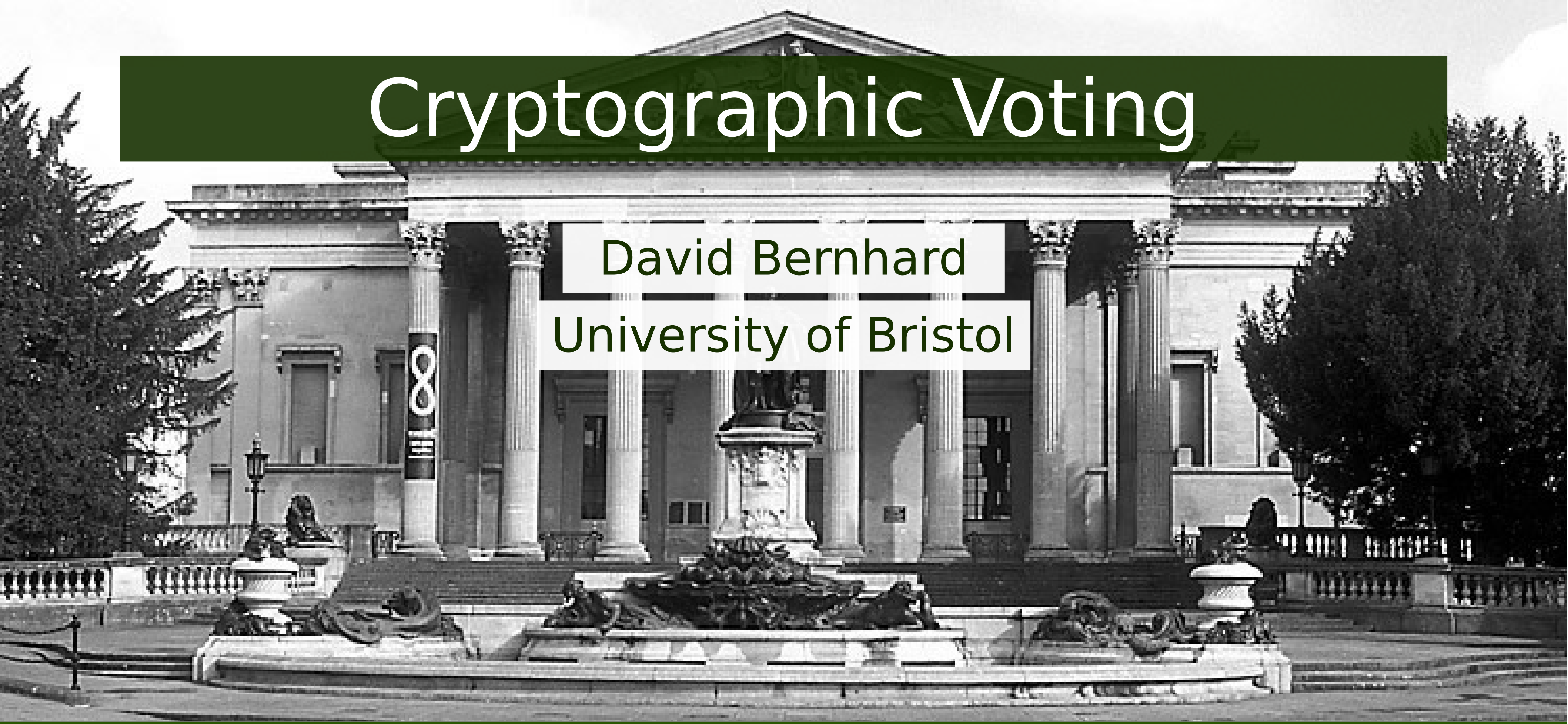


Cryptographic Voting

David Bernhard
University of Bristol

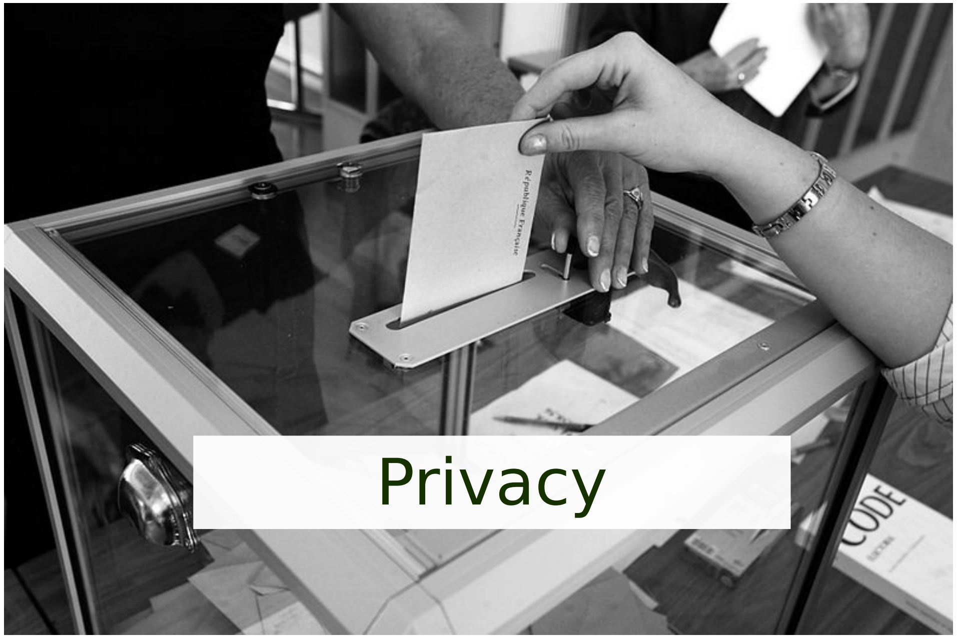
Voting

IAU XXVIth General Assembly
IAU

République Française
CODE

Voting

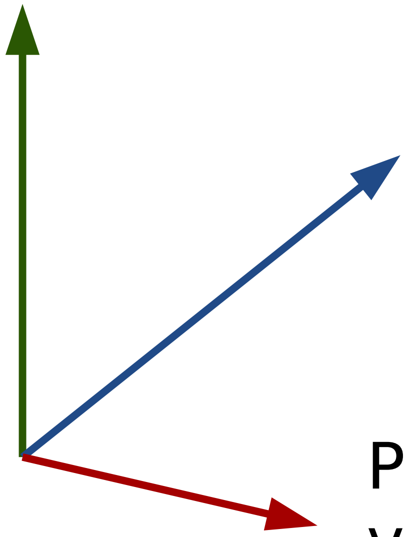
Verifiability



Privacy

Dimensions

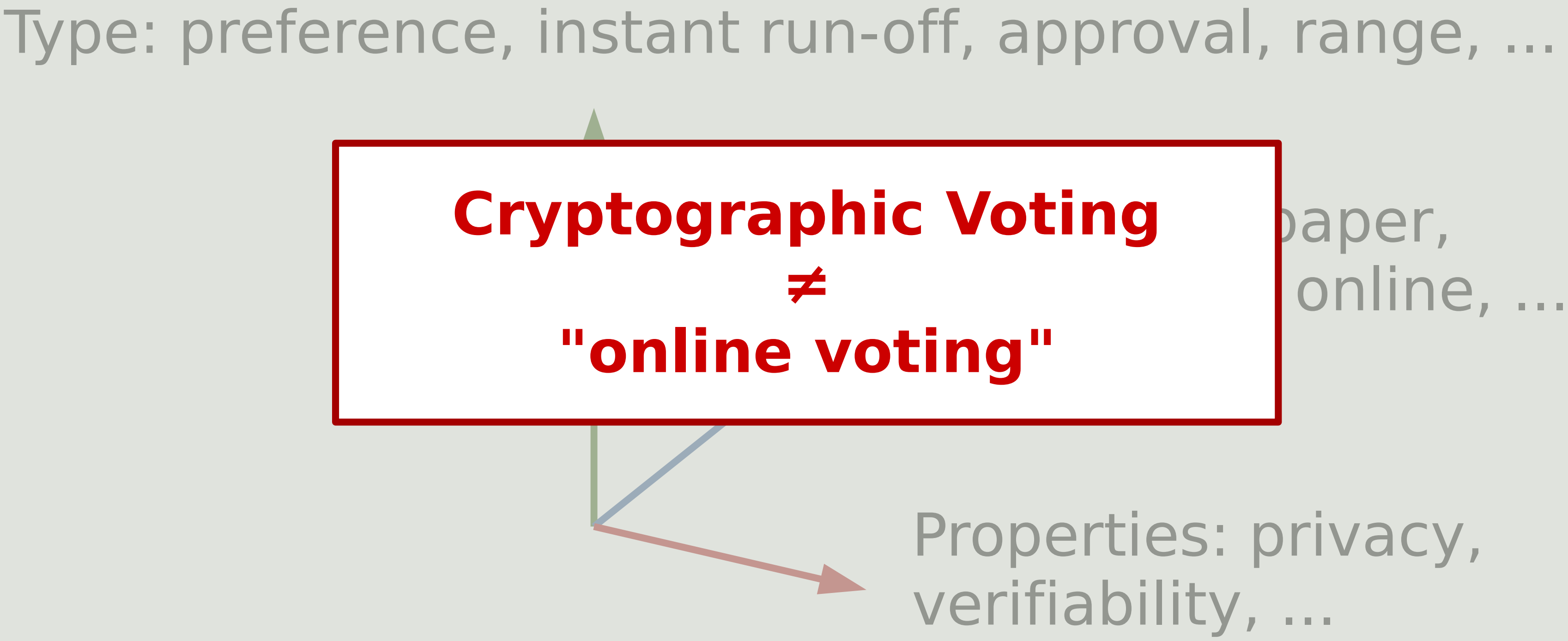
Type: preference, instant run-off, approval, range, ...



System: paper, machine, online, ...

Properties: privacy, verifiability, ...

Dimensions



Type: preference, instant run-off, approval, range, ...

paper,

online, ...

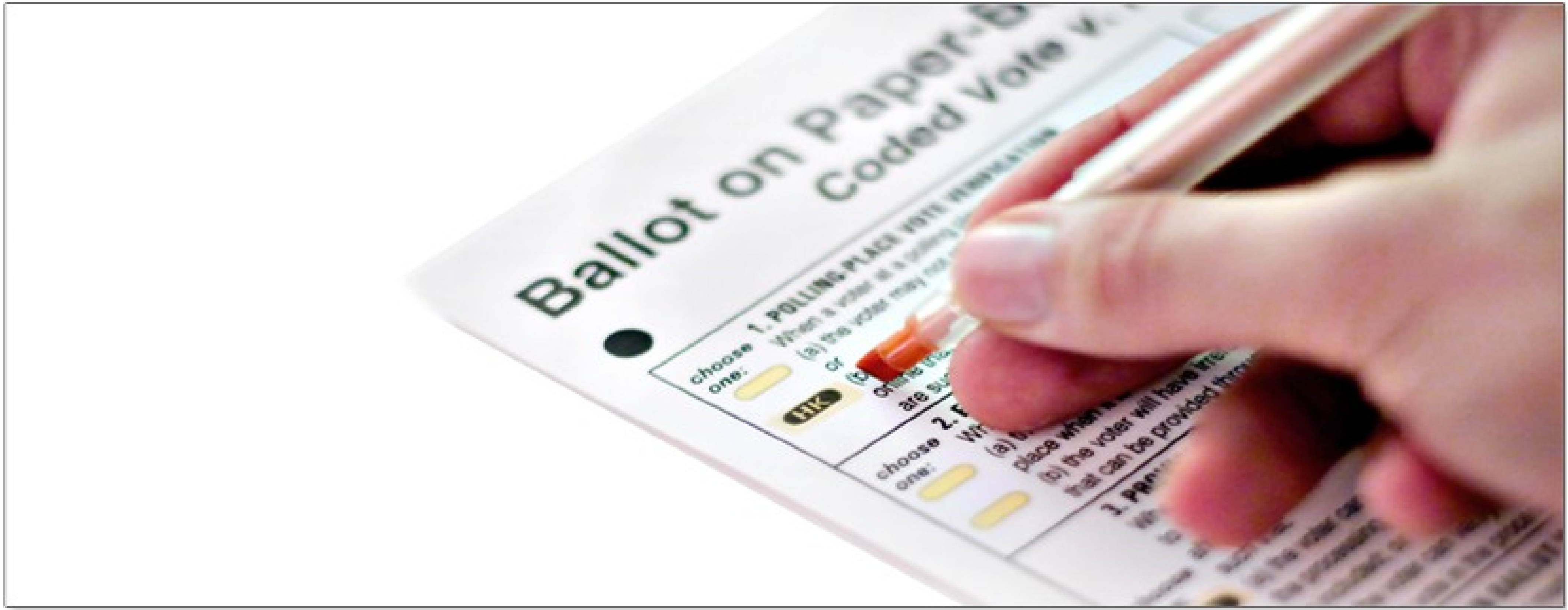
Properties: privacy, verifiability, ...

Cryptographic Voting

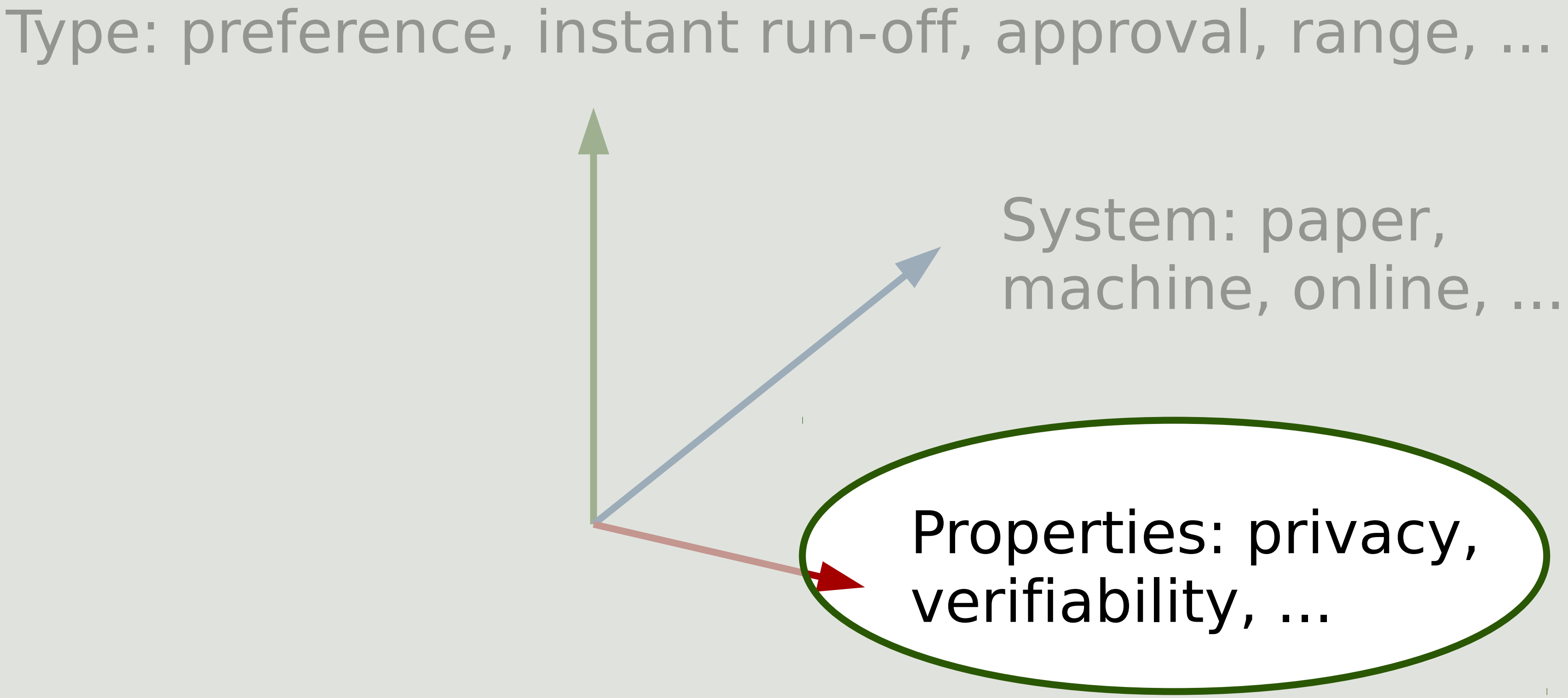
≠

"online voting"

Scantegrity



Dimensions



Type: preference, instant run-off, approval, range, ...

System: paper, machine, online, ...

Properties: privacy, verifiability, ...

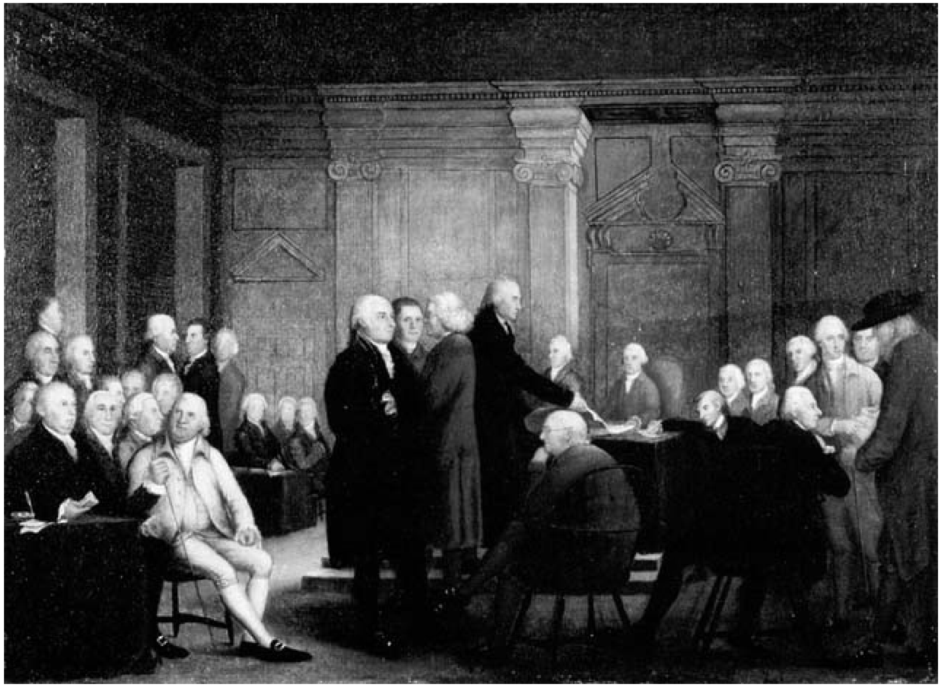
Election Properties (I)

Only eligible voters should be able to vote, and only once each, and only for permitted choices.

The vote cast by each voter should be the one she intended to cast.

The announced result should correspond to the votes actually cast.

Bulletin Boards



John Hancock	YES
John Adams	YES
Benjamin Franklin	YES
John Penn	YES
Thomas Jefferson	YES

Bulletin Boards

Bulletin Board: contains public data posted by voters.

Verifiability

Verifiability: I can observe that an election was tallied correctly.

Systems: Bulletin board, show of hands.

Election Properties (II)

I do not want anyone to know how I voted.

I do want to know how my representatives voted.

Election Properties (II)

I do not want anyone to know how I voted.

I do want to know how my representatives voted.

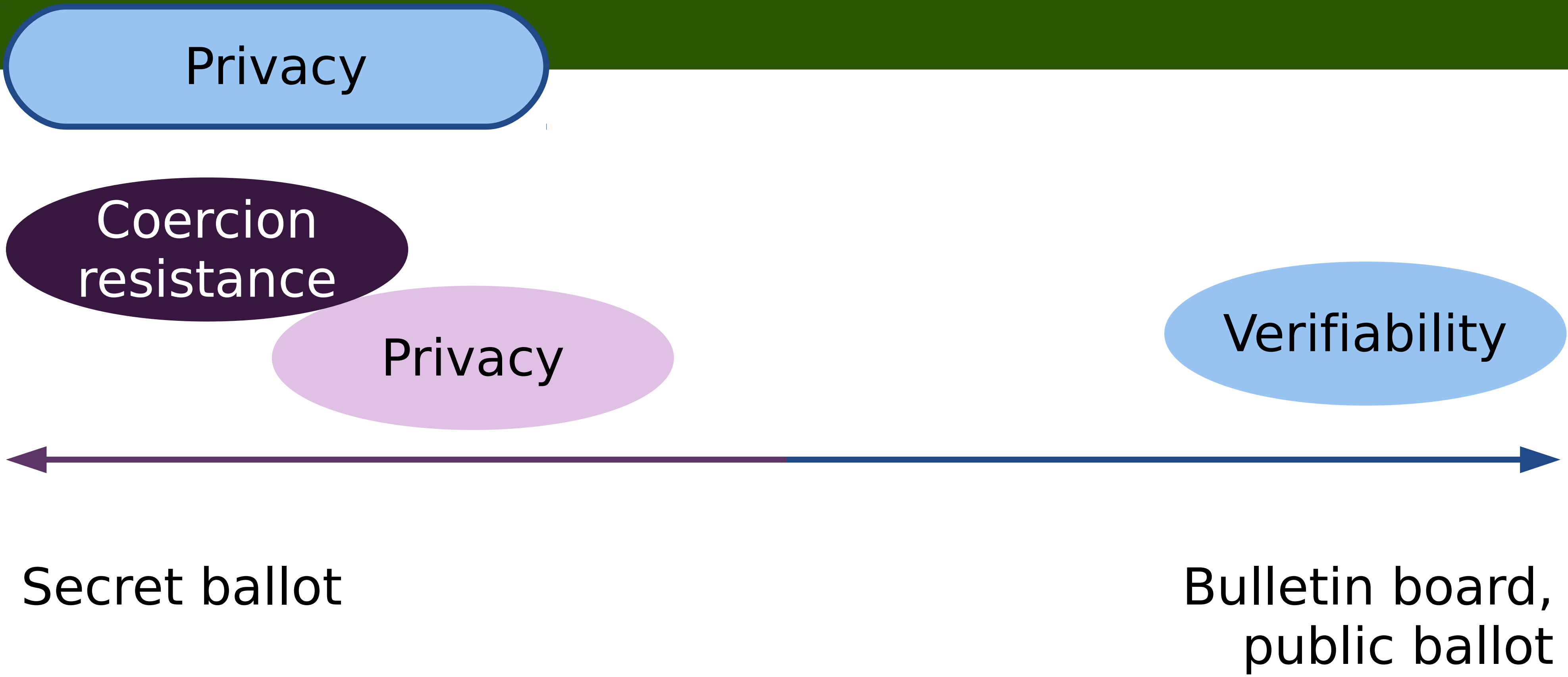
Voters should not be bribed or intimidated into voting a certain way.

Privacy

Privacy (secret ballot): no-one can tell how I voted.

Coercion-resistance: I cannot prove to someone how I voted.

Systems: voting booth, ballot box, ...



Privacy

Coercion resistance

Privacy

Verifiability

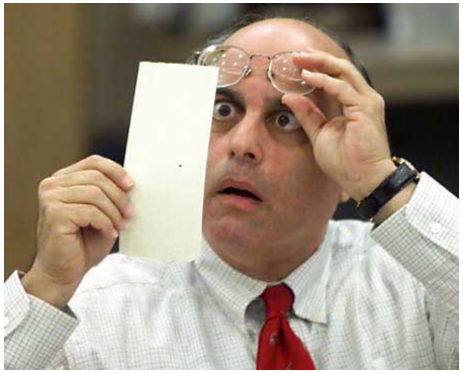
Secret ballot

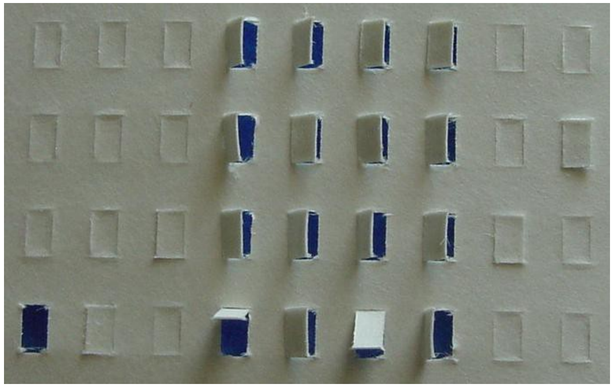
Bulletin board,
public ballot

Trust

Secret ballot: trust election officials?

Trust voting machines?





Ok ... so what is cryptographic voting, then?

Cryptographic Voting

Privacy

+

Verifiability

Cryptographic Voting

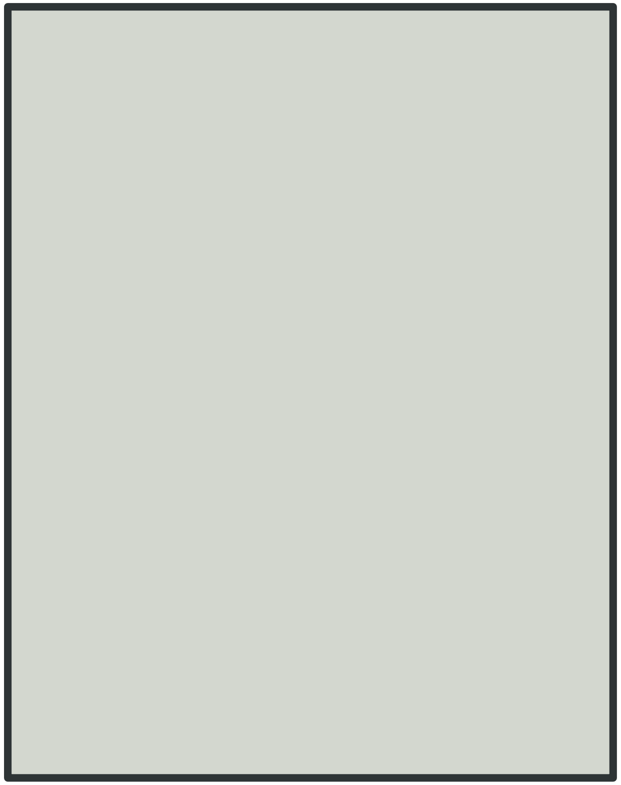
Publicly verifiable secret-ballot elections.

Easier to verify and trust than current "voting machines".

Helios

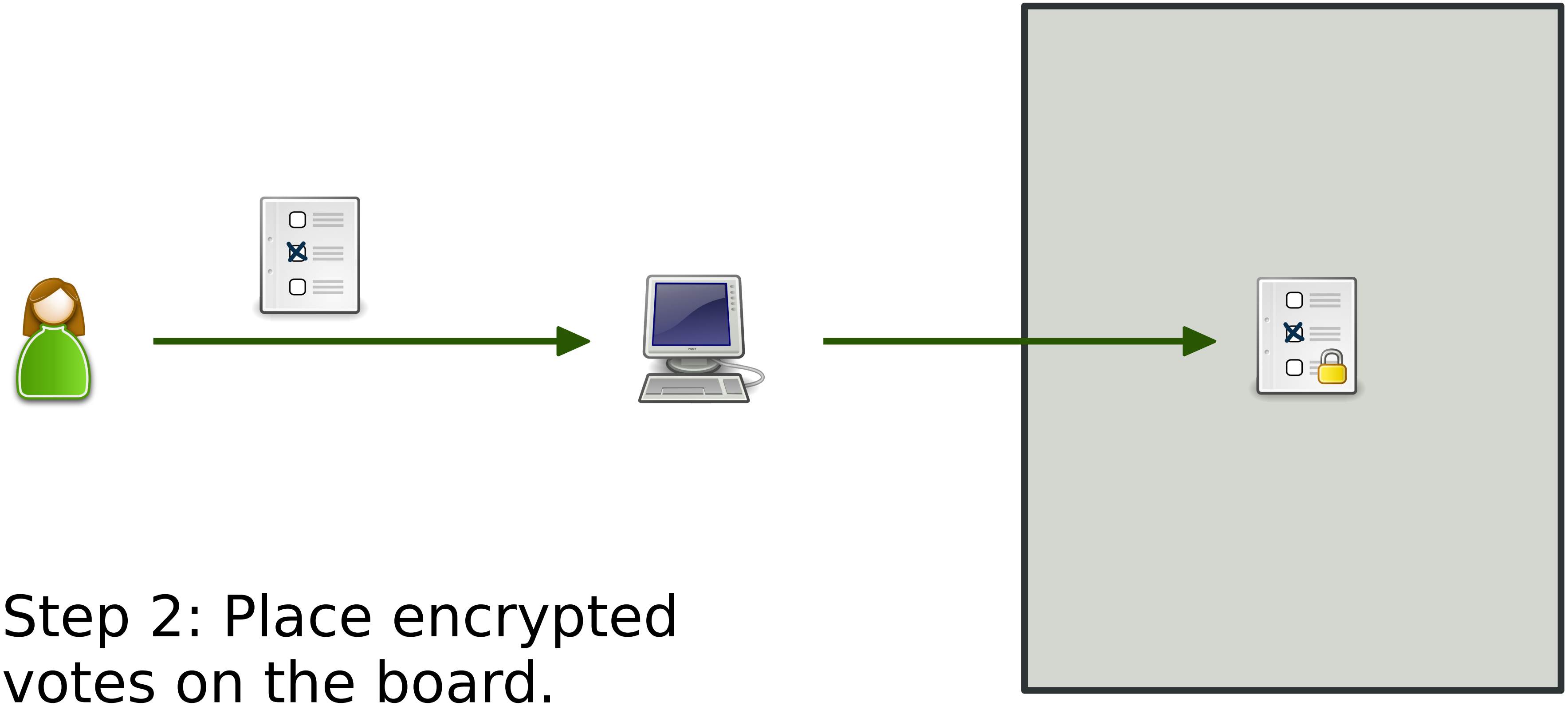
- IACR board
- President of UC Louvain
- Princeton University Student Government

Cryptographic Voting



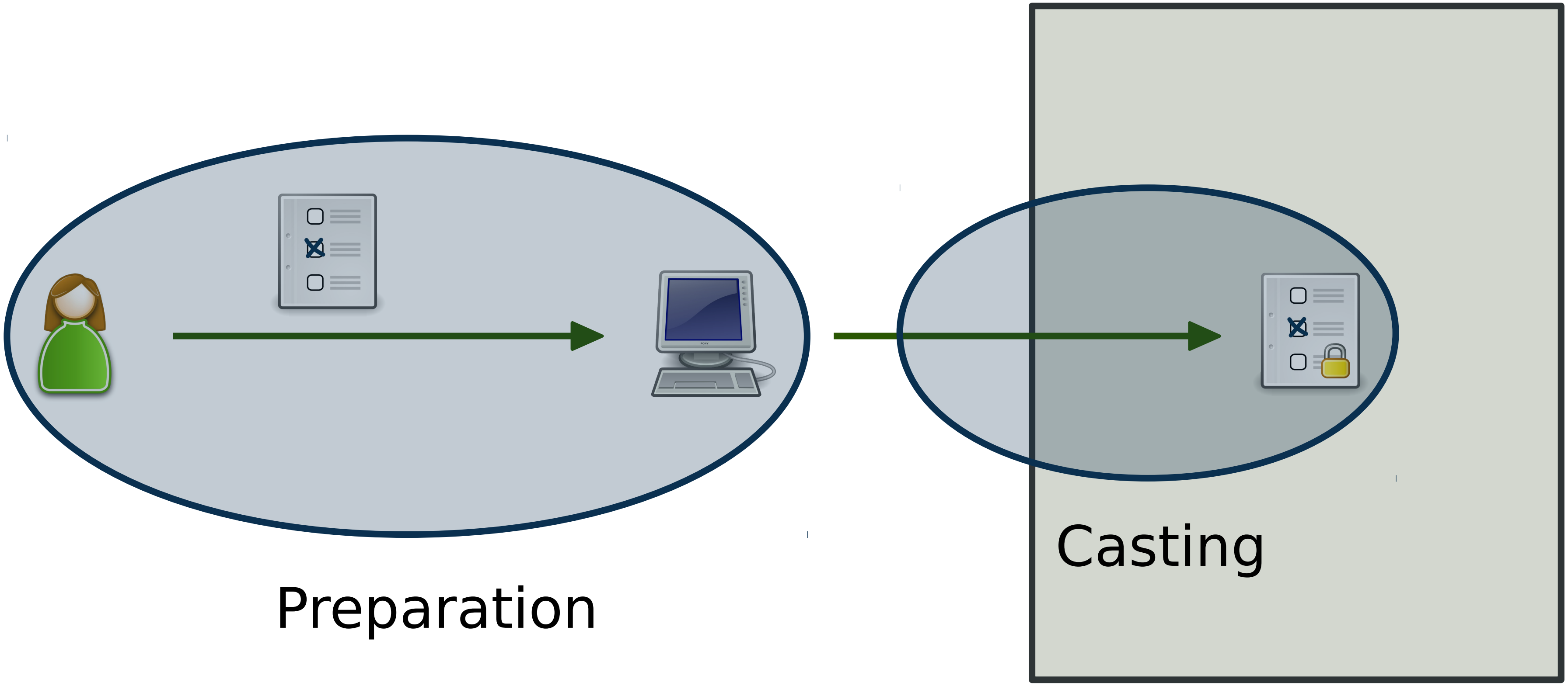
Step 1: Bring back the bulletin board.

Voting



Step 2: Place encrypted votes on the board.

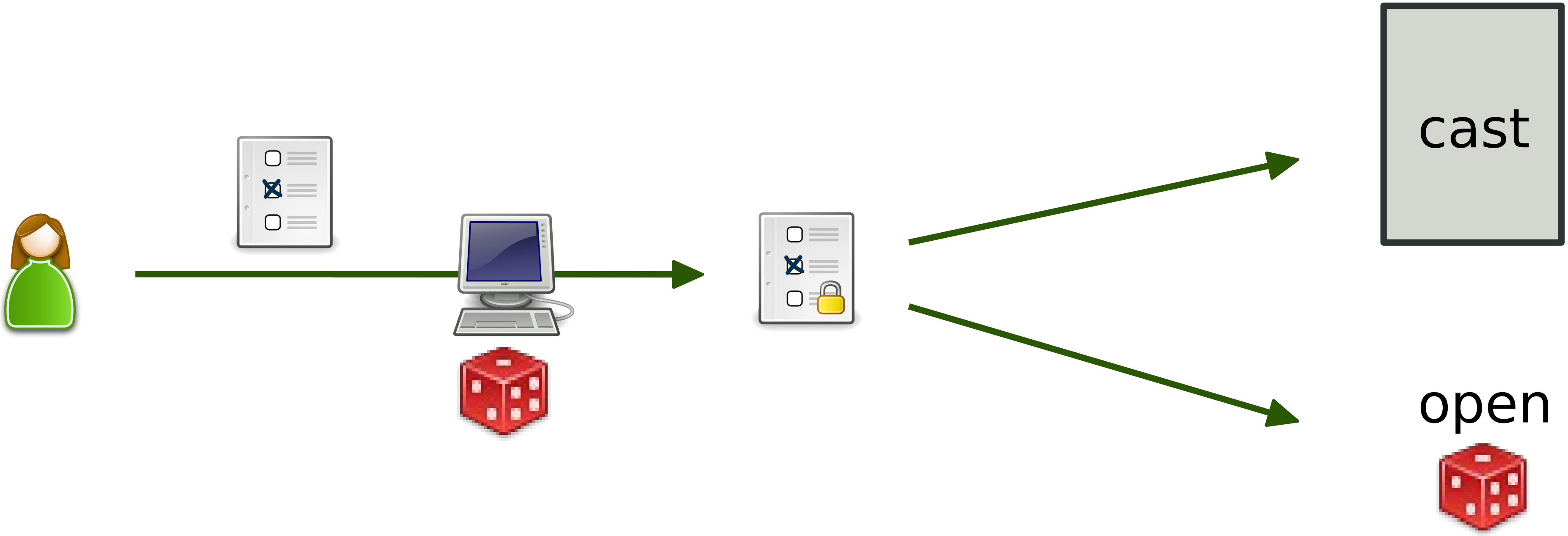
Voting



Preparation

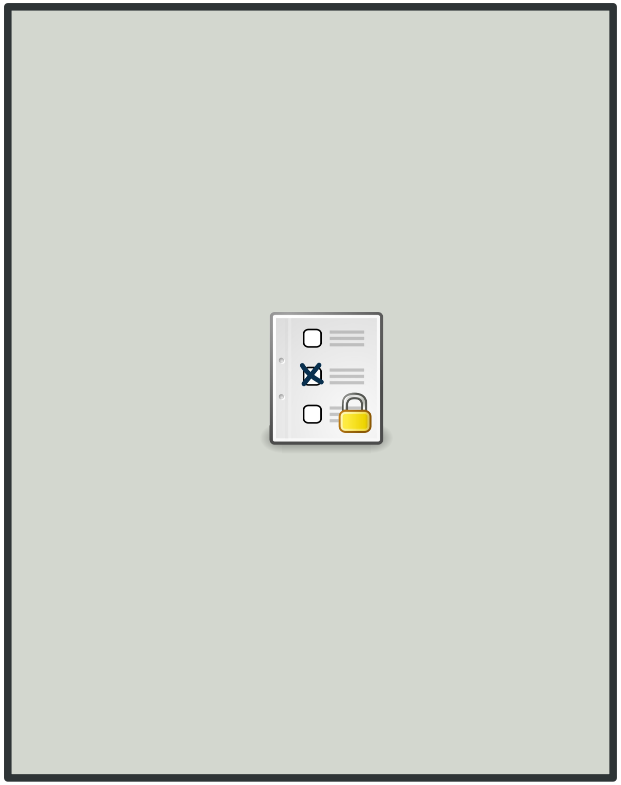
Casting

Auditing Ballots

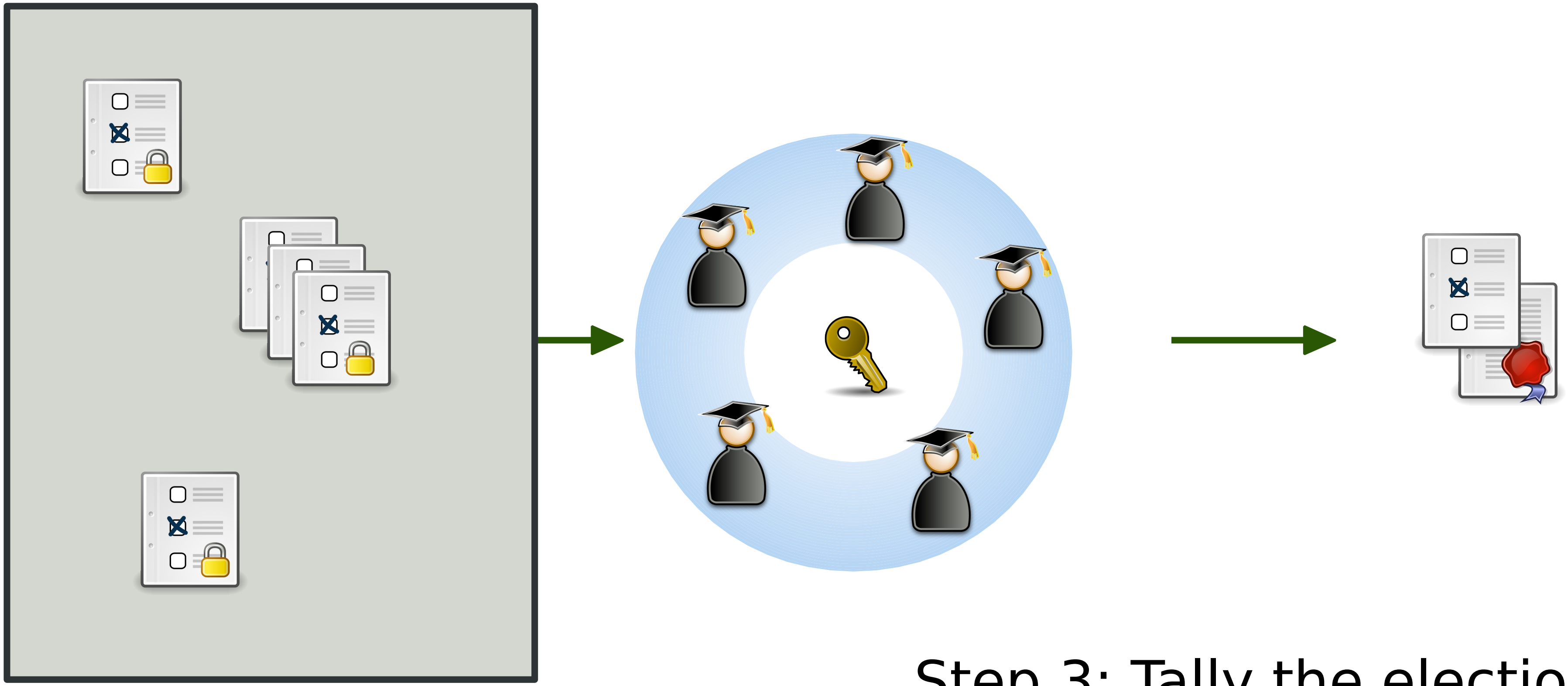


Voting

Voters can keep a copy of their ballot and check that it appears on the final board.

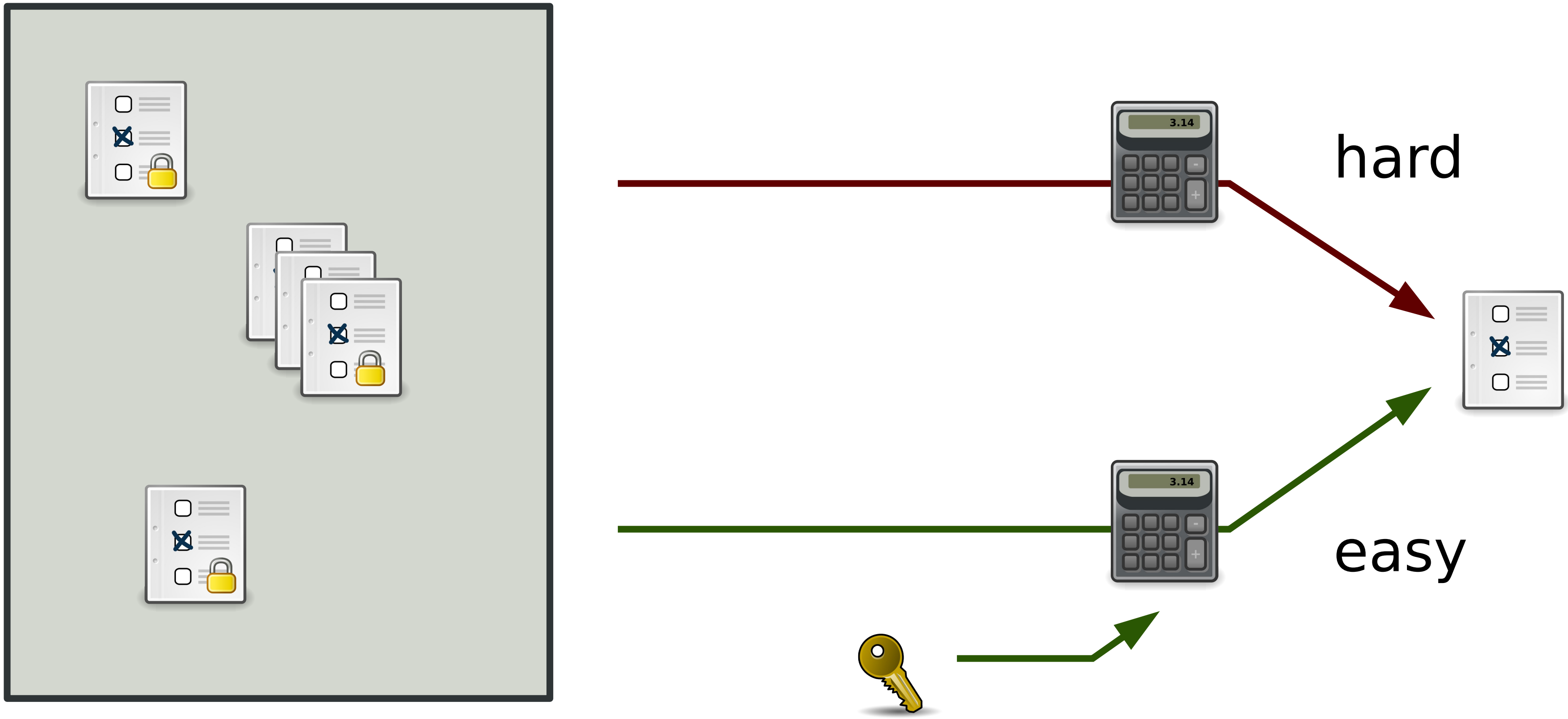


Tallying

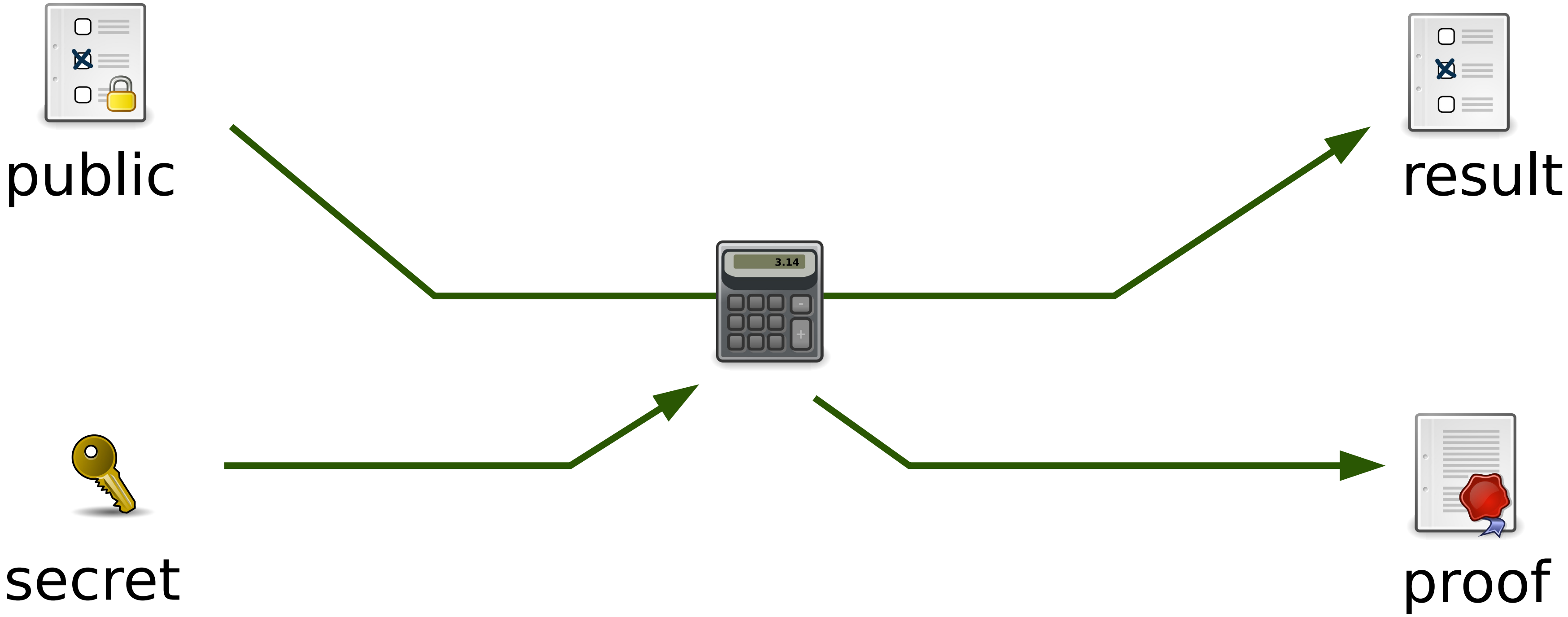


Step 3: Tally the election.

Tallying



Verifiable Computation



Privacy

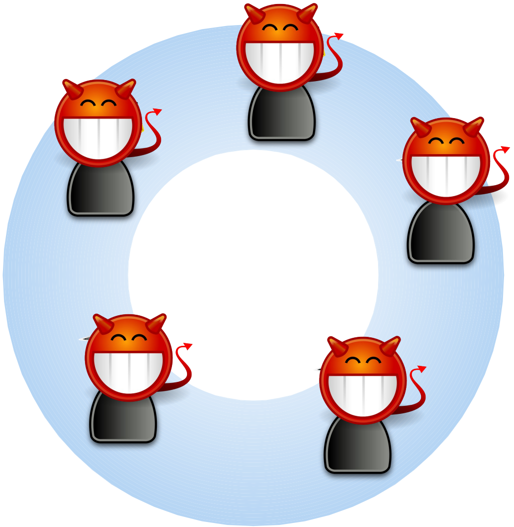
All but one administrator compromised:

Still cannot decrypt individual ballots.

Verifiability

Even if all administrators are compromised:

Still cannot claim an incorrect result.

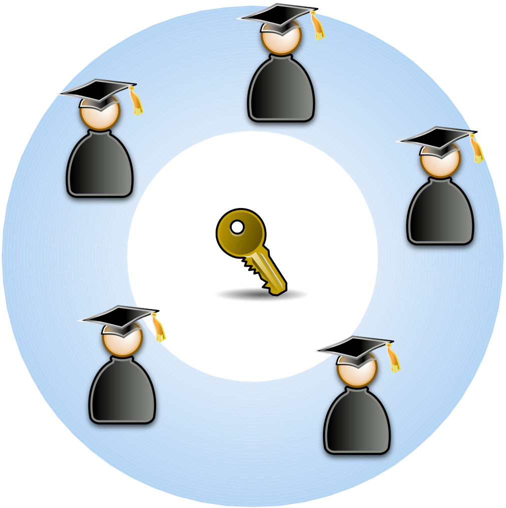


Tallying

Administrators *facilitate* rather than carry out tallying.

Tallying is *verifiable.*

Trust assumptions are very different to "vote counters" in pen-on-paper elections.



Is it secure?

My Work

Security model: abstraction of real world that can be analysed mathematically.

Security proof/argument: shows that an abstraction of a voting system meets an abstract model.

Proofs?

(My personal opinion)

A security argument is like a safety certificate: it shows that a cryptographic system conforms to certain standards or "best practice".

This does not prove that a system cannot fail. It gives assurance that risks of some types of failure have been mitigated.

Helios

Used in practice but no security argument – I tried to provide one.

Cortier/Smyth: possible privacy compromise under certain circumstances.

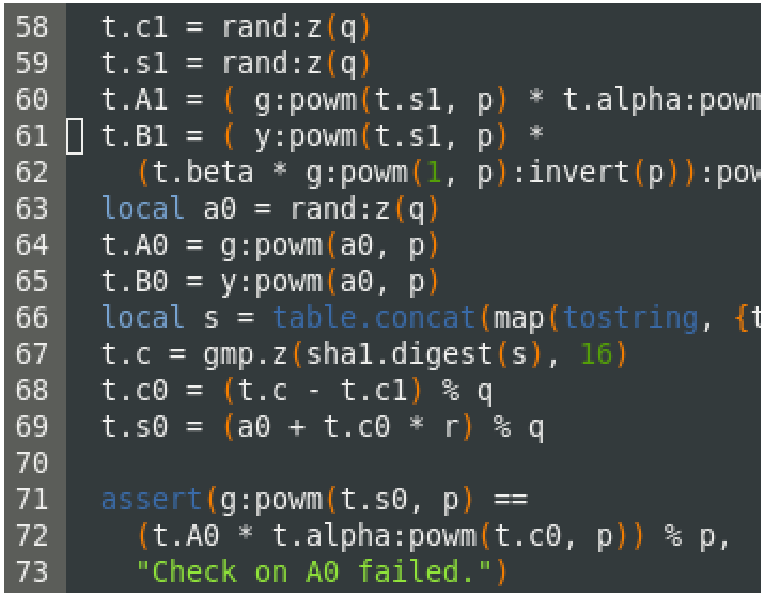
Some details of Helios were interfering with my attempt at a security argument ...

helios

Bad Ballots

I can create "bad" ballots that erase a tally in an election.

Don't try this at home – I can detect such ballots, too.



```
t.c1 = rand:z(q)
t.s1 = rand:z(q)
t.A1 = ( g:powm(t.s1, p) * t.alpha:powm
t.B1 = ( y:powm(t.s1, p) *
  (t.beta * g:powm(1, p):invert(p)):pow
local a0 = rand:z(q)
t.A0 = g:powm(a0, p)
t.B0 = y:powm(a0, p)
local s = table.concat(map(tostring, {t
t.c = gmp.z(sha1.digest(s), 16)
t.c0 = (t.c - t.c1) % q
t.s0 = (a0 + t.c0 * r) % q

assert(g:powm(t.s0, p) ==
  (t.A0 * t.alpha:powm(t.c0, p)) % p,
  "Check on A0 failed.")
```

Bad Ballots

Sample election with votes:

Yes	2
No	0
Maybe	1

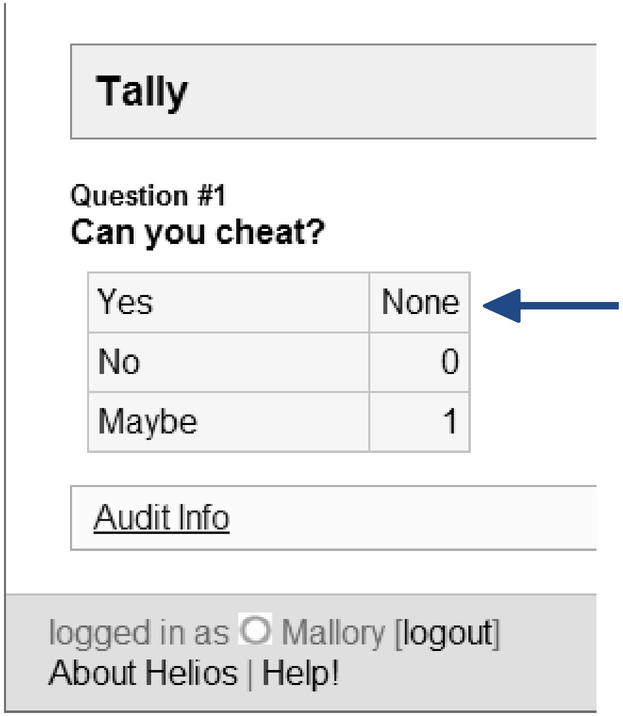
Bad ballot cast for "yes".

Bad Ballots

Sample election with votes:

Yes	2
No	0
Maybe	1

Bad ballot cast for "yes".



Tally

Question #1
Can you cheat?

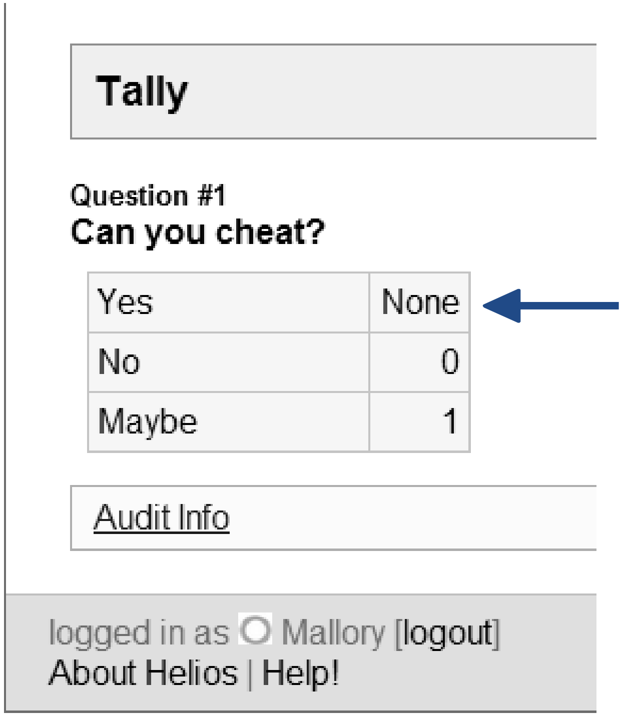
Yes	None
No	0
Maybe	1

Bad Ballots

Sample election with votes:

Yes 2
No 0
Maybe 1

Bad ballot cast for "yes".



Tally

Question #1
Can you cheat?

Yes	None
No	0
Maybe	1

Audit Info

logged in as ○ Mallory [logout]
About Helios | Help!

None

=

"null"

=

Something has gone very, very wrong

~~Verifiability~~

If all administrators are compromised:

The election result can be tampered with.

This attack is undetectable.

Consequences

Helios is easy to fix (the next version will be patched based on our work).

Paper at Asiacrypt 2012.
Cryptographic theory is relevant for practice.

So why aren't we using crypto-voting yet?

Quick Recap

I am trying to sell you an idea, not a product.

Cryptographic voting can offer both *privacy* and *verifiability*.

Verifiability makes a system *easier* to trust.

Coercion?

Election fraud, coercion and bribery are real problems – and need to be addressed in any "practical" system.

Helios is designed for low-coercion environments only.

Vote privacy is mostly just a step towards coercion-resistance.

Challenges

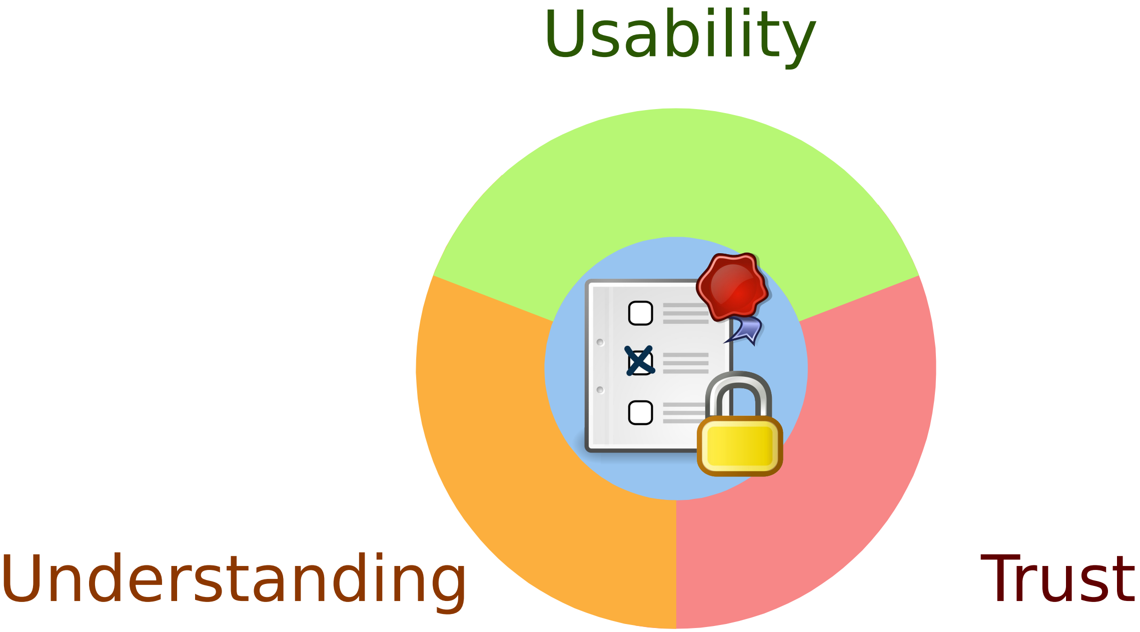
What is the single, most important property a voting system should possess?

Challenges

What is the single, most important property a voting system should possess?

Simplicity.

Challenges



The Future

Where do we go from here?

Prediction:
The next steps from here to a widely deployed system will probably have very little to do with cryptography.

Thank you