1 Contexte

La BPCE explore les opportunités qu'offre le 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 $123\,456\,789$, un entier assez grand. Chaque paquet de 3 chiffres sera chiffré séparément. Afin de chiffrer le premier paquet 789, 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 : $c = m + e \times S = 789 + 39 \times 1\,000\,007 = 39\,001\,062$.

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 Remarques et limites

3.1 Remarques techniques : premières limites

1. 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.

2. La multiplication ne peut se faire terme à terme, il faut utiliser une multiplication semblable à celle des polynômes. Il est tout à faire possible de considérer la liste des paquets comme la liste des coefficients d'un polynôme.

3.2 Faiblesse de sécurité

Le système de chiffrement présenté n'inclut qu'une seule source d'aléatoire et est linéaire. Il est vulnérable à des attaques assez simples. Avec Python, il est possible de retrouver les 5 premiers chiffres de la clé privée en quelques secondes en utilisant un grand nombre d'échantillons. Il s'agit d'une inversion de système linéaire, qui est rendue impossible avec l'introduction d'un terme de bruit dans les systèmes utilisés, se basant sur le problème LWE (Learning With Errors), introduit en 2005 par Oded Regev.

3.3 Faiblesse de performance

La plupart des systèmes de chiffrement modernes utilisent l'arithmétique modulaire, ce qui permet de ne pas manipuler des entiers trop grands. Ici, un grand nombre de calculs peut mener à une explosion de la taille des entiers manipulés, ce qui peut être problématique en termes de performance, ou même de mémoire.

4 Conclusion et perspectives

Ce système de chiffrement est un premier pas vers la compréhension des systèmes de chiffrement homomorphes. Il présente un avantage considérable dans sa simplicité, mais peut être compromis assez facilement.

S'il peut donner une première idée fondatrice autour du chiffrement homomorphe, les recherches de ces dernières années ont permis de mettre en place des systèmes plus robustes et plus performants : en plus du problème LWE empêchant l'inversion des systèmes, l'utilisation de polynômes permet d'exploiter le problème RLWE (Ring Learning With Errors), qui permet notamment d'utiliser des clés beaucoup plus petites que celles utilisées auparavant, par exemple par Gentry en 2009.