In preferential voting schemes, universal verifiablity can reveal your ballot if there is a large number of candidates. How can we solve this?

Verifiable Homomorphic Tallying for the Schulze Vote Counting Scheme

Mukesh Tiwari, Dirk Pattinson, Thomas Haines

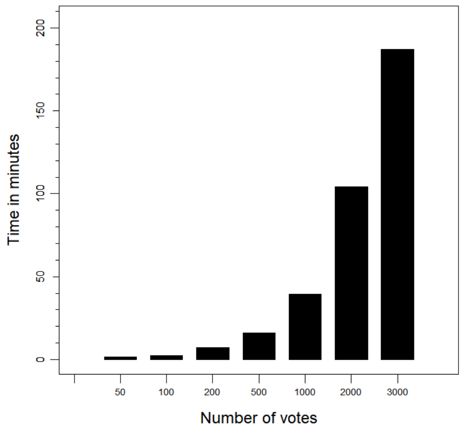
1 BACKGROUND AND PROBLEM

Universal verifiablity allows anyone to check that the announced result is correct. However, it may lead to coercion and vote selling.

2 METHODS

1. Compute the final tally homomorphically from encrypted ballots
2. Decrypt the final tally to compute winners and losers
3. Augment the scrutiny sheet with Zero-Knowledge-Proofs about various claims

3 RESULTS



4 SOFTWARE INDEPENDENCE

- Scrutiny Sheet for independent verification
- Implementation is formally verified in Coq

DETAILS

Attack: In a election, a coercer would ask a voter to mark her first and the rest of the candidates in certain order (a unique permutation which would serve as an identifier for the voter).

Feasibility of Attack: Dr Kevin Bonham, a political reporter from Tasmania, was able to link 15 similar ballots posted on bulletin board to a particular family on Facebook.

Additive ElGamal Encryption: $(g^r, h^r g^m)$

Homomorphic Property: $(g^{r_1}, h^{r_1} g^{m_1}) * g^{r_2}, h^{r_2} g^{m_2}) = (g^{r_1+r_2}, h^{r_1+r_2} g^{m_1+m_2})$

Zero-Knowledge-Proof: sigma protocols are efficient way to achieve zero-knowledge-proof. A concrete example of sigma protocol is Schnorr protocol, where the goal of a prover P is to prove the knowledge of discrete log in a Group of order q (q is prime) to a verifier V. Furthermore, g is the generator of group G, x is the public input, and w is private input with relation $x = g^w$. The protocol follows:

1. Prover P randomly selects an element r from [0 . . . q), computes $a = g^r$ and sends a to verifier V
2. Verifier V randomly selects an element c from [0 . . . q) and sends it to P
3. Prover P sends $z = r + c * w$ to V. V checks $g^z = a * x^c$

Schulze Method is a preferential voting scheme, which rests on relative margins between two candidates, i.e. the number of voters that prefer one candidate over another.

Australian National University

Download the paper →