



CRYPI

Groupe 1

Valentin Lucotte
Léo Blanc-di-pasqual
Oscar Mrad
Hector Colin

Problématique

Comment effectuer des opérations entre plusieurs entités sans compromettre la confidentialité des données ?

Sommaire.

1

SMC

2

Garbled Circuit

3

Bibliothèque

4

Expérience

5

Défis


6

Amélioration

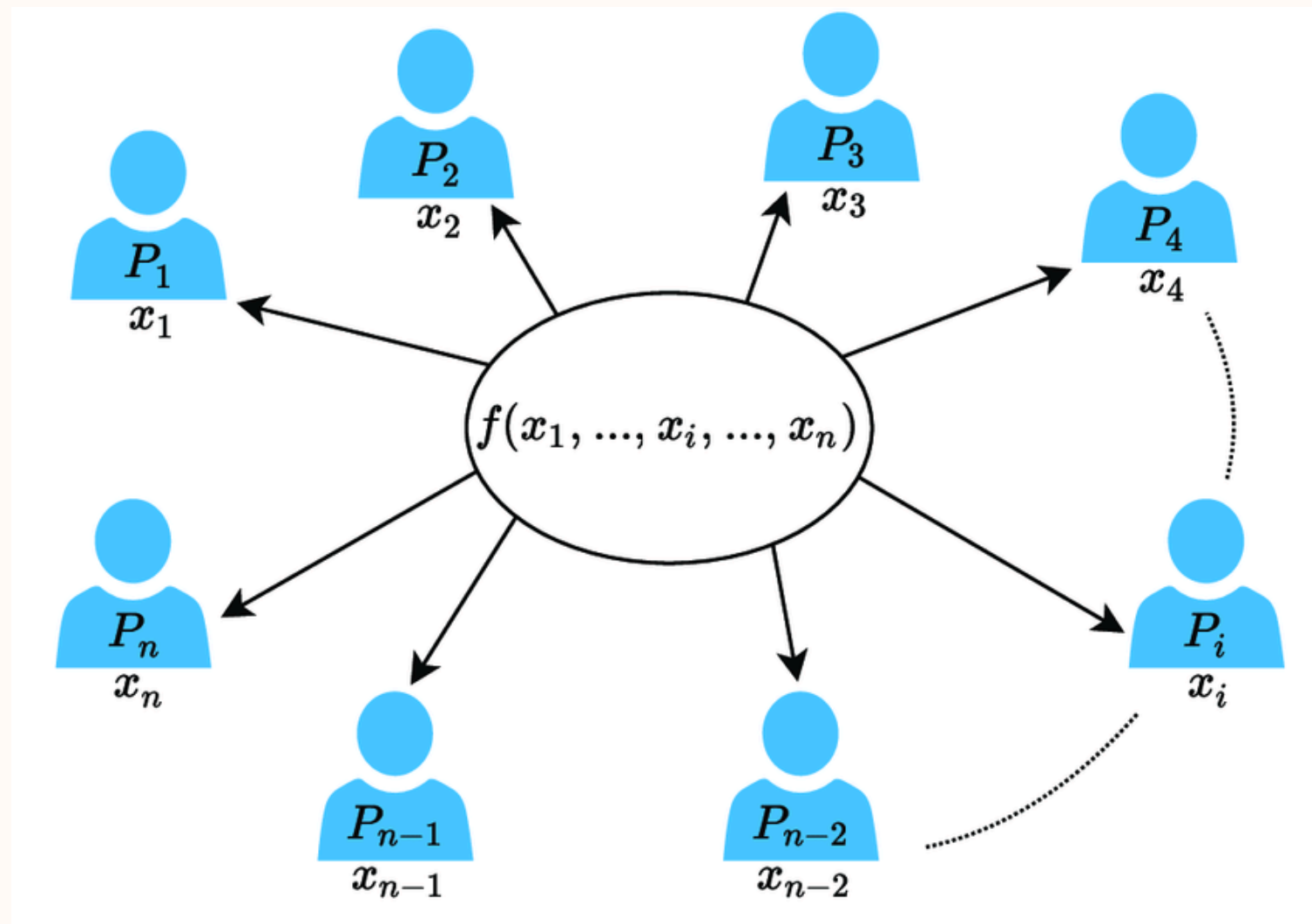
7

Conclusion

SMC

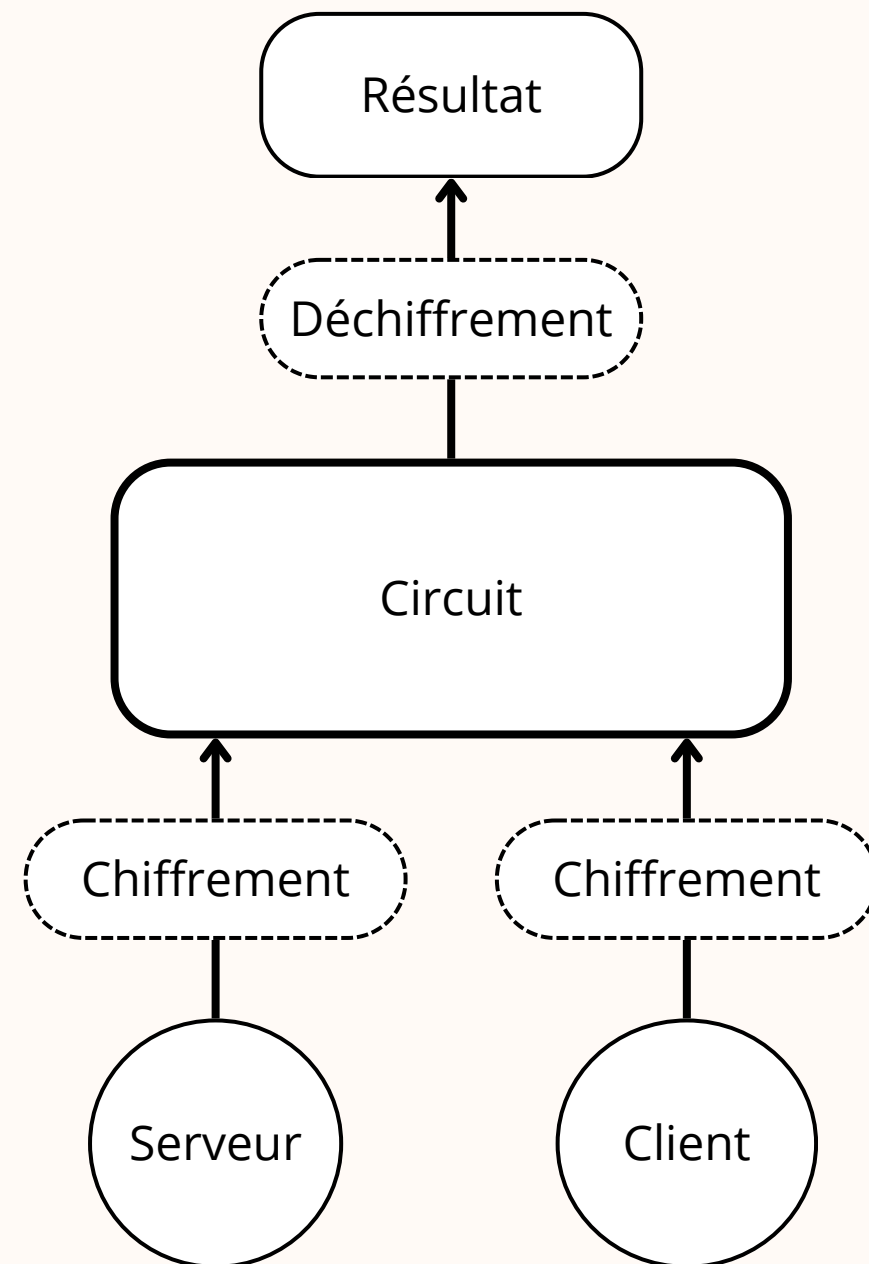
- SMC: Secure Multi-party Protocol
 - 1970: Apparition des premiers protocoles SMC.
 - 1982: Introduction formelle du calcul sécurisé à deux parties (2PC) par Andrew Yao.
 - 1986: Généralisation de cette approche pour permettre plusieurs parties.
- 

Objectifs du SMC



- Collaboration
- Confidentialité
- Intégrité

Garbled Circuit Protocole



Ce protocole permet à deux utilisateurs d'insérer leurs données dans un circuit qui calculera, à l'aide d'opérations prédéterminées, un résultat qui sera ensuite déchiffré et communiqué à tous.

L'intérêt de ce protocole est que le calcul se fait entre deux données chiffrées, de sorte qu'un tiers ou un des clients peut l'appliquer sans que les données puissent être dévoilées à autrui, même au deuxième participant. Il est aussi impossible de deviner les données fournies à partir du résultat, même si l'on possède l'une des deux."

Bibliothèque

Plusieurs bibliothèques:

- dlib -> traitement d'images
- face_recognition -> Reconnaissance faciale
- MPyC -> calcul multipartite sécurisé
- PyFhel -> chiffrement homomorphe

Expérience

- Expériences sur :
 - 50 photos
 - 34 personnes
- Taux de succès :
 - 100%
- Taux réelle estimée :
 - 99% (face_recognition success rate)
- Temps de calculs :
 - 10 sec

Défis

- Chiffrement des vecteurs à envoyer au serveur depuis le client
- Communications des données sous le bon format
- Temps du traitement des données

Amélioration

Points à améliorer:

- Faire une interface plus ergonomique
- Mises en cache des résultats
- Sécuriser la base de donnée

Conclusion

- Authentification qui fonctionne
 - Temps d'exécution rapide
 - Taux de succès important
-
- Différents points d'amélioration
 - Optimisation possible



Questions