periodica polytechnica

Electrical Engineering
51/3-4 (2007) 141–146
doi: 10.3311/pp.ee.2007-3-4.08
web: http://www.pp.bme.hu/ee

RESEARCH ARTICLE

A secure electronic voting scheme

Andrea Huszti

Received 2007-12-03

Abstract

In this paper a new electronic voting scheme is described which guarantees coercion-resistance as well as privacy, eligibility, unreusability and verifiability. The proposed protocol can be implemented in practical environment, since it does not require untappable channel or voting booth, only anonymous channels are applied.

Keywords

electronic voting · cryptographic protocols · receipt-freeness · coercion-resistance

Andrea Huszti

Faculty of Informatics, University of Debrecen, P.O. Box 12, H-4010 Debrecen,

Number Theory Research Group, MTA, Hungary

e-mail: ahuszti@inf.unideb.hu

1 Introduction

The research on electronic voting is a very important topic for the progress of democracy. If a secure and convenient electronic voting system is provided, it will be used more frequently to collect people's opinion for many kinds of political and social decisions through cyber space. Traditional paper-based voting can be time consuming and inconvenient. Electronic voting not only accelerate the whole process, but makes it less expensive and more comfortable for the voters and the authorities as well. It also reduces the chances of errors. Electronic voting schemes should provide all basic features that conventional voting does, further should furnish more services in order to make the process more trusted and secure.

Many extensive researches have been conducted on the subject. The literature provides three basic cryptographic approaches for secure electronic voting.

Voting schemes based on homomorphic encryption. Let $\mathcal{PT}$ be the plaintext space and $\mathcal{CT}$ the ciphertext space such that $\mathcal{PT}$ is a group under the operation $\oplus$ and $\mathcal{CT}$ is a group under the operation $\otimes$. Let $E_r(m)$ denote encryption of the message m using random parameter r. An encryption scheme is $(\otimes, \oplus)$-*homomorphic*, if for given $c_1 = E_{r_1}(m_1)$ and $c_2 = E_{r_2}(m_2)$, there exists an r such that

$$c_1 \otimes c_2 = E_r(m_1 \oplus m_2).$$

The first homomorphic encryption voting scheme was proposed in [6]. For further references we refer to [4],[8],[11],[12],[13].

Voting schemes based on mix-nets. Main idea of mix-nets is to permute and modify some sequence of objects in order to hide the correspondence between elements of the original and the final sequence. Servers of mix networks encrypt, permute and re-encrypt the sequences of input elements, it is crucial that one of the servers must be trusted. See [1],[5],[7],[16].

Voting schemes based on anonymous channels. These schemes are very popular in practice due to their efficiency and their support for any type of encryption. Anonymous

channels are used to conceal the identity of the sender. Usually ballots and identifying material are passed through anonymous channels. Schemes using anonymous channels several times use blind signatures, [5],[1–3, 9, 10, 15].

1.1 Previous work

In traditional elections, a voting booth not only allow voters to keep their vote secret, but it prevents vote-buying and coercion. The notions of *receipt-freeness* and *uncoercibility* were introduced by Benaloh and Tuinstra [6]. Roughly stated, receipt-freeness is the inability of a voter prove to an adversary that he voted in a particular manner, even if the voter wishes to do so. For formal definition see [10]. The property of receipt-freeness ensures that an attacker is not able to trace back voter's exact behaviour, therefore a vote-buyer (coercer) does not obtain a reasonable proof. Hirt and Sako [12] showed that [6] does not possess receipt-freeness and introduced a receipt-free voting based on homomorphic encryption. Lee and Kim [13] proposed a receipt-free version of [11] keeping optimal performance, privacy, robustness and universal verifiability. Sako and Kilien [7] proposed a multi-authority receipt-free scheme applying a mix network and also homomorphic encryption for tallying. Mix-net is used for tallying in [16] and at some point during the voting process voters post ballot to the bulletin board via anonymous channel. In [16] property of *coercion-resistance* is introduced. A coercion-resistant scheme gives a possibility for the voter to cheat an adversary who instructs him to vote in a given manner, but the adversary cannot determine whether the voter behaved as instructed, even if the adversary asks the voter to divulge his private keying material or to abstain from voting. Okamoto [9] proposed a voting scheme which he himself later showed to lack the postulated receipt-freeness, a repaired version using blind signatures appears in [10].

Most of the receipt-free schemes in literature make some basic assumptions about the communication channel between the voter and the election authorities. One of the physical assumptions is a *voting booth* [6] that allows a voter secretly and interactively communicate with an authority. A weaker assumption is an *untappable channel* [7, 9, 10, 12] that is a one-way physical apparatus providing perfect secrecy in an information-theoretic sense. Several authors in the literature have pointed out the difficulty of their implementation. Untappable channels also force voters to use specified voting locations.

In our scheme untappable channels or voting booth are not employed, voters use anonymous channels [5] that can be realized in practice using mix-nets. We do not rely on tamper-resistant hardware [14] either in order to achieve receipt-freeness. The proposed protocol does not require any complex cryptographic primitives like zero-knowledge protocols, secret sharing or threshold cryptosystems [8],[11],[4][16]. However, it also provides basic requirements including coercion resistance, verifiability, eligibility, unreusability and privacy.

2 Preliminaries

2.1 Requirements

In order to be functional in practice, an electronic voting scheme has to satisfy not only all the standard features of the conventional paper-based voting methods, but also should provide more efficient voting services. E-voting comparing to the traditional election allows adversaries to intrude the voting process in an easier way, even if there is a small security gap in the design. Thus the scheme should be protected against these techniques, the requirements are as follows:

Eligibility. Only eligible voters can cast votes.

Privacy. All votes remain secret. No coalition of participants not containing the voter himself can gain any information about the voter's vote.

Unreusability. Every eligible voter can cast only one vote.

Fairness. No participants can gain any knowledge about the partial tally before the counting stage. Knowledge of any intermediate result about the election can influence the voters.

Robustness. No voter can disrupt the election, any invalid vote will be detected and not counted in the final tally.

Individual verifiability. Each eligible voter should be able to verify that his vote was committed as intended and made into the final tally as cast.

Universal verifiability. Any participant or passive observer can check that the election is fair, the final result is exactly the sum of the votes.

Receipt-freeness, Uncoercibility. The voter cannot reveal his ballot to any adversary. Before the election someone can bribe the voter with a demand of casting his favourite vote. Receipt-freeness avoids vote-buying. Uncoercibility means that a voter cannot be forced into casting a particular vote by an adversary. During the election a coercer can observe the public information, the communication between the voter and the authorities and can even order the voter how he should behave during the voting process with generating him the random bits.

Definition of receipt-freeness was introduced in [10]: Given published information $\mathcal{X}$ (public parameters and information on the bulletin board), adversary $\mathcal{C}$ interactively communicates with a voter V in order to force V to cast $\mathcal{C}$'s favourite vote c^* to an authority $\mathcal{A}$, and finally $\mathcal{C}$ decides whether to accept $View(\mathcal{X} : V)$ or not, and $\mathcal{A}$ decides whether to accept c^* or not. The coercer gets any message from the bulletin board immediately after it is put on the board. $View(\mathcal{X} : V)$ means published information $\mathcal{X}$, c^* and messages that $\mathcal{C}$ receives communicating with V.

Definition 1. *A voting system is receipt-free, if there exists a voter V, such that for any adversary $\mathcal{C}$ can cast c $(c \neq c^*)$ which is accepted by the authority $\mathcal{A}$ under the condition that $View(\mathcal{X} : V)$ is accepted by $\mathcal{C}$.*

There are several attacks that should be considered in case of electronic voting. Several real-word attacks [16] are enumerated below:

Randomization attack. An attacker coerces a voter to submit randomly formed ballot. In this attack it is not possible to learn what candidate the voter casts a ballot for. The effect of this attack is to cancel the voter's vote with large probability.

Forced-abstention attack. An attacker forces a voter to abstain from voting. This attack happens if an adversary is able to follow who is eligible for voting and who has already voted. Being aware of this knowledge he threatens voters and effectively excludes them from the voting process.

Simulation attack. In this attack an adversary coerces or bribes the voter to reveal his private keying material and then pretends to be the voter and casts his own favourite vote.

Definition 2. *A scheme is called coercion-resistant if it offers not only receipt-freeness, but also defense against randomization, forced-abstention and simulation attacks.*

2.2 Participants

Several participants contribute in an election system. If we had one absolutely reliable authority we would need no more authorities, and the voting process would be very simple. Since the situation is different in practise, the responsibility should be shared among several authorities. It is crucial to consider how much a participant can be trusted. Besides voters only two authorities are necessary for the proposed scheme.

Voters. Let denote voters by $\mathcal{V} = \{V_1, V_2, \ldots, V_n\}$. A voter wants to have the guarantee that his vote is counted in the final tally and if a fraud is suspected there should be a possibility to make his claim. Authorities do not trust voters at all.

Registry. Denoted by $\mathcal{R}$, this authority is responsible for generating private and public keying material, all the information sufficient for voters and the authority in order to complete the voting process. At the end of the process the Registry publishes the final tally.

Voting Authority. Denoted by $\mathcal{A}$, this authority is charged with processing ballots. In essence the Voting Authority manages the election. Voting Authority can also act as a voter.

2.3 Channels

In the proposed scheme various types of communication channels are used. Since this scheme is designed for a real-world environment untappable channel and voting booth are avoided, because of the difficulty of their implementation.

Public channel. Any participant can send a message to any other participant through a public channel. Message sent through this channel can be tapped, and the identity of the sender can be traced back.

Anonymous channel. This channel guarantees the anonymity of the sender. Receiver of the message that has been sent through anonymous channel does not have any information about the identity of the sender. Realization of this channel is described in [5] based on a mix-net approach.

Bulletin board. Bulletin board ($\mathcal{BB}$) is publicly readable. The Registry can write, and nobody can delete or change anything on it. Bulletin board can be considered as a public channel with memory.

2.4 Assumptions

1 The security of the proposed scheme relies on the correctly generated public and secret key pairs for the voters (PK_V, SK_V) and for the Voting Authority (PK_A, SK_A), too. It is also assumed that the Registry gives private key information only to the proper participants.

2 Since the responsibility of the security is shared, we suppose that the Registry and the Voting Authority do not collude. They both follow the steps of the protocol, not providing more information to each other that they are supposed to.

3 An adversary may coerce a voter to cast his vote in a prescribed manner. He can request voter's credential (V_{ID}, SK_V) right after the registration phase and dictates all random parameters (x, a) for the voter.

4 We suppose that voters 'personally' participate in the election. The adversary may not continuously watch over the shoulder of the voter, monitor his hard-drive, etc. During the voting there is a moment when the voter is alone and not being watched. A coercer is able to communicate with a voter right after the registration phase, and before and after the election.

5 The Voting Authority is honest in a sense that it does not collaborate with an adversary, does not give any information about the election and it does not generate spurious votes.

3 The Voting Scheme

3.1 Protocol description

The proposed election procedure consists of three distinctive stages: *Authorizing*, *Voting* and *Tallying*.

During the Authorizing stage the voter authenticates himself and receives his credentials, the Voting Authority gets the voter roll containing the corresponding public keys and all system parameters are generated.

During the Voting stage voters create their ballots. Voting Authority checks eligibility of the voters and if they have already voted before. Voters receive their encrypted ballots signed by the Voting Authority, if a fraud is detected the voter makes a claim. At the end voters pass the corresponding decrypting keys of the encrypted ballots to the Registry. Ballots and bulletin board information are passed through an anonymous channel.

During the Tallying stage the Voting Authority sends encrypted ballots to the Registry. The ballots are being decrypted

and the final results with the votes are listed on the bulletin board. Voters confirm that their ballots are on the bulletin board. If his ballot is not listed correctly, he makes a claim.

During the voting process public and anonymous channels are used and encrypted messages are sent. For the communication between the voters and the Voting Authority instead of higher degree residue encryption the more efficient discrete logarithm encryption is recommended. Let denote an encryption with public key PK by Enc_{PK}.

Let define a candidate slate to be an ordered set of m distinct identifiers $\{c_1, c_2, \ldots, c_m\}$, each of which corresponds to a voter choice, typically a candidate or party name.

3.2 Functions

Several functions are applied in the proposed election scheme. Let denote p a large prime and g an element of $\mathbb{Z}/p\mathbb{Z}$. The details of these functions are as follows:

Voting. Function $vote(V_{ID}, SK_V, x, a, c) \rightarrowtail ballot$ takes the voter's identification number V_{ID}, secret key SK_V, vote c and two randomly chosen parameters x, a as input and outputs the ballot. The form of the ballot is $V_{ID}||r||y$, where

$$r \equiv \mathrm{Enc}_{SK_v}(g)$$
$$y \equiv g^{-x} \pmod{p}$$

and $||$ is the notation of concatenation. This function generates the ballot itself being processed by the Voting Authority.

Eligibility. Function $ifeligible(PK_V, r) \rightarrowtail \{0, 1\}$ takes the voter's public key PK_V and the received element r as input. It returns 1 if

$$\mathrm{Dec}_{PK_V}(r) \equiv g$$

and 0 if the congruence above is not satisfied. This function checks if a voter is eligible for voting or not, *i.e.* if he possesses the proper private keying material V_{ID}, SK_V.

Verification. The function $verify(r, z, s, y) \rightarrowtail \{0, 1\}$ calculates if

$$r^z \equiv g^s \cdot y \pmod{p}$$

congruence holds. It outputs 1 if it is correct and 0 otherwise. This function verifies if s sent by the voter is calculated well and by the same voter who previously *voted* with values y and r, where element z is randomly generated by the Voting Authority.

In the following we discuss each step in more details. Fig. 1 shows the steps of the voting protocol.

3.2.1 Authorizing stage

$$\mathcal{R} \longrightarrow \mathcal{V} : (V_{ID}, SK_V, PK_A)$$
$$\mathcal{R} \longrightarrow \mathcal{A} : (V_{ID}, PK_V)$$

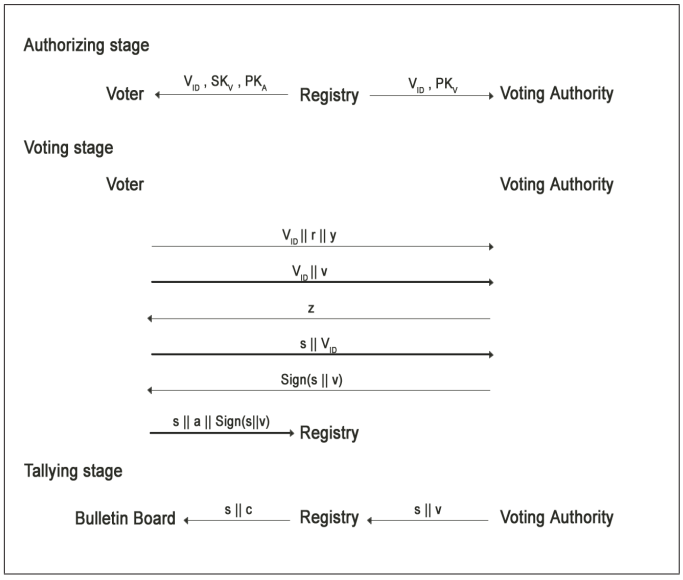

Fig. 1. The voting scheme

Before the voting process the voter must register with Registry verifying his identity. Registry issues a credential to each eligible voter and prepares a list of registered voters. A credential consists of voter's secret key SK_V, an identification number V_{ID}, public key of the Voting Authority PK_A. The voter roll contains key pairs (V_{ID}, PK_V), where PK_V is the public key of the corresponding voter. This list is delivered to the Voting Authority. In this stage all public system parameters are generated and published, such as p, q large primes, where $q|(p-1)$ and $g \in \mathbb{Z}/p\mathbb{Z}$ of order q.

3.2.2 Voting stage

$$\mathcal{V} \longrightarrow \mathcal{A} : \mathrm{Enc}_{PK_A}(V_{ID}||r||y)$$
$$\mathcal{V} \longrightarrow \mathcal{A} : \mathrm{Enc}_{PK_A}(V_{ID}||v)$$
$$\mathcal{A} \longrightarrow \mathcal{V} : \mathrm{Enc}_{PK_V}(z)$$
$$\mathcal{V} \longrightarrow \mathcal{A} : \mathrm{Enc}_{PK_A}(s||V_{ID})$$
$$\mathcal{A} \longrightarrow \mathcal{V} : Sign(s||v)$$
$$\mathcal{V} \longrightarrow \mathcal{R} : \mathrm{Enc}_{PK_R}(s||a||Sign(s||v))$$

The voter chooses random integers a, x, calculates his ballot with function $vote$, encrypts it with the public key of the Voting Authority and sends it. The voter calculates

$$v \equiv y^a \cdot c \pmod{p}$$

concatenates V_{ID} and v and passes it through an anonymous channel. When the Voting Authority receives the message, decrypts it, according to V_{ID} extracts PK_V from the voter roll. Giving PK_V and r to function $ifeligible$ as an input verifies eligibility of the voter. If the voter is eligible for voting it stores all the information, thus the authority can also find out if the voter cast his vote before or not. If the voter is not eligible or

has already cast his vote, the Voting Authority bars the voter out of the election.

Voting Authority generates a random integer z, encrypts it with the voter's public key and sends it. After calculating

$$s \equiv x + zSK_V \pmod{q}$$

the voter concatenates it with V_{ID} and sends it to the Voting Authority using anonymous channel.

After receiving all the information the Voting Authority looks up r, z, y associated to V_{ID} and runs function $verify$. If it returns 0, then the voter is disclosed from the election otherwise the pair (s, v) is signed and sent back to the voter. After confirming the received signature the voter sends it with the decrypting key a and s to the Registry. If a fraud is detected, then he sends $\mathrm{Enc}_{PK_A}(V_{ID}||r||y)$ through a public channel, $\mathrm{Enc}_{PK_A}(s||v||z||V_{ID})$ through an anonymous channel to the Voting Authority. Voting Authority makes sure of the existence of random parameter z and corresponding values and after applying functions $ifeligible$ and $verify$ sends back $Sign(s||v)$.

3.2.3 Tallying stage

$$\mathcal{A} \longrightarrow \mathcal{R} : \mathrm{Enc}_{PK_R}(s||v)$$
$$\mathcal{R} \longrightarrow \mathcal{BB} : (s||c)$$

After the voting phase is finished the Registry receives $(s||v)$ pairs from the Voting Authority, checks validity of the signature received from the voter, computes c from v, publishes the pair of (s, c) and the relevant voting statistics on $\mathcal{BB}$. In this stage the voter confirms if his vote is correctly listed on $\mathcal{BB}$. If the pair (s, c) calculated by the voter is not on $\mathcal{BB}$, then he sends $\mathrm{Enc}_{PK_R}(s||v||a||Sign(s||v))$ through an anonymous channel.

3.3 Security analysis

Theorem 3. *The proposed e-voting scheme is secure, i.e. it satisfies eligibility, privacy, unreusability, fairness, robustness, individual and universal verifiability and coercion-resistance.*

Proof. ***Eligibility.*** During the Authorizing stage a voter is registered only after identifying himself. Only eligible voters receive credential material. Voting Authority ensures eligibility before accepting the ballot by running function $ifeligible$. The Voting Authority cannot impersonate an eligible voter without the official credential issued by the Registry. Therefore, the proposed scheme satisfies eligibility.

Privacy. The vote is encrypted during the process, only in the Tallying stage it is decrypted by the secret key of the Registry. After revealing the votes on $\mathcal{BB}$ and assuming that the Registry and the Voting Authority do not collude, nobody can trace back the identity of the voter.

Unreusability. Each voter possesses different secret key and V_{ID}. If a voter tries to vote with the same credential again the Voting Authority detects it since all the necessary values are stored. Since he cannot generate any other voter's credential, every eligible voter can cast a vote only once.

Fairness. Only in the Tallying stage votes are decrypted, and final results are posted, thus during the voting phase no one has information about any intermediate results.

Robustness. Invalid votes cast by malicious voters are detected in the Tallying stage, after decrypting ballots. These (s, c) pairs are marked as invalid by the Registry, or any party can notice them and ask to do it. No coalition of voters can disrupt the election.

Individual verifiability. In the Tallying stage if a voter cannot find the proper (s, c) pair on $\mathcal{BB}$ makes a claim. Since the $\mathcal{BB}$ is publicly readable voters can make sure of their own ballots. A voter makes a claim in a way that he shows the signature received and checked in the Voting stage.

Universal verifiability. The final tally and all the votes are listed on $\mathcal{BB}$. Anyone can check the correctness of the results, since $\mathcal{BB}$ is readable by everyone and not erasable or changeable by anyone.

Receipt-freeness, Uncoercibility. The coerced voter V wants to cast vote c, while the adversary $\mathcal{C}$ forces the voter to cast his favourite vote c^*. Voter V calculates the necessary values and functions with value c, follows the steps of the protocol, thus $\mathcal{A}$ accepts v and sends (s, v) to $\mathcal{R}$. At the same time V states to $\mathcal{C}$, he cast vote c^*.
In our scheme

$$View(\mathcal{X} : V) : \{V_{ID}, SK_V, x, a, c^*, z^*, s^*\}.$$

We assume $\mathcal{C}$ generates random integers x, a to V and right after the Authorization stage communicating with V coercer $\mathcal{C}$ is aware of V_{ID}, SK_V. Using anonymous channels $\mathcal{C}$ cannot trace back the message was passed by V to $\mathcal{A}$ or $\mathcal{R}$, in other words even if $\mathcal{C}$ calculates $\mathrm{Enc}_{PK_A}(V_{ID}||v)$, $\mathrm{Enc}_{PK_A}(s||V_{ID})$ and $\mathrm{Enc}_{PK_R}(s||a||Sign(s||v))$ is not able to control if V sent the same messages or not. After the election V chooses an (s', c') pair from $\mathcal{BB}$, where $c' = c^*$ and let $s^* = s'$. It is assumed that the moment when V receives z and calculates s the voter is alone and not being watched, hence V can calculate and state to $\mathcal{C}$ z^*, where

$$s^* \equiv x + z^* SK_V \pmod{q}.$$

Since after verifying all the calculations $\mathcal{C}$ accepts $View(\mathcal{X} : V)$, therefore the proposed scheme is receipt-free and uncoercible.

Randomization attack. The randomization attack is prevented, since adversary cannot coerce a voter to cast a different, randomly formed, invalid vote. The adversary cannot verify if the coerced voter has cast the prescribed vote or not.

Forced-abstention attack. Even if an adversary can see the voter roll, *i.e.* the list of registered voters, still he is not able to verify if a certain voter has cast a vote or not. Assuming the Voting Authority does not collude with the coercer, the only information he has is on $\mathcal{BB}$. It is not possible to find out the voter from the listed pairs of (s, c).

Simulation attack. Even if a voter provides his private keying material $(V_I D, SK_V)$ after the Authorizing stage and before the Voting stage, he cannot be coerced by an adversary. An attacker is not able to verify the correctness of the received private keying material.

The proposed scheme satisfies receipt-freeness and protects against randomization, forced-abstention and simulation attack, therefore it is coercion-resistant. □

4 Conclusions

The proposed protocol fulfils requirements for electronic election schemes, such as eligibility, privacy, unreusability, fairness, robustness, individual and global verifiability and coercion-resistance. It is offered to employ it in a small-scale practical environment (e.g. companies), where the authorities participating do not collude and the voting authority do not collaborate with voters. No complex cryptographic primitives are applied, besides easy calculations it computes digital signature and for communication between the participants discrete logarithm encryption (e.g. EL-Gamal) is recommended.

References

1 **Chaum D**, *Elections with unconditionally secret ballots and disruption equivalent to breaking RSA*, Advances in Cryptology - EUROCRYPT '88, LNCS, 1988, pp. 177-182.

2 **Boyd C**, *A new multiple key cipher and an improved voting scheme*, Advances in Cryptology - EUROCRYPT '89, LNCS, 1988, pp. 615-625.

3 **Fujioka A, Okamoto T, Ohta K**, *A practical secret voting scheme for large scale elections*, Advances in Cryptology – ASISACRYPT '92, LNCS, 1992, pp. 244-251.

4 **Iversen KR**, *A cryptographic scheme for computerized general elections*, Advances in Cryptology – CRYPTO '91, LNCS, 1992, pp. 405-419.

5 **Park C, Itoh K, Kurosawa K**, *Efficient anonymous channel and all/nothing election scheme*, Advances in Cryptology – EUROCRYPT '93, LNCS, 1993, pp. 248-259.

6 **Benaloh J, Tuinstra D**, *Receipt-free secret-ballot elections*, Proceedings of the 26th ACM Symposium on the Theory of Computing, ACM, 1994, pp. 544-553.

7 **Sako K, Kilian J**, *Receipt-free mix-type voting schemes – a practical solution to the implementation of voting booth*, Proceedings of EUROCRYPT '95, LNCS, 1995, pp. 393-403.

8 **Cramer R, Franklin M, Schoenmakers B, Young M**, *Multi-authority secret-ballot elections with linear work*, Advances in Cryptology - EUROCRYPT '96, LNCS, 1996, pp. 72-83.

9 **Okamoto T**, *An electronic voting scheme*, Proceedings of IFIP '96, Advanced IT Tools, 1996, pp. 21-30.

10 _____, *Receipt-Free Electronic Voting Schemes for Large Scale Elections*, Proceedings of Workshop of Security Protocols '97, LNCS, 1996, pp. 125-132.

11 **Cramer R, Gennaro R, Schoenmakers B**, *A secure and optimally efficient multi-authority election scheme*, Proceedings of EUROCRYPT '97, LNCS, 1997, pp. 103-118.

12 **Hirt M, Sako K**, *Efficient receipt-free voting based on homomorphic encryption*, Proceedings of EUROCRYPT 2000, LNCS, 2000, pp. 539-556.

13 **Lee B, Kim K**, *Receipt-free electronic voting through collaboration of voter and honest verifier*, Proceeding of JW-ISC2000, 2000, pp. 101-108.

14 **Magkos E, Burmester M, Chrissikopoulos V**, *Receipt-freeness in large-scale elections without untappable channels*, First IFIP Conference on E-Commerce, E-Business, E-Government (I3E), 2001, pp. 683-694.

15 **I. Ray, Narasimhamurthi N**, *An anonymous electronic voting protocol for voting over the Internet*, Third International Workshop on Advanced Issues of E-Commerce and Web-Based Information Systems (WECWIS '01), 2001, pp. 188.

16 **Juels A, Catalano D, Jakobsson M**, *Coercion-Resistant Electronic Elections*, Proceedings of the 2005 ACM workshop on Privacy in the electronic society, 2005, pp. 61-70.