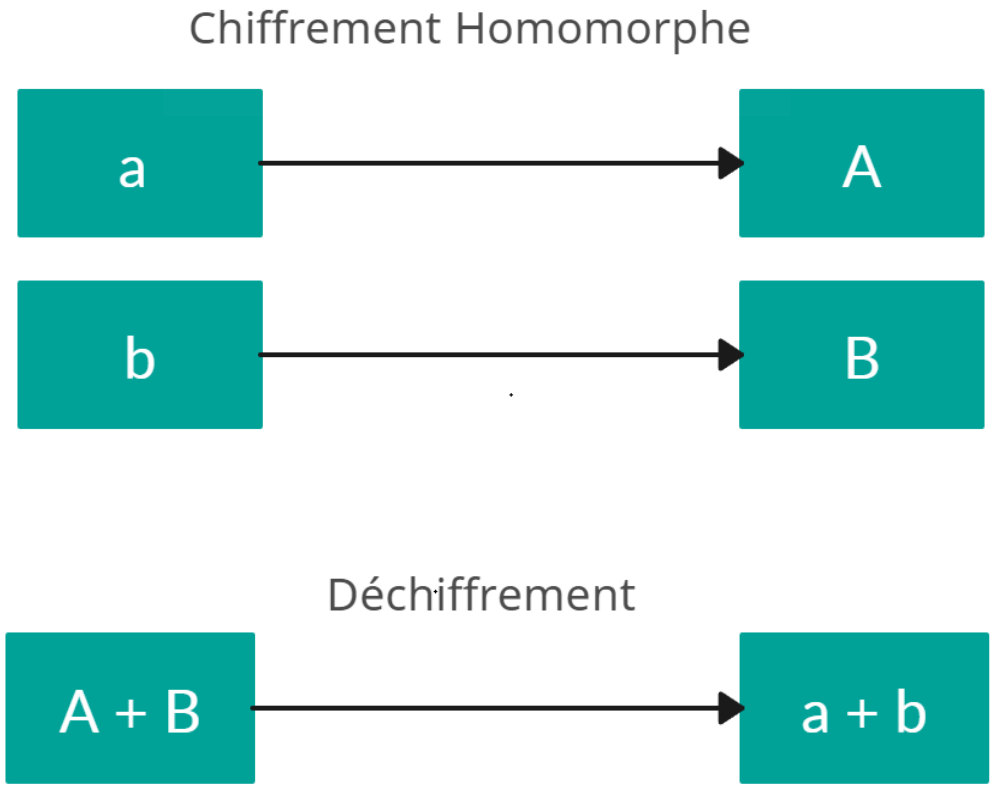
Project 5 : E-voting based on Homomorphic Encryption

Gautier Alexandre
Bazin Timothée
Lena Félix
Tripier Léo

Groupe 6

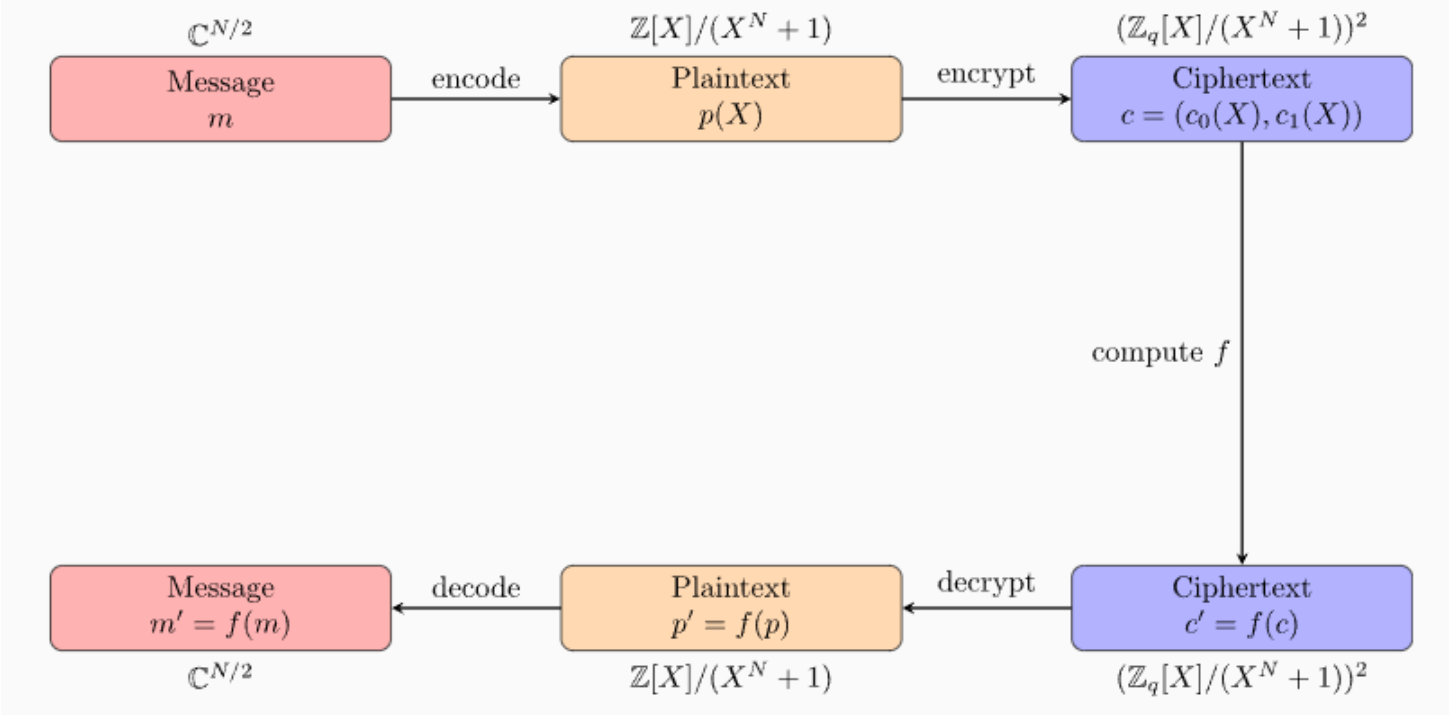
Chiffrement Homomorphe

- Chiffrer des données en commutant les opérations
- Systèmes partiellement/totalement homomorphe
- Différents algorithmes, différente précisions / opérations / difficultés de résolutions



Protocole CKKS

- Protocole de chiffrement homomorphe
- Commute de nombreuses opérations
(addition, multiplication, rotation)
- Chiffrement via des polynômes
- Assez précis pour gérer le décompte d'un vote
- Difficulté de résolution mathématique



La librairie TenSEAL

- Implémente le protocole CKKS
- API python
- Facilité d'intégration

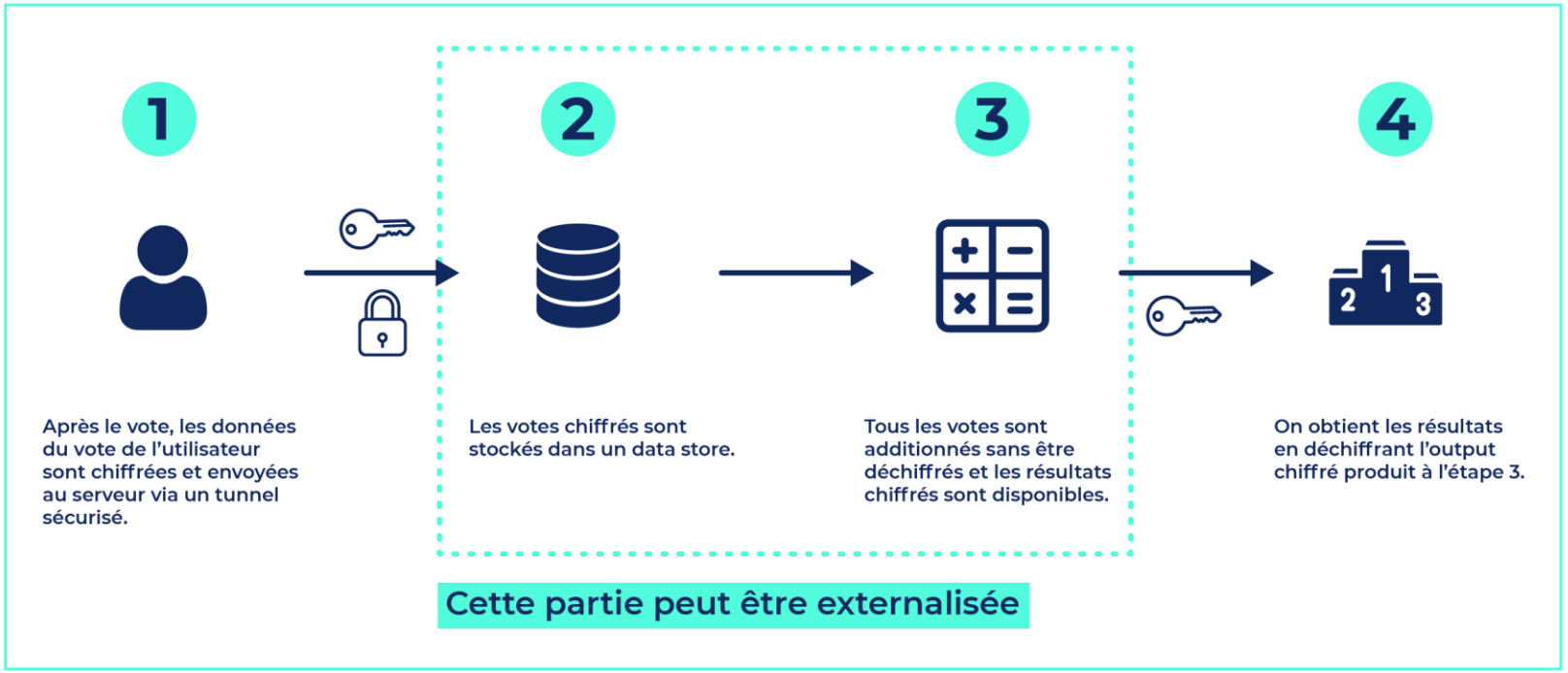
OpenMined/
TenSEAL

A library for doing homomorphic encryption operations on tensors

24 Contributors | 174 Used by | 585 Stars | 131 Forks

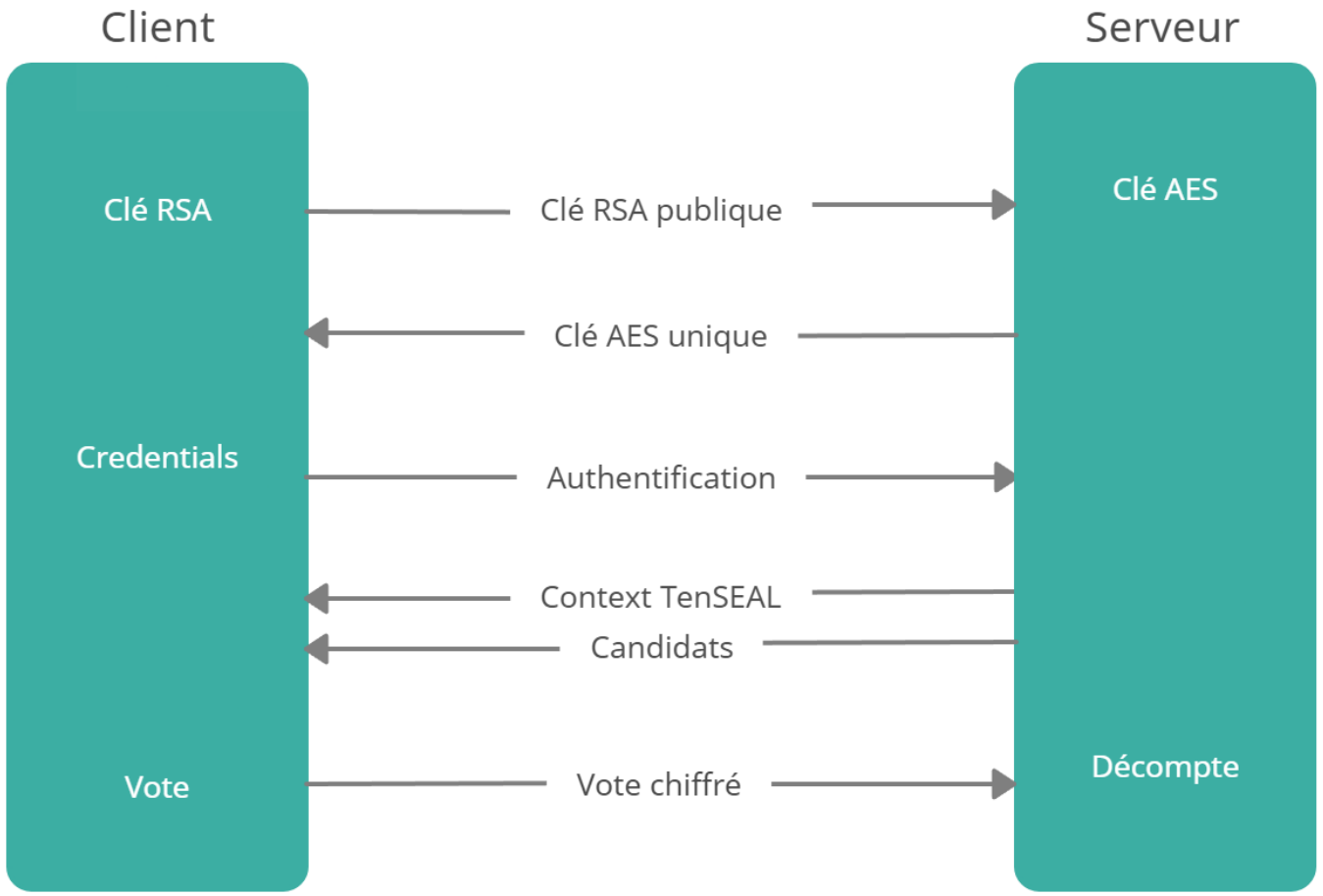
Notre POC

- Authentification utilisateur
- Vote anonyme et confidentiel
- Décompte sur une instance différente



Notre POC

- Authentification utilisateur
- Vote anonyme et confidentiel
- Décompte sur une instance différente



Voies d'amélioration

Authentification forte / multi-facteurs

Fournir un reçu chiffré, vérifié **par un tiers** de confiance

Créer une empreinte pour **chaque bulletin**


Merci de votre attention