Thomas Lépine – 5A SAGI

Veille R&D – Chiffrement Homomorphe

Petit rappel général sur la cryptographie

La cryptographie c'est la science de la protection d'informations, à la frontière entre l'informatique et les mathématiques. Celle-ci est aujourd'hui partout, et permet de protéger des messages (assurant confidentialité, authenticité et intégrité) en s'aidant souvent de secrets ou clés. Un avantage de la cryptographie, c'est que les algorithmes qui la composent sont connus de tous, et donc sont vus et revus par une communauté afin de s'assurer qu'il n'y a pas de failles.

C'est bien beau tout ça, mais qu'est-ce que le chiffrement homomorphe ?

Chiffrement homomorphe – Présentation générale

En cryptographie, un chiffrement homomorphe est un chiffrement qui possède certaines caractéristiques algébriques qui le font commuter avec une opération mathématique, c'est-à-dire, que le déchiffrement du résultat de cette opération sur des données chiffrées donne le même résultat que cette opération sur les données non chiffrées. Cette propriété permet de confier des calculs à un agent externe, sans que les données ni les résultats ne soient accessibles à cet agent.

Des fichiers chiffrés peuvent être stockés sur un cloud, mais nous sommes tous d'accord pour dire que si l'on a besoin d'utiliser ces fichiers, par exemple modifier un fichier texte ou interroger une base de données, nous devons déchiffrer les données et les rendre vulnérables. Le chiffrement homomorphe complet ou FHE (Fully Homomorphic Encryption) est un système cryptographique créé par Craig Gentry, doctorant à Stanford et travaillant à IBM Research en 2009.

L'un des intérêts du chiffrement homomorphe est qu'un tiers peut faire des calculs sur les messages chiffrés sans les déchiffrer tout en permettant de rendre le résultat utilisable, c'est-à-dire déchiffrable. Autre exemple, plusieurs spécialistes médicales pourraient mettre à jour le dossier d'un patient, ajouter des ordonnances, etc, sans connaitre tout le dossier médical complet du patient. Le chiffrement homomorphe est un domaine de recherche actif encore aujourd'hui, afin de s'assurer qu'il remplisse toutes les fonctions recherchées, sans présenter de failles.

Chiffrement homomorphe – Types de chiffrement

La recherche d'une méthode générale de calcul sur les données chiffrées a constitué beaucoup de travaux de recherche depuis la publication du RSA en 1978. Le chiffrement homomorphique

« complet » n'est pas facilement atteignable, c'est pourquoi on distingue 3 types de chiffrement :

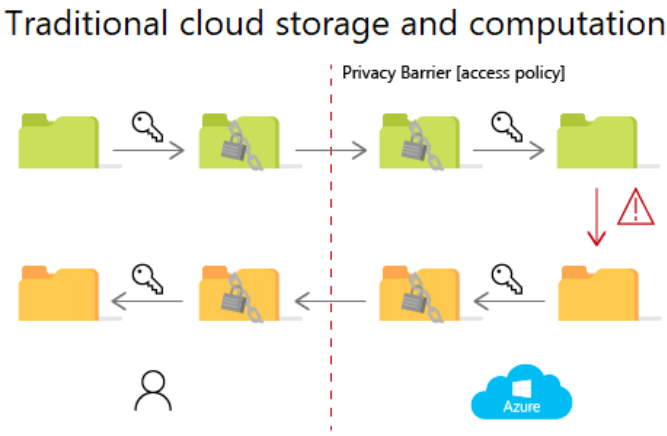
- Assez homomorphe (SHE Somewhat Homomorphic Encryption) où seulement les opérations d'additions et de multiplications sont possibles (en nombre limité).
- Partielle (PHE Partially Homomorphic Encryption) où uniquement certaines fonctions mathématiques peuvent être effectuées sur les valeurs chiffrées. Ainsi, une seule opération (addition ou multiplication) peut être effectuée un nombre de fois illimité sur le texte chiffré.
- Complète (FHE Fully Homomorphic Encryption)

Il reste encore de la recherche à effectuer afin d'essayer de généraliser l'utilisation du chiffrement dit « complet ».

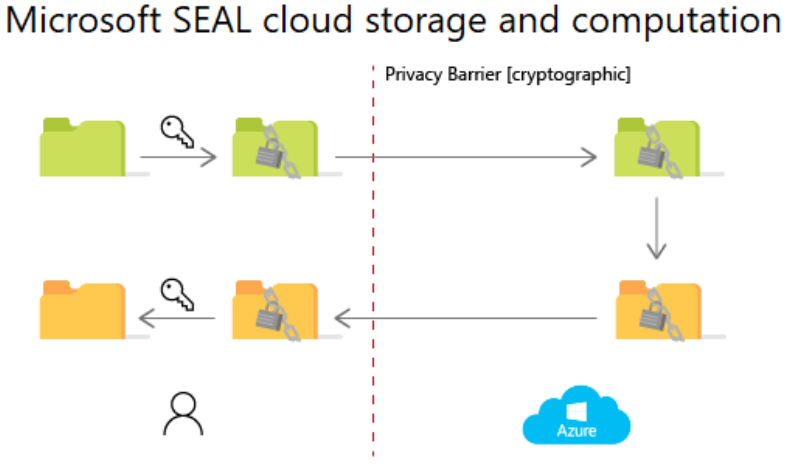
Chiffrement entièrement homomorphe – Intérêts

Le but du chiffrement entièrement homomorphe est d'autoriser les calculs sur des données encore chiffrées. Les données peuvent ainsi demeurer confidentielles lors de leur traitement afin de pouvoir effectuer des tâches utiles sur les données stockées dans des environnements non sécurisés. Petit bémol néanmoins, la mise en œuvre de FHE est difficile, il est encore au stade de développement pour que son utilisation soit généralisable.

Pour bien comprendre le but recherché, je propose un schéma trouvé sur le site de Microsoft résumant la situation. Si on prend l'exemple de fichiers chiffrés puis mis dans un cloud, pour faire des modifications dessus, il faut d'abord le déchiffrer, effectuer les modifications, puis le rechiffrer. Cela expose donc les données pendant plusieurs instants.



Au contraire, avec le chiffrement entièrement homomorphique, la modification se fait sur les données encore chiffrées.



Autre avantage, on peut par exemple ne récupérer qu'une seule partie des données et pas la totalité. Un type d'opération pourrait être une sorte de « masque » permettant de ne récupérer qu'une partie du contenu. Si je reprends mon exemple du dossier médical, le dentiste pourrait ne récupérer que les radios des dents et le groupe sanguin du patient par exemple, sans avoir accès aux données physiologiques ou aux maladies de celui-ci.

De plus, Craig Gentry a mentionné lors de sa soutenance de thèse que *« le chiffrement entièrement homomorphe présente de nombreuses applications. Il permet notamment de transmettre des requêtes privées à un moteur de recherche : l'utilisateur envoie une requête chiffrée et le moteur de recherche calcule une réponse chiffrée succincte sans même consulter la requête en texte clair. »* et permettrait donc ici aussi, d'empêcher certaines attaques ou violation de la vie privée qu'un « man in the middle » pourrait réaliser. Il ne pourrait pas comprendre les messages qui ont été échangé.

Chiffrement entièrement homomorphe – Limites

Une limite est visible sur les applications qui exécutent des algorithmes complexes et / ou volumineux. Le système de chiffrement entièrement homomorphe actuel nécessite beaucoup plus de temps pour effectuer les calculs sur la version chiffrée des données que sur une version déchiffrée. Bien que d'ordre polynomial, cette différence souvent assez importante entraîne un ralentissement des opérations. Donc si les fichiers sont stockés sur un cloud par exemple, il faut des serveurs puissants pour s'assurer de réaliser les opérations dans un temps acceptable.

Une partie de la recherche sur le chiffrement homomorphe consiste à limiter l'impact de la phase de réamorçage, soit en essayant de l'éviter au maximum, soit en en améliorant les performances pour le rendre moins rédhibitoire. Le réamorçage est la méthode qui repose sur l'idée suivante : puisque la qualité du chiffré se dégrade au fil des multiplications, si l'on est capable de déchiffrer homomorphiquement le chiffré, alors on obtient un nouveau chiffré nettoyé à l'évaluation homomorphe près. Le gros inconvénient de cette méthode est qu'elle reste encore coûteuse en puissance nécessaire.

Chiffrement homomorphe – Les grands acteurs

Plusieurs grandes entreprises ont déjà montré leur intérêt envers cette technologie et effectuent leurs propres recherches sur le sujet. On peut retrouver Microsoft qui ont réussi à résoudre plusieurs soucis que présentait le FHE et PHE. Ils proposent une suite d'outils de chiffrement homomorphique avec SEAL.

IBM est également un acteur important dans la recherche de ce type de chiffrement. Ils ont eux aussi développé des outils permettant de démocratiser ce chiffrement avec « IBM FHE Toolkit » disponible sur MacOs, Linux, iOS et prochainement sur Android.

CONCLUSION

Le chiffrement homomorphe représente l'avenir des techniques cryptographiques, car il permet d'effectuer des opérations sur des données chiffrées sans la nécessité de les déchiffrer. Ce type de chiffrement peut actuellement avoir des utilisations diverses, comme par exemple la sécurisation des données stockées sur le cloud, le stockage de données financières, système de e-vote, etc …

Les prochaines années nous diront si l'utilisation de ce type de chiffrement est généralisable et fonctionnelle pour tous les types d'utilisations, et s'il pourra rester sans failles face à la puissance des ordinateurs quantiques qui peuvent émerger à tout moment.

Sitographie

https://fr.wikipedia.org/wiki/Chiffrement_homomorphe

https://www.lemondeinformatique.fr/actualites/lire-ibm-veut-democratiser-le-chiffrement-homomorphe-complet-79345.html

https://www.youtube.com/watch?v=VLbe5WnQsDw

https://www.zdnet.fr/actualites/ibm-experimente-le-chiffrement-homomorphe-des-donnees-pour-l-entreprise-39915117.htm

https://www.venafi.com/fr/blog/le-chiffrement-homomorphe-definition-et-utilisation

http://www.bibmath.net/crypto/index.php?action=affiche&quoi=moderne/homomorphe

https://www.servicesmobiles.fr/cest-quoi-le-cryptage-homomorphique-dans-votre-smartphone-63152

https://www.ontrack.com/fr-fr/blog/le-chiffrement-homomorphe

https://docs.microsoft.com/fr-fr/azure/architecture/solution-ideas/articles/homomorphic-encryption-seal

https://blog.matlink.fr/chiffrement-homomorphique/

https://youtu.be/JyK1BnmXQwU

https://tel.archives-ouvertes.fr/tel-02150082

https://fhe-website.mybluemix.net/?_ga=2.79760799.920435847.1591368422-686610639.1585934283