Soient n, d, t des entiers, et q un entier premier.
Si $(M_i)_{i\leq t}$ est une famille de matrices de mêmes dimensions, on désigne par $[M_{i\leq t}]$ la matrice par blocs qui correspond à l'empilement des $(M_i)_{i\leq t}$:

$$\begin{bmatrix} M_1 \\ M_2 \\ \dots \\ M_t \end{bmatrix}$$

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 défini $A := [\mathrm{Toep}^{d,n}(a_i)_{i\leq t}]$ où, si P est un polynôme de degré au plus n, alors $\mathrm{Toep}^{d,n}(P)$ est une matrice à d lignes et $n+d$ colonnes, dont la j-ème ligne est constituée des coefficients de $x^{j-1}P$. Par exemple,

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

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 utilisées ici 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 :

$$\mathbb{P}(\mathrm{rg}(A) = n+d) \geq 1 - (\frac{3}{2n^{1.5}\log n})^{\frac{\log n}{3}}$$

Preuve : On commence par rappeller 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 uniforméments dans $\mathbb{Z}/q\mathbb{Z}$. Ce polynôme est non nul, par exemple on peut choisir $a_1 = 1$, $a_2 = x^d$, $a_3 = x^{2d}$, $\dots$ et alors $A_1 = \mathrm{Id}$ 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 mutuellements indépendantes. Alors :

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

Ce qui donne bien l'inégalité voulue.