Projet BPCE FHE - Execsum sur un 1er système de chiffrement

Ethan Bandasack, Mathis Bottinelli, Malo Leroy

Mars 2025

1 Contexte

La BPCE explore les opportunités possibles de la du chiffrement complètement homomorphe (FHE) afin d'exploiter pleinement la puissance de calcul offerte par les technologies de cloud computing. L'objectif est de permettre le calcul de fonctions sur des données chiffrées sans jamais les déchiffrer. Plusieurs défis se présentent alors dans cette quête, principalement la complexité des opérations et la sécurité des données.

2 Un premier système de chiffrement

Afin de chiffrer des entiers arbitrairement grands, il est possible de considérer un premier système de chiffrement assez simple. Voir l'exemple ci-dessous :

On cherche à chiffrer 123 456 789 876 543 210, un entier assez grand. Chaque paquet de 3 chiffres sera chiffré séparément. Afin de chiffrer le premier paquet = 210, une clé secrète $S = 1000007$ assez grande est choisie, et un bruit $e = 39$ aléatoire est généré. Le chiffré c est alors calculé comme suit :

$$c = m + e \times S = 210 + 39 \times 1000007 = 39210273.$$

Pour déchiffrer, il suffit de calculer le reste de la division euclidienne de c par S.

Les propriétés homomorphes peuvent se démontrer : il est possible de réaliser des additions et des multiplications sur les chiffrés sans avoir besoin de les déchiffrer.

3 Limites

Une première remarque : lorsque deux chiffrés sont additionnés, l'addition se fait "terme à terme", chaque paquet de 3 chiffres est additionné séparément. Il faut pouvoir gérer les retenues, car un résultat pourra éventuellement dépasser 999. Cela peut se gérer assez facilement. La même chose se produit dans le cas de la multiplication.

Première remarque sur la multiplication : la multiplication ne peut se faire terme à terme, il faut utiliser une multiplication semblable à celle des polynômes. Ce n'est pas un problème, il est même naturel de considérer la liste des paquets comme la liste des coefficients d'un polynôme.

Deuxième remarque, plus importante, sur la multiplication : la taille des chiffrés.