

Applications des couplages en cryptographie

Lê Thái Hoàng

12th July 2005

Remerciements

Ce rapport est mon mémoire de stage du master "Algèbre et Géométrie" de l'université Paris 6, effectué au sein du département informatique de l'ENS. Je tiens à remercier mon directeur de stage Prof. Jacques Stern et Phong Nguyen qui m'ont offert l'occasion de découvrir un nouveau domaine. Je suis reconnaissant du département informatique qui m'a envoyé à la conférence sur les couplages en Irlande pour enrichir mes connaissances sur ce domaine très actif et expérimenter pour la première fois une conférence de recherche. Je voudrais aussi remercier mes collègues dans l'équipe GRECC qui m'ont accueilli dans une ambiance chaleureuse lors du stage, spécialement Hiệu et Michel qui m'ont beaucoup aidé et donné des conseils pour ce rapport.

Contents

1	Introduction	4
2	Courbes elliptiques	7
2.1	Courbes algébriques	7
2.1.1	Fonctions sur des courbes algébriques	8
2.1.2	Morphismes de courbes	9
2.1.3	Diviseurs	10
2.1.4	Reciprocité de Weil	11
2.2	Courbes elliptiques	12
2.3	Loi de groupe	13
2.4	Isogénies	14
2.5	Courbes elliptiques définies sur des corps finis	16
3	Couplages	19
3.1	Couplage de Weil	19
3.2	Couplage de Tate	23

3.3	Algorithme de Miller	25
3.3.1	L'algorithme	25
3.3.2	Implantations efficaces	28
3.4	Plongement de MOV et de FR	29
3.4.1	Les plongements	29
3.4.2	Degré de plongement	30
3.5	Distorsions	32
3.5.1	Définitions	33
3.5.2	Utilisation en cryptographie	34
3.6	Conditions cryptographiques	35
4	Applications	37
4.1	La structure de groupe de $E(\mathbf{F}_q)$	37
4.2	Protocole de Diffie-Hellman pour trois parties	38
4.3	Le problème de Diffie-Hellman dans les groupes de couplage	39
4.4	Chiffrement à base d'identité	40

Chapter 1

Introduction

L'étude des courbes elliptiques en mathématiques remonte au problème des nombres congrus, un des problèmes non résolus les plus anciens en théorie des nombres. Le nom "elliptique" vient probablement des fonctions complexes doublement périodiques qui sont liées avec les courbes elliptiques sur \mathbb{C} . Cependant, ce n'est qu'au début du 20^e siècle que la théorie des courbes elliptiques est formalisée et étudié avec les travaux de Mordell. A ce jour les courbes elliptiques sont devenues un sujet de recherche très actif avec la preuve célèbre du théorème de Fermat.

Quoique anciennes, les courbes elliptiques ne sont entrées en scène en cryptographie, plus précisément, en cryptographie à clé publique qu'il y a une vingtaine d'années. La cryptographie à clé publique est, elle aussi, un sujet moderne. C'est une invention de Diffie et Hellman en 1975, mais ce n'est que trois ans plus tard qu'on a un exemple concret avec le chiffrement qui porte le nom de Rivest, Shamir et Adelman. L'utilisation des courbes elliptiques est l'initiative de H. W. Lenstra en 1985 pour la factorisation des entiers. Dans la même année, Koblitz et Miller ont indépendamment proposé les courbes elliptiques pour des protocoles cryptographiques.

Une des propriétés importantes des courbes est l'existence d'une structure de groupe abélien sous-jacente les points d'une courbe. Sur une courbe, la loi de groupe est relativement facile à calculer mais le problème du logarithme discret est difficile faute d'algorithme effectif par rapport à son homologue pour le groupe multiplicatif d'un corps fini.

D'ailleurs sur les courbes elliptiques, il existe des fonctions dont les corps finis manquent. Ce sont les couplages de Weil et de Tate. 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. Le calcul des couplages a été cru inefficace jusqu'à l'invention de l'algorithme de Miller en 1986. Cependant, à l'époque les couplage n'avaient pas encore trouvé d'applications concrètes.

Les premières applications des couplages en cryptologie sont cryptanalytiques. En 1993 Menezes et al. utilisent le couplage de Weil pour réduire le problème du logarithme discret sur une courbe à celui dans un corps fini. Un an plus tard, Frey et 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 avec les travaux de Sakai, Ohgishi, et Kasahara. L'application la plus impressionnante des couplages est le chiffrement à base d'identité. Boneh et Franklin proposent 2001 un schéma fondé sur les couplages et qui est entièrement réalisable, ainsi résolvant le problème posé par Shamir en 1984. En suite les couplages ont trouvé de nombreuses applications : signature à base d'identité, signature courte, etc., et plus encore à venir. En ce moment les couplages sont un sujet très actif en cryptographie à base des courbes elliptiques.

D'un point de vue philosophique, on voit une similitude entre l'histoire des courbes elliptiques et l'histoire des couplages : d'abord ils sont utilisés pour "faire du mal", c'est à dire pour des buts cryptanalytiques, et après ils sont utilisés pour "faire du bien", c'est à dire pour des buts cryptographiques. Cela dit, en cryptologie, rien n'est utilisé pour un usage unique, tant bien que mal.

On présente le plan du rapport :

Dans le chapitre 2, on définit et étudie les courbes elliptiques, notamment celles sur un corps fini. On énonce et démontre quelques propriétés et résultats importants dont on a besoin pour la suite, dont la réciprocité de Weil, qui est cruciale dans la définition des couplages de Tate et de Weil. Les références pour ce chapitre sont [3] et [2].

Dans le chapitre 3, on définit les couplages de Tate et de Weil et démontrent

leurs propriétés. On décrit aussi l'algorithme de Miller pour calculer les couplages. On va ensuite discuter sur les plongements des points d'une courbes dans un corps via les couplages, ainsi que sur les distorsions, qui servent à trouver des points indépendents.

Le chapitre 4 est consacré aux applications des couplages en cryptographie, y compris le protocole de Diffie-Hellman pour trois parties et le chiffrement à base d'identité.

Chapter 2

Courbes elliptiques

2.1 Courbes algébriques

D'abord on rappelle les notions préliminaires sur les variétés affines et projectives. Soit K un corps, \bar{K} sa clôture algébrique. L'espace affine \mathbf{A}^n est l'ensemble des n -uplets (x_1, \dots, x_n) avec $x_i \in \bar{K}$. L'espace projectif \mathbf{P}^n est l'ensemble des classes d'équivalence de $\mathbf{A}^{n+1} \setminus (0, \dots, 0)$ avec la relation d'équivalence $(x_0, \dots, x_n) \sim (y_0, \dots, y_n)$ s'il existe $0 \neq \lambda \in \bar{K}$ tel que $x_i = \lambda y_i$ pour tout i . La classe de (x_0, \dots, x_n) est notée $[x_0, \dots, x_n]$. Une fois l'indice i fixé, \mathbf{A}^n s'identifie à un sous-ensemble de \mathbf{P}^n via l'application

$$\phi_i : (x_1, \dots, x_n) \mapsto [x_1, \dots, x_{i-1}, 1, x_i, \dots, x_n]$$

Un ensemble algébrique dans \mathbf{A}^n est l'ensemble des solutions d'un système d'équations polynomiales à coefficients dans K . À un ensemble algébrique V on associe l'idéal $I(V)$ des polynômes $P \in K[x_1, \dots, x_n] = K[X]$ annihilant les points de V . V est dit une variété si $I(V)$ est un idéal premier dans $\bar{K}[X]$. Pour une variété V son corps des fonctions est le corps des fractions de l'anneau intègre $K[V] = K[X]/I(V)$. Sa dimension, notée $\dim(V)$, est le degré de transcendance de $\bar{K}(V)$ sur \bar{K} . Une variété V est lisse au point P si pour tout système (f_1, \dots, f_m) de générateurs de $I(V)$, la matrice $(\partial f_i / \partial x_j(P))_{1 \leq i \leq m, 1 \leq j \leq n}$ est de rang $n - \dim(V)$.

Un polynôme $P(x_1, \dots, x_n)$ est homogène de degré d si pour tout $\lambda \in K$, $P(\lambda x_1, \dots, \lambda x_n) = \lambda^d P(x_1, \dots, x_n)$. Un idéal de $K[X]$ est homogène s'il est

engendré par des polynômes homogènes. Un ensemble algébrique dans \mathbf{P}^n est l'ensemble des solutions (modulo la relation d'équivalence) d'un système d'équations polynomiales homogènes à coefficients dans K . A un ensemble algébrique V on associe l'idéal homogènes $I(V)$ engendré des polynômes homogènes $P \in K[X]$ annihilant les points de V . V est dit une variété si $I(V)$ est un idéal premier dans $\bar{K}[X]$. Les propriétés d'une variété projective peuvent être définies en terme de celles de la variété affine $V \cap \mathbf{A}^n$. Si on choisit $\mathbf{A}^n \subset \mathbf{P}^n$ de sorte que $V \cap \mathbf{A}^n \neq \emptyset$, la dimension de V est celle de $V \cap \mathbf{A}^n \neq \emptyset$. V est lisse en P si $V \cap \mathbf{A}^n$ est lisse en P (si on choisit \mathbf{A}^n de sorte que $P \in V \cap \mathbf{A}^n$).

2.1.1 Fonctions sur des courbes algébriques

Une courbe est une variété projective de dimension 1. On s'intéresse au corps des fonctions sur une courbe lisse.

Soit C une courbe lisse, $P \in C$. On pose $M_P = \{f \in \bar{K}[V] : f(P) = 0\}$ qui est un idéal premier de $\bar{K}[V]$. L'anneau local de $\bar{K}[C]$ en P , $\bar{K}[C]_P$ est définie par la localisation de $K[V]$ en M_P .

Proposition 2.1. *$\bar{K}[C]_P$ est un anneau à valuation discrète.*

On a donc une valuation

$$\text{ord}_P : \bar{K}[C]_P \rightarrow \{0, 1, \dots\} \cup \{\infty\},$$

$$\text{ord}_P(f) = \max\{d \in \mathbf{Z} : f \in M_P^d\}$$

et l'étend en $\bar{K}(C)$ en posant $\text{ord}_P(f/g) = \text{ord}_P(f) - \text{ord}_P(g)$. Une uniformisante de C en P est une fonction de valuation 1. On dit qu'une fonction f est définie en P si $\text{ord}_P(f) \geq 0$, a un pôle en P ou un zéro en P selon que $\text{ord}_P(f) < 0$ ou $\text{ord}_P(f) > 0$.

Proposition 2.2. *Soit C une courbe lisse, $f \in \bar{K}(C)$. Alors il n'y a qu'un nombre fini de points P où f a un pôle ou un zéro. Si f n'a pas de pôle ni zéro, alors f est constante.*

2.1.2 Morphismes de courbes

Définition 2.1. Soit V_1, V_2 deux variétés dans \mathbf{P}^n . Une application rationnelle de V_1 dans V_2 est une application $\phi : V_1 \rightarrow V_2$, $\phi = [f_0, f_1, \dots, f_n]$ où $f_0, f_1, \dots, f_n \in \bar{K}(C_1)$ telle que pour tout point $P \in V_1$ où f_0, \dots, f_n sont définies, $\phi(P) = [f_0(P), \dots, f_n(P)] \in V_2$

L'application ϕ est définie (ou régulière) en $P \in V_1$ s'il existe une fonction $g \in \bar{K}(V_1)$ telle que les gf_i sont définies et ne sont pas toutes nulles en P . On pose alors $\phi(P) = [gf_0(P), gf_1(P), \dots, gf_n(P)]$

Lorsqu'une application rationnelle est définie en tout point, on l'appelle un morphisme.

Proposition 2.3. Toute application rationnelle entre courbes est définie en tout point. Donc pour les courbes, on peut parler de façon interchangeable des applications rationnelles et des morphismes.

Remarque : Soit C courbe et f une fonction sur K . Alors f définit une application rationnelle qu'on note encore f , de C dans $\mathbf{P}^1 : P \mapsto [f(P), 1]$.

Théorème 2.4. Un morphisme de courbes non constant est surjectif.

Un morphisme $\phi : C_1 \rightarrow C_2$ défini sur K entre deux courbes induit une application entre les deux corps de fonctions $\phi^* : K(C_2) \rightarrow K(C_1)$ définie par $\phi^*(f) = f \circ \phi$.

Théorème 2.5. Si $\phi : C_1 \rightarrow C_2$ est un morphisme défini sur K alors $K(C_1)$ est une extension finie de $\phi^*K(C_2)$.

On définit le degré d'un morphisme ϕ par $\deg(\phi) = [K(C_1) : \phi^*K(C_2)]$. On définit aussi

$$\phi_* : K(C_1) \rightarrow K(C_2) \phi_* = (\phi^*)^{-1} \circ N_{K(C_1)/\phi^*K(C_2)}.$$

Définition 2.2. Soit $\phi : C_1 \rightarrow C_2$ un morphisme de courbes. L'indice de ramification de ϕ en $P \in C_1$ est

$$e_\phi(P) = \text{ord}_P(\phi^*t_{\phi(P)})$$

où $t_{\phi(P)} \in K(C_2)$ est une uniformisante en $\phi(P)$.

Proposition 2.6. *Pour tout $Q \in C_2$,*

$$\sum_{P \in \phi^{-1}(Q)} e_\phi(P) = \deg(\phi)$$

2.1.3 Diviseurs

Définition 2.3. *Soit C une courbe. Un diviseur sur C est une somme formelle $\sum_P n_P P$ où les P sont des points sur C et qu'il n'y a qu'un nombre fini de terme n_P qui sont non nuls.*

Algorithmiquement, un diviseur est une liste de couples $(n_P, P) \in \mathbf{Z}^*$. On note $Div(C)$ l'ensemble des diviseurs sur une courbe C . Pour un diviseur $D = \sum_P n_P [P]$ on parle de son support $\text{supp}(D) = \{P : n_P \neq 0\}$, et de son degré $\deg D = \sum_P n_P$.

On considère l'ensemble des diviseurs de degré 0, noté $Div^0(C)$. Soit f une fonction rationnelle sur C on définit le diviseur associé à f , $\text{div}(f) = \sum_P \text{ord}_P(f)[P]$, la somme étant finie car une fonction rationnelle n'a qu'un nombre fini de pôles et de zéros. Un diviseur de la forme $\text{div}(f)$ est appelé principal.

Proposition 2.7. *Soit f une fonction rationnelle sur C . Alors $\text{div}(f)$ est de degré 0.*

Le groupe des diviseurs principaux est donc un sous-groupe des diviseurs de degré 0. Le quotient de ces groupes est appelé le groupe des classes de diviseur de degré 0 sur C et noté $Pic^0(C)$.

Proposition 2.8. *Soit C_1, C_2 deux courbes lisses, et $\phi : C_1 \rightarrow C_2$ une application rationnelle. Alors :*

- $\deg(\phi^*D) = \deg(\phi)\deg(D)$ pour tout diviseur D sur C_2 .
- $\phi^*(\text{div}f) = \text{div}(\phi^*f)$ pour toute fonction rationnelle f sur C_2 .
- $\deg(\phi_*D) = \deg D$ pour tout diviseur D sur C_1 .

- $\phi_*(\text{div} f) = \text{div}(\phi_* f)$ pour toute fonction rationnelle D sur C_1 .

Donc ϕ induit les applications $\phi^* : \text{Pic}^0(C_2) \rightarrow \text{Pic}^0(C_1)$ et $\phi_* : \text{Pic}^0(C_1) \rightarrow \text{Pic}^0(C_2)$

2.1.4 Réciprocité de Weil

Définition 2.4. Soient $D = \sum_P n_P P$ un diviseur et $f \in K(C)$ tels que leur support soient disjoints. On définit

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

Remarques :

- Pour f une fonction rationnelle, D_1, D_2 deux diviseurs alors $f(D_1 + D_2) = f(D_1)f(D_2)$ (à condition que les trois termes existent).
- Si D est de degré 0, alors la valeur de $f(D)$ ne change pas quand on remplace f par cf où c est une constante. Autrement dit $f(D)$ ne dépend que de $\text{div}(f)$.

Proposition 2.9. Soit f, g deux fonctions rationnelles sur une courbe lisse C , alors

$$f(\text{div}(g)) = g(\text{div}(f))$$

On a un lemme suivant :

Lemme 2.10. Si $\phi : C_1 \rightarrow C_2$ alors

- $f(\phi^* D) = (\phi_* f)(D)$ pour tout $f \in K(C_1), D \in \text{Div}(C_2)$
- $f(\phi_* D) = (\phi^* f)(D)$ pour tout $f \in K(C_2)^*, D \in \text{Div}(C_1)$.

Revenons à la proposition. On la montre d'abord dans le cas où $C = \mathbf{P}^1$. On identifie $\mathbf{P}^1(\bar{K})$ à $\bar{K} \cup \{\infty\}$. f et g sont donc des fractions rationnelles dans $\bar{K}(x)$. Soit $f = \prod_{i=1}^n (x - a_i)^{\alpha_i}, g = \prod_{j=1}^m (x - b_j)^{\beta_j}$. Alors

$\operatorname{div}(f) = \sum_{i=1}^n \alpha_i [a_i] + \alpha_\infty [\infty]$ et $\operatorname{div}(g) = \sum_{j=1}^m \beta_j [b_j] + \beta_\infty [\infty]$, où $\alpha_\infty = -\sum_{i=1}^n \alpha_i$, $\beta_\infty = -\sum_{j=1}^m \beta_j$. Supposons que les support de $\operatorname{div}(f)$ et de $\operatorname{div}(g)$ soient disjoints et ne contiennent pas le point à l'infini. Donc $a_i \neq b_j$ pour tout i, j et $\sum_{i=1}^n \alpha_i, \beta_\infty = -\sum_{j=1}^m \beta_j$.

Donc $f(\operatorname{div}(g)) = \prod_{1 \leq i \leq n, 1 \leq j \leq m} (b_j - a_i)^{\alpha_i \beta_j}$.
De même,

$$\begin{aligned} g(\operatorname{div}(f)) &= \prod_{1 \leq i \leq n, 1 \leq j \leq m} (a_i - b_j)^{\alpha_i \beta_j} \\ &= (-1)^{\sum_{1 \leq i \leq n, 1 \leq j \leq m} \alpha_i \beta_j} f(\operatorname{div}(g)) \\ &= (-1)^{(\sum_{1 \leq i \leq n} \alpha_i)(\sum_{1 \leq j \leq m} \beta_j)} f(\operatorname{div}(g)) = f(\operatorname{div}(g)) \end{aligned}$$

Donc $f(\operatorname{div}(g)) = g(\operatorname{div}(f))$. Si ∞ est dans le support de $\operatorname{div}(f)$, ce qui est le cas si le dénominateur et le numérateur de f ne sont pas de même degré, alors on ∞ n'est pas dans le support de g et $g(\infty) = 1$. On a les mêmes équations et la proposition est vraie dans ce cas.

Pour le cas général, soit i l'identité sur \mathbf{P}^1 . Alors $\operatorname{div}(i) = [0] - [\infty]$. On voit g comme une fonction $C \rightarrow \mathbf{P}^1$ et $\operatorname{div}(g) = g^*(\operatorname{div}(i))$. On a donc

$$f(\operatorname{div}(g)) = f(g^*(i)) = (g_* f)(\operatorname{div}(i)).$$

On a $g_* f$ est une fonction sur \mathbf{P}^1 , donc après la réciprocity de Weil sur \mathbf{P}^1 , on a $(g_* f)((\operatorname{div}(i))) = i((\operatorname{div}(g_* f)))$. Enfin, $i(\operatorname{div}(g_* f)) = (g^* i)((\operatorname{div}(f))) = i \circ g(\operatorname{div}(f)) = g(\operatorname{div}(f))$.

2.2 Courbes elliptiques

Définition 2.5. Une courbe elliptique E est une courbe projective d'équation

$$Y^2Z + a_1XYZ + a_3YZ = X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3$$

avec $(a_1, a_2, a_3, a_4, a_6) \in \bar{K}^5$. Elle est définie sur K si les a_i sont dans K .

On suppose par convention que la courbe est non singulière. Il n'y a qu'un seul point sur E de coordonnée $Z = 0$, à savoir $[0, 1, 0]$. On l'appelle le

point à l'infini. Les autres points de E s'identifient à l'ensemble des points $(x, y) \in \mathbf{A}^2$ qui satisfont l'équation

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

Deux courbes elliptiques E_1 et E_2 définies sur K sont dites isomorphes s'il existe un changement de coordonnées $(x, y) \mapsto (u^2x + r, u^3y + u^2sx + t)$ où $u, r, s, t \in K, u \neq 0$, qui transforme l'équation de E_1 en celle de E_2 .

2.3 Loi de groupe

L'ensemble $E(K)$ est un groupe abélien si on le munit de la loi d'addition suivante : Pour tout $P = (x_P, y_P)$ de $E(K)$,

$$P + O_E = O_E + P = P \text{ et } -P = (x_P, -y_P - a_1x_P - a_3)$$

Pour tout point $P = (x_P, y_P)$ et $Q = (x_Q, y_Q)$, les coordonnées de $P + Q$ sont définies par

$$\begin{cases} x_{P+Q} = \lambda^2 + a_1\lambda - a_2 - x_P - x_Q \\ y_{P+Q} = -(\lambda + a_1)x_{P+Q} - \nu - a_3 \end{cases} \quad (2.1)$$

où

$$\lambda = \begin{cases} (y_Q - y_P)/(x_P - x_Q) \text{ si } P \neq Q \\ (3x_P^2 + 2a_2x_P + a_4 - a_1y_P)/(2y_P + a_1x_P + a_3) \text{ sinon} \end{cases} \quad (2.2)$$

et $\nu = y_P - \lambda x_P$.

Cette loi de groupe a une interprétation géométrique. Soit P, Q deux points différents de la courbe (et différents du point à l'infini O). On trace la droite (PQ) . Deux cas peuvent se produire :

- La droite coupe la courbe en un 3^è point (on démontre qu'il y a au plus 3 points d'intersection entre une droite et la courbe). Le symétrique de ce 3^è point par rapport à l'axe des abscisses est $P + Q$.
- La droite ne coupe la courbe qu'en P et Q . Ce n'est possible que si (PQ) est parallèle à l'axe des ordonnées. On définit alors $P + Q = O$ (point à l'infini).

Si $P = Q$, on considère la tangente à la courbe en P , et on définit $P + P$ comme ci-dessus.

Pour démontrer que c'est bien une loi de groupe, il n'y a que l'associativité qui n'est pas triviale. Pour cela on peut utiliser la force brutale, ou bien établir une correspondance entre les points de E et les classes de diviseurs de degré 0, puis vérifier l'associativité sur ce dernier. On a le théorème suivant

Théorème 2.11. *Soit E une courbe elliptique. Alors le groupe des points sur E est isomorphe à $\text{Pic}^0(E)$, le groupe des classes de diviseurs de degré 0 sur E , via la correspondance $P \mapsto [P] - [O]$.*

Corollaire 2.12. *Soit $D = \sum n_P [P]$ un diviseur de degré 0. Alors D est principal si et seulement si $\sum n_P P = O$ dans E .*

2.4 Isogénies

Définition 2.6. *Soient E_1, E_2 deux courbes elliptiques définies sur un corps K . Une isogénie est un morphisme $\phi : E_1 \rightarrow E_2$ tel que $\phi(O_{E_1}) = O_{E_2}$.*

Théorème 2.13. *Toute isogénie est un homomorphisme de groupe. Par conséquent tout morphisme est la composition d'un homomorphisme de groupe et d'une translation (c-à-d un morphisme de la forme $P \mapsto P + Q$ avec Q fixé).*

Démonstration. Soit $I : E_1 \rightarrow E_2$ une isogénie. Elle induit une application

$$\begin{aligned} I_* : \text{Pic}^0(E_1) &\rightarrow \text{Pic}^0(E_2) \\ \text{classe de } \sum n_i [P_i] &\mapsto \text{classe de } \sum n_i [I(P_i)] \end{aligned}$$

qui est un homomorphisme de groupes. Puis on a le diagramme commutatif suivant :

$$\begin{array}{ccc} E_1 & \cong & \text{Pic}^0(E_1) \\ I \downarrow & & \downarrow \\ E_2 & \cong & \text{Pic}^0(E_2) \end{array}$$

ce qui montre que I est un homomorphisme de groupes.

Lorsque $E_1 = E_2$, une isogénie est appelée un endomorphisme. L'ensemble des endomorphismes d'une courbe elliptique E définie sur K forme un anneau

noté $End_K(E)$. On appelle aussi l'anneau des endomorphisme de E l'anneau $End_{\bar{K}}$ où \bar{K} est une clôture algébrique de K . Un endomorphisme invertible s'appelle un automorphisme. L'ensemble des automorphismes forme un groupe.

Soit \mathcal{A} une algèbre finiment engendrée sur \mathbf{Q} . Un ordre de \mathcal{A} est un sous-anneau \mathcal{B} de \mathcal{A} qui est finiment engendré comme \mathbf{Z} -module et qui satisfait $\mathcal{B} \otimes \mathbf{Q} = \mathcal{A}$. Une algèbre de quaternion est une algèbre de la forme $\mathbf{Q} + \mathbf{Q}\alpha + \mathbf{Q}\beta + \mathbf{Q}\alpha\beta$ avec les règles de multiplication $\alpha^2, \beta^2 \in \mathbf{Q}, \alpha^2 < 0, \beta^2 < 0, \beta\alpha = -\alpha\beta$. La proposition suivante parle de la structure de l'anneau endomorphisme d'une courbes elliptique :

Proposition 2.14. *L'anneau des endomorphismes d'une courbes elliptique est soit \mathbf{Z} , soit un ordre dans un corps quadratique imaginaire, soit un ordre dans une algèbre de quaternion.*

Définition 2.7. *L'endomorphisme de Frobenius est défini par $(x, y) \mapsto (x^q, y^q)$, $O \mapsto O$. Ses points fixes sont les points \mathbf{F}_q -rationnels.*

Comme une isogénie est un morphisme on peut parler de son degré, défini par $[K(E_1) : I^*K(E_2)]$.

Définition 2.8. *Soit $I : E_1 \rightarrow E_2$ une isogénie. Il existe une isogénie $\hat{I} : E_2 \rightarrow E_1$, appelée isogénie duale de I , telle que $\hat{I} \circ I = [\deg(I)]_{E_1}$ et $\deg(\hat{I}) = \deg(I)$.*

Théorème 2.15. *Soit $[m]$ la multiplication par $m : [m](P) = mP$. Alors $\deg[m] = m^2$. Par conséquent :*

- 1) *Si $\text{char}(K) = 0$ ou m est premier avec $\text{char}(K)$, alors $E[m] \cong \mathbf{Z}_m \oplus \mathbf{Z}_m$.*
- 2) *Si $\text{char}(K) = p$, alors $E[p^e] = O$ pour tout e , ou $E[p^e] \cong \mathbf{Z}_{p^e}$ pour tout e .*

Démonstration.(esquisse) Par récurrence on montre que $\widehat{[m]} = [m]$. Soit $d = \deg(\phi)$, on a $[d] = \widehat{[m]} \circ [m] = [m^2]$. Donc $d = m^2$. Dans le cas 1), on a $\sharp E[m] = \deg[m] = m^2$. De même, pour tout diviseur d de m , on a $\sharp E[d] = d^2$. Donc la seule structure de groupe possible pour $E[m]$ est $E[m] \cong \mathbf{Z}_m \oplus \mathbf{Z}_m$.

2.5 Courbes elliptiques définies sur des corps finis

Désormais on s'intéresse aux courbes sur des corps finis. Soit E une courbe elliptique définie sur $F(q)$ où $q = p^m$, p un nombre premier.

Théorème 2.16. (Hasse) Soit $\#E(\mathbf{F}_q) = q + 1 - t$. Alors $|t| \leq 2\sqrt{q}$

Démonstration.(esquisse) Soit ϕ le Frobenius sur \mathbf{F}_q . Alors on a $\#E(\mathbf{F}_q) = \#\ker(1 - \phi) = \deg(1 - \phi)$, et $\deg(\phi) = q$. On a l'inégalité $|\deg(1 - \phi) - \deg(\phi) - 1| \leq 2\sqrt{\deg(\phi)}$, puisque \deg est une forme quadratique définie positive.

Une conséquence importante du théorème de Hasse est qu'on peut choisir un point P sur une courbe $E(F_q)$ en un temps probabiliste polynomial. On appelle t la trace de la courbe E .

Théorème 2.17. (Waterhouse) Il existe une courbe elliptique E/\mathbf{F}_q telle que $E(\mathbf{F}_q)$ ait $q + 1 - t$ éléments si et seulement si l'une de ces conditions suivantes est satisfaite :

(i) $t \not\equiv 0 \pmod{p}$ et $t^2 \leq 4q$.

(ii) m est impaire et soit

– $t = 0$

– $t^2 = 2q$ et $p = 2$

– $t^3 = 3q$ et $p = 3$

(iii) m est paire et soit

– $t^2 = 4q$

– $t^2 = q$ et $p \not\equiv 1 \pmod{3}$

– $t = 0$ et $p \not\equiv 1 \pmod{4}$

Théorème 2.18. (Weil) Soit $\#E(\mathbf{F}_q) = q + 1 - t$. Alors $\#E(\mathbf{F}_{q^k}) = q^k + 1 - \alpha^k - \beta^k$ où α et β sont les racines complexes de l'équation $X^2 - tX + q = 0$

Structure de groupe:

Proposition 2.19. $E(F_q)$ est un groupe abélien de rang égal à 1 ou 2. En plus

$$E(\mathbf{F}_q) \cong \mathbf{Z}_{n_1} \oplus \mathbf{Z}_{n_2}$$

où $n_1|n_2$ et $n_1|q-1$.

Démonstration. Le fait que $E(\mathbf{F}_q)$ est un groupe de rang ≤ 2 vient du fait que c'est un sous-groupe du groupe de torsion $E[N]$ où $N = \#E(\mathbf{F}_q)$, dont le rang est ≤ 2 d'après le théorème 2.15. En moyen du couplage de Weil introduit dans le chapitre suivant on peut montrer que $n_1|q-1$. En effet, comme $E(\mathbf{F}_q) \cong \mathbf{Z}_{n_1} \oplus \mathbf{Z}_{n_2} \supset E[n_1]$, le couplage e_{n_1} est bien défini sur $E(\mathbf{F}_q)$ et donc fournit un homomorphisme injectif d'un sous-groupe cyclique d'ordre n_1 de $E[n_1]$ dans \mathbf{F}_q^* . Donc $n_1|q-1$.

Dans la section 4.1 on donne un algorithme pour trouver n_1 et n_2 .

Courbes supersingulières. On s'intéresse à des courbes particulières, appelées supersingulières.

Définition 2.9. Une courbe E de trace t définie sur un corps de caractéristique p est dite singulière si p divise t .

Comme un corollaire de du théorème 2.17 on a:

Proposition 2.20. Soit E une courbes définie sur F_q . Alors E est supersingulière si et seulement si $t^2 = 0, q, 2q, 3q$ ou $4q$.

Autres définitions alternatives pour les courbes supersingulières :

- $E[p^r] = 0$ pour une/toute valeur de r .
- $End(E)$ est un ordre dans une algèbre de quaternions

Proposition 2.21. Soit E une courbe non supersingulière. Alors $End(E)$ est commutatif.

Le théorème suivant décrit la structure de $E(F_q)$ pour les courbes supersingulières.

Théorème 2.22. Soit $\#E(F_q) = q + 1 - t$.

- (i) Si $t^2 = q, 2q$ ou $3q$, alors $E(\mathbf{F}_q)$ est cyclique
- (ii) Si $t^2 = 4q$, alors $E(\mathbf{F}_q) \cong \mathbf{Z}_{\sqrt{q-1}} \oplus \mathbf{Z}_{\sqrt{q-1}}$ où $E(\mathbf{F}_q) \cong \mathbf{Z}_{\sqrt{q+1}} \oplus \mathbf{Z}_{\sqrt{q+1}}$ selon que $t = 2\sqrt{q}$ ou $t = -2\sqrt{q}$
- (iii) Si $t = 0$ et $q \not\equiv 3 \pmod{4}$, alors $E(\mathbf{F}_q)$ est cyclique. Si $t = 0$ et $q \equiv 3 \pmod{4}$, alors $E(\mathbf{F}_q)$ est cyclique ou $\cong \mathbf{Z}_{(q+1)/2} \oplus \mathbf{Z}_2$.

Chapter 3

Couplages

Un couplage est une application bilinéaire de groupes, *c-à-d* une application $e : G_1 \times G_2 \rightarrow G_3$ où G_1, G_2 sont des groupes additifs et G_3 un groupe multiplicatif tels que $e(S_1 + S_2, T) = e(S_1, T)e(S_2, T)$ et $e(S, T_1 + T_2) = e(S, T_1)e(S, T_2)$. Un exemple est donné par l'application suivante :

$$\begin{aligned} f : M_k(\mathbf{Z}_n) \times M_k(\mathbf{Z}_n) &\rightarrow \mathbf{F}_p \\ (A, B) &\mapsto a^{\text{Tr}(AB)} \end{aligned}$$

où $a \in \mathbf{F}_p$ 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 $M_k(\mathbf{Z}/n\mathbf{Z})$. A ce jour les couplages connus en cryptographie sont les couplage de Tate et de Weil.

3.1 Couplage de Weil

Soit E une courbe elliptique définie sur \mathbf{F}_q . On rappelle que si $D = \sum n_P P$ un diviseur et f une fonction rationnelle tels que $\text{supp}(D)$ et $\text{supp}(\text{div}(f))$ sont disjoints, on peut définir $f(D) = \prod f(P)^{n_P}$.

Définition 3.1. *Soit m un nombre naturel premier avec la caractéristique de \mathbf{F}_q , K une extension de \mathbf{F}_q telle que tous les points de $E[m]$ soient 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 $D_P \sim [P] - [O]$ et $D_Q \sim [Q] - [O]$ et que les supports de*

D_P et de D_Q soient 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 $\text{div}(f_{D_P}) = mD_P$ et $\text{div}(f_{D_Q}) = mD_Q$. Le couplage de Weil est une application

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

définie par

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

Remarque : Le couplage est bien défini (c-à-d il ne dépend pas du choix de D_P et de D_Q) car pour tout $g : f_{D_P + \text{div}(g)}(D_Q) / f_{D_Q}(D_P + \text{div}(g)) = f_{D_P}(D_Q) / f_{D_Q}(D_P)$. 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 $(f_{D_P}(D_Q) / f_{D_Q}(D_P))^m = f_{D_P}(mD_Q) / f_{D_Q}(mD_P) = 1$ d'après la réciprocity 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 3.1.

$$e_m(P, Q) = \frac{f_Q(T) f_P(Q - T)}{f_P(-T) f_Q(P + T)} \quad (3.1)$$

où f_P et f_Q sont des fonctions telles que $\text{div}_{f_P} = m[P] - m[O]$ et $\text{div}_{f_Q} = m[Q] - m[O]$.

Démonstration. 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 $\text{div}(g) = m[P + T] - m[T]$. On a donc $g = f_P \circ \tau_{-T}$ où τ_{-T} est la translation par $-T$. Donc $g(Q)/g(O) = f_P(Q - T) / f_P(T)$, et on trouve la formule demandée.

Proposition 3.2. *Le couplage de Weil a les propriétés suivantes :*

- 1) *bilinéarité :* $e_m(S_1 + S_2, T) = (S_1, T)(S_2, T)$ et $e_m(S, T_1 + T_2) = (S, T_1)(S, T_2)$
- 2) *alternance :* $e_m(T, T) = 1$. Par conséquent $e_m(S, T) = e_m(T, S)^{-1}$
- 3) *non-dégénérescence :* Si $e_m(S, T) = 1$ pour tout $S \in E[m]$ alors $T = O$.
- 4) *action galoisienne :* pour tout $\sigma \in \text{Gal}(\bar{\mathbf{F}}_q / \mathbf{F}_q)$ 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 $e_{mm'}(S, T) = e_m(m'S, T)$

Démonstration.

- 1) Soient $P, Q, R \in E[m]$, f_1, f_2, f_3 fonctions telles que $\text{div}(f_1) = m[P] - m[O] = mD_1$, $\text{div}(f_2) = m[Q] - m[O] = mD_2$, $\text{div}(f_3) = m[R] - m[O] = mD_3$. 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 3.1 on a $e(P, P) = \frac{f_n(T) f_n(P-T)}{f_n(-T) f_n(P+T)}$ pour $P \neq O, \pm P$. 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 $O, \pm P$. Si m est impair, alors la caractéristique est impair, 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 $R \in E(\bar{K})$. Pour tout $X \in E(\bar{K})$ soit χ_X une fonction telle que $\text{div}(\chi_X) = m[X] - (m-1)[R] - [Y]$, où $Y = mX - (m-1)R$. Soit f une fonction telle que $\text{div}(f) = m[P] - m[O]$. 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

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

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

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

Comme $e_m(P, Q) = 1$ pour tout $Q \in E[m]$, 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 $f(Y)f(R)^{m-1} = (h \circ \tau_{(m-1)R})^m(Y)$. Comme R est constant, on a

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

Donc $[P] \sim [O]$ ce qui montre que $P = O$.

- 5) Soit $mm'P = O, mQ = O, \operatorname{div}(f_1) = mm'[P] - mm'[O], \operatorname{div}(f_2) = m[Q + T] - m[T], \operatorname{div}(f_3) = m[m'P] - m[O]$. 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 $\operatorname{div}(f_3) = m[m'P] - m[O] = \operatorname{div}(f_1) + m([m'P] + (m' - 1)[O] - m'[P])$, donc on peut supposer $f_3 = f_1 f_4^m$ où f_4 est une fonction telle que $\operatorname{div}(f_4) = [m'P] + (m' - 1)[O] - m'[P]$. Alors

$$\begin{aligned} e_{mm'}(P, Q) &= \frac{f_3 f_1^{-m}([Q + T] - [T])}{f_2^m([P] - [O])} \\ &= \frac{f_3([Q + T] - [T]) f_1(-\operatorname{div}(f_2))}{f_2^m([P] - [O])} \\ &= \frac{f_3([Q + T] - [T])}{f_2^m([P] - [O]) f_2(\operatorname{div}(f_4))} \text{ d'après la réciprocity de Weil} \\ &= e_m(m'P, Q) \end{aligned}$$

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

Proposition 3.3. *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 $e_m(P, P_1) = e_m(P, P_2)$.*

Démonstration. On sait que $E[m] \cong \mathbf{Z}_m \oplus \mathbf{Z}_m$ d'après le théorème 2.15. Soit $Q \in E[m]$ 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 $dQ \neq O$ 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 $E[n]$, on obtient un homomorphisme de groupe de $E[n]$ dans l'image du couplage, *c-à-d* μ_m . On va développer cette idée dans 3.4.

3.2 Couplage de Tate

Définition 3.2. Soit l un nombre naturel premier avec la caractéristique de \mathbf{F}_q . Soit $K = \mathbf{F}_{q^k}$ une extension de \mathbf{F}_q qui contient 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 $D_P \sim [P] - [O]$ 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 $\text{div}(f_{D_P}) = lD_P$. Le couplage de Tate est une application

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

définie par

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

Remarque :

- Le couplage de Tate est bien défini car si on remplace $D(P)$ par un diviseur équivalent $D(P) + \text{div}(g)$, alors $f_{D(P)+\text{div}(g)}(D(Q)) = f_{D(P)}(D(Q))g(D(Q))^l \equiv f_{D(P)}(D(Q)) \text{ modulo } K^{*l}$. De même, $f_{D(P)}(D(Q) + \text{div}(g)) = f_{D(P)}(D(Q))f_{D(P)}(\text{div}(g)) = f_{D(P)}(D(Q))g(D(P))^l \equiv f_{D(P)}(D(Q)) \text{ modulo } K^{*l}$ 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 $f_{D(P)}(D(Q + lR)) = f_{D(P)}(D(Q))f_{D(P)}(l([R] - [O])) = f_{D(P)}(D(Q))f_{D(P)}([R] - [O])^l \equiv f_{D(P)}(D(Q)) \text{ modulo } K^{*l}$.
- Contrairement au couplage de Weil qui prend les deux arguments dans le même groupe, le couplage de Tate prend dans deux groupes différents $E(K)[l]$ et $E(K)/lE(K)$. Ces deux groupes ont le même cardinal.
- Toute classe d'équivalence de $E(K)/lE(K)$ contient un représentant dans le 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 3.1:

Proposition 3.4.

$$t_l(P, Q) = \frac{f_P(Q + T)}{f_P(T)} \quad (3.2)$$

où f_P est une fonction telle que $\text{div}(f_P) = l[P] - l[O]$, et $T \in E(K)$ tel que les points $T, Q + T, P, O$ soient distincts.

Pour que le couplage rende une valeur exacte on peut définir

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

Proposition 3.5. *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 $\sigma \in \text{Gal}(\bar{\mathbf{F}}_q/\mathbf{F}_q)$ on a $t_l(S, T)^\sigma = t_l(S^\sigma, T^\sigma)$

Démonstration.

- 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 [8], ou encore une preuve plus élémentaire dans [6].

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 -ième près, 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 $P \in E(\mathbf{F}_q)$, ce qui est souvent le cas dans les applications cryptographique, on a le résultat suivant :

Proposition 3.6. *Soit $P \in E(\mathbf{F}_q)[l], P \neq O, l$ premier. Si le degré de l'extension $k > 1$ alors $t_l(P, P)$ est trivial (c-à-d sa valeur est une puissance l -ième dans K).*

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

Corollaire 3.7. *Soit $P \in E(\mathbf{F}_q)[l]$ d'ordre exact $l, P \neq O, l$ premier. Si $Q \in E(\mathbf{F}_{q^k})[l]$ un point de torsion d'ordre exact l et indépendant de P , alors $t_l(P, Q)$ n'est pas trivial.*

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

3.3 Algorithme de Miller

3.3.1 L'algorithme

Le calcul des couplages de Tate et de Weil a été cru inefficace jusqu'à ce que Miller trouve l'algorithme décrit dans cette section. D'après les formules des propositions 3.1 et 3.4, le calcul des couplages revient au calcul de la valeur d'une fonction rationnelle f_P en un point T sachant que $\text{div}(f_P) = n[P] - n[O]$ où P est un point d'ordre n .

L'idée est d'introduire une suite des fonctions $f_{n,P}$ comme suit :

$$f_{0,P} = f_{1,P} = 1$$

$$f_{k+1,P} = f_{k,P} g_{P,kP} / g_{(k+1)P, -(k+1)P}$$

où $g_{U,V}$ est l'équation de la droite passant par U et V . Comme $\text{div}(g(U, V)) = [U] + [V] + [-(U + V)] - 3[O]$, par récurrence on a

$$\text{div}(f_{k,P}) = k[P] - (k - 1)[O] - [kP]$$

et finalement pour $k = n$ on a $f_{n,P} = f_P$. Par récurrence on peut démontrer la formule suivante :

$$f_{u+v,P} = f_{u,P} f_{v,P} g_{uP,vP} / g_{(u+v)P, -(u+v)P}$$

grâce à quoi on peut calculer la valeur de $f_{n,P} = f_P$ en utilisant une chaîne d'addition.

Plus précisément, on a :

$$\begin{aligned} f_{2u,P} &= f_{u,P}^2 g_{uP,uP} / g_{2uP, -2uP} \\ f_{u+1,P} &= f_{u,P} g_{uP,P} / g_{(u+1)P, -(u+1)P} \end{aligned}$$

On a l'algorithme suivant :

Algorithme 3.1. 1) Poser $t = \lceil \log_2(l) \rceil - 1$, $V = P$, $f = 1$. Soit (n_t, \dots, n_0) la représentation binaire de n .

2) Pour $i = t - 1, \dots, 0$:

- Poser $f = f^2 g_{V,V}(T) / g_{2V, -2V}(T)$. Poser $V = 2V$.
- Si $n_i = 1$ alors poser $f = f g_{V,P}(T) / g_{V+P, -V-P}(T)$, $V = V + P$.

3) Retourner f .

Le calcul du couplage de Tate se fait en 2 applications de cet algorithme, alors que le couplage de Miller en prend 4. Cependant, prenons la formule 3.4, au lieu de calculer $f_P(Q+T)$ et $f_P(T)$ séparément puis calculer leur quotient, on peut calculer à chaque étape $f_{k,P}(Q+T) / f_{k,P}(T)$ donc le calcul du couplage de Tate se fait en une seule application. On a l'algorithme suivant pour le couplage de Tate :

Algorithme 3.2. 1) Choisir $T \in E(\mathbf{F}_{q^k})$ au hasard. Calculer $S = Q + T \in E(\mathbf{F}_{q^k})$.

2) Poser $t = \lceil \log_2(l) \rceil - 1$, $V = P$, $f = 1$. Soit (l_t, \dots, l_0) la représentation binaire de l .

3) Pour $i = t - 1, \dots, 0$:

- Poser $f = f^2 \frac{g_{V,V}(S) g_{2V, -2V}(T)}{g_{V,V}(T) g_{2V, -2V}(S)}$, $V = 2V$.
- Si $l_i = 1$ alors poser $f = f \frac{g_{V,P}(S) g_{V+P, -V-P}(S)}{g_{V,P}(T) g_{V+P, -V-P}(S)}$, $V = V + P$.

4) retourner f .

On peut faire de même avec le couplage de Weil, mais ce dernier prend 2 applications de l'algorithme.

Remarques :

- L'algorithme 3.1 pour calculer $f_P(T)$ est probabiliste. On peut le rendre déterministe en calculant le terme dominant au lieu de la fonction elle-même, mais ce faisant l'algorithme perd l'efficacité.
- Sa complexité est d'ordre $O(\log l)$ sans compter l'arithmétique dans le corps de base. A chaque étape interviennent au plus 2 additions sur $E(K)$ ainsi que des multiplications dans $K = \mathbf{F}_{q^k}$. Le calcul du couplage est donc efficace lorsque le degré de l'extension k reste petit.
- A chaque étape la valeur de f n'est pas définie si T est dans le support de $g_{V,V}/g_{2V,-2V}$, à savoir $\pm V, \pm 2V$, ou si T est dans le support de $g_{V,P}/g_{V+P,-V-P}$, à savoir $\pm V, \pm P, \pm(V+P)$. Donc pour que l'algorithme rende un résultat, il faut que T évite au plus $4(t+1)$ points, ce qui est négligeable si la courbe a assez de points. Plus précisément, pour le couplage de Tate, la probabilité que l'algorithme marche est $\leq 16\log_2(l)/\#E(K) \leq 16\log_2 l/l$. Pour le couplage de Weil la probabilité est $\leq 32\log_2 m/\#E(K) \leq 32\log_2 m/m$. Dans les applications m et l sont grands donc ces probabilités sont petites.
- En général le couplage de Weil prend deux fois plus de temps que le couplage de Tate. C'est parce que dans la formule du couplage de Weil, il y a deux fonctions qui interviennent alors que pour le couplage de Tate il n'y en a qu'une.

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 petit. Or l'extension correspondant au couplage de Weil est plus large que celle du couplage de Tate (voir la section 3.4). Une supériorité 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.

3.3.2 Implantations efficaces

Dans cette section on décrit quelques idées pour améliorer des algorithmes 3.1 et 3.2

- On peut choisir l un nombre premier de poids de Hamming petit, plus concrètement, de la forme $2^\beta \pm 2^\alpha \pm 1$ pour réduire le nombre d'étape dans l'algorithme 3.1.
- Si $P \in E(\mathbf{F}_q)$ beaucoup d'opérations sont effectuées dans \mathbf{F}_q au lieu de \mathbf{F}_{q^k} .
- Pour chaque étape il y a une division. On peut toujours garder $f_P(T)$ sous la forme d'un quotient et n'effectue la division qu' à la fin.
- En caractéristique 3, pour la courbe $E : y^2 = x^3 - x + b$, on a la formule de triplement : $3(x, y) = (x + y^2 + y^6, -y^9)$, qui est sans division et rend donc le calcul moins couteux. On peut donc modifier l'algorithme 3.1 en remplçant le représentation binaire de n par la représentation ternaire $n = (n_t, \dots, n_0)$ où $n_i \in \{0, \pm 1\}$, réduisant le nombre d'étape ainsi que le nombre d'opérations dans \mathbf{F}_{q^k} .
- Dans [22] Barreto et al. démontrent le théorème suivant :

Théorème 3.8. *Si le degré de plongement $k_t > 1$, alors*

$$\tilde{t}_l(P, Q) = t_l(P, Q)^{(q^k-1)/l} = f_P(Q)^{(q^k-1)/l}$$

Donc on peut simplifier les termes à multiplier dans chaque étape de 3.2.

- Pour certaines courbes, les dénominateurs dans l'algorithme de Miller peuvent être mis au rebut. C'est parce que les dénominateurs deviennt l'unité lors de l'exponentiation finale.

3.4 Plongement de MOV et de FR

3.4.1 Les plongements

Les couplages de Weil et de Tate décrits dans la section précédente fournissent un homomorphisme d'un sous-groupe cyclique du groupe de torsion dans le groupe multiplicatif d'une extension du corps de base. En effet, si $P \in E[m]$ est fixé, on cherche $Q \in E[m]$ tel que $e_m(P, Q)$ soit une racine primitive de l'unité d'ordre m , ce qui est possible d'après 3.3. Alors l'application $R \mapsto e_m(R, Q)$ est un isomorphisme de $\langle P \rangle$ dans le groupe des racines m -ièmes de l'unité. La réduction du groupe $\langle P \rangle$ au groupe des racines de l'unité permet de résoudre le problème du logarithme discret dans $\langle P \rangle$. C'est la réduction de Menezes-Okamoto-Vanstone.

On le résume dans l'algorithme suivant

Algorithme 3.3. *Algorithme de réduction de MOV :*

Entrée : $P \in E(\mathbf{F}_q)$ d'ordre m , et $R \in \langle P \rangle$.

Sortie : un entier l tel que $R = lP$.

- 1) Trouver k minimal tel que $E[m] \in E(\mathbf{F}_{q^k})$
- 2) Trouver $Q \in E[m]$ tel que $\alpha = e_m(P, Q)$ soit d'ordre m .
- 3) Calculer $\beta = e_m(R, Q)$.
- 4) Calculer l , le logarithme discret de β par rapport à α dans \mathbf{F}_{q^k} .

D'une manière similaire, avec le couplage de Tate on a la réduction de Frey-Rück:

Algorithme 3.4. *Algorithme de réduction de FR :*

Entrée : $P \in E(\mathbf{F}_q)$ d'ordre premier m , et $R \in \langle P \rangle$.

Sortie : un entier l tel que $R = lP$.

- 1) Trouver k minimal tel que $\mu(m) \subset \mathbf{F}_{q^k}$

- 2) Trouver $Q \in E(\mathbf{F}_{q^k})$ tel que $Q \notin mE(\mathbf{F}_{q^k})$ (et donc $t_m(P, Q)$) n'est pas trivial).
- 3) Calculer $\alpha = t_m(P, Q)^{(q^k-1)/m}$ et $\beta = t_m(R, Q)^{(q^k-1)/m}$.
- 4) Calculer l , le logarithme discret de β par rapport à α dans \mathbf{F}_{q^k} .

3.4.2 Degré de plongement

Au premier regard, avec les réduction ci-dessus on aurait cru que le problème du logarithme discret sur les courbes elliptiques n'est pas plus difficile que celui sur les corps finis. Ce n'est le cas que quand l'extension dans laquelle le couplage est défini est de degré petit. Dans cette section on va étudier le degré des extensions.

Dans le cas du plongement de MOV on se ramène à un corps de degré k_w où k_w est le plus petit entier k tel que $E[m] \subset E(\mathbf{F}_{q^k})$. Dans le cas du plongement de FR on travaille avec un corps de degré k_t où k_t est le plus petit entier k tel que \mathbf{F}_{q^k} contient m racines m -ièmes de l'unité. De façon équivalente k_t est le plus petit entier k tel que m divise $q^k - 1$. On appelle k_w le degré de plongement de Weil et k_t le degré de plongement de Tate (par rapport à m).

Proposition 3.9. *On a toujours $k_t \leq k_w$.*

Démonstration. Il suffit de montrer que si $E[m] \subset E(\mathbf{F}_{q^k})$ alors $E(\mathbf{F}_{q^k})$ contient m racines m -ièmes de l'unité. Or le couplage de Weil fournit un isomorphisme d'un sous-groupe cyclique d'ordre m de $E[m]$ dans le groupes de racines m -ièmes de l'unité, d'où la conclusion.

Cependant, dans la plupart des cas les couplages de Tate et de Weil prennent la même extension. En effet, on a :

Théorème 3.10. *(Balasubramanian, Koblitz) Soit m premier, m divise $N = \#E(\mathbf{F}_q)$, m ne divise pas $q - 1$. Alors $E[m] \subseteq E(\mathbf{F}_{q^k})$ si et seulement si m divise $q^k - 1$. Donc $k_w = k_t$.*

Démonstration.(esquisse) Soit (P, Q) deux générateurs de $E[m]$, P est défini sur \mathbf{F}_q . La matrice de l'endomorphisme de Frobenius, vu comme application linéaire de $E[m]$ est $\begin{pmatrix} 1 & 0 \\ a & q \end{pmatrix}$. On a $\sigma^k = \begin{pmatrix} 1 & 0 \\ a(1 + q + \dots + q^{k-1}) & q^k \end{pmatrix}$. Lorsque $q \not\equiv 1 \pmod{l}$, $\sigma^k = 1$ si et seulement si $q^k \equiv 1 \pmod{l}$.

Le meilleur algorithme pour le problème du logarithme discret sur un corps de cardinal q est de complexité $\exp(c(\log q)^{1/3}(\log \log q)^{2/3})$, où c est une constante absolue. Donc si le couplage est défini sur une extension de degré d , le temps de résoudre le problème du logarithme discret sur une courbe elliptique est au moins $\exp(c(\log q^d)^{1/3}(\log \log q^d)^{2/3})$, ce qui n'est pas pratique si d est grand. En général, le degré de plongement est d'ordre q si on admet la conjecture d'Artin sur les racines primitives.

On va voir ensuite deux classes de courbes pour lesquelles les degrés de plongement sont petits.

Courbes supersingulières. La première classe est celle des courbes supersingulières. On a le théorème suivant :

Théorème 3.11. *(Menezes, Okamoto, Vanstone) Pour les courbes supersingulières, $k_w \leq 6$. Par conséquent on a aussi $k_t \leq 6$.*

En effet, d'après 2.22, pour une courbe supersingulière d'ordre $q+1-t$ définie sur \mathbf{F}_q , elle appartient à une des classes suivantes :

- 1) $t = 0$ et $E(\mathbf{F}_q) \cong \mathbf{Z}_{q+1}$
- 2) $t = 0$ et $E(\mathbf{F}_q) \cong \mathbf{Z}_{(q+1)/2} \oplus \mathbf{Z}_2$, et $q \equiv 3 \pmod{4}$.
- 3) $t^2 = q$ (et m est pair).
- 4) $t^2 = 2q$ (et $p = 2$ et m est impair).
- 5) $t^2 = 3q$ (et m est pair).
- 6) $t^2 = 4q$ (et m est pair).

On donne une esquisse de la démonstration. En utilisant le théorème de Weil 2.18 on peut déterminer la structure de groupe de $E(\mathbf{F}_{q^k})$ à partir de celle de $E(\mathbf{F}_q)$. En général ceci est vrai pour les courbes supersingulières : si $E(\mathbf{F}_q)$ est de type (n_1, n_2) c-à-d $E(\mathbf{F}_q) \cong \mathbf{Z}_{n_1} \oplus \mathbf{Z}_{n_2}$ où n_1 divise n_2 , alors il existe c tel que $E(\mathbf{F}_{q^k})$ soit de type cn_1, cn_2 . On teste les valeurs successives de k et trouve que pour un $k \leq 6$ on a $E(\mathbf{F}_{q^k}) \supset E[n_2] = \mathbf{Z}_{n_2} \oplus \mathbf{Z}_{n_2}$ (car n_2 divise $\#E(\mathbf{F}_q) = q - t + 1$ et est premier avec q puisque p divise q) $\supset E[m]$.

On résume les informations dans le tableau suivant :

Class	t	structure de groupe	n_2	k
1	0	cyclique	$q+1$	2
2	0	$\mathbf{Z}_{(q+1)/2} \oplus \mathbf{Z}_2$	$(q+1)/2$	2
3	$\pm\sqrt{q}$	cyclique	$q+1 \mp \sqrt{q}$	3
4	$\pm\sqrt{2q}$	cyclique	$q+1 \mp \sqrt{2q}$	4
5	$\pm\sqrt{3q}$	cyclique	$q+1 \mp \sqrt{3q}$	6
6	$\pm 2\sqrt{q}$	$\mathbf{Z}_{\sqrt{q}\mp 1} \oplus \mathbf{Z}_{\sqrt{q}\mp 1}$	$\sqrt{q} \mp 1$	1

Courbes de MNT. Jusqu'en 2001 les seules courbes de degré de plongement petit connues sont les courbes supersingulières. Dans [7] Miyaji, Nakabayashi et Takano décrivent une méthode de construction de courbes non-supersingulières de degré de plongement (de FR) $k = 3, 4, \dots$. Ils démontrent ce résultat :

Théorème 3.12. *Soit E une courbe elliptique non-supersingulière définie sur \mathbf{F}_q , t la trace de E (donc $\sharp E(\mathbf{F}_q) = q + 1 - t$). Alors :*

- $k = 3$ si et seulement s'il existe $l \in \mathbf{Z}$ tel que $q = 12l^2 - 1$ et $t = -1 \pm 6l$.
- $k = 4$ si et seulement s'il existe $l \in \mathbf{Z}$ tel que $q = l^2 + l + 1$ et $t = -l$ ou $l + 1$.
- $k = 6$ si et seulement s'il existe $l \in \mathbf{Z}$ tel que $q = 4l^2 + 1$ et $t = 1 \pm 2l$.

Reste à construire des courbes dans l'une des trois classes ci-dessus. On peut construire une courbe elliptique si on connaît q et t , en utilisant la méthode dite multiplication complexe. La construction revient à résoudre des équations de Pell dont la solution est connue. Pour les détails voir [7]. Une question ouverte est de construire des courbes d'autres degrés relativement petits (disons $k \leq 20$) car la méthode de MNT ne s'applique pas aux autres degrés.

3.5 Distorsions

Les distorsions ont été trouvées par Verheul [16]. A l'origine elles ont été utilisées pour fournir les isomorphismes efficacement calculables entre les courbes CTP (*c-à-d* les courbes elliptiques sur \mathbf{F}_{p^2} d'ordre $p^2 - p + 1$). Il s'est avéré que les distorsions ont l'avantage qu'elles envoient les points à des points indépendents. Or, trouver des points indépendents est un problème important pour faire les couplages.

3.5.1 Définitions

Définition 3.3. Soit E une courbe elliptique définie sur un corps $K = \mathbf{F}_q$, K' une extension de K , P un point de $E(K)$. Une distorsion (définie sur K') pour P est un endomorphisme D défini sur K' tels que P et $D(P)$ sont indépendants. Une distorsion pour $E(K)$ est une distorsion pour tout point $P \neq O$ de $E(K)$.

Remarques :

- En général $D(P)$ n'est pas défini sur K . C'est toujours le cas si P est d'ordre l et que $E[l] \not\subset E(K)$. Le terme distorsion est donc justifié.
- Si P est d'ordre premier l , $D(P)$ est aussi d'ordre l puisque D est un homomorphisme de groupe. Donc une distorsion pour P existe seulement si l n'est pas divisible par p la caractéristique de K (sinon $E[l]$ serait cyclique), et $E[l] \cong \mathbf{Z}_l \times \mathbf{Z}_l$.
- Notons $End_{K'}(E[l])$ l'anneau des endomorphismes définis sur K' , restreints à $E[l]$. Il s'identifie à un sous-groupe des applications l -linéaires sur \mathbf{F}_l^2 . Alors les distorsions pour P sont des applications qui n'ont pas P comme vecteur propre.

Proposition 3.13. (Verheul) Soit E une courbe non-supersingulière, P d'ordre l tels que le degré de plongement de MOV par rapport à l , $k_w > 1$. Alors il n'y a pas de distorsions pour les points d'ordre l .

Démonstration. Soit P un point d'ordre l , F_K le Frobenius sur K , alors

$$D(P) = D(F_K(P)) = F_K(D(P))$$

la deuxième égalité résulte du fait que $End(E)$ est commutatif si E est non-supersingulière. Donc $D(P)$ est aussi fixé par F_K et est donc dans $E(K)$. C'est aussi un élément de $E[l]$. Comme P et $D(P)$ sont indépendants ils engendrent $E[l]$. Donc $E[l] \subset E(K)$, contradiction avec l'hypothèse $k_w > 1$.

La situation est différente pour les courbes supersingulières :

Proposition 3.14. Si E est supersingulière, alors $End_{K'}(E[l]) \cong M_2(\mathbf{Z}_l)$, l'anneau des matrices 2×2 à coefficients dans \mathbf{Z}_l . En particulier il existe amples distorsions pour un point P donné d'ordre l .

Si on enlève la condition $k_w > 1$, c'est à dire $E[l] \subset E(K)$, les distorsions peuvent exister pour les courbes non-supersingulière. Par exemple, on prend la courbe E/\mathbf{F}_{197} . Elle est de cardinal 196, donc n'est pas supersingulière. Le groupe de torsion $E[7] \subset E(\mathbf{F}_{197})$ est engendré par $P_1 = (24, 23)$ et $P_2 = (173, 125)$. L'application $\phi : (x, y) \mapsto (-x, 14y)$ est un endomorphisme et envoie P_1 en P_2 . Elle est donc une distorsion pour P_1 , et pour tout point $\neq O$ de $\langle P_1 \rangle$. Un résultat plus précis est donné dans [16]. Cependant, ce cas n'est pas intéressant pour les applications en cryptographie, car en général on veut que l soit un nombre premier proche de $\#E(\mathbf{F}_{q^k})$, alors que pour que $E[l] \subset E(\mathbf{F}_{q^k})$, il faut que $l^2 | \#E(\mathbf{F}_{q^k})$.

On va donner ensuite des exemples de distorsions qui sont efficacement calculables :

- Le schéma originel de Boneh-Franklin de chiffrement à base d'identité utilise les courbes d'équation $y^2 = x^3 + 1$ sur \mathbf{F}_p où p est un nombre premier, $p \equiv 2 \pmod{3}$. Elles sont de cardinal $p + 1$. une distorsion est donnée par $\phi : (x, y) \mapsto (x, \omega y)$ où $\omega \in \mathbf{F}_{p^2} \setminus \mathbf{F}_p, \omega^3 = 1$. Plus généralement, cela marche avec les courbes d'équation $y^2 = x^3 + a, a \in \mathbf{F}_p$.
- Pour la courbe $E : y^2 = x^3 - bx$ définie sur $\mathbf{F}_p, p \equiv 3 \pmod{4}, \phi : (x, y) \mapsto (-x, iy)$ où $i \in \mathbf{F}_{p^2} \setminus \mathbf{F}_p, i^2 = -1$ est une distorsion.
- Les premières distorsions sont étudiées sur les courbes CTP d'équation $E : y^2 = x^3 + a$ définie sur $\mathbf{F}_{p^2}, p \equiv 2 \pmod{3}, a$ est un carré mais pas un cube dans \mathbf{F}_{p^2} . L'application $\phi : (x, y) \mapsto (u^2 x^p, u^3 y^p)$, où $u \in \mathbf{F}_{p^6}, u^{1-p} = a$ est une distorsion pour tout point P d'ordre différent de 3.

3.5.2 Utilisation en cryptographie

Couplages modifiés. On peut se servir des distorsions pour fabriquer des couplages qui sont "fortement non-dégénérés" sur $E(K)[l]$, c-à-d $e(P, Q) \neq 1$ pour tout $P, Q \in E(K)[l]$ différents de O , et qui conservent encore les autres propriétés (bilinearité, etc.). Soit ϕ une distorsion pour $E[l]$. On définit

- Couplage de Weil modifié : $\hat{e}(P, Q) = e(P, \phi(Q))$

- Couplage de Tate modifié : $\hat{t}(P, Q) = t(P, \phi(Q))$

Cela a l'avantage que $e(P, P) \neq 1$ pour $P \neq O$, propriété essentielle pour résoudre le problème DDH dans $\langle P \rangle$ ainsi que pour construire le protocole entre trois parties (voir applications).

Dans les applications cryptographiques on travaille plutôt avec les groupes cyclique d'ordre premier. On veut donc définir les couplages sur les groupes d'ordre premier.

Couplages asymétriques. Soit $P, Q \in E[m]$ deux points indépendants. Posons $G_1 = \langle P \rangle$, $G_2 = \langle Q \rangle$. On sait que $e_m(P, Q) \neq 1$. Le couplage de Weil (ou de Tate) restreint à $G_1 \times G_2$ sont donc fortement non-dégénéré. Ce couplage prend deux points dans deux groupes cyclique différents et donne une racine de l'unité. C'est donc un couplage asymétrique. Ce dont on a besoin, ce sont deux points indépendants au départ (ce qui peut être difficile s'il n'y a pas de distorsions).

Couplage symétrique. Soit $P \in E[m]$, les couplages de Weil et de Tate modifiés restreints à $G_1 \times G_1$ sont toujours des couplages fortement non-dégénérés grâce à la forte non-dégénérescence des couplages modifiés. Ce couplage prend deux points dans le même groupe et donne une racine de l'unité. En général c'est plus pratique que les couplages asymétriques.

3.6 Conditions cryptographiques

On a vu les couplage d'un point de vue théorique. En pratique, beaucoup d'autres conditions sur la courbe, sur le corps etc. sont demandées pour assurer l'efficacité, la sécurité, etc. Les conditions idéales pour faire les couplages sont :

- Une courbe E sur \mathbf{F}_q .
- \mathbf{F}_q n'est pas trop grand.

- Un grand nombre premier l (au moins 160 bits) tel que $l \nmid \#E(\mathbf{F}_q)$ mais $l^2 \nmid \#E(\mathbf{F}_q)$.
- Le degré de plongement k petit.
- Pour la sécurité, il faut que le problème du logarithme discret soit difficile dans le groupe de départ ($E[l]$) ainsi que dans le groupe d'arrivée ($\mathbf{F}_{q^k}^*$). Donc il faut que l'extension \mathbf{F}_{q^k} soit grande (au moins 1024 bits).
- Il existe une distorsion sur E pour la facilité de trouver des points indépendants du couplage.

Outre les trois courbes mentionnées dans la section 3.5, il y a d'autres courbes qui sont convenables pour ces buts cryptographiques, en caractéristiques 2 et 3 :

- Les courbes $E_i : y^2 + y = x^3 + x + a_i$ sur \mathbf{F}_2 , où $a_1 = 0, a_2 = 1$. Elles sont de degré de plongement 4. $\#E_i(\mathbf{F}_{2^l}) = 2^l \pm 2^{(l+1)/2} + 1$ (l impair). Distorsion $(x, y) \mapsto (u^2x + s^2, y + u^2sx + s)$ où $u \in \mathbf{F}_{2^2}$ et $s \in \mathbf{F}_{2^4}$ tels que $u^2 + u + 1 = 0$ et $s^2 + (u + 1)s + 1 = 0$.
- Les courbes $E_i : y^2 = x^3 - x + a_i$ sur \mathbf{F}_3 , où $a_1 = 1, a_2 = -1$. Elles sont de degré de plongement 6. $\#E_i(\mathbf{F}_{3^l}) = 3^l \pm 3^{(l+1)/2} + 1$ (l impair). Distorsion $(x, y) \mapsto (\alpha - x, iy)$ où $i \in \mathbf{F}_{3^2}$ et $\alpha \in \mathbf{F}_{3^3}$ tels que $i^2 + 1 = 0$ et $\alpha^3 - \alpha - a_i = 0$.

Chapter 4

Applications

4.1 La structure de groupe de $E(\mathbf{F}_q)$

On rappelle que si E est une courbe elliptique définie sur \mathbf{F}_q , alors $E(\mathbf{F}_q)$ est un groupe abélien de rang égal à 1 ou 2. En plus $E(\mathbf{F}_q) \cong \mathbf{Z}_{n_1} \oplus \mathbf{Z}_{n_2}$ où $n_1 | n_2$ et $n_1 | q - 1$.

Dans cette section on donne un algorithme pour calculer n_1 et l_2 .

Algorithme 4.1. (Miller):

- 1) Calculer $N = \#E(K)$ (en utilisant l'algorithme de Schoof ou une des ses variantes).
- 2) Prendre P, Q au hasard dans E .
- 3) Calculer $s = \text{ord}(P), t = \text{ord}(Q)$ (pour cela on doit savoir la factorisation de N).
- 4) Calculer $m = \text{ppcm}(s, t)$ et $\zeta = e_m(P, Q)$, une racine d'unité.
- 5) Calculer $d = \text{ord}(\zeta)$, vérifier si $md = N$.
- 6) Si vrai alors $n_1 = d, n_2 = m$. Sinon revenir à 2).

Théorème 4.1. Cet algorithme donne le résultat en temps $S(q) + F(N) + O(\log^2 q)$ où $F(N)$ est le temps de factoriser N , $S(q)$ est le temps de calculer $|E(K)|$.

Démonstration. On $m \leq n_2$, car l'ordre de tout élément de $E(K)$ est diviseur de n_2 . On a aussi $d \leq n_1$. En effet, comme $E(K) \cong \mathbf{Z}_{n_1} \oplus \mathbf{Z}_{n_2}$, il existe $U, V \in E(K)$ deux générateurs tels que U soit d'ordre n_1 et V soit d'ordre n_2 . Ecrivons $P = aU + bV, Q = a'U + b'V$, on a :

$$\begin{aligned} e_m(P, Q)^{n_1} &= e_m(aU + bV, a'U + b'V)^{n_1} \\ &= e_m(U, V)^{n_1(ab' - ba')} \text{ (par bilinéarité et alternance)} \\ &= e_m(n_1U, V)^{ab' - ba'} = 1. \end{aligned}$$

Donc on a toujours $dm \leq n_1n_2 = \#E(K)$. Supposons qu'on ait égalité. Alors on doit avoir à la fois $m = n_2$ et $d = n_1$. La deuxième égalité implique que $\text{pgcd}(ab' - ba', n_1) = 1$, ou bien P et Q sont des générateurs de $E(K)$. Dans ce cas la première égalité est aussi satisfaite.

Alors on a vérifié que cet algorithme donne le résultat correct. Reste à voir la complexité. L'étape 1) prend le temps $S(q)$. En étape 2), on va d'abord factoriser N , ce qui se fait en temps $F(N)$. Le (seul !) algorithme pour calculer l'ordre d'un élément dans un groupe fini d'exponent M (*c-à-d* $g^M = 1$ pour tout g) est de complexité $O(\log^2 M)$.

Remarques

- On peut encore améliorer cet algorithme, sachant qu'à l'étape 2 il suffit de connaître la factorisation de $\text{pgcd}(N, q - 1)$.
- Cet algorithme est probabiliste, mais la probabilité qu'une paire de points $(P, Q) \in E(K)^2$ engendre $E(K)$ est $C/\log \log \#E(K)$, où C est une constante absolue.

4.2 Protocole de Diffie-Hellman pour trois parties

C'est la première application constructive des couplages. Supposons qu'il y ait un couplage symétrique $e : G_1 \times G_1 \rightarrow G_2$, P un générateur de G_1 . Supposons que les trois parties A, B, C souhaitent échanger un clé privée à travers d'un canal qui non sécurité. Elles font comme suit :

- A, B, C prennent des entier a, b, c au hasard, et émettent aP, bP, cP .

- Chacune est capable de calculer la clé commune qui est $e(bP, cP)^a = e(aP, cP)^b = e(aP, bP)^c = e(P, P)^{abc}$.

Un adversaire qui récupère aP, bP et cP peut trouver la clé s'il est capable de résoudre le problème dit Diffie-Hellman bilinéaire (BDH), c'est à dire de retrouver $e(P, P)^{abc}$ sachant aP, bP et cP .

Notons que la non-dégénérescence est essentielle pour ce schéma, sinon l'image du couplage serait triviale. A l'origine, comme les distorsions ne sont pas connues, le schéma de Joux avait affaire au couplage asymétrique. Dans ce cas on a besoin de deux points indépendants P, Q et A, B, C émettent $(aP, aQ), (bP, bQ), (cP, cQ)$. La clé commune est donc $e(bP, cQ)^a = e(aP, cQ)^b = e(aP, bP)^c = e(P, Q)^{abc}$. Cette fois-ci la sécurité dépend du problème dit Co-BDH : étant donné P, aP, bP, Q, aQ, cQ , calculer $e(P, Q)^{abc}$. L'avantage du couplage symétrique est que la taille de l'entrée est deux fois plus petite, et chaque partie émet un seul point au lieu de deux.

4.3 Le problème de Diffie-Hellman dans les groupes de couplage

Soit G_1, G_2 deux groupes d'ordre l premier et $e : G_1 \times G_1 \rightarrow G_2$ un couplage fortement non-dégénéré qui est efficacement calculable. Alors il permet de résoudre le problème DDH dans G_1 . En effet, il suffit de vérifier pour P_1, P_2, P_3, P_4 dans G_1 si $e(P_1, P_4) = e(P_2, P_3)$. Si maintenant on a en plus un homomorphisme efficacement calculable $\phi : G_3 \rightarrow G_1$ alors le problème DDH est aussi résoluble dans G_3 . Un cas intéressant est que $G_3 = G_2$. Pour ce cas particulier, on a mieux :

Théorème 4.2. (Verheul) *Supposons que G_2 est un sous-groupe du groupe multiplicatif $\mathbf{F}_{q^k}^*$. S'il existe un homomorphisme efficacement calculable $\phi : G_2 \rightarrow G_1$ alors le problème CDH est résoluble dans G_1 et G_2 .*

Démonstration. Soit g un générateur de G_2 . Soit $e(\phi(g), \phi(g)) = g^\lambda \in G_2$ (λ est inconnu). Si on connaît $g^a, g^b \in G_2$, on peut calculer $e(\phi(g^a), \phi(g^b)) = g^{\lambda ab}$. Notre but est d'enlever le facteur λ dans la puissance. On a la formule suivante :

$$e(\phi(g^{\lambda^i}), \phi(g^{\lambda^j})) = g^{\lambda^{i+j+1}}$$

ce qui permet de calculer $g^{\lambda^{q-2}} = g^{\lambda^{-1}}$ en temps $O(\log q)$, en utilisant une chaîne d'addition. Maintenant, on a $e(\phi(g^{\lambda ab}), \phi(g^{\lambda^{-1}})) = g^{\lambda ab}$. Donc on a résolu le problème de CDH dans G_2 . Un argument analogue permet de résoudre le problème de CDH dans G_1 .

Application : la sécurité du cryptosystème XTR. Dans le cryptosystème XTR, on travaille avec le sous-groupe d'ordre $p^2 - p + 1$ du groupe multiplicatif $\mathbf{F}_{p^2}^*$, appelé le groupe XTR. Les éléments de XTR sont représentés par leur trace sur \mathbf{F}_{p^2} , à savoir $Tr(g) = g + g^p + g^{1-p} \in \mathbf{F}_{p^2}$. Via cette représentation, les calculs dans XTR se ramènent à ceux dans \mathbf{F}_{p^2} , qui sont efficaces.

Maintenant il existe des courbes elliptiques sur \mathbf{F}_{p^2} de cardinal $p^2 - p + 1$. Ce sont des courbes appelées CTP, isomorphes à celles d'équation $y^2 = x^3 + a$, où a est un carré mais pas un cube dans \mathbf{F}_{p^2} . Le plongement de MOV fournit un homomorphisme efficacement calculable de groupe de ces courbes dans le groupe XTR. Il est donc naturel de suggérer que la sécurité de XTR est la même que celle des courbes CTP. C'est vrai si l'inverse de l'homomorphisme au-dessus est aussi efficacement calculable. Verheul [16] a donné une réponse négative. En effet, d'après le théorème 4.2 l'existence d'un tel homomorphisme de XTR dans une courbe CTP entraînerait que le problème de CDH est résoluble dans les courbes CTP et dans le groupe XTR, ce qui est fort improbable car c'est l'hypothèse de sécurité de XTR !

4.4 Chiffrement à base d'identité

C'est une des applications frappantes des couplages. Shamir pose ce problème en 1984 et ce n'est qu'en 2001 qu'il a été résolu (en moyen des couplages par Boneh et Franklin et par Cocks qui utilise le symbole de Jacobi). On présente ici le schéma originel de Boneh-Franklin.

Le schéma consiste en 4 algorithmes : **Setup** pour générer les paramètres du système, **Extract** pour donner à chaque utilisateur une clé privée correspondant à son identité, **Encrypt** pour coder un message envoyé à un utilisateur et **Decrypt** pour déchiffrer le message codé reçu.

Setup:

- 1) Générer un nombre premier q , deux groupes d'ordre q , $(G_1, +)$ et $(G_2, *)$, et un couplage symétrique $e : G_1 \times G_1 \rightarrow G_2$. Choisir P arbitraire dans G_1^* .
- 2) Prendre s arbitraire dans \mathbf{Z}_q^* , poser $P_{pub} = sP$.
- 3) Choisir des fonctions de hachage $H_1 : \{0, 1\}^* \rightarrow G_1^*$ et $H_2 : \{0, 1\}^n \rightarrow G_2^*$ pour un certain n .

L'espace des messages est $\mathcal{M} = \{0, 1\}^n$ et l'espace des chiffrés est $\mathcal{C} = G_1^* \times \{0, 1\}^n$. Les paramètres du système sont $params = \langle q, G_1, G_2, e, n, P, P_{pub}, H_1, H_2 \rangle$. La clé maître est $s \in \mathbf{Z}_q^*$.

Extract: Pour une identité $ID \in \{0, 1\}^*$

- 1) Calculer $Q_{ID} = H_1(ID) \in G_1^*$.
- 2) La clé privée de ID est $d_{ID} = sQ_{ID}$, où s est la clé maître.

Encrypt: Pour chiffrer un message $M \in \mathcal{M}$ avec la clé publique ID

- 1) Calculer $Q_{ID} = H_1(ID) \in G_1^*$.
- 2) Prendre $r \in \mathbf{Z}_q^*$ au hasard.
- 2) Le chiffré est $C = \langle rP, M \oplus H_2(g_{ID}^r) \rangle$, où $g_{ID} = e(Q_{ID}, P_{pub}) \in G_2^*$.

Decrypt: Soit $C = \langle U, V \rangle \in \mathcal{C}$ un chiffré de l'identité ID . Pour déchiffrer C avec la clé privée $d_{ID} \in G_1^*$, calculer $V \oplus H_2(e(d_{ID}, U)) = M$.

On vérifie que **Decrypt** et **Encrypt** sont bien compatibles grâce à la propriété bilinéaire des couplages.

Bibliography

- [1] **Ian F. Blake, Gadiel Seroussi, Nigel P. Smart** (editors) : *Advances in Elliptic Curve Cryptography* (London Mathematical Society Lecture Note Series 317), Cambridge University Press (2005).
- [2] **A. J. Menezes** : *Elliptic curve public key systems*, Kluwer Academic Publishers, 1993.
- [3] **J. Silverman** : *The arithmetic of elliptic curves*, Springer-Verlag, 1986.
- [4] **S. D. Galbraith** : *Supersingular curves in cryptography*, Advances in Cryptology - Asiacrypt'2001, Lecture Notes on Computer Science 2248, Springer-Verlag (2002), pp. 495-513.
- [5] **M. Maas** : *Pairing-Based Cryptography*, Master Thesis, Technische Universiteit Eindhoven, 2004.
- [6] **F. Heß** : *A Note on the Tate Pairing of Curves over Finite Fields*, 2002. Submitted preprint.
- [7] **A. Miyaji, M. Nakabayashi, S. Takano** : *New Explicit Conditions of Elliptic Curve Traces for FR-Reduction*, IEICE Transactions on Fundamentals E84-A(5) (2001), pp. 1234–1243.
- [8] **G. Frey, H. Rück** : *A remark concerning m -divisibility and the discrete logarithm in the divisor class group of curves*, Mathematics of Computation, 62 (1994), pp. 865-874.
- [9] **G. Frey, M. Müller, H. Rück** : *The Tate Pairing and the Discrete Logarithm Applied to Elliptic Curve Cryptosystems*, IEEE Transactions on Information Theory 45(5) (1999), pp. 1717-1719.
- [10] **V. S. Miller** : *The Weil Pairing, and Its Efficient Calculation*, Journal of Cryptology 17 (2004), pp. 235 - 261

- [11] **V. S. Miller** : *Use of elliptic curves in cryptography*, Advances in Cryptology - CRYPTO '85, LNCS218, (1986), pp 417-426.
- [12] **N. Koblitz** : *Elliptic curve cryptosystems*, Mathematics of Computation 48, 1987, pp 203–209.
- [13] **L. S. Charlap, R. Coley** : *An Elementary Introduction to Elliptic Curves II*, CCR Expository Report No. 34, 1990, disponible à <http://www.idaccr.org/reports/er34.ps>.
- [14] **L. S. Charlap, D. P. Robbins** : *An Elementary Introduction to Elliptic Curves*, CCR Expository Report No. 31, 1988, disponible à <http://www.idaccr.org/reports/er31.ps>.
- [15] **A. Joux** *A One Round Protocol for Tripartite Diffie–Hellman*, Journal of Cryptology 17 (2004), pp. 263 - 276.
- [16] **E. R. Verheul** : *Evidence that XTR Is More Secure than Supersingular Elliptic Curve Cryptosystems*, Journal of Cryptology 17 (2004), pp. 277 - 296.
- [17] **D. Boneh, B. Lynn, H. Shacham** : *Short Signatures from the Weil Pairing*, Journal of Cryptology 17 (2004), pp. 297 - 319
- [18] **A. K. Lenstra, E. R. Verheul** *An overview of the XTR public key system*, Proceedings of the Warsaw Conference on Public-Key cryptography and computational number theory.
- [19] **I. M. Duursma, H.-S. Lee** : *Tate Pairing Implementation for Hyperelliptic Curves $y^2 = x^p - x + d$* , Advances in Cryptology – Asiacrypt'2003, Lecture Notes on Computer Science 2894, Springer-Verlag (2003), pp. 111-123.
- [20] **P. S. L. M. Barreto, S. Galbraith, C. O hEigearthaigh, M. Scott** : *Efficient pairing computation on supersingular abelian varieties*, Cryptology ePrint Archive, Report 2004/375, 2004.
- [21] **P. S. L. M. Barreto, B. Lynn, M. Scott** : *Efficient Implementation of Pairing-Based Cryptosystems*, Journal of Cryptology 17 (2004), pp. 321-334.
- [22] **P. S. L. M. Barreto, H. Y. Kim, B. Lynn, M. Scott** : *Efficient Algorithms for Pairing-Based Cryptosystems* Advances in Cryptology – Crypto'2002, Lecture Notes on Computer Science 2442, Springer-Verlag (2002), pp. 354–368.

- [23] **R. Schoof** : *Elliptic curves over finite field and the computation of square roots mod p* , Mathematics of Computation, 44(1985), pp. 483-494.
- [24] **R. Schoof** : *Nonsingular plane cubic curves over finite fields*, Journal of Combinatorial Theory, A 46 (1987), pp. 183-211.
- [25] **R. Balasubramanian, N. Koblitz** : *The Improbability That an Elliptic Curve Has Subexponential Discrete Log Problem under the Menezes—Okamoto—Vanstone Algorithm*, Journal of Cryptology 2 (1998), pp. 141 - 145.
- [26] **E. Waterhouse** : *Abelian varieties over finite fields*, Ann. Sci. Ecole. Norm. Sup. 2 (1969), pp. 521-560.