Achievement

Mukesh Tiwari

I am the first researcher to develop a method for the Schulze method to count encrypted ballots. In addition, I have formalised my method in the Coq theorem prover and extracted an OCaml code that was able to produce the result for a small election, 10000 encrypted ballots, in reasonable amount of time. This work was particularly very challenging because it involved many concepts, e.g., zero-knowledge-proof, mix-network, that were needed to ensure the universal verifiability of an election. Even though these concepts are very familiar in cryptography, they have never been formalised in the Coq theorem prover with the purpose to extract an OCaml code, that can be used in a real world election. Therefore, I had to figure out all the details from scratch to ensure the universal verifiability. Interestingly, many researchers not using a theorem prover leave the details, but in my case, I needed to flesh down every single detail. In addition, I am the first researcher, with my other research collaborators, to write a formally verified scrutiny sheet checker for the International Association for Cryptologic Research (IACR) election and Swiss election (submitted to USENIX). Our scrutiny sheet checker is the first formally verified software program to establish software independence, coined by Ron Rivest.