Abstract

This thesis introduces innovative methods to strengthen public trust in large-scale elections, particularly in contexts like Indian elections, through a dual voting system that integrates cryptographic techniques with paper audit trails. The first contribution is the development of a new dual voting design that improves upon existing protocols by addressing their various usability and security flaws.

The thesis also introduces the concept of "recoverability" from audit failures and voter disputes and proposes a protocol called OpenVoting that in addition to being publicly verifiable is also publicly recoverable. OpenVoting allows provable identification of corrupted polling booths in the face of disputes and enables recovery by selective re-election only at the corrupted booths. This is done while leaking only the minimum possible information required for recovery. A key technical innovation that enables this capability is the novel concept of a "traceable mixnet." Traceable mixnets extend the concept of a traditional mixnet that is typically used in voting protocols to anonymise and shuffle votes while preserving privacy. They allow proving special membership relationships between input ciphertexts and output plaintexts of the mixnet in zero-knowledge, enabling election recovery without leaking any additional information.

Finally, the thesis proposes a secure protocol for electoral rolls and polling-booth eligibility verification to prevent voter list manipulation, ballot stuffing and various voter profiling attacks. These advancements bridge the gap between cryptographic security and practical electoral needs, contributing to more secure and transparent elections.