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.