Significance of Publications

Mukesh Tiwari

1 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.)