A Formally Verified Schulze Method

Mukesh Tiwari
Supervisors:
Dirk Pattinson
Rajeev Gore
Michael Norrish

Australian National University

Research School of Computer Science

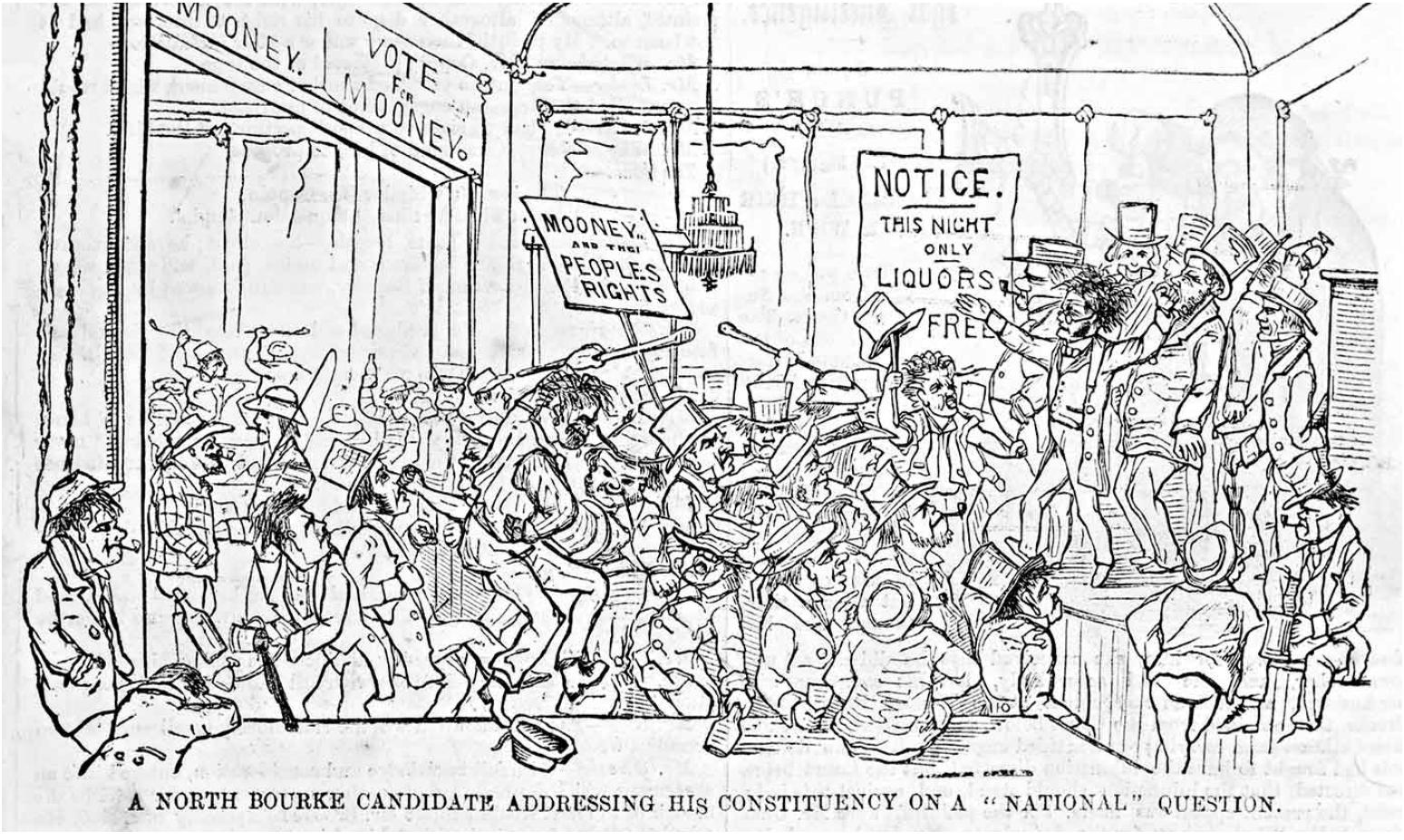
12 September, 2019

Talk Outline

- Motivation
- Schulze Voting as Evidence Carrying Computation
- Scaling it to count millions ballot
- Verifiable Homomorphic Tallying for the Schulze Vote Counting Scheme
- Machine Checked Properties
- Certificate : Verifying Elections Formally
- Future Work

Motivation

Election held in 1855 in Victoria, Australia was conducted in pub!



A NORTH BOURKE CANDIDATE ADDRESSING HIS CONSTITUENCY ON A "NATIONAL" QUESTION.

Motivation

2019 Election, NSW, Australia

Motivation

- What changed between 1855 and 2019 ?

Motivation

- What changed between 1855 and 2019 ?
- From getting drunk on free beer and discussing issues of national importance, we have gone sober and eat democracy sausage!

Motivation

- What changed between 1855 and 2019 ?
- From getting drunk on free beer and discussing issues of national importance, we have gone sober and eat democracy sausage!
- Privacy

Motivation

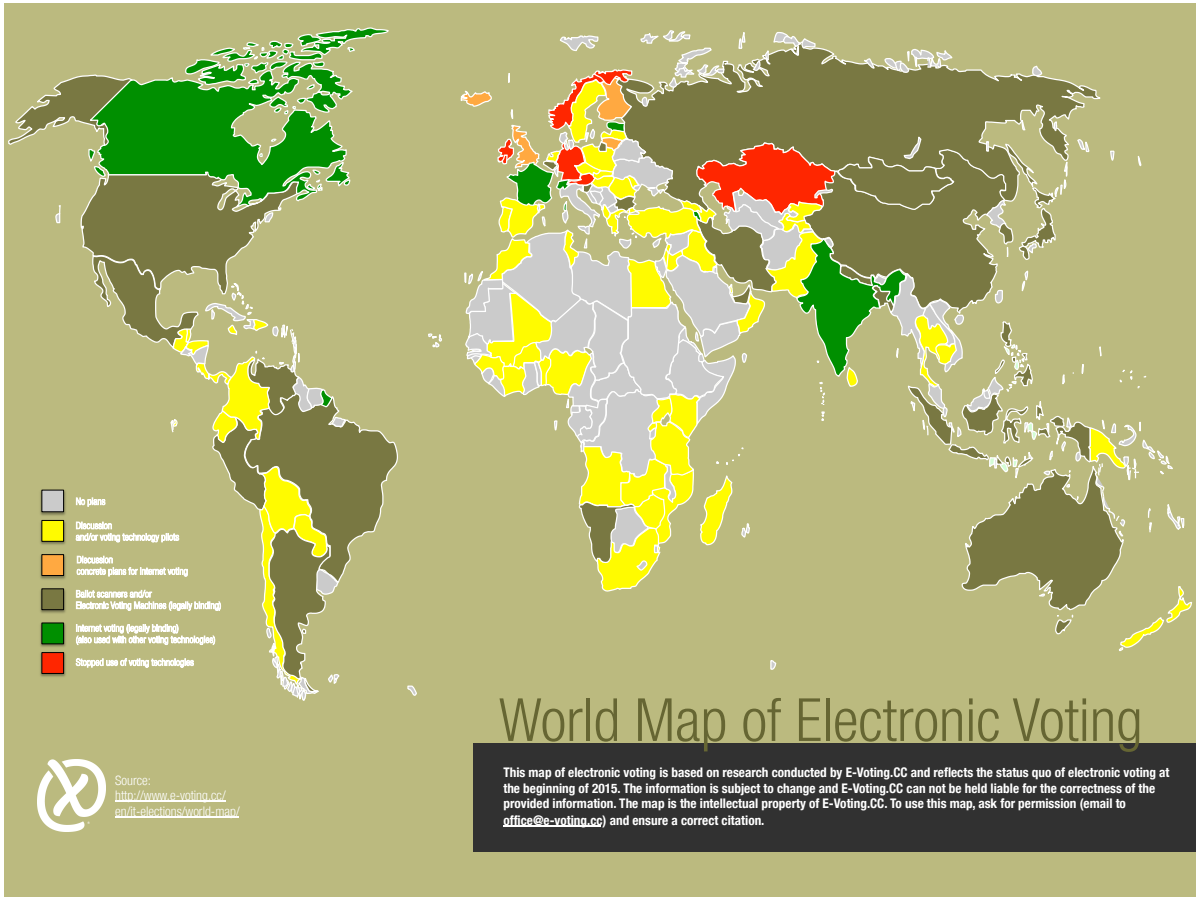
- What changed between 1855 and 2019 ?
- From getting drunk on free beer and discussing issues of national importance, we have gone sober and eat democracy sausage!
- Privacy
- Verifiability

Motivation

- What changed between 1855 and 2019 ?
- From getting drunk on free beer and discussing issues of national importance, we have gone sober and eat democracy sausage!
- Privacy
- Verifiability

Motivation

- What about Privacy and Verifiability in electronic voting ?



Motivation

NSW election 2015: iVote flaw 'allowed vote to be changed'; electoral commission fixes vulnerability - ABC News (Australian Broadcasting Corporation) - Mozilla Firefox

https://www.abc.net.au/news/2015-03-23/ivote-security-hack-allowed-change-of-vote-security-expert-says/6340168

NSW election 2015: iVote flaw 'allowed vote to be changed'; electoral commission fixes vulnerability

AM By Will Ockenden

Updated 24 Mar 2015, 11:43am

A "major security hole" that could allow an attacker to read or change someone's vote has been discovered in the New South Wales online iVote platform, security experts say.

The iVote system allows people to lodge their votes for Saturday's state election online, instead of visiting a physical polling station.

It aims to make voting easier for the disabled or for people who live long distances from polling booths.

However computer security researchers said they found a critical issue and alerted the NSW Electoral Commission on Friday afternoon.

The commission said the problem was fixed over the weekend and it expected 200,000 people would use the system in the lead up to the election.

University of Melbourne research fellow Vanessa Teague — who, along with Professor Alex Halderman from the University of Michigan, found the security vulnerability — said it was a difficult hack to pull off, but could potentially affect ballots en masse.

"We've been told repeatedly that votes are perfectly secret and the whole system is secure and it can't be tampered with and so on, and we've shown very clearly than that's not true - that these votes are not secret and they can be tampered with," Dr Teague said.

She said the attack could allow another person to either read, or even manipulate a vote, before it was sent to the electoral commission's servers.

"The analogue would be pulling someone's postal vote envelope out of the post, pulling out their vote and finding out how they intended to vote and then putting a different ballot in instead," Dr Teague said.

"The point of course with the electronic equivalent is that an attacker wouldn't necessarily need to be in New South Wales to do this and they could potentially do this in an automated way to a very, very large number of votes."

PHOTO: The electoral commission said 200,000 people were expected to use the iVote system for the 2015 NSW election. (ABC News: Brad Ryan)

RELATED STORY: NSW online ballot paper error 'disadvantaged' parties, court action flagged

RELATED STORY: UNE academic researches mobile and electronic voting

AUDIO: Listen to Will Ockenden's full report (AM)

Full coverage: NSW election

Map: NSW election results

As it happened: NSW election

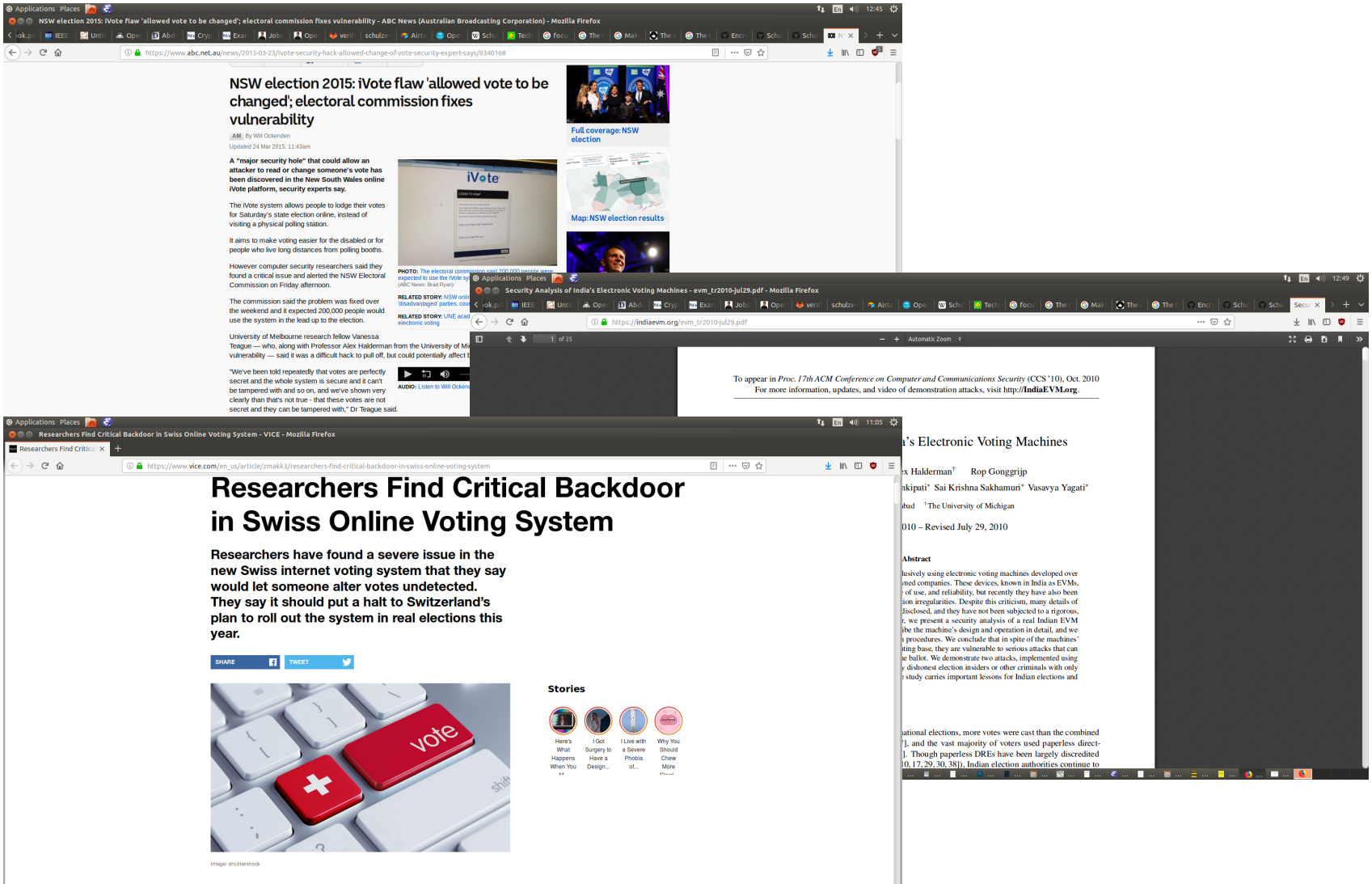
Photo gallery: NSW election

Public float poles and wires

Motivation


NSW election 2015: iVote flaw 'allowed vote to be changed'; electoral commission fixes vulnerability - ABC News (Australian Broadcasting Corporation) - Mozilla Firefox
https://www.abc.net.au/news/2015-03-23/ivote-security-hack-allowed-change-of-vote-security-expert-says/6340168
NSW election 2015: iVote flaw 'allowed vote to be changed'; electoral commission fixes vulnerability
By Will Ockenden
Updated 24 Mar 2015, 11:43am
A "major security hole" that could allow an attacker to read or change someone's vote has been discovered in the New South Wales online iVote platform, security experts say.
The iVote system allows people to lodge their votes for Saturday's state election online, instead of visiting a physical polling station.
It aims to make voting easier for the disabled or for people who live long distances from polling booths.
However computer security researchers said they found a critical issue and alerted the NSW Electoral Commission on Friday afternoon.
The commission said the problem was fixed over the weekend and it expected 200,000 people would use the system in the lead up to the election.
University of Melbourne research fellow Vanessa Teague — who, along with Professor Alex Halderman from the University of Mi
vulnerability — said it was a difficult hack to pull off, but could potentially affect
"We've been told repeatedly that votes are perfectly secret and the whole system is secure and it can't be tampered with and so on, and we've shown very clearly than that's not true - that these votes are not secret and they can be tampered with," Dr Teague said.
She said the attack could allow another person to either read, or even manipula
to the electoral commission's servers.
"The analogue would be pulling someone's postal vote envelope out of the post
finding out how they intended to vote and then putting a different ballot in instead
"The point of course with the electronic equivalent is that an attacker wouldn't n
South Wales to do this and they could potentially do this in an automated way to
of votes."
iVote
Full coverage: NSW election
Map: NSW election results
Security Analysis of India's Electronic Voting Machines - evm_tr2010-jul29.pdf - Mozilla Firefox
https://indiaevm.org/evm_tr2010-jul29.pdf
To appear in Proc. 17th ACM Conference on Computer and Communications Security (CCS '10), Oct. 2010
For more information, updates, and video of demonstration attacks, visit http://IndiaEVM.org.
Security Analysis of India's Electronic Voting Machines
Hari K. Prasad* J. Alex Halderman† Rop Gonggrijp
Scott Wolchok† Eric Wustrow† Arun Kankipati* Sai Krishna Sakhamuri* Vasavya Yagati*
*Netindia, (P) Ltd., Hyderabad †The University of Michigan
Released April 29, 2010 – Revised July 29, 2010
Abstract
Elections in India are conducted almost exclusively using electronic voting machines developed over the past two decades by a pair of government-owned companies. These devices, known in India as EVMs, have been praised for their simple design, ease of use, and reliability, but recently they have also been criticized following widespread reports of election irregularities. Despite this criticism, many details of the machines' design have never been publicly disclosed, and they have not been subjected to a rigorous, independent security evaluation. In this paper, we present a security analysis of a real Indian EVM obtained from an anonymous source. We describe the machine's design and operation in detail, and we evaluate its security in light of relevant election procedures. We conclude that in spite of the machines' simplicity and minimal software trusted computing base, they are vulnerable to serious attacks that can alter election results and violate the secrecy of the ballot. We demonstrate two attacks, implemented using custom hardware, which could be carried out by dishonest election insiders or other criminals with only brief physical access to the machines. This case study carries important lessons for Indian elections and for electronic voting security more generally.
1 Introduction
India is the world's largest democracy. In recent national elections, more votes were cast than the combined population of the United States and Canada [57], and the vast majority of voters used paperless direct-recording electronic (DRE) voting machines [25]. Though paperless DREs have been largely discredited in the academic security literature (e.g., [4, 5, 9, 10, 17, 29, 30, 38]), Indian election authorities continue to

Motivation


NSW election 2015: iVote flaw 'allowed vote to be changed'; electoral commission fixes vulnerability
Full coverage: NSW election
Map: NSW election results
Security Analysis of India's Electronic Voting Machines - evm_tr2010-jul29.pdf - Mozilla Firefox
To appear in Proc. 17th ACM Conference on Computer and Communications Security (CCS '10), Oct. 2010
For more information, updates, and video of demonstration attacks, visit http://IndiaEVM.org.
Researchers Find Critical Backdoor in Swiss Online Voting System - VICE - Mozilla Firefox
Researchers Find Critical Backdoor in Swiss Online Voting System
Researchers have found a severe issue in the new Swiss internet voting system that they say would let someone alter votes undetected. They say it should put a halt to Switzerland's plan to roll out the system in real elections this year.
SHARE
TWEET
Stories
Image: shutterstock

Definition and Assumption

- End to End verifiability
  - every voter can verify that their ballot was cast as intended

Definition and Assumption

- End to End verifiability
  - every voter can verify that their ballot was cast as intended
  - every voter can verify that their ballot was collected as cast

Definition and Assumption

- End to End verifiability
  - every voter can verify that their ballot was cast as intended
  - every voter can verify that their ballot was collected as cast
  - everyone can verify final result on the basis of the collected ballots.

Definition and Assumption

- End to End verifiability
  - every voter can verify that their ballot was cast as intended
  - every voter can verify that their ballot was collected as cast
  - everyone can verify final result on the basis of the collected ballots.
- We assume first two part of "End to End verifiability" and work on third part.

Schulze Voting as Evidence Carrying Computation [ITP 2017]

- Pros
  - Formally verified implementation in Coq

Schulze Voting as Evidence Carrying Computation [ITP 2017]

- Pros
  - Formally verified implementation in Coq
  - Verifiable because we generate certificate

Schulze Voting as Evidence Carrying Computation [ITP 2017]

- Pros
  - Formally verified implementation in Coq
  - Verifiable because we generate certificate
  - Certificates are accessible to anyone with basic math literacy

Schulze Voting as Evidence Carrying Computation [ITP 2017]

- Pros
  - Formally verified implementation in Coq
  - Verifiable because we generate certificate
  - Certificates are accessible to anyone with basic math literacy
- Cons
  - Horribly slow and not practical for real life election

Schulze Voting as Evidence Carrying Computation [ITP 2017]

- Pros
  - Formally verified implementation in Coq
  - Verifiable because we generate certificate
  - Certificates are accessible to anyone with basic math literacy
- Cons
  - Horribly slow and not practical for real life election
  - No privacy and possibly susceptible to coercion

Scaling it to count millions ballot [Evote 2017]

- Pros
  - Formally verified implementation in Coq

Scaling it to count millions ballot [Evote 2017]

- Pros
  - Formally verified implementation in Coq
  - Verifiable because we generate certificate

Scaling it to count millions ballot [Evote 2017]

- Pros
  - Formally verified implementation in Coq
  - Verifiable because we generate certificate
  - Certificates are accessible to anyone with basic math literacy

Scaling it to count millions ballot [Evote 2017]

- Pros
  - Formally verified implementation in Coq
  - Verifiable because we generate certificate
  - Certificates are accessible to anyone with basic math literacy
  - Blazing fast for real life elections

Scaling it to count millions ballot [Evote 2017]

- Pros
  - Formally verified implementation in Coq
  - Verifiable because we generate certificate
  - Certificates are accessible to anyone with basic math literacy
  - Blazing fast for real life elections
- Cons

Scaling it to count millions ballot [Evote 2017]

- Pros
  - Formally verified implementation in Coq
  - Verifiable because we generate certificate
  - Certificates are accessible to anyone with basic math literacy
  - Blazing fast for real life elections
- Cons
  - No privacy and possibly susceptible to coercion

Verifiable Homomorphic Tallying for the Schulze Vote Counting Scheme [VSTTE 2019]

- Pros
  - Formally verified implementation in Coq assuming axioms on the cryptographic primitives

Verifiable Homomorphic Tallying for the Schulze Vote Counting Scheme [VSTTE 2019]

- Pros
  - Formally verified implementation in Coq assuming axioms on the cryptographic primitives
  - Verifiable because we generate certificate

Verifiable Homomorphic Tallying for the Schulze Vote Counting Scheme [VSTTE 2019]

- Pros
  - Formally verified implementation in Coq assuming axioms on the cryptographic primitives
  - Verifiable because we generate certificate
  - Privacy because we don't reveal the content of ballots

Verifiable Homomorphic Tallying for the Schulze Vote Counting Scheme [VSTTE 2019]

- Pros
  - Formally verified implementation in Coq assuming axioms on the cryptographic primitives
  - Verifiable because we generate certificate
  - Privacy because we don't reveal the content of ballots
- Cons

Verifiable Homomorphic Tallying for the Schulze Vote Counting Scheme [VSTTE 2019]

- Pros
  - Formally verified implementation in Coq assuming axioms on the cryptographic primitives
  - Verifiable because we generate certificate
  - Privacy because we don't reveal the content of ballots
- Cons
  - Horribly Slow (10,000 ballots in 25 hours)

Verifiable Homomorphic Tallying for the Schulze Vote Counting Scheme [VSTTE 2019]

- Pros
  - Formally verified implementation in Coq assuming axioms on the cryptographic primitives
  - Verifiable because we generate certificate
  - Privacy because we don't reveal the content of ballots
- Cons
  - Horribly Slow (10,000 ballots in 25 hours)
  - Certificates are only accessible to someone having specialized knowledge of cryptography

Verifiable Homomorphic Tallying for the Schulze Vote Counting Scheme [VSTTE 2019]

- Pros
  - Formally verified implementation in Coq assuming axioms on the cryptographic primitives
  - Verifiable because we generate certificate
  - Privacy because we don't reveal the content of ballots
- Cons
  - Horribly Slow (10,000 ballots in 25 hours)
  - Certificates are only accessible to someone having specialized knowledge of cryptography
  - Trusting on Java code in realized extracted code

Machine Check Properties [On Going CPP 2020 ?]

- Condercet Winner (Finished)
- Reversal symmetry (Almost There)
- Monotonicity
- Smith Set

Certificate : Verifying Elections Formally [CCS 2019]

- We developed a general framework for Sigma Protocol
- Instantiate with IACR 2018 election data
- We proved some computationally intense result inside Coq

Certificate

```
V: [A3 B1 C2 D4,..], I: [], M: [AB:0 AC:0 AD:0 BC:0 BD:0 CD:0]
-------------------------------------------------------------
V: [A1 B0 C4 D3,..], I: [], M: [AB:-1 AC:-1 AD:1 BC:1 BD:1 CD:1]
-------------------------------------------------------------
V: [A3 B1 C2 D4,..], I: [A1 B0 C4 D3], M: [AB:-1 AC:-1 AD:1 BC:1 BD:1 CD:1]
-------------------------------------------------------------------------
                        . . .
-------------------------------------------------------------------------
V: [A1 B3 C2 D4], I: [A1 B0 C4 D3], M: [AB:2 AC:2 AD:8 BC:5 BD:8 CD:8]
-------------------------------------------------------------------------
V: [], I: [A1 B0 C4 D3], M: [AB:3 AC:3 AD:9 BC:4 BD:9 CD:9]
-----------------------------------------------------------
winning: A
  for B: path A --> B of strength 3, 4-coclosed set:
    [(B,A),(C,A),(C,B),(D,A),(D,B),(D,C)]
  for C: path A --> C of strength 3, 4-coclosed set:
    [(B,A),(C,A),(C,B),(D,A),(D,B),(D,C)]
  for D: path A --> D of strength 9, 10-coclosed set:
    [(D,A),(D,B),(D,C)]
losing: B
  exists A: path A --> B of strength 3, 3-coclosed set:
    [(A,A),(B,A),(B,B),(C,A),(C,B),(C,C),(D,A),(D,B),(D,C),(D,D)]
losing: C
  exists A: path A --> C of strength 3, 3-coclosed set:
    [(A,A),(B,A),(B,B),(C,A),(C,B),(C,C),(D,A),(D,B),(D,C),(D,D)]
losing: D
  exists A: path A --> D of strength 9, 9-coclosed set:
    [(A,A),(A,B),(A,C),(B,A),(B,B),(B,C),(C,A),(C,B),(C,C),(D,A),(D,B),
     (D,C),(D,D)]
```

Future Work

- See all of you again in December of final presentation [December 2019]
- Risk limiting audit
- Verifying the cryptographic code

Thank You!