A Formally Verified Schulze Method

Mukesh Tiwari
Supervisors:
Dirk Pattinson
Rajeev Gore
Michael Norrish

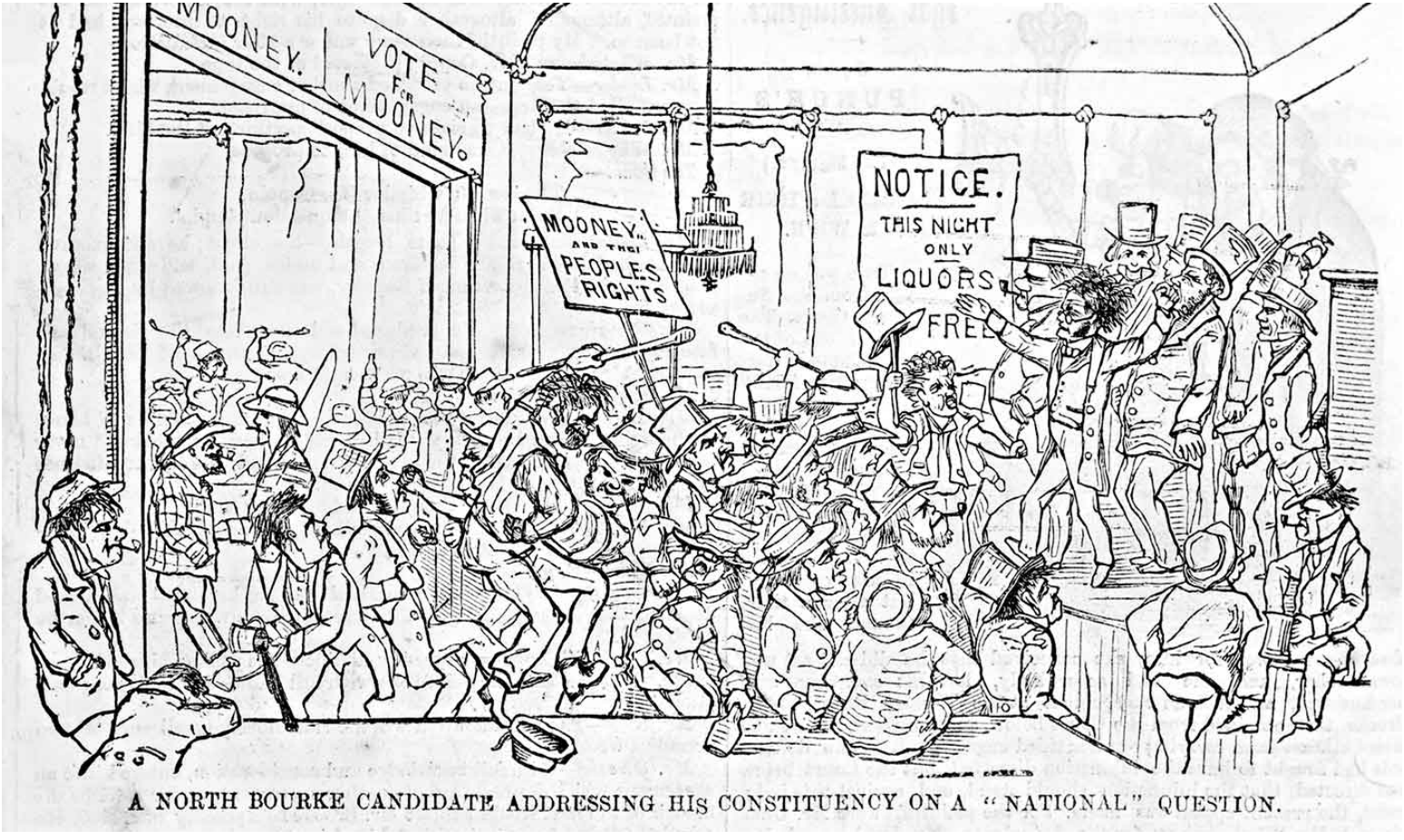
Australian National University

Research School of Computer Science

12 September, 2019

Background

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



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

Background

- Pros
  - Correctness
  - Verifiability
  - Free Beer
- Cons
  - Corruption
  - Intimidation
  - Violence
  - Unfair (women and poor were not allowed to even vote)

Background

2019 Election, NSW, Australia

Background

- Pros
  - Privacy
  - Verifiability
  - Correctness
- Cons
  - Sadly, no free beer

Background

Paper-based voting system slows down UK election results

Electoral experts say British traditions leave it out of step with other democracies

Ballot papers are counted in Cardiff © Getty

John Murray Brown MAY 6 2017

British elections provide plenty of political drama, but the amount of time it takes to tally the ballots leaves the UK out of step with global counterparts.

Background

WA senate election re-run to cost $20 million

By James Massola
February 25, 2014 — 11.19pm

A A A

- Australian politics: full coverage
- The Pulse Live with Judith Ireland
- Some Austalians voted more than once: AEC

The re-run of the West Australian senate election will cost taxpayers as much as $20 million, nearly double initial estimates of $10-13 million.

And the Griffith by-election that saw Labor's Terri Butler edge out the LNP's Bill Glasson to take former prime minister Kevin Rudd's former seat of Griffith cost taxpayers another $1.194 million.

Acting electoral commissioner Tom Rogers told Senate estimates late on Tuesday night that the lower estimates for the statewide by-election had been merely been an early estimate of the cost of heading back to the polls.

Mr Rogers said the Australian Electoral Commission was still finalising estimates but the bill could run to about $20 million for taxpayers.

The figure does not include the $3 million or so in public funding that will be handed to political

Background

Electoral commission's massive logistical effort across vast seat of Lingiari in Top End

By Emilia Terzon and Jacqueline Breen

Posted 10 May 2019, 6:54am

PHOTO: Voters have their say at a remote community early polling booth at Daly River. (ABC News: Emilia Terzon)

Early voting in one of the country's biggest electorates is underway with the Australian Electoral Commission (AEC) staging a "mammoth" logistical effort in the Northern Territory seat of Lingiari.

The numbers speak for themselves: the AEC will travel across 35,000 kilometres to hold remote polling in 200 places, to collect results before election day on May 18.

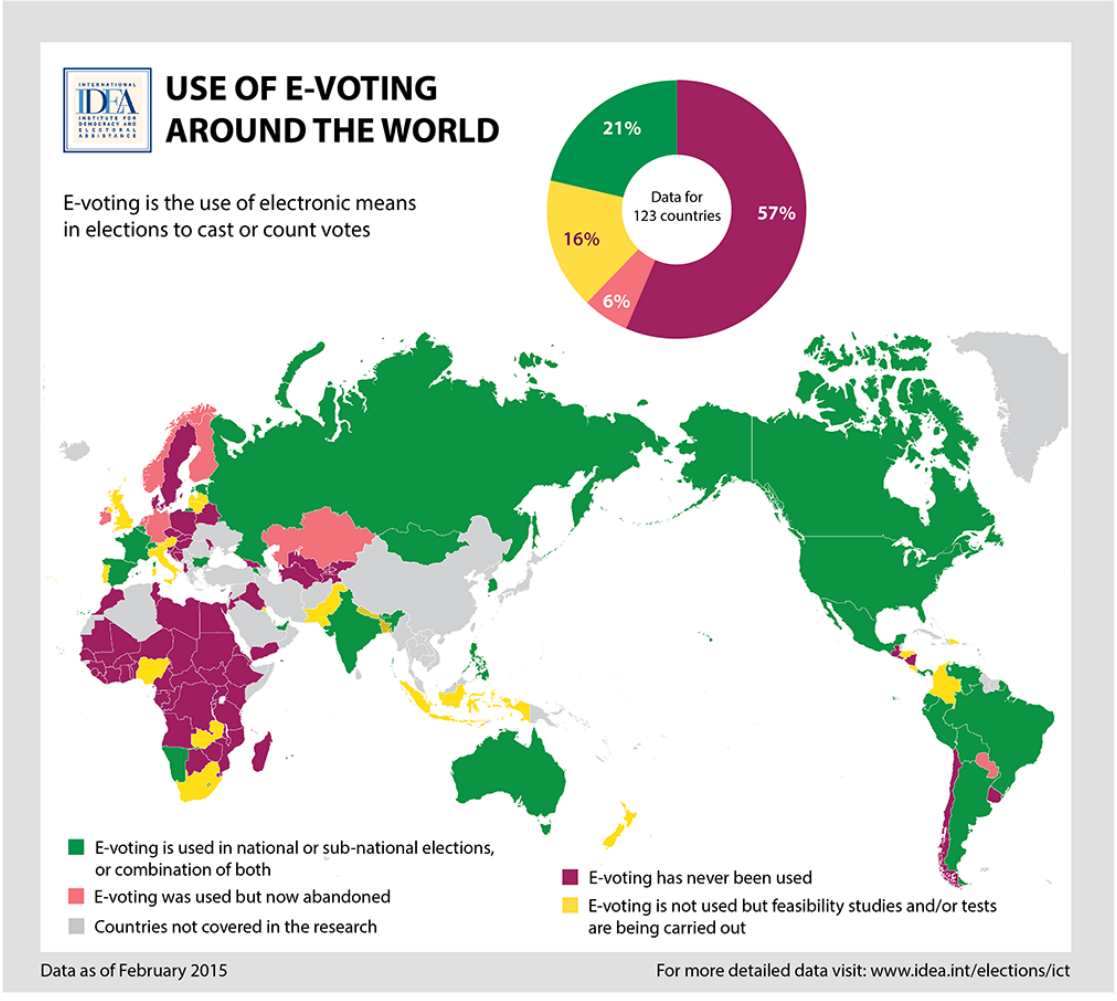
RELATED STORY: Eyes focus north as Morrison, Shorten race to snatch Territory seats

RELATED STORY: 'A national scandal': More than 10 per cent of Territorians not enrolled to vote

Key points:

- The Australian Electoral Commission has spoken of the complexities in serving voters across the huge land mass of the NT's Lingiari

Electronic Voting



Electronic Voting

Applications Places

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.

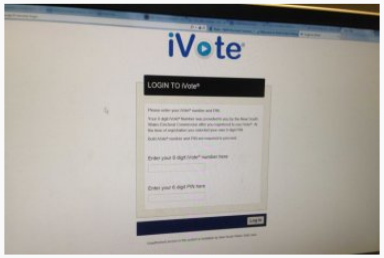


PHOTO: The electoral commission said 200,000 people were expected to use the iVote system for the 2015 NSW election. (ABC News: Brad Ryan)

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

RELATED STORY: UNE academic researches mobile and electronic voting

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.

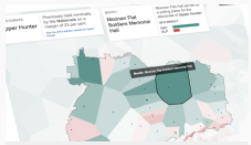
"We've been told repeatedly that votes are perfectly secret and the whole system is secure and it can't be tampered with and so on, and we've shown very clearly than that's not true - that these votes are not secret and they can be tampered with," Dr Teague said.

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

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.

Full coverage: NSW election



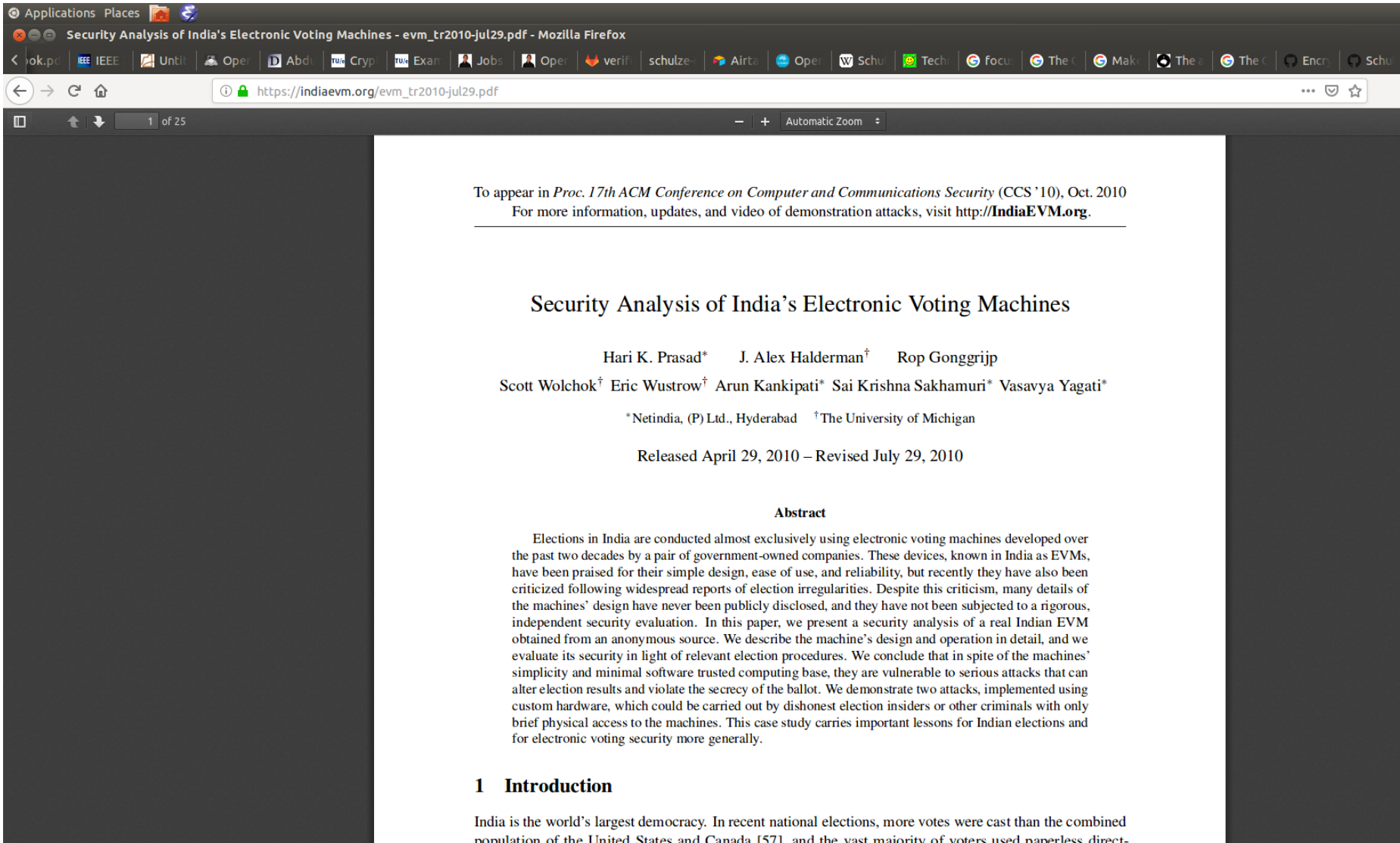
Map: NSW election results

As it happened: NSW election

Photo gallery: NSW election

Public float poles and

Electronic Voting



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

Electronic Voting

Applications Places

Researchers Find Critical Backdoor in Swiss Online Voting System - VICE - Mozilla Firefox

Researchers Find Critical

https://www.vice.com/en_us/article/zmakk3/researchers-find-critical-backdoor-in-swiss-online-voting-system

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

Image: shutterstock

Stories

Here's What Happens When You

I Got Surgery to Have a Design...

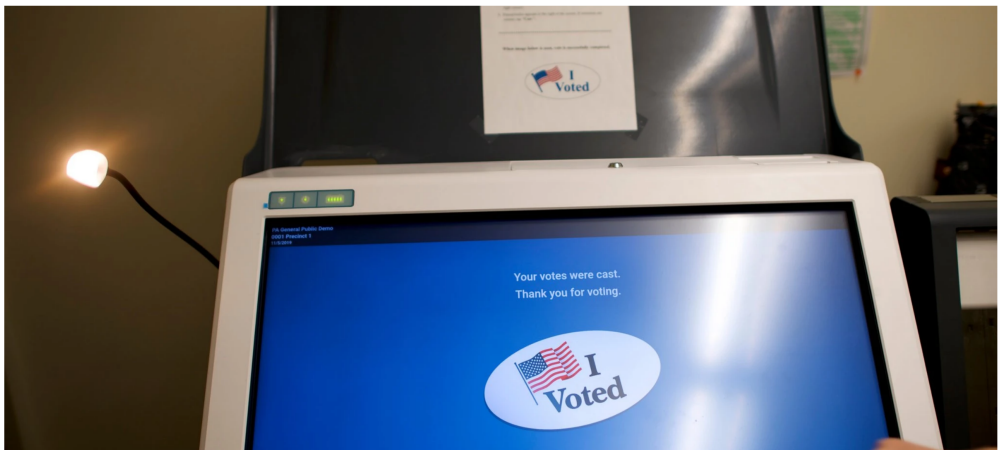
I Live with a Severe Phobia of...

Why You Should Chew More

Electronic Voting

A Pennsylvania County's Election Day Nightmare Underscores Voting Machine Concerns

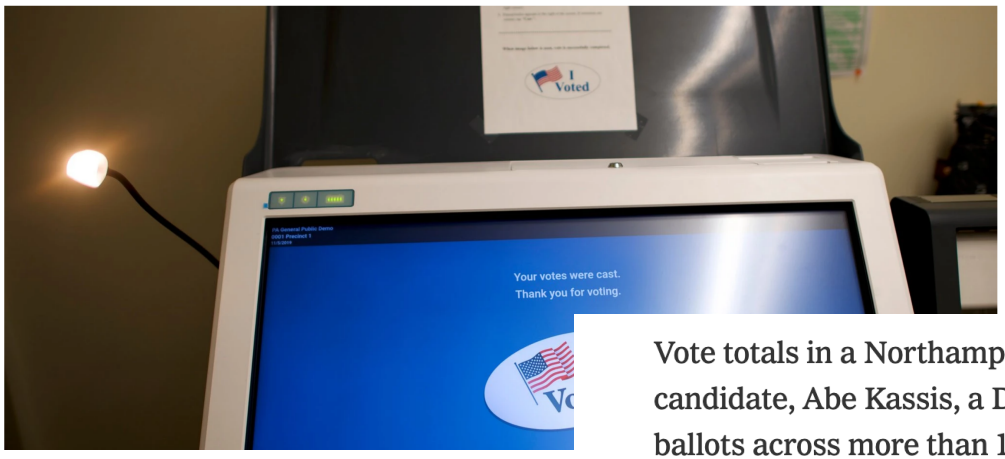
How "everything went wrong" in Northampton County.



Electronic Voting

A Pennsylvania County's Election Day Nightmare Underscores Voting Machine Concerns

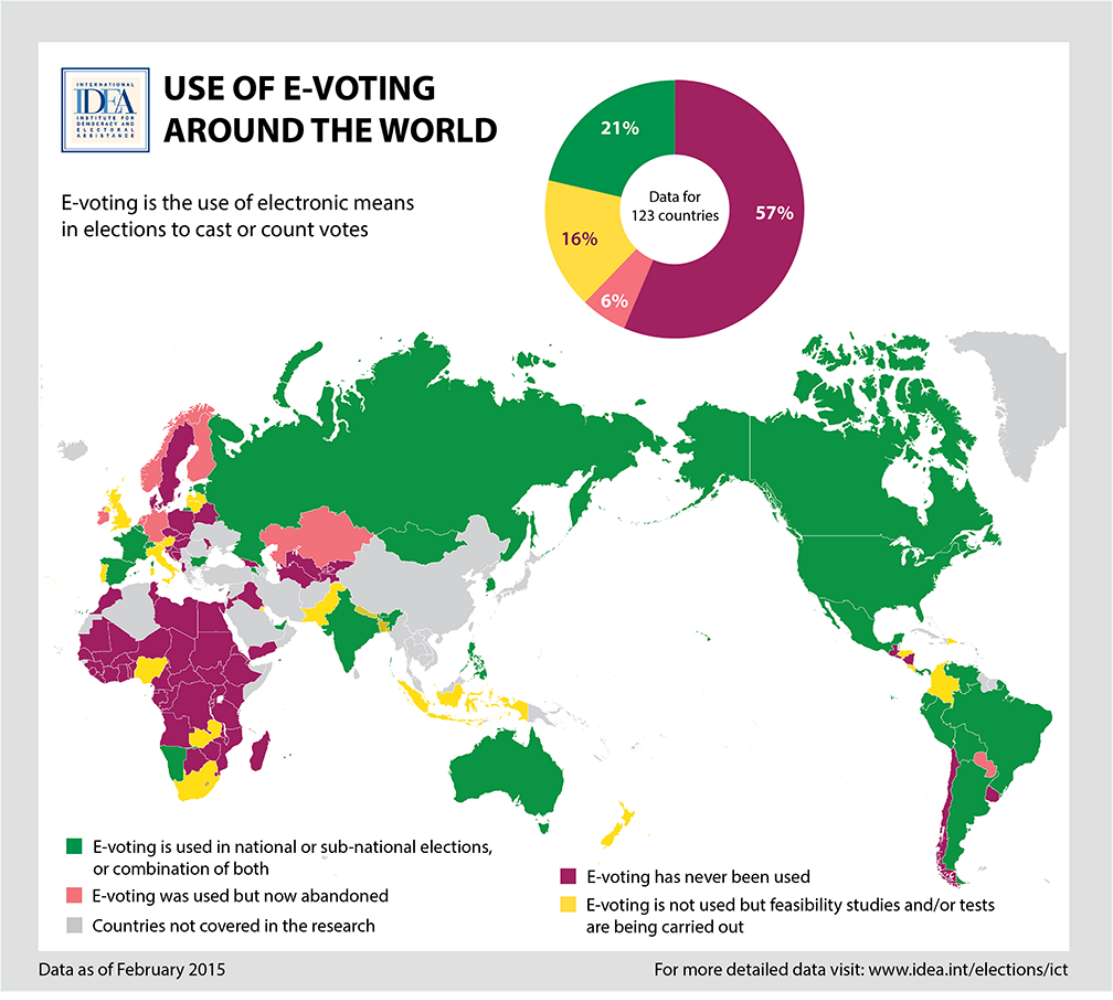
How "everything went wrong" in Northampton County.



Vote totals in a Northampton County judge's race showed one candidate, Abe Kassis, a Democrat, had just 164 votes out of 55,000 ballots across more than 100 precincts. Some machines reported zero votes for him. In a county with the ability to vote for a straight-party ticket, one candidate's zero votes was a near statistical impossibility. Something had gone quite wrong.

Electronic Voting

Countries in the Pink



Withdrawn from Electronic Voting

- Netherlands: Information Leakage
- Germany: Not Verifiable

Motivation

- Correctness
- Verifiability
- Privacy

Schulze Method

- Candidate set $C = \{c1, \ldots, cm\}$
- Vote multiset $P = \{b1, \ldots, bn\}$
- Vote is represented as function $b : C \to \mathbb{N}$

Rank all candidates
in order of preference

[4] Lando Calrissian

[3] Boba Fett

[1] Mace Windu

[2] Poe Dameron

[2] Maz Kanata

Schulze Method

- Construct a margin function (matrix) $m : C \times C \to \mathbb{Z}$.

$$m(c, d) = \sharp\{b \in P \mid c >_b d\} - \sharp\{b \in P \mid d >_b c\}$$

- We will interpret the margin function m as a graph, say G.

Schulze Method

- A directed *path* in G from candidate c to candidate d is a sequence

$$c \xrightarrow{m(c,c_1)} c_1 \xrightarrow{m(c_1,c_2)} c_2 \qquad \cdots \qquad c_n \xrightarrow{m(c_n,d)} d$$

- The strength, st, of a path in G is

$$st(c_0, \ldots, c_{n+1}) = \min\{m(c_i, c_{i+1}) \mid 0 \leq i \leq n\}.$$

Schulze Method

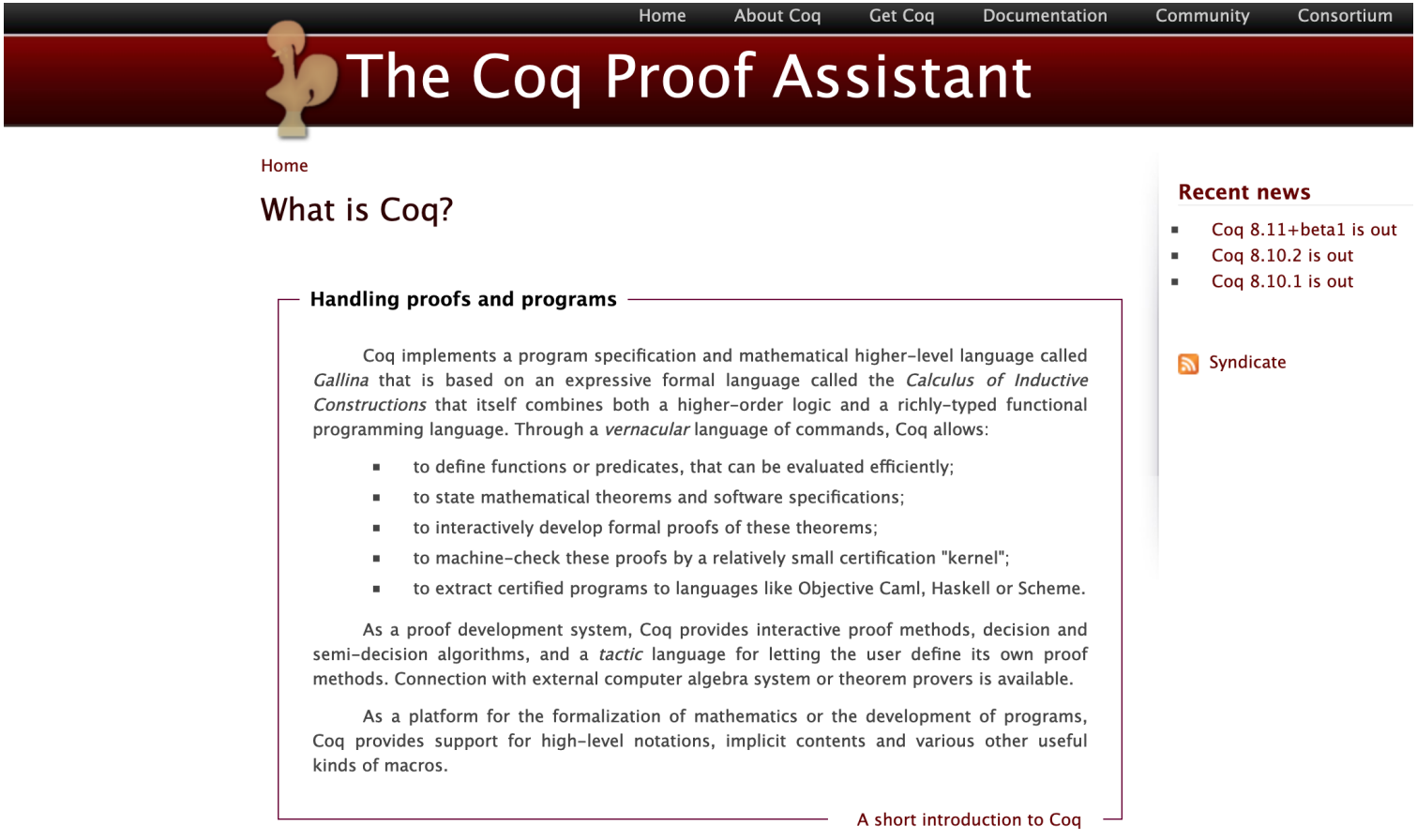
- We compute the generalized margin, M, between two candidate c d as

$$M(c, d) = \max\{st(p) : \text{p is path from c to d in G}\}$$

- The winning set is defined as

$$W = \{c \in C : \forall d \in C \setminus \{c\}, M(c, d) \geq M(d, c)\}$$

Correctness



Coq in Action

Natural Number with addition function and proof of commutativity and associativity

```
{- Natural Number Definition-}
Inductive nat :=
| O : nat
| Suc : nat -> nat.

{- Addition on Natural Numbers -}
Fixpoint add (n m : nat) : nat :=
  match n with
  | O => m
  | Suc n' => Suc (add n' m)
  end.

{- Commutative Property  -}
Theorem add_commute : forall (n m : nat), add n m = add m n.
Proof.
  (* proof terms omitted *)
Qed.
```

Coq in Action

Graph Theory

```
{- Propositional Path -}
Inductive Path (k: Z) : node -> node -> Prop :=
| unit c d : m c d >= k -> Path k c d
| cons  c d e :
    m c d >= k -> Path k d e -> Path k c e.

{- Notion of winner at prop level -}
Definition wins_prop (c: node) :=
  forall d : node, exists k : Z,
   Path k c d /\
   (forall l, Path l d c -> l <= k).

{- Notion of loser at prop level -}
Definition loses_prop (c : node) :=
  exists k: Z, exists  d: node,
   Path k d c /\
   (forall l, Path l c d -> l < k).
```

Verifiability (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.

Verifiability by Scrutiny Sheet

```
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)]
```

Privacy by Homomorphic Encryption

- A encryption scheme is homomorphic if for any two plaintext x and y: $Enc_{pk}(x) \bigotimes Enc_{pk}(y) = Enc_{pk}(x \bigoplus y)$
- $Enc(m_1, r_1) := (g^{r_1}, g^{m_1} * h^{r_1})$
- $Enc(m_2, r_2) := (g^{r_2}, g^{m_2} * h^{r_2})$
- $Enc(m_1, r_1) * Enc(m_2, r_2) = (g^{r_1+r_2},\ g^{m_1+m_2} * h^{r_1+r_2})$

In Reality, it looks more messy

$g = 4, h = 4922859360787499095466607161477777608 7$
(13449645143730022101228603336170713009 3,
10222721011125778006576417922765826410 7)
(90549562016409048906553052880573051723,
14973766480913023217342348558030544758 0)
(11183864691309926814452565123193527538 5,
23076766166773179621624801755228562722)
(16360967526688511750725314553046957450 7,
13684092549193311600688148156555226669 8)

Zero-Knowledge-Proof

Did you all trust me when I claimed that the all the values are encryption of 0?

Zero-Knowledge-Proof

- Given a public parameters (G, g, p, h) and private parameter x such that $h := g^x$.
- Claim: message m is honest decryption of (c_1, c_2) (where $c_1 = g^r$ and $c_2 = g^m * h^r$)
- Proof: $(g, h, c_1, c_2 \cdot g^{-m})$ is a *Diffie Hellman* tuple

Zero-Knowledge-Proof

Diffie Hellman Tuple: a tuple (g, h, u, v) is a *Diffie Hellman* tuple if there $\exists\ w \mid u = g^w \wedge v = h^w$.

- P chooses a random r and sends $a = g^r$ and $b = h^r$.
- V sends a random e
- P sends $z = r + e \cdot w$
- V check $g^z = a \cdot u^e$ and $h^z = b \cdot v^e$

$g^z = g^{r+e \cdot w} = a \cdot (g^w)^e = a \cdot u^e$
$h^z = h^{r+e \cdot w} = b \cdot (h^w)^e = b \cdot v^e$

Zero-Knowledge-Proof

Claimed: $(g, h, c_1, c_2 \cdot g^{-m})$ is a *Diffie Hellman* tuple

$(g, h, c_1, c_2 \cdot g^{-m})$

$= (g, h, g^r, g^m \cdot h^r \cdot g^{-m})$

$= (g, h, g^r, h^r)$

$= (g, h, u, v)$

Could I have faked it?

$(g, h, g^r, g^m \cdot h^r \cdot g^{-m_1})$

$= (g, h, g^r, h^r \cdot g^{m-m_1})$

Schulze Voting as Evidence Carrying Computation

- 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

- 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

- 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

Certificate : Verifying Elections Formally

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

Machine Check Properties

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

Future Work

- Formalizing cryptographic code (Shuffle Proof)
- Formalizing the properties of Schulze method
- Formaly verified checker
- Risk Limiting Audit
- Formalizing Code Extraction (Not related to our project, but highly needed for electronic voting)

Publications

1. Pattinson, D. and Tiwari, M., 2017. Schulze Voting as Evidence carrying computation. In Proc. ITP 2017, vol. 10499 of Lecture Notes in Computer Science, 410–426. Springer.
2. Lyria Bennett Moses, Rajeev Goré, Ron Levy, Dirk Pattinson, Mukesh Tiwari. No More Excuses: Automated Synthesis of Practical and Verifiable Vote-Counting Programs for Complex Voting Schemes. E-VOTE-ID 2017: 66-83
3. Thomas Haines, Dirk Pattinson, and Mukesh Tiwari. 2019. Verifiable Homomorphic Tallying for the Schulze Vote Counting Scheme. 11th International Conference Verified Software: Theories, Tools, and Experiments. VSTTE 2019 (to appear)

Publications

1. Thomas Haines, Rajeev Goré, and Mukesh Tiwari. 2019. Verified Verifiers for Verifying Elections. In Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security (CCS '19)
2. Milad K. Ghale, Rajeev Goré, Dirk Pattinson, Mukesh Tiwari. Modular Formalisation and Verification of STV Algorithms. E-Vote-ID 2018: 51-66

Thank You!