1-out-of-L Electronic Voting with Ballot-Cancellation Property Using Double Encryption*

Yong-Sork Her†, Kenji Imamoto†, and Kouichi Sakurai††

†Graduate School of Information Science and Electrical Engineering, Kyushu University, Fukuoka, 812-8581 Japan
††Faculty of Information Science and Electrical Engineering, Kyushu University, Fukuoka, 812-8581 Japan

Summary
In this paper, we present an electronic voting (namely e-voting) system based on cryptographic techniques. Recently, some countries have used e-voting systems using an electronic voting device instead of a voting sheet. These e-voting systems are the early stage which is not online voting. Many cryptographers have studied on-line e-voting systems based on cryptographic techniques. For a secure on-line e-voting system, it is required some requirements like privacy, unreusability, verifiability, receipt-freeness, and so on. In this paper, we point out that it can be happened a vote-selling and a vote-coercion in the conventional voting (i.e., the paper voting) by a cellular phone with camera and a mini digital camera. To prevent the vote-selling and a vote-coercion, a few receipt-free schemes have been proposed in the e-voting system area. The existing 1-out-of-L e-voting systems are based on ElGamal cryptosystem. We compare the computational complexity of the proposed 1-out-of-L e-voting system with that of the 1-out-of-L e-voting system based on ElGamal cryptosystem. Moreover, we extend the proposed 1-out-of-L e-voting system to ballot-cancellation property. The existing e-voting systems had been overlooked the ballot-cancellation property. There is the reason that the ballot is cancelled according to an election law. For our e-voting system with ballot-cancellation property, we extend the homomorphic property based on r-th residue encryption. The extended homomorphic property is used to cancel votes with guaranteeing anonymity and privacy. When the ballot is cancelled, the ballot-cancellation scheme should satisfy privacy and verifiability.

Key words:
Electronic voting, Privacy, Security, Ballot-cancellation, 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 [2,4,6,7,8,9] based on cryptography techniques have been proposed. However, most of the proposed e-voting schemes had overlooked a ballot-cancellation scheme. Many researchers think that there is no the reason to be cancelled the ballot in e-voting system.
However, there are some reasons that the ballot should be cancelled according to the e-voting systems or the election law. We introduce the reasons as follows.

Case1. Under the special condition which the right of casting the ballot is an Election Day, if absentee voters die or lose the right of casting the ballot before the Election Day, the ballots of the absentee voters should be cancelled.
Case2. It can be found a substitute vote or illegal vote by a voter.
Case3. When some voters can give up their vote during voting, a malicious election committee maybe cast votes instead of them.

Case1 can be happened by an election law of each country, and *Case2* and *Case3* can be happened by the defect of e-voting system. Actually, to prevent an illegal ballot and a substitute ballot like *Case2* and *Case3*, a voter should prove his voting (namely *proof of validity of the ballot*), and election committees should prove his computation (namely *proof of validity of encryption or decryption*).
However, if the illegal ballot or the substitute ballot is found in the existing e-voting systems, the e-voting systems will be stopped.
To prevent the problem of *Case3*, some e-voting systems [4,7] use threshold secret sharing schemes based on the collaboration of multi-party. However, the computation complexities of these e-voting systems are higher than that of other e-voting system which does not use the collaboration of multi-party [11].
Case1 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 into two; *Voting point* and *Election day*.
In case that the right of casting the ballot is an Election Day(*i.e.*, Japan's election law), the ballot-cancellation

Manuscript received January, 2006.
* A preliminary version of this paper was published as follows: Her, Y.S, Imamoto, K. and Sakurai, K. (2005) `E-voting System with Ballot-Cancellation Based on Double-Encryption', Pre-proceeding of the international Workshop on Information Security Applications 2005, pp.525--532.

scheme for the successful absentee e-voting is required (See table 1).

1.2 Conventional Voting Methods

1.2.1 Absentee voting method

Here, we introduce the conventional absentee voting and its ballot-cancellation scheme. A voter registers in the voter list as an absentee voter.

(i) The qualification of the absentee voter is different according to the election law.
(ii) Before an Election Day, the absentee voter receives a voting sheet and two envelopes for casting a ballot from the election committee. (In case that the right of casting the ballot is the voting point, the absentee voter receives only one envelope.)
(iii) After the absentee voter casts the ballot at a secret place such as a voting place, he inserts the ballot into the first envelope.
(iv) He inserts the enveloped ballots into the second envelop and signs the certification on the second envelope.
(v) A delivery man delivers the double enveloped ballot to the election committee.

In this case, we can consider 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.

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

1.2.2 Ballot-cancellation scheme

- In the 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 lose the right of casting the ballot, the election committee deletes his vote. Still, the election committee does not know his voting content.

In this ballot-cancellation scheme, a malicious election committee may see the voting content.
For the secure ballot-cancellation scheme, the following conditions must be carefully considered.
***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 the absentee voting for a perfect e-voting system.

1.2.3 Vote-coercion and Vote-selling

Here, we dispute on a receipt-freeness. Actually, the receipt-freeness was proposed only for the e-voting system. Since Benaloh and Tuinstra [1] first introduced the concept of receipt-freeness to prevent a vote-selling and a vote-coercion, some receipt-free schemes have been proposed just for the e-voting system. Voters should not prove to a third party how they voted. If the voter has a receipt on his vote, the vote-selling or the vote-coercion can be happened in the e-voting system. These attacks bring about a fatal mistake in the e-voting system.
In this section, we argue on the receipt-freeness of the conventional voting (*i.e.*, paper voting). In case of the conventional voting, the voter casts a ballot in a secret place as a voting booth with one voting-sheet, and inserts it into a voting box. Then, only the voting-sheet can become the receipt. Everyone trusts that the voter can not take the receipt on his voting. Even if the voter gets out of the voting place with his voting-sheet, the voting-sheet can not become the receipt because the voting-sheet becomes an invalid vote and a useless vote.
By development of electronic technique, we can get easily a mini digital camera and a cellular phone with camera. The voter is easily portable these devices, and he can enter to the voting booth with these devices. After he casts a ballot, he is able to photograph his ballot. The photographed picture can become the receipt. To prevent that kind of receipt in the conventional voting, an election committee must block carrying of these devices using a special detection at the voting place. We want to say 'it is required the receipt-freeness in the conventional voting, too.

1.3 Cryptographic Primitives

1.3.1 Homomorphic property

Cohen and Fischer [3] applied first the homomorphic functions to e-voting system. Recently, many e-voting systems [4,7,11] have been used the homomorphic property for achieving universal verifiability. A general definition of the notion is as follows [4]. 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 $c = c_1 \otimes ... \otimes c_m$ 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.

1.3.2 r-th residue encryption

We introduce r-th residue encryption, its homomorphism property, and the extended homomorphism property.

Secret key: two large prime numbers: p_T, q_T

Public key : $N_T (= p_T q_T), y_T$ (y_T is a random number)

Plaintext: v_i ($0 \le v_i \le r$)

Encryption : $Z_i = y_T^{v_i} x^r \bmod N_T$, (x is a random number)

[r : odd]	[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 $(e_1, e_2) = 2$

Decryption

mod p_T	mod q_T
$Z_i^{(p_T-1)/e_1} = (y_T^{v_i} x^r)^{(p_T-1)/e_1}$	$Z_i^{(q_T-1)/e_2} = (y_T^{v_i} x^r)^{(q_T-1)/e_2}$
$= (y_T^{(p_T-1)/e_1})^{v_i} (x^{r/e_1})^{(p_T-1)}$	$= (y_T^{(q_T-1)/e_2})^{v_i} (x^{r/e_2})^{(q_T-1)}$
$= (y_T^{(p_T-1)/e_1})^{v_i}$	$= (y_T^{(q_T-1)/e_2})^{v_i}$

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

$$(y_T^{(p_T-1)/e_1})^i \bmod p_T \quad \text{and} \quad (y_T^{(q_T-1)/e_2})^i \bmod q_T \qquad (1)$$

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,

$$\begin{aligned} E(m+n) &= y^{m+n} x^r \bmod N, \\ E(m)E(n) &= (y^m x^r \bmod N)(y^n x^r \bmod N) \\ &= y^{m+n} x^r \bmod N \end{aligned} \qquad (2)$$

Therefore, $E(m+n) = E(m)E(n)x^r \bmod N$ (3)

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

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

$$E(m-n) = \{E(m)/E(n)\}x^r \bmod N \qquad (4)$$

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,

$$\begin{aligned} E(m-n) &= y^{m-n} x^r \bmod N, \\ E(m)/E(n) &= (y^m x^r \bmod N)/(y^n x^r \bmod N) \\ &= y^{m-n} x^r \bmod N \end{aligned} \qquad (5)$$

Therefore,

$$E(m-n) = \{E(m)/E(n)\}x^r \bmod N \qquad (6)$$

1.4 Our Contribution

In this paper, we first propose the ballot-cancellation scheme for the e-voting system. As mentioned in section 1.1, there are a few reasons that the ballot should be cancelled. We concentrate on the ballot-cancellation by election law (*Case1*).

When the ballot is cancelled, privacy and verifiability should be guaranteed. 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.*[4] proposed a very efficient multi-authority election schemes which guarantee privacy, robustness, and universal verifiability in [4].

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 [11].

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 both RSA cryptosystem and r-residue cryptosystem with homomorphic property. We use freely double encryption scheme of Yamaguchi *et al.*'s e-voting system. Our goal is to design the efficient 1-out-of-L e-voting system with the ballot-cancellation property.

First, we check Cramer *et al.*' s and Yamaguchi *et al.*'s e-voting schemes are able to support the ballot-cancellation property.

In conclusion, if the multi-party knows the relation between the ballot and corresponding to shared decryption key, Cramer *et al.* 's scheme has the ballot-cancellation property. However, Yamaguchi *et al.*'s scheme does not satisfy the ballot-cancellation property as it is. We modify this e-voting system to be satisfied the ballot-cancellation property. For enhancing Yamaguchi *et al.*'s scheme to

support the ballot-cancellation, we extend the homomorphism property of r-th residue encryption. The existed homomorphism property of r-th residue encryption enables just to add up ballots.
Actually, we need the subtraction to cancel the ballots. We propose the extended homomorphism property of r-th residue encryption.

Second, 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 that his vote is one of them.
For this proof, we propose L possibilities for r-th residue encryption. The voter can prove that his vote is one of L possibilities without opening his vote through this proof method.
Moreover, we propose the proof of validity of ballots 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 computational 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 $LO(M)$, 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.

Finally, 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.

In section 2, we check whether yes-no voting of Cramer *et al.*'s scheme and Yamaguchi *et al.*'s scheme can be applied to ballot-cancellation property or not. We extend Yamaguchi *et al.*'s yes-no voting system to 1-out-of-L e-voting system in section 3. We apply the proposed 1-out-of L e-voting to ballot-cancellation property. In section 5, we evaluate the performance of the computational complexities in our scheme and Cramer *et al.*'s scheme.

2. Ballot-cancellation in 1-out-of-2 e-voting system

In this section, we review two e-voting systems: one is Cramer *et al.*'s scheme [4] and the other is Yamaguchi *et al.*'s scheme [11]. As mentioned in section 1.4, it is known that the former scheme is very efficient and satisfies all requirements except for the receipt-freeness. The latter system used double encryption based on r-th residue encryption and RSA cryptosystem. This system has been proposed to overcome the disadvantage of the e-voting system based on multi-party. That is, the e-voting system based on multi-party has much computational complexity.
In this section, we check whether two e-voting systems can be applied to the ballot-cancellation property or not, and extend these e-voting systems to the ballot-cancellation property.

2.1 Cramer *et al.*'s Scheme

2.1.1 Overview of Cramer *et al.* 's scheme

We introduce Cramer *et al.*'s scheme [4] shortly [5]. Their e-voting system consists of multi-party.

Summary: voters publicly send their votes encrypted by ElGamal cryptosystem. The decryption key is shared between the multi-party. After the voting time is over, votes are multiplied and multi-party decrypts the sum of votes as the result of the election.
Initialization phase: the multi-party shares the decryption key s. Public key (p, g, h), commitments of the shares $h_j = g^{s_j}$ and a fixed generator G of G_q are published.
Voting phase: the voter V_i chooses his vote; $m_0 = G$ for yes-vote, $m_1 = 1/G$ for no-vote. The encrypted vote is $(x, y) = (g^k, h^k m_j)$, where k is random and $j \in 0,1$. Voters add a proof that his vote is correct form. For this, a non-interactive proof is suitable (See [4] for details).
Counting phase: the product of all valid encrypted votes $(X, Y) = (\Pi_i x_i, \Pi_i y_i)$ is formed. The multi-party jointly executes the decryption protocol and gets the value of $W = Y / X^s$. We can get $W = G^T$, where T is a different between the number of yes-votes and no-votes; $-M \le T \le M$; M is a number of eligible voters. Hence, $T = \log_G W$, which is in general hard to compute. The value of the T can be determined using $O(M)$ modular multiplications by interactively computing $G^{-M}, G^{-M+1}, \Lambda$ until W is found.

2.1.2 Apply to ballot-cancellation

In order to apply Cramer *et al.*'s scheme to the ballot-cancellation property, it is required a special center, namely Cancellation Center (CC). The cancellation center just checks the right of casting the ballot. Both initialization phase and voting phase are the same as those

in the original scheme. We add checking phase to Cramer *et al.*'s scheme.

Checking Phase: the cancellation center checks the right of casting the ballot of the voter. The checking result is marked in the bulletin board.

Counting Phase: multi-party checks the marked result by the cancellation center. They omit shared decryption keys of the marked ballots. Then, it is required the condition that the multi-party should know the relation between the ballot and corresponding to shared decryption key. The product of all valid encrypted votes $(X,Y)=(\Pi_i x_i, \Pi_i y_i)$ except the cancelled ballot is formed. They compute the final tally like Cramer *et al.*'s scheme.

Table 2: Notations

	For signature	
	Secret key	Public key
Voter	$d_{v_i}, p_{v_i}, q_{v_i}$	$e_{v_i}, N_{v_i}(=p_{v_i}q_{v_i})$
Center1	$d_{C_1}, p_{C_1}, q_{C_1}$	$e_{C_1}, N_{C_1}(=p_{C_1}q_{C_1})$
Center2	$d_{C_2}, p_{C_2}, q_{C_2}$	$e_{C_2}, N_{C_2}(=p_{C_2}q_{C_2})$
	For encryption / decryption	
	Secret key	Public key
Voter	$d'_{v_i}, p'_{v_i}, q'_{v_i}$	$e'_{v_i}, N'_{v_i}(=p'_{v_i}q'_{v_i})$
Center1	d_1, p_1, q_1	$e_1, N_1(=p_1q_1)$
Center2	p_2, q_2	$r, y, N_2(=p_2q_2)(N_1>N_2)$

2.1.3 Analysis

We showed Cramer *et al.*'s scheme is able to have the ballot-cancellation property. In their scheme, the proof of validity of the ballot on each ballot is proved independently. That is, i vote has not an influence on $i+1$ vote in the proof of validity of the ballot. Therefore, the ballots which should be cancelled exclude from the computation of final tally. When the multi-party omits the shared decryption key of cancelled ballot, the multi-party should prove the validity of the cancelled decryption key. In this paper, we remain this problem as an open problem.

2.2 Yamaguchi *et al.*'s Scheme

In this section, we introduce Yamaguchi *et al.*'s scheme based on double encryption. We omit proofs of validity of the ballot, the procedures for encryption and decryption in Yamaguchi *et al.*'s scheme. Table 2 shows notations for Yamaguchi *et al.*'s scheme and our 1-out-of-L e-voting scheme of section 3. Table 3 is the bulletin board of Yamaguchi *et al.*'s scheme.

2.2.1 Overview of Yamaguchi *et al.* 's scheme

Phase 1. By Voters

Step 1-1. A voter V_i selects his/her ballot $m_i(\in 0,1)$.

Step 1-2. He/She encrypts m_i with center2's public key y, N_2.

$$Z_i = y^{m_i} x_i^r \bmod N_2 \quad (7)$$

, where $x_i \in_R Z^*_{N_2}$

Step 1-3. He/She encrypts Z_i with center1's public keys e_1, N_1.

$$E_i \equiv Z_i^{e_1} \bmod N_1 \quad (8)$$

Step 1-4. He/She generates the commitment data C_i for Z_i.

$$C_i \equiv G^{Z_i} \bmod p_0 \quad (9)$$

Step 1-5. He/She constructs the ballot: compute a hashed value $H_i = hash(E_i, C_i, MSG_{v_i})$ and its signature $(H_i)^{d_{v_i}} \bmod N_{v_i}$.

The ballot is $(ID_{v_i}, E_i, C_i, MSG_{v_i}, (H_{v_i})^{d_{v_i}} \bmod N_{v_i})$, where ID_{v_i} is voter ID.

Step 1-6. He/She cast the ballot to the bulletin board (Area A).

Phase 2. By Center1

Step 2-1. Read on the ballot on the bulletin board and retrieve the corresponding voter's public key e_{v_i} and check the signature of the voter, and check the eligibility of the voter, and check if the casting of ballot is first time or not. Add the accepted mark on the bulletin board (Area B).

Step 2-2. Decrypt the accepted ballot with center1's secret key, and obtain Z_i.

$$Z_i \equiv E_i^{d_1} \bmod N_1$$

,compute $G^{Z_i} \bmod p_0$ and compare $G^{Z_i} \bmod p_0$ with C_i.

Step 2-3. Let the multiplied ballot in the previous steps be Z_j, and the current ballot be Z_i. Multiply Z_j by Z_i and compute the commitment data.

$$C_{(j,i)} = G^{Z_j Z_i} \bmod p_0 \quad (10)$$

and cast $C_{(j,i)}$ to the bulletin board(Area **C**) accompanied by Proof 1 $(C_j, C_i, C_{(j,i)})$, where $C_j \equiv G^{Z_j} \bmod p_0$ and $C_i = G^{Z_i} \bmod p_0$ for proving that the multiplications are correctly executed (Area **E**).

Step 2-4. When the deadline is reached, the multiplied ballot is $Z_a = \Pi_{i=1}^{l} Z_i \bmod N_2$, where l is the total number of ballots.

Phase 3. By Center2

Step 3-1. Read marked D of the bulletin board and check the signature of center1. Verify the protocol $(C_j, C_i, C_{(j,i)})$ and $(C_n, C_m, C_{(n,m)})$, and if all of multiplication is accepted, then center2 adds the accepted mark on the bulletin board(Area E).

Step 3-2. Decrypt Z with center2's secret key p_2 and q_2 and obtain the final tally M.

$Z_v = \Pi_{i=1}^{v} Z_i = y^M X^r \bmod N_2$, $M = \Sigma_{i=!}^{v} m_i$, $X = \Pi_{i=1}^{v} x_i$

, where v is the number of valid voters.

Step 3-3. Center2 computes a hashed value $H_{C_2} = hash(Z_v, MSG_{C_2})$ and its signature $(H_{C_2})^{d_{C_2}} \bmod N_{C_2}$.

Step 3-4. Center2 sends the following data to the bulletin board (Area F).

Step 3-5. Center1 reads the data from the bulletin board (Area F), checks the signature of center2, and verifies the proof of validity. The result is marked the bulletin board (Area G).

2.2.2 Apply to ballot-cancellation

In order to apply Yamaguchi *et al.*'s scheme to the ballot-cancellation scheme, it is required Cancellation–center and the extended homomorphism property of r-th residue encryption (See section 1.3.1).

In this scheme, center1 decrypts the double encrypted ballot and gets the encrypted ballot Z_i (See step 2-2).

But, center1 does not cast the encrypted ballot Z_i until the deadline reached because center2 can get always the vote from the encrypted ballot Z_i during voting. So, Yamaguchi *et al.* used the commitment data C_i. Center1 casts the commitment data C_i instead of the encrypted ballot Z_i to the bulletin board. Also, center1 computes the multiplied commitment data $C_{(j,i)}$ (See step 2-3). That is, i vote has an influence on $i+1$ vote in the proof of validity of the ballot. This point is different with Cramer *et al.*'s scheme. To be cancelled the ballot, we extend the homomorphism property based on r-th residue encryption (See section 1.3.2). The ballot-cancellation scheme based on Yamaguchi *et al.*'s scheme is as follows.

1-1. Cancellation–center checks the right of casting the ballot, and the checking result is marked on the bulletin board (Area **D'**) of table 4.

1-2. After the deadline is reached, center1 computes the multiplied ballot Z on all the ballots and the multiplied commitment data $C(=G^Z \bmod p_0)$, and casts C to the bulletin board.

1-3. (For the ballot-cancellation) Let the multiplied cancellation- ballot in the previous step be Z_n, and the current cancellation- ballot be Z_m. Multiply Z_n by Z_m, compute the commitment data $C_{(n,m)} = G^{Z_n Z_m} \bmod p_0$ and cast $C_{(n,m)}$ to the bulletin board (Area **C'**). The proving that the multiplications $(C_n, C_m, C_{(n,m)})$ are correctly executed uses that of Yamaguchi *et al.*'s scheme.

1-4. Center1 computes the multiplied commitment data $C_b(=G^{Z_b} \bmod p_0)$ from $(C_n, C_m, C_{(n,m)})$, and gets the multiplied ballot Z_b on all cancelled ballots.

1-5. Center1 computes the multiplied ballot Z_v on all

Table 3: Bulletin Board of Yamaguchi *et al.*'s scheme

Ballots		Commitment data for multiplication	Final tally in encrypted form		Finally tally	
Voter's own designated section **A**	Accepted mark section **B**	Center1's own designated section **C**	Center1's own designated section **D**	Valid mark section **E**	Center2's own designated section **F**	Valid mark section **G**

Table 4: Bulletin Board for our ballot-cancellation scheme

Ballots		Commitment data for multiplication	Ballot-cancellation or not	Final tally in encrypted form		Finally tally	
Voter's own designated section **A'**	Accepted mark section **B'**	Center1's own designated section **C'**	CC's own designated section **D'**	Center1's own designated section **E'**	Valid mark section **F'**	Center2's own designated section **G'**	Valid mark section **H'**

valid ballots using the extended homomorphism property based on r-th residue encryption and the multiplied commitment data $C_v (= G^{Z_v} \bmod p_0)$, and casts C_v to the bulletin board.

$$Z_v = Z / Z_b \quad (11)$$

1-6. Center1 casts Z_v to the bulletin board, and center2 computes the final tally from Z_v as the original scheme.

3. Our 1-out-of-L E-voting System

3.1 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 [4,10] 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 [11].

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 [10], it uses the following proof.

- The voter V_i casts his vote v_i from the set

Table 5: Our 1-out-of-L e-voting system

Phase 1. By Voters (V)	
1-1. $Voting - list_{i=1}^{L} G_i$	L Generator ($0 \le G_1, \Lambda, G_L \le r$)
1-2. $V \leftarrow m_i (i = 1, \Lambda, L)$ from the set G_1, Λ, G_L	Voting
1-3. $Z_i = y^{m_i} x_i^r \bmod N_2$ (by C_2's public key y, N_2)	The first encryption
1-4. $E_i \equiv Z_i^{e_1} \bmod N_1$ (by C_1's public key e_1, N_1)	Double encryption
1-5. $C_i \equiv G^{Z_i} \bmod p_0$	Generate a commitment data
1-6. $V \rightarrow Verifier$ (Proof of validity on the voting content)	L possibilities for r-th residue encryption
1-7. $(H_i)^{d_{v_i}} \bmod N_{v_i} \leftarrow H_i = hash(E_i, C_i, MSG_{v_i})$	A voter's signature
1-8. $(ID_{v_i}, E_i, C_i, MSG_{v_i})^{d_{v_i}} \bmod N_{v_i} \rightarrow BB$	Ballot casting
Phase 2. By Center1 (C_1)	
2-1. $Z_i \equiv E_i^{d_1} \bmod N_1$	Decryption
2-2. Compute $G^{Z_i} \bmod p_0$ and compare $G^{Z_i} \bmod p_0$ with C_i of the voter	Proof of validity of encrypted vote
2-3. $C_{(j,i)} = G^{Z_j Z_i} \bmod p_0 \rightarrow BB$	Multiplication of the commitment data (Z_j : multiplication of the previous step, Z_i : current commitment data)
2-4. $(C_j, C_i, C_{(j,i)}) \rightarrow BB$	Commitment data
2-5. $(ID_{C_1}, Z, MSG_{C_1}, H_{v_i})^{d_{C_1}} \bmod N_{C_1} \rightarrow BB$	Casting of multiplied vote
2-6. $Z = \Pi_{i=1}^{l} Z_i = y^M X^r \bmod N_2$, where l is the total number of ballots	Multiplication of encrypted votes
Phase 3. By Center2 (C_2)	
3-1. Verify $(C_j, C_i, C_{(j,i)})$	Checking of Center1's signature
3-2. $Z = \Pi_{i=1}^{l} Z_i = y^M X^r \bmod N_2$, $M = k_1 G_1 + k_2 G_2 + \Lambda + k_L G_L$, $X = \Pi_{i=1}^{l} x_i$	Decryption from encrypted voting content
3-3. $M = k_1 G_1 + k_2 G_2 + \Lambda + k_L G_L$, where $k_i (i = 1, \Lambda, L)$ is each number of gained ballot	Final tally casting (See section 3.3)

$\{M^0, M^1, ..., M^{L-1}\}$, 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

$$\log_G(GC_0) = \log_g U_i \vee \log_G(G^M C_0) = \log_g U_i ... \vee \log_G(G^{M^{L-1}} C_0) = \log_g U_i \quad (12)$$

, 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 6 shows the proof of validity of the ballot for 1-out-of-L e-voting based on double-encryption.

3.2 Our 1-out-of-L E-voting

Table 5 shows our 1-out-of-L e-voting scheme.

3.3 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 [4].

$$W = G_1^{k_1} G_2^{k_2} ... G_L^{k_L} \quad (13)$$

For the final tally, we should compute each $k_i (i = 1, ..., L)$ from W as follows [5].

Table 6: Proof of validity of ballot

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

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

$$W / G_L^m = (G_1 / G_L)^{T_1} (G_2 / G_L)^{T_2} ... (G_{L-1} / G_L)^{T_{L-1}} \quad (14)$$

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.

$$W = k_1 G_1 + ... + k_L G_L \quad (15)$$

Therefore, the final tally can be computed with $O(M)$.

Table 7: Comparison with the computation of the final tally

	The final tally
Our Scheme	$W = k_1 G_1 + \Lambda + k_L G_L$
[4]	$W / G_L^m = (G_1 / G_L)^{T_1} \Lambda\ (G_{L-1} / G_L)^{T_{L-1}}$

4. Ballot-cancellation Scheme Based on 1-out-of-L E-voting

4.1 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 1.3.2), *L* possibilities for r-th residue encryption and the proof of validity of ballot (See table 6). 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).

$$Z = y^{M} x^{r} \bmod N_2, \quad M = k_1 G_1 + \Lambda + k_L G_L$$
$$Z_b = y^{M_b} x^{r} \bmod N_2, \quad M_b = k_1' G_1 + \Lambda + k_L' G_L \tag{16}$$

Center1 gets Z_v from the following equation.

$$Z_v = Z / Z_b$$

Center2 can get the final valid ballot M_v.

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

, where

$$M_v = M - M_b = (k_1 G_1 + \Lambda + k_L G_L) - (k_1' G_1 + \Lambda + k_L' G_L) = k_1'' G_1 + \Lambda + k_L'' G_L. \tag{17}$$

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

4.2 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 [5].

Privacy1. It is easy to see the vote, but it is impossible to trace it back to the voter.

Privacy2. It is impossible or computationally infeasible to see the actual vote, but it is easy to see the identity of the voter.

Privacy3. 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 center1 computes the ballot-cancellation, he does not know the voting content because the voting content is encrypted by center2's public key. Also, center2 just computed the final tally from the multiplied ballot. If center1 does not collude with center2, 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.

5. Comparison of Computational Complexity

In this section, we compare the computational complexity of our scheme with that of the scheme in [4](See table 8). Cramer *et al.* pointed out that decryption in an e-voting system based on r-th residue cryptosystem is too slow for a large-scale election [4]. However, Yamaguchi *et al.* [11] showed that the r-th residue cryptosystem can be applied effectively for large-scale elections using the Shanks'baby-step giant-step algorithm (See [11] for details). In table 8, l and M mean the number of eligible votes and candidates respectively. In case of our scheme based on r-th residue encryption, we assume that the prime q is larger than twice the number of voters l as the scheme of [4]. Cramer *et al.* assumes that l is less $q/2$ for any reasonable security parameter k. When M is 5 or 10, the measurement results of computational complexity are showed in fig.1 and fig.2

Table 8: Computational complexities of our scheme and [4]

	Our scheme	[4]
Encryption	$O(l)$	$O(l)$
Decryption	$O(l)$ $MO(l) + O(l^{1/2})$	$O(l^{M-1})$
Proofs	$O(l)$	$O(l+M) : (l > m)$
Total	$(M+3)O(l) + O(l^{1/2})$	$2O(l) + O(l^{M-1})$

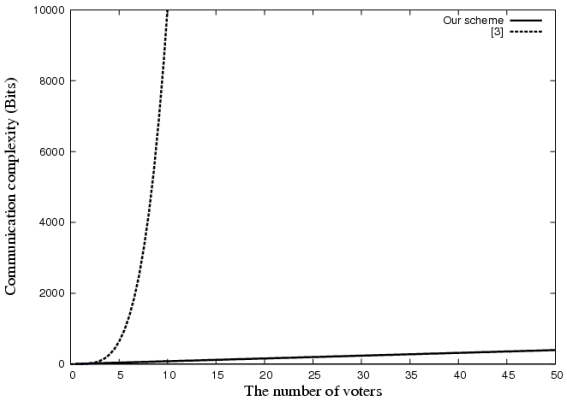


Fig. 1 Computational complexity : M=5.

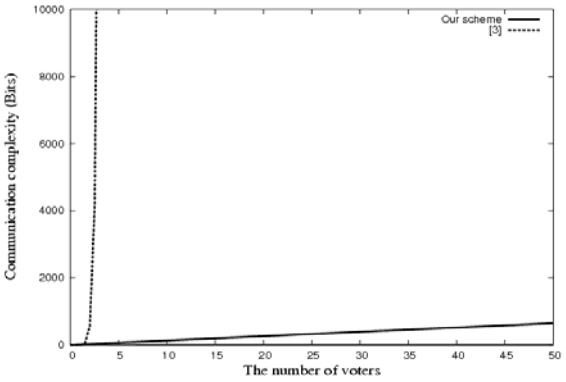


Fig. 2 Computational complexity : M=10.

6. Conclusion

In this paper, we first proposed ballot-cancellation scheme for an absentee voter based on Yamaguchi *et al*.'s scheme. Yamaguchi *et al*. proposed the e-voting system based on double encryption for privacy, universal verifiability and robustness. We applied Yamaguchi *et al*.'s scheme to the ballot-cancellation scheme.

Moreover, 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.

References

[1] Benaloh,J.C., and Tuinstra,D. ``Receipt-free secret-vote elections.", Prof.26th ACM Symposium on the Theory of Computing, pp.544-553, 1994

[2] 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

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

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

[5] P.Diplomová, ``Electronic Voting Schemes." April, 2002.

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

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

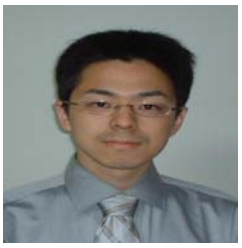
[8] Park,C., Itoh,K., Kurosawa,K., ``Efficient Anonymous Channel and All / Nothing Election Scheme." EUROCRYPT '93, LNCS765, Springer-Verlag, Berlin Heidelberg 1994.

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

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

[11] 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.

Yong-Sork HER received his master degree from the Graduate school of Information and Communication, Daegu University, Korea in 1998. He is currently working toward the Ph.D degree in the Graduate School of Information Science and Electrical Engineering, Kyushu University since 2002. His research interests include electronic voting, electronic auction, and hash function based on cryptographic techniques.



Kenji Imamoto received his master degree from the Graduate School of Information Science and Electrical Engineering, Kyushu University in 2004. He is currently working toward the Ph.D degree in the Graduate School of Information Science and Electrical Engineering, Kyushu University. His current research interests are in certified e-mail and authenticated key exchange. He is a member of the Institute of Electronics, Information and Communication Engineers.

Kouichi Sakurai received his Dr. degree in engineering from Faculty of Engineering, Kyushu University in 1993. Since 1994 he has been working for Department of Computer Science of Kyushu University as an associate professor, and now he is a full professor from 2002. His current research interests are in cryptography and information security. Dr. Sakurai is a member of the Information Processing Society of Japan, the Mathematical Society of Japan, ACM and the International Association for Cryptology Research.