E-voting System with Ballot-Cancellation Based on Double-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：Preproc. of International Workshop on Information Security Applications 2005. I, pp.525-532, 2005-08. MIC, KIISC
バージョン：
権利関係：

E-voting System with Ballot-Cancellation Based on Double-Encryption

Yong-Sork Her[1], Kenji Imamoto[1], and Kouichi Sakurai[2]

[1] Graduate School of Information Science and Electrical Engineering, Kyushu University, 6-10-1, Hakozaki, Higashi-ku, Fukuoka, 812–8581 Japan
{ysher, imamoto}@itslab.csce.kyushu-u.ac.jp
[2] Faculty of Information Science and Electrical Engineering, Kyushu University, 6-10-1, Hakozaki, Higashi-ku, Fukuoka, 812–8581 Japan
sakurai@csce.kyushu-u.ac.jp

Abstract. In this paper, we first propose an e-voting system with a ballot-cancellation property. The existing voting systems had overlooked about the ballot-cancellation property. There is the reason that the ballot is cancelled according to an election law. 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 cast ballots should be cancelled according to the election law. 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 analyze whether these e-voting schemes can be applied to the ballot-cancellation scheme or not. Second, we propose a 1-out-of-L e-voting based on Yamaguchi *et al.*'s scheme. Finally, we extend this 1-out-of-L e-voting to the ballot-cancellation scheme.

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 such as manpower, time, and money. To overcome these problems, many e-voting systems [4, 2, 5, 6] based on cryptography techniques have been proposed. However, most of proposed e-voting systems had overlooked about a ballot-cancellation property. Many researchers think that there are not reasons to be cancelled the ballot in e-voting systems. We introduce the reasons as follows.
Case 1. Under the special condition which the right of casting the ballot is election day, if an absentee voters die or lost the right of casting the ballot before election day, then the ballots of the absentee voters should be cancelled.
Case 2. It can be found a substitute vote or an illegal vote by a voter.
Case 3. It can be found a substitute vote by a malicious election committee.

Case 2 and *Case 3* can be happened by the defect of the e-voting system. We concentrate on *Case 1*. *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*. In the case of the former (*i.e.*,Japan's election law), it is required the ballot-cancellation scheme for the successful e-voting (See table 1). 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 cast ballots should be cancelled according to the election law. For the secure ballot-cancellation property, we need the following conditions .
- *Privacy* When the ballot is cancelled, everyone should not know the voting content.
- *Verifiability* Everyone can check whether or not the ballot is cancelled correctly.

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 Cryptographic preliminaries

1.2.1 Extended homomorphism property based on r-th residue encryption

We extend the homomorphism property of r-th residue encryption in order to apply to ballot-cancellation e-voting. 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.

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

Then,

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

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

1.2.2 L possibilities for discrete logarithm and for r-th residue encryption

■ **L possibilities for discrete logarithm**

In a 1-out-of-L e-voting system, a voter 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 [7], 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 $\sum v_i$ using homomorphic property.

■ **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 $0 \leq G_1, ..., G_L < r$. $\{G_1, ..., G_L\}$ 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.

Table 2. Proof of validity of ballot

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

1.3 Our contribution

First, we check whether Cramer *et al.*' s scheme and Yamaguchi*et al.*' scheme can be applied to the ballot-cancellation property or not. In conclusion, Cramer *et al.* 's scheme has the ballot-cancellation property. The proof of validity of the ballot on each ballot is proved independently. That is, a previous vote has not an influence on the next vote in the proof of validity of the ballot. Therefore, the ballots which should be cancelled exclude from the computation of final tally. However, Yamaguchi *et al.*'scheme does not satisfy the ballot-cancellation property as it is. In their proof of validity of the ballot, a previous vote has an influence on the next vote. Therefore, we modify this e-voting system to

be satisfied the ballot-cancellation property. To modify this e-voting system, we extend the homomorphism property of r-th residue encryption. The existing 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 his vote is one of them. For this proof, we propose L possibilities for r-th residue encryption. Moreover, we propose the proof of validity of ballot for our 1-out-of-L e-voting based on r-th residue encryption. 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, 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. However, 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.

2 Apply Cramer *et al.*'s scheme and Yamaguchi *et al.*'s scheme to Ballot-cancellation (1-out-of-2 e-voting system)

In this section, we concentrate on two e-voting systems (Please refer to [2] and [8] for the detaild contents). One is Cramer *et al.*'s scheme [2] and the other is Yamaguchi *et al.*'s scheme [8]. It is known that the former scheme is very efficient and satisfies all requirements except for the receipt-freeness. The latter used double encryption using r-th residue encryption and RSA cryptosystem. In this section, we check whether two e-voting systems can be applied to the ballot-cancellation scheme or not, and extend these e-voting systems to the ballot-cancellation property. 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, they should prove the validity of cancelled decryption key. In this paper, we remain this problem as open problem. In order to apply Yamaguchi *et al.*'s scheme to the ballot-cancellation scheme, we need the cancellation-center and the extended homomorphism property of r-th residue encryption. In this scheme, center1 decrypts the double encrypted ballot and gets the encrypted ballot Z_i (See table 3). However, 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 cast 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 table 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.

3 1-out-of-L e-voting system based on Yamaguchi *et al.* [8]

3.1 Model of our 1-out-of-L e-voting

Model
Our e-voting system consists of three-center; *Center1, Center2* and *Cancellation Center*.
- Voter (V) : A voter is divided to two voters; a (general) voter and an absentee voter. We consider on a voter including an absentee voter. If the voter dies or losts the right of casting the ballot before Election Day, the voter 's ballot will be cancelled, keeping privacy and verifiability.
- Center1(C_1): The role of center1 is similar to that of [8]. She has the secret key of the RSA cryptosystem and takes the double-encrypted ballots and invalid ballots from the bulletin board. He computes the multiplied and encrypted valid ballots from them using the extended homomorphism r-th residue encryption. Then, he does not know the voting content because he can not decrypt the encrypted ballot.
- Center2(C_2): The role of center2 is similar to that of [8], too. He gets the multiplied and encrypted valid ballots from the bulletin board, and computes the final tally using his secret key.
- Cancellation-Center (CC) : After the voting time is over, cancellation-center (CC) checks the result whether the ballot is cancelled or not on the bulletin board. He should know the relation between the voter and the encrypted ballot. CC does not participate in a vote calculation.
- Bulletin Board(BB): In the bulletin board, everyone can see whether a voter votes or not. However, they can not erase and modify voting contents. Keeping privacy of absentee voter, we can know only the fact whether the absentee voter ' s ballot is valid vote or not.

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

Table 3 shows our 1-out-of-L e-voting system.

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 [2].

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

Table 3. Our 1-out-of-L e-voting system

Phase 1. By Voter (V)	
1-1. $Voting - list_{i=1}^{L} G_i$	L Generator $(0 \leq G_1, ..., G_L \leq r)$
1-2. $V \leftarrow m_i (i = 1, ..., L)$ from the set $G_1, ..., G_L$	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 Center 1 (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. $Z = \prod_{i=1}^{l} Z_i = y^M X^r \bmod N_2$, where l is the total number of ballots	Multiplication of encrypted votes
Phase 3. By Center 2 (C_2)	
3-1. Verify $(C_j, C_i, C_{(j,i)})$	Checking of center 1's signature
3-2. $Z = \prod_{i=1}^{l} Z_i = y^M X^r \bmod N_2$, $M = k_1 G_1 + k_2 G_2 + ... + k_L G_L$, $X = \prod_{i=1}^{l} x_i$	Decryption from encrypted voting content
3-3. $M = k_1 G_1 + k_2 G_2 + ... + k_L G_L$, where k_i $(i = 1, ..., L)$ is each number of gained ballot	Final tally casting (See section 3.3)

For the final tally, we should compute each k_i from W as follows [3].
Note that the condition $\sum_{i=1}^{L} k_i = m, m \leq M$ (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.

$$W = k_1 G_1 + k_2 G_2 + ... + k_L G_L$$

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

Table 4. Comparison with the computation of the final tally

	The final tally	Computational Complexity
Our Scheme	$W = k_i G_1 + k_2 G_2 + ... + k_L G_L$	$O(M)$
[2]	$W/G_L^m = (G_1/G_L)^{T_1} (G_2/G_L)^{T_2} ... (G_{L-1}/G_L)^{T_{L-1}}$	$O(M^{L-1})$

4 Ballot-cancellation scheme based on our 1-out-of-L e-voting

4.1 Our ballot-cancellation scheme

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 section 1.2 and table 2). Center1 and center2 progress as table 3, and cancellation-center checks only the right of casting the ballot of voters. That is, after the deadline is reached, center1 computes the total multiplied ballots (Z) and the multiplied of cancelled ballots (Z_b).

$$Z = y^M X^r \bmod N_2,\ M = k_1 G_1 + ... + k_L G_L$$
$$Z_b = y^{M_b} X^r \bmod N_2,\ M_b = k'_1 G_1 + ... + k'_L G_L$$

Center 1 gets Z_v from the following equation.

$$Z_v = Z/Z_b$$

Center 2 can get the final valid ballot M_v.

$$Z_v = y^{M_v} X^r \bmod N_2,\ M_v = k''_1 G_1 + ... + k''_L G_L$$

, 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.

4.2 Security

In this section, we analyze security of ballot-cancellation scheme of 1-out-of-L e-voting. The requirements for a secure 1-out-of-L e-voting keep up with those of Yamaguchi*et al.*

Privacy Our ballot-cancellation scheme satisfies the following privacy condition. To achieve privacy, a few approaches have been proposed [3].

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

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. However, 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 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 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.

Acknowledgement
The first author supported by the Grant-in-Aid for Creative Scientific Re-search No.14GS0218 (Research on System LSI Design Methodology for Social Infrastructure) of the Ministry of Education, Science and Culture (MEXT), and by the 21st Century COE Program 'Reconstruction of Social Infrastructure Related to Information Science and Electrical Engineering '. The authors would like to thank Dr.Wonil Lee and anonymous referees who provided useful comments.

References

1. 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.
2. Cramer,R., Gennaro,R., Schoenmakers,B., "A secure and optimally efficient multi-authority election scheme." European Transactions on Telecommunication, 8:481-489, Eurocrypt 1997.
3. P.Diplomová, "Electronic Voting Schemes." Master thesis, April, 2002. http://people.ksp.sk/ zuzka/elevote.pdf
4. 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.
5. Hirt,M , Sako,K., "Efficient receipt-free voting based on homomorphic encryption." Eurocrypt 2000, LNCS1807, pp539-556, 2000.
6. Sako,K., Kilian,J., "Receipt -Free Mix-Type Voting Scheme." EUROCRYPT '95, LNCS921, pp393-403, Springer-Verlag, Berlin Heidelberg 1995.
7. Scheonmakers,B. "A Simple Publicly Verifiable Secret Sharing Scheme and Its Application to Electronic Voting." Advances in Cryptology-CRYPTO, LNCS1666, pp148-164,1999.
8. 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.