Titre : Le chiffrement cherchable autorisé - de la théorie à la pratique

Encadrantes : Nesrine Kaaniche et Maryline Laurent

Contexte et description :

Le chiffrement cherchable (SE) [1] est une technique de chiffrement avancé qui permet aux utilisateurs de faire une recherche par mots clés chiffrés sur des données chiffrées. L'objectif du SE est d'externaliser l'opération de recherche à un tiers (un médiateur, par exemple un serveur de stockage distant), qui va travailler à l'aveugle sur une base de données, c'est-à-dire il va identifier les données pertinentes sans avoir à les déchiffrer. Le SE est particulièrement utile pour les scénarios de réutilisation des données.

Cependant, les systèmes SE existants posent la question de l'autorisation et de la délégation dynamique, permettant à différents utilisateurs d'accéder à des sous-ensembles de données externalisées. Ce besoin est accompagné d'un cadre juridique rythmé par les lois et directives autour de la protection de la vie privée (GDPR, e-privacy), qui assure la régulation de la collecte, du stockage et de l'utilisation des données, incluant entre autres le principe de la minimisation de données. Dans ce contexte, plusieurs approches ont été proposées, notamment en s'appuyant sur des primitives cryptographiques, telles que le chiffrement à base d'attributs [2, 3].

Dans ce contexte, l'objectif du projet consiste en :

- L'étude du schéma de chiffrement cherchable autorisé à base d'attributs
- L'analyse des propriétés de sécurité et de protection de la vie privée (privacy) du schéma proposé pour un scénario de réutilisation des données
- L'implémentation des différentes briques logicielles

Compétences requises :

- De bonnes connaissances en mathématiques (Algèbre linéaire)
- Bon niveau en développement (Python et C)

Livrables :

- Prototype du schéma SE
- Rapport synthétisant tous les aspects : la description de la solution, l'analyse des propriétés, l'implémentation, les difficultés rencontrées, …

Références :

1. Bösch, C., Hartel, P., Jonker, W. and Peter, A., 2014. A survey of provably secure searchable encryption. *ACM Computing Surveys (CSUR)*, *47*(2), pp.1-51
2. Michalas, A., 2019, April. The lord of the shares: Combining attribute-based encryption and searchable encryption for flexible data sharing. In Proceedings of the 34th ACM/SIGAPP symposium on applied computing (pp. 146-155).
3. Yin, H., Zhang, J., Xiong, Y., Ou, L., Li, F., Liao, S. and Li, K., 2019. CP-ABSE: A ciphertext-policy attribute-based searchable encryption scheme. IEEE Access, 7, pp.5682-5694.