

GI, the Gesellschaft für Informatik, publishes this series in order

- to make available to a broad public recent findings in informatics (i.e. computer science and information systems)
- to document conferences that are organized in cooperation with GI and
- to publish the annual GI Award dissertation.

Broken down into the fields of "Seminars", "Proceedings", "Monographs" and "Dissertation Award", current topics are dealt with from the fields of research and development, teaching and further training in theory and practice. The Editorial Committee uses an intensive review process in order to ensure the high level of the contributions.

The volumes are published in German or English

Information: <http://www.gi-ev.de/service/publikationen/lni/>

The 2006 conference on Electronic Voting took place in Castle Hofen near Bregenz at the wonderful Lake Constance from 2<sup>nd</sup> to 4<sup>th</sup> of August. This volume contains the twenty papers selected for the presentation at the conference out of more than forty submissions. To assure scientific quality, the selection was based on a strict and anonymous review process. The papers cover the following subjects: e-voting experiences, social, legal, political, democratic and security issues of e-voting, as well as solutions on how to (re)design election workflows, and finally how to implement and observe electronic voting systems.



Robert Krimmer (Ed.): Electronic Voting 2006

P-86

# GI-Edition

## Lecture Notes in Informatics

Robert Krimmer (Ed.)

# Electronic Voting 2006

2<sup>nd</sup> International Workshop  
Co-organized by Council of Europe,  
ESF TED, IFIP WG 8.5 and E-Voting.CC

August, 2<sup>nd</sup> – 4<sup>th</sup>, 2006  
in Castle Hofen, Bregenz, Austria

# Proceedings



# Coercion-Resistant Electronic Elections with Observer

Jörn Schweisgut

Mathematical Institute  
University of Giessen  
Arndtstraße 2  
D-35392 Giessen, Germany  
Joern.Schweisgut@math.uni-giessen.de

**Abstract:** We introduce an electronic election scheme, that is coercion-resistant, a notion introduced by Juels et al. in [JCJ05]. In our scheme we encrypt the credentials that serve as an authorisation to vote during registration. By using a MIX-cascade we can omit one time-consuming plaintext equivalence test in the tallying. In addition, the observer facilitates registration and voting for the benefit of the voter. Pseudonymisation of the ciphertexts during the voting period implies a permanent secrecy of the submitted votes.

## 1 Introduction

In 2000 Hirt and Sako [HS00] presented the first electronic voting scheme in which voters were not able to prove their voting decision. This so-called receipt-freeness was achieved under the unrealistic assumption of an untappable channel from each authority to each voter. To solve this problem, Magkos et al. [MBC01] introduced an election scheme in 2001 which is based on a tamper-proof device, a so-called observer. That system has been improved in the following in [Sch06].

Besides the long unsolved problem of receipt-freeness, there are further possibilities for an attack on electronic elections, which were described by Juels et al. in [JCJ05] in 2005. They summed up these attacks by the notion of coercion-resistance and proposed a first coercion-resistant voting scheme. In this paper, an election scheme is presented, which is based on the usage of credentials as a proof of authorisation to vote. The tallying is more efficient than in the scheme by Juels et al. and minimises the voter's effort in the registration and voting phase by employment of an observer.

Even if the encryption was broken the receipt-freeness would be lost but the secrecy of the votes could be guaranteed due to the pseudonymisation, nevertheless.

## 2 An efficient coercion-resistant observer-based election scheme

For the sake of concreteness, we describe in our paper an electronic voting scheme with a non-malleable ElGamal encryption. The scheme also works with other encryption-systems, e.g. Cramer-Shoup (cp. [CS98]) or Modified-ElGamal (cp. [JCJ05]).

### 2.1 Setup

The MIX-servers define together a multiplicative group  $G$  with prime order  $|G|=:q$  and a generator  $g$  of  $G$ . Then they all generate an ElGamal key pair  $(s, h)$  with  $h=g^s$  (cp. [Ped91]). Each authority  $A_j$  receives a share  $s_j$  of  $s$  in a  $(t, n)$ -threshold secret-sharing-scheme and is publicly committed to this share by  $h_j = g^{s_j}$ . This key  $h$  is published as the public-key of the voting-authorities.

### 2.2 Registration

Each voter  $V_i$ , ( $i=1, \dots, n$ ), is informed by the authorities, goes to the registration office and authenticates himself towards the registrars. Then the observer is given to the voter.

The voter chooses a random value  $z_V \in_R Z_q$  and computes  $h_V = g^{z_V}$  as a public share of  $z_V$ . This value  $h_V$  is stored on the observer. It is important that the observer itself does not know  $z_V$ .

The registrars create a probabilistic encryption  $E(\sigma)$  of a random string  $\sigma \in_R G$  with the public-key  $h$  of the authorities in a distributed threshold manner (cp. [GJKR99]). This ciphertext is transferred to the voter and stored on the voter's observer. The registration authorities re-encrypt  $E(\sigma)$  and prove to the voter, that the obtained value  $E'(E(\sigma))$  is a correct re-encryption of the transferred ciphertext. In order to prevent the voter from transferring this proof we therefore use a designated-verifier proof (cp. [JSI96]). In addition to  $E(\sigma)$  the voter creates a fake credential  $\sigma'$  and encrypts it with the public-key of the voting authorities. This value is also stored on the observer as well as the public-key of the authorities.

At the end of the registration-phase a list  $V$  of the voter's credentials is published by the registrars via a robust, verifiable decryption-MIX-cascade of the voting authorities.

### 2.3 Voting

The votes are decrypted by the MIX-cascade in the tallying and published as plaintexts. Therefore, we can choose a representation of the candidates that enables us to simply tally the votes by adding the values. The candidates are described in a number system with the number of candidates  $n_L$  as its basis. Let be  $L = (m_1, \dots, m_{n_L}) = (1, n_L, n_L^2, \dots, n_L^{n_L-1})$  the set of candidates.

Each voter chooses random numbers  $a, a' \in_R Z_q$  and encrypts his candidate choice  $m$  out of  $L$ :  $(x, y) = (g^a, h^a m)$ . Furthermore, he computes  $g^{a'}$ . These values are sent to the observer which chooses random values  $b, b' \in_R Z_q$  and re-encrypts the ciphertext:

$$(x', y') = (g^b g^a, h^b h^a m).$$

In addition to this, the observer re-encrypts the stored ciphertext  $E(\sigma)$  of the credential with the public-key of the authorities and obtains  $E''(E(\sigma))$ . It calculates  $g^{a'+b'}$  and the necessary value for the non-malleability

$$b \cdot H(g, x', y', g^{a'+b'}, E''(E(\sigma))) + b'.$$

The cryptographic hash-function  $H$  serves as a challenge in the non-interactive zero-knowledge proof of non-malleability.

The observer sends

$$(x', y', g^{a'+b'}, b \cdot H(g, x', y', g^{a'+b'}, E''(E(\sigma))) + b', E''(E(\sigma)))$$

to the voter.

If the observer works correctly the voter can compute  $(g^b, h^b)$  from it. Then the voter can complete the non-interactive zero-knowledge-proof of non-malleability and independent vote-creation respectively:

$$(a+b)H(g, x', y', g^{a'+b'}, E''(E(\sigma))) + (a'+b').$$

Without any knowledge of the used values  $a$  and  $b$  it is impossible to create this message (cp. [TY98]).

In order not to stress the measure of confidence in the observer, the observer proves correct encryption in a designated-verifier proof to the voter.

The voter has to prove publicly, that he has encrypted a valid candidate choice. This can be done e.g. by a non-interactive witness-indistinguishable proof  $P$  (cp. [CDS94]). If not, he could cast any message as a vote, which would not be tallied, but its value could be used as a receipt towards a coercer. This does not mean that the voter cannot void his vote. It is possible that one option on the candidate list is "cancel vote".

Then the encrypted non-malleable ElGamal message together with the encrypted credential as an authorisation and the proof  $P$  is:

$$E(m) = (x', y', g^{a'+b'}, (a+b)H(g, x', y', g^{a'+b'}, E''(E(\sigma))) + (a'+b'), E''(E(\sigma)), P).$$

The voter sends all this to the electronic bulletin board, a publicly readable memory to which everyone can append but not erase or alter data.

Therefore, the zero-knowledge proof of non-malleability and the proof of a correct candidate choice are publicly verifiable.

The messages from the voters to the bulletin board have to be sent via an anonymous channel. Such a channel can be achieved by employment of a MIX-cascade. To guarantee a permanent secrecy of the votes, the messages from the voters have to be secured by enabling voters to cast ballots in public places or from any point of the net. Thereby, the votes are mixed with other ones even if the encryption and thus the anonymity of the MIX-cascade is broken.

## **2.4 Tallying**

Votes without a valid zero-knowledge proof of non-malleability or without a valid proof  $P$  are ignored. According to a predetermined policy, the votes are ignored that have been cast together with equal credentials, i.e. equivalent credential ciphertexts. That means that at most one vote per credential will be tallied. To decide whether two ciphertexts are encryptions of the same underlying credential, a pairwise plaintext equivalence test (cp. [JJ00]) is used. Afterwards the votes pass the verifiable robust decryption-MIX-cascade. Thereby, the parts of the message that include the credential and the vote are not separately but synchronously permuted. The output of the MIX-cascade is a randomly permuted list of pairs, each pair consisting of a plaintext-vote and a credential. The credentials are compared with the list  $V$  of authorised credentials. Votes without valid credentials are deleted. The remaining votes are publicly tallied.

## **3 Criteria and Analysis**

Up to now there have been no common criteria for democratic electronic elections. But it would be wise if the electronic elections fulfil at least the requirements that are set on conventional secret ballot elections. In addition there are some further requirements that derive from the media (e.g. correctness, verifiability, non-malleability and coercion-resistance).

The described voting scheme fulfils all the demands that are put up for traditional secret ballot election and to a great extent the requirements that have been set up for electronic voting schemes so far.

### **3.1 Authorization, Unforgeability, Single vote**

The verification of the authorization and the unforgeability of votes are guaranteed by comparing the credentials with the list of valid credentials. After the registration the valid credentials are anonymised and published via a verifiable MIX-cascade. With this list, everybody can check if a message comes from an authorized voter, but it is impossible to find out from which one. Unauthorized messages are ignored.

The unforgeability of votes is based on the security of the scheme used to encrypt the credentials. Such public-key encryptions are not indefinitely secure. On the other hand one does not need a perfect secure encryption (i.e. a one-time-pad) as a break of the scheme is only advantageous for an adversary in the period before the actual tallying.

If only the first cast votes with correct credentials are considered for the tallying and later submitted votes of the same voter are declared invalid and are erased, then it is guaranteed that one voter can only cast one valid vote.

### **3.2 Verifiability**

As the bulletin board is publicly readable, everybody can prove the non-malleability (independent vote-creation) and that the votes contain valid elements of the candidate list. The plaintext-equivalence-tests for the encrypted credentials to prevent double-voting are also publicly verifiable. During the tallying the votes are sent through a MIX-cascade and decrypted. So the actual tallying can be done by everyone. This means that the verifiability of the voting schemes derives directly from the verifiability of the MIX-cascade.

### **3.3 Correctness**

The correctness of the tallying is guaranteed if all voters are able to cast the vote of their choice, i.e. all voters can understand and check the encryption of the observer. This is ensured by the designated-verifier- and the witness-indistinguishable-proof, the verifiability of the MIX-cascade and the public tallying of the plaintext votes.

### **3.4 Honesty, Robustness**

A dishonest voter is not able to submit an invalid vote that is accepted and tallied. On the one hand he has to include a proof, that the cast vote contains a valid candidate choice. On the other hand the votes are decrypted and invalid votes will be ignored.

It is due to the verification of each action of each MIX-Server that fraudulent authorities can be identified and excluded. As long as there are not more than a certain threshold of dishonest MIX-servers the election can be completed without them. Therefore the voting scheme is robust.

### **3.5 Expenses**

The complexity of communication depends on the used proofs, i.e. the designated-verifier proof, the zero-knowledge-proof of non-malleability and the witness-indistinguishable-proof of the valid choice. These proofs can be efficiently implemented and the communication costs are independent of the number of authorities as well as of the number of candidate choices.

The registration can be done for several elections. The efforts on the side of the voters are acceptable.

### **3.6 Anonymity**

The anonymity of each voter is guaranteed if the used credential cannot be traced back to the voter. That is the case in this voting scheme, as the votes are cast via an anonymous channel (MIX-cascade) *and* the voters can cast their votes from any point of the net. It is impossible to find out which choice a voter has made, even whether a specific voter has cast a vote.

Only those who know the credential of a voter prior to the tallying may find out *if* a voter has submitted his message. Assuming that the used encryption would be broken anytime after the tallying, then the credentials and the anonymous channel still conceal the relation between the votes and the voters - as long as the voter has not given his correct credential away prior to the tallying.

### **3.7 Independent vote-creation**

It is impossible to copy a vote of another voter, because he has to prove in zero-knowledge that he knows the randomness used to encrypt the vote. Due to the non-malleability (i.e. chosen-ciphertext-security) of the encryption, it is impossible for an adversary to cast a vote that bears a known relation to a vote of another voter.

### **3.8 Coercion-resistance**

The voting scheme is receipt-free, i.e. it is impossible that a voter creates a receipt which indicates his choice. If he was able to create one, he would be coercible or corruptible. It is even thinkable that the voter is controlled by an adversary and casts the vote the adversary wants him to. As long as he uses a fake credential, this vote will not be tallied and the voter can still cast his vote he wants to. In addition to that, the scheme is secure against a randomization attack as it is possible in [HS00], because only *one* candidate choice has to be encrypted to construct and cast a vote. It is not even noticeable if a voter has cast a vote and that is why it is impossible to force a voter to abstain from the election. Therefore the scheme is coercion-resistant.

## **4 Conclusion**

The electronic voting scheme fulfils the requirements set on democratic electronic elections in section 3 including coercion-resistance.

If the encryption-key of the authorities was compromised, the pseudonymisation would guarantee the secrecy of the votes, unless the voter publishes his pseudonym before the actual tallying takes place.

The observer does not fulfil the "classical" tasks of an observer (cp. [CP92] and [CP93]) but it rather serves as a convenient and secure transport.

If an adversary forces a voter to hand over his observer, then the voter can give him a wrong PIN. That results in the fact that the observer uses the fake-credential. The voter is able to vote without observer even if the adversary has tried to vote with his observer before.

By using the encryption of credentials and the MIX-cascade for the generation of the list of authorised credentials, we can omit one of the time-consuming plaintext-equivalence tests during the tallying.

Only the plaintext-credentials have to be compared.

## References

- [CDS94] Ronald Cramer, Ivan Damgård and Berry Schoenmakers: Proofs of Partial Knowledge and Simplified Design of Witness Hiding Protocols. In Yvo Desmedt, editor, *CRYPTO '94*, LNCS 839, pages 174-187. Springer, 1994.
- [CP92] David Chaum and Torben P. Pedersen: Wallet Databases with Observers: In *CRYPTO '92*, LNCS 740, pages 89-105. Springer, 1992.
- [CP93] Ronald Cramer and Torben P. Pedersen: Improved Privacy in Wallets with Observers (Extended Abstract): In *EUROCRYPT '93*, LNCS 765, pages 329-343. Springer, 1993.
- [CS98] Ronald Cramer and Victor Shoup: A Practical Public Key Cryptosystem Provably Secure Against Adaptive Chosen Ciphertext Attack: In Hugo Krawczyk, editor, *CRYPTO '98*, volume 1462 of *LNCS 1462*, pages 13-25. Springer, 1998.
- [GJKR99] Rosario Gennaro, Stanislaw Jarecki, Hugo Krawczyk, and Tal Rabin: Secure Distributed Key Generation for Discrete-Log Based Cryptosystems: In *EUROCRYPT '99*, pages 295-310, 1999.
- [HS00] Martin Hirt and Kazue Sako: Efficient Receipt-Free Voting Based on Homomorphic Encryption: In *EUROCRYPT '00*, LNCS 1807, pages 539-556. Springer, 2000.
- [JCJ05] Ari Juels, Dario Catalano, and Markus Jakobsson: Coercion-Resistant Electronic Elections: In *WPES '05*. ACM CCS, November 2005.
- [JJ00] Markus Jakobsson and Ari Juels: Mix and Match: Secure Function Evaluation via Ciphertexts: In Tatsuaki Okamoto, editor, *ASIACRYPT '00*, LNCS 1976, pages 162-177. Springer, 2000.
- [JSI96] Markus Jakobsson, Kazue Sako, and Russell Impagliazzo: Designated Verifier Proofs and Their Applications: In *EUROCRYPT '96*, LNCS 1070, pages 143-154. Springer, 1996.
- [MBC01] Emmanouil Magkos, Mike Burmester, and Vassilios Chrissikopoulos: Receipt-Freeness in Large-Scale Elections without Untappable Channels: In *I3E '01*, IFIP Conference Proceedings 202, pages 683-694. Kluwer, 2001.
- [Ped91] Torben P. Pedersen: Non-interactive and information-theoretic secure variable secret sharing: In *CRYPTO '91*, pages 129-140, 1991.
- [Sch06] Jörn Schweisgut: Effiziente elektronische Wahlen mit Observer: In *GI - Sicherheit 2006*, LNI Proceedings P-77. Gesellschaft für Informatik e.V. (GI), February 2006.
- [TY98] Yiannis Tsiounis and Moti Yung: On the Security of ElGamal Based Encryption: In *PKC '98*, LNCS 1431, pages 117-134. Springer, 1998.