

IBM aide à préparer ses clients à la prochaine génération de technologie de chiffrement

Les nouveaux services de chiffrement homomorphe de l'entité sécurité d'IBM offriront une formation, une assistance de la part d'experts et un environnement de test pour concevoir des applications prototypes en utilisant de nouvelles techniques de chiffrement. Un chiffrement totalement homomorphe pourrait permettre aux données sensibles de rester chiffrées, même lorsqu'elles sont analysées dans des environnements Cloud ou tiers.

ARMONK, N.Y., 17 décembre 2020 : Aujourd'hui, IBM Security a lancé un nouveau service qui permet aux entreprises d'expérimenter le chiffrement totalement homomorphe (Fully Homomorphic Encryption : FHE) - une technologie émergente conçue pour permettre aux données de rester chiffrées même lorsqu'elles sont traitées ou analysées dans des environnements Cloud ou tiers. Les nouveaux services de chiffrement homomorphe d'IBM Security offrent aux entreprises une formation, une assistance de la part d'experts et un environnement de test permettant aux clients de développer des applications prototypes pouvant tirer parti du FHE.

Avec la croissance du Cloud hybride, les données sensibles seront encore plus largement stockées, partagées et analysées entre les plateformes et différents acteurs, les exposant à divers risques de sécurité. Alors que les techniques de chiffrement actuelles permettent de protéger les données pendant leur stockage et leur transit, les données doivent être déchiffrées pendant leur traitement ou leur analyse – ce qui crée une fenêtre d'opportunité pendant laquelle les données sont plus vulnérables au vol ou à l'exposition. Le FHE est une technologie de chiffrement émergente et avancée qui permet aux données de rester chiffrées y compris pendant leur traitement, ce qui pourrait combler cette lacune critique dans les solutions de chiffrement actuellement utilisées.

*« Le chiffrement totalement homomorphe offre un potentiel énorme pour l'avenir de la protection de la vie privée et du Cloud computing, mais les entreprises doivent commencer à se familiariser avec le FHE et à l'expérimenter avant de pouvoir tirer pleinement parti de ce qu'il a à offrir », a déclaré **Sridhar Muppidi, Chief Technology Officer, IBM Security**. « En apportant à nos clients l'expertise et les ressources d'IBM en matière de cryptographie, qui stimulent l'innovation dans leurs secteurs d'activité spécifiques, nous pouvons travailler ensemble pour créer une nouvelle génération d'applications qui tirent parti des données sensibles, sans compromettre leur confidentialité. »*

S'appuyant sur le travail et les outils développés par IBM Research et IBM Z, les nouveaux services de chiffrement homomorphe d'IBM Security fournissent un environnement d'hébergement évolutif sur IBM

Cloud, ainsi que des services de conseil et d'infogérance pour aider les clients à commencer à s'informer et à concevoir des solutions prototypes qui peuvent tirer parti du FHE.

Avec les progrès de la technologie FHE, ces solutions peuvent permettre aux entreprises d'appliquer des fonctions telles que la recherche, l'analyse et l'IA à leurs données sensibles dans un environnement, sans révéler ces données aux autres services - ce qui les aide à maintenir la conformité et la confidentialité dans le cadre d'une stratégie de sécurité "zero trust". De plus, le FHE est basé sur la cryptographie par réseau euclidien qui est considérée comme « résistante aux ordinateurs quantiques », c'est-à-dire résistante à la vitesse de calcul de ces ordinateurs.

Comblant le fossé entre la recherche et l'adoption précoce

Les algorithmes de FHE sont en cours de développement par IBM et la communauté des chercheurs depuis plus d'une décennie, mais les calculs FHE étaient à l'origine trop lents pour une utilisation quotidienne - il fallait des jours ou des semaines pour des calculs qui prennent quelques secondes sans chiffrement. Avec la croissance exponentielle de la puissance de calcul de l'industrie et les progrès des algorithmes de FHE, les tests ont montré que le FHE peut désormais être exécuté en quelques secondes par bit[1], ce qui le rend suffisamment rapide pour de nombreux types de cas d'usage dans le monde réel et pour les premiers essais avec les entreprises.

Gartner estime que d'ici 2025, au moins 20 % des entreprises disposeront d'un budget pour des projets incluant le chiffrement totalement homomorphe, contre moins de 1 % aujourd'hui[2].

Au début de l'année, IBM a publié des outils et du matériel pédagogique pour les développeurs et a travaillé avec certains clients sur les premiers [programmes pilotes](#) pour le FHE. IBM Security passe maintenant à l'étape suivante pour faire connaître le FHE à un public plus large, en lançant une offre de service unique en son genre pour aider les entreprises à se lancer dans le chiffrement totalement homomorphe.

Disponibles dès aujourd'hui, les nouveaux [services de chiffrement homomorphe d'IBM Security](#) sont conçus pour aider à éduquer et préparer les clients à concevoir et déployer des applications compatibles FHE à mesure que la technologie atteindra sa maturité dans un avenir proche. Le service comprend l'accès à la fois aux outils et à l'expertise nécessaires pour démarrer avec le FHE, notamment :

- Les outils de FHE développés par IBM Research, qui fournissent des modèles pour les cas d'usage courants de FHE tels que la recherche chiffrée, l'IA et le machine learning
- Des indications, du conseil et une assistance pédagogique fournis par des experts en cryptographie d'IBM, aidant les entreprises à acquérir les compétences nécessaires pour concevoir et travailler avec des applications compatibles FHE
- Un environnement d'hébergement évolutif sur IBM Cloud permettant aux développeurs de commencer

à expérimenter et à concevoir des prototypes pour leurs propres applications compatibles FHE

Dans le cadre de ce service, IBM travaillera en étroite collaboration avec ses clients pour développer de nouveaux prototypes et de nouveaux cas d'usage pouvant tirer parti de la technologie FHE - l'offre initiale étant axée sur les développeurs et les ingénieurs en cryptographie. Certains des cas d'usage initiaux comprennent la réalisation d'analyses sur des données chiffrées, la conduite de recherches chiffrées tout en dissimulant la requête et le contenu de la recherche, puis l'entraînement de modèles d'IA et de machine learning tout en maintenant les contrôles de confidentialité et de respect de la vie privée existants.

Ressources complémentaires et multimédias :

- Kit média : Pour des images, des vidéos et du contenu additionnel sur le chiffrement totalement homomorphe (FHE), son fonctionnement et les cas d'usage potentiels :
<https://newsroom.ibm.com/Homomorphic-Encryption-Services>
- Pour en savoir plus sur les nouveaux services de chiffrement totalement homomorphe d'IBM Security :
ibm.com/security/services/homomorphic-encryption
- Inscrivez-vous [ici](#) pour un webinaire d'IBM Security sur le FHE et la nouvelle offre, qui aura lieu le 21 janvier 2021

A propos d'IBM Security

IBM Security offre aux entreprises l'une des gammes de produits et services de sécurité les plus performantes et intégrées du marché. Ce portefeuille, qui repose sur les recherches du mondialement célèbre IBM X-Force®, permet aux organisations de gérer efficacement les risques et de se défendre face aux menaces émergentes. IBM compte parmi les plus grandes organisations mondiales dédiées à la recherche, au développement et à la conception de solutions de sécurité, gère 70 milliards d'événements de sécurité par jour dans plus de 130 pays, et possède plus de 10 000 brevets dans le domaine de la sécurité. Pour de plus amples informations, rendez-vous sur <https://www-03.ibm.com/security/fr-fr/>, suivez IBM Security sur Twitter ou consultez [le blog IBM Security Intelligence](#).

Contacts presse :

IBM

Gaëlle Dussutour

Tél. : + 33 (0) 6 74 98 26 92

dusga@fr.ibm.com

Weber Shandwick pour IBM

Robin Legros / Eric Chauvelot

Tél. : + 33 (0)6 68 04 57 83 / +33 (0)6 21 64 28 48

ibmfrance@webershandwick.com

[1] FHE has been demonstrated at speeds of seconds per bit in select research/field trials.

[2] Gartner, “Emerging Technologies: Homomorphic Encryption for Data Sharing With Privacy,” Mark Driver, 23 April 2020.
