Cryptographic Protocols for Electronic Voting

David Wagner

UC Berkeley

Abstract. Electronic voting has seen a surge of growth in the US over the past five years; yet many questions have been raised about the trustworthiness of today's e-voting systems. One solution that has been proposed involves use of sophisticated cryptographic protocols to prove to voters that their vote has been recorded and counted correctly. These protocols are of interest both for their use of many fundamental tools in cryptography (e.g., zero-knowledge proofs, mixnets, threshold cryptosystems) as well as because of the social importance of the problem. I will survey some promising recent work in this area, discuss several open problems for future research, and suggest some ways that cryptographers might be able to contribute to improving the integrity of public elections.

C. Dwork (Ed.): CRYPTO 2006, LNCS 4117, p. 393, 2006.