ravel

CENTRE HENRI LEBESGUE CENTRE DE MATHÉMATIQUES

LES MATHS VECTEUR D'INNOVATION

Semaine d'Étude Mathématiques-Entreprises

La cryptographie homomorphe au service du traitement de données sécurisées

La cryptographie homomorphe [1] permet de chiffrer des données afin de préserver leur confidentialité tout en permettant de faire des calculs sur les données chiffrées, "en aveugle", c'est-à-dire sans les déchiffrer. Pour cela, mathématiquement parlant, l'algorithme de chiffrement doit commuter avec des opérations élémentaires, qui sont au minimum l'addition et la multiplication. Un exemple d'application d'un chiffrement homomorphe pour la délégation de calculs pourrait être le cas de figure où un utilisateur souhaiterait faire un calcul, dont il ne connaît pas les modalités ou pour lequel il ne disposerait pas des ressources nécessaires, et aimerait faire appel à un service de cloud computing pour effectuer ses calculs tout en préservant la confidentialité des données. C'est en particulier important dans le domaine médical.

Parmi tous les algorithmes possibles, ceux qui se sont imposés sur les dix dernières années sont tous basés sur le problème dit Learning With Errors (LWE), pour des raisons de performances et de sécurité. Malheureusement cette technique introduit un bruit dans le message chiffré, qui peut augmenter au cours des calculs homomorphes, jusqu'à rendre incorrect son déchiffrement. La clé pour résoudre ce problème a été inventée par l'un des acteurs majeurs dans ce domaine, Craig Gentry [2]. Il s'agit de la notion de bootstrap, qui consiste à "rafraîchir" le message chiffré sans le déchiffer, en diminuant le bruit.

L'objectif de ce sujet est de rechercher et tester une méthode performante pour réduire le bruit du message chiffré sans le déchiffrer. Parmi les solutions de bootstrap proposées, celle de Ducas et Micciancio [3] est l'une des plus performantes. Ce travail sera accompagné par la start-up Ravel Technologies, spécialisée dans le chiffrement homomorphe.

Références

[1] Page Wikipedia https://fr.wikipedia.org/wiki/Chiffrement_homomorphe

[2] Craig Gentry, Fully homomorphic encryption using ideal lattices (Thèse de doctorat), 2009.

[3] Léo Ducas et Daniele Micciancio, FHEW: Bootstrapping Homomorphic Encryption in less than a second, Eurocrypt, 2015.