# Cryptology ePrint Archive: Report 2011/568

**Single Layer Optical-scan Voting with Fully Distributed Trust**

*Aleksander Essex and Christian Henrich and Urs Hengartner*

**Abstract:** We present a new approach for cryptographic end-to-end verifiable optical-scan voting. Ours is the first that does not rely on a single point of trust to protect ballot secrecy while simultaneously offering a conventional single layer ballot form and unencrypted paper trail. We present two systems following this approach. The first system uses ballots with randomized confirmation codes and a physical in-person dispute resolution procedure. The second system improves upon the first by offering an informational dispute resolution procedure and a public paper audit trail through the use of self-blanking invisible ink confirmation codes. We then present a security analysis of the improved system.

**Category / Keywords:** cryptographic protocols / election schemes

**Publication Info:** Full version of paper appearing at the 3rd international conference on E-voting and Identity (VoteID 2011)

**Date:** received 20 Oct 2011

**Contact author:** aessex at cs uwaterloo ca