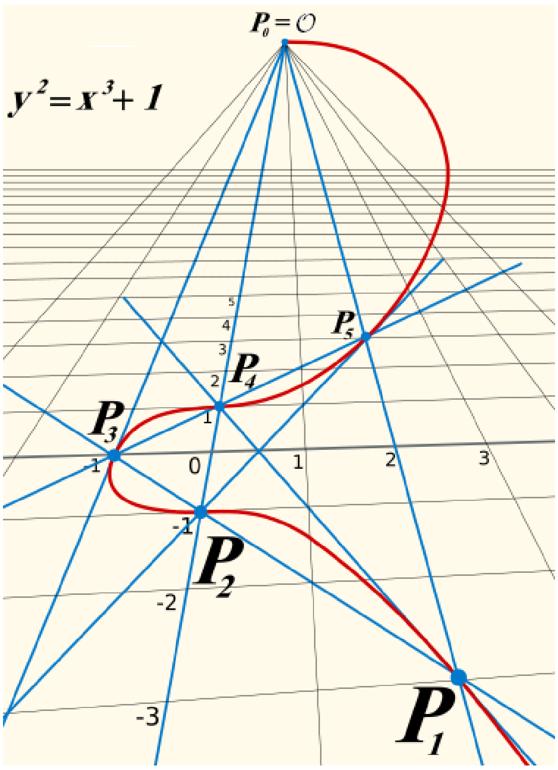
Ecole Polytech de Marseille
Case 925
13288 Marseille cedex 9

Année 5
Option : Systèmes Informatiques Critiques et Applications

Cours de Cryptographie Avancée

Courbes Elliptiques
Application à la Cryptographie



Par

Stéphane Ballet et Alexis Bonecaze

Table des matières

Chapitre 1

Introduction

D'une manière générale la cryptographie permet l'échange sécurisé de données entre deux entités souvent nommées Alice et Bob dans la littérature. Le développement des nouvelles technologies de télécommunication a eu pour effet de multiplier les actions nécessitant un certain niveau de sécurité.

De nos jours la cryptographie fait partie intégrante de notre quotidien. En effet, elle est sous-jacente dans de nombreux domaines dont les systèmes de cartes à puces. Par exemple, lors de l'utilisation d'une carte bancaire, pour effectuer un retrait à un guichet automatique, ou un achat sur internet, après avoir été identifié comme étant le véritable titulaire du compte à débiter. La cryptographie permet de protéger l'accès à certaines données comme les informations bancaires, médicales, ou encore celles échangées sur le réseau internet .

L'algorithme le plus répandu de nos jours, RSA, algorithme décrit en 1977 par Rivest, Shamir et Adleman (d'où son nom), utilise l'arithmétique modulaire (modulo un entier N de grande taille). Sa sécurité repose sur le fait qu'il est difficile de déterminer la factorisation en nombres premiers de N, surtout s'il est de grande taille. L'existence d'algorithmes de factorisation rapides (dont l'algorithme ECM, *Elliptic Curve Method*, utilisant les courbes elliptiques) est un problème pour ce cryptosystème. Ils entrainent le recours à des entiers N de plus en plus grands afin de garantir la sécurité. Par conséquent RSA voit sa performance diminuer au fil du temps.

Les systèmes cryptographiques basés sur les courbes elliptiques permettent d'obtenir un gain en efficacité dans la gestion de clés. En effet, de tels cryptosystèmes nécessitent des clés de taille beaucoup plus modeste (par exemple, une clé de 160 bits lorsque RSA utilise une clé de 1024 bits, à un niveau de sécurité équivalent) ce qui représente un avantage pour les systèmes utilisant les cartes à puces dont l'espace mémoire est très limité. De plus, les algorithmes de calculs liés aux courbes elliptiques sont plus rapides, et ont donc un débit de générations et d'échanges de clé beaucoup plus important.

Dans un premier temps nous présenterons la théorie des courbes elliptiques, et comment les appliquer à la cryptographie. Nous étudierons, dans un second temps, l'aspect pratique des courbes elliptiques.

Chapitre 2

Généralités sur les courbes elliptiques

2.1 Introduction

Dans cette partie nous allons dans un premier temps définir de manière succincte les courbes elliptiques et en dégager les principales propriétés, puis dans un second temps nous verrons comment munir ce type de courbes d'une structure de groupe abélien.

Les définitions et théorèmes cités dans ce chapitre font référence aux travaux de Marc Joyes [2] et Reynald Lercier [3], ainsi qu'aux cours de cryptographie de Stéphane Ballet [1] et Yves Driencourt [4].

2.2 Définitions

Définition 1

Une courbe elliptique *est une paire* $(E, \mathcal{O})$ *où :*

– *E est une cubique irréductible non-singulière de genre 1,*

– *$\mathcal{O} \in E$.*

Définition 2

Une courbe elliptique est définie sur un corps $\mathbb{K}$ *si :*

– *E est une courbe sur $\mathbb{K}$ (i.e. donnée par l'annulation d'un polynôme de $\mathbb{K}[X, Y]$),*

– *$\mathcal{O}$ est un point de la courbe dont les coordonnées sont dans $\mathbb{K}$.*

Notation 3

L'ensemble des points de E à coordonnées dans $\mathbb{K}$ sera noté $E(\mathbb{K})$.

2.3 Equation de Weierstrass

2.3.1 Définition

Définition 4

On appelle espace projectif de dimension 2 associé à un corps $\mathbb{K}$*, noté* $\mathbb{P}^2(\mathbb{K})$*, l'ensemble des classes* $(X : Y : Z)$*, appelés coordonnées homogènes de la relation d'équivalence :*

$$\forall (X,Y,Z) \in \ \mathbb{K}^3 \backslash \{0_{\mathbb{K}^3}\}, \quad \forall (X',Y',Z') \in \ \mathbb{K}^3 \backslash \{0_{\mathbb{K}^3}\},$$
$$(X,Y,Z) \equiv (X',Y',Z') \Leftrightarrow \exists \ t \in \ \mathbb{K}^* \begin{cases} X' = tX \\ Y' = tY \\ Z' = tZ \end{cases}$$

Théorème 1

Si E *est une courbe elliptique définie sur* $\mathbb{K}$*, alors il existe* $\Phi : E(\mathbb{K}) \to \mathbb{P}^2(\mathbb{K})$ *qui fournit un isomorphisme de* $E(\mathbb{K})$ *sur une courbe* $C(\mathbb{K})$ *tel que* $\Phi(\mathcal{O}) = (0 : 1 : 0)$ *donnée par l'équation de Weierstrass suivante :*

$$C : \ F(X,Y,Z) = Y^2Z + a_1XYZ + a_3YZ^2 - X^3 - a_2X^2Z - a_4XZ^2 - a_6Z^3 = 0$$

où $(a_1, ..., a_4, a_6) \in \mathbb{K}^5$.

Ainsi, l'ensemble des points d'une courbe elliptique E définie sur $\mathbb{K}$ est donc équivalent à :

$$E(\mathbb{K}) = \{(X : Y : Z) \in \mathbb{P}^2(\mathbb{K}), F(X,Y,Z) = 0\}$$

Remarque 1

- *Seule une classe d'équivalence de cet ensemble vérifie* $Z = 0$*, il s'agit de la classe* $(0 : 1 : 0)$ *que nous nommerons* point à l'infini *et noterons* $\mathcal{O}$*. Pour toutes les autres classes, il existe un unique représentant de la forme* $(X : Y : 1)$*. C'est pourquoi nous considérerons par la suite* $E(\mathbb{K})$ *comme la réunion de* $\mathcal{O}$ *et de l'ensemble des couples* (x, y)*, où* $x = X/Z$ *et* $y = Y/Z$ *représentent les coordonnées non-homogènes, vérifiant l'équation*
$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 \ ,$$
i.e. :
$$E(\mathbb{K}) \ = \ \{\mathcal{O}\} \ \cup \ \{(x,y) \in \mathbb{P}^2(\mathbb{K}) / y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6\}$$
- $\mathcal{O}$ *est le seul point à l'infini et il n'est pas singulier car* $\partial F/\partial Z(0,1,0) = 1 \neq 0$.

2.3.2 Discriminant et j-invariant

Voici quelques notions utiles à l'étude des courbes définies par une équation de Weierstrass :

Soient les quantités :

$$\begin{aligned}
b_2 &= a_1^2 + 4a_2, \\
b_4 &= a_1 a_3 + 2a_4, \\
b_6 &= a_3^2 + 4a_6, \\
b_8 &= b_2 a_6 - a_1 a_3 a_4 + a_2 a_3^2 - a_4^2, \\
c_4 &= b_2^2 - 24 b_4, \\
c_6 &= -b_2^3 + 36 b_2 b_4 - 216 b_6.
\end{aligned}$$

Définition 5
On appelle discriminant*, noté* Δ*, la quantité* $\Delta = -b_2^2 b_8 - 8b_4^3 - 27b_6^2 + 9b_2 b_4 b_6$

Théorème 2
Soit C *une courbe définie sur un corps* $\mathbb{K}$ *par une équation de Weierstrass, alors :*

$$C \textit{ non-singulière} \iff \Delta \neq 0$$

Définition 6
On appelle invariant modulaire *ou* j-invariant*, et on note* j*, la quantité :* $j = c_4^3 \Delta^{-1}$

Remarque 2
Puisque qu'une courbe elliptique est non-singulière, son discriminant est tel que $\Delta \neq 0$*. Ainsi l'invariant modulaire d'une courbe elliptique est toujours bien défini.*

Définition 7
Une courbe elliptique est dite supersingulière *lorsque son j-invariant est nul, i.e.* $j = 0$*.*

2.4 Exemple

Soit E la courbe elliptique définie sur $\mathbb{R}$ par l'équation de Weierstrass $y^2 = x^3 - x$.

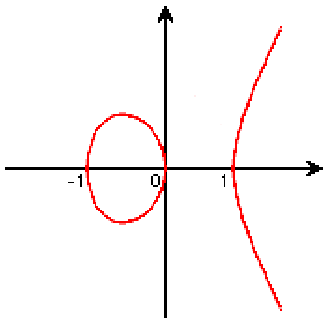


FIGURE 2.1 – Représentation de E

On a :

$$a_1 = a_2 = a_3 = a_6 = 0 \quad \text{et} \quad a_4 = -1$$

On en déduit :

$$\begin{aligned} b_2 = b_6 &= c_6 = 0, \\ b_4 &= -2, \\ b_8 &= -1, \\ c_4 &= 48. \end{aligned}$$

Le calcul du discriminant donne donc : $\Delta = 64$ et l'invariant modulaire vaut alors : $j = 1728$, la courbe elliptique E n'est donc ni singulière ni supersingulière.

2.5 Loi de groupe

L'ensemble des points d'une courbe elliptique, comme nous allons voir dans ce qui suit, peut être muni d'une loi de groupe commutative. Cette loi de composition interne sera notée de manière additive et nous permettra de définir la multiplication d'un point par un nombre entier. Nous disposerons alors du matériel nécessaire pour introduire le problème du logarithme discret sur les courbes elliptiques, d'où l'enjeu de celle-ci d'un point de vue cryptographique.

2.5.1 Définition et construction

La loi de composition interne va être définie à l'aide du théorème suivant :

Théorème 3 ***Règle de la sécante tangente***
Soient E une courbe elliptique et D une droite, toutes deux définies sur un corps $\mathbb{K}$.
Si D coupe E en deux points (comptés avec leur multiplicité) alors D coupe E en trois points (comptés avec leur multiplicité).

De ce théorème une première loi de composition interne que nous noterons $*$ peut être déduite. Elle servira à construire la loi de groupe sur l'ensemble des points d'une courbe elliptique :

Définition 8 ***Loi de composition interne de la sécante tangente***
Soit $E(\mathbb{K})$ une courbe elliptique définie sur un corps $\mathbb{K}$. D'après le théorème précédent, puisqu'une courbe elliptique est irréductible et non singulière :
- *Soient deux points distincts $P, Q \in E(\mathbb{K}), P \neq Q$, alors la droite (PQ) recoupe la courbe $E(\mathbb{K})$ en un troisième point noté $P * Q$.*
- *Soit un point $P \in E(\mathbb{K})$ alors on peut définir $P * P$ comme le point d'intersection de la courbe $E(\mathbb{K})$ avec sa tangente au point P.*

Dans un premier temps la loi de groupe abélien d'une courbe elliptique va être définie d'un point de vue géométrique, comme suit. Nous verrons dans la sous section suivante comment la définir de manière explicite.

Théorème 4 ***Théorème de Poincaré***
Soit un corps $\mathbb{K}$. Si $(E, \mathcal{O})$ est une courbe elliptique définie sur $\mathbb{K}$, alors la loi

$$\begin{array}{rccc} + : & E(\mathbb{K}) \times E(\mathbb{K}) & \longrightarrow & E(\mathbb{K}) \\ & (P, Q) & \longmapsto & \mathcal{O} * (P * Q) \end{array}$$

confère à $(E, \mathcal{O})$ une structure de groupe abélien d'élément neutre $\mathcal{O}$.

2.5.2 Formules explicites de l'addition

Nous allons à présent donner les formules explicites permettant de calculer les coordonnées du point $R = P + Q$, résultant de l'addition de deux points P et Q d'une courbe elliptique $E(\mathbb{K})$ donnée par une équation de Weierstrass.

Bien entendu, de par la structure de groupe de $(E(\mathbb{K}),+)$, on sait que $P+\mathcal{O} = \mathcal{O}+P = P$ et le calcul du résultat d'une telle addition est trivial, de même que le cas $\mathcal{O} + \mathcal{O} = \mathcal{O}$.

Les cas où $\mathcal{O}$ est un des deux termes de l'addition de deux points de $E(\mathbb{K})$ ayant été traités, nous allons nous intéresser au cas où celui-ci n'est aucun des deux termes de l'addition.

Puisque seules les coordonnées homogènes du point à l'infini $\mathcal{O}$ vérifient $Z = 0$, nous travaillerons avec les coordonnées non-homogènes.

Les formules permettant le calcul des coordonnées de l'opposé d'un point s'expriment ainsi :

Définition 9 ***Opposé d'un point***
Soit (x_P, y_P) les coordonnées non-homogènes d'un point P de $E(\mathbb{K})$.
Alors son opposé $Q = -P$ a pour coordonnées :

$$\begin{cases} x_Q = x_P \\ y_Q = -y_P - a_1 x_p - a_3 \end{cases}$$

Voici les formules explicites permettant d'additionner deux points distincts et non opposées (il convient donc de vérifier que les points à additionner ne sont pas opposés) :

Définition 10 ***Addition***
Soient :
- *$E(\mathbb{K})$ une courbe elliptique donnée par l'équation de Weierstrass,*
$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6.$$
- *(x_P, y_P) et (x_Q, y_Q) les coordonnées non-homogènes respectives de P et Q deux points non opposés l'un de l'autre, de $E(\mathbb{K})$.*
- *$R = P + Q \in E(\mathbb{K})$ de coordonnées non-homogènes (x_R, y_R).*

Alors on a $\begin{cases} x_R = \lambda^2 + a_1\lambda - a_2 - x_P - x_Q \\ y_R = -(\lambda + a_1)x_R + \lambda x_P - x_Q \end{cases}$

avec λ tel que : $\begin{cases} \lambda = \frac{y_P - y_Q}{x_P - x_Q} \text{ si } x_P \neq x_Q \\ \\ \lambda = \frac{3{x_P}^2 + 2a_2x_P + a_4 - a_1y_P}{2y_P + a_1x_P + a_3} \text{ si } x_P = x_Q \end{cases}$

Notons que si $Q \neq -P$ et $x_P = x_Q$, alors $P = Q$. Par conséquent, l'addition de P et Q revient à doubler le point P.

2.6 Multiplication par un entier

Comme nous l'avons vu précédemment, il est possible d'additionner deux points d'une courbe elliptique. En revanche il n'existe pas de multiplication entre deux points. Grâce à une succession d'additions, nous allons, cependant, pouvoir définir la multiplication d'un point par un entier. Cette multiplication est d'autant plus importante que l'exponentiation modulaire définie sur $(\mathbb{Z}/p\mathbb{Z})^*$ (succession de multiplications d'un élément de $(\mathbb{Z}/p\mathbb{Z})^*$) a un équivalent sur le groupe abélien formé par la courbe elliptique.

Définition 11
Soient $E(\mathbb{K})$ une courbe elliptique, un point $P \in E(\mathbb{K})$, et un entier $n \in \mathbb{N}^*$.
On définit les multiples de P *par* $n \cdot P = \underbrace{P + \cdots + P}_{n \text{ fois}}$.
Cette définition peut être étendue par $\begin{cases} 0_{\mathbb{N}} \cdot P = \mathcal{O}, \\ -m \cdot P = m \cdot (-P). \end{cases}$

2.7 Isomorphismes et formes canoniques

L'équation d'une courbe elliptique peut prendre une forme simplifiée, dite canonique. Cette forme canonique diffère légèrement suivant la caractéristique de $\mathbb{K}$.

Théorème 5
Soient deux courbes elliptiques E_a et E_b définies sur un corps $\mathbb{K}$.
Si E_a et E_b sont isomorphes alors leurs j-invariants sont égaux, ce que l'on note : $j(E_a) = j(E_b)$.

Remarque 3
La réciproque de ce théorème est vraie dès lors que $\mathbb{K}$ est algébriquement clos.

Proposition 6
Soit E une courbe elliptique donnée dans $\mathbb{K}$ par une équation de Weierstrass.
Alors il existe un isomorphisme $(x, y) \longmapsto (u^2x + r,\ u^3y + u^2sx + t)$ qui ramène cette courbe à l'une des courbes dont l'équation canonique est donnée dans le tableau suivant :

Condition		Equation	Discriminant Δ	j-invariant
$Car(\mathbb{K}) \neq 2, 3$		$y^2 = x^3 + a_4x + a_6$	$-16(4a_4^3 + 27a_6^2)$	$1728 \cdot 4a_4^3/(4a_4^3 + 27a_6^2)$
$Car(\mathbb{K}) = 2$	$j_E = 0$	$y^2 + a_3y = x^3 + a_4x + a_6$	a_3^4	0
	$j_E \neq 0$	$y^2 + xy = x^3 + a_2x^2 + a_6$	a_6	$1/a_6$
$Car(\mathbb{K}) = 3$	$j_E = 0$	$y^2 = x^3 + a_4x + a_6$	$-a_4^3$	0
	$j_E \neq 0$	$y^2 = x^3 + a_2x^2 + a_6$	$-a_2^3a_6$	$-a_2^3/a_6$

Table 2.1 – Equation de Weierstrass et caractéristique du corps de définition

Remarque 4
Cet isomorphisme conserve les propriétés de la courbe.

2.8 Les courbes elliptiques définies sur un corps fini

Nous considèrerons par la suite connues les notions élémentaires sur les corps, à savoir celles concernant les lois et la caractéristique d'un corps, les isomorphismes de corps ainsi que le théorème de Wedderburn, énonçant que les corps finis sont commutatifs.

2.8.1 Cardinalité

Définition 12
Le nombre de points du groupe $E(\mathbb{F}_q)$, appelé cardinalité de la courbe elliptique *et noté $Card(E(\mathbb{F}_q))$, est le nombre de solutions de l'équation de Weierstrass (cf p. 3).*

Vu comme un polynôme de $\mathbb{F}_q[Y]$, l'équation de Weierstrass est du second degré. De ce fait il existe, pour chaque valeur de x, au plus deux valeurs de y telles que le couple (x, y) vérifie cette équation. Puisque $x \in \mathbb{F}_q$, il y a q choix de valeurs possibles pour x, et donc en comptant $\mathcal{O}$, au plus $2q + 1$ couples sont solutions de l'équation de Weierstrass.

En moyenne on a une chance sur deux pour que, x étant fixé, l'équation en y admette des solutions dans $\mathbb{F}_q$.

Ceci est résumé par le théorème suivant :

Théorème 7 *Théorème de Hasse*
Soit $E(\mathbb{F}_q)$, où $q = p^n \in \mathbb{N}$, une courbe elliptique.
On a alors :

$$Card(E(\mathbb{F}_q)) = q + 1 \pm 2\sqrt{q}$$

Ce théorème ne fournit qu'un encadrement du nombre de points de la courbe. Or en cryptographie, il est essentiel de connaître le nombre précis de points de la courbe elliptique manipulée. Des algorithmes ont donc été construits dans le but de connaître le nombre exact de points d'une courbe elliptique.

Algorithme de comptage

Les algorithmes de comptage sont devenus un enjeu de taille dans la recherche en cryptographie. Schoof, en 1985, fut le premier à proposer un algorithme de complexité polynômiale en $log\ q$: $O(log^8 q)$. Les travaux d'Atkin, Elkies, puis Couveignes aboutissent à un algorithme de complexité en $O(log^5 q)$. Le principe de ces algorithmes est donné dans la sous-section 4.2.2.

Théorème 8
Une courbe elliptique $E(\mathbb{F}_q)$, où $q = p^n$, de cardinal $q + 1 - t$ est supersingulière si et seulement si $t \equiv 0\ mod(p)$

2.8.2 Structure de groupe

Théorème 9 ***Théorème de Kronecker***
Soit G un groupe abélien d'ordre fini, alors il existe une suite $(a_n)_{n\in\mathbb{N}}$ tel que :

– $\forall\ i \in \{1, \ldots, s-1\},\ \ n_{i+1} \mid n_i,$

– $G \cong \mathbb{Z}/n_1\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/n_s\mathbb{Z}$ *, où* $s \geq 2.$

Le groupe G est alors dit de type $(n_1, \ldots, n_s)$ et de rang s.

Voici un corollaire de ce théorème appliqué aux courbes elliptiques :

Corollaire 10
$E(\mathbb{F}_q)$ est un groupe abélien de rang 1 ou 2, dit cyclique ou bicyclique.
Le type de ce groupe est (n_1, n_2) :

$$i.e.\ E(\mathbb{F}_q) = \mathbb{Z}/n_1\mathbb{Z} \oplus \mathbb{Z}/n_2\mathbb{Z} \quad avec\ n_2 \mid n_1\ et\ n_2 \mid q-1.$$

Théorème 11
$E(\mathbb{F}_q)$ est un groupe de torsion i.e. $\forall\ P \in E(\mathbb{F}_q),\ \exists\ k \in \mathbb{N}^*,\ k \cdot P = \mathcal{O}.$

Définition 13

On appelle point de m-torsion *un point* $P \in E(\overline{\mathbb{F}}_q)$, *où* $\overline{\mathbb{F}}_q$ *est la clôture algébrique de* $\mathbb{F}_q$, *tel que* $m \cdot P = \mathcal{O}$.

Notation 14

On notera $E[m]$ *le sous-groupe de* $E(\overline{\mathbb{F}}_q)$ *des points de* m*-torsion, et* $E(\mathbb{F}_q)[m]$ *le sous-groupe de* $E[m]$ *des points de* m*-torsion contenus dans* $E(\mathbb{F}_q)$.

La structure de $E[m]$ est donnée par le théorème suivant :

Théorème 12

Soient $E(\overline{\mathbb{F}}_q)$ *une courbe elliptique définie sur* $\overline{\mathbb{F}}_q$, *et* m *un entier naturel.*

- *Si* m *est premier avec la caractéristique de* $\mathbb{F}_q$, *alors :*
$$E[m] = \mathbb{Z}/m\mathbb{Z} \oplus \mathbb{Z}/m\mathbb{Z}.$$
- *Si* m *est une puissance de la caractéristique de* $\mathbb{F}_q$, *alors :*
$$\begin{cases} E[m] = \{\mathcal{O}\} \text{ si } E \text{ est supersingulière,} \\ E[m] = \mathbb{Z}/m\mathbb{Z} \text{ sinon.} \end{cases}$$

Chapitre 3

Courbes elliptiques et cryptographie

3.1 Introduction

Dans la pratique, les courbes elliptiques destinées à des applications cryptographiques doivent être définies sur un corps premier $\mathbb{F}_p$ ou sur un corps fini $\mathbb{F}_{2^n}$.

Les cryptosystèmes utilisant les courbes elliptiques définies sur $\mathbb{F}_{2^n}$ doivent se plier à certaines exigences pour garantir une meilleure sécurité. De telles courbes sont cependant de moins en moins utilisées car le corps $\mathbb{F}_{2^n}$ est considéré comme trop structuré. Cependant les calculs sur de tels cryptosystèmes ont l'avantage d'être plus faciles à implémenter.

Les cryptosystèmes utilisant les courbes elliptiques définies sur les corps finis de la forme $\mathbb{F}_p$ peuvent être compromis par l'*attaque MOV* évoquée dans la section suivante. La taille des clés utilisées doit alors respecter les critères de sécurité appliqués au problème du logarithme discret dans un corps fini, on perd alors l'intérêt d'utiliser les courbes elliptiques.

Le contenu de ce chapitre a pu être rédigé notamment grâce aux études de Reynald Lercier [3] et Marc Joyes [2] ainsi que le cours d'Yves Driencourt [4].

3.2 Courbes elliptiques sur $\mathbb{K} = \mathbb{F}_{2^n}$

3.2.1 Courbes elliptiques convenables d'un point de vue cryptographique

Dans le cadre des courbes elliptiques définies sur $\mathbb{F}_{2^n}$, corps de caractéristique 2, il existe deux formes simplifiées de l'équation de Weierstrass :

$$\begin{aligned} y^2 + xy &= x^3 + a_2x^2 + a_6 \; mod(2^n) \quad (3.1) \\ y^2 + a_3y &= x^3 + a_4x + a_6 \; mod(2^n) \quad (3.2) \end{aligned}$$

D'après le tableau 2.1 p.9 donnant les discriminants et les j-invariants de chacune de ces deux équations, on s'aperçoit que la seconde équation est celle d'une courbe supersingulière (son j-invariant est nul), or les courbes supersingulières sont sujettes à l'*attaque MOV* :

Attaque MOV

Les travaux menés en 1993 par Menezes, Okamoto et Vanstone, qui ont donné leurs noms à l'*attaque MOV*, montrent que le problème du logarithme discret sur $E(\mathbb{F}_p)$ peut être ramené à celui du logarithme discret dans $(\mathbb{F}_{p^k})^*$. En particulier dans le cas de courbes supersingulières, il peut être ramené à celui du logarithme discret sur $\mathbb{F}_{p^k}$ avec $k \in \{1, 2, 3, 4, 6\}$, généralement $k = 2$. Cela induit un risque car la réduction à un tel problème se fait en temps polynomial en $O(log\ p)$, et la résolution du problème du logarithme discret est alors réalisable par un algorithme probabiliste sous-exponentiel.

En conclusion, les courbes elliptiques décrites par l'équation (3.2) sont donc à éviter d'où la définition suivante :

Définition 15
On dira d'une courbe elliptique qu'elle est convenable sur $\mathbb{F}_{2^n}$ *lorsque son équation canonique est du type (3.1).*

3.2.2 Formules explicites des opérations

Opposé

Soit $P(x_P, y_P)$ un point d'une courbe elliptique $E(\mathbb{F}_{2^n})$.
Son opposé Q a pour coordonnées : $\begin{cases} x_Q = x_P \\ y_Q = x_P + y_P \end{cases}$

Addition

Soient :
- $E(\mathbb{F}_{2^n})$ une courbe elliptique convenable sur $\mathbb{F}_{2^n}$,

- Deux points de $E(\mathbb{F}_{2^n})$, $P\ (x_P, y_P)$ et $Q\ (x_Q, y_Q)$ non opposés.

Alors si $R = (x_R, y_R) = P + Q$:

$$\begin{cases} x_R = \lambda^2 + \lambda + a_2 + x_P + x_Q \\ y_R = (\lambda + 1) \cdot x_R + \lambda \cdot x_P + y_P \end{cases}$$

où $\begin{cases} \lambda = \frac{y_P + y_Q}{x_P + x_Q} & \text{si } x_P \neq x_Q \\ \lambda = \frac{x_P^2 + y_P}{x_P} & \text{si } x_P = x_Q \end{cases}$

Multiplication par un entier $n \in \mathbb{N}$

Soient $E(\mathbb{F}_{2^n})$ une courbe elliptique, un point $P \in E(\mathbb{F}_{2^n})$, et un entier $n \in \mathbb{N}^*$.
Comme précédemment nous allons définir la multiplication par un entier par une succession d'additions : $\begin{cases} n \cdot P = \underbrace{P + \cdots + P}_{n \text{ fois}} \\ 0_{\mathbb{N}} \cdot P = \mathcal{O} \\ (-m) \cdot P = m \cdot (-P) \end{cases}$

3.2.3 Exemple

Soient :

- Le corps fini $\mathbb{F}_{2^4} = \mathbb{F}_2 / < X^4 + X + 1 >$

- $\alpha \in \mathbb{F}_{2^4}$ tel que $\mathbb{F}_{2^4} =< \alpha >$ et racine du polynôme $X^4 + X + 1$ irréductible sur $\mathbb{F}_{2^4}$

- La courbe elliptique $E(\mathbb{F}_{2^4})$ définie par l'équation de Weierstrass $y^2 + x \cdot y = x^3 + \alpha^4 \cdot x^2 + 1$

Notons tout d'abord que par construction le corps $\mathbb{F}_{2^4}$ est tel que

$$\mathbb{F}_{2^4} = \{[x_3\ x_2\ x_1\ x_0],\ (x_0, x_1, x_2, x_3)\ \in \mathbb{F}_{2^4}\}$$

où $[x_3\ x_2\ x_1\ x_0] = x_3 \cdot \alpha^3 + x_2 \cdot \alpha^2 + x_1 \cdot \alpha^1 + x_0 \cdot \alpha^0$.
Il possède donc 16 éléments. En effet, il est constitué de $4 - uplets$ d'éléments de $\mathbb{F}_2$.
$[x_3\ x_2\ x_1\ x_0]$ sera appelé écriture vectorielle dans la base canonique $\mathcal{B} = \{\alpha^3, \alpha^2, \alpha^1, \alpha^0\}$.

Explicitons $\mathbb{F}_{2^4}$ en fonction de α :
Puisque $\mathbb{F}_{2^4}$ est un corps de caractéristique 2, $(\alpha + 1)^2 = \alpha^2 + 1$. De plus α est une racine du polynôme $X^4 + X + 1$, donc $\alpha^4 + \alpha + 1 = 0$, d'où $\alpha^4 = \alpha + 1$.

Rappelons aussi que $|(\mathbb{F}_{2^4})^*| = 15$ donc $\alpha^n = \alpha^{n \ mod(15)}$.

$$\begin{aligned}
\alpha^5 &= \alpha^4 \cdot \alpha = (\alpha+1)\cdot\alpha = \alpha^2+\alpha \\
\alpha^6 &= \alpha^5 \cdot \alpha = \alpha^3+\alpha^2 \\
\alpha^7 &= \alpha^6 \cdot \alpha = \alpha^4+\alpha^3 = \alpha^3+\alpha+1 \\
\alpha^8 &= (\alpha^4)^2 = (\alpha+1)^2 = \alpha^2+1 \\
\alpha^9 &= \alpha^8 \cdot \alpha = \alpha^3+\alpha \\
\alpha^{10} &= \alpha^9 \cdot \alpha = \alpha^4+\alpha^2 = \alpha^2+\alpha+1 \\
\alpha^{11} &= \alpha^{10} \cdot \alpha = \alpha^3+\alpha^2+\alpha \\
\alpha^{12} &= \alpha^{11} \cdot \alpha = \alpha^4+\alpha^3+\alpha^2 = \alpha^3+\alpha^2+\alpha+1 \\
\alpha^{13} &= \alpha^4+\alpha^3+\alpha^2+\alpha = \alpha^3+\alpha^2+1 \\
\alpha^{14} &= \alpha^4+\alpha^3+\alpha = \alpha^3+\alpha+\alpha+1 = \alpha^3+1
\end{aligned}$$

Le tableau suivant donne les correspondances entre l'écriture des éléments de $\mathbb{F}_{2^4}$ sous la forme d'une puissance de α, d'une combinaison linéaire d'éléments de $\mathcal{B}$, ainsi que sous leur forme vectorielle :

Ecriture sous forme de puissance de α	Ecriture en combinaison linéaire de $\{\alpha^0, \alpha^1, \alpha^2, \alpha^3\}$	Ecriture vectorielle dans la base $\mathcal{B}$
0	0	[0 0 0 0]
α^0	1	[0 0 0 1]
α^1	α	[0 0 1 0]
α^2	α^2	[0 1 0 0]
α^3	α^3	[1 0 0 0]
α^4	$\alpha+1$	[0 0 1 1]
α^5	$\alpha^2+\alpha$	[0 1 1 0]
α^6	$\alpha^3+\alpha^2$	[1 1 0 0]
α^7	$\alpha^3+\alpha+1$	[1 0 1 1]
α^8	α^2+1	[0 1 0 1]
α^9	$\alpha^3+\alpha$	[1 0 1 0]
α^{10}	$\alpha^2+\alpha+1$	[0 1 1 1]
α^{11}	$\alpha^3+\alpha^2+\alpha$	[1 1 1 0]
α^{12}	$\alpha^3+\alpha^2+\alpha+1$	[1 1 1 1]
α^{13}	$\alpha^3+\alpha^2+1$	[1 1 0 1]
α^{14}	α^3+1	[1 0 0 1]

TABLE 3.1 – Correspondances entre les différentes écritures des éléments de $\mathbb{F}_{2^4}$

Soit $P\ (1, \alpha^6)$ un point de $\mathbb{F}_{2^4} \times \mathbb{F}_{2^4}$.

Montrons que P est un point de la courbe elliptique $E(\mathbb{F}_{2^4})$. Pour cela il suffit de prouver que leurs coordonnées vérifient l'équation $y^2 + xy = x^3 + \alpha^4 x^2 + 1$:

$$\begin{aligned} y_P^2 + x_P y_P &= (\alpha^6)^2 + \alpha^6 \\ &= \alpha^{12} + \alpha^3 + \alpha^2 \\ &= \alpha + 1 \end{aligned} \qquad \begin{aligned} x_P^3 + \alpha^4 x_P^2 + 1 &= 1 + \alpha^4 + 1 \\ &= \alpha^4 \\ &= \alpha + 1 \end{aligned}$$

d'où $y_P^2 + x_P y_P = x_P^3 + \alpha^4 x_P^2 + 1 \Leftrightarrow P \in E(\mathbb{F}_2)$.

Nous allons maintenant déterminer les coordonnées du point $R = 3 \cdot P$:

Dans un premier temps nous calculerons les coordonnées du point $Q = 2 \cdot P$, puis dans un second temps nous obtiendrons $R = 3 \cdot P$ par le calcul $R = P + Q$.

Voici le calcul des coordonnées du point $Q = 2P$:

Commençons par calculer le terme λ défini plus haut (dans le cas "$P = Q$") :

$$\lambda \;=\; \frac{1^2 + \alpha^6}{1} = \alpha^6 + 1 = \alpha^3 + \alpha^2 + 1 = \alpha^{13}$$

On a donc :

$$\begin{cases} x_Q = (\alpha^{13})^2 + \alpha^{13} + \alpha^4 \\ y_Q = (\alpha^{13} + 1)x_Q + \alpha^{13} + \alpha^6 \end{cases} \Leftrightarrow \begin{cases} x_Q = \alpha^{11} + \alpha^3 + \alpha^2 + 1 + \alpha + 1 \\ y_Q = \alpha^6 x_Q + \alpha^3 + \alpha^2 + 1 + \alpha^3 + \alpha^2 \end{cases} \Leftrightarrow \begin{cases} x_Q = 0 \\ y_Q = 1 \end{cases}$$

Vérifions que le point $Q\ (0, 1)$ appartient également à la courbe $E(\mathbb{F}_{2^4})$:

$$y_Q^2 + x_Q y_Q \;= 1 \qquad x_Q^3 + \alpha^4 x_Q^2 + 1 \;= 1$$

Calculons ensuite le point $R = 3 \cdot P = P + Q$:

Le calcul du terme λ (dans le cas "$P \neq Q$") donne :

$$\lambda \;=\; \frac{1 + \alpha^6}{1 + 0} = \alpha^6 + 1 = \alpha^3 + \alpha^2 + 1 = \alpha^{13}$$

$$\begin{cases} x_R = (\alpha^{13})^2 + \alpha^{13} + \alpha^4 + 1 \\ y_R = (\alpha^{13}+1)x_R + \alpha^{13}\cdot 1 + \alpha^6 \end{cases} \Leftrightarrow \begin{cases} x_R = \alpha^{11} + \alpha^3 + \alpha^2 + 1 + \alpha \\ y_R = (\alpha^3+\alpha^2)x_R + \alpha^3 + \alpha^2 + 1 + \alpha^3 + \alpha^2 \end{cases}$$
$$\Leftrightarrow \begin{cases} x_R = \alpha^3 + \alpha^2 + \alpha + \alpha^3 + \alpha^2 + \alpha + 1 \\ y_R = \alpha^6 x_R + 1 \end{cases}$$
$$\Leftrightarrow \begin{cases} x_R = 1 \\ y_R = \alpha^6 + 1 \end{cases}$$
$$\Leftrightarrow \begin{cases} x_R = 1 \\ y_R = \alpha^{13} \end{cases}$$

Le point $R\ (1, \alpha^{13})$ appartient lui aussi à la courbe $E(\mathbb{F}_{2^4})$:

$$\begin{aligned} y_R^2 + x_R y_R &= (\alpha^{13})^2 + \alpha^{13} \\ &= \alpha^{11} + \alpha^3 + \alpha^2 + 1 \\ &= \alpha + 1 \end{aligned} \qquad \begin{aligned} x_R^3 + \alpha^4 x_R^2 + 1 &= 1 + \alpha^4 + 1 \\ &= \alpha^4 \\ &= \alpha + 1 \end{aligned}$$

3.3 Logarithme discret généralisé

Définition 16 *Logarithme discret*

Soient $(G, \circ)$ un groupe cyclique d'ordre n et γ un élément générateur de G.

Tout élément g du goupe G s'écrit alors comme une puissance de γ (si la loi $\circ$ est noté multiplicativement) i.e.

$$\forall g \in G,\ \exists!\ k \in \mathbb{Z}/n\mathbb{Z},\ g = \gamma^k.$$

On peut ainsi construire un isomorphisme log_γ de G dans $\mathbb{Z}/n\mathbb{Z}$. Cet isomorphisme est appelé logarithme discret de base *γ.*

On appelle alors problème du logarithme discret *le problème qui consiste à déterminer k connaissant γ et $g = \gamma^k$.*

Définition 17 *Problème du logarithme discret généralisé*

Soient :

– *$(G, \circ)$ un groupe fini d'ordre n,*
– *γ un élément de G,*
– *$H =< \gamma >= \{\gamma^i = \underbrace{\gamma \circ \ldots \circ \gamma}_{i\ fois}, i \geq 0\}$ le sous groupe de G engendré par γ,*
– *δ un élément de H*

Le problème du logarithme discret généralisé *consiste à déterminer l'unique $n \in \mathbb{N}$ tel que* $\begin{cases} 0 \leq n \leq |H| - 1 \\ \gamma^n = \delta \end{cases}$

Remarque 5

Lorsque la loi de groupe est notée additivement, ce qui est le cas des groupes qui nous concernent, on note alors la succession d'opérations par une multiplication et non une puissance.

Ce problème peut être difficile suivant le groupe dans lequel il est posé. Ainsi le niveau de sécurité du cryptosystème basé sur les courbes elliptique dépend de la courbe elliptique utilisée.

Voici le problème du logarithme discret généralisé écrit avec les notations propres aux groupes des points de courbes elliptiques :

Définition 18 *Problème du logarithme discret généralisé appliqué aux courbes elliptiques*

Soient :

- $(E(\mathbb{K}), +)$ *le groupe des points d'une courbe elliptique,*
- P *un point de* $E(\mathbb{K})$ *d'ordre* n*,*
- Q *un point de* $E(\mathbb{K})$ *tel que* $\begin{cases} Q = k \cdot P \\ k \leq n \end{cases}$

Connaissant la courbe $E(\mathbb{K})$ *et les points* P *et* Q *de* $E(\mathbb{K})$*, déterminer l'entier* k*.*

Chapitre 4

Problèmes liés à l'utilisation des courbes elliptiques en cryptographie

Les travaux de Tanja Lange et David Bernstein [10], ceux de Samuel Grau [9] et de Pierrick Gaudry [12], mais également les rapports de stage de Christophe Arene [8] et Miguel Garcia [11], ont permis la rédaction de ce chapitre.

Comme nous allons le voir par la suite, l'implémentation des opérations sur une courbe elliptique varie suivant le choix de la représentation utilisée pour définir cette courbe. L'efficacité des algorithmes de calcul de l'ordre d'un point dépend de cette implémentation. Ce choix est donc primordial.

Naturellement la sélection de la courbe elliptique est elle aussi décisive pour assurer un niveau de sécurité suffisant. Nous évoquerons donc les recommandations du NIST.

4.1 Généralités sur l'implémentation des opérations

Dans cette partie nous présenterons les algorithmes de calculs sur les points d'une courbe elliptique.

Quel que soit le corps de définition d'une courbe elliptique, les formules explicites des opérations sur les points sont similaires.

Pour plus de clarté nous étudierons donc le cas d'une courbe définie sur $\mathbb{F}_{2^n}$, les notations associées étant plus simples.

Soit $E(\mathbb{F}_{2^n})$ une courbe elliptique représentée en coordonnées affines (ou non-homogènes) et donnée par l'équation :

$$y^2 + xy = x^3 + a_2x^2 + a_6.$$

Lorsque le modèle de Weierstrass est utilisé, l'addition définie sur une courbe elliptique est décomposée en deux cas suivant que l'on additionne deux points distincts ou qu'on double un point. Deux algorithmes sont donc employés pour l'addition.

Voici deux algorithmes effectuant chacun une de ces opérations sur la courbe elliptique $E(\mathbb{F}_{2^n})$, le premier additionnant deux points distincts, le second doublant un point :

Addition de 2 points distincts
Entrées : $P = (x_P, y_P), Q = (x_Q, y_Q) \in E(\mathbb{F}2^n)$.
Sorties : $R = P + Q = (x_R, y_R) \in E(\mathbb{F}2^n)$.
Début
$X \leftarrow x_P + x_Q$;
$\lambda \leftarrow \frac{y_P+y_Q}{X}$;
$x_R \leftarrow \lambda^2 + \lambda + X + a_2$:
$y_R \leftarrow (\lambda+1)x_R + \lambda x_P + y_P$;
Retourner (x_R, y_R) ;
Fin

TABLE 4.1 – Algorithme d'addition de deux points distincts

Double d'un point
Entrées : $P = (x_P, y_P) \in E(\mathbb{F}2^n)$.
Sorties : $R = 2P = (x_R, y_R) \in E(\mathbb{F}2^n)$.
Début
$\lambda \leftarrow x_P + \frac{y_P}{x_P}$;
$x_R \leftarrow \lambda^2 + \lambda + a_2$:
$y_R \leftarrow x_P^2 + \lambda x_R + x_R$;
Retourner (x_R, y_R) ;
Fin

TABLE 4.2 – Algorithme de doublement d'un point

Le calcul de l'opposé d'un point d'une courbe elliptique peut être exécuté par l'algorithme suivant :

Opposé d'un point
Entrées : $P = (x_P, y_P) \in E(\mathbb{F}2^n)$.
Sorties : $R = -P \in E(\mathbb{F}2^n)$.
Début
$x_P \leftarrow x_P$:
$y_P \leftarrow x_P + y_P$;
Retourner (x_P, y_P) ;
Fin

TABLE 4.3 – Algorithme de calcul de l'opposé d'un point

L'algorithme suivant, qui utilise ceux décrits précédemment, permet de traiter l'addition dans un cadre plus général :

Addition de 2 points
Entrées : $P = (x_P, y_P), Q = (x_Q, y_Q) \in E(\mathbb{F}2^n)$.
Sorties : $R = P + Q = (x_R, y_R) \in E(\mathbb{F}2^n)$.
Début
Si $(P = \mathcal{O})$ **alors**
Retourner $Q = (x_Q, y_Q)$;
FinSi
Si $(Q = \mathcal{O})$ **alors**
Retourner $P = (x_P, y_P)$;
FinSi
Si ($P =$*Opposé d'un point*(Q)) **alors**
Retourner $\mathcal{O}$;
FinSi
Si $(P = Q)$ **alors**
Retourner *Double d'un point*(P) ;
Sinon
Retourner *Addition de 2 points distincts*(P, Q) ;
FinSi
Fin

TABLE 4.4 – Algorithme généralisé du calcul d'une addition

Un autre calcul, très important dans le cadre de la cryptographie, est celui qui permet la multiplication d'un point par un entier. En effet, cette opération est indispensable pour appliquer le problème du logarithme discret. Voici un algorithme qui effectue ce calcul :

Multiple d'un point
Entrées : $k = (k_t, \ldots, k_1, k_0)_2 \in \mathbb{N}, P = (x_P, y_P) \in E(\mathbb{F}2^n)$.
Sorties : $R = kP = (x_R, y_R) \in E(\mathbb{F}2^n)$.
Début
$Q \leftarrow \mathcal{O}$;
Pour i de t à 0 **faire**
$Q \leftarrow 2Q$;
Si $k_i = 1$ **alors**
$Q \leftarrow Q + P$;
FinSi
FinPour
Retourner Q ;
Fin

TABLE 4.5 – Algorithme du calcul d'un multiple d'un point

Comme nous pouvons le constater, le calcul de l'addition de deux points ainsi que le doublement d'un point consiste à effectuer un inverse, deux multiplications et une élévation au carré. Cependant, calculer l'inverse d'un élément de $\mathbb{F}_{2^n}$ est obtenu à l'aide d'un algorithme dont la complexité est élevée.

Ce problème peut être contourné en choisissant de représenter cette courbe elliptique à l'aide, par exemple, des coordonnées projectives (ou homogènes). Elle est alors définie par l'équation :

$$Y^2Z + XYZ = X^3 + a_2X^2Z + a_6Z^3.$$

En effet, le résultat $R\ (X_R : Y_R : Z_R)$ de l'addition de deux points de la courbe elliptique $P\ (X_P : Y_P : Z_P)$ et $Q\ (X_Q : Y_Q : Z_Q)$ est donné par :

$$\begin{cases} X_R = BE \\ Y_R = C(AX_P + BY_P)Z_Q + (A+B)E \\ Z_R = B^3 \end{cases} \quad \text{où} \quad \begin{cases} A = Y_PZ_Q + Y_QZ_P \\ B = X_PZ_Q + X_QZ_P \\ C = B^2 \\ D = Z_PZ_Q \\ E = (A^2 + AB + a_2C)D + BC \end{cases}$$

Les coordonnées du point $Q = 2P$, doublement du point P, s'obtient à l'aide des formules suivantes :

$$\begin{cases} X_Q = CE \\ Y_Q = BE + C(E + A^2) \\ Z_Q = CD \end{cases} \quad \text{où} \quad \begin{cases} A = X_P^2 \\ B = A + Y_PZ_P \\ C = X_PZ_P \\ D = C^2 \\ E = B(B+C) + a_2D \end{cases}$$

En coordonnées projectives il n'y a donc pas de calcul d'inverse pour l'addition ni pour le doublement d'un point.
Une addition nécessite alors seize multiplications et deux élévations au carré, un doublement demande quant à lui huit multiplications et trois élévations au carré.
Dans chacun de ces deux cas, le calcul de l'opposé ne nécessite qu'une somme.

Le fait que l'addition de deux points P et Q d'une courbe elliptique nécessite des formules distinctes selon que P soit égal ou non à Q peut rendre le cryptosystème sensible à l'attaque nommée *side-channel attack*. Celle-ci consiste, en effet, à détecter de manière physique une différence entre les deux cas, basée sur le temps de calcul, l'énergie consommée, voire même le son produit lors des calculs.

Depuis peu, l'apparition d'un nouveau modèle de courbes elliptiques, le modèle d'Edwards, unifiant les formules d'addition et de doublement, a permis de réduire le temps de calcul des opérations et de faire face à ce type d'attaque.

4.2 Calcul de l'ordre d'un point et d'une courbe elliptique

4.2.1 Calcul de l'ordre d'un point P

Déterminer les coordonnées d'un point P d'une courbe elliptique $E(\mathbb{K})$ revient à fixer aléatoirement un élément x de $\mathbb{K}$ et vérifier que l'équation de Weierstrass définissant cette courbe, alors ramenée à une équation du second degré, admet une solution $y \in \mathbb{K}$. De par la structure de corps de $\mathbb{K}$, les formules de résolution des racines d'un trinôme sont valables, On peut donc facilement déterminer $y \in \mathbb{K}$.

Connaissant les coordonnées d'un point P et la factorisation en produit de facteurs premiers de l'ordre de $E(\mathbb{K})$, il est possible de déterminer l'ordre de P en temps polynomial.

Voici un algorithme qui nous permet un tel de calcul :

Ordre d'un point
Entrées : $P = (x_P, y_P) \in E(\mathbb{F}2^n), \#E = {p_1}^{e_1} \cdot \ldots \cdot {p_r}^{e_r}$.
Sorties : $k \in \mathbb{N}$
Début
$m \leftarrow \#E$
Pour i de 1 à r **faire**
$m \leftarrow m/{p_i}^{e_i}$;
$Q \leftarrow mP$;
Tant que $Q \neq 0$ **faire**
$Q \leftarrow p_i Q$;
$m \leftarrow m p_i$;
FinTantQue
FinPour
Retourner m ;
Fin

TABLE 4.6 – Algorithme du calcul de l'ordre d'un point d'une courbe elliptique

4.2.2 Calcul de l'ordre d'une courbe $E(\mathbb{K})$

Le théorème de Hasse (énoncé p 9) sur le nombre de points d'une courbe elliptique fournit l'approximation :

$$|E(\mathbb{F}_q)| = q + 1 \pm 2\sqrt{q}$$

Afin de trouver le nombre exact de points, il est suffisant de trouver ce nombre modulo $R > 4\sqrt{q}$.

L'algorithme de Schoof calcule donc

$$q + 1 - |E(\mathbb{F}_q)| \pmod{r_i}$$

pour plusieurs petits nombres premiers r_i, où $\prod r_i = R$. Le résultat final est obtenu par combinaison via le théorème des restes chinois.

Chapitre 5

Application des courbes elliptiques à la cryptographie

5.1 L'échange de clés de Diffie-Hellman

EC-DH (Elliptic Curve Diffie Hellman) est un protocole d'échange de clés secrètes.

En voici une description :

Alice et Bob souhaite disposer d'une clé secrète commune. Il se mettent d'accord sur le choix d'une courbe elliptique $E(\mathbb{K})$ où $\mathbb{K}$ est un corps fini, et sur le choix d'un point P de cette courbe. Ces choix sont connus de tous.

Ils choisissent alors respectivement un entier a et un entier b. Ces entiers constitueront leurs clés privées.

Chacun d'eux calcule alors respectivement $A = aP$ et $B = bP$.

Alice envoie alors à Bob le point A et celui-ci lui envoie le point B.

Alice effectue alors le calcul $aB = abP$ et Bob le calcul $bA = abP$. Ils disposent maintenant d'une clé secrète commune abP.

Si quelqu'un, que nous appelerons Oscar, espionne leurs communications et intercepte les points A et B, le problème du logarithme discret garantit qu'il ne sera pas en mesure de déterminer les entiers a et b. Il ne pourra donc pas reconstituer la clé abP commune à Alice et Bob.

Oscar dispose cependant d'une manière d'espionner ces conversations s'il est en mesure de substituer un nouveau message à celui d'Alice puis à celui de Bob :

La courbe $E(\mathbb{K})$ et le point P étant connus de tous, il peut choisir un entier c et calculer le point $C = cP$.

Oscar intercepte le message d'Alice, récupère le point A et le remplace par C.
De même il intercepte le message de Bob, récupère le point B et le remplace par C.
Il calcule alors les points $Q_A = cA = caP$ et $Q_B = cB = cbP$.
De leurs côtés Alice et Bob ont reçu tous les deux le point $C = cP$ et ont alors calculé respectivement les points $aC = acP = Q_A$ et $bC = bcP = Q_B$.
Lorsque Alice envoie un message à Bob, elle le chiffre alors avec la clé Q_A.
Oscar intercepte ce message, le déchiffre car il est en possession de la clé Q_A, puis le rechiffre à l'aide de la clé Q_B. Il envoie le message chiffré, modifié ou non, à Bob qui le déchiffre grâce à sa clé Q_B.

Oscar doit alors intercepter toutes les conversations entre Alice et Bob pour ne pas que ceux-ci s'aperçoivent de sa présence. En effet ne disposant pas de clé commune, Alice et Bob ne sont plus en mesure de déchiffrer ces messages sans l'intervention d'Oscar.

La faiblesse de ce protocole réside donc dans le fait qu'il ne permet pas d'authentifier les auteurs des messages émis.

5.2 La signature EC-DSA

Nous allons maintenant présenter une utilisation des courbes elliptiques : Le schéma de signature électronique EC-DSA (Elliptic Curve Digital Signature Algorithm) dont le fonctionnement est similaire à la signature DSA.

Le mécanisme DSA (Digital Signature Algortihm) repose sur le problème du logarithme discret sur les corps finis. Comme nous l'avons vu précédemment, il peut donc être appliqué aux courbes elliptiques. L'intérêt de cette pratique provient du fait que, à un niveau de sécurité équivalent, l'utilisation des courbes elliptiques permet des calculs plus rapides et réclame moins de mémoire par rapport à l'utilisation d'un corps fini. En effet, pour un niveau de sécurité équivalent, cet algorithme travaille avec des clés de plus petite taille, par exemple 160 bits au lieu de 1024 pour le DSA classique, tout en conservant les tailles des signatures.

Rappelons l'algorithme DSA appliqué aux courbes elliptiques :
Soient :
- un point P d'une courbe elliptique $E(\mathbb{K})$ d'ordre n premier où $\mathbb{K}$ est un corps fini,
- H une fonction de hachage,
- m le message à signer.

La mise en place du schéma EC-DSA nécessite une paire de clés, l'une publique, l'autre privée. La clé publique est accessible à tous et permet à chacun de vérifier l'intégrité du message et l'authenticité de l'entité qui l'a envoyé.

Préparation des clés :

Alice souhaite envoyer un message m signé par le protocole EC-DSA à Bob. Pour cela elle va choisir une paire de clé (clé publique, clé privée) en procédant comme suit :

- Elle choisit un entier s entre 1 et $n-1$.
- Elle calcule $Q = sP$.
- Sa clé publique sera Q et sa clé privée $s = log_P(Q)$.

On remarque que c'est le problème du logarithme discret de base P qui garantit la difficulté de déterminer la clé privée s connaissant la clé publique Q.

Signature :

Alice dispose maintenant de la paire de clés dont elle a besoin. Pour signer son message elle procède ainsi :

- Elle choisit de manière aléatoire un nombre k entre 1 et $n-1$.
- Elle calcule :
  - $kP = (x, y)$
  - $u = x \ mod \ n$
  - $v = \frac{H(m)+su}{k} \ mod \ n$ où $H(m)$ est une fonction de hachage
- Si u ou v sont nulles, elle recommence, sinon la signature est la paire (u, v).

Vérification :

Bob reçoit le message m signé par le couple (u,v), il doit :

- contrôler que u et v sont bien entre 1 et $n-1$.
- vérifier que $u = x \ mod \ n$ sachant que $(x, y) = (\frac{H(m)}{v} mod \ n)P + (\frac{u}{v} mod \ n)Q$.
- vérifier que Q est différent de $(0, 0)$ et que Q appartient bien à la courbe elliptique $E(\mathbb{K})$.
- vérifier que nQ donne $(0, 0)$.

Justification :

Quiquonque voudrait se faire passer pour Alice devrait être en mesure d'envoyer un couple (u, v) vérifiant :

$$\begin{cases} u = x \ mod \ n \\ (x, y) = (\frac{H(m)}{v} mod \ n)P + (\frac{u}{v} mod \ n)Q. \end{cases}$$

Pour cela il devra alors être capable de déterminer s connaissant Q, et donc résoudre le problème du logarithme discret.

5.3 Normes actuelles et recommandations

Dans le cadre de son programme de modernisation cryptographique, l'Agence de Sécurité Nationale des Etats-Unis (NSA) a promulgué un ensemble d'algorithmes cryptographiques appelé *Suite B.*

Suite B contient les indications suivantes :

– pour la signature : ECDSA, avec les courbes construites sur un corps premier $\mathbb{F}_p$ où p est un entier respectivement de taille 256 bits et 384 bits, approuvées par FIPS 186-2
– pour l'échange de clé : ECDH ou ECMQV, avec les mêmes courbes que précédemment, recommandées par NIST Special Publication 800-56A

Chapitre 6

Conclusion

Les cryptosystèmes basés sur les courbes elliptiques se posent en alternative efficace face à l'incontournable RSA. En effet, ils exploitent un problème mathématique différent, qui est réputé pour sa solidité égale à RSA pour des clés de longueur bien inférieure. Cela les rend parfaitement adaptés aux utilisations embarquées, comme les cartes à puce par exemple, où la mémoire et la puissance des processeurs ne sont pas suffisants pour réaliser en un temps convenable les calculs exigés par RSA.

De nos jours la cryptographie est en perpétuelle évolution afin de pouvoir répondre aux besoins de sécurisation des données qui ne cessent d'augmenter. En effet, les cryptosystèmes se doivent d'être performants face à des attaques de plus en plus nombreuses. C'est pourquoi nous ne pouvons pas prédire combien de temps les cryptosystèmes basés sur les courbes elliptiques seront les plus efficaces au niveau sécurité. Cependant, l'univers des courbes elliptiques étant très vaste, ces dernières font toujours l'objet de recherches en cryptologie ainsi que dans d'autres domaines tels que la mécanique.

Table des figures

Liste des tableaux

Bibliographie

[1] Stéphane BALLET, Cours de cryptographie, M2 MINT, Université de la Méditerranée Aix-Marseille II, 2008.

[2] Marc JOYE, Introduction élémentaire à la théorie des courbes elliptiques, UCL Crypto Group Technical Report Series, 1995.
http : //sciences.ows.ch/mathematiques/CourbesElliptiques.pdf

[3] Reynald LERCIER, Courbes elliptiques et cryptographie, Sécurité des systèmes d'information, 2004.
http : //www.chear.defense.gouv.fr/fr/think_tank/archives/rstd/64/rstd64p59.pdf

[4] Yves DRIENCOURT, Le problème du logarithme discret et les courbes elliptiques, Cours de DEA, Université de la Méditerranée Aix-Marseille II, 2001.
http : //math.univ − bpclermont.fr/ rebolledo/page − fichiers/projetMichael.pdf

[6] Benjamin JEANNE et Thierry PERN sous la direction de Jean-Marc COUVEIGNES, Courbes elliptiques et leurs applications à la cryptographie, GRIM Université de Toulouse II Le Mirail et ESM Saint-Cyr, 1999.

[7] Douglas STINSON, Cryptographie : Théorie et pratique, International Thomson Publishing France, 1995.

[8] Christophe ARENE, Etude d'un nouveau modèle pour les courbes elliptiques, Rapport de stage M2 MDFI, Université de la Méditerranée Aix-Marseille II, 2008.

[9] Samuel GRAU, Courbes elliptiques Implémentation de la signature électronique, Université de Rouen, 2004/2005.
http : //www.scribd.com/doc/5078124/Courbes − Elliptiques − Implementation − de − la − Signature − Electronique

[10] Tanja LANGE et David BERNSTEIN, Faster addition and doubling on elliptic curves, Asiacrypt, 2007.
http : //cr.yp.to/newelliptic/newelliptic − 20070906.pdf

[11] Miguel GARCIA, Développement sur les courbes de Koblitz, Rapport de stage M2 MINT, Université de la Méditerranée Aix-Marseille II, 2008.

[12] Pierrick GAUDRY, Algorithmes de comptage de points d'une courbe définie sur un corps fini, LORIA CNRS Nancy 2006.
http : //www.loria.fr/ gaudry/publis/pano.pdf

[13] Wikipedia, Elliptic Curve Digital Signature Algorithm (ECDSA).
http : //fr.wikipedia.org/wiki/Courbe_elliptique

[14] NSA, NSA Suite B Cryptography.
http : //www.nsa.gov/ia/programs/suiteb_cryptography/index.shtml

[15] Pierre BARTHÉLÉMY, Robert ROLLAND et Pascal VÉRONCryptographie, principes et mises en oeuvre, Lavoisier, 2005.