FHE 1

Ethan Bandasack

Mars 2025

1 Introduction

Le système permet de traiter des entiers. Notons à ce titre $\mathcal{X} \subseteq \mathbb{N}$ l'ensemble des entrées.

Notons également $D > 0$ un paramètre du système qui servira à découper les entrées.

Une clé est un élément $S \in \mathbb{N}$ (qui n'a ici pas besoin d'être premier).

Sauf mention contraire au cours du document, x et y sont des éléments de $\mathcal{X}$ représentant une entrée inconnue.

2 Chiffrement

Commençons par décomposer x en base D de sorte que

$$x = \overline{x_{n-1} \dots x_2 x_1 x_0}^{(D)} = \sum_{i=0}^{n-1} x_i D^i \tag{1}$$

Le chiffrement se compose de la façon suivante :

- On génère un bruit aléatoire $e \in (\mathbb{N}^*)^n$
- On chiffre x en $\mathcal{C}(x, S) = \Big(S \times e_i + x_i\Big)_{0 \leq i < n}$

2.1 Hypothèse 1

On considère que n est assez grand pour que x, et tous les autres nombres considérés, soient représentables dans cette base, c'est-à-dire que $x_i \in \{0, \dots, D^n - 1\}$.

3 Déchiffrement

Si $S \geq D$, alors $\mathcal{S}(x, S)$ peut être déchiffré en prenant la division euclidienne de chaque composante par S. On obtient alors $(x_i)_{(0 \leq i < n)}$ (en effet, tous les x_i sont compris entre 0 et $D-1$), ce qui donne immédiatement x si on connaît la base D (voir **??**).

On note d'ailleurs qu'en notant $P_x = \sum_{i=0}^{n-1} x_i X^i$, on a $x = P_x(D)$. On gardera cette notation pour la suite.

On va d'ailleurs considérer que $\mathcal{C}(x, S)$ est un polynôme de $\mathbb{Z}_D[X]$ à coefficients entiers positifs entre 0 et $D - 1$.

4 Propriétés homomorphes

4.1 Addition

La propriété d'homomorphie pour l'addition entre deux éléments de $\mathcal{X}$ est assurée si $S \geq 2D-1 = (D-1)+(D-1)+1$.

4.1.1 Démonstration

Si $S \geq 2D-1$, alors pour $x, y \in \mathcal{X}$, on a :

$$\mathcal{C}(x,S)+\mathcal{C}(y,S) = \sum_{i=0}^{n-1} \Big(S(e_i^{(x)}+e_i^{(y)})+x_i+y_i\Big)X^i = \mathcal{C}(x+y,S) \tag{2}$$

car pour tout i, $0 \leq x_i + y_i \leq 2D-2 < S$.

4.2 Multiplication

La propriété d'homomorphie pour la multiplication entre deux éléments de $\mathcal{X}$ est assurée si $S \geq D^2-2D+2 = (D-1)(D-1)+1$.

4.2.1 Démonstration

Si $S \geq D^2-2D$, alors pour $x, y \in \mathcal{X}$, on a :

$$\begin{aligned}
\mathcal{C}(x,S)\mathcal{C}(y,S) &= \sum_{i=0}^{n-1}\sum_{j=0}^{n-1}\Big(Se_i+x_i\Big)\Big(Se_j+y_j\Big)X^{i+j} && (3)\\
&= \sum_{i=0}^{2n-2}\sum_{\substack{0\leq j,k<n\\ j+k=i}}\Big(S^2e_je_k+S(e_jy_k+x_je_k)+x_jy_k\Big)X^i && (4)\\
&= \mathcal{C}\Big(\sum_{i=0}^{2n-2}\sum_{\substack{0\leq j,k<n\\ j+k=i}} x_jy_kD^i, S\Big) && (5)
\end{aligned}$$

Le passage à la dernière ligne se justifie car, pour tout i, $0 \leq x_iy_i \leq (D-1)^2 < D^2-2D+2 \leq S$.

On remarque de plus que $\displaystyle\sum_{i=0}^{2n-2}\sum_{\substack{0\leq j,k<n\\ j+k=i}} x_jy_kD^i = \sum_{i=0}^{n-1}\sum_{j=0}^{n-1} x_jy_kX^{j+k} = P_x(D)P_y(D) = xy$.

Enfin, d'après l'hypothèse **??**, on a peut arrêter la somme à $n-1$, ce qui montre d'ailleurs que $P_{xy}(D) = P_x(D)P_y(D)$.

On a bien $\mathcal{C}(x,S)\mathcal{C}(y,S) = \mathcal{C}(xy,S)$.

4.3 Fonction polynomiale

On déduit de la partie **??** que, par récurrence, $\mathcal{C}(kx,S) = k\mathcal{C}(x,S)$ pour tout $k \in \mathbb{N}$ (à condition que $S \geq k(D-1)+1$).

On en déduit de la même façon que la propriété d'homomorphie est assurée pour une somme de $k \in \mathbb{N}^*$ éléments de $\mathcal{X}$ si $S \geq k(D-1)+1$.

Idem pour la multiplication de $k \in \mathbb{N}^*$ éléments de $\mathcal{X}$ si $S \geq (D-1)^k + 1$.

En ajoutant la partie **??**, on peut généraliser cette propriété à toute fonction polynomiale à plusieurs variables à coefficients entiers positifs $P : \mathbb{N}^k \longrightarrow \mathbb{N}$ du moment que $S > P(D-1, \ldots, D-1)$.

4.3.1 Démonstration

Soit $P : \mathbb{N}^k \longrightarrow \mathbb{N}$ une fonction polynomiale à plusieurs variables à coefficients entiers positifs. On note donc $P(x_1, \ldots, x_k) = \sum\limits_{\substack{i_1,\ldots,i_k \geq 0 \\ \prod_j i_j \leq d}} a_{i_1,\ldots,i_k} \prod\limits_{j=1}^{k} x_j^{i_j}$, avec $a_{i_1,\ldots,i_k} \in \mathbb{N}$ et d le degré de P.

Supposons que $S > P(D-1, \ldots, D-1)$. Alors pour $(x_1, \ldots, x_k) \in \mathcal{X}^k$, on applique d'abord la propriété d'homomorphie pour la multiplication de $\sum\limits_{j=1}^{k} i_j$ éléments de $\mathcal{X}$:

$$P(\mathcal{C}(x_1, S), \ldots, \mathcal{C}(x_k, S)) = \sum_{\substack{i_1,\ldots,i_k \geq 0 \\ \prod_j i_j \leq d}} a_{i_1,\ldots,i_k} \prod_{j=1}^{k} \mathcal{C}(x_j, S)^{i_j} = \sum_{\substack{i_1,\ldots,i_k \geq 0 \\ \prod_j i_j \leq d}} a_{i_1,\ldots,i_k} \mathcal{C}\Big(\prod_{j=1}^{k} x_j^{i_j}, S \Big) \tag{6}$$

car pour tous $i_1, \ldots, i_k$, $0 \leq \prod\limits_{j=1}^{k} x_j^{i_j} \leq (D-1)^{\sum_{i=1}^{k} i_j} \leq (D-1)^d \leq P(D-1, \ldots, D-1) < S$.

Ce n'est vrai que si le coefficient correspondant $a_{i_1,\ldots,i_k}$ est non nul, dans le cas contraire cela n'a aucune incidence sur $P(\mathcal{C}(x_1, S), \ldots, \mathcal{C}(x_k, S))$.

On applique ensuite la propriété d'homomorphie pour l'addition de $\sum\limits_{\substack{i_1,\ldots,i_k \geq 0 \\ \prod_j i_j \leq d}} a_{i_1,\ldots,i_k}$ éléments de $\mathcal{X}$:

$$P(\mathcal{C}(x_1, S), \ldots, \mathcal{C}(x_k, S)) = \sum_{\substack{i_1,\ldots,i_k \geq 0 \\ \prod_j i_j \leq d}} a_{i_1,\ldots,i_k} \mathcal{C}\Big(\prod_{j=1}^{k} x_j^{i_j}, S \Big) = \mathcal{C}\Big(P(x_1, \ldots, x_k), S \Big) \tag{7}$$

car pour tous $i_1, \ldots, i_k$, $0 \leq \sum\limits_{\substack{i_1,\ldots,i_k \geq 0 \\ \prod_j i_j \leq d}} a_{i_1,\ldots,i_k} \prod\limits_{j=1}^{k} x_j^{i_j} \leq \sum\limits_{\substack{i_1,\ldots,i_k \geq 0 \\ \prod_j i_j \leq d}} a_{i_1,\ldots,i_k} (D-1)^d \leq P(D-1, \ldots, D-1) < S$.