Le chiffrement homomorphe rÃ©concilie traitement informatique etÂ vie privÃ©e

Description

Le chiffrement homomorphe est une branche de la cryptologie qui permet dâ€™effectuer des calculs sur des donnÃ©es cryptÃ©es sans les dÃ©crypter au prÃ©alable, assurant ainsi la sÃ©curitÃ© du traitement externalisÃ© dâ€™informations sensibles comme les donnÃ©es personnelles, les donnÃ©es de santÃ©, les donnÃ©es financiÃ¨res ou encore le vote Ã©lectronique.

Le chiffrement est ditÂ Â«Â homomorpheÂ Â»Â (de mÃªme forme), parce que le dÃ©chiffrement du rÃ©sultat dâ€™une opÃ©ration rÃ©alisÃ©e avec des donnÃ©es chiffrÃ©es donne un rÃ©sultat identique Ã lâ€™opÃ©ration effectuÃ©e sur ces mÃªmes donnÃ©es non chiffrÃ©es. Lâ€™intÃ©rÃªt dâ€™une telle mÃ©thode de chiffrement est notamment deÂ rÃ©soudre les problÃ©matiques de sÃ©curitÃ© liÃ©es Ã lâ€™externalisation de calculs portant sur des donnÃ©es sensibles,Â Ã lâ€™heure oÃ¹ le nombre de cyberattaques contre des acteurs du cloud computing croÃ®t chaque annÃ©e.

Si le concept est nÃ© dans les annÃ©es 1970, il faudra attendre prÃ¨s de quarante ans pour que Craig Gentry, informaticien amÃ©ricain, propose en 2009, dans sa thÃ¨se de doctorat, le premier systÃ¨me de chiffrement entiÃ¨rement homomorphe (*Fully Homomorphic Encryption*, FHE). Le chiffrement est ditÂ Â«Â entiÃ¨rement homomorpheÂ Â»Â car il supporte les opÃ©rations dâ€™additions et de multiplication un nombre arbitraire de fois. Et câ€™est le principe sur lequel repose le chiffrement.

Comme lâ€™explique Laria Chillotti dans sa thÃ¨se de doctorat sur ce sujet, soutenue en 2018 Ã lâ€™universitÃ© Paris-Saclay,Â *Â«Â dans tous les schÃ©mas de chiffrement homomorphe proposÃ©s, les chiffrÃ©s contiennent une petite quantitÃ© de bruit, nÃ©cessaire pour des raisons de sÃ©curitÃ©. Quand on fait des calculs sur les chiffrÃ©s Â«Â bruitÃ©sÂ Â», le bruit augmente et, aprÃ¨s avoir Ã©valuÃ© un certain nombre dâ€™opÃ©rations, ce bruit devient trop grand et, sâ€™il nâ€™est pas contrÃ´lÃ©, risque deÂ compromettreÂ le rÃ©sultat des calculsÂ Â»*. Lâ€™innovation proposÃ©e par Craig Gentry repose sur la notion deÂ *Â«Â bootstrapÂ Â»*, qui consiste selon lui Ã *Â«Â Â«Â rafraÃ®chirÂ Â»* *le message chiffrÃ©* *sansÂ le dÃ©chiffrer, en diminuant le bruitÂ Â»*. Depuis 2009, quatre gÃ©nÃ©rations de schÃ©mas de chiffrement homomorphe ont Ã©tÃ© proposÃ©es, le plus rÃ©cent datant de 2016, afin notamment dâ€™amÃ©liorer les opÃ©rations de dÃ©chiffrement dont le caractÃ¨re chronophage a longtemps empÃªchÃ© toute application pratique.

Prenons lâ€™exemple dâ€™un programme de recherche qui doit rÃ©aliser des calculs sur des donnÃ©es mÃ©dicales sensibles, comme des donnÃ©es biomÃ©triques, mais ne disposant pas dâ€™une puissance de calcul suffisante. Lâ€™Ã©quipe en charge de ce programme voudrait effectuer ces calculs sur EuroHPC, lâ€™infrastructure paneuropÃ©enne de supercalculateurs (voirÂ *La rem*Â nÂ°45, p.16). Dans

un scÃ©nario traditionnel de chiffrement asymÃ©trique, lâ€™Ã©quipe de recherche crypte les donnÃ©es mÃ©dicales sensibles avec une clÃ© publique afin de les envoyer vers EuroHPC. Ces mÃªmes donnÃ©es seront ensuite dÃ©chiffrÃ©es Ã lâ€™aide dâ€™une clÃ© privÃ©e pour Ãªtre confiÃ©es aux supercalculateurs. Enfin, les rÃ©sultats des calculs, ainsi que les donnÃ©es, seront Ã nouveau chiffrÃ©s avant dâ€™Ãªtre transmis Ã lâ€™Ã©quipe de recherche. Si les donnÃ©es sont bien cryptÃ©es lors de lâ€™envoi, les calculs portent en revanche sur des donnÃ©es en clair, ce qui est particuliÃ¨rement risquÃ©, voire interdit par la lÃ©gislation en vigueur.

Une solution sÃ©curisÃ©e de bout en bout consisterait, pour lâ€™Ã©quipe de recherche, Ã recourir au chiffrement homomorphe pour chiffrer les donnÃ©es mÃ©dicales sensibles avec une clef publique transmise Ã EuroHPC. Les supercalculateurs effectueraient alors les calculs demandÃ©s sur ces donnÃ©es non dÃ©chiffrÃ©es, tandis que les rÃ©sultats seraient dÃ©chiffrÃ©s par lâ€™Ã©quipe de recherÂche Ã lâ€™aide dâ€™une clef privÃ©e. GrÃ¢ce au chiffrement homomorphe,Â les donnÃ©es sur lesquelles EuroHPC a effectuÃ© des calculs seront restÃ©es chiffrÃ©es tout au long de la procÃ©dure, sans aucune altÃ©ration des rÃ©sultats, dont le dÃ©chiffrement revient uniquement au commanditaire initial.

Le vote Ã©lectronique fournit un autre exemple de lâ€™usage du chiffrement homomorphe. Un systÃ¨me de vote Ã©lectronique classique rassemble au mÃªme endroit les votes des participants, prÃ©alablement cryptÃ©s, qui sont alors dÃ©cryptÃ©s puis additionnÃ©s afin de calculer les rÃ©sultats du vote. Le dÃ©pouillement prÃ©sente donc un risque de fraude puisque les donnÃ©es sont dÃ©cryptÃ©es pour effectuer le comptage des voix.Â Un systÃ¨me de vote Ã©lectronique basÃ© sur le chiffrement homomorphe chiffre le vote dÃ¨s sa saisie et envoie les donnÃ©es sur un serveur oÃ¹ sont ensuite effectuÃ©es les additions, sans que les donnÃ©es aient eu Ã Ãªtre dÃ©chiffrÃ©es.

Quelques freins empÃªchent encore lâ€™usage Ã grande Ã©chelle de ce mode de chiffrement, notamment le ralentissement considÃ©rable du temps de calcul effectuÃ© sur des donnÃ©es chiffrÃ©es. En 2009, ce temps de calcul pouvait Ãªtre un milliard de fois supÃ©rieur au temps requis avec des donnÃ©es non chiffrÃ©es. NÃ©anmoins, la diversitÃ© des possibilitÃ©s dâ€™application du chiffrement homomorphe suscite fortement lâ€™intÃ©rÃªt des chercheurs et des entreprises, comme la sociÃ©tÃ© franÃ§aise Ravel Technologies, crÃ©Ã©e en 2018, au sein de laquelle une quinzaine de mathÃ©maticiens travaillent exclusivement Ã amÃ©liorer ce temps de traitement. En janvier 2023, lâ€™entreprise a annoncÃ© avoir dÃ©veloppÃ© un nouveau schÃ©ma de cryptage entiÃ¨rement homomorphique avec un temps de traitement extrÃªmement rapide. Mehdi Sabeg, prÃ©sident de la sociÃ©tÃ©, expliquait Ã cette occasion dans les colonnes deÂ *La Tribune*Â que,Â *Â«Â dans le processus, le chiffrÃ© du message contient du bruit qui augmente au fur et Ã mesure des traitements et quâ€™il faut gÃ©rer. 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 nÃ©cessitent le traitement de grands volumes de donnÃ©es avec une trÃ¨s faible latence, comme la publicitÃ© programmatique par exempleÂ Â»*.

Le chiffrement homomorphe rÃ©pond Ã©galement Ã un enjeu de souverainetÃ© numÃ©rique.Â LesÂ *hyperscalers*Â â€“ fournisseurs dâ€™infrastructures rÃ©pondant aux besoins de plus en plus importants du

big data â€“ et autres acteurs du cloud sont amÃ©ricains et lâ€™Europe ne sera vraisemblablement pas en mesure de rattraper son retard sur ce marchÃ© crucial. Or, lorsquâ€™une entreprise Ã©trangÃ¨re confie des donnÃ©es en clair Ã un acteur amÃ©ricain, le gouvernement des Ã‰tats-Unis, en vertu du Clarifying Lawful Overseas Use of Data Act, dit Cloud Act, votÃ© en mars 2018, peut contraindre cet acteur Ã lui communiquer des donnÃ©es personnelles stockÃ©es sur ses serveurs situÃ©s aux Ã‰tats-Unis ou dans un pays Ã©tranger, et ce, mÃªme si cette lÃ©gislation est en contradiction avec le rÃ¨glement gÃ©nÃ©ral pour la protection des donnÃ©es personnelles (RGPD) en Europe (voirÂ *La rem*Â nÂ°42-43, p.21).

Le chiffrement homomorphe contournerait cette extraterritorialitÃ© du droit amÃ©ricainÂ en permettant de confier aux incontournables prestataires amÃ©ricains du cloud des donnÃ©es chiffrÃ©es rendues inexploitables par autrui, Ã lâ€™exception de leur propriÃ©taire.

SourcesÂ :

- Â« Fully Homomorphic Encryption Using Ideal Lattices Â», Craig Gentry, thÃ¨se de doctorat, Stanford University et IBM Watson, 2009.
- Â« Le chiffrement homomorphe Â», Ely, linuxfr.org, 13 janvier 2014.
- Â« Vers lâ€™efficacitÃ© et la sÃ©curitÃ© du chiffrement homomorphe et du cloud computing Â», Ilaria Chillotti, thÃ¨se de doctorat en informatique soutenue Ã lâ€™universitÃ© Paris-Saclay (ComUE), dans le cadre de lâ€™Ã‰cole doctorale Sciences et technologies de lâ€™information et de la communication, en partenariat avec le Laboratoire de MathÃ©matiques de Versailles (laboratoire) et de lâ€™UniversitÃ© de Versailles-Saint-Quentin-en-Yvelines (Ã©tablissement opÃ©rateur dâ€™inscription), theses.fr, 17 mai 2018.
- Â« [Cahier Technique] Cryptographie homomorphe, lâ€™art de partager sans divulguer Â», Renaud Sirdey, Arnaud Grivet-SÃ©bert, CÃ©dric Goy-Pailler, usinenouvelle.com, 21 juillet 2022.
- Â« Bien comprendre le chiffrement homomorphe Â», GaÃ©tan Raoul, lemagit.fr, 7 octobre 2022.
- Â« Les promesses du chiffrement homomorphe pour traiter les donnÃ©es privÃ©es Â», ClÃ©mentine Laurens, lemonde.fr, 4 janvier 2023.
- Â« Innovation : cette startup franÃ§aise rÃ©volutionne le chiffrement homomorphe Â», Marc Endeweld, latribune.fr, 27 janvier 2023.

Categorie

1. Techniques

date crÃ©Ã©e
23 mai 2023
Auteur
jacquesandrefines