Projet : Vote Cryptographique

Fondements théoriques

Abdelkader Gouaich

2023

Table des matières

1 Introduction

Nous allons développer, au cours des prochaines séances, un système de vote électronique distribué basé sur des principes cryptographiques.

Notre projet se situe à l'intersection de la cryptographie et des systèmes informatiques distribués, avec des implications dans les domaines des sciences politiques et des théories du choix social.

Nous aspirons à concevoir un système de vote à la fois sécurisé et transparent,

en exploitant des techniques développées dans le cadre de la théorie de l'information et de la cryptographie pour garantir l'intégrité et l'anonymat des votes.

Nous envisageons également d'appliquer des techniques issues des systèmes distribués pour rendre ce système ouvert et résistant à la manipulation et au contrôle centralisé.

2 Les fondements

2.1 Cryptographie

La cryptographie, avec des concepts tels que le chiffrement asymétrique et les fonctions de hachage, constitue le pilier des systèmes de vote cryptographique.

Le domaine de la cryptographie moderne s'appuie sur les travaux fondateurs de Rivest, Shamir et Adleman (RSA) ainsi que de Diffie et Hellman []. Ces recherches ont introduit le concept de chiffrement asymétrique.

D'un point de vue mathématique, la formulation d'un problème de chiffrement est relativement simple.

Il s'agit de concevoir une fonction, f, qui soit inversible, f^{-1}, afin de coder et décoder un message.

$$c = f(m)$$
$$m = f^{-1}(c)$$

Une telle fonction f devient pertinente lorsque le coût computationnel nécessaire pour déterminer sa fonction inverse, à partir d'un ou de plusieurs messages codés, est suffisamment élevé pour décourager toute tentative de déchiffrement.

Le chiffrement asymétrique, ou cryptographie à clé publique, s'inscrit dans ce cadre, avec une particularité : l'utilisation d'une paire de paramètres nommés *clés*.

Nous disposons d'une paire de clés : une clé publique et une clé privée. Ces deux clés sont interdépendantes, liées par une relation mathématique permettant de trouver aisément la fonction inverse en présence des deux clés. Cependant, la connaissance de la seule clé publique ne suffit pas pour retrouver cette fonction inverse de manière raisonnable.

Cela implique les points suivants :

- La clé publique, partageable, sert à chiffrer les messages ou à vérifier une signature numérique.
- La clé privée, gardée secrète, est utilisée pour déchiffrer un message ou signer numériquement.

Fonctionnellement, cela se traduit par la définition des fonctionnalités suivantes :

Une paire d'entiers (p, q) constitue une paire de clés asymétriques si nous pouvons définir deux fonctionnalités C, D telles que :

$$C(p) = f$$
$$D(q) = f^{-1}$$

Nous ajoutons à ces spécifications la contrainte que la connaissance de $C, Detp$, ainsi que des messages clairs et chiffrés, ne permet pas de retrouver aisément la clé privée q.

La robustesse d'un algorithme de chiffrement, tel que RSA, réside dans sa capacité à répondre à ces spécifications tout en minimisant les informations transmises à un cryptanalyste pour deviner l'élément manquant à partir des données publiquement disponibles $C, Detp$.

Nous trouvons deux cas d'utilisation courants des algorithmes de chiffrement asymétrique:

2.1.1 Chiffrement et déchiffrement

Un message chiffré avec la clé publique d'un destinataire ne peut être déchiffré qu'avec la clé privée correspondante du destinataire.

Inversement, un message chiffré avec la clé privée peut être déchiffré par n'importe qui ayant la clé publique correspondante, ce qui est utile pour la signature numérique.

2.1.2 La signature numérique

La signature numérique est un mécanisme qui permet de garatir que le contenu du message n'a pas été modifié.

L'expéditeur peut générer et chiffrer un résumé du message (généré par une fonction de hachage) avec sa clé privée. Cela s'appelle une signature numérique.

La clé publique de l'expéditeur peut certifier que la signature correspond au message, assurant ainsi l'authenticité et l'intégrité du message.

3 Systèmes de Vote Cryptographiques

Un système de vote cryptographique va utiliser des techniques semblables à celle développée dans la cryptographie pour développer un système de vote ou des électeurs vont voter sur une liste de choix possibles.

David Chaum, cryptographe éminent, a été un pionnier dans ce domaine avec le développement de "DigiCash". Ses innovations ont posé les jalons des premiers systèmes de vote électronique sécurisés. Depuis, plusieurs systèmes ont été développés avec des caractéristiques différentes. Nous pouvons par exemple citer le système Helios qui est utilisé dans le monde académique et associatif pour organiser des scrutins par internet. Une présentation du système Helios est proposée en Annexe.

Les votes dans Helios sont chiffrés et le décompte peut être vérifié par tous. Cependant, nous devons avoir une certaine confiance dans le serveur Helios pour gérer correctement les bulletins de vote et le processus de décompte.

3.1 Caractéristiques Clés des Systèmes de Vote Cryptographiques

La communauté scientifique a dévelopé une liste de critères pour un système de vote cryptographique; il devra entre autres:

- **Anonymat** : Préserver l'anonymat des électeurs tout en validant leur éligibilité. Il doit être impossible de relier un vote à un électeur.
- **Intégrité** : Assurer l'impossibilité de modifier, supprimer ou dupliquer les votes de manière indétectable.
- **Exhaustivité** : Tous les votes valides doivent être correctement comptés.
- **Vérifiabilité** : Permettre aux électeurs et aux observateurs de confirmer que les votes ont été correctement comptabilisés.
- **Résistance aux Coercitions** : Protéger les électeurs contre toute contrainte à révéler leur choix de vote.
- **Accessibilité** : Faciliter la participation des électeurs, quel que soit leur emplacement.
- **Éligibilité** : Seuls les électeurs légitimes doivent pouvoir participer à l'élection.
- **Validité** : Les votes invalides doivent être facilement détectables et écartés.
- **Équité** : Les résultats anticipés ne doivent pas être obtenus, car ils pourraient influencer le vote des électeurs restants.

Notre objectif est de développer de façon incrémentale plusieurs systèmes de vote qui vont répondre favorablement et de façon progressive à ces critères.

3.2 Les fonctions homomorphiques

Les fonctions homomorphiques dans les systèmes de vote électronique sont fondamentales pour permettre un décompte des votes tout en préservant l'anonymat des électeurs.

L'homomorphisme dans le contexte mathématique général représente simplement une indépendance sur l'ordre des opérations quand deux structures sont liées entre elles. Si une fonction f fait le lien entre deux structures qui possèdent des opérations internes $(G, +)$ et $(H, \oplus)$; nous dirons que f est un homorphisme ssi:

$$f(x + y) = f(x) \oplus f(y)$$

Dit autrement:

- Nous pouvons réaliser l'opération + dans le monde G et ensuite transporter le résultat vers H
- Nous pouvons transporter chaque opérandes vers H et réaliser l'opération $\oplus$ ensuite
- Dire que f est une homomorphisme revient à dire que ces deux "procédures" sont équivalentes.

Dans le contexte de la cryptographie f est une fonction de chiffrement et l'homomorphisme se réfère à la capacité de réaliser des opérations sur des données chiffrées (cryptées) sans les déchiffrer et d'obtenir un résultat correct mais chiffré.

Cette propriété est particulièrement utile pour garantir la confidentialité des votes tout en permettant leur décompte.

3.2.1 Description des Fonctions Homomorphiques

Une fonction homomorphique permet de réaliser certaines opérations algébriques sur des données chiffrées de telle sorte que, une fois les données déchiffrées, le résultat est le même que si les opérations avaient été effectuées sur les données en clair.

En d'autres termes, si vous avez deux éléments chiffrés, disons `c(a)` et `c(b)`, où `c` est une fonction de chiffrement, une fonction homomorphique `f` vous permet de calculer `f(c(a), c(b))` de telle sorte que cela équivaut à `c(f(a, b))`.

3.2.1.1 Addition Homomorphique : Supposons que chaque vote est chiffré en un nombre (par exemple, 1 pour "oui" et 0 pour "non"). Avec une fonction homomorphique additive, vous pouvez additionner ces votes chiffrés.

Si `c(1)` représente un vote "oui" chiffré et `c(0)` un vote "non" chiffré, alors `c(1) + c(0) + c(1)` donnerait le total chiffré des votes.

En déchiffrant le résultat, vous obtenez $c^{-1}c(1+0+1) = 2$, ce qui représente le total des votes "oui".

3.2.1.2 Multiplication Homomorphique De manière similaire, pour une fonction homomorphique multiplicative, la multiplication de votes chiffrés est possible.

Si `c(2)` représente un vote "oui" chiffré et `c(1)` un vote "non" chiffré, alors `c(2) * c(1) * c(2)` donnerait le total chiffré des votes.

En déchiffrant le résultat, vous obtenez $c^{-1}c(2 * 1 * 2) = 2^2$, en prenant le logarithme nous aurons le total des votes "oui".

3.3 Application dans les Systèmes de Vote Électronique

Dans le cadre d'un système de vote électronique qui emploie le chiffrement homomorphique, chaque bulletin de vote est soumis à un processus de chiffrement individuel. Cette approche garantit la confidentialité de chaque vote. Une fois chiffrés, ces bulletins sont agrégés, généralement par le biais d'une opération d'addition, pour produire un total global, lui aussi chiffré. Ce total chiffré représente l'ensemble des votes, mais sans révéler les choix individuels.

Par la suite, une entité de confiance, souvent une autorité électorale, procède au déchiffrement de ce total chiffré. Ce processus révèle le résultat final de l'élection, tout en préservant l'anonymat des votes. Ainsi, bien que le résultat global soit connu, l'association entre un électeur spécifique et son choix de vote reste confidentielle et anonyme.

Ce système offre donc un double avantage : il assure l'intégrité du processus électoral en permettant un décompte précis et vérifiable des votes, tout en protégeant la confidentialité des choix individuels des électeurs. Cela représente une avancée significative dans le domaine des technologies de vote, offrant une solution à la fois sûre et respectueuse de la vie privée des électeurs.

4 Annexe

4.1 Le système Helios

Helios est un système de vote électronique en ligne conçu pour offrir à la fois transparence et confidentialité. Il est souvent utilisé pour les élections académiques, associatives et autres petits scrutins.

Helios permet aux électeurs de vérifier que leur vote a été enregistré tel qu'ils l'ont exprimé. Après avoir voté, chaque électeur reçoit un "reçu" qu'il peut utiliser pour s'assurer que son vote est inclus dans le décompte final.

Helios permet à quiconque de vérifier que les votes ont été comptés correctement. Le décompte des votes est transparent et peut être vérifié indépendamment par n'importe quel observateur.

Les votes sont chiffrés par le navigateur de l'électeur avant d'être envoyés au serveur Helios. Cela signifie que même les administrateurs du système de vote ne peuvent pas voir pour qui l'électeur a voté.

Pour le décompte, Helios utilise le décompte homomorphe pour garantir que les votes individuels restent secrets tout en permettant un décompte public.

Helios offre une certaine résistance à la coercition. Par exemple, un électeur peut changer son vote jusqu'à la clôture du scrutin, ce qui rend difficile pour un coerciteur de s'assurer que l'électeur a voté d'une manière spécifique.