Titre : Analyse et implémentation d'un schéma de signature post-quantique préservant la vie privée

Encadrantes : Nesrine Kaaniche et Maryline Laurent

Contexte et description:

La sécurité de la cryptographie usuelle repose sur des problèmes mathématiques réputés difficiles à résoudre, par exemple, trouver un logarithme discret ou décomposer de grands nombres en facteurs premiers. Toutefois, cette cryptographie est menacée par une percée technologique : l'ordinateur quantique. En effet, les ordinateurs classiques et quantiques reposent sur des modes de fonctionnement différents, ce qui rend les ordinateurs quantiques capables de résoudre efficacement plusieurs problèmes mathématiques, notamment le logarithme discret. Cette menace intéresse le monde scientifique académique et industriel, qui continue à proposer des alternatives pouvant lui résister. L'une de ces alternatives, parmi les plus prometteuses aujourd'hui, repose sur des problèmes géométriques d'un objet mathématique, connu sous le nom du réseau Euclidien.

Avec le développement des systèmes d'informations et l'émergence de services de données avec des cycles de vie qui peuvent s'étendre sur plusieurs décennies, plusieurs acteurs se préparent à cette transition. Cette transition est accompagnée 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 personnelles, incluant entre autres le principe de la minimisation de données (e.g., en s'authentifiant à un service) [3].

Télécom SudParis a proposé les premières briques d'une solution d'authentification basée sur FALCON (FALCON est un schéma de signature basé sur les réseaux euclidiens et proposé à la standardisation NIST [1,2]) et les preuves à apport nul de connaissance (zero knowledge proof) adapté aux réseaux Euclidiens.

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

- L'étude du schéma d'authentification proposé.
- L'analyse de propriétés de sécurité et protection de la vie privée de la solution d'authentification
- La proposition d'amélioration du schéma et implémentation des différentes briques.

Compétences requises :

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

Livrables :

- Prototype du schéma de signature post-quantique
- Rapport

Références :

1. https://csrc.nist.gov/Projects/post-quantum-cryptography
2. https://csrc.nist.gov/projects/post-quantum-cryptography/round-3-submissions
3. Kaaniche, N., Laurent, M., & Belguith, S. (2020). Privacy enhancing technologies for solving the privacy-personalization paradox: Taxonomy and survey. JNCA