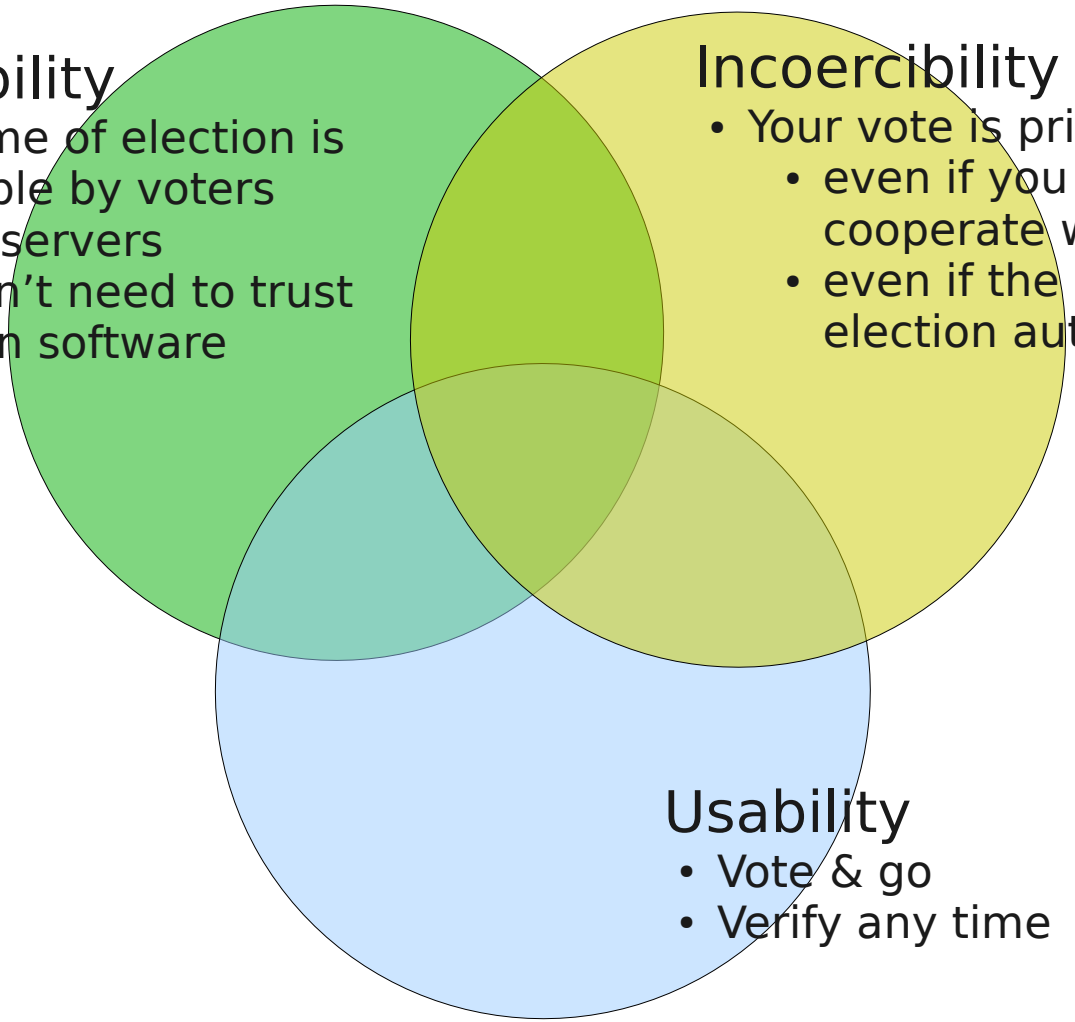
Corruption evidence in electronic voting

(work in progress)

Sergiu Bursuc / Gurchetan S. Grewal /
Mark D. Ryan / Peter Y. A. Ryan

SecVote 2012, Dagstuhl
17 July 2012

Desired properties for internet voting



Verifiability

- Outcome of election is verifiable by voters and observers
- You don’t need to trust election software

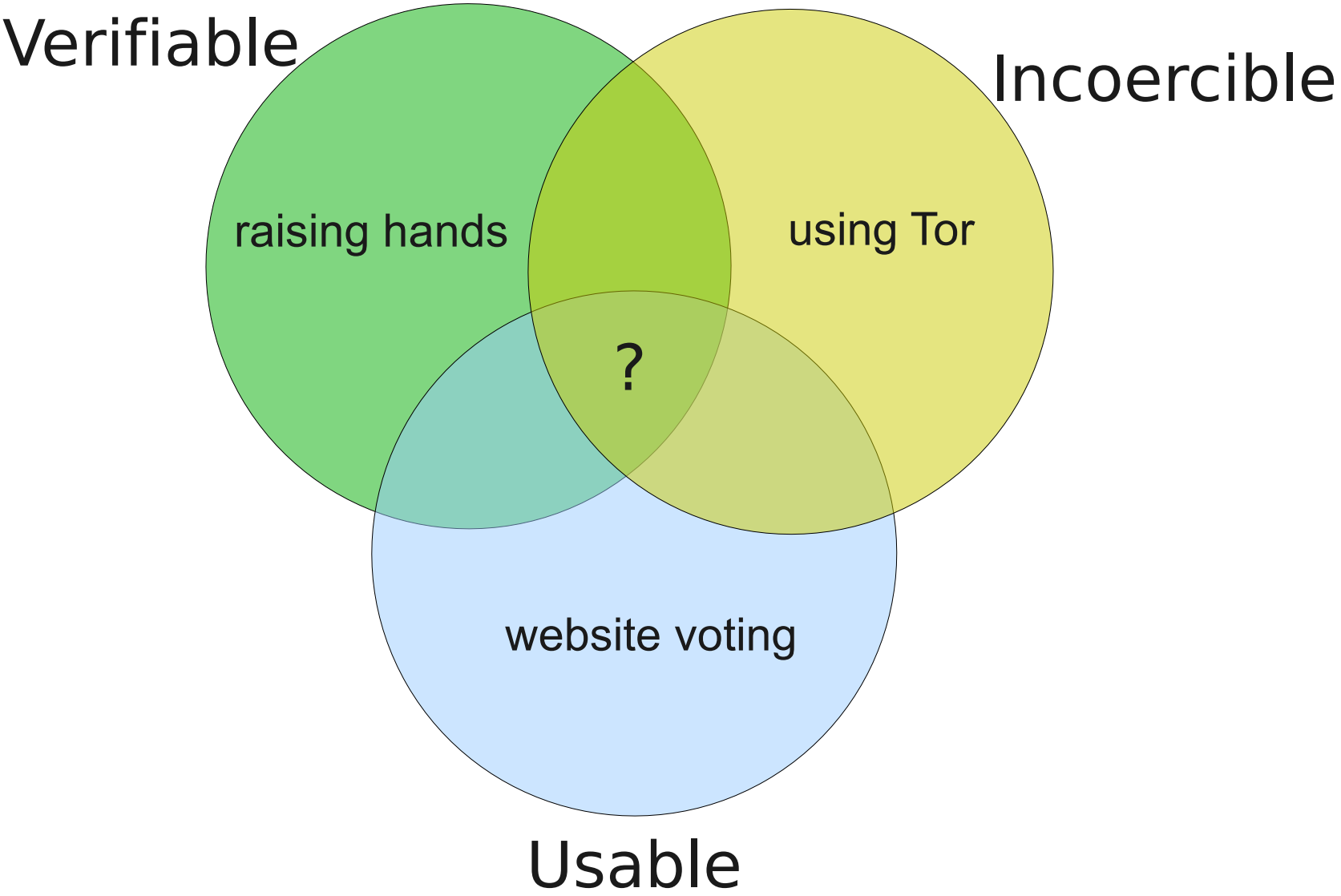
Incoercibility

- Your vote is private
  - even if you try to cooperate with a coercer
  - even if the coercer is the election authorities

Usability

- Vote & go
- Verify any time

Examples


Verifiable
Incoercible
raising hands
using Tor
?
website voting
Usable

- Can you have all three properties?
  - It depends on the *trust assumptions*.
  - Probably cannot have all three under reasonable assumptions.

- Which one do you want to give up (or weaken)?

Resistance or evidence?

What we want:

- Primary aim: revisit "coercion resistance"
- Also: increase usability, and improve trust assumptions

Method:

- New concepts: corruption

Resistance or evidence?

What we want:

- Primary aim: revisit "coercion resistance"
- Also: increase usability, and improve trust assumptions

Method:

- New concepts: corruption, and corruption evidence

Resistance or evidence?

What we want:

- Primary aim: revisit "coercion resistance"
- Also: increase usability, and improve trust assumptions

Method:

- New concepts: corruption, and corruption evidence
- Verifiability: IV + UV + EV + CV

Resistance or evidence?

What we want:

- Primary aim: revisit "coercion resistance"
- Also: increase usability, and improve trust assumptions

Method:

- New concepts: corruption, and corruption evidence
- Verifiability: IV + UV + EV + CV
- Incoercibilty: replace with coercer-independence

Allows "best effort" security instead of "military" security

Corruption

Corruption occurs whenever:

- coercion occurs, e.g., someone forces you or bribes you to reveal your credential;
- someone puts malware on your computer to alter your ballot, or to divulge your vote or your credential;
- someone intercepts your credentials, e.g. from the post.

Corruption generalises coercion.

Corruption evidence

An election system is *corruption-evident* if

- there exists a *test ce* that can be performed on the bulletin board such that, for any execution τ,

$$m - d \leq ce(bb(\tau)) \leq m + d$$

where m is the number of corrupted voters and d is the number of dishonest voters.

To achieve c.e., voters must be able to act undetectably by coercer *(coercer independence)*.
E.g., must be able to submit a ballot undetectably.

Caveat Corruptor

Caveat Corruptor

- intended for Internet voting
- uses best effort privacy
- borrows ideas liberally, but especially from [JCJ/Civitas]

Caveat Corruptor: what the voter does

1. Voter obtains her credentials, e.g., by post.
2. Voter chooses platform on which to construct her ballot.
   - smartphone applet
   - standalone bootable program (memtest86-like)
   - app for favourite OS, downloaded from source of choice
   - browser applet from source of choice
   - HTTPS connection to server of choice
3. Voter submits her ballot to the collector.
4. Voter repeats 1-3 as many times as she wants, for the same candidate; at most one of them will be counted. If she votes for multiple candidates, it will be marked as corruption.

Observation:

- Voter can use multiple devices to cast multiple votes. If there exists one device which is *integrity-honest* (she doesn't need to know which)
  - either the vote will be counted for the preferred candidate
  - or corruption will be recorded.

Ballot formation applet for novices

UK Parliamentary Election 2014

Birmingham, Selly Oak constituency

- ☐ Stephen McCabe (Labour)
- ☐ Nigel Dawkins (Conservative)
- ☐ Dave Radcliffe (Liberal Democrat)
- ☐ Lynette Orton (BNP)
- ☐ Jeffrey Burgess (UKIP
- ☐ James Burn (Green)
- ☐ Samuel Leeds (Christi

Voter's credential:

Calculate Ballot

Your encrypted ballot:

Qa3+MXgqTE2FkHWK14n5QFGbjucvTeeFlNApnbGdGnNqsfVAvgi/Etu+B78hCuB

94MAVQRi+LDo5ckcAUX2pMDCAJJ/kOvPeBNaDTdmtFPjFoXwq5n2U7JCdCqS/1s

qlIRFxsu3SwB+IRuejSyALEqtlnIIxzCxqtXEvqX0s6zt8sez1/uApn/eFEG9/8

GgkiFwe7Xo1WKYxTwdMa5HMTS4lL0Jq1mzua77DRIA4FpBsU+EhO6npYqcKvtbv

5uaIY+2foPPKq7Flk3iE2CtNhPJ6QI61Ku2KjSJ6mnyhTbyEB70jpOacSEfzGlV

0H9StCN2OnsHAC0uCd/OyDrNHuA==

You should paste this value to the website at election2014.gov.uk.

Ballot formation applet for experts

Caveat Corruptor ballot-forming applet

pk_R

pk_T

Voter's credential

$rand_R$

$rand_T$

Vote

Calculate Ballot

Your encrypted ballot:

Qa3+MXgqTE2FkHWK14n5QFGbjucvTeeFlNApnbGdGnNqsfVAvgi/Etu+B78hCuB

94MAVQRi+LDo5ckcAUX2pMDCAJJ/kOvPeBNaDTdmtFPjFoXwq5n2U7JCdCqS/1s

qlIRFxsu3SwB+IRuejSyALEqtlnIIxzCxqtXEvqX0s6zt8sez1/uApn/eFEG9/8

GgkiFwe7Xo1WKYxTwdMa5HMTS4lL0Jq1mzua77DRIA4FpBsU+EhO6npYqcKvtbv

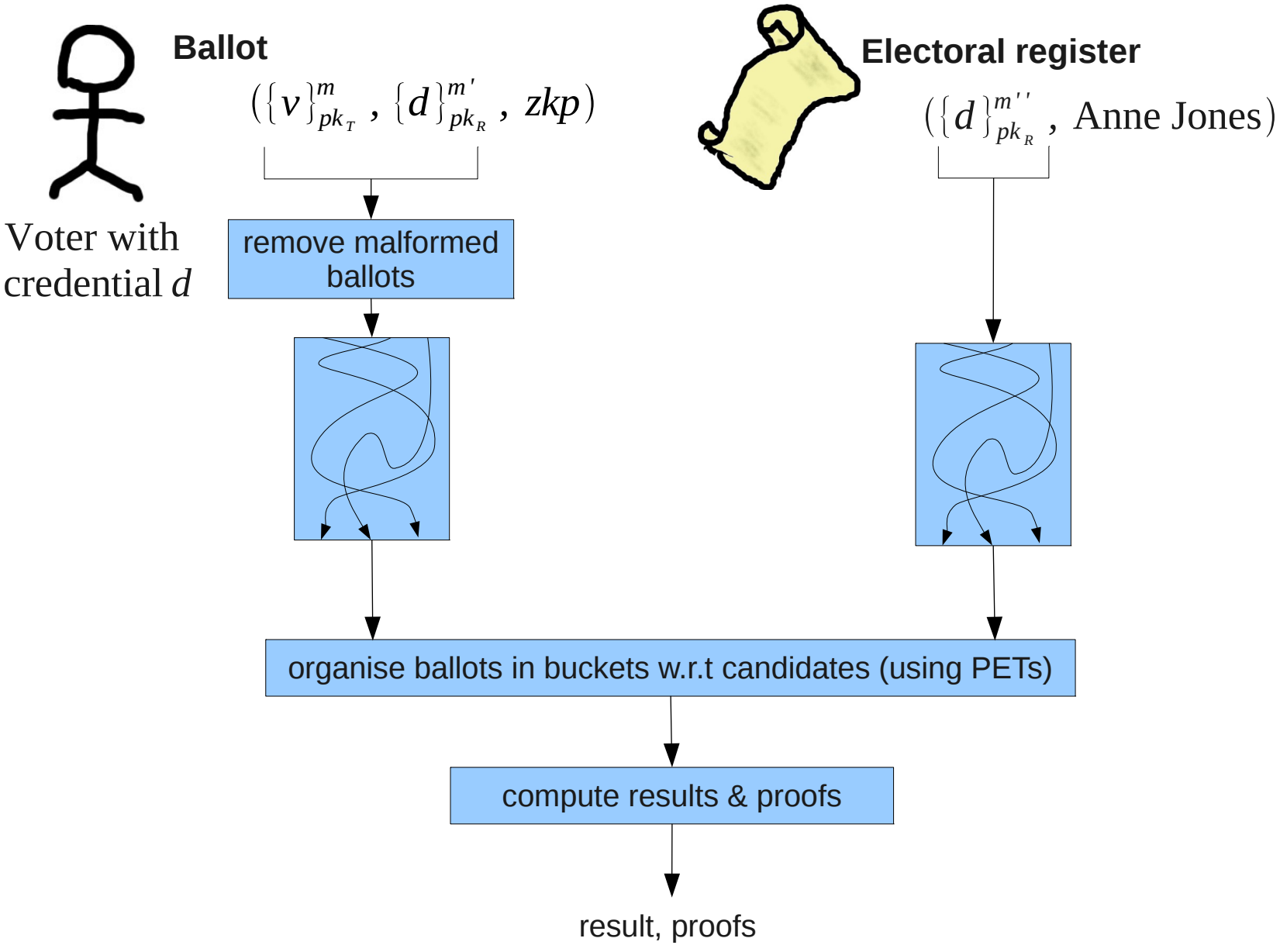
5uaIY+2foPPKq7Flk3iE2CtNhPJ6QI61Ku2KjSJ6mnyhTbyEB70jpOacSEfzGlV

0H9StCN2OnsHAC0uCd/OyDrNHuA==

$rand_R$ pSGkxaQRxypkzL08kFo9og==

$rand_T$ lwf+YABhpvHgcS4KpJYhxg==

Caveat Corruptor (based on JCJ-Civitas)

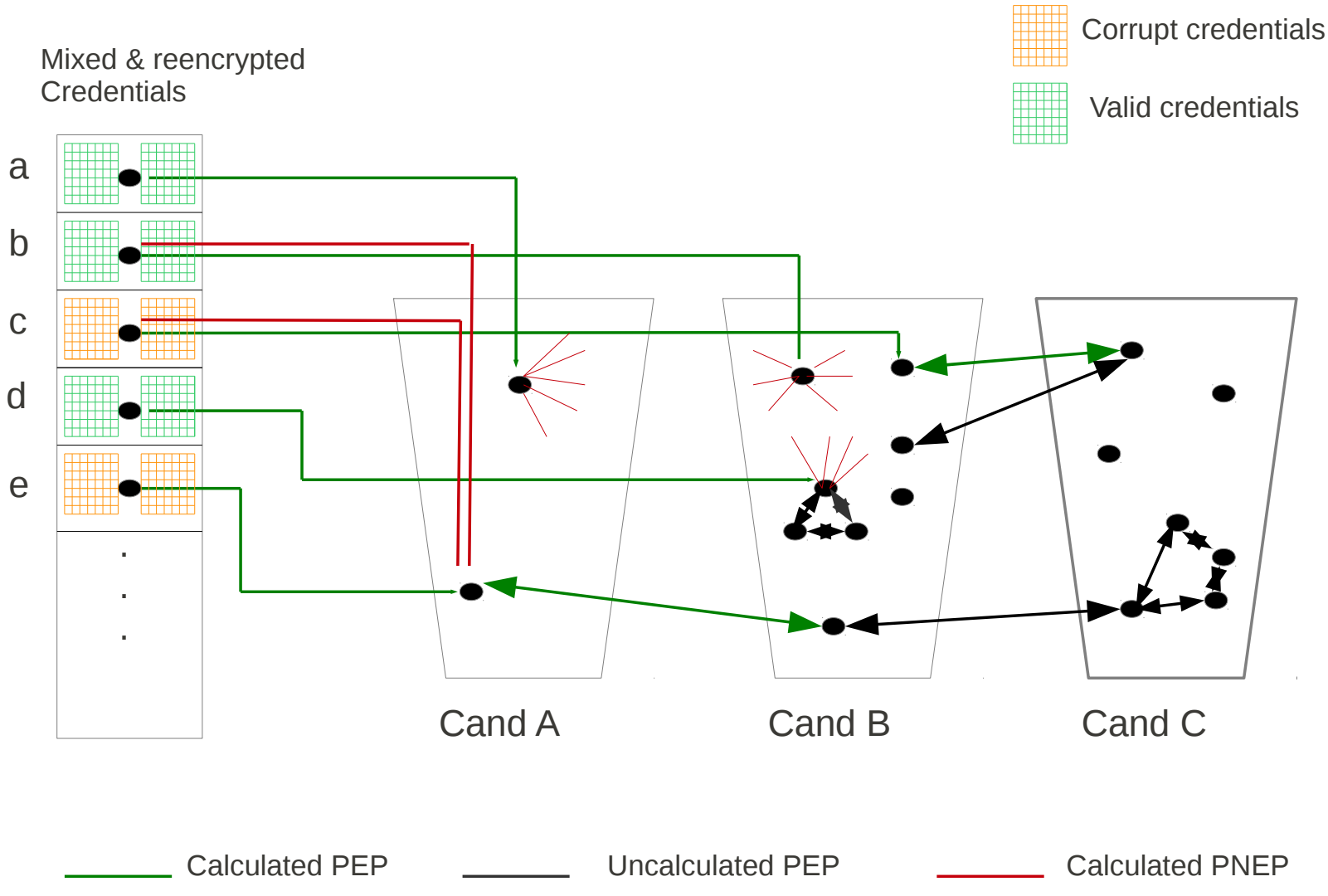


Caveat Corruptor: what the system does

A ballot has the form $\left(\{v\}^{m}_{pk_T}, \{d\}^{M'}_{pk_R}, zkp\right)$, where $\{\cdot\}^{\cdot}_{\cdot}$ is randomised encryption that supports re-encryption, plaintex equivalence testing, and verifiable threshold decryption.
On receipt of the ballots, the system:

- verifiably-re-encryption-mixes the ballots
- uses PETs to group ballots into buckets corresp. to cand.
- uses PETs to determine if any creds. are present in two diff. buckets
- mark all the credentials corrupt if present in different buckets, count them once if just present in one bucket.
- uses PETs to discard ballots not corresponding to a credential on the published electoral roll
- verifiably-decrypts the votes in the ballots to be counted

All of these computations can be verified by any observer or voter.


Corrupt credentials
Valid credentials
Mixed & reencrypted
Credentials
a
b
c
d
e
Cand A
Cand B
Cand C
Calculated PEP
Uncalculated PEP
Calculated PNEP

Announcement of Results

For the 48,783,530 (100%) eligible credentials:

- In 44,539,363 (91.3%) cases, ballots for a single candidate were received, and a representative one ballot per voter will be counted.
- In the remaining 4,244,167 (8.7%) cases, ballots for multiple candidates were received, and these are recorded as corrupted credentials and will not be counted.

The election officials must now recommend whether the results of this election should be carried.

Caveat Corruptor

- An attacker can corrupt a voter:
  - just demands her credential, and votes on her behalf
  - or, persuades her to use a corrupt ballot forming applet
  - or, installs malware on her machine, etc
- But the system will receive multiple ballots for the voter with different votes. They will not be counted, but the fact will be published.
  - The most the coercer can achieve is forced abstention.
  - The degree of corruption (= forced abstention) will be published, and is verifiable.

Possible attacks

Attack	Mitigation
Attacker persuades you to use a corrupt applet that leaks your vote, or submits his preference instead of yours.	Use multiple applets. You can check your ballot on another computer (expert mode).
Attacker steals your credential (unknown to you), or forces you to reveal your credential (known to you).	Vote normally.
Attacker tries to disrupt the election by making it appear as if there were lots of coercion.	Attacker needs to steal or coerce a large number of voters.

Trust assumptions

Trust assumptions

- At least one of the devices available to the voter is *integrity-honest*. The voter is not required to know which one it is.
  - She will achieve this by using multiple devices.
- The voter is capable of preventing the coercer from observing that she cast a ballot.
  - Normally, she will achieve this by making assumptions about the coercer's capabilities.
  - For extremely powerful coercers, she may wish to use the ballot-forming computer inside a Faraday cage, and destroy it afterwards. (In this case, the ballot is copied and pasted by hand.)

Conjecture

Caveat Corruptor satisfies coercion-evidence, with the test

$$ce(bb(\tau)) = |\{c \in \mathsf{Cred} \mid \exists b, b'.\, cred(b) = cred(b') = c, cand(b) \neq cand(b')\}|$$

What if the results look like this?

For the 48,783,530 (100%) eligible credentials:

- In 24,391,765 (50%) cases, ballots for a single candidate were received, and a representative one ballot per voter will be counted.
- In the remaining 24,391,765 (50%) cases, ballots for multiple candidates were received, and these are recorded as corrupted credentials and will not be counted.

This means that there was a general failure of security of the credentials, or there was a lot of protest votes, or people misunderstood how to vote. All of this is important evidence.

Avoiding dishonest voters

Corruption evidence assumes voters are *honest* (i.e. they vote, and for a single candidate):

$$m - d \leq ce(bb(\tau)) \leq m + d$$

where m is the number of corrupted voters, and d the number of dishonest voters.

Voters can be dishonest in two ways:

- Doing nothing; leads to undetected coercion.
  Solution: voting compulsory
- Voting for > 1 distinct candidates, perhaps as a protest: leads to inflated estimate of corruption. Solution?: this form of ptotest is made illegal.

Conclusions

Idea of *corruption evidence*

- Reduce security requirements
  - coercion resistance $\rightsquigarrow$ coercer independence
- Increase usability
  - best-effort security instead of military-grade security

Instantiation with Caveat Corruptor

Current work

- Formal definition of corruption evidence, and evaluation of conditions under which Caveat Corruptor satisfies it
- Other corruption and coercion-evident systems