Chiffrement homomorphe : IBM passe à la phase commerciale

Le chiffrement homomorphe devient une réalité commerciale chez IBM. Le groupe américain vient de lancer une offre sur son cloud public. Il y a intégré sa « boîte à outils » *open source* fondée sur la bibliothèque logicielle HElib*. Et l'a assortie d'un environnement de développement.

L'ensemble s'accompagne de prestations de conseil. En ligne de mire, deux usages en particulier : l'analyse de données et l'entraînement de modèles d'apprentissage automatique. Et de manière générale, toute opération impliquant le traitement d'informations qu'on a des raisons de conserver chiffrées. IBM évoque entre autres l'identification biométrique, l'étude de données comportementales à des fins de lutte contre la fraude et le partage d'informations entre établissements de santé.

Aucun tarif n'est pour le moment communiqué au public. On surveillera notamment les coûts d'infrastructure, au vu des ressources de calcul qu'exige le chiffrement homomorphe.

** IBM développe HElib depuis 2009 et l'a placée en* open source *en 2013. La bibliothèque implémente les cryptosystèmes de Brakerski-Genrty-Vaikuntanathan et de Cheon-Kim-Kim-Song. Elle permet un chiffrement qualifié de « totalement homomorphe ». Ce au sens où l'ensemble des fonctions calculables peuvent être évaluées (sur les plans additif et multiplicatif).*

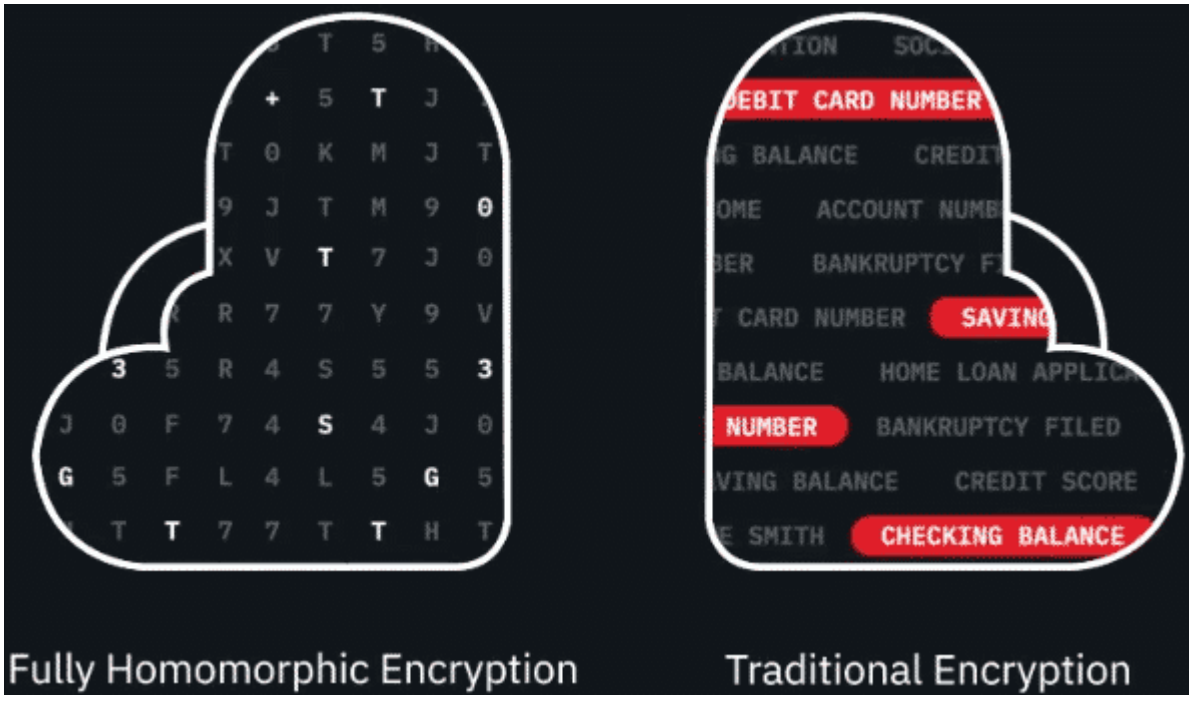

Illustration principale © Sergey Nivens – shutterstock.com