

Democracy, Security and Evidence
let's have all three
ASIACRYPT 2018

Vanessa Teague

University of Melbourne

December 5, 2018

Secure voting system designs predate computers

Actually, they predate paper too.



- ▶ The votes are private.
- ▶ The election result is publicly verifiable.

image: Sharon Mollerus. https://commons.wikimedia.org/wiki/File:Athenian_Secret_Ballot.jpg

End-to-end verifiability

1. Voters can check that their vote is cast as they intended and
2. included in the count.
3. The election result is publicly verifiable.

Helios

Used in IACR elections.

1. Voters can challenge ciphertexts and demand to see the randomness used to generate them, which can then be confirmed using another device. They cast one they haven't challenged.
2. Voters can look up the ciphertext on a public bulletin board.

Audited Ballots for IACR 2017 Election - Mozilla Firefox

https://vote.heliosvoting.org/helios/elections/4f4814b7-87e5-47c5-a85d-09f4a2f945cf/audited

Helios Voting About Code Docs FAQ Privacy Help!

IACR 2017 Election — Audited Ballots [\[back to election\]](#)

When you prepare a ballot with Helios, you immediately receive a smart ballot tracker. Before you choose to cast that ballot, you have the option to ask Helios to “break open” that encrypted ballot and verify that Helios encrypted your ballot correctly. Once that’s done, you can post that opened ballot here, on the audited ballots’ list, for everyone to verify (your identity is not included). Once you’ve done this, you have to re-encrypt your choices and obtain a different smart ballot tracker. This helps reduce the chance that someone might coerce you to vote differently from your true choice.

These ballots are *not* cast, and they will not be counted. They are just here for auditing purposes, to spot-check that Helios is properly encrypting voter’s choices.

To verify an audited ballot, copy its entire content and paste it in the [single ballot verifier](#).

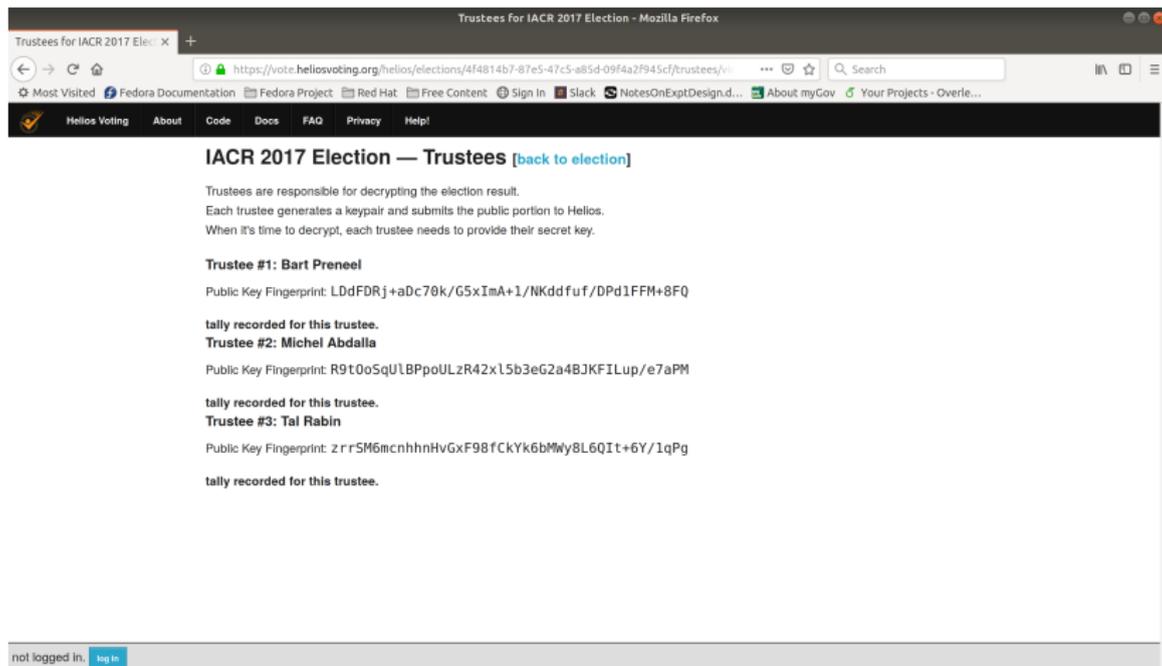
Audited Ballots 1 - 50

4SnB2hnF7ZLs7wQvJFyIUSTFN0Gc/EMvTMD09McabIQ [view]
4yGMbD0n5zI5wfZty13bgzgg@YYPWeUgUryYGH0rBjPjU [view]
9mwq5s7sTV19DAIXw4sEoNxAZ27/k7Gqc2rDHTI0haKs [view]
9oJjYnTdxwBytyFgkT19pIQfnA8+rK0TwtU/BRqM3W90 [view]
bG+FH0jaYcMT06CBMFBVns2t6PG9GFvV9fCYKFAKBMU [view]
f9CKj1imcb0DcD7skffKxmwBzaky5cL+JGeKwFKdMJQ [view]
FbhEhoaq3kqLrnzd9EqBy8m87roMdjvnFMZz/6APgak [view]

Helios (cont'd)

Used in IACR elections.

- 3 Votes are added using homomorphic encryption. The total is decrypted and proven correct with ZKPs.



The screenshot shows a web browser window titled "Trustees for IACR 2017 Election - Mozilla Firefox". The address bar shows the URL: <https://vote.heliosvoting.org/helios/elections/4f4814b7-87e5-47c5-a85d-09f4a2f945cf/trustees/vi>. The page content includes a navigation menu with links for Helios Voting, About, Code, Docs, FAQ, Privacy, and Help!.

IACR 2017 Election — Trustees [\[back to election\]](#)

Trustees are responsible for decrypting the election result.
Each trustee generates a keypair and submits the public portion to Helios.
When it's time to decrypt, each trustee needs to provide their secret key.

Trustee #1: Bart Preneel
Public Key Fingerprint: LDdFDRj+aDc70k/G5xImA+1/NKddfuf/DPd1FFM+8FQ
tally recorded for this trustee.

Trustee #2: Michel Abdalla
Public Key Fingerprint: R9t0o5qULBPpouLzR42xL5b3eG2a4BJKFIUp/e7aPM
tally recorded for this trustee.

Trustee #3: Tal Rabin
Public Key Fingerprint: 2r r5M6mcnhhhHvGxF98fCkYk6bMMy8L6QIt+6Y/1qPg
tally recorded for this trustee.

At the bottom left, there is a "not logged in. [login](#)" link. At the bottom right, there are navigation icons for back, forward, and search.

Known attacks, weaknesses, etc.

1. It's not receipt-free: you can remember the randomness used to encrypt your vote, and thus prove what you cast.
2. Voters could be tricked into not verifying properly.
3. Voters could be tricked into going to the wrong website.
4. Voters could be tricked into not looking at the real bulletin board.
5. Some older variants are vulnerable to the “clash attack,” in which ≥ 2 voters think the same vote is theirs. (This is fixed by generating IDs carefully.)
6. ...

What is evidence exactly?

- ▶ Is it enough for the result to be verifiable, or should we insist that it be verified?
- ▶ What if none of the (other) voters bother verifying?
- ▶ Do we need statistical confidence, e.g. from Risk-Limiting Audits of paper ballots?
- ▶ Or does the possibility of getting caught disincentivize cheating?

What is evidence exactly?

- ▶ Is it enough for the result to be verifiable, or should we insist that it be verified?
- ▶ What if none of the (other) voters bother verifying?
- ▶ Do we need statistical confidence, e.g. from Risk-Limiting Audits of paper ballots?
- ▶ Or does the possibility of getting caught disincentivize cheating?

My two cents: it's a little like Popper's definition of a scientific theory. An election process that is verifiable might still give you a wrong answer (if nobody verified), but an election process that's not verifiable isn't an election process at all.

What would you do if you were running this in Australia?

e.g. our paper on privacy-preserving tallying of preferential votes
(which can't be counted by addition).

with Kim Ramchen, Chris Culnane and Olivier Pereira:

<https://eprint.iacr.org/2018/246>

Instant-runoff Voting (IRV)

Used in Australia, Canada, India, Ireland, U.K., U.S., ...

The image shows two ballot papers side-by-side. The left one is for the Newcastle electorate, and the right one is a green ballot paper. Both show a list of candidates with numbers in boxes next to their names. A blue arrow points from the '1' next to Michael Osborne on the Newcastle ballot to the '1' next to Andrew Tracey on the green ballot.

House of Representatives (Small green ballot)

Electorate of NEWCASTLE

10 CHENOFF, Michael AUSTRALIAN FIRST PARTY
2 ALCOCK, Zane BOUNDER AVIATION
7 MCELLEAN, Yvonne Daily PREMIER INVESTMENT
4 HOLDING, Fred INDEPENDENT
3 SCURRY, Susanna INDEPENDENT
9 CAINE, Brian CHRISTIAN DEMOCRATIC PARTY (RED THE GREENS)
8 ABBOTT, Janice LIBERAL
6 HIGGINS, Lawrence Joseph AUSTRALIAN INDEPENDENTS
5 CLAYDON, Sharon LIBERAL
1 OSBORNE, MICHAEL THE GREENS

Number the small ballot paper as shown. You must number all boxes. Use numbers only.

please return for re-use

HOUSE OF REPRESENTATIVES (green ballot paper)

On the green ballot paper You must number every box Vote 1 Tracy Andrew then others of your choice

5 MITCHELL, Rob
6 ANDERSON, James
9 BARKER, Neil
7 JERMYN, Chris
2 LEE, Ross
1 TRACEY, Andrew AUSTRALIAN COUNTRY PARTY
4 TRUSCOTT, Geoff
8 VAINA, Cathy
3 LONG, Dorothy Lorraine

Instant-runoff Voting (IRV)

Used in Australia, Canada, India, Ireland, U.K., U.S., ...



Counting process (single winner):

1. Count votes, using 1st preference only
If a candidate gets majority, he wins
2. Remove candidate with lowest number of votes
“Shift left” the ballots that contained a vote for that candidate
Go back to 1.

Publishing complete votes causes a privacy problem

- ▶ Because the number of permutations can be much larger than the number of voters.
- ▶ So the coercer demands a particular permutation and then punishes the voter if it doesn't appear.

Verifiable Tallying for IRV

This would provide IRV tallies that only leak partial counts at each round (which is required in most places anyway).

Verifiable Tallying for IRV

This would provide IRV tallies that only leak partial counts at each round (which is required in most places anyway).

But we need fully homomorphic encryption or verifiable MPC!

Verifiable Tallying for IRV

This would provide IRV tallies that only leak partial counts at each round (which is required in most places anyway).

But we need fully homomorphic encryption or verifiable MPC!

- ▶ Fully homomorphic encryption still looks expensive/cumbersome

Verifiable Tallying for IRV

This would provide IRV tallies that only leak partial counts at each round (which is required in most places anyway).

But we need fully homomorphic encryption or verifiable MPC!

- ▶ Fully homomorphic encryption still looks expensive/cumbersome
- ▶ Secret sharing based verifiable MPC solutions [BaumDO'14] use
 - ▶ secure channels between voters and trustees
 - ▶ distributed key generation (not fully threshold) in covert adversary model

Verifiable Tallying for IRV

This would provide IRV tallies that only leak partial counts at each round (which is required in most places anyway).

But we need fully homomorphic encryption or verifiable MPC!

- ▶ Fully homomorphic encryption still looks expensive/cumbersome
- ▶ Secret sharing based verifiable MPC solutions [BaumDO'14] use
 - ▶ secure channels between voters and trustees
 - ▶ distributed key generation (not fully threshold) in covert adversary model
- ▶ Threshold public key encryption based solutions rely on:
 - ▶ RSA moduli with unknown factors [CramerDN01, SchoenmakersV15]
⇒ key generation cumbersome

Somewhat Homomorphic Encryption with Encryption Switching

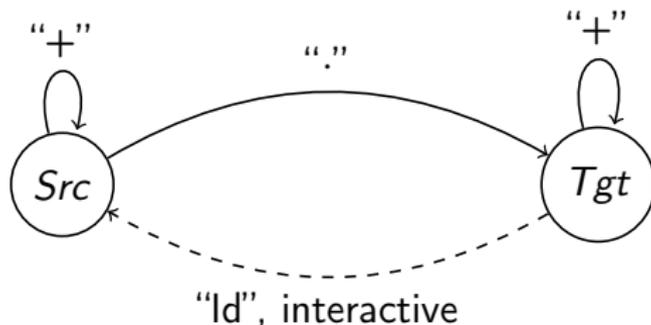
Our solution:

- ▶ Design a somewhat homomorphic encryption scheme with threshold key generation in the malicious adversary setting
⇒ we can do many “+” and one “.” (then more “+”)
[BonehGohNissim05, CatalanoFiore15]

Somewhat Homomorphic Encryption with Encryption Switching

Our solution:

- ▶ Design a somewhat homomorphic encryption scheme with threshold key generation in the malicious adversary setting
⇒ we can do many “+” and one “.” (then more “+”)
[BonehGohNissim05, CatalanoFiore15]
- ▶ Design a multi-party encryption switching protocol from *target* space to *source* space
⇒ after switching, we can do one more multiplication!

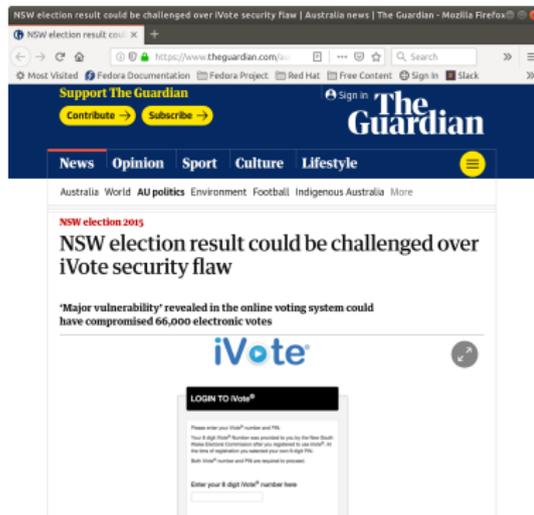


What actually happens when Internet voting runs in Australia?

- ▶ The Australian State of New South Wales runs an Internet voting system called iVote.

What actually happens when Internet voting runs in Australia?

- ▶ The Australian State of New South Wales runs an Internet voting system called iVote.



NSW election result could be challenged over iVote security flaw | Australia news | The Guardian - Mozilla Firefox

NSW election result could be challenged over iVote security flaw

Major vulnerability revealed in the online voting system could have compromised 66,000 electronic votes

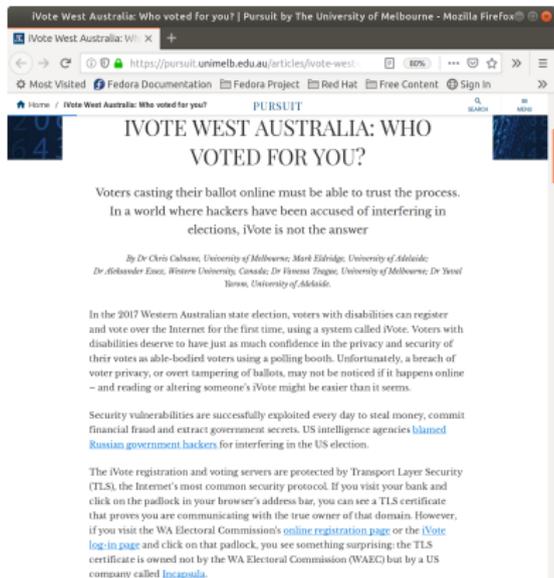
iVote

LOGIN TO iVote®

Please enter your iVote® number and PIN

Your iVote® number was provided to you by the Western Australian Electoral Commission when you applied to use iVote®. An iVote® PIN is generated for you when you log in. Both iVote® number and PIN are essential to access iVote.

Enter your 8 digit iVote® number here



iVote West Australia: Who voted for you? | Pursuit by The University of Melbourne - Mozilla Firefox

iVote West Australia: Who VOTED FOR YOU?

Voters casting their ballot online must be able to trust the process. In a world where hackers have been accused of interfering in elections, iVote is not the answer

By Dr Chris Cabane, University of Melbourne; Mark Edridge, University of Adelaide; Dr Aleksander Enes, Western University; Canada; Dr Francis Tsopas, University of Melbourne; Dr Yoon, University of Adelaide.

In the 2017 Western Australian state election, voters with disabilities can register and vote over the Internet for the first time, using a system called iVote. Voters with disabilities deserve to have just as much confidence in the privacy and security of their votes as able-bodied voters using a polling booth. Unfortunately, a breach of voter privacy, or overt tampering of ballots, may not be noticed if it happens online – and reading or altering someone's iVote might be easier than it seems.

Security vulnerabilities are successfully exploited every day to steal money, commit financial fraud and extract government secrets. US intelligence agencies [blamed Russian government hackers](#) for interfering in the US election.

The iVote registration and voting servers are protected by Transport Layer Security (TLS), the Internet's most common security protocol. If you visit your bank and click on the padlock in your browser's address bar, you can see a TLS certificate that proves you are communicating with the true owner of that domain. However, if you visit the WA Electoral Commission's [online registration page](#) or the [iVote log-in page](#) and click on that padlock, you see something surprising: the TLS certificate is owned not by the WA Electoral Commission (WARC) but by a US company called [Incapsula](#).

Is it end-to-end verifiable?

- ▶ “Verification” consists of telephoning an automated system that reads back your vote to you.

Is it end-to-end verifiable?

- ▶ “Verification” consists of telephoning an automated system that reads back your vote to you.
- ▶ The Electoral Commission said after the election that “Some 1.7% of electors who voted using iVote® also used the verification service and none of them identified any anomalies with their vote.”

Is it end-to-end verifiable?

- ▶ “Verification” consists of telephoning an automated system that reads back your vote to you.
- ▶ The Electoral Commission said after the election that “Some 1.7% of electors who voted using iVote® also used the verification service and none of them identified any anomalies with their vote.”
- ▶ A year later they admitted that about 10% of calls hadn’t been able to retrieve any vote at all.

So are they going to fix that?

An independent inquiry recently released the report of its investigation into iVote. They said:

- ▶ iVote is used only for a small fraction of votes (about 6%),

¹But we should add some verifiability.

So are they going to fix that?

An independent inquiry recently released the report of its investigation into iVote. They said:

- ▶ iVote is used only for a small fraction of votes (about 6%),
- ▶ therefore nobody will bother to attack it,

¹But we should add some verifiability.

So are they going to fix that?

An independent inquiry recently released the report of its investigation into iVote. They said:

- ▶ iVote is used only for a small fraction of votes (about 6%),
- ▶ therefore nobody will bother to attack it,
- ▶ therefore it is secure in a realistic attacker model,

¹But we should add some verifiability.

So are they going to fix that?

An independent inquiry recently released the report of its investigation into iVote. They said:

- ▶ iVote is used only for a small fraction of votes (about 6%),
- ▶ therefore nobody will bother to attack it,
- ▶ therefore it is secure in a realistic attacker model,
- ▶ therefore it should be expanded nationwide.¹

Report at http://www.elections.nsw.gov.au/about_us/plans_and_reports/independent_reports/report_on_the_ivote_system

¹But we should add some verifiability.

What about academic concerns re large-scale undetectable electoral fraud?

“The key difficulty I have with this argument is that it places too much weight on theoretical possibility and not enough on empirical likelihood, or probability of things occurring.”

Did I promise not to mention the Telecommunications Assistance and Access bill?

[The Opposition said] the bill was still “far from perfect and there are likely to be significant outstanding issues.”

What can we do?