Clémence Audibert
Alexis Mellier
Gabrielle Lalou

Rapport Artishow

Quels sont les enjeux sociaux et environnementaux de notre projet ?

Contexte

L'algorithme dit de Secret Sharing, inventé par Shamir en 1979, permet à un dealer possédant un secret *s* de générer ce qu'on appelle des shares de *s* et de les distribuer à un nombre *n* de personnes en qui il ne fait pas totalement confiance. L'étape vulnérable du secret sharing est la distribution des shares, une autre faiblesse est qu'un dealer corrompu pourrait mal former les shares, de sorte qu'elles ne garantiraient pas l'unicité du secret reconstruit. Dans ce contexte, notre travail est de poser le socle théorique nécessaire à la compréhension du modèle et à l'implémentation dans un premier temps, et puis de travailler sur l'implémentation dans un second temps. Dans cette deuxième partie, nous utilisons la bibliothèque RUST TFHE de Zama qui permet le chiffrement homomorphe avec LWE (*Learning With Error*).

Applications

On peut retrouver cet algorithme aussi bien dans le calcul distribué sur des secrets partagés, dans des élections (dont il préserve la confidentialité), dans la délégation d'un portefeuille digital à plusieurs machines dont aucune n'est de confiance, divulgation automatique d'un secret générée suite à un événement public…

L'algorithme pourra également être très utile en cryptographie post-quantique. Le problème LWE a déjà permis de trouver des protocoles de key sharing, chiffrement et chiffrement homomorphe ; le Shamir Secret Sharing est de plus très intéressant en termes de complexité.

Confidentialité des Données et Réduction des Risques de Violation de Données

Pour rappel, l'algorithme de Shamir permet de diviser un secret en plusieurs parts, distribuées à différentes personnes. Il contribue ainsi à réduire les risques de violation de données. Les techniques traditionnelles de stockage centralisé sont souvent plus vulnérables aux attaques de pirates informatiques. En utilisant Shamir Secret Sharing, les données sont dispersées, ce qui rend la tâche des dealers beaucoup plus difficile.

Le chiffrement homomorphe offre ensuite une solution efficace aux entreprises et institutions étatiques confrontées au dilemme d'effectuer des calculs sur des données confidentielles tout en préservant leur sécurité. Celle-ci peut être cruciale dans des domaines tels que la santé, la finance ou les communications gouvernementales, où la confidentialité des individus et le bon fonctionnement des institutions sont en jeu.

Souvent, des contraintes financières et matérielles obligent institutions et entreprises à externaliser ces calculs vers du cloud computing. Mais celles-ci s'inquiètent de confier leurs informations sensibles à des tiers, craignant les risques de divulgation ou d'exploitation malveillante.

C'est là que le chiffrement homomorphe entre en jeu. Ce chiffrement résout ce problème en permettant l'exécution d'opérations sur des données chiffrées, préservant ainsi leur confidentialité même lorsqu'elles sont traitées dans le cloud. Cela signifie que les entreprises et institutions peuvent profiter des capacités de calcul du cloud sans compromettre la sécurité de leurs informations sensibles.

Ethique et Collaboration

En utilisant le Shamir Secret Sharing dans notre implémentation, nous répondons de plus aux défis éthiques liés au partage de secrets, étape primordiale lors de la collaboration d'individus. Il s'agit en effet de distribuer la clé secrète en plusieurs parts, c'est-à-dire de

garantir la confidentialité tout en répartissant la confiance de manière équitable. Cela garantit la protection des données tout en minimisant les risques de compromission ou d'abus de pouvoir.

Impact Environnemental

L'utilisation de l'algorithme de Shamir Secret réduit en principe la consommation d'énergie en évitant de centraliser les shares dans des data centers et en les distribuant à plusieurs ressources informatiques. Leur utilisation devient ainsi plus efficace et l'empreinte carbone de l'industrie technologique est diminuée.

Cependant, l'utilisation de cet algorithme peut aussi entraîner une augmentation de la consommation de ressources informatiques, notamment en termes de puissance de calcul nécessaire pour l'évaluation, distribution, et la reconstruction des parts de clés.

Pour le chiffrement homomorphe, au moment d'appliquer des opérations aux données, entreprises et institutions recourent cette fois au cloud computing. Celui-ci réduit en effet la nécessité pour elles d'investir massivement dans du matériel informatique coûteux, et minimise leurs besoins de maintenance et de mise à niveau. Cette approche permet ainsi de limiter l'empreinte carbone associée à la fabrication, à la mise en service et au remplacement fréquent de ces équipements.

Ce type de chiffrement demande certes des ressources supplémentaires et plus de temps pour effectuer les opérations, augmentant la consommation énergétique des data centers. Cette augmentation de la demande en ressources pourrait entraîner une empreinte carbone plus importante pour ces centres. Cependant, ils s'orientent vers une utilisation de plus en plus responsable de l'énergie - Google, Microsoft et AWS se sont par exemple engagés à alimenter leurs centres de données avec 75 % d'énergie renouvelable d'ici 2025, et prévoient d'être totalement neutres en carbone d'ici 2030. La réduction de l'empreinte carbone des entreprises et l'orientation plus sobre des data centers résulte ainsi en une diminution de la consommation énergétique globale.

Défis Économiques

Du point de vue économique, l'adoption généralisée du chiffrement homomorphe influence aussi les modèles commerciaux liés au cloud computing. La capacité à garantir un niveau de sécurité et de confidentialité supérieur peut constituer un avantage compétitif pour les fournisseurs de services cloud.

Cependant, les entreprises spécialisées dans le stockage de données en data centers pourraient voir leur modèle commercial menacé par l'algorithme de Shamir, très décentralisé.