

## Le chiffrement homomorphe réconcilie traitement informatique et vie privée

### Description

**Le chiffrement homomorphe est une branche de la cryptologie qui permet d'effectuer des calculs sur des données cryptées sans les décrypter au préalable, assurant ainsi la sécurité du traitement externalisé d'informations sensibles comme les données personnelles, les données de santé, les données financières ou encore le vote électronique.**

Le chiffrement est dit « homomorphe » (de même forme), parce que le déchiffrement du résultat d'une opération réalisée avec des données chiffrées donne un résultat identique à l'opération effectuée sur ces mêmes données non chiffrées. L'intérêt d'une telle méthode de chiffrement est notamment de résoudre les problématiques de sécurité liées à l'externalisation de calculs portant sur des données sensibles, à l'heure où le nombre de cyberattaques contre des acteurs du cloud computing croît chaque année.

Si le concept est né dans les années 1970, il faudra attendre près de quarante ans pour que Craig Gentry, informaticien américain, propose en 2009, dans sa thèse de doctorat, le premier système de chiffrement entièrement homomorphe (*Fully Homomorphic Encryption*, FHE). Le chiffrement est dit « entièrement homomorphe » car il supporte les opérations d'additions et de multiplication un nombre arbitraire de fois. Et c'est le principe sur lequel repose le chiffrement.

Comme l'explique Laria Chillotti dans sa thèse de doctorat sur ce sujet, soutenue en 2018 à l'université Paris-Saclay, « dans tous les schémas de chiffrement homomorphe proposés, les chiffrés contiennent une petite quantité de bruit, nécessaire pour des raisons de sécurité. Quand on fait des calculs sur les chiffrés « bruités », le bruit augmente et, après avoir évalué un certain nombre d'opérations, ce bruit devient trop grand et, s'il n'est pas contrôlé, risque de compromettre le résultat des calculs ». L'innovation proposée par Craig Gentry repose sur la notion de « *bootstrap* », qui consiste selon lui à « *rafraîchir* » le message chiffré sans le déchiffrer, en diminuant le bruit ». Depuis 2009, quatre générations de schémas de chiffrement homomorphe ont été proposées, le plus récent datant de 2016, afin notamment d'améliorer les opérations de déchiffrement dont le caractère chronophage a longtemps empêché toute application pratique.

Prenons l'exemple d'un programme de recherche qui doit réaliser des calculs sur des données médicales sensibles, comme des données biométriques, mais ne disposant pas d'une puissance de calcul suffisante. L'équipe en charge de ce programme voudrait effectuer ces calculs sur EuroHPC, l'infrastructure paneuropéenne de supercalculateurs ([voir La rem n°45, p.16](#)). Dans un scénario traditionnel de chiffrement asymétrique, l'équipe de recherche crypte les données médicales sensibles avec une clé publique afin de les envoyer vers EuroHPC. Ces mêmes données seront ensuite déchiffrées à l'aide d'une clé privée pour être confiées aux supercalculateurs. Enfin, les résultats des calculs, ainsi que les données, seront à nouveau

---

chiffrés avant d'être transmis à l'équipe de recherche. Si les données sont bien cryptées lors de l'envoi, les calculs portent en revanche sur des données en clair, ce qui est particulièrement risqué, voire interdit par la législation en vigueur.

Une solution sécurisée de bout en bout consisterait, pour l'équipe de recherche, à recourir au chiffrement homomorphe pour chiffrer les données médicales sensibles avec une clef publique transmise à EuroHPC. Les supercalculateurs effectueraient alors les calculs demandés sur ces données non déchiffrées, tandis que les résultats seraient déchiffrés par l'équipe de recherche à l'aide d'une clef privée. Grâce au chiffrement homomorphe, les données sur lesquelles EuroHPC a effectué des calculs seront restées chiffrées tout au long de la procédure, sans aucune altération des résultats, dont le déchiffrement revient uniquement au commanditaire initial.

Le vote électronique fournit un autre exemple de l'usage du chiffrement homomorphe. Un système de vote électronique classique rassemble au même endroit les votes des participants, préalablement cryptés, qui sont alors décryptés puis additionnés afin de calculer les résultats du vote. Le dépouillement présente donc un risque de fraude puisque les données sont décryptées pour effectuer le comptage des voix. Un système de vote électronique basé sur le chiffrement homomorphe chiffre le vote dès sa saisie et envoie les données sur un serveur où sont ensuite effectuées les additions, sans que les données aient eu à être déchiffrées.

Quelques freins empêchent encore l'usage à grande échelle de ce mode de chiffrement, notamment le ralentissement considérable du temps de calcul effectué sur des données chiffrées. En 2009, ce temps de calcul pouvait être un milliard de fois supérieur au temps requis avec des données non chiffrées. Néanmoins, la diversité des possibilités d'application du chiffrement homomorphe suscite fortement l'intérêt des chercheurs et des entreprises, comme la société française Ravel Technologies, créée en 2018, au sein de laquelle une quinzaine de mathématiciens travaillent exclusivement à améliorer ce temps de traitement. En janvier 2023, l'entreprise a annoncé avoir développé un nouveau schéma de cryptage entièrement homomorphique avec un temps de traitement extrêmement rapide. Mehdi Sabeg, président de la société, expliquait à cette occasion dans les colonnes de *La Tribune* que, « *dans le processus, le chiffré du message contient du bruit qui augmente au fur et à mesure des traitements et qu'il faut gérer. Notre solution permet de gagner quatre ordres de grandeur sur la performance. Au point de rendre le chiffrement homomorphe utilisable efficacement dans des applications qui nécessitent le traitement de grands volumes de données avec une très faible latence, comme la publicité programmatique par exemple* ».

Le chiffrement homomorphe répond également à un enjeu de souveraineté numérique. Les *hyperscalers* – fournisseurs d'infrastructures répondant aux besoins de plus en plus importants du big data – et autres acteurs du cloud sont américains et l'Europe ne sera vraisemblablement pas en mesure de rattraper son retard sur ce marché crucial. Or, lorsqu'une entreprise étrangère confie des données en clair à un acteur américain, le gouvernement des États-Unis, en vertu du Clarifying Lawful Overseas Use of Data Act, dit Cloud Act, voté en mars 2018, peut contraindre cet acteur à lui communiquer des données personnelles stockées sur ses serveurs situés aux États-Unis ou dans un pays étranger, et ce, même si cette législation est en contradiction avec le règlement général pour la protection des données personnelles (RGPD) en Europe ( voir [La rem n°42-43, p.21](#) )

).

Le chiffrement homomorphe contournerait cette extraterritorialité du droit américain en permettant de confier aux incontournables prestataires américains du cloud des données chiffrées rendues inexploitable par autrui, à l'exception de leur propriétaire.

Sources :

- « Fully Homomorphic Encryption Using Ideal Lattices », Craig Gentry, thèse de doctorat, Stanford University et IBM Watson, 2009.
- « Le chiffrement homomorphe », Ely, linuxfr.org, 13 janvier 2014.
- « Vers l'efficacité et la sécurité du chiffrement homomorphe et du cloud computing », Ilaria Chillotti, thèse de doctorat en informatique soutenue à l'université Paris-Saclay (ComUE), dans le cadre de l'École doctorale Sciences et technologies de l'information et de la communication, en partenariat avec le Laboratoire de Mathématiques de Versailles (laboratoire) et de l'Université de Versailles-Saint-Quentin-en-Yvelines (établissement opérateur d'inscription), theses.fr, 17 mai 2018.
- « [Cahier Technique] Cryptographie homomorphe, l'art de partager sans divulguer », Renaud Sirdey, Arnaud Grivet-Sébert, Cédric Goy-Pailler, usinenouvelle.com, 21 juillet 2022.
- « Bien comprendre le chiffrement homomorphe », Gaétan Raoul, lemagit.fr, 7 octobre 2022.
- « Les promesses du chiffrement homomorphe pour traiter les données privées », Clémentine Laurens, lemonde.fr, 4 janvier 2023.
- « Innovation : cette startup française révolutionne le chiffrement homomorphe », Marc Endeweld, latribune.fr, 27 janvier 2023.

## Categorie

### 1. Techniques

#### **date créée**

23 mai 2023

#### **Auteur**

jacquesandrefines