1-out-of L E-voting System with Efficient Computational Complexity Based on r-th Residue Encryption

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

Imamoto, Kenji
Graduate School of Information Science and Electrical Engineering, Kyushu University

Sakurai, Kouichi
Faculty of Information Science and Electrical Engineering, Kyushu University

出版情報：IEICE Technical Report, ISEC2005-59. 105 (194), pp.117-122, 2005-07. IEICE
バージョン：
権利関係：

社団法人 電子情報通信学会
THE INSTITUTE OF ELECTRONICS,
INFORMATION AND COMMUNICATION ENGINEERS

信学技報
TECHNICAL REPORT OF IEICE

1-out-of-L E-voting System with Efficient Computational Complexity Based on r-th Residue Encryption

Yong-Sork HER † Kenji IMAMOTO † and Kouichi SAKURAI ‡

† Graduate School of Information Science and Electrical Engineering, Kyushu University, 6-10-1, Hakozaki, Higashi-ku, Fukuoka, 812--8581 Japan

‡ Faculty of Information Science and Electrical Engineering, Kyushu University, 6-10-1, Hakozaki, Higashi-ku, Fukuoka, 812--8581 Japan

E-mail: † {ysher, imamoto}@itslab.csce.kyushu-u.ac.jp, ‡ sakurai@csce.kyushu-u.ac.jp

Abstract In this paper, we propose an e-voting system with a ballot-cancellation property. The existed voting systems had overlooked about the ballot-cancellation scheme. There is the reason that the ballot is cancelled according to an election law. For example, when a right of casting the ballot is Election Day, the ballot-cancellation scheme is needed for an absentee voter. Usually, the absentee voter casts a ballot before Election Day. If the absentee voters which cast a ballot die or lost the right of casting the ballot before Election day, the ballots of absentee voters should be cancelled according to the election law. When the ballot is cancelled, the ballot-cancellation scheme should satisfy privacy and verifiability. Cramer *et al.* proposed a very efficient multi-authority election schemes which guarantee privacy, robustness, and universal verifiability at Eurocrypt'97. Yamaguchi *et al.* pointed out that the e-voting system based on multi-party has much computing resources, and proposed the two-centered e-voting protocol based on r-th residue encryption and RSA cryptosystem. However, their system is just yes-no voting. First, we propose a 1-out-of-L e-voting based on Yamaguchi *et al.*'s scheme. Second, we extend this 1-out-of-L e-voting to the ballot-cancellation scheme.

Keyword E-voting, Mix-net, Ballot-cancellation scheme, Cryptography

1. Introduction

1.1. Motivation

A voting has been used as the most important means in democratic decision-making. The conventional voting has a few problems; manpower, time, money and so on. To overcome these problems, many e-voting systems [FOO92,PIK93,CC96,CGS97,HS00,SK95] based on cryptography techniques have been proposed. However, most of proposed e-voting schemes had overlooked about a ballot-cancellation scheme. Many researchers think that there is not the reason to be cancelled the ballot in e-voting system. However, there are the reasons to be cancelled the ballot according to the e-voting system or the election law. We introduce the reasons as follows.

Case 1. Under the special condition which the right of casting the ballot is Election Day, if absentee voters die or lost the right of casting the ballot before Election Day, the ballots of the absentee voters should be cancelled.

Case 2. It can be found a substitute vote or illegal vote by a voter.

Case 3. It can be found a substitute vote by a malicious election committee.

Table 1. Ballot-cancellation scheme by the right of casting the ballot

The right of casting the ballot	Ballot-cancellation property
Election Day	Necessary
A voting point	Unnecessary

Case 1 can be happened by the election law of each country, and *Case 2* and *Case 3* can be happened by the defect of e-voting system. Actually, to prevent an illegal ballot and a substitute ballot like *Case 2* and *Case 3*, a voter should prove on his voting (namely *proof of validity of the ballot*), and an election committee should prove on his computation (namely *proof of validity of encryption or decryption*).

But, if the illegal ballot or the substitute ballot is found in the proposed e-voting systems, the e-voting systems will be stopped. Also, to prevent the problem of *Case 3*, some e-voting systems[CGS97,HS00] use threshold secret sharing scheme using multi-party. But, the computation complexity of these e-voting systems is higher than other e-voting system which does not use multi-party [YKDKT03]. *Case 1* is related to the right of casting the

ballot. The right of casting the ballot is different by the election law. The right of casting the ballot is divided to two; the voting point and Election Day.

The case which the right of casting of ballot is Election Day (i.e., Japan's election law) is required the ballot-cancellation scheme for the successful absentee e-voting (See table 1). Here, we introduce the conventional absentee voting and its ballot-cancellation scheme.

Absentee voting method in the conventional voting method

The voter registers in the voter list as an absentee voter. The qualification of absentee voter is different according to the election law.

- Before Election Day, the absentee voter receives voting sheet and two envelopes for casting a ballot from the election committee. (When the right of casting the ballot is the voting point, the absentee voter receives only one envelope.)
- After the absentee voter casts the ballot at a secret place such as a voting place, he inserts the ballot into the first envelope.
- He inserts the enveloped ballots into the second envelop and signs the certification on the second envelope.
- A delivery man delivers the double enveloped ballot to the election committee.

Then, it can be happened the following problems.

- *Delivery delay* : A delivery man can deliver the enveloped ballot after the vote counting is over.

- *Delivery omission* : A delivery man may not deliver it to the election committee.

Ballot-cancellation scheme in the conventional voting method

- In Election Day, seeing the signature of the absentee voter on the second envelope, the election committee checks the right of casting the ballot of the absentee voter.
- If the absentee voters die or lost the right of casting the ballot, the election committee deletes his vote. Then, election committee does not know his voting content.

In this ballot-cancellation scheme, a malicious election committee may be seeing the voting content. For the secure ballot-cancellation scheme, it is required the following conditions.

- *Privacy*: When the ballot is cancelled, everyone should not know the voting content.

- *Verifiability:* Everyone has to check whether or not the ballot is cancelled correctly.

In this paper, we concentrate on the ballot-cancellation scheme of absentee voting for perfect e-voting system.

1.2. Homomorphic property in r-th residue encryption

Cohen and Fischer [CF85] applied first the homomorphic functions to e-voting system. Recently, many e-voting systems [CGS97,YKDKT03,HS00] have been used the homomorphic property for achieving universal verifiability. A general definition of the notion is as follows [CGS97]. Let ξ denote a probabilistic encryption scheme. Let M be the message space and C the ciphertext space such that M is a group under operation $\oplus$ and C is a group under operation $\otimes$.

We say that ξ is a $(\oplus,\otimes)$-homomorphic encryption scheme if for any instance E of the encryption scheme if for any instance E of the encryption scheme, given $c_1 = E_{r_1}(m_1)$ and $c_2 = E_{r_2}(m_2)$, there exists an r such that

$$c_1 \otimes c_2 = E_r(m_1 \oplus m_2)$$

Homomorphic encryption schemes are important for the construction of election protocols. If one has a $(\oplus,\otimes)$ scheme, then if c_i are the encryptions of the single votes, by decrypting $c = c_1 \otimes \ldots \otimes c_m$ one obtains the tally of the election, without decrypting single votes. Here, we introduce the homomorphisim based on r-residue encryption and extend it in order to apply to the ballot-cancellation scheme.

A. Homomorphic property based on r-th residue encryption

The r-residue encryption satisfies the following homomorphism.

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

For example, we define $E(m)$ and $E(n)$ as follows.

$$E(m) = y^m x^r \bmod N, \quad E(n) = y^n x^r \bmod N$$

Then,

$$\begin{aligned} E(m+n) &= y^{m+n} x^r \bmod N, \\ E(m)E(n) &= (y^m x^r \bmod N)(y^n x^r \bmod N) \\ &= y^{m+n} x^r \bmod N \end{aligned}$$

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

B. Extended homomorphic property based on r-th residue encryption

We can define $E(m-n)$ as follows.

$$E(m-n) = \{E(m)/E(n)\}x^r \bmod N$$

For example, we define $E(m)$ and $E(n)$ as follows.

$$E(m) = y^m x^r \bmod N, \quad E(n) = y^n x^r \bmod N, \quad (m > n)$$

Then,

$$E(m-n) = y^{m-n}x^r \bmod N,$$
$$E(m)/E(n) = (y^m x^r \bmod N)/(y^n x^r \bmod N)$$
$$= y^{m-n}x^r \bmod N$$

Therefore,

$$E(m-n) = \{E(m)/E(n)\}x^r \bmod N$$

1.3. Our contribution

In this paper, we propose the ballot-cancellation scheme for an e-voting system. As mentioned in section 1.1, there are a few reasons that the ballot is cancelled. We concentrate on the ballot-cancellation by election law (*Case 1*). When the ballot is cancelled, it should be guaranteed privacy and verifiability. That is, everyone should not know the voting content of the cancelled ballot (*Privacy*) and should verify that the ballot is cancelled fairly (*Verifiability*). Cramer *et al.* [CGS97] proposed a very efficient multi-authority election schemes which guarantee privacy, robustness, and universal verifiability at Eurocrypt'97. Yamaguchi *et al.*[YKDKT03] pointed out that the e-voting system based on multi-party has much computing resources, and proposed the two-centered e-voting protocol based on r-th residue encryption and RSA cryptosystem. We concentrate on Yamaguchi *et al.*'s e-voting system which has the less computing resources. Yamaguchi *et al.*'s e-voting system used double encryption based on RSA cryptosystem and r-residue cryptosystem with homomorphic property. Our goal is the efficient 1-out-of-L e-voting system with the ballot-cancellation property.

- **First**, we propose a 1-out-of-L e-voting based on Yamaguchi *et al.*'s scheme. In case of the 1-out-of-L e-voting, a voter has L possibilities and should prove his vote is one of them. For this proof, we propose L possibilities for r-th residue encryption. The voter can prove his vote is one of L possibilities through this proof method. Moreover, we propose the proof of validity of ballot for our 1-out-of-L e-voting based on r-th residue encryption. Yamaguchi *et al.* 's proof is just for yes-no voting. When we compare the computation complexity of the proposed 1-out-of-L e-voting with that of the 1-out-of-L e-voting based on ElGamal encryption, we can know that our e-voting system is very efficient computational complexity. That is, the computation complexity of the 1-out-of-L e-voting based on ElGamal encryption has $O(M^{L-1})$ and our 1-out-of-L e-voting has just $O(M)$, where M is the number of voters. In the case of the 1-out-of-L e-voting based on ElGamal encryption, we must compute for each possibly as yes-no e-voting based on ElGamal encryption. But, we compute the final tally for a lump in the proposed 1-out-of-L e-voting.
- **Second**, we extend our 1-out-of-L e-voting system to the ballot-cancellation scheme. For our 1-out-of-L e-voting with the ballot-cancellation scheme, we use the extended homomorphic r-th residue encryption, L possibilities and the proof of validity of ballot for r-th residue encryption.

2. 1-out-of-L e-voting system based on [YKDKT03]

2.1. L possibilities for discrete logarithm and for r-th residue encryption

Many proposed e-voting systems are just for yes-no voting. In the real world, 1-out-of-L voting is more required than yes-no voting for democratic decision-making. Most proposed 1-out-of-L e-voting schemes [Sch99,CGS97] are based on ElGamal encryption and publicly verifiable secret sharing (PVSS). The publicly verifiable secret sharing in the e-voting system is used in order to satisfy robustness. That is, although some participant colludes with other participants, the voting system is successful. Usually, the e-voting system based on the publicly verifiable secret sharing consists of multi-authority. Multi-authority voting systems require much computational resources [YKDKT03].

In this section, we extend Yamaguchi *et al.*'s scheme to 1-out-of-L e-voting system. A voter has L possibilities in 1-out-of-L e-voting system, and he should prove his vote is one among L possibilities. In the case of the

1-out-of-L e-voting system based on publicly verifiable secret sharing scheme [Sch99], it uses the following proof.

- The voter V_i casts his vote v_i from the set $\{M^0, M^1, ..., M^{L-1}\}$, where M is the number of voters.
- He distributes the secret g^{s_i} among the authorities and publishes the value $U_i = g^{s_i + v_i}$. The proof of

$$\log_G(GC_0) = \log_g U_i \vee \log_G(G^M C_0)$$
$$= \log_g U_i ... \vee \log_G(G^{M^{L-1}} C_0) = \log_g U_i$$

, where $C_0 = G^{s_i}$ is published as a part of distribution protocol. The authorities decrypt the value Σv_i using homomorphic property. The original Yamaguchi *et al.*'s e-voting system is only for yes-no voting. They used a coin proof with value 0 or 1. The vote which can be selected by the voter is 0 or 1. For proof of validity of the ballot, Yamaguchi *et al.* used the extended bit-commitment proof using discrete logarithm. This proof is applied when the message probability is *1/2*. In 1-out-of-L- voting, the message probability which the voter can select is *1/L*. Therefore, to apply Yamaguchi *et al.*'s e-voting system to 1-out-of-L e-voting, it needs the proof of *L* possibilities for r-th residue encryption and the proof of validity of the ballot.

L possibilities for r-th residue encryption

We propose L possibilities for r-th residue encryption as follows.

- Suppose that a voter chooses his vote m_i from the set $\{G_1, ..., G_L\}$ which are generators of N_2 and $0 \le G_1, ..., G_L < r$. $\{G_1, ..., G_L\}$ of L possibilities are encrypted to $\{Z_1, ..., Z_L\}$, where $Z_i \equiv y^{m_i} x_i^r \bmod N_2$.
- The voter proves that his vote is one of the set

$$\log_y(Z_i S / R) = \log_y(Z_1 S / R) \vee, ..., \vee \log_y(Z_L S / R)$$

,where $S = s_i^r$, $R = x_i^r \bmod N_2$, and $s_i (\in N_2)$ is a random number. By L possibilities for r-th residue encryption, the voter can prove the validity of his voting without revealing his voting. Table 2 shows the proof of validity of the ballot for 1-out-of-L e-voting based on double-encryption.

2.2. Our 1-out-of-*L* e-voting

Our 1-out-of-L voting uses double encryption based on r-residue encryption and RSA encryption like Yamaguchi *et al.*'s scheme [YKDKT03] and consists of two centers, *Center 1* and *Center 2*.

1-1. Take L generators $G_1, ..., G_L$ of N_2 like [CGS97] where $0 \le G_1, ..., G_L < r$. A voter chooses his vote $m_i (i = 1, ..., L)$ from the set $\{G_1, ..., G_L\}$.

1-2. The voter proves his vote is one among L generators using L possibilities of r-th residue encryption.

1-3. The voter generates Z_i, E_i and C_i like Yamaguchi *et al.*'s scheme.

1-4. The progress procedure is same with Yamaguchi *et al.*'s scheme before the computation of final tally.

1-5. Center 2 decrypt Z with his secret key p_2 and q_2 and obtain the final tally M.

$$Z = \Pi_{i=1}^{l} Z_i = y^M X^r \bmod N_2, \quad M = k_1 G_1 + ... + k_L G_L,$$
$$X = \Pi_{i=1}^{l} x_i$$

The final tally M is

$$M = k_1 G_1 + ... + k_L G_L$$

, where $k_i (i = 1, ..., L)$ is each number of gained ballot.

2.3. The computation of final tally

In this section, we compare the computation complexity of our 1-out-of-L e-voting with that of 1-out-of-L e-voting based on ElGamal encryption. In 1-out-of-L voting systems based on ElGamal encryption, we can get the finally tally W as follows [CGS97].

$$W = G_1^{k_1} G_2^{k_2} ... G_L^{k_L}$$

For the final tally, we should compute each $k_i (i = 1, ..., L)$ from W as follows [Dip02].

Note that the condition $\Sigma_{i=1}^{L} k_i = m, \quad m \le M$ (m is the number of the voters participating in the voting) can be exploited by reducing the problem to a search for $k_1, ..., k_{L-1}$ satisfying

$$W / G_L^m = (G_1 / G_L)^{T_1} (G_2 / G_L)^{T_2} ... (G_{L-1} / G_L)^{T_{L-1}}$$

The native method needs time $O(m^{L-1})$. However, we get the final tally in our 1-out-of-L e-voting scheme as follows.

$$W = k_1 G_1 + ... + k_L G_L$$

Therefore, the final tally can be computed with $O(m)$. In table 3, we compare the computational complexity of our

scheme with that of [CGS97].

Table 2. Proof of validity of ballot

Prover P		Verifier V
$C_i = G^{Z_i} \bmod p_0$ *where* $Z_i \equiv y^{m_i} x_i^r \bmod N_2$		
	$t \in_R Z_{N_2}^*$ $\xleftarrow{t}$	
$T \equiv y^{-m_i} t^r \bmod N_2$, $\tilde{T} = G^T \bmod p_0$, $W = TZ_i \bmod N_2$		
	$\xrightarrow{\tilde{T},\ W}$	
		$G^W \stackrel{?}{=} C_i \tilde{T}$

3. Ballot-cancellation scheme based on 1-out-of-L e-voting

3.1. Our ballot-cancellation scheme based on 1-out-of-L e-voting

In this section, we introduce the ballot-cancellation scheme in 1-out-of-L e-voting. We use the extended homomorphic r-th residue encryption (See section 1.2), L possibilities for r-th residue encryption and the proof of validity of ballot (See table 2). Cancellation center, center1 and center2 progress as the ballot-cancellation of 1-out-of-L e-voting of section 2. That is, after the deadline is reached, center1 computes the total multiplied ballots (Z) and the multiplied of cancelled ballots (Z_b).

$$Z = y^M x^r \bmod N_2, \quad M = k_1 G_1 + ... + k_L G_L$$
$$Z_b = y^{M_b} x^r \bmod N_2, \quad M_b = k_1' G_1 + ... + k_L' G_L$$

Center 1 gets Z_v from the following equation.

$$Z_v = Z / Z_b$$

Center 2 can get the final valid ballot M_v.

$$Z_v = y^{M_v} x^r \bmod N_2, \quad M_v = k_1'' G_1 + ... + k_L'' G_L$$

, where

$$M_v = M - M_b = (k_1 G_1 + ... + k_L G_L) - (k_1' G_1 + ... + k_L' G_L)$$
$$= k_1'' G_1 + ... + k_L'' G_L.$$

Each $k_i'' \{i = 0,...,L\}$ is the number of obtained ballot.

3.2. Security

In this section, we analyze security of ballot-cancellation scheme of 1-out-of-L e-voting.

- **Privacy**

To achieve privacy, a few approaches have been proposed [Dip02].

Privacy 1. It is easy to see the vote, but it is impossible to trace it back to the voter.

Privacy 2. It is impossible or computationally infeasible to see the actual vote, but it is easy to see the identity of the voter.

Privacy 3. Both seeing, the actual vote and obtaining the identity of the voter is impossible or computationally infeasible.

Privacy of our ballot-cancellation scheme satisfies *privacy 2*. For the ballot-cancellation, anyone has to know the relation between a voter and his vote. In our e-voting scheme, cancellation center takes charge of that part.

But, he does not take part in the computation of vote and just check the right of casting the ballot of the absentee voter. When center 1 computes the ballot-cancellation, he does not know the voting content because the voting content is encrypted by center 2's public key. Also, center 2 just computed the final tally from the multiplied ballot. If center1 does not collude with center 2, it is guaranteed privacy.

- **Verifiability**

Everyone can verify the cancelled ballot through the bulletin board. Also, they can know whether the votes are cancelled or not exactly using commitment data C_i .

4. Conclusion

In this paper, we proposed first ballot-cancellation scheme for an absentee voter based on Yamaguchi *et al.*'s scheme. Yamaguchi *et al.* proposed the e-voting

Table 3. Comparison with the computation of the final tally

	The final tally	Computational Complexity
Our scheme	$W = k_1 G_1 + ... + k_L G_L$	$O(M)$
[CGS97]	$W / G_L^m = (G_1 / G_L)^{T_1} (G_2 / G_L)^{T_2} ... (G_{L-1} / G_L)^{T_{L-1}}$	$O(M^{L-1})$

system based on double encryption for privacy, universal verifiability, and robustness. We extended Yamaguchi *et al.*'s scheme to 1-out-of-L e-voting, and proposed 1-out-of-L e-voting system with the ballot-cancellation property.

For the 1-out-of-L e-voting system with the ballot-cancellation property, we proposed the extended homomorphic r-th residue encryption, *L* possibilities and the proof of validity of ballot for r-th residue encryption.

Acknowledgement

The first author 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).

Reference

[CC96] Canor,L.F., and Cytron,R.K., “ Design and Implementation of a Practical Security-Conscious Electronic Polling System, ” WUCS-96-02, Department of Computer Science, Washington University, St. Louis, Jan, 1996

[CF85] Cohen,J.D, Fischer,M.J.,``A robust and verifiable cryptographically secure elelction schme." In Proc.26th IEEE Symp. on Foundation of Computer.Science, pages 372-382, Portland, 1985.IEEE.

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

[Dip02] P.Diplomov¥'{a}, ``Electronic Voting Schemes." April, 2002.

[FOO92] Fujioka,A., Okamoto,T., Ohta,K., ``A Practical Secret Voting Scheme for Large Scale Elections." In Advances in Cryptology-AUSCRYPT '92, LNCS718, Springer-Verleg, Berlin, pp.244-251, 1993,

[HS00] Hirt,M , Sako,K., ``Efficient receipt-free voting based on homomorphic encryption." Eurocrypt 2000, LNCS1807, pp539-556, 2000.

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

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

[Sch99] Scheonmakers,B.,``A Simple Publicly Verifiable Secret Sharing Scheme and Its Application to Electronic Voting." Advances in Cryptology-CRYPTO, LNCS1666, pp148-164,1999.

[YKDKT03] Yamaguchi,H., Kitazawa,A., Doi,H., Kurosawa,K., Tsuji,S., ``An Electronic Voting Protocol Preserving Voter's Privacy" IEICE Trans. INF.&SYST., Vol.E86-D, No.9, September, 2003.