Cryptographie Avancée

Un aperçu

Yann Rotella

UVSQ - Université Paris-Saclay

23 avril 2026

Plan du Cours

Questions

Anonymat

Les backdoors

Le FHE

D'autres trucs funs

Dernier moment pour poser des questions

- Avez-vous des questions ?

Plan du cours

1. Histoire de la cryptographie (jusqu'à 1950)
2. Théorie de Shannon, concept de sécurité
3. Définitions de Sécurité et Primitives
4. Stratégies de Conceptions (des Chiffrements par Bloc)
5. Cryptanalyse des Chiffrements par Bloc
6. Fonctions de Hachage Cryptographiques
7. Modes Opératoires, MACs et AEAD
8. Arithmétique, Diffie-Hellman, El-Gamal et Réductions
9. Arithmétique, RSA, RSA-OAEP
10. Signatures numériques et authentification
11. Certificats, protocoles et confiance
12. Aperçu de Cryptographie Avancée

L'ANONYMAT ET LE RÉSEAU TOR

OBJECTIF

*Préserver **au mieux** l'anonymat.*

- Dans une communication classique, même chiffrée, un observateur sait quelle adresse IP parle à quelle adresse IP
- ✍ Une solution : le réseau Tor et le routage dit « en onion ».

Les portes dérobées (backdoors)

Principe

*Mettre **intentionnellement** une faiblesse dans un algorithme de chiffrement la cacher et la garder*

- ✍ Quel principe du cours est réaffirmé par l'existence de telles techniques ?
- Conception des algorithmes de chiffrement : par qui ?
- Le cas de `DUAL_EC_DRBG`.
- Le cas de `GEA 1`.
- Le cas de `Kuznyechik` ?

Le chiffrement complètement homomorphe

Principe

On souhaite réaliser des opérations sur des données chiffrées sans révéler le clair. On veut un chiffrement tel que pour tout m_1 et m_2, on ait

- $\mathrm{Enc}(pk, m_1 + m_2) = \mathrm{Enc}(pk, m_1) \circ \mathrm{Enc}(pk, m_2)$
- $\mathrm{Enc}(pk, m_1 \times m_2) = \mathrm{Enc}(pk, m_1) \cdot \mathrm{Enc}(pk, m_2)$

✍ Applications ?

✍ Performances ?

Questions

Anonymat

Les backdoors

Le FHE

D'autres trucs funs

Et plein d'autres !

- Les preuves à divulgation nulles de connaissance
- Calcul MultiPartite Sécurisé (MPC)
- Cryptographie Post-Quantique (Réseaux, Codes, Multivariable, Isogénies)
- Cryptographie Quantique (BB84)
- Cryptanalyse