

A Protocol for Anonymous and Accurate E-Polling

Danilo Bruschi Andrea Lanzi Igor Nai Fovino

Dipartimento di informatica e Comunicazione,
Università degli studi di Milano, via Comelico 39/41,
I-20135 Milano MI, Italy
bruschi@dico.unimi.it, andrew@security.dico.unimi.it, nai@dico.unimi.it

TCGOV, TED CONFERENCE ON E-GOVERNMENT, 2005



Table of content

- 1 E-polling system
 - E-polling vs E-voting
- 2 Protocol introduction
 - Protocol Objects
 - Protocol mechanisms
- 3 Credential system
 - Credential system definition
 - Type of anonymous credentials
 - Credential system mechanism



Table of content

- 1 E-polling system
 - E-polling vs E-voting
- 2 Protocol introduction
 - Protocol Objects
 - Protocol mechanisms
- 3 Credential system
 - Credential system definition
 - Type of anonymous credentials
 - Credential system mechanism



Table of content

- 1 E-polling system
 - E-polling vs E-voting

- 2 Protocol introduction
 - Protocol Objects
 - Protocol mechanisms

- 3 Credential system
 - Credential system definition
 - Type of anonymous credentials
 - Credential system mechanism



Table of content

- 4 Correctness Analysis
 - One time credential
 - Weak Accuracy
 - Privacy property
- 5 Architecture prototype
 - Architecture prototype
- 6 Future works



Table of content

- 4 Correctness Analysis
 - One time credential
 - Weak Accuracy
 - Privacy property
- 5 Architecture prototype
 - Architecture prototype
- 6 Future works



Table of content

- 4 Correctness Analysis
 - One time credential
 - Weak Accuracy
 - Privacy property

- 5 Architecture prototype
 - Architecture prototype

- 6 Future works



E-polling vs E-voting

E-polling vs E-voting

Any e-democracy system should provide means for stimulating citizens participation:

- The *E-polling system* is a fundamental component of any e-democracy and it is used by people to express their opinion.
- The *E-voting system* is another component used by people to express their vote. In e-voting the proof of the properties is more restricted than e-polling systems.



E-polling properties

E-polling properties

- **Democracy:** the voters can vote only once, and only the voters can vote.
- **Weak Accuracy:** The system can tolerate some errors on the votes without compromising the final result.
- **Privacy:** votes remain anonymous.



E-voting properties

E-voting properties

- **Democracy:** the voters can vote only once, and only the voters can vote.
- **Accuracy:** beside to guarantee that the vote cannot be tampered (a voter's vote cannot be altered, duplicate, or removed without being detected), in these systems, must exist some mechanisms to avoid the selling of the vote and to be sure that really a voter performs the vote.
- **Privacy:** votes remain anonymous.



Protocol Objects

Protocol Objects

- **Voter**: the subject interested in participating to a polling.
- **Polling Server**: the unit that collects the votes.
- **Trusted Third Party (TTP)**: an entity which guarantees the eligibility of a voter and releases the vote certificate.
- **Anonymous credential**: this object is used to provide several properties: *Anonymous* and *Democracy* properties.
- **Vote Certificate**: a digital certificate which witnesses the eligibility of a user to participate to a polling session.



Prevoting phase

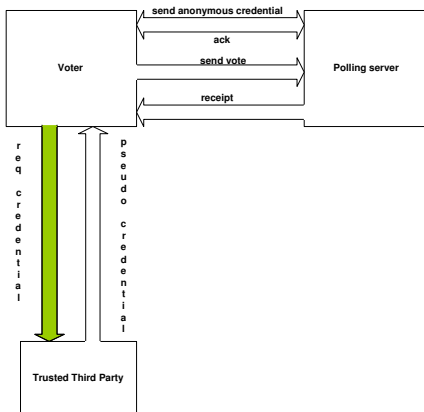
Prevoting phase

This phase has to be completed by the *voters* before the voting phase, it involves the *voters* and the *Trusted Third Party* (TTP) and it follows these steps:

- the *Voter* performs the face to face authentication with Trusted Third Party.
- the *Trusted Third Party* releases to the voter the vote certificate (i.e a random number) used by the voter to unlock the pseudo credential.



Protocol scheme

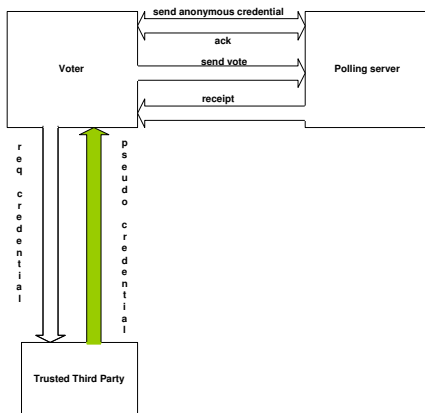


Protocol Phases

- 1 Request credential
- 2 Send pseudo credential
- 3 Send anonymous credential
- 4 Send Vote
- 5 Send the receipt



Protocol scheme

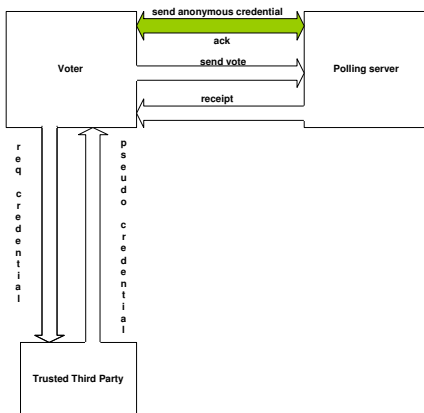


Protocol Phases

- 1 Request credential
- 2 Send pseudo credential
- 3 Send anonymous credential
- 4 Send Vote
- 5 Send the receipt



Protocol scheme

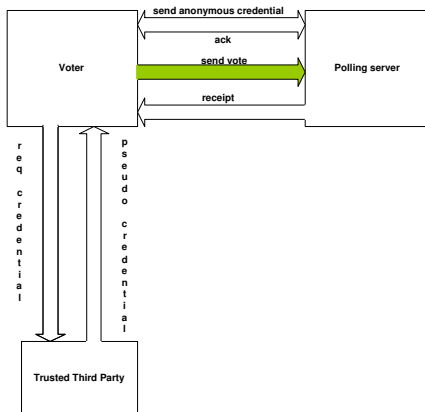


Protocol Phases

- 1 Request credential
- 2 Send pseudo credential
- 3 **Send anonymous credential**
- 4 Send Vote
- 5 Send the receipt



Protocol scheme

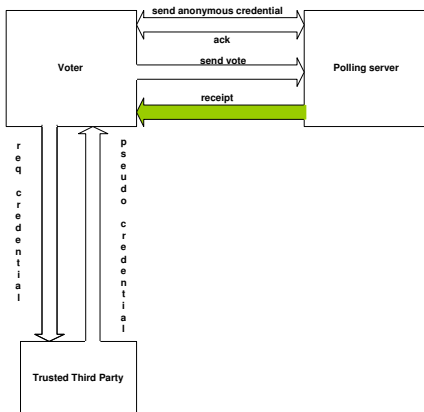


Protocol Phases

- 1 Request credential
- 2 Send pseudo credential
- 3 Send anonymous credential
- 4 **Send Vote**
- 5 Send the receipt



Protocol scheme



Protocol Phases

- 1 Request credential
- 2 Send pseudo credential
- 3 Send anonymous credential
- 4 Send Vote
- 5 **Send the receipt**



Credential system definition

The Credential system is composed by two objects and one mechanism:

objects and mechanism

- **Pseudo credential:** this is the first object yielded by the protocol.
- **Anonymous credential:** this is the object used by the voter to perform the voting phase.
- **Blind signature:** this mechanism is used to guarantee the anonymous property about the pseudo credential.



Pseudo credential

In the protocol there are two kind of credentials and they are used in two different steps of the protocol:

Pseudo credential

This credential is required in the first step of the protocol and it is transformed by a voter in anonymous credential. It is built by TTP and composed by one field:

A random number released by TTP to a voter during the prevoting phase multiply for a credential signed by Trusted Third Party. The random number is used to lock the anonymous credential.



Anonymous credential

Anonymous credential

This credential is required to perform the vote phase and it provides the anonymous property to the voter. It is composed by two fields:

- **cred**: the credential chosen by the voter.
- **TTP_sign(cred)**: the credential chosen by the voter and signed through the blind signature scheme by Trusted Third Party.



Blind signature

Blind Signature

Beside the objects, the credential system is composed by one important mechanism, the blind signature scheme:

It was introduced by Chaum D. in 1982 [Crypto '82] and it used to sign something without disclosing the signed object to the application that yields the signature.



One time credential

The objects and mechanisms defined in the protocol allow to guarantee the whole properties that the e-polling system has to satisfy.

One time credential

Property 1. A voting credential can be used only once

This property can be violated only if the voter is able to get more the one credential or used a signed credential more times. This is not possible because the TTP releases only a signed credential to the voter and a polling server can track the use of the credential.



Weak Accuracy property

Weak Accuracy property

Property 2. The protocol satisfies the weak accuracy property

This property can be violated in two ways:

- Performing a man middle attack between a client and polling server
- Compromising the polling server itself and modifying the votes

The first attack is not possible because we use an encrypted channel and the second attack is avoided by the release of a receipt to the voter.



Privacy property (1)

In order to preserve the privacy violation we use the two credential system objects and the blind signature scheme.

Privacy property

Property 3. The protocol satisfies the privacy property

In order to satisfy this property we have to preserve two other properties:

- Unlinkability between the random number chosen by the voter to build anonymous credential, and the same random number that has to be signed by a Trusted Third Party.
- To allow the voter to vote in anonymous and authenticated way.



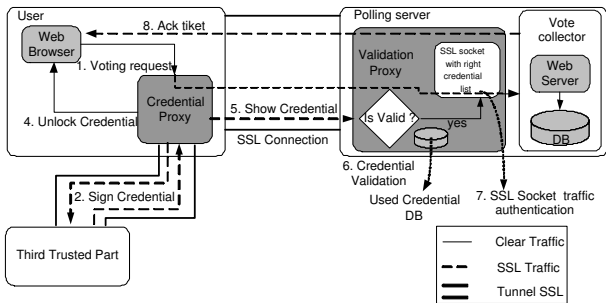
Privacy property (2)

Privacy property (2)

- In order to satisfy the unlinkability between the random number chosen by the voter and signed by a TTP we adopted a blind signature scheme.
- The anonymous and authenticated characteristics are provided by the anonymous credential, this object in fact it doesn't contain any information about the voter and is authenticated by a TTP sign.



Architecture prototype



Future works

- Improving the e-polling protocol to add network privacy (see Anonymous Web transactions with Crowds [Reiter and Rubin 1999 ACM Press]).
- Biometric credential protection.
- Real case study and performance evaluation.

