Design of the Secure E-voting System Including Absentee Voters Which Enables Ballot-Cancellation Based on Double Encryption

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

Sakurai, Kouichi
Faculty of Computer Science and Communication Engineering, Kyushu University

Kim, Shin-Hwan
School of Computer and Communication Engineering, Daegu University, KOREA

https://doi.org/10.15017/6030

出版情報：Proc. of 2003 International Conference on Computers, Communications and Systems. 1, pp.69-74, 2003-02. BK21 IT Division, Daegu University
バージョン：
権利関係：

Design of the Secure E-voting System Including Absentee Voters Which Enables Ballot-Cancellation Based on Double Encryption

Yong-Sork HER[†], Kouichi SAKURAI[††], Shin-Hwan KIM[†††]

[†]Graduate School of Information Science and Electrical Engineering
Kyushu University, JAPAN
e-mail : ysher@tcslab.csce.kyushu-u.ac.jp
[††]Faculty of Computer Science and Communication Engineering
Kyushu University, JAPAN
e-mail : sakurai@csce.kyushu-u.ac.jp
[†††]School of Computer and Communication Engineering,
Daegu University, KOREA
e-mail : shkim@daegu.ac.kr

Abstract

Many electronic voting schemes have been proposed without considering an absentee voting. In this paper, we propose the secure e-voting scheme including an absentee voter based on double encryption, which can cancel the ballot in voting results, called ***ballot-cancellation.*** The double encryption scheme for e-voting system was proposed in [Hersch97][TYKK98]. The double encryption of [Hersch97] was only for strengthen encryption of the vote. On the other hand, Tsujii *et at.* proposed two double encryptions based on two independent authorities in [TYKK98]. The voting content is encrypted by two public keys of two independent authorities. Two authorities enable the mutual checking on each authority. In this paper, we modify double encryption of [TYKK98] and introduce the ballot-cancellation scheme based on r-th residue encryption. Also, for a voter's authentication, we use the blind signature based on [FOO92]. [FOO92] scheme was known as one of the standard schemes in e-voting. EVOX[Du99] and Sensus[CC96] had been implemented by [FOO92]. The disadvantage of this scheme is walk away. That is, after a voter cast the voting, a voter should send bit-commitment again for checking in counting stage. To prevent this disadvantage, we use the blind signature and double encryption by two mutual independent authorities (administrator and tallier) without using bit-commitment. In our scheme, we do not use a voter's key. So, after a voter casts the voting, a voter knows only signature value on own vote. This scheme can prevent an effluence of the voting content by a voter's key.

Keyword: Cryptography, Electronic Voting, Double encryption, Ballot-cancellation, Absentee voter, Security

1. Introduction

1.1 Motivation

It has been proposing many e-voting systems based on cryptography techniques [PIK93][TYKK98][OMAFO99]. A few systems of these are used in real election. But most of proposed e-voting schemes had overlooked about an absentee voter although an absentee voting takes the important percentage in real election. For practically e-voting system, an absentee voting must be necessarily included in e-voting system. 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. An absentee voter enforces the voting before Election Day and the vote is counted on Election Day. Therefore, it is high the possibility to be happened vote-buying and coercion because it remains one or two weeks till the counting of votes. We define the requirements of real e-voting system as follows.

- can include absentee voters for real e-voting system
- can cancel the ballot
- can keep the privacy without using a voter's key

1.2 Challenging issues

In Japan, the first electronic voting was enforced at Okayama on 23 June,2002. in order to select a mayor and a councilman of Nimi-city [MC]. In the same election, voting results were published by each voting method (See Table 1). A general voter used the e-voting system and anabsentee voter used the existing voting method. Because of using two election Okayama's voting is Electronic voting, not online voting [VH]. This was brought on new privacy problem without the existing voting method. We can know voting results in support of a general voter and an absentee voter by parties and candidate groups. The ratio of votes obtained is different between a general voter and an absentee voter. This difference can be used by political tactics. We notice the result of Okayama election in Japan.

In this paper, our issues are divided two. One is the ballot-cancellation for an absentee voter, the other is that it prevents an effluence of the voting content.

1.3 Our contribution

In this paper, we propose the e-voting system including an absentee voter based on blind signature, double-encryption and the ballot-cancellation. 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 keeps the private. Also, we use the blind signature and don't use a voter's private key. 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 [TYKK98].

Table 1. Ratio of votes obtained of candidate in Okayama e-voting

Candidate	E-voting <General voter>	The existing voting method <Absentee voter>
Candidate 1	78.4%	69.6%
Candidate 2	9%	11.5%
Candidate 3	5%	13.3%
Candidate 4	7.6%	5.6%
Total	100% <14,966 persons>	100% <1,719 persons>

1.4 Comparison of out proposal to the previous

In subsection we compare our schemes with [TYKK98] and [FOO92] (See Table 2). The meaning of Independent is that two authorities play each role. For example, there are two authorities, which are administrator and tallier, in FOO92. These two authorities play the independent role that administrator issues the signature on the security of the voting content after a voter cast the voting and tallier computes the result of voting. In case of mutual independent, two authorities take part in the security and results of voting and take the collective responsibility on the voting.

Table 2. Difference of between our e-voting system with TYKK98 and FOO92

Identity	**FOO92**	**TYKK98**	**Our system**
Two authorities	*Independent*	*Mutual independent*	***Mutual independent***
Ballot-cancellation	*No*	*No*	***Yes***
Voter's key for encryption	*Use*	*Use*	***Not use***

1.5 Organization of our paper

This paper is organized as follows: **Section 2** describes the voting procedure and **Section 3** describes the security in proposal e-voting system. Conclusions are given in **Section 4.**

2. Procedure of proposed e-voting system for an absentee voter

■ Notation

➢ ***Voter***

- Voter: V_i
- ID of each voter: ID_i
- Voting contents of Voter: v_i (v_i = 0 or 1)
- σ_i : voter's sign (RSA digital signature)
- e_i : blind value

➢ ***Administrator A***

- Public key : $< e_A, N_A >$
- Private key : $< d_A, p_A, q_A >$

  $N_A = p_A q_A, \quad e_A N_A \equiv 1 \bmod (p_A - 1)(q_A - 1)$
- p_A, q_A : large prime numbers
- k_i : Variable of the right of casting the ballot on Voter (k_i = 0 or 1)
- M : Summation of voting results
- σ_A : Absentee center's sign (RSA digital signature)

➢ ***Tallier T***

- Public key : $< N_T, y_T >$

  ($N_T = p_T \cdot q_T$, y_T is random number)
- Private key : $< p_T, q_T >$
- p_T, q_T : large prime numbers

< Stage I : Double encryption >

- Voter V_i selects vote v_i and encrypts v_i with the public-key $< N_T, y_T >$ of Tallier.

$$Z_i = y_T^{v_i} x^{r_{v_i}} \bmod N_T \quad (1)$$

-Voter V_i encrypts Z_i twice with the public-key $< e_A, N_A >$ of Administrator.

$$C_i = Z_i^{e_A} \bmod N_A \quad (2)$$

< Stage II: Blind Signature >

- V_i blinds C_i as follows.

$$e_i = x(C_i, r_i) \quad (3)$$

,where r_i is a randomly chosen blinding factor.

- V_i signs e_i as $s_i = \sigma_i(e_i)$.
- V_i sends $< ID_i, e_i, s_i >$ to administrator A.
- Administrator A checks the following parts.

  . s_i is a valid signature of e_i

  . ID_i is registered in a list and V_i has the right to vote
- If all checks pass, Administrator A sings d_i as following and sends it to Voter: $d_i = \sigma_A(e_i)$
- V_i unblinds d_i to obtain the signature y_i as follows:

$$y_i = \delta(d_i, r_i) \quad (4)$$

- V_i checks that y_i is a valid signature of administer for message x_i.
- A announces the number of voters who were given the administrator's signature, and sends $< ID_i, e_i, s_i >$ to bulletin board.
- Voter V_i sends $< C_i, y_i >$ to administrator A via an anonymous channel.

<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 $< d_A, p_A, q_A >$ 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 (11)

$$Z_c = \prod_{i=1}^{h} Z_i \bmod N_T \tag{5}$$

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

$$(ID_A)^{d_A}, Z_c \bmod N_A \tag{6}$$

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

$$\begin{aligned} C_v &= \prod_{i=1}^{h} (C_i)^{k_i} \bmod N_A \\ C_e &= (Z_c)^{e_A} \bmod N_A \end{aligned} \tag{7}$$

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

$$\begin{aligned} Z_c &= \prod_{i=1}^{h} (Z_i)^{k_i} \bmod N_T = \prod_{i=1}^{h} (y_T{}^{v_i} x^{r_{v_i}})^{k_i} \bmod N_T \\ &= \prod_{i=1}^{l} (Z_i)^1 \prod_{i=l+1}^{n} (Z_i)^0 = \prod_{i=1}^{l} (Z_i) \end{aligned} \tag{8}$$

, 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 >

$$Z_l = \prod_{i=1}^{l} (Z_i)^1 \quad \text{: Valid ballot} \tag{9}$$

$$Z_n = \prod_{i=l+1}^{n} (Z_i)^0 \quad \text{: Invalid ballot} \tag{10}$$

- Last results of the voting are as follows.

$$Z_l = \prod_{i=1}^{l} (Z_i)^1 = \prod_{i=1}^{h} (y_T{}^{v_i} x^{r_{v_i}}) \bmod N_T \tag{11}$$

$$= y_T{}^{M} x^{r_{v_i}} \bmod N_T ,$$

$$M = \sum_{i=1}^{l} v_i \tag{12}$$

3. 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 the mutual checking.

■ **The ballot-cancellation**

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. (See equation (8)). 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. (Refer to equation (9) and (10)). We can 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:

$$Z = \prod_{i=1}^{10} (Z_i)^{K_i} = Z_1{}^{K_1} Z_2{}^{K_2} Z_3{}^{K_3} Z_4{}^{K_4} Z_5{}^{K_5} Z_6{}^{K_6} Z_7{}^{K_7} Z_8{}^{K_8} Z_9{}^{K_9} Z_{10}{}^{K_{10}} \tag{13}$$

Suppose $k_1 = k_4 = 0$ (In e-voting, k_1, k_4 are invalid ballot (cancel)). The result of equation (13) is as following.

$$Z = Z_2{}^{K_2} Z_3{}^{K_3} Z_5{}^{K_5} Z_6{}^{K_6} Z_7{}^{K_7} Z_8{}^{K_8} Z_9{}^{K_9} Z_{10}{}^{K_{10}} \tag{14}$$

In the equation (14), k_1, k_4 give not the influence others variables.

- **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 following.

- The number of signature d_i : $d = \sum_{i=1}^{l} d_i$

(The total number of an issue signature)

- The number of a voter Z_i : $Z_c = \prod_{i=1}^{h} Z_i \bmod N_T$

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

4. 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 parts 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

[Cha81] D.Chaum "Untraceable electronic mail, return add resses, and digital pseudonyms" In Communications of the ACM, pp84-88, 1981.

[CF85] J.D Cohen and M.J. Fischer. " A robust and verifiable cryptographically secure election scheme" In Proc.26th IEEE Symp. On Foundation of Comp. Science, pages 372-382, Portland, 1985.IEEE.

[FOO92] 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,

[PIK93] C.Park, K.Itoh, K.Kurosawa " Efficient Anonymous Channel and All / Nothing Election Scheme" EUROCRYPT '93, LNCS765, Springer-Verlag, Berlin Heidelberg 1994.

[BT94] J.Cohen Benaloh and D.Tuinstra "Receipt-Free Secret-Ballot Elections" In STOC 94, pp544-553.1994

[SK95] K.Sako, J.Kilian " Receipt –Free Mix-Type Voting Scheme" EUROCRYPT '95, LNCS921, pp393-403, Spring er-Verlag, Berlin Heidelberg 1995.

[CC96] 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.

[CM96] R.Cramer, M.Franklin, B, Schoenmakers, M.Yung "Multi-Authority Secret-Ballot Elections with Linear Work" EUROCRYPT '96, LNCS1070, Springer-Verlag, Berlin Heidelberg 1996.

[Hersch97] M.A.Herschberg, " Secure Electronic Voting O ver the World Wide Web", Master Thesis in Electronic Engi neering and Computer Science, Massachusetts Institute of T echnology, 1997

[CGS97] R. Cramer, R.Gennaro and B.Schoenmakers "A secure and optimally efficient multi-authority electio n scheme" European Transactions on Telecommunicatio n, 8:481-489, Eurocrypt 1997.

[TYKK98] S.Tsujii, H.Yamaguchi, A.Kitazawa, K.Kurosawa " A Method for Voting Protocols with regards to Privacy" ISEC98-42, 1998.

[Du99] B.W. DuRette "Multiple administrators for elect ronic voting" http://theory.lcs.mit.edu/~cis/theses/DuRett e-bachelors.pdf, May, 1999

[OMAFO99] 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.

[HS2000] M.Hirt , K.Sako "Efficient receipt-free voting based on homomorphic encryption" Eurocrypt 2000, LNCS1807, pp539-556, 2000.

[BFPPS01] O.Baudron, P.-A. Fouque, D.Pointcheval, G.Po upard, J.Stern " Practical Multi-Candidate Election System" ACM 2001.

[JJ2002] A.Juels, M.Jakobsson "Coercion-resistant Elect ronic Elections" http://eprint.iacr.org/2002/165/, Nov,20 02

[VH] http://www.votehere.com

[MC] http://www.mainichi.co.jp/ (June.24.2002)