14109 MAGAT Hind

La sécurité de vote par internet

Le résultat d'élection américain de 2020 conduit le président sortant à accuser ce vote de fraude sans aucune preuve, ce qui m'a tellement rendu intéressante par ce domaine pour savoir dans quel point le vote par internet conserve la sécurité d'un choix d'électeur.
Ce sujet s'inscrit particulièrement dans le thème proposé, en effet garantir la sécurité d'une élection s'avère être un casse tête, il faut cacher le choix de chaque votant pour respecter la confidentialité du vote, et ne pas affecter la situation sociétale.

Une demande de confidentialité a été enregistrée pour ce MCOT.

Positionnement thématique (ETAPE 1)

MATHEMATIQUES (Algèbre), MATHEMATIQUES (Mathématiques Appliquées), INFORMATIQUE (Informatique Théorique).

Mots-clés (ETAPE 1)

Mots-Clés (en français)	**Mots-Clés** (en anglais)
La confidentialité	*Confidentiality*
La vérifiabilité	*verifiability*
Cryptage, décryptage	*Encryption, decryption*
El gamal	*El gamal*
Belenios	*Belenios*

Bibliographie commentée

Le vote électronique est un système automatisé, notamment des scrutins, qui est compatible avec le monde d'aujourd'hui, car se rendre dans un bureau de vote et lisser un papier dans une urne pour voter apparaitre loin de notre réalité dans notre monde hyper connecté où tous les achats et les opérations ne demandent qu'un clic sur un smartphone. Le vote par internet est intégré dans le monde politique pour diverse raison : son utilisation simple et rapide aussi il n'occasionne pas de longs déplacements et il offre une consultation plus fréquente des électeurs. En effet Suisse poursuite le vote en ligne depuis 2014 car 65% a l'internet .aussi Estonie choisie le vote à l'urne en continuant de voter par internet depuis 2013 (21 % des électeurs)[4][5].

Le vote par internet n'est pas une technologie récente pendant plusieurs années il continue à se développer .En 2017 la France a insisté sur le vote traditionnelle et non électronique , en l'accusant de fraude , cela nécessite de poser des question en terme de sécurité qu'on doit traiter ,mais avant jetant un coups d'œil sur les caractéristique de sécurité de ce vote dans le domaine informatique partielles :

La confidentialité et la transparence : veut dire le secret de vote , c'est-à-dire personne ne peut découvrir la clé secrète d'un autre et donc modifier le choix d'un électeur

la vérifiabilité : tout votant a le droit de vérifier que le résultat correspond au bulletin dans

l'urne et aussi vérifier que les bulletins appartiennent au votants légitimes [4].
Plus généralement, parler de la sécurité de vote, c'est s'expliquer les protocoles et la plate forme utilisée. Trouvant Belenios comme un protocole de vote conçus dans les équipes projets communs Inria loria Pesto et Caramba, il s'agit d'un protocole constitue de deux phase comme le vote conditionnelle de papier classique [1] :

Phase de vote : avant de voter on associe à chaque votant deux clés public et privé (ou bien chiffrement ou déchiffrement) .Autrement dit tout le monde peut chiffrer alors que seules les personnes ayant la clé de déchiffrement peuvent déchiffrer (c'est le principe d'un système de déchiffrement asymétrique).A travers ces clés chaque électeur chiffre son choix en appuyant 0 ou 1 avec la clé publique de l'élection, on parle d'un cryptage [2] .

Phase de dépouillement : afin d'expliquer cette phase, il est nécessaire de détailler le fonctionnement de l'algorithme de chiffrement .Dans Belenios le chiffrement utilisé est le système El Gamal qui a une propriété essentielle dite homomorphe [5]. Plus précisément, multiplier les chiffrés des voteS est exactement la somme des chiffrés. Grace à cette propriété, il est facile de calculer le résultat de l'élection mais sous forme chiffrée, il ne reste don que déchiffrer le résultat par les autorités en les confiant la clé publique (décryptage).

Dans cette étude on va montrer à l'aide de principe el gamal présent dans les protocole de vote l'impossibilité de changer le choix d'un électeur , c'est-à-dire connaitre la clé privé d'un électeur.

Problématique retenue

Si le vote provoque des conflits politiques, on se demande comment fonctionne ce vote, comment on peut démonter grâce au principe de el Gamal le maximum possible que ce système est bien sécurisé.

Objectifs du TIPE

· Citer les propriétés que doit vérifier un vote électronique et consacrer à une d'elles.

· Faire une étude mathématique du principe el gamal afin de prouver la confidentialité vers ce vote.

· Faire une étude informatique de ce principe et l'appliquer à un simple exemple.

Références bibliographiques (ETAPE 1)

[1] Stéphane Glondu : Belenios specification : *https://www.belenios.org/specification.pdf*
[2] Johannes Buchmann : Introduction à la cryptographie : *chapitres: 8 et 9, DOI: DUNOD*
[3] Stéphanie Delaune, Steve Kremer : Spécificité des protocoles de vote électronique : *article ; 16 Janvier 2009 , page 2,3*
[4] Pr Loÿs THIMONIER : la cryptographie homomorphe: vers le vote électronique à grande échelle : *Présentation-conférence-du-8-février-2020-sur-cryptographie, page 9,10,8*

[5] NICOLAS BONVIN : Système de vote électronique : *Projet de Master Janvier 2005 ,page 5*

DOT

[1] *Pendant l'été :recherche du sujet et compréhension du travail demandé.*

[2] *A partie d'Octobre : choix de sujet.*

[3] *Novembre jusqu'à Janvier: savoir les propriétés que doit vérifier un vote électronique et comprendre le principe de el gamal présent dans les protocoles de vote.*

[4] *Janvier jusqu'à Mars : chercher la sécurité de ce vote dans le principe de el gamal et comprendre l'étude informatique dans mon sujet*

[5] *Après l'écrit: essayer de finaliser mon programme python et commencer la présentation .*