Projet de Recherche . 2020-2021

Faculté des Sciences et Techniques
Master 1 - Maths. CRYPTIS

Polynômes de Permutations

A l'attention de :
M. NECER

Rédigé par :
PIARD A.
JACQUET R.
CARVAILLO T.

Table des matières

Notation

$\mathbb{F}_q$	Corps de *Galois* à q éléments.
$\mathbb{F}_q{}^*$	Ensemble des éléments inversibles de $\mathbb{F}_q$
$\overline{\mathbb{F}_p}$	Clôture algébrique de $\mathbb{F}_p$.
$\mathbb{F}_q[X]$	Anneau des polynômes en l'indéterminée X à coefficients dans $\mathbb{F}_q$.
$\mathbb{P}\mathfrak{o}\mathbb{l}\mathbb{y}$	Ensemble des polynômes de permutation sur $\mathbb{F}_q$
$deg(f)$	Degré du polynôme f.
$P(X) \wedge Q(X)$	PGCD de P et Q.
$\mathbb{F}_p(\alpha)$	Corps de décomposition de α

Introduction

La structure de groupe, qui paraît si simple en apparence, est à la base du développement de théories bien moins triviales. De cette notion est née celle d'anneau, puis de corps. L'étude des groupes finis permet de formaliser rigoureusement des concepts naturels comme ceux de symétries, de permutations, ... Ce dernier point est celui qui nous intéressera. Bien que nous soyons déjà grandement familier avec le groupe des permutations S_n de l'ensemble à n éléments, en tant qu'algébriste nous trouvons plaisir à exhiber de nouveaux moyens d'entrevoir des notions fondamentales, tout en les reliant à des structures agréables.
Dans cet ersatz de mémoire, nous nous concentrerons sur une modélisation bien particulière des permutations.
Nous nous donnerons pour cela les moyens théoriques nécessaire. L'ensemble à permuter sera représenté par le corps fini à $q = p^n$ éléments $\mathbb{F}_q$, avec p premier et $n \in \mathbb{N}$. Quant aux permutations, elles seront « représentées » par un objet assez surprenant au vu de notre étude ; les polynômes. Nous verrons que certains polynômes permettent une permutation de $\mathbb{F}_q$, ils seront donc dit de permutation. On munira ensuite cet ensemble de polynômes d'une structure bien connue...

Dans une première partie, nous effectuerons l'essentiel des rappels de théorie des corps nécessaire à notre étude. Dans une seconde, seront exhibées les premières propriétés fondamentales des polynômes de permutations. Dans une troisième, nous verrons des premiers critères d'identifications, avec une implémentation pour certains d'entre eux. Et enfin, une dernière sera articulée par la présentation de « grandes familles » de polynômes de permutations.

1 Construction des Corps Finis

1.1 Existence et unicité

Soit $\mathbb{K}$ un corps quelconque et soit φ le morphisme suivant :

$$\varphi : \left| \begin{array}{ccc} \mathbb{Z} & \longrightarrow & \mathbb{K} \\ n & \longmapsto & n \cdot 1_{\mathbb{K}} \end{array} \right.$$

Définition 1. Soit $\mathbb{K}$ un corps quelconque. Toute partie $\mathcal{P}$ de $\mathbb{K}$ vérifiant :

- $\mathcal{P}$ est non vide et est une partie stable pour $+$ et $\times$ de $\mathbb{K}$ et $\mathcal{P}$ muni des lois induites par celles de $\mathbb{K}$ est lui-même un corps.
- $\mathcal{P}$ est un sous-anneau de $\mathbb{K}$, $1 \in \mathcal{P}$ et $(p \in \mathcal{P}^* = \mathcal{P} - \{0\} \Rightarrow p^{-1} \in \mathcal{P}^*)$.
- $\mathcal{P}$ est un sous-groupe de $(\mathbb{K}, +)$ et $\mathcal{P}^*$ muni de la loi $\times$ est un sous-groupe multiplicatif $(\mathbb{K}^*, \times)$.

est appelée sous-corps de $\mathbb{K}$.

Définition 2. Soit $\mathbb{K}$ un corps quelconque.

- $\mathbb{K}$ est dit premier s'il ne contient aucun sous-corps strict.
- Si $\mathbb{K}$ est un corps, le sous-corps de $\mathbb{K}$ engendré par $1_{\mathbb{K}}$ est un corps premier, c'est le sous-corps premier de $\mathbb{K}$.

Le noyau du morphisme φ est un idéal de $\mathbb{Z}$ et donc de la forme $k\mathbb{Z}$ pour $k \in \mathbb{Z}$. Par le premier théorème d'isomorphisme on a $\mathrm{Im}(\varphi) \cong \mathbb{Z}/n\mathbb{Z}$. Par intégrité de $\mathbb{Z}/n\mathbb{Z}$, $n = 0$ ou n est un nombre premier. Si $n = 0$ alors φ est injective et donc le sous-corps premier de $\mathbb{K}$ est isomorphe à $\mathbb{Q}$. Si $n \neq 0$ alors le sous-corps premier est isomorphe à $\mathbb{Z}/n\mathbb{Z}$ et n s'appelle la **caractéristique** de $\mathbb{K}$.

Définition 3. Soient L et $\mathbb{K}$ deux corps. Si L/K est une extension de corps alors L est un espace vectoriel sur K, où l'addition vectorielle est l'addition dans L et la multiplication par un scalaire $K \times L$ est la restriction à $K \times L$ de la multiplication dans L. La dimension du K-espace vectoriel L est appelée le degré de l'extension et est notée $[L : K]$.

Définition 4. Soit P un polynôme sur un corps K. On appelle corps de décomposition de P sur K une extension L de K telle que :

- dans $L[X]$, $P(X)$ est produit de facteurs de degré 1,
- les racines de $P(X)$ engendrent L.

Proposition 1. *Soit P un polynôme sur un corps K. Alors P admet un corps de décomposition, unique à K-isomorphisme près.*

Proposition 2.

— *Le cardinal de* $\mathbb{K}$ *est une puissance de* p.

— *Réciproquement, pour tout* $n \in \mathbb{N}^*$, *il existe un corps* $\mathbb{K}$ *de cardinal* p^n. *En outre* $\mathbb{K}$ *est unique à isomorphisme près.*

Démonstration.

— Puisque le sous-corps premier de $\mathbb{K}$ est isomorphe à $\mathbb{Z}/p\mathbb{Z}$, alors $\mathbb{K}$ est naturellement muni d'une structure de $\mathbb{Z}/p\mathbb{Z}$-espace vectoriel. On note $n = [\mathbb{K} : \mathbb{Z}/p\mathbb{Z}]$. Alors $\#\mathbb{K} = \#(\mathbb{Z}/p\mathbb{Z})^n = p^n$.

— Soit $n \in \mathbb{N}^*$. Si $\mathbb{K}$ est un corps fini de cardinal p^n, alors $\mathbb{K}$ est le corps de décomposition de $X^{p^n} - X$ sur $\mathbb{Z}/p\mathbb{Z}$: en effet, puisque pour tout $x \in \mathbb{K}$, x est racine de $X^{p^n} - X$ alors $X^{p^n} - X$ possède ses p^n racines dans $\mathbb{K}$.
Réciproquement, soit K le corps de décomposition de X^{p^n} sur $\mathbb{Z}/p\mathbb{Z}$. Soit $\mathcal{K}$ l'ensemble des éléments de K qui sont racines de $X^{p^n} - X$. On vérifie que $\mathcal{K}$ est un sous-corps de K. Puisque $1_K \in \mathcal{K}$, et si $x, y \in \mathcal{K}$ alors $x^{p^n} = x$ et $y^{p^n} = y$, donc $(x+y)^{p^n} x + y$ et $(xy^{-1})^{p^n} = xy^{-1}$, si bien que $x + y, xy^{-1} \in \mathcal{K}$. Par ailleurs la dérivée formelle, $(X^{p^n} - X)' = -1$ est premier avec $X^{p^n} - X$ donc les racines de $X^{p^n} - X$ sont simples. On en déduit alors que $\#\mathcal{K} = p^n$. Finalement $K = \mathcal{K}$ est un corps à p^n éléments et il est unique à isomorphisme près en vertu de l'unicité du corps de décomposition de $X^{p^n} - X$ sur $\mathbb{Z}/p\mathbb{Z}$.

□

On notera dorénavant $\mathbb{F}_q$ **le** corps fini à $q = p^n$ éléments.

1.2 Construction

Soit $P \in \mathbb{F}_p[X]$ un polynôme irréductible sur $\mathbb{F}_p$. On note $n = \deg(P)$. Puisque P est irréductible, l'idéal (P) est donc maximal. Le quotient $\mathbb{F}_p[X]/(P)$ est le corps de rupture de P sur $\mathbb{F}_p$ de cardinal p^n. Afin de montrer que l'on peut toujours construire les corps finis nous allons montrer que pour tout $n \in \mathbb{N}^*$ il existe un polynôme irréductible sur $\mathbb{F}_p$ de degré n.

Proposition 3. *Soit* $n \in \mathbb{N}^*$, *on définit* $\mathcal{P}(n,p)$ *par*

$$\mathcal{P}(n,p) = \{P \in \mathbb{F}_p[X],\ P \text{ unitaire, irréductible de degré } n\}.$$

Alors pour tout $n \in \mathbb{N}^*$ *on a,*

$$X^{p^n} - X = \prod_{d|n} \prod_{P \in \mathcal{P}(n,p)} P.$$

Démonstration.

— Soit P un facteur irréductible de $X^{p^n} - X$ sur $\mathbb{F}_p$ de degré d. Le corps de rupture de P sur $\mathbb{F}_p$ est de cardinal p^d du corps de décomposition $X^{p^n} - X$ sur $\mathbb{F}_p$, c'est-à-dire F_{p^n}, donc d divise n.

— Réciproquement, on suppose que d divise n et soit $P \in \mathcal{P}(n,p)$. Soit α une racine de P dans le corps de rupture de P sur $\mathbb{F}_p$. Alors on a $\mathbb{F}_p(\alpha) \simeq \mathbb{F}_{p^d}$. D'où α est racine de $X^{p^n} - X$. Or, puisque P est irréductible, alors P est le

polynôme minimal de α sur $\mathbb{F}_p$ donc P divise $X^{p^n} - X$. En outre les facteurs irréductible de $X^{p^n} - X$ sur $\mathbb{F}_p$ sont simples puisque P est le polynôme minimal de α et que P divise $X^{p^n} - X$.

□

Corollaire 1. Soit $n \in \mathbb{N}^*$, il existe un polynôme irréductible de degré n sur $\mathbb{F}_p$.

Démonstration. En conservant les notations de la proposition précédente, il s'agit de montrer que $\#\mathcal{P}(n,p) > 0$. Pour ce faire on évalue le degré de l'égalité

$$X^{p^n} - X = \prod_{d|n} \prod_{P \in \mathcal{P}(n,p)} P.$$

on a alors

$$p^n = \sum_{d|n} d \cdot \#\mathcal{P}(n,p)$$

On en déduit alors que pour tout $d \in \mathbb{N}^*$ on a $p^d \geq d \cdot \#\mathcal{P}(n,p)$, puis,

$$\begin{aligned} n \cdot \#\mathcal{P}(n,p) &= p^n - \sum_{d|n, d \neq n} d \cdot \#\mathcal{P}(n,p) \\ &\geq p^n - \sum_{d|n, d \neq n} p^d \\ &\geq p^n - \sum_{d=1}^{n-1} p^d \\ &\geq p^n - p\frac{p^{n-1} - 1}{p-1} > 0 \end{aligned}$$

Puisque n est positif alors $\mathcal{P}(n,p) > 0$. □

2 Polynômes de permutations

2.1 Quelques généralités

Rappelons d'abord ce qu'est un polynôme dans le cas général.

Définition 5. Soit K un ensemble non vide. On appelle polynôme en l'indéterminée X, toute application

$$P : \left| \begin{array}{ccc} K & \longrightarrow & K \\ X & \longmapsto & \sum_{i=0}^{n} a_i X^i,\ a_i \in K. \end{array} \right.$$

Définition 6. Soit K un ensemble fini de cardinal $n \in \mathbb{N}^*$. Une permutation de K est une bijection de K dans K.

Avec ces deux définitions, nous pouvons alors introduire la notion de polynôme de permutation.

Définition 7. Soit P un polynôme de $\mathbb{F}_q[X]$. P est appelé **polynôme de permutation** de $\mathbb{F}_q$ si et seulement si la fonction associée

$$P : \left| \begin{array}{ccc} \mathbb{F}_q & \longrightarrow & \mathbb{F}_q \\ X & \longmapsto & P(X) \end{array} \right.$$

est une permutation, c'est-à-dire est bijective.

Exemples. On se place dans $\mathbb{F}_5$.

1. Le polynôme X^3 est un polynôme de permutation. En effet, l'application

$$P : \left| \begin{array}{ccc} \mathbb{F}_5 & \longrightarrow & \mathbb{F}_5 \\ X & \longmapsto & X^3 \end{array} \right.$$

est clairement bijective.

2. Le polynôme X^2 n'est pas un polynôme de permutation. Considérons l'application

$$P : \left| \begin{array}{ccc} \mathbb{F}_5 & \longrightarrow & \mathbb{F}_5 \\ X & \longmapsto & X^2 \end{array} \right.$$

En effet cette application n'est pas injective. Soient $(X, Y) \in (\mathbb{F}_5 \times \mathbb{F}_5)$. On a $P(X) = P(Y)$ si et seulement si $X^2 = Y^2$. En prenant $X = 2$ et $Y = 3$ on fausse l'injectivité.

De manière plus générale, nous avons pour $k \in \mathbb{N}$:

Proposition 4. *X^k est un polynôme de permutation de $\mathbb{F}_q$ si et seulement si $pgcd(k, q-1) = 1$.*

Démonstration. $\Leftarrow$ Supposons que $pcgd(k, q-1) = 1$. Soit

$$P : \left| \begin{array}{ccc} \mathbb{F}_q & \longrightarrow & \mathbb{F}_q \\ x & \longmapsto & P(x) \end{array} \right.$$

Si $pcgd(k, q-1) = 1$, i.e. si $k \nmid q-1$ ou $q-1 \nmid k$, il est évident que $\forall x \in \mathbb{F}_q \backslash \{0\}$, $x^k \neq 0$. Donc 0 est le seul antécédent de 0. $\mathbb{F}_q$ étant un corps, on a $\mathbb{F}_q^* = \mathbb{F}_q^\times$, donc $|\mathbb{F}_q^*| = q-1$. Soit α un générateur de $\mathbb{F}_q^*$. La théorie élémentaire des groupes nous donne $| < \alpha^k > | = \frac{q-1}{pcgd(k,q-1)}$. Et donc par hypothèse, $| < \alpha^k > | = q-1$. Donc $P(\alpha)$ engendre $P(\mathbb{F}_q^*)$ et par cardinalité nous obtenons la conclusion voulue.

$\Rightarrow$ Nous allons raisonner par contraposée, i.e. montrer que $pcgd(k, q-1) \neq 1 \Rightarrow$ x^k n'est pas un polynôme de permutation.
Supposons donc $pcgd(k, q-1) = m$, où $m \in \mathbb{N}$. On obtient donc

$$\left\{ \begin{array}{l} k = k'.m \\ q-1 = q'.m \end{array} \right.$$

Et par suite, $k = k'.\frac{q-1}{q}$.
Donc, $X^k = X^{k'.\frac{q-1}{q}} = (X^{(q-1)})^{\frac{k'}{q'}} = 1$. Donc, $\forall x \in \mathbb{F}_q^\times$, $P(x) = 1$, l'application associé n'est donc pas bijective, par conséquent P n'est pas un polynôme de permutation.
On obtient donc l'équivalence souhaitée. □

2.2 Histoire de groupes...

2.2.1 Préliminaires, l'interpolation de Lagrange

Les motivations et descriptions analytiques détaillées de cette notion n'entrent pas dans le cadre de ce projet. Nous nous contenterons donc de rappeler, dans notre cadre, la définition suivante :

Définition 8. Soit

$$\phi : \left| \begin{array}{ccc} \mathbb{F}_q & \longrightarrow & \mathbb{F}_q \\ x & \longmapsto & \phi(x) \end{array} \right.$$

Le problème est de trouver un polynôme P, de degré minimal $\leq q$, tel que

$$P(x) = \phi(x), \forall x \in \mathbb{F}_q.$$

Proposition 5 (Admise)**.** *L'unique solution au problème présenté ci-dessus est donnée par*

$$P(x) := \sum_{d \in \mathbb{F}_q} \phi(d). \frac{\prod\limits_{c \in \mathbb{F}_q, c \neq d} (x-c)}{\prod\limits_{c \in \mathbb{F}_q, c \neq d} (d-c)}$$

Proposition 6. *De manière plus élégante, nous avons*

$$P(x) := \sum_{d\in\mathbb{F}_q} \phi(d)(1-(x-d)^{q-1})$$

Démonstration. De manière générale, nous avons que $X^q - X = \prod_{c\in\mathbb{F}_q}(X-c)$, donc

$$\begin{aligned}\prod_{c\in\mathbb{F}_q, c\neq d}(x-c) &= \frac{\prod_{c\in\mathbb{F}_q}(x-c)}{x-d}\\ &= \frac{x^q-x}{x-d}\\ &= \frac{x^q-d^q-(x-d)}{x-d}\\ &= (x-d)^{q-1}-1\end{aligned}$$

En appliquant cette égalité pour $x = d$, on obtient que

$$\prod_{c\in\mathbb{F}_q, c\neq d}(d-c) = -1$$

Finalement, on obtient que

$$\sum_{d\in\mathbb{F}_q}\phi(d).\frac{\prod_{c\in\mathbb{F}_q, c\neq d}(x-c)}{\prod_{c\in\mathbb{F}_q, c\neq d}(d-c)} = \sum_{d\in\mathbb{F}_q}\phi(d)(1-(x-d)^{q-1})$$

et la proposition est ainsi prouvée. □

Remarque 1. Il est facile de voir que si ϕ est un polynôme, alors l'interpolation de Lagrange est une simple application du théorème des restes chinois.
Il suffit de considérer la solution P du système

$$\begin{cases}\phi \equiv 1 \pmod{X-c_1}\\ \phi \equiv 1 \pmod{X-c_2}\\ \ldots\\ \phi \equiv 1 \pmod{X-c_q}\end{cases}$$

pour s'en convaincre.

De cette remarque découle le fait que pour travailler sur des polynômes de permutation, il suffit de les regarder modulo $X^q - X$. Nous allons dès lors obtenir une structure intéressante, celle de groupe.

2.2.2 Un groupe, enfin !

Proposition 7. *L'ensemble* $\mathbb{P}\mathrm{ol}\mathbb{y}$ *des polynômes de permutation à coefficients dans* $\mathbb{F}_q$ *et de degré inférieur à* q *muni de la loi de composition* $\circ$ *est un groupe, i.e,* $(\mathbb{P}\mathrm{ol}\mathbb{y}, \circ)$ *est un groupe.*

Démonstration. Soient $P = \sum_{i\in[\![0,q-1]\!]} A_i X^i$, $Q = \sum_{j\in[\![0,q-1]\!]} B_j X^j$ et $R = \sum_{k\in[\![0,q-1]\!]} C_k X^k$ des polynômes à coefficients dans $\mathbb{F}_q$.

- ♣ La composée de deux polynômes est encore un polynôme. Il est de plus facile de remarquer que si l'on permute un ensemble deux fois, cela reste un ensemble permuté. La composition de deux polynômes de permutation est donc un polynôme de permutation. Nous avons donc notre loi interne.
- ♣ Montrons son associativité :
  D'une part, on a

$$(P\circ Q)\circ R$$

$$= \sum_{i\in[\![0,q-1]\!]} A_i \left(\sum_{j\in[\![0,q-1]\!]} B_j X^j\right)^i \circ \left(\sum_{k\in[\![0,q-1]\!]} C_k X^k\right)$$

$$= \sum_{i\in[\![0,q-1]\!]} A_i \left(\sum_{j\in[\![0,q-1]\!]} B_j \left(\left(\sum_{k\in[\![0,q-1]\!]} C_k X^k\right)\right)^j\right)^i$$

  puis,

$$P\circ(Q\circ R)$$

$$= \left(\sum_{i\in[\![0,q-1]\!]} A_i X^i\right) \circ \left(\sum_{j\in[\![0,q-1]\!]} B_j \left(\left(\sum_{k\in[\![0,q-1]\!]} C_k X^k\right)\right)^j\right)$$

$$= \sum_{i\in[\![0,q-1]\!]} A_i \left(\sum_{j\in[\![0,q-1]\!]} B_j \left(\left(\sum_{k\in[\![0,q-1]\!]} C_k X^k\right)\right)^j\right)^i$$

  donc la loi $\circ$ est associative.
- ♣ Le neutre est évidemment le polynôme constant égal à 1.
- ♣ Rappelons que, par définition, un polynôme de permutation est une application bijective de $\mathbb{F}_q$. Il suffit donc de considérer son application réciproque P^{-1} pour obtenir Q tel que $P\circ Q = 1$. Ceci nous donne l'élément neutre. Ceci marche toujours modulo $X^q - X$ car

$$\Pi : \left| \begin{array}{ccc} \mathbb{F}_q[X] & \longrightarrow & \mathbb{F}_q[X]/(X^q - X) \\ P & \longmapsto & [P]_{X^q-X} \end{array} \right.$$

  est un morphisme d'anneaux.

Il s'ensuit que $(\mathbb{P}\mathrm{ol}\mathbb{y}, \circ)$ est un groupe. □

Proposition 8. *On a l'isomorphisme suivant,* $(\mathbb{P}\mathrm{ol}\mathbb{y}, \circ) \cong \mathbb{S}_q$*, où* $\mathbb{S}_q$ *est le groupe des permutations de l'ensemble* $[\![1, ..., q]\!]$*.*

Démonstration. La difficulté de cette preuve réside dans le fait qu'un polynôme de $\mathbb{F}_q$ peut être représenté par une permutation très complexe et inversement. On rappelle que dans $\mathbb{S}_q$, toute permutation τ peut être représentée comme produit de transpositions. Dans notre cas il est suffisant de considérer les transpositions échangeant uniquement les éléments 0 et $a \in \mathbb{F}_q$ que l'on note $\tau_{0,a}$. Il vient alors que pour toutes transpositions de $\mathbb{S}_q$ échangeant deux éléments a et b de $\mathbb{F}_q$ on a,

$$\tau_{0,a} \cdot \tau_{0,b} \cdot \tau_{0,a} = \tau_{a,b}$$

si bien que l'on exhibe le polynôme associé à la transposition

$$\tau_{0,a} : \mathbb{t}(x) = -a^2 \left[\left((x-a)^{q-2} + a^{-1} \right)^{q-2} - a \right]^{q-2}$$

Il est facile de le vérifier dans le cas où $a = 1$. On considère le corps $\mathbb{F}_p$. On remarque que

$$\mathrm{g}_1(x) - x = \begin{cases} 1 & \text{si } x = 0 \\ -1 & \text{si } x = 1 \\ 0 & \text{sinon.} \end{cases}$$

On en déduit alors que $\mathrm{g}_1(x) - x = (ax + b) + \prod_{k=2}^{p-1}(x - k)$

En appliquant notre égalité pour $x = 1$ et $x = 0$ on obtient le système suivant,

$$\begin{cases} 1 & = -b(p-1)! \\ -1 & = -(a+b)(p-2)! \end{cases}$$

Or, puisque dans $\mathbb{F}_p$ on a $(p-1)! = -1$ et $(p-2)! = 1$ alors on en déduit que $(a, b) = (0, 1)$ et donc $\mathrm{g}_1(x) = x + \prod_{k=2}^{p-1}(x - k)$. □

Proposition 9. *Soit* α *un élément primitif de* $\mathbb{F}_q$*, alors* $(\mathbb{P}\mathrm{ol}\mathbb{y}, \circ)$ *est engendré par* $\{\alpha X,\ X + 1,\ X^{q-2}\}$

Démonstration. Remarquons tout d'abord que, pour $a, b \in \mathbb{F}_q$,

— $< aX > = < \alpha^m X > = < \alpha X >^m$ (cette dernière égalité découle de la loi de composition)

— $< \alpha X >^{m-n} < X+1 >< \alpha X >^{n}$
$=< \alpha X >^{m-n} < \alpha^{n} X + 1 >$
$=< \alpha^{m-n} X >< \alpha^{n} X + 1 >$
$=< \alpha^{m-n}(\alpha^{n} X + 1) >$
$=< \alpha^{m} X + \alpha^{m-n} >$,
ce qui nous donne un générateur de la forme $< aX + b >$.

Il suffit ensuite de considérer la forme générale du polynôme correspond à la transposition $\tau_{0,a}$, en remarquant que

$$\tau_{0,a} =< -a^2 X >< X^{q-2} >< X - a >< X^{q-2} >< X + a^{q-2} >< X^{q-2} >< X - a >$$

Il est ensuite aisé de construire n'importe quel polynôme de permutation en sachant que $\tau_{0,a} \cdot \tau_{0,b} \cdot \tau_{0,a} = \tau_{a,b}$ □

3 Premiers critères d'identifications avec implémentations

Nous venons de voir les premières définitions et propriétés sur les polynômes de permutation. Il est plus que nécessaire, avant de se lancer dans la tâche ardue qu'est l'étude des polynômes de permutations, de se donner les moyens de les identifier, ou tout du moins de savoir les reconnaître. Dans cette partie, nous verrons plusieurs critères triviaux, qui seront implémentés en *Python* via *Sagemath*.

3.1 Considérations triviales

Une manière bien simple de reconnaître un polynôme de permutation consiste à en calculer toutes les images, puis de les comparer une à une. Si une image est égale à une autre, i.e. l'application n'est pas injective, alors le polynôme ne sera pas de permutation. On obtient dès lors le critère suivant :

Critère 1. Un polynôme $P \in \mathbb{F}_q[X]$ est une permutation de $\mathbb{F}_q$ si et seulement si

$$\prod_{c\in\mathbb{F}_q} (X - P(c)) = X^q - X$$

En plus d'être très peu élégante, cette méthode requiert une puissance de calcul, croissante et en le degré du polynôme et en le cardinal du corps dans lequel on se place.

Il est également possible de faire la démarche en sens inverse et de considérer les antécédents. On obtient alors le critère suivant :

Critère 2. P est un polynôme de permutation si et seulement si $\forall \alpha \in \mathbb{F}_q$,

$$deg((X^q - X) \wedge (P(X) - \alpha)) = 1$$

Démonstration. En effet, le fait que $deg((X^q - X) \wedge (P(X) - \alpha)) \neq 1$ signifie que $X^q - X$ et $P(X) - \alpha$ ont comme facteur commun $\prod_{c\in\mathbb{F}_q, P(c)=\alpha} (X - c)$, donc $P(X) - \alpha$ s'annule en plusieurs points et finalement P n'est pas une bijection.
Réciproquement, si $deg((X^q - X) \wedge (P(X) - \alpha)) = 1$, alors le seul facteur commun à $X^q - X$ et $P(X) - \alpha$ est $X - c$, où c est tel que $P(c) = \alpha$. La conclusion s'ensuit. □

3.2 Le critère d'Hermite-Dickson

Soit $q = p^n$ une puissance d'un nombre premier quelconque. On rappelle que la fonction

$$\Pi : \left| \begin{array}{ccc} \mathbb{F}_q[X] & \longrightarrow & \mathbb{F}_q[X]/(X^q - X) \\ P & \longmapsto & [P]_{X^q - X} \end{array} \right.$$

définit un morphisme d'anneaux, de sorte que, $\overline{(P(X))^k} = \overline{P(X)}^k \pmod{X^q - X}$. On se donne également un polynôme P à coefficients dans $\mathbb{F}_q$, et l'ensemble

$$A_{p,q} := \{k \in [\![1, q-2]\!] \text{ tels que } p \nmid k\}$$

Énonçons maintenant le

Critère 3 (Hermite-Dickson)**.** P est un polynôme de permutation si et seulement si les deux conditions suivantes sont réunies :

1. pour tout $k \in A_{p,q}$, $deg(\overline{(P(X))^k}) < q-1$
2. $deg(\overline{(P(X))^{q-1}}) = q-1$

3.3 Implémentations

Commençons par ce premier algorithme de test pour trouver les polynômes de permutations. Cet algorithme est développé en *Sage*.

```
def estDePermutation(f, q):
    R.<x> = GF(q) # Corps fini à q éléments
    S.<t> = PolynomialRing(R) # Anneau de polynômes sur F_q en l'indéterminée t
    f = S(f)
    image = []
    for i in R:
        temp = f(i)
        if temp in image: # si l'application n'est pas injective
                          # le polynôme ne peut être de permutation
            return(False)
        else:
            image.append(temp)
    return(True)

q = 2
deg = 4
R.<x> = GF(q)
S.<t> = PolynomialRing(R)
print(" Les polynômes de permutations à coefficients dans F_" + str(q) +
" de degré au plus " + str(deg) + " sont :")
for f in S.polynomials(of_degree=deg):
    if estDePermutation(f, q):
       print( f )
```

```
 Les polynômes de permutations à coefficients dans F_2 de degré au plus 4 sont :
t^4
t^4 + 1
t^4 + t^2 + t
t^4 + t^2 + t + 1
t^4 + t^3 + t
t^4 + t^3 + t + 1
t^4 + t^3 + t^2
t^4 + t^3 + t^2 + 1
```

FIGURE 1 – Affichage de l'exécution

Nous allons ensuite présenter une implémentation sous forme algorithmique du **Critère 1** présenté précédemment. Cet algorithme est développé en *Sage*.

```
def estDePermutation(f, q):
    R.<x> = GF(q) # Corps fini à q éléments
    S.<t> = PolynomialRing(R) # Anneau de polynômes sur F_q en l'indéterminée t
    f = S(f)
    temp = t - f(R(0)) # R(0) désigne le premier élément du corps F_q
    for i in R:
        if R(0) == i:
            continue
        temp = temp * (t - f(i))
    if temp == t**q - t:
        return (True)
    return (False)

q = 2
deg = 4
R.<x> = GF(q)
S.<t> = PolynomialRing(R)
test1 = t**4 + t**3 + t
test2 = t**4 + t**3 + 1
answer1 = "non"
answer2 = "non"
if estDePermutation(test1, q):
    answer1 = "oui"
if estDePermutation(test2, q):
    answer1 = "oui"
print("Critère 1 :")
print("Le polynôme " + str(test1)  + " est de permutation ? " + answer1)
print("Le polynôme " + str(test2)  + " est de permutation ? " + answer2)
```

```
Critère 1 :
Le polynôme t^4 + t^3 + t est de permutation ? oui
Le polynôme t^4 + t^3 + 1 est de permutation ? non
```

FIGURE 2 – Affichage de l'exécution

Cet algorithme nécessite plus de calculs que le précédent mais permet de donner une réponse directe à la question "Est ce que $P \in \mathbb{F}_q[X]$ est de permutation ?".

Nous allons présenter aussi un algorithme permettant une implémentation du **Critère 2**. Il a été lui aussi développé en *Sage*.

```
def estDePermutation(f, q):
    R.<x> = GF(q) # Corps fini à q éléments
    S.<t> = PolynomialRing(R) # Anneau de polynômes sur F_q en l'indéterminée t
    f = S(f)
    a = t**q - t
    for element in R:
        if (a.gcd(f - element)).degree() != 1:
            return (False)
    return(True)

q = 2
R.<x> = GF(q)
S.<t> = PolynomialRing(R)
test1 = t**4 + t**3 + t**2 + 1
test2 = t**4 + t**3 + 1
answer = "non"
answer2 = "non"
if estDePermutation(test1, q):
    answer = "oui"
if estDePermutation(test2, q):
    answer2 = "oui"
print(str(test1) + " est de permutation ? " + answer)
print(str(test2) + " est de permutation ? " + answer2)
```

```
t^4 + t^3 + t^2 + 1 est de permutation ? oui
t^4 + t^3 + 1 est de permutation ? non
```

FIGURE 3 – Affichage de l'exécution

Cet algorithme est assez intéressant car il permet de tester directement un polynôme bien spécifique, à l'instar du premier qui permet de lister les polynômes de permutations de degré précisé.

Enfin nous allons présenter une implémentation du **Critère de Hermite-Dickson**. Cette implémentation a également été réalisée en *Sage*.

```
def estDePermutation(f, q):
    R.<x> = GF(q) # Corps fini à q éléments
    S.<t> = PolynomialRing(R) # Anneau de polynômes sur F_q en l'indéterminée t
    f = S(f)
    a_pk = []
    for i in range(0, q-2):
        if p % k != 0:
            a_pk.append(i)
    for j in a_pk:
        if (f(t)**j % (t**q - t)).degree() > q - 1:
            return (False)
    if (f(t)**(q-1) % (t**q - t)).degree() == q - 1:
        return (True)
    return (False)

q = 2
deg = 4
R.<x> = GF(q)
S.<t> = PolynomialRing(R)
test1 = t**4 + t**3 + t
test2 = t**4 + t**3 + 1
answer1 = "non"
answer2 = "non"
if estDePermutation(test1, q):
    answer1 = "oui"
if estDePermutation(test2, q):
    answer1 = "oui"
print("Critère Hermite-Dickson :")
print("Le polynôme " + str(test1)  + " est de permutation ? " + answer1)
print("Le polynôme " + str(test2)  + " est de permutation ? " + answer2)
```

```
Critère Hermite-Dickson :
Le polynôme t^4 + t^3 + t est de permutation ? oui
Le polynôme t^4 + t^3 + 1 est de permutation ? non
```

FIGURE 4 – Affichage de l'exécution

Cet algorithme est le plus complexe et est celui qui nécessite le plus d'opérations. Il est en revanche plus intéressant en termes de développement et de structures car il utilise des calculs plus conséquents.

Remarque

Les algorithmes que nous venons de concevoir présentent une caractéristique commune, et non des moindres, ils sont déterministes. Un polynôme entré en paramètre est ou n'est pas de permutation. Cela paraît évident, les algorithmes implémentés décident selon des critères rigoureusement démontrés. Cependant, la complexité de ces derniers n'est pas des plus optimales si l'on est tenté de les éprouver sur

des valeurs de q ou même de n extrêmement grandes. Il est aisé de remarquer cela en considérant le *critère 2*. Soyons fou, et mettons que l'on veuille tester si le polynôme $X^{987654321} + X^{12345678} + X^3 + 1$ est de permutation dans le corps à $3^{757} = 1481113296616977741464105532513750734030421355207$ éléments selon ce même critère. Il faudrait donc dans la pire des situations (qui ici correspond à celle où le polynôme est de permutation !) effectuer ce nombre astronomique de calculs de pgcd. Cet algorithme peut être amélioré, selon le sens que l'on donne à ce terme. La première considération qui nous vient à l'esprit est de se demander s'il est réellement nécessaire de tester toutes les valeurs de cet affreux corps fini, si en tester une partie suffirait à nous indiquer avec une forte *probabilité* si un polynôme est, ou non, de permutation. C'est dans ce contexte qu'interviennent les méthodes probabilistes, qui améliorent, au sens de la complexité, nos algorithmes. Elles ne sont certes pas exactes, mais les applications à la cryptologie sont une de nos principales sources de motivations. Notre intérêt est donc également portés sur l'efficacité des algorithmes. Nous détaillerons quelques une de ces méthodes dans un prochain rendu.

4 Classes de polynômes

Les méthodes d'identifications que nous venons de voir sont certes fonctionnelles, mais non raffinées. Elles sont extrêmement coûteuses en terme de puissance de calcul. Il est donc primordial d'établir une liste de critères permettant d'accélérer le processus. Cette partie y sera entièrement consacrée. Pour ce faire, nous travaillons sur des "familles" de polynômes. Nous n'aurons pas la prétention d'en donner une liste exhaustive ; cependant dans ce premier rendu nous donnerons les plus élémentaires. Une étude plus approfondie sera faite au second semestre.

4.1 Polynômes exceptionnels

Avant de commencer, rappelons la

Proposition 10. *L'ensemble $\mathbb{F}_q[X,Y]$ des polynômes en les indéterminées X et Y à coefficients dans $\mathbb{F}_q$ est muni d'une structure d'anneau, et est construit comme suit :*

$$\mathbb{F}_q[X,Y] = (\mathbb{F}_q[X])[Y] = (\mathbb{F}_q[Y])[X]$$

Définition 9. Un polynôme en les deux indéterminées X et Y est dit absolument irréductible s'il est irréductible sur toute extension de $\mathbb{F}_q$. En d'autres termes, s'il est irréductible sur la clôture algébrique $\overline{\mathbb{F}_q}$ de $\mathbb{F}_q$.

Remarque 2. On rappelle que toute extension de $\mathbb{F}_q$ est algébrique, il en va de même de sa clôture.

On se donne une suite d'entiers $(m_i)_{i\geq 1}$ avec $m_i \geq 1$ qui tend vers $+\infty$. On la construit en outre de telle sorte que $\forall i \geq 1$, m_i divise m_{i+1} et i divise m_i. Pour fixer les idées on prend $m_i = i!$. On pose $K_0 = \mathbb{F}_p$ et pour tout $i \geq 1$, soit K_i un corps de décomposition sur K_{i-1} du polynôme $X^{p^{m_i}} - X$. Alors $K_i \cong \mathbb{F}_{p^{m_i}}$ et on a une suite croissante

$$K_0 \subseteq K_1 \subseteq K_2 \subseteq ...$$

Définition 10. On appelle clôture algébrique de $\mathbb{F}_p$ notée $\overline{\mathbb{F}_p}$ la réunion des K_i :

$$\overline{\mathbb{F}_p} = \bigcup_{i\geq 1} K_i.$$

Définition 11. On dit qu'un polynôme en l'indéterminée X est exceptionnel sur $\mathbb{F}_q$ si aucun facteur irréductible du polynôme en les indéterminées X et Y

$$\Psi(X,Y) := \frac{P(X) - P(Y)}{X - Y}$$

n'est absolument irréductible. En d'autres terme, si les facteurs irréductibles admettent une décomposition sur une extension de $\mathbb{F}_q$.

Avant de nous aventurer dans l'énoncé de critères, voyons un premier exemple de polynôme exceptionnel.

Exemple 1. Considérons le polynôme $P(X) := X^3 + 3X^2 + 3X \in \mathbb{F}_q$, où q est choisit tel qu'il soit la puissance d'un nombre premier impair.
Construisons le fameux polynôme $\Psi(X, Y)$ à partir de P :

$$\begin{aligned}
\Psi(X,Y) &= \frac{P(X) - P(Y)}{X - Y} \\
&= \frac{X^3 + 3X^2 + 3X - Y^3 - 3Y^2 - 3Y}{X - Y} \\
&= \frac{X^3 - Y^3 + 3X^2 - 3Y^2 + 3X - 3Y}{X - Y} \\
&= \frac{(X-Y)(X^2+Y^2) - XY^2 + YX^2 + 3(X+Y)(X-Y) + 3X - 3Y}{X - Y} \\
&= \frac{(X-Y)(X^2+Y^2) + XY(X-Y) + 3(X+Y)(X-Y) + 3X - 3Y}{X - Y} \\
&= X^2 + Y^2 + XY + 3(X+Y) + 3 \\
&= X^2 + (3+Y)X + Y^2 + 3Y + 3
\end{aligned}$$

Nous avons donc un polynôme de degré 2 en l'indéterminée X. Faisons une étude de discriminant.
$\Delta_{\Psi(X,Y)} = (3+Y)^2 - 4(Y^2 + 3Y + 3) = -3(Y+1)^2$
Nous pouvons dès à présent distinguer deux cas :

— -3 est un carré dans $\mathbb{F}_q$, i.e. $\exists c \in \mathbb{F}_q$ tel que $c^2 = -3$. Les racines de Ψ existent donc et

$$\Psi(X,Y) = (X - \frac{-Y - 3 + c(Y+1)}{2})(X - \frac{-Y - 3 - c(Y+1)}{2}).$$

Ces facteurs étant de degré 1, il est clair qu'ils sont irréductibles sur toute extension de $\mathbb{F}_q$. Ψ présente donc des facteurs absolument irréductibles, il n'est donc pas un polynôme exceptionnel.

— dans le cas contraire, $\Psi(X, Y)$ est irréductible dans $\mathbb{F}_q[X, Y]$. Cependant, -3 sera par définition un carré dans la clôture algébrique de $\mathbb{F}_q$ (Il suffit de considérer le polynôme $X^2 - 3$...). Nous sommes donc dans la même situation que dans le premier cas, à la subtilité près que cette fois-ci, Ψ admet des facteurs irréductibles dans une extension de $\mathbb{F}_q$ et non dans $\mathbb{F}_q$. Donc, peu nous importe la réductibilité de ces dit facteurs ! Il s'ensuit que, par définition, Ψ est un polynôme exceptionnel.

Énonçons maintenant un critère fondamental :

Critère 4. Tout polynôme exceptionnel à coefficients dans $\mathbb{F}_q[X]$ est un polynôme de permutation.

Exemple 2. De l'exemple précédent, il découle que $P := X^3 + 3X^2 + 3X$ est un polynôme de permutation si -3 n'est pas un carré dans $\mathbb{F}_q$.
Dans $\mathbb{F}_5 \simeq \mathbb{Z}/5\mathbb{Z}$, $-3 = 2$ qui n'est pas un carré, donc P est un polynôme de permutation. En revanche, dans $\mathbb{F}_3 \simeq \mathbb{Z}/3\mathbb{Z}$, $-3 = 0 = 9 = 3^2$, donc P n'est pas un polynôme de permutation.

Remarque 3. La réciproque de ce théorème est fausse. Même s'il existe des conditions sous lesquelles elle a lieu, nous nous contenterons de donner un contre exemple.

Exemple 3. Soit $q = p^n$ une puissance d'un nombre premier quelconque. Soit $P := X^p$, nous avons clairement $pgcd(q-1, p) = 1$. La *Proposition 4* nous assure donc que P est un polynôme de permutation. Calculons une nouvelle fois le fameux polynôme $\Psi(X, Y)$ à partir de P :

$$\begin{aligned}\Psi(X,Y) &= \frac{P(X)-P(Y)}{X-Y} \\ &= \frac{X^p - Y^p}{X-Y} \\ &= \frac{(X-Y)^p}{X-Y} \quad \text{(on travaille sur un corps de caracteristique } p\text{)} \\ &= (X-Y)^{p-1}\end{aligned}$$

Or, les $(X - Y)$ sont évidemment irréductibles sur toute extension de $\mathbb{F}_q$, donc P n'est pas un polynôme exceptionnel.

Nous allons maintenant énoncer une proposition, qui sera admise pour le moment. Sa démonstration s'appuie sur des éléments complexes de la théorie de *Galois*. Nous nous laissons l'opportunité de le démontrer en ce second semestre.

Proposition 11. *Soit $q = p^n$ une puissance d'un nombre premier quelconque. Soit $k \in \mathbb{N}$ tel que $pgcd(k, q-1) > 1$. Alors, il n'existe pas de polynôme exceptionnel à coefficients dans $\mathbb{F}_q$ de degré k.*

4.2 Polynômes linéarisés

Nous allons maintenant nous intéresser à la notion de polynômes linéarisés qui, sous certaines conditions que nous allons évoquer, donnent lieu à des polynômes de permutation.

Définition 12. On appelle polynômes linéarisés de $\mathbb{F}_{p^n} = \mathbb{F}_q$ les polynômes de la forme $\sum_{i=0}^{k} a_i X^{p^i} \in \mathbb{F}_{p^n}$, $n \in \mathbb{N}$ et p premier.

Ces polynômes correspondent aux applications $\mathbb{F}_q$-linéaires.
Beaucoup d'exemples de polynômes de permutations peuvent être générés à partir de ce type de polynômes, c'est pourquoi nous introduisons maintenant le critère suivant :

Critère 5. Un polynôme de permutation de $\mathbb{F}_q$ est de permutation sur toutes les extensions finies de $\mathbb{F}_q$ si et seulement s'il est de la forme $ax^{p^h} + b$ avec $a \neq 0$ et $h \geq 0$.

Avec ce critère peuvent venir quelques théorèmes permettant d'identifier des polynômes de permutations, tels que :

Proposition 12. *Un polynôme linéarisé est de permutation si et seulement si* 0 *est son unique racine dans* $\mathbb{F}_{p^n}$.

Démonstration. Soit L un polynôme linéarisé de $\mathbb{F}_{p^n} = \mathbb{F}_q$. Il est évident que 0 est racine de L.
$\Rightarrow$ On va supposer que L est de permutation. Par définition, l'application associée

$$L : \left| \begin{array}{ccc} \mathbb{F}_q & \longrightarrow & \mathbb{F}_q \\ X & \longmapsto & L(X) \end{array} \right.$$

est bijective, donc injective donc 0 admet un antécédent unique.

$\Leftarrow$ Par contraposée.
On va montrer que si 0 n'est pas racine unique de L, alors L n'est pas de permutation. Si 0 n'est pas racine unique de L, alors 0 admet plusieurs antécédents par L et l'application associée n'est donc pas injective. La conclusion s'ensuit. □

Théorème 1 (Admis)**.** *Pour tout polynôme linéarisé* $L \in \mathbb{F}_q[x]$*, il existe* $a \in \mathbb{F}_q$ *tel que* $L(x) - ax$ *soit un polynôme de permutation.*

5 Applications en cryptographie

Cette partie est très largement inspirée de notre référence numéro 2 en raison de la qualité de celle-ci et du manque de ressources sur internet à ce sujet.

La cryptologie, étant le nom donné à la « science du secret », est un terme englobant à la fois la cryptographie, discipline servant à protéger des messages, et la cryptanalyse, discipline servant à déchiffrer des messages codés par des techniques cryptographiques, sans en connaître la méthode de chiffrement utilisée.
Nous allons donc commencer par quelques applications de polynômes de permutation en cryptographie.

La cryptographie se divise en deux grandes parties : la cryptographie à clé publique et la cryptographie à clé secrète.
La cryptographie à clé publique utilise deux clés distinctes. Une pour chiffrer et une pour déchiffrer. On parle alors de chiffrement asymétrique car les deux clés sont différentes. Le terme clé publique vient du fait qu'on peut rendre publique la clé de chiffrement étant donné que celle-ci n'est pas censée donner d'informations sur la clé de déchiffrement, ni en être son sosie.
Quant à elle, la cryptographie à clé secrète utilise la même clé pour chiffrer et déchiffrer. On parle alors de chiffrement à clé secrète, car rendre publique la clé de chiffrement impliquerait que n'importe qui puisse déchiffrer les messages qui ne lui sont pas destinés. Cela briserait donc le principe de *confidentialité* censé être assuré par la cryptographie.

5.1 À clé publique

L'application des polynômes de permutation en cryptographie a majoritairement vu le jour aux alentours de 1978 avec l'apparition du cryptosystème RSA pour la signature et le chiffrement à clé publique. Bien que certains mathématiciens, tels que Levine et Brawley, avaient commencés à s'intéresser aux polynômes de permutation et à leurs applications en cryptographie légèrement plus tôt.

5.1.1 RSA et polynômes de permutation

Rappelons brièvement l'algorithme de chiffrement RSA, utilisé également pour la signature.

On choisit p et q deux nombres premiers impairs très grand et on note n leur produit. C'est à dire, $n = pq$. On calcule ensuite $\phi(n) = (p-1)(q-1)$ et on choisit un nombre e de sorte que e soit premier avec $\phi(n)$. Ainsi, on peut obtenir d tel que $d = e^{-1} \mod \phi(n)$.
La clé publique sera alors le couple (n, e) et la clé secrète sera le d. En possession de ces deux clés, nous pouvons désormais chiffrer et déchiffrer des messages par la méthode RSA, en fixant bien sûr les valeurs de p et q.
Le chiffrement d'un message **m** s'effectuera ainsi :

$$c \equiv m^e \mod n,$$

et le déchiffrement ainsi :

$$m \equiv c^d \mod n.$$

Dans ce chiffrement, le polynôme de permutation se retrouve être X^e, où $X \in \mathbb{Z}/n\mathbb{Z}[X]$. Ce polynôme de permutation possède plusieurs avantages.
Il s'agit d'un monôme donc il est définissable très facilement, et malgré tout, retrouver X à partir du résultat de $X^e \mod n$ est impossible en un temps raisonnable sans connaître d, c'est à dire sans connaître p et q, en considérant la puissance des ordinateurs et algorithmes de résolution actuels.
De plus, le chiffrement est « relativement » efficace car il s'agit d'une simple exponentiation modulaire que certains algorithmes sont capables d'effectuer en un temps intéressant.

5.1.2 Cryptographie multivariée et polynômes de permutation

la cryptographie multivariée repose sur l'utilisation de polynômes multivariés à coefficients dans un corps fini. Il s'agit d'ailleurs d'une des directions de recherches considérées pour développer des algorithmes de cryptographies post-quantiques.
Le premier schéma de chiffrement de cette famille fut élaboré en 1988 par **Tsutomu Matsumoto** et **Hideki Imai**. Dans ce système, un polynôme central $X^{q^n+1} \in \mathbb{F}_q$ va être masqué par deux applications linéaires bijectives S et T. La partie chiffrement ne sera que la composition (dans $\mathbb{F}_q$) suivante :

$$S \circ X^{q^n+1} \circ T,$$

où ce polynôme représente la clé publique.
Ce polynôme assure la bijectivité et offre une représentation assez compacte de la clé.

A l'attention des bg, question 1. Est-ce qu'on en parle ? En effet, en prenant un polynôme de degré algébrique 2, on est assuré que la clé publique obtenue est de la forme

$$\sum_{0 \geq i,j < n} a_{i,j} X^{q^i+q^j} + \sum_{0 \geq k < n} b_k X^{q^k}$$

Il suffit donc de $\frac{n(n+1)}{2}$ éléments de $\mathbb{F}_q$ pour définir ce polynôme, à comparer aux q^{n-2} coefficients pour un polynôme de permutation en général.

Cependant, ce schéma fut rapidement cryptanalysé. La référence [5] est un scan de l'article de **Jacques PATARIN** sur sa cryptanalyse de ce schéma. Malgré tout, le système présenté par **Matsumoto** et **Imai** a inspiré de nombreuses variantes de schémas dont HFE (pour *Hidden Field Equations*), notamment introduit par **Jacques PATARIN**, et par extensions HFE-v qui regroupe plusieurs algorithmes tel que *quartz*. Cette famille de chiffrement connaît des attaques de complexité exponentielle alors que la signature ne coûte presque rien pour la personne qui signe. De plus, ces schémas ont les signatures les plus courtes parmi tous les schémas de signature à clé publique connus. Par conséquent, parvenir à effectuer ces algorithmes avec des polynômes de permutations pourraient accroître les performances mais ceci reste une supposition, à l'heure d'aujourd'hui.

5.2 À clé secrète

5.2.1 Les fonctions APN

Un principe d'attaque en cryptanalyse différentielle est d'identifier des couples de textes clairs dont la différence est fixée, et dont la différence des chiffrés correspondants est fortement biaisée.
Pour définir ce que sont les fonctions APN, et ensuite expliquer leur lien avec les polynômes de permutation et la cryptographie, nous devons d'abord introduire la notion de dérivée d'une fonction discrète.

Définition 13. Soient $n \in \mathbb{N}$, p un nombre premier et f une fonction de $\mathbb{F}_{p^n}$ dans $\mathbb{F}_{p^n}$. Pour tout $a \in \mathbb{F}_{p^n}$, la dérivée de f au point a est :

$$D_a f : \left| \begin{array}{ccc} \mathbb{F}_{p^n} & \longrightarrow & \mathbb{F}_{p^n} \\ x & \longmapsto & f(x+a)+f(x). \end{array} \right.$$

Définition 14. Soit f une fonction de $\mathbb{F}_{p^n}$ dans $\mathbb{F}_{p^n}$. Pour tout a, $b \in \mathbb{F}_{p^n}$, on définit

$$\delta_f(a,b) = \#\{x \in \mathbb{F}_{p^n} | D_a f(x) = b\}$$

et

$$\delta(f) = \max_{a \neq 0, b \in \mathbb{F}_{p^n}} \delta_f(a,b).$$

Lorsque la caractéristique est supérieure à 2, il est possible d'avoir δ_f égal à 1. Les fonctions vérifiant cette valeur de δ sont appelées fonctions *Parfaitement Non-linéaires*, ou PN.
En caractéristique égale à 2, c'est à dire dans les $\mathbb{F}_{2^n}$, on a

$$D_a f(x) = f(x+a) + f(x) = D_a f(x+a)$$

car

$$\begin{aligned} D_a f(x+a) &= f(x+a+a) + f(x+a) \\ &= f(x+2a) + f(x+a) \\ &= f(x) + f(x+a) \\ &= D_a f(x) \end{aligned}$$

Ce résultat implique que $\delta(f)$ est supérieur ou égal à 2.
Les fonctions dites APN, pour *Almost Perfect Nonlinear*, sont les fonctions pour lesquelles cette borne est atteinte.

Proposition 13. *Soit f définie par la définition 13. La fonction f est APN si et seulement si le polynôme*

$$Q(X) = \frac{f(X)}{X^2} = \sum_{i=1}^{n-1} c_i x^{2^i - 1}, c_i \in \mathbb{F}_{2^n}$$

est un polynôme de permutation.

Démonstration. □

5.2.2 Les fonctions courbes

Autres que les fonctions APN, il existe également les fonctions courbes, importantes en cryptographie à clé secrète.

6 Applications en cryptanalyse

7 Applications dans d'autres domaines

Conclusion

Les rappels sur les corps finis étaient primordiaux . Il était nécessaire de bien définir l'environnement sur lequel nous allions travailler, d'être pourvu de bases solides, de manière à énoncer limpidement les premières définitions et propriétés des polynômes de permutations sur les corps finis. L'étude de ces polynômes est un vaste domaine des mathématiques. Il trouve de nombreuses applications, notamment en cryptologie. Nous avons ici tâché de nous en tenir aux points essentiels de leur étude, de manière à ne pas saturer notre travail d'informations superflues.

Il est fréquent qu'un polynôme de permutation présentant une apparence complexe, ne corresponde finalement qu'à une permutation simple. Et réciproquement, une permutation compliquée sera généralement « représentable » par un polynôme de permutation simple. En tant qu'étudiant en cryptologie, cela ne peut que nous ravir. L'implémentation en sera d'autant plus facile, et ainsi l'application en cryptologie.
Ceci nous a conduit, tout du long, à exhiber différents critères d'identifications et à implémenter certains d'entre eux. Ces derniers permettent de décider quels polynômes sont, ou non, de permutations ; et donc à fortiori d'en trouver de « bons » pour une application en cryptologie.
Notre principale préoccupation est de trouver des algorithmes déterministes efficaces. C'est à dire effectuant les calculs souhaités en un temps au plus polynomial. Notons toutefois que les algorithmes actuels commencent à donner des résultats en temps satisfaisant.

Références

[1] KEBLI Salima, Polynômes de permutation sur des corps finis et équations diophantiennes, Université d'Oran1 Ahmed Ben Bella, juin 2017.

[2] Yann Laigle-Chapuy, Polynômes de permutation et applications en cryptographie - Cryptanalyse de registres combinés, Université Pierre et Marie Curie, Paris VI, Décembre 2009.

[3] Wikipedia, https ://fr.wikipedia.org/wiki/Interpolation_lagrangienne

[4] Matsumoto-Imai Cryptosystems // Paragraphe 2.1 (page 12, ...)
https ://bilder.buecher.de/zusatz/20/20816/20816314_lese_1.pdf

[5] PATARIN Jacques, Cryptanalysis of the Matsumoto and Imai Public Key Scheme of Eurocrypt'88,
https ://link.springer.com/content/pdf/10.1007/3-540-44750-4_20.pdf