New Receipt-free Voting Scheme Using Double-trapdoor Commitment

Xiaofeng Chen[1], Qianhong Wu[2], Fangguo Zhang[1], Baodian Wei[1], Byoungcheon Lee[3], Hyunrok Lee[4], and Kwangjo Kim[4]

[1] School of Information Science and Technology,
Sun Yat-sen University, Guangzhou 510275, P.R.China
{isschxf,isszhfg,weibd}@mail.sysu.edu.cn
[2] Computer School of Wuhan University, Wuhan 430079, P.R.China
qhwu@xidian.edu.cn
[3] Department of Information Security,
Joongbu University, Chungnam 312-702, KOREA
sultan@joongbu.ac.kr
[4] International Research center for Information Security (IRIS)
Information and Communications University(ICU),
103-6 Munji-dong, Yusong-ku, Taejon 305-714, KOREA
{tank,kkj}@icu.ac.kr

Abstract. It is considered to be the most suitable solution for large scale elections to design an electronic voting scheme using blind signatures and anonymous channels. Based on this framework, Okamoto first proposed a receipt-free voting scheme [23] for large scale elections. However, in the following paper, Okamoto [24] proved that the scheme [23] is not receipt-free and presented two improved schemes. One scheme requires the help of the voting commission and the other needs a stronger physical assumption of the voting booth. In this paper, we utilize the double-trapdoor commitment to propose a new receipt-free voting scheme based on blind signatures for large scale elections. Neither the voting commission nor the voting booth is required in the proposed scheme. We also present a more efficient zero-knowledge proof for secret permutation. Therefore, our scheme is more efficient than Okamoto's schemes [23, 24] with the weaker physical assumptions. Moreover, we prove that our scheme achieve the desired security notations.

Key words: Electronic voting, Receipt-freeness, Double-trapdoor commitment, Blind signature.

1 Introduction

Electronic voting is one of the most significant applications of cryptography. Plenty of research work has been done in the past twenty years. The electronic voting schemes can be categorized by their approaches into

three types: schemes using blind signatures [14, 23, 24], schemes using mix-nets [1, 2, 10, 19, 25, 26, 28], and schemes using homomorphic encryption [6, 8, 9, 12, 13, 17, 18, 27].

The concept of receipt-freeness was firstly introduced by Benaloh and Tuinstra [6] to solve the misbehaver of "vote buying" or "coercion" in the electronic voting. Based on the assumption of a voting booth, they also proposed two voting schemes using homomorphic encryptions. The first one is a single authority voting scheme and fails to maintain vote secrecy. The second scheme is extended to a multi-authority scheme achieving vote secrecy. However, Hirt and Sako [17] proved that the scheme could not satisfy the property of receipt-free and proposed the first practical receipt-free voting scheme based on homomorphic encryption.

Receipt-free voting protocol based on a mix-net channel was first proposed by Sako and Kilian [28], which only assumes one-way secret communication from the authorities to the voters. However, a significant disadvantage of this protocol is the heavy processing load required for tallying in mix-net schemes.

The only receipt-free voting schemes using blind signatures were proposed by Okamoto [24]. However, the first scheme requires the help of voting commission and the second one needs a stronger physical assumption of voting booth.

In this paper, we revisit Okamoto's receipt-free voting schemes using blind signatures. We then use the double-trapdoor commitment to propose a new receipt-free voting scheme based on blind signature. Neither the voting commission nor the voting booth is required in the proposed scheme. So, it is more efficient and practical for large scale elections than Okamoto's voting schemes [24].

1.1 Related Work

Blind signatures, introduced by Chaum [11], allow a recipient to obtain a signature on message m without revealing anything about the message to the signer. Blind signatures play an important role in a plenty of applications such as electronic voting, electronic cash where anonymity is of great concern.

Fujioka, Okamoto, and Ohta [14] proposed the first practical voting scheme for large scale elections based on blind signatures. Moreover, Cranor and Cytron designed and implemented a voting system named Sensus based on this scheme. The main disadvantage of [14] is that all voters have to join the ballot counting process. This is because in the counting stage the tally authority needs the help of each voter to open the commitment

(ballot) in the bit-commitment scheme. Ohkubo *et al* [21] proposed an improved voting scheme based on blind signature which allowed the voters to walk away once they finished casting their votes. The scheme used a threshold encryption scheme instead of a bit-commitment scheme [20]. However, the scheme is not receipt-free.

Okamoto [23] proposed a new voting scheme based on blind signature. The scheme tried to use a trapdoor commitment scheme [5] to reach the receipt-freeness. The concept of trapdoor commitment (also called chameleon commitment) was first introduced by Brassard, Chaum, and Crepeau [5] for zero-knowledge proofs. In a trapdoor commitment scheme, the holder with a trapdoor knowledge can open a commitment in any possible ways in the open phase. Therefore, the scheme satisfies the property of receipt-free only if the trapdoor information is known by the voters. Okamoto [24] then proposed two improved voting schemes which ensure that the voters know the trapdoor information, therefore both of the schemes can satisfy the receipt-freeness. The first scheme requires an untappable channel and a voting commission, and the second one requires the stronger physical assumption of a voting booth, where a voter provides a zero-knowledge proof that he/she knows the trapdoor information.

In other electronic commerce protocols such as electronic auction and contract signing, similar concepts were also introduced to prevent the corresponding crimes. For example, Abe and Suziki [4] introduced the idea of receipt-free auctions to prevent bid-rigging in the auction protocol. In the contact signing, if a party can provide a proof that he is capable of choosing whether to validate or invalidate the contract, he may obtain a better contact. Garay *et al* [16] first introduced the concept of abuse-free contact signing to solve this problem.

1.2 Organization

The rest of the paper is organized as follows: The model and definitions for electronic voting are given in Section 2. Some preliminaries are provided in Section 3. The proposed receipt-free voting scheme and its security and efficiency analysis are given in Section 4. The non-interactive zero-knowledge proof required in our voting scheme is presented in Section 5. Finally, conclusions will be made in Section 6.

2 Model and Definitions

In this section, we briefly describe the model and security requirements of electronic voting [6, 14].

2.1 Model

- **Participants:** Voting scheme involves in the following participants: voters, administrator authorities, and tally authorities.
- **Physical Assumptions:** The general physical assumptions for voting consist of untappable channel, voting booth, anonymous channel, and bulletin board.

2.2 Security Requirements

We present the security requirements as follows:

- *Completeness*: All valid votes should be counted correctly.
- *Privacy*: All votes must be kept secret.
- *Soundness*: The dishonest voter can not disrupt the voting.
- *Unreusability*: No voter can vote more than once.
- *Eligibility*: No one who is not allowed to vote can vote.
- *Fairness*: Nothing can affect the voting.
- *Verifiability*: No one can falsify the result of the voting.
- *Receipt-freeness*: Anyone, even if the voter himself, must not be able to construct a receipt proving the content of his vote.

3 Preliminaries

In this section, we introduce the notion of double-trapdoor commitment and Okamoto's receipt-free voting scheme based on blind signatures [24].

3.1 Double-trapdoor Commitment Based on RSA

Gennaro [15] first introduced the notion of multi-trapdoor commitment, which actually consists of a family of trapdoor commitments. Each commitment scheme in the family is double-trapdoor since it consists of a master trapdoor and a specific trapdoor. A master trapdoor can be used to compute all specific trapdoors in the family. Moreover, The knowledge of a specific trapdoor allows anyone only to open a commitment of the corresponding scheme in any desired way.

Gennaro [15] proposed a multi-trapdoor commitment scheme based on strong RSA assumption. Ateniese and de Medeiros [3] presented an RSA-based trapdoor (chameleon) hash function without key exposure, which can be used to obtain a commitment scheme based on RSA in the sense of Gennaro [15]. In the following, we recall this well known commitment scheme.

- **Key Generation Algorithm:** Let t and k be security parameters. Let $n = pq$ be the product of two primes $p, q \in \{2^{k-1}, \cdots, 2^k - 1\}$. A random prime integer $e > 2^t$ is relatively prime to the order $\phi(n) = (p-1)(q-1)$ of the multiplicative residues modulo n. The secret key d is computed such that $ed = 1 \mod \phi(n)$. The master public key is (n, e) and the master trapdoor is (p, q, d).
- **Commitment Algorithm:** Let $\mathcal{C} : \{0,1\}^* \to \{0, \cdots, 2^{2k} - 1\}$ be a secure hash-and-encode scheme, mapping arbitrary strings to integers less than n. Given a specific public key $g = \mathcal{C}(L)$ in $\mathbb{Z}_n^*$, the specific trapdoor is extracted as $B = g^d \mod n$. To commit to x $(0 \leq x < e)$ the sender chooses $r \in_R \mathbb{Z}_n^*$ and computes $Com = g^x r^e \mod n$, *i.e.*, the commitment algorithm is

$$Com(x, r) = g^x r^e \mod n.$$

- **Open Algorithm:** To decommit the sender reveals x, r and the receiver can verify the validity by checking $0 \leq x < e$ and the above equation.

Lemma 1. *[3] Under the RSA assumption the scheme Com described above is an unconditionally secret, computationally binding double-trapdoor commitment scheme. The specific trapdoor information is* $B = g^d \mod n$.

3.2 Okamoto's Receipt-free Voting Scheme

In this section we briefly introduce Okamoto's receipt-free voting scheme [23]. The participants of this scheme are voters V_i $(1 \leq i \leq I)$, an administrator A, and a timeliness commission member T. Let (e, n) be the RSA public key of A for signatures, and H be a hash function. We also denote $S_{V_i}(m)$ the signature of V_i for message m, and $E_A(m)$ the encryption of m using A's public key. The scheme consists of the following stages:

- **Authorizing Stage:** Let p and q be prime such that $q|p-1$, g and h be independently selected generators of subgroup of $\mathbb{Z}_p^*$ with order q.
  - V_i randomly generates $\alpha_i \in \mathbb{Z}_q$, and calculates $G_i = g^{\alpha_i} \mod p$. V_i makes his/her vote v_i and computes

$$m_i = BC(v_i, r_i) = g^{v_i} G_i^{r_i} \mod p$$

    using random number r_i, here $BC(v_i, r_i)$ is a trapdoor commitment. V_i chooses a random number $t_i \in \mathbb{Z}_n^*$ and computes

$$x_i = H(m_i || G_i) t_i^e \mod n.$$

V_i generates his/her signature $z_i = S_{V_i}(x_i)$ for x_i. V_i also computes $E_A(x_i||z_i||ID_{V_i})$ and sends it to A.

- A decrypts the message and checks that voter V_i has the right to vote, by using the voter's list. A also checks whether V_i has already applied. If V_i does not have the right or has already applied, A rejects. If V_i is accepted, A checks the signature z_i of message x_i. If they are valid, then A generates signature $y_i = x_i^{1/e} \mod n$ and sends y_i to V_i.
- V_i obtains A's signature $s_i = H(m_i||G_i)^{1/e} \mod n$ of message m_i.

– **Voting Stage:** V_i sends $(m_i||G_i, s_i)$ to the bulletin board through an anonymous channel. V_i also sends (v_i, r_i, m_i) to T through an untappable anonymous channel.
– **Claiming Stage:** V_i checks that his/her ballot is listed on the bulletin board. If not, V_i claims this by showing $(m_i||G_i, s_i)$.
– **Counting Stage:** T publishes the list of votes v_i in random order on the board, and also shows a non-interactive modification of zero-knowledge proof, σ, to prove that the list of v_i contains only correct open values of the list of m_i without revealing the linkage between m_i and v_i. In other words, T publishes $(v'_1, \cdots, v'_I)$, which is a random order list of v_i. That is, $v'_i = v_{\pi(i)}$ $(1 \le i \le I)$, here π is a random permutation of I elements. Given $(m_1, \cdots, m_I)$ and $v'_1, \cdots, v'_I$, T proves that he knows (π, r_i) such that

$$m_i = BC(v_i, r_i), \;\; v'_i = v_{\pi(i)}.$$

This scheme satisfies the property of receipt-free if and only if the voter knows the value of α_i, *i.e.*, he can open the commitment freely using α_i such that $v_i + \alpha_i r_i = v'_i + \alpha_i r'_i \mod q$. However, if α_i is generated by a coercer C, and C forces V_i to use $G_i = g^{\alpha_i} \mod p$ for V_i's commitment, then V_i cannot open the commitment in more than one way without the information of α_i. Hence the voting scheme is not receipt-free.

Okamoto [24] proposed an improved voting scheme using voting booth, which is a stronger physical assumption than untappable channel. The improved scheme is almost the same as the original one except for an additional procedure in the voting stage as follows:

V_i proves to T through an anonymous voting booth that V_i knows α_i in a zero-knowledge manner. If T accepts V_i's proof, then T accepts his vote. This enforces V_i knows the information α_i in any conditions. Therefore, the receipt-free is satisfied.

4 Proposed Receipt-free Voting Scheme

4.1 High-level Description of the Scheme

As stated above, only when the voter V_i knows the information of the trapdoor, he can open the commitment freely. In Okamoto's improved scheme [24], V_i must prove he knows the trapdoor in a zero-knowledge manner through a stronger assumption of voting booth.

In this paper, we still use the weaker physical assumption of untappable channel as in [23] to construct a receipt-free voting scheme. The key point is how to make the voters to obtain the trapdoor information. We will use the double trapdoor commitment scheme in section 3.1 to reach the aim. Note that the specific trapdoor in the commitment scheme is an RSA signature of the administrator A. Moreover, the signature is also a proof that V_i is an eligible voter. Therefore, V_i must know the specific trapdoor, which is generated by A and the coercer C can not control this.

Note that both Okamoto's schems [23, 24] and our scheme can assume no anonymous channel through the use of the mix-net method [10].

4.2 Our Voting Scheme

The participants of our scheme are I eligible voters V_i $(1 \leq i \leq I)$, an administrator A, and L timeliness commission members T_i $(1 \leq i \leq L)$. We assume that the number of collusive timeliness commission members is no more than a threshold Γ. Let (e, n) be the RSA public key of A for signatures, where e is a sufficiently large prime, and $\mathcal{C} : \{0,1\}^* \rightarrow \{0, \cdots, 2^{2k} - 1\}$ be a secure hash-and-encode scheme, mapping arbitrary strings to integers less than n. We also denote $S_{V_i}(m)$ the signature of V_i for message m, and $E_A(m)$ the encryption of m using A's public key. We assume that a legitimate vote is a prime p satisfying $1 < p < e$. The scheme consists of the following stages:

– **Authorizing Stage:**

- V_i chooses a random number $t_i \in \mathbb{Z}_n^*$ and a random message m_i, he then computes

$$x_i = {t_i}^e \mathcal{C}(m_i) = {t_i}^e J_i \mod n,$$

where $\mathcal{C}(m_i) = J_i$. V_i generates his/her signature $z_i = S_{V_i}(x_i)$ for x_i. V_i also computes $E_A(x_i||z_i||ID_{V_i})$ and sends it to A.

- A decrypts the message and checks that voter V_i has the right to vote, by using the voter's list. A also checks whether V_i has already applied. If V_i does not have the right or has already applied, A rejects. If V_i is accepted, A checks the signature z_i of message x_i. If they are valid, then A generates signature $y_i = x_i^{\frac{1}{e}} \mod n$ and sends y_i to V_i.
- V_i obtains A's signature $s_i = J_i^{\frac{1}{e}} \mod n$ of message m_i.

– **Voting Stage:**
- V_i makes his/her vote v_i and computes

$$H_i = BC(v_i, r_i) = J_i^{v_i} {r_i}^e \mod n$$

using a double-trapdoor commitment scheme based on RSA.
- V_i sends (H_i, m_i) and (a, b) to the bulletin board through an anonymous channel, here (a, b) is a knowledge proof of s_i. The non-interactive knowledge proof can be constructed as follows: Choose a random number $u \in \mathbb{Z}_n^*$ and define $a = u^e \mod n, c = \mathcal{H}(H_i, m_i, a)$, and $b = us_i^c \mod n$, where $\mathcal{H}$ is a cryptographic hash function. If $b^e = a\mathcal{C}(m_i)^c \mod n$, the proof is accepted.
- V_i makes Γ-out-of-L secret shares for secret triple (s_i, v_i, r_i) and then sends the j-th shares (s_i^j, v_i^j, r_i^j) and H_i to T_j $(1 \leq j \leq L)$ through an untappable channel.

– **Claiming Stage:** V_i checks that his/her ballot is listed on the bulletin board. If not, V_i claims this by showing (H_i, m_i, a, b).

– **Counting Stage:** All of the timeliness commission members T_j $(1 \leq j \leq L)$ together recover the secret (s_i, v_i, r_i). If s_i is a valid signature for message m_i, they publish the list of votes v_i in a random order on the board, and also show a non-interactive zero-knowledge proof σ to prove that the list of v_i contains only correct open values of the list of H_i without revealing the linkage between H_i and v_i. In other words, T_j $(1 \leq j \leq L)$ publish $(v'_1, \cdots, v'_I)$, which is a random order list of v_i. That is, $v'_i = v_{\pi(i)}$ $(1 \leq i \leq I)$, where π is a random permutation of I elements. Given $(H_1, \cdots, H_I)$ and $(v'_1, \cdots, v'_I)$, T_j $(1 \leq j \leq L)$ together prove that they know (π, r_i) such that

$$H_i = BC(v_i, r_i), \;\; v'_i = v_{\pi(i)}.$$

The detailed description of how to calculate σ can be found in section 5. In section 5.4, we present a zero-knowledge proof σ which is similar to [24]. In section 5.5, we present a much more efficient zero-knowledge proof.

4.3 Security Analysis

Theorem 1. *The proposed scheme satisfies the properties of completeness, privacy, soundness, unreusability, eligibility, fairness, verifiability, receipt-freeness.*

Proof. We show that our scheme satisfies all the security properties listed in section 2.2.

- *Completeness*: Since V_i can check that his/her vote listed on the bulletin board, any valid vote are counted correctly.
- *Privacy*: Due to the blind signature scheme, the relation of the pairs between (x_i, ID_{V_i}) and (m_i, s_i) is hidden. In the voting stage, (s_i^j, v_i^j, r_i^j) and H_i are sent to T_j $(1 \leq j \leq L)$ through an untappable channel, therefore, no one can trace the communication and violet the privacy of the voter. In the claiming stage, the voter only show the pair (H_i, m_i, a, b) to claim the disruption. In the counting stage, the votes v_i is listed in a random order, so no one can know the relation between ID_{V_i} and v_i.
- *Soundness*: In the counting stage, T_j $(1 \leq j \leq L)$ can together check the validity of a vote with

$$H_i = BC(v_i, r_i) = J_i^{v_i} {r_i}^e \mod n.$$

- *Unreusability*: To vote twice, the voter must have two valid signatures of A. However, A issues only one (blind) signature for each eligible voter.
- *Eligibility*: Only the person who has the signature of A is allowed to vote.
- *Fairness*: The counting stage is done after the claiming stage and T provides a knowledge proof that v_i' is a permutation of v_i, no one can affect the result of voting.
- *Verifiability*: This is ensured by the zero-knowledge proof σ provided by T.
- *Receipt-freeness*: The receipt-freeness of the proposed scheme can be deduced from the property of double-trapdoor commitment scheme. Note that with the specific trapdoor s_i, the voter V_i can open the commitment in any ways. That is, given any vote v_i^*, V_i can compute $r_i = r_i^* s_i^{v_i^* - v_i} \mod n$ such that

$$J_i^{v_i} {r_i}^e = J_i^{v_i^*} {r_i^*}^e \mod n.$$

Note that the specific trapdoor s_i is generated by A and used to provide a zero-knowledge proof that V_i is eligible, so C can not control the value of s_i freely. Moreover, V_i sends (s_i^j, v_i^j, r_i^j) to T_j $(1 \leq j \leq L)$ through an untappable channel, so V_i must know the information of s_i. Also, the list of votes v_i are published in a random order on the board, the coercer C can not know the relation between v_i and H_i. Therefore, even the voter V_i provides the coercer C a pair (H_i, v_i^*, r_i^*) such that $H_i = J_i^{v_i^*} r_i^{*e} \mod n$, which is not a receipt that v_i^* is V_i's vote. □

4.4 Efficiency Analysis

The computation complexity of the Authorizing stage and Voting stage in our proposed scheme is almost the same as that of Okamoto's scheme, which only needs three modular exponentiations. The most time-consuming operation in our voting scheme is also computing the non-interactive zero-knowledge proof σ in the Counting stage. The complexity of computing σ in the Okamoto's scheme is $O(Ik)$, where I is the number of the voters and $k > 80$ is a security parameter. However, the complexity of our scheme is only $O(I)$ due to a more efficient secret permutation representation with a product of primes. Therefore, our scheme is about k times more efficient than Okamoto's scheme.

5 Knowledge Proof of Secret Permutation

In this section, we present zero-knowledge proofs of secret permutations. We begin with sub-protocols and use the conventional notation

$$ZK\{x|(y,x) \in \mathcal{R}\}$$

to denote a zero-knowledge proof protocol that the prover knows a secret witness x of y for the NP-relation $\mathcal{R}$. Meanwhile, we argue that the following interactive protocol can be easily converted into a non-interactive one if we use a one-way hash function.

5.1 Proof of Knowledge of Double-trapdoor Commitment

Let $y = g^x r^e \mod n$ be a double-trapdoor commitment as defined in section 3.1. We recall the protocol to prove the knowledge of (x, r) to an honest verifier without a strict range check of x. In this case, x is indeed a represent of the equivalent class $[x] = \{x + ae\}$ for integers a. We

denote the protocol by $ZK\{x, r|y = g^x r^e \mod n\}$. We follow Okamato's construction [22] to present the following protocol:

The prover randomly chooses $\alpha \in \{0, 1, \cdots, e^2\}, a \in \mathbb{Z}_n^*$ and sends $A = g^\alpha a^e \mod n$ to the verifier. The verifier challenges with a random integer $c \in \{0, 1, \cdots, e\}$. The prover answers with $\beta = \alpha + cx, b = ar^c \mod n$. The verifier accepts the proof if $g^\beta b^e = Ay^c \mod n$ and $0 \leq \beta < 2e^2$. Otherwise, it rejects.

5.2 Equality Proof of Double-trapdoor Commitments

This protocol is to prove that two double-trapdoor commitments as defined above commit to the same message. We denote the protocol by $ZK\{x, r_1, r_2|y_1 = g_1^x r_1^e \mod n \wedge y_2 = g_2^x r_2^e \mod n\}$, where y_1, y_2, g_1, g_2 are known.

The prover randomly chooses $\alpha \in \{0, 1, \cdots, e^2\}, a_1, a_2 \in \mathbb{Z}_n^*$ and sends $A_1 = g_1^\alpha a_1^e \mod n$ and $A_2 = g_2^\alpha a_2^e \mod n$ to the verifier. The verifier challenges with a random integer $c \in \{0, 1, \cdots, e\}$. The prover answers with $\beta = \alpha + cx, b_1 = a_1 r_1^c \mod n, b_2 = a_2 r_2^c \mod n$. The verifier accepts the proof if $g_1^\beta b_1^e = A_1 y_1^c \mod n$, $g_2^\beta b_2^e = A_2 y_2^c \mod n$ and $0 \leq \beta < 2e^2$. Otherwise, it rejects.

5.3 Inequality Proof of Committed Value

We present a protocol to prove that a committed value in the above double-trapdoor is not zero and denoted the protocol by

$$ZK\{x, r|g^x r^e \mod n \wedge x \neq 0\}.$$

The protocol can be constructed using the above protocol as follows: $ZK\{x, r, x', t, R|y = g^x r^e \mod n \wedge z = y^{x'} s^e \mod n \wedge z/g^{xx'} = R^e \mod n \wedge xx' \neq 0\}$, here xx' will be given to the verifier.

5.4 Knowledge Proof of Secret Permutation

Assume that π be a permutation on $\{1, \cdots, I\}$ and $\{x'_1, \cdots, x'_I\}$ be an open set of integers for $0 < x'_i < e$. This protocol is to prove the knowledge of permutation π such that $y_i = g_i^{x_i} r_i^e$ and $x_{\pi(i)} = x'_i$. Denote the protocol by

$$\sigma = ZK\{\pi, r_i|y_i = g_i^{x_i} r_i^e \mod n \wedge x_{\pi(i)} = x'_i \wedge 1 \leq i \leq I\}.$$

The detailed protocol is as follows.

1. The prover generates random permutation $\tau \in S_I$, and randomly chooses $v_i, w_i \in \mathbb{Z}_n^*$, and computes

$$Y_i = y_i v_i^e \mod n,\ Z_i = g_{\tau(i)}^{x'_{\tau(i)}} w_i^e \mod n.$$

   The prover sends $\{Y_i, Z_i\}$ to the verifier.
2. The verifier randomly selects a challenge bit $c \in \{0, 1\}$ and sends it to the prover.
3. If $c = 0$, the prover sends (τ, v_i, w_i) to the verifier. If $c = 1$, the prover computes $\rho = \pi^{-1} \circ \tau^{-1}$, $R_i = w_{\rho(i)}/(v_i r_i) \mod n$ and sends (ρ, R_i) to the verifier.
4. If $c = 0$, the verifier checks whether the following equations hold or not

$$Y_i = y_i v_i^e \mod n,\ Z_i = g_{\tau(i)}^{x'_{\tau(i)}} w_i^e \mod n.$$

   If $c = 1$, the verifier checks whether the following equation holds or not

$$Z_{\rho(i)}/Y_i = R_i^e \mod n.$$

5. Repeating steps 1 to 4 for $\ell = poly(|n|)$ times.

5.5 Improved Knowledge Proof of Secret Permutation

The above protocols uses the cut-and-choose technique and needs repeat $\ell \geq 80$ times and has a complexity $O(I\ell)$. In the following we present a more efficient protocol to prove the knowledge of a secret permutation.

Here, we assume that $1 < x'_i < e$ $(i = 1, \cdots, I)$ are all primes and let $x' = \prod_{i=1}^{I} x'_i$. Note that in this case,

$$\{x_{\pi(i)} = x'_i \wedge 1 \leq i \leq I\} \Leftrightarrow \{x_i \neq 1 \wedge \prod_{i=1}^{I} x_i = x'\}.$$

Then we have that

$$\sigma = ZK\{\pi, r_i | y_i = g_i^{x_i} r_i^e \mod n \wedge x_{\pi(i)} = x'_i \wedge 1 \leq i \leq I\}$$

$$\Leftrightarrow$$

$$ZK\{x_i, r_i | y_i = g_i^{x_i} r_i^e \mod n \wedge x_i \neq 1 \wedge \prod_{i=1}^{I} x_i = x'\}.$$

For $i = 1, \cdots I$, let

$$\tau_i = ZK\{x_i, r_i | y_i = g_i^{x_i} r_i^e \mod n \wedge x_i - 1 \neq 0\}.$$

Moreover, we let

$$\sigma_1 = ZK\{x_2, r_2, s_2 | z_2 = y_1^{x_2} s_2^e \mod n \wedge y_2 = g_2^{x_2} r_2^e \mod n\},$$

$$\sigma_2 = ZK\{x_3, r_3, s_3 | z_3 = z_2^{x_3} s_3^e \mod n \wedge y_3 = g_3^{x_3} r_3^e \mod n\},$$

$$\cdots$$

$$\sigma_{I-1} = ZK\{x_I, r_I, s_I | z_I = z_{I-1}^{x_I} s_I^e \mod n \wedge y_n = g_I^{x_I} r_I^e \mod n\},$$

$$\sigma_I = \{r | z_I / g_1^{x'} = r^e \mod n\}.$$

Note that $z_I = g_1^{x_1 \cdots x_n} r^e$. We obtain that

$$\sigma = \sigma_1 \wedge \cdots \wedge \sigma_I \wedge \tau_1 \wedge \cdots \wedge \tau_I,$$

where σ_i can be completed with the basic protocol in section 4.2 and τ_i can be realized with the basic protocol in section 4.3. Since the cost of σ_i and τ_i is also $O(1)$, the cost of σ is $O(I)$. Therefore, it is more efficient than the protocol in section 5.4.

6 Conclusion

The approach for realizing electronic voting using blind signatures and anonymous channel seems to be the most suitable and promising for large scale elections. Receipt-free voting schemes can prevent vote-buying and coercion. Okamoto [23] presented a receipt-free electronic voting scheme based on this framework. However, the following paper [24] proved this scheme was not receipt-free and presented two improved schemes, one scheme requires the help of the voting commission and the other needs a stronger physical assumption of the voting booth. In this paper, we utilize the double-trapdoor commitment to propose a new receipt-free voting scheme for large scale elections. Moreover, we prove the proposed scheme satisfies the security requirements.

Acknowledgement

This work is supported by National Natural Science Foundation of China (No. 60503006 and 60633030), Natural Science Foundation of Guangdong, China (No. 05300706), 973 Program (2006CB303104), and NSFC-KOSEF Joint Research Project (No. 60611140543).

References

1. M. Abe. *Mix-networks on permutation networks*, Advances in Cryptology-ASIACRYPT 1999, LNCS 1716, pp.258-273. Springer- Verlag, 1999.
2. R. Aditya, B. Lee, C. Boyd, and E. Dawson, *An Efficient Mixnet-Based Voting Scheme Providing Receipt-Freeness*, Trustbus 2004, LNCS 3184, pp.152-161. Springer-Verlag, 2004.
3. G. Ateniese and B. de Medeiros, *On the key-exposure problem in chameleon hashes*, SCN 2004, LNCS 3352, pp.165-179, Springer-Verlag, 2005.
4. M. Abe and K. Suzuki, *Receipt-Free Sealed-Bid Auction*, ISC 2002, LNCS 2433, pp.191-199, Springer-Verlag, 2002.
5. G. Brassard, D. Chaum, and C. Crepeau, *Minimum disclosure proofs of knowledge*, Journal of Computer and System Sciences, 37(2), pp.156-189, 1988.
6. J. Benaloh and D. Tuinstra, *Receipt-free secret-ballot elections*, Proc. of 26th Symp. on Theory of Computing-STOC 1994, pp.544-553, 1994.
7. R. Cramer, I. Damgard and B. Schoenmakers, *Proofs of partial knowledge and simplified design of witness hiding protocols*, Advances in Cryptology-CRYPTO 1994, LNCS 839, pp.174-187, Springer-Verlag, 1994.
8. J. Benaloh and M. Fischer, *A robust and verifiable cryptographically secure election scheme*, Proc. 26th IEEE Symposium on the Foundations of Computer Science (FOCS), pp. 372-382, 1985.
9. R. Cramer, M. Franklin, B. Schoenmakers, and M. Yung, *Multi-authority secret-ballot elections with linear work*, Advances in Cryptology-EUROCRYPT 1996, LNCS 1070, pp.72-83, Springer-Verlag, 1996.
10. D. Chaum, *Untraceable electronic mail, return addresses, and digital pseudonyms*, Communications of the ACM, 24(2), pp.84-88, 1981.
11. D. Chaum, *Blind signature for untraceable payments*, Advances in Cryptology-EUROCRYPT 82, Plenum Press, pp.199-203, 1982.
12. R. Cramer, R. Gennaro and B. Schoenmakers, *A Secure and Optimally Efficient Multi- Authority Election Scheme*, Advances in Cryptology-EUROCRYPT 1997, LNCS 1233, pp.103-118, 1997.
13. J. Benaloh and M.Yung, *Distributing the Power of a Government to Enhance the Privacy of Voters*, Proc. 5th ACM Symposium on Principles of Distributed Computing (PODC), pp.52-62, ACM, 1986.
14. A. Fujioka, T. Okamoto, and K. Ohta, *A practical secret voting scheme for large scale election*, Advances in Cryptology- AUSCRYPT 1992, LNCS 718, pp.244-260, Springer-Verlag, 1992.
15. R. Gennaro, *Multi-trapdoor commitments and their applications to proofs of knowledge secure under concurrent man-in-the-middle attacks*, Advances in Cryptology-CRYPTO 2004, LNCS 3152, pp.220-236, Springer-Verlag, 2004.
16. J.A. Garay, M. Jakobsson, and P. MacKenzie, *Abuse-Free Optimistic Contract Signing*,Advances in Cryptology-CRYPTO 1999, LNCS 1666, pp. 449-466, Springer-Verlag, 1999.
17. M. Hirt and K.Sako, *Efficient receipt-free voting based on homomorphic encryption*, Advances in Cryptology-EUROCRYPT 2000, LNCS 1807, pp.393-403, Springer-verlag, 2000.
18. B. Lee and K. Kim, *Receipt-free electronic voting scheme with a tamper-resistant randomizer*, ICISC 2002, LNCS 2587, pp.389-406, Springer-Verlag, 2002.
19. B. Lee, C. Boyd, E. Dawson, K. Kim, J. Yang, and S. Yoo, *Providing Receipt-Freeness in Mixnet-Based Voting Protocols*, ICISC 2003, LNCS 2971, pp.245-258, Springer-Verlag, 2003.

20. M. Naor, *Bit commitment using peseudo-randomness*, Advances in Cryptology-CRYPTO 1989, LNCS 435, pp.128-136, Springer-Verlag, 1990.
21. M. Ohkubo, F. Miura, M. Abe, A. Fujioka, and T. Okamoto, *An Improvement on a Practical Secret Voting Scheme*, ISW 1999, LNCS 1729, pp. 225-234, Springer-Verlag, 1999.
22. T. Okamoto, *Provably Secure and Practical Identification Schemes and Corresponding Signature Schemes*, Advances in Cryptology-CRYPTO 1992, LNCS 740, pp. 31-53, Springer-Verlag, 1992.
23. T. Okamoto, *An electronic voting scheme*, IFIP World Conference 1996, Advanced IT Tools, pp.21-30, Chapman Hall, 1996.
24. T. Okamoto, *Receipt-free electronic voting schemes for large scale elections*, Proceeding of Workshop on Security Protocols 1997, LNCS 1361, pp.25-35, Springer-Verlag, 1997.
25. C. Park, K. Itoh, and K. Kurosawa, *Efficient anonymous channel and all/nothing election scheme.*, Advances in Cryptology-EUROCRYPT 1993, LNCS 765, pp.248-259, Springer-Verlag, 1993.
26. M. Jakobsson, *A Practical Mix*, Advances in Cryptology-EUROCRYPT 1998, LNCS 1403, pp. 448-461, Springer-Verlag, 1998.
27. K. Sako and J. Kilian, *Secure voting using partially compatible homomorphisms*, Advances in Cryptology-CRYPTO 1994, LNCS 839, pp.411-424. Springer-Verlag, 1994.
28. K. Sako and J. Kilian, *Receipt-free mix-type voting scheme: a practical solution to the implementation of a voting booth*, Advance in Cryptology-EUROCRYPT 1995, LNCS 921, pp.393-403, Springer-verlag, 1995.