Cryptocalcul Homomorphe

Calculer sans décrypter

Depuis quelques années, la cryptographie connait une petite révolution avec le développement de la théorie des cryptosystèmes dits homomorphes, permettant *in fine* de réaliser des calculs arbitrairement complexes directement sur des données chiffrées, soit de « cryptocalculer ».

Ces cryptosystèmes fournissent les fondements nécessaires pour la mise en œuvre de services préservant la confidentialité des données par construction.

En effet, les données adressées à un interlocuteur, transitant par un serveur ou par le cloud et faisant l'objet d'un traitement, sont cryptées en permanence, les traitements étant réalisés sur données cryptées. Les progrès extrêmement rapides réalisés ces dernières années en matière de performances permettent d'envisager l'intégration de cette technologie dans de premiers prototypes industriels.

CONTACT
showroomceatech@cea.fr