The Wombat Voting System

Alon Rosen

School of Computer Science
Herzliya Interdisciplinary Center
Herzliya 46150, Israel

Abstract:

In this talk I will describe the Wombat voting system, an academic project whose main objective is to explore the feasibility of end-to-end verifiable voting. The project involved designing a cryptographically-based system that simultaneously satisfies voter privacy and public verifiability, along with strong emphasis on simplicity of design and compatibility with more traditional, paper based, voting systems. The system was deployed in three real-life, small-scale elections (op to 2100 voters) on three occasions in 2011 and 2012.

Joint work with Jonathan Ben-Nun, Niko Farhi, Morgan Llewellyn, Ben Riva, Amnon Ta-Shma, and Douglas Wikström.