Significance of Publications

Mukesh Tiwari

1 Schulze Voting as Evidence Carrying Computation

Author List: Dirk Pattinson, Mukesh Tiwari (I lead the Coq development)

In a paper-ballot election, scrutineers ensure correctness and verifiability, but the situation is complicated in electronic voting (e-voting) because everything is done by a (unverified) computer program. This, however, may not convince a loser, and in electronic voting, convincing a loser is utmost importance than convincing a winner. Therefore, in this paper we develop a method of (data) evidence carrying computation for the Schulze method, a complex voting with a lot of nice social-choice properties. Our method not only produces an evidence (least fixpoint) for the winners but it also produces an evidence (greatest fixpoint) for the losers of an election. In addition, we have formalised the method in the Coq theorem prover and from this (constructive) formalisation, we extracted OCaml code that could count millions of ballots.

2 Verifiable Homomorphic Tallying for the Schulze Vote Counting Scheme

Author List: Thomas Haines, Dirk Pattinson, Mukesh Tiwari (I am the lead author but the names are in alphabetical order)

The Schulze method has been around for 25 years, but until my work, there was no protocol to avoid the "Italian" attack, which is one of the prominent attacks on a preferential ballot voting method. This paper develops a protocol to avoid the "Italian" attack on the Schulze method. In addition, the protocol has been verified the Coq theorem prover to ensure that there is no gap between pen-and-paper proof and the actual implementation. In addition, my mathematically proven correct implementation was able to count 10,000 encrypted ballots within 24 hours. (the "Italian" attack is a tactic where a coercer seeks to link a specific ballot to a particular voter, when the number of participating candidates are significantly high in a preferential ballot election. The coercer demands the voter to rank a particular candidate first and the remaining candidates in a specific permutation. After the voter casts their ballot, the coercer checks if the exact permutation specified by the coercer appears the published bulletin board to see or not.)

3 Machine-checking Multi-Round Proofs of Shuffle: Terelius-Wikstrom and Bayer-Groth

Author List: Thomas Haines, Rajeev Gore, Mukesh Tiwari (I worked on special soundness and zero-knowledge proof)

Evidence producing (verifiable) mix-network is a critical part of e-voting, but there is currently no mathematically proven correct implementation of mix-networks. This paper develops a verified implementation of Bayer-Groth mix-network in the Coq theorem prover and prove that it follows (i) completeness, (ii) (special) soundness and (iii) zero-knowledge proof. In addition, it also debunks the decade old myth that Terelius-Wikstrom algorithm is a zero-knowledge proof. We have proved in the Coq theorem prover that it is a zero-knowledge argument. This is first, to the best of my knowledge, mathematically proven correct implementation of mix-network and our implementation can be used to verify Swiss elections (Bayer-Groth mix-network is used in elections in Switzerland).