Significance of Publications

Mukesh Tiwari

1 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).