暗号技術に基づく不在者投票を考慮した電子選挙システムの設計

許, 容碩
九州大学システム情報科学府

櫻井, 幸一
九州大学大学院システム情報科学研究院

https://doi.org/10.15017/4784350

出版情報：九州大学情報基盤センター年報. 3, pp.37-46, 2003-03. 九州大学情報基盤センター
バージョン：
権利関係：

暗号技術に基づく不在者投票を考慮した電子選挙システムの設計

Design of E-voting System with an Absentee voter Based on Cryptographic Techniques

許容碩 *　　櫻井 幸一 **
Yong-Sork HER*　　Kouichi SAKURAI**

* 九州大学システム情報科学府
* Department of Computer Science and Communication Engineering, Kyushu University
** 九州大学システム情報科学研究院
**Faculty of Information Science and Electrical Engineering, Kyushu University

要旨　提案されている多くの電子投票システムでは不在者投票に対して考慮されていない. 実際の選挙において電子投票を利用するためには, 不在者も利用できるようにするべきである. 日本の現行の選挙法では不在者が投票を実施した後, 開票日の前に死亡したり, 投票権を喪失した場合には, その投票は無効票として処理される. したがってこのような状況に対応できる電子投票システムが必要である. 本論文では不在者も利用できる安全な無記名の電子投票システムを提案する. 提案する電子投票システムでは、二重公開鍵暗号を用いた投票プロトコルを利用することで秘密性を守りながら, 投票後の投票値の無効化手法を導入する.

Abstract　Many electronic voting schemes have been proposed without considering an absentee voting. For practically e-voting system, an absentee voting must be necessarily included in e-voting system. According to the existing election law of Japan, after an absentee voter enforces the voting, if absentee voter died or lost the right of casting the ballot before the tallying, the voting contents of this absentee are dealt with invalid. It needs e-voting system that is considered such these points in order to compose the real e-voting system. In this paper, we propose the secure unsigned e-voting scheme including an absentee voter We introduce the e-voting scheme based on double encryption which the ballot can be canceled, called the ballot -cancellation, with keeping the privacy.

1 Introduction

It has been proposing many e-voting systems based on cryptography techniques [4][6][11][13], i.e. 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

1.1 On-line voting vs Electronic Voting

There are a few kinds of voting systems in present. This voting system is a way of using computer technology to record votes, transmit ballots and tabulate elections [17]. The definition of Electronic voting is that it uses an electronic device in the voting method. That is, electronic touch screens as Okayama's e-voting (See subsection 1.2) replace paper ballots and it puts a store device instead of the ballot box. The characters of these voting methods are automatic processing and counting of voting. These parts are disadvantages in the existing voting system including the paper voting. Online voting is an upgrade from E-voting, in which the Internet is used to transmit ballots to the central computer and where voting stations can move beyond the poll site to community kiosks and, eventually to voting from PCs and Internet appliances [17]. So, it needs more powerful a voter's authentication and the security in online voting based on cryptography techniques. If the secure on-line voting is implemented and used in real election, it will be used more easily decisions of democracy country. Also, the problem of distance in the election will be gone.

1.2 Challenging issues

What is a problem if a general voter uses e-voting system and an absentee voter uses the existing voting? There is the real good example. 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 [18]. methods in the same election, voting results were published by each voting method (See table 1). A general voter used the e-voting system and an absentee voter used the existing voting method. Because of using two election Okayama's voting is Electronic voting, not online voting [17]. 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.

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 %
Tatal	100 %	100 %
	14,966 persons	1,719 persons

1.3 Requirements of proposed 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 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 happend 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.

■ Not using a voter's key

Most of developed e-voting schemes use a voter's encryption key for the encryption of the vote. If the encryption key of a voter is exposed to a third party or other people, it can be exposed the voting content. So, the management of voter's keys is very important problem in e-voting. Especially, in case of an absentee voter, it is required especial caution in the management of an absentee voter's keys because it remains one or two weeks till the counting.

■ Robustness

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

■ Fairness

Nothing can after affect the voting.

1.4 Basic works

■ Double encryption

Double-encryption [9] [11] is very useful to use both secrecy and authenticity because it applies successive transformations with different modular. Because double encryption uses two key-pair, we must consider the range of keys. The detailed explanation is as follows:

- Notation
  - p_A, q_A : the prime number is choosen by user A
  - $n_A = p_A q_A$, $\phi(n_A) = (p_A - 1)(q_A - 1)$
  - E_A : User A's encryption key
  - D_A: User A's decryption key
  - $E_A D_A \equiv 1 \ mod \ \phi(n_A)$
  - p_B, q_B : the prime number is choosen by user B
  - E_B : User B's encryption key
  - D_B: User B's decryption key
  - $n_B = p_B q_B$, $\phi(n_B) = (p_B - 1)(q_B - 1)$
  - $E_B D_B \equiv 1 \ mod \ \phi(n_B)$
  - M, M' : plaintext
  - C, C' : ciphertext
  - h : a threshold value.

-Basic conception

- User A want to send the signed secret message to User B.

$$C = E_B(D_A(M)) \qquad (n_A < h < n_B) \qquad (1)$$

, where h is a threshold value and $D_A(M) : A$ signed message.

- User B recovers M and checks A's signature as follows:

$$\begin{aligned} E_A(D_B(C)) &= E_A(D_B(E_B(D_A(M))) \\ &= E_A(D_A(M)) = M \end{aligned} \qquad (2)$$

-Extension of conditions

We explain the double encryption that is changed the condition from equation (1). Kohnfelder suggests another approach, pointing out that if $C = E_B(D_A(M))$ is not computable because $n_A < n_B$ then $C' = D_A(E_B(M))$ is computable.

- Case 1 : $n_A < n_B$

: The same of equation(2)

- Case 2 : $n_A > n_B$

$$\begin{aligned} D_B(E_B(C')) &= D_B(E_A(D_A(E_B(M))) \\ &= D_B(E_B(M)) = M \end{aligned}$$

In case1, a judge of A's signature must be able to verify that M originated with A. B send B's private key to C and C checks with$X = D_B(C)$ and M , whether not or $M = M'$ as follows.

$$M' = E_A(X)$$

In case2, the judge computes with C'and M as follows.

$$\begin{aligned} X &= E_B(M) \\ X' &= E_A(C) = E_A(D_A(E_B(M))) \end{aligned}$$

Using double-encryption, we can provide both secrecy and authenticity at same time.

■ Ballot-cancellation

We propose the ballot-cancellation scheme in this paper. 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 (13)). The voting content is exponential and the exponential v_i 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 (14)). 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:

$$\begin{aligned} Z &= \prod_{i=1}^{10} (Z_i)^{k_i} \\ &= Z_1^{k_1} Z_2^{k_2} Z_3^{k_3} Z_4^{k_4} Z_5^{k_5} Z_6^{k_6} Z_7^{k_7} Z_8^{k_8} Z_9^{k_9} Z_{10}^{k_{10}} \end{aligned} \tag{3}$$

Suppose $k_1 = k_4 = 0$ (In e-voting, k_1, k_4 are invalid ballot). The result of (3) is as following.

$$Z = Z_2^{k_2} Z_3^{k_3} Z_5^{k_5} Z_6^{k_6} Z_7^{k_7} Z_8^{k_8} Z_9^{k_9} Z_{10}^{k_{10}} \tag{4}$$

In the equation of (4), k_1, k_4 give not the influence others variables.

1.5 Related works

■ FOO92[3] scheme

In FOO92 scheme, the e-voting system consists of three. That is the administrator, a voter, the tallier. It is connected with anonymous channel between with a voter and the tallier. This scheme used blind signature and bit-commitment scheme. The disadvantage of this scheme is that a voter does not satisfy with walk-away because of using of bit-commitment. That is, after a voter cast the voting, a voter should send randomly chosen key $k_j$again for checking in counting stage.

■ TYKK98 [11] scheme

In 1998, Tsujii, Yamaguchi, Kitazawa and Kurowawa proposed the election model which can be practically available in the real-world election [11]. In [11], they used the ZKIP, RSA and r-th residue cryptosystem for homomorphic encryption. The characters of this system are two separate authorities (center1, center2) and double encryption. When a voter encrypts the voting content, a voter does double encryption using the public key of each authority. And then, it can prevent the risk that one authority takes the responsibility on results of whole election. Also, two authorities can prevent the forgery or the alteration on voting contents or results and can detect the illegality on voting result of each authority. The double encryption is very useful to use in e-voting system (see the next section (2)). E-vox [9][12] which was proposed by M.A.Herschberg introduced double encryption scheme in e-voting. In voting stage, a voter encrypts the vote with tallier's public key and anonymizer's public key. That is, it used double encryption for strengthen encryption on the vote. Two authorities (Tallier and Anonymizer) of E-vox had not the independence and the mutual checking of the vote. But, Double encryption of [11] enables the mutual checking on voting results as well as the decrease of responsibility on voting results through two independent authorities. Advantages of double encryption are as follows.

- It has the independence and the mutual checking by two separated authorities.
- It can be reduced the responsibility on voting results.
- In order to compute voting results, it needs two private keys of two authorities. It can not compute voting results with one private key.
- It can build up the security on voting contents.

1.6 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 does 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 [11].

1.7 Comparison of our proposal to the previous

In subsection, we compare our schemes with [11] and [3] (See table2). The meaning of Independent is that two authorities play each role. For example, there are two authorities, which are administrator and tallier, in [3]. 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. Ratio of votes obtained of candidate in Okayama e-voting

Identity	F0092	TYKK98	Our e-voting
Dependence of authorities	No	Yes	Yes
Ballot-cancellation	No	No	Yes
Voter's key for encryption	Use	Use	Not use

1.8 Organization of our paper

This paper is organized as follows: Section 2 describes the construction of proposal e-voting system. Section 3 describes the voting procedure and Section 4 describes the security in proposal e-voting system. Conclusions remark appears in Section 5.

2 Construction of proposed e-voting system

2.1 Overview of our e-voting

The goal of our e-voting system is ballot-cancellation with an absen-tee voter as well as basic requirements. For these, we use two independent authorities and double encryption. After a voter selects a candidate, the vote is encrypted by two public keys of administrator and tallier. A voter can not know the vote and proves the vote to a third trust or buyers. The double encrypted vote is blinded by the blind factor of a voter, and signed by a voter and sent to administrator. An administrator checks the voter and the vote, and signs the blinded value and returns a voter. So, a voter can take the own blind factor and the blind signature of administrator. To prepare the claim of a voter, these values will be used. After the voting time is over, a administrator checks whether a voter keeps the right of casting the ballot or not, a administrator assigns the value of the parameter and decrypts the double encrypted ballot and computes the product of the encrypted ballot. After tallier compares own computation results with the computed result by administrator and publishes the last result of the voting.

2.2 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.

-Voter

A voter is divided 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. For example, 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

reservation to Election office.

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

-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

-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.

3 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
  - e_i : blind value
- Administrator (See Appendix A.1)
  - Public key : $< e_A, N_A >$
  - Private key : $< d_A, p_A, q_A >$
  - p_A, q_A: large prime numbers
  - k_i: Vairable of the right of casting the ballot on Voter ($k_j = 0$ or 1)
  - M: Summation of voting results
  - σ_A : The sign of absentee center
- Tallier(See Appendix A.2)
  - Public key : $< N_T, y_T >$
  - 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.

$$Z_i = y_T^{v_i} x^{r_{vi}} \mod N_T \tag{5}$$

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

$$C_i = Z_i^{e_A} \mod N_A \tag{6}$$

[Stage II: Blind Signature]

- V_i blinds C_i as following.

$$e_i = x(C_i, r_i) \tag{7}$$

,wherer_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 signs d_i as following and sends it to Voter:

$$d_i = \sigma_A(e_i) \tag{8}$$

- V_i unblinds d_i to obtain the signature d_i as follows:

$$y_i = \delta(d_i, r_i) \tag{9}$$

- V_i checks that y_i is a valid signature of the administrator for message x_i . If the checks fails, V_i sends

$< C_i, y_i >$ to bulletin board.
- 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 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)

$$Z_c = \prod_{i=1}^{h} Z_i \mod N_T \quad (10)$$

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

$$(ID_A)^{d_A}, \quad Z_c \mod N_A \quad (11)$$

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

$$\begin{aligned} C_v &= \prod_{i=1}^{h} (C_i)^{k_i} \mod N_A \quad (12) \\ C_e &= (Z_c)^{e_A} \mod N_A \end{aligned}$$

, 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 as follows.

$$Z_c = \prod_{i=1}^{h} (Z_i)^{k_i} \mod N_T \quad (13)$$

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

,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)

$$\begin{aligned} Z_l &= \prod_{i=1}^{l} (Z_i)^1 : Valid - ballot \quad (14) \\ Z_n &= \prod_{i=l+1}^{n} (Z_i)^0 : Invalid - ballot \end{aligned}$$

- Last results of the voting are as follows.

$$\begin{aligned} Z_l &= \prod_{i=1}^{l} (Z_i)^1 \mod N_T \quad (15) \\ &= \prod_{i=1}^{h} (y_T^{v_i} x^{r_{v_i}}) \mod N_T \\ &= y_T^M x^{r_{v_i}} \mod N_T \end{aligned}$$

$$M = \sum_{i=1}^{l} v_i \quad (16)$$

4 Security of proposed e-voting system

■ Privacy

For privacy, everyone except a voter should not know the relation of a voter and the vote. Our e-voting system provides services as follows for privacy.
- After a voter does voting, a voter encrypts the voting content by two public keys

$$A_i = y_T^{v_i} x^{r_{vi}} \mod N_T, \quad C_i = Z_i^{e_A} \mod N_A$$

Here, a voter can not prove on the voting of one's own to the third party or other people because the voting is encrypted by two public keys. Especially, the voting is encrypted by a voter's key.

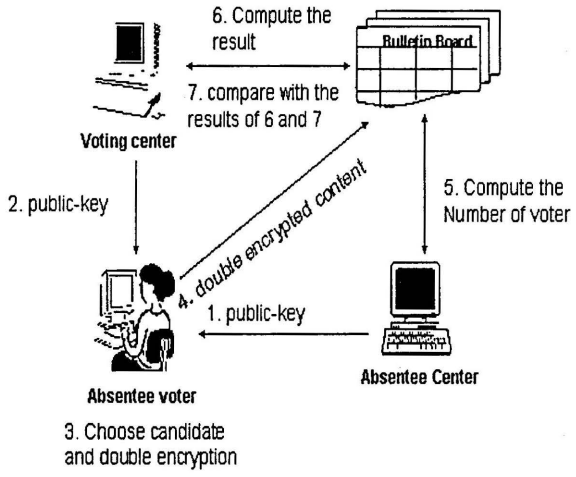

Fig. 1 Overview of our e-voting

- To prevent the fabication or the deletion of the voting by two authorities, a voter blinds with administrator on the double encrypted voting (C_i).
- After a voter blinds $e_i = x(C_i, r_i)$ the double encrypted voting (C_i) and signs ($s_i = \sigma_i(e_i)$) it, and send $< ID_i, e_i, s_i >$ with one's own ID to administrator.
- A voter can be taken the double encrypted voting and the signature d_i of administrator.
- If a voter wants a claim on one's vote, he can know the vote through administrator's signature d_i.
- After all, a voter can not proof one's own vote by oneself.

■ 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.

■ Security on the fabrication of the vote

- Voter-Administrator

  We use blind signature for the security of between a vote and administrator. After a voter cast the voting, the voting content is encrypted by two public keys of administrator and tallier. Then, a voter and administrator prove the double encrypted voting through blind signature. If it happens the problem in mutual proofs, a voter and administrator send each signature (s_i, d_i) to bulletin board. The security of a voter and administrator is kept by the blind signature. Also. although a voter want to deceive the vote together with administrator, they cannot see the original vote or proof on the original vote because they can not know the secret key of tally $< p_T, q_T >$.

- 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 of vote is computed by tallier. But, administrator can check on the voting result through a few methods as follows.
  - The number of signatured_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.

■ University verifiability

Administrator can compute the number of signature and the encrypted ballot, and compares with the last result of tallier. All computation results are posted on the bulletin board together with the right of casting the ballot and other information.

■ Fairness

In our e-voting system, four participants have mutual independent relationship and can be hold each other in check from the encryption of the vote to the computation of the vote. So, nothing can affect the voting process.

■ Robustness

The system can tolerate a certain number of faulty participants. Because the double encryption based

on RSA and r-th residue encryption and blind signature is used, robustness is guaranteed.

5 Conclusions

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 for the ballot-cancellation. In case of the ballot-cancellation, this scheme can apply to Japanese election law. Also, it can be happened the situation to be cancelled the ballot by some reasons (forge, lost the right of canting and so on). 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.

Acknowledgements

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. He is grateful for their support

参考文献

[1] D.Chaum *"Untraceable electronic mail, return addresses, and digital pseudonyms"* In Communications of the ACM, pp84-88, 1981.

[2] J.D Cohen and M.J. Fischer *"A robust and verifiable cryptographically secure elelction schme"* In Proc.26th IEEE Symp. on Foundation of Comp.Science, pages 372-382, Portland, 1985.IEEE.

[3] A.Fujioka, T. Okamoto, K.Ohta. *"A Practical Secret Voting Scheme for Large Scale Elections"* in Advaces in Cryptology-AUSCRYPT '92, LNCS718, Springer-Verleg, Berlin, pp.244-251, 1993,

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

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

[6] K.Sako, J.Kilian *"Receipt -Free Mix-Type Voting Scheme"* EUROCRYPT '95, LNCS921, pp393-403, Springer-Verlag, Berlin Heidelberg 1995.

[7] 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

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

[9] M.A.Herschberg *"Secure Electronic Voting Over the World Wide Web"* Master Thesis in Electronic Engineering and Computer Science, Massachusetts Institute of Technology, 1997

[10] 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.

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

[12] B.W. DuRette *"Multiple administrators for electronic voting"* http://theory.lcs.mit.edu/ cis/theses/DuRette-bachelors.pdf May, 1999

[13] 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.

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

[15] O.Baudron, P.-A. Fouque, D.Pointcheval, G.Poupard, J.Stern *"Practical Multi-Candidate Election System"* ACM 2001

[16] A.Juels, M.Jakobsson *"Coercion-resistant Electronic Elections"* http://eprint.iacr.org/2002/165/, Nov,2002

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

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

Appendix

A . r-th Residue encryption

Secret key: Two large prime numbers : p_T, q_T
Public key: $N_T = (p_T q_T)$, y_T (y is a random number)
Voting: v_i
Encryption $Z_i = y_T^{v_i} x^{r v_i} \mod N_T$
, x is a random number

$[case1] r : odd$	$[case2] r : even$
$gcd(p_T - 1, r) = e_1$	$gcd(p_T - 1, r) = e_1$
$gcd(q_T - 1, r) = e_2$	$gcd(q_T - 1, r) = e_2$
$r = e_1 e_2$	$2r = e_1 e_2$
$gcd(e_1, e_2) = 1$	$gcd(e_1, e_2) = 2$

(17)

Decryption

$$\begin{aligned} & \mod p_T \\ Z_i^{(p_T-1)/e_1} &= (y_T^{v_i} x^{r v_i})^{(p_T-1)/e_1} \\ &= (y_T^{(p_T-1)/e_1})^{v_i} (x^{r/e_1})^{(p_T-1)} \\ &= (y_T^{(p_T-1)/e_1})^{v_i} \end{aligned} \tag{18}$$

$$\begin{aligned} & \mod q_T \\ Z_i^{(q_T-1)/e_2} &= (y_T^{v_i} x^{r v_i})^{(q_T-1)/e_2} \\ &= (y_T^{(q_T-1)/e_2})^{v_i} (x^{r/e_2})^{(q_T-1)} \\ &= (y_T^{(q_T-1)/e_2})^{v_i} \end{aligned} \tag{19}$$

- Choose i , $(1 < i < r)$ and compare the following equation.

$$(y_T^{(p_T-1)/e_1})^i \mod p_T \quad and \quad (y_T^{(q_T-1)/e_2})^i \mod q_T \tag{20}$$

B. RSA

Secret key: $< p_T, q_T, d_A >$ (p_T and q_T are two large prime numbers)
- Compute $N_A = p_T q_T$ and $\phi(n_A) = (p_A - 1)(q_A - 1)$
- Select a random number e, $1 < e < \phi(n_A)$, such that $gcd(e, \phi) = 1$
- Use the extended Euclidean algorithm to compute the unique integer d , such that $ed \equiv 1 \mod \phi(n_A)$
Public key: $< e_A, N_A >$
Encrypted vote: Z_i
Encryption: $C_i = Z_i^{e_A} \mod N_A$
Decryption: Use the private key d_A to recover $Z_i = C_i^{d_A} \mod N_A$
Proof: (k is an integer)

$$\begin{aligned} Z_i^{e_A d_A} &= Z_i^{1+k\phi(n_A)} \mod N_A \\ &= Z_i (Z_i^{\phi(n_A)})^k \mod N_A \\ &= Z_i \mod N_A \end{aligned} \tag{21}$$