An e-Voting Scheme with Improved Resistance to Bribe and Coercion

Wei-Chi Ku and Chun-Ming Ho

Department of Computer Science and Information Engineering

Fu Jen Catholic University, Taipei, Taiwan.

wcku@csie.fju.edu.tw

Abstract. Bribe and coercion are common in conventional voting systems and usually will lead to a biased result that imparts the desired democracy. However, these problems become more difficult to solve when using e-voting schemes. Up to now, many e-voting schemes have been proposed to provide receipt-freeness and uncoercibility to solve these problems. Unfortunately, none is both secure and practical enough. In this paper, we describe an e-voting scheme that can solve or at least lessen the problems of bribe and coercion, and can be realized with current techniques. By using smart cards to randomize part content of the ballot, the voter can not construct a receipt. By using physical voting booths, bribers and coercers can not monitor the voter while he votes. Unlike conventional voting systems, the voter of the proposed scheme can choose any voting booth that is convenient and safe to him. Furthermore, the performance of the proposed schemes is optimal in that time and communication complexity for the voter is independent of the number of voting authorities.

Keywords: e-voting scheme, receipt-freeness, uncoercibility, smart cards, voting booth, homomorphic encryption

1 Introduction

Voting is regarded as one of the most effective methods for individuals to express their opinions on a given topic. However, conventional paper-based voting methods are inconvenient for voters, and therefore the accuracy of the voting results will be affected more or less. As the computing, communicating, and cryptographic techniques progress rapidly, increasing emphasis has been placed on developing e-voting (electronic voting) schemes capable of providing more efficient voting services than conventional paper-based voting methods. Some standards related to e-voting are under formulation, e.g., IEEE P1583 [20] is developing a standard for the evaluation of e-voting equipments. However, e-voting also allows for the possibility of adversaries to affect or even disrupt the voting in an easier way even if there is only a tiny security flaw in the design. It has been widely recognized that a secure e-voting scheme should satisfy not only completeness, privacy, unreusability, eligibility, fairness, verifiability, and robustness, but also receipt-freeness and uncoercibility.

In conventional voting systems, a voting booth not only allows voters to keep their ballots secret, but also prevents ballot (or vote) selling and coercion. The notions of *receipt-freeness* and *uncoercibility* for e-voting were introduced by Benaloh and Tuinstra [4]. Receipt-freeness ensures that the voter can be convinced that his ballot is counted without getting a receipt, and uncoercibility ensures that the voter can not convince the coercer of the content of his ballot. Preventing the threats of bribe and coercion in

e-voting schemes has been the subject of recent researches. Most initial receipt-free e-voting schemes such as [4, 19] assumes the existence of an untappable channel, which can guarantee the message exchanged between the communicants is perfectly secret to others. However, such an assumption can not be realized with current techniques [14]. In addition, the briber or the coercer can prescribe private random bits that the voter must use, thus neither receipt-freeness nor uncoercibility is effectively provided by these schemes.

Recently, Magkos, Burmester, and Chrissikopoulos [14] proposed a receipt-free e-voting scheme based on the *virtual voting booth* that is implemented with a smart card. Receipt-freeness is achieved by distributing the voting procedure between the voter and the smart card. The voter and the smart card jointly contribute randomness for the encryption of the ballot. However, Magkos-Burmester-Chrissikopoulos' e-voting scheme must assume that the briber or the coercer does not monitor the voter during the every moment of voting, which is clearly unreasonable, i.e., it can not effectively prevent bribe and coercion in practical environments. In this paper, we will describe a practical e-voting scheme that is an enhanced version of Magkos-Burmester-Chrissikopoulos' e-voting scheme with improved resistance to bribe and coercion. Voting booths and smart cards are used for achieving receipt-freeness and uncoercibility. To provide convenience to voters, sufficient voting facilities are supplied in sufficient public voting booths. Unlike conventional paper-based voting systems, the voter can choose any voting booth that is convenient and safe to him in the proposed e-voting scheme. By using smart cards to randomize part of content of the ballot, the voter can not construct a receipt. In addition, the time complexity and the communication complexity for the voter are independent of the number of voting authorities. Finally, we will show that the proposed e-voting scheme satisfies completeness, privacy, unreusability, eligibility, fairness, verifiability, robustness, receipt-freeness, and uncoercibility.

2 Background

In 1982, Chaum [8] pioneered the notion of e-voting, and then several concrete schemes, e.g., [11] and [23], were subsequently proposed. However, these earlier e-voting schemes are unsuitable for being deployed in large-scale environments because a failure of a single voter would disrupt the entire voting. Later, some e-voting schemes for large-scale environments have been proposed. Chaum [9] described an e-voting scheme based on the sender untraceable email system, which assumes that at least one mix is trust. Based on multiple key ciphers, Boyd [1, 2] proposed an e-voting scheme, in which the voting authority can easily falsify the ballots. Since knowledge of the intermediate results could distort further voting, Fujioka, Okamoto, and Ohta [11] proposed an e-voting scheme capable of solving the fairness problem by using the bit-commitment function. No one, including the voting authority, can know the intermediate result of the voting. In addition, they also proposed another e-voting scheme [15] based on a public bulletin board, which is realized by a committee of several members that can perform the same function as the mix specified in [8]. Unfortunately, the security of their e-voting schemes relies on the cooperation of the voters. In 1985, Cohen and Fisher [5] initially proposed an e-voting scheme based on the homomorphic encryption technique, which can conceal the content of ballots. Next, similar e-voting schemes have been proposed by Benaloh and Yung [4] and Sako and Kilian [19], respectively, with each one having its merits and limitations. In a homomorphic encryption based e-voting scheme, the voter sends an encrypted ballot through the public channel, which is often implemented by a bulletin board. The encrypted ballots can be decrypted by any set of at least t authorities. This will prevent small coalition of malicious authorities to abuse their role and to violate voter's privacy. Encryption method used for encrypting ballots is homomorphic in that multiplication of the encrypted ballots is an encrypted sum of ballots. The public should be able to distinguish between the valid and the invalid encrypted ballots. Inva-

lid ballots should be rejected. Usually, the voter is required to prove that his ballot is one of the correct forms without disclosing any other information about his ballot. However, none of the above mentioned e-voting schemes satisfies receipt-freeness, which implies that bribe and coercion can not be prevented.

In 1994, Benaloh and Tuinstra [3] initially introduced two receipt-free e-voting schemes using physical voting booths. To achieve universal verifiability, they employed a special bulletin board, which is like a broadcast channel with memory to the extent that any party can see the contents of it and each voter can post ballot by appending his ballot to the record designated for him. In particular, no party can erase anything from the bulletin board. The ballot does not reveal any information on the ballot but it is ensured by an accompanying proof that the ballot contains a valid ballot and nothing else. Unfortunately, Hirt and Sako [13] showed that Benaloh-Tuinstra's e-voting scheme is not receipt-free, and then proposed an efficient receipt-free e-voting scheme. However, Hirt-Sako's e-voting scheme must assume the existence of untappable channels from the authority to the voter, and thus can not be realized in practical environments currently [14].

In 1996, Cramer, Franklin, and Schoenmakers [6] described an e-voting scheme that can provide information-theoretic privacy by employing multiple voting authorities. The time and communication complexity for the individual voter is linear in the number of voting authorities. Later, Cramer, Gennaro, and Schoenmakers [7] proposed an improved e-voting scheme, in which time complexity and communication complexity for the voter are independent of the number of voting authorities. However, receipt-freeness is not achieved in their e-voting schemes. Recently, Magkos, Burmester, and Chrissikopoulos [14] proposed a receipt-free and uncoercible e-voting scheme that is a variant of Cramer-Gennaro-Schoenmakers' e-voting scheme with additional using of a so-called virtual voting booth that is implemented with a smart card. In particular, untappable channels are not required in their scheme. The voter and the smart card jointly contribute randomness to the encryption of the ballot. Within the virtual voting booth, the voter interactively communicates with his smart card. However, their scheme implicitly assumes that the briber or the coercer will not monitor the voter during every moment of voting, which is clearly an unreasonable assumption. That is, the use of virtual voting booths in Magkos-Burmester-Chrissikopoulos' e-voting scheme can not effectively provide uncoercibility in practical environments.

3 The Proposed e-Voting Scheme

3.1 Preliminary

The proposed e-voting scheme involves many voters and n voting authorities. A bulletin board, denoted by BB, on which each active participant can publish information, is installed to record all ballots publicly. All communications through BB is public and can be read by any party. No party can erase any information from BB, but each active participant can append messages to his own designated record. A ballot can be decrypted by any set of at least t authorities, and it is assumed that no more than t-1 voting authorities conspire. Up to now, e-voting schemes without using voting booths suffer from bribe and coercion sacrifice uncoercibility to establish correctness for the voting results, i.e., the voter may be bribed or coerced to vote for a certain candidate and is possibly obliged to vote under the supervision of bribers or coercers. In the proposed e-voting scheme, we employ the physical voting booth, denoted by VB, which can perform voter authentication. VB is only protected by guards, and is not assumed to guarantee the secrecy of the communication between the voter and voting authorities.

The proposed e-voting scheme relies on a homomorphic version of the ElGamal cryptosystem [10]. Our construction works in subgroups G_q of order q of Z_p^*, where p and q are large primes such that $q | p$-1,

and both g and G are generators of G_q. Given a message m, the encryption of m is the ElGamal encryption of G_m with base g, i.e., $(x, y) = (g^a, h^a G^m)$, where s is the secret key, $h = g^s$ is the public key, and a is a random number. All operations are performed under modulo p, and we drop the operator mod p throughout this paper for clearness. Due to the homomorphic properties of the used encryption method, a particular ElGamal encryption scheme, the final tally can be verified by any observer. Privacy of each individual ballot is guaranteed by the security strength of the ElGamal cryptosystem used to encrypt the ballot. To provide multi-way voting with L options, we select L distinct generators G_1, G_2, …, and G_L, and accumulate the ballots for each option separately. The proof of validity of the ballot (x, y) is a proof of knowledge of

$$\log_g x = \log_h (y / G_1) \vee \log_g x = \log_h (y / G_2) \vee ... \vee \log_g x = \log_h (y / G_L) .$$

The voter can generate the proof only for one generator G_j, where $j \in \{1,2,..., L\}$, thus it is guaranteed that he will vote for only one option. The voter has to show that among the elements $(x_i, y_i) = (x, y/G_i)$ for $i = 1, 2, \ldots, L$, there is a re-encryption of $(x, y) = (1, 1)$. Assume that the re-encryption of (x, y) is (x_z, y_z), where $z \in \{1,2,..., L\}$, and that the witness is v, i.e. $(x_z, y_z) = (xg^v, yh^v)$. Such a 1-out-of-$L$ re-encryption proof protocol can be illustrated by Fig. 1.

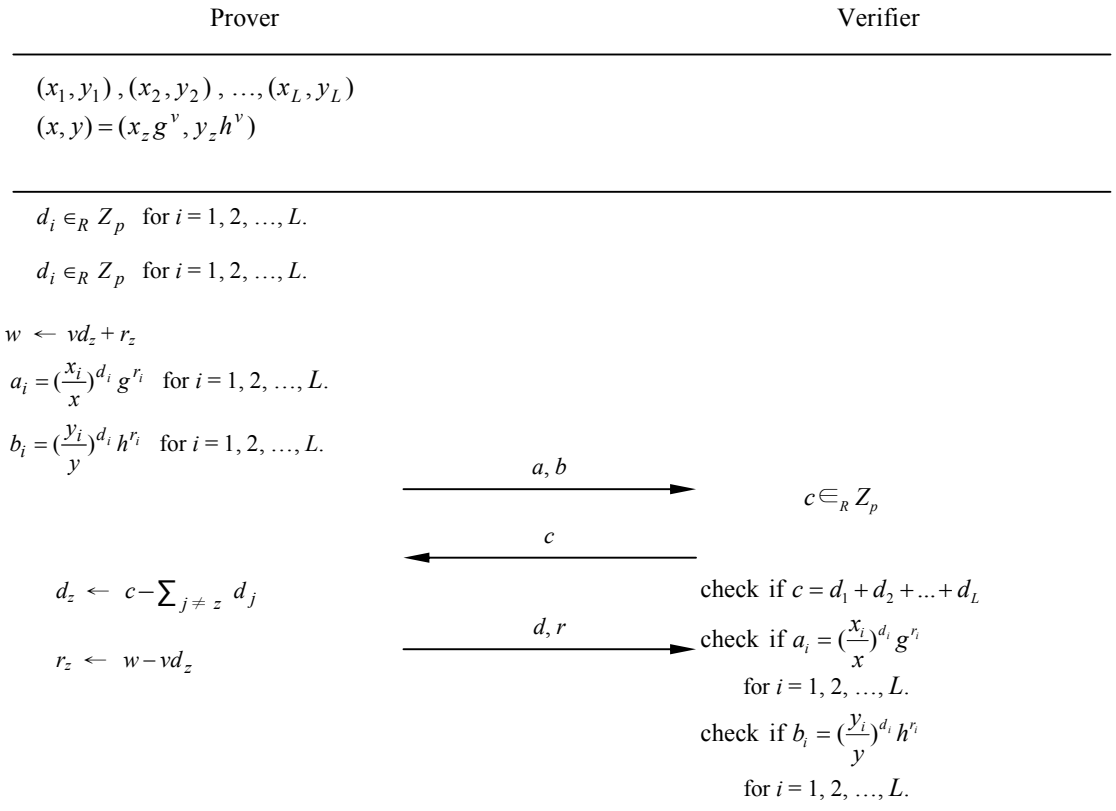

Fig. 1. The 1-out-of-L re-encryption proof.

Note that a, b, d, and r are vectors such that $a = (a_1, a_2,\ldots, a_L)$, $b = (b_1, b_2,\ldots, b_L)$, $d = (d_1, d_2,\ldots, d_L)$, and $r = (r_1, r_2,\ldots, r_L)$. The sent items a_i and b_i commit the prover to d_i and r_i for $i = 1, 2, \ldots, z-1, z+1, \ldots, L$ (excluding z). Since $a_z = g^{vd_z+r_z}$ and $b_z = h^{vd_z+r_z}$, a_z and b_z only commit the prover to a value $w = vd_z + r_z$. As the prover knows v, he can still change d_z and r_z after this round. The verifier challenges the prover to modify his d and r such that $c = d_1 + d_2 + \ldots + d_L$. Then, the prover modifies the items d_z and z_t to satisfy $c = d_1 + d_2 + \ldots + d_L$ and $w = vd_z + r_z$, and sends the modified $(d_1, d_2, \ldots, d_L)$ and $(r_1, r_2, \ldots, r_L)$ to the verifier. This persuades the verifier that among L encrypted pairs, there is only one re-encryption of (x, y) and that the prover knows the randomness of the re-encryption.

3.2 The Scheme

To join the system, the voter has to register to a voting authority first. After authentication and registration, the voter will get a personal smart card, denoted by SC, which contains the certificate of the shared public encryption key of the distributed voting authorities. Next, the voter enters his secret signature key and the certificate of the corresponding public key. It is assumed that all public key certificates are issued by the certification authority, which is administrated by a trust and independent institution. The public key certificates of all participants are published before voting. We also assume that SC is tamper-proof and can be activated only by the authentic user's unique biometric characteristic that can not be transferred to other people, e.g., fingerprints. During voting, the voter posts a ballot accompanied with a proof that the ballot is valid without revealing its actual content. Both VB and SC contribute randomness to the ballot so that the voter cannot construct a receipt. The voter has to be convinced that VB has done things correctly without finding out the randomness added by it. The voter must obtain a proof of correctness of the encryption performed by VB before submitting his ballot to BB. This proof must be non-transferable; otherwise, it may be used as a receipt for this ballot. For this purpose, the verifier can be implemented by using either the beacon [18] as a trusted source of random bits or the Fiat-Shamir heuristic [12], which is being used in the proposed e-voting scheme. A digital signature scheme, e.g., RSA or DSA, is used to control access to the various entries on BB. The ballot should be encrypted with the public key shared by the voting authorities to achieve ballot secrecy, and the voter must not know the corresponding private key for decryption. A key generation protocol is used to generate the private key, denoted by s, jointly shared by all the n voting authorities. The secrecy of ballots is protected against coalitions of up to t-1 authorities. Encrypted ballots are accumulated when ballots are aggregated. A decryption protocol [16, 17] is invoked by voting authorities to jointly decrypt the tally of the accumulated ballots without explicitly reconstructing s. Let SC_i denote the smart card of voter i. The expression 'Alice → Bob: m' represents that Alice sends m to Bob. The proposed e-voting scheme involves the ballot generation phase, the ballot casting phase, the public verification phase, and the tallying phase, and can be described as in the following.

Ballot Generation Phase

The ballot generation phase can be invoked at any time prior to the deadline of voting.

Step G1. Voter i:

- goes to a VB that is convenient and safe for him.
- authenticates to VB with his smart card SC_i that has been activated by his biometric characteristic.

Step G2. Voter i:

- uses SC_i to generate random numbers r_j for $j = 1, 2, \ldots, L$.
- uses SC_i to compute $e(j) = (g^{r_j}, h^{r_j} G_j)$ for $j = 1, 2, \ldots, L$.
- $\rightarrow$ VB : $e(j)$ (for $j = 1, 2, \ldots, L$.)

Step G3. VB:

- generates random numbers R_j for $j = 1, 2, \ldots, L$.
- computes $E(j) = (e_1(j) g^{R_j}, e_2(j) h^{Rj})$ for $j = 1, 2, \ldots, L$, where $e(x) = (e_1(x), e_2(x))$.
- generates random numbers D_j for $j = 1, 2, \ldots, L$, and computes

$$(a_j, b_j) = (g^{D_j}, h^{D_j}) \quad \text{for } j = 1, 2, \ldots, L.$$

- generates random numbers w_j and N_j for $j = 1, 2, \ldots, L$, and computes

$$s_j = g^{w_j} h^{R_j N_j} \quad \text{for } j = 1, 2, \ldots, L.$$

- $\rightarrow$ Voter i: $E(j)$, (a_j, b_j), s_j (for $j = 1, 2, \ldots, L$)

Then, the following steps G4 ~ G6 are executed several times depending on how Voter i can be convinced that VB has done things for him correctly in Step G3. One more successful round of executing G4 ~ G6 can reduce the possibility of being cheated to $1/2^{|c|}$, where |c| denotes the bit length of c.

Step G4. Voter i $\rightarrow$ VB: c. // c is a random challenge //

Step G5. VB:

- computes $u_j = D_j + R_j (c + w_j)$ for $j = 1, 2, \ldots, L$.
- $\rightarrow$ Voter i: w_j, N_j, u_j (for $j = 1, 2, \ldots, L$.)

Step G6. Voter i:

- computes

$$g^{w_j} h^{R_j N_j} \quad \text{for } j = 1, 2, \ldots, L.$$

$$(g^{R_j})^{c+w_j} a_j \quad \text{for } j = 1, 2, \ldots, L.$$

$$(h^{R_j})^{c+w_j} b_j \quad \text{for } j = 1, 2, \ldots, L.$$

- if $(s_j \neq g^{w_j} h^{R_j N_j}) \vee (g^{u_j} \neq (g^{R_j})^{c+w_j} a_j) \vee (h^{u_j} \neq (h^{R_j})^{c+w_j} b_j)$ for $j = 1, 2, \ldots, L$, goes to Step G2.

Ballot Casting Phase

The ballot casting phase can be invoked at any time prior to the deadline of voting. For Voter i, he will enter this phase after finishing the steps specified in the ballot generation phase.

Step C1. Voter i:

- uses SC_i to generate random numbers d_j, k_j, and w'_j, and to compute

$$a_j = (x_j)^{d_j} g^{k_j} \quad \text{for } j = 1, 2, \ldots, z-1, z+1, \ldots, L \text{ (excluding } z)$$

$$b_j = (y_j)^{d_j} h^{k_j} \quad \text{for } j = 1, 2, \ldots, z-1, z+1, \ldots, L \text{ (excluding } z)$$

$$a_z = g^{w_z + w'_z}$$

$$b_z = h^{w_z + w'_z}$$

where $z \in \{1, 2, ..., L\}$ is the number representing the option selected by Voter i.

- uses SC_i to compute

$$B = H(ID_i, x, y, x_1, \ldots, x_L, y_1, \ldots, y_L, a_1, \ldots, a_L, b_1, \ldots, b_L)$$

$$d_z = B - \sum_{j \neq z} d_j \quad \text{for } j = 1, 2, \ldots, L.$$

Step C2. Voter i $\rightarrow$ VB: B, d_j (for $j = 1, 2, \ldots, L$)

Step C3. VB $\rightarrow$ Voter i: $K_j = w_j + R_j d_j$ (for $j = 1, 2, \ldots, L$)

Step C4. Voter i:

- uses SC_i to compute $r_z = w'_z - k_z d_z + K_z$.
- $\rightarrow$ BB : $E(z)$, B, d_1, d_2, …, d_L, r_1, r_2, …, r_L with signature.

Public Verification Phase

The public verification phase can be invoked at any time prior to the tallying phase.

Step V1. Any party can:

- check the authenticity of ($E(z)$, B, d_1, d_2, …, d_L, r_1, r_2, …, r_L) by verifying its corresponding signature in each record on BB. If fails, the representative Voting Authority should clean the record; otherwise, any party can ask the representative Voting Authority to do so.
- verify the validity of $E(z) = (x, y)$ by using its corresponding (B, d_1, d_2,…, d_L, r_1, r_2, …, r_L) in each record on BB. If fails, the representative Voting Authority should mark this record as INVALID BALLOT.

Tallying Phase

The tallying phase is invoked only once after the deadline of the whole voting.

Step T1. Voting Authorities:

compute $(X, Y) = (\prod x_i, \prod y_i)$, where x_i and y_i denote the valid x and y of Voter i, respectively.

- jointly (at least t voting authorities) compute

$$W = \frac{Y}{X^s} = G_1^{T_1} G_2^{T_2} \cdots G_L^{T_L}.$$

- determine final tally T_1, T_2, …, T_L from W.
- announce the result.

Note that the time complexity of computing $T_1, T_2, \ldots, T_L$ from W is $O(M^{L-1})$ [7], where M denotes the number of the voters, and can be reduced considerably to $O((\sqrt{M})^{L-1})$ by a generalization of *the baby-step giant-step algorithm* [7].

4 Security Analysis

In this section, we will show that the proposed e-voting scheme is secure, i.e., it satisfies completeness, privacy, unreusability, eligibility, fairness, verifiability, robustness, receipt-freeness, and uncoercibility.

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

Sketch of Proof: Since the bulletin board is open to the public and no encrypted ballot can be erased from the bulletin board, any party can verify the validity of each encrypted ballot. Therefore, no valid encrypted ballot posted on it can be dropped or wrongly handled. Due to the homomorphic properties of the used encryption method, the final tally is the sum of all valid ballots, i.e., all ballots are counted correctly. Hence, the proposed e-voting scheme satisfies completeness.

Lemma 2 (privacy). In the proposed e-voting scheme, all ballots are secret.

Sketch of Proof: Since the ballot is encrypted with the public key shared by the voting authorities, the encrypted ballot can be individually decrypted from its corresponding ballot only by using the private key jointly shared by voting authorities. However, this decryption can be performed only when t or more voting authorities participate, which contradicts the assumption that no more than t-1 voting authorities conspire. Therefore, the proposed e-voting scheme ensures privacy.

Lemma 3 (unreusability). In the proposed e-voting scheme, no voter can vote twice.

Sketch of Proof: Each encrypted ballot is posted in the record designated to the voter on the bulletin board. Since a digital signature technique is used to control access to the entries of the bulletin board, any party can verify the authenticity of each encrypted ballot by verifying its signature. If a voter wants to vote twice, he has to cast his additional encrypted ballot in the record designated to another voter. Clearly, his additional encrypted ballot will be rejected because he can not generate the correct signature for it. In addition, since each encrypted ballot should be accompanied with a proof that it contains a valid ballot, he can not cast an encrypted ballot containing an invalid value. Therefore, the proposed e-voting scheme satisfies unreusability.

Lemma 4 (eligibility). In the proposed e-voting scheme, only eligible voters can vote.

Sketch of Proof: Since each encrypted ballot posted in the record designated to the voter on the bulletin board is accompanied with the voter's signature, no one except the certification authority can impersonate as an eligible voter to vote. In addition, the certification authority will be caught if he undertakes such an impersonation. Note that even if the voting authorities conspire, they can not impersonate as an eligible voter to vote. Therefore, the proposed e-voting scheme satisfies eligibility.

Lemma 5 (fairness). No one can know the intermediate results of the voting in the proposed e-voting scheme.

Sketch of Proof: The private key jointly shared by voting authorities can only be used in the tallying phase once to decrypt the encrypted final tally. It is only when t or more voting authorities conspire prior to the tallying phase that the decryption can be performed to obtain intermediate result. However, it contradicts the assumption that no more than t-1 voting authorities conspire. Hence, the proposed e-voting scheme provides fairness to voters.

Lemma 6 (verifiability). In the proposed e-voting scheme, the result of the voting can be verified.

Sketch of Proof: Since the public can verify the authenticity of each encrypted ballot by verifying its signature and no encrypted ballot can be erased from the bulletin board, we can verify the integrity of the encrypted final tally. Due to the homomorphic properties of the used encryption method, the final tally is verifiable to any observer. Thus, the proposed e-voting scheme satisfies individual and universal verifiability.

Lemma 7 (robustness). In the proposed e-voting scheme, no voter can disrupt the voting.

Sketch of Proof: Since each encrypted ballot posted on the bulletin board should be accompanied with a proof, the public can verify its validity with its proof. An encrypted ballot cast by a malicious voter containing invalid value will be marked as an invalid ballot by the representative voting authority; otherwise, any party can ask the representative voting authority to do so. Thus, no voter can disrupt the voting, i.e., the proposed e-voting scheme satisfies robustness.

Lemma 8 (receipt-freeness). In the proposed e-voting scheme, the voter can not reveal his ballot to others.

Sketch of Proof: Both the voting booth and the smart card contribute randomness to the ballot. Since the voter does not know the randomness added by the voting booth, he can not construct a receipt directly. In addition, the voter must be given a proof of correctness of the encryption performed by the voting booth before the encrypted ballot is submitted to the bulletin board. By employing the Fiat-Shamir heuristic [12], the proof for each encrypted ballot is non-transferable and can not be used a receipt. Hence, the proposed e-voting scheme satisfies receipt-freeness.

Lemma 9 (uncoercibility). In the proposed e-voting scheme, a voter can not be coerced into casting a particular ballot by a coercer.

Sketch of Proof: By employing voting booths with guards, no one can monitor the voting process of others. Thus, the only way for the coercer to know the content of a ballot is checking its voter's receipt. Since the proposed voting scheme satisfies receipt-freeness, uncoercibility is also satisfied.

Theorem 1. The proposed e-voting scheme is secure.

Proof: From Lemma 1 ~ Lemma 9, we can infer that the proposed e-voting scheme is secure.

5 Conclusion

Bribe and coercion are common in conventional voting systems and usually lead to a biased result that imparts the desired democracy. These problems become more terrible and harder to solve in an e-voting scheme. Most e-voting schemes focus on providing the utmost convenience to the voter in that the voter can vote at any place by using a personal computer with Internet accessing capability. Although many e-voting schemes without using voting booths are claimed to provide receipt-freeness, bribe and coercion can not be effectively prevented since the voter may be bribed or coerced to vote for a certain candidate and is obliged to vote under the supervision of the briber or the coercer. Therefore, to effectively solve this problem with current techniques, voting booths should be used again. Several e-voting schemes using voting booths have been proposed. However, these schemes do not effectively provide uncoercibility because the briber or the coercer can prescribe private random bits that the voter should use. In this paper, we have described a secure e-voting scheme that can be realized in practical environments. In addition to satisfying completeness, unreusability, eligibility, fairness, and verifiability, the proposed e-voting scheme can prevent or at least lessen bribe and coercion. Unlike the usage of voting booths in conventional paper-based voting systems, the voter can choose any voting booth that is convenient and safe to him in the proposed e-voting scheme. In addition, the proposed e-voting scheme is suitable for large-scale elections in that the time complexity and the communication complexity for the voter are independent of the number of voting authorities.

References

[1] C. Boyd, "Some Applications of Multiple Key Ciphers," *Advances in Cryptology－EUROCRYPT'88*, pp.234–238, Springer-Verlag, 1987.

[2] C. Boyd, "A New Multiple Key Ciphers and an Improved Voting Scheme," *Advances in Cryptology －EUROCRYPT'89*, pp.617–625, Springer-Verlag, 1990.

[3] J. Benaloh and D. Tuinstra, "Receipt-Free Secret-Ballot Elections," *Proc. 26th Symposium on Theory of Computing* (*STOC'94*), pp.544–553, 1994.

[4] J. Benaloh and M. Yung, "Distributing the Power of a Government to Enhance the Privacy of Voters," *Proc. 27th IEEE Symposium on Principles of Distributed Computing* (*PODC*), pp.52–62, 1986.

[5] J. Cohen and M. Fischer, "A Robust and Verifiable Cryptographically Secure Election Scheme," *Proc. 26th IEEE Symposium on Principles of Distributed Computing* (*PODC*), pp.52–62, 1985.

[6] R. Cramer, M. Franklin, B. Schoenmakers, and M. Yung, "Multi-Authority Secret-Ballot Elections with Linear Work," *Advances in Cryptology－EUROCRYPT'96*, vol.1070 of *LNCS*, pp.72–83, Springer-Verlag, May 1996.

[7] R. Cramer, R. Gennaro, and B. Schoenmakers, "A Secure and Optimally Efficient Multi-Authority Election Scheme," *European Transactions on Telecommunications*, no.8, pp.481–489, 1997. Preliminary version in *Advances in Cryptology－EUROCRYPT'97*.

[8] D. Chaum, "Untraceable Electronic Mail, Return Addresses and Digital Pseudonyms," *Communications of ACM*, vol.24, no.2, pp.84–88, 1981.

[9] D. Chaum, "Elections with Unconditionally Secret Ballots and Disruption Equivalent to Breaking RSA," *Advances in Cryptology－EUROCRYPTO'88*, pp. 177–182. Springer-Verlag, 1988.

[10] T. ElGamal, “A Public-Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms,” *Advances in Cryptology—CRYPTO’84*, vol.196 of *LNCS*, pp.10–18, Springer-Verlag, 1984.

[11] A. Fujioka, T. Okamoto, and K. Ohta, “A Practical Secret Voting Scheme for Large Scale Elections,” *Advances in Cryptology—AUSCRYPT’92*, pp.244–251, 1992.

[12] A. Fiat and A. Shamir, “How to Prove Yourself: Practical Solutions to Identification and Signature Problems,” *Advances in Cryptology—CRYPTO’86*, vol.263 of *LNCS*, pp.186–194, Springer-Verlag, 1986.

[13] M. Hirt and K. Sako, “Efficient Receipt-Free Voting Based on Homomorphic Encryption,” *Advances in Cryptology—EUROCRYPT 2000*, vol.1807 of *LNCS*, pp.539–556. Springer-Verlag, 2000.

[14] E. Magkos, M. Burmester, and V. Chrissikopoulos, “Receipt-Freeness in Large-Scale Elections without Untappable Channels,” *Proc. 1st IFIP Conference on E-Commerce / E-business / E-Government*, pp.683–693, Kluwer Academics Publishers, 2001.

[15] T. Okamoto, A. Fujioka, and K. Ohta, “A Practical Large Scale Secret Voting Scheme Based on Non-Anonymous Channels,” *Proc. of SCIS93, IC*, Jan. 1993.

[16] T. Pedersen, “A Threshold Cryptosystem without a Trusted Party,” *Advances in Cryptology—EUROCRYPT’91*, vol.547 of *LNCS*, pp.522–526, Springer-Verlag, 1991.

[17] T. Pedersen, “Distributed Provers and Verifiable Secret Sharing Based on the Discrete Logarithm Problem,” PhD thesis, Aarhus University, Computer Science Department, Aarhus, Denmark, Mar. 1992.

[18] M. Rabin, “Transaction Protection by Beacons,” *Journal of Computer Systems Science*, vol.27, no.2 , pp.256–267, 1983.

[19] K. Sako and J. Kilian, “Receipt-Free Mix-Type Voting Scheme—A Practical Solution to the Implementation of a Voting Booth,” *Advances in Cryptology—EUROCRYPT’95*, vol.921 of *LNCS*, pp.393–403, Springer-Verlag, 1995.

[20] IEEE P1583, Available: http://grouper.ieee.org/groups/scc38/1583/index.htm.