Electronic Voting Protocol for the Receipt-freeness Based on Internet

Her, Yong-Sork
Graduate Graduate School of Information Science and Electrical Engineering, Kyushu University

Sakurai, Kouichi
Faculty of Information Science and Electrical Engineering, Kyushu Univ.

出版情報：Proc. of International Workshop Western Decision Sciences Institute. 1, pp.101-107, 2004-04
バージョン：
権利関係：

ELECTRONIC VOTING PROTOCOL FOR THE RECEIPT-FREENESS BASED ON INTERNET

Yong-Sork HER, Graduate *Graduate School of Information Science and Electrical Engineering, Kyushu Univ., 6-10-1, Hakozaki, Higashi-ku, Fukuoka, 812-8581, Japan, +81-92-642-3867, ysher@itslab.csce.kyushu-u.ac.jp*

Kouichi SAKURAI, Faculty of Information Science and Electrical Engineering, Kyushu Univ., 6-10-1, Hakozaki, Higashi-ku, Fukuoka, 812-8581, Japan, +81-92-642-3867, sakurai@csce.kyushu-u.ac.jp

ABSTRACT

In this paper, we introduce electronic voting protocol for the receipt-freeness based on Internet. Several receipt-free schemes have been proposed for e-voting and e-auction. The receipt-free scheme means that a voter should not prove to a third party and other people. But, it can be forged an information of voting by the participating authorities (e.g. administrator, tallier and so on) and coercer. First, we define the concept of the refined receipt-free scheme for a ***V***oter, ***A***dministrator, ***T***allier and ***C***oercer. We call ***RFV***, ***RFA, RFT,*** and ***RFC***. Second, we propose e-voting system which satisfies the refined receipt-free scheme. Finally, we compare the proposed e-voting system with the existed e-voting systems through computation and communication complexity.

1. Introduction

1.1 Motivation

Receipt-free schemes have been proposing for successful e-voting system [3][4][9][11]. Benaloh and Tuinstra[3] proposed the first receipt-free in e-voting system. Abe and Suzuki[8] proposed the first receipt-free scheme for e-auction. Sako and Kilian [4] proposed e-voting protocol with the receipt-free scheme using untappable channel. But, the disadvantage of [4] is that much load can be happened in tallying because of mix-net scheme. In [11], Okamoto proved e-voting scheme with the expanded receipt-free scheme of [10] based on trapdoor bit-commitment using untappable channel such as physical assumption.

1.2 The refined receipt-free scheme

In this section, we refined the receipt-free schemes for e-voting system as follows.

(1) ***Receipt-free of Voter (RFV)***: *A voter should not prove his/her voting content to other people.* Of course, he/she knows his/her voting content. A malicious voter may copy the voting content of other voter by simply duplicating the voting content.

(2) ***Receipt-free of Administrator (RFA)***: *Administrator can not prove voter's voting content to other people.*

Administrator (or Verifier) should not free to lie about the voting content which is sent by voter. It should prevent to communicate with other people and forge the voting information by administrator.

(3) ***Receipt-free of Tallier (RFT)***: *Tallier can not prove voter's voting content to other people. RFT is similar to RFA, but it is different who flow out the voting content.*

The goal of receipt-free scheme is to prevent the vote selling and artificial manipulation.

1.3 Analysis of known receipt-free scheme

In this section, we analyze the e-voting system of [4] and [11] in aspect of receipt-free scheme. In [4], they proposed the mix-type receipt-free voting scheme using the multi-center. Mix-type scheme of this e-voting system plays a role for concealing the chosen candidates. Also, this scheme uses chameleon bit-commitment based on

discrete-log. For each voter, the last counting center posts encrypted 1-votes and 0-votes in random order and commits to the ordering using chameleon bit commitments. But, the voter can open these commitments arbitrarily. Moreover, the voter knows how each center shuffled the encrypted voting content, and knows the leakage of his/her voting. So, it does not satisfy with ***RFV***.

In [11], he assumes an untappable channel and the parameter registration committee (PRC). A physical apparatus which is called an "untappable channel" for voter V_i can send out a message m, to recipient R, and all others can know (information theoretically) nothing about m. Let $R_1, R_2, \cdots, R_N$ be PRC members Public parameters are the same with the original scheme. V_i randomly generates $\alpha_i \in Z_q$ and splits α_i into N pieces, $\alpha_{i,1}, \cdots, \alpha_{i,N}$ such that $\alpha = \alpha_{i,1}, \cdots, \alpha_{i,N} \bmod q$. V_i then calculates $G_i = g^{\alpha_i} \bmod p$,and $G_{i,j} = g^{\alpha_{i,j}} \bmod p \quad (j = 1, \cdots, N)$. In voting stage, a voter sends (v_i, r_i, m_i) to timeless commission member T through an untappable anonymous channel. T publishes the list of votes in random order on the board, and also shows a non-interactive modification of zero-knowledge proof σ, to prove that the list of V_i contains only correct open values of the list of m_i without revealing the linkage between m_i and V_i. The important core of their receipt-scheme is σ that everyone with the exception of T does not know how to calculate σ. But, a voter V_i knows α_i, $\alpha = \alpha_{i,1}, \cdots, \alpha_{i,N} \bmod q$, $G_i = g^{\alpha_i} \bmod p$, $G_{i,j} = g^{\alpha_{i,j}} \bmod p$, m_i, x_i and A's blind signature s_i. The advantage of this scheme is that most of information on voting contents are concentrated to the voter. For example, $(m_i \| G_i \| G_{i,1} \| \cdots \| G_{i,N}, s_i)$ is published by voter on the bulletin board. Everyone can see data on the bulletin board. A voter can prove his/her vote to a malicious people. Because a voter know $(m_i \| G_i \| G_{i,1} \| \cdots \| G_{i,N}, s_i)$ from bulletin board and can open $(m_i \| G_i \| G_{i,1} \| \cdots \| G_{i,N}, s_i)$. It should be the distributed voting content for receipt-free scheme.

1.4 Our contribution

Recently, the receipt-free scheme is to be issued in e-voting and e-auction. For successful receipt-freeness, we should consider an outsider (or coercer) as well as all the participating authorities. In this paper, we refined the receipt-free scheme. As a basis of the refined receipt-free scheme, we analyzed receipt-free schemes of [4] and [11] (refer to Table 2). Both receipt-free schemes do not satisfy all the refined receipt-free schemes. In this paper, we proposed e-voting system which can satisfy the refined receipt-free scheme based on chameleon bit-commitment and secret sharing scheme. In the existed receipt-free schemes based on bit-commitment scheme, a voter generates secret seeds of bit-commitment. Therefore, a voter can open these commitments at any time. This can be caused that a voter can prove his/her voting to other people. To prevent this problem, administrator generates the secret seeds in the proposed e-voting system as Table 1.

Table 1 Comparison with the generator of secret seeds

	Who generates the secret seeds?
Our system	Administrator
[11]	Voter
[4]	Voter

Moreover, in application system based on cryptography techniques, efficiency and security are very important schemes. In this paper, we compared efficiency in aspect of computation and communication complexity. When a voter casts the voting, the scheme of [11] needs the communication complexity of *5O(m)+O(b)* . This result is same with our scheme. In case of [4], it needs the communication complexity of *3O(m)+2O(b).* In conclusion, the scheme of [4]

needs more challenger-response than [11] and our scheme. Satisfying all the refined receipt-free, our scheme has the same communication complexity with the scheme of [11]. In Section 4, we will give a more detailed explanation about computation and communication complexity.

Table 2 Comparison of the refined receipt-free scheme

	RFV	RFA	RFT
Our System	**Yes**	**Yes**	**Yes**
[4]	**No**	**No**	**Yes**
[11]	**No**	**No**	**Yes**

2. Related works

2.1 RSA encryption

RSA cryptosystem, named after its inventors R.Rivest, A.Shamir, and L.Adleman, is the most widely used public-key cryptosystem.

- Generate two large random p and q (each roughly the same size)
- Compute $n = pq$ and $\Phi(n) = (p-1)(q-1)$
- Select a random integer e, $1 < e < \Phi$, such that gcd(e, Φ)=1
- Use the refined Euclidean algorithm to compute the unique integer d, $1 < d < \Phi$, such that $ed \equiv 1 (\mathrm{mod}\, \Phi)$.
- Public key is (n, e) and private key is d.

2.2 Bit-commitment using variable secret sharing

For *RFT* and *RFC*, we use bit-commitment using Variable Secret Sharing (called VSS). VSS was proposed by A.Shamir [1]. A dealer divides some secret information into n, and divides the divided information among n-participants. By means of need, it is restored to the original state by means of need. We apply this VSS to bit-commitment as follows.

- A dealer chooses his secret key $x_j \in Z_q$ of bit-commitment and publishes his public key $h_j = g^{x_j}$
- A dealer chooses his secret seeds $r_{i,j} \in Z_q$ randomly and computes a sequence of bit-commitment

$$C_{k,j} = g^m h_j^{r_{k,j}}$$

, where m is the important message.

- A dealer divides $C_{k,j}$ to k, and distributes the divided $C_{k,j}$ between each participant.

$$C_{k,j} = C_{1,j} + C_{2,j} + \cdots + C_{k,j}$$
$$= g^{m_{1,j}} h_j^{r_{1,j}} + g^{m_{2,j}} h_j^{r_{2,j}} + \cdots + g^{m_{k,j}} h_j^{r_{k1,j}}$$

- To recover, it needs the divided $C_{k,j}$ of each participant.

3. E-voting system for the refined receipt-free scheme

3.1 Players

Voter V_i**.** A voter follows the election law of each country.

Administrator A**.** Administrator has a list of legitimated voters and plays the role of the determination whether the ballot is valid or not, and verifies double-voting. Also, administrator generates bit-commitment for the receipt-free.

Multi-tallier T_j $\{T_j \mid j = 0,1,2,\cdots,k\}$**.** Our e-voting system needs $k+1$ talliers from T_0 to T_k. Tallier T_0 plays the role for counting of voting results.

Bulltin-Board ***BB*****.** In bulletin board, everyone can see whether a voter casts to voting or not. But, they can not erase and modify voting contents. Bulletin board plays a important roles to prevent the voting forgery.

Preparation

The proposal E-voting system consists of Voter, Administrator, Multi-tallier, and Bulletin-Board. Let A be administrator and $\{T_j \mid j = 0,1,2,\cdots,k\}$ be Talliers and $C = \{l \mid l = 0,1,2,\cdots,k\}$ be candidates. Voter can choose the i-th candidate. Let be large primes $p = 2q+1$, q and a generator g of order q subgroup of Z^*_p.

3.2 Procedure

■ **Notation**

- v_i : Voting content of a voter
- d_{e_1}, N_A : Public key of administrator ($N_A = p_A q_A$)
- p_A, q_A , p_T, q_T : Large prime numbers
- S_i : Signature of administrator
- x : Random number
- N_T : Public key of administrator ($N_T = p_T q_T$)
- N_T, y : Public key of tallier T_0
- $r_{i,j}$: Secret seeds of bit-commitment ($r_{i,j} \in Z_q$)
- x_j : Secret key of bit-commitment by administrator ($x_j \in Z_q$)
- h_j : Public key of bit-commitment by administrator ($h_j = g^{x_j}$)

***(1)* Stage I : Authentication of a voter**

- Voter V_i makes his/her ID_i , and encrypts ID_i with administrator's public key $< d_{e_1}, N_A >$ as follows, and sends it to administrator.

$$B_i = (ID_i)^{d_{e_1}} \bmod N_A$$

- Administrator decrypts B_i with his/her secret key, and checks the right to voting and signs B_i as follows.

$$S_i = \sigma_i(B_i)$$

- Administrator sends S_i to voter, and sends $(S_i \| ID_i)$ to Bulletin-Board.

***(2)* Stage II : Voting stage**

- Voter chooses a vote v_i and encrypts v_i using the public key $< N_T, y >$ of tallier T_0 .

$$Z_i = y_T{}^{v_i} x^{r_t} \bmod N_T$$

- Voter encrypts $(S_i \| Z_i)$ using the public key of administrator.

$$E_A(S_i \| Z_i)$$

- Voter sends $E_A(S_i \| Z_i)$ to administrator.
- Administrator decrypts $E_A(S_i \| Z_i)$ and checks S_i and Z_i .
- Administrator chooses his secret key $x_j \in Z_q$ of chameleon bit-commitment and his public key $h_j = g^{x_j}$.
- Administrator chooses his secret seeds $r_{l,j} \in Z_q$ $(j = 1,2,\cdots,k)$ randomly and computes a sequence of chameleon bit-commitments. l is the number of voters.

$$C_{l,j} = g^{Z_i} h_j{}^{r_{l,j}}$$

- Administrator publishes the sequence of commitments $(C_{l,1}, C_{l,2}, \cdots, C_{l,k})$.
- Administrator sends each commitment $(C_{l,1}, C_{l,2}, \cdots, C_{l,k})$ to each tallier $(T_1 - T_k)$.

***(3)* Stage III : Counting stage**

- Administrator proves to each tallier T_j that administrator knows the secret key $\log_g h_j = x_j$ of the chameleon bit-commitment and the discrete logs $\log_g C_{l,j}$ by the interactive zero-knowledge proof.
- Administrator sends secret seeds $_j$

counting. In order to be opened the voting content, it needs tallier T_o's secret key, and it has to receive the secret seed $r_{l,j}$ for decryption. But, he can not know these data.

Theorem 2 (RFA) *Administrator can not prove voter's voting content to other people.*
After a voter cast the voting, a voter encrypts the voting v_i with the public key of tallier T_o, and sends the encrypted voting Z_i content to administrator with signature of administrator. Administrator can check whether a voter is a legal voter or not with his signature and voter's ID of bulletin board. But, he can not decrypt the encrypted Z_i, because he does not know tallier T_o's secret key.

Theorem 3 (RFT) *Tallier can not prove voter's voting content to other people.*
Our e-voting system consists of $k+1$ tallier. Tallier T_o plays a role as the counting of voting results, and talliers $(T_1 - T_k)$ play roles to manage secret seeds $r_{l,j}$ of chameleon bit-commitment. Because administrator re-encrypts the encrypted voting content Z_i, and sends $C_{l,j}(j=1,\cdots k)$ to talliers $(T_1 - T_k)$. Talliers $(T_1 - T_k)$ do not know the voting content.

Table 3 and Table 4 show communication complexities of the existed e-voting systems and our e-voting scheme. The number of voter, multi-tallier(or multi-center), and candidate is *a, b, m* respectively. $\leftrightarrow$ means both-direction communication, $\rightarrow$ means one-way direction. Also, BB is bulletin board, and $B_j \Rightarrow A_i$ means the one-way untappable channel from B_j *to* A_i.
Table 5 shows computational complexities of the existed e-voting system and our e-voting scheme.

Table 3 The communication complexity of the existed e-voting systems and our e-voting scheme

		Pattern	Roun	Vol
[11]	**Voting**	$V_i \rightarrow BB$	*a*	*O(m)*
	Voting	$V_i \rightarrow T$	*a*	*O(m)*
	Voting	$V_i \Rightarrow R_j$	*b × a*	*O(m)*
	Voting	$R_j \rightarrow BB$	*a*	*O(m)*
	Claiming	$R_j \rightarrow BB$	*a × m*	*O(m)*
	Counting	$T \leftrightarrow BB$	*b*	*O(b)*
[4]	**Voting**	$C_j \rightarrow BB$	*b*	*O(m)*
	Voting	$C_j \rightarrow BB$	*2b*	*2O(b)*
	Voting	$C_j \rightarrow V_i$	*b × a*	*O(m)*
	Voting	$C_j \Rightarrow V_i$	*a*	*O(m)*
Our Scheme	**Authentication**	$v_i \leftrightarrow A$	*2a*	*O(m)*
	Authentication	$v_i \rightarrow A$	*a*	*O(m)*
	Voting (Commit)	$B_j \rightarrow BB$	*b*	*O(m)*
	Voting (Proof)	$A_i \leftrightarrow BB$	*3b*	*O(m)*
	Voting (Secret Share)	$B_j \rightarrow A_i$	*b × a*	*O(m)*
	Counting	$A_i \leftrightarrow BB$	*a × m*	*O(m)*

Table 4 The comparison of communication complexity

Scheme	Volume of communication complexity
[11]	*5O(m)+O(b)*
[4]	*3O(m)+2O(b)*
Our scheme	*5O(m)+O(b)*

Table 5 The computation complexity of the existed e-voting systems and our e-voting scheme

		Communication Complexity

[11]	Voter	*m* chameleon BCs, *1+m* proofs and *m* secret sharings
[4]	Voter	*m* chameleon BCs, *1+m* proofs and *m* secret sharings
	Centers	M interpolations and verifications of the commitment
Our Scheme	Voter	*m* chameleon BCs, *1+m* proofs and *m* secret sharings
	Administrator	*m* interpolations and verifications of the commitments

5. Conclusion

Recently, several receipt-free schemes have been proposed for secure e-voting and e-auction. But, these schemes did not consider to all the participating authorities. In this paper, we defined the refined receipt-free scheme for e-voting. Moreover, we proposed e-voting protocol which satisfies the refined receipt-free scheme.

We compared the proposed e-voting system with [4] and [11] in aspect of computation and communication complexity. The communication complexity of the proposed e-voting is similar to those of [4] and [11]. But, the proposed e-voting system satisfies the refined receipt-free scheme, RFV, RFA, RFT, and RFC.

ACKNOWLEDGEMENT

The first author has been supported by the Grant-in-Aid for Creative Scientific Research No.14GS0218 (Research on System LSI Design Methodology for Social Infrastructure, Head of Researchers : Prof. Hiroto Yasuura, System LSI Research center, Kyushu University) of the Ministry of Education,Science, Sports and Culture(MEXT) from 2002 to 2006.

REFERENCES

[1] A. Shamir, " How to share a secret" Communications of the ACM, pp612-613, 1979.

[2] G.Brassard, D. Chaum and C. Crèpeau,"Minimum Disclosure Proofs of Know ledge", Journal of Computer and System Sciences, Vol.37, No.2, pp156-189, 1988.

[3] J. Benaloh and D.Tuinstra, " Receipt-Free Secret-Ballot Elections", Proc. of STOC'94, pp544-553, 1994.

[4] K.Sako and J. Kilian, "Receipt-Free Mix-type Voting Scheme", Proc, of Eurocrytpt'95, LNCS 921, Springer-Verlag, pp393-403, 1995.

[5] K.Sako and J. Kilian, "Secure Voting Using Partially Compatible Homomorphisms", Proc. of Crypto'94, LNCS 839, Springer-Verlag, pp411-424, 1994.

[6] J. Benaloh and M. Yung, "Distributing the Power of a Government to Enhance the Privacy of Votes", Proc. of PODC'86, pp.52-62, 1986.

[7] K.J.KIM, J.H. KIM, B.C. LEE, and G.W. A, "Experimental Design of Worldwide Internet Voting System using PKI" SSGRR2001, L'Aquila, italy, Aug, 2001.

[8] M.Abe and K. Suzuki, "Receipt-Free Sealed-Bid Auction", ISC2002, LNCS 2433, pp191-199, 2002

[9] M.Hirt and K.Sako, "Efficient receipt-free voting based on homomorphic encryption", Eurocrypt 2000, LNCS 1807, pp539-556, 2000.

[10] T. Okamoto, "An Electronic Voting Scheme", Proc. of IFIP'96, Advanced IT Tools, Chapman & Hall, pp 21-30, 1996.

[11] T. Okamoto, "Receipt-Free Electronic Voting Schemes for Large Scale Elections", Security Protocols Workshop, 1997.