International Journal of Swarm Intelligence and Evolutionary Computation

Darwish and El-Gendy, Int J Swarm Intel Evol Comput 2017, 6:2
DOI: 10.4172/2090-4908.1000158

Research Article

Open Access

A New Cryptographic Voting Verifiable Scheme for E-Voting System Based on Bit Commitment and Blind Signature

Ashraf Darwish* and Maged M El-Gendy

Department of Computer Science, Helwan University, Egypt

Abstract

The main challenge in electronic voting (EV) systems is the security issue which has gained an interest of researchers in the last twenty years. EV system is one of the most important Internet-related activities. Recently many countries moved to electronic voting instead of a traditional one for many reason. Electronic voting has been studied for over the last twenty years. Until now, many EV schemes have been proposed. However, there is no a complete solution in both theoretical and practical areas. So, the researchers try to preserve the cryptographic primitives to build e-voting schemes with high efficiency to achieve these requirements. In this paper, we present a new cryptographic verifiable voting system. The digital signature represents one of the most important applications of cryptographic protocols In order to implement the cryptographic protocols in the field EV systems, it is important to secure the communication channels to the legal users. Therefore, the main target of this paper is to design a scheme which is more effective and achieving higher security properties based on bit commitment infrastructure and digital signature technology. In this system, the improper behavior of the voter will be detected and invalid or double votes will not be taken into account. In addition, the voter has the ability to prove that his vote is in correct form without disclosing any other information about his vote and his decision.

Keywords: Cryptography; Public key infrastructure (PKI); Bit commitment schemes (BCS); Blind signature; Electronic voting system; Security and privacy

Introduction

In the next few years, various applications and services will increasingly depend on computer networks and the collected amount of data also will be incredibly large. Thus cryptography technologies will be applied in most areas of computing such as EVs and cryptographic protocols will become more important. The cryptographic verifiable electronic voting system is a web-based system. The web-based scheme is accessed by the voter through his web browser. The cryptographic voting system is an open-audit system, universally verifiable, with several features included in the scheme for verification and control purposes.

The cryptographic voting scheme implements cryptographic techniques using standard algorithms to maintain ballot secrecy while providing a mathematical proof that the election tally was correctly computed.

In the voting system, the votes are encrypted with a hybrid system using the standard algorithms RSA, AES (256-bit session key length), SHA and ANSI.X9.17 cryptographic random bits generator, as an example. When the application is initialized, it does not access the Internet until the vote is completely encrypted and digitally signed and ready to be cast.

The Norwegian voting scheme created for elections, uses strong cryptographic methodology for security, integrity and verification providing a scheme for Internet voting [1]. The Internet voting scheme will never be secure completely. The sacrifices has to be considered. The scheme supporting public key cryptography and the National Electoral Committee has its private key, opens the encrypted votes on the Election Day. In this paper, the proposed cryptographic voting system allows voter-verification of ballots.

There are several attacks that should be considered in case of electronic voting schemes. The first one is the Randomization attack, in which an attacker coerces a voter to submit randomly formed ballot [2]. The effect of this attack is to cancel the voter's vote with large probability. The second one is the Forced-abstention attack in which 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 because he can threaten voters and effectively excludes them from the voting process. The third one is the Simulation attack in which an adversary coerces or bribes the voter to reveal his private key and then pretends to be the voter and casts his own favorite vote.

In this paper, we present a new cryptographic voting scheme based on the Public Key Infrastructure (PKI), RSA Public Key Technology and Blind Digital Signature based on RSA cryptosystem. We first summarize cryptographic primitives used in our proposed scheme. Finally, we discuss the security of our proposed scheme. The proposed cryptographic voting scheme in this paper satisfies the following properties which have been proposed in [3].

- **Voter privacy:** while it must be ensured that the eligible voters can cast a ballot, it must be impossible to connect the voter identity with the content of his/her cast vote.
- **Vote verifiability:** votes must be verified independently by their voters that were inserted in final tally and must be counted correctly. There are two types of verifiability that are Universal Verifiability in which anyone can check that the published final tally is really the sum of the votes and Individual Verifiability

***Corresponding author:** Ashraf Darwish, Department of Computer Science, Helwan University, Cairo, Egypt, Tel: +2-0105645222; Fax: 002-25552468; E-mail: ashraf.darwish.eg@ieee.org

Received June 05, 2017; **Accepted** June 16, 2017; **Published** June 23, 2017

Citation: Darwish A, El-Gendy MM (2017) A New Cryptographic Voting Verifiable Scheme for E-Voting System Based on Bit Commitment and Blind Signature. Int J Swarm Intel Evol Comput 6: 158. doi: 10.4172/2090-4908.1000158

in which each eligible voter can verify that his vote was really counted.

- **Democracy:** each eligible voter has the right to cast his vote and is not allowed for anyone to vote for others.
- **Robustness:** the system must be secure and non-infiltrated by adversaries preventing any harmful behavior of voters, by authorities or strangers.
- **Receipt-freeness:** No one must know the content of the voter's vote. This property prevents vote selling or buying.
- **Correctness:** An election scheme is said to be correct if the ballots are counted correctly.
- **Fairness:** No participant can gain any knowledge, except his vote, about the (partial) tally before the counting stage.
- **Coercion-resistance:** An election scheme is said to be coercion resistance if the voter cannot cooperate with a coercer to prove to him that she voted in a certain way.

The remainder of this paper is as follows. Section II presents the related work. In section III, we describe some basics and background related to the cryptographic e-voting systems. Section IV presents the proposed system in this paper. Section V presents the analysis and discussion about the proposed system. The conclusion and future work are presented in section VI.

Related Work

Currently, there is an interest of researchers in the field of Internet voting (I-voting), but there are many countries that are not implemented such systems. I-voting is a criticized and highly complex topic. The voting via Internet is desirable but with the use of the Internet, we will have new threats. The need to improve the security techniques for the development of End to End (E2E) encryption verifiable voting schemes. End to End (E2E) scheme are fantastic at detecting fraud. Such schemes can provide greater assurance that the election outcome is correct than traditional schemes.

Electronic voting (EV) has attracted much interest recently and a variety of schemes have been proposed. These schemes can be divided into three main approaches: based on blind signature, mix networks and homomorphic encryption in a holomorphic cryptosystem, there is a homomorphism between an algebra based on the plaintext domain and an algebra based on the cipher text domain [4-22]. Schemes based on blind signature are thought to be simple, efficient and suitable for large scale elections. The different encryption primitives have been used in many e-voting schemes before and the way in which these primitives are combined make the following five schemes do not satisfy the same properties [23-25]. In the literature, there are many EV schemes have been proposed in the last twenty years. Authors in presented the first e-voting scheme based on digital signature for large scale elections [3]. The main problem of this scheme is that all voters should be involved in the ballot counting process due to in the counting stage the authority needs the help of each voter to open the ballot in the bit-commitment scheme. A new scheme has been proposed in to improve voting scheme based on blind signatures [26]. In addition, the threshold encryption scheme is used in this system instead of a bit-commitment scheme and the analysis of the results showed that this scheme is not receipt-free. Moreover, authors in presented a new e-coting system based on blind signature and a trapdoor commitment scheme has been used in this scheme in order to solve the problem of receipt-freeness [27]. The trapdoor commitment concept has been presented in for zero-knowledge proofs [28]. In a trapdoor commitment scheme, the holder can freely open a commitment in the open phase to enable the scheme to satisfy the property of receipt-free only if the trapdoor information is known by the voters. Therefore, authors in presented two improved voting schemes which ensure that the voters know the trapdoor information [29]. Authors in utilize the double-trapdoor commitment to propose a new receipt-free voting scheme based on blind signatures for large scale elections with more efficient zero-knowledge proof for secret permutation process [30]. In tables we summarize the well-known five schemes according to their primitives, achieved properties and attacks [31-33] (Tables 1-3).

Basics and Background

Basic definitions

Trapdoor functions appeared on the scene in the field of cryptography in the mid-1970s with the deployment of asymmetric (or public key) encryption techniques by Diffie-Hellman Group [34]. In many cryptosystems there are many that rely on the trapdoor one-way function, as an example El Gamal protocol and RSA cryptosystem [35,36].

	Primitives used					
Voting Schemes	Zero Knowledge Proof	Blind Signature Scheme	Homomorphic Encryption	Mix-Net Scheme	RSA Signature Scheme	El Gamal Cryptosystem
Foo's Scheme	√	√				
Radwin Scheme	√	√			√	
Jaung and Lei's Scheme		√			√	√
Cramer et al. Scheme	√		√			√
Pret-Voter	√			√		

Table 1: Some schemes and their primitives.

	Achieved properties						
Voting Schemes	Eligibility	Privacy	Individual Verifiability	Universal Verifiability	Fairness	Receipt Freeness	Correctness
Foo's Scheme	√	√	√		√		
Radwin Scheme	√	√	√				
Jaung and Lei's Scheme	√	√	√				
Cramer et al. Scheme	√	√		√			
Pret-Voter		√	√	√		√	

Table 2: Some schemes and their achieved properties.

	Achieved properties						
Voting Schemes	**Correction Resistance**	**Privacy**	**Individual Verifiability**	**Universal Verifiability**	**Fairness**	**Receipt Freeness**	**Correctness**
Foo's Scheme				√		√	
Radwin Scheme				√		√	
Jaung and Lei's Scheme						√	√
Cramer et al. Scheme				√		√	
Pret-Voter	√			√			

Table 3: Attacks found against the selected five schemes.

Definition 1

A trap-door one way function, f_k is a family of invertible functions indexed by a parameter k in an index set, I, "the trap-door" such that [34]:

1. It easy to pick a value of *k* at a random,
2. When k is known, it is easy to find algorithm E_k and D_k that easily to compute f_k and f_k^{-1} respectively.
3. When k is not known, $\forall$ *k*, in the range of
4. f_k, it is infeasible to find x such that $f_k(x)$=y even when the algorithm E_k is known.

Definition 2

A hash function h is a mapping from the set of all finite strings of characters from an alphabet A_1 to a string of characters from an alphabet A_2 with fixed length. For any x, h(x) is called the hash value, or message digest.

Definition 3

Let $l(n)$ be some function such that $l(n)>n$, $G_n: \{0, 1\}^n \rightarrow \{0, 1\}^{l(n)}$ is a pseudo-random bit generator (PRBG) if for all polynomials, p and all polynomial time algorithms, A, that attempt to distinguish between outputs of the generator and truly random sequences, except for finitely many *n*'s [37]:

$$|pr\ (A(y)=1)-pr\ (A(G_n(s)=1))|<1/p(n),$$

where the probabilities are taken over $y\epsilon\{0, 1\}^{l(n)}$ and $S\epsilon\{0, 1\}^n$ are chosen uniformly at random.

Blind digital signature

A blind digital signature has been introduced by Chaum in 1983 [38]. It resembles as digital signature however it allows somebody for example an authority to get someone else to sign a message without disclosing the contents of the message. It can be useful in cryptographic election systems where anonymity is required; meaning that the signature is used to authenticate the voters without revealing the content of the ballot therefore the authority does not know whom to vote for. Many blind signatures schemes have been proposed in and they typically share two basic security properties that are blindness and unforgeability [31-34,39-41]. The security requirements for blind signatures have been formalized by Juels et al. [32] and by Pointcheval and Stern [23]. In a blind signature scheme, three entities participate which are: the sender who blinds the message before it is signed and sends it to the signer, the signer, who signs the blinded message and sends it to the receiver and the receiver, who verifies the signature, accepts or rejects the message.

The blind digital signature scheme has five phases:

1. **Key generation**: The signer generates his private and public keys.
2. **Blinding:** The sender creates his private and public keys. The private key is used to blind the message to sends it to the signer.
3. **Signing**: The signer signs the blinded message by his private key and some signing algorithm and sends the signature to the sender.
4. **Unblinding:** The sender received his blinded message from the signer to obtain unblinding version of the signature and send the message and the signature to the receiver.
5. **Verification:** The receiver verifies the signature using the signer's public key and check the message. Then he accepts or rejects the message accordingly.

If the signer has RSA public (n, e) and the corresponding private key, d, the requester obtains blind signature of the message $m\epsilon Z_n$ as follows: The sender blinds his message m to $m'=mr^e$ mod n, where $r\epsilon_R Z_n$ is random and sends m' to the signer [38].

- The signer signs the blinded message m' and sends its signature

$s'=m'^d$ mod n to the sender.

- s' is sent back to the sender, who can then remove the blinding factor to reveals:

s=s'/r mod n.

- The receiver retrieves the desired signature s of the message m by computing

$s=s'/r=m'^d/\ r=m^d r^{ed}/r=m^d\ r/r=m^d$ mod n

Public key infrastructure (PKI)

PKI is a system that allows integration of various services that are related to cryptography [42,43]. The PKI helps to make a sender of a message has the right to retrieve the receiver's public key and give the sender confidence that the key belongs to the receiver. The most common uses of PKI and its public key cryptography are electronic voting system. The main properties that can be satisfied by the use of the PKI technology in our proposed e-voting system will satisfy the following two properties:

- **Efficiency:** The Information needed should be available for the various modules of the e-voting protocols from PKI infrastructure in as little time as possible.
- **Reliability:** Corruption in the components of the PKI must not expose the voting process to risk.

PKI using X.509 (PKIX): PKIX is the most popular PKIs that use X.509, which determines a certificate format and procedures for distributing the public keys by Public Key Certificates PKCs signed by

Certificate Authorities (CAs). X.509 determines one way of certificate revocation where each CA periodically (e.g. hourly, daily or weekly) issued a signed list of the serial numbers of certificates that have been revoked so-called Certificate Revocation List (CRL).

Bit commitment schemes (BCS)

A BCS (blob) is a basic component of many cryptographic protocols.

In this paper, we have proposed secure verifiable transfer protocols for the exchange of secrets on EV system as a distributed environment. This secure verifiable transfer protocol is based on using bit commitment using one-way functions where the security in our protocols also can be chosen as a random number. Consider one party, P, sends (commits) to the other party, V, a bit, b; in such a way that V can verify that it is indeed the value P originally sent. A good way to think about it is that P wrote and locked the bit in a box and she is the only one who has the key. She gives the box to V (the commit stage) and when the time is ripe she opens it and V knows that the contents have not been tampered since the box was always in his possession.

Definition 4

A bit commitment protocol consists of two stages as follows [44]:

1. The commit stage: P has a bit, b, on her input tape, which she wishes to commit to V. She and V exchange messages. At the end of stage V has some information that represents b written on his output tape.
2. The revealing stage: P and V exchange message (where there output tapes from the commit stage are serving as input tapes for this stage). At the end of the exchange V write b on its output tape.

The Proposed Cryptographic Electronic Voting Scheme

A. System overview

Firstly, the proposed new cryptographic voting scheme in our paper is based on the following principle

(i) Only eligible voters have the right to vote.

(ii) Data of eligible voters come from the State Population Register.

(iii) The eligible voters are able to vote one time only.

(iv) If the authorities discover any attacks against electronic voting process, the Election Commission has stopped electronic voting process and cancels the result of the vote.

The proposed new cryptographic voting scheme depends on blind signature scheme using RSA based Public Key Infrastructure (PKI) [41,45]. Each eligible voter must have an e-token as a passport to certify himself to the system. For authentication, the voter must connect to network server by his token which it gets from any electronic certification authority in the country. The token like a secure USB contains information about the voter like the user name, public key and private key related to him. BCS protocol is built to achieve a secure protection between the voters and the network servers. In the proposed solution we considered the hypothesis that we have a secure authentication method which in this case represented by the RSA key pair certification, which was issued by a national qualified electronic certification authority (NQ-CA) serve each voter. One of the most important features in our proposed scheme is that we used the bit commitment scheme (BCS) technology to secure the communications between the voters and the authorities' servers. The proposed electronic voting protocol has the following components which are:

1. **Voter Application (VA):** This is a web application help the voters first to register them before starting the voting phase. The voter Application (VA) is responsible also for defining the voters to the e-voting system and gives the system authentication data to log into the e-voting system.
2. **Trusted Server Authority (TSA):** It is responsible for authenticate the voters, loading a candidates' list on computer screens and storing the blinded ballots until the end of voting phase. It is responsible for issuance of electronic certificates, which are stored on e-tokens devices.
3. **Counting Server Authority (CSA):** It is responsible for counting the votes after receiving it from the voter.
4. **Publishing Server Authority (PSA):** It is responsible for publishing the identification number of the voters ID's with the corresponding signed votes.

B. The proposed scheme design

The proposed electronic voting scheme in this paper consists of the following four stages:

Initialization stage

The trusted server authority (TSA) sets up a blind signature scheme (η, Χ, σ, δ, Γ) where:

- η: Is a polynomial-time probabilistic algorithm, that constructs the signer's public key (PK) and its corresponding secret key (SK),
- *X*: Is a polynomial-time blinding algorithm, that on input a voter's vote v_i, a public key PK and a random string r_i, constructs a blind vote B_i,
- σ: Is a polynomial-time signing algorithm, that on input the blind vote B_i and the secret key SK, constructs a blind signature,
- δ: Is a polynomial-time unblind algorithm, that on input a blind signature S_i and the random string r_i,
- Γ: Is a polynomial-time signature-verifying algorithm that on input a message signature pair (B_i, L_i) and the public key PK outputs either yes or no result.
- The authorities (TSA, CSA) use his RSA keys (n, e) for blind signatures: The RSA keys (n, e) (for blind signatures) are PK_{TSA}, SK_{TSA}, PK_{CSA}, SK_{CSA}.
- The person who wants to vote must go to NQ-CA to obtain his electronic certification keys loaded on an e-token device.

Registration stage

- The voter (V_i) contacts to Trusted Server Authority (TSA) for registration via BCS highly secure channel.
- When the connection is done, the Trusted Server Authority (TSA) verifies the eligibility of the voter by sending a query to LDAP of NQ-CA server. If the voter is not eligible; the voter in that case is prevented from voting.
- In the same time, if the eligible voter has already voted before, if yes the (TSA) prevents the voter from voting.

Voting stage

- In the voting phase, the national authority (NA) appears the list of the candidates on the computer and the voter (V_i) casts his vote (v_i) once, then the voter generates a random number, where $r_i \in_R Z_n$ to blind the vote as follows:

v_i=cast (Vote)

$B_i = v_i * (r_i)_{PK_{TSA}}$

this implies to: $B_i = X(v_i, \mathrm{PK}_{TSA}, r_i)$ such that X is the blind function.

Then voter (V_i) sign his ballot B_i by his private key SK_{vi} as $L_i = [B_i]_{SK_{v_i}}$, this implies to $L_i = \sigma(B_i, SK_{vi})$ by using his token and send L_i to the trusted server authority (TSA) via BCS secure channel.

The trusted server authority (TSA) verifies the voter's signature by the voter's public key PK_{vi} as follows:

$$\Gamma(B_i, L_i, PK_{vi}) = \left[[B_i]_{SK_{v_i}} \right]_{PK_{v_i}}$$

The trusted server authority (TSA) signs the ballot by his private key SK_{TSA} and multiply the value by secret key (K) generated from the pseudo random number generator ANSI.X9.17 and encrypted it by the public key of the CSA as follows:

$$S_i = \sigma(B_i, SK_{v_i}) = [\, v_i * (r_i)_{\mathrm{PK}_{TSA}} \,]_{SK_{TSA}} = (v_i)_{SK_{TSA}} * r_i$$

$\grave{S}_i = r_i * v_i^{SK_{TSA}} * K^{PK_{CSA}}$ and send this value to the voter (V_i) via BCS secure channel.

- When the system calculates the digital signature on the vote value, it will catch the time stamp on line from NQ-CA time stamp server via BCS secure channel. It represents a proof on the voter.

The voter V_i unblinds $\grave{S}_i$ and sends the unblinded value to the counting server authority via BCS secure channel as:

$$e_i = \delta\left(\grave{S}_i, r_i\right) = r_i * v_i^{SK_{TSA}} * K^{PK_{CSA}} * \frac{1}{r_i} = v_i^{SK_{TSA}} * K^{PK_{CSA}}$$

Counting and publishing stages

- The counting server authority (CSA) signs the value which received by voter as

$$X_i = \left[v_i^{SK_{TSA}} * K^{PK_{CSA}} \right]_{SK_{CSA}} = \left[v_i^{SK_{TSA}} \right]_{SK_{CSA}} * \mathrm{K}$$

The counting server authority (CSA) removes the K value and sends the resulting value to the publishing server authority via BCS secure channel. The publishing server authority publishes the resulting value in the public directory associated with the identification number ID of the voter V_i. The counting server authority (CSA) verifies the signatures as:

$$[[\left[\mathrm{v}_i^{\mathrm{SK_{TSA}}} \right]_{\mathrm{SK_{CSA}}}]_{\mathrm{pK_{CSA}}}]_{\mathrm{pK_{TSA}}}$$

After that, the CSA records the resulting value as a certified vote and records it in its certified server. The CSA increases the counter by 1. Finally, CSA counts the correct votes and announces the winner candidate. The proposed NCVVS scheme is presented in Figure 1.

C. The security analysis of the proposed scheme

The security of our scheme based on highly secure standard components that are PKI technology, blind signature schemes, BCS protocols and the national qualified electronic certification authority NQ-CA.

Theorem

The proposed e-voting scheme NCVVS is secure, i.e., it satisfies

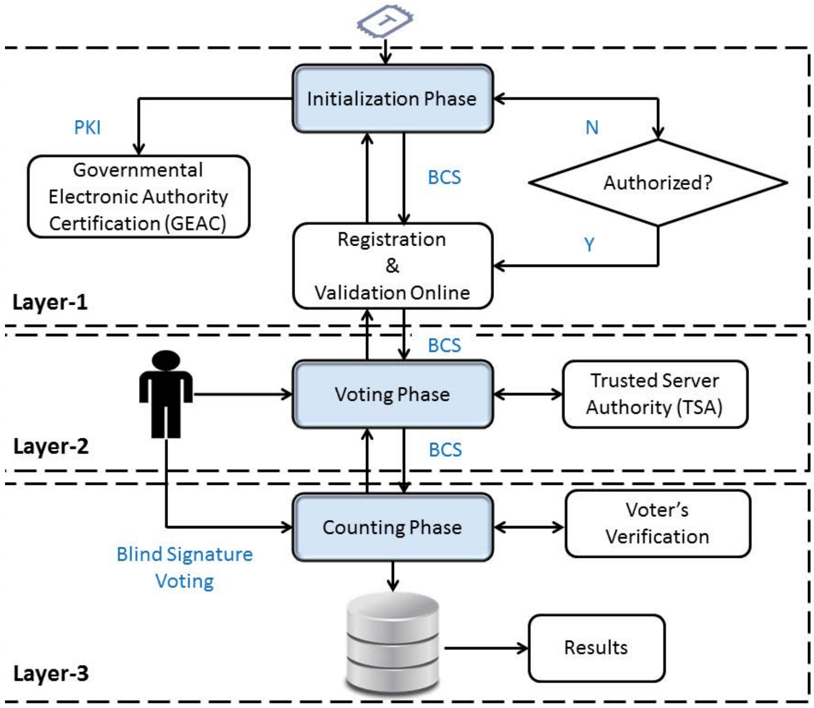

Figure 1: The proposed scheme design for electronic voting system.

Privacy, fairness, receipt-freeness, Correctness, individual verifiability, voter robustness and efficient flexible.

Proof

In our proposed NCVVS-scheme, the privacy is obtained because no one can determine the vote because K value is unpredictable number because K is a pseudo random number generated from standard PRBG ANSI. X9.17. Thus it is impossible to know or to predict the voter identity with the content of his/her vote.

Before the counting stage, no participate can gain any knowledge except his vote about the partial tally because the protocol use blind signature scheme. On the voting result in the voting stage, no one can know the value of the secret key so the fairness property is satisfied in our protocol. The protocol is designed to be receipt-freeness since no one can know the content of the vote because the vote is blinded by a secret key that is encrypted by the public key of the counting server authority (CSA).

Correctness is obtained when the voter signs the ballot, his/her certificate is sent to the trusted server authority (TSA). So the number of certificates is equal to the number of the published votes at the counting phase.

When the ballots are signed by the TSA and CSA published the result, the voter can verify that his vote was counted therefore the scheme supports individual verifiability. The protocol also fulfils the voter robustness because the administrator (TSA) cannot cast extra votes since every voter must check if his (her) ballot is on the published list. Furthermore, it can be considered as efficient because very little computation is necessary and the system works well with its legal authorities and the results are submitted to a central authority. Finally, no restrictions on the ballot form, our protocol can support any type of election process and therefore it is flexible.

D. The characteristics of the proposed scheme:

The proposed scheme satisfies the receipt-freeness and protected against the randomization attack, the forced-abstention attack and the simulation attack, therefore it is coercion-resistant as follows:

1. **Randomization attack.** This attack is prevented, since the adversary cannot verify if the coerced voter has cast the prescribed vote or not since in the voting stage the voter's vote is blinded by using the blind signature technique.
2. **Forced-abstention attack.** If an adversary can see the list of the registered voters, the adversary will not be able to verify if a certain voter has cast a vote or not since the information of the voter is appearing only at the counting stage when the authority CSA published the pair (l_i, ID_i).
3. **Simulation attack.** This attack is covered because if an adversary coerced a voter to reveal his private key, the voter behavior in this case can inform about theft of his token.

Discussion and Analysis

The voting systems via the Internet will improve the accessibility and provide more convenient voting process. The promises of accuracy, security and precision will drive the electronic voting direction forward. The Internet voting systems are now developing into being categorized as cryptographic voting systems, not only to provide the security needs but also to provide possibilities of verification. The purpose of cryptographic verifiable voting systems are to prevent incorrect recording and tallying, by making the processes verifiable for everyone.

The Internet systems are vulnerable to more and new threats and fraud. The need for better mechanisms of authentication, anonymity, integrity, confidentiality, secrecy, etc., are highly important. The development of Internet voting systems for both security against all possible threats and for verification purpose.

The National Institute of Standard and Technology (NIST) in the United States of America had a workshop called end-to-end verifiable voting systems, which is an improvement of the verification in voting systems. Voting over the Internet can be done from remote locations using a computer connected to the Internet. But when referring to Internet voting in this paper we mean voter cast from a remote location, for instance through the web browser of the home computer, via the Internet. These Internet voting systems are also called cryptographic voting systems.

To vote over the Internet the voter needs a digital signature to log into the system, for instance identify himself with a PIN code and a smart card from the national qualified electronic certification authority NQ-CA. The voter submits his choice and the encrypted ballot is transmitted over the Internet to a remote server of the election system. The remote voting schemes can also be designed so the phone can be used to cast votes via GSM network. The area of remote voting is growing and in the last decade, several countries have developed and they have tested the use of Internet voting.

The essential blocks of the NCVVS-voting system depends on the national ID infrastructure represented in the national qualified certification authority NQ-CA. This infrastructure plays a central role in the country's high-tech and e-government strategy. The National ID cards are smartcards with the ability to support standard cryptographic algorithms. With the use of card readers and client software, for anybody in the country can authenticate via website to perform legal signatures on documents. The smart cards are used for e-government services.

In the proposed NCVVS-voting system, voters use the ID-cards to authenticate to the servers and to sign their ballots. Each card contains two RSA key pairs, one for authentication and another one to calculate the digital signature. The digital certificates binding the public keys to the card holder's identity and stored them on a smart card besides publishing them in a public LDAP (Lightweight Directory Access Protocol) database of the NQ-CA. The card does not allow exporting the private keys, so all cryptographic operations are performed internally. Each key is associated with a PIN code that provided to authorize every operation.

Our proposed solution can also use mobile phones system with special SIM cards for authentication and signing. The NCVVS-voting system uses public key cryptography to provide double envelope protection for ballots that used for highly secure voting. The outer envelope (a digital signature) establishes the voter's identity, while an inner envelope (public key encryption) protects the secrecy of the ballot.

Once each voter's eligibility has been established, the signature is stripped off, leaving a set of masking encrypted ballots. These ballots are moved to a separate server that decrypts and counts them. One core strength of NCVVS-voting scheme is the National ID card infrastructure and the cryptographic facilities that provides like the standard algorithms RSA (256), SHA and ANSI. X9.17 cryptographic random bits generator. While the ID cards cannot prevent every important attacks, they make some kinds of attacks harder. The cards also provide an intelligent solution for remote voter authentication.

Cryptographic techniques that achieve end-to-end verifiability enable individual voters to verify that every vote has been counted accurately. In real elections, NCVVS-voting system uses a Hardware Security Module (HSM) in order to handle the election private key and to decrypt the votes. We assume for purposes of this paper that ID cards and the associated infrastructure are secure.

After casting a vote with NCVVS system, the voter receives a confirmation email containing the ballot fingerprint (and also the fingerprint of the election) calculated by SHA (256) [46]. NCVVS system has a bulletin board of all cast votes in an election that is managed by a trusted server, NCVVS system has a bulletin board of all cast votes in an election that is managed by the Published Server Authority (PSA). On this bulletin board all ballots are posted for everyone to see. On this bulletin board in NCVVS system, the "ballot fingerprint" of the cast votes is displayed together with a voter name or voter identification number ID. On this list, the voter find his ID and not only check that his vote is on the bulletin board, but also the fingerprint matches the one he cast and received in the confirmation email [47].

The voter can go to the audit web site. There, he will find a detailed specification that describes the file formats, encryption mechanisms and process by which you can audit the election.

Conclusion and Future Work

We presented, in this paper, how the proposed model achieved security properties comparing between the proposed model and many published models**.** We concluded that the proposed model is more secure than other models and it is suitable for use in major elections on a large scale. After casting a vote with NCVVS system, the voter receives a confirmation email containing the ballot fingerprint (and also the fingerprint of the election) calculated by standard hash function SHA (256) [46].

The use the computers for voting has many advantages, but a system for electronic voting requires means to preserve every aspects of the traditional voting systems especially the security features like authentication, secrecy and anonymity. The proposed system protect against at least the well-known attacks, errors and electronic fraud.

A well-designed e-voting system can produce an audit trail even stronger than that of conventional systems (including paper-based systems). The future of e-voting electronic systems can use the current technologies and tools including smart cards, biometrics (e.g. voice, fingerprint, retinal recognition - for identification), as well as mobile voting. Research effort is needed to determine to what extent such technologies are useful for e-voting process practically. The implementation and the real applications of e-voting processes have to cover the legal issues.

References

1. Miller VS (1986) Use of elliptic curves in cryptography.
2. Bellare M, Rogaway P (2005) Introduction to modern cryptography.
3. Fujioka A, Okamoto T, Ohta K (1992) A practical secret voting scheme for large scale elections. Adv Cryptol-AUCRYPT'92. Springer-Verlag, pp. 244-251.
4. Fujioka A, Okamoto T, Ohta K (1992) A practical secret voting scheme for large scale elections. Adv Cryptol-AUCRYPT'1992. Springer-Verlag, pp. 244-251.
5. Okamoto T (1996) An electronic voting scheme. IFIP World Conference, Advanced IT Tools, Chapman Hall, pp. 21-30.
6. Okamoto T (1997) Receipt-free electronic voting schemes for large scale elections. Proceeding of Workshop on Security Protocols 1997, LNCS, 1361, Springer-Verlag, pp. 25-35.
7. Abe M (1999) Mix-networks on permutation networks. Adv Cryptol-ASIACRYPT 1999, LNCS, 1716, Springer-Verlag, pp. 258-273.
8. Aditya R, Lee B, Boyd C, Dawson E (2004) An efficient mix-net based voting scheme providing receipt-freeness. Springer-Verlag.
9. Chaum DL (1981) Untraceable electronic mail, return addresses and digital pseudonyms. Communications of the ACM 24: 84-88.
10. Lee B, Boyd C, Dawson E, Kim K, Yang J, et al. (2003) Providing receipt-freeness in mix-net based voting protocols. Springer-Verlag.
11. Park C, Itoh K, Kurosawa K (1993) Efficient anonymous channel and all/nothing election scheme. Adv Cryptol-EUROCRYPT 1993, Springer-Verlag, pp. 248-259.
12. Jakobsson M (1998) A practical mix. Adv Cryptol-EUROCRYPT 1998, Springer-Verlag, pp. 448-461.
13. Sako K, Kilian J (1995) Receipt-free mix-type voting scheme: A practical solution to the implementation of a voting booth. Adv Cryptol-EUROCRYPT 1995, Springer-Verlag, Berlin, pp. 393-403.
14. Benaloh J, Fischer M (1985) A robust and verifiable cryptographically secure election scheme. In: Proceeding of 26th IEEE Symposium on the Foundations of Computer Science (FOCS, pp. 372-382.
15. Benaloh J, Tuinstra D (1994) Receipt-free secret-ballot elections. In: Proceedings of 26th Symposium on Theory of Computing (STOC), pp. 544-553.
16. Benaloh J, Yung M (1986) Distributing the power of a government to enhance the privacy of voters. Proceedings of Fifth ACM Symposium on Principles of Distributed Computing (PODC), pp. 52-62.
17. Cramer R, Damgard I, Schoenmakers B (1994) Proofs of partial knowledge and simplified design of witness hiding protocols. Adv Cryptol-CRYPTO 1994, Springer-Verlag, pp. 174-187.
18. Cramer R, Franklin M, Schoenmakers B, Yung M (1996) Multi-authority secret-ballot elections with linear work. Adv Cryptol-EUROCRYPT 1996, Springer-Verlag, pp. 72-83.
19. Cramer R, Gennaro R, Schoenmakers B (1997) A secure and optimally efficient multi-authority election scheme. Adv Cryptol-EUROCRYPT 1997, LNCS, Springer-Verlag 1233: 103-118.
20. Hirt M, Sako K (2000) Efficient receipt-free voting based on homomorphic encryption. Adv Cryptol-EUROCRYPT 2000, LNCS, Springer-Verlag 1807: 393-403.
21. Lee B, Kim K (2002) Receipt-free electronic voting scheme with a tamper-resistant randomizer. ICISC 2002, LNCS, Springer-Verlag 2587: 389-406.
22. Sako K, Kilian J (1994) Secure voting using partially compatible homomorphisms. Adv Cryptol-CRYPTO 1994, LNCS, Springer-Verlag 839: 411-424.
23. Pointcheval D, Stern J (2000) Security arguments for digital signatures and blind signatures. J Cryptol 13: 361-396.
24. Rivest R, Adleman L, Dertouzos M (1978) On data banks and privacy homomorphisms. In: Foundations of Secure Computation.
25. Juang WS, Lei CL, Yu PL (1998) A verifiable multi-authorities secret elections allowing abstaining from voting. Int Comput Symp 45: 672-682.
26. Ohkubo M, Miura F, Abe M, Fujioka A, Okamoto T (1999) An improvement on a practical secret voting scheme. ISW 1999, LNCS, Springer-Verlag 1729: 225-234.
27. Okamoto T (1996) An electronic voting scheme. IFIP World Conference Advanced IT Tools, Chapman Hall, pp. 21-30.
28. Brassard G, Chaum D, Crepeau C (1988) Minimum disclosure proofs of knowledge. J Comput Syst Sci 37: 156-189.
29. Okamoto T (1997) Receipt-free electronic voting schemes for large scale elections. Proceeding of Workshop on Security Protocols, LNCS, Springer-Verlag 1361: 25-35.
30. Chen X, Wu Q, Zhang F, Tian H, Wei B, et al. (2010) New receipt-free voting scheme using double-trapdoor commitment. Inform Sci 181:1493-1502.

31. Boldyreva A (2003) Threshold signatures, multi-signatures and blind signatures based on the Gap-Diffie-Hellman-Group signature scheme. Springe-Verlag.

32. Juels A, Luby M, Ostrovsky R (1997) Security of blind digital signatures. Springer-Verlag 1294: 150-164.

33. Kiayias A, Zhou HS (2008) Equivocal blind signatures and adaptive UC-Security. Springer-Verlag 4948: 340-355.

34. Juang WS, Lei CL (1997) A secure and practical electronic voting scheme for real world environment.

35. Gjosteen K (2013) The Norwegian internet voting protocol.

36. Okamoto T (2006) Efficient blind and partially blind signatures without random oracles. Springer-Verlag.

37. Blakley GR (1979) Safeguarding cryptographic keys. In: Proceedings of AFIPS 1979 National Computer Conference 48: 313-317.

38. Chaum D (1987) Demonstrating that a public predicate can be satisfied without revealing any information about how. In: Advances in Cryptography-Crypto' 86 Proceedings, Springer Verlag 263: 195-199.

39. Kiayias A, Zhou HS (2005) Concurrent blind signatures without random oracles.

40. Fischlin M (2006) Round-Optimal composable blind signatures in the common reference string model.

41. Radwin MJ (1995) An untraceable, universally verifiable voting scheme. Seminar in Cryptology 1995.

42. Chaum DL (1988) Elections with unconditionally-secret ballots and disruption equivalent to breaking RSA.

43. Lee B, Boyd C, Dawson E, Kim K, Yang J, et al. (2003) Providing receipt freeness in mix-net based voting protocols.

44. Boneh D, Franklin M (2003) Identity-based encryption from the Weil pairing. SIAM J Comput 32: 586-615.

45. Rabin MO (1979) Digitalized signatures and public-key functions as intractable as factorization. Technical Report MIT/LCS/TR-212, MIT Laboratory for Computer Science.

46. Sako K, Kilian J (1994) Secure voting using partially compatible homomorphisms. Adv Cryptol-CRYPTO’94, Springer Verlag.

47. Rueppel R (1986) Analysis and design of stream ciphers. Springer.