ElectionGuard

A Cryptographic Toolkit to Enable Verifiable Elections

Josh Benaloh
Microsoft Research

Michael Naehrig
Microsoft Research

Olivier Pereira
Microsoft Research and UC Louvain

Dan S. Wallach
Rice University

Crisis of Confidence

- We have a crisis of confidence in U.S. elections today.

- Millions of Americans do not have confidence in the results of U.S. elections.

Brazil 2023

The Facts …

Regardless of how you view these concerns, there are some objective truths…

- We are not providing voters with substantive evidence that their votes have been correctly counted.
- Instead, we are asking voters to trust their local election officials, equipment vendors, etc.

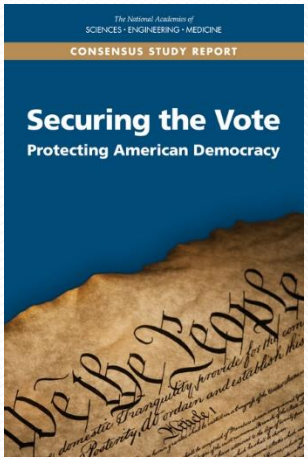
End-to-End Verifiability

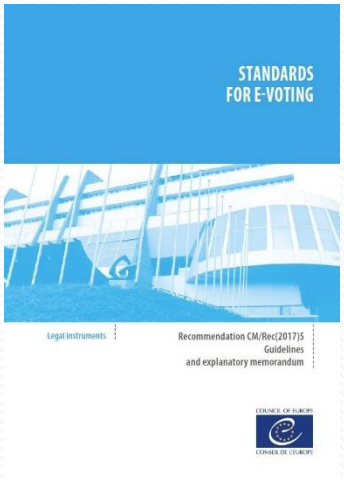
There is technology that has evolved over the last 40 years that directly addresses these concerns.

An election is *end-to-end (E2E) verifiable* if

1. Voters can verify that their own selections have been correctly recorded.
2. Anyone can verify that the recorded votes have been correctly tallied.

Expert Reports and Standards





UNITED STATES ELECTION ASSISTANCE COMMISSION

VVSG 2.0

Past Experience

- There have been dozens of academic designs for E2E-verifiable election systems.
- Many have been implemented and used in student elections and similar venues.
- Some have been built and used for Internet elections.
- At least one has been used for in-person public elections.

What's Different Here?

ElectionGuard is *not* an election system.

Instead, ElectionGuard is a set of free, open-source tools that vendors can incorporate into their election systems to enable E2E-verifiability.

ElectionGuard Structure

ElectionGuard has a simple, flexible API.

- Generally, ElectionGuard can run within existing systems and is typically called once with the contents of each ballot collected and returns a confirmation code to be given to the voter.
- ElectionGuard can work with touch-screen systems, optical scanners, Internet voting, and even vote-by-mail.

Guiding Principle

Verifying the integrity of an election should be as easy as possible.

- ElectionGuard uses integer groups rather than elliptic curves.
- Only four simple operations are required for verification.
  - Modular Addition
  - Modular Multiplication
  - Modular Exponentiation
  - Hash Computation (SHA-256)

Eliminating Trustee Complexity

- ElectionGuard uses threshold encryption to protect the privacy of votes.
- But the individual proofs of correct (partial) decryption are algebraically combined so that verifiers see only a single decryption and verification proof for each tally.

ElectionGuard Deployments

In-person Public Elections

- 2020 – Fulton, WI
  with VotingWorks
- 2020 – Inyo County, CA (audit)
  with VotingWorks
- 2022 – Preston, ID
  with Hart Intercivic
- 2023 – College Park, MD
  with Hart Intercivic

Other Elections (Remote)

- 2020 – U.S. House Dem Caucus
  with Markup
- 2023 – Neuilly-sur-Seine, FRANCE
  with Electis
- 2023 – Utah absentee voters
  with Enhanced Voting
- 2024 – internal election
  with Concordium

ElectionGuard Status

- Stable v2.1 design specification released
- Draft v2.0 data format spec released
- Various implementations in C, Python, Rust, Kotlin, etc.
- Managed by Election Technology Initiative

Future Work

- More, larger deployments
- Expanding use cases (mixnet version to enable ranked-choice-voting and verifiable write-ins)
- Continue research on optimizing and simplifying verification by introducing SNARKs and similar techniques
- Broadening the network of vendors, verifiers, contributors, and reviewers

References

- ElectionGuard

  https://www.electionguard.vote/

  https://github.com/Election-Tech-Initiative/electionguard

- National Academies report

  https://www.nationalacademies.org/our-work/the-future-of-voting-accessible-reliable-verifiable-technology

- U.S. Vote Foundation report

  https://www.usvotefoundation.org/E2E-VIV

- U.S. Election Assistance Commission Guidelines

  https://www.eac.gov/voting-equipment/voluntary-voting-system-guidelines

- Council of Europe Standards for E-Voting

  https://book.coe.int/en/legal-instruments/7609-standards-for-e-voting-recommendation-cmrec20175-guidelines-and-explanatory-memorandum.html

Questions?