Le but de ce problème est d'étudier précisément le comportement du calcul de base de Gröbner pour des systèmes issus de la cryptanalyse algébrique du cryptosystème "Hidden Matrix".

Remarque importante: les questions sont indépendantes et peuvent être traitées dans n'importe quel ordre.

1 Description du cryptosystème Hidden Matrix

Ce cryptosystème est similaire au cryptosystème HFE du cours mais les objets de base sont des matrices X de taille $n \times n$. Soit $\mathscr{A}$ l'algèbre des matrices n-par-n sur le corps fini $\mathbb{K}$. Dans la suite $\mathbb{K} = \mathbb{F}_p$ où p est un entier premier.

Pour encoder un message m on le découpe en n^2 blocs de taille p. C'est à dire $m = [m_1, \ldots, m_{n^2}] \in \mathscr{B} = \mathbb{K}^{n^2}$. Ainsi, à tout vecteur de taille n^2, on peut associer une matrice:

$$\psi \left(\begin{array}{ccc} \mathscr{B} = \mathbb{K}^{n^2} & \longrightarrow & \mathscr{A} \\ m = [m_1, \ldots, m_{n^2}] & \longmapsto & \psi(m) = \begin{bmatrix} m_1 & m_2 & \cdots & m_n \\ m_{n+1} & m_{n+2} & \cdots & m_{2n} \\ \vdots & & & \vdots \\ m_{n+1} & m_{n+2} & \cdots & m_{2n} \end{bmatrix} \end{array} \right)$$

1.1 Clé Privée

On suppose qu'une matrice $M \in \mathscr{A}$ est fixée. La clé privée est la donnée

- d'une application:

$$F \begin{pmatrix} \mathscr{A} & \longrightarrow & \mathscr{A} \\ A & \longmapsto & F(A) = A^2 + MA \end{pmatrix}$$

- deux matrices $\mathbf{S}$ et $\mathbf{T}$ de tailles $n^2 \times n^2$.

On peut aussi voir la fonction F comme agissant sur des vecteurs de $\mathscr{B}$ en considérant la fonction $F' = \psi^{-1} \circ F \circ \psi$. Ainsi, à partir d'un message m le chiffré est $c = \mathbf{S}F'(\mathbf{T}m)$.

Question 1. *Soit $C \in \mathscr{A}$, on suppose qu'il existe une procédure efficace pour calculer les solutions $F(X) = C$. Expliquer alors comment retrouver le message m à partir de $c = \mathbf{S}F'(\mathbf{T}m)$.*

1.2 Clé Publique

On considère un vecteur $x = (x_1, \ldots, x_{n^2})$ où les x_i sont des variables symboliques. La clé publique est constituée des n^2 polynômes dans $\mathbb{K}[x_1, \ldots, x_{n^2}]$ dans:

$$\mathbf{S}F'(\mathbf{T}x).$$

1.3 Cryptanalyse algébrique

On va montrer qu'on peut calculer efficacement une base de Gröbner de l'idéal:

$$J = \left\langle \mathbf{S}F'(\mathbf{T}X) - \mathbf{S}F'(\mathbf{T}A) \right\rangle.$$

Question 2. *Expliquer pourquoi, du point de vue du calcul des bases de Gröbner, on peut se contenter d'étudier l'idéal I engendré par les équations:*

$$I = \left\langle X^2 + MX - A^2 - MA \right\rangle. \tag{1}$$

(Note: on ne demande pas une preuve formelle, mais de donner les principaux arguments.)

1.4 Équations de bas degré

On considère l'idéal engendré par toutes les composantes de :

$$\Delta = (\Delta_{i,j})_{1 \leq i,j \leq n} = X^2 + MX - B = 0.$$

Définition. Les espaces vectoriels suivants sont définis par récurrence:

$$\begin{aligned} I_{d,0} &= \mathsf{Vect}_{\mathbb{K}}\left(\Delta_{i,j} \mid \ 1 \leqslant i,j \leqslant n\right) \\ I_{d,1} &= \mathsf{Vect}_{\mathbb{K}}\left(x_{i,j} f \mid \ 1 \leqslant i,j \leqslant n \text{ et } f \in I_{d,0}\right) \\ I_{d,k} &= \mathsf{Vect}_{\mathbb{K}}\left(x_{i,j} f \mid \ 1 \leqslant i,j \leqslant n \text{ et } f \in I_{d,k-1} \text{ et } deg(f) \leq d-1\right) \end{aligned}$$

On définit alors $I_d = \bigcup_{k=0}^{\infty} I_{d,k}$.

Question 3. *On fixe d. Montrer* brièvement *que pour tout $f \in I_d$, on a $deg(f) \leq d$ et qu'on peut calculer une d-base de Gröbner (c'est à dire une base tronquée en degré d) de I_d en temps polynômial.*

On peut donc interpréter l'indice k comme étant le nombre d'étapes dans l'algorithme F_4 ou F_5 pour calculer une base de $I_{d,k}$.

1.5 Cas particulier $M = 0$

Question 4. *Montrer que dans l'idéal $I_{3,1}$ il y a les n^2 équations linéaires:*

$$XB - BX.$$

Question 5. *En déduire le nombre d'équations linéaires après n étapes. C'est à dire dans $I_{3,n}$.*

1.6 Corps de caractéristique quelconque ($p \neq 2$)

Question 6. *Montrer que les équations quadratiques suivantes sont dans $I_{3,1}$:*

$$P_1 = X \cdot M \cdot X + (B + M^2) \cdot X - X \cdot B - M \cdot B \in I_{3,1}.$$

Question 7. *Pour tout $k \geq 1$, montrer que les équations quadratiques suivantes sont dans $I_{3,k}$:*

$$P_k = X \cdot (M^k + A_k) \cdot X + B_k \cdot X + X \cdot C_k + D_k \in I_{3,k}.$$

1.7 Corps de caractéristique $p = 2$

On suppose dans cette section que $p = 2$.

Question 8. *Lorsque $\mathbb{K} = \mathbb{F}_2$, montrer que $C_M(z) = C_{M^2}(z)$. La notation $C_M(z)$ désigne le polynôme caractéristique de la matrice M dont les racines sont les valeurs propres de M.*

Question 9. *On note $tr(M) = \sum_{i=1}^{n} M_{i,i}$ la trace de la matrice M. Déduire de la question **??** que $tr(M^2) = tr(M)$.*

Question 10. *Montrer alors que l'équation linéaire suivante est dans $I_{3,0}$:*

$$Q_0 = tr((M + I)X) - tr(B) \in I_{3,0}.$$

Question 11. *Montrer que l'équation linéaire suivantes est dans $I_{3,1}$:*

$$Q_1 = tr(XM + (B + M^2)XM - XBM - MBM) \in I_{3,1}.$$

Question 12. *Montrer que les équations linéaires suivantes sont dans $I_{3,k}$:*

$$Q_k = tr((X + B_k X + XC_k + D_k)(M^k + A_k)) \in I_{3,k}.$$

1.8 Conclusion

Question 13. *Compléter le tableau suivant en indiquant le nombre d'équations après k étapes de calcul de l'algorithme F_4:*

Nombre d'équations/Cas	char$(\mathbb{K}) \neq 2$	char$(\mathbb{K}) = 2$	$M = 0$
Nb d'équations quadratiques après k étapes	...	...	0
Nb d'équations linéaires après k étapes	0	...	...
Total Nb d'équations quadratiques après n étapes	...	...	0
Total Nb d'équations linéaires après n étapes	0	...	...

Question 14. *À votre avis, que peut on dire sur la complexité du calcul de base de Gröbner de l'idéal engendré par les équations de la clé publique du cryptosystème Hidden Matrix ?*