Voter de façon sûre par Internet

opportunité ou illusion ?

Steve Kremer

LORIA & Inria Nancy - Grand'Est

Sécurité Informatique:
Mythes et Réalité
8-9 décembre 2016 – Paris

The County Election, 1852 by George Caleb Bingham

Internet elections

Political legally binding Internet elections in Europe:

- parliamentary elections in **Switzerland** (several cantons)
- parliamentary election in **Estonia** (all eligible voters)
- municipal and county elections in **Norway** (selected municipalities, selected voter groups)
- parliamentary elections in in **France** ("expats")

But also **banned in Germany, Ireland, UK**

Even more **professional elections**

E-voting

Essential **security properties** of (e-)voting:

- **Integrity** of the election
- **Secrecy** of the vote

E-voting

Essential **security properties** of (e-)voting:

- **Integrity** of the election
- **Secrecy** of the vote

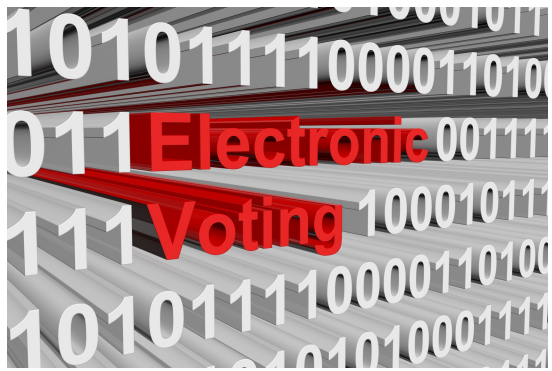
Warning:

With Internet voting (like any remote voting) there is no private voting booth!

Cryptographic protocols to the rescue?

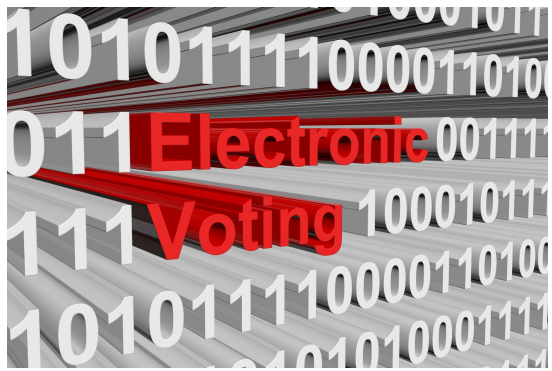
Cryptographic protocols everywhere!

- Distributed programs that
- use crypto primitives (encryption, digital signature ,. . .)
- to ensure security properties (confidentiality, authentication, anonymity,. . .)

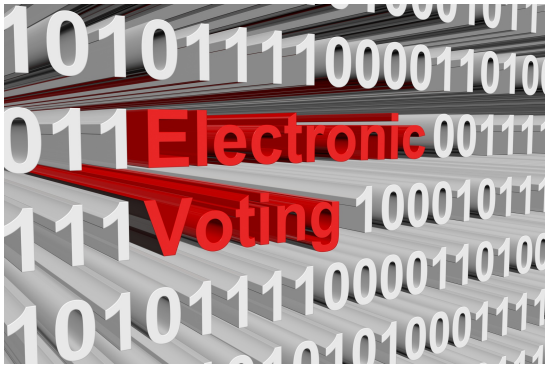


Cryptographic protocols everywhere!

- Distributed programs that
- use crypto primitives (encryption, digital signature ,. . .)
- to ensure security properties (confidentiality, authentication, anonymity,. . .)



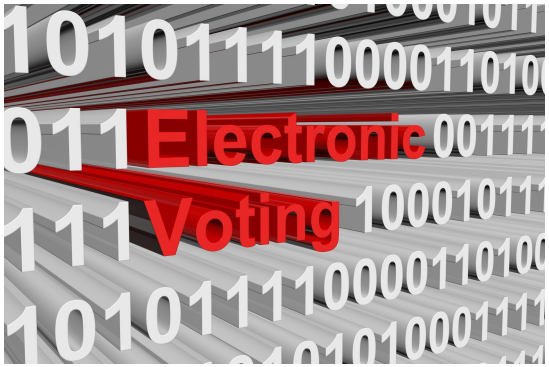
Cryptographic protocols are tricky!



Cryptographic protocols are tricky!

Bhargavan et al.:FREAK, Logjam, SLOTH, ...

Cremers et al., S&P'16

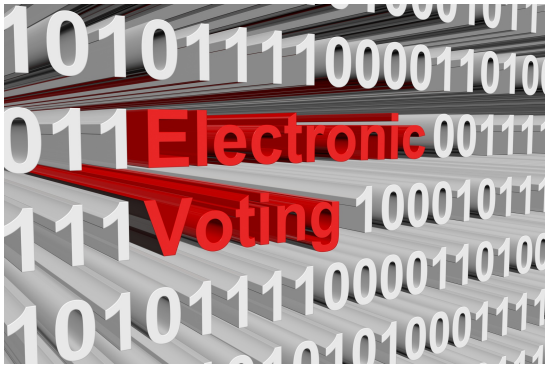


Cryptographic protocols are tricky!

Bhargavan et al.:FREAK, Logjam, SLOTH, ...

Cremers et al., S&P'16

Arapinis et al., CCS'12

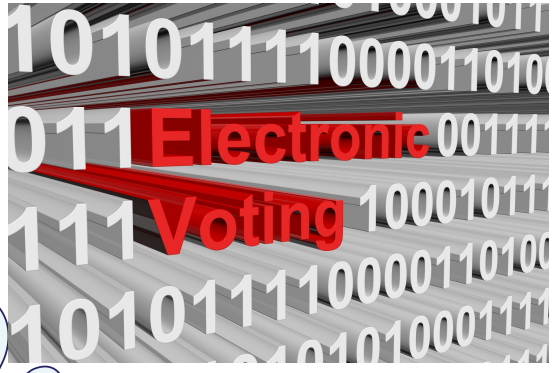


Cryptographic protocols are tricky!

Bhargavan et al.:FREAK, Logjam, SLOTH, ...

Cremers et al., S&P'16

Arapinis et al., CCS'12



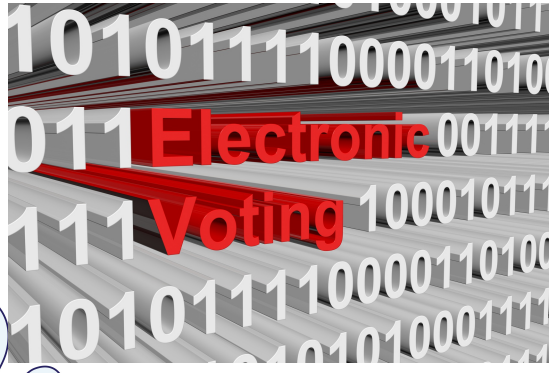
Cortier & Smyth, CSF'11

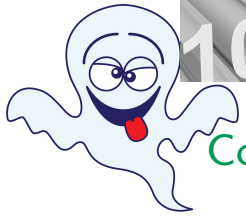
Cryptographic protocols are tricky!

Bhargavan et al.:FREAK, Logjam, SLOTH, . . .

Cremers et al., S&P'16

Arapinis et al., CCS'12





Cortier & Smyth, CSF'11

Steel et al., CSF'08, CCS'10

Specificities of e-voting

Complicated properties:

- vote privacy: no-one should learn my vote
- receipt-freeness/coercion resistance, everlasting privacy
- end-to-end verifiability: everyone should be able to verify that votes have been correctly counted

Complicated crypto:

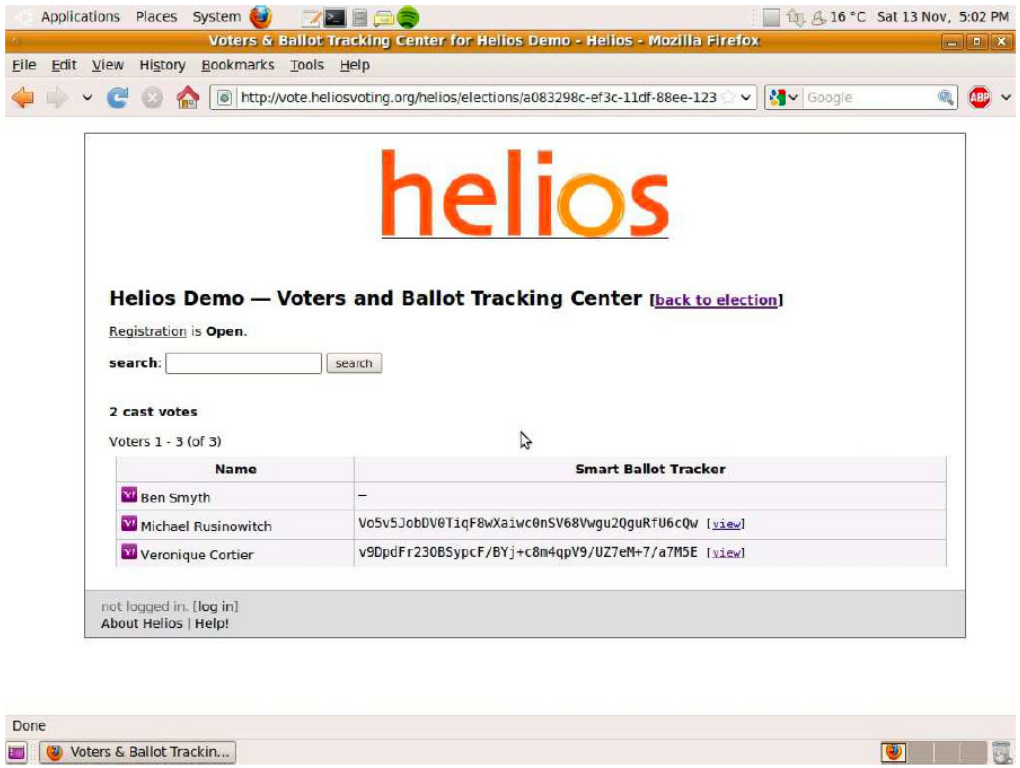
- zero-knowledge proofs, homomorphic encryption, threshold cryptography, ...

Arbitrary number of participants

The Helios e-voting protocol

Verifiable online elections via the Internet

http://heliosvoting.org/



Already in use:

- Election at Louvain University Princeton
- Election of the IACR board (major association in Cryptography)

Designed for low-coercion environments (not receipt-free).

Behavior of Helios (simplified)

Phase 1: voting

Bulletin Board

Alice	$\{v_A\}_{pk(E)}$	$v_A = 0$ or 1
Bob	$\{v_B\}_{pk(E)}$	$v_B = 0$ or 1
Chris	$\{v_C\}_{pk(E)}$	$v_C = 0$ or 1

Behavior of Helios (simplified)

Phase 1: voting

$\{v_D\}_{pk(E)} \longrightarrow$

Bulletin Board

Alice	$\{v_A\}_{pk(E)}$	$v_A = 0$ or 1
Bob	$\{v_B\}_{pk(E)}$	$v_B = 0$ or 1
Chris	$\{v_C\}_{pk(E)}$	$v_C = 0$ or 1

$pk(E)$: election public key

Behavior of Helios (simplified)

Phase 1: voting

Bulletin Board		
Alice	$\{v_A\}_{pk(E)}$	$v_A = 0$ or 1
Bob	$\{v_B\}_{pk(E)}$	$v_B = 0$ or 1
Chris	$\{v_C\}_{pk(E)}$	$v_C = 0$ or 1
David	$\{v_D\}_{pk(E)}$	$v_D = 0$ or 1

$pk(E)$: election public key

Behavior of Helios (simplified)

Phase 1: voting

Bulletin Board

Alice	$\{v_A\}_{pk(E)}$	$v_A = 0$ or 1
Bob	$\{v_B\}_{pk(E)}$	$v_B = 0$ or 1
Chris	$\{v_C\}_{pk(E)}$	$v_C = 0$ or 1
David	$\{v_D\}_{pk(E)}$	$v_D = 0$ or 1
...	...	

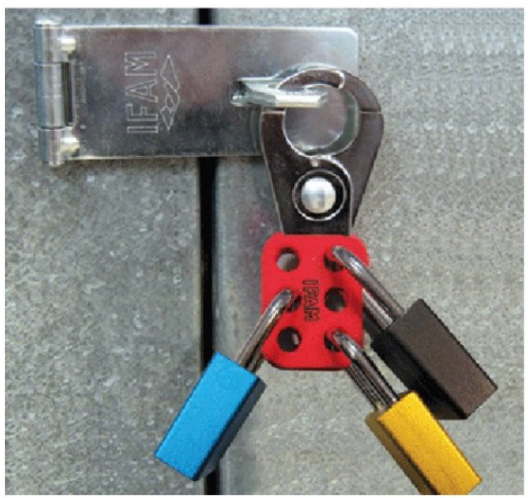
$pk(E)$: election public key

Behavior of Helios (simplified)

Phase 1: voting

Bulletin Board		
Alice	$\{v_A\}_{pk(E)}$	$v_A = 0$ or 1
Bob	$\{v_B\}_{pk(E)}$	$v_B = 0$ or 1
Chris	$\{v_C\}_{pk(E)}$	$v_C = 0$ or 1
David	$\{v_D\}_{pk(E)}$	$v_D = 0$ or 1
...	...	

$pk(E)$: election public key; private key shared among trustees.



Behavior of Helios (simplified)

Phase 1: voting

Bulletin Board		
Alice	$\{v_A\}_{pk(E)}$	$v_A = 0$ or 1
Bob	$\{v_B\}_{pk(E)}$	$v_B = 0$ or 1
Chris	$\{v_C\}_{pk(E)}$	$v_C = 0$ or 1
David	$\{v_D\}_{pk(E)}$	$v_D = 0$ or 1
...	...	

Phase 2: Tallying using homomorphic encryption (El Gamal)

$$\prod_{i=1}^{n} \{v_i\}_{pk(E)} = \{\sum_{i=1}^{n} v_i\}_{pk(E)}$$

based on $g^a * g^b = g^{a+b}$

$\rightarrow$ Only the final result needs to be decrypted!

$pk(E)$: election public key; private key shared among trustees.

This is oversimplified!

Bulletin Board	
Alice	$\{v_A\}_{pk(E)}$
Bob	$\{v_B\}_{pk(E)}$
Chris	$\{v_C\}_{pk(E)}$
David	$\{v_D\}_{pk(E)}$
...	...

$v_A = 0$ or 1

$v_B = 0$ or 1

$v_C = 0$ or 1

Result: $\{v_A + v_B + v_C + v_D + \cdots\}_{pk(E)}$

This is oversimplified!

Bulletin Board		
Alice	$\{v_A\}_{pk(E)}$	$v_A = 0$ or 1
Bob	$\{v_B\}_{pk(E)}$	$v_B = 0$ or 1
Chris	$\{v_C\}_{pk(E)}$	$v_C = 0$ or 1
David	$\{v_D\}_{pk(E)}$	$v_D = 100$
...	...	

Result: $\{v_A + v_B + v_C + 100 + \cdots\}_{pk(E)}$

A malicious voter can cheat!

This is oversimplified!

Bulletin Board		
Alice	$\{v_A\}_{pk(E)}$	$v_A = 0$ or 1
Bob	$\{v_B\}_{pk(E)}$	$v_B = 0$ or 1
Chris	$\{v_C\}_{pk(E)}$	$v_C = 0$ or 1
David	$\{v_D\}_{pk(E)}$	~~$v_D = 100$~~
...	...	

Result: $\{v_A + v_B + v_C + v_D + \cdots\}_{pk(E)}$

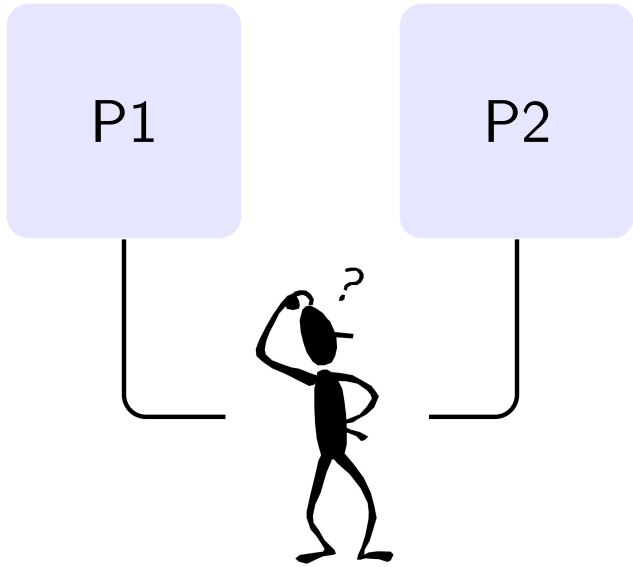
~~A malicious voter can cheat!~~

In Helios: use Zero Knowledge Proof

$$\{v_D\}_{pk(E)}, \text{ZKP}\{v_D = 0 \text{ or } 1\}$$

How to define vote privacy?

The notion of indistinguishability



Naturally modelled using **equivalences** from process calculi

$P_1 \approx P_2$ iff for all processes A, we have that:

$$A \mid P_1 \to 1 \text{ if, and only if, } A \mid P_2 \to 1$$

How to define vote privacy?

How can we model

"**the attacker does not learn my vote (0 or 1)**"?

How to define vote privacy?

How can we model

"**the attacker does not learn my vote (0 or 1)**"?

- The attacker cannot learn the value of my vote

How to define vote privacy?

How can we model

"**the attacker does not learn my vote (0 or 1)**"?

- The attacker cannot learn the value of my vote
  $\rightsquigarrow$ but the attacker knows values 0 and 1

How to define vote privacy?

How can we model

"**the attacker does not learn my vote (0 or 1)**"?

- ~~The attacker cannot learn the value of my vote~~
- The attacker cannot distinguish A votes and B votes: $V_A(v) \approx V_B(v)$

How to define vote privacy?

How can we model

"**the attacker does not learn my vote (0 or 1)**"?

- ~~The attacker cannot learn the value of my vote~~

- The attacker cannot distinguish A votes and B votes:
  $V_A(v) \approx V_B(v)$
  $\rightsquigarrow$ but identities are revealed

How to define vote privacy?

How can we model

"**the attacker does not learn my vote (0 or 1)**"?

- ~~The attacker cannot learn the value of my vote~~
- ~~The attacker cannot distinguish A votes and B votes: $V_A(v) \approx V_B(v)$~~
- The attacker cannot distinguish A votes 0 and A votes 1: $V_A(0) \approx V_A(1)$

How to define vote privacy?

How can we model

"**the attacker does not learn my vote (0 or 1)**"?

- ~~The attacker cannot learn the value of my vote~~
- ~~The attacker cannot distinguish A votes and B votes: $V_A(v) \approx V_B(v)$~~
- The attacker cannot distinguish A votes 0 and A votes 1: $V_A(0) \approx V_A(1)$
  $\rightsquigarrow$ but election outcome is revealed

How to define vote privacy?

How can we model

"**the attacker does not learn my vote (0 or 1)**"?

- ~~The attacker cannot learn the value of my vote~~
- ~~The attacker cannot distinguish A votes and B votes: $V_A(v) \approx V_B(v)$~~
- ~~The attacker cannot distinguish A votes 0 and A votes 1: $V_A(0) \approx V_A(1)$~~
- The attacker cannot distinguish the situation where two honest voters swap votes:

$$V_A(0) \parallel V_B(1) \approx V_A(1) \parallel V_B(0)$$

Vote privacy in Helios?

Bulletin Board		
Alice	$\{v_A\}_{pk(E)}$	$v_A = 0$ or 1
Bob	$\{v_B\}_{pk(E)}$	$v_B = 0$ or 1

Vote privacy in Helios?

$\{v_A\}_{pk(E)} \longrightarrow$

Bulletin Board		
Alice	$\{v_A\}_{pk(E)}$	$v_A = 0$ or 1
Bob	$\{v_B\}_{pk(E)}$	$v_B = 0$ or 1
Chris	$\{v_A\}_{pk(E)}$	

Replay attack break vote privacy:
Alice must have voted for the winner!

Attack found when trying to formally prove privacy

Election transparency

In **traditional elections**:

- transparent ballot box
- observers
- ...

Election transparency

In **traditional elections**:

- transparent ballot box
- observers
- ...

In **e-voting**: ensuring absence of bugs/backdoors seems impossible

$\rightsquigarrow$ **End-to-end Verifiability**

- **Individual verifiability**: vote cast as intended

  e.g., voter checks his encrypted vote is on a public bulletin board
- **Universal verifiability**: vote counted as casted

  e.g., crypto proof that decryption was performed correctly
- **Eligibility verifiability**: only eligible votes counted

  e.g., crypto proof that every vote corresponds to a credential

$\rightsquigarrow$ **Verify the election, not the system!**

From Helios to Belenios

Helios does not guarantee **Eligibility verifiability**

$\rightsquigarrow$ **ballot stuffing** possible by dishonest Bulletin Board

From Helios to Belenios

Helios does not guarantee **Eligibility verifiability**

$\rightsquigarrow$ **ballot stuffing** possible by dishonest Bulletin Board

Belenios: variant of Helios

- introduce credential issuer
- public credentials allow to verify eligibility
- private credentials necessary to vote (unknown to Bulletin Board)

Developped at LORIA by CARAMBA and PESTO teams

Used by CNRS, INRIA, LORIA, ...

Everlasting privacy

Publishing encrypted votes on BB: **a threat for vote privacy**?

- Future technology/scientific advances may break encryptions
- How long must a vote remain private?
  1 year? 10 years? 100 years? 10^{10} years?
- Impossible to predict the necessary key length with certainty:
  typical recommendations for less than 10 years

Everlasting privacy

Publishing encrypted votes on BB: **a threat for vote privacy**?

- Future technology/scientific advances may break encryptions
- How long must a vote remain private?
  1 year? 10 years? 100 years? 10^{10} years?
- Impossible to predict the necessary key length with certainty:
  typical recommendations for less than 10 years

$\rightsquigarrow$ **everlasting privacy**: guarantee privacy even if crypto is broken

Everlasting privacy

Publishing encrypted votes on BB: **a threat for vote privacy**?

- Future technology/scientific advances may break encryptions
- How long must a vote remain private?
  1 year? 10 years? 100 years? 10^{10} years?
- Impossible to predict the necessary key length with certainty:
  typical recommendations for less than 10 years

$\rightsquigarrow$ **everlasting privacy**: guarantee privacy even if crypto is broken

Achieving everlasting privacy:

- Do not publish encryption on the BB, but only a **perfectly hiding commitment**
- Replace identities by **anonymous credentials** $\rightsquigarrow$ **Belenios**

Voting on untrusted client

Proofs generally assume (implicitly) **trustworthy client software**

Privacy: malware may leak vote
Verifiability: malware may change vote before encryption

Potential use of dedicated malware for changing votes demonstrated

- by Laurent Grégoire in French national election ("expats")
- by Paavo Pihelgas in Estonian parlament election

Voting on untrusted client

Proofs generally assume (implicitly) **trustworthy client software**

Privacy: malware may leak vote
Verifiability: malware may change vote before encryption

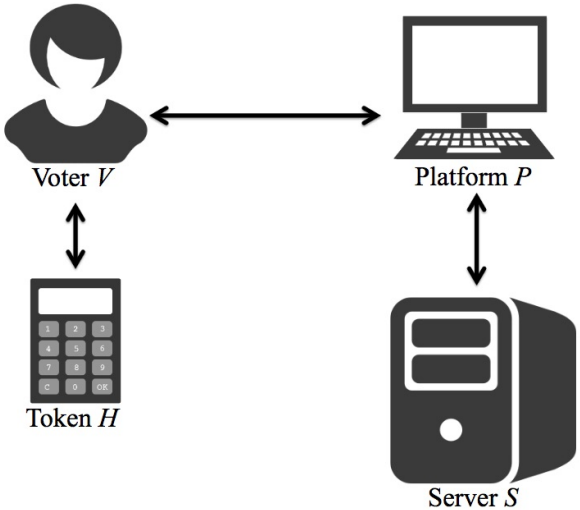
Potential use of dedicated malware for changing votes demonstrated

- by Laurent Grégoire in French national election ("expats")
- by Paavo Pihelgas in Estonian parlament election

Some mitigations:

- Benaloh challenge in Helios/Belenios: cut and choose technique allows for audit
- Code voting: distribution of personalised code sheets

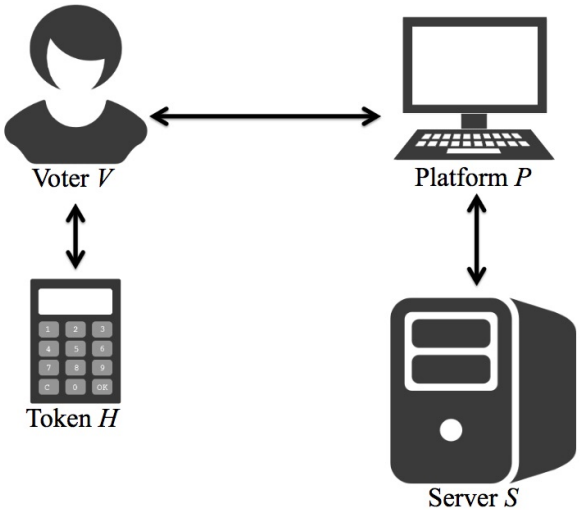
The DU-Vote protocol: *"Voting with untrusted devices"*



- First protocol to achieve both privacy and verifiability, even on malware infected platform
- Uses small external device and (low-entropy) codes

Grewal et al: Du-Vote: Remote Electronic Voting with Untrusted Computers. CSF'15

The DU-Vote protocol: *"Voting with untrusted devices"*



- First protocol to achieve both privacy and verifiability, even on malware infected platform
- Uses small external device and (low-entropy) codes

Inria Nancy

COMMUNICATIONS OF THE ACM

Search

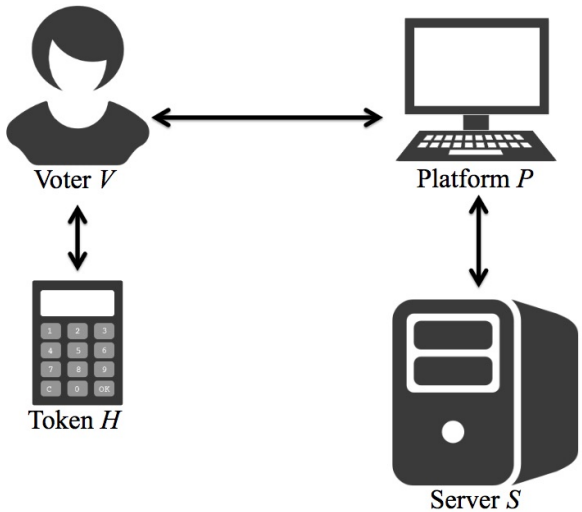
HOME | CURRENT ISSUE | NEWS | BLOGS | OPINION | RESEARCH | PRACTICE | CAREERS | ARCHIVI

Home / News / Online Voting a Step Closer Thanks to Breakthrough... / Full Text

ACM TECHNEWS

Online Voting a Step Closer Thanks to Breakthrough in Security Technology

The DU-Vote protocol: *"Voting with untrusted devices"*



- First protocol to achieve both privacy and verifiability, even on malware infected platform
- Uses small external device and (low-entropy) codes

Our security analysis: severe attacks (e.g. change vote in an undetectable way)

$\rightsquigarrow$ still an active research area

Grewal et al: Du-Vote: Remote Electronic Voting with Untrusted Computers. CSF'15

Kremer, Rønne: Du-Vote: An intensive analysis of DU-Vote. EuroS&P'16

Conclusion

- Voting through the Internet is a form of **remote voting**
- **Distribution of credentials** (login/password) is a sensitive procedure (above all if no existing infrastructure)
- Good **privacy** and **verifiability** guarantees if client is trusted
  $\rightsquigarrow$ **malware resistance** an active research topic
- **Receipt-freeness** / **coercion-resistance** can be achieved but solutions are generally complicated
- **In cryptography we trust?**
  $\rightsquigarrow$ complicated procedures – need to **trust experts**