

Aspects cryptographiques des corps finis

Robert Rolland

`rolland@iml.univ-mrs.fr`

C.N.R.S., Institut de Mathématiques de Luminy

F13288 Marseille cedex 9, France

I-1. Problématique

La **cryptographie à clé publique** repose sur la notion de **fonction à sens unique** (avec ou sans trappe).

- **Fonction à sens unique** : fonction "facile à calculer", et "difficile à inverser en pratique" pour presque toute instance.
- **Fonction à sens unique avec trappe**: fonction à sens unique facile à inverser si on connaît une clé.

I-1.1 Exemples importants

- **la fonction RSA** (problème de la factorisation).
Utilisée pour le chiffrement RSA, la signature RSA.
- **la fonction carrée**(problème de la factorisation)
(problème de la résiduosit  quadratique) (probl me
de l'extraction d'une racine carr e). Utilis e pour
l'identification de Fiat-Shamir.
- **la fonction puissance** (probl me du logarithme
discret et probl mes connexes). Utilis e dans le
chiffrement d'ElGamal, la signature DSA, ECDSA,
l' change de cl s de Diffie-Hellman.

I-1.2 Le problème du logarithme discret

Commençons par le cas où on travaille dans le groupe multiplicatif $G = (\mathbb{Z}/p\mathbb{Z})^*$ où p est un "grand" nombre premier. Ce groupe est **cyclique**. Fixons un générateur α de ce groupe :

$$G = \{1, \alpha, \alpha^2, \dots, \alpha^{p-2}\}.$$

Problème du logarithme discret : soit $x \in G$, trouver l'exposant k tel que $x = \alpha^k$.

Cette fonction est considérée comme étant à sens unique. On ne lui connaît pas de trappe.

I-1.2 Le logarithme discret (suite)

On est amené à généraliser le problème du logarithme discret et à en trouver des variantes pour les raisons suivantes :

- Dans $(\mathbb{Z}/p\mathbb{Z})^*$ on connaît des algorithmes sous-exponentiels. Solution : trouver des groupes plus résistants.
- Pas de trappe connue. Solution : introduire des problèmes qui constituent des variantes du logarithme discret.
- Besoin des preuves de sécurité : élargir le nombre de problèmes réputés difficiles.

I-1.2.1 Autres groupes utilisés

Idées : utiliser

- Le groupe multiplicatif d'un corps fini : pas mieux, existence d'algorithmes sous-exponentiels.
- Un sous groupe d'ordre premier de $(\mathbb{Z}/p\mathbb{Z})^*$: c'est effectivement utilisé et permet de manipuler des exposants plus petits.
- Le groupe des points d'une courbe elliptique sur un corps fini : on ne connaît pas d'algorithme sous-exponentiel (sauf pour des cas particuliers).

I-1.2.2 Utilisations et variantes

Voici quelques techniques cryptographiques de base utilisant le problème du logarithme discret (ou ses variantes)

- L'échange de clés de Diffie-Hellman
- Le chiffrement d'ElGamal
- La signature DSA

Ces techniques mettent en évidence le problème de **Diffie-Hellman**.

I-1.2.3 Le problème de Diffie-Hellman

Soit G un groupe multiplicatif fini cyclique ayant n éléments, dont on note α un générateur.

- **Problème calculatoire de Diffie-Hellman (CDH) :**
Étant donnés deux éléments quelconques x et y de G (qui s'écrivent donc $x = \alpha^s$ et $y = \alpha^t$ avec $0 \leq s, t \leq n - 1$) calculer $z = \alpha^{st}$.
- **Problème décisionnel de Diffie-Hellman (DDH) :**
Étant donnés trois éléments quelconques x, y et z de G ($x = \alpha^s$ et $y = \alpha^t$) a-t-on $z = \alpha^{st}$?

I-1.2.4 Relations entre ces problèmes

Il est clair que :

DDH est réductible à CDH, lequel est réductible à DLP.

Il reste à savoir si DLP est strictement plus dur que CDH, et si CDH est strictement plus dur que DDH. On ne connaît aucun exemple où CDH est facile sans que DLP le soit. De plus Si $\#G$ n'est pas divisible par le carré d'un grand nombre premier, on peut montrer que CDH ne peut pas être plus facile que DLP. En revanche on a des exemples de groupes où DDH est facile et où on ne connaît aucun algorithme polynômial pour CDH.

I-2. Les corps finis

Les **corps finis** sont en général des bons alphabets pour écrire des données en raison de leur structure riche. On dispose ainsi de deux opérations : une addition et une multiplication. Les corps finis $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ où p est un nombre premier jouent un rôle particulier, on les appelle les **corps premiers**.

I-2.1 Résultats de base

- **Caractéristique.** Tout corps fini a pour caractéristique un nombre premier p .
- **Sous corps premier.** Tout corps fini F de caractéristique p admet \mathbb{F}_p comme sous-corps. En particulier F est un espace vectoriel sur \mathbb{F}_p . Le corps \mathbb{F}_p est appelé sous-corps premier de F .

I-2.1 Résultats de base (suite)

- **Nombre d'éléments.** Le nombre d'élément q d'un corps fini est une puissance de la caractéristique : $q = p^s$. L'exposant s est la dimension du corps F sur son sous-corps premier.
- **Nombre d'éléments (réciproque).** Pour tout entier $q = p^s$, il existe un corps fini et un seul (à un isomorphisme de corps près) ayant q éléments.

I-2.1 Résultats de base (suite)

- **Réalisation.** Soit $P(X)$ un polynôme de degré s à coefficients dans \mathbb{F}_p , irréductible sur \mathbb{F}_p . Le quotient $\mathbb{F}_p[X]/(P(X))$ est le corps à p^s éléments.
- **Réalisation (réciproque).** Pour tout nombre premier p , et pour tout degré s , il existe un polynôme $P(X) \in \mathbb{F}_p[X]$ irréductible sur \mathbb{F}_p de degré s . Donc si $q = p^s$, $\mathbb{F}_q = \mathbb{F}_p[X]/(P(X))$.

Remarque : En fait pour tout $q = p^s$ et tout degré n , il existe un polynôme $P(X) \in \mathbb{F}_q[X]$ irréductible sur \mathbb{F}_q de degré n .

I-2.1 Résultats de base (suite)

Nombre de polynômes irréductibles normalisés de degré n sur \mathbb{F}_q :

$$I_q(n) = \frac{1}{n} \sum_{d|n} q^d \mu\left(\frac{n}{d}\right).$$

Fonction de Möbius : soit $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$,

$$\mu(n) = \begin{cases} 0 & \text{si } n \text{ divisible par un carré} \\ (-1)^k & \text{sinon} \end{cases}$$

I-2.2 Exemples

1) Corps à 8 éléments : polynôme irréductible choisi :
 $P(X) = X^3 + X + 1$. Tout élément de \mathbb{F}_8 a une représentation unique sous la forme d'un polynôme de degré ≤ 2 . Nous noterons (a_0, a_1, a_2) le polynôme $a(X) = a_0 + a_1X + a_2X^2$.

Addition (addition des polynômes) :

$$(1, 0, 1) + (0, 1, 1) = (1, 1, 0)$$

Multiplication (multiplication des polynômes modulo

$$P(X)): (1, 1, 1) * (0, 1, 1) = (0, 0, 1).$$

$$I_2(3) = 2; (X^3 + X + 1; X^3 + X^2 + 1)$$

I-2.2 Exemples (suite)

2) Corps à 9 éléments : polynôme irréductible choisi :
 $P(X) = X^2 + X + 2$. Tout élément de \mathbb{F}_9 a une représentation unique sous la forme d'un polynôme de degré ≤ 1 . Nous noterons (a_0, a_1) le polynôme $a(X) = a_0 + a_1X$.

Addition (addition des polynômes) :

$$(2, 1) + (1, 1) = (0, 2)$$

Multiplication (multiplication des polynômes modulo

$$P(X)) : (1, 1) * (2, 1) = (0, 2).$$

$$I_3(2) = 3; (X^2 + X + 2; X^2 + 2X + 2; X^2 + 1)$$

I-2.2 Exemples (suite)

2) Corps à 256 éléments :

polynôme irréductible (AES) :

$$P(X) = X^8 + X^4 + X^3 + X + 1.$$

autre polynôme irréductible :

$$P(X) = X^8 + X^7 + X^6 + X + 1.$$

$$I_2(8) = 30;$$

Le polynôme utilisé par AES est celui qui a les plus petits exposants. Il n'est pas primitif (ses racines sont d'ordre 51).

I-2.3 Ordres

Pour tout élément β non nul d'un corps fini \mathbb{F}_q

$$\beta^{q-1} = 1.$$

On peut dire aussi que les éléments d'un corps fini \mathbb{F}_q sont toutes les solutions de l'équation $X^q - X = 0$ dans la clôture algébrique de \mathbb{F}_p .

L'ordre d'un élément $\beta \neq 0$ est le plus petit entier $e \geq 1$ tel que $\beta^e = 1$. L'entier e est l'ordre du sous-groupe multiplicatif engendré par β , donc e divise $q - 1$.

I-2.3 Ordres (suite)

Réciproquement, tout diviseur e de $p - 1$ est l'ordre d'exactly $\phi(e)$ éléments. En particulier, il existe $\phi(p - 1)$ éléments d'ordre $p - 1$. Ces éléments sont des générateurs du groupe multiplicatif \mathbb{F}_q^* , on les appelle **éléments primitifs**. Le groupe multiplicatif \mathbb{F}_q^* est donc cyclique.

Si β est d'ordre e , alors β^i ($1 \leq i \leq e$) est d'ordre $\frac{\text{ppcm}(e,i)}{i}$. En particulier les éléments d'ordre e sont les β^i tels que $\text{pgcd}(e, i) = 1$.

I-2.4 Polynôme minimal

Soit $q = p^s$. Soit $\beta \neq 0$ un élément de \mathbb{F}_q^* . Le **polynôme minimal** de β est le polynôme normalisé $M_\beta(X)$ de plus petit degré à coefficients dans \mathbb{F}_p tel que $M_\beta(\beta) = 0$.

I-2.4.1 Résultats techniques

On travaille dans le corps fini \mathbb{F}_q où $q = p^s$.

$$(x + y)^p = x^p + y^p;$$

$$(x + y)^{p^t} = x^{p^t} + y^{p^t};$$

Si $M(X) \in \mathbb{F}_p[X]$ alors

$$M(X)^{p^t} = M(X^{p^t}).$$

En particulier, si β est racine de $M(X)$ alors β^{p^t} aussi.

I-2.4.2 Forme d'un polynôme minimal

- 1) Le polynôme minimal d'un élément est irréductible et divise $x^q - x$.
- 2) Le polynôme minimal d'un élément est générateur de l'idéal des polynômes qui ont cet élément pour racine.
- 3) Le polynôme minimal d'un élément est de degré $\leq s$. Si l'élément est primitif il est de degré s (réciproque fausse).

Le polynôme minimal d'un élément primitif est **un polynôme primitif**.

1-2.4.2 Forme d'un polynôme minimal (suite)

Si $M_\beta(X)$ est le polynôme minimal de β , il se décompose entièrement sur \mathbb{F}_q , ses racines sont simples et de la forme β^{p^t} .

$$Z = \{\beta, \beta^p, \beta^{p^2}, \dots, \beta^{p^{r-1}}\}$$

où r est le plus petit entier ≥ 1 tel que $\beta^{p^r} = \beta$. L'entier r est le plus petit entier ≥ 1 tel que l'ordre de β divise $p^r - 1$. Toutes les racines de $M_\beta(X)$ ont le même ordre. Si $M_\beta(X)$ est primitif toutes ses racines sont primitives.

1-2.4.2 Forme d'un polynôme minimal (suite)

Le degré d'un polynôme minimal est un diviseur de s .

L'ensemble des polynômes minimaux des éléments de \mathbb{F}_q est constitué de tous les facteurs irréductibles sur \mathbb{F}_p de $X^q - X$.

$$X^q - X = \prod_{M \text{ minimal}} M(X).$$

I-2.5 Représentations d'un élément

Soit $q = p^s$ et $P(X) \in \mathbb{F}_p[X]$ un polynôme primitif de degré s . Ainsi $\mathbb{F}_q = \mathbb{F}_p[X]/(P(X))$. Les éléments de \mathbb{F}_q ont donc une représentation comme des polynômes de degré $< s$. Par exemple $(a_0, a_1, \dots, a_{s-1})$ sera l'élément de \mathbb{F}_q représenté par le polynôme $a_0 + a_1X + \dots + a_{s-1}X^{s-1}$. Soit α la classe du polynôme X . L'élément α (racine de $P(X)$) est un élément primitif. Donc $\mathbb{F}_q^* = \{1, \alpha, \alpha^2, \dots, \alpha^{q-2}\}$. Ceci nous donne une deuxième représentation des éléments de \mathbb{F}_q .

1-2.5 Représentations d'un élément (suite)

La représentation sous forme polynômiale est commode pour l'addition. La représentation sous forme exponentielle est commode pour la multiplication. Hélas le passage d'une représentation à l'autre n'est pas simple, voire inextricable pour de gros corps (problème du log discret). Donc en dehors du cas où le corps est suffisamment petit pour qu'on puisse stocker les tables d'exponentielles et de logarithmes, on ne pourra pas faire usage exclusif de cette double représentation pour accélérer les calculs.

I-2.6 Sous-corps

Soit \mathbb{F}_q un corps fini ($q = p^n$ avec p premier). Tout corps fini qui est une extension de \mathbb{F}_q est un corps de la forme \mathbb{F}_{q^m} . Réciproquement, tout corps fini dont le nombre d'éléments est une puissance de q est une extension de \mathbb{F}_q . Remarquons que $q^m = p^{mn}$.

Exprimé autrement on peut dire que les sous-corps de \mathbb{F}_{p^k} sont les \mathbb{F}_{p^s} où s divise k .

Les sous-corps de \mathbb{F}_{16} sont $\mathbb{F}_2, \mathbb{F}_4, \mathbb{F}_{16}$.

I-2.6.1 Extension intermédiaire

Soit $q = p^s$. Considérons les corps $E = \mathbb{F}_q$ et $F = \mathbb{F}_{q^m}$.
On peut définir F directement comme extension de \mathbb{F}_p
grâce à un polynôme $P(X) \in \mathbb{F}_p[X]$ de degré sm
irréductible sur \mathbb{F}_p

$$F = \mathbb{F}_p[X]/(P(X)),$$

où à travers E grâce à un polynôme $Q(X) \in E[X]$ de
degré m irréductible sur E

$$F = E[X]/(Q(X)).$$

I-2.6.2 Groupe de Galois

Si \mathbb{F}_{q^m} est une extension de \mathbb{F}_q , le groupe G des \mathbb{F}_q -automorphismes de \mathbb{F}_{q^m} est cyclique, engendré par l'automorphisme de Frobenius

$$\sigma_q(x) = x^q$$

et a exactement m éléments. Donc cette extension est une extension de Galois de groupe de Galois

$$G = \{I, \sigma_q, \sigma_q^2, \dots, \sigma_q^{m-1}\}.$$

I-2.7 Bases normales

Il existe une base normale de l'espace \mathbb{F}_{q^m} sur \mathbb{F}_q ,

$$\alpha, \alpha^q, \alpha^{q^2}, \dots, \alpha^{q^{m-1}},$$

c'est à dire un vecteur cyclique (vecteur α dont les itérés successifs par le Frobenius forment une base)

$$\alpha, \sigma_q(\alpha), \sigma_q^2(\alpha), \dots, \sigma_q^{m-1}(\alpha).$$

Grâce aux bases normales on a une nouvelle représentation des éléments d'un corps fini.

Remarque : Il existe un vecteur cyclique primitif.

I-2.7.1 Caractérisation

Nous étudions l'extension \mathbb{F}_{q^m} de \mathbb{F}_q . Écrivons $m = m_1 p^e$ de telle sorte que $m_1 \wedge p = 1$. Alors en posant $t = p^e$ on obtient

$$X^m - 1 = (X^{m_1} - 1)^t = \left(\prod_{i=1}^r \phi_i(X) \right)^t$$

où les $\phi_i(X)$ sont des polynômes normalisés à coefficients dans \mathbb{F}_q , deux à deux distincts, irréductibles sur \mathbb{F}_q . Posons

$$\Phi_i(X) = \frac{X^m - 1}{\phi_i(X)}.$$

I-2.7.1 Caractérisation (suite)

Le résultat principal pour caractériser les bases normales est le théorème suivant :

Théorème 1 *Un élément $\alpha \in \mathbb{F}_{q^m}$ est normal si et seulement si pour tout $1 \leq i \leq r$:*

$$\Phi_i(\sigma_q)(\alpha) \neq 0.$$

Cette condition se simplifie dans certains cas particuliers.

- $m_1 = 1$. Dans ce cas $m = p^e$.
- $e = 0$ et m_1 premier. Dans ce cas $m = m_1$.

Dans ces cas un polynôme irréductible

$X^m + a_1 X^{m-1} + \dots + 1$ est normal si et seulement si $a_1 \neq 0$.

I-2.7.2 Construction

Il y a diverses méthodes pour construire des bases normales générales. En voici une basée sur le théorème suivant.

Théorème 2 *Soit $P(X)$ un polynôme irréductible de degré m sur \mathbb{F}_q . Soit α une racine de $P(X)$ dans \mathbb{F}_{q^m} . posons*

$$G(X) = \frac{P(X)}{(X - \alpha)P'(\alpha)}.$$

Alors il existe au moins $q - m(m - 1)$ éléments u de \mathbb{F}_q tels que $g(u)$ soit normal dans l'extension \mathbb{F}_{q^m} de \mathbb{F}_q .

I-2.8.1 Les opérations : l'addition

Soit

$$\{\alpha_0, \alpha_1, \dots, \alpha_{m-1}\}$$

où $\alpha_i = \alpha^{q^i}$, une base normale de l'extension $\mathbb{F}_{q^m}/\mathbb{F}_q$.

L'élément $a = \sum_{i=0}^{m-1} a_i \alpha_i$, de \mathbb{F}_{q^m} , a pour **matrice ligne** dans cette base $A(a) = (a_0, a_1, \dots, a_{m-1})$.

- **La somme** $c = a + b$ de deux éléments a et b de matrices respectives $A(a)$ et $A(b)$ se fait en additionnant les composantes correspondantes :
 $c_i = a_i + b_i$ ou encore $A(c) = A(a) + A(b)$.

I-2.8.2 L'exponentiation

- **Exponentiation par q .** Les coordonnées de a^q sont obtenue par une rotation vers la droite

$$A(a^q) = (a_{n-1}, a_0, a_1, \dots, a_{n-2}).$$

Ceci est très rapide et accélère les algorithmes du type "exponentiation by q and multiply", surtout dans le cas $q = 2$ (algorithme "square and multiply").

I-2.8.3 La multiplication

- Le produit $c = ab$ de deux éléments a et b de matrices respectives $A(a)$ et $A(b)$ utilise les matrices

$$T_k = \left(t_{i,j}^{(k)} \right)_{\substack{i=0 \dots m-1 \\ j=0 \dots m-1}}$$

où $t_{i,j}^{(k)} \in \mathbb{F}_q$ est la composante sur α_k du produit $\alpha_i \alpha_j$:

$$\alpha_i \alpha_j = \sum_{k=0}^{m-1} t_{i,j}^{(k)} \alpha_k.$$

Si $A(c) = (c_0, \dots, c_{m-1})$, $c_k = A(a)T_k A(b)^t$.

I-2.8.3 La multiplication (suite)

En fait il suffit d'implémenter la multiplication par la matrice T_0 en vertu de l'égalité

$$t_{i,j}^{(k)} = t_{i-k,j-k}^{(0)}.$$

$$\text{Donc } c_k = A(a^{q^{-k}})T_0A(b^{q^{-k}})t.$$

($A(a^{q^{-k}})$ et $A(b^{q^{-k}})$ sont obtenus par des rotations vers la gauche.) Le nombre de 1 de la matrice T_0 (Noté C_N et appelé **complexité** de la base) est donc très important puisque

$$c_k = \sum_{\substack{i=0 \dots m-1 \\ j=0 \dots m-1}} a_{i+k} b_{j+k} t_{i,j}^{(0)}$$

I-2.9 Bases normales optimales

Pour toute base normale de $\mathbb{F}_q^m / \mathbb{F}_q$, $C_N \geq 2m - 1$.

Lorsque $C_N = 2m - 1$, on dit que la base est **optimale**.

La question est de savoir s'il y a toujours une base optimale. La réponse est non. Voici les deux seules classes de bases optimales (à une équivalence près, c'est à dire à une multiplication par un élément de \mathbb{F}_q près).

Les bases de ces deux classes sont appelées respectivement **bases de Type I** et **bases de Type II**.

1-2.9 Bases normales optimales (suite)

- **Bases de Type I.** C'est le cas où $m + 1$ est premier, et où q est un élément primitif de $\mathbb{Z}/(m + 1)\mathbb{Z}$. Alors les m racine $(m + 1)^{eme}$ de l'unité autres que 1 forment une base normale optimale de $\mathbb{F}_q^m / \mathbb{F}_q$.
- **Bases de Type II.** C'est le cas où q est une puissance de 2 et $2m + 1$ est premier et où
 - soit 2 est un élément primitif de $\mathbb{Z}/(2m + 1)\mathbb{Z}$
 - soit $2n + 1 \equiv 3 \pmod{4}$ et 2 engendre le groupe des résidues quadratiques dans $\mathbb{Z}/(2m + 1)\mathbb{Z}$.

Alors $\alpha = \gamma + \gamma^{-1}$, où γ est une racine primitive $(2m + 1)^{eme}$ de l'unité, engendre une base normale optimale de $\mathbb{F}_q^m / \mathbb{F}_q$.