

Si $(A_i)_{i \leq t}$ est une famille de matrices, on désigne par $[A_{i \leq t}]$ la matrice par blocs qui correspond à l'empilement des $(A_i)_{i \leq t}$:

$$\begin{bmatrix} A_1 \\ A_2 \\ \dots \\ A_t \end{bmatrix}$$

On considère les $(a_i)_{i \leq t}$ variables aléatoires uniformes sur $(\mathbb{Z}/q\mathbb{Z})^n[X]$ (i.e chaque coefficient est choisi uniformément).

On définit $A := [\text{Toep}^d(a_i)_{i \leq t}]$, où $\text{Toep}^d(P)$ est une matrice à d lignes et $\deg(P) + d$ colonnes, dont la j -ème ligne est constituée des coefficients de $x^{j-1}P$. Par exemple,

$$\text{Toep}^3(X^2 + 3X + 1) = \begin{bmatrix} 1 & 3 & 2 & 0 & 0 \\ 0 & 1 & 3 & 2 & 0 \\ 0 & 0 & 1 & 3 & 2 \end{bmatrix}$$

Pour donner du contexte, en pratique on a $t = O(\log n)$, $d = n/2$ et $q \geq n^{2.5} \log n$

Ainsi les Toeplitz sont des matrices environ 3 fois plus larges que longues, et A est une matrice très longue. Le rang maximum de cette dernière est donc $n + d$

Théorème :

Avec une probabilité $\geq 1 - (\frac{n+d}{q})^{\lfloor t/\lceil \frac{n+d}{d} \rceil \rfloor}$, on a que A est de rang plein.

Si on utilise les ordres de grandeurs proposés dans le schéma de chiffrement, on a :

$$\mathbb{P}(\text{rg}(A) = n + d) \geq 1 - \left(\frac{1}{n^{\frac{3}{2}} \sqrt{\log n}}\right)^{\log n}$$

Preuve : On commence par rappeler de lemme de Schwartz-Zippel : pour un polynôme multivarié non nul de degré n , à coefficients dans $\mathbb{Z}/p\mathbb{Z}$, la probabilité d'annuler ce polynôme en choisissant les variables uniformément est au plus $\frac{n}{p}$.

On considère donc la matrice carré constituée des $n + d$ premières lignes de A , que l'on note A_1 . Le déterminant de cette sous-matrice est un polynôme à plusieurs variables, de degré $n + d$, dont les variables sont choisies uniformément dans $\mathbb{Z}/q\mathbb{Z}$. Ce polynôme est non nul, par exemple on peut choisir $a_1 = 1$, $a_2 = x^d$, $a_3 = x^{2d}$, ... et alors $A_1 = \text{Id}$ et donc $\det(A_1) = 1 \neq 0$.

Alors, d'après le lemme, on a que :

$$\mathbb{P}[\det(A_1) = 0] \leq \frac{n + d}{q}$$

On peut ensuite répéter ce processus pour les sous-matrices suivantes. Cependant, afin de conserver l'indépendance, il faut faire attention à ne pas reprendre une Toeplitz déjà utilisée. Ainsi, A_k sera la sous matrice carré commençant à la $(k-1)d \lceil \frac{n+d}{d} \rceil$ -ème ligne. Au total, on pourra donc avoir au moins $\lfloor t/\lceil \frac{n+d}{d} \rceil \rfloor$ sous matrices carrés dont les entrées sont mutuellement indépendantes. Alors :

$$\begin{aligned} \mathbb{P}(\text{rg}(A) < n + d) &\leq \mathbb{P}\left(\bigcap_{k \leq \lfloor t/\lceil \frac{n+d}{d} \rceil \rfloor} \det A_k = 0\right) \\ &= \mathbb{P}[\det(A_1) = 0]^{\lfloor t/\lceil \frac{n+d}{d} \rceil \rfloor} \\ &= \left(\frac{n + d}{q}\right)^{\lfloor t/\lceil \frac{n+d}{d} \rceil \rfloor} \end{aligned}$$

Ce qui donne bien l'inégalité voulue.