Self-Enforcing E-Voting: Trustworthy Elections in The Presence of Corrupt Authorities

Dr Feng Hao, School of Computing Science, Newcastle University

European Research Council
Established by the European Commission

European Commission
Horizon 2020
European Union funding
for Research & Innovation

Overview

In SEEV, we envision a new paradigm of voting systems for future elections that are fully verifiable yet without requiring any trusted tallying authorities (TAs). Throughout the history of democratic voting, trusted authorities have been playing a critical role in ensuring the integrity of the tallying process in all voting systems, let it be paper-based or DRE-based. The state-of-the-art in the e-voting research is voting systems that are End-to-End (E2E) verifiable, meaning that the voter is able to verify the integrity of the tallying process from the moment of casting the vote to receiving the tally in the end. However, previously proposed E2E voting systems all require a set of Tallying Authorities who are cryptographic experts tasked to perform the decryption and tallying operations. These TAs mimic the role of trusted counting staff in traditional paper-based voting. But implementing such TAs in practice has proved particularly difficult. The vision in the SEEV project is to develop a whole new type of voting systems that are E2E verifiable, but without any tallying authorities (Figure 1). In other words, the systems are "self-enforcing".

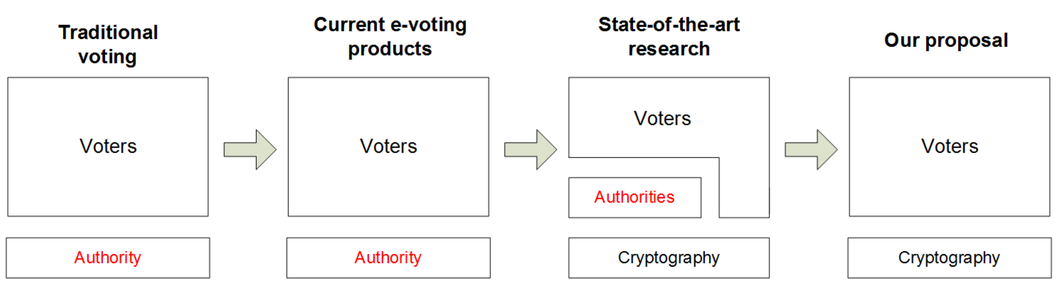


Figure 1. Evolution of trust in voting systems

What's wrong with the current e-voting?

A fundamental problem with currently deployed e-voting systems (e.g., those used in USA, India and Brazil) is that they are unverifiable (Figure 2). Essentially each system works like a black-box. After voting, the voter has no means of telling whether their vote was correctly recorded. At the end of the election, the system announces the tallied result for each candidate, but any independent verification of this result is impossible.

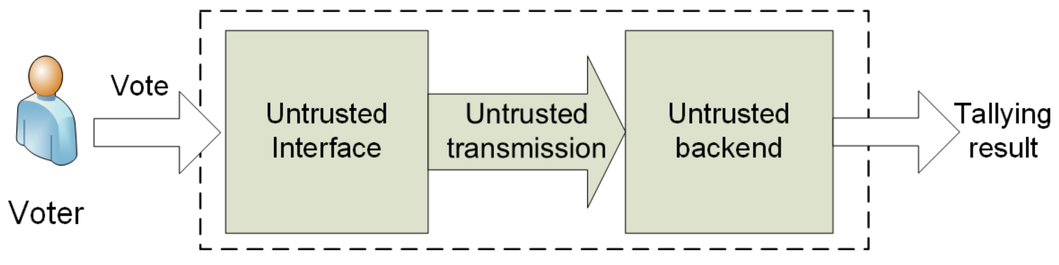


Figure 2. unverifiable e-voting system

The state-of-the-art in e-voting research

For over two decades, researchers have been working on solutions to address the lack of verifiability in e-voting systems. The state-of-the-art is voting systems that are end-to-end (E2E) verifiable. In such a system, the voter obtains a receipt when casting their vote. The receipt is encrypted, so it cannot be used for selling vote or proving to a coercer how one had voted. All previous E2E voting systems proposed in the past twenty years require a set of trustworthy TAs who must have the computing and cryptographic expertise to perform complex decryption and tallying operations (Figure 3). However, implementing such TAs in practice has proved particularly difficult.

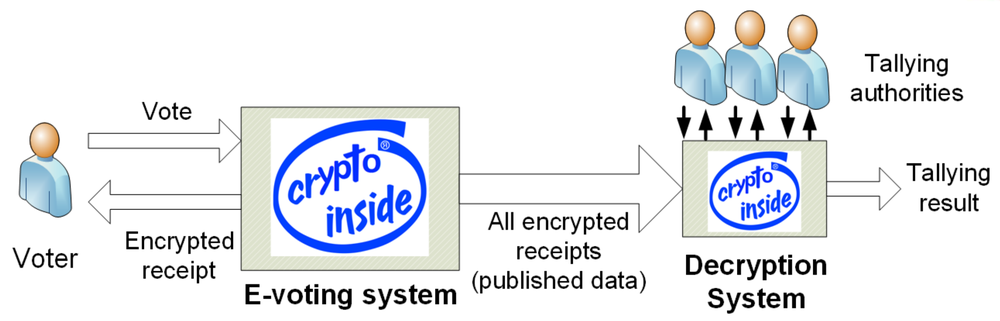


Figure 3. TA-based E2E e-voting system

Going beyond the state-of-the-art

We propose to completely remove the dependence on trusted TAs to perform the tallying process. The voting systems that we propose are still end-to-end verifiable, but without any TAs. We term such systems as "self-enforcing e-voting". The key idea is to design novel encryption schemes such that multiplying the ciphertexts will cancel out random factors added in the encryption process, hence allowing anyone to verify the tally. This effectively replaces TAs with a public algorithm (Figure 4).

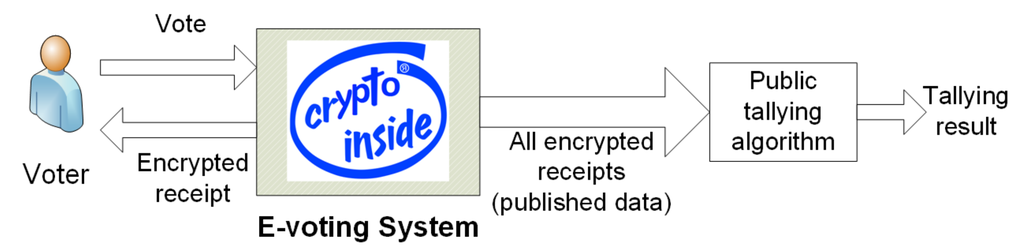
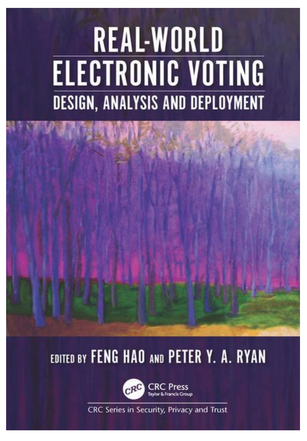


Figure 4. TA-free E2E e-voting system (self-enforcing e-voting)

Results (2013-2016)



An edited book "Real-World Electronic Voting: Design, Analysis and Deployment" published by CRC Press, Taylor & Francis, 2017 .

International patent filed on a new SEEV system for polling station voting based on the DRE-ip protocol.

A prototype of verifiable classroom voting based on SEEV, which has been used regularly in classroom voting and student awards competition in the campus of Newcastle University since 2013

The Economist

Ranked 3rd place in 2016 Economist Cybersecurity Challenge on digital voting over the blockchain (the only UK university in the top three finalists among 19 university teams from the UK and USA)

25 papers published in high-ranking conferences and journals

Acknowledgement

SEEV. Self-enforcing e-voting: trustworthy elections in the presence of corrupt authorities, ERC Starting Grant, 2013-2017, £1,060,510

SEEVCA. Self-enforcing e-voting for commercial applications, ERC Proof-of-Concept Grant, 2016-2017, £107,042