
# Project 5 : E-voting based on Homomorphic Encryption

Groupe 06 :

Gautier Alexandre

Tripier Léo

Bazin Timothée

Lena Félix

# Table des matières

# Chapitre 1

# Introduction

Dans un monde de plus en plus numérique, les processus traditionnels sont constamment révolutionnés par l'innovation technologique. L'un de ces processus est le vote lors des élections, où le défi consiste à créer un système de vote électronique sûr, confidentiel et fiable. Dans ce contexte, nous avons crée un Proof of Concept d'une plateforme d'E-voting qui permet aux utilisateurs de s'authentifier et de voter de manière confidentielle grâce à un chiffrement homomorphe. Dans ce document, nous allons détailler notre projet, en expliquant le fonctionnement du chiffrement homomorphe, le protocole de chiffrement choisi, le choix de la librairie de chiffrement, les résultats obtenus, les difficultés rencontrées et les pistes d'amélioration.

# Chapitre 2

# Vue d'ensemble du chiffrement homomorphe

Le chiffrement homomorphe est une méthode de chiffrement par algorithme permettant de commuter certaines opérations mathématiques. Donc pour simplifier, on souhaite conserver la possibilité d'effectuer une ou plusieurs opérations mathématiques sur la valeur chiffrée tout en conservant le même résultat que sur la valeur non chiffrée.

Par exemple, si vous prenez deux valeurs, a et b, et que vous les chiffrez avec un algorithme homomorphe pour obtenir A et B, alors une opération effectuée sur a et b (par exemple, a+b) équivaut à la même opération effectuée sur A et B (soit A+B). C'est à dire qu'une fois déchiffrer, A+B vaudrat a+b. En termes d'utilités, cela permet de déléguer les tâches de calculs à une instance à laquelle nous ne faisons pas totalement confiance. On peut ainsi lui transmettre la valeur chiffrée et les opérations à effectuer, puis récupérer le résultat et le déchiffrer pour obtenir notre résultat. De cette façon, la confidentialité des données est conservée et nous avons été en mesure de déléguer la tâche de calcul.

Il existe différents algorithmes de chiffrement homomorphe. La principale différence concerne les systèmes partiellement ou totalement homomorphes. Dépendant des besoins, il est possible d'avoir un système homomorphe uniquement sur certaines opérations (par exemple la multiplication d'entiers dans un anneau modulaire).

Dans notre cas, pour une plateforme de vote en ligne, le chiffrement homomorphe est particulièrement utile afin de garantir à la fois l'anonymat de l'électeur et l'intégrité ainsi que la confidentialité du vote. Nous verrons dans les parties suivantes le détail de l'implémentation, l'idée générale étant de dissocier le vote (valeur qui

sera chiffrée) du décompte des votes (qui s'effectuera sur les valeurs chiffrées afin de garantir la confidentialité).

En chiffrant chaque vote, on garantit la confidentialité du vote et l'anonymat de l'électeur. Le chiffrement étant homomorphe, il est possible de compter tous les votes sans jamais avoir à les déchiffrer individuellement. On peut simplement additionner tous les votes chiffrés pour obtenir un total chiffré, puis déchiffrer ce total pour obtenir le nombre final de votes pour chaque candidat. De plus, cela permet de préserver l'intégrité du vote, car à aucun moment pendant le processus de comptage les votes individuels ne sont exposés. Comme le processus de chiffrement est basé sur des principes mathématiques solides, il est extrêmement difficile pour quiconque d'altérer le résultat du vote sans que cette modification soit détectée.

# Chapitre 3

# Description détaillée du protocole de chiffrement homomorphe choisi

Pour notre protocole de chiffrement nous utilisons plusieurs chiffrements différents. Nous utilisons un chiffrement AES pour chiffrer les données d'authentification des utilisateurs (identifiants et mot de passe). Puis un chiffrement RSA pour transmettre la clé AES.

Enfin, pour le protocole de chiffrement des votes nous avons utilisé le protocole Cheon-Kim-Kim-Song (CKKS). Il s'agit d'un système de chiffrement homomorphe complet qui permet d'effectuer des calculs sur des données chiffrées, parmi lesquelles des opérations d'addition, de multiplication et de rotation, sans avoir à déchiffrer ces données.

C'est un système de chiffrement basé sur le problème du Ring Learning With Errors, qui est un problème de calcul difficile sur des anneaux de polynômes. Ce protocole de chiffrement utilise une variante de ce problème pour obtenir un système de chiffrement sécurisé de par la difficulté de résolution des calculs. Le protocole CKKS comprend les trois étapes suivantes :

Génération de clés : Le système génère une paire de clés, une clé publique pour le chiffrement et une clé privée pour le déchiffrement. Ces clés sont basées sur une structure d'anneau de polynômes. Dans notre cas, ces clés sont des objets gérés par la librairie TenSEAL, qui sont particulièrement lourd. Cela implique donc un échange d'une grande quantité de bytes.

Chiffrement : Le système chiffre les données en utilisant la clé publique. Les données sont d'abord converties en polynômes, puis ces polynômes sont chiffrés en

utilisant la clé publique.

Déchiffrement : Le système déchiffre les données chiffrées en utilisant la clé privée. Les données chiffrées sont converties en polynômes, puis ces polynômes sont déchiffrés en utilisant la clé privée pour obtenir les données originales.

Le principal avantage du chiffrement CKKS est la précision des calculs sur les données chiffrées. Il est aussi à noter que la sécurité du protocole CKKS est basée sur la difficulté du problème duRing Learning With Errors. Si un algorithme efficace était découvert pour résoudre ce problème, alors la sécurité du chiffrement CKKS pourrait être compromise.

# Chapitre 4

# Critères et processus pour le choix de la librairie de chiffrement homomorphe

Pour la librairie nous permettant d'implémenter notre chiffrement homomorphe, nous avons fait le choix de TenSEAL. Nous avons d'abord essayé d'utiliser la librairie Paillier mais après avoir fait face à plusieurs problèmes nous nous sommes tournés vers TenSEAL, librairie très complète pour le chiffrement et qui présente notamment l'avantage d'avoir une documentation très riche.

La librairie TenSEAL est une bibliothèque open source et bénéficie d'une communauté active d'utilisateurs et de développeurs qui peuvent fournir un soutien, notamment sur des forums. Elle offre une interface de programmation simple et intuitive, ce qui facilite l'utilisation du chiffrement dans notre plateforme d'E-voting. De plus, elle est l'une des principales bibliothèques de chiffrement homomorphe en termes de performance. Elle offre également une grande flexibilité en ce qui concerne les types de données et les opérations qui peuvent être traitées.

Enfin, TenSEAL utilise des protocoles de chiffrement sécurisés ce qui nous permettra d' assurer la confidentialité et l'intégrité des votes.

# Chapitre 5

# Résultats des expériences conduites

Pour assurer l'authenticité de chaque utilisateur, notre plateforme utilise des mots de passe salés et hachés. Cela nous permet également d'empêcher un électeur de voter plus d'une fois. Le chiffrement homomorphe permet de traiter des données chiffrées sans jamais avoir à les déchiffrer. Cela garantit que le vote de chaque utilisateur reste confidentiel tout au long du processus, protégeant ainsi le principe fondamental du secret du vote. De cette façon, nous sommes en mesure de garantir l'anonymat du votant, la confidentialité de son vote (car il est chiffré tout au long du processus) ainsi que l'intégrité de son vote. Cela nous permet d'assurer l'exactitude du décompte final.

# Chapitre 6

# Difficultés rencontrées au cours du projet

Lors de la mise en œuvre de notre plateforme d'E-voting, nous avons rencontré plusieurs défis techniques, notamment en ce qui concerne le chiffrement AES avec CKKS et l'utilisation de clés RSA pour le chiffrement asymétrique.

L'une des difficultés majeures a été liée à la gestion du padding (bourrage) pour le chiffrement AES en utilisant le schéma de chiffrement homomorphe CKKS. Le padding est une technique utilisée pour s'assurer que les blocs de données à chiffrer sont de la taille correcte. Cependant, nous avons rencontré des problèmes avec cette approche en raison des contraintes spécifiques du chiffrement CKKS. Ces problèmes ont finalement conduit à notre décision de nous tourner vers la bibliothèque TenSEAL, qui offre une interface plus intuitive pour le chiffrement homomorphe.

Un autre défi était lié à la taille de la clé RSA que nous avions initialement prévue d'utiliser pour le chiffrement asymétrique. Nous avons découvert que cette clé était trop petite pour chiffrer l'objet utilisé par la bibliothèque TenSEAL. Pour surmonter ce problème, nous avons décidé de passer à un chiffrement AES, qui est un schéma de chiffrement symétrique, ce qui nous a permis de ne plus être limités par la taille de la clé. Cependant, nous avons encore rencontré des problèmes avec le padding AES nous pempêchant de chiffrer l'objet contexte de TenSEAL ainsi que le vote déjà chiffré par l'algorithme homomorphe. Pour maintenir les avantages du chiffrement asymétrique, nous utilisons toujours ce dernier pour chiffrer la clé de chiffrement symétrique.

La mise en place d'un hachage avec du sel pour les identifiants et mots de passe des utilisateurs a également présenté des difficultés. Le hachage avec sel est une

technique de sécurité qui consiste à ajouter une donnée aléatoire, ou "sel", à un mot de passe avant de le hacher, afin de le rendre plus résistant aux attaques par brute force. La mise en œuvre de cette technique a été un défi en raison de la nécessité de gérer le sel de manière sécurisée, à la fois lors du stockage des mots de passe hachés et lors de la transmission des mots de passe pour l'authentification.

En outre, l'interopérabilité de ces différentes technologies de chiffrement et de hachage a représenté un autre défi. Assurer une intégration fluide et sécurisée entre ces composants a nécessité une compréhension approfondie de chaque technologie, ainsi qu'une attention particulière aux détails lors de la conception et de la mise en œuvre de notre plateforme.

# Chapitre 7

# Voies d'amélioration du projet

Bien que notre plateforme fonctionne et soit sécurisée, il est toujours possible d'améliorer la sécurité d'un système. Voici plusieurs améliorations possible afin de rendre la plateforme plus sécurisé et de mieux garantir l'intégrité et la confidentialité des votes :

- Ajouter une authentification à plusieurs facteurs pour les utilisateurs lorsqu'ils se connectent à la plateforme. Cela pourrait impliquer l'utilisation d'un code unique envoyé par SMS ou par e-mail, ou l'utilisation d'une application d'authentification. Cette mesure augmente la difficulté pour un attaquant d'usurper l'identité d'un utilisateur.

- Fournir un reçu de vote chiffré qui peut être vérifié par un tiers de confiance afin que les utilisateurs puissent avoir la confirmation que leur vote à été pris en compte.

- Créer une empreinte de chaque bulletin de vote pour être en mesure de vérifier l'intégrité des bulletins de vote et s'assurer qu'ils n'ont pas été modifiés après avoir été envoyés par l'électeur.

Il faudra également s'assurer que tous les systèmes, logiciels et bibliothèques utilisés par notre plateforme sont régulièrement mis à jour pour corriger les éventuelles failles et vulnérabilités de sécurité.

# Chapitre 8

# Conclusion

La mise en place d'une plateforme d'E-voting fiable et sécurisée est un défi complexe qui nécessite une approche multidimensionnelle pour assurer l'intégrité, la confidentialité et l'anonymat des votes. En utilisant des technologies de chiffrement homomorphe avancées, notre projet a pu mettre en place un système qui répond à ces besoins. Malgré les défis rencontrés, notre plateforme a montré qu'il est possible de mettre en œuvre une solution de vote en ligne sécurisée qui respecte les principes fondamentaux du vote démocratique. Cependant, la sécurité est un processus continu, et nous devons continuer à rechercher des moyens d'améliorer et de renforcer notre système. Cela pourrait impliquer l'ajout de nouvelles fonctionnalités de sécurité, comme l'authentification à plusieurs facteurs, ainsi que des tests de pénétration réguliers pour identifier et corriger les éventuelles failles de sécurité. En fin de compte, nous avons réussi à créer une plateforme pour assurer l'anonymat, la confidentialité ainsi que l'intégrité des votes comme souhaiter.