Which e-voting problems do we need to solve?

Vanessa Teague

CRYPTO 2021

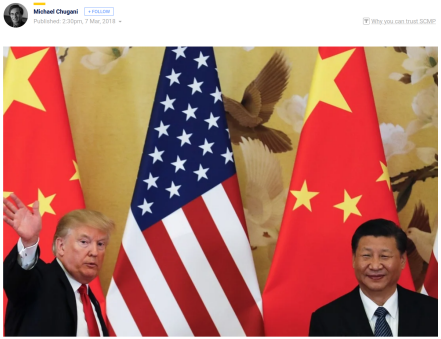
Thinking Cybersecurity Pty. Ltd. and the Australian National University

Based on joint work with many many excellent people...

Is democracy really stuffed?

Xi's world or Trump's? The choice is between prosperous authoritarianism or chaotic freedom in the new cold war

Michael Chugani says Chinese President Xi Jinping and US President Donald Trump represent two different philosophies, one promising stable and prosperous authoritarianism, the other, chaotic democracy with greater personal and internet freedom



US President Donald Trump and Chinese President Xi Jinping after a joint press conference at the Great Hall of the People in Beijing in 2017. The two leaders represent differing world views on a polarised global stage. Photo: AP

Actually it's authoritarianism that's chaotic.

But insecure electoral processes jeopardize the core self-correction property of democracy.

https://www.scmp.com/comment/insight-opinion/article/2136084/xis-world-or-trumps-choice-between-prosperous

What can cryptographers do?

- This talk is addressed to cryptographers who'd like to help support their own democracies.
- **Assumption:** I'm going to keep believing in the basic rationality of most of our species, even if the empirical evidence in support of this thesis is a bit iffy at the moment.

Some things we can do

Find bugs and gaps in existing schemes

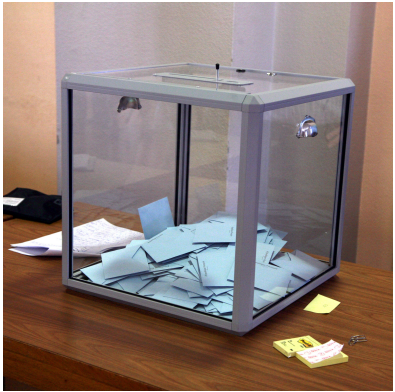
Design new schemes

Teach people to think adversarially

What are the security requirements?

Public verifiability and the secret ballot

whether you're using paper



or bronze

...or computers

Pics from https://commons.wikimedia.org/wiki/File:Election_presidentielle_2007_Lausanne_MG_2761.jpg and https://commons.wikimedia.org/wiki/File:Athenian_Secret_Ballot.jpg. Creative Commons.

Are there bugs or security problems in existing Internet voting schemes?

- SwissPost/Scytl
- iVote/NSW
- Voatz
- Civitas/JCJ
- Estonia?

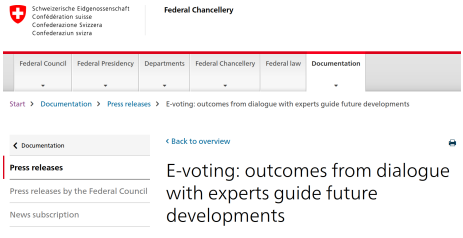
A short overview of the Swisspost/Scytl/New South Wales/iVote problems

- They were *verification* bugs: a cheating prover could pass verification but manipulate votes
- There is nothing wrong with the Bayer-Groth mixnet, nor with the Fiat-Shamir heuristic applied to Chaum-Pedersen Proofs, nor with Pedersen commitments, but
- Swisspost/Scytl/iVote implemented the Bayer-Groth mixnet with Pedersen commitments without verifying that the parameters were created s.t. nobody would know the trapdoor.
  - Joint work with Sarah Jamie Lewis and Olivier Pereira[1]; independently noticed by Thomas Haines and Ralf Haenni
  - **Actually the provers (mixers) did know the trapdoor**
- Swisspost/Scytl/iVote implemented the 'weak' Fiat-Shamir Heuristic for decryption proofs
  - sound against a prover who can't choose the statement
  - **but the provers could (partly) choose the statement**

[1] Haines, Lewis, Pereira, T "How not to prove your election outcome," IEEE S&P '20

Swisspost/Scytl and New South Wales/iVote: different democracies respond very differently (1 - Switzerland)

Each country realised they had run, or were running, broken systems in real elections. This is what happened in Switzerland...[2]



[2]CoI statement: I've received $ from the Swiss Federal Chancellery for consulting work associated with their expert dialogue. All the reports are (or soon will be) public.

Swisspost/Scytl and New South Wales/iVote: different democracies respond very differently (2 - New South Wales)

...and this is what happened in New South Wales

From a parliamentary committee hearing[3] after questions about the bugs

> **Mr CANT:** Some of the mathematics is beyond me as well. But if you look at the submission that Dr Vanessa Teague made, one of the principles that we try to apply is to make it so it is verifiable from the input of the vote all the way through to the count. More so than in any other voting channel, there are checks and mathematical proofs in place to prove that the data that was put into the system matches the data that comes out the other end. We have independent auditors who audit that process. We have got a cryptographer who comes in to check all the cryptographing to ensure that all the mathematical proofs operate correctly.

Injecting rational scientific evidence sometimes works. Sometimes it doesn't. Empirical testing on your own democracy is encouraged. Also make sure your country has transparency laws, not secrecy laws.

[3] Parliament of New South Wales, 18 Nov 2019
https://www.parliament.nsw.gov.au/ladocs/transcripts/2265/Corrected%20Transcript%20-%20Public%20Hearing%20-%20Administration%20of%20the%20NSW%20State%20Election%20-%2018%20November%202019.pdf

Quality academic systems aren't perfect either

- The Juels-Catalano-Jakobsson coercion-resistant voting scheme requires universally-verifiable *Plaintext Equivalence Proofs*
- But the paper refers to distributed-trust *Plaintext Equivalence Tests*
- The Civitas implementation uses *Plaintext Equivalence Tests*
- There is nothing wrong with the *primitive*, and nothing wrong with the *protocol*
- but universal verifiability fails[4]
- because of misalignment between the properties assumed by the protocol, and the properties achieved by the primitive.

Even Helios has had bugs—that's why Olivier Pereira knew to look for Weak F-S in the SwissPost system.

This probably shouldn't surprise anyone, given that every sufficiently large software system has security problems and bugs, but it surprises me that people keep being surprised when it happens.

[4] McMurtry, Pereira, T "When is a test not a proof?" ESORICS '20

What about the Estonian system?

But we know how to do cast-as-intended verification don't we?

Accountability: It really matters whether "catching" a cheater allows you to prove who cheated

Accessible voting over the Internet?

The things needed for actual cast-as-intended verification without a paper ballot are the least-usable things anywhere in security.

This may not be the fault of cryptographers[5]

Can Voters Detect Malicious Manipulation of Ballot Marking Devices?

Matthew Bernhard, Allison McDonald, Henry Meng, Jensen Hwa, Nakul Bajaj*, Kevin Chang, J. Alex Halderman

University of Michigan *The Harker School

***Abstract*—Ballot marking devices (BMDs) allow voters to select candidates on a computer kiosk, which prints a paper ballot that the voter can review before inserting it into a scanner to be tabulated. Unlike paperless voting machines, BMDs provide voters an opportunity to verify an auditable physical record of their choices, and a growing number of U.S. jurisdictions are adopting them for all voters. However, the security of BMDs depends on how reliably voters notice and correct any adversarially induced errors on their printed ballots. In order to measure voters' error detection abilities, we conducted a large study (N = 241) in a realistic polling place setting using real voting machines that we modified to introduce an error into each printout. Without intervention, only 40% of participants reviewed their printed ballots at all, and only 6.6% told a poll worker something was wrong. We also find that carefully designed interventions can improve verification performance. Verbally**

However, BMDs do not eliminate the risk of vote-stealing attacks. Malware could infect the ballot scanners and change the electronic tallies—although this could be detected by rigorously auditing the paper ballots [50]—or it could infect the BMDs themselves and alter what gets printed on the ballots. This latter variety of cheating cannot be detected by a post-election audit, since the paper trail itself would be wrong, and it cannot be ruled out by pre-election or parallel testing [51]. Instead, BMD security relies on voters themselves detecting such an attack. This type of human-in-the-loop security is necessary in many systems where detection and prevention of security hazards cannot be automated [18]. However, as several commentators have recently pointed out [7], [20], [51], its effectiveness in the context of BMDs has not been established

[4]Bernhard, Matthew, Allison McDonald, Henry Meng, Jensen Hwa, Nakul Bajaj, Kevin Chang, and J. Alex Halderman. "Can Voters Detect Malicious Manipulation of Ballot Marking Devices?." IEEE S & P 2020

Different countries vote differently, so different solutions may (or may not) work

- e.g. Code voting usability
- empirical studies[6] show that, when incorporated into the voting process, it's more effective than challenge-based methods
- It obviously doesn't work for Australia because we have preferential voting
- it also doesn't work for a lot of the US either because there are zillions of contests
- Its trust assumptions are much stronger

Think about the requirements for your country.

[6] Kulyk, Oksana, Jan Henzel, Karen Renaud, and Melanie Volkamer. "Comparing 'challenge-based' and 'code-based' internet voting verification implementations." In IFIP Conference on Human-Computer Interaction, pp. 519-538. Springer, Cham, 2019.

Receipt Freeness[8] is really really hard

- Receipt-freeness is achievable in a polling place (where the voter doesn't control the voting computer, but you'd better hope the adversary doesn't either)
- Also remotely in a "passive" sense in which, if you follow the protocol, you can't subsequently prove how you voted. Many schemes have this property (though plenty don't)
- But really being unable to prove how you voted, even if you have the opportunity to deviate from the protocol (e.g. by bringing in some special values from the coercer), is really hard, especially if the voter controls the means of election
- Even in a polling place, it's harder than it seems[7]

[7] Moran, Tal, and Moni Naor. "Split-ballot voting: everlasting privacy with distributed trust." ACM Transactions on Information and System Security (TISSEC) 13, no. 2 (2010): 1-43.

[8] Josh Benaloh and Dwight Tuinstra, "Receipt-Free Secret Ballot Elections" STOC 1994

Five things that are much easier in a polling place

1. Privacy/coercion
   because voter is alone
   unless they have their smart phone...
2. Receipt freeness
   because voter doesn't control the voting device
3. Accountability
   because you might be able to prove the system malfunctioned
4. Easier individual verification
   because the authorities can keep a paper ballot
5. "Carefully designed interventions" to encourage careful verification

Image from https://commons.wikimedia.org/wiki/File:2016_Australian_Election_-_Voting_booths.jpg. Creative Commons.

Risk Limiting Audits

Risk-limiting audits (RLAs) offer a statistical guarantee: if a full manual tally of the paper ballots would show that the reported election outcome is wrong, an RLA has a known minimum chance of leading to a full manual tally. The probability of mistakenly certifying a wrong election result is bounded by the *Risk Limit*.

- Extensive theory for various kinds of election setups
- First-past-the-post, instant-runoff, D'Hondt, etc
- Open-source software[9]

Limitations:

- You can only verify if you are physically present
- Paper-ballot custody assumption

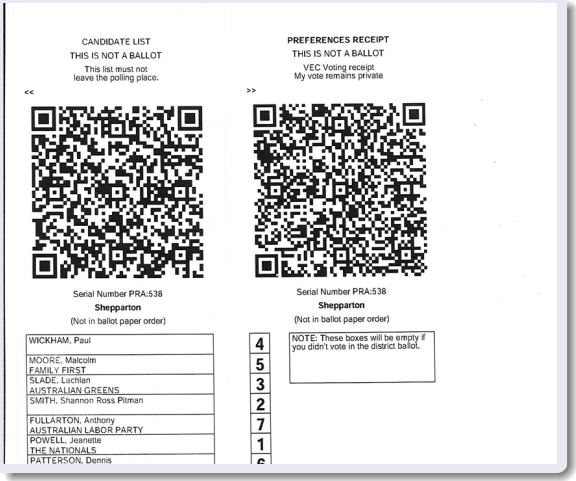
[9] Philip Stark's SHANGRLA: `https://github.com/pbstark/SHANGRLA`, VotingWorks's ARLO: `https://www.voting.works/risk-limiting-audits`

Risk Limiting Audits

Actually *running* an RLA as a publicly-verifiable process requires some crypto.[10]

[10] Image from Ars Technica.

End-to-end verifiable voting in a polling place


CANDIDATE LIST

THIS IS NOT A BALLOT

This list must not leave the polling place.

<<

Serial Number PRA:538

Shepparton

(Not in ballot paper order)

WICKHAM, Paul	4
MOORE, Malcolm FAMILY FIRST	5
SLADE, Lachlan AUSTRALIAN GREENS	3
SMITH, Shannon Ross Pitman	2
FULLARTON, Anthony AUSTRALIAN LABOR PARTY	7
POWELL, Jeanette THE NATIONALS	1
PATTERSON, Dennis	6

PREFERENCES RECEIPT

THIS IS NOT A BALLOT

VEC Voting receipt
My vote remains private

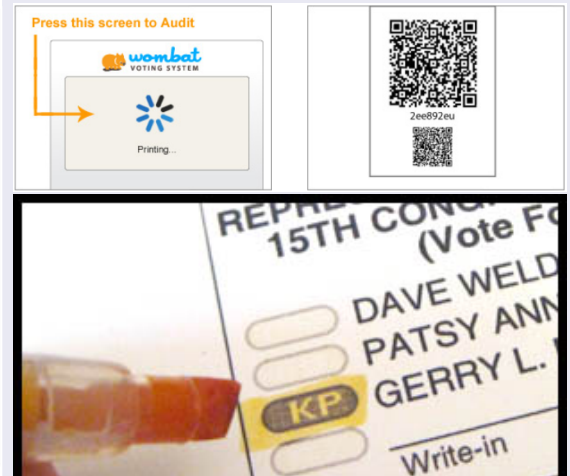
>>

Serial Number PRA:538

Shepparton

(Not in ballot paper order)

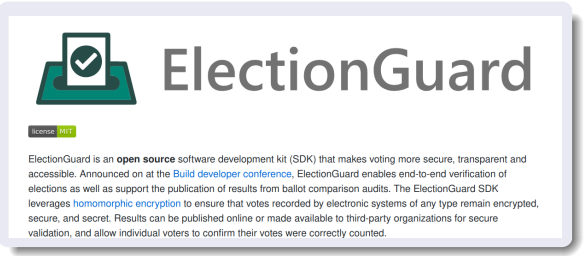
NOTE: These boxes will be empty if you didn't vote in the district ballot.



vVote https://arxiv.org/pdf/1404.6822.pdf, Wombat Voting https://wombat.factcenter.org/, Scantegrity II https://scantegrity.com/

Hybrid schemes: best of end-to-end verifiability & RLAs

- Cryptographic evidence that your ballot was counted, even if you don't trust the paper-ballot custody in the polling place
- Statistical evidence that the election outcome is right, even if you don't trust the crypto



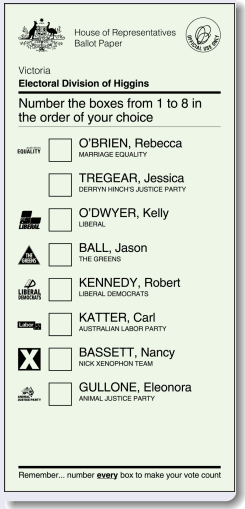
Technical open problems

-  Cryptographic verification that can be escalated if the result is close
-  Publicly-verifiable privacy
-  Cast as intended verification is the hardest part. You have to design it for your own country, because nothing designed for a different country is likely to work.
-  "Carefully designed interventions" to encourage careful verification
-  Hybrid schemes for remote voting?
-  Eligibility Verifiability with a private voter list?

Reality check

In Victoria, the code to arrange candidates on a ballot[a] is (was) open[b]

```
public static class BallotDrawHelper
{
    private static readonly Random random = new Random();
    public static int[] GenerateRandomPositions(int count)
    {
        if (count <= 0)
            throw new ArgumentOutOfRangeException("count");
        {
            var positions = new List<int>(count);
                for (int i = 0; i < count; i++)
            {
                int next;
                do
                { next = random.Next(1, count + 1);
                } while (positions.Contains(next));
                positions.Add(next);
            }
            return positions.ToArray();
        }
    }
}
```



[a] Ballot image from https://en.wikipedia.org/wiki/Electoral_system_of_Australia

[b] Wayback machine: https://web.archive.org/web/20150728062821/http://www.vec.vic.gov.au/files/EMS/BallotDrawHelper.txt

What else can we do?

Find out what's wrong with your own electoral system and fix it before the election

Try to get an agreement on *requirements*

Persuade your fellow citizens that they need to build evidence into their electoral processes, rather than building them so that everything looks OK.