

Définition1:

soit *m un nombre premier avec la caractéristique de* IF_q , K *une extension de* IF_q *telle que tout les points* $E[m]$ *soit définis sur K (autrement dit* $E[m] \subset E(K)$ *). Soient* $P, Q \in E[m]$.

Soient A, B *diviseurs de degré 0 tels que* $D_P \sim [P]-[0]$ *et* $D_Q \sim [Q]-[0]$ *et que les supports de* D_p *et de* D_Q *sont disjoints (on peut prendre* $D_p = [P+T]-[T]$, $D_Q = [Q+S]-[S]$ *avec* S, T *convenables).soient* f_{D_P}, f_{D_Q} *des fonctions telles que*

$$div(f_{D_P}) = m\,D_P \text{ et } div(f_{D_Q}) = m\,D_Q$$ *.le couplage de Weil est une application*

$$e_m : E[m] \times E[m] \to \mu_m(K)$$

définie par

$$e_m(P,Q) = f_{D_P}(D_Q) / f_{D_Q}(D_P)$$

Remarque 1 : le couplage est bien défini (c'est-à-dire ne dépend pas du choix de D_P et de D_Q car pour tout g: $f_{D_P+div(g)}(D_Q)/f_{D_Q}(D_P + div(g)) = f_{D_P}(D_Q)/f_{D_Q}(D_P)$. De même, si on remplace D_Q par un diviseur équivalent, la valeur de $f_{D_P}(D_Q) / f_{D_Q}(D_P)$ ne change pas. C'est une racine de l'unité car $\left(f_{D_P}(D_Q)/f_{D_Q}(D_P)\right)^m = f_{D_P}(mD_Q)/f_{D_Q}(mD_P) = 1$ d'après la réciprocité de *Weil*

Si on choisit $D_p = [P+T]-[T], D_Q = [Q+S]-[S]$ de sorte que T, S, Q + S, P + T soient différents, alors on a une expression explicite pour $e_m(P,Q)$

***proposition* 1**:

$$\boldsymbol{e_m(P,Q) = \frac{f_Q(T)}{f_P(-T)} \frac{f_P(Q-T)}{f_Q(P+T)}} \qquad \textbf{(2.1)}$$

Où f_P *et* f_Q *sont des fonctions telles que* $div_{f_P} = m[P] - m[O]$ *et* $div_{f_Q} = m[Q] - m[O]$

Preuve :

D'après la définition de e_m (P, Q) on a $e_m(P,Q) = \frac{g(Q)/g(O)}{f_Q(P+T)/f_{Q(T)}}$

où g est une fonction telle que $div(g) = m[P+T] - m[T]$ on a donc $g = f_P \circ \tau_{-T}$ où τ_{-T} est la translation par $-$ T.Donc $g(Q) \ / \ g(0) = f_P(Q-T) \ / \ f_P(T)$ et on trouve la formule demandée.

***Proposition 2*:**

le couplage de Weil à *les propriétés suivante :*([*Sil*86]$p96-98$)

1 • bilinéaire : $e_m(S_1+S_2,T) = e_m(S_1,T)e_m(S_2,T)$ *et*

$$e_m(S,\ T_1+T_2) = e_m(S,T_1)e_m(S,T_2)$$

2 • alternance ***(antisymétrique)*** : $e_m(T,T) = 1$ *par conséquent*

$$e_m(S,T) = e_m(T,S)^{-1}$$

3• non − dégénérescence : *si* $e_m(S,T) = 1$ *pou tout* $S \in E[m]$ *alors* $T = O$

4 • action galoisienne : *pour tout* $\sigma \in Gal(\bar{F}_q/F_q)$ *on a* $e_m(S,T)^\sigma = e_m(S^\sigma, T^\sigma)$

5• compatibilité : *si* $S \in E[mm']$ *et* $T \in E[m]$ *alors* $e_{mm'}(S,T) = e_m(m'S,T)$

Preuve :

1 • soient $P,Q,R \in E[m]$, f_1, f_2, f_3 fonctions telles que

$$div(f_1) = m[P] - m[O] = mD_1$$
$$div(f_2) = m[Q] - m[O] = mD_2$$
$$div(f_3) = m[R] - m[O] = mD_3$$

Alors

$$e_m(P+Q,R) = \frac{f_1\, f_2(D_3)}{f_3(D_1+D_2)} = \frac{f_1(D_3)f_2(D_3)}{f_3(D_1)\,f_3(D_2)} = e_m(P,R)e_m(Q,R)$$. De même

$$e_m(P,Q+R) = e_m(P,Q)e_m(P,R)$$

2 • d'après la formule **(**2.1) on a $e(P,P)=\dfrac{f_n(T)}{f_n(-T)}\dfrac{f_n(P-T)}{f_n(P+T)}$ pour $P\neq 0,\pm P$.

Si on prend T d'ordre 2, alors $T=-T$ et $e_m(P,P)=1$. Reste à montrer qu'un tel choix est faisable.

Si m est pair, alors un tel T est différent de $0,\pm P$.

Si m impair, alors la caractéristique est impaire, donc il y a 3 points d'ordre 2 dans E , l'un d'entre eux est différent de $\pm P$ et on le prend pour T

3 - Soit $P\in E[m]$ tel que $e_m(P,Q)=1$ pour tout $Q\in E[m]$. Fixons $R\in E(\overline{K})$ pour tout $X\in E(\overline{K})$ soit χx une fonction telle que $div(\chi x)=m[X]-(m-1)[R]-[Y]$ où $Y=mX-(m-1)R$

Soit f une fonction telle que $div(f)=m[P]-m[0]$.Alors on a :

$$f(Y)f(R)^{n-1}=\left(\frac{f(X)}{\chi x([P]-[O])}\right)^m$$

En effet, le terme à droite est égal à

$$\frac{f^n(X)}{\chi x(m[P]-m[O])}=\frac{f(m[X])}{\chi x(div(f))}=f(m[X]-div(\chi x))=f([Y]+(m-1)[R]).$$

Soit $Q\in E[m]$, g une fonction telle que $div(g)=m[Q+X]-[Q]=div(\chi_{X+Q})-div(\chi_x)$.

on a

$$\frac{f(X+Q)}{\chi_{X+Q}([P]-[O])}=\frac{f([X+Q]-[X])f(X)}{f_2([P]-[O])\chi_X([P]-[O])}=e_m(P,Q)\frac{f(X)}{\chi_X([P]-[O])}$$

Comme $e_m(P,Q)=1$ pour tout $Q\in End[m]$ il existe une fonction h telle que :

$$\frac{f(X)}{\chi_X([P]-[O])}=h(mX)=h(Y+(m-1)R)$$

Donc pour tout Y , on a f(Y)f(R)$^{m-1}$ = $\left(h \circ \tau_{(m-1)R}\right)^m$ (y).comme R est constante, on a

$m[P] - m[O] = div(f) = m\, div\left(h \circ \tau_{(m-1)R}\right)$

Donc [P] ~ [O] ce qui montre que P = O

5• soit $mm'P = 0, mQ = 0, div(f_1) = m\,m'[P] - mm'[O], div(f_2) = m[Q+T] - m[T]$,

$div(f_3) = m[m'P] - m[O]$ .Alors $e_{mm'}(P,Q) = \frac{f_1([Q+T]-[T])}{f_2^m([P]-[O])}$ et

$e_m(m'P,Q) = \frac{f_3([Q+T]-[T])}{f_2([m'P]-[O])}$

on a

$div(f_3) = m[m'P] - m[O] = div(f_1) + m([m'P] + (m'-1)[O] - m'[P])$

,donc on peut supposer $f_3 = f_1 f_4^n$ où f_4 est une fonction telle que

$div(f_4) = [m'P] + (m'-1)[O] - m'[P]$

.Alors

$e_{mm'}(P,Q) = \frac{f_3\, f_1^{-m}([Q+T]-[T])}{f_2^m([P]-[O])} = \frac{f_3([Q+T]-[T])\, f_1(-div(f_2))}{f_2^m([p]-[O])}$

$= \frac{f_3([Q+T]-[T])}{f_2^m([p]-[O])\, f_2(div(f_4))}$ d'après la réciprocité de Weil

$= e_m(m'P,Q)$

Le couplage de Weil en gros sert à tester l'indépendance des points dans $E[m]$ .En effet, si P et Q sont linéairement indépendant, $e_m(P, Q) = 1$.on le précise dans la proposition suivante :

Proposition 3 : *soit* $P \in E[m]$ *d'ordre exacte* m. *Alors il existe* $Q \in E[m]$ *tel que* $e_m(P,Q)$ *soit une racine primitive d'ordre* m *de l'unité .par conséquent si* $p_1, p_2 \in E[m]$, P_1 *et* P_2 *sont dans le même coset de* $\langle p \rangle$ *si et seulement si* $e_m(P,P_1) = e_m(P,P_2)$

Preuve:

On sait que E[m] ≅ $\mathbb{Z}_m \oplus \mathbb{Z}_m$ (d'après la proposition **7** du chapitre 1). Soit Q ∈ E[m] tel que P et Q soit deux générateurs de E[m]. Alors Q est aussi d' ordre m, et tout point

de E[m]s$'$écrit comme combinaison linéaire de P et de Q. S$'$il existe $0 < d < m$ tel que $e(P,Q)^d = 1$, alors $e(P,dQ) = 1$. En plus $dQ \neq 0$ car Q est d$'$ordre m. Pour tout $aP + bQ \in E[m]$ on a : $e(aP + bQ, dQ) = e(P,dQ)^a = 1$, ce qui est en contradiction avec la non dégénérescence du couplage de *Weil*. Donc $e_m(P,Q)$ est une racine primitive d$'$ordre m de l$'$unité. Maintenant si $P_1 - P_2 = uP + vQ$, alors $e_m(P,P_1) = e_m(P,P_2)e_m(P,vQ)$ et $e_m(P,P_1) = e_m(P,P_2)$ si et seulement si $vQ = o$

Ce résultat assure que si un point du couplage est fixé et que l'autre varie dans E[m], on obtient un homomorphisme de groupe de E[m] dans l'image du couplage c'est-à-dire μ_m .

2. 2. Couplage de Tate :

Définition 2 : *Soit* l un nombre naturel premier avec la caractéristique de IF_q.

Soit $K = IF_{q^k}$ une extension de IF_q qui contiennent toutes les racines de l$'$unité d$'$ordre l . Soient $P \in E(K)[m]$, $Q \in E(K)$. Soient D_P, D_Q diviseurs de degré 0 tels que modulo K^* , $D_P \sim [P] - [O]$ et $D_Q \sim [Q] - [O]$ et que les supports de D_P et de D_Q soient disjoints.

Soient f_{D_p} une fonction telle que $div\left(f_{D_p}\right) = l\, D_p$ .Le couplage de Tate est une application

$$t: E(K)[l] \times E(K)/lE(K) \longrightarrow K^*/K^{*l}$$

définie par

$$t(P,Q) = f_{D_p}(D_p)\ modulo\ K^{*\,l}$$

Remarque 2:

- Le couplage de Tate est bien défini car si on remplace D(P) par un diviseur équivalent $D(P) + div(g)$, alors $f_{D(P)+div(g)}(D(Q)) = f_{D(p)}(D(Q))g(D(Q))^l$ $\equiv f_{(D_p)}(D(Q)) \bmod k^*$.de même, $f_{(D_p)}(D(Q) + div(g))$

  $= f_{D(p)}(D(Q))f_{D(p)}(div(g))$

  $= f_{D(p)}(D(Q))\, g(D(P))^l \equiv f_{D(p)}(D(Q)) \bmod K^{*l}$

d'après la réciprocité de *Weil*. Enfin si $R \in E(K)$ alors on peut choisir

$D_{Q+lR} = D_Q + l([R] - [O])$ et

$$f_{D(P)}(D(Q + lR)) = f_{D(P)}(D(Q))f_{D(P)}(l([R] - [O]))$$
$$= f_{D(P)}(D(Q))f_{D(P)}([R] - [O])^l$$
$$\equiv f_{D(P)}(D(Q)) \bmod K^{*l}$$

- Contrairement au couplage de *Weil* qui prend les deux arguments dans le même groupe, le couplage de *Tate* prend dans deux groupes différent $E(K)[l]$ et $E(K)[l]\backslash lE(K)$. Ces deux groupes ont le même cardinal.

- Toute classe d'équivalence de $E(K)\backslash l\,E(K)$ contient un représentant dans le même groupe de torsion $E[l]$

En prenant $D_P = [P] - [O]$, $D[Q] = [Q + T] - [T]$ on obtient une formule explicite pour le couplage de Tate similaire à la formule de la proposition (**1**)

***Proposition* 4** :

$$t_l(P, Q) = (f_p(Q + T))/(f_p(T)) \qquad (2.2)$$

Où f_p *est une fonction telle que* $div\left(f_p\right) = l[P] - l[O]$ *et* $t \in E(K)$ *tel que les points* $T, Q + T, P, O$ *soient distincts*.

Pour que le couplage rend une valeur exacte on peut définir

$$\tilde{t}(P, Q) = (f_p(D_Q))^{(q^k-1)/l}$$

***Proposition* 5** : le couplage de $TATE$ a les propriétés suivantes :

1) $t_l(O, T) \in (K^*)^l$ *pour tout* $T \in E(K)$
2) *Si* $Q \in lE(K)$ *alors* $t_l(P, Q) \in (K^*)^l$ *pour tout* $S \in E(K)[l]$
3) *bilinéarité :* $t_l(S_1 + S_2, T) = t_l(S_1, T)\ t_l(S_2, T)$ *et* $t_l(S, T_1 + T_2) = t_l(S, T_1)\ t_l(S, T_2)$
4) $non - dégénérescence$: *Si* $t_l(S, T) == 1$ *pour tout* $T \in E(K)[l]$ *alors* $S = 0$.

5) *action galoisienne : pour tout* $\sigma \in Gal(\bar{F}_q/F_q)$*on a* $t_l(S,T)^\sigma = t_l(S^\sigma, T^\sigma)$

Preuve :

1) Si $P = O$ alors on peut choisir pour $f_{D(P)}$ la fonction constante 1.

2) On a déjà montré ce point pour montrer que le couplage est bien défini.

3) La bilinéarité est évidente.

4) non − dégénérescence : on peut consulter une preuve dans [GH94], ou encore une Preuve plus élémentaire dans [F. Heb02].

En général il n'y a pas de relation évidente entre le couplage de *Tate* et le couplage de *Weil*. Cependant si $P, Q \in E[m]$ on a $e_m(P,Q) = t_m(P,Q)/t_m(Q,P)$ à une puissance m − iéme prés, ce qui vient directement des définitions. Contrairement au couplage de *Weil* pour lequel $e_m(P,P)$ est toujours 1, $t_l(P,P)$ n'est pas nécessairement 1. Cependant pour $P \in E(IF_q)$,ce qui est souvent le cas dans les applications cryptographique, on a le résultat suivant :

Proposition 6 : *Soit* $P \in E(IF_q)[l]$, $P \neq 0$, *l premier. Si le degré de l'extension* $k > 1$ *alors* $t_l(P,P)$ *est trivial* (*c'est* − à − *dire sa valeur est une puissance l* − *iéme dans* $E(K)$.

preuve : On a $t_l(P,P)=g(D)$ où $div(g) = l[P] - l[O]$ et $D \sim [P] - [O]$ Comme $P \in E(IF_q)[l]$, $g \in IF_q(E)$ et $g(D) \in IF_q$. Si $k > 1$, alors l ne divise pas $q - 1$ (sinon IF_q contiendrait les l racines l-iéme de l'unité). Tout élément de IF_q est une puissance l -iéme dans IF_{q^k}. Donc $t_l(P,P)$ est trivial.

Corollaire 1 : *Soit* $P \in E(IF_q)[l]$ *d'ordre exact l* , $P \neq 0$, *l premier. Si* $Q \in E(IF_q)[l]$ *un point de torsion d'ordre exact l et indépendant de* P, *alors* $t_l(P,Q)$ *n'est pas trivia l.*

preuve : Supposons que $t_l(P,Q)$soit trivial. Soit $R \in E(IF_{q^k})$. Il existe un point de l-torsion, disons $\grave{R}$, dans le même coset que R. Alors $t_l(P,R) \equiv t_l(P,\grave{R})$ Comme P et Q sont deux générateurs de E[l], $\grave{R}$ s'écrit $\grave{R} = aP + bQ$. Alors $t_l(P,\grave{R}) = t_l(P,Q)^b$ qui est une puissance l –iéme , ce qui est en contradiction avec la non-dégénérescence du couplage de *Tate*

2. 3. Algorithme de Miller :

L'algorithme de Miller rend possible les applications en cryptographie , dans la mesure où , lorsque le degré de prolongement k n'est pas trop grand, il permet un calcul efficace de ceux ci

2.3.1 Principe de l'algorithme

On rappelle que les couplages de $Tate\ et\ Weil$ requièrent le calcul de la fonction $f_p \in IF_q$ telle que $div(f_P) = l[P] - l[O]$.Celui-ci peut se faire de façon incrémentale en utilisant la loi de groupe géométrique. Le diviseur $D = (P) + (Q) - 2(O)$ peut en effet se réécrire sous la forme $D = (P + Q) - (O) + div(h)$ avec h qui se calcule aisément en considérant les fonctions affines l et v telles que $l = 0$ est l'équation de la droite passant par P et Q et v =0 est celle de la droite passant par $P + Q$ et O

$div(l) = (P) + (Q) + \big(-(P + Q)\big) - 3(O)$ et $div(v) = (P + Q) + \big(-(P + Q)\big) - 2(O)$

, donc on a $(P) + (Q) - 2(O) = (P + Q) - (O) + div(l) - div(v)$

$= (P + Q) - (O) + div(l/v)$

On peut ainsi trouver de proche en proche pour tout $i \in \mathbb{Z}$ des fonctions f_i telles que

$$i(P) - i(O) = ([i]P) - (O) + div(f_i) \qquad (2.3)$$

et en particulier $i = l$ on retrouve $f_P = f_l$

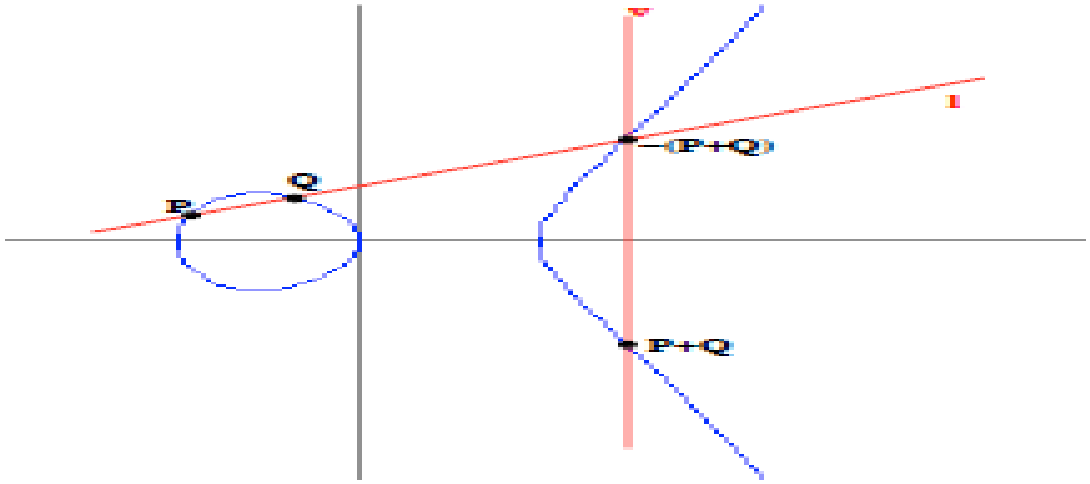


Fig 1 – Courbe elliptiqued'équation réduite $y^2 = x^3 = ax + b$

De façon plus détaillée, connaissant f_i et f_j vérifiant l'équation (2.3), on construit f_{i+j} en constatant que si l et v sont des fonctions affines telles que $l = 0$ est l'équation de la droite passant par [i]P et [j]P et $v = 0$ est celle de la droite passant par [i + j]P et O, alors

$$(i+j)(P)\text{-}(i+j)(O) = ([i]P + [j]P) - 2(O) + div(f_i f_j)$$

$$= ([i+j]P) - (O) + div\left(\frac{l}{v}\right) + div(f_i f_j)$$

$$= ([i+j]P) - (O) + div\left(\frac{l f_i f_j}{v}\right)$$

En particulier, $f_{i+j} = \frac{l f_i f_j}{v}$ convient.

En initialisant la suite à $f_0 = 1$ et en utilisant une chaîne d'addition pour l ,comme par exemple celle utilisée dans l'algorithme double et addition, on obtient alors l'algorithme de *Miller* ([Mil86]) :

*Alg*1. *Algorithme de Miller*

$Entrée: P \in E[l], l = (l_{k-1} \ldots . l_0)_2$

$Sortie: f\ telle\ que\ Div\ (f) = l(p) - l(O)$

$f \leftarrow 1$

$T \leftarrow P$

$Pour\ i = k - 1$ à $0\ faire$

$l \leftarrow tangente\ en\ T$

$v \leftarrow droite\ passant\ par\ 2T\ et\ O$

$f \leftarrow f^2 \frac{l}{v}$

$T \leftarrow 2T$

$Si\ l_i = 1\ alors$

$l \leftarrow droite\ passant\ par\ P\ et\ T$

$v \leftarrow droite\ passant\ par\ P + T\ et\ Q$

$f \leftarrow f \frac{l}{v}$

$T \leftarrow T + P$

$fin\ si$

$fin\ pour$

$retourne\ f$

---

2. 3. 2 Raffinements :

Les couplages de Tate et Weil s'obtiennent en évaluant la fonction f_P sur le diviseur D_Q, soit en calculant le quotient $\frac{f_P(Q+S)}{f_P(S)}$ où $s \in E\left(f_{q^k}\right)$ est bien choisi. On peut donc réduire la quantité de mémoire requise par l'algorithme en évaluant à chaque étape la fonction f en $Q + S$ et S.On peut également évité les divisions faites à chaque étape, en les ramenant à une seule division en fin d'algorithme oncernant le choix de S, on doit cependant prendre quelques précautions. Soit n_i le i-éme entier apparaissant dans la chaîne d'addition de l, on note f_{n_i}, l_{n_i} et v_{n_i}, les fonctions f, l et v obtenues à la ième étape de l'algorithme. On a donc $\left(f_{n_i}\right) = n_i(P) - ([n_i]P) - (n_i - 1)(O)$,

ce qui oblige pour l'évaluation a prendre S et $Q+S$ différents de O , P et $[n_i]P$. Un autre problème peut intervenir lors de l'évaluation des fonctions l et v à chaque tour de boucle :Par exemple le diviseur de l_{n_i} peut être égal soit à $2(T)+(-[2]T)-3(O)$, t à $(P)+(T)+\big(-(P+T)\big)-3(O)$, en particulier – $[n_i]P$ est un zéro de l_{n_i} .Avec un raisonnement similaire pour v, on en déduit que S et $Q+S$ doivent également être différents de $-[n_i]P$.

Au total, il y a donc $o\big(\log_2(l)\big)$ points à éviter pour le choix de S,ce qui lorsque l est grand, n'est pas très contraignant (par exemple si on choisit S dans le sous $-$ groupe à l points engendré par P ,la probabilité de prendre un S qui ne convient pas est de l'ordre de $c\log_2(l)/l$,donc négligeable pour l assez grand). On convient donc que Speut être pris au hasard sur $E\big(IF_{q^k}\big)$ et même dans $E\big(IF_q\big)$ pour simplifier au maximum les calculs.

On peut simplifier le calcul du couplage de *Weil* à l'aide du résultat suivant :

Théorème 1: ([Mil04] $Prop.$ 8).
Soient $P,Q\in E[l]$ *tels que* $P\neq Q$. *Alors*

$$e_l\langle P,Q\rangle=(-1)^l\ \frac{f_P(Q)}{f_Q(P)}$$

*O*ù f_p *et* f_Q *sont les fonctions obtenues avec l'algorithme de Miller* 2.3.1.

De la même façon, on simplifie le calcul du couplage de Tate avec le théorème suivant :

Théorème2 : *Soient* $P\in E\left(IF_{q^k}\right)$ *et* $Q\in E\left(IF_{q^k}\right)/l\,E\left(IF_{q^k}\right)$ *tel que* $Q\neq P,O$. *Alors*

$$\boldsymbol{\langle P,Q\rangle_l=f_P(Q)^{\frac{q^k-1}{l}}}$$

où f_P est la fonction obtenue avec l'algorithme de *Miller* 2.3.1.

preuve : On note $\tau_Q: R\to R+Q$ la translation par le point Q. Pour tout point $S\in E\left(IF_{q^k}^*\right)$ tel que $S\neq O,P,-Q,P-Q$,on a

$$e_l\langle P, Q\rangle = \left(\frac{f_P \circ \tau_Q(S)}{f_P(S)}\right)^{\frac{q^k-1}{l}}, \text{ et}$$

$$\operatorname{div}\frac{f_P \circ \tau_Q}{f_P} = \operatorname{div}(f_P \circ \tau_Q) - \operatorname{div}(f_P) = l(P-Q) - l(-Q) + l(O)$$

Soit v l'équation affine de la droite verticale passant par $P-Q$ et ℓ l'équation affine de la droite passant par P et $-Q$, alors

$$\begin{cases} div\ v = (P+Q) + (Q-P) - 2(O) \\ div\ \ell = (P) + (-Q) + (Q-P) - 3(O) \end{cases}$$

en particulier

$$\boldsymbol{div}(\boldsymbol{f_P} \circ \boldsymbol{\tau_Q}) = \boldsymbol{div}\left(\frac{\boldsymbol{v}}{\boldsymbol{\ell}}\right)^{\boldsymbol{l}}$$

Par conséquent,

$$\frac{f_P \circ \tau_Q(S)}{f_P(S)} = c\left(\frac{v(S)}{\ell(S)}\right)^l \Rightarrow \langle P, Q\rangle_l = c^{\frac{q^k-1}{l}} \qquad (\mathbf{2.4})$$

Afin de déterminer la constante c, on considère l'écriture de $\frac{f_P \circ \tau_Q}{f_P} = c\left(\frac{v}{\ell}\right)^l$ dans l'anneau local E_0 des germes de fonctions en O. Soit $Z = \frac{x}{y}$ une uniformisant au point O ,*alors*

- $v = x_{P-Q} = Z^{-2}\big(1 + zu(z)\big)\ o\overline{7}u \in E_0$
- $\ell = y - \alpha x - \beta = Z^{-3}\big(1 + zv(z)\big)\ o\overline{7}v \in E_0$
- $f_P \circ \tau_Q = f_P(Q)\big(1 + zt(z)\big)\ o\overline{7}t \in E_0$
- $f_{P=z^{-l}}\big(f_0 + zf_1(z)\big)\ o\overline{7}f_0, f_1 \in E_0$

Si on construit f_P récursivement avec l'algorithme de *Miller* , à l'aide d'équations de droites de type $x - \gamma = 0$, $y - \delta x - \lambda = 0$, on a nécessairement f_P normalisée en O, c'est -à-dire $f_0 = 1$. on en déduit avec (2.4):

$$c = f_P(Q)$$

Il est donc possible de simplifier l'algorithme de *Miller* en évaluant la fonction construite en Q à chaque itération.

Remarque 3:

En pratique, on préfèrera utiliser le couplage de $Tate$, qui ne requiert qu'une seule évaluation de la fonction f_P en Q, plutôt que le couplage de $Weil$ qui impose une évaluation de f_Q en P et une division supplémentaire

2.3.3. Implémentation et étude de la complexité :

On détaille (alg2.3.3) l'algorithme permettant de calculer $f_P(Q)$.alors de la dernière étape de l'algorithme, il faut faire attention au fait que ℓ est une droite verticale et v la droite à l'infini.Par ailleurs, à la fin de l'algorithme, on doit avoir $T = O$,ce qui permet de vérifier que l'ordre de P est correct.

Remarque 4 : Il est clair que pour calculer $\frac{f_P(Q+S)}{f_P(S)}$, il ne faut pas appeler deux fois l'algorithme, mais l'adapter pour évaluer f_{n_i} à chaque étape en $Q + S$ et en S.

Complexité de l'algorithme de *Miller* amélioré :

Les opérations les plus couteuses dans l'algorithme sont les divisions dans IF_q pour le calcul de λ et les multiplications dans IF_{q^k} pour le calcul de f_{n_i} à chaque étape, ainsi que la division de f_1 par $f_2$dans IF_{q^k} à la fin de l'algorithme.

Pour les algorithmes classiques permettant de multiplier deux éléments d'un corps fini IF_q, la complexité est en $o((\log q)^\mu)$ où μ dépend de l'algorithme utilisé (typiquement $\mu = \log 3$ pour Karastuba). Une division dansIF_qest donc de complexité en $o((\log q)^{\mu+1})$. Au final, on a donc une complexité pour Miller en

$$o(log\ l + (k\ log\ q)^{\mu} + (log\ q)^{\mu+1} + (k\ log\ q)^{\mu+1}) = o\big((logq)^{\mu+1}(log\ l + k^{\mu+1})\big)$$

Cette complexité est polynomiale en q et l, mais exponentielle en k.
Malheureusement les courbes ayant un petit degré de plongement sont très rares [BK98], ce qui imposera de travailler avec des courbes particulières, dites courbes bien couplées (voir section 3)

2.4. Comparaison des couplages de *Tate* et de *Weil* :

Comme on a vu, le couplage de $Weil$ prend deux fois plus de temps que le couplage de $Tate$. Un défaut du couplage de $Tate$ est que sa valeur n$'$est pas unique. Cela peut être résolu en élevant le couplage de $Tate$ à la puissance $(q^k - 1)/l$, Même avec cette exponentiation le calcul du couplage de *Tate* est encore plus rapide que celui du couplage de *Weil*. En outre, le calcul du couplage est efficace quand l'extension du corps de base, sur laquelle le couplage est défini, est petite. Or l'extension correspondant au couplage de *Weil* est plus large que celle du couplage de *Tate*.Une supériorités majeure du couplage de *Tate* sur le couplage de *Weil* est que le couplage de *Weil* n'est défini que sur les courbes elliptiques. Le couplage de *Tate*, en revanche, peut être généralisé sur les courbes de genre >1 (dans ce cas il n'est plus défini sur des points, mais sur des classes de diviseurs de degré 0). Pour ces raisons le couplage de *Tate* l'emporte sur le couplage de *Weil* dans les applications cryptographiques

2. 5. Groupe cyclique avec couplage :

2. 5. 1. Couplage parfait :

Soit G un groupe cyclique d'ordre n. Un tel groupe a une structure canonique de $\mathbb{Z}-$ module: $\forall (k,x) \in \mathbb{N} \times G, kx = x + x + x \dots \dots + x \;\; et \; (-k)x = -(kx)$. On note $\widehat{G}$ le dual de ce groupe, c'est-à-dire le groupe de $(\mathbb{Z}/\mathrm{n}\mathbb{Z})$ formes linéaires sur Γ.

Un couplage est une application $(\mathbb{Z}/\mathrm{n}\mathbb{Z})$ bilinéaire d'un couple de groupes cycliques dans un troisième groupe cyclique, tous de même ordre n.Il existe un couplage de $\mathrm{G} \times \widehat{\mathrm{G}}$ dans $\mathbb{Z}/\mathrm{n}\mathbb{Z}$, appelé couplage canonique de G et défini par :

$$e_c : \begin{pmatrix} G \times \hat{G} & \longrightarrow & \mathbb{Z}/n\mathbb{Z} \\ (x,v) & \mapsto & v(x) \end{pmatrix}$$

Soient G, G$'$ et G$''$ trois groupes cyclique de même ordre n. Un couplage e de $\mathrm{G} \times \mathrm{G}'$ Dans G$''$ est dit parfait s'il est isomorphe (en tant que couplage) au couplage canonique de G,c'est $-$ à $-$ dire s'il existe trois isomorphismes de groupes m: $\mathrm{G} \longrightarrow \mathrm{G}$, m$'$: $\mathrm{G}' \rightarrow \widehat{\mathrm{G}}$ et m$''$: $\mathbb{Z}/\mathrm{n}\mathbb{Z} \longrightarrow \mathrm{G}''$ tels que $\forall (x,y) \in G \times G', e(x,y) = m''\left(e_c\left(m(x), m'(y)\right)\right)$

$$\begin{array}{ccc} e: G \times G' & \longrightarrow & G'' \\ m \downarrow \ \downarrow m' & & \uparrow \ m'' \\ e_c: G \times \widehat{G} & \longrightarrow & \mathbb{Z}/n\mathbb{Z} \end{array}$$

On considère un ensemble A de n élément, et un couple $(f, h) \in F(A)^2$: on souhaite d'écrire l'ensemble des couplages parfaits de $A_f \times A_f$ dans A_h. Par définition, un tel couplage se déduit de trois isomorphismes de groupes m , m' et m''

$$\begin{array}{ccccc} e: A_f & \times & A_f & \rightarrow & A_h \\ \downarrow & & \downarrow & & \uparrow \\ e_c: A_f & \times & \widehat{A_f} & \rightarrow & \mathbb{Z}/n\mathbb{Z} \end{array}$$

Sans perte de généralité, on peut fixe $m = id$, $m'' = h$ et $m' = \widehat{f^{-1}} \circ i \circ f^{-1}$, où i est un isomorphisme quelconque de $\mathbb{Z}/n\mathbb{Z}$ dans $\widehat{\mathbb{Z}/n\mathbb{Z}}$, et où $\hat{f}$ est l'isomorphisme dual de f, c'est-à-dire $\hat{f}$: $v \in \widehat{A_f} \rightarrow v \circ f \in \widehat{\mathbb{Z}/n\mathbb{Z}}$.

Pour tout ensemble A et tout couple $(f, h) \in F(A)^2$,la description d'un couplage parfait de $A_f \times A_f$ dans A_h est alors équivalente à la donnée d'un isomorphisme i de $\mathbb{Z}/n\mathbb{Z}$ dans $\widehat{\mathbb{Z}/n\mathbb{Z}}$.

Remarque5 :

Le couplage parfait e, en tant qu'application bilinéaire, est défini de manière unique par la valeur de $e(f(1), f(1))$ De même l'isomorphisme i est défini de manière unique par la valeur de $i(1)$, et indirectement par la valeur de $e(f(1), f(1))$.

On en déduit que pour tout couple$(f, h) \in F(A)^2$,il existe un unique couplage parfait e tel que

$$\boldsymbol{e(f(1), f(1)) = h(1)}$$

Dans la suite de ce chapitre, on limitera l'étude des groupes avec couplage au seul cas du couplage parfait vérifiant $e(f(1), f(1)) = h(1)$. Comme le couplage défini par

$(x, y) \in A_{f^2} \longrightarrow h\left(f^{-1}(x), f^{-1}(y)\right) \in A_h$ convient, c'est l'unique couplage parfait mentionné dans la remarque précédente.

2.5.2 Famille générique des groupes cycliques avec couplage

on considère un ensemble A de n éléments, et l'ensemble F(A) de toutes les bijections de $\mathbb{Z}/n\mathbb{Z}$ dans A. Pour tout sous $-$ ensemble $S \subset F(A)$,soit P(A, S) la famille de groupes cycliques avec couplage paramétrée par l'ensemble $\{(f, h) \in S^2\}$. A partir d'uncouple $(f, h) \in S^2$,on construit les structures de groupes A_f et A_h.On construit de plus le couplage parfait $e_{f,h}$ de $A_f \times A_f$ dans A_h défini par :

$$e_{f,h} : \left(\begin{array}{ccc} A_f \times A_f & \rightarrow & A_h \\ (x, y) & \mapsto & h\left(f^{-1}(x), f^{-1}(y)\right) \end{array} \right)$$

Définition* 3** : (Famille générique de groupes cycliques avec couplage***)

Soit $B(n)$ l'ensemble des écritures binaires des entiers entre 0 et $n-1$. La famille de groupes cycliques avec couplage $P(B(n), FB(n))$ est appelée famille générique de groupes cycliques d'ordre n avec couplage. L'union de toutes ces familles, lorsque n est un entier non nul, est appelée famille générique de groupes cycliques avec couplage. Comme expliqué précédemment, les morphismes f et h peuvent être efficacement calculés à partir des structures de groupes de $B(n)_f$ et de $B(n)_h$ A l'inverse, les applications réciproques f^{-1} et h^{-1} ne sont pas directement accessibles.

2. 5. 3 Famille de représentations de groupes cycliques avec couplage

Définition 4 : Soient L et M deux langages sur {0,1} Une famille de représentations de groupes cycliques avec couplage, sur ces langages L et M, est :

$-$la donnée de deux familles de représentations de groupes cycliques, la première sur L et la seconde sur M:$\left(\Gamma, (L_\gamma)_{\gamma \in \Gamma}\right)$ et $(\Delta, (M_\delta)_{\delta \in \Delta})$

$-$ la donnée d'un ensemble de paramètres $\Omega \subset \Gamma \times \Delta$

$-$pour tout paramètre $\alpha = (\gamma, \delta) \in \Omega$, la donnée d'un couplage parfait e_α de $L_\gamma \times L_\gamma$ dans M_γ calculable en temps polynomial et tel que $e_\alpha = (g_\gamma, g_\gamma) = g_\delta$.

Lorsque Ω_1 (respectivement Ω_2) représente l'ensemble des parties gauches (respectivement droites) des éléments de l'ensemble des paramètres , cette famille est

notée :

$$\left(\Omega, \left(L_\gamma\right)_{\gamma\in\Omega_1}, (M_\delta)_{\delta\in\Omega_2}, (e_\alpha)_{\alpha\in\Omega}\right)$$

2.5.4 Problèmes bilinéaires Diffie − Hellman

On peut désormais présenter quelques problèmes bilinéaires classiques dans le formalisme établi pour les familles de représentations de groupes cycliques avec couplage :

Définition 5 : *S'oit* $(\Omega, (L\_\gamma)\_(\gamma \in \Omega\_1), (M\_\delta)\_(\delta \in \Omega\_2), (e\_\alpha)\_(\alpha \in \Omega))$ *une famille de représentations de groupes cycliques avec couplage sur les langages* L *et* M. *Dans cette famille,*

– *un algorithme résolvant le problème bilinéaire Diffie − Hellman calcule l'élément* $log_{g_\gamma}(w), e_{(\gamma,\delta)}(x,y)$ *dans le groupe* M_δ à *partir des données* $(\gamma,\delta)\in\Omega$,$(w,x,y)\in\left(L_\gamma\right)^3$

– *un algorithme résolvant le problème bilinéaire décisionnel Diffie − Hellman décide si* z *est égal* à $log_{g_\gamma}(w), e_{(\gamma,\delta)}(x,y)$ *dans le groupe* M_δ à *partir des données* $(\gamma,\delta)\in\Omega$, $(w,x,y)\in\left(L_\gamma\right)^3, z \in M_\delta$

Comme précédemment, on peut généraliser ces définitions au cas de la famille générique de groupes cycliques avec couplage, avec les mêmes entrées et sorties, mais avec seulement un accès à des oracles pour le calcul des différentes lois et du couplage

3. Construction des courbes elliptiques bien couplées :

Soit E une courbe elliptique définie sur $IF_q(q = p^d)$, r un entier premier différent de p divisant $\#E(IF_q)$ et k le degré de plongement associé. On note $G_1 = \langle P \rangle$ où $P \in E(IF_q)[r]$, $G_2 = \langle Q \rangle$ où $Q \in E(IF_{q^k})[r]$ et $G_3 = \mu_r \subset IF_{q^k}$.

on verra dans la section 4.2, si e: $G_1 \times G_2 \longrightarrow G_3$ est un couplage, les groupes G_1 , G_2 et G_3 doivent vérifier des hypothèses de sécurité, imposant certaines conditions sur les paramétres q, r et k. le degré de plongement k ne doit également pas être trop grand en pratique, pour que les temps de calculs restent raisonnables.

Lorsqu'on peut trouver une courbe E pour laquelle tous ces critères sont vérifiés, on dit que la courbe est adaptée ou pairing − friendly.

3.1 Utilisation du couplage de *Tate* :

on rappelle que le couplage de *Tate* est non dégénéré sur

$$E(IF_{q^k})[r] \times E(IF_{q^k})/rE\left(IF_{q^k}\right) \longrightarrow \mu_r \subset IF^*_{q^k}$$
$$(P, Q) \mapsto \langle P, Q \rangle$$

en particulier si $P \in E(IF_q)[r]$ on peut toujours trouver $Q \in E\left(IF_{q^k}\right)/r\,E\left(IF_{q^k}\right)$ tel que $\langle P, Q \rangle \neq 1$

Si l'on souhaite utiliser ce couplage dans le contexte cryptographique présentera en section 4, il est pertinent de déterminer à quelle condition on a un isomorphisme entre les groupes $E(IF_{q^k})[r]$ et $E(IF_{q^k})[r]/rE\left(IF_{q^k}\right)$.

la suite exacte

$$0 \longrightarrow E\left(IF_{q^k}\right)[r] \longrightarrow E\left(IF_{q^k}\right) \longrightarrow rE\left(IF_{q^k}\right) \longrightarrow 0$$

Permet déjà de dire que

$$rE(IF_{q^k}) \simeq E(IF_{q^k})/rE\left(IF_{q^k}\right)[r],$$

avec en particulier $\#\,E(IF_{q^k})[r] = \#\,(E(IF_{q^k})/rE(IF_{q^k}))$

Il suffit donc de voir à quelle condition le morphisme naturel de groupes $\varphi: E\left(IF_{q^k}\right)[r] \longrightarrow E\left(IF_{q^k}\right)/rE\left(IF_{q^k}\right)$ est injectif. Si $R \in \ker(\varphi)$ alors il existe $S \in E\left(IF_{q^k}\right)$

tel que $R = [r]S$, en particulier $S \in E\left(IF_{q^k}\right)[r^2]$.

montrer que φ est injectif revient à monter que les points rationnels de r^2 $-$ torsion sont nécesserment des points rationnels de $r - trsion$. *on a donc l'équivalence*:

$$E(IF_{q^k})[r] \simeq E(IF_{q^k})/rE\left(IF_{q^k}\right) \Leftrightarrow E\left(IF_{q^k}\right)[r^2] = E(IF_{q^k})[r]$$

Pour pouvoir utiliser le couplage de $Tate$ pour les applications cryptographiques, on devra donc s'assurer que l'on est bien sous l'hypothèse suivante :

$$E\left(IF_{q^k}\right)[r^2] = E(IF_{q^k})[r] \qquad (1.3)$$

Remarque1 :
Dans le cas où cette hypothèse ne serait pas vérifiée, on peut toujours utiliser le couplage de $Weil$, qui a l'avantage de toujours être non dégénéré sur $E[r] \times E[r]$, mais au prix d'une Perte d'efficacité dans les temps de calculs (cf remarque de la section 2.3.2).

La proposition suivante donne un critère simple pour déterminer quand le couplage de $Tate$ peut être utilisé :

Proposition 1 : $Si\ r^2 \| \#E\left(IF_{q^k}\right)$ $(c'est - à - dire\ r^2 / \#E\left(IF_{q^k}\right)\ et\ r^3 \nmid \#E\left(IF_{q^k}\right)$ $et\ k > 1, alors$ $(l'hypothèse\ (1.3) est\ vérifiée).\ En\ particulier, le\ couplage\ de\ Tate$ $est\ non\ dégénérée\ sur\ E[r] \times E[r]$

Preuve : D'après une proposition de $(Balasubramanian\ et\ Koblitz)$ on a :
comme $r^3 \nmid \#E\left(IF_{q^k}\right)$, on a nécessairement $E\left(IF_{q^k}\right)[r^2] \simeq \mathbb{Z}/r\mathbb{Z} \times \mathbb{Z}/r\mathbb{Z}$ donc $E\left(IF_{q^k}\right)[r^2] = E(IF_{q^k})[r]$.

On détermine dans la suite sur quel groupe G_1 il est possible de prendre Tate comme self $-$pairing.

Lorsque $k > 1$, *on ne pourra pas l'utiliser tel quel sur* $E(IF_{q^k})[r]$:

Proposition 2 : $Soient\ E\ une\ courbe\ elliptique\ définie\ sur\ IF_q, G_1$ $un\ sous -$ $groupe\ de\ E\left(IF_q\right)\ engendré\ par\ un\ point\ P \in E\left(IF_q\right)[r]\ de\ r - torsion$ $(r\ premier\ et\ r \neq p)\ et\ k\ le\ degré\ de\ plongement\ associé.\ On\ suppose\ k > 1$.

Si $R \in E(IF_{q^d})$ où d/k et $d < k$, alors $\langle P, R\rangle_r = 1$.

En particulier, $\langle P, P\rangle_r = 1$ et le couplage de *Tate* restreint à $E(IF_q)[r] \times E(IF_q)[r]$ est dégénéré.

Preuve : f_p étant une fonction définie sur IF_q et D_R étant un diviseur défini sur IF_{q^d}, $f_p(D_R)$ est un élément de $IF_{q^d}^*$ qui est nécessairement trivial dans le quotient $IF_{q^k}^*/\left(IF_{q^k}^*\right)^r$.
En effet, comme r est premier et $d < k$, $IF_{q^d}^*$ ne contient aucune racine primitive $r-$iéme de l'unité. Le morphisme de groupes $\pi: x \in IF_{q^d}^* \longmapsto x^r \in IF_{q^d}^*$ est donc injectif, en particulier tout élément de IF_{q^d} est une puissance $r-$ieme d'un élément de IF_{q^d}.

Ainsi en prenant $d = 1$, on a que $\langle P, P\rangle_r = 1$ et par bilinéarité le couplage de *Tate* est dégénéré sur $G_1 = \langle P\rangle$. Par ailleurs, avec le lemme suivant :

***lemme*1**: *soit* $d \geq 1$ *un entier quelconque , alors*:

$$E(l) \subset E\left(IF_{q^d}\right) \Longrightarrow \mu_l \subset IF_{q^d}^*$$

***preuve du lemme*1**: le couplage de Weil étant non dégénéré , il existe deux points de $l-$ torsion $P, Q \in \text{div}^{\circ}_{F_{q^d}}(E)$ et $f_P, f_Q \in IF_{q^d}(E)$, on a alors $e_l(P, Q) \in IF_{q^d}$ comme l est premier $e_l(P, Q)$ est une racine primitive qui engendre μ_l , en particulie $\mu_l \subset F_{q^d}^*$ □

comme $k > 1$, $E\left(IF_q\right)$ ne peut contenir toute la r-torsion $E[r]$. Autrement dit $E\left(IF_q\right) \simeq \mathbb{Z}/r\mathbb{Z}$ en particulier $G_1 = E\left(IF_q\right)[r]$ et le couplage est dégénéré sur les points rationnels de r-torsion.

Dans le cas où le degré de plongement vaut 1, la non dégénérescence de *Tate* vu comme $self-$pairing sur $G_1 = E\left(IF_q\right)[r]$ n'est pas toujours assurée, sauf dans le cas suivant (on distinguera dans la preuve tous les autres cas de figure possibles) :

Proposition 3 : *Soient E une courbe elliptique définie sur* IF_q , G_1 *un sous* $-$ *groupe de* $E\left(IF_q\right)$ *engendré par un point* $P \in E\left(IF_q\right)[r]$ *de* $r-$ *torsion* (r *premier et* $r \neq p$. *On Suppose que le degré de plongement associé* k *vaut* 1.

Si $r^2 \nmid \#E\left(IF_q\right)$, alors l'hypothèse (1.3) est vérifiée et $\langle P,P\rangle \neq 1$. En particulier le couplage de Tate vu comme self-pairing sur $E\left(IF_q\right)[r]$ est non dégénéré.

Preuve : On cherche à déterminer dans quels cas on a $E(IF_q)[r^2]=E(IF_q)[r]$

$E(IF_q)[r^2]$ étant à la fois un sous-groupe de $E(IF_q)$ et de $E[r^2]\simeq \mathbb{Z}/r^2\mathbb{Z}\times\mathbb{Z}/r^2\,\mathbb{Z}$, nécessairement

$$\#E(IF_q)[r^2]/pgcd(\#E(IF_q),r^4)$$

On détaille ici tous les cas de figure possibles :

- **Cas 1** : $r^2 \nmid \#E(IF_q)$,c'est − à − dire. $\#E(IF_q)[r^2] = r$

Comme $E(IF_q)[r]$ est un sous − groupe d'ordre au moins r de $E(IF_q)[r^2]$, $E(IF_q)[r^2] = E(IF_q)[r] \simeq \mathbb{Z}/r\mathbb{Z}$. Le couplage de *Tate* est alors non dégénéré sur $E(IF_q)[r]\times E(IF_q)[r]$. Le sous groupe $E(IF_q)[r]$ étant cyclique, on en déduit que le couplage de *Tate* est non dégénéré sur $G_1 \times G_1$.

- **Cas 2** : $r^2\backslash\#E(IF_q)$ et $r^3 \nmid \#(IF_q)$, c'est − à − dire. $\#E(IF_q)[r^2]\backslash r^2$

On distingue à nouveau plusieurs cas suivant la structure de $E(IF_q)[r]$ et de $E(IF_q)[r^2]$ vus comme sous-groupes de $E(IF_q) \simeq \mathbb{Z}/n_1\mathbb{Z}\times\mathbb{Z}/n_2\mathbb{Z}$ (où n_1 / n_2) :

– si r^2/n_2 , alors $E(IF_q)$ admet un sous-groupe isomorphe à Z/r^2Z de points de r^2-torsion. Par conséquent $E(IF_q)[r^2] \simeq \mathbb{Z}/r^2\mathbb{Z}$,
qui admet un unique sous-groupe d'ordre r , ce qui impose $E(IF_q)[r] \simeq rE(IF_q)[r^2]$.
En particulier le couplage de Tate est dégénéré sur $G_1\times G_1$.

–si r/n_1,alors $E(IF_q)$ admet un sous-groupe isomorphe à $\mathbb{Z}/r\mathbb{Z}\times\mathbb{Z}/r\mathbb{Z}$ de points de r − torsion. Par conséquent $E(IF_q) \simeq \mathbb{Z}/r\mathbb{Z}\times\mathbb{Z}/r\mathbb{Z} = E[r]$ et comme $E(IF_q)[r^2]$ admet au plus r^2 éléments,$E(IF_q)[r] = E(IF_q)[r^2]$.Dans ce cas le couplage de *Tate* est non dégénéré sur $E(IF_q)[r]\times E(IF_q)[r]$ en particulier il existe un point rationnel Q de r − torsion tel que $\langle P, Q\rangle \neq 1$. Il est à noter cependant, que comme $E(IF_q)$ n'est pas cyclique, Q n'est pas nécessairement dans le groupe engendré par P, et que donc on ne peut conclure quant à la non − dégénérescence du couplage sur G_1.

- **Cas 3** : r^3 / $\#E(IF_q)$ et $r^4 \nmid \#E(IF_q)$, c'est − à − dire. $\#E(IF_q)[r^2]$ / r^3

Ce cas se traite de façon similaire au cas 2, en distinguant deux sous-cas :

– si $r|n_1$ et r^2/n_2 , alors $E(IF_q)$ admet un sous-groupe isomorphe à $\mathbb{Z}/r\mathbb{Z}\times\mathbb{Z}/r^2\,\mathbb{Z}$ de points de r^2-torsion.
En particulier $E(IF_q)[r^2] \simeq \mathbb{Z}/r\mathbb{Z}\times\mathbb{Z}/r^2\,\mathbb{Z}$ et donc le sous-groupe des points rationnels de

r-torsion est $E(IF_q) \simeq \mathbb{Z}/r\mathbb{Z} \times \mathbb{Z}/r\mathbb{Z} = E[r]$.
Le couplage de *Tate* est alors dégénéré sur G1.

–si r^3/n_2 alors $E(IF_q)[r^2] \simeq \mathbb{Z}/r^2\mathbb{Z}$ et ce qui ramène au cas 2a.

- **Cas 4** : $r^4 / \#E(IF_q)$, c'est − à − dire. $\# E(IF_q)[r^2] / r^4$

On distingue trois sous -cas :

– soit $r \nmid n_1$ et r^4 / n_2 , alors on est ramené au cas 2a
– soit $r|n_1$ et r^3 / n_2 , alors on est ramené au cas 3a.
– soit r^2/n_1 et r^2/n_2 , alors $E(IF_q)[r^2] \simeq Z/r^2Z \times Z/r^2Z$, ce qui implique $E(IF_q)[r] = rE(IF_q)[r^2]$, en particulier le couplage de Tate est dégénéré sur $G_1 \times G_1$.

les courbes qui vérifient les hypothéses de la proposition 3 disposent d'un Self − paring particuliérement simple, et donc intéressantes d'unpoint de vue cruptographique.

Malheureusement ces courbes sont assez difficiles à obtenir (voir exmple en fin de section 3.3)

Dans la suite , on supposera toujours que l'hypothése(1.3)est vérifiée.

3. 2 Courbes supersinguliére et applications de distorsion :
le degré de plongement associeraux point de r − torsion d'unecourbes supersingulier E est toujour petit, en particulier les courbes supersinguliére sont de bon condidats pour les courbes bien couplées (pairing friendly).

De façon plus précise, on a le résultat suivant, dû à *Menezes*, *Okamoto et Vanstone*, dont on donne une ébauche de preuve lorsque p > 3 :

Proposition 4 : ([**CFA 06**] **p. 124**).
Soit E une courbe elliptique supersinguliére définie sur IF_q $(q = p^d)$, *admettant un point d'ordre r premier différent de p. Le degré de plongement k associé* à *r vérifie* :
– si p = 2, alors k ≤ 4
– si p = 3, alors k _≤6
– si p ≥5, alors k ≤3 ; si de plus d = 1, alors k ≤ 2

et ces bornes sont toujours atteintes.

Preuve : pour simplifier, on prendra p > 3 et $j(E) \in IF_p$ (on sait que on a toujoursj(E) $\in F_{p^2}$).
on va montrer qu'alors nécessairement K = 1 ou K = 2

Etant donnée $j(E) \in IF_p$, il est possible de trouver une courbe E_0 définie sur IF_p telle que

$j(E_0) = j(E)$([Sil86] p. 50). par consequent, E et E_0 sont IF_{q^2} – isomorphes via un changement de coordonnées de Weierstrass

En particulier, les $q^2 -$ iéme Frobenius définis sur E et E_0 ont même polynôme caractéristique. Comme est définie sur IF_p , on peut également calculer le q^2-iéme Frobenius en fonction du $p -$ iéme Frobenius :$\Phi_p^2 = \Phi_p^{2d}$.On considère alors les Polynômes caractéristiques $\chi_{\Phi_p}(X) = (X - \alpha)(X - \beta)$ de Φ_p et $\chi_{\Phi_q^2}(X) = \left(X - \alpha^{2d}\right)$ $\left(X - \beta^{2d}\right)$ de Φ_q^2 définis sur E_0 .

E étant supersinguliére, le polynôme caractéristique de Φ_p défini sur E est de la forme $\chi_{\Phi_p}(X) = (X - a)(X - b)$ avec $\mathrm{tr}\left(\Phi_p\right) = a + b = 0 \bmod p$ et $ab = p^d$, en particulier $\mathrm{tr}\left(\Phi_{q^2}\right) = a^2 + b^2 = 0 \bmod p$. De $\alpha^{2d} + \beta^{2d} = a^2 + b^2 = 0 \bmod p$ et $\alpha\beta = p = 0 \bmod p$,on déduit $\mathrm{tr}\left(\Phi_p\right) = \alpha + \beta = 0 \bmod p$. Avec la borne de Hasse, on a $\left|\mathrm{tr}\left(\Phi_p\right)\right| \leq 2\sqrt{p}$ où $p > 3$, donc $\mathrm{tr}\left(\Phi_p\right) = 0$.Ainsi,$\alpha = -\beta = \pm i\sqrt{p}$ et $\#E\left(IF_{q^2}\right) = \chi_{\Phi_q^2}(1) = \left(1 - (-1)^d\, p^d\right)^2$

$$= \left(1 - (-1)^d\, q\right)^2$$

donc$\left[r \text{ premier et } r \,/\, \#E\left(IF_{q^2}\right)\right] \Longrightarrow r/\left(1 - (-1)^d\, q\right) \Longrightarrow k = 1 \text{ou} 2$ suivant la parité de d son a la classification des courbes supersinguliére en fonction du degré de plongement

Théorème 1 : ([**Wat69**], [**SX95**]).
Soit E une courbe supersinguliére définie sur IF_q de trace t. Alors on est dans l'un des 5 *cas suivants*:

- ✓ *soit* $q = p^{2b}$ *et* $t = \pm 2\sqrt{q}$, *alors le degré de plongement k vaut*1,
- ✓ *soit* $q = p^a$ *avec*$(a\ impair)$*ou* $(p \not\equiv 1\ mod 4\ et\ a\ pair)$ *et* $t = 0, alors\ k = 2$
- ✓ *soit* $q = p^{2b}$ *avec* $p \not\equiv 1\ mod 3\ et\ t = \pm 2\sqrt{q}$, $alors\ k = 3$,
- ✓ *soit* $q = 2^{2b+1}$ *et* $t = \pm\sqrt{2q}$,$alors\ k = 4$
- ✓ *soit* $q = 3^{2b+1}$ *et* $t = \pm\sqrt{3q}$,$alors\ k = 6$

Les courbes supersinguliére ont donc l'avantage d'avoir un petit degré de plongement associé, ce qui rend possible le calcul de couplage. On montre dans ce qui suit qu'elles ont également l'avantage d'être naturellement munies de self – pairing.

Les couplages de *Tate* et de *Weil* utilisés tels quels n'étant pas de bons candidats pour les self – pairings (étant généralement dégénérés sur $E\left(IF_q\right)[r] \times E\left(IF_q\right)[r]$on utilisera la technique due à *Verheul* [Ver04] qui consiste à introduire des endomorphismes particuliers appelés applications de distorsion :

Définition 1 : (**Applications de distorsion**):
Soit $P \in E[r]$*un point de* $r-$*torsion. Une application de distorsion relativement au groupe* $\langle P\rangle$*, est un endomorphisme* $\varphi \in End(E)$ *tel que pour tout* $Q \in \langle P\rangle \{O\}$, $\varphi(Q) \notin \langle P\rangle$.

Si l'on peut trouver un tel endomorphisme sur E, alors il est facile de définir un self − pairing e sur $E(IF_q)[r] \times E(IF_q)[r]$ à partir du couplage de *Weil* ou de *Tate* :

Proposition 5: *On note indifféremment e le couplage de Weil ou de Tate. Si* $\varphi \in End(E)$ *est une application de distorsion, alors pour* $k > 1$:

$$E(IF_q)[r] \times E(IF_q)[r] \longrightarrow \boldsymbol{\mu_r} \subset \boldsymbol{IF_{q^k}^*}$$
$$(P, Q) \mapsto \hat{e}(P, Q) = e(P, \varphi(Q))$$

est un self $-$ *pairing.*

Preuve : Soit $P \in E(IF_q)$ un point d'ordre premier r. Comme φ est un endomorphisme de E, $([r] \circ \varphi)(P) = \varphi([r]P) = 0$, en particulier $\varphi(P) \neq O$ est d'ordre r dans $E(IF_{q^k})$.
On a donc trouvé une base {P, φ(P)} de $E[r] = E(IF_{q^k})[r]$, et comme $e(P, P) = 1$ (prop. 3), par non − dégénérescence de $Tate - Weil$ on a bien $\hat{e}(P, P) \neq 1$.
On montre que cette construction n'est en fait possible que sur les courbes supersinguliéres:

Théorème 2: *Soit E une courbe elliptique et* $P \in E(IF_q)[r]$ *un point de* $r-$*torsion. On suppose le degré de plongement* $k > 1$.

S'il existe une application de distorsion φ relativement au groupe ⟨P⟩, alors E est supersinguliére.

Preuve :D'après le lemme précédent,$\langle P\rangle = E(IF_q)[r]$. Par conséquent $\varphi(P) \in E(IF_{q^k})[r] \backslash E(IF_q)$,donc on a $\boldsymbol{\Phi_q}(\varphi(P)) \neq \varphi(P) = \varphi(\boldsymbol{\Phi_q}(P))$. End(E) est alors non commutatif, et la courbe est supersinguliére

Théorème 3: (Existence d'applications de distorsion [Ver04]).
On note ψ *l'application naturelle qui* à *un endomorphisme* $\varphi \in End(E)$*associe sa restriction* $\varphi_r \in End(E[r]) \simeq \mathcal{M}_2(\mathbb{Z}/r\mathbb{Z})$ *définie sur l'ensemble des points de* $r-$ *torsion . Si E est une courbe supersinguliére, alors* ψ *est surjective. En particulier, il existe toujours une application de distorsion sur une courbe supersinguliére* "

Preuve: On montre que ker (ψ) = [r]End(E) : soit f ∈ ker (ψ), alors E[r] ⊂ ker(f), c'est-à-dire. ker([r])⊂ ker(f).Comme [r] est séparable, le théorème de factorisation des isogénies

(voir [Sil86] cor. III.4.11) assure l'existence de g ∈ End(E) tel que f = [r] ∘g.

On rappelle également que si E est supersinguliére, alors End(E) est un ℤ-module de rang 4 , par conséquent on a :

$$\text{Im } \psi \simeq \text{End}(E)/([r]\text{End}(E)) \simeq (\mathbb{Z}/r\mathbb{Z})^4$$

et donc est surjective.

Voici quelques exemples classiques de courbes supersinguliére pour lesquelles on connaît des applications de distorsion.

Exemple : ([Gal05]).

- $k = 2$:

$$E : y^2 = x^3 + a, \text{courbe définie sur } IF_p \text{ où } p \equiv 2 \bmod 3$$

cardinalité: $\#E(IF_p) = p + 1$

application de distorsion : $(x, y) \mapsto (\zeta x, y), \zeta$ tel que $\zeta^3 = 1$

- $k = 2$:

$$E : y^2 = x^3 + x, \text{courbe définie sur } IF_p \text{ où } p \equiv 3 \bmod 4$$

cardinalité : $\#E(IF_p) = p + 1$
application de distorsion : $(x, y) \mapsto (-x, iy), i^2 = -1$

- $k = 3$:

$E : y^2 = x^3 + a$, courbe définie sur IF_{p^2} où $p \equiv 5 \bmod 6$
et $a \in IF_{p^2} \setminus IF_p$ est un carré, mais pas un cube

cardinalité : $\#E(IF_{p^2}) = p^2 - p + 1$ application de distorsion :

$$(x, y) \mapsto \left(\frac{x^p}{\gamma a^{(p-2)/3}}, \frac{y^p}{a^{(p-1)/2}}\right), \qquad \gamma \in IF_{p^6} \text{ tel que } \gamma^3 = a$$

- $k = 4$:

$$E : y^2 + y = x^3 + x + a, \text{courbe définie sur } IF_2$$

cardinalité : $\#E(IF_{2^{2b+1}}) = 2^{2b+1} \pm 2^{b+1} + 1$
application de distorsion : $(x, y) \mapsto (u^2x + s^2, y + u^2sx + s), u \in IF_{2^2}$ et $s \in IF_{2^4}$
tels que $u^2 + u + 1 = 0$ et $s^2 + (u + 1)s + 1 = 0$

- $k = 6$:

$$E : y^2 = x^3 - x \pm 1, \text{courbe définie sur } IF_3$$

cardinalité : $\#E(IF_{3^{2b+1}}) = 3^{2b+1} \pm 3^{b+1} + 1$
application de distorsion : $(x, y) \mapsto (\alpha - x, iy), i \in IF_{3^2}$ et $\alpha \in IF_{3^3}$ tels que $i^2 = -1$ et $\alpha^3 - \alpha \mp 1 = 0$

On renvoie à [GR04] pour plus de détails sur la construction d'applications de distorsion. A titre d'application, on démontre avec les applicatios de distorsion, l'antisymétrie du couplage de $Tate$ sur les courbes supersinguliére. ceci justifie que $Tate$ quel n'est pas un bon condidat pour la construction de self − pairing sur ces courbes, puisqu'il n'éxiste pas de sous − groupe cyclique de E[r] sur lequel $Tate$ ne soit pas dégénéré.

Proposition 6 : (Antisymétrie du couplage de Tate sur les courbes supersinguliére).
Soit E supersinguliére définie sur IF_q , $r \mid \#E(IF_q)$ *et* $k > 1$ *le degré de plongement correspondant. Alors pour tous points* $P, Q \in E(IF_{q^k})[r], \langle P, Q\rangle = \langle Q, P\rangle^{-1}$

Preuve : On sait que

$$E\left(IF_{q^k}\right)[r] \simeq \mathbb{Z}/r\mathbb{Z} \times \mathbb{Z}/r\mathbb{Z},$$

on étudie alors les valeurs propres et vecteurs propres de l'endomorphisme de $Frobenius$ agissant sur cet espace vectoriel :

***Lemme* 2** : (*Couplage de Tate et valeurs propres du Frobenius*).
Soient $\lambda \in \mathbb{Z}/r\mathbb{Z}$ *une valeur propre de l'endomorphisme de Frobenius vu comme application* $\mathbb{Z}/r\mathbb{Z} - linéaire$ *de* $E[r]$*et* $P \in E[r]$ *un vecteur propre associé* à λ *. Alors*

$$\langle P, P\rangle = 1.$$

Preuve : On a d'une part

$$\langle \varphi(P), \varphi(P)\rangle = \langle P, P\rangle^{\lambda^2}$$

et d'autre part

$$\langle \varphi(P), \varphi(P)\rangle = \langle \widehat{\varphi} \circ \varphi(P), P\rangle = \langle P, P\rangle^{q}$$

Ainsi si $\langle P, P\rangle \neq 1$, alors $\mathbf{r}/(\boldsymbol{\lambda^2 - q})$. Mais ceci est impossible, étant donné que les racines modulo r du polynôme caractéristique du Frobenius

$$\chi(\varphi)(X) = X^2 - \mathrm{Tr}(\varphi)X + q$$

sont 1 et q, et que l'on a supposé $l \wedge q = 1$ et $k > 1$.

Soit P et Q deux points engendrant la r − torsion, on choisira P rationnel et $Q \in E\left(IF_{q^k}\right)[r]$ vecteur propre de l'endomorphisme de *Frobenius*, associé à la Valeur propre q.
En particulier $\langle P, P\rangle = \langle Q, Q\rangle = 1$. Comme E est supersinguliére , il existe(ver04)p289. une application de distorsion $\varphi \in End(E)$ telle que la matrice de φ soit de la forme :

$$Mat_{\varphi} = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \text{ avec } c, b \neq 0 \bmod r$$

On a alors d'une part

$$\langle \varphi(P), \varphi(Q)\rangle = \langle \hat{\varphi} \circ \varphi(P), Q\rangle = \langle P, Q\rangle^{\deg \varphi}$$

et d'autre part

$$\langle \varphi(P), \varphi(Q)\rangle = \langle P, P\rangle^{ab} \langle P, Q\rangle^{ad} \langle Q, P\rangle^{bc} \langle Q, Q\rangle^{cd} = \langle P, Q\rangle^{ad} \langle Q, P\rangle^{bc}$$

Donc

$$\langle P, Q\rangle^{\deg \varphi - ad} = \langle Q, P\rangle^{bc}$$

Comme $\deg \varphi = \det \varphi \bmod r$, on en déduit que

$$(\langle P, Q\rangle \langle Q, P\rangle)^{bc} = 1$$

Si $\langle P, Q\rangle, \langle Q, P\rangle \in \mu_r$ est non trivial, il est d'ordre r, en particulier $bc \equiv 0 \bmod r$ ce qui est exclus.
Finalement, $(\langle P, Q\rangle \langle Q, P\rangle) = 1$ et le couplage de Tate est antisymétrique.

Pour obtenir un degré de plongement supérieur à 6, il est nécessaire de travailler avec des courbes ordinaires munies de couplages asymétriques. Malheureusement, comme ces courbe sont en général un degré de plongement bien trop gros (de l'ordre de q), une recherche de courbe aléatoire ne fournira pas de courbes pairing − friendly. On peut cependant construire grâce à la méthode de multiplication complexe (CM)plusieurs familles de courbes ordinaires (courbes MNT, de $Brezing - Weng, de\ Freeman \ldots$) avec un degré de plongement prescris.

On présente dans ce qui suit les éléments clefs de la méthode CM, ainsi que la construction de courbes MNT pour un degré de plongement $k = 6$.

3.3 Construction de courbes par la méthode CM :

Atkin et *Morain* dans [AM93]adaptent au cas des corps finis la méthode de multplication complexe (CM)utilisée pour les courbes elliptiques détinies sur $\mathbb{C}$.

Etant données q un nombre premier et un entier t dans la borne de *Hasse*, cette méthode permet de trouver une courbe E définie sur IF_q ayant $q + 1 - t$ points.

L'idée est de retrouver à partir du polynôme caractéristique de l'endomorphisme de *Frobenius* sur $E(IF_q)$

$$X^2 - tX + q = 0 \qquad (3.5)$$

des informations sur l'anneau End(E) des endomorphisme de la courbe. on considére le discriminant de l'équation(3.5) que l'on écrit sous la forme

$$4q - t^2 = Dy^2 \qquad (3.6)$$

où $-D$ est un entier appelé discriminant fondamental tel que $-D \neq 1$ et

- ✓ soit $D \equiv 3 \bmod 4$ et sans facteurs carrés,
- ✓ soit $D = 4m$ avec $m \equiv 1$ ou $2 \bmod 4$ sans facteurs carrés.

La méthode d'*Atkin* et *Morain* consiste à construire E telle que End(E)soit l'anneau des entiers de $Q(\sqrt{-D})$. On introduit à cette effet le polynôme de classe de *Hilbert* $H_D(X) \in \mathbb{Z}[X]$ Dont les racines dans IF_q sont toutes des $j-$ invariants de courbes ayant l'anneau d'endomorphisme souhaité. Lalgorithme qui permet de calculer ce polynôme consiste à reconstruire les coefficients de H_D à partir de ses complexes, que l'onobtient via des formules à base de séries convergentes ([Coh93] p. 415).

Pour retrouver la courbe à partir de son invariant modulaire , on utilise le résultat suivant :

***Proposition* 7** : ([*BSS*00] *Lem.VIII*. 3.).
Tout élément de IF_q est le $j-$ invariant d'une courbe elliptique définie sur IF_q
En particulier, si $j \neq 0, 1728$, alors on peut prendre la coube d'équation

$$y^2 = x^3 + 3k\,c^2x + 2kc^3$$

où $k = \frac{j}{1728 - j}$ et $c \in IF_q$ quelconque

Si E et $\widetilde{E}$ ont le même invariant modulaire $j \neq 0,1728$, alors soit $\widetilde{E}$ est isomorphe à E sur IF_q, soit $\widetilde{E}$ est une tordue quadratique de E et sa trace est opposé de celle de E .

le probléme est que cette méthode ne peut fonctionner que pour D relativement petit. La taille des coefficients et le degré de ce polynôme sont en effet en $O(\sqrt{D})$, ce qui nécessite de prendre en pratique $D < 2^{25}$, et un choix adapté pour les valeurs de q et t.

Exemple:On cherche une courbe sur IF_{17} de trace $t = 3$ et donc ayant $q + 1 - t = 15$ points rationnels. Alors $4q - t^2 = 59 = D$ et

$$H_{-59}(X) = X^3 + 30197678080X^2 - 140811576541184X + 3746431940018831 36$$

Les racines dans IF_{17} de $H_{-59}(X) \equiv X^3 - 5X^2 - 5X + 5 \bmod 17$ sont 2, 7 et 13.

Pour $j = 2$, on trouve la courbe d'équation $y^2 = x^3 + 12x + 8$ qui est de cardinalité $15 = q + 1 - t$.
Pour $j = 7$, on trouve la courbe d'équation $y^2 = x^3 + x + 12$ qui est de cardinalité $15 = q + 1 - t$.
Pour $j = 13$, on trouve la courbe d'équation $y^2 = x^3 + 6x + 4$ qui est de cardinalité $15 = q + 1 - t$.

3.4 Un exemple de courbes ordinaires : les courbes MNT

La stratégie de *Miyaji*, *Nakabayashi* et *Takano* [MNT01] consiste à paramétrer Quadratiquement q et t, en s'inspirant du résultat suivant :

Théoréme 4 : *Soit E une courbe elliptique ordinaire définie sur* IF_q *dont le nombre de points rationnels* $q + 1 - t$ *est premier et de degré de plongement* $k = 6$. *Alors il existe un entier l tel que*

$$q = 4l^2 + 1 \text{ et } t = 1 \pm 2l$$

En réinjectant ce paramétrage dans (3.6), on trouve:

$$4(4l^2 + 1) - (1 \pm 2l)^2 = Dy^2 \iff 12l^2 \mp 4l + 3 = Dy^2$$
$$\iff (6l \mp 1)^2 + 8 = 3Dy^2$$

ce qui raméne à la résolution d'une équation diophantienne de la forme

$$x^2 - 3\,Dy^2 = -8 \qquad (3.7)$$

où $x = 6l \mp 1$. ce type d'équation diopantienne est appelé équation de *Pell* généralisée.

pour construire une courbe ordinaire avec $k = 6$, on choisit un discriminant fondamental $-D$, et on cherche parmi les couples (x, y) solution d'équation(3.7), ceux qui vérifient

$x \equiv \pm 1 \bmod 6$ et tels que $q = 1 + 4\left(\frac{x \pm 1}{6}\right)^2$ soit un grand nombre premier. on vérifie ensuite que $q + 1 - t$ où $t = 1 \pm \frac{x \pm 1}{6}$ posséde un grand facteur premier et un degré de plongement $k = 6$. si aucune solution ne remplit ces critéres, on passe au discriminant fondamental suivant

Remarque2 : On peut restreindre les valeurs possibles pour D en remarquant si on a une solution de l'équation (3.7), alors -8 (et donc -2) est carré modulo 3D. Donc si p est facteur premier de D, p vérifie nécessairement $p \equiv 1$ ou 3 mod 8. par ailleur, D doit être impair pour que $x \equiv \pm 1 \bmod 6$.

Pour résoudre une équation de Pell généralisée, la technique consiste d'abord à chercher une solution minimale (x_0, y_0) de l'équation de Pell

$$x^2 - 3\,Dy^2 = 1 \qquad (3.8)$$

Une telle solution vérifie

$$\left|\frac{x_0}{y_0} - \sqrt{3D}\right| < \frac{1}{2y_0^2}$$

et peut donc être obtenue en détectant, dans le développement en fractions continues de p 3D, la première réduite $\frac{x_0}{y_0}$ où x_0 et y_0 vérifient l'équation (3.8) (voir [Z´00] prop. 1.28).
On détaille l'algorithme permettant de calculer les réduites du développement en fractions continues de $\sqrt{n}$:

***Lemme* 3** : *soient a_k le $k-$ iéme coefficient intervenant dans le devloppement en fractions continues de* $\sqrt{n}$:

$$\sqrt{n} = a_0 + \frac{1}{a_1 + \frac{1}{a_2 + \cdots .}} = [a_0, a_1, a_2 \dots \dots \dots \dots . .]$$

on definit r_k par

$$\sqrt{n} = a_0 + \frac{1}{a_1 + \frac{1}{\dots a_{k-1} + \frac{1}{r_k}}}$$

autrement dit,

$$r_k = [a_k, a_{k+1}, \dots]$$

Alors il existe des suites d'entier(b_k) et (c_k) telles que

$$\begin{cases} r_k = \dfrac{b_k + \sqrt{n}}{c_k} \\ a_k = \left\lfloor \dfrac{a_0 + b_k}{c_k} \right\rfloor \\ b_{k+1} = a_k c_k - b_k \\ c_{k+1} = 2a_k b_k - a_k^2 c_k + c_{k-1} \\ a_0 = \lfloor \sqrt{n} \rfloor \\ b_0 = 0 \\ c_{-1} = n, c_0 = 1, c_1 = n - a_0^2 \end{cases}$$

preuve : Par définition, $r_0 = \sqrt{n}$, donc $b_0 = 0$ et $c_0 = 1$. Puis, $r_1 = \dfrac{1}{r_0 - a_0} = \dfrac{\sqrt{n} + a_0}{n - a_0^2}$, dont on déduit $b_1 = a_0$ et $c_1 = n - a_0^2$ on verifie finalement par réccurence les relations sur r_k, b_k, c_k.par ailleurs

$$a_k = \lfloor r_k \rfloor = \left\lfloor \frac{a_0 + b_k + \sqrt{n} - a_0}{c_k} \right\rfloor = \left\lfloor \frac{a_0 + b_k}{c_k} \right\rfloor$$

puisque $|\sqrt{n} - a_0| < 1$

il est alors facile de calculer par récurrence la k − iéme réduite $\frac{x_k}{y_k} = [a_0 \ldots . . a_k]$ ([zoo]p17)

$$\begin{cases} x_k = a_k x_{k-1} + x_{k-2} \\ x_k = a_k y_{k-1} + y_{k-2} \\ x_{-1} = 1, x_0 = a_0, x_1 = a_0 a_1 + 1 \\ y_{-1} = 0, y_0 = 1, y_1 = a_1 \end{cases}$$

On en déduit l'algorithme suivant :

Alg. Calcul d'une solution minimale (x, y) *de l'équation de Pell* $x^2 - ny^2 = 1$

$ENTREÉ: n$
$SORTIE: x, y$
$a_0 \leftarrow \lfloor \sqrt{n} \rfloor, a \leftarrow a_0, b \leftarrow 0, \tilde{c} \leftarrow n, c \leftarrow 1, \tilde{x} \leftarrow 1, x \leftarrow a_0, \tilde{y} \leftarrow 0, y \leftarrow 1$
répéter
$b' \leftarrow ac - b$
$c' \leftarrow 2ab - a^2 c + \tilde{c}$
$a \leftarrow \left\lfloor \frac{a_0 + b'}{c'} \right\rfloor$
$x' \leftarrow ax + \tilde{x}$
$y' \leftarrow ay + \tilde{y}$
$b \leftarrow b'$
$\tilde{c} \leftarrow c$
$c \leftarrow c'$
$\tilde{x} \leftarrow x$
$x \leftarrow x'$
$\tilde{y} \leftarrow y$
$y \leftarrow y'$

jusqu'à ce que: $x^2 - ny^2 = 1$

Remarque 3: Il est classique que le développement en fractions continues de $\sqrt{n}$ est périodique. Si on note k la période, une solution pour Pell est trouvée au bout de k itérations si k est pair ou 2k itérations si k est impair. En particulier, l'algorithme s'arrête.

On détaille ensuite comment résoudre l'équation de Pell généralisée (3.7) :

Lemme 4 : (Résolution de l'équation généralisée de Pell).
Si $\boldsymbol{n} > N^2$, *alors les solutions de l'équation généralisée de Pell*

$$x^2 - ny^2 = N \qquad (3.9)$$

s'il en existe, s'obtiennent comme des réduites du développement en fractions continues de $\sqrt{n}$.

preuve : On a

$$\begin{aligned} x^2 - ny^2 = N &\Leftrightarrow \left(x - \sqrt{n}\, y\right)\left(x + \sqrt{n}y\right) = N \\ &\Leftrightarrow \left(\frac{x}{y} - \sqrt{n}\right)\left(\frac{x}{y} + \sqrt{n}\right) = \frac{N}{y^2} \\ &\Leftrightarrow \left|\frac{x}{y} - \sqrt{n}\right| < \frac{1}{2y^2} \end{aligned}$$

en particulier $\frac{x}{y}$ est une réduite du développement en fractions continues de $\sqrt{n}$.

Remarque 4 : Il est à noter également [Mat00]que si l'équation de *Pell* généralisée (3.7) Admet une solution (x_p, y_p), alors cette solution sera détectée lors de la recherche de la solution minimale (x_0, y_0)de l'équation de Pell (3.8).On obtient alors une infinité de solutions pour (3.7) en considérant les éléments de la forme

$$\left(x_p + \sqrt{3D}y_p\right)\left(x_0 + \sqrt{3D}y_0\right)^k \text{ avec } k \in \mathbb{Z}$$

Exemple :
Pour $D = 43$, on trouve un développement en fractions continues de $\left(\sqrt{3D}\right)$ égal à $[11; \overline{2;\ 1;\ 3;\ 1;\ 6;\ 1;\ 3;\ 1;\ 2;\ 22}]$ et donc la solution de l'équation

$$x^2 - 129y^2 = 1$$

est obtenue en écrivant

$$\frac{x}{y} = [11;\ 2;\ 1;\ 3;\ 1;\ 6;\ 1;\ 3;\ 1;\ 2] = \frac{16855}{1484} .$$

Au passage, la réduite $[11] = \frac{11}{1}$ donne une solution particulière pour l'équation de Pell généralisée :

$$11^2 - 129 \times 12 = -8$$

On construit ensuite une famille de solutions de la forme

$$x + y\sqrt{129} = (11 + \sqrt{129})(16855 + 1484\sqrt{129})^n, \qquad n \in \mathbb{Z} .$$

Pour chaque solution, on teste si le $q = 1 + 4\left(\frac{x\pm1}{6}\right)^2$ correspondant est premier et si la cardinalité correspondante $\left(= q + 1 - t, \text{où } t = 1 \pm 2\left(\frac{x\pm1}{6}\right)\right)$ possède un grand facteur premier :

- $n = 0 : (x, y) = (11, 1), l = 2, q = 17$ est premier, $t = 5$ donc $q + 1 - t = 13$
- $n = 1 : (x, y) = (376841, 33179), l = 62807, q = 15778876997$ n'est pas premier.
- $n = -1 : (x, y) = (-6031, 531), l = -1005, q = 4040101$ n'est pas premier.
- $n = 2 : (x, y) = (12703310099, 1118464089), l = 2117218350, q = 17930454166306890001$ n'est pas premier.
- $n = -2 : (x, y) = (-203305021, 17900009), l = -33884170, q = 4592547906355601$ est premier, $t = -67768339$
  donc $q + 1 - t = 4592547974123941 = 13 \times 2347 \times 150521057131$.

la solution trouvée pour $n = -2$ donne une cardinalité ayant un facteur premier de 37 bits et un degré de plongement $k = 6$. le pôlynome de classe de Hilbert pour $-D = -43$ est de degré 1:

$$H_{-43}(X) = X + 884736000$$

et admet 4592547021619601 comme racine modulo 4592547906355601. une courbe d'invariant modulaire
4592547021619601 sur $IF_{4592547906355601}$ est donnée par l'équation :

$$\widetilde{E}: y2 = X^3 + 2564278200474279\ X + 1709518800316186$$

on constate que le nombre de point de cette courbe n'est pas égal à $q + 1 - t$. il est donc égal à $q + 1 + t$, et on prend donc pour la courbe cherchée E une tordue de $\widetilde{E}$.
Par exemple :

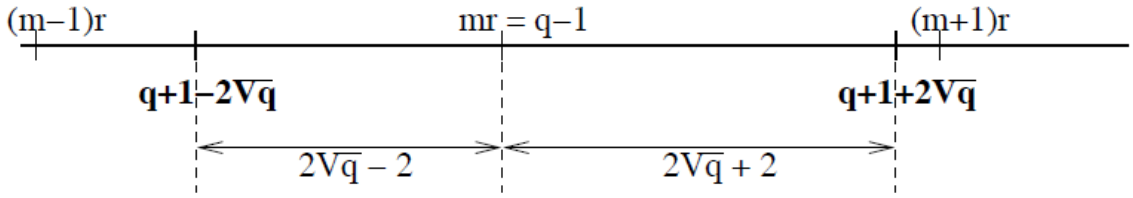
$$E : y^2 = x^3 + 1763476217229032x + 3447467182151685$$

il est à noter cependant que la méthode de multiplication complexe présentée ici ne permet pas de résoudre tous les probléme de construction de courbes:

Exemple: courbes de trace 2 et de degré de plogement $k = 1$).
lorsque r est un diviseur de $\#E(IF_q)$ assez grand , ou de façon plus précise $r \geq 2\sqrt{q}+2$, les courbes elliptiques admettant des points de $r -$ torsion et un degré de plogement égal à 1, ont nécessairement leur $q -$ iéme morphisme de Frobenuis de trace égale à 2.

En effet, si on note $I = \left[q + 1 - 2\sqrt{q}\ ; q + 1 + 2\sqrt{q}\ \right]$ l'intervalle des valeurs possibles pour $\#E(IF_q)$ donnée par la borne de Hasse, on a $(q - 1) \in I$ qui est le seul multiple

possible de r dans cet intervalle:



En particulier, $q - 1 = \#E(IF_q) = q + 1 - Tr\,\Phi_q$ et $Tr\,\Phi_q = 2$.
la construction d'une courbe de trace2 vérifiant les proprietés de la proposition precedente. dans lecas où le degré de plongement vaut 1 pose a priopi probleme.

si on utilise la méthode de multiplication complexe, on doit choisir un discriminant fondamental D sans facteur carré et petit, puis trouver $q = p^d$ et y tels que $4q - (Tr\Phi_q)^2 = y^2D$. dans ce cas precis, comme $Tr(Tr\Phi_q) = 2$, on a $y^2D = 4(q - 1)$,

en particulier si r est un grand facteur premier de $q - 1$, nécessairement r/y, donc $r^2/q - 1$.
D'autre méthode doivent donc être envisagées pour la construction de telles courbes.

4. Application des courbes Elliptiques en cryptologie :

Les couplages de $Weil$ et $Tate$ ont des propriétés particulièrement intéressantes pour la cryptographie, dans la mesure où on connaît un algorithme efficace pour les calculer.
A titre d'exemple, on présente dans ce qui suit une de leurs toutes premières applications (en 1993) à la cryptanalyse ainsi que des exemples célèbres de protocoles les utilisant.

Alg. 2 Algorithme de Miller amélioré

ENTRÉE : $P=(x_1,y_1)\in E(\mathbf{F}_q)[l]$, $Q=(x_2,y_2)\in E(\mathbf{F}_{q^k})[l]$, $l=(l_{k-1}...l_0)_2$
SORTIE : $f(Q)$ où f telle que $\mathrm{div}(f)=l(P)-l(O)$
(**Variables :** $T=(x_3,y_3)\in E(\mathbf{F}_q)$, $f_1,f_2,\lambda\in E(\mathbf{F}_{q^k})$)
$f_1\leftarrow 1$
$f_2\leftarrow 1$
$T\leftarrow P$
pour $i=k-1$ à 1 **faire**
  $\lambda\leftarrow$ coefficient de la tangente à E en T
  $f_1\leftarrow f_1^2(y_2-\lambda(x_2-x_3)-y_3)$
  $f_2\leftarrow f_2^2(x_2+2x_3-\lambda^2)$
  $T\leftarrow 2T$
  si $l_i=1$ **alors**
    $\lambda\leftarrow$ coefficient de la droite passant par P et T
    $f_1\leftarrow f_1(y_2-\lambda(x_2-x_1)-y_3)$
    $f_2\leftarrow f_2(x_2+x_3+x_1-\lambda^2)$
    $T\leftarrow T+P$
  fin si
fin pour
si $l_0=1$ **alors**
  $\lambda\leftarrow$ coefficient de la tangente à E en T
  $f_1\leftarrow f_1^2(y_2-\lambda(x_2-x_3)-y_3)$
  $f_2\leftarrow f_2^2(x_2+2x_3-\lambda^2)$
  $T\leftarrow 2T$
  $f_1\leftarrow f_1(x_2-x_1)$
  $T\leftarrow T+P$
sinon
  $f_1\leftarrow f_1^2(x_2-x_3)$
  $f_2\leftarrow f_2^2$
  $T\leftarrow 2T$
fin si
retourner $\frac{f_1}{f_2}$

4. 1 Attaque de $MOV/Frey-Ru\ddot{c}k$:

$(E(IF_q), +)$ étant un groupe commutatif, si $r \neq p$ est un diviseur premier du nombre de Points rationnels $\#E(IF_q)$ de la courbe, alors il existe un point $P \in E(IF_q)[\rho]$d'ordre r. Avec les mêmes notations que précédemment, on s'intéresse au problème du logarithme discret sur $E(IF_q)[r]$

Etant donnés $P, P' \in E(IF_q)[r]$ tels que : $[m]P = P'$, trouver m.

Pour une courbe elliptique quelconque, on ne connaît que des algorithmes génériques, type Baby step, Giant step de complexité en calcul exponentielle en $O(\sqrt{r})$ Grâce aux propriétés de bilinéarité et de non dégénérescence du couplage de $Tate$, il est possible de transférer ce problème dans le groupe multiplicatif d'un corps fini (attaque de $Frey - Ruck$ [FR94] ou attaque de $Menezes, Okamoto\ et\ Vanstone$ [MOV93]). En effet,

$\langle [m]P, Q\rangle = \langle P, Q\rangle^m \in \mu_r \subset IF_{q^k}$ où k est le degré d'immersion.

Si on choisit Q tel que $\langle P, Q\rangle \neq 1$, on se ramène au problème du log discret dans $IF_{q'}^*$ $(q' = q^k)$. Sur un tel groupe, il existe des algorithmes, basés sur le calcul d'index, de complexité sous $-$ exponentielle en $O\left(e^{c(\log q')^{\frac{1}{3}}(\log\log q')^{\frac{2}{3}}}\right)$.

En particulier pour les courbes admettant des sous $-$ groupes de r $-$ torsion pour lesquels le degré d'immersion k est proche de 1, l'attaque MOV est plus performante que les algorithmes standards .

$Menezes, Okamoto$ et $Vanstone$ ont également montré que le degré de plongement d'une courbe supersinguliére est toujours plus petit que 6 (voir section 4.2); il faut donc être particulièrement prudent lorsque l'on utilise ce type de courbe. Pour parer à l'attaque MOV, il sera nécessaire en particulier de prendre q grand.

Par exemple, supposons que l'on souhaite travailler avec une courbe supersinguliére définie sur IF_q, avec $k = 2$. Pour avoir une sécurité de 80 bits, r doit avoir au moins 160 bits afin de contrer les attaques génériques type Baby $-$ step, giant $-$ step; mais p^k doit aussi comporter au moins 1024 bits pour contrer l'attaque MOV, ce qui impose $|P|_2 \geq 512$. Le cofacteur de r dans $\#E(IF_p)$ est donc très grand, ce qui entraine une perte d'efficacité au niveau mémoire, temps de calcul et bande passante.

On décrit dans la suite les schémas cryptographiques à clé publique fondamentaux basés sur des couplages. Dans chaque cas, on précise les propriétés du couplage utilisées, ainsi que les hypothèses standards à faire pour assurer la sécurité.

4. 2 Hypothèses de sécurité liées aux couplages :

Dans les schémas cryptographiques que l'on va décrire, on utilise essentiellement deux types de couplages non dégénérés :

- les self $-$ pairings, de la forme $\hat{e}: G_1 \times G_2 \longrightarrow G_3$ bilinéaire et non dégénéré, où G_1et G_3 sont deux groupes cycliques d'ordre r premier.
- les couplages asymétriques, plus simples à construire, et qui sont de la forme $e: G_1 \times G_2 \longrightarrow G_3$ bilinéaire et non dégénéré, où G_1, G_2et G_3 sont des groupes cycliques d'ordre r premier.

Les courbes elliptiques (et hyperelliptiques)sont pour l'instant les seuls contextes connus dans lesquels de tels couplages sont calculables de façon efficace. Généralement, on prend $G_1 = \langle P \rangle$ où P est un point rationnel de r-torsion d'une courbe elliptique E définie sur IF_q ($q = p^d$,$l \neq p$ premier), $G_2 = \langle Q \rangle$ où $Q \in E(IF_{q^k})$ est un point de r-torsion non multiple de P et $G_3 = \mu_r \subset IF_{q^k}$ le groupe des racines $r - iéme$ de l'unité.

On rappelle que pour assurer la sécurité des cryptosystème classiques basés sur le calcul du logarithme discret, on utilise un groupe $G = \langle P \rangle$ noté additivement, dans lesquels l'un des trois problèmes suivants au moins est difficile :

- DDH ($Decisional\ Diffie - Hellman\ problem$) : étant donnés $P, [a]P, [b]P$ et $[c]P$, déterminer si $ab = c$.
- $CDH(Computational\ Diffie - Hellman\ problem)$: étant donnés $P, [a]P\ et\ [b]P$ Calculer $[ab]P$
- DL ($Discret\ Log\ problem$) : étant donnés $P\ et\ [a]P$, trouver α.

Ces trois problèmes sont clairement classés par ordre de difficulté croissante.

Mais lorsqu'on travaille avec des groupes admettant un couplage, ces problèmes ne sont plus nécessairement appropriés. Si par exemple, on considère pour simplifier les notations des $self-pairings$, c'est $-$ à $-$ dire des applications bilinéaires symétriques non dégénérés $\hat{e}: G_1 \times G_1 \longrightarrow G_3$ où$G_1 = \langle P \rangle$ est un groupe cyclique noté additivement, le problème DDH sur G_1 devient facile. Il est par contre pertinent d'introduire les problèmes suivants :

- $DBDH(Decisional\ Bilinear\ Diffie - Hellman\ problem)$: étant donnés $P, [a]P,$ $[b]P$ et $[c]P$ dans G_1 et $\hat{e}(P,P)^d$,déterminer si $\delta = \alpha\beta\chi$.

- BDH ($Bilinear\ Diffie - Hellman\ problem$) : étant donnés $P, [a]P, [b]P\ et\ [c]P$ dans G_1, calculer $\hat{e}(P,P)^{abc}$

- Inversion problème : étant donnés P et $\hat{e}([a]P, P)$,trouver $[a]P$.

Remarque 1: De la même façon qu'un algorithme permettant de résoudre DL peut être utilisé pour résoudre CDH et DDH,il est possible de trouver des relations entre les complexités de ces différents problèmes :

- $\boldsymbol{BDH \propto CDH_{G_1}}$

On suppose qu'on connaît un algorithme permettant de résoudre CDH sur G_1.
Avec cet algorithme, on peut, étant donnés $P, [a]P, [b]P\ et\ [c]P$, calculer $[ab]P$ puis $\hat{e}([ab]P, [c]P) = \hat{e}(P,P)^{abc}$, ce qui permet de résoudre BDH sur $\langle G_{1,} G_3, \hat{e} \rangle$.

- $\boldsymbol{BDH \propto CDH_{G_1}}$

Etant donnés $P, [a]P, [b]P\ et\ [c]P$, on peut calculer grâce à la bilinéarité $\hat{e}(P,P)^{bc} = \hat{e}([b]P, [c]P)$ $et\ \hat{e}(P,P)^a = \hat{e}([a]P, P)$ pour en déduire grâce à l'algorithme de

résolution de CDH_{G_3} le couplage $\hat{e}([ab]P,[c]P) = \hat{e}(P,P)^{abc}$,

- $\boldsymbol{BDH \propto Inv}$

Etant donnés $P, [a]P, [b]P\ et\ [c]P$,on peut calculer $\hat{e}([a]P,[b]P)$= $\hat{e}([ab]P\ ,P)$ et en déduire $[ab]P$ grâce à l'algorithme d'inversion. Il est alors facile de calculer $\hat{e}([ab]P,[c]P) = \hat{e}(P,P)^{abc}$

- $\boldsymbol{DDH_{G_3} \propto Inv}$

La loi de groupe sur G_3étant notée multiplicativement, on cherche étant donnés g, g^a, g^b, g^c à déterminer si $g^c = g^{ab}$ .Grâce à Inv,on peut déduire de g^a(resp.g^b, g^c) la valeur de $[a]P$ (resp $[b]P$, $[c]P$). Avec les propriétés du couplage, il est alors facile de déterminer si $\hat{e}([ab]P\ ,P) = \hat{e}([a]P,[b]P)$ est égal à $\hat{e}([c]P,P\ )$

Par contre la réduction $CDH \propto BDH$ est encore un problème ouvert (voir[BF03], [Jou04]).

Il est par ailleurs possible d'adapter ces problèmes au cas où le couplage serait asymétrique. Par exemple, pour un couplage $e: G_1 \times G_2 \longrightarrow G_3$,on définit le problème suivant :
$\boldsymbol{co-BDH}$ (Co-bilinear $Diffie-Hellman$ problem) : étant donnés P (resp. Q) un générateur de G_1 (resp. G_2), $[a]P$,$[b]P$,$[a]Q\ et\ [c]Q$ calculer $e(P,Q)^{abc}$.

4. 3 Distribution non interactive de clés basée sur l'identité :

En 2000, $Sakai, Ohgishi\ et\ Kasahara$ ([SOK00]) ont mis au point une version non interactive du protocole d'échange de clés en utilisant des couplages. Dans ce contexte, on se donne :
–un système de paramètres $\{G_1, G_3, \hat{e}\}$, où G_1 et G_3 sont des groupes cycliques d'ordre r, et $\hat{e}: G_1 \times G_1 \longrightarrow G_3$ est une application bilinéaire, symétrique et non dégénérée.
– une fonction de hachage $H_1: \{0;1\}^* \longrightarrow G_1$ Un tiers de confiance ou PKG (Private Key Generator)est responsable de la certification de l'identité d'un intervenant et de la maintenance du système de paramètres. Il détient une clé secrète $S \in \mathbb{Z}_r^*$,appelée master Key, permettant de délivrer à un intervenant une clé secrète basée sur son identité. Pour obtenir un secret commun, Alice et Bob suivent les deux étapes suivantes du protocole :

1. chacun demande au PKG de lui générer un secret S à partir de sa propre identité (on peut prendre par exemple comme identifiant son adresse de courrier électronique) :
   – Alice reçoit $S_A = [S]Q_A$, où $Q_A = H_1(Id_A)$
   – Bob reçoit $S_B = [S]Q_B$ où $Q_B = H_1(Id_B)$

2. chacun peut alors calculer la clé commun K_{AB} sans discussion préalable :
   – Alice calcule $K_{AB} = \hat{e}\big(S_A, H_1(Id_B)\big) = \hat{e}(Q_A, Q_B)^S$
   – Bob calcule $K_{AB} = \hat{e}(H_1(Id_A), S_B) = \hat{e}(Q_A, Q_B)^S$

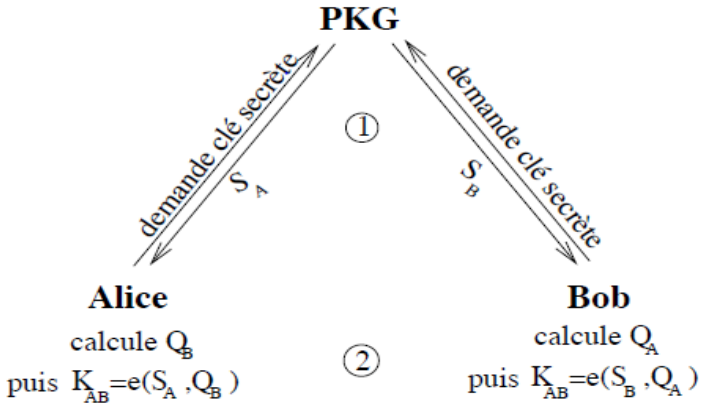


FIG. 2 – Distribution non interactive de clés basée sur l'identité

Remarque1 :
Les rôles d'*Alice* et de *Bob* étant complètement symétriques, une seule fonction de hachage à valeurs dans G_1 est utilisée, ce qui justifie l'utilisation d'un self-pairing.

Sécurité:
Il est clair que si Charlie sait résoudre le problème BDH, alors il est facile pour lui de retrouver la clé secrète K_{AB} d'*Alice et Bob* . En effet, *Charlie* connaît l'identité d'*Alice* et *Bob*, donc peut calculer Q_A *et* Q_B, il choisit alors un point Q comme générateur de G_1(par exemple $Q = H_1(Id_C)$ et demande au PKG de calculer la valeur $[S]Q$.
S'il sait résoudre BDH, connaissant $Q, Q_A = [a]Q$, $Q_B = [b]Q$ *et* $[s]Q$, il peut calculer $\hat{e}(Q,Q)^{abs} = \hat{e}(Q_A, Q_B)^S = K_{AB}$.

Dupont et *Enge* ([DE06]) ont prouvé pour une version quasi-similaire à celle de [SOK00] qu'être capable de trouver la clé dégénérée par ce protocole est aussi difficile que de résoudre le problème BDH.

Comparaison avec le schéma de distribution de clé ECDH :
Une alternative courante pour qu'Alice et Bob puissent s'échanger une clé est d'utiliser le protocole $ECDH$ (Elliptic Curve $Diffie - Hellman$). Dans le schéma $Diffie - Hellman$ original, on dispose d'un groupe Γ d'ordre premier r engendré par un point P pour lequel CDHest difficile. Alice choisit un secret $a \in \mathbb{Z}_r^*$ et envoie $qA = [a]P$ à Bob.
De même Bob envoie à Alice $qB = [b]P$ où $b \in \mathbb{Z}_r^*$ est son secret. Ils peuvent alors Calculer leur clé secrète commune $K_{AB} = [a]q_B = [b]q_A = [ab]P$, et un attaquant passif reste impuissant tant que CDH est difficile sur $G = \langle P \rangle$.

Cette version de $Diffie - Hellman$ n'est cependant pas satisfaisante puisqu'Alice et Bob ne s'authentifient pas l'un auprès de l'autre, en particulier une attaque type "man-in-the -middle" est rendue possible. Pour que Bob puisse être sûr que q_A a bien été envoyé par *Alice*, celle-ci doit tout d'abord posséder un jeu de clés (k_p^A, k_s^A) , ainsi qu'un certificat, contenant son identité et sa clé publique k_p^A , qui est signé par une autorité de certification (AC). Elle peut alors signer q_A avec sa clé privée k_s^A et Bob vérifie la signature avec la clef publique k_p^A figurant dans son certificat.

Il est intéressant de comparer les avantages et inconvénients de ces deux protocoles

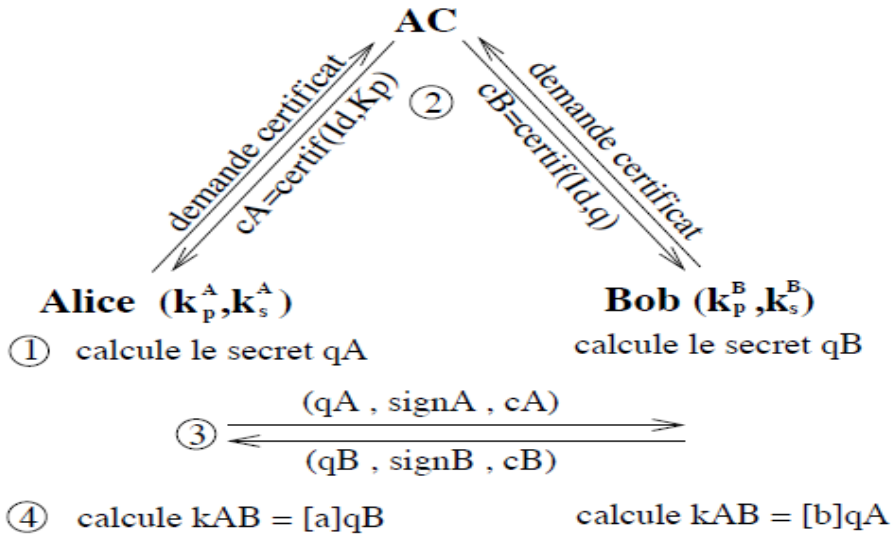


FIG. 3 – Distribution de clé ECDH avec signature et certificat.

Protocole de [SOK00]	Protocole ECDH
- *identity-based* : l'identité d'un intervenant est utilisée comme clé publique de celui-ci - Alice peut calculer la clé K_{AB} sans aucune intervention de Bob - demande au PKG d'un secret - Confiance totale accordée au PKG : celui-ci peut en effet faire un séquestre de clés (*key escrow*)	- *non identity-based* : un certificat est nécessaire pour associer une clé publique à un intervenant - Alice doit attendre de recevoir la valeur q_B calculée par Bob pour pouvoir calculer la clé commune k_{AB} - demande à l'AC d'un certificat pour la clé publique servant à signer - Pas de sequestre de clé possible

4.4 Un protocole $Diffie-Hellman$ pour trois parties en un tour :

Une idée naïve de protocole $Diffie-Hellman$ pour trois parties permettrait à Alice, Bob et Charlie d'échanger un secret après 2 tours : on se donne un groupe G d'ordre premier r engendré par P, et chaque intervenant procède de la façon suivante

	Alice	*Bob*	*Charlie*
Secret	A	B	C
1ere tour	envoie $[a]P$ à Bob	envoie $[b]P$ à Charlie	envoie $[c]P$ à Alice
2éme tour	envoie$[a]([c]P)$à Bob	envoie$[b]([a]P)$ à Charlie	*envoie* $[c]([b]P)$ à Alice
Calcul de K_{ABC}	$[a]([cb]P)$	$[b]([ac]P)$	$[c]([ba]P)$

En 2000, $Joux$ propose une version de ce protocole en un tour utilisant des couplages ([Jou04]):

on dispose d'un système de paramètres $(G_1, G_2, \hat{e}, P)$ où G_1 est un groupe cyclique d'ordre premier r engendré par P et $\hat{e}: G_1 \times G_1 \longrightarrow G_3$ est un self-pairing. On modifie le protocole précédent de la façon suivante :

	Alice	Bob	Charlie
Secret	a	b	c
1er tour	broadcast $[a]P$	broadcast $[b]P$	broadcast $[c]P$
Calcul de K_{ABC}	$\hat{e}([b]P, [c]P)^a$	$\hat{e}([a]P, [c]P)^b$	$\hat{e}([a]P, [b]P)^c$

Ici encore, la sécurité est basée sur BDH

Comme c'est le cas dans l'article original de[$Jou04$], il est possible de faire un échange entre trois parties sans utiliser de self − pairing : on choisit un système de paramètres $(G_1, G_2, G_3, \hat{e}, P)$ où G_1 et G_3 sont des groupes cycliques d'ordre premier r ,ainsi qu'un couplage bilinéaire $e: G_1 \times G_2 \longrightarrow G_3$ non dégénéré. Le protocole à Suivre est :

	Alice	Bob	Charlie
Secret	a	b	c
1er tour	broadcast $[a]P, [a]Q$	broadcast$[b]P, [b]Q$	broadcast $[c]P, [c]Q$
Calcul de K_{ABC}	$e([b]P, [c]Q)^a$	$e([a]P, [c]Q)^b$	$e([a]P, [b]Q)^c$

L'avantage de ce schéma est que l'on peut utiliser directement le couplage de$Tate$ (ou $Weil$) sur n'importe quel type de courbe. Cependant il présente l'inconvénient d'utiliser deux fois plus de bande passante, puisque chaque intervenant ayant pour secret s doit transmettre $[s]P$ et $[s]Q$. Sa sécurité s'appuie sur l'hypothèse que $co - BDH$ est difficile.

4. 5 Le chiffrement de Boneh − Franklin basé sur l'identité :

Le chiffrement proposé par $Boneh - Franklin$ en 2001 est considéré comme l'application la plus importante des couplages en cryptographie, puisqu'il répond à un problème de chiffrement basé sur l'identité posé par *Shamir* en 1986 et resté jusqu'alors sans réponse [Sha85].

On présente la version la plus simple (Basic Ident)de ce chiffrement, afin de mettre en valeur les idées principales de *Boneh-Franklin*. Un schéma plus complet et prouvé plus sûr (Full Ident) est également donné dans [BF03].

On se place dans le même type d'infrastructure que pour [SOK00] : le BKG publie un système de paramètres $(G_1, G_3, \hat{e})$,un générateur Π deG_1, ainsi que le point $P_{pub} = [s]$P obtenu à partir de la clé maître (master Key)$s \in \mathbb{Z}_r^*$.En plus de $H_1: \{0;1\}^* \longrightarrow G_1$, on met à disposition des utilisateurs une 2éme fonction de hachage $H_2: G_3 \longrightarrow \{0;1\}^n$, où n est le nombre de bits des messages transmis.

De façon générale, un schéma de chiffrement basé sur l'identité (IBE) est défini par la donnée de 4 algorithmes ***Setup***, ***Extract*** (qui fournit à un intervenant une clé privée basée sur son

identité) , ***Encrypt*** et ***Decrypt*** .On donne le détail de ces algorithmes pour le schéma de *Boneh-Franklin :*

– ***Setup*** prend en entrée un paramètre de sécurité à partir du quel sont générés les paramètres du système décrits précédemment : $\langle G_{1,}, G_3, \hat{e}, P, P_{pub}, H_1, H_2 \rangle$

L'espace des messages est $M = \{0;1\}^n$ et l'espace des chiffrés est $C = G_1 \times \{0;1\}^n$

– ***Extract*** prend en entrée l'identité Id d'un utilisateur et fournit à celui-ci la clé privée correspondante $S_{Id} = [s]H_1(Id)$

– ***Encrypt*** permet de chiffrer un message$M \in \mathcal{M}$ destiné à un utilisateur à partir de son identité Id en 3 étapes :

1. Calculer : $Q_{Id} = H_1(Id) \in G_1$
2. Tirer un nombre aléatoire : $t \in \mathbb{Z}_r^*$
3. Calculer le chiffré C de M: $C = \langle [t]P, M \oplus H_2\left(\hat{e}\left(Q_{Id},, P_{pub}\right)^t\right)\rangle$

– ***Decrypt*** permet de déchiffrer $C = \langle C_1, C_2 \rangle$ adressé à l'utilisateur Id grâce à sa clé privée S_{Id} en calculant

$$M' = C_2 \oplus H_2\left(\hat{e}(S_{Id}, C_1)\right)$$

Pour vérifier la consistance de ce schéma, il suffit de remarquer que

$$\hat{e}\left(Q_{Id},, P_{pub}\right)^t = \hat{e}(Q_{Id}, P)^{st} = \hat{e}([s]Q_{Id}, [t]P) = \hat{e}(S_{Id}, C_1)$$

Sécurité :

Comme dans [$SOK00$], on peut réduire la sécurité de ce schéma à BDH: siBob adresse un message chiffré $C = \langle C_1, C_2 \rangle$ à Alice, Charlie a accès à , $P, P_{pub} = [s]P$, $C_1 = [t]P$ et $Q_A = H_1(Id_A) = [a]P$ (la clé publique d'Alice) et donc peut calculer, avec un algorithme résolvant BDH, $\hat{e}\ (P,P)^{sat} = \hat{e}\left(P_{pub}, Q_A\right)^t$, ce qui lui permet de retrouver le message clair. Réciproquement, *Boneh* et *Franklin* montrent que dans le modèle de l'oracle aléatoire, le chiffrement décrit (BasicIdent) est sémantiquement sûr contre les attaques à texte clair choisi en autorisant des requêtes de clés privées (*IND-ID-CPA*) sous l'hypothèse que *BDH* est difficile.

Remarque 2:

On constate qu'il est tout à fait possible de remplacer le self-pairing $\hat{e}$ par un couplage asymétrique $e: G_1 \times G_2 \longrightarrow G_3$

– on modifie ***Setup*** en prenant $P, P_{pub} \in G_2$,

– dans ***Extract***, on choisit des clés $S_{Id} = [s]Q_{Id} \in G_1$

– ***Encrypt*** et ***Decrypt*** fonctionnent de la même façon en remplaçant $\hat{e}$ par e.

En particulier, on peut utiliser pour ce schéma une variété de courbes elliptiques plus étendue.

Conclusion:

Un couplage est une application notée $\mathbf{e}$: $(\mathbf{G_1},+)\times(\mathbf{G_2},+)\to(\mathbf{G_3},+)$où : $(\mathbf{G_1},+)$ et $(\mathbf{G_2},+)$sont des groupes abéliens, le plus souvent des sous $-$ groupes de courbe elliptique définie sur un corps fini, et $(\mathbf{G_3},\times)$un groupe multiplicatif (commutatif) vérifiant :

- $\forall P,P'\in G_1,\forall Q,Q'\in G_2:\ e(P+P',Q)=e(P,Q).e(P',Q)$
  $et\quad e(P,Q+Q')=e(P,Q).e(P,Q')$ $(Bilinéarité)$
- $\forall P\in G_1\neq\{0\},\exists Q\in G_2\ tel\ que\ e(P,Q)\neq 1$ $(non\ dégénérescence)$

Ainsi, et comme conséquence : $\forall k\in Z,\ e(kP,Q)=e(P,Q)^k=e(P,kQ)$

La propriété de bilinéarité d'un couplage a permis de transférer le problème du logarithme discret, problème qui consiste à déterminer l'entier **n** connaissant les points **P** et **nP**, depuis le groupe $\mathbf{E}(\mathbf{K})$des points $\mathbf{K}-$ rationnels d'une courbeelliptique définie sur le corps fini **K**, en un problème de logarithme discret sur un corps fini beaucoup plus facilement résoluble (attaque MOV en 1993 et $Frey\ Rück$ en 1994).

Depuis quelques années, la recherche sur l'application des couplages aux constructions de protocoles cryptographiques a débouché sur de nombreux résultats substantiels tels que les constructions de protocoles cryptographiques robustes, comme le chiffrement bas sur l'Identité développé par $Boneh$ et $Franklin$ en 2001, l'échange de $Diffie\ Hellman$ à trois conçu par $Joux$ en 2001, les schémas de signature courte proposés par $Boneh$, $Lynn$ et $Shacham$ en 2001 : les couplages les plus utilisés dans ce cadre sont ceux de $Weil$ et $Tate$ et se présentent comme les outils les plus utilisés à l'heure actuelle en cryptographie.

Le calcul d'un couplage nécessite la connaissance des éléments suivants :

- Une courbe elliptique
  $\frac{E}{K}=\left\{(x,y)\in KxK,\ y^2=x^3+ax+b\right\}\cup\{0_E\}$ où K est un corps (commutatif) contenant
- un corps fini IF_p , $a\ et\ b\ \in IF_p$;
- **r** un premier divisant $\mathrm{E}(\mathrm{IF_p})$, ainsi que l'ensemble $E[r]=\left\{P\in E(\bar{IF}_p);[r]P=0_E\right\}$

- Le degré de plongement $\boldsymbol{k}$ défini comme étant le plus petit entier tel que r \ $(p^k - 1)$ on a alors $\boldsymbol{E[r] \subset E(F_{p^k})}$.
- La fonction rationnelle de *Miller* notée $\boldsymbol{f_{r,P}}$ admettant **P** comme zéro d'ordre **r** et le point $\boldsymbol{[r]P}$ comme pôle.

La principale difficulté est de pouvoir calculer ces couplages avec des algorithmes qui soient les plus rapides possibles : l'algorithme le plus utilisé jusqu'à présent a été proposé par *Miller* en 1985 (qui renvoie précisément **fr**, **P**), mais depuis l'apparition de la cryptographie à base de couplages, les efforts se concentrent sur l'optimisation de cet algorithme.

Le but de notre travail a été double : d'abord rappeler la théorie des courbes elliptiques notamment sur des corps finis, puis donner un aperçu de l'algorithmique des couplages à base de courbes elliptiques, en présentant les aspects constructifs et calculatoires de ces applications bilinéaires.

Les perspectives en ce domaine seraient de tenter d'optimiser les protocoles déjà existants (en termes de temps de calcul), et peut − être de concevoir de nouveaux protocoles cryptographiques basés sur les couplages, non plus sur des courbes elliptiques, mais sur courbes algébriques plus générales, bien adaptées aux applications.

📖[*ADMRK*02] ***E*.*Al* − *Daoud***, ***R*.*Mahmod***, ***M*.*Rushdan***, *and* ***A*.*Kilicman***. *A new additionformula for elliptic curves over GF*(2 *n*). *IEEE Transactions on Computers*, 51 : *pages*(972_975), 2002.

📖 [*AM*93] ***A*.*O*.*L*.*Atkin*** *and* ***F*.*Morain***. *Elliptic curves and primality proving*. *Math*. *Comp*., 61(203), (*pages* : 29– 68),1993.

📖[*BF*03] ***Dan Boneh*** *and* ***Matthew Franklin***. *Identity − based encryption from the Weil pairing*. *SIAM J*. *Comput*., 32(3)(*pages* : 586– 615), (*electronic*), 2003.

📖[BJ02] ***E. Brier & M. Joye***. *Weierstrass elliptic curve and side-channel attacks. In Public Key Cryptography, (PKC), volume 2274 of LNCS, (pages 335- 345*)2002

📖[*BK*98] ***R*.*Balasubramanian*** *and* ***Neal Koblitz***.*The improbability that an elliptic curve has subexponential discrete log problem under the Menezes − Okamoto − Vanstone algorithm*. *J*. *Cryptology*, 11(2) : *pages*(141– 145),1998.

📖[*BSS* 00] ***I*.*F*.*Blake***, ***G*.*Seroussi***, *and* ***N*.*P*.*Smart***. *Elliptic curves in cryptography*, *volume* 265 *of London Mathematical Society Lecture Note Series*. . *Reprintof the* 1999 *original*. *Cambridge University Press*, *Cambridge*, 2000.

📖[*CFA*06] ***Henri Cohen***, ***Gerhard Frey***, ***Roberto Avanzi***, ***Christophe Doche***, ***Tanja Lange***, ***Kim Nguyen***, ***and Frederik Vercauteren***, *editors*. *Handbook of elliptic and hyperelliptic curve cryptography*. *DiscreteMathematics and its Applications* (*Boca Raton*). *Chapman & Hall/CRC*, *Boca Raton*, *FL*, 2006.

📖[*CF*06] ***H*.*Cohen*** & ***G*.*Frey***. *editors* . *Handbook of Elliptic and Hyperelliptic Cryptography*. *Chapman & Hall*. 2006.

📖[*CMO*98] ***H*.*Cohen***, ***A*.*Miyaji***, & ***T*.*Ono***, *Efficient elliptic curve exponentiation using mixed coordinates*. *In ASIACRYPT*, *LNCS*. *Springer*1998

📖[*Coh*93] ***Henri Cohen***. *A course in computational algebraic number theory*, *volume* 138 *of Graduate Texts in Mathematics*. *Springer − Verlag*, *Berlin*, 1993.

📖[*DE*06] ***Régis Dupont*** *and* ***Andreas Enge***. *Provably secure non − interactive keydistribution based on pairings*. *Discrete Appl*. *Math*., 154(2), (*pages* : 270– 276), 2006

📖[*FH*02] ***F*.*Heb*** : *A Note on the Tate Pairing of Curves over Finite Fields*, 2002. *Submitted preprint*.

📖[*FR*94] ***Gerhard Frey*** *and* ***Hans − Georg Rück***. *A remark concerning m − divisibilityand the discrete logarithm in the divisor class group of curves*. *Math*. *Comp*., 62(206), (*pages* : 865– 874), 1994.

🕮[*Gal*05] ***Steven D. Galbraith***. *Pairings. In Advances in elliptic curve cryptography, volume* 317 *of LondonMath. Soc. Lecture Note Ser.* (*pages* 183– 213). *Cambridge Univ. Press, Cambridge*, 2005.

🕮[*GH*94] ***G. Frey, H. R*Äuck** : *A remark concerning m − divisibility and the discrete logarithm in the divisor class group of curves, Mathematics of Compu − tation*, 62 (*pages*. 865 − 874)1994.

🕮[*GR*04] ***Steven D. Galbraith*** *and* ***Victor Rotge****r. Easy decision Diffie − Hellman groups. LMS J. Comput. Math.*, 7 : 201– 218 (*electronic*), 2004.

🕮[*HMV*04] ***D. Hankerson, A. Menezes*** & ***S. Vanstone***. *Guide to Elliptic Curve Cryptography. Springer*2004.

🕮[*HT*00] ***A. Higuchi*** & ***N. Takagi***. *A fast addition algorithm for elliptic curve arithmetic in gf*(2*n*)*using projective coordinatates. Inf. Process. Lett.*, 76(3): , (*pages* 101 − 103)2000

🕮[*Jou*04] ***Antoine Joux***. *A one round protocol for tripartite Diffie − Hellman. J. Cryptology*, 17(4), (*pages* : 263– 276),2004

🕮[*KJJ*99]***P. Kocher, J. Jaffe***, & *B. Jun. Differential power analysis. In Advancesin cryptology − CRYPTO, volume* 1666 *of LNCS, pages* 388_397. *Springer*, 1999
.

🕮[*Koc*96]***P. Kocher***. *Timing attacks on implementations of diffe hellman, RSA, DSS and other systems. In Advances in cryptology − CRYPTO, volume* 1109 *ofLNCS*. (*pages* 104_113). *Springer.august* 1996

🕮[*Lan*04]***T. Lange***. *A note on lópez dahab coordinates. Technical report, Technical University of Denmark*, 2004.

🕮[*LD*98] ***J. Lopez*** & *R. Dahab. Improved algorithms for elliptic curve arithmetic in GF*(2 *n*). *In Selected Areas in Cryptography, SAC, volume* 1556 *of LNCS*, , (*pages* 201 − 212). *Springer*. 1998

🕮[*LD*99] ***J. Lopez*** & *R. Dahab. Fast multiplication on elliptic curves over GF*(2*m*) *without precomputation. In Cryptographic Hardware and Embedded Systems, (CHES), volume* 1717 *of LNCS*, (*pages* 316_327). *Springer*1999.

🕮[*Mat*00] ***Keith Matthews***. *The Diophantine equation* $x^2 - Dy^2 = N, D > 0$. *Expo. Math.*, 18(4), (*pages*: 323– 331),2000.

🕮[*Mil*86] ***Victor S. Miller***. *Short programs for functions on curves. In IBM Thomas J. Watson ResearchCenter, http ://crypto. stanford. edu/miller/miller. ps*. 1986

🕮[*Mil*04] ***Victor S. Miller***. *The Weil pairing, and its efficient calculation. J. Cryptology*, 17(4) , (*pages* 235– 261)2004

📖[MNT01] **Atsuko Miyaji**, **Masaki Nakabayashi**, and **Shunzo Takano**. New explicit condition of elliptic curve traces for FR − reductions. IEICE Trans. Fundamentals, E84(5), (pages: 1234– 1243), 2001

📖[Mon87] **P. Montgomery**. Speeding the pollard and elliptic curve methods of factorization. Mathematics of Computation, 48: (pages 243 − 264)1987.

📖[MOV93] **Alfred J. Menezes**, **Tatsuaki Okamoto**, and **Scott A. Vanstone**. Reducing elliptic curve logarithms to logarithms in a finite field. IEEE Trans. Inform. Theory, 39(5), (pages : 1639– 1646), 1993

📖[MWZ96] **A. J. Menezes**, **Y. H Wu** & R. J. Zuccherato. An elementary introduction to hyperelliptic curves. Technical report, Departement of C&O, University of Waterloo, 1996

📖[QS01] **J. J. Quisquater** &D. Samyde. Electromagnetic analysis (ema) : Measures and counter − measures for smart cards. In Proceedings of the International Conference on Research in Smart Cards : Smart Card Programming and Security, volume 2140 of LNCS, (pages 200_210). Springer2001.

📖[Sha85] **Adi Shamir**. Identity − based cryptosystems and signature schemes. In Advances in cryptology (Santa Barbara, Calif., 1984), volume 196 of Lecture Notes in Comput. Sci., (pages 47– 53). Springer, Berlin, 1985.

📖[Sch00]**W. Schindler**. A timing attack against rsa with the chinese remainder theorem. In Cryptographic Hardware and Embedded Systems (CHES), volume 1965 of LNCS, (pages 109_124). Springer2000.

[ShI71] **SHIMURA Goro**. «Introduction to the Arithmetic Theory of Automorphic Function », Princeton University Press, 1971 .

📖[Sho97]**V. Shoup**. Lower bounds for discrete logarithms and related problems. In Eurocrypt, volume 1233 of LNCS, (pages 256_266)1997.

📖[Sil86] **J. H. Silverman**. The Arithmetic of Ellitpic Curves. . Classification AMS = 1401, 14G 99, 14H 05, 14 K 15. GT − Springer1986

📖[SOK00] **Ryuichi Sakai**, **Kiyoshi Ohgishi**, and **Masao Kasahara**. Cryptosystems based on pairing. In Proc. Of SCIS 2000, 2000.

📖[SX95] **Henning Stichtenoth and Chao Ping Xing**. On the structure of the divisor class gr

of a class of curves over finite fields. Arch. Math. (Basel), 65(2): (pages: 141– 150), 1995

.

📖[Ver04] **Eric R. Verheul**. Evidence that XTR is more secure than supersingular elliptic

curve cryptosystems. J. Cryptology, 17(4): (*pages*: 277– 296), 2004

📖[*Wat*69] ***William C. Waterhouse***. *Abelian varieties over finite fields. Ann. Sci. Ecole Norm. Sup.* (4), 2 : (*pages*: 521– 560), 1969

📖[*Z*´00] ***Gilles Zémor***. *Cours de cryptographie, volume* 6 *of Enseignement des Mathématiques. Cassini, Paris*, 2000.

📖[*ZM*07] ***M. ZITOUNI***. *Géométrie, Arithmétique et Algorithmique des Courbes Elliptiques . OPU − Alger*, 2007.