Receipt-free Electronic Voting through Collaboration of Voter and Honest Verifier

Byoungcheon Lee   Kwangjo Kim

ICU (Information and Communications University)
58-4, Hwaam-Dong, Yusung-Ku, Taejon, 305-348, KOREA
Tel : +82-42-866-6158, Fax : +82-42-866-6154
E-mail: {sultan,kkj}@icu.ac.kr

Abstract In this paper, we propose a new electronic voting scheme which guarantees receipt-freeness as well as privacy, universal verifiability and robustness. The result of Cramer, Gennaro, and Schoenmarkers[CGS97] proposed at Eurocrypt'97 seems to be promising because it provides optimal performance, privacy, robustness, and universal verifiability. But in their scheme, receipt-freeness was left as an open problem. The failure of receipt-freeness in [CGS97] comes from the fact that the ballot is generated and posted on the bulletin board wholly by the voter. To add receipt-freeness to [CGS97] while keeping other useful properties, we introduce a trusted third party called honest verifier(HV). In the proposed electronic voting scheme, the voter and HV collaborate through an interactive voting protocol to generate a ballot and it's proof of validity. Finally the vote and it's proof of validity are posted on the bulletin board.

Keywords: Electronic voting, receipt-freeness, honest verifier, universal verifiability, proof of validity, proof of knowledge, multi-party computation.

1 Introduction

The research on electronic voting is a very important topic for the progress of democracy. If a secure and convenient electronic voting system is provided, it will be used more frequently to collect people's opinion for many kind of political and social decisions through cyber space. In cryptographic aspect it is considered as an important application of secure multi-party computation.

Many extensive researches have been conducted on the subject and now an extensive list of requirements for electronic voting is available[FOO92, CGS97]. The requirements are as follows:

- **Privacy** - All votes must be secret.
- **Completeness** - All valid votes are counted correctly.
- **Soundness** - The dishonest voter cannot disrupt the voting.
- **Unreusability** - No voter can vote twice.
- **Eligibility** - No one who isn't allowed to vote can vote.
- **Fairness** - Nothing must affect the voting.
- **Robustness** - The voting system should be successful regardless of partial failure of the system.
- **Universal verifiability** - Anyone can verify the validity of voting and tallying process.
- **Receipt-freeness** - The vote cannot be proven to a buyer.

To satisfy these requirements, a variety of approaches have been tried. Starting from an electronic voting scheme using blind signature [Cha81], the main stream of the current research can be classified into the following three approaches:

- **Homomorphic encryption based schemes** : [Ben87], [SK94], [CFSY96], [CGS97]
- **Mix-net based schemes** : [PIK93], [SK95], [Pfi94], [MH96], [Abe98], [Jak98]
- **Verifiable Secret Sharing based schemes** : [Sta96], [FO98], [Sch99]

Other additional cryptographic primitives such as bit commitment [Nao89], secret sharing [Sha79], or dining cryptographer problem [Cha88] are partially employed to design an electronic voting scheme.

To the best of our knowledge, there is no single ideal scheme which satisfies all the requirements described above. The result of Cramer, Gennaro, and Schoenmarkers[CGS97] proposed at Eurocrypt'97 seems to be promising because it satisfies most of the requirements. It is a multi-authority election scheme which uses threshold homomorphic encryption, bulletin board, proof of knowledge, and proof of validity. In [CGS97], the voter posts a single ElGamal encryption as a ballot and its proof of validity on the bulletin board. The proof of validity of ballot can be verified by anyone, so it provides universal verifiability. It shows also optimal performance in the sense that time and communication complexities are minimal both for the voters and the authorities. But as the authors have mentioned, it does not provide receipt-freeness.

The failure of receipt-freeness in [CGS97] comes from the fact that the ballot is generated and posted on the bulletin board wholly by the voter. In this paper, we extend the scheme to provide receipt-freeness. For this purpose we introduce a trusted third party, called honest verifier(HV), who interacts with voter to verify the validity of the voter's first ballots, to generate the final ballots, and to generate the proof of validity of the final ballot.

During the voting protocol, HV generates a random pair (u, v) using a randomly generated secret exponent β and sends it to the voter. The voter verifies the validity of the received random pair, multiplies it to the first ballot(ElGamal encryption of the vote) to generate the final ballot, and posts it on the bulletin board. On the other hand, HV verifies the validity of the voter's first ballot and generate the proof of validity of the final ballot. Because the final ballot is generated by the voter and HV, the voter cannot prove anything to a buyer without knowing HV's secret exponent β. Using the proof of validity, anyone can verify the validity of the final ballot.

The paper is organized as follows : Section 2 describes briefly the basic building blocks required for our proposed election scheme. Section 3 describes our receipt-free electronic voting scheme. Various aspects of security analysis are discussed in section 4. Finally we conclude in section 5.

2 The Building Blocks

The basic building blocks for our voting scheme are homomorphic ElGamal encryption, threshold ElGamal encryption, proof of knowledge, proof of validity, and bulletin board. In this section, we describe these terms briefly.

2.1 Homomorphic ElGamal Encryption

Consider an ElGamal encryption system [ElG85] for subgroups G_q of order q of Z_p^*, where p and q are large primes such that $q \mid p-1$. If a receiver chooses a private key s, the corresponding public key is $h = g^s$ where g is the generator of G_q. Given a message $m \in G_p$, encryption of m is given by $(x, y) = (g^\alpha, h^\alpha m)$ for a randomly chosen $\alpha \in_R Z_q$. To decrypt the ciphertext (x, y), the receiver recovers the plaintext as $m = y/x^s$ using the private key s.

In our proposed voting scheme, we consider a multi-way election of 1-out-of-K choices where K is the number of candidates. We take K independently selected generators $G_i, 1 \leq i \leq K$ and use them as the messages for voting. So the ElGamal encryption of the voting for the candidate i is given by $(x, y) = (g^\alpha, h^\alpha G_i)$. In this case, the ElGamal encryption has homomorphic property and the final tally can be computed by a single decryption of the product of all valid ballots.

2.2 Threshold ElGamal Encryption

A threshold public-key encryption scheme is used to share a secret key among a set of receivers such that messages can be decrypted only when a substantial subset of receivers cooperate. More detailed description is found in [CGS97] and [Ped91]. It consists of key generation protocol, encryption algorithm, and decryption protocol.

Consider a (t, n)-threshold encryption scheme where the secret key is shared among n tallying authorities A_j $(1 \leq j \leq n)$ and decryption is possible only when more than t authorities cooperate. Through the key generation protocol, each authority A_j will possess a share $s_j \in Z_q$ of a secret s. Each authority publishes the value $h_j = g^{s_j}$ as a commitment of the share s_j. The shares s_j are chosen such that the secret s can be reconstructed from any subset Λ of t shares using appropriate Lagrange coefficients,

$$s = \sum_{j \in \Lambda} s_j \lambda_{j,\Lambda}, \quad \lambda_{j,\Lambda} = \prod_{l \in \Lambda \setminus \{j\}} \frac{l}{l-j} \qquad (1)$$

The public key $h = g^s$ is announced to all participants in the system.

Encryption of a message m using the public key h is given by $(x, y) = (g^\alpha, h^\alpha m)$ which is the same as the ordinary ElGamal encryption. To decrypt a ciphertext $(x, y) = (g^\alpha, h^\alpha m)$ without reconstructing the secret s, the authorities execute the following protocol:

1. Each participating authority A_j broadcasts $w_j = x^{s_j}$ and proves the equality of the following discrete logs in zero-knowledge using the proof of knowledge protocol given in the next section.
$$\log_g h_j = \log_x w_j.$$
2. Let Λ denote any subset of authorities who passed the zero-knowledge proof. By raising x to both sides of equation (1), the plaintext can be recovered as
$$m = y / \prod_{j \in \Lambda} w_j^{\lambda_{j,\Lambda}}.$$

2.3 Proof of Knowledge of Common Exponent

A prover wants to show the possession of a common exponent $\beta \in_R Z_q$ satisfying $u = g^\beta$ and $v = h^\beta$ to a verifier without exposing it. An efficient protocol for this problem is described in [CP93] as shown in Figure 1. Through an interactive protocol with the verifier, the prover proves the possession of β without exposing it. This protocol is used in the voting and tallying stages.

$$
\begin{array}{lcl}
\textbf{Prover(HV)} & & \textbf{Verifier(voter)} \\
[(u,v) = (g^\beta, h^\beta)] & & \\
w \in_R Z_q & & \\
(a,b) \leftarrow (g^w, h^w) & \xrightarrow{\quad a,b \quad} & c \in_R Z_q \\
 & \xleftarrow{\quad c \quad} & \\
r \leftarrow w + \beta c & \xrightarrow{\quad r \quad} & g^r \stackrel{?}{=} a u^c \\
 & & h^r \stackrel{?}{=} b v^c
\end{array}
$$

Figure 1: Proof of knowledge of common exponent of $(u, v) = (g^\beta, h^\beta)$.

2.4 Proof of Validity of Ballot (x, y)

Assume that the voter chooses the i-th candidate. Then the ElGamal encryption of the choice G_i is given by $(x, y) = (g^\alpha, h^\alpha G_i)$. The voter wants to prove that the ballot (x, y) contains a valid vote without exposing the value G_i. This is a witness indistinguishable proof of knowledge [FS90] of the relation given by

$$\log_g x = \log_h (y/G_1) \ \vee \ \cdots \ \vee \ \log_g x = \log_h (y/G_K).$$

Using the idea of [CDS94] and [CGS97], we have designed an interactive protocol for the proof of validity of a ballot in a multi-way election of 1-out-of-K choices as shown in Figure 2. This protocol is used in voting stage by the voter and HV to prove the validity of a ballot.

$$
\begin{array}{lcl}
\textbf{Voter} & & \textbf{Honest Verifier} \\
[(x,y) = (g^\alpha, h^\alpha G_i)] & & \\
w \in_R Z_q & & \\
a_i = g^w, b_i = h^w & & \\
\text{For } j = 1, ..., i-1, i+1, ..., K & & \\
\quad d_j, r_j \in_R Z_q & & \\
\quad a_j = g^{r_j} x^{d_j} & & \\
\quad b_j = h^{r_j} (y/G_j)^{d_j} & & \\
(A, B) = (a_1, b_1), ..., (a_K, b_K) & & \\
 & \xrightarrow{\quad (x,y), (A,B) \quad} & c \in_R Z_q \\
 & \xleftarrow{\quad c \quad} & \\
d_i = c - \sum_{j \neq i} d_j & & \\
r_i = w - \alpha d_i & & \\
(D, R) = (d_1, r_1), ..., (d_K, r_K) & & \\
 & \xrightarrow{\quad (D,R) \quad} & c \stackrel{?}{=} d_1 + \cdots + d_K \\
 & & \text{For } j = 1, ..., K \\
 & & \quad a_j \stackrel{?}{=} g^{r_j} x^{d_j} \\
 & & \quad b_j \stackrel{?}{=} h^{r_j} (y/G_j)^{d_j}
\end{array}
$$

Figure 2: Proof of validity of ballot $(x, y) = (g^\alpha, h^\alpha G_i)$.

2.5 Bulletin Board

In this paper bulletin board is used as a public communication channel which can be read by any party. But each legitimate party can write message only on its designated section. No party can erase any information from the bulletin board.

Each record associated with a voter has four fields: Challenge, Response, Ballot, and Proof. So the bulletin board is organized as follows:

- Name - Voter's name
- Challenge Field(CF) - HV posts the challenge value.
- Response Field(RF) - voter posts the response value.
- Proof field(PF) - HV posts the proof of validity for the final ballot.

- Ballot field(BF) - voter posts the final ballot.

During the voting protocol, interactive proof of validity is executed. HV records its challenge on CF and the voter records its response on RF. At the end of the voting protocol, HV posts the proof of validity of the final ballot on PF and the voter posts the final ballot on BF. To control access to the various sections of the bulletin board, each legitimate party has to be identified by digital signature.

3 New Receipt-free Electronic Voting Scheme

3.1 Structure of Voting Scheme

We now propose a new electronic voting scheme by assembling the building blocks presented in the previous section. In our voting system, the four participants and their roles are as follows.

1. *n-tallying authorities*($A_1, ..., A_n$) : They share the secret key of the threshold ElGamal encryption by executing the key generation protocol. When the deadline is reached, they collect all the valid ballots to generate a product of ballots and decrypt it through an interactive decryption protocol. More than t authorities should cooperate for successful decryption.

2. *l-voters*($V_1, ..., V_l$) : Voter participates in the voting through an interactive voting protocol with HV. Firstly, voter generates the first ballot (x, y) and then generates the final ballot $(x_f, y_f) = (xu, yv)$ by multiplying it with the random pair (u, v). Voter posts the final ballot on the BF of the bulletin board.

3. *Honest verifier(HV)* : HV participates in the voting protocol through an interactive voting protocol with voter. HV verifies the validity of the voter's first ballot and provides the voter with a random pair (u, v) which is generated by using a secret exponent β. Finally HV generates the proof of validity of the final ballot and posts it on the bulletin board.

4. *Certificate authority(CA)* : CA issues Certificates which certify the identity of all the participants of the voting system.

The proposed electronic voting system consists of the following stages.

1. *System set-up* : Authorities generate the system parameters for ElGamal cryptosystem (p, q, g) and the independent generators representing the K candidates, $G_i's$ for $i = 1, ..., K$. Tallying authorities execute the key generation protocol to generate the public key for ElGamal encryption of the vote and the corresponding secret shares. The system parameters and public key are published on the bulletin board.

2. *Registration of legitimate voters* : Authorities register all the legitimate voters on the bulletin board. Authorities should identify the voters by the certificate issued by CA.

3. *Voting* : Voters execute the interactive voting protocol.

4. *Tallying* : Tallying authorities collect all the valid ballots and jointly execute the (t, n) threshold ElGamal decryption protocol. They decide the final result from the decryption and publish it.

5. *Verification* : Anyone can universally verify the validity of the result.

3.2 Voting Procedure

Our voting protocol is an interactive protocol between voter and HV and is a combination of two subprotocols - the proof of validity of the first ballot(PV1) and the proof of knowledge of common exponent(PK). At the end of the protocol, HV generates the proof of validity of the final ballot(PV2) from the previous protocol values. We summarize the proposed voting protocol as follows:

Step 1. Voter (Commitment for PV1)

- Choose a vote $G_i, 1 \leq i \leq K$.
- Choose random $\alpha, w_1 \in_R Z_q$.
- Generate the first ballot, $(x, y) = (g^{\alpha}, h^{\alpha} G_i)$.
- Compute $a_i = g^{w_1}, b_i = h^{w_1}$.
- For $j = 1, ..., i-1, i+1, ..., K$, choose random $d_j, r_j \in_R Z_q$ and compute $a_j = g^{r_j} x^{d_j}, b_j = h^{r_j} (y/G_j)^{d_j}$.
- $(A, B) = (a_1, b_1), ..., (a_K, b_K)$
- Voter sends (x, y) and (A, B) to HV.

Step 2. HV (Challenge for PV1 and commitment for PK)

- Choose random $\beta, w_2 \in_R Z_q$.

- Compute $(u, v) = (g^{\beta}, h^{\beta})$.
- Compute $(a, b) = (g^{w_2}, h^{w_2})$.
- Choose a random challenge for PV1, $c_1 \in_R Z_q$.
- HV sends $(u, v), (a, b)$, and c_1 to voter.
- HV posts c_1 on CF of the bulletin board.

Step 3. Voter (Response to PV1 and challenge for PK)

- Generate responses to PV1, $d_i = c_1 - \sum_{j \neq i} d_j, r_i = w_1 - \alpha d_i$.
- $(D, R) = (d_1, r_1), ..., (d_K, r_K)$
- Choose a random challenge for PK, $c_2 \in_R Z_q$.
- Voter sends (D, R) and c_2 to HV.
- Voter posts (D, R) on RF of the bulletin board.

Step 4. HV (Verification of PV1, response to PK, and generation of PV2)

- Verify PV1, $c_1 \stackrel{?}{=} d_1 + \cdots + d_K$, and $a_j \stackrel{?}{=} g^{r_j} x^{d_j}, b_j \stackrel{?}{=} h^{r_j} (y/G_j)^{d_j}$ for $j = 1, ..., K$.
- Generate a response to PK, $r = w_2 + \beta c_2$.
- Generate PV2, $s_j = a_j u^{d_j}, t_j = b_j v^{d_j}$ for $j = 1, ..., K$.
- $(S, T) = (s_1, t_1), ..., (s_K, t_K)$.
- HV sends r to voter.
- HV posts (S, T) on PF of the bulletin board.

Step 5. Voter (Verification of PK and PV2)

- Verify PK, $g^r \stackrel{?}{=} a u^{c_2}$ and $h^r \stackrel{?}{=} b v^{c_2}$.
- Compute the final ballot, $(x_f, y_f) = (xu, yv)$.
- Get PV2 from PF of the bulletin board and verify it, $s_j \stackrel{?}{=} g^{r_j} x_f^{d_j}$ and $t_j \stackrel{?}{=} h^{r_j} (y_f/G_j)^{d_j}$ for $j = 1, ..., K$.
- Voter posts the final ballot (x_f, y_f) on BF of the bulletin board.

Step 6. Anyone (Verification of PV2)

- Anyone can verify PV2 by $c_1 \stackrel{?}{=} d_1 + \cdots + d_K$, and $s_j \stackrel{?}{=} g^{r_j} x_f^{d_j}$ and $t_j \stackrel{?}{=} h^{r_j} (y_f/G_j)^{d_j}$ for $j = 1, ..., K$.

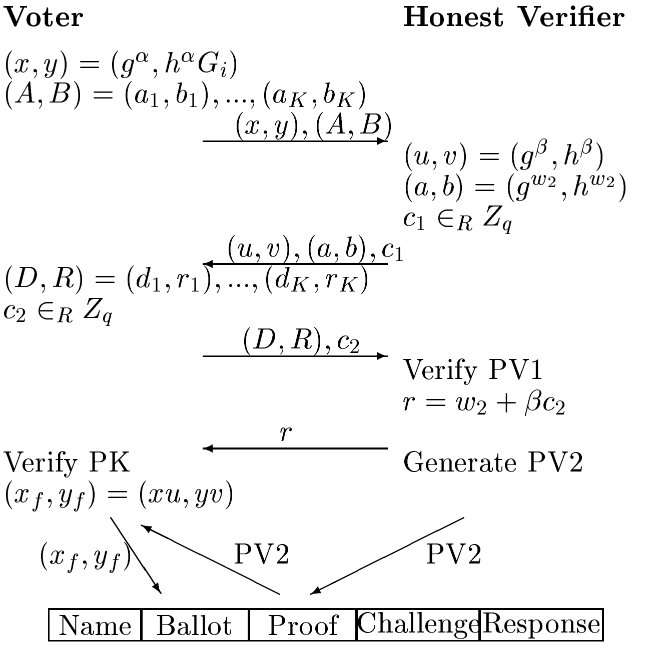

Figure 3: The proposed electronic voting protocol(simplified form).

For the ease of understanding, the proposed voting protocol is shown in Figure 3 in simplified form.

The voter prove the validity of the first ballot (x, y) to HV using PV1 protocol and HV prove the validity of the random pair (u, v) to voter using PK protocol. HV also generate the validity of the final ballot by using the previous protocol values. The voter finally generate the final ballot by $(x_f, y_f) = (xu, yv)$. HV posts the challenge c_2 on CF and PV2 on PF, while the voter posts the response (D, R) on RF and the final ballot on BF. The final ballot (x_f, y_f) can be decrypted in the same way using the secret key s because $v/u^s = 1$ is satisfied. Because the final ballot is generated through collaboration of voter and HV, the voter cannot prove anything without the secret information β. So our protocol provides receipt-freeness.

In the voting protocol, HV generates PV2 by using PV1 and (u, v). (A, B), c_1, and (D, R) can prove the fact that (x, y) is a valid ballot. By multiplying (a_j, b_j) with (u^{d_j}, v^{d_j}), (x, y) and (u, v) are combined into (x_f, y_f), so PV2 can be verified using only (x_f, y_f). Now anyone can universally verify the validity of the final ballot.

3.3 Tallying Procedure

When the deadline of voting is reached, a designated authority collects all the valid ballots and calculates the product $(X, Y) = (\prod_{i=1}^{l} x_{f,i}, \prod_{i=1}^{l} y_{f,i})$. Anybody can check the validity of the product because all the final ballots are posted on the bulletin board and their validity can be verified universally. The n tallying authorities jointly execute the decryption protocol for (X, Y) to obtain $W = Y/X^s$. Because the secret key s is shared among n tallying authorities, any subset of t authorities who cooperate for decryption can decrypt (X, Y) to obtain W. Note that the secret key s is not reconstructed but just X^s is computed in the decryption process.

Now we get $W = G_1^{T_1} G_2^{T_2} \cdots G_K^{T_K}$ where $T_1, \ldots, T_K$ are the result of the election. Computation of $T_1, \ldots,$ T_K requires the computation of the discrete logarithm problem and it is generally considered as a computationally hard problem. In this case, it requires $O(l^{(K-1)/2})$ time to get the result. It is feasible only for a reasonable size of l and K. It is considered that the proposed electronic voting scheme is suitable for small scale election. If this scheme is used for large scale election, the authorities can divide the total product (X, Y) into several smaller parts (X_i, Y_i) of reasonable size and conquer them one by one.

4 Security analysis

The proposed voting protocol satisfies the extensive requirements of electronic voting.

- Privacy is satisfied because the tallying procedure is executed only for the product of many valid ballots.
- Completeness is guaranteed by the proof of validity of the final ballot and the use of public bulletin board. Anyone can verify the validity of the ballots and the correctness of ballot collection.
- Soundness is satisfied because any dishonest voter cannot pass the proof of validity and proof of knowledge protocol.
- Unreusability is satisfied because each voter can vote only once on the public bulletin board.
- Eligibility is satisfied because only the legitimate voters registered on the bulletin board can participate in the voting.
- Fairness is satisfied because voter and HV cannot get any partial information of other's secret from the protocol.
- Robustness is guaranteed because (t, n) threshold ElGamal encryption scheme is used.

We will describe more on receipt-freeness and universal verifiability in the following section.

4.1 Receipt-freeness

The proposed election scheme can provide receipt-freeness. The final ballot (x_f, y_f) is computed by multiplying voter's first ballot $(x, y) = (g^\alpha, h^\alpha G_i)$ with a random-looking pair (u, v) which is generated by HV using a randomly-chosen secret exponent β. To prove the vote for G_i, the voter has to present the exponent $\alpha + \beta$ and G_i to a buyer to show $(x_f, y_f) = (g^{\alpha+\beta}, h^{\alpha+\beta} G_i)$. But without knowing the exponent β, the voter cannot prove anything.

Theorem 1 *In the proposed electronic voting scheme, the vote cannot be proven if the proof of knowledge of (u, v) is not given.*

Proof: Assume that HV does not require PK and the voter does not need to prove it. Then the voter can disguise anything as a valid vote. Although the voter has voted for G_i, he can insist on a false vote for $G_k (k \neq i)$ by presenting a false $(x, y') = (g^\alpha, h^\alpha G_k)$ and $(u, v') = (u, v G_i / G_k)$ satisfying $(x_f,$ $y_f) = (xu, y'v')$. So the valid and false vote are indistinguishable.

Moreover, the public information of PV2 $\{ (S, T),$ $c_1, (D, R) \}$ does not provide any help. The voter may try to prove his valid vote for G_i by presenting the valid (x, y) and (a_j, b_j) satisfying $a_j = g^{r_j} x^{d_j}$ and $b_j = h^{r_j} (y/G_j)^{d_j}$. But he can also disguise a false vote for $G_k (k \neq i)$ as a valid one by presenting $(x, y') = (g^\alpha, h^\alpha G_k)$ and $(a_j, b'_j) = (g^{r_j} x^{d_j}, h^{r_j} (y'/G_j)^{d_j}$ satisfying $a_j = g^{r_j} x^{d_j}$ and $b'_j = h^{r_j} (y'/G_j)^{d_j}$. So the valid and false vote are indistinguishable. Consequently, the vote cannot be proven if PK of (u, v) is not given.

□

So the buyer has to require the proof of validity of (u, v) and the voter cannot prove anything.

4.2 Universal verifiability

PV2 is generated by HV combining PV1 and (u, v). (A, B), c_1, and (D, R) can prove the validity of (x, y). By multiplying (a_j, b_j) with (u^{d_j}, v^{d_j}), (x, y) and (u, v) are combined into (x_f, y_f) in (s_j, t_j), so the validity of PV2 can be verified using only (x_f, y_f) by anyone. Although PV1 is multiplied with (u^{d_j}, v^{d_j}) to generate PV2, the validity of PV1 is also preserved in PV2.

5 Conclusion

We have proposed a new electronic voting scheme which satisfies receipt-freeness and universal verifiability along with all the useful properties of [CGS97]. For this purpose we introduce a trusted third party, called honest verifier(HV), who interacts with voter to verify the validity of the voter's first ballots, to generate the final ballots, and to generate the proof of validity of the final ballot. The final ballot (x_f, y_f) is generated by multiplying voter's initial ballot (x, y) and HV's random pair (u, v). Without knowing the HV's random exponent β, voters cannot prove anything to a buyer, so receipt-freeness is provided. The proof of validity of the final ballot(PV2) is generated and posted by HV, and it guarantees the universal verifiability of the validity of ballots.

References

[Abe98] M. Abe, "Universally Verifiable Mix-net with Verification Work Independent of the Number of Mix-servers", In Advances in Cryptology – Eurocrypt 98, LNCS Vol. 1403, Springer-Verlag, pp. 437–447, 1998.

[Ben87] J. Benaloh, "Verifiable secret-ballot elections", PhD thesis, Yale University, Department of Computer Science, New Haven, CT, September 1987.

[BT94] J. Benaloh and D. Tuinstra, "Receipt-free secret-ballot elections", In Proc. of 26th Symp. on Theory of Computing (STOC'94), pp. 544-553, New York, 1994.

[CDS94] R. Cramer, I. Damgard, and B. Schoenmakers, "Proofs of partial knowledge and simplified design of witness hiding protocols", In Advances in Cryptology – Crypto'94, Vol. 839, LNCS, Springer-Verlag, pp. 174–187, 1994.

[Cha81] D.L. Chaum, "Untraceable, electronic mail, return addresses, and digital pseudonyms", Com. of the ACM, Vol. 24, No.2, pp. 84-88, 1981.

[Cha88] D.L. Chaum, "The dining cryptographer problems : unconditionally sender and recipient untraceability", J. of Cryptology, Vol. 1, No.1, pp.65–75, 1988

[CFSY96] R. Cramer, M. Franklin, B. Schoenmakers, and M. Yung, "Multi-authority secret ballot elections with linear work", In Advances in Cryptology – Eurocrypt '96, Vol. 1070, LNCS, Springer-Verlag, pp. 72–83, 1996.

[CGS97] R. Cramer, R. Gennaro, and B. Schoenmakers, "A secure an optimally efficient multi-authority election schemes", In Advances in Cryptology – Eurocrypt '97, Vol.1233, LNCS, Springer-Verlag, pp. 103–118, 1997.

[CP93] D. Chaum and T. Pedersen, "Wallet databases with observers", In Advances in Cryptology – Crypto'92, Vol. 740, LNCS, Springer-Verlag, pp. 89–105, 1993.

[ElG85] T. ElGamal, "A public key cryptosystem and a signature scheme based on discrete logarithms", IEEE Trans. on IT, Vol.31, No.4, pp.467-472, 1985.

[FO98] E. Fujisaki and T. Okamoto, "A practical and provably secure scheme for publicly verifiable secret sharing and its application", In Advances in Cryptology – Eurocrypt'98, Vol. 1403, LNCS, Springer-Verlag, pp. 32-46, 1998.

[FOO92] A. Fujioka, T. Okamoto, and K. Ohta, "A practical secret voting scheme for large scale election", In Advances in Cryptology – Auscrypt'92, LNCS, Springer-Verlag, pp. 244–251, 1992.

[FS90] U. Feige and A. Shamir, "Witness indistinguishable and witness hiding protocols", Proceedings of the 22nd Annual ACM Symposium on Theory of Computing, pp. 416–426, 1990.

[Jak98] M. Jakobsson, "A Practical Mix", In Advances in Cryptology – Eurocrypt 98, LNCS Vol. 1403, Springer-Verlag, pp. 449–461, 1998.

[MH96] M. Michels and P. Horster, "Some Remarks on a Receipt-Free and Universally Verifiable Mix-Type Voting Scheme", In Advances in Cryptology – Asiacrypt 96, LNCS Vol.765, Springer-Verlag, pp. 125–132, 1996.

[Nao89] M. Naor, "Bit commitment using pseudo-randomness", In Advances in Cryptology – Crypto'89, Vol. 435, LNCS, Springer-Verlag, pp. 128–136, 1990.

[NR94] V. Niemi and A. Rendall, "How to prevent buying of votes in computer elections", In Advances in Cryptology – Asiacrypt'94, Vol. 917, LNCS, Springer-Verlag, pp. 141–148, 1994.

[Ped91] T. Pedersen, "A threshold cryptosystem without a trusted party", In Advances in Cryptology – Eurocrypt '91, Vol. 547, LNCS, Springer-Verlag, pp. 522–526, Berlin, 1991.

[Pfi94] B. Pfitzmann, "Breaking an efficient anonymous channel", In Advances in Cryptology – Eurocrypt'94, Vol. 950, LNCS, Springer-Verlag, pp. 332–340, 1994.

[PIK93] C. Park, K. Itoh, and K. Kurosawa, "Efficient anonymous channel and all/nothing election scheme", In Advances in Cryptology – Eurocrypt'93, Vol. 765, LNCS, Springer-Verlag, pp. 248–259, 1994.

[Sch99] B. Schoenmaker, "A simple publicly verifiable secret sharing scheme and its application to electronic voting", In Advances in Cryptology – Crypto'99, Vol. 1666, LNCS, Springer-Verlag, pp. 148-164, 1999.

[Sha79] A. Shamir, "How to share a secret", Com. of the ACM, Vol. 22, No.11, pp. 612–613, 1979.

[SK94] K. Sako and J. Killian, "Secure voting using partial compatible homomorphisms", In Advances in Cryptology – Crypto'94, Vol. 839, LNCS, Springer-Verlag, pp. 411-424, 1994.

[SK95] K. Sako and J. Kilian, "Receipt-free mix-type voting scheme – a practical solution to the implementation of a voting booth", In Advances in Cryptology – Eurocrypt'95, Vol. 921, LNCS, Springer-Verlag, pp. 393–403, 1995.

[Sta96] M. Stadler, "Publicly verifiable secret sharing", In Advances in Cryptology – Eurocrypt'96, Vol. 1070, LNCS, Springer-Verlag, pp. 190–199, 1996.