Every Vote Counts: Ensuring Integrity in Large-Scale Electronic Voting

Speaker: Feng Hao

School of Computing Science
Newcastle University, UK

USENIX EVT/WOTE'14

Acknowledgment

Joint work with:

- Matthew Kreeger (Thales E-Security, UK)
- Brian Randell (Newcastle University, UK)
- Dylan Clarke (Newcastle University, UK)
- Siamak F. Shahandashti (Newcastle University, UK)
- Peter Hyun-Jeen Lee (Newcastle University, UK)

European Research Council

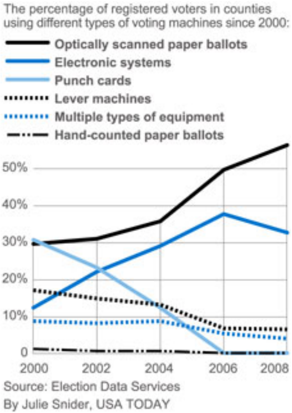
E-voting has been widely used worldwide

Direct Recording Electronic (DRE)

Internet voting

- Local polling station voting using DRE
  - 100% DRE usage in elections in India, Brazil
- Remote e-voting using Internet
  - Estonia held the first national Internet election in 2007

However, e-voting is controversial

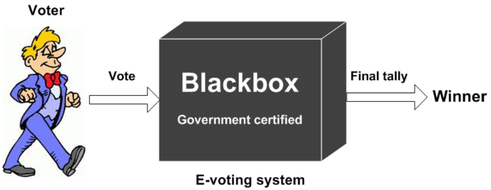


- 2000, rapid adoption of e-voting in US.
- 2006, quick abandonment by several states.
- 2008, Netherlands suspended e-voting.
- 2009, Germany suspended e-voting.
- 2009, Ireland suspended e-voting.
- 2014, Norway suspended e-voting.

What's the future of e-voting?

Will e-voting be more widely used? Or should it be abandoned?

What's wrong with current e-voting deployment?



- They are unverifiable, working like a blackbox.
- Governments hoped to establish trust by certification.
- But it takes only one successful attack on a "certified" system to destroy the confidence.

End-to-End (E2E) verifiable e-voting

- Lesson from the past: verifiability is important
- But that isn't anything new
- E2E verifiable e-voting has been known for over 20 years
- Many E2E systems proposed in the past
- So the problem solved?

However, there is a gap between theory and practice

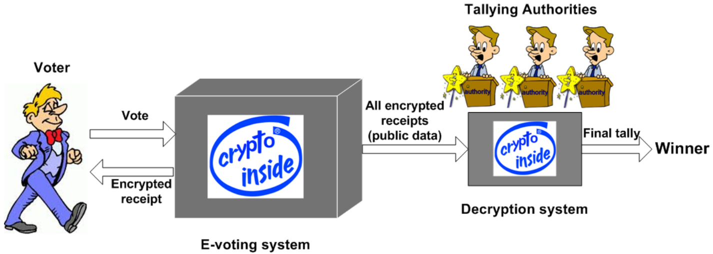
- Despite the extensive theoretical research on E2E, the practical impact has been limited.

Narrowing the gap - an engineering approach

- We take an engineering approach.
- The basic engineering principle: simplicity
- "Keep everything as simple as possible, but not simpler"
- Hence, we start by asking:

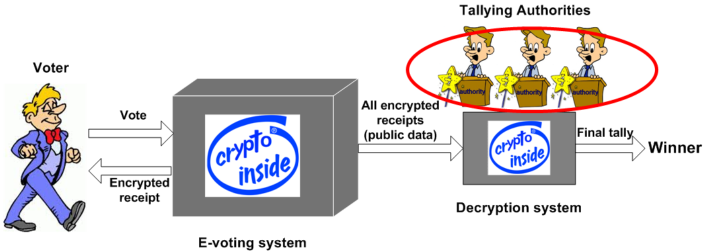
Is the current E2E system as simple as it can be?

The state-of-the-art in E2E



- Basically the same as 20 years ago.
- All existing E2E schemes can be described by this architecture.

Where might be the problem?



- Existing E2E schemes require trustworthy Tallying Authorities.
- Our hypothesis: the TAs are a significant hurdle in deployment

Case study: Helios-based UCL election

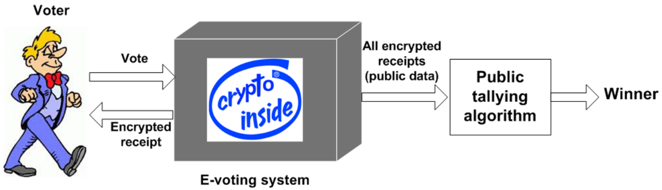
- Helios was used to elect the president of UCL in 2009.
- Tallying authorities presented "one particularly difficult issue".
  - Authorities were selected from university students/staff.
  - But they knew little about crypto.
  - They didn't know how to generate private keys.
  - They didn't know how to distribute private keys.
  - They didn't know how to store private keys.
  - They didn't know how to create backup of private keys.
- Practical solutions
  - Another group of "experts" did most of the actual work.
  - Authorities were given the USB sticks with private keys.
  - Meanwhile, all keys were backed up by a trusted third party.

A motivating question for research

- Helios (and other E2E) requires a TA-based infrastructure
- Setting up such an infrastructure is a significant overhead

Is this overhead always necessary?

A new approach: self-enforcing electronic voting



- At first glance, it may look impossible: performing decryption without any decryption key
- However, it is actually possible.
- The basic intuition: canceling out random factors.

A concrete protocol: DRE-i

- Direct Recording Electronic with Integrity (DRE-i)
- In this talk, we will focus on a local DRE-based election.

1. Setup phase
    - Pre-compute electronic ballots
2. Voting phase
    - Vote intuitively without needing to understand crypto at all
3. Tallying phase
    - Universal verification on tally without involving any authority

Phase 1: Setup (single-candidate example)

Ballot no i	rand pub	"No" Cryptogram	"Yes" cryptogram
1	g^{x_1}	$g^{x_1 y_1}$, 1-out-of-2 ZKP	$g^{x_1 y_1} \cdot g$, 1-out-of-2 ZKP
2	g^{x_2}	$g^{x_2 y_2}$, 1-out-of-2 ZKP	$g^{x_2 y_2} \cdot g$, 1-out-of-2 ZKP
...		...	...
n	g^{x_n}	$g^{x_n y_n}$, 1-out-of-2 ZKP	$g^{x_n y_n} \cdot g$, 1-out-of-2 ZKP

$g^{y_i} = \prod_{j<i} g^{x_j} / \prod_{j>i} g^{x_j}$ (see Hao, Zielinski, SPW'06)

1. Well-formedness: Any single cryptogram is either "No" or "Yes".
2. Concealing: A single cryptogram doesn't reveal "No" or "Yes"
3. Revealing: A pair of cryptograms reveal "No"/"Yes".
4. Self-tallying: Any arbitrary selection of a cryptogram from each of the N ballots, one can easily compute how many "Yes" votes.

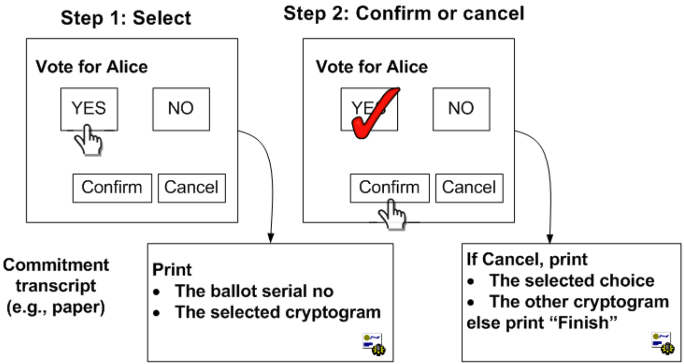
Cancellation formula - an example

Example

Assume $N = 4$.

$$\begin{aligned}\sum_i x_i y_i = & \qquad\qquad\quad - x_1x_2 - x_1x_3 - x_1x_4 \\ & + x_2x_1 \qquad\quad - x_2x_3 - x_2x_4 \\ & + x_3x_1 + x_3x_2 \qquad\quad - x_3x_4 \\ & + x_4x_1 + x_4x_2 + x_4x_3 \qquad\qquad = 0.\end{aligned}$$

Phase 2: Voting



- Receipt is coercion-free: because of the concealing property.
- Ballot casting assurance: due to the revealing property.

Phase 3: Tallying

Ballot no i	g^{x_i}	g^{y_i}	**Published vote** V_i	**ZKPs**
1	g^{x_1}	g^{y_1}	Valid: $g^{x_1 y_1}$	a 1-out-of-2 ZKP
2	g^{x_2}	g^{y_2}	Valid: $g^{x_2 y_2} \cdot g$	a 1-out-of-2 ZKP
...	...	...	...	...
n	g^{x_n}	g^{y_n}	Dummy: $g^{x_n y_n}$, $g^{x_n y_n} \cdot g$	Two 1-out-of-2 ZKP

- Anyone is able to compute $\prod V_i = g^{\sum x_i y_i} \cdot g^{v_i} = g^{\sum v_i}$
- Note that $\sum x_i y_i = 0$ (cancellation formula)

What if some ballots are missing? – A fail-safe mechanism

- Say a small subset L of ballots are found missing
- One trivial solution
  - Re-publish $g^{x_i y_i}$ for $i \in L$
  - But this harms secrecy of individual ballots - leaks too much
- A better solution
  - Publish $A = \prod_{i \in L} g^{x_i y_i}$ (with ZKPs to prove A is well-formed)
  - Minimum leakage: only the partial tally of missing ballots (assuming the attacker has the receipts of all missing ballots).

Comparison between DRE-i with related work

	Blackbox DRE	DRE-i	Previous E2E
TA involvement	No	**No**	Yes
Ballot casting assurance	No	**Yes**	Yes
Transmission integrity	No	**Yes**	Yes
Tallying Integrity	No	**Yes**	Yes
Ballot secrecy	UI	**UI, setup**	UI, setup, TA
Voter privacy	Anonymity	**Anonymity**	Anonymity
Receipt	No	**Yes**	Yes
Crypto-awareness of voter	No	**No**	Yes
Crypto-awareness of auditor	N/A (impossible)	**No**	Yes
Crypto-awareness of verifier	N/A (impossible)	**Yes**	Yes

Previous local DRE-based E2E schemes: Chaum (2004), Adida and Neff (2006)

Comparison between DRE-i with related work

	Blackbox DRE	DRE-i	Previous E2E
TA involvement	No	**No**	Yes
Ballot casting assurance	No	**Yes**	Yes
Transmission integrity	No	**Yes**	Yes
Tallying Integrity	No	**Yes**	Yes
Ballot secrecy	UI	**UI, setup**	UI, setup, TA
Voter privacy	Anonymity	**Anonymity**	Anonymity
Receipt	No	**Yes**	Yes
Crypto-awareness of voter	No	**No**	Yes
Crypto-awareness of auditor	N/A (impossible)	**No**	Yes
Crypto-awareness of verifier	N/A (impossible)	**Yes**	Yes

Previous local DRE-based E2E schemes: Chaum (2004), Adida and Neff (2006)

Comparison between DRE-i with related work

	Blackbox DRE	DRE-i	Previous E2E
TA involvement	No	**No**	Yes
Ballot casting assurance	No	**Yes**	Yes
Transmission integrity	No	**Yes**	Yes
Tallying Integrity	No	**Yes**	Yes
Ballot secrecy	UI	**UI, setup**	UI, setup, TA
Voter privacy	Anonymity	**Anonymity**	Anonymity
Receipt	No	**Yes**	Yes
Crypto-awareness of voter	No	**No**	Yes
Crypto-awareness of auditor	N/A (impossible)	**No**	Yes
Crypto-awareness of verifier	N/A (impossible)	**Yes**	Yes

Previous local DRE-based E2E schemes: Chaum (2004), Adida and Neff (2006)

Comparison between DRE-i with related work

	Blackbox DRE	DRE-i	Previous E2E
TA involvement	No	**No**	Yes
Ballot casting assurance	No	**Yes**	Yes
Transmission integrity	No	**Yes**	Yes
Tallying Integrity	No	**Yes**	Yes
Ballot secrecy	UI	**UI, setup**	UI, setup, TA
Voter privacy	Anonymity	**Anonymity**	Anonymity
Receipt	No	**Yes**	Yes
Crypto-awareness of voter	No	**No**	Yes
Crypto-awareness of auditor	N/A (impossible)	**No**	Yes
Crypto-awareness of verifier	N/A (impossible)	**Yes**	Yes

Previous local DRE-based E2E schemes: Chaum (2004), Adida and Neff (2006)

Comparison between DRE-i with related work

	Blackbox DRE	DRE-i	Previous E2E
TA involvement	No	**No**	Yes
Ballot casting assurance	No	**Yes**	Yes
Transmission integrity	No	**Yes**	Yes
Tallying Integrity	No	**Yes**	Yes
Ballot secrecy	UI	**UI, setup**	UI, setup, TA
Voter privacy	Anonymity	**Anonymity**	Anonymity
Receipt	No	**Yes**	Yes
Crypto-awareness of voter	No	**No**	Yes
Crypto-awareness of auditor	N/A (impossible)	**No**	Yes
Crypto-awareness of verifier	N/A (impossible)	**Yes**	Yes

Previous local DRE-based E2E schemes: Chaum (2004), Adida and Neff (2006)

Comparison between DRE-i with related work

	Blackbox DRE	DRE-i	Previous E2E
TA involvement	No	**No**	Yes
Ballot casting assurance	No	**Yes**	Yes
Transmission integrity	No	**Yes**	Yes
Tallying Integrity	No	**Yes**	Yes
Ballot secrecy	UI	**UI, setup**	UI, setup, TA
Voter privacy	Anonymity	**Anonymity**	Anonymity
Receipt	No	**Yes**	Yes
Crypto-awareness of voter	No	**No**	Yes
Crypto-awareness of auditor	N/A (impossible)	**No**	Yes
Crypto-awareness of verifier	N/A (impossible)	**Yes**	Yes

Previous local DRE-based E2E schemes: Chaum (2004), Adida and Neff (2006)

Comparison between DRE-i with related work

	Blackbox DRE	DRE-i	Previous E2E
TA involvement	No	**No**	Yes
Ballot casting assurance	No	**Yes**	Yes
Transmission integrity	No	**Yes**	Yes
Tallying Integrity	No	**Yes**	Yes
Ballot secrecy	UI	**UI, setup**	UI, setup, TA
Voter privacy	Anonymity	**Anonymity**	Anonymity
Receipt	No	**Yes**	Yes
Crypto-awareness of voter	No	**No**	Yes
Crypto-awareness of auditor	N/A (impossible)	**No**	Yes
Crypto-awareness of verifier	N/A (impossible)	**Yes**	Yes

Previous local DRE-based E2E schemes: Chaum (2004), Adida and Neff (2006)

Comparison between DRE-i with related work

	Blackbox DRE	DRE-i	Previous E2E
TA involvement	No	**No**	Yes
Ballot casting assurance	No	**Yes**	Yes
Transmission integrity	No	**Yes**	Yes
Tallying Integrity	No	**Yes**	Yes
Ballot secrecy	UI	**UI, setup**	UI, setup, TA
Voter privacy	Anonymity	**Anonymity**	Anonymity
Receipt	No	**Yes**	Yes
Crypto-awareness of voter	No	**No**	Yes
Crypto-awareness of auditor	N/A (impossible)	**No**	Yes
Crypto-awareness of verifier	N/A (impossible)	**Yes**	Yes

Previous local DRE-based E2E schemes: Chaum (2004), Adida and Neff (2006)

Comparison between DRE-i with related work

	Blackbox DRE	DRE-i	Previous E2E
TA involvement	No	**No**	Yes
Ballot casting assurance	No	**Yes**	Yes
Transmission integrity	No	**Yes**	Yes
Tallying Integrity	No	**Yes**	Yes
Ballot secrecy	UI	**UI, setup**	UI, setup, TA
Voter privacy	Anonymity	**Anonymity**	Anonymity
Receipt	No	**Yes**	Yes
Crypto-awareness of voter	No	**No**	Yes
Crypto-awareness of auditor	N/A (impossible)	**No**	Yes
Crypto-awareness of verifier	N/A (impossible)	**Yes**	Yes

Previous local DRE-based E2E schemes: Chaum (2004), Adida and Neff (2006)

Comparison between DRE-i with related work

	Blackbox DRE	DRE-i	Previous E2E
TA involvement	No	**No**	Yes
Ballot casting assurance	No	**Yes**	Yes
Transmission integrity	No	**Yes**	Yes
Tallying Integrity	No	**Yes**	Yes
Ballot secrecy	UI	**UI, setup**	UI, setup, TA
Voter privacy	Anonymity	**Anonymity**	Anonymity
Receipt	No	**Yes**	Yes
Crypto-awareness of voter	No	**No**	Yes
Crypto-awareness of auditor	N/A (impossible)	**No**	Yes
Crypto-awareness of verifier	N/A (impossible)	**Yes**	Yes

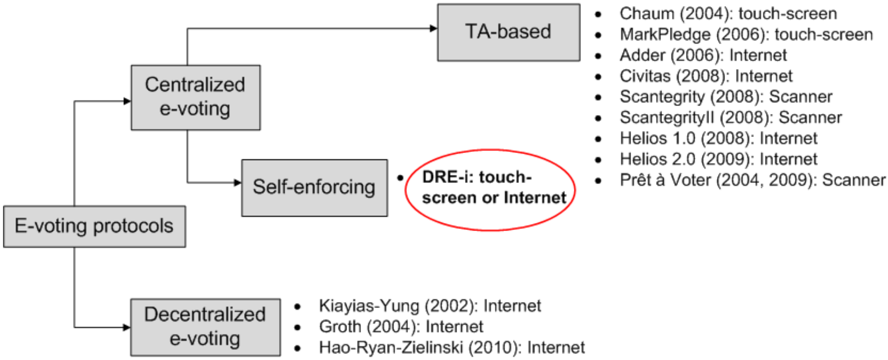
Previous local DRE-based E2E schemes: Chaum (2004), Adida and Neff (2006)

Comparison between DRE-i with related work

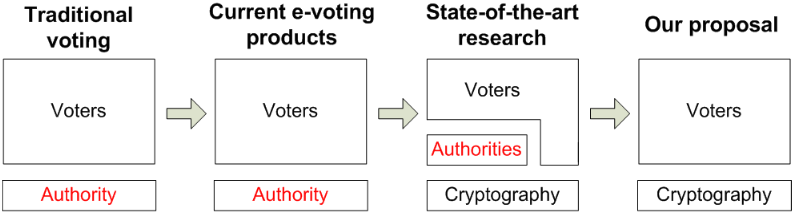
	Blackbox DRE	DRE-i	Previous E2E
TA involvement	No	**No**	Yes
Ballot casting assurance	No	**Yes**	Yes
Transmission integrity	No	**Yes**	Yes
Tallying Integrity	No	**Yes**	Yes
Ballot secrecy	UI	**UI, setup**	UI, setup, TA
Voter privacy	Anonymity	**Anonymity**	Anonymity
Receipt	No	**Yes**	Yes
Crypto-awareness of voter	No	**No**	Yes
Crypto-awareness of auditor	N/A (impossible)	**No**	Yes
Crypto-awareness of verifier	N/A (impossible)	**Yes**	Yes

Previous local DRE-based E2E schemes: Chaum (2004), Adida and Neff (2006)

Categorization of e-voting systems



Summary



- Existing E2E all require a TA-based infrastructure
- We show such an infrastructure is not always necessary
- We present a DRE-i protocol for for local DRE-based elections
- Future work: self-enforcing e-voting for STV and others

Q & A

Thank you!