International Journal of Scientific and Innovative Mathematical Research(IJSIMR)
Volume 10, Issue 1, 2022, PP 1-12
ISSN No. (Online) 2347-3142
DOI: https://doi.org/10.20431/2347-3142.1001001
www.arcjournals.org

Cryptanalyse des fonctions à sens Unique Exponentielle Modulaire à l'aide des Bases de Gröbner

MAYALA LEMBA Francis[1], ENGOMBE NGONGO Josette[2], MAYALA NKUMBIEME Pélagie[3], MONGONDA MODJENGE John[4], ENGOMBE WEDI Boniface[1]

[1]*Département de Mathématique et Informatique, Université Pédagogique Nationale*

[2]*CRED, Université Pédagogique Nationale*

[3]*CRIDUPN, Université Pédagogique Nationale*

[4]*Institut Supérieur Pédagogique de la Gombe*

Corresponding Author:** ***MAYALA LEMBA Francis, *Département de Mathématique et Informatique, Université Pédagogique Nationale*

Resumé: *Cet article a pour but de présenter la Cryptanalyse des fonctions à sens unique exponentielle modulaire à l'aide des bases de Gröbner. En effet le problèmes calculatoirement difficile : « le problème de fonction à sens unique exponentielle modulaire, dont la réciproque est appelée logarithme discret [1], qui est à la base de l'échange de clef Diffie-Hellman et de cryptosystème El Gamal.*

Nous avons proposé une nouvelle approche innovante pour la résoudre, cette approche, consiste à trouver d'abord une méthode de paramétrisation, qui traduit une fonction exponentielle modulaire à un système d'équations polynomiales soluble par les bases de Gröbner afin de trouver toutes les solutions entières possibles du système d'équations.

Mots clé: *Bases de Gröbner, Cryptanalyse, Cryptosystème, El Gamal, Calculatoirement difficile, fonction à sens unique, système d'équations.*

1. INTRODUCTION

La cryptologie, science du secret englobant la cryptographie (écriture secrète) et la cryptanalyse (étude des attaques contre les mécanismes de cryptographie) [2] a connu, au cours du vingtième siècle (plus précisément, au milieu des années 1970), une révolution paradigmatique profonde.

C'est dans les années 1970 qu'émerge pour la première fois le concept de cryptographie à clef publique, permettant de s'affranchir du délicat problème de la distribution de clefs. L'article fondateur de Diffie et Hellman [3], basé sur des idées de Merkle [22], introduit la notion de fonction à sens unique qui est au cœur de ce nouveau paradigme cryptographique.

Les fonctions à sens unique sont des situations mathématiques asymétriques. En d'autres termes, étant donnée une fonction f, il est possible connaissant x de calculer « facilement » $f(x)$; mais connaissant un élément de l'ensemble image de f, il est « difficile » ou impossible de trouver son antécédent.

Une fonction à sens unique (ou bien one-way function, en anglais) est une fonction qui peut être aisément calculée, mais qui est difficile à inverser. En d'autres termes, une fois une image Inf d'une fonction f est donnée, il est difficile de lui trouver un antécédent.

En dépit de réelles avancées technologiques, le problème de fonctions à sens unique modulaire consiste à trouver, en temps raisonnable, la résolution du problème de logarithmes discrets (en anglais Discrete Logarithm Problem, DLP). Il reste, aujourd'hui encore, un problème ouvert, quoiqu'il ait suscité l'intérêt des chercheurs, néophytes ou savants, depuis des siècles, voire des millénaires.

De ce qui précède, des questions méritent d'être posées et étudiées avec une attention toute particulière : Est-il possible de résoudre le problème les fonctions à sens unique exponentielle modulaire à l'aide de Bases de Gröbner ? Comment faire pour avoir un système d'équations polynomial soluble par les bases de Gröbner ?

Compte tenu de la problématique qui précède, nous avons utilisé la méthode de paramétrisation, qui traduit une fonction à sens unique modulaire à un système d'équations polynomiales solubles à l'aide

de la méthode de bases de Gröbner[1], pour nous permettre d'avoir la base ou le générateur g (premier résultat) et aussi toutes les solutions entières possibles de la classe d'équivalence de cette fonction.

Le problème fondamental de bases de Gröbner est de chercher les solutions d'un système d'équations algébriques : $\begin{cases} f_1(x_1, \dots, x_n) = 0 \\ \dots \\ f_m(x_1, \dots, x_n) = 0 \end{cases}$

où, les polynômes $f_1, \dots, f_m$ sont des polynômes en les variables $x_1, \dots, x_n$ et à coefficients dans un corps $\mathbb{K}$ dans lequel on sait calculer (par exemple $\mathbb{Q}$ ou $\mathbb{F}_p$). Lorsque $\mathbb{K} = \mathbb{F}_p$ les méthodes proposées sont souvent sans équivalent [4].

Tout au long de cet exercice, notre article vise les objectifs suivants : de retrouver la valeur de x de la fonction à sens unique exponentielle modulaire, à l'aide de l'algorithme de Buchberger en déterminant les bases de Gröbner, de déterminer toutes les solutions entières possibles de la fonction (sans avoir une fonction à sens unique avec trappe secrète).

Comme l'indique le titre, notre étude s'intéresse aux techniques Cryptanalyse des fonctions à sens unique exponentielle modulaire à l'aide des bases de Gröbner.

Nous avons utilisé la méthode de bases de Gröbner pour la résolution des systèmes d'équations polynomiaux en utilisant l'algorithme de Buchberger ; ensuite, nous avons illustré le cas de ElGamal.

Dans les lignes qui suivent nous allons présenter la cryptanalyse à de la fonction à sens unique exponentielle modulaire, c'est-à-dire la théorie des attaques de la cryptographie à clef publique.

2. FONCTION A SENS UNIQUE ET A BRECHE SECRETE [5, 3]

2.1. Introduction

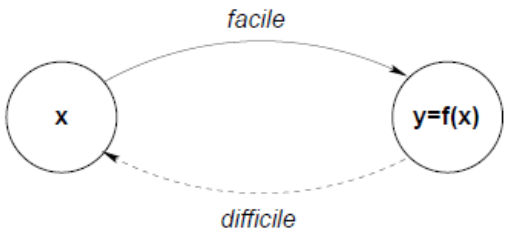
Les fonctions à sens unique (ou one-way function en anglais) constituent le socle sur lequel repose pour l'essentiel l'édifice de la cryptographie théorique. De façon informelle, une fonction est à sens unique si les valeurs des images sont efficacement calculables, mais, étant donnée une valeur, il est pratiquement impossible de trouver un antécédent qui a cette valeur pour image.

Cette propriété énoncée ainsi de façon informelle est celle qui est attendue en pratique, mais cette définition s'avère insuffisante pour faire opérer cette notion dans des cas concrets. Une formalisation est nécessaire [5].

Les notions de fonction à sens unique et de fonction à brèche secrète sont au cœur de la cryptographie à clé publique et on définit dans cette partie les notions de fonction à sens unique et de fonction à trappe qui proviennent de la théorie de la complexité [6, 7]. Les fonctions à sens unique sont des éléments de base de la plupart des protocoles cryptographique.

2.2. Fonction à sens unique

Considérons deux ensembles arbitraires X et Y et une fonction $f: X \to Y$. Soit $f(X)$ l'ensemble image de X par f. La fonction f est dite à sens unique si pour tout x de X, il est facile de calculer $f(x)$ (autrement dit, f peu être calculée en temps polynomial) et s'il est difficile de trouver, pour la plupart des $y \in f(X)$ un $x \in X$ tel que $f(x) = y$ (en d'autres termes ce dernier problème doit être dans la classe NP voire NP-complet) [8].



[1] Les bases de Gröbner constituent un outil important pour la résolution de systèmes algébriques, et leur calcul est souvent la partie difficile de la résolution. Elles servent par exemple à résoudre le problème Ideal Membership (d'appartenance à un idéal), est un problème EXPSPACE-complet. La complexité du calcul de base de Gröbner dans le cas le pire est $2^{2^{O(n)}}$ (où n est le nombre de variables), mais pour des systèmes possédant un nombre fini de solutions, la complexité n'est plus que simplement exponentielle : $D^{O(n^2)}$ (où D est le maximum des degrés des polynômes engendrant l'idéal).

Principe d'une fonction à sens unique (Dumas J-G., 2007)

2.3. Importance des fonctions à sens unique

Les fonctions à sens unique ne peuvent pas servir telles quelles de système de chiffrement en utilisant $f(M)$ pour chiffrer M puisque même le destinataire légal ne serait pas en mesure de déchiffrer le cryptogramme. En d'autres termes on ne peut pas les utiliser telles quelles pour le chiffrement. Un message chiffré à l'aide d'une fonction à sens unique n'est pas d'une utilité : personne ne peut le déchiffrer à un temps raisonnable. Pour la cryptographie à clé publique, nous avons besoin de ce que l'on appelle une fonction à sens unique à brèche secrète [9].

2.4. Fonction à sens unique trapdoor

La notion de fonction à sens unique à trappe est d'une utilité plus immédiate pour la cryptographie à clé publique.

Soit (f_r) une suite d'applications à sens unique, on dit que cette suite est munie d'une trappe ou qu'elle est trapdoor si pour tout r la connaissance d'un « secret » (une donnée mathématique supplémentaire) permet d'inverser la fonction f_r avec un nombre de calculs polynomial en r.

Une conséquence des définitions c'est que la donnée de f ne doit pas permettre de calculer le « secret » avec un nombre de calculs polynomial en r, sinon f ne serait plus à sens unique [10].

En d'autres termes, il est facile de calculer $f(x)$ étant donné x et difficile de calculer x étant donné $f(x)$. Toutefois, il existe une information secrète, y, il est facile de calculer x.

Une montre est un bon exemple de fonction à sens unique à brèche secrète. Il est facile de démonter une montre mécanique en ses centaines de pièces. Il est très difficile de remettre les pièces ensemble pour reconstruire une montre qui fonctionne. Toutefois, grâce à l'information secrète que constitue le plan de montage de la montre, il est bien plus facile de reconstruire la montre [11]. (pas pour un spécialiste de la marque ou un réparateur expérimenté)

Un important cas spécial d'exponentiation modulaire se produit lorsque l'exposant est 2 et que le module est d'une forme particulière. Ce deuxième exemple de candidat au titre de fonction à brèche secrète requiert un peu de théorie des nombres pour être compris. Nous dirons qu'un entier $n = pq$ est un entier de Blurn, s'il est le produit de deux nombres premiers p et q distincts, (exemple 391=17x23), qui sont tous deux congrus à 3 modulo 4. Soit $\mathbb{Z}_n^*$ l'ensemble des entiers compris entre 1 et $n - 1$ qui ne sont ni divisibles par p ni par q. On note par RQn le sous-ensemble de $\mathbb{Z}_n^*$ constitué des nombres qui sont des carrés parfaits modulo n. Les éléments de RQn sont appelés résidus quadratiques modulo n.

À titre d'exemple, soient $p = 19$ et $q = 23$, et donc $n = 437$. Dans ce cas, 135 et 139 appartiennent à $\mathbb{Z}_n^*$, mais pas 133 (puisque 133 = 19 x 7). De plus, 135 n'est pas un résidu quadratique modulo 437 puisqu'il n'existe pas d'entier a tel que $a^2 = 135\ mod\ 437$, alors que 139 en est un puisque $24^2 = 576 = 139\ mod\ 437$.

Énonçons quelques théorèmes pertinents sans les démontrer. Le nombre d'éléments dans $\mathbb{Z}_n^*$ est $(p-1)(q-1)$ et exactement le quart d'entre eux sont des résidus quadratiques. Chaque résidu quadratique possède exactement quatre racines réelles distinctes dans $\mathbb{Z}_n^*$ et une seule d'entre elles est elle-même un résidu quadratique. Nous appellerons cette racine carrée particulière la racine carrée principale. Dans notre exemple, 24 est la racine carrée principale de 139 modulo 437, et les trois autres racines carrées sont 185, 252 et 413. La signification cryptographique est que la capacité d'extraire des racines carrées est algorithmiquement équivalente à la capacité de factoriser n. En d'autres mots, celui qui connaît les facteurs de n peut calculer efficacement des racines principales modulo n, alors que de tels calculs sont aussi difficiles que factoriser n pour celui qui en ignore les facteurs.

Notre deuxième candidat au titre de fonction à brèche secrète devrait maintenant être évident. Quelqu'un choisit p et q au hasard et calcule $n = pq$ qu'il rend public. À partir de n, n'importe qui peut calculer efficacement des carrés modulo n, mais seul notre ami peut facilement inverser cette opération (en supposant que la factorisation de n soit difficile). Dans cet exemple, n est l'information publique et sa factorisation est la brèche secrète [7].Mathématiquement nous illustrons la construction d'un système de chiffrement à clé publique au moyen d'un problème NP-complet[2], celui du sac à dos que l'on peut

[2] Les problèmes NP-complets forment une classe de problèmes pour lesquels aucun algorithme de temps de calcul polynomial n'est connu.

lire dans [11]. Il s'agit du chiffre de Merkle-Hellman, qui a été publié presque en même temps que RSA que nous présenterons plus loin.

2.5. Application [12]

Supposons qu'Alice dispose d'une fonction $f: I_r \to I_r$ à sens unique munie d'une trappe, elle la rend publique (sur sa page web par exemple). Par la suite, si Bob veut lui envoyer un message $m \in I_r$ de façon sûre, il calcule $f(m)$ et l'envoie à Alice. La fonction f joue le rôle du coffre-fort évoqué en introduction, car Alice est la seule qui peut trouver un antécédent de $f(m)$.

Pour qu'Alice soit sûre de trouver m, et ainsi déchiffrer le message de Bob, il faut que $f(m)$ ait un seul antécédent (qui est donc m), cette condition sera remplie si la fonction f est bijective.

Par conséquent, si nous disposons d'un moyen de construire des bijections à sens unique munies d'une trappe (permutations one-way, trapdoor), alors il est aisé de faire de la cryptographie à clé publique.

3. FONCTION EXPONENTIELLE ET LOGARITHME DISCRET

3.1. Exponentiation Modulaire

L'exponentiation modulaire, appelée aussi exponentielle discrète, est une fonction à sens unique est définie par :

$$f: \begin{vmatrix} \mathbb{Z}_p^* \to \mathbb{Z}_p^* \\ x \to \alpha^x \end{vmatrix}$$

où α est choisi de préférence primitif pour que f soit bijective. Tous les algorithmes connus pour inverser cette fonction, nécessitent un temps de calcul non polynomial en $log(p)$ [13].

3.2. Logarithme Discret

Si l'on veut rester très général, le problème du logarithme discret peut se formuler dans n'importe quel groupe. Soit G un groupe cyclique de cardinal n que l'on note multiplicativement. Le logarithme discret d'un élément se définit comme suit.

(Logarithme discret). Soit g un générateur de G et a un élément de G. On appelle logarithme discret en base g de a, l'unique élément x de $\mathbb{Z}/n\mathbb{Z}$ tel que : $g^x = a$.

Souvent, on considérera le logarithme discret de a comme étant l'unique représentant entier de x dans $[0 \dots n-1]$, mais il est capital de garder a` l'esprit le fait que ce logarithme n'est réellement défini que modulo $n = \#G$.

Le problème du calcul du logarithme discret (que l'on note DL en abrégé) est un problème généralement difficile (plus ou moins en fonction du groupe G). Dans de nombreuses situations, cela permet de fabriquer des cryptosystèmes, car cette asymétrie entre le problème du calcul du logarithme (difficile), et celui du calcul des puissances (facile) est propice pour la cryptographie. Diffie et Hellman [3] ont été les premiers à bâtir un cryptosystème à partir de cette situation.

3.3. Les Algorithmes Exponentiels

Parmi les algorithmes permettant de résoudre le problème du logarithme discret sur un groupe fini G de cardinal n, on trouve d'abord les algorithmes exponentiels (en $log\, n$), ayant plus exactement une complexité en $\mathcal{O}(\sqrt{n})$. Le point intéressant est que de tels algorithmes existent pour n'importe quel groupe G, pourvu qu'il satisfasse aux hypothèses minimales suivantes (ces hypothèses correspondent à la notion de groupe générique, au sens de [14, 15].

3.4. Définition (Groupe générique)

Pour un groupe fini G de cardinal n, on fait les hypothèses minimales suivantes. On suppose qu'il existe un entier $\alpha \geq 0$ tel que :

- Les éléments de G sont représentés de façon unique sur $\mathcal{O}((\log n)^\alpha)$ bits.
- Les opérations dans le groupe G (multiplication, inversion) se calculent en $\mathcal{O}((\log n)^\alpha)$.
- Le cardinal du groupe G est connu.

Cette hypothèse n'est pas tout à fait anodine. Elle est néanmoins satisfaite pour l'immense majorité des groupes rencontrés en cryptologie (à l'exception possible des groupes de tresses).

Dans bien des cas la valeur minimale possible de α est différente dans les deux conditions mentionnées ci-dessus.

Dans les lignes qui suivent, nous allons parler des bases de Gröbner, mettre en exergue le bénéfice que peut procurer.

4. BASES DE GRÖBNER

Dans ce point, nous commençons par préciser quelques définitions.

4.1. Définition

Soit $I \subset \mathbb{K}[x_1, \dots, x_n]$ un idéal non trivial. Alors

a. On note par $LT(I)$ l'ensemble de tous les termes dominants des éléments de I ; c'est-à-dire

$$LT(I) = \{cx^{\alpha}, f \in I \quad avec\ LT(f) = cx^{\alpha}\}$$

b. On note par $\langle LT(I)\rangle$ l'idéal engendré par les éléments de $LT(I)$.

Rappelons que si I est un idéal d'un anneau A donné, on dit que I est généré par $a_1, \dots, a_s$ si chaque élément a de I est une combinaison dans A des éléments a_i, c'est-à-dire si

$$I = \left\{\sum_{i=1}^{s} \alpha_i a_i,\ \alpha_i \in A\ \forall\ i \in \{1, 2, \dots, s\}\right\}$$

Dans ce cas on écrit $I = \langle a_1, \dots, a_s\rangle$ et on dit aussi que I est finiment engendré, pour simplement dire que I est engendré par un nombre fini d'éléments. L'ensemble $\{a_1, \dots, a_s\}$ est appelée base (ou génératrice) de l'idéal I. Remarquons que dans le cas de $\mathbb{K}[x_1, \dots, x_n]$, pour I = $\langle f_1, \dots, f_s\rangle$, on n'a pas nécessairement $< LT(I)> = \langle LT(f_1), \dots, LT(f_s)\rangle$; c'est le théorème de Dickson [16, 17] qui garantit, que l'idéal $< LT(I) >$ est finiment engendré, c'est-à-dire il existe $g_1, g_2, \dots, g_t \in I$ tels que $\langle LT(I)\rangle = \langle LT(g_1), \dots, LT(g_t)\rangle$.

Pour ainsi dire, $\langle LT(I)\rangle$ admet toujours une base. La question d'existence d'une base pour toute idéal (I $\subset \mathbb{K}[x_1, \dots, x_n]$) non triviale est garantie par le théorème de base de Hilbert [18] : tout idéal $I \subset \mathbb{K}[x_1, \dots, x_n]$ est finiment engendré, c'est-à-dire il existe $g_1, \dots, g_t \in I$ tels que $I = \langle g_1, \dots, g_t\rangle$.

4.2. Définition (Base de Gröbner)

Fixons-nous un ordre monômial $>$ et un idéal $I \subset \mathbb{K}[x_1, \dots, x_n]$. Un sous-ensemble fini $G = \{g_1, \dots, g_t\}$ de I est dit base de Groebner de I si

$\langle LT(g_1), \dots, LT(g_t)\rangle = \langle LT(I)\rangle$

De manière équivalente, $G = \{g_1, \dots, g_t\} \subset I$ est une base de Groebner de I si, et seulement si le terme dominant de tout élément de I est divisible par un des $LT(g_i)$, c'est-à-dire G base de Groebner si pour tout $f \in I$, il existe $j \in \{1, 2, \dots, t\}$ tel que $LT(g_j)$ divise $LT(f)$.

On va continuer dans le reste de cette section à calculer les bases de Groebner de certains idéaux et dans la prochaine à en illustrer quelques applications. On doit noter que tout idéal de $\mathbb{K}[x_1, \dots, x_n]$ admet une base de Gröbner (selon le théorème de Dickson [16, 17]) et inversement une base de Gröbner pour un idéal de $\mathbb{K}[x_1, \dots, x_n]$ est aussi une base de celui-ci [16, 17].

4.3. Exemples

1) Soit l'idéal $I = \langle f_1, f_2\rangle = \langle x^3 - 2xy, x^2y - 2y^2 + x\rangle \subset [x, y]$. On se propose de déterminer la base de Gröbner de I. Donnons-nous l'ordre $>_{grevlex}$. L'ensemble $\{f_1, f_2\}$ n'est pas une base de Gröbner de I. En effet, avec cet ordre on a $LT(f_2) = x^2y$ donc $\langle LT(f_1), LT(f_2)\rangle = \langle x^3, x^2y\rangle$. Aussi, $LT(f_1) = x^3 \in \langle LT(I)\rangle$ par définition mais $x^3 \notin \langle LT(f_1), LT(f_2)\rangle$ puisque x^2y ne divise x^3.

2) Cependant, si $I = \langle x + z, y - z\rangle$, alors $G = \{g_1, g_2\} = \{x + z, y - z\}$ est une base de Gröbner de I suivant l'ordre $>_{lex}$. En effet, $LT(g_1) = x$ et $LT(g_2) = y$ tous deux appartiennent à $\langle LT(g_1), LT(g_2)\rangle = \langle x, y\rangle$.

On résume dans la proposition ci-dessous les propriétés de bases de Gröbner.

4.4. Proposition

Soit $G = \{g_1, \dots, g_t\}$ une base de Gröbner d'un idéal $I \subset \mathbb{K}[x_1, \dots, x_n]$ et $f \in \mathbb{K}[x_1, \dots, x_n]$ et Alors il existe un et un seul $r \in \mathbb{K}[x_1, \dots, x_n]$ tel que

[1] Aucun de $LT(g_i)$ ne divise aucun terme de r.

[2] Il existe $g \in I$ tel que $f = g + r$.

Le polynôme r est en particulier le reste de la division de f par G.

Démonstration. La division de f par G permet d'écrire $f = a_1 g_1 + \cdots + a_t g_{t,} + r,$ où r est le reste et satisfait (i).

De même (ii) est satisfait en prenant $g = a_1 g_1 + \cdots + a_t g_t \in I$ comme I est un idéal dans $\mathbb{K}[x_1, \ldots, x_n]$.

4.5. Corollaire

Soit $G = \{g_1, \ldots, g_t\}$ une basse de Gröbner pour un ideal $I \subset \mathbb{K}[x_1, \ldots, x_n]$ et $f \in \mathbb{K}[x_1, \ldots, x_n]$. Alors $f \in I$ si et seulement si le reste de la division de f par G est nul.

Démonstration. La preuve est immédiate. En effet, si le reste de la division de f par G est nul, alors $f = a_1 g_1 + \cdots + a_t g_t + 0$ soit $f = a_1 g_1 + \cdots + a_t g_t$, donc $f \in I$. Inversement si $f \in I$, alors $f = f + 0$ qui satisfait les conditions de la proposition précédente Donc le reste de la division de f par G est nul.

4.6. Définition (Polynôme S)

Soient $f, g \in \mathbb{K}[x_1, \ldots, x_n]$ deux polynômes tels que $miltideg(f) = \alpha$ et $miltideg(f) = \beta$ et $\gamma = (\gamma_1, \ldots, \gamma_n)$ avec $\gamma_i = max\{\alpha_i, \beta_i\}$ pour tout i. Le polynôme S de f et g est la combinaison définie par

$$S(f, g) = \frac{x^\gamma}{LT(f)}.f - \frac{x^\gamma}{LT(g)}.g$$

Par exemple, soit $f = x^3y^2 + x^2y^3 + x$ et $g = 3x^4y + y \in \mathbb{R}[x, y]$ avec l'ordre $>_{grevlex}$. Alors on a $\alpha = (3, 2), \beta = (4, 1)$ de sorte que $\gamma = (max\{3, 4\}, max\{2, 1\}) = (4, 2)$. Donc

$$S(f, g) = \frac{x^4y^2}{x^3y^2}.f - \frac{x^4y^2}{3x^3y}.g$$

$$= x.f - \frac{1}{3}.y.g$$

$$= x^3y^3 + x^2 - \frac{1}{3}.y^3$$

Le polynôme S sert de test pour la détermination des bases de Gröbner comme l'indique le théorème suivant dont on renvois la preuve à [16, 17].

4.7. Théorème (Critère de Buchberger)

Soit I un idéal non trivial de $\mathbb{K}[x_1, \ldots, x_n]$ et $G = \{g_1, \ldots, g_t\} \subset I$. G est une base de Gröbner pour I si et seulement pour toute paire i, j telle que $i \neq j$ le reste de la division de $S(g_i, g_j)$ par G est nul (pour un certain ordre donné).

En guise d'exemple, considérons l'idéal $I = \langle y - x^2, z - x \rangle$ de $\mathbb{R}[x, y, z]$. Alors $G = \{y - x^2, z - x^3\}$ est une basse de Gröbner de I pour l'ordre $y > z > x$. En effet, on calcule $S(f, g)$ et on obtient :

$$S(y - x^2, z - x^3) = \frac{yz}{y}(y - x^2) - \frac{yz}{y}(z - x^3) = -zx^2 + yx^3$$

L'algorithme de la division de $S(y - x^2, z - x^3)$ permet d'obtenir

$$S(y - x^2, z - x^3) = x^3.(y - x^2) + (-x^2).(z - x^3) + 0.$$

Ce qui établit que le reste de la division de $S(y - x^2, z - x^3)$ par G est nul ; donc G est une base de Gröbner de I.

On doit faire remarquer que la détermination d'une base de Gröbner pour un idéal est un problème difficile. L'algorithme de Buchberger va permettre de déterminer les bases de Gröbner mais la complexité reste aussi prépondérante pour des calculs analytiques efficaces que l'on est souvent appelé à faire recours aux programmes informatiques pour cette tâche, notamment les logiciels Sage, Mathematical ou Maple qui disposent de paquets implémentant l'algorithme de Buchberger et d'autres. Le moteur de recherche Wolfram/Alpha reste aussi un outil important dans ce sens et fournit amples détails (Wolfram/Alpha, 2022).

Terminons cette section par donner le théorème de Buchberger qui indique que l'on peut calculer une base de Gröbner pour un idéal en un nombre fini d'étapes. Pour la preuve, on recourt à [18, 16].

4.8. Théorème (Buchberger)

Soit $I = \langle f_1, \dots, f_s \rangle$ un idéal non trivial de $\mathbb{K}[x_1, \dots, x_n]$. Alors la base de Gröbner de I peut être construite en un nombre fini d'étapes.

Pour produire une base de Gröbner pour un idéal $I =< f_1, \dots, f_s > \subset \mathbb{K}[x_1, \dots, x_n]$, on se sert essentiellement du critère de Buchberger. L'idée est d'atteindre l'ensemble générateur de I par adjonction des polynômes de I. Plus précisément, on ajoute les restes non nuls de la division des polynômes $S(f_i, f_j)$ de deux polynômes distincts de I par l'ensemble générateur.

Illustrons cela par un exemple suivant l'ordre $>_{grevlex}$. Précisons d'abord cette notation empruntée de [18]. Si $F = \{f_1, f_2 \dots, f_s\}$ est un ensemble des polynômes dans $\mathbb{K}[x_1, \dots, x_n]$, pour tout $i \neq j$ on notera

$$\overline{S(f_i, f_j)}^F$$

le reste de la division de $S(f_i, f_j)$ par les polynômes $f_1, f_2, \dots, f_s$ de F.

Soit maintenant l'idéal $I = \langle f_1, f_2 \rangle$. Le calcul de $S(f_1, f_2)$ donné par $S(f_1, f_2) = -x^2 \in I$ et le reste de la division de $S(f_1, f_2)$ par $F = \{f_1, f_2\}$ est $-x^2$ qui n'est pas non nul. Donc on ajoute $f_3 = -x^2$ à $F = \{f_1, f_2\}$ de sorte que l'on ait $F = \{f_1, f_2, f_3\}$. On teste si cet ensemble est une base de Gröbner en utilisant le critère de Buchberger. On calcule :

$S(f_1, f_2) = f_3$ donc

$\overline{S(f_1, f_3)}^F = 0$

$S(f_1, f_3) = (x^3 - 2xy) - (-x)(-x^2) = -2xy,$ et

$\overline{S(f_1, f_3)}^F = -2xy \neq 0$

On pose dans ce cas $f_4 = -2xy$ et l'ajoute dans l'ensemble générateur. Ainsi on a $F = \{f_1, f_2, f_3, f_4\}$. En continuant ainsi, nous avons :

$\overline{S(f_1, f_2)}^F = \overline{S(f_1, f_3)}^F = 0$

$S(f_1, f_4) = y(x^3 - 2xy) - (-1)x^2(-2xy) = -2xy^2 = yf_4,$ donc

$\overline{S(f_1, f_4)}^F = 0,$

$S(f_2, f_3) = (x^2y - 2y^2 + x) - (-y)(-x^2) = -2xy^2 + x,$ mais

$\overline{S(f_2, f_3)}^F = -2y^2 + x \neq 0.$

Comme le dernier reste n'est pas nul, on pose $f_4 = -2y^2 + x$ et l'ajoute dans l'ensemble générateur. On pose $F = \{f_1, f_2, \dots, f_5\}$. On peut montrer que

$$\overline{S(f_i, f_j)}^F = 0 \qquad \forall\, 1 \leq i, j \leq 5$$

Par le critère de Buchberger, on obtient une base de Gröbner suivant l'ordre $>_{grevlex}$ pour l'idéal I. Elle est donnée par

$$G = \{f_1, f_2, f_3, f_4, f_5\} = \{x^3 - 2xy, x^2y - 2y^2 + x, -x^2, -2xy, -2y^2 + x\}$$

On voit clairement que la base de Gröbner construite ainsi, en suivant cette démarche, à partir de l'ensemble générateur de I, contient toujours F.

4.9. Résolutions des équations polynomiales

Considérons le système

$$f_i(x_1, x_2, \dots, x_s) = 0, \quad i = 1, \dots, n.$$

Soit $I = \langle f_1, f_2, \dots, f_s \rangle$ l'idéal engendré par les polynômes fi de ce système. Résoudre ce système consiste à trouver tous les points de la variété affine $\mathbb{V}(I)$. On a vu que $\mathbb{V}(I) = I$ et on peut déterminer

cette variété à l'aide de toute base de I. Si l'ensemble générateur de I n'est pas une base de Gröbner, on détermine la base de Gröbner pour cet idéal qui va permettre de résoudre ce système.

Illustrons cela par des exemples.

1. Considérons les équations suivantes

$x^2 + y^2 + z^2 = 1$

$x^2 + z^2 = y$

$x = z$

dans $\mathbb{C}^3$. Ces équations génèrent l'idéal $I = \langle x^2 + y^2 + z^2 - 1,\ x^2 + z^2 - y, x - z\rangle \subset \mathbb{C}[x, y, z]$. Résoudre ce système se réduit alors de trouver tous les points de la variété $\mathbb{V}(I)$. On peut calculer $\mathbb{V}(I)$ dans n'importe quelle base de I. On utilise le moteur Wolfram/ Alpha, on obtient

$g_1 = x - z$

$g_2 = y - 2z^2 = 0$

$g_3 = 4z^2 + 2z^2 - 1 = 0$

Donc la résolution du système $g_i = 0$ pour tout $i \in \{1, 2, 3\}$ permet de calculer $\mathbb{V}(I)$, car $I = \langle g_1, g_2, g_3\rangle$. La dernière équation est une équation polynômiale d'une seule variable, z, que l'on peut résoudre. La résolution de

$4z^2 + 2z^2 - 1 = 0$

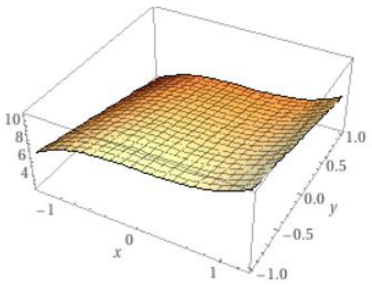
fournit

$$z \pm \frac{1}{2}\sqrt{\pm\sqrt{5} - 1}$$

Avec cette solution, on obtient tous les points de notre variété affine vu que $\mathbb{V}(I) = \mathbb{V}(g_1, g_2, g_3)$, donc les solutions de notre système.

2. Soit l'équation $x^3 - 2y + 7 = 0$ dans $\mathbb{R}[x, y]$ qui représente une courbe de niveau d'une surface dans l'espace affine $\mathbb{R}^2$. On peut également utiliser les bases de Gröbner pour résoudre cette équation, c'est-à-dire trouver toutes les solutions de cette équation.

Au polynôme $f(x, y) = x^3 - 2y + 7$ est associée un objet géométrique, une surface dans l'espace affine $\mathbb{R}^2$ comme le montre cette figure :



Le point (3, 10) est un point de cette variété, car $3^3 - 2 * 10 - 7 = 0$.

On va paramétrer cette surface. On pose, par exemple, $x = t + 1$. Alors on obtient le système

$f(x, y, z) \equiv t - x - 1 = 0$

$g(x, y, z) \equiv t^3 + 3t^2 + 3t - 2y - 6 = 0$

qui est un système d'équations polynômes dans $\mathbb{Z}[x, y, t]$. Soit $I = \langle f, g\rangle$ l'idéal de $\mathbb{Z}[t, x, y]$ engendré par f et g pour lequel on peut déterminer une base de Groebner. Le moteur Wolfram/Alpha fournit [19] :

Integer root

$$t = 2n, \quad x = 2n+1, \quad y = 4n^3 + 6n^2 + 3n - 3, \quad n \in \mathbb{Z}$$

Ce point avait comme but de fournir au lecteur le bagage mathématique nécessaire pour mieux scruter la quintessence de base de l'algèbre sur méthodes de bases de Gröbner et le point suivant, constituera une contribution, et se focalisera sur une attaque du cryptosystème à publique basé sur les fonctions à sens uniques modulaire exponentielle.

5. ATTAQUES CRYPTOGRAPHIQUES

5.1. Introduction

Dans ce point, nous allons présenter notre technique de cryptanalyse. L'hypothèse généralement à fournir est que l'opposant, Oscar, connaît le système cryptographique utilisé. Ceci est appelé le principe de Kerckhoff [20]. Bien sûr, si Oscar ne connaît pas le procédé employé, sa tâche sera bien plus difficile, mais on ne souhaite pas baser la sécurité du système sur la protection (sans doute incertaine) de la description des fonctions cryptographiques. Le but est donc d'étudier les systèmes cryptographiques suivant le principe de Kerckhoff.

Une attaque évidente du chiffrement à clé publique basé sur les fonctions à sens uniques exponentielles modulaires, dont la réciproque est appelée logarithme discret consiste à tenter de résoudre le problème de logarithme discret basé sur le cryptosystème El Gamal.

5.2. Recherche de toutes les solutions entières à l'aide Bases de Gröbner

5.2.1. Méthode de paramétrage

Soit la fonction $f: x \to x^p \ (mod\ n)$.

Par définition d'équivalence (Jeanneret A., Lines D., 2008)

$f: x \to x^p \ (mod\ n)$

$x^p \equiv i \ (mod\ n)$

$\Leftrightarrow x^p = i + nk \ \ o\grave{u}\ k \in \mathbb{Z}$

$\Longrightarrow x^p - i - nk = 0$

Posons $x = y + a, \forall a \neq 0 \in \mathbb{Z}$

Nous avons

$(y + a)^p - i - nk = 0 \quad (*)$

or

$$(y+a)^p = \sum_{j}^{p} \binom{j}{p} y^{p-j} a^j$$

$$= \binom{o}{p} y^p a^0 + \binom{1}{p} y^{p-1} a^1 + \cdots + \binom{p}{p} y^0 a^p$$

$$= y^p + pay^{p-1} + \cdots + a^p$$

Donc notre $(*)$ polynôme devient :

$y^p + pay^{p-1} + \cdots + a^p - i - nk = 0$

Nous avons donc un système d'équations polynomiales

$$\begin{cases} x - y - a = 0 \\ y^p + pay^{p-1} + \cdots + a^p - i - nk = 0 \end{cases}$$

5.2.2. Algorithme de Buchberger

En appliquant l'Algorithme de Buchberger [21].

Input : F un ensemble fini de P
Résultat : une base de Gröbner pour l'idéal I
Engendré par F

Begin

$G \leftarrow F$;

$G_2 \leftarrow F$;

while $G_2 \neq G$ do

$G_2 \leftarrow G$

for $f, g \in G_2 \times G_2$ do

if $LM(f) < LM(g)$ then

$\bar{s} \leftarrow \overline{S(f,g)}^G$;

if $\bar{s} \neq 0$ then

Add $\bar{s}$ to G

return G ;

Exactitude et résiliation

1. A chaque étape de l'algorithme, $G \subset I$ et $\langle G \rangle = I$ tiennent.

2. Si $G_2 = G$ donc $\overline{S(f,g)}^G = 0$ pour tout $f, g \in G$et, selon le critère de Buchberger G est une base de Gröbner.

3. L'égalité $G_2 = G$ se fait en un nombre fini d'étapes puisque les idéaux $\langle LM(G) \rangle$, dans les itérations de la boucle, forment une chaîne ascendante. Cette chaîne d'idéaux se stabilise après un nombre fini d'itérations et à ce moment $\langle LM(G) \rangle = \langle LM(G_2) \rangle$ tient ce qui implique $G_2 = G$.

on obtient une base de Gröbner et toutes les solutions entières qui représente les classes d'équivalence $(nk + b)$.

5.2.3. Preuve (Exemple de l'attaque de la fonction à sens unique par la méthode une approche innovante)

Prenons par exemple le cas de la fonction f suivante :

$f: x \to x^3 \ (mod\ 100)$.

Tentons de résoudre le problème suivant : trouver x tel que $x^3 \equiv 11(mod\ 100)$. On a pour cela :

$x^3 \equiv 11(mod\ 100) \Longrightarrow x^3 = 11 + 100y \Longrightarrow x^3 - 100y - 11 = 0\ (*)$

Posons $x = z + 1$ $(2*)$,

Nous avons $x^3 = (z+1)^3 = z^3 + 3z^2 + 3z + 1$

Donc l'équation $(*)$ devient

$z^3 + 3z^2 + 3z + 1 - 100y - 11 = 0$

$\Longrightarrow z^3 + 3z^2 + 3z + 100y - 10 = 0$ $(3*)$

De $(2*)$ et $(3*)$ nous avons donc le système d'équations polynomiales

$$\begin{cases} x - z - 1 = 0 \\ z^3 + 3z^2 + 3z + 100y - 10 = 0 \end{cases}$$

qui peut être résolu par la méthode de base de Gröbner.

La résolution de ce système en s'aidant du moteur de calcul formel WolframAlpha (Arnault F., 2002) permet d'obtenir

$G = \{100y - z^3 - 3z^2 - 3z + 10, x - z - 1\}$

qui est la base de Gröbner engendré par les polynômes formant ce système et la résolution par ce même moteur fournit toutes les solutions entières de notre système, à savoir :

$x = 100n + 71, y = 10000n^3 + 21300n^2 + 15123n + 3579, z = 1OOn + 70.$

On en déduit la solution de l'équation $(*), x = 100n + 71$ qui n'est rien d'autre que la classe d'équivalence $\overline{71}$ modulo 100.

Ce point était consacré essentiellement sur la cryptanalyse d'un crytosystème à clé publique basée sur les fonctions à sens unique exponentielle.

6. CONCLUSION

Cet article présente la réflexion que nous avons menée autour des attaques de fonctions à sens unique exponentielle modulaire, dont la réciproque est appelée logarithme discret. Bien que ce domaine de recherche soit très spécifique, son étude complète requiert néanmoins des compétences dans des disciplines variées de la mathématique comme la théorie algébrique des nombres et de l'informatique.

Outre sa pluridisciplinarité, le domaine des attaques répond à un réel besoin industriel. Dans l'industrie des cartes à puce, ces attaques sont considérées comme une menace réelle, et protéger les cartes contre les attaques de fonctions à sens unique exponentielle modulaire, relève d'un enjeu économique important.

Dans l'approche globale de cet article, nous avons proposé des nouvelles approches de résolution des fonctions à sens unique modulaire exponentielle, combinant les bases de Gröbner. Nous avons fait appel à une méthode de paramétrisation, afin d'avoir un système d'équations polynômiales soluble par les bases de Gröbner pour enfin, de trouver toutes les solutions possibles, le générateur g de la fonction sous forme de classe d'équivalence $(nk + b)$.

BIBLIOGRAPHIE

[1] Boneh D. and Venkatesan R., Rounding in lattices and its cryptographic applications, In Proc. of the 8th Symposium on Discrete Algorithms, pages 675–681. ACM, 1997.

[2] Schneier B., Cryptographie Appliquée : Algorithme, protocoles et codes source en C, Ed. Vuibert Informatique, 2017.

[3] Diffie W. and Hellman M. E., New directions in cryptography. IEEE Trans. Information Theory, ITa-22(6) :644-654, 1976.

[4] Faugère J.C., Calcul efficace des bases de Gröbner et Applications, Springer-Verlag, February 9, 2007.

[5] Kelsey J. and Kohno T., Herding Hash Functions and the Nostradamus Attack. In Serge Vaudenay, editor, EUROCRYPT, volume 4004 of Lecture Notes in Computer Science, pages 183–200. Springer, 2006. 1.2.2, 1.3.4, 6.2.3, 8.3.3.

[6] Rivest R. L., Cryptography. In Handbook of Theoretical Computer Science volume A, chapter 13. Ed. Elsevier, 1990.

[7] Brassard G., Cryptographie contemporaine, Ed. Masson, Paris, 1993

[8] Stern J., La science du secret, Editions Odile Jacob, Paris, 1998.

[9] Adleman L.M., A subexponential algorithm for the discrete logarithm problem with applications to cryptography. In Found. Comp. Sci. Symp. (FOCS 1979), pages 55–60. IEEE, 1979.

[10] Bailly-Maitre G., Arithmétique et cryptologie, Ed. Ellipses, Paris, 2021.

[11] Salomaa A., Public Key Cryptography, EATCS monographs, Ed. Springer, Verlag, 1990.

[12] El Gamal T., A public key cryptosystem and a signature scheme based on discrete logarithms. In Advances in cryptology - CRYPTO 1984, volume 196 of Lecture Notes in Comput. Sci., pages 10-18. Springer, Berlin, 1985.

[13] Thomé E., Computation of discrete logarithms in $GL(2^{607})$ Dans C. Boyd et E. Dawson, éditeurs, Advances in Cryptology ASIACRYPT 2001. Lecture Notes in Comput. Sci., volume 2248, pages 107,124. Springer Verlag, 2001. Proc. 7th International Conference on the Theory and Applications of Cryptology and Information Security, Dec. 9 ,13, 2001, Gold Coast, Queensland, Australia.

[14] Nechaev V. I., Complexity of a determinate algorithm for the discrete logarithm, Mathematical Notes, 55(2):165-172, 1994.

[15] Shoup V., Lower bounds for discrete logarithms and related problems. Dans W. Fumy, éditeur, Advances in Cryptology - EUROCRYPT '97. Lecture Notes in Comput. Sci., volume 1233, pages 256-266. Springer-Verlag, 1997. Proc. International Conference on the Theory and Application of Cryptographic Techniques, Konstanz, Germany, May 1997.

[16] O'Shea D., Cox D. and Little O.J., Ideals, Varieties, and Algorithms, Springer, Berlin, 1992.

[17] Eisenbud D., Commutative Algebra, with a View Toward Algebraic Geometry, Springer, Berlin, 2009.

[18] O'Shea D., Cox D. and Little O.J, Using Algebraic Geometry, Springer, Berlin, 1998.

[19] https ://www.wolframalpha.com/, 25/06/2022.

[20] Guillaume J., Dumas JL., Roch É., Tannier S., Varrette, correction, théorie des codes Compression, cryptage, Dunod, Paris, 2007 ISBN 9-78-210-050692-7

[21] Klin M. · Gareth A., Aleksandar J., Algorithmic Algebraic Combinatorics and Gröbner Bases, Ed. Springer-Verlag Berlin Heidelberg, 2009.

[22] Stinson D., Cryptographie Théorie et pratique, Ed. Vuibert, Paris 2001.

AUTHOR'S BIOGRAPHY

MAYALA LEMBA Francis he teaches in the "Université Pédagogique Nationale", Democratic Republic of the Congo. His research (Cryptography).

ENGOMBE NGONGO Josette est chercheuse au Centre de Recherche pour le Développement de l'Education, de l'Université Pédagogique Nationale (CREDE), en République Démocratique du Congo. josetteengombe@gmail.com

MAYALA NKUMBIEME Pélagie est chercheuse au Centre de Recherche Interdisciplinaire de l'Université Pédagogique Nationale (CRIDUPN), en République Démocratique du Congo. mayalapelagie@gmail.com

MONGONDA MODJENGE John est enseignant à Institut Supérieur Pédagogique de la Gombe (ISP-Gombe), en République Démocratique du Congo. johnny1mongonda@gmail.com

ENGOMBE WEDI Boniface is a Professor in the Department of Mathematics and Computer Science, in the Faculty of Science, at the "Université Pédagogique Nationale", Democratic Republic of the Congo. engwedi@gmail.com

Citation: *MAYALA LEMBA Francis.et.al, Cryptanalyse des fonctions à sens Unique Exponentielle Modulaire à l'aide des Bases de Gröbner, International Journal of Scientific and Innovative Mathematical Research (IJSIMR), vol. 10, no. 1, pp. 1-12, 2022. Available : DOI: https://doi.org/ 10.20431/2347-3142.1001001*