CRYPI - Project 5: E-voting based on Homomorphic Encryption

Paul LEROUX – Paul FRANCOIS-MARSAL
Erwan Polès – Julien LUNG-YUT-FONG

Sommaire

I. Vue d’ensemble de l’Homomorphic Encryption

II. Choix du protocol utilisé

III. Critères et processus de sélection de la bibliothèque

IV. Résultats des expériences menées

V. Défis rencontrés au cours du projet

VI. Mesures recommandées pour améliorer le projet

I - Vue d'ensemble de l'Homomorphic Encryption

Homomorphic : opérations sans déchiffrer

Protection de la vie privée

utile pour l'e-voting : **ne jamais dévoiler les votes**

Variantes : Partiellement homomorphe (PHE)

Totalement homomorphe (FHE)

Semi-partiellement homomorphe (FHE)

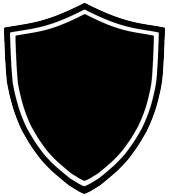
II - Choix du protocole utilisé

BFV (Brakerski-Fan-Vercauteren)

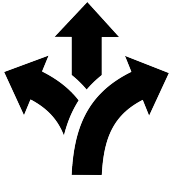
Performances et efficacité

Vitesse d’exécution

Résistance aux attaques



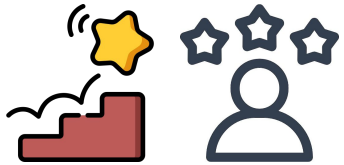
Flexibilité



III - Critères et processus de sélection de la bibliothèque

Sécurité

Popularité



Performances, efficacité

Facilité d’utilisation

Windows SEAL

IV - Résultats des expériences menées

Expériences : 

chiffrement / déchiffrement d'un nombre

chiffrement d'un vote

addition / multiplication

cas réel : 10 000 votes

Statistiques : 

chiffrement moyen : ~10ms

déchiffrement moyen: ~20ms

addition homomorphe: ~100ms

multiplication homomorphe: ~200ms

Résultats : 

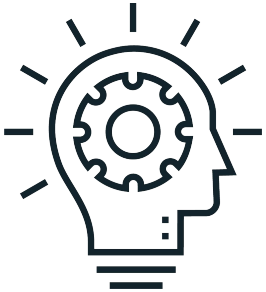
impact de la **taille de clé**

compromis entre sécurité et performance

SEAL : bibliothèque performante

V - Défis rencontrés au cours du projet

Comprendre le FHE



Stockage de données

Développer le site web

Authentification

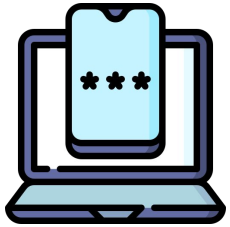
VI - Mesures recommandées pour améliorer le projet

Accessibilité du site

Base de données identifiant électeurs

Connexion HTTPS

Double authentification



Merci de nous avoir écouté