# The Secure Electronic Voting System for Absentee

Her, Yong-Sork
Kyushu University

Sakurai, Kouichi
Kyushu University



出版情報：電気関係学会九州支部連合大会講演論文集. 1, pp.355-355, 2002-08. 電気関係学会九州支部連合大会
バージョン：
権利関係：

# The Secure Electronic Voting System for Absentee

Yong-Sork Her, Kouichi SAKURAI
Kyushu University

**Abstract**

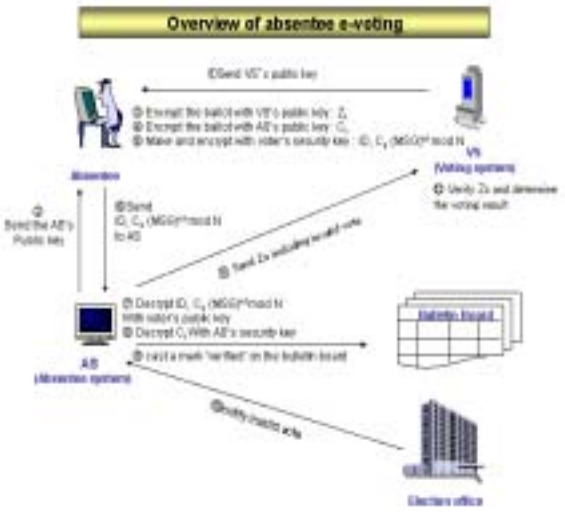
In this paper, we propose the absentee e-voting system based on security, completeness and verifiability. We use r-th residue cryptography for homomorphic encryption, ZKIP (Zero-Knowledge interactive proofs), RSA algorithm for the secure absentee e-voting.

## 1. Introduction

The absentee voting plays the important percentage in the existing voting system. But, the absentee vote can not look forward to the security because of transmit by mail. The absentee does not know whether one's voting is exactly counted or not.

## 2. The proposal e-voting system for absentee

Our proposal e-voting system for absentee consists of four parts. Fig.1 shows the structure of e-voting system. This system consists of five parts that is Absentee, Absentee system, Voting system, Bulletin Board and Election office.




<Fig.1> Overview of e-voting system

### 2.1 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 notification of invalid vote from Election office
- Send the received results of absentee voting to VS

### 2.2 Voting system

Voting system verifies the received voting result from absentee system and announces the voting results.

## 3. Voting Procedure

① Register an absentee $V_i$ in Election office.
② Receive the VS's public key $< N_2, y>$
③ Receive the AS's public key $< e_{ci}, N_1 >$
④ Choose absentee $V_i$ vote : $m_i$, 1 for yes-vote and 0 for no-vote
⑤ Encrypt $m_i$ with the public key $(N_2, y)$ of VS
$$Z_i = Y^{mi} x^r \bmod N_2$$
⑥ Encrypt $Z_i$ with the public key $(e_{c1}, N_1)$ of AS
$$C_i = Z_i^{\ eci} \bmod N_i$$
⑦ Make absentee voter's ID($ID_i$) and absentee voter's message ($MSG_i$), containing absentee's name and date of voting
⑧ Sign with absentee's secret key.
⑨ Send $ID_i, C_i\ (MSG_i)^{ei} \bmod N$ to AS
⑩ Decrypt $ID_i, C_i\ (MSG_i)^{ei} \bmod N$ with absentee's public key
⑪ Decrypt $C_i$ with AS's security key
⑫ Cast a mark 'Verified' on the bulletin board
⑬ Notify invalid vote (absentee died or lost the voting right) from Election office
⑭ Compute $Z_c = Z_i - Z'_i$ ($Z_i$ is valid ballot, $Z'_i$ is invalid ballot)
( $\mathbf{1} \le \mathbf{i} \le \mathbf{h}$ , The valid ballots are $\mathbf{1} \le \mathbf{i} \le n$ and the invalid ballots are $\mathbf{n+1} \le \mathbf{i} \le \mathbf{h}$) ; $Z_c = Z_i - \mathbf{Z'}_i$
$= \Pi_{i=1}^{\ n} Z_i \bmod N_2 - \Pi_{i=n+1}^{\ h} Z'_i \bmod N_2$
⑮ Make $ID_{ci}, Z_c\ (MSG_{ci})^{dci} \bmod N_1$ using AS's secret key
⑯ Send $ID_{ci}, Z_c\ (MSG_{ci})^{dci} \bmod N_1$ to VS
⑰ Decrypt $ID_{ci}, Z_c\ (MSG_{ci})^{dci} \bmod N_1$ with AS's public key
⑱ Verify $Z_c$ and determine the voting result

## 4. Conclusions

We proposed the absentee e-voting system and considered the absentee died or loss the right of casting the ballot in Election Day. Also, we kept the privacy, completeness, verifiability 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] S, Tshjii, H.Yamaguchi, A.Kitazawa, K.Kurosawa " A Method for Voting Protocols with regards to Privacy " ISEC98-42, Nov.1998.
[2] J.Cohen, M.Yung " Improving Privacy in Cryptographic Elections " February 1986.
http://research.microsoft.com/~benaloh/
[3] J.Benaloh, M. Yung " Distributing the Power of a Government to Enhance the Privacy of Voters " Calgary, AB. August 1986. (New York, USA: ACM 1986), pp. 52--62.
[4]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
[5]A.J.Menezes, P.C.van Oorschot, S.A. Vanstone " Handbook of Applied Cryptograhpy " CRC, 1997