ELSEVIER

Computer Communications 22 (1999) 279–286

computer communications

A secure and practical electronic voting scheme

Wei-Chi Ku, Sheng-De Wang*

Department of Electrical Engineering, National Taiwan University, Taipei, Taiwan

Received 9 January 1998; received in revised form 19 August 1998; accepted 19 August 1998

Abstract

Electronic voting schemes can be divided into homomorphism encryption and anonymous channel based schemes. The former type requires massive communications and computation, thereby, inappropriate for large-scale voting. However, the soundness of the latter type heavily relies on the cooperation of the voters. Under these schemes, voting is disrupted if some voter abstains in the intermediate stages. In this article, we present a secure electronic voting scheme of the latter type. The proposed scheme is practical in that its assumptions are quite appropriate for realistic environments. More specifically, the soundness of the proposed scheme does not rely on the cooperation of the voters. © 1999 Elsevier Science B.V. All rights reserved.

Keywords: Electronic voting schemes; Anonymous channel; Cryptographic techniques

1. Introduction

Voting is widely regarded as an effective means for people to express their opinions on a given topic. Theoretically, the intentions of the voters and the voting method can affect the voting results. Conventional paper-based voting methods are inconvenient for voters and then will diminish the accuracy of the voting results. Voters living far from their domiciled homes, e.g., students and servicemen from out of town, may waive their voting rights. Therefore, increasing emphasis has been placed on developing electronic voting schemes capable of providing more efficient voting services than the conventional paper-based voting methods.

However, an electronic voting also allows for the possibility of adversaries to affect or even disrupt voting in an easier way even if there is a tiny security flaw in the design. Fujioka, et al. [1] indicated that a secure electronic voting scheme should fulfill several security requirements. First, only the eligible voters can vote and each voter can vote only once. The ballots of the eligible voters should be correctly accumulated in the tally. In addition, the ballot should be secret so that others cannot infer the intention of the voter. With ballot secrecy, the voter may feel free to express his or her intentions without fear of retribution. As the voted ballots lack physical protections such as the polling boxes in conventional voting methods, the results of the voting should be verifiable. Further, the voting cannot be disrupted by the voter regardless of whether or not he or she will be traced. Such a requirement is critical when applying the voting scheme to a large-scale environment. Moreover, the intermediate results cannot be learned by anyone so that the further voting will not be affected.

Many electronic voting schemes [1–18] have been proposed. These schemes can be categorized as either homomorphism encryption based or anonymous channel based. Obviously, a secure scheme of either type should fulfill the security requirements mentioned earlier. However, a theoretically secure scheme will be considered impractical if its assumption is unreasonable or its involved communications and computation are notably high. From this perspective, no scheme is secure and practical. The schemes belonging to the first type require massive communications and computation, therefore, are unsuitable for large-scale voting. Schemes belonging to the second type, which involve several stages, contain the assumption that no voter abstains from the voting in the intermediate stages. However, it is unrealistic to assume that all the voters follow the protocol. Clearly, these schemes are not sound in real environments, i.e., any voter can easily disrupt the voting. This article constructs a secure electronic voting scheme also belonging to the second type. Particularly, the soundness of the proposed scheme does not rely on the cooperation of the voters.

The rest of this article is organized as follows: Section 2 briefly reviews previous work on voting schemes. Section 3 presents an electronic voting scheme belonging to the

* Corresponding author. Tel.: + 886-223635251 Ext. 441; e-mail: sdwang@hpc.ee.ntu.edu.tw

PII: S0140-3664(98)00241-2

second type. Next, Section 4 analyzes the security of the proposed scheme. According to those results, the proposed scheme fulfills all the security requirements for a secure voting scheme. Further, the proposed scheme and other schemes are compared. Conclusions are finally made in Section 5.

2. Literature review

Chaum [2] pioneered the notion of electronic voting in 1982. Several concrete schemes (e.g., Yao [3] and Demillo et al. [4]) have been subsequently proposed. In these schemes, the voters must send encrypted messages back and forth until they all are convinced of the outcome of the voting, i.e., each voter cannot vote independently. These schemes are inappropriate for large-scale environments because a failure of a single voter would disrupt the voting. Many voting schemes [1,5–18] for large-scale environments have been proposed. In general, these schemes can be divided into homomorphism encryption based and anonymous channel based [1]. The homomorphism encryption technique conceals the content of votes, while the anonymous channel technique conceals the identity of the voters.

Cohen and Fisher [12] proposed the original scheme of the first type. Several schemes of this type have been proposed by Benaloh and Yung [13], Iversen [14], and Sako and Kilian [15], respectively, with each one having its merits and limitations. These schemes use a higher degree of residue encryption technique. In general, the schemes of the first type require massive communications and computation, thereby making them inappropriate for large-scale voting.

As this study focuses on constructing a scheme of the second type, schemes of the second type are addressed more emphatically. The schemes of the second type are constructed over the anonymous channel, such as the untraceable email system [2] and the public bulletin board system [6]. An anonymous channel is a channel that can suppress the origin of the message. Chaum [2] pioneered the concept of an anonymous channel, the sender untraceable email system, which assumes that at least one *mix* is trust. The prototype of the second type is also proposed by Chaum [2,5]. Though a single failure of a voter will disrupt the voting, it is guaranteed that the failure can be traced. Later, Nurmi et al. [7] proposed an electronic voting scheme based on ANDOS protocols [19]. To obtain the secrets of the authority as ballots, the voters must communicate with each other. In addition, the voter can easily disrupt the voting. Similar problem can also be found in the scheme proposed by Nurmi and Salomaa [8]. Boyd [9,10] proposed a voting scheme based on multiple key ciphers. However, that scheme is limited because the authority can falsify the ballots.

In 1992, Fujioka et al. [1] stressed the importance of fairness for voting. For example, knowledge of the intermediate results could distort further voting. They proposed a voting scheme capable of solving the fairness problem by using the bit-commitment function [26]. No one, including the authority, can know the intermediate result of the voting. However, the security of their scheme relies on the assumption that no voter abstains in the intermediate stages of the voting. Later, they proposed another scheme [6] based on a public bulletin board, which is used as the anonymous channel. Such a bulletin board is realized by a committee of several members that can perform the same function as the *mix* in Ref. [2]. Their scheme requires an enormous amount of communications to send the ballot from the voter to the ballot box. In addition, its security relies on the cooperation of the voters.

Many schemes belonging to the second type suffer from ballot collision because they use random strings to distinguish each voter's ballot. To resolve this problem, Juang and Lei [11] proposed a scheme based on the so-called *uniquely blind signature* technique. If each voter is cooperative, his or her ballot does not collide with those of others. Clearly, such an assumptions is unrealistic. In addition, an adversary can impersonate a legitimate voter and falsely cast a ballot, thereby violating the voting right which belongs to that eligible voter. Further, their scheme does not provide fairness.

Despite their contributions, schemes belonging to the second type are limited in that the security relies on the cooperation of the voters. Voting would be disrupted if any voter abstains in the intermediate stages. In other words, these schemes are not sound. This weakness restricts their practical applications.

3. The proposed scheme

In this section, we present an electronic voting scheme based on the anonymous channel. The model of the proposed scheme involves voters, an eligibility checker (E), a ballot collector (C), and a set of N scrutineers (S_1, S_2, …, S_N). The institution E is used to verify the eligibility of the voter, and C is used to collect the ballots. In contrast to E and C, the scrutineers S_1, S_2, …, S_N are separately administered by the candidates and some unbiased parties (e.g., the court). The scrutineers are installed to prevent C from improperly handling the voted ballots, and it is assumed that at least one scrutineer is responsible at any moment.

The voting procedure consists of three stages: registration state, collecting stage, and opening stage. Each voter can choose to participate thoroughly, to participate but abstain in the intermediate stages (the collecting stage or the opening stage), or not to participate at all. Restated, we do not assume that no voter abstains in the intermediate stages. Alternatively, we assume that the voter who has registered but then abstains in the collecting stage agrees to transfer his

or her voting right to the authority. In contrast, the voting right of the voter who has registered but then abstains in the opening stage will not be transferred to the authority. A table ET is installed in E and is used to record the registration information of the registered voters. Another table CT is installed in C to record all voted ballots. Both tables are public throughout the whole voting.

As RSA cryptosystem [20] is the basic building block of the proposed scheme, we briefly introduce it for the readers' convenience. To establish a RSA cryptosystem, two large primes p and q should be first selected and kept secretly. Then the modulo of the cryptosystem, n, whose value is defined by the product of p and q, is published. The security of RSA is based on the factorization problem in that it is computationally infeasible to compute the factors of n, i.e., p and q. When a public key e is selected, the corresponding private key d can be computed according to the equation $(e) \times (d) = 1 \pmod{(p-1) \times (q-1)}$. Knowing the value of $(p-1) \times (q-1)$, one can compute d from e by using the Fermat's Little Theorem or the Extended Euclidean Algorithm [25]. Given a message $m \in (0, n)$, its corresponding ciphertext c can be derived by computing $c = m^e \pmod{n}$. Then, the plaintext m can be recovered by computing $c^d = m^{e \times d} = m \pmod{n}$. The symmetry in modular arithmetic, encryption and decryption are mutual inverses. Therefore, RSA can also be used as a digital signature scheme. Given a message $m \in (0, n)$, its corresponding signature s can be derived by computing $s = m^d \pmod{n}$. Then, s can be verified by checking whether $s^e \pmod{n}$ equals m. For simplicity, we use (p, q, n, e, d) to denote an instance of RSA.

Another cryptographic technique used in the proposed scheme is the blind signature technique proposed in [21], whose security is based on the difficulty of factoring a large composite integer. The blind signature scheme can be applied to the situation that a signature requester wants to obtain the signature of another principal, the signer, on a message without leaking its content. In contrast to a general signature scheme, the blind signatures scheme ensures *unlinkability*, i.e., the signature requester can prevent the signer from acquiring the exact correspondence in the actual signing process. That is, the signer cannot derive the content of the message presented by the signature requester.

In the proposed scheme, we also assume the existence of a one-way permutation function f. The one-way permutation function f satisfies: (a) Given x, it is easy to compute $f(x)$; (b) For two distinct values x_1 and x_2, the values of $f(x_1)$ and $f(x_2)$ are not equal, and (c) Given $f(x)$ it is computationally infeasible to determine x. Some researchers [22,23] are convinced that the discrete logarithm function $f(x) = g^x \bmod P$, where g is a generator of the cyclic group under the modulo P, is a one-way permutation function when P is a large prime and x is an integer with large entropy within the range $(0, P)$.

In the scheme, each participant (excluding the scrutineer) should select his or her own RSA cryptosystem. E and C determine their RSA cryptosystems, denoted by $(p_E, q_E, n_E, e_E, d_E)$ and $(p_C, q_C, n_C, e_C, d_C)$, respectively. Each voter, say voter i, determines his RSA cryptosystem $(p_i, q_i, n_i, e_i, d_i)$. To prevent reblocking [20], n_i should be selected such that $n_i > \{V \| n_E\}$, where V is the voting identifier and $\|$ denotes the concatenation operation. The voting identifier is a long random number that no one knows its value prior to the voting. All n's and e's of the participants should be made public in a way that they can be accessed and verified by anyone, e.g. by using ISO/ITU-T X.509 [21].

To simplify the description of the protocol, two Boolean functions, including *Registered*( ) and *Unique*( ), are used. The function *Registered*(β) is true only when voter β has registered for voting and *Unique*(γ) is true only when ballot γ differs from other ballots listed on CT. The expression $A \rightsquigarrow B$: m represents that the message m is transmitted from A to B by the anonymous channel. The instruction *SKIP* means leaving off the current step and go to the next step and, the instruction *TERM* means terminating the transaction. ID_i is the plaintext identity of voter i. The notation sel_i denotes the intention of voter i.

3.1. Registration stage

Step 1. Voter i:

1. generates three secret keys, $k1_i, k2_i$, and $k3_i$ such that $\{\mathrm{ID}_i \| k1_i\} < P$, $\{sel_i \| k2_i\} < P$, and $k3_i < n_E$.
2. computes tag_i : $tag_i = f(\{\mathrm{ID}_i \| k1_i\})$.
3. computes h_i (the hidden sel_i) : $h_i = f(\{sel_i \| k2_i\})$.
4. computes b_i : $b_i = \{V \| tag_i \| h_i\}$.
5. computes sb_i : $sb_i = (k3_i)^{e_E}(b_i) \bmod n_E$.
6. computes the registration request req_i : $req_i = (\{V \| sb_i\})^{d_i} \bmod n_i$.

The secret keys, $k1_i$, $k2_i$, and $k3_i$, are unpredictable long random numbers. The token tag_i is used to distinguish the ballot of voter i from those of others and, therefore, should be unique. In addition, ID_i cannot be inferred from tag_i. Clearly, uniquely assigning tag_i by the authority would allow one to trace the ballots. However, randomly assigning tag_i would cause ballot collision when the number of voters is large. As ID_i is unique and $k1_i$ is an unpredictable long random numbers, the value $tag_i = f(\{\mathrm{ID}_i \| k1_i\})$ can be used to distinguish the ballot of voter i from others without revealing ID_i according to the property of one-way hash function. Similarly, as $h_i = f(\{sel_i \| k2_i\})$ and $h_j = f(\{sel_j \| k2_j\})$, $h_i \neq h_j$ when the values of sel_i and sel_j are distinct.

To prevent E from placing a spurious or old req_i on ET, sb_i is concatenated with V before it is encrypted with d_i in Step 1 (6). As sb_i is computed under the module n_E and $\{V \| sb_i\}$ is encrypted under the module n_i, it is necessary that $n_i > \{V \| n_E\}$; otherwise, it is not guaranteed that $\{V \| sb_i\}$ can be recovered from req_i. Such a problem is commonly referred to as the reblocking problem of RSA [20]. The generation procedure of req_i is depicted in Fig. 1.

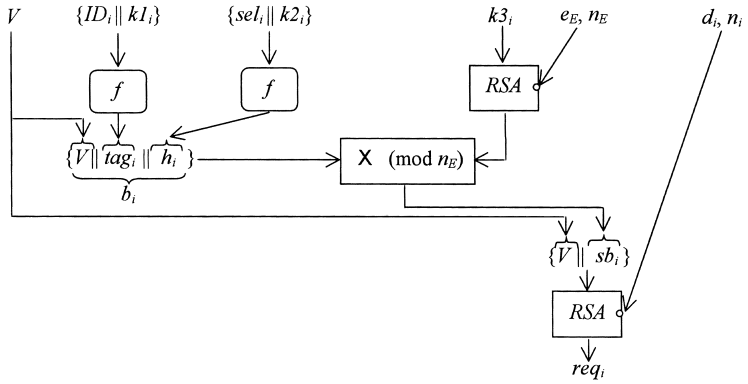

Fig. 1. The generation procedure of req_i.

Step 2. Voter $i \rightarrow E$: (ID_i, req_i).

Step 3. E:

if (ID_i matches an eligible voter's identity)

if (not *Registered*(ID_i))

deciphers req_i with e_i to obtain $\{V \| sb_i\}$;
if (V is correct)

computes the blind voting ticket y_i : $y_i = (sb_i)^{d_E} \bmod n_E$;
stores req_i and y_i in the entry of voter i on ET;

else *TERM* //V is incorrect.

else *SKIP* //*Registered*(ID_i).

else *TERM* //ID_i does not match any eligible voter's identity.

If ID_i is valid and req_i and y_i have been recorded in the entry of voter i on ET, i.e., voter i has registered before, E directly skips to Step 4. This checkpoint can prevent voter i from voting more than once and avoid unnecessary computations. As ET is public during the whole voting, y_i is used as the evidence that E has signed sb_i.

Step 4.$E \rightarrow$ voter i : y_i.

Step 5. Voter i:

1. computes the voting ticket t_i:

$$t_i = (y_i)(k3_i)^{-1} \bmod n_E = ((sb_i)^{d_E} \bmod n_E)(k3_i)^{-1} \bmod n_E$$

$$= (((k3_i)^{e_E}(b_i))^{d_E})(k3_i)^{-1} \bmod n_E$$

$$= (k3_i)(b_i)^{d_E}(k3_i)^{-1} \bmod n_E = (b_i)^{d_E} \bmod n_E;$$

2. if $((t_i)^{e_E} \bmod n_E = (b_i))$

stores t_i;

else go to Step 2.

In the registration stage, the blind signature technique [24] is used in a way that voter i is the signature requester and E is the signer. According to the property of the blind signature technique, voter i can obtain the voting ticket t_i (i.e., the signature of E on b_i) without revealing its content to E. The content of ET after the registration stage may look like Table 1.

3.2. Collecting stage

Step 1. $i \rightsquigarrow C$: t_i.
Step 2. C:

1. computes $(t_i)^{e_E} \bmod n_E (= \{V \| tag_i \| h_i\})$;
2. if (V is correct) and ($Unique(\{tag_i \| h_i\})$).

computes the corresponding receipt z_i : $z_i = \{tag \| h_i\}^{d_C} \bmod n_C$;
stores(t_i, tag_i, h_i, z_i) into the least unused entry, supposed w_i, of CT;

else *TERM*.

The fact that we do not assume that the voter uses f properly to generate his tag allows for the possibility that two or more tags will be the same. In Step 2 (2), we verify the uniqueness of $\{tag_i \| h_i\}$ instead of only tag_i alone. As mentioned earlier, different *sel*s produce different *h*s. Therefore, the ballot whose tag is not produced properly does not collide with the ballots containing different intentions. In contrast, the ballot whose tag is not generated properly may at most collide with the ballots containing the same

Table 1
The content of ET after the registration stage

	Registration information	
Voter ID	Registration request	Blind voting ticket
ID_1	req_1	y_1
ID_2	—	—
ID_3	req_3	y_3
⋮	⋮	⋮
ID_i	req_i	y_i
⋮	⋮	⋮

Table 2
The content of CT after the collecting stage

Entry	Voting ticket	Receipt	Ballots			Key
			Tag	Hidden *sel*	Opened *sel*	
1	t_j	z_j	tag_j	h_j	—	—
2	t_u	z_u	tag_u	h_u	—	—
3	t_l	z_l	tag_l	h_l	—	—
⋮	⋮	⋮	⋮	⋮	⋮	⋮
w_i	t_i	z_i	tag_i	h_i	—	—
⋮	⋮	⋮	⋮	⋮	⋮	⋮

Table 3
The content of CT after the opening stage

Entry	Voting ticket	Receipt	Ballots			Key
			Tag	Hidden *sel*	Opened *sel*	
1	t_j	z_j	tag_j	h_j	sel_j	$k2_j$
2	t_u	z_u	tag_u	h_u	—	—
3	t_l	z_l	tag_l	h_l	sel_l	$k2_l$
⋮	⋮	⋮	⋮	⋮	⋮	⋮
w_i	t_i	z_i	tag_i	h_i	sel_i	$k2_i$
⋮	⋮	⋮	⋮	⋮	⋮	⋮

intention, which implies that the uncooperative voter cannot invalidate the ballots containing different intentions.

Step 3. $S_1, S_2, \ldots, S_N$:

if $((t_i, tag_i, h_i, z_i)$ is not correctly recorded on CT))

force C to fix it.

As assumed in the proposed scheme, if any voted ballot is not correctly handled, at least one scrutineer forces C to fix it immediately. Therefore, the voted ballots are ensured to be correctly handled. As assumed earlier, the voter who has registered but then abstains in the collecting stage is willing to transfer his or her voting right to the authority. If some registered voters abstain in the collecting stage, the tally of the records on ET exceeds the tally of the collected ballots on CT. The authority can stuff ballots up to the number of the difference between these two tables after the deadline of the collecting stage and before the starting time of the opening stage. The content of CT after the collecting stage may look like Table 2.

3.3. Opening stage

Step 1. Voter i:

locates out the entry number of (t_i, tag_i, h_i, z_i) on CT, i.e., w_i;

$\rightsquigarrow C : w_i, k2_i, sel_i$

Step 2. C:

1. if (sel_i is valid)

   retrieves the data in the w_i entry of CT;

   else *TERM*;

2. if $(h_i = f(\{sel_i \| k2_i\}))$

   enters $(k2_i, sel_i)$ to the w_i entry of CT;

   else *TERM*.

By looking up CT, voter i can locate the entry number of his ballot, say w_i. To open his or her ballot, voter i sends w_i, $k2_i$, and sel_i to C through the anonymous channel. If sel_i is valid, C computes $f(\{sel_i \| k2_i\})$ and then verifies whether it equals the retrieved h_i from w_i entry. If they are equal, the ballot of voter i is thus successfully opened.

Step 3. $S_1, S_2, \ldots, S_N$:

If $(k2_i, sel_i)$ is not correctly recorded in the w_i, entry of CT)

force C to fix it.

As assumed, if any ballot is not correctly opened, at least one scrutineer forces C to fix it. The ballots on CT can be divided into two kinds, unopened and opened ones. After the deadline of the opening stage, C counts the ballots and announces the result. As CT is public all the time, anyone can also verify the voting result announced by C. The content of CT after the opening stage may look like Table 3.

4. Security analysis and comparisons

In this section, we analyze the security of the proposed scheme and then compare it with several similar schemes.

4.1. Security analysis of the proposed scheme

Fujioka et al. [1] defined the security requirements for a secure electronic voting scheme. Herein, their definition is adapted, with slight modification in expression, as the security criteria for the proposed scheme.

Definition 1. An electronic voting scheme is secure if it has the following properties:

1. *Completeness*: all ballots are counted correctly.
2. *Soundness:* no voter can disrupt the voting.
3. *Privacy:* all ballots must be secret.
4. *Unreusability:* no voter can vote twice.
5. *Eligibility:* only the eligible voters can vote.
6. *Fairness:* no one can know the intermediate results of the voting.
7. *Verifiability:* the result of the voting can be verified.

In the following, we demonstrate that the proposed scheme fulfills these requirements by using seven lemmas as in the following:

Lemma 1 (completeness). All ballots are counted correctly in the proposed scheme.

Proof. As it is assumed that at least one of the scrutineers $S_1, S_2, \ldots, S_N$ is responsible at any moment in the voting, no valid ballot is dropped or wrongly handled. The ballot of a registered voter which does not collide with other ballots is accepted and correctly counted. However, if a ballot collision occurs, only one of the collided ballots is accepted and correctly counted. Assume that the two collided ballots come from voter i and voter j, the collision implies $(tag_i \| h_i) = (tag_j \| h_j)$, or equivalently, $tag_i = tag_j$ *and* $h_i = h_j$. Equation $tag_i = tag_j$ indicates that at least one voter does not generate his tag properly. If the ballot of voter i is accepted first, the ballot of voter j is rejected. Then, the voting right of voter j will be transferred to the authority. As f is a one-way permutation function, h_i is the value of $f(\{sel_i \| k2_i\})$, and h_j is the value of $f(\{sel_j \| k2_j\})$, $h_i = h_j$ means $\{sel_i \| k2_i\} = \{sel_j \| k2_j\}$, i.e., $sel_i = sel_j$ *and* $k2_i = k2_j$ An uncooperative voter can at worst inhibit his or her own voting right or the voting right of the voters who have the same intention. However, the voter should know such an effect and then determine whether he or she should generate his or her tag properly or not. Therefore, all ballots are counted correctly, i.e., the proposed scheme is complete. □

Lemma 2 (soundness). No voter can disrupt the voting in the proposed scheme.

Proof. The voting is disrupted if the tally of the records on CT exceeds the tally of the records on ET. Each voter can only have four legal choices in the voting: (a) not to register, (b) to register but abstain in the collecting stage, (c) to register and participate the collecting stage but abstains in the opening stage, and (d) to participate the registration stage, the collecting stage, and the opening stage. If he or she chooses (a), the tallies of the records on CT and the records on ET are not influenced. In situation (c) and (d), both tallies are increased by one. However, if the voter chooses (b), his or her voting right is taken over by the authority and then both tallies are also increased by one. Thus, no legal action disrupts the voting. However, consider a situation in which the voter does not act legally. Under this circumstance, invalid and duplicated voting tickets are rejected in Step 2 (2) of the collecting stage. Actually, a voter can falsify the voting ticket only when he or she has obtained d_E, which contradicts the assumption that RSA is secure. Thus, no voter can disrupt the voting, i.e., the proposed scheme satisfies soundness. □

Lemma 3 (privacy). All ballots must be secret, i.e., the relationship between the voter and his ballot is concealed in the proposed scheme.

Proof. The adversary can understand the relationship between voter i and his intention sel_i in three different ways. First, the relationship of tag_i and sel_i is bounded on CT after the opening stage. Then, if the adversary can derive ID_i from tag_i, the privacy of voter i is violated. Clearly, if the value of tag_i is assigned with a random number, the adversary cannot infer ID_i from it. Contrarily, if ID_i can be inferred from properly generated tag_i, the privacy of voter i is violated. However, as the properly generated tag_i equals the value of $f(\{ID_i \| kl_i\})$, this hypothesis clearly contradicts the property of the one-way permutation function. Second, if the adversary can know the sender's identity of the t_i transmitted in Step 1 of the collecting stage or the sender's identity of the $(w_i, k2_i, sel_i)$ transmitted in Step 1 of the opening stage, the privacy of voter i is violated. However, this hypothesis contradicts the assumption that the untraceable email system can suppress the origin of the transmitted message. Third, sel_i is opened from h_i in the opening stage and the anonymity of voter i is not protected in the registration stage. Then, if the content of b_i (containing h_i) can be known in the registration stage, the privacy of voter i is violated. This hypothesis contradicts the assumption that the blind signature scheme is secure. Therefore, the proposed scheme ensures the voter's privacy. □

Lemma 4 (unreusability). In the proposed scheme, no voter can vote twice.

Proof. In the registration stage, voter i can only obtain one y_i. From y_i he or she can compute at most one voting ticket t_i. As a voting ticket which collides with one recorded on CT would be rejected in the collecting stage, reusing the same voting ticket is useless. However, as V is unique and can be used as a nonce between voter i and E_i reusing old voting ticket is useless. In addition, as V is an unpredictably long number, its value is unknown before the voting starts. Therefore, voter i cannot reserve a voting ticket for future voting. Therefore, the proposed scheme satisfies unreusability. □

Lemma 5 (eligibility). In the proposed scheme, only the eligible voters can vote.

Proof. As n_i is selected by voter i and d_i is kept secret by him or herself, voter i can be impersonated by the adversary to register when RSA is broken. However, this contradicts the assumption that RSA is secure. In addition, as n_E is selected by E and d_E is kept by him or herself, an adversary

can falsify a voting ticket only when he or she has obtained d_E, thereby contradicting the assumption that RSA is secure. Therefore, the proposed scheme satisfies the criterion of eligibility. □

Lemma 6. (fairness). No one can know the intermediate results of the voting in the proposed scheme.

Proof. The intention sel_i is concealed in h_i, which is the value of $f(\{sel_i \| k2_i\})$, until voter i anonymously sends $k2_i$ to C in the opening stage. As the opening stage is started only when the collecting stage is completed, no one including the authority can know sel_i in the registration stage or the collecting stage. Therefore, the proposed scheme provides fairness to the voters. □

Lemma 7 (verifiability). In the proposed scheme, the result of the voting can be verified.

Proof. Both ET and CT are public during the entire voting process. The eligibility of the registered data of voter i on ET can be verified by each individual with e_i and n_i. The ballot of voter i on CT can be verified by each individual with e_E, n_E, e_C, n_C, and the corresponding $k2_i$. Thus, the proposed scheme satisfies the criterion of verifiability. □

Theorem 1. The proposed scheme is secure.

Proof. From Lemma 1 – Lemma 7, we can infer that the proposed scheme is secure. □

4.2. Comparisons

In this subsection, we compare the proposed scheme with the schemes of Nurmi–Salomaa (NS) [8], Juang–Lei (JL) [11], and Fujioka–Okamoto–Ohta (FOO) [1]. These schemes are compared as their models and procedures resemble those of the proposed scheme. To make the comparisons unbiased, all these schemes are evaluated under the same situation in which the authority attempts to cheat and some voters are uncooperative, e.g., they may abstain from voting in the intermediate stages. As previously analyzed, the proposed scheme satisfies all the seven security requirements of a voting scheme. Herein, we only briefly address the weakness of the compared voting scheme.

First, the ballot of an eligible voter may be rejected in JL scheme and FOO scheme. Therefore, both schemes fail to provide completeness. As described in Section 2, NS scheme, JL scheme, and FOO scheme do not provide soundness, i.e., a voter can easily disrupt the voting with these schemes. With respect to privacy, all the compared schemes can ensure ballot secrecy. The fact that the ballots of NS scheme can be identical allows for a voter to vote more than once without disrupting the voting if someone else abstains in the intermediate stage. Therefore, NS scheme does not provide unreusability.

In the NS scheme, one is regarded as an eligible voter if he or she has obtained a secret within a large set of secrets. However, the adversary can attempt a sequence of subsequent values and if the density of the secrets set is not large enough, he or she can hit one. In JL scheme, an adversary can impersonate a legitimate voter to vote, simultaneously, inhibit the voting right belongs to that eligible voter. Therefore, NS scheme and JL scheme fail to provide eligibility. Among the compared schemes, only the FOO scheme can provide fairness. Restated, anyone can know the intermediate results of the voting with NS scheme or JL scheme. Further, all the compared schemes provide verifiability. The comparison results are depicted in Table 4, in which '✓'denotes the scheme satisfies the security requirement and '▲' denotes the scheme fails to satisfy the security requirements.

5. Discussion and conclusion

This article presents a secure electronic voting scheme. The proposed scheme assumes the following: (a) An anonymous channel exists, (b) A one-way permutation function exists, (c) RSA is secure, (d) At least one scrutineer is responsible at any moment in the voting, and (e) One who has registered but then abstains in the collecting stage agrees that his voting right is transferred to the authority. In the article, the effects of bribe and persecution have seldom been analyzed. Such conducts are common in conventional paper-based voting and usually led to a biased result that imparts the desired democracy. Unfortunately, these illegal matters cannot be averted in the proposed scheme. In contrast, this problem will become even more terrible and harder to resolve. Voters may be bribed or persecuted to vote for a certain candidate and are possibly obliged to vote under the supervision of the bribers or persecutors. Several receipt-free voting schemes [16–18] were designed to solve this problem. The receipt-freeness property enables voters to conceal how they have voted even from a powerful adversary who is trying to coerce him or her. However, even if an ideal receipt-free voting scheme exists, this problem is still not entirely resolved. One solution suggested herein is that sufficient voting facilities are supplied in conventional public voting booths and all the voters should choose anyone of such public voting booths to vote. In contrast to the conventional paper-based voting, the voter can choose a voting site convenient to him to vote.

Table 4
Security features of NS, JL, FOO and the proposed scheme

Requirement	Scheme NS scheme [8]	JL scheme [11]	FOO scheme [1]	Our voting scheme
Completeness	✓	▲	▲	✓
Soundness	▲	▲	▲	✓
Privacy	✓	✓	✓	✓
Unreusability	▲	✓	✓	✓
Eligibility	▲	▲	✓	✓
Fairness	▲	▲	✓	✓
Verifiability	✓	✓	✓	✓

References

[1] A. Fujioka, T. Okamoto, K. Ohta, A practical secret voting scheme for large scale elections, Advances in Cryptology – AUCRYPT'92, Springer-Verlag, Berlin, 1992, pp. 244–251.

[2] D. Chaum, Untraceable electronic mail, return addresses and digital pseudonyms, Commun ACM 24 (2) (1981) 84–88.

[3] A. Yao, Protocols for secure communications, Proceedings 23rd Annual IEEE Symposium Foundations of Computer Science, 1982 pp. 160–164.

[4] R. Demillo, N. Lynch, M. Merritt, Cryptographic protocols, Proceedings 14th Annual ACM Symposium, Theory of Computing, 1982 pp.382–400.

[5] D. Chaum, Elections with unconditionally secret ballots and disruption equivalent to breaking RSA, Advances in Cryptology – EUROCRYPT'88, Springer-Verlag, Berlin, 1988, pp. 177–182.

[6] T. Okamoto, A. Fujioka, K. Ohta, A practical large scale secret voting scheme based on non-anonymous channels, Proceedings of SCIS93, 1C, Japan, January 1993.

[7] H. Nurmi, A. Salomaa, L. Santean, Secret ballot elections in computer networks, Computer & Security 10 (1991) 553–560.

[8] H. Nurmi, A. Salomaa, Conducting secret ballot elections in computer networks: problems and solutions, Annals of Operations Research 51 (1994) 185–194.

[9] C. Body, Some applications of multiple key ciphers, Advances in Cryptology – EUROCRYPT'88, Lecture Notes in Computer Science, Springer-Verlag, Berlin, 1987, pp. 234–238.

[10] C. Boyd, A new multiple key ciphers and an improved voting scheme, Advances in Cryptology – EUROCRYPT'89, Springer-Verlag, Berlin, 1990, pp. 617–625.

[11] W. Juang, C. Lei, A collision-free secret ballot protocol for computerized general elections, Computers & Security 15 (4) (1996) 339–348.

[12] D. Cohen, M.H. Fisher, A robust and verifiable cryptographically secure election scheme, Proceedings of the 26th Annual IEEE Symposium on the Foundations of Computer Science, 1985, pp. 372–382.

[13] J. Benaloh, M. Yung, Distributing the power of a government to enhance the privacy of voters, ACM symposium on Principles of Distributed Computing, 1986 pp. 52–62.

[14] K.R. Iversen, A cryptographic scheme for computerized general elections, Advances in Cryptology – CRYPTO'91, Springer-Verlag, Berlin, 1991, pp. 405–419.

[15] K. Sako, J. Kilian, Secure voting using partially compatible homomorphisms, Advances in Cryptology – CRYPTO'94, Lecture Notes in Computer Science, Springer-Verlag, Berlin, 1995, pp. 411–424.

[16] V. Niemi, A. Renvall, How to prevent buying of votes in computer elections, Advances in Cryptology – ASIACRYPT'94, Springer-Verlag, Berlin, 1994, pp. 141–148.

[17] J. Benaloh, D. Tuinstra, Receipt free secret ballot elections, Proceedings of the 26th Annual ACM Symposium on the Theory of Computing, 1994, pp. 544–553.

[18] K. Sako, J. Kilian, Receipt-free mix-type voting scheme – a practical solution to the implementation of a voting booth, Advances in Cryptology – EUROCRYPT'95, Springer-Verlag, Berlin, 1995, pp. 393–403.

[19] A. Renvall, ANDOS: a simple protocol for secret selling of secrets, EATCS Bull. 47 (1990) 178–186.

[20] R.L. Rivest, A. Shamir, L. Adleman, A method for obtaining digital signatures and public key crypto-system, Commun. ACM 21 (1978) 120–126.

[21] ISO/ITU-T, Recommendation X.509: the directory authentication framework, 1993.

[22] W. Diffie, M.E. Hellman, New directions in cryptography, IEEE Transactions on Information Theory, IT-22, 1976, pp. 644–654.

[23] S. Pohlig, M.E. Hellman, An improved algorithm for computing logarithms over GF(p) and its cryptographic significance, IEEE Transaction on Information Theory, IT-24, 1978, pp. 106–110.

[24] D. Chaum, Blind signature for untraceable payments, Advances in Cryptology – CRYPTO'82, Springer-Verlag, Berlin, 1983, pp. 199–203.

[25] D. Knuth, The art of Computer Programming, 2, Addison-Wesley, 1981 2nd edition.

[26] K. Ohta, T. Okamoto, A. Fujioka, Secure bit commitment function, Advances in Cryptology – EUROCRYPT'92, Springer-Verlag, Berlin, 1992, pp. 324–340.