Information Sciences 181 (2011) 1493–1502

Contents lists available at ScienceDirect

Information Sciences

journal homepage: www.elsevier.com/locate/ins

New receipt-free voting scheme using double-trapdoor commitment ☆

Xiaofeng Chen [a,*], Qianhong Wu [b], Fangguo Zhang [c], Haibo Tian [c], Baodian Wei [c], Byoungcheon Lee [d], Hyunrok Lee [e], Kwangjo Kim [e]

[a] Key Laboratory of Computer Networks and Information Security, Ministry of Education, Xidian University, Xi'an 710071, PR China
[b] Key Laboratory of Aerospace Information Security and Trusted Computing, Ministry of Education, Wuhan University, Wuhan 430079, PR China
[c] School of Information Science and Technology, Sun Yat-sen University, Guangzhou 510275, PR China
[d] Department of Information Security, Joongbu University, Chungnam 312-702, Republic of Korea
[e] Department of Computer Science, KAIST, Daejeon 305-714, Republic of Korea

ARTICLE INFO

Article history:
Received 18 April 2009
Received in revised form 28 January 2010
Accepted 18 December 2010
Available online 28 December 2010

Keywords:
Electronic voting
Receipt-freeness
Blind signature
Double-trapdoor commitment

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 [30] for large scale elections. However, in the following paper, Okamoto [31] proved that the scheme [30] was not receipt-free and presented two improved schemes. One scheme requires the help of the parameter registration committee 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 parameter registration committee nor the voting booth is required in our scheme. We also present a more efficient zero-knowledge proof for secret permutation. Therefore, our scheme is much more efficient than Okamoto's schemes [30,31] with the weaker physical assumptions. Moreover, we prove that our scheme can achieve the desired security properties.

© 2010 Elsevier Inc. All rights reserved.

1. Introduction

Electronic voting is one of the most significant applications of cryptography. Plenty of research work has been done in the past 20 years. The existing electronic voting schemes can be categorized by their research approaches into three types: schemes using blind signatures [21,30,31], schemes using mix-nets [1,3,10,26,32,33,36], and schemes using homomorphic encryption [7–9,17–19,24,25,35].

One essential property of electronic voting is the privacy of the ballot. If a voter is not required to keep his/her ballot secret, the voter could be coerced by a political boss or an employer with power or money into casting a certain ballot. This will affect the final result of the voting and destroy the fairness of the election. In some sense, democracy cannot be achieved since it depends on a proper and fair administration of the election. Therefore, the content of a vote should never be revealed before the counting stage of the voting. Moreover, a voter could not provide a receipt to any third party to prove that a certain vote was casted.

Benaloh and Tuinstra [8] firstly introduced the concept of receipt-freeness to solve the problems of "vote buying" or "coercion" in the electronic voting. Based on the assumption of a voting booth, they also proposed two voting schemes using homo-

☆ An extended abstract of this paper has been presented at the Eighth International Workshop on Information Security Applications, 2007, pp. 395–409 [16].

* Corresponding author.
E-mail address: xfchen@xidian.edu.cn (X. Chen).

0020-0255/$ - see front matter © 2010 Elsevier Inc. All rights reserved.
doi:10.1016/j.ins.2010.12.012

morphic encryption. 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 [24] 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 [36], 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 two receipt-free voting schemes using blind signatures were proposed by Okamoto [31], where a single-trapdoor commitment is used to ensure the receipt-freeness. However, the first scheme requires the help of the parameter registration committee and the second one needs a stronger physical assumption of the voting booth.

Our contribution. In this paper, we point out that the traditional single-trapdoor commitment is unsuitable for design receipt-free voting schemes. We then use the double-trapdoor commitment to propose a new receipt-free voting scheme based on blind signatures. Neither the parameter registration committee nor the voting booth is required in the proposed voting scheme. So, it is more efficient and practical for large scale elections than Okamoto's voting schemes [31].

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 [21,30,28], electronic cash [11,20] where anonymity is of great concern.

Fujioka, Okamoto, and Ohta [21] 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 [21] 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. [28] proposed an improved voting scheme based on blind signatures 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 [27]. However, the scheme is not receipt-free.

Okamoto [30] proposed a new voting scheme based on blind signatures. The scheme tried to use a trapdoor commitment scheme [6] to ahieve the receipt-freeness. The concept of trapdoor commitment (also called chameleon commitment) was first introduced by Brassard, Chaum, and Crepeau [6] for zero-knowledge proofs. In a trapdoor commitment scheme, the holder with a trapdoor knowledge can open a commitment in any possible way in the open phase. Therefore, the scheme satisfies the property of receipt-free only if the trapdoor information is known by the voters. Okamoto [31] 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 group of parameter registration committee, 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 [2] introduced the idea of receipt-free auctions to prevent bid-rigging in the auction protocol. In the contract 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 contract. Garay et al. [23] first introduced the concept of abuse-free contract signing to solve this problem.

1.2. Organization

The rest of the paper is organized as follows: Some preliminaries are given in Section 2. Okamoto's receipt-free voting schemes are revisited 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. Preliminaries

In this section, we first describe the model and security requirements of electronic voting, and then introduce the notion of trapdoor commitment.

2.1. Electronic voting

The participants of an electronic voting scheme are voters, administrator authorities, and tally authorities. Also, there are four kinds of physical assumption about the communication channel between participants in voting schemes.

- *Untappable channel:* it is a one-way channel between two participants. Communication through an untappable channel is perfectly secret to all other parties.

- *Voting booth:* it is a two-way channel between two participants. Communication through a voting booth is perfectly secret to all other parties. That is, a voting booth is a two-way untappable channel.
- *Anonymous channel:* it is a channel guaranteeing the anonymity of the sender. Recipient of the message that has been sent through the anonymous channel does not know the identity of the sender.
- *Bulletin board:* it is a public-broadcast channel with memory. Any party (even third-parties) can read information from the bulletin board. Any active party can post messages in a specially designed area of bulletin board, but no one can erase or overwrite messages from the bulletin board.

Generally, a voting system consists of the following stages:

- *Authorizing stage:* The administrator authorities first publish the system parameters for the election, and then verify the identities and eligibility of the voters. Only the authorized voters with a certificate issued by the administrator authorities are permitted to cast a unique vote in the election. The authorized voters also generate their public/secret key pair for the election.
- *Voting stage:* Referring to the candidate slate, the authorized voters cast their ballots to the bulletin board.
- *Claiming stage:* The voter checks whether his/her ballot is listed on the bulletin board or not. If not, the voter claims this to the administrator authorities by showing the certificate.
- *Counting stage:* The tally authorities together compute the final result of the election, along with a proof for the correctness of the result.

A secure voting scheme should satisfy the following requirements [8,21,25,31]:

- *Completeness*: All valid votes should be counted correctly.
- *Privacy*: All votes must be kept secret.
- *Soundness*: The dishonest voter cannot disrupt the voting. More precisely, the correctness of a ballot could be verified by the tally authorities.
- *Unreusability*: No voter can vote more than once.
- *Eligibility*: No one who is not allowed to vote can vote. That is, only the eligible voters can cast a ballot.
- *Fairness*: No one can falsify the result of the voting.
- *Verifiability*: Every voter can verify that the ballot-counting is performed correctly. Moreover, if the election result can be verified by any interested third party, this is called universal verifiability.
- *Receipt-freeness*: Anyone, even if the voter himself, must not be able to construct a receipt proving the content of his vote. It is trivial that receipt-freeness is strictly stronger than privacy.

2.2. Double-trapdoor commitment schemes

A commitment scheme consists of two phases, the first one in which a sender commits to a message and the second one in which the sender reveals the committed message to the receiver. A trapdoor (or chameleon) commitment scheme allows a sender to commit to a message with perfect privacy. That is, even with infinite computing power, the receiver cannot guess the committed message better than at random. This is because the sender with the trapdoor could open the commitment in any possible way. Therefore, trapdoor commitment schemes are often used to achieve the receipt-freeness in the electronic voting and auction schemes [2,12,18,30,31].

There is only one trapdoor in the traditional trapdoor commitment schemes. A potential disadvantage in the single-trapdoor trapdoor commitment schemes is that the trapdoor information will be revealed if two different opening ways are provided. This is called the key exposure problem of trapdoor commitment (or hash) schemes [4,5,13]. If the trapdoor of the victim is revealed, it is a receipt that the victim has submitted a different ballot to cheat the coercer. Therefore, we argue that there is a potential risk if a single-trapdoor trapdoor commitment scheme is used to design receipt-free voting or auction schemes.

Gennaro [22] 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. The double-trapdoor commitment schemes (or chameleon hash families) play an important role in designing efficient chameleon signatures and on-line/off-line signatures without key exposure [4,5,13–15].

Gennaro [22] proposed a multi-trapdoor commitment scheme based on the strong RSA assumption. Ateniese and de Medeiros [5] presented an RSA-based trapdoor (chameleon) hash function without key exposure, which can be used to obtain an RSA-based commitment scheme in the sense of Gennaro [22]. 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 $p,q \in \{2^{k-1}, \ldots, 2^k - 1\}$. 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 $ed = 1 \bmod \phi(n)$. The master public key is (n,e) and the master trapdoor is (p,q,d).

- *Commitment Algorithm:* Let $\mathcal{C}: \{0,1\}^* \to \{0, \ldots, 2^{2k}-1\}$ 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 $B = g^d \bmod n$. To commit to x $(0 \leqslant x < e)$ the sender chooses $r \in_R \mathbb{Z}_n^*$ and computes $Com = g^x r^e \bmod n$, i.e., the commitment algorithm is

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

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

Lemma 1 [5]. *Under the RSA assumption the scheme Com described above is an unconditionally secret, computationally binding double-trapdoor commitment scheme. The specific trapdoor information is $B = g^d \bmod n$.*

3. Revisiting Okamoto's receipt-free voting schemes

In this section we briefly introduce Okamoto's receipt-free voting schemes [30,31] and then give a further discussion about the receipt-freeness of the schemes.

The participants of the scheme [30] are voters $V_i (1 \leqslant i \leqslant I)$, 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 $G_i = g^{\alpha_i} \bmod p$. V_i makes his/her vote v_i and computes

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

    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

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

    V_i generates his/her signature $z_i = S_{V_i}(x_i)$ for x_i and then sends the ciphertext $E_A(x_i \| z_i \| ID_{V_i})$ 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 $y_i = x_i^{1/e} \bmod n$ and sends y_i to V_i.
  - V_i obtains A's signature $s_i = H(m_i \| G_i)^{1/e} \bmod n$ 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 $(v'_1, \ldots, v'_I)$, which is a random order list of v_i. That is, $v'_i = v_{\pi(i)} (1 \leqslant i \leqslant I)$, here π is a random permutation of I elements. Given $(m_1, \ldots, m_I)$ and $v'_1, \ldots, v'_I$, 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 $v_i + \alpha_i r_i = v'_i + \alpha_i r'_i \bmod q$. However, if α_i is generated by a coercer C, and C forces V_i to use $G_i = g^{\alpha_i} \bmod p$ 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 [31] proposed an improved voting scheme using a voting booth, which is a stronger physical assumption than an 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.

Further analysis: 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 [31], V_i must prove he knows the trapdoor in a zero-knowledge manner through a stronger assumption of the voting booth. However, we argue that the Okamoto's voting scheme cannot achieve the receipt-freeness if the (only) timeliness commission member colludes with the coercer. Consider the following new attack of Okamoto's scheme which used only one timeliness commission member: Suppose the voters can choose the trapdoor freely and make trapdoor commitment on their votes. The coercer/buyer cannot check whether the voter performs according to his order since the voter can open his vote in any possible way. But if the timeliness commission member is dishonest, he can provide the original opening of a commitment to the coercer. If one voter opens the commitment in another way when being asked by the coercer, then the coercer/buyer can use the collision to compute the voter's trapdoor as a receipt. If the victim

submitted a vote as the coercer/buyer ordered, he just opened the commitment in the same way. This is also a receipt that the victim submitted a certain vote. Therefore, we argue that the threshold trust model is more suitable for Okamoto's receipt-free voting schemes.

4. Our proposed receipt-free voting scheme

4.1. High-level description of the scheme

In this paper, we still use the weaker physical assumption of the untappable channel as in [30] to construct a receipt-free voting scheme. The key point is how to make the voters obtain the trapdoor information. We will use the double trapdoor commitment scheme in Section 2.2 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 cannot control this. On the other hand, all commission members together recover the specific trapdoor in the counting stage. Therefore, when a dishonest commission member T_j provides C a collision for a certain commitment, it cannot be viewed as a proof since he can also open the commitment freely.

Note that both Okamoto's schemes [30,31] 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 $V_i(1 \leqslant i \leqslant I)$, an administrator A, and L timeliness commission members $T_i(1 \leqslant i \leqslant L)$. 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 $\mathcal{C}: \{0,1\}^* \to \{0, \ldots, 2^{2k}-1\}$ 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
    $$x_i = t_i^e \mathcal{C}(m_i) = t_i^e J_i \bmod n,$$
    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 $y_i = x_i^{\frac{1}{e}} \bmod n$ and sends y_i to V_i.
  - V_i obtains A's signature $s_i = J_i^{\frac{1}{e}} \bmod n$ of message m_i, which can be viewed as a certificate issued by A.
- *Voting stage:*
  - V_i makes his/her vote v_i and computes
    $$H_i = BC(v_i, r_i) = J_i^{v_i} r_i^e \bmod n$$
    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 $a = u^e \bmod n$, $c = \mathcal{H}(H_i, m_i, a)$, and $b = u s_i^c \bmod n$, where $\mathcal{H}$ is a cryptographic hash function. If $b^e = a\mathcal{C}(m_i)^c \bmod n$, 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 $T_j(1 \leqslant j \leqslant L)$ 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 $T_j(1 \leqslant j \leqslant L)$ 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, $T_j(1 \leqslant j \leqslant L)$ publish $(v'_1, \ldots, v'_I)$, which is a random order list of v_i. That is, $v'_i = v_{\pi(i)} (1 \leqslant i \leqslant I)$, where π is a random permutation of I elements. Given $(H_1, \ldots, H_I)$ and $(v'_1, \ldots, v'_I)$, $T_j(1 \leqslant j \leqslant L)$ 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 [31]. In Section 5.5, we present a much more efficient zero-knowledge proof.

Remark 1. For the simplicity of description, we use an administrator A in the proposed voting scheme which is the same as [21,30,31]. However, it is difficult to find a fully trusted third party in the internet. If the administrator A is not honest, he can

produce a valid record (H_i,m_i,a_i,b_i) on the bulletin board without being traced and thus falsify the final result of the election. All the previous schemes [21,30,31] suffer from this problem. Trivially, the problem can be solved if we use multiple administrators. For more details, please refer to [30,31].

Remark 2. As an anonymous referee suggested, there should exist a physical shelter for each voter to perform the whole voting process in order to avoid the physical attack in the real applications.

4.3. Security analysis

In this section, we prove that our voting scheme satisfies all the security properties listed in Section 2.1.

Theorem 1. *The proposed scheme satisfies the properties of completeness.*

Proof 1. During the claiming stage, V_i can check whether his/her vote is listed on the bulletin board. This ensures that any valid vote are counted correctly.

Theorem 2. *The proposed scheme satisfies the properties of privacy.*

Proof 2. 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 $T_j(1 \leqslant j \leqslant L)$ 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.

Theorem 3. *The proposed scheme satisfies the properties of soundness.*

Proof 3. In the counting stage, $T_j(1 \leqslant j \leqslant L)$ can together check the validity of a vote with the equation

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

Theorem 4. *The proposed scheme satisfies the properties of unreusability.*

Proof 4. To vote twice, the voter must have two valid certificates of A. However, A issues only one (blind) signature for each eligible voter. □

Theorem 5. *The proposed scheme satisfies the properties of eligibility.*

Proof 5. During the authorizing stage, only the eligible voter V_i can obtain a valid certificate (m_i,s_i) of A. Furthermore, only the eligible voter V_i could provide a knowledge proof for s_i in the voting stage. □

Theorem 6. *The proposed scheme satisfies the properties of fairness.*

Proof 6. The counting stage is done after the claiming stage and $T_j(1 \leqslant j \leqslant L)$ together provide a knowledge proof that v_i' is a permutation of v_i, hence no one can affect the result of voting. □

Theorem 7. *The proposed scheme satisfies the properties of verifiability.*

Proof 7. Due to the zero-knowledge proof σ provided by $T_j(1 \leqslant j \leqslant L)$, any interested party could verify the result of the election. □

Theorem 8. *The proposed scheme satisfies the properties of Receipt-freeness.*

Proof 8. 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 way. That is, given any vote v_i^*, V_i can compute $r_i = r_i^* s_i^{v_i^* - v_i} \bmod n$ such that

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

Table 1
Comparison with Okamoto's receipt-free voting schemes.

Properties	Scheme 1 [31]	Scheme 2 [31]	Our scheme
Computation (Authorizing stage)	(l + 4) *E* + 1*C* (Sign) + 1*C* (Enc)	4*E* + 1*C* (Sign) + 1*C* (Enc)	1*E* + 1*C* (Sign) + 1*C* (Enc)
Computation (Voting stage)	l*E*	1*E*	4*E*
Computation (Counting stage)	*O* (kl)	*O* (kl)	*O* (l)
Commitment scheme	Single trapdoor	Single trapdoor	Double trapdoor
Assumption	Untappable channel; PRC	Voting booth	Untappable channel

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* cannot control the value of s_i freely. Also, the list of votes v_i are published in a random order on the board, the coercer *C* cannot 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 $H_i = J_i^{v_i^*} r_i^{*e} \bmod n$, which is not a receipt that v_i^* is V_i's vote.

On the other hand, note that $T_j (1 \leqslant j \leqslant L)$ together recover the specific trapdoor in the counting stage, so any commission member can also open a commitment freely at this time. That is, when a dishonest commission member T_j provides *C* a collision (v_i, r_i) for a certain commitment H_i, it cannot be viewed as a proof since he can present any collision for the commitment. □

4.4. Efficiency analysis

We compare the efficiency of our scheme with that of Okamoto's receipt-free voting schemes [31]. We denote by *C*(Sign) and *C*(Enc) the computation cost of performing a signature and encryption, respectively. We also denote by *E* the modular exponentiation, and by *l* the number of parameter registration committee (PRC). We omit other operations such as modular multiplication and hash in all schemes. Table 1 presents the comparison between Okamoto's schemes and our scheme.

The computation complexity of the Authorizing stage and Voting stage in our proposed scheme is almost the same as that of Okamoto's second scheme. 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 schemes is $O(kl)$, where *l* is the number of the voters and $k > 80$ is a security parameter. However, the complexity of our scheme is only $O(l)$ due to a more efficient secret permutation representation with a product of primes. Therefore, our scheme is about $O(k)$ times more efficient than Okamoto's scheme.

In the following, we present the comparison in details. In Okamoto's schemes [30,31], each vote requires $2k$ modular exponentiations with double bases for each T_j. If we assume that $|p| = 1024$ and $|q| = 160$, then each modular exponentiation requires 160×1.75 modular multiplications with 1024 bits on average using standard binary method for double bases. Therefore, the total computational complexity for σ is about $560k$ modular multiplications per vote for each T_j, which is less than *k* RSA decryptions with 1024 bit modulus [30]. In our proposed scheme, we also assume $|n| = 1024$ and $|e| = 160$. The computation for each σ_i and τ_i requires about 5 modular exponentiations with double bases, respectively. So, the total computational complexity for σ is about less than 5 RSA decryptions with 1024 bit modulus per vote for each T_j. Currently, an RSA decryption with 1024 bit modulus only takes about 1.92 ms on a 3 GHz Pentium IV [34]. If we assume the number of the voter is 1 million, then the total time of computing σ is less than 3 h. Therefore, our voting scheme is practical for large scale elections.

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 $y = g^x r^e \bmod n$ be a double-trapdoor commitment as defined in Section 2.2. 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 $ZK\{x,r|y = g^x r^e \bmod n\}$. We follow Okamato's construction [29] to present the following protocol:

The prover randomly chooses $\alpha \in \{0, 1, \ldots, e^2\}, a \in \mathbb{Z}_n^*$ and sends $A = g^\alpha a^e \bmod n$ to the verifier. The verifier challenges with a random integer $c \in \{0,1, \ldots, e\}$. The prover answers with $\beta = \alpha + cx, b = ar^c \bmod n$. The verifier accepts the proof if $g^\beta b^e = Ay^c \bmod n$ and $0 \leqslant \beta < 2e^2$. 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 $ZK\{x, r_1, r_2 | y_1 = g_1^x r_1^e \bmod n \wedge y_2 = g_2^x r_2^e \bmod n\}$, where y_1, y_2, g_1, g_2 are known.

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

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

The protocol can be constructed using the above protocol as follows:

$ZK\{x, r, x', s, R | y = g^x r^e \bmod n \wedge z = y^{x'} s^e \bmod n \ \wedge z / g^{xx'} = R^e \bmod n \ \wedge xx' \neq 0\}$, here xx' will be given to the verifier.

5.4. Knowledge proof of secret permutation

Assume that π be a permutation on $\{1, \ldots, I\}$ and $\{x'_1, \ldots, x'_I\}$ 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

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

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

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

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 $\rho = \pi^{-1} \circ \tau^{-1}$, $R_i = w_{\rho(i)} / (v_i r_i) \bmod n$ and sends (ρ, R_i) to the verifier.

(4) If $c = 0$, the verifier checks whether the following equations hold or not

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

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

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

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

5.5. Improved knowledge proof of secret permutation

The above protocol uses the cut-and-choose technique and needs repeat $\ell \geqslant 80$ 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 $1 < x'_i < e (i = 1, \ldots, I)$ are all primes and let $x' = \prod_{i=1}^I x'_i$. Note that in this case,

$$\{x_{\pi(i)} = x'_i \wedge 1 \leqslant i \leqslant I\} \Longleftrightarrow \left\{ x_i \neq 1 \wedge \prod_{i=1}^I x_i = x' \right\}.$$

Then we have that

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

$$\Longleftrightarrow$$

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

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

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

Moreover, we let

$$\sigma_1 = ZK\{x_2, r_2, s_2 | z_2 = y_1^{x_2} s_2^e \bmod n \ \wedge y_2 = g_2^{x_2} r_2^e \bmod n\},$$
$$\sigma_2 = ZK\{x_3, r_3, s_3 | z_3 = z_2^{x_3} s_3^e \bmod n \ \wedge y_3 = g_3^{x_3} r_3^e \bmod n\},$$
$$\ldots$$
$$\sigma_{I-1} = ZK\{x_I, r_I, s_I | z_I = z_{I-1}^{x_I} s_I^e \bmod n \wedge y_n = g_I^{x_I} r_I^e \bmod n\},$$
$$\sigma_I = ZK\{r | z_I / g_1^{x_I} = r^e \bmod n\}.$$

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

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

where σ_i can be completed with the basic protocol in Section 5.2 and τ_i can be realized with the basic protocol in Section 5.3. 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 channels seems to be the most suitable and promising for large scale elections. Receipt-free voting schemes can prevent the problem of vote-buying and coercion. Okamoto [30] presented a receipt-free electronic voting scheme based on this framework. However, the following paper [31] proved this scheme was not receipt-free and presented two improved schemes, one scheme requires the help of the parameter registration committee 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 desired security requirements.

Acknowledgements

The authors are grateful to the anonymous referees for their invaluable suggestions for improving this paper. This work is supported by the National Natural Science Foundation of China (Nos. 60970144, 60503006, 61003244, 61070168, and 60803135), the Fundamental Research Funds for the Central Universities (Nos. K50510010003 and JY10000901034), and Program of the Science and Technology of Guangzhou, China (No. 2008J1-C231-2).

Appendix A. An example of zero-knowledge proof σ for $I = 3$

Input: (H_1, H_2, H_3) and (v'_1, v'_2, v'_3) such that each v'_i for $i = 1,2,3$ is a prime less than e.
Prove: T proves that he knows (π, r_i) such that $H_i = J_i^{v_i} r_i^e$ and $v'_i = v_{\pi(i)}$ for $i = 1,2,3$ without revealing (π, r_i) as follows:

(1) *T* provides the zero-knowledge proof τ_i for $i = 1,2,3$. Note that

$$\tau_i = ZK\{v_i, r_i | H_i = J_i^{v_i} r_i^e \bmod n \wedge v_i - 1 \neq 0\}.$$

This is equivalent to prove

$$ZK\{v_i, r_i | H_i / J_i = J_i^{v_i - 1} r_i^e \bmod n \wedge v_i - 1 \neq 0\}.$$

Trivially, τ_i can be completed with the basic protocol in Section 5.3.

(2) *T* provides the zero-knowledge proof σ_i for $i = 1,2,3$. Note that

$$\sigma_1 = ZK\{v_2, r_2, s_2 | z_2 = H_1^{v_2} s_2^e \bmod n \wedge H_2 = J_2^{v_2} r_2^e \bmod n\},$$

$$\sigma_2 = ZK\{v_3, r_3, s_3 | z_3 = z_2^{v_3} s_3^e \bmod n \wedge H_3 = J_3^{v_3} r_3^e \bmod n\},$$

$$\sigma_3 = ZK\{r | z_3 / J_1^{v'_1 v'_2 v'_3} = r^e \bmod n\}.$$

Trivially, σ_i can be completed with the basic protocol in Section 5.2. Moreover, if we define $r = r_1^{v_2 v_3} s_2^{v_3} s_3$, then $z_3 = J_1^{v_1 v_2 v_3} r^e$. So we have $v_1 v_2 v_3 = v'_1 v'_2 v'_3$.

Note that if v'_i is a prime, $v_i > 1$, and $v_1 v_2 v_3 = v'_1 v'_2 v'_3$, it is trivial that $v'_i = v_{\pi(i)}$. This is the main trick of zero-knowledge proof $\sigma = \sigma_1 \wedge \sigma_2 \wedge \sigma_3 \wedge \tau_1 \wedge \tau_2 \wedge \tau_3$.

References

[1] M. Abe, Mix-networks on permutation networks, Advances in Cryptology-ASIACRYPT 1999, LNCS, 1716, Springer-Verlag, 1999. pp. 258–273.

[2] M. Abe, K. Suzuki, Receipt-free sealed-bid auction, ISC 2002, LNCS, 2433, Springer-Verlag, 2002. pp. 191–199.
[3] R. Aditya, B. Lee, C. Boyd, E. Dawson, An efficient mixnet-based voting scheme providing receipt-freeness, Trustbus 2004, LNCS, 3184, Springer-Verlag, 2004. pp. 152–161.
[4] G. Ateniese, B. de Medeiros, Identity-based chameleon hash and applications, Financial Cryptography and Data Security 2004, LNCS, 3110, Springer-Verlag, 2004. pp. 164–180.
[5] G. Ateniese, B. de Medeiros, On the key-exposure problem in chameleon hashes, SCN 2004, LNCS, 3352, Springer-Verlag, 2005. pp. 165–179.
[6] G. Brassard, D. Chaum, C. Crepeau, Minimum disclosure proofs of knowledge, Journal of Computer and System Sciences 37 (2) (1988) 156–189.
[7] J. Benaloh, M. Fischer, A robust and verifiable cryptographically secure election scheme, in: Proc. 26th IEEE Symposium on the Foundations of Computer Science (FOCS), 1985, pp. 372–382.
[8] J. Benaloh, D. Tuinstra, Receipt-free secret-ballot elections, in: Proc. of 26th Symp. on Theory of Computing-STOC 1994, 1994, pp. 544–553.
[9] J. Benaloh, M. Yung, Distributing the power of a government to enhance the privacy of voters, Proc. Fifth ACM Symposium on Principles of Distributed Computing (PODC), ACM, 1986. pp. 52–62.
[10] D. Chaum, Untraceable electronic mail, return addresses, and digital pseudonyms, Communications of the ACM 24 (2) (1981) 84–88.
[11] D. Chaum, Blind signature for untraceable payments, Advances in Cryptology-EUROCRYPT, 82, Plenum Press, 1982. pp. 199–203.
[12] X. Chen, B. Lee, K. Kim, Receipt-free electronic auction schemes using homomorphic encryption, ICISC 2003, LNCS, 2971, Springer-Verlag, 2003. pp. 259–273.
[13] X. Chen, F. Zhang, K. Kim, Chameleon hashing without key exposure, ISC 2004, LNCS, 3225, Springer-Verlag, 2004. pp. 87–98.
[14] X. Chen, F. Zhang, W. Susilo, Y. Mu, Efficient generic on-line/off-line signatures without key exposure, ACNS 2007, LNCS, 4521, Springer-Verlag, 2007. pp. 18–30.
[15] X. Chen, F. Zhang, W. Susilo, Y. Mu, H. Lee, K. Kim, Efficient generic on-line/off-line (threshold) signatures without key exposure, Information Sciences 178 (21) (2008) 4192–4203.
[16] X. Chen, Q. Wu, F. Zhang, B. Wei, B. Lee, H. Lee, K. Kim, New receipt-free voting scheme using double-trapdoor commitment, in: The Eighth International Workshop on Information Security Applications, 2007, pp. 395–409.
[17] R. Cramer, I. Damgard, B. Schoenmakers, Proofs of partial knowledge and simplified design of witness hiding protocols, Advances in Cryptology-CRYPTO 1994, LNCS, 839, Springer-Verlag, 1994. pp. 174–187.
[18] R. Cramer, M. Franklin, B. Schoenmakers, M. Yung, Multi-authority secret-ballot elections with linear work, Advances in Cryptology-EUROCRYPT 1996, LNCS, 1070, Springer-Verlag, 1996. pp. 72–83.
[19] R. Cramer, R. Gennaro, B. Schoenmakers, A secure and optimally efficient multi-authority election scheme, Advances in Cryptology-EUROCRYPT 1997, LNCS, 1233, Springer-Verlag, 1997. pp. 103–118.
[20] C. Fan, Ownership-attached unblinding of blind signatures for untraceable electronic cash, Information Sciences 176 (3) (2006) 263–284.
[21] A. Fujioka, T. Okamoto, K. Ohta, A practical secret voting scheme for large scale election, Advances in Cryptology-AUSCRYPT 1992, LNCS, 718, Springer-Verlag, 1992. pp. 244–260.
[22] 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, Springer-Verlag, 2004. pp. 220–236.
[23] J. Garay, M. Jakobsson, P. MacKenzie, Abuse-free optimistic contract signing, Advances in Cryptology-CRYPTO 1999, LNCS, 1666, Springer-Verlag, 1999. pp. 449–466.
[24] M. Hirt, K. Sako, Efficient receipt-free voting based on homomorphic encryption, Advances in Cryptology-EUROCRYPT 2000, LNCS, 1807, Springer-Verlag, 2000. pp. 393–403.
[25] B. Lee, K. Kim, Receipt-free electronic voting scheme with a tamper-resistant randomizer, ICISC 2002, LNCS, 2587, Springer-Verlag, 2002. pp. 389–406.
[26] B. Lee, C. Boyd, E. Dawson, K. Kim, J. Yang, S. Yoo, Providing receipt-freeness in mixnet-based voting protocols, ICISC 2003, LNCS, 2971, Springer-Verlag, 2003. pp. 245–258.
[27] M. Naor, Bit commitment using peseudo-randomness, Advances in Cryptology-CRYPTO 1989, LNCS, 435, Springer-Verlag, 1990. pp. 128–136.
[28] M. Ohkubo, F. Miura, M. Abe, A. Fujioka, T. Okamoto, An improvement on a practical secret voting scheme, ISW 1999, LNCS, 1729, Springer-Verlag, 1999. pp. 225–234.
[29] T. Okamoto, Provably secure and practical identification schemes and corresponding signature schemes, Advances in Cryptology-CRYPTO 1992, LNCS, 740, Springer-Verlag, 1992. pp. 31–53.
[30] T. Okamoto, An electronic voting scheme, IFIP World Conference 1996, Advanced IT Tools, Chapman Hall, 1996. pp. 21–30.
[31] T. Okamoto, Receipt-free electronic voting schemes for large scale elections, Proceeding of Workshop on Security Protocols 1997, LNCS, 1361, Springer-Verlag, 1997. pp. 25–35.
[32] C. Park, K. Itoh, K. Kurosawa, Efficient anonymous channel and all/nothing election scheme, Advances in Cryptology-EUROCRYPT 1993, LNCS, 765, Springer-Verlag, 1993. pp. 248–259.
[33] M. Jakobsson, A practical mix, Advances in Cryptology-EUROCRYPT 1998, LNCS, 1403, Springer-Verlag, 1998. pp. 448–461.
[34] M. Scott, N. Costigan, W. Abdulwahab, Implementing cryptographic pairings on smartcards, CHES 2006, LNCS, 4249, Springer-Verlag, 2006. pp. 134–147.
[35] K. Sako, J. Kilian, Secure voting using partially compatible homomorphisms, Advances in Cryptology-CRYPTO 1994, LNCS, vol. 839, Springer-Verlag, 1994. pp. 411–424.
[36] K. Sako, 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, Springer-Verlag, Berlin, 1995. pp. 393–403.