Université Claude Bernard Lyon 1

Cahier des charges - Procédés cryptographiques pour le vote électronique

IOANNOU Orestis

Encadrant:
Laguillaumie Fabien

January 21, 2015

1 Présentation du Projet

Ce projet de recherche concerne le vote électronique et plus précisément les différents procédés cryptographiques pour assurer la sécurité, l'intégrité des votes ainsi que l'interaction privée entre le système et les utilisateurs qui votent.

1.1 Pourquoi voter en ligne est difficile?

Le vote électronique pose une série des problèmes à résoudre afin d'assurer le bon fonctionnement d'une élection. Les principaux problèmes se résument à la compréhension des notions suivantes:

- Démocratie: Les électeurs admissibles peuvent voter uniquement une fois.
- Vérifiabilité: La personne qui vote a besoin d'informations afin d'être sure que sa vote a été bien prise en compte et pour le candidat qu'elle désirait.
- Incoercibilité: Bien que la personne qui vote doit s'assurer de la vérifiabilité, il est d'autant nécessaire de pouvoir prouver à une personne tierce que notre chiffrée ainsi que sa preuve peut correspondre à plusieurs possibilités. Ceci empêchera la coercition ainsi qu'il servira a réduire les motivations d'acheter des vote vue que la personne intéressé ne pourra pas dire si son argent a bien servit.
- Détection d'erreurs: Il est important que le système puisse se rendre compte des éventuelles erreurs et les corriger
- Adversaires: le type d'adversaires de ce système est vaste. D'une part la malhonnêteté des électeurs et des fonctionnaires électoraux et d'autre part la motivation des parties politiques d'influencer les élections rendent le vote particulièrement problématique.
- Précision: Le résultat de l'élection doit être précis, ce qui signifie que les bulletins de vote ne peuvent pas être modifiés ni remplacés.

Ces problèmes ainsi que d'autres qui concernent uniquement le monde de l'internet (canal de communication sécurisé, possibilité de tracer les actions effectuées sur le réseau) créent une situation intéressante pour étudier et élaborer des solutions.

1.2 Contexte

Le projet rentre dans ce cadre particulier et vise à étudier ces nombreuses questions et plus précisément étudier un protocole de vote, développée par Ben Adida ainsi que son implémentation sous forme d'un système complet. Des références sur ce lien `https://vote.heliosvoting.org/`. Le système HELIOS est en ligne depuis 2007 et compte déjà plus de 100.000 votes.

1.3 Objectifs

Durant ce projet, ma recherche se concentra sur l'étude des différents protocoles et systèmes cryptographiques. Plus précisément je serais confronté au chiffrement homomorphe, aux preuves à connaissance nulle, aux mix-nets et aux signatures en blanc. Vue que l'implémentation déjà existante est effectuée en utilisant le chiffrement homomorphe ElGamal dans un groupe fini $\mathbb{Z}/p\mathbb{Z}$, et que le code est Open Source, la motivation ultime serait d'implémenter ce protocole en utilisant les courbes elliptiques.

On distingue donc deux objectifs:

- Le premier objectif est d'atteindre à une implémentation fonctionnelle des différents protocoles utilisant des courbes elliptiques sous forme des modules
- Le but ultime serait de proposer une version complète de Helios inspirée par celle qui existe qui utilisera le module des courbes elliptiques.

1.4 Contraintes

Le développement se fera en Python 2.7. Comme Helios est déjà implémenté sous Python ce choix était naturel.

2 Détails sur le travail à réaliser

Ce projet permettra la mise en œuvre et l'étude de différents procédés cryptographiques qui sont utiles pour le vote électronique. Concrètement les notions suivantes:

2.1 Chiffrement asymétrique homomorphe

Cette méthode repose sur l'utilisation d'une clé publique (qui est diffusée) et d'une clé privée (gardée secrète), l'une permettant de chiffrer et l'autre de déchiffrer. La notion d'homomorphie exprime la possibilité d'effectuer une opération sur le chiffré qui produira le même effet lors du déchiffrement. Cette notion est particulièrement utile pour le vote électronique puisque nous voulons calculer la somme des vœux de chaque candidat sans déchiffrer un par un les vœux de l'électeur.

2.2 Courbes elliptiques

Les courbes elliptiques sont des objets mathématiques qui sont utiles pour des opérations asymétriques. Un des intérêts de ces objets est que les clés employées pour un tel chiffrement sont plus courtes qu'avec un système fondé sur le problème de la factorisation comme RSA.

2.3 Mix-nets

C'est une famille de modes de routage favorisant l'anonymat par l'usage de serveurs intermédiaires multiples re-routant l'information sans avoir accès à celle-ci ni connaître son origine ou sa destination finale. Pour notre étude cette notion est utile afin de garantir qu'une personne qui fait des écoutes sur le canal de transmission ne sera pas capable d'identifier la provenance des chiffrés, donc des votes.

2.4 Preuves à connaissance nulle

Ceci est un concept utilisé dans le cadre de l'authentification et de l'identification. Il désigne un protocole sécurisé dans lequel une entité nommée "prouveur", prouve mathématiquement à une autre entité, le " vérificateur", qu'une assertion est vraie sans toutefois révéler une autre information que la véracité de la proposition.

3 Calendrier

Dates	Taches
Période avant 19 Janvier	Familiarisation avec les courbes elliptiques et étude générale du sujet.
19/01 - 26/01	Développement des procédés homomorphes, déchiffrement et étude des preuves à connaissance nulle. Étude du cours sur le vote électronique par Dr. Rivest de l'université de MIT.
26/01 - 09/02	Développement des preuves à connaissance nulle, des mix-nets.
09/02 - 16/02	Étude de la problématique des élections avec plus de deux candidats.
16/02 - 27/02	Amélioration du code et mise en place d'un système Helios avec des courbes elliptiques.

Références

[1] B.Adida, Advances in Cryptographic Voting Systems `http://assets.adida.net/research/phd-thesis.pdf`.

[2] Lectures of Dr.Rivest on advanced cryptography `http://courses.csail.mit.edu/6.897/spring04/materials.html`.

[3] Helios online documentation `http://documentation.heliosvoting.org/`.

[4] B.Adida, C. Andrew Neff, Ballot Casting Assurance `https://www.usenix.org/legacy/events/evt06/tech/full_papers/adida/adida.pdf`.

[5] B.Adida, Helios: Web-based Open-Audit Voting `https://www.usenix.org/legacy/events/sec08/tech/full_papers/adida/adida.pdf`.