Why Public Boards are Required in E-Voting Systems Based on Threshold Blind Signature

Reto E. Koenig, Eric Dubuis, Rolf Haenni

Univeristy of Fribourg
&
University of Applied Science Berne

24.07.2010

UNIVERSITAS FRIBURGENSIS

Berner Fachhochschule

HASLERSTIFTUNG

Outline

1. Introduction
2. Blind Signature Voting Scheme
3. Multiple Authorities
4. Attack on Democracy
5. Solution
6. Conclusion

Why This Talk?

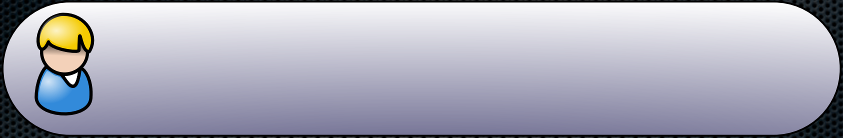
Default blind signature schemes...

- ...are simple and understandable
- ...are used in many E-Voting / E-Cash Protocols
- ...bear a severe weakness
  if used within a threshold protocol

Outline

1. Introduction
2. Blind Signature Voting Scheme
3. Multiple Authorities
4. Attack on Democracy
5. Solution
6. Conclusion

Voters Will



The voter...

- ...gets the ballot...
- ...declares the will onto the ballot.

Voters Will

Vote for one option:
□ Joe Smith
□ John Citizen
□ Jane Doe
□ Fred Rubble
□ Mary Hill
Authorization:

The voter...

- ...gets the ballot...
- ...declares the will onto the ballot.

Filling in the Ballot

Voters Will

Vote for one option:

☐ Joe Smith

☒ John Citizen

☐ Jane Doe

☐ Fred Rubble

☐ Mary Hill

Authorization:

The voter...

- ...gets the ballot...
- ...declares the will onto the ballot.

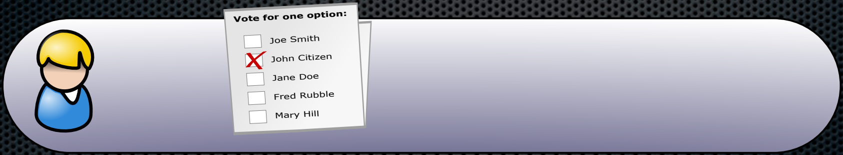
Blinding

Vote for one option:
□ Joe Smith
☒ John Citizen
□ Jane Doe
□ Fred Rubble
□ Mary Hill

The voter...

- ...blinds the vote for the voting authority...

Blinding



The voter...

- ...blinds the vote for the voting authority...

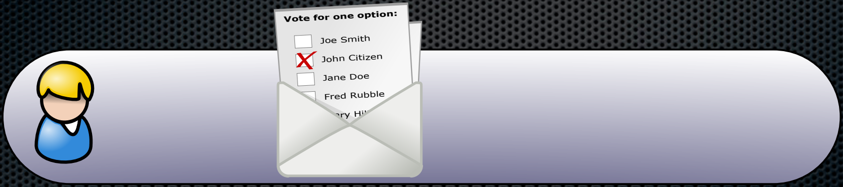
Blinding

Authorization:

The voter...

- ...blinds the vote for the voting authority...

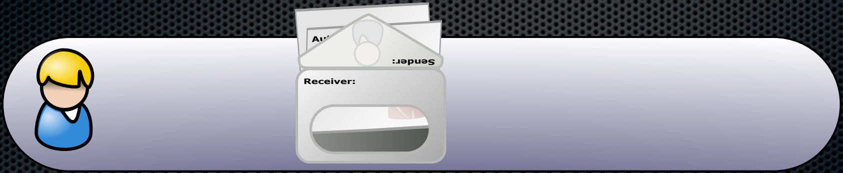
Blinding



The voter…

- …blinds the vote for the voting authority…

Blinding



The voter...

- ...blinds the vote for the voting authority...

Blinding

The voter...

- ...blinds the vote for the voting authority...

Voter - Signing

The voter...

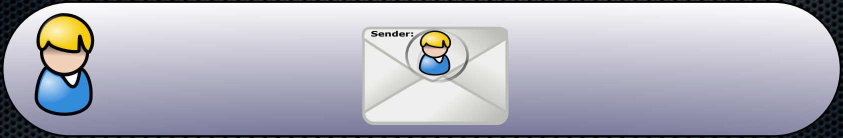
- ...signs the blinded vote...

Voter - Signing

The voter...

- ...signs the blinded vote...

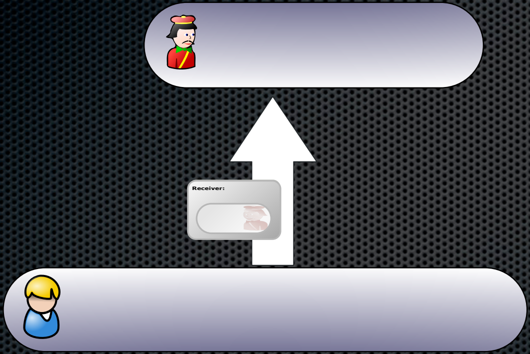
Voter - Signing



The voter...

- ...signs the blinded vote...

Transmission



The voter...

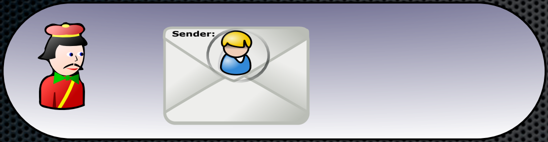
- ...sends the blinded vote to the authority.

Verifying the Eligibility

The authority...

- ...verifies the eligibility of the voter...
- ...by consulting and updating the voter roll...

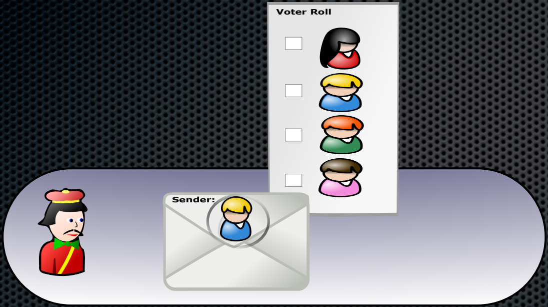
Verifying the Eligibility



The authority...

- ...verifies the eligibility of the voter...
- ...by consulting and updating the voter roll...

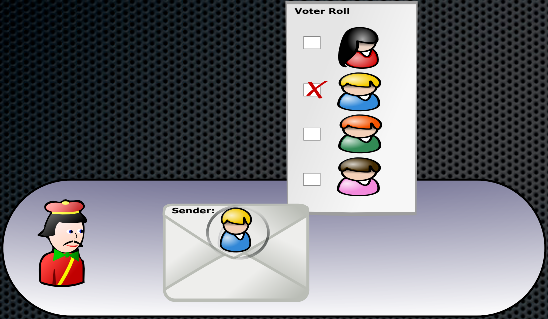
Verifying the Eligibility



The authority...

- ...verifies the eligibility of the voter...
- ...by consulting and updating the voter roll...

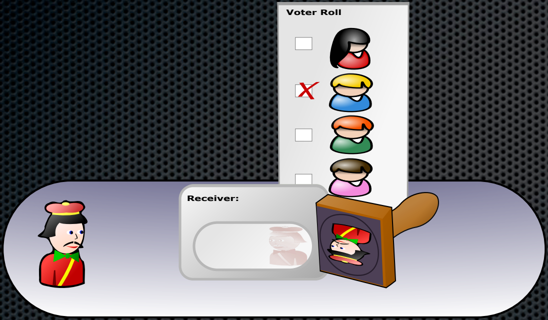
Verifying the Eligibility



The authority...

- ...verifies the eligibility of the voter...
- ...by consulting and updating the voter roll...

Authority - Signing



The authority...

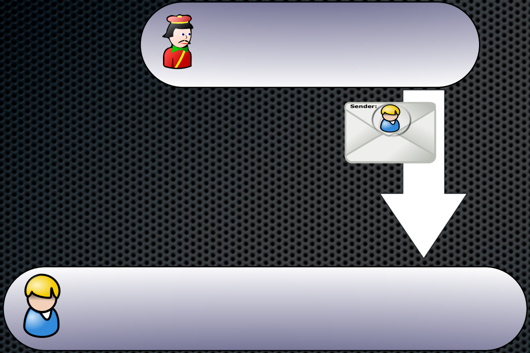
- ...blindly signs the vote in the envelope...

Authority - Signing

The authority...

- ...blindly signs the vote in the envelope...

Transmission



The authority...

- ...sends the blindly signed vote back to the voter.

Unblinding

The voter...

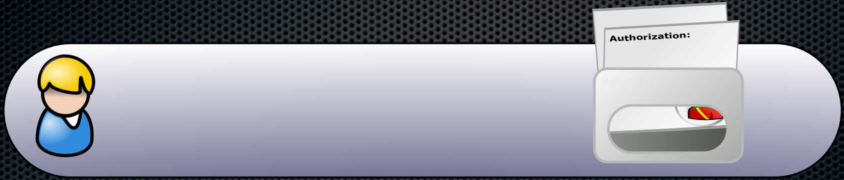
- ...unblinds the vote...
- ...is ready to cast an authorized anonymous vote.

Unblinding

The voter...

- ...unblinds the vote...
- ...is ready to cast an authorized anonymous vote.

Unblinding



The voter...

- ...unblinds the vote...
- ...is ready to cast an authorized anonymous vote.

Unblinding

Vote for one option:

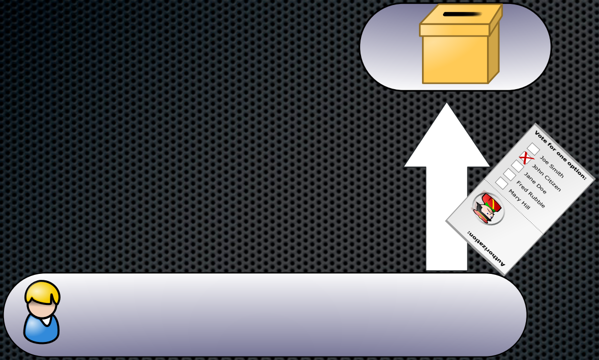
- □ Joe Smith
- ☒ John Citizen
- □ Jane Doe
- □ Fred Rubble
- □ Mary Hill

Authorization:

The voter...

- ...unblinds the vote...
- ...is ready to cast an authorized anonymous vote.

Transmission



The voter...

- ...sends the authorized vote to the ballot box...

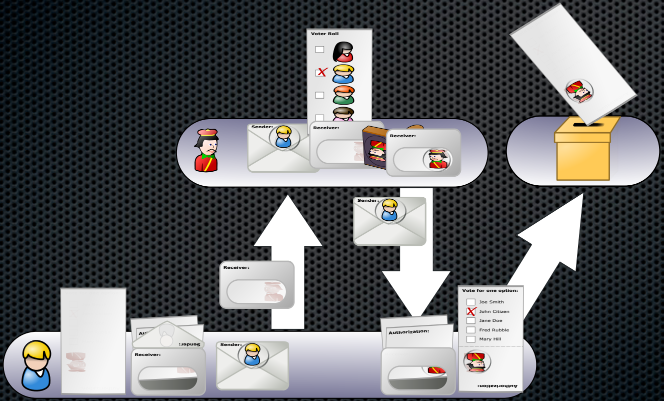
Vote Casting

Vote for one option:
□ Joe Smith
☒ John Citizen
□ Jane Doe
□ Fred Rubble
□ Mary Hill
Authorization:

The ballot box...

- ...accepts the authorized vote. (E2E-Verifiable)

Scheme Overview



Standard RSA-Blind Signature Scheme

Definition

$V =$ Voter

$A =$ Authority

$B =$ Ballot box

$v =$ Vote

$e, m =$ Public key of signing authority

$d =$ Private key of signing authority

$r =$ Random blinding factor

Scheme (everything $\mod m$)

$$V \rightarrow A : v' = vr^e$$
$$V \leftarrow A : s' = v'^d = v^d r^{ed} = v^d r$$
$$V : s = s' r^{-1} = v^d r r^{-1} = v^d$$
$$V \rightarrow B : (v, s)$$

Scheme in Action

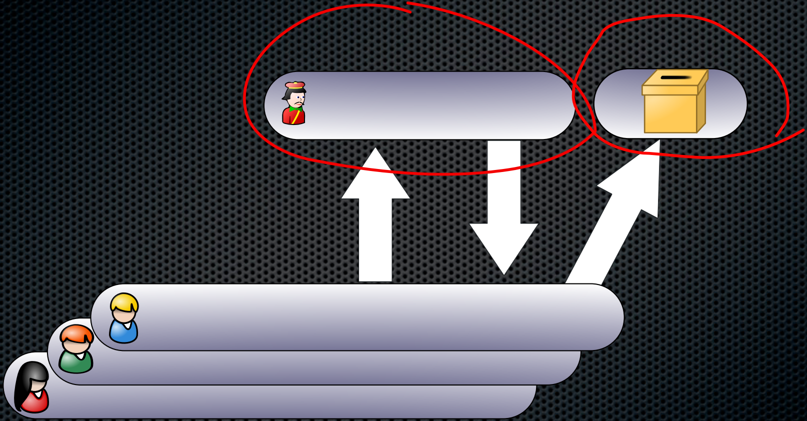
A list of some protocols use this scheme:

A. Fujioka et al	A practical secret voting scheme for large scale elections. Advances of Auscrypt'92, LNCS 718:244?251, 1992.
T. Okamoto	An electronic voting scheme. Proceedings of IFIP'96, pages 21?30, 1996.
Zhe Xia, Schneider	S.A. (2007) A New Receipt-Free E-Voting Scheme Based on Blind Signature (Abstract) , IaVoSS Workshop on Trustworthy Elections (WOTE) , 2006
...	...

Outline

1. Introduction
2. Blind Signature Voting Scheme
3. Multiple Authorities
4. Attack on Democracy
5. Solution
6. Conclusion

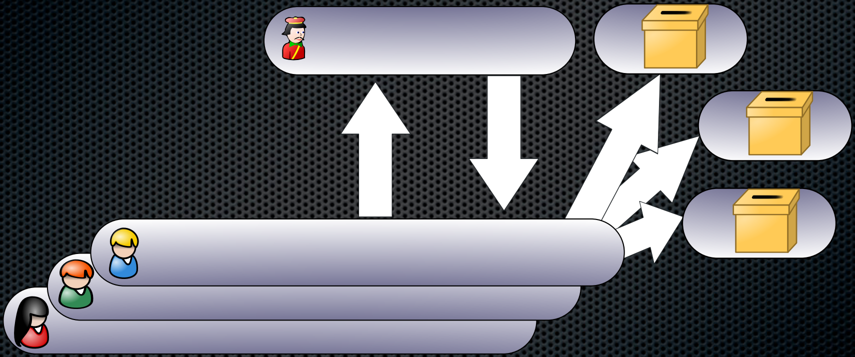
Single Point of Failure



Only one single...

- ...authority
- ...ballot box

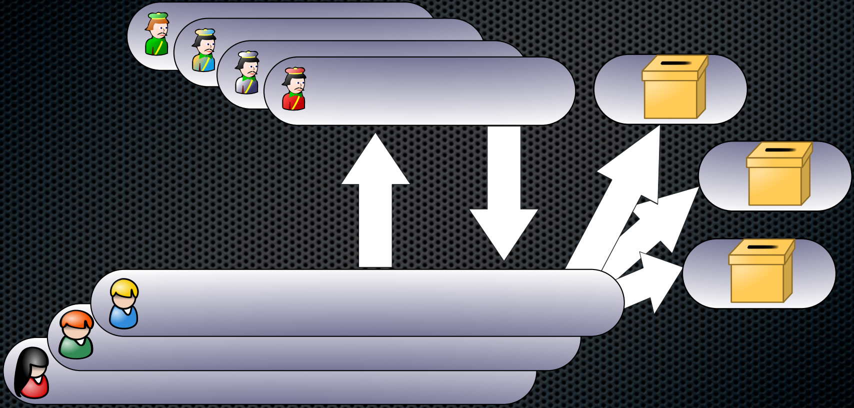
Multiple Ballot Boxes



The replication of the...

- ... ballot box does not affect blind signature scheme

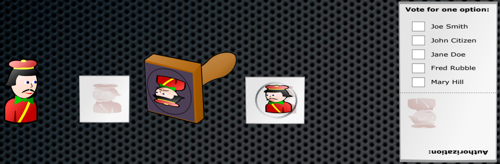
Multiple Authorities (Needs complete scheme re-design)



The replication of the...

- ...authority requires complete re-design of the signature scheme

Single Voting Authority



Vote for one option:

- □ Joe Smith
- □ John Citizen
- □ Jane Doe
- □ Fred Rubble
- □ Mary Hill

Authorization:

Instead of a single...

- ...authority...
- ...authority signature vote

… a multiple…

Multiple Instances…

- of authorities are needed.

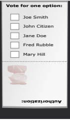
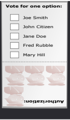
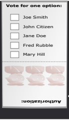
Amount of Required Signatures for n authorities

Is the protocol safe against...

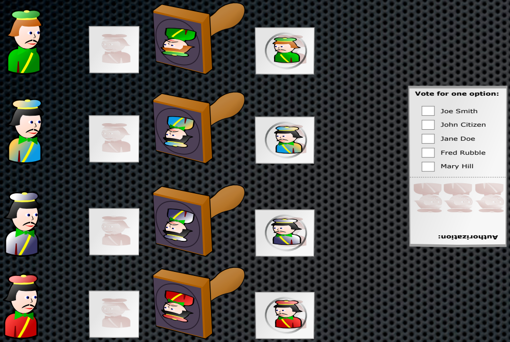
	Failure	Boycott	Masquerade

Amount of Required Signatures for n authorities

Is the protocol safe against...

	Failure	Boycott	Masquerade
 Vote for one option: ☐ Joe Smith ☐ John Citizen ☐ Jane Doe ☐ Fred Rubble ☐ Mary Hill Authorization: 1 out of n	Yes	Yes	No
 Vote for one option: ☐ Joe Smith ☐ John Citizen ☐ Jane Doe ☐ Fred Rubble ☐ Mary Hill Authorization: n out of n	No	No	Yes
 Vote for one option: ☐ Joe Smith ☐ John Citizen ☐ Jane Doe ☐ Fred Rubble ☐ Mary Hill Authorization: t out of n	Yes	Yes	Yes

Ballot For Threshold Voting Authorization



Vote for one option:

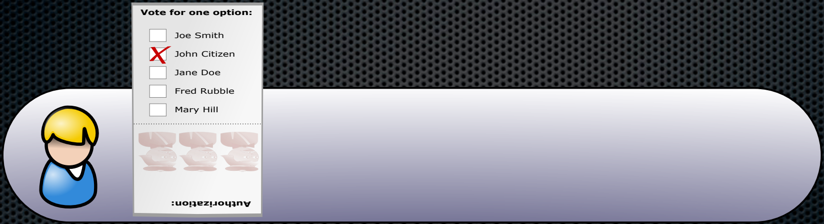
□ Joe Smith
□ John Citizen
□ Jane Doe
□ Fred Rubble
□ Mary Hill

Authorization:

Threshold

- … authority signature vote. (i.e. Less signatures required than authorities available)

Voting / Blinding



Vote for one option:

- □ Joe Smith
- ☒ John Citizen
- □ Jane Doe
- □ Fred Rubble
- □ Mary Hill

The voter...

- ...votes...
- ...blinds the vote for an arbitrary chosen authority...

Voting / Blinding

The voter...

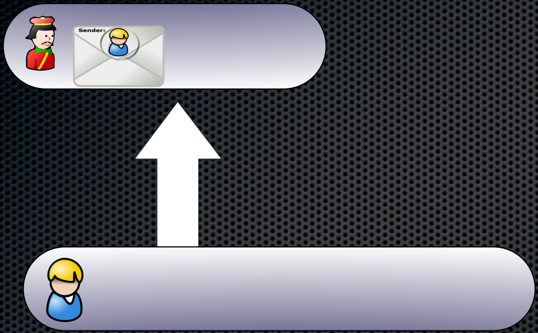
- ...votes...
- ...blinds the vote for an arbitrary chosen authority...

Signing / Sending

The voter…

- …signs the blinded vote
- …sends it to the chosen authority.

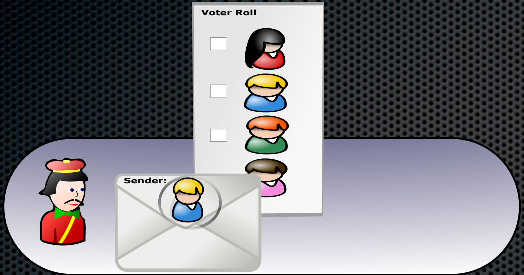
Signing / Sending



The voter...

- ...signs the blinded vote
- ...sends it to the chosen authority.

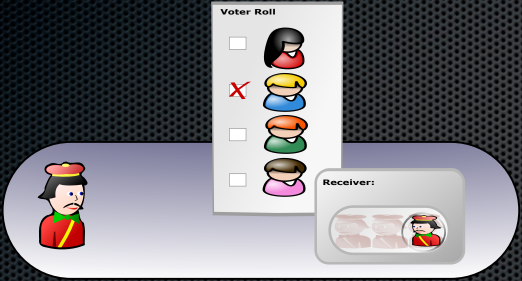
Requesting Authorization



The authority...

- ...verifies the eligibility of the voter...
- ...by consulting and updating the voter roll...

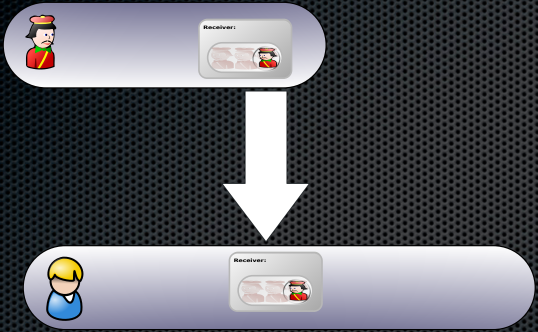
Requesting Authorization



The choosen authority...

- ...blindly signs the vote in the envelope...
- ...sends the blindly signed vote back to the voter.

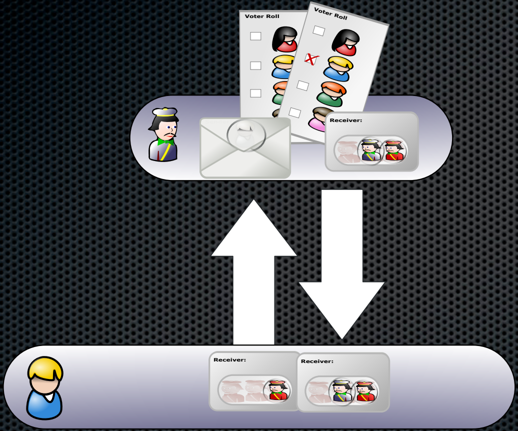
Requesting Authorization



The choosen authority...

- ...blindly signs the vote in the envelope...
- ...sends the blindly signed vote back to the voter.

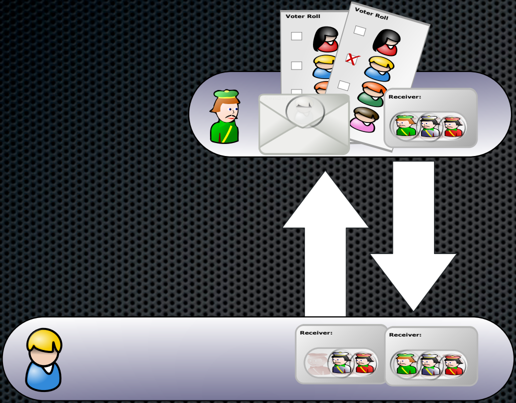
Requesting Authorization



This procedure is repeated...

- ...with other arbitrary chosen authorities...
- ...until the authorization-signature threshold is reached

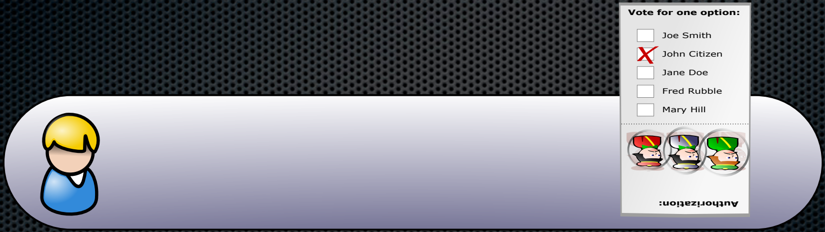
Requesting Authorization



This procedure is repeated...

- ...with other arbitrary chosen authorities...
- ...until the authorization-signature threshold is reached

Requesting Authorization



Vote for one option:

□ Joe Smith
☒ John Citizen
□ Jane Doe
□ Fred Rubble
□ Mary Hill

Authorization:

This procedure is repeated...

- ...with other arbitrary chosen authorities...
- ...until the authorization-signature threshold is reached

Modified Threshold RSA-Blind Signature Scheme

Definition

$V =$ Voter

$A_i =$ Authority

$B =$ Ballot box

$v =$ Vote

$e_i, m_i =$ Public key of signing authority

$d_i =$ Private key of signing authority

$r =$ Random blinding factor

Scheme

$$
\begin{aligned}
& V \rightarrow A_1 : v'_1 = vr^{e_1} \\
& V \leftarrow A_1 : s'_1 = v'^{d_1} = v^{d_1} r^{e_1 d_1} = v^{d_1} r \\
& \vdots \\
& V \rightarrow A_t : v'_t = vr^{e_t} \\
& V \leftarrow A_t : s'_t = v'^{d_t} = v^{d_t} r^{e_t d_t} = v^{d_t} r \\
& V \rightarrow B : (v, \{s_1, \ldots, s_t\}) \text{ where } s_i = s'_i r^{-1} = v^{d_i} r r^{-1} = v^{d_i}
\end{aligned}
$$

Scheme in Action

A list of some protocols use this scheme:

B. W. DuRette Multiple administrators for electronic voting. Bachelor thesis, Massachusetts (EVOC) Institute of Technology, Boston, USA, 1999.

R. Joaquim, A. Zuquete, and P. Ferreira REVS a robust electronic voting system. In IADIS International Conference e-Society 2003, pages 95103, Lisbon, Portugal, 2003

... ...

Outline

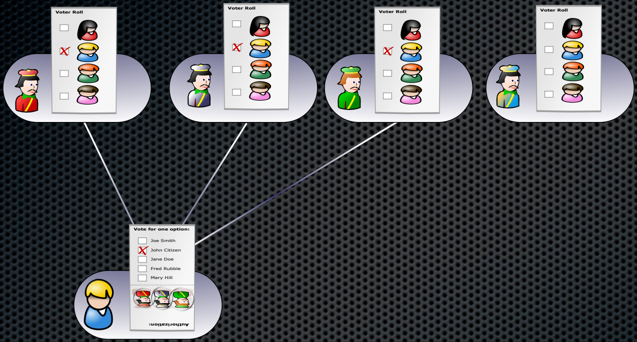
1. Introduction
2. Blind Signature Voting Scheme
3. Multiple Authorities
4. Attack on Democracy
5. Solution
6. Conclusion

Colluding Voters

Imagine...

- 3-voters collude (whereas 3 is our sample threshold out of n=4)
- 3-voters create 4 valid votes.

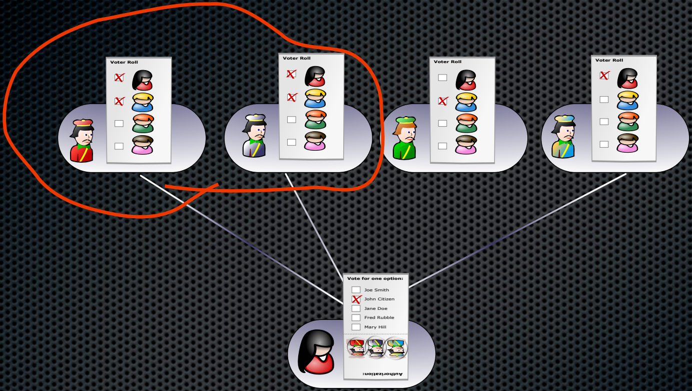
What the Authorities Know



After round 1

- 3 out of 4 authorities signed for voter 1
- 3 out of 4 authority do 'know' about voter 1

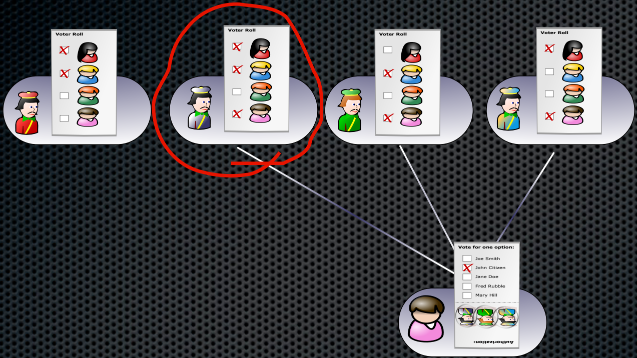
What the Authorities Know



After round 2

- 3 out of 4 authorities signed for voter 2
- 2 out of 4 authorities 'know' about both voters

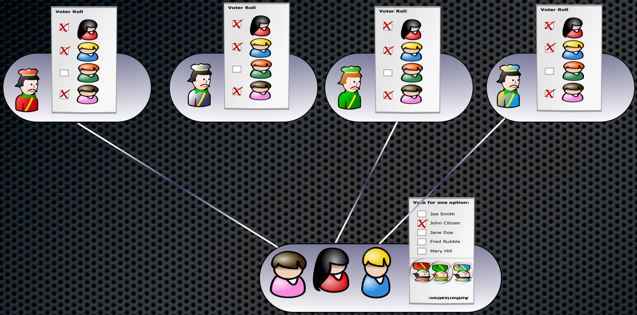
What the Authorities Know



After round 3

- 3 out of 4 authorities signed for voter 3
- only 1 authority 'knows' about all voters

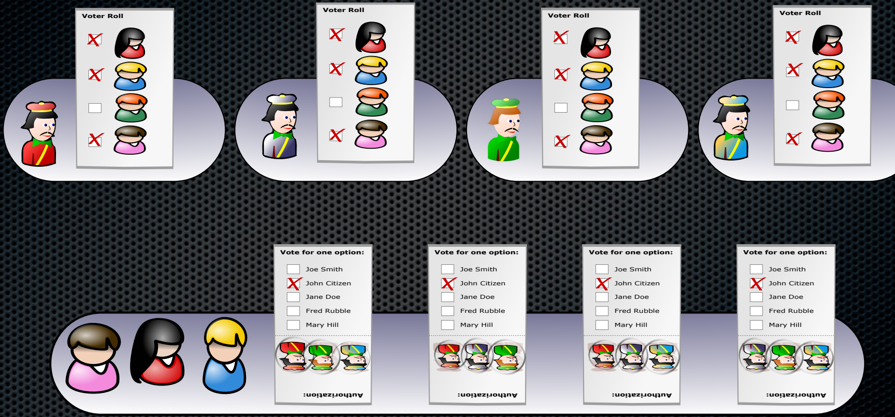
Breaking Democracy



After round 4

- The colluding three voters have a fourth vote signed
- 3 Voters Generated 4 Valid Votes

Breaking Democracy



After round 4

- The colluding three voters have a fourth vote signed
- 3 Voters Generated 4 Valid Votes

Impact on Democracy

Definition

v_+ = Amount of additional valid votes
N = Amount of authorities available
t = Threshold (Amount of authorities needed to get a valid vote)
V_c = Amount of colluding voters

In general

$$v_+ = \lfloor \frac{N-t}{t} V_c \rfloor$$

In our example, where $N = 4$ and $t = \frac{3}{4}N = 3$ and $V_c = 3$

$$v_+ = \frac{V_c}{3} = 1$$

In an example, where $t = \frac{2}{3}N$ and $V_c = 1000$

$$v_+ = \frac{V_c}{2} = 500$$

Outline

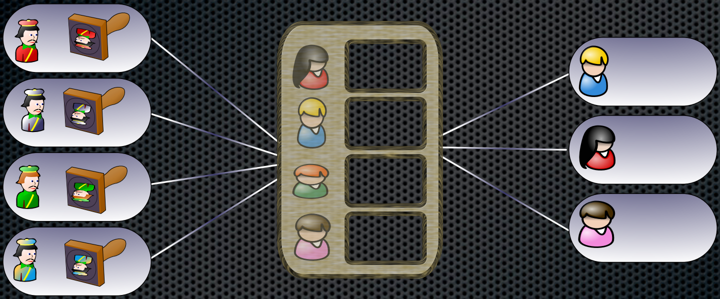
1. Introduction
2. Blind Signature Voting Scheme
3. Multiple Authorities
4. Attack on Democracy
5. Solution
6. Conclusion

Public Bulletin Board

Common knowledge

- The knowledge of each authority must be universally accessible

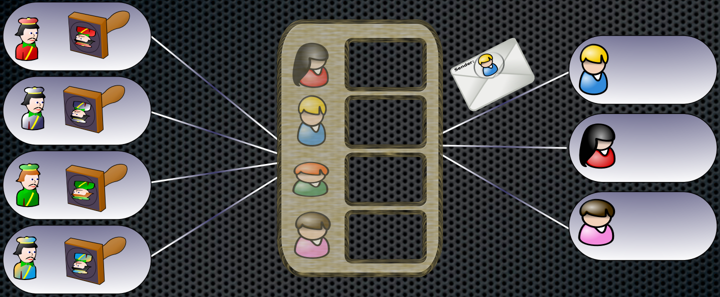
Graph of Knowledge



Common knowledge

- The public board manages the voter roll

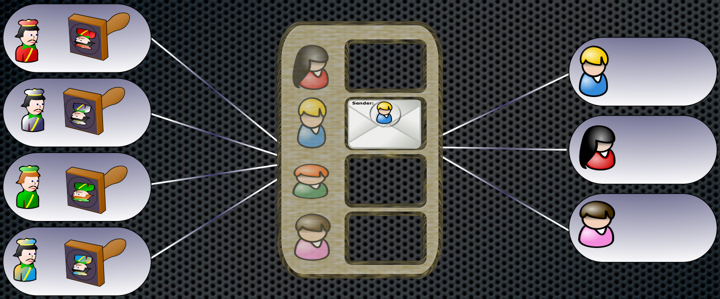
Granting The Right to Vote



The voter...

- ...transfers the blinded vote to the public board

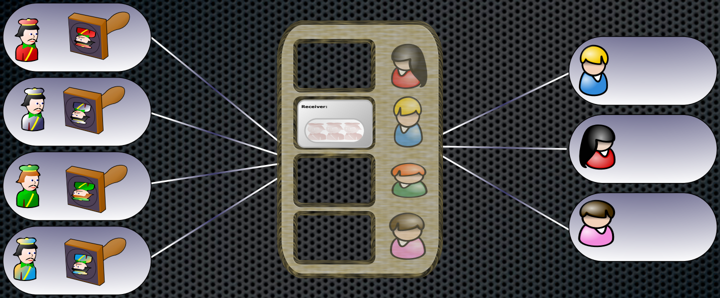
Granting The Right to Vote



The public board...

- ...accepts one vote per voter only

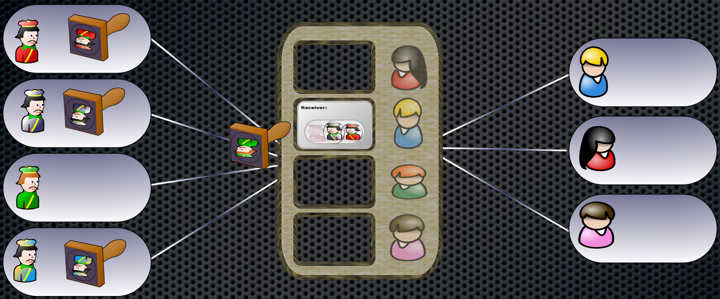
Granting The Right to Vote



The authorities...

- blindly sign the vote on the public board

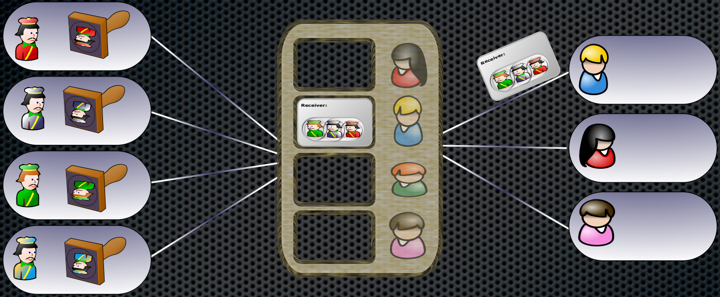
Granting The Right to Vote



The authorities...

- blindly sign the vote on the public board

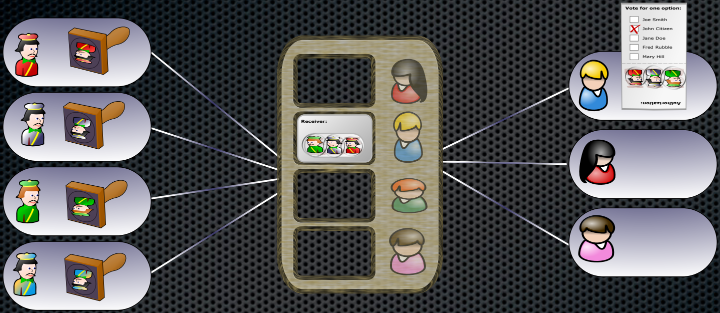
Granting The Right to Vote



The voter...

- ...copies the blindly signed vote from the public board
- ...casts the signed vote.

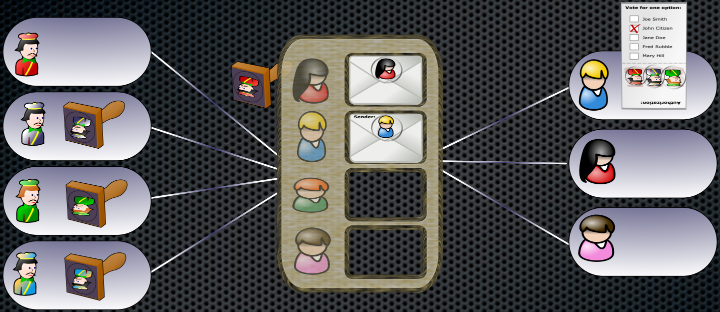
Granting The Right to Vote



The voter...

- ...copies the blindly signed vote from the public board
- ...casts the signed vote.

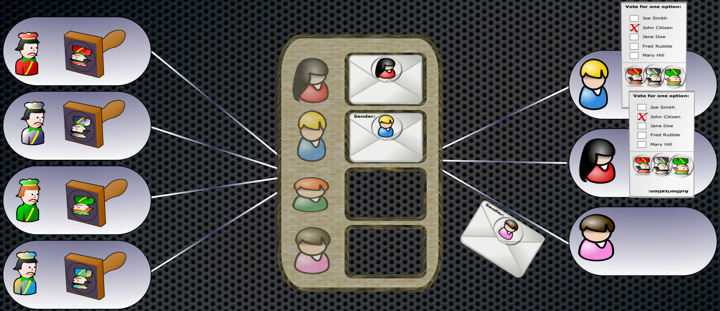
Granting The Right to Vote



Every eligible voter...

- ...gets the signature this way

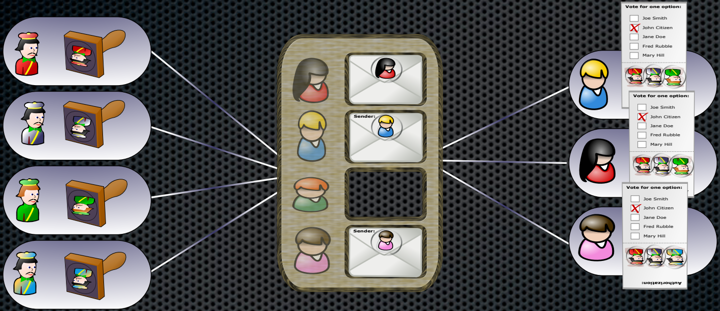
Granting The Right to Vote



After 3 rounds 3 voters...

- ...voted and can not do so a fourth time.

Granting The Right to Vote



After 3 rounds 3 voters...

- ...voted and can not do so a fourth time.

Modified threshold RSA-blind signature scheme maintaining democracy

Possible Threshold-Aware RSA-Blind Signature Scheme (using the same blinding-factor for every signer)

$$
\begin{aligned}
&V \rightarrow PB : v' = v r^{e_1 \cdots e_N}\\
&PB \leftrightarrow A_1 : s'_1 = v'^{d_1} = v^{d_1} r^{e_1 \cdots e_N d_1} = v^{d_1} r^{e_2 \cdots e_N} = v^{d_1} R_1\\
&\vdots\\
&PB \leftrightarrow A_t : s'_t = v'^{d_t} = v^{d_t} r^{e_1 \cdots e_N d_t} = v^{d_t} r^{e_1 \cdots \cancel{e_t} \cdots e_N} = v^{d_t} R_t\\
&V \leftarrow PB : \{s'_1, \ldots, s'_t\}\\
&V : s_1 = s' r^{-(e_2 \cdots e_N)} = v^{d_1} R_1 R_1^{-1} = v^{d_1}\\
&\vdots\\
&V : s_t = s' r^{-(e_1 \cdots \cancel{e_t} \cdots e_N)} = v^{d_t} R_t R_t^{-1} = v^{d_t}\\
&V \rightarrow B : (v, \{s_1, \ldots, s_t\})
\end{aligned}
$$

Outline

1. Introduction
2. Blind Signature Voting Scheme
3. Multiple Authorities
4. Attack on Democracy
5. Solution
6. Conclusion

Conclusion

Findings

- Blind signature schemes (RSA as well as ElGamal) are ready for single authority signature for a any information
- E-Voting protocols are not allowed to contain any single point of failure
- Maintaining democracy in threshold blind sig. schemes requires every authority to provably sign the very same information
- It is possible to render the blind signature schemes safe for democracy by using a public bulletin board

BUT: The prised simplicity of blind signature schemes does not longer hold true.