Towards Eligible Voting Schemes

Student: Louis Holley, Supervisor: Prof. Bogdan Warinschi, Project Type: Research

University of Bristol, Department of Computer Science

Introduction

Cryptographic voting is the notion of elections with well-defined security guarantees. Such voting schemes can, for instance, enable any participant of an election to verify that their ballot was counted and that the announced result matches the ballots cast (**verifiability**), whilst not revealing how any individual voted (**privacy**). Traditional election systems do not support verifiability - they rely on trust. Much work has been done in the study of crypto-voting to reduce the level of trust participants must invest into the results of elections, but certainty cannot be achieved without cryptographic proofs, which themselves are not possible without clear definitions of security properties. A particular security property that is lacking a clear definition in the literature is **eligibility**, which is the idea that only eligible voters can vote in an election, and only once per voter. An example of a crypto-voting scheme that guarantees both privacy and end-to-end verifiability, is the one used by **Belenios**[a], which builds on the well-known **Helios**[b] voting system. Although intuitively Belenios appears to satisfy the notion of eligibility, of course we should not be satisfied with intuition alone. This project serves both to formalize (as generically as is feasible) a definition for the eligibility of a voting scheme, and to prove that Belenios satisfies eligibility according to that definition.

[a] http://www.belenios.org/
[b] https://heliosvoting.org/

1. Project Outline

In cryptography, security notions are presented as games. If an adversary can win a game with non-negligible probability, a scheme is deemed insecure with respect to the property defined by that game. The first task of this project is to formulate a game-based definition of eligibility. This game can then be used to prove that Belenios satisfies eligibility. To do this, we assume the existence of an adversary that wins the eligibility game, and show that the existence of such an adversary would result in a contradiction, usually with some common cryptographic hardness assumption.

2. A Crypto-Voting Primer

David Chaum proposed crypto-voting in the 80s, but it has only relatively recently started to be used in practice. Usually, a threshold encryption scheme is used - this is a public-key encryption scheme where a group of some threshold size is required to exchange decryption shares and recover the message. This means that to some extent, even authorities behaving dishonestly cannot jeopardize the security of an election.

One way to compute the result for an election as a function of the ballots whilst maintaining voter privacy is to use an encryption scheme that is homomorphic. In such a scheme, with a ciphertext $\mathbf{c_1}$ for a message $\mathbf{m_1}$ and a ciphertext $\mathbf{c_2}$ for a message $\mathbf{m_2}$, $\mathbf{c_1} \cdot \mathbf{c_2}$ provides an encryption of $\mathbf{m_1} \cdot \mathbf{m_2}$. This allows us to get a result for the election without decrypting any individual's vote. Since all the ballots are encrypted, we can make them publicly available, and this is what facilitates strong guarantees such as end-to-end verifiability.

3. Preliminary Results

We have formulated a game-based definition for eligibility. It comprises three sub-games which work as follows:

- a `Uniqueness` game, which ensures that each tallied ballot is associated with a unique voter credential so that no one can vote twice,
- a `Countable` game, which ensures that only 'countable' votes are tallied, since some voting schemes facilitate re-voting, and
- an `ID` game, which ensures that ballots can only be constructed if they can be attributed to some credential.

An adversary that can win any of the aforementioned sub-games with non-negligible probability demonstrates insecurity with respect to the eligibility of a voting scheme.

4. Progress and Status

Todo:

- ~~Formalize definition for eligibility of voting schemes~~
- Prove that Belenios satisfies eligibility
- Potential extension: investigate eligibility verifiability (any observer can verify that only eligible voters voted) for Belenios

University of BRISTOL