Computational Election Verifiability:
Definitions and an Analysis of Helios and Civitas

Anonymized for submission to CCS 2014

ABSTRACT

New definitions of election verifiability in the computational model of cryptography are proposed. The definitions formalize notions of voters verifying their own votes, auditors verifying the tally of votes, and auditors verifying that only eligible voters vote. The Helios (Adida et al., 2009) and Civitas (Clarkson et al., 2008) election schemes are shown to satisfy these definitions. Previous computational definitions (Juels et al., 2010) are shown to permit election schemes vulnerable to attacks, whereas the new definitions prohibit those schemes.