But du projet

Les projets peuvent être réalisés par groupe de 2 max.

Que faire:

• Choisissez un partenaire (ou décidez de travailler seul).

• Choisissez un sujet dans la liste ci-dessous.

• Documentez-vous sur le sujet choisi et écrivez un maximum de 10 rapport de page répondant aux questions suivantes :

1. Quel est le but de cette technologie ?

2. Décrire le contexte historique, les articles fondateurs, les articles sur le sujet....

3. Est-ce un sujet brûlant aujourd'hui ? Pourquoi?

4. Coût de déploiement ?

5. Algorithmes, implémentations, performances, tableaux de benchmark, systèmes d'exploitation pris en charge (win/mac/linux/android/ios) ?

6. Avantages et inconvénients ?

7. Menaces en termes de cryptanalyse et/ou attaques sur le protocole, cibles potentielles…

• Faites une présentation expliquant le sujet devant la classe.

Thèmes proposés

• Codes correcteurs d'erreurs et compression : code de Hamming, Code Huffman, capacité du canal, bruit, etc.

• Les MAC et leurs constructions : HMAC, Davies-Meyer construction, SHA3 comme MAC, etc. Antoine & Hugo

• Signatures : (EC)DSA, Signature Schnorr, . . .

• Cryptage authentifié : Encrypt-then-MAC, MAC-then-Encrypt, modes spéciaux tels que GCM, . . .

• La complexité de la factorisation et son implication sur les tailles clés : Guillisa

• La dureté du logarithme discret sur les corps finis et sa implication sur les tailles de clé

• La dureté du logarithme discret sur les courbes elliptiques et courbes hyperelliptiques et leur implication sur les tailles clés

• Keccak/SHA-3 Sacha et Julien

• Cryptographie basée sur un réseau

• Les menaces d'un ordinateur quantique sur la cryptographie classique : Loan Théo

• Preuves sans connaissance

• Calcul multipartite sécurisé

• Cryptage (entièrement) homomorphe

• Protocoles TLS & IKE (d'un point de vue crypto) : Kelyan MARCHAL et David CHRUSCIEL

• Attaques par canal latéral

• Autre chose si vous avez une bonne idée ! (demandez-moi d'abord ...)

Documentation

Vous êtes autorisé à regarder Wikipedia. Mais le copier-coller, c'est stupide ! Recommandations :

• En général, pensez toujours : quelle crypto, où et pourquoi ? (cryptosystème, taille des clés, . . . )

• Quelles garanties de sécurité, quels adversaires, . . . ?

• Pensez à l'avenir : est-ce que ce cryptosystème/technologie viable à long terme ?

• Donnez des informations pertinentes aujourd'hui ! Il n'y a pas des années .....

• Les papiers cryptographiques sont la plupart du temps disponibles sur eprint.iacr.org. Si vous avez besoin d'un papier et que vous ne le trouvez pas, demandez moi!

Le plus important : motivez, argumentez et expliquez vos résultats !

Chronologie

Dates limites :

• Choix des groupes et des sujets : 11 février

• Planification du rapport : 14 mars

• Rapport : 16 mai

• Présentation orale : 23 mai 2022

Évaluation:

• Grade R pour le rapport et grade S pour la présentation

• Peut être différent pour deux membres d'un groupe

• Note finale du projet : (R + S)/2