GossipGuard

GOSSIPGUARD

SÉCURITÉ QUANTIQUE POUR LA COMMUNICATION INTER-PROCESSUS

Présenté par:
youssra zarri
hiba sidinou
amal sab
oussama bagy
noussair bouanani
fatimaezzahra ennassiri

Encadré par:
prof ali azougagh

GossipGuard

INTRODUCTION

GossipGuard

COMPRENDRE L'IPC

POURQUOI L'IPC EST ESSENTIEL

L'isolation empêche les conflits entre processus

Mais pour collaborer, les processus doivent communiquer

Exemples :

- Serveur web et traitement d'image
- Application vidéo (filtrage, rendu)

GossipGuard

Pourquoi avoir utilisé les signaux ?

Avantages

- Légers et rapides
- Faciles à implémenter
- Idéaux pour des notifications simples

Inconvénients

- Peu de données (juste un numéro)
- Risque de fusion ou perte de signaux
- Asynchronisme difficile à gérer

GossipGuard

CRYPTOGRAPHIE POST-QUANTIUE

un ensemble de techniques de chiffrement conçues pour rester sécurisées même face à la puissance des ordinateurs quantiques. Elle vise à remplacer les algorithmes classiques, comme RSA, qui pourraient être cassés facilement à cause de nouveaux algorithmes quantiques comme celui de Shor.

GossipGuard

INTRODUCTION À MCELIECE

Proposé en 1978 par Robert McEliece, cet algorithme utilise des codes correcteurs d'erreurs pour assurer la sécurité, et est une des premières solutions contre les ordinateurs quantiques.

Bien que jugé trop lent au début à cause des grandes tailles de clés, les progrès en calcul ont ravivé son intérêt pour la cryptographie post-quantique.

McEliece est l'un des algorithmes les plus prometteurs pour contrer les attaques quantiques, contrairement à RSA et ECC qui sont vulnérables

GossipGuard

McEliece - Processus simplifié

Génération de clés:

- Clé privée = code correcteur + matrices secrètes
- Clé publique dérivée de la clé privée

Chiffrement :

- Message clair multiplié par la clé publique
- Ajout d'erreurs contrôlées pour sécuriser

Déchiffrement :

- Utilisation de la clé privée
- Correction des erreurs pour retrouver le message original

GossipGuard

Avantages Et Inconvénients

01

avantages

- Résistant aux attaques des ordinateurs quantiques
- Algorithme éprouvé et robuste
- Bonne efficacité pour les grandes clés

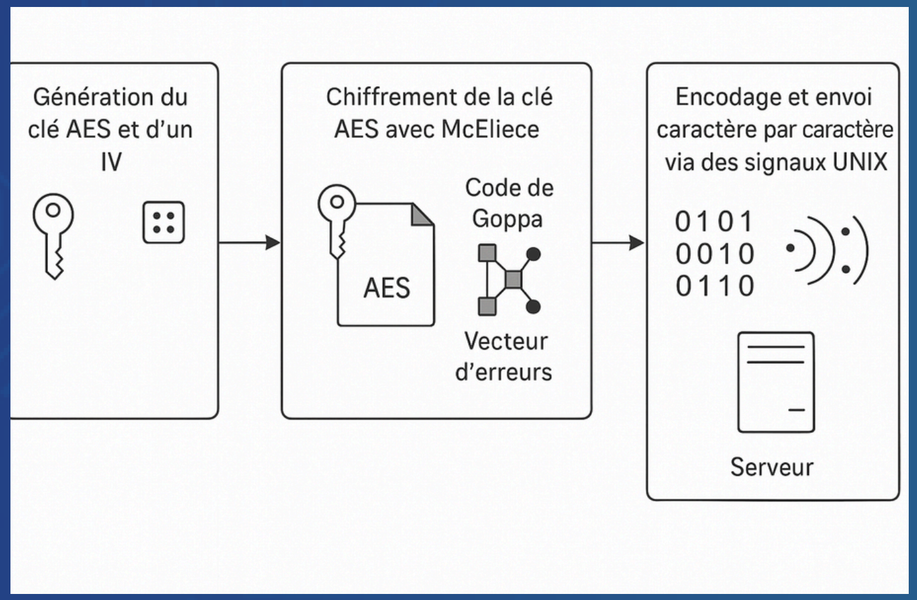
02

Inconvénients

- Taille des clés très grande
- Impact possible sur la vitesse et la performance

GossipGuard

CHIFFREMENT AES ET MCELIECE DANS GOSSIPGARD



Le message est chiffré avec AES, un algorithme symétrique rapide et efficace, et ensuite la clé AES elle-même est chiffrée avec McEliece, un algorithme asymétrique qui est résistant aux attaques quantiques.

- **Pourquoi ce choix ?**

Parce que AES est très performant pour chiffrer les données rapidement, mais il faut protéger la clé AES, sinon on peut déchiffrer le message. Donc on utilise McEliece, qui permet de sécuriser la clé AES même face à un attaquant très puissant, comme un ordinateur quantique.

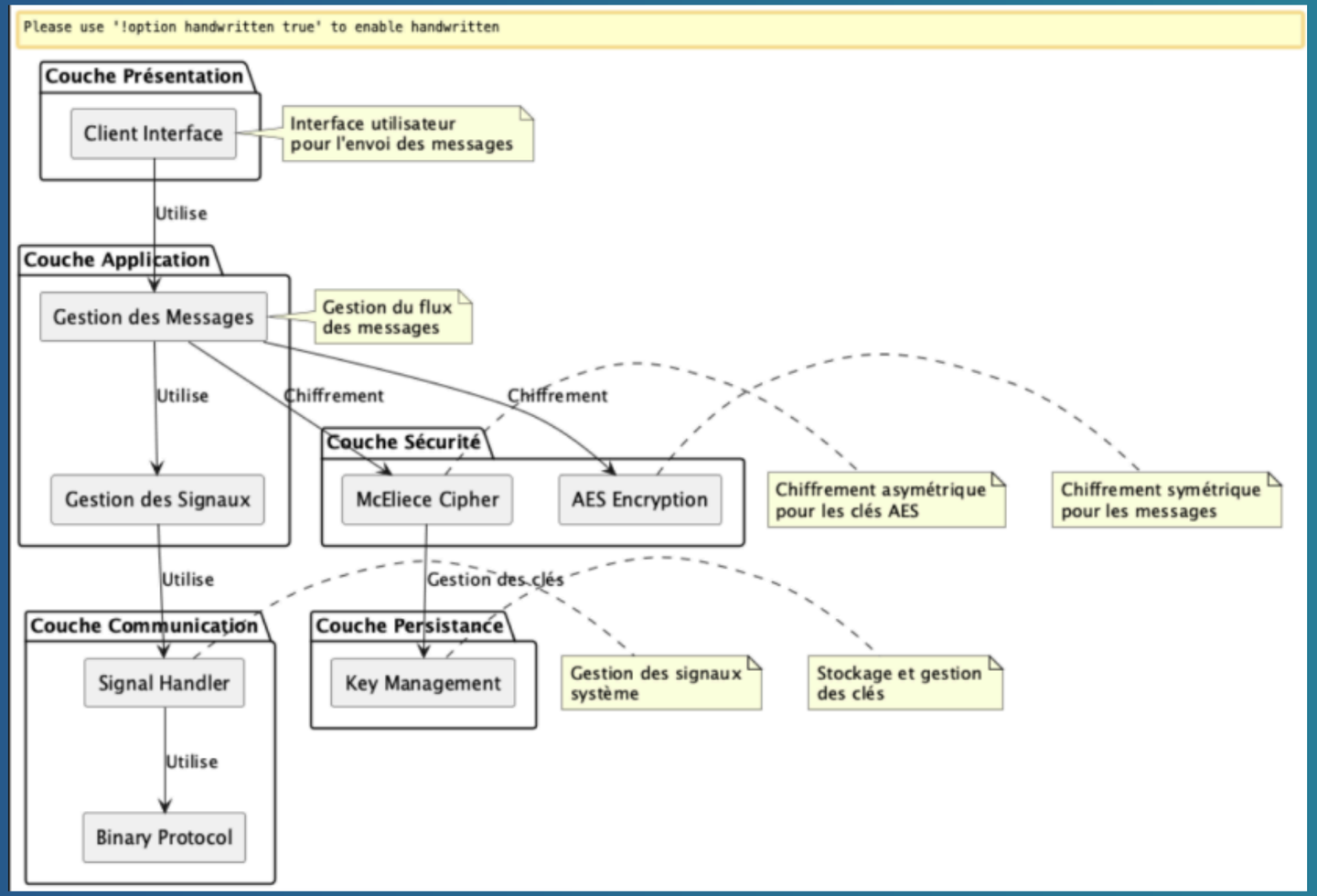
Côté implémentation :

- Le client génère une clé AES et un vecteur d'initialisation (IV).
- Il chiffre le message avec AES en mode CBC.
- Ensuite, il chiffre la clé AES avec McEliece, en utilisant un code de Goppa et un vecteur d'erreurs.
- Finalement, le tout est encodé et envoyé caractère par caractère via des signaux UNIX vers le serveur.

GossipGard

ARCHITECTURE

- **AES** : chiffre le message (rapide, symétrique)
- **McEliece** : chiffre la clé AES (asymétrique, résistante au quantique)
- **Signaux UNIX** : utilisés pour la transmission des données
- **Couches séparées** : interface, chiffrement, communication, gestion des clés
- **Architecture modulaire** : chaque couche a un rôle précis



GossipGard

FONCTIONNEMENT TECHNIQUE CLIENT & SERVEUR

Communication par signaux UNIX et chiffrement hybride

GossipGard

FONCTIONNEMENT DU CLIENT

Interface CLI :

- Lancement via la commande : python3 client.py <PID_serveur> <Message>

Étapes principales :

- Génère une clé AES aléatoire (256 bits)
- Chiffre le message en AES-CBC
- Chiffre la clé AES avec la clé publique McEliece
- Encode IV + message chiffré en base64
- Assemble tout sous forme : clé_chiffrée | IV | message_chiffré
- Envoie le tout bit par bit au serveur via signaux :
  SIGUSR1 → bit 1
  SIGUSR2 → bit 0
- Termine par un caractère nul '\0' pour signaler la fin du message

GossipGard

FONCTIONNEMENT **DU SERVEUR**

Réception par signaux :

- Attend les signaux SIGUSR1 et SIGUSR2
- Reconstruit chaque octet à partir des bits reçus
- Lorsqu'un '\0' est reçu → déclenche le déchiffrement

Étapes de déchiffrement :

- Déchiffre la clé AES avec la clé privée McEliece
- Décode IV et message chiffré depuis base64
- Déchiffre le message avec AES-CBC
- Affiche le message en clair

GossipGard

ARCHITECTURE DE SÉCURITÉ

1- Double couche de chiffrement

2- McEliece pour l'échange de clés

3- AES-256 pour le chiffrement des messages

GossipGard

MCELIECE CHIFFREMENT ASYMÉTRIQUE

Résistant aux attaques quantiques

chiffrer et déchiffrer la clé AES

GossipGard

CHIFFREMENT DES MESSAGES

- Clé de 256 bits avec IV aléatoire
- Mode CBC + padding PKCS7
- Efficace et rapide pour chiffrer les données

GossipGard

THANK YOU!