*Agrégation externe de mathématiques, session 2019*
*Épreuve de modélisation, option C : Algèbre et Calcul Formel*

# (*C02-public*)

**Résumé :** On étudie une extension de protocoles de chiffrement et d'échange de clés en utilisant des polynômes.

**Mots clefs :** polynômes, corps finis.

► *Il est rappelé que le jury n'exige pas une compréhension exhaustive du texte. La présentation, bien que totalement libre, doit être organisée et le jury apprécie qu'un plan soit annoncé en préliminaire. L'exposé doit être construit en évitant la paraphrase et mettant en lumière les connaissances, à partir des éléments du texte. Il doit contenir des illustrations informatiques réalisées sur ordinateur, ou, à défaut, des propositions de telles illustrations. Des pistes de réflexion, indicatives et largement indépendantes les unes des autres, vous sont proposées en fin de texte.*

## 1. Introduction

Le présent texte s'intéresse au développement de méthodes efficaces permettant, de manière sécurisée, à deux protagonistes de s'accorder, publiquement et sans se connaître préalablement, sur un secret commun, tout en faisant qu'un tiers ne puisse deviner ce secret qu'au prix d'une quantité de calculs irréaliste.

De nombreux protocoles cryptographiques reposent sur l'existence de fonctions dites difficiles à inverser, c'est-à-dire des fonctions pour lesquelles les images des éléments sont effectivement calculables et ceci en temps raisonnable mais dont les images réciproques ne le sont pas. Le protocole lui-même utilise l'évaluation de la fonction, tandis que sa sécurité est fondée sur la difficulté à inverser la fonction.

Ici, nous allons utiliser une fonction difficile à inverser particulière, ayant en plus des propriétés algébriques agréables. Soit $G$ un groupe fini, et $g \in G$. Considérons alors l'application $\exp_g : x \mapsto g^x$, où $x$ est un entier. Dans certains groupes $G$, cette fonction est présumée difficile à inverser, et donc utilisable en cryptographie.

Voici une brève description d'un protocole de partage de clé entre deux correspondants $\mathscr{A}$ et $\mathscr{B}$ basé sur cette fonction à sens unique.

— $\mathscr{A}$ par exemple choisit un groupe $G$ et $g \in G$ et les communique à $\mathscr{B}$,
— $\mathscr{A}$ choisit sa contribution au secret : $a$, calcule $s_{\mathscr{A}} = g^a$ et l'envoie à $\mathscr{B}$,
— $\mathscr{B}$ choisit sa contribution au secret : $b$, calcule $s_{\mathscr{B}} = g^b$ et l'envoie à $\mathscr{A}$,
— $\mathscr{A}$ et $\mathscr{B}$ calculent respectivement $s_{\mathscr{B}}^a$ et $s_{\mathscr{A}}^b$ qui sont une même quantité qui devient leur secret commun.

La famille de groupes $G$ la plus classique est la famille des groupes $(\mathbb{Z}/p\mathbb{Z})^*$, pour $p$ un nombre premier.

Le choix d'un groupe $G$ est un compromis entre la taille des éléments de $G$ (car il faut, dans le protocole, transmettre des éléments de $G$) et la difficulté présumée à inverser la fonction. Par taille d'un élément d'un ensemble $E$, on sous-entend implicitement le choix d'une représentation des éléments de $E$, c'est-à-dire la donnée d'un entier $t$ (la taille) et d'une injection de $E$ dans $\{0,1\}^t$. On souhaite également que cette injection et son inverse à gauche soient "calculables efficacement". Noter que $t \geqslant \lceil \log \operatorname{card} E / \log 2 \rceil$.

Le but du présent texte est de construire et étudier une famille alternative de groupes $H$, liée aux groupes multiplicatifs des corps à $p^2$ éléments.

La partie 2 est une partie préparatoire, tandis que la partie 3 construit le cadre algébrique du protocole. La partie 4 est de nature plus arithmétique et étudie les aspects calculatoires de la mise en œuvre du protocole.

## 2. Préambule algébrique

Dans toute la suite, $p$ désignera un nombre premier impair et, pour toute puissance $q$ de $p$, $\mathbb{F}_q$ un corps à $q$ éléments. Nous utiliserons dans la suite deux suites de polynômes $P_n$ et $S_n$ apparaissant dans le Lemme suivant :

**Lemme 1.** *Pour tout entier naturel, il existe un unique polynôme $P_n$ (resp $S_n$) de $\mathbb{F}_p[X]$ tel que les identités suivantes soient vérifiées dans $\mathbb{F}_p(X)$ :*

$$P_n\left(\frac{1}{2}\left(X+\frac{1}{X}\right)\right) = \frac{1}{2}\left(X^n + \frac{1}{X^n}\right), \quad \textit{(resp. } S_n\left(\frac{1}{2}\left(X+\frac{1}{X}\right)\right) = \frac{X^n - 1/X^n}{X - 1/X}\textit{)}.$$

*Les suites $(P_n)_{n\geqslant 0}, (S_n)_{n\geqslant 0}$ vérifient les relations de récurrence :*
*(a)* $S_0(X) = 0$, $S_1(X) = 1$, $P_0(X) = 1$ *et* $P_1(X) = X$,
*(b)* $S_{n+1}(X) - 2XS_n(X) + S_{n-1}(X) = P_{n+1}(X) - 2XP_n(X) + P_{n-1}(X) = 0$.

*Éléments pour la preuve de l'unicité.* Supposons que $R$ et $Q$ vérifient $R((X+1/X)/2) = Q((X+1/X)/2)$, et soit $\ell$ un entier assez grand. Alors pour tout $\alpha \in \mathbb{F}_{p^\ell}$, il existe $y \in \mathbb{F}_{p^{2\ell}}$ tel que $2\alpha = y + 1/y$, et donc $\alpha$ est racine de $R - Q$. □

On peut alors déduire de la définition et de l'unicité prouvée dans le Lemme 1 :

**Théorème 2.** *Les suites définies précédemment vérifient les propriétés suivantes, pour tout $m, n \geqslant 0$ :*

*(1)* $S_{mn}(X) = S_m(P_n(X))S_n(X)$,

*(2)* $P_{mn}(X) = P_m(P_n(X))$,

*(3)* $P_{m+n}(X) = 2P_m(X)P_n(X) - P_{m-n}(X)$, *si* $m \geq n$.

## 3. Protocole de partage de clé

Étudions la sécurité du protocole de l'introduction dans le cas où $G = \mathbb{F}_{p^2}^*$. La taille d'un élément de $G$, de l'ordre de $2\log p$, étant à peu près le double de celle d'un élément de $\mathbb{F}_p^*$, cette étude n'a de sens que si la fonction correspondante est significativement plus difficile à inverser.

On définit le morphisme

$$\begin{aligned} \varphi : \mathbb{F}_{p^2}^* &\to \mathbb{F}_p^* \\ x &\mapsto x^{p+1}. \end{aligned}$$

Remarquons que si l'on sait inverser l'exponentiation dans le groupe $\mathrm{Im}(\varphi)$ et dans le groupe $\mathrm{Ker}(\varphi)$, on sait l'inverser dans $\mathbb{F}_{p^2}^*$ – en effet, si $\varphi(x) = \varphi(g)^t$, on a $x/g^t \in \mathrm{Ker}(\varphi)$.

Cela nous conduit à étudier l'inversion de l'exponentiation dans le plus petit groupe $\mathrm{Ker}(\varphi)$, et en particulier à chercher une représentation de ses éléments de taille $\approx \log p$.

**Proposition 3.** *Considérons l'application $\psi$ de $\mathrm{Ker}(\varphi)$ dans $\mathbb{F}_{p^2}$ définie par $x \mapsto (x+1/x)/2$.*
*Alors $\psi$ est à valeurs dans $\mathbb{F}_p$, et $\psi(x) = \psi(y)$ si et seulement si $x = y$ ou $xy = 1$.*

*Démonstration.* On vérifie que $\psi(x)^p = \psi(x)$ pour $x \in \mathrm{Ker}(\varphi)$. □

Nous introduisons la relation d'équivalence $\mathscr{R}$ sur $\mathrm{Ker}(\varphi)$ définie par $x\mathscr{R}y$ si et seulement si $\psi(x) = \psi(y)$.

En particulier, il existe une injection de $\mathrm{Ker}(\varphi)/\mathscr{R}$ dans $\mathbb{F}_p$. Ceci implique qu'il existe une représentation des éléments de $H := \mathrm{Ker}(\varphi)/\mathscr{R}$ de taille $\approx \log p$.

Notons que la multiplication de $\mathbb{F}_{p^2}^*$ ne « passe pas au quotient », et que $H$ n'a donc pas de structure naturelle de groupe. Néanmoins, le protocole ne suppose que d'être capable de calculer $g^x$ pour $g \in \mathrm{Ker}(\varphi)$ et $x$ entier, et cette quantité est bien définie, comme le montre la proposition suivante :

**Proposition 4.** *On a, pour tout $g \in \mathrm{Ker}(\varphi)$ et tout $t$ entier naturel,*

$$\psi(g^t) = P_t(\psi(g)).$$

Le protocole s'écrit alors de la manière suivante :

**Définition-Proposition 5.** *Les polynômes $P_n$ étant définis comme précédemment, les étapes suivantes définissent un nouveau protocole de partage de clé :*

*(1) $\mathscr{A}$ par exemple choisit deux entiers $g$ et $p$ avec $g < p$ et $p$ premier impair et les communique à $\mathscr{B}$,*

*(2) $\mathscr{A}$ choisit sa contribution au secret : $a < p$, calcule $s_{\mathscr{A}} = P_a(g) \bmod p$ et l'envoie à $\mathscr{B}$,*

*(3) $\mathscr{B}$ choisit sa contribution au secret : $b < p$, calcule $s_{\mathscr{B}} = P_b(g) \bmod p$ et l'envoie à $\mathscr{A}$,*

*(4) $\mathscr{B}$ et $\mathscr{A}$ calculent respectivement $P_b(s_{\mathscr{A}}) \bmod p$ et $P_a(s_{\mathscr{B}}) \bmod p$ qui sont égales et deviennent leur secret commun.*

Stricto sensu, ce protocole ne correspond au cadre algébrique décrit plus haut que si $g = \psi(u), u \in \mathrm{Ker}(\varphi)$ . Néanmoins, on vérifie, grâce au Théorème 2, que le protocole d'échange de clés est correct dans tous les cas, et la proposition suivante complète l'étude algébrique de ce protocole :

**Proposition 6.** *Soit $g \in \mathbb{F}_p$ ; on a toujours $g = \psi(u), u \in \mathrm{Ker}(\varphi)$ ou $g = \psi(u), u \in \mathbb{F}_p^*$.*

## 4. Aspects calculatoires du protocole

Intéressons nous au coût, en terme de calcul, de ce protocole. Une première possibilité consisterait à calculer les polynômes (soit par la récurrence du début, soit par des méthodes plus efficaces), puis de les évaluer. Cette idée n'est néanmoins pas praticable, car le degré de $P$ est trop grand pour espérer le stocker en machine.

### 4.1. *Une version matricielle*

Il existe des algorithmes efficaces pour calculer $\exp_g$ dans un groupe quelconque. Nous allons tenter de nous en inspirer. Pour cela, nous donnons une autre définition de la suite $P_n(x)$ pour $x \in \mathbb{F}_p$ :

$$\begin{pmatrix} P_n(x) \\ P_{n+1}(x) \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ -1 & 2x \end{pmatrix} \begin{pmatrix} P_{n-1}(x) \\ P_n(x) \end{pmatrix} \quad n \geqslant 1, \quad \text{et} \quad P_0(x) = 1, \quad P_1(x) = x.$$

En général, le coût d'une multiplication matricielle est de huit multiplications entières et quatre réductions modulaires. On obtient ainsi une complexité en $O(\log(p))$ opérations dans $\mathbb{F}_p$.

### 4.2. *Une version polynomiale*

Une autre méthode consiste en l'utilisation du polynôme caractéristique de la matrice définissant la suite $(P_n)$ : $\chi(\lambda) = \lambda^2 - 2x\lambda + 1$. Nous pouvons chercher la puissance $n$-ième de la matrice en calculant $\lambda^n$ modulo le polynôme caractéristique $\chi(\lambda)$.

Ce calcul de $\lambda^n$ peut aussi se faire par une méthode d'exponentiation rapide, qui nécessite alors $O(\log p)$ opérations dans $\mathbb{F}_p[\lambda]/(\chi(\lambda))$. Une étape de « multiplication » dans cette algèbre, consiste alors en la multiplication de deux polynômes linéaires (qui coûte 4 multiplications scalaires a priori, mais peut s'optimiser en trois multiplications) et une réduction, qui coûte deux multiplications scalaires.

Noter que dans les analyses ci-dessus, les additions et soustractions modulaires, moins coûteuses que les multiplications quand $p$ est grand, ont été négligées.

### 4.3. *Suites mixtes*

Nous dirons qu'une suite croissante d'entiers $(x_k)_{0\leqslant k\leqslant N}$ est une suite mixte pour l'entier $n$ si $x_0 = 0, x_1 = 1, x_N = n$ et, pour tout $2 \leqslant j \leqslant N$, il existe trois entiers $0 \leqslant a, b, c < j$ tels que $x_j = x_b + x_c$ et $x_a = x_c - x_b$.

Ainsi la suite $0, 1, 2$ est-elle une suite mixte pour l'entier 2. L'intérêt de ces suites réside dans le fait, conséquence du Théorème 2 (3), que d'une suite mixte $(x_k)_{0\leqslant k\leqslant N}$ pour l'entier $n$ on peut déduire un algorithme de calcul de $P_n(\psi(g))$ utilisant $N-1$ multiplications (où l'on néglige les multiplications par 2).

La méthode matricielle décrite supra peut se réinterpréter en terme de suite mixte. On peut également construire des suites mixtes de la manière suivante, étant donné l'entier $n$ : on choisit $r < n$, premier avec $n$, et on part de l'ensemble $\mathscr{S} := \{n, r, n-r, |n-2r|\}$. À chaque étape, on ajoute à $\mathscr{S}$ la différence entre les deux plus petits éléments de $\mathscr{S}$, et on s'arrête quand on a ajouté 0 à $\mathscr{S}$.

**Proposition 7.** *La suite obtenue en triant les éléments de $\mathscr{S}$ par ordre croissant est une suite mixte pour l'entier $n$.*

*Démonstration.* Il suffit de prouver que 1 est bien dans $\mathscr{S}$ à la fin de la construction. □

Tous les choix de $r$ ne sont pas intéressants ; ainsi $r = n-1$ est un mauvais choix, comme dans toutes les situations où les deux plus petits éléments de $\mathscr{S}$ se trouvent être d'ordre de grandeur très différent à une étape de l'algorithme. On peut même montrer qu'un choix aléatoire de $r$ est, en moyenne, un mauvais choix.

Diverses heuristiques peuvent alors être adoptées, par exemple prendre pour $r$ la partie entière de $n\cdot(\sqrt{5}-1)/2$, ou construire des stratégies spécifiques quand les deux plus petits éléments $d > e$ de $\mathscr{S}$ sont d'ordres de grandeur très différents ; par exemple, si $d$ est pair, ajouter $d/2$ à $\mathscr{S}$.

## Suggestions et pistes de réflexion

► *Les pistes de réflexion suivantes ne sont qu'indicatives et il n'est pas obligatoire de les suivre. Vous pouvez choisir d'étudier, ou non, certains des points proposés, de façon plus ou moins approfondie, mais aussi toute autre question à votre initiative. Vos investigations comporteront une partie traitée sur ordinateur et, si possible, des représentations graphiques de vos résultats. À défaut, si vos illustrations informatiques n'ont pas abouti, il est conseillé d'expliquer ce que vous auriez souhaité mettre en œuvre.*

— On pourra compléter les preuves des diverses assertions du texte ;
— On pourra détailler la notion, présentée dans l'introduction, de la taille d'un élément ;
— On pourra illustrer par des exemples certains résultats énoncés dans le texte ;
— On pourra illustrer à l'aide de l'ordinateur un des protocole cryptographique présenté dans le texte ;
— On pourra commenter, en lien avec le Théorème 2, le fait que $g \in \mathbb{F}_p$ est de la forme $\psi(u)$ avec $u \in \mathbb{F}_p$ ou $u \in \mathrm{Ker}(\varphi)$ ;

— On pourra regarder les suites mixtes obtenues via la version matricielle (Section 4.1), pour l'exponentiation naïve ou l'exponentiation rapide ;
— On pourra illustrer la proposition 7 pour des choix variés de $r$ et $n$, ou chercher le $r$ optimal pour un (petit) $n$ donné.