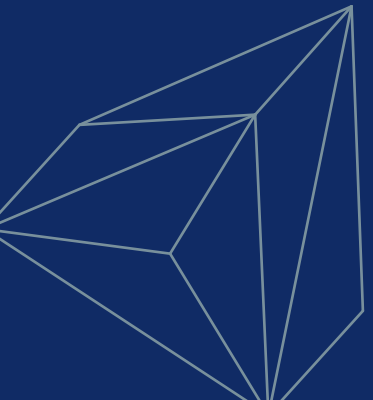
CIA

Vue d'ensemble

Loïc Rouquette

Présentation Générale



Déroulement du Cours

- CM : $4 \times 2h$
- TP : $6 \times 3h$

Plan

Séance 1 : CM1
Fondations de la Communication Sécurisée

Séance 2 : TP 1
Mise en place d'un canal TLS

Séance 3 : CM2
Chiffrement authentifié pour l'IIoT

Séance 4 : TP2
Protection d'un flux de données de capteur

Séance 5 : CM3
Signatures classiques et post-quantiques

Séance 6 : TP3
Benchmark de signatures numériques

Séance 7 : TP4
Prototypage d'un processus sécurisé OTA

Séance 8 : CM4
Les nouvelles frontières de la cryptographie

Séance 9 : CM 5
Échange de clés post-quantiques avec un KEM

Séance 10 : TP 5
Première Analyse Homomorphe

Acquis d'apprentissage visés

À la fin du cours, en s'appuyant sur des bibliothèques cryptographiques standards, les étudiants seront capables de :

- **Configurer** un canal de communication sécurisé (via TLS 1.3) entre deux applications, en sélectionnant une suite de chiffrement (**cipher suite**) adaptée aux contraintes de performance et de sécurité.
- **Utiliser** une bibliothèque pour appliquer un schéma de chiffrement authentifié léger afin de protéger un flux de données dans un scénario IIoT.
- **Comparer** par l'expérimentation les performances (latence, usage CPU) de différents algorithmes de signature (RSA, ECDSA, Dilithium) pour un cas d'usage de validation de commande machine.
- **Intégrer** une signature numérique dans un processus de mise à jour logicielle (**Secure OTA**) pour en garantir l'authenticité et l'intégrité.
- **Mettre en œuvre** un échange de clés sécurisé au sein d'un prototype, en substituant un Mécanisme d'Encapsulation de Clé (KEM) post-quantique à un algorithme classique (Diffie-Hellman).
- **Opérer** une analyse statistique simple (ex: une moyenne) sur des données chiffrées en utilisant une bibliothèque de cryptographie homomorphe.

Évaluations

- Contrôle continu : 40% (2 notes de TP)
- Projet final : 60%