

# Ballot-Cancellation Protocol of E-voting Based on Two Independent Authorities

Yong-Sork HER

Graduate School of Information Science and Electrical Engineering, Kyushu University, Japan

Address: 6-10-1, Hakozaki, Higashiku, Fukuoka, 812-8581, Japan

Tel: +81-92-642-3867

[ysher@itslab.csce.kyushu-u.ac.jp](mailto:ysher@itslab.csce.kyushu-u.ac.jp)

Kouichi SAKURAI

Faculty of Computer Science and Communication Engineering, Kyushu University, Japan

Address: 6-10-1, Hakozaki, Higashiku, Fukuoka, 812-8581, Japan

Tel: +81-92-642-3867

[sakurai@csce.kyushu-u.ac.jp](mailto:sakurai@csce.kyushu-u.ac.jp)

**Abstract:** Recently, many e-voting systems have been proposed for successful election. It should be satisfied many requirements for successful e-voting. In this paper, we propose the *ballot-cancellation scheme* in order to manage invalid ballots. Many proposed e-voting systems have been proposed without considering invalid ballots. It can be happened an invalid ballot during e-voting, and then we should consider to treat the invalid ballot keeping the privacy and the security.

## Introduction

It has been proposing many e-voting systems based on cryptography techniques [3][5][9][10]. A few systems of these are used in real election. But, most of proposed e-voting schemes had overlooked about a ballot-cancellation, which can cancel the ballot in voting results with keeping the privacy and the security. We should consider many situations for secure e-voting. Also, we found the special character on an absentee voting in Japan election law. According to Japan election law, after an absentee voter enforces the voting, if an absentee voter died or lost the right of casting the ballot before the Election Day, it is the invalid ballot. And then, we should cancel that ballot in the tallying with keeping the privacy and universal verifiability of an absentee voter.

In this paper we consider the ballot-cancellation scheme including an absentee e-voting. For the successful e-voting system, we must consider an absentee voter together with a general voter. For the ballot-cancellation scheme, we use the modified r-residue cryptography using homomorphic encryption. When the ballot is cancelled, everyone can not know the vote. That is, it is kept the private. After a voter cast the voting, the vote is double encrypted by two public keys of administrator and tallier. In our scheme, the ballot is cancelled without knowing the content of voting and the mark remains in the bulletin board. We introduced the double encryption of [9].

## Our ballot-cancellation protocol

In our scheme, the ballot-cancellation was based on r-th residue using homomorphic encryption. After a voter enforces the vote, a voter encrypts the voting content with r-th residue encryption. The voting content is exponential  $v_i$  and the exponential of the

encrypted voting content  $Z_i$  is  $k_i$ . First, our system checks the value of  $k_i$ , and then if  $k_i = 0$ , the encrypted voting content is 1. We can do the ballot-cancellation without knowing the voting content. So, it keeps a voter's privacy. There is an example of the ballot-cancellation as follows:

$$Z = \prod_{i=1}^{10} (Z_i)^{k_i} = Z_1^{k_1} Z_2^{k_2} Z_3^{k_3} Z_4^{k_4} Z_5^{k_5} Z_6^{k_6} Z_7^{k_7} Z_8^{k_8} Z_9^{k_9} Z_{10}^{k_{10}} \quad (1)$$

Suppose  $k_1 = k_4 = 0$  (In e-voting,  $k_1$  and  $k_4$  are invalid ballot (cancel)). The result of equation (1) is as follows.

$$Z = Z_2^{k_2} Z_3^{k_3} Z_5^{k_5} Z_6^{k_6} Z_7^{k_7} Z_8^{k_8} Z_9^{k_9} Z_{10}^{k_{10}} \quad (2)$$

In the equation (2),  $k_1$  and  $k_4$  do not give the influence others variables.

## Requirements for proposal e-voting system

In this paper, our goal is the secret e-voting including an absentee voter that can cancel the ballot. So, it should be satisfied as the following requirements.

**Privacy :** Privacy is the basic requirement in E-voting. The concept of privacy is that all votes must be secret. That is, everyone should not know to associate individual votes and voters.

**Security :** Many researches had been processing for the security of e-voting system. Most of e-voting systems consist of a few authorities. For the security, above all, it should not be concentrate the responsibility on voting results in an authority. Also, each authority enables the mutual checking on the vote result. In e-voting system, it is very important for the security to share equally roles on e-voting.

**Ballot-Cancellation :** It can be happened the situation that the ballot is cancelled in the tallying. For example, forge of voting, the voting by illegal voter and so on. It can not stop the voting due to a few illegal voters. When it does the ballot-cancellation, it must keep the transparency on the privacy and the fairness of an absentee voter. For really e-voting system, it needs the ballot-cancellation scheme.

**Universal verifiability :** Generally, a voter wants to know whether one's ballot includes exactly in the tallying or not. A voter can be claimed one's ballot to election office. The e-voting system should always prepare it.

**Robustness :** The voting system should be successful regardless of partial failure of the system.

**Fairness :** Nothing can after affect the voting.

## Construction of proposal e-voting system

### Construction of our e-voting

Our e-voting system consists of four organizations. That is, Voter (a general voter and an absentee voter), Tallier, Administrator including a voter's list and Bulletin board.

#### (1) Voter

A voter is divided into a general voter and an absentee voter. In this paper, we explain the e-voting in aspect of an absentee voter. A person who can not go to the voting place in Election Day is an absentee voter because of the public business or health and so on. The definition of an absentee voter is different by the election law of each country. An absentee e-voting can be connecting with a military voting because a military takes the best high ratio in absentee voters. An absentee voter must previously reserve to Election office.

#### (2) Administrator

Administrator has a list of legitimated absentee voters and plays the role of the determination whether the ballot is valid or not and

verifies the unresuability. The roles of Administrator are as follow s.

- Verify whether an absentee voter is a regal voter or not / whether voting is one time or not.
- Cast a mark 'verified' on the bulletin board

### (3) Tallier

Tallier verifies the received voting result from administrator whether this result is valid or not. Tallier computes voting results and announces voting results. The detailed roles are as follows.

- Compute voting results
- Compare with the number of voter that is computed by administrator
- Send voting results to bulletin board

### (4) Bulletin Board

In bulletin board, everyone can see whether a voter votes or not. But, they can not erase and modify voting contents. Keeping the security of absentee voter, we can know only the fact whether an absentee voter votes or not. In the real absentee voting, an absentee voter can not know the transmission of one's voting content. Also, absentee voter can request for the verification whether the content of absentee voting is exactly counted or not. For these, we use the Bulletin board.

**Table 1. Notation for proposal e-voting system**

<i>Voter</i>	<i>Administrator</i>	<i>Tallier</i>
<ul style="list-style-type: none"> <li>- Voter: <math>V_i</math></li> <li>- ID of each voter: <math>ID_i</math></li> <li>- Voting contents of Voter: <math>v_i</math> (<math>v_i = 0</math> or <math>1</math>)</li> <li>- <math>\sigma_i</math>: voter's sign (RSA digital signature)</li> <li>- <math>e_i</math>: blind value</li> </ul>	<ul style="list-style-type: none"> <li>- Public key : <math>\langle e_A, N_A \rangle</math></li> <li>- Private key : <math>\langle d_A, p_A, q_A \rangle</math> <math>N_A = p_A q_A, \quad e_A N_A \equiv 1 \pmod{(p_A - 1)(q_A - 1)}</math> <math>N_A \geq N_T^{e_A}</math></li> <li>- <math>p_A, q_A</math>: large prime numbers</li> <li>- <math>k_i</math>: Variable of the right of casting the ballot on Voter (<math>k_i = 0</math> or <math>1</math>)</li> <li>- <math>M</math>: Summation of voting results</li> <li>- <math>\sigma_A</math>: Absentee center's sign (RSA digital signature)</li> </ul>	<ul style="list-style-type: none"> <li>- Public key : <math>\langle N_T, y_T \rangle</math> (<math>N_T = p_T \cdot q_T</math>, <math>y_T</math> is random number)</li> <li>- Private key : <math>\langle p_T, q_T \rangle</math></li> <li>- <math>p_T, q_T</math>: large prime numbers</li> </ul>

## Procedure of proposed e-voting system for an absentee voter

### (1) Stage I : Double encryption

- Voter  $V_i$  selects vote  $v_i$  and encrypts  $v_i$  with the public-key  $\langle N_T, y_T \rangle$  of Tallier.

$$Z_i = y_T^{v_i} x^{r_{v_i}} \pmod{N_T} \quad (3)$$

- Voter  $V_i$  sends  $Z_i$  to Administrator A.
- Administrator A encrypts  $Z_i$  twice with the public-key  $\langle e_A, N_A \rangle$  of Administrator A.

$$C_i = Z_i^{e_A} \pmod{N_A} \quad (4)$$

### (2) Stage II : Blind Signature

- Voter  $V_i$  blinds  $C_i$  as follows.

$$e_i = x(C_i, r_i) \quad (5)$$

, where  $r_i$  is a randomly chosen blinding factor.

- Voter  $V_i$  signs  $e_i$  as  $s_i = \sigma_i(e_i)$  and sends  $\langle ID_i, e_i, s_i \rangle$  to administrator A.

- Administrator  $A$  checks the follows parts.

- .  $s_i$  is a valid signature of  $e_i$
- .  $ID_i$  is registered in a list and voter  $V_i$  has the right to vote

- If all checks pass, Administrator  $A$  signs  $d_i$  as follows and sends it to voter:  $d_i = \sigma_A(e_i)$

- Voter  $V_i$  unblinds  $d_i$  to obtain the signature  $y_i$  as follows:

$$y_i = \delta(d_i, r_i) \quad (6)$$

- Voter  $V_i$  checks that  $y_i$  is a valid signature of administrator for message  $x_i$ .

- Administrator  $A$  announces the number of voters who were given the administrator's signature, and sends  $\langle ID_i, e_i, s_i \rangle$  to bulletin board.

- Voter  $V_i$  sends  $\langle C_i, y_i \rangle$  to administrator  $A$  via an anonymous channel.

### (3) Stage III : The ballot-cancellation

- Administrator  $A$  checks the signature  $y_i$  of the ballot  $C_i$  using the administrator's verification key.

- If the check succeeds, Administrator  $A$  decrypts  $C_i$  using private key  $\langle d_A, p_A, q_A \rangle$  and gets  $Z_i$ .

- Administrator  $A$  checks the voter's right of casting the ballot and sends results to bulletin board. (Invalid ballot  $k_i=0$ , Valid ballot  $k_i=1$ )

- Administrator  $A$  computes the product for the collection as equation (12)

$$Z_c = \prod_{i=1}^h Z_i \text{ mod } N_A \quad (7)$$

- Administrator  $A$  creates ID  $ID_A$  and encrypts  $ID_A, Z_c$  with Administrator  $A$ 's private key  $\langle d_A, p_A, q_A \rangle$ .

$$(ID_A)^{d_A}, Z_c \text{ mod } N_A \quad (8)$$

- In order to confirm the computed  $Z_c$  by Administrator  $A$ , Voting center computes

$$\begin{aligned} C_v &= \prod_{i=1}^h C_i \text{ mod } N_A \\ C_e &= (Z_c)^{e_A} \text{ mod } N_A \end{aligned} \quad (9)$$

, where  $C_v$  is a product of encrypted votes on the Bulletin board. Tallier  $T$  compares  $C_v$  with  $C_e$ , if  $C_v = C_e$ , Administrator  $A$  convinces the computed  $Z_c$ .

#### <Proof on equation (9)>

In the administrator condition of Table 1, let be  $N_A \geq N_T^{e_A}$ . If  $h$  is 2,

$$\begin{aligned} C_v &= \prod_{i=1}^h C_i \text{ mod } N_A = (C_1 \times C_2) \text{ mod } N_A = \{(Z_1^{e_A} \text{ mod } N_A)(Z_2^{e_A} \text{ mod } N_A)\} \text{ mod } N_A \\ C_e &= (Z_c)^{e_A} \text{ mod } N_A = \{(Z_1 \text{ mod } N_A)(Z_2 \text{ mod } N_A)\}^{e_A} \text{ mod } N_A \end{aligned} \quad (10)$$

For  $C_v = C_e$ , it must be satisfied the following equation,

$$(Z_1^{e_A} \text{ mod } N_A)(Z_2^{e_A} \text{ mod } N_A) \stackrel{?}{=} \{(Z_1 \text{ mod } N_A)(Z_2 \text{ mod } N_A)\}^{e_A} \quad (11)$$

In equation 3,  $Z_i$  is always less than  $N_T$ , That is,  $Z_1$  and  $Z_2$  are less than  $N_T$ . In case of  $N_A \geq N_T^{e_A}$ ,  $Z_1^{e_A} \text{ mod } N_A$  is  $Z_1^{e_A}$ .

$$(Z_1^{eA} \bmod N_A)(Z_2^{eA} \bmod N_A) = Z_1^{eA} Z_2^{eA} \quad (12)$$

Also, the following equation is satisfied because of  $N_A \geq Z_1, Z_2$

$$(Z_1 \bmod N_A)(Z_2 \bmod N_A)^{eA} = (Z_1 Z_2)^{eA} \quad (13)$$

- Tallier  $T$  decrypts the encrypted ballot  $Z_i$  and accumulates each  $Z_i$  as follows.

$$Z_c = \prod_{i=1}^h (Z_i)^{k_i} \bmod N_T = \prod_{i=1}^h (y_T^{v_i} x^{r_{v_i}})^{k_i} \bmod N_T = \prod_{i=1}^l (Z_i)^1 \prod_{i=l+1}^n (Z_i)^0 = \prod_{i=1}^l (Z_i) \quad (14)$$

, where  $k_i$  is the decision value whether an absentee keeps the right of casting the ballot or not ( $k_i = 0$  or  $1$ )

<  $h = l + n$  ,  $h$ : whole ballot ,  $l$ : valid ballot ,  $n$ : Invalid ballot >

$$Z_l = \prod_{i=1}^l (Z_i)^1 \quad : \text{Valid ballot} \quad \quad \quad Z_n = \prod_{i=l+1}^n (Z_i)^0 \quad : \text{Invalid ballot} \quad (15)$$

- Last results of the voting are as follows.

$$Z_l = \prod_{i=1}^l (Z_i)^1 = \prod_{i=1}^h (y_T^{v_i} x^{r_{v_i}}) \bmod N_T = y_T^M x^{r_{v_i}} \bmod N_T, \quad (16)$$

$$M = \sum_{i=1}^l v_i \quad (17)$$

## Security of proposed e-voting system

### Privacy

In our e-voting system, the vote is encrypted by double-encryption. That is, after a voter does voting, a voter encrypts the voting content by two public keys, and encrypts with  $ID_i$  and the double encrypted voting contents  $C_i$  by one's private key and send it bulletin board. Although administrator decrypts the voting content, administrator can not see the voting content because of be double encrypted. Tallier can not see voter's ID because of has not the private key of administrator. No one can know the relation between a voter  $ID_i$  and voting contents.

### Security on two independent centers (Administrator, Tallier)

Administrator checks a voter's identification and can compute the number of voter. Tallier computes the last voting result and compares the voting result with the computed summation by administrator. Administrator and voting center can check mutually.

### Security on the fabrication of the vote

#### - Voter - Administrator

In this system, we use blind signature for the security of the vote instead of the voter's key. After a voter cast the voting, the voting content is encrypted by two public keys of administrator and tallier. Then, a voter blinds ( $e_i = x(C_i, r_i)$ ) the encrypted content ( $C_i$ ) and sends it to administrator. The voter can receive the signature value ( $d_i = \sigma_A(e_i)$ ) from administrator. If a voter want claim own content, a voter can confirm the content through the signature value of administrator.

#### - Administrator – Tallier

The vote is encrypted by two public keys of administrator and tallier. For the decryption of the vote (the counting), it needs two private keys of administrator and tallier. The last result  $M$  of vote is computed by tallier. But, administrator can check on the voting result through a few methods as follows.

- The number of signature  $d_i$ :  $d = \sum_{i=1}^l d_i$  / The number of a voter  $Z_i$ :  $Z_c = \prod_{i=1}^h Z_i \bmod N_A$

Administrator and tallier can keep each other in check on the voting results because the vote is encrypted by two public keys of administrator.

## Conclusion

In this paper, we proposed an e-voting system including an absentee voter based on double encryption, blind signature and the ballot-cancellation. In order to use double encryption, we used r-residue encryption and RSA, and used the variable  $k_i$  for the ballot-cancellation. In case of the ballot-cancellation, it can be happen the situation to be cancelled the ballot by some reasons (forge, lost the right of canting and so on). Also, we used blind signature and double encryption without using a voter's key. In e-voting parts, it had overlooked on the absentee voter and the ballot-cancellation. The absentee voting is very important in real election. In order to realize the secure e-voting in real world, we must more research on part s of an absentee voter.

## Acknowledgments

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

## References

1. J.D Cohen and M.J. Fischer. "A robust and verifiable cryptographically secure election scheme" In Proc.26<sup>th</sup> IEEE Symp. On Foundation of Comp. Science, pages 372-382, Portland, 1985.IEEE.
2. A.Fujioka, T. Okamoto, K.Ohta. "A Practical Secret Voting Scheme for Large Scale Elections", in Advances in Cryptology-AUSCRYPT '92, LNCS718, Springer-Verleg, Berlin, pp.244-251, 1993,
3. C.Park, K.Itoh, K.Kurosawa "Efficient Anonymous Channel and All / Nothing Election Scheme" EUROCRYPT '93, LNCS765, Springer-Verlag, Berlin Heidelberg 1994.
4. J.Cohen Benaloh and D.Tuinstra "Receipt-Free Secret-Ballot Elections" In STOC 94, pp544-553.1994
5. K.Sako, J.Kilian "Receipt -Free Mix-Type Voting Scheme" EUROCRYPT '95, LNCS921, pp393-403, Springer-Verlag, Berlin Heidelberg 1995
6. L.F. Canor and R..K. Cytron, "Design and Implementation of a Practical Security-Conscious Electronic Polling System", WUCS-96-02, Department of Computer Science, Washington University, St. Louis, Jan, 1996.
7. M.A.Herschberg, "Secure Electronic Voting Over the World Wide Web", Master Thesis in Electronic Engineering and Computer Science, Massachusetts Institute of Technology, 1997
8. R. Cramer, R.Gennaro and B.Schoenmakers "A secure and optimally efficient multi-authority election scheme" European Transactions on Telecommunication, 8:481-489, Eurocrypt 1997.
9. S.Tsujii, H.Yamaguchi, A.Kitazawa, K.Kurosawa "A Method for Voting Protocols with regards to Privacy" ISEC98-42, 1998.
10. M.Ohkubo, F.Miura, M.Abe, A. Fujioka, T.Okamoto "An Improvement on a Practical Secret Voting Scheme" ISW'99, LNCS 1729, pp225-234, 1999.
11. M.Hirt , K.Sako "Efficient receipt-free voting based on homomorphic encryption" Eurocrypt 2000, LNCS1807, pp539-556, 2000.
12. <http://www.votehere.com>
13. <http://www.mainichi.co.jp/> (June.24.2002)

**"References available upon request from Yong-Sork Her or Prof. K. Sakurai "**