Survey of Revoting in Evoting: A formal analysis perspective

Islam Faisal
Hussam El-Araby
Muhammad Faisal

Supervised by Prof. Sherif El-Kassas

Evoting

Use of electronic means in the voting process

The voting process

Electorate, Candidates ➔ Casting ➔ Counting ➔ Results

Electronic casting

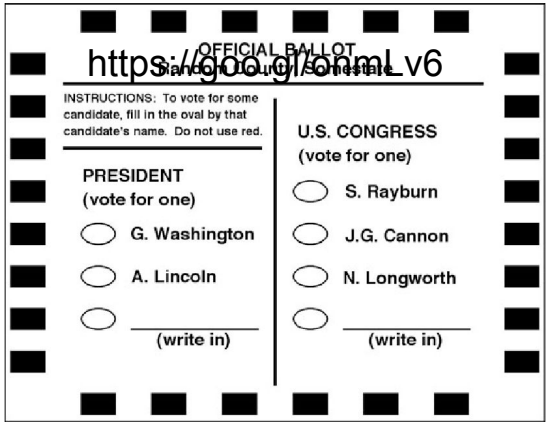
Electronic counting

History of Evoting

- 1960s, punch cards
(first electronic counting)

(Barlow)

-1980s, Marksense
(electronic counting)



https://goo.gl/onmLv6

(https://goo.gl/onmLv6)

(Barlow)

History of Evoting

- 1990s, Direct Recording Electronic (DRE)
(first electronic casting)

(https://goo.gl/Tm1PBA)

- 2000s, Online voting, piloted by Estonia
(first off-site electronic casting)

(https://goo.gl/NqrqdK)

-late 2000s, E2E systems
(voter verifiable process)

(Barlow)

The Ideal Voting System

1. Only authorized voters can vote.
2. No one can vote more than once.
3. No one can determine for whom anyone else voted.
4. No one can duplicate anyone else's vote.
5. No one can change anyone vote without being discovered.
6. Every voter can make sure that his vote has been taken into account in the final tabulation.

Can be applied to both traditional and electronic voting

(Schneier)

Promised Benefits

- A more accurate, efficient, accessible, and easily administered voting system.

- Address concerns about the risks associated with previous methods of voting.

- Voice voting and non secret paper ballots ➜ problems: coercion, violence, and vote buying.

- Secret paper ballot (most widely used voting method as of today) ➜ addressed risks above but problems: ballot fraud, more difficult to audit and verify the process.

(Alvarez)

Challenges

- Unaudited proprietary software. (the black box problem)

- Wider hacking and security risks.

- Electronic technology is more vulnerable to undetectable manipulation.

- Loss of the separation of privilege, openness, redundancy and true auditability (especially when using electronic casting with counting).

- Opens door for a large scale attack on the voting process. (Machines, Communications)

(Alvarez, Bernhard)

Ideal Voting Requirements - Another look

- The core requirement of the voting process is elections integrity.

- Beyond the details of the implementation, elections integrity is about two core goals.

1. Convincing evidence that the outcomes are correct
2. Privacy, or convincing assurance that there is no evidence about how any given person voted.

- Obvious tension: need for evidence one way, lack of it in another way.

(Bernhard)

E2E verifiability

- Rather than attempting to verify all lines of code or closely monitor all of the many processes in an election.

- Just provide electorate with convincing evidence they can directly verify elections integrity themselves directly. (Distributed public audit).

An end to end verifiable system has three kinds of verifiability:

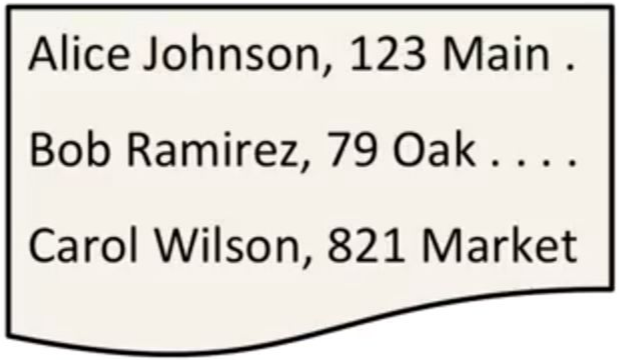
- Cast as intended
- Collected as cast
- Tallied as collected

- Evoting provides new ways to implement E2E verifiability that were not achievable without traditional means. (Bernhard)

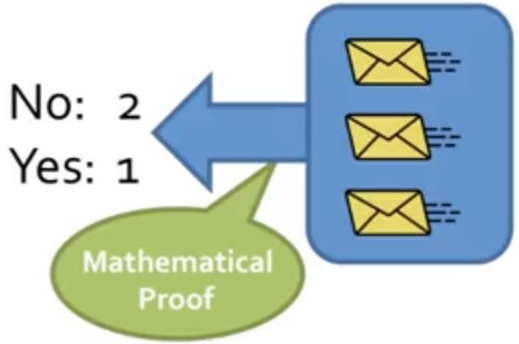
E2E verifiability

Anyone who cares to do so can:

Check that their own encrypted votes are correctly listed.



Check that other voters are legitimate.



Check the mathematical proof of the correctness of the tally.

(Halderman)

Coercion

- An E2E verifiable electronic voting system can fail to provide election integrity in several ways, but we focus here on coercion and its resistance.

- A voting system is **coercion resistant** if there is exists a way for a coerced voter to cast their vote such that her coercer cannot distinguish whether or not she followed the coercer's instructions.

- Coercion resistance can be achieved by **receipt freeness.** A voting system is receipt free if a voter is unable to prove how they voted even if she actively wants to do so and deviates from normal protocol. (Ex: Electronic cast v.s. capturing pen and paper)

(Bernhard)

Revoting

- But receipt freeness is not enough with physical coercion **while casting.** Especially when voting is allowed to happen online.

- We can use revoting in different ways.

- Allow multiple votes with the last one only binding.
- Allow in person voting to override remote voting
- Alarm codes in form of fake credentials that users can login with when under coercion.

- Example, Estonian voting allows voter to cast a paper ballot that removes their online vote.

- **Assumption,** there exists some time where a voter can access the voting system uncoerced. If otherwise the coercer is always with the coerced during the casting period then this is futile. **Assumption,** it is not achievable to coerce enough people for the whole casting period with a well designed coercion resistance system. (Bernhard)

Formal Methods

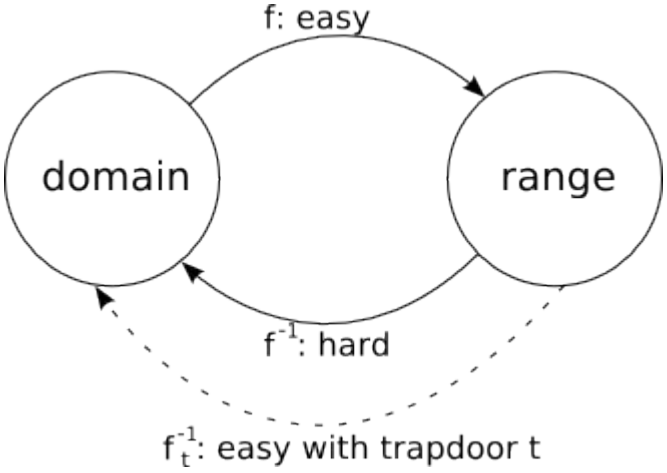
- Describe security protocols unambiguously
- Allow for formal reasoning about security properties
- Easily extend and amend protocols

lemma Eligible_Only:

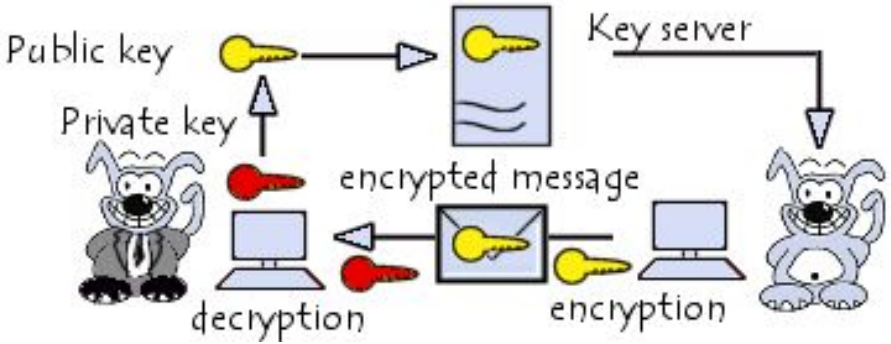
(All V S P m #i . (ReceivedVote(V , S , P , m) @ i)

==> Ex #j . (AssociatedVoter(V , S , P) @j & j < i))

Cryptographic Primitives



Tom Roeder, CS5430, Cornell University



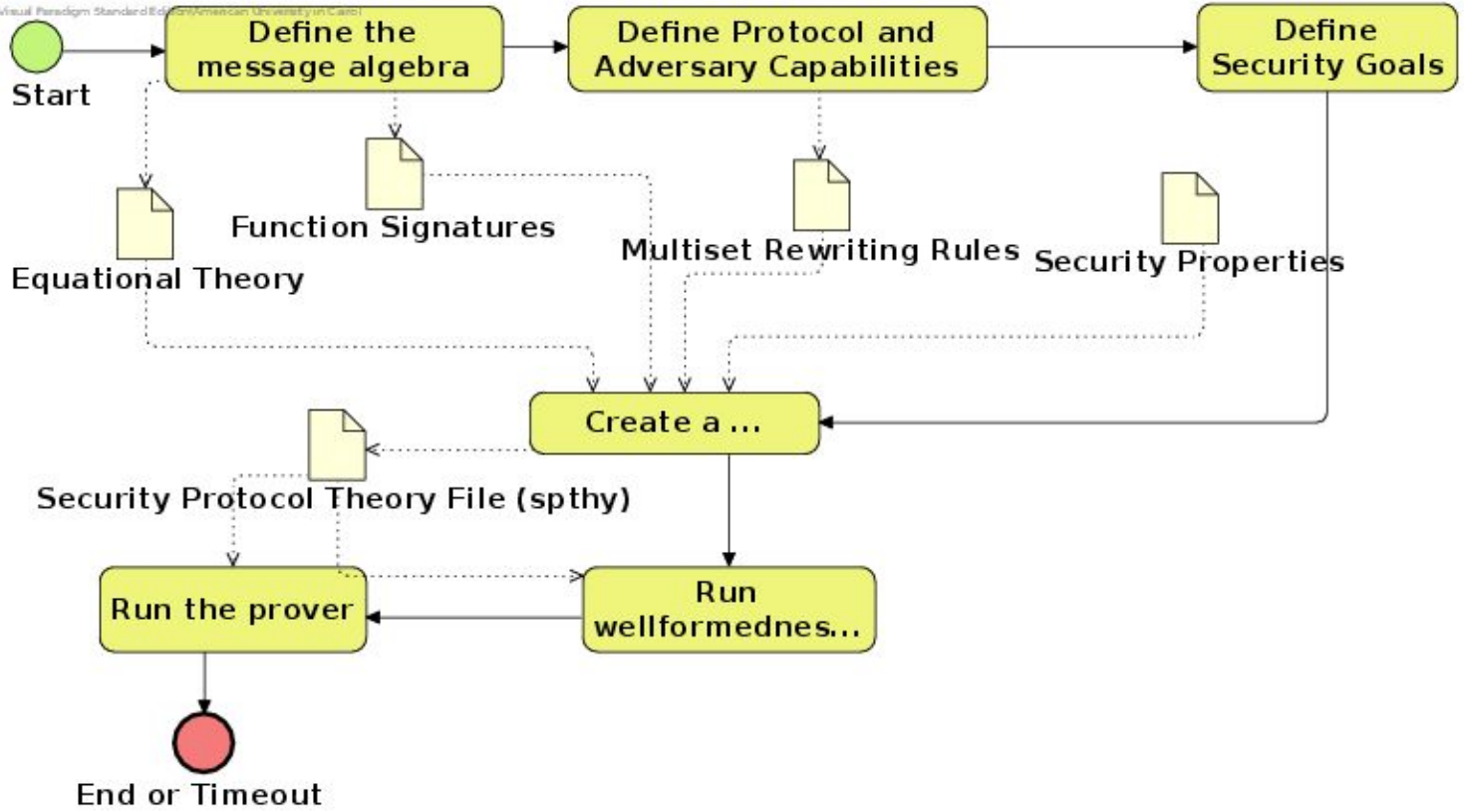
Public-Key Systems, ccm.net

Symbolic Vs. Computational Models [Blanchet]

- Messages are strings or pairings of strings
- Cryptographic primitives as blackboxes
- Assumes perfect cryptography
- Adversary is an active network channel attacker
- Usually, uses equational theory to model algebraic properties
    - dec(enc(x, y), y) = x

- Messages are bitstrings
- Cryptographic primitives are functions from bitstrings to bitstrings
- adversary is any probabilistic Turing machine
- A security property is considered to hold when the probability that it does not hold is negligible in the security parameter
    - Ex. the adversary has a negligible probability of distinguishing encryptions of two messages of the same length

Symbolic Model in Tamarin-Prover



Formal Analysis Efforts

- Bruni et al. analyzed the Selene voting protocol to verify receipt-freeness and vote-privacy using Tamarin-Prover
- Cremers et al. proposed a method based on sufficient conditions for ballot secrecy in the symbolic model (revoting wasn't considered)
- Cortier et al. analyzed variants of the Helios protocol in the computational model using EasyCrypt (including re-voting policies)
- What we are working on:
    - Models for other voting protocols in the computational model
    - Investigating the feasibility of modeling revoting policies in the symbolic model

Parting Thoughts

- Importance of audits and open-design.

- In E2E-verifiable systems, public audit is essential for achieving integrity of elections.

- Practical implementations are not as clean as theoretical models

- Electronic E2E verifiable voting will be a game changer. But as any other advancement, technology needs to exist first before it can be successfully used in real life.

References

- Alvarez, R. M., & Hall, T. E. (2010). Electronic elections: The perils and promises of digital democracy. Princeton, NJ: Princeton University Press.
- Barlow, L. (2003). An introduction to electronic voting. *CiteSeerX.-2003*.
- Bernhard, M., Benaloh, J., Halderman, J. A., Rivest, R. L., Ryan, P. Y., Stark, P. B., ... & Wallach, D. S. (2017, October). Public Evidence from Secret Ballots. In International Joint Conference on Electronic Voting (pp. 84-109). Springer, Cham.
- Blanchet, B.: Security Protocol Verification: Symbolic and Computational Models
- Bruni, A., Drewsen, E., & Schürmann, C. (2017, October). Towards a Mechanized Proof of Selene Receipt-Freeness and Vote-Privacy. In International Joint Conference on Electronic Voting (pp. 110-126). Springer, Cham.
- Cortier, V., Drăgan, C. C., Dupressoir, F., Schmidt, B., Strub, P. Y., & Warinschi, B. (2017, May). Machine-Checked Proofs of Privacy for Electronic Voting Protocols. In Security and Privacy (SP), 2017 IEEE Symposium on (pp. 993-1008). IEEE.
- Cremers, C., & Hirschi, L. (2017). Improving Automated Symbolic Analysis for E-voting Protocols: A Method Based on Sufficient Conditions for Ballot Secrecy. arXiv preprint arXiv:1709.00194.
- Halderman, J. Alex . (2013) Securing Digital Democracy. Coursera.
- Meier, S., Schmidt, B., Cremers, C., Basin, D.: The TAMARIN Prover for the Symbolic Analysis of Security Protocols
- Maaten, E. (2004). Towards remote Evoting: Estonian case. *Electronic Voting in Europe-Technology, Law, Politics and Society*, *47*, 83-100.
- Schneier, B. (1996). Applied cryptography: Protocols, algorithms, and source code in C.