Du-Vote: Remote Electronic Voting with Untrusted Computers (Invited Talk)

Mark Ryan, Gurchetan Grewal, Michael Clarkson, and Liqun Chen

University of Birmingham, UK
m.d.ryan@cs.bham.ac.uk

Abstract. Du-Vote is a new remote electronic voting protocol that eliminates the often-required assumption that voters trust general-purpose computers. Trust is distributed in Du-Vote between a simple hardware token issued to the voter, the voters's computer, and a server run by election authorities. Verifiability is guaranteed with statistically high probability even if all these machines are controlled by the adversary, and privacy is guaranteed as long as at least either the voter's computer or the server is not controlled by the adversary. The design of the Du-Vote protocol is presented in this paper. A new non-interactive zero-knowledge proof is employed to verify the server's computations. The security of the protocol is analyzed to determine the extent to which, when components of the system are malicious, privacy and verifiability are maintained.

Keywords: du-vote, electronic voting protocol