Multi-Candidate E-Voting System for Absentee

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

Sakurai, Kouichi
Graduate School of Information Science & Electrical Engineering, Kyushu University

出版情報：Proc. of the 2002 Korea-Japan Joint Symposium on Advanced Engineering & Science. 1, pp.111-117, 2002-08. Korea-Japan Joint Symposium on Advanced Engineering & Science
バージョン：
権利関係：

Multi-Candidate E-Voting System for Absentee

Yong-Sork HER, Kouichi SAKURAI

Graduate School of Information Science & Electrical Engineering
Kyushu University, Fukuoka, 812--8581, Japan
ysher@tcslab.csce.kyushu-u.ac.jp, sakurai@csce.kyushu-u.ac.jp

ABSTRACT

The voting plays important roles in a democratic country. Due to the problems of the existed voting m ethod, the new voting methods, electronic voting system, have been developing using the computer net work and cryptographic techniques. Many electronic voting schemes have been introduced for secure electronic voting systems. In this paper, we propose the secure electronic voting for absentee e-voting system. The absentee voting plays the important percentage in the existing voting system. But, the abs entee vote can not look forward to the security because of transmit by mail. The absentee does not kno w whether one's voting is exactly counted or not. In this paper, we propose the absentee e-voting syste m based on security, completeness and verifiability. We use r-th residue cryptography for homomorphi c encryption, ZKIP (Zero-Knowledge interactive proofs), RSA algorithm. Also, we propose the ne w method of tallying for multi-candidate. The goals of out voting system are the absentee vot ing based on privacy, universal verifiability, reuseability and multi-candidate.

1. Introduction

The world's democracy has been carried out the voting system by means of public opinions and decision-makings. The method of voting is a little difference by countries. Paper voting system is widely used in many countries and has been used for a long time. But, the losses related to manpower, time, and money in carrying out paper voting are still for too great for most counties. To depend on the advancement in electronic and the technologies of information and telecommunications, many countries are developing the new voting system. The core of e-voting is only legal voter to voting and correct counting must be getting. In voting and counting process, the voting and counting haven't to being modify and omit. A several items for successful e-voting system are as following[8][13][14].

-Privacy**:** It is must keep the secret between all voter and votes.
-Completeness: All valid votes should be counted exactly.
-Unreusability: All legal voter can vote only one-time
-Fairness: Nothing has not to affect the voting.
-Eligibility: No one who is not allowed to vote can vote
-Soundness: Anyone cannot disturb the voting.
-Verifiability: Anyone can identify the votes result.

2. The first e-voting of Japan

2.1 Overview

In Japan, the first electronic voting was enforced at Okayama on 23, June, 2002 in order to select the mayor and a councilman of Niimi city[24]. The used voting system is touch panel method like ATM (Automated-teller machine) of bank. The voting sequence is as follow.
① after a voter does the voter authentication; he/she receives the cryptography input IC card.
② He inputs the IC card in voting terminal and he selects the candidate as the voting screen seeing.
③ When he goes out the voting place, return the IC card to the election committee.
The voting result is recorded in the recorder that is located in the voting terminal and can be

Table 1. Analysis on OKAYAMA's e-voting

Items	The existed voting - 1994 (Paper voting)	The electronic voting - 2002
The number of officer in the voting place (43-voting place)	180 persons	178 persons
The number of officer in the counting place	85 persons	58 persons
The number of admission member	13 persons	13 persons
The counting time **- major** **- councilman**	 3 hours 4 hours 25 minutes	 25 minutes 25 minutes
The number of an invalid ballots **- major** **- councilman**	 242 214	 0 0
The voting ratio	92.06 %	86.82%
The costs of election	\11,630,000	\16,460,000

automatic counted. Table 1 shows the comparison of the existed voting and e-voting in Niimi-city.

2.2 Analysis results

In this paper, we analyze the e-voting of Okayama. This e-voting have a disadvantage and advantage. First, the advantages are as follows.

- The counting time was shortened. Indeed, the voting result can know as soon as the voting finishes. But, it takes the time that collect the recorder from tens of voting place and verify the voting result. When we compare the existed voting system, it is epoch-making thing and reduces the cost and time for the ballot counting.
- It can be reduced the invalid ballots. There was no end to the controversy about the invalid ballots. It is possible a blank ballot (a voter is not choose the candidate), but is not the invalid ballots. Therefore, it is not the controversy about the invalid ballots.
- It can be reduced the number of election officer. The number of officer is few different when the existed voting compares with the e-voting of Okayama. This is caused the first e-voting.
- In this e-voting, the election costs was high than the existed voting system. It is need many moneys for the costs of initial development but it can reduce the election costs.
- The handicapped person cans the voting in the e-voting. Especially, a visual handicapped person cans the voting through a headset.

The disadvantages and problems are as follows.

- A voter has the problems of the confidence about new voting system. Although the necessity of a new method such as e-voting is recognized, the credibility on the new voting equipment is quite low. It needs the previously practice about the e-voting method before the actual e-voting is doing.
- It should make up some countermeasures for e-voting terminal trouble. In the e-voting of Okayama, it was happened the two voting terminals trouble of 154 voting terminals.
- It can be occurred the mistake of election officer. It needs the previously education to the elections officer and a voter.
- The absentee voting in the Okayama election is same with the existing voting used on the mail voting. So, it needs more time for the counting. In the election law of Japan, it is not permit the e-voting of absentee.

In case of absentee voting, it was used to the existed voting method. That is, absentee voted the voting before general voting does. The absentee's voting contents transmitted by mail and counted by tallier's hands. According to

Japan's election law, if an absentee died or loss the right of casting the ballot in Election Day, the absentee's voting contents is dealt with invalid. The election law is different by each country. This paper based on this absentee election law.

2.3 The requirements of absentee e-voting by analysis results

The characters of Absentee e-voting must consider as following.

- Before general voting does, absentee voting must enforce.
- In Election Day, absentee voting contents are counted with general voting contents.
- There is a special case. After absentee voter enforced the voting, if absentee voter died or the loss of the right of casting the ballot before the Election Day (the absentee voting contents is counted), the voting contents of this absentee is dealt with invalid.

In order to implement the secure absentee e-voting, we must consider the character of absentee e-voting as well as basic requirements of e-voting. Especially, our design goals are completeness and verifiability. In the existing absentee voting, the absentee does not know that the exactly counting and the identification of one's voting. But our proposal e-voting system is improved about these points. In this paper, it puts three systems: voting system, absentee system and bulletin board. We adopt r-th residue cryptography for homomorphic encryption, ZKIP, RSA algorithm[25].

Section 3 explains the cryptography algorithm. In section 4, we introduce the election procedure.

3. Cryptography algorithm

We use the r-th residue cryptosystem, ZKIP (Zero-knowledge interactive proofs) and RSA cryptosystem for absentee e-voting.

3.1 r-th residue cryptosystem

The parameters and the encryption /decryption processing are as follows.

- Secret key : Two large prime p and q
- Public Key : $N (=pq), y$
- Plain-text : $m (0 \le m \le r)$
- Cipher-text : $E(m) = y^m x^r \bmod N$, , where r is a random number
- Decryption : Compute mod p and mod q about as following equation.

$$\{E(m)\}^{(p-1)/e1} = (y^{(p-1)/e1})^m \bmod p$$
$$\{E(m)\}^{(q-1)/e2} = (y^{(q-1)/e2})^m \bmod q$$

Compare,

$$(y^{(p-1)/e1})^i \bmod p \text{ and } (y^{(q-1)/e2})^i \bmod q$$

The important character in r-th residue cryptosystem is homomorphism. That is,

$$E(m+n) = E(m)E(n)x^r \bmod N$$

3.2 RSA cryptosystem

The 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 $Ø(n)= (p-1)(q-1)$
- Select a random integer $e, 1 < e < Ø$, such that $gcd (e, Ø) =1$
- Use the extended Euclidean algorithm to compute the unique integer $d, 1 < d < Ø$, such that $ed \equiv 1 \pmod{Ø}$.
- Public key is (n,e) and private key is d.

3.3. ZKIP(Zero-knowledge interactive proofs)

Zero-knowledge protocols enable to convince anyone who wants to be assured that some information is collect without giving away any information about the secrets involved.

Absentee system must confirm whether Absentee ballot is valid or not. Also, it is invalid ballot in case of absentee death or the loss of the right of casting the ballot. Then, we must deal with the contents of the vote without doing not know about contents of the vote itself. Then, we use this protocol.

3.4 New computation method of tallying

In this paper, we propose the new computation method of tallying using prime factorization. This method is as follow. Suppose a voter is 10-person and a candidate is 3-person.

The prime number is assigned each candidate as table 2.

If a voter choose the candidate, and then the prime number of a candidate is assigned the

voting contents. Table 3 shows the example.

Table.2 Prime number on each candidate

Candidate	Prime number
A	2
B	3
C	5

Table 3. Example of virtual voting

	Voting 1 (Candidate)	Voting 2 (Candidate)	Voting 3 (Candidate)
Voter 1	2 (A)	3 (B)	2 (A)
Voter 2	3 (B)	2 (A)	5 (C)
Voter 3	3 (B)	2 (A)	2 (A)
Voter 4	3 (B)	3 (B)	2 (A)
Voter 5	5 (C)	2 (A)	5 (C)
Voter 6	2 (A)	3 (B)	3 (B)
Voter 7	5 (C)	3 (B)	5 (C)
Voter 8	5 (C)	5 (C)	5 (C)
Voter 9	5 (C)	3 (B)	3 (B)
Voter 10	2 (A)	5 (C)	2 (A)
Multiplication of voting contents	**135000**	**48600**	**90000**
Results of voting	**A(3), B(3), C(4)**	**A(3), B(5), C(2)**	**A(4), B(2), C(4)**

In case of voting 1, the multiplication of voting result is 135,000. This value computes the prime factorization only one as follow.
Voting 1 : $135000 = 2^3 \times 3^3 \times 5^4$
Voting 2 : $48600 = 2^3 \times 3^5 \times 5^2$
Voting 3 : $90000 = 2^4 \times 3^2 \times 5^4$
That is, the exponential number is the result of voting.

4. Election Procedure

4.1 Absentee voter

In the existing voting system, the problem of absentee voting is one of the most sensitive parts. Absentee election votes before a general voter votes and it needs the previously reservation.
The components are as follow.

- Each absentee voter V_i *(i= 1 - h)*
- Choose absentee V_i vote : m_i , 1 for yes-vote and 0 for no-vote
- Encrypt m_i with the public key (N_2, y) of ES(Election System) :

$$Z_i = y^{mi} x^r \bmod N_2$$

- Encrypt *Zi* with the public key (e_{c1}, N_1)

$$C_i = Z_i^{\,eci} \bmod N_i$$

- Absentee voter's ID : ID_i
- Absentee voter's message: MSG_i, containing absentee's name and date of voting and signs with absentee's secret key.
- Ballot ; $ID, C_i, (MSG_i)di \bmod N$

4.2 Absentee system

Absentee system has a list of legitimated absentee voters and plays the role of the determination whether the ballot is valid or not and can verify the unresuability. The roles of Absentee system are as follow.

- Decrypt the message of absentee voter
- Verify the absentee voter
- Cast a mark 'verified' on the bulletin board
- Received the value of invalid vote from Election office
- Send the received results of absentee voting to VS

4.3 Voting system

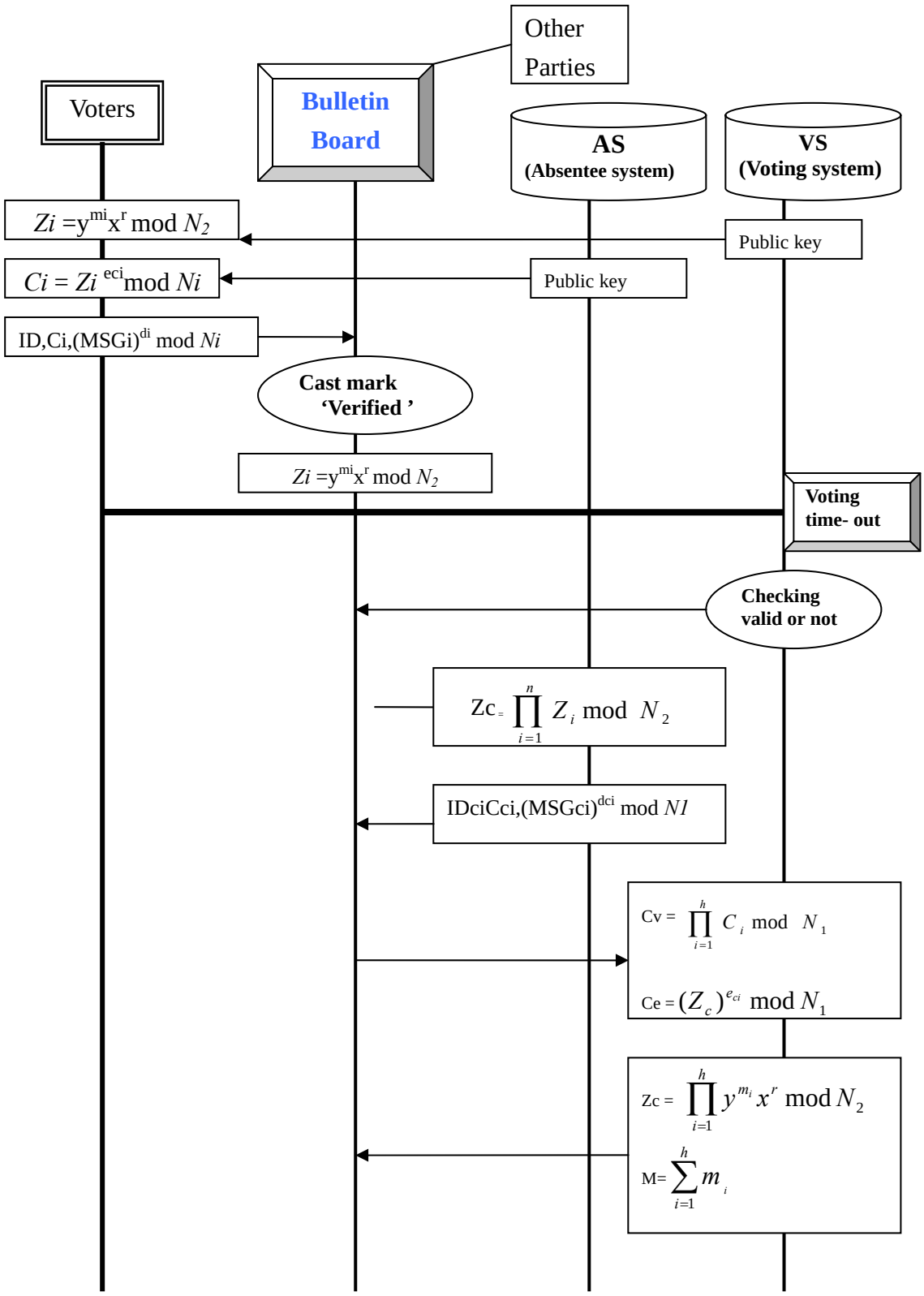
Voting system verifies the received voting result from absentee system whether this result is valid or not. The voting systme computes the voting results with the new tallying method and announce the voting results.

4.4 Voting procedure

Fig.1 shows flow of the proposed e-voting s ystem for absentee. In Fig.2, we can see the overview of e-voting system.

Register an absentee V_i in Election office.
Receive the VS's public key $< N_2, y >$
Receive the AS's public key $< e_{ci}, N_1 >$
Choose absentee *Vi* vote : m_i , 1 for yes-vote and 0 for no-vote

Fig.1 Flow of absentee E-voting System



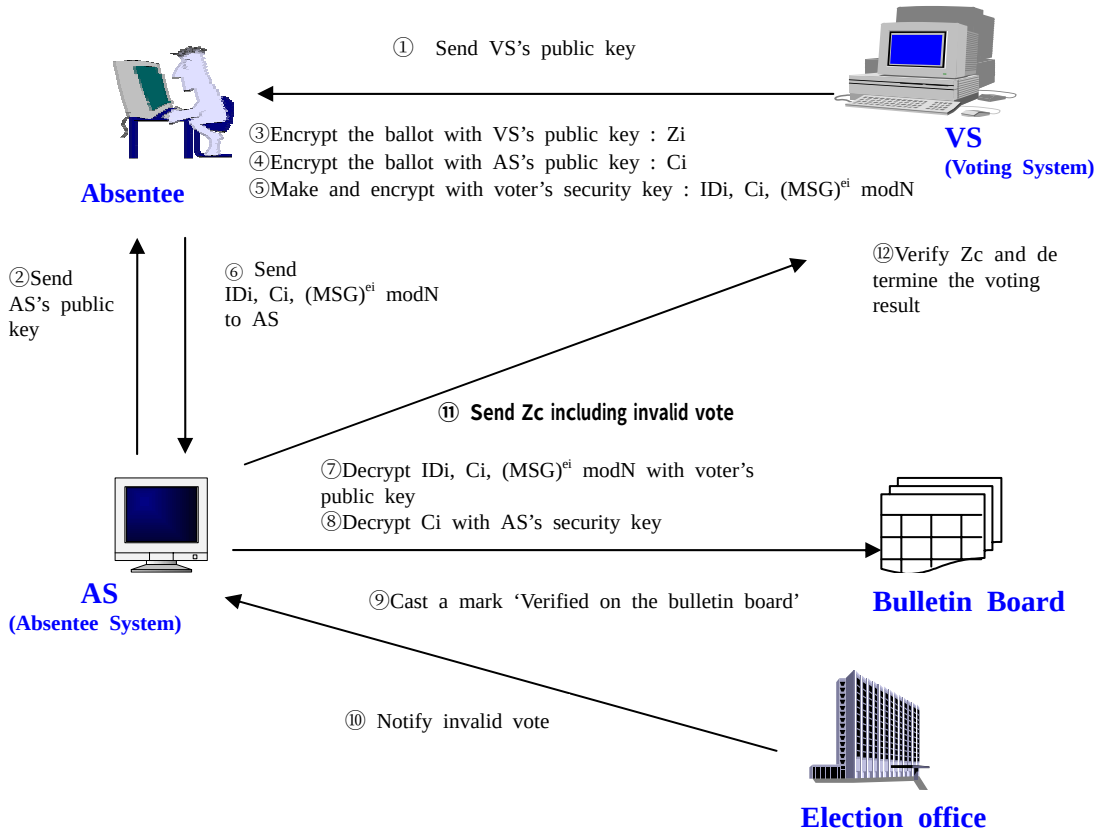


Fig. 2 Overview of absentee voting system

Encrypt m_i with the public key (N_2, y) of VS

$$Z_i = y^{mi} x^r \bmod N_2$$

Encrypt Z_i with the public key (e_{c1}, N_1) of AS

$$C_i = Z_i^{\,eci} \bmod N_i$$

Make absentee voter's ID(ID_i) and absentee voter's message ($MSGi$), containing absentee's name and date of voting

Sign with absentee's secret key.

Send ID, C_i, $(MSG_i)^{ei} \bmod N$ to AS

Decrypt ID, C_i, $(MSG_i)^{ei} \bmod N$ with absentee's public key

Decrypt C_i with AS's security key

Cast a mark 'Verified' on the bulletin board for university verifiability.

Notify invalid vote (absentee died or lost the voting right) from Election office

If a absentee ballot is invalid ballot, Cast a mark 'invalid ballots' on the bulletin board

Bulletin board computes

$$Z_c = \prod_{i=1}^{n} Z_i \bmod N_2$$
$$= y^{mi} x^r \bmod N_2$$

Multiply $\prod_{i=1}^{n} m_1$ and the result of computation send to VS

The result is computed the method of pri me factorization, announce of the voting resu lt.

Seeing the exponential of prime factorization, announce of the voting result.

5. Conclusions

We proposed an e-voting system for absentee voter based on the proposed tallying method. Most of e-voting system is not suitable the e-voting system of multi-candidate because of the difficulty of tallying and security of e-voting system. We proposed the new tallying method for multi-candidate based on prime factorization. In this paper, we decided the invalid or valid ballot whether a absentee died or not by the Election Day. The voting contents are not known anyone and mix with the general voting content and keep the privacy of absentee.

The election law is different by each country. So, it needs e-voting suitable to the election law in order to realize of e-voting.

Reference

[1]Avi Rubin. Security Considerations for remote electronic voting over the Internet, 2000 http://avirubin.com/e-voting.security.pdf

[2]B.Schoenmakers “Fully Auditable Electronic Secret-Ballot Elections” Internet Techhology, http://www.win.tue.nl

[3]Internet Policy Institute. Internet Voting. http://www.internetpolicy.org

[4]Irwin Mann, CFP '93.- Open Voting Systems, New York University, Mar, 1993

[5]J.H Kim, K.G Kim “ Design of secure Internet Voting Protocol under PKI” IRIS and ICU

[6]K.J Kim, J.H Kim, B.C Lee, and G.W Ahn “Experimental Design of Worldwide Internet Voting System using PKI” SSGRR2001, L'Aquila, Italy, Aug. 6-10, 2001 http://caislab.icu.ac.kr/pub/paper_international/body.html

[7]L.F.CRANOR, R.K.Cytron “Sensus : A Security-Conscious Electronic Polling System for the Internet” http://theory.lcs.mit.edu/~cis/voting

[8]M.Ohkubo, M.Abe, A.Fujioka and T.Okamoto, “An Improvement on a Practical Secret Voting Scheme” Information Security’99, LNCS Vol.1729, pp 225-234, Springer-Verlag, 1999

[9]M.S.LEE “ Modern Cryptography “ Gyousa, vol 1, Mar. 2000

[10]Mark A. Herschberg, Secure Electronic Voting Using the World Wide Web, Master's Thesis. MIT, Jun, 1997

[11]Michael Shamos. CFP '93- Electromic voting-evaluating the threat. http://www.cpsr.org/

[12]National Commission on Federal Election Reform. http://www.reformelections.org

[13]National Security Research Instiute “Modern Cryptology” Kyungmoon, 2000

[14]R. Cramer, M.Franklin, B.Schoenmakers, M.Yung “ Multi-Authority Secret-Ballot Elections With Linear Work” EUROCRYPT’96, pp72-83, Springer-Verlag, LNCS Vol.1070, 1996 http://www.cs.ucdavis.edu/franklin/research

[15]Ronald L. Rivest, David Jefferson, Shuki Bruck, A Modular Voting Architecture ("Frogs") , August 18, 2001

[16]Ronald L. Rivest, “Electronic Voting” Laboratory for Computer Science, Massachusetts Institute of Technology, Cambrige, MA 02139, http://theory.lcs.mit.edu/~rivest/Rivest/ElectronicVoting. Pdf

[17]Ronald L. Rivest,, Security in Voting Technology, MIT, May 24.2001

[18]Roy G. Saltman. Accuracy, integrity, and security in computerized vote-tallying. Technical report, Computer Science and Technology, National Bereau of Standards, Gaithersburg, MD20899, August 1988. NBS Special Publication 500-158. http://www.itl,nist,gov

[19]Senator Dary. L.Jones, Newsletter, Vol 1 .Issue2

[20]Uchida AKI “ A Analysis of Electronic Voting , Electronic Greeting Card System and the plan of System by using Cryptography technology” Kyushu Univ, Dept of Communication Engineering, Feb.2001

[21]Y. S Her, G. J. Kim “ Implementation of the Electronic Vote System Using Internet” the paper for M.S in Taegu Univ.

[22]Y.S HER, K. SAKURAI “The Analysis of Current State and Future on the E-voting System” SCIS2002. Vol.1, pp537-542, 29. Jan. 2002, Japan

[23]Y.S HER, K. SAKURAI, J.G.KIM “ The Current State and Issue on the Implementation of Electornic Voting System in Internet” PYIWIT02,

[24] THE MAINICHI NEWSPAPERS http://www.mainichi.co.jp/

[25] S, Tshjii, H.Yamaguchi, A.Kitazawa, K.Kurosawa “ A Method for Voting Protocols with regards to Privacy“ ISEC98-42, Nov.1998.

[26] J.Cohen, M.Yung “ Improving Privacy in Cryptographic Elections“ February 1986. http://research.microsoft.com/~benaloh/

[27] J.Benaloh, M. Yung “ Distributing the Power of a Government to Enhance the Privacy of Voters “ Proceedings of the 5th Symposium on Principles of Distributed Computing. Calgary, AB. August 1986. (New York, USA: ACM 1986), pp. 52--62.