社団法人　情報処理学会　研究報告
IPSJ SIG Technical Report

2004－ＣＳＥＣ－26　(50)
2004／7／21

普遍再暗号化 Mix-net により無証拠性および全体検証性を実現した電子投票システム

許　容碩† 　今本　健二† 　櫻井　幸一‡

†九州大学大学院システム情報科学府
‡九州大学大学院システム情報科学研究院　〒812-8581 福岡市東区箱崎 6-10-1
E-mail: †{ysher, imamoto}@itslab.csce.kyushu-u.ac.jp, ‡sakurai@csce.kyushu-u.ac.jp

あらまし　Sako と Killian は無証拠性と全体検証性を満足する Mix-net 電子投票システムを提案した。それに対し、Michels と Horster は、Sako らの電子投票システムにおけるプライバシと頑健性の問題を指摘した。本論文では、Golle らにより提案された普遍再暗号化を用いた Mixnet を導入することにより、プライバシと頑健性、および無証拠性や全体検証性を同時に満たし、効率的な計算が可能な電子投票システムを提案する。また、普遍再暗号化を用いた Mixnet におけるミキシングの有効性を証明するため、既存の Designated-Verifier Re-encryption Proof を修正し、提案システムへ適用する。さらに、提案システムでは通常の選挙で使われている投票用紙と類似の電子投票用紙、および上書き可能な公開掲示板を導入している。

キーワード　電子投票システム、普遍再暗号化 mix-net, 無証拠性,全体検証性,電子投票用紙、上書き可能な公開掲示板

Receipt-free and Universal verifiable E-Voting System Based on Universal Re-encryption Mix net

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

† Graduate School of Information Science and Electrical Engineering, Kyushu University

‡ Faulty of 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　Sako and Killian proposed mix-net e-voting system which satisfies receipt-free and universal verifiability. Michels and Horster pointed out that Sako-Killian scheme does not satisfy robustness and privacy. Golle et al. proposed universal re-encryption mix net which satisfies correctness and communication privacy. In this paper, we propose mix-net e-voting system which satisfies receipt-free and universal verifiability as well as robustness and privacy based on universal re-encryption mix net. In order to apply universal re-encryption to mix-net e-voting system, we modify designated-verifier re-encryption proof. The modified designated-verifier re-encryption proof is used to prove the valid of mixing. Also, we introduce E-voing Sheet which is similar to a real voting, and an Overwritable Bulletin Board which can be changed the contents of bulletin board by each mix-center.

Keywords　E-voting system, Universal re-encryption mix-net, Receipt-freeness, Universal verifiability, E-voting Sheet, Overwritable Bulletin Board.

1. Introduction

1.1. Motivation

Many e-voting systems have been proposed for secure on-line voting [PIK93][SK95][OMAFO99][HS00]. A few systems of these are used in real election. But, e-voting system is controversial recent topic. The recent topics of e-voting system are receipt-freeness and universal verifiability. Receipt-freeness means that a voter can not to construct a receipt to proving the content of his vote. Universal verifiability means that anyone can verify a correctness of election. Sako and Killian[SK95] proposed mix-net e-voting system to solve receipt-freeness and universal verifiability. A mix-net was pro-posed by [Cha81]. A mix-net is used to apply many applications as

anonymous channel. A mix-net takes a list of ciphertexts $(c_1, c_2, ..., c_N)$ of users $1, ..., N$ and outputs a permuted list of the plaintexts $(m_1, m_2, ..., m_N)$ without revealing the relationship between $(c_1, c_2, ..., c_N)$ and $(m_1, m_2, ..., m_N)$. Generally, a mix-net provides anonymity, privacy, and robustness as follows.

- Privacy : The messages are sent anonymously.
- Anonymity : Anyone should not know the relation between a sender and his message.
- Robustness : Although one mix-center is stopped, it should not affect an entire system.
- Individual Verifiability : A sender has to check whether or not his message has reached its destination.

Michels and Horster [MH96] pointed out that Sako-Killian's scheme has problems of privacy and robustness. Golle et al. [GJJS04] proposed a new type of public-key crypto-system that permits universal re-encryption of ciphertexts. Like standard re-encryption, universal re-encryption transforms a ciphertext C into a now ciphertext C' with same corresponding plaintext. Moreover, they proposed a mix-net based on their universal re-encryption.

1.2. Related works

As above mentioned, many schemes for secure e-voting system have been proposed (See appendix B). Fujioka, Okamoto and Ohta [FOO92] proposed a practical secret voting scheme for large scale elections based on blind signature and bit-commitment. Ohkubo et al.[OMAFO99] upgraded the e-voting scheme of [FOO92] through threshold encryption instead of bit-commitment scheme. Benaloh and Tuinstra[BT94] proposed the first receipt-free scheme for e-voting system. They put physically guarantees secret communication, as a voting booth, between the authorities and each voter. Sako and Kilian [SK95] proposed receipt-free voting protocol based on a mix-net channel. They assumed the existence of one-way secret communication, as an untappable private channel, between each authority and each voter. The important disadvantage of this scheme is that much load can be happened in tallying because of mix-net scheme [HS00]. Hirt and Sako[HS00] introduced the efficient receipt-free voting based on homomorphic encryp-tion. To achieve a receipt-freeness, they used schemes of [SK95] and [CGS97].

Jakobsson[Ja98] proposed a practical mix to achieve privacy, robustness, and verifi-ability in 1998. He used Blinding I, Blinding II, Unblinding I and Unblinding II. Des-medt and Kurosawa [DK00] showed an attack such that at least one malicious mix-center can prevent computing the correct output. And, Jakobsson [Ja99] proposed a flash mix-net to achieve privacy, robustness and verifiability. His mix-net consists of blinding protocol and unblinding protocol using two dummy elements which are inserted into the input list at the beginning of the protocol in flash mix. The blinding protocol consists of the first re-encryption and the second re-encryption. Mitomo and Kurosawa [MK00] showed the attack method of Jokobsson's flash mix under the condition which at most t among v mix-centers and at most $N-2$ among N senders is malicious.

1.3. Our contributions

The goal of our system is to construct mix-net e-voting system which satisfies universal verifiability, receipt-freeness, privacy and robustness. Moreover, we propose e-voting system which has more realistic constructions (See Table 1). Cryptographic techniques of our e-voting system are based on devices which are used in a real voting. That is, we apply hardware devices of a real voting to cryptographic techniques as follows.

E-voting Sheet (ES) : We propose firstly E-voting Sheet (We call ES) like a voting sheet of a real voting. In a real voting, after an election committee checks a voter, and he gives a voting sheet to a voter in a voting place. Similar to a real voting, to cast a vote is required ES in our e-voting system. The difference between ES and a voting sheet is whether all voters use the same voting sheet or not. That is, a voter uses the same voting sheet in a real voting. However, each voter in our e-voting uses the different ES. If all voters use the same ES like a real voting, a coercer can check voting content of a malicious voter. For instance, the coercer who is one of valid voters orders other voters to cast a special candidate. The coercer can compare his encrypted voting content with encrypted voting contents of voters. He requires the encrypted voting contents of voters. If his encrypted voting content is different with those of voters, the coercer punishes voters who do not cast the ordered candidate. Also, he rewards for voters who cast the ordered candidate. So, we use the different ES according to each voter. For the management of ES, we use a special authority, ES-center. ES is issued by ES-center and the last mix-center which computes of the voting result in our e-voting. We suppose that ES-center and the last mix-center never collude.

Table 1. Real Voting VS. Our E-voting system

Property	Real Voting	Our e-voting
Anonymity, Weak universal verifiability	Voting paper	E-voting Sheet (*ES*)
Privacy	Voting booth	Untappable Channel
Receipt-free ness	Voting box	Universal Re-encryption Mix-net, Overwritable Bulletin Board

Here, we define properties of ES as follows.

- Anyone can not modify or copy ES.
- Anyone can not hide or write his secret number on ES.

Overwritable Bulletin Board (OBB) : A few e-voting systems[CRG97] [OMAFOO99] uses general bulletin board. Properties of General bulletin board are

- Anyone can see contents of bulletin board
- Anyone can not modify or erase contents of bulletin board.

We introduce a special bulletin board which can overwrite contents of bulletin board. We call Overwritable Bulletin Board, and write OBB in this paper. Due to a mix-net, we use OBB. As above mentioned, a mix-net is

used to guarantee privacy, robustness and anonymity. Most of e-voting systems based on mix-net used Zero Knowledge Interactive Proof (ZKIP). But, these systems require the high computation complexity and time complexity, because each mix-center must prove how to shuffle an input message [HS00]. Also, this proof has some connection with universal verifiability. To decrease the computation complexity and time complexity in this proof, we use OBB and modify designated-verifier universal re-encryption proof [JSI06] instead of ZKIP (See appendix A). The roles of each mix center except the last mix-center are as follows.

-Each mix-center re-encrypts and mixes his input messages.
-Each mix-center posts the mixed output message to OBB in a random order.
-Each mix-center proves how to shuffle his output messages to the next mix-center using the modified designated-verifier re-encryption proof.

We suppose that only a mix-center can overwrite contents of OBB.

Untappable Channel : To achieve receipt-freeness, e-voting schemes make some physical assumption as communication channel [Oka97][BT94][SK95][HS00] [Hirt01][LK03]. We suppose that the existences of one-way untappable channels from the last mix center to ES-center and from a voter to ES-center. In table 2, we compare our e-voting system with other e-voting schemes based on a mix-net.

Table 2. Comparison of mix-net e-voting systems

	PIK93	SK95	HS00	Our scheme
Receipt-freeness	*No*	*Yes*	*Yes*	*Yes*
Universal Verifiability	*No*	*Yes*	*Yes*	*Yes*
Privacy	*Yes*	*No*	*Yes*	*Yes*
Robustness	*Yes*	*No*	*Yes*	*Yes*
Voting for multi-candidate	-	-	-	*Yes*

(*Yes* means that the property is satisfied. *No* means that the property does not satisfied. - means that the authors did not consider the property.)

In this paper, we propose two e-voting systems which are Yes-No voting and Multi-candidates voting. A voting content of Yes-No voting is 0 or 1. In case of e-voting for multi-candidate, we assign small prime numbers to multi-candidate, and use a 1-out-of-L voting scheme like [CFSY96][CGS97][LK02]. But, we do not use threshold en-cryption, but ES in e-voting system for an efficient implementation. The assigned prime numbers instead of multi-candidate's id plays an important role to be confirmed the voting result.

2. Universal Re-encryption mix-net

2.1. Overview of universal re-encryption mix-net

The outline of Golle et al.'s universal re-encryption for mix-net is as follows.
- Every input to the mix-net is encrypted under the public key of the recipient for whom it is intended.
- Thus, unlike standard re-encryption mix-net, universal mix-net accepts ciphertexts encrypted under the individual public keys of receivers, rather than encrypted the unique public key of the mix network.
- The output of a universal mix-net is a set of ciphertexts.
- Recipients can retrieve from the set of output ciphertexts those addressed to them, and decrypt them.

Key generation (*UKG*)

Output (PK,SK)= $(y = g^x, x)$ for $x \in_U Z_q$.

Encryption (*UE*)

Input comprises a message m, a public key y, and a random encryption factor $r = (k_0, k_1) \in Z_q^2$.

The output is a ciphertext

$$C = [(\alpha_0, \beta_0); (\alpha_1, \beta_1)] = [(my^{k_0}, g^{k_0}); (y^{k_1}, g^{k_1})]$$

We write $C = UE_{PK}(m, r)$ or $C = UE_{PK}(m)$ for brevity.

Universal mixing

Any server can be called upon to mix the concept of the bulletin board. This involves two operations : (1) The server re-encrypts all the universal ciphertexts on the bulletin board using ***URe***, and (2) The server writes the resulting new ciphertexts back to the bulletin board in random order, overwriting the old ones. It is also desirable that a mix server be able to prove that it operated correctly.

2.2. Analysis of Universal re-encryption mix-net

The advantages of Universal Re-encryption are as follows.
- Can be done without knowledge of public keys
- Construct a mix-net of this kind in which servers hold no public or private keying material.
- Half as efficient as standard ElGamal encryption.

The main properties of universal mix-net are as follows.
- Universal mix-net holds no keying material.
- Universal mix-net guarantees forward anonymity.
- Universal mix-net does not support escrow capability

In universal re-encryption mix-net, if a malicious mix-server S_t selects $k_0^t = k_1^t$, a coercer can know the inputs from the outputs of S_t as follows.

Input :

$$C^{t-1} = [(\alpha_0^{t-1}, \beta_0^{t-1}); (\alpha_1^{t-1}, \beta_1^{t-1})]$$

Output :

$$C^t = [(\alpha_0^t, \beta_0^t);(\alpha_1^t, \beta_1^t)]$$
$$= [(\alpha_0^{(t-1)}\alpha_1^{(t-1)k_0^t}, \beta_0^{(t-1)}\beta_1^{(t-1)k_0^t});(\alpha_1^{(t-1)k_1^t}, \beta_1^{(t-1)k_1^t})]$$

In case of $k_0^t = k_1^t$, Out put is

$$C^t = [(\alpha_0^t, \beta_0^t);(\alpha_1^t, \beta_1^t)]$$
$$= [(\alpha_0^{(t-1)}\alpha_1^{(t-1)k_0^t}, \beta_0^{(t-1)}\beta_1^{(t-1)k_0^t});(\alpha_1^{(t-1)k_0^t}, \beta_1^{(t-1)k_0^t})]$$

Then, a coercer can get parts of C^{t-1} from C^t as follows.

$$C^{t-1} = [(\alpha_0^{(t-1)}\alpha_1^{(t-1)k_0^t}, \beta_0^{(t-1)}\beta_1^{(t-1)k_0^t});(\alpha_1^{(t-1)k_0^t}, \beta_1^{(t-1)k_0^t})]$$

$$\alpha_0^{t-1} = \alpha_0^{(t-1)}\alpha_1^{(t-1)k_0^t} / \alpha_1^{(t-1)k_0^t}$$
$$\beta_0^{t-1} = \beta_0^{(t-1)}\beta_1^{(t-1)k_0^t} / \beta_1^{(t-1)k_0^t}$$

But, if only one mix-center among n mix-centers is trust, privacy, anonymous and robustness are guaranteed. Only, the trust mix-center should select each different random re-encryption factor.

3. Model of our e-voting

3.1 Entities

Voter V_i ($\{i \mid i = 1,...,z\}$): A voter votes only by a voting rule.

Mix center C_i ($\{j \mid j = 1,...,n\}$)

- Each mix-center generates a random encryption factor to re-encrypt ES, and re-encrypts *Voting Vector* which consists of encrypted voting content and encrypted *ES*.
- The last center recovers a voter's ES and compute the voting result.

ES-Center

- ES-center takes a valid voter list, and checks whether a voter is a valid voter or not through one-way untappable channel.
- He generates ES jointly with the last mix-center.
- He verifies the computed voting result by the last mix-center.
- For the privacy of a voter, we suppose that ES-center and the last-center never collude. Also, assume that ES-center is a trust authority and can not cast a vote.

Bulletin Board *BB*

- Anyone can see contents of *BB*, but can not modify or erase it.

Overwritable Bulletin board *OBB*

- Only each mix-center overwrites contents in OBB. Other people can only see it.

3.2 Overview of our e-voting

Our e-voting protocol runs as follows.

Issue of ES

1. We suppose that ES-center takes a valid voters list. ES-center and the last mix -center jointly generate ES.
2. After ES-center checks a voter's id and signature through one-way untappable channel, he sends ES and encrypted ES to a valid voter.
3. ES-center posts a valid voter's ID to BB.

Voting stage

1. A voter chooses a voting content, and encrypts a voting content with ES.
2. A voter generates *Voting Vector* which consists of encrypted voting content and encrypted ES by ES-center to OBB.
3. The first mix-center gets *Voting Vector* from OBB and re-encrypts *Voting Vector* with his random encryption factor as the original universal re-encryption mix-net. He overwrites the old *Voting Vector* in OBB in a random order.
4. To prove a valid of mixing of the first mix-center, the first mix-center (Prover) proves to the second mix-center (Verifier) without leaking his random encryption factor(See appendix A). He sends his proof to the designated field of BB.
5. Other mix-centers from the second mix-center to $n-1$ mix-center re-encrypt *Voting Vector* with their random encryption factors and overwrite the old *Voting Vector* in OBB. Each mix-center proves his mixing to the next mix-center using the modified designated-verifier re-encryption proof.

Counting stage

1. The last mix-center decrypts a voter's ES. He computes the voting result with ES.
2. ES-center verifies the computed voting result with the number of issued ES and the published voting result by the last mix-center.

4. E-voting procedures

Notation

ES_i : E-voting sheet of a voter i.

m_i ($=0$ or 1): Voting contents of a voter i for Yes-No voting.

$K_j^i = (k_{j,0}^i, k_{j,1}^i) \in Z_q^2$: Random encryption factor of mix center C_j ($1 \le j \le n$), where $1 \le i \le z$, $k_{j,0}^i \neq k_{j,1}^i$

ζ_j^i : Re-encrypted *Voting Vector* by mix center C_j ($1 \le j \le n$).

$r_{ES_i} (\in_R Z_{p-1})$: A unique random number of ES-center for generating ES.

p, q : Random numbers ($p = 2q+1$)

H : Hash function such as SHA-1

y_n, y_L : Public keys of the last mix-center ($y_n = g^{x_n}, y_L = g^{x_L}$)

x_n, x_L : Secret keys of the last mix-center

Issue of *ES*

1. Before voting, ES-center generates a unique random number r_{ES_i} ($\in_R Z_{p-1}$), and generates ES with r_{ES_i} and a public key y_L of the last mix-center as follows.

$$ES_i = y_L^{r_{ES_i}} \bmod p$$

, where i is the number of a valid voter; $i = 1,2,\cdots,z$.

2. ES-center generates $k_{0,1}^i (\in Z_q^2)$ and encrypts ES_i with $k_{0,1}^i$ and a public key y_n of the last mix-center as follows.

$$\zeta_{0,1}^i = (ES_i y_n^{k_{0,1}^i}, g^{k_{0,1}^i})$$

Proof of validity of *E-voting Sheet* (*Proof-ES*)

1. After *ESs* are issued (Before voting), ES-center computes as follows.

$$ES_z(C) = \prod_{i=1}^{z} ES_i$$

, where z is the total number of a valid voter.

2. Also, ES-center computes as follows.

$$E_i = g^{r_{ES_i}}$$

$$EC = \prod_{i=1}^{z} E_i$$

3. The last mix-center verifies the proof of validity of ES.

$$ES_i(C) \stackrel{?}{=} (EC)^{x_L}$$

Voting Stage

1. ES-center checks whether a voter is a valid voter or not with a voter's id and signature through one-way untappable channel. If a voter is a valid voter, he posts his ID and sends ES to a voter. If not, ES-center rejects him.

2. ES-center generates $\zeta_{0,1}^i$ and sends it to a valid voter Vi.

3. Vi chooses a voting content m_i (=0 or 1) which 1 is Yes-vote or 0 is No-vote, and encrypts m_i as follows.

$$v_i = (ES_i)^{m_i}$$

4. Vi generates a random encryption factor $k_{0,0}^i \in Z_q^2$. He computes $\zeta_{0,0}^i$ a public key y_n of the last mix-center C_n and $k_{0,0}^i$ as follows.

$$\zeta_{0,0}^i = (v_i y_n^{k_{0,0}^i}, g^{k_{0,0}^i})$$

5. He generates *Voting Vector* ζ_0^i with his $\zeta_{0,0}^i$ and received $\zeta_{0,1}^i$ from ES-center as follows.

$$\zeta_0^i = [\zeta_{0,0}^i, \zeta_{0,1}^i] = [(x_{0,0}^i, y_{0,0}^i), (x_{0,1}^i, y_{0,1}^i)]$$
$$= [(v_i y_n^{k_{0,0}^i}, g^{k_{0,0}^i}), (ES_i y_n^{k_{0,1}^i}, g^{k_{0,1}^i})]$$

5. Vi posts ζ_0^i on *OBB*.

Mixing Stage

1. The first mix-center C_1 generates a random encryption factor $K_1^i = (k_{1,0}^i, k_{1,1}^i) \in Z_q^2$, where $k_{1,0}^i \neq k_{1,1}^i$. She computes *Voting Vector* ζ_1^i with K_1^i as follows.

$$\zeta_1^i = [\zeta_{1,0}^i, \zeta_{1,1}^i] = [(x_{1,0}^i, y_{1,0}^i), (x_{1,1}^i, y_{1,1}^i)]$$
$$= [(x_{0,0}^i x_{0,1}^{i\ k_{1,0}^i}, y_{0,0}^i y_{0,1}^{i\ k_{1,0}^i})(x_{0,1}^{i\ k_{1,1}^i}, y_{0,1}^{i\ k_{1,1}^i})]$$

2. For proof of validity of mixing, C_1 chooses $u_{1,1}^1, u_{1,2}^1, r^1, t^1 \in Z_q^2$ and computes

$$[(a,b),(c,d)] = [(y^{u_{1,1}^1}, g^{u_{1,1}^1}), (y^{u_{1,2}^1}, g^{u_{1,2}^1})], F = g^{r^1} y_2^{t^1}$$

, where $y_2 (= g^{x_2})$ is a public key and x_2 is a private key of the second mix center C_2.

3. The first mix center computes $S = H(a,b,c,d,F,x_{1,0}^i, y_{1,0}^i, x_{1,1}^i, y_{1,1}^i)$, $T = u_{1,1}^1 - k_{0,0.}^i - k_{0,1}^i k_{1,0}^i$ and $U = u_{1,2}^1 - k_{0,1}^i k_{1,1}^i$. Then, he sends (r^1, t^1, S, T, U) and ζ_1 to the second mix center C_2.

4. The second mix-center verifies as follows.

$$S \stackrel{?}{=} (y^T x_{1,0}^i, g^T y_{1,0}^i, y^U x_{1,1}^i, g^U y_{1,1}^i, g^{r^1} y_2^{t^1}, x_{1,0}^i, y_{1,0}^i, x_{1,1}^i, y_{1,1}^i)$$

5. C_1 sends ζ_1^i to OBB in a random order, and posts the proof to the designated fields of BB.

6. C_2 gets ζ_1^i from OBB, and re-encrypts ζ_1^i with $K_2^i = (k_{2,0}^i, k_{2,1}^i) \in Z_q^2$ as follows.

$$\zeta_2^i = [\zeta_{2,0}^i, \zeta_{2,1}^i] = [(x_{2,0}^i, y_{2,0}^i), (x_{2,1}^i, y_{2,1}^i)]$$
$$= [(x_{1,0}^i x_{1,1}^{i\ k_{2,0}^i}, y_{1,0}^i y_{1,1}^{i\ k_{2,0}^i})(x_{1,1}^{i\ k_{2,1}^i}, y_{1,1}^{i\ k_{2,1}^i})]$$

, where $k_{2,0}^i \neq k_{2,1}^i$.

7. C_2 proves ζ_2^i to the third mix center C_3 using designated-verifier universal re-encryption proof as that of the first mix center. Also, he sends the proof to the designated fields in the bulletin board, and overwrites the old ones.

8. Other mix centers from C_3 to C_{n-1} re-encrypt repeatedly like that of C_2 or C_1.

9. The last mix center C_n gets

$$\zeta_{n-1}^i=[\zeta_{n-1,0}^i,\zeta_{n-1,1}^i]=[(x_{n-1,0}^i,y_{n-1,0}^i),(x_{n-1,1}^i,y_{n-1,1}^i)]$$
$$=[(x_{n-2,0}^i x_{n-2,1}^{i\,k_{n-1,0}^i},y_{n-2,0}^i y_{n-2,1}^{i\,k_{n-1,0}^i})(x_{n-2,1}^{i\,k_{n-1,1}^i},y_{n-2,1}^{i\,k_{n-1,1}^i})]$$

Counting Stage

1. After the voting time is over, the last mix-center C_n computes ES from $\zeta_{n-1,1}^i$ and can get the ES of a voter as follows.

$$ES_i=x_{n-2,1}^{i\,k_{n-1,1}^i}/(y_{n-2,1}^{i\,k_{n-1,1}^i})^{x_n}$$

2. He computes

$$ES_h(C_n)=\prod_{i=1}^{h}ES_i$$

, where $1\le i\le h$. ($i=1\sim h$, the number of voters who cast a voting.)

3. Also, ES-center computes the number of used ES

$$\prod_{i=1}^{h}ES_i=ES_h(C)$$

4. The last mix-center and ES-center verify the valid voters' number using the number of used ES.

$$ES_h(C_n)\stackrel{?}{=}ES_h(C)$$

5. The last mix-center computes the voting result as follows.

$$If\quad x_{n-2,0}^i x_{n-2,1}^{i\,k_{n-1,0}^i}/(y_{n-2,0}^i y_{n-2,1}^{i\,k_{n-1,0}^i})^{x_n}=1,$$
then $m_i=0$ (*No-vote*)
else $m_i=1$ (*Yes-Vote*)

6. The last mix-center posts the voting results to BB.

$$M=\sum_{i=0}^{h}(m_i=1)$$

7. ES-center can compare computed voting result by the last mix-center with the number of used *ES* ***(Proof-Counting)***.

5 Security and Efficiency of the proposed e-voting system

5.1 Security

Privacy : ES-center can know a voter's ID and ES, and the last center can know the relation between ES and a voter's voting content. Unless ES-center and the last center collude, privacy is guaranteed. To prevent a forgery of ES, ES-center sends the original *ES* with the encrypted ES to a voter. So, a voter can not insert his secret number in ES.

Unreuseability : Because ES-center takes a valid voters list, and can check a voter. So, double-voting is impossible.

Universal verifiability : Universal verifiability is based on correctness. To achieve universal verifiability including Correctness, our e-voting systems proves correctness in every steps using Proof-ES, Proof-Mixing and Proof-Counting. Also, anyone checks whether other voters reach the last mix-center or not through the number of issued ES and the voting result.

Receipt-free : In our scheme, although a voter knows his ES and voting content, he can not modify and erase his ES. Because he does not know the secret key of the last center, he can not prove his voting to a coercer or other party. Although a voter colludes with a malicious mix-center, he can not affect his voting. Also, in mixing stage, $F=g^{r^1}y_2^{t^1}$ can be used as a trapdoor commitment like [CLK03]. A malicious mix-center knows his private key x_2, he can compute r' and t' such as $r'+x_2t'=r^1+x_2t^1$. He can open freely the commitment as he wants and generates the re-encryption proof for any bidding (See mixing stage of section 4.1).

Robustness : In case of universal re-encryption mix-net, it needs only the secret key of the last mix-enter to decrypt a ciphertext. Other mix-centers only re-encrypt and mix his input message. That is, other mix-center does not effect on his input message. So, even if only one mix-center is trust, robustness is guaranteed.

5.2 Efficiency

Table 3. Computational complexities of our scheme, [LK02] and [BFPPS01]

	Our scheme	**[LK02]**	**[BFPPS01]**
One voter	1 *encryption*	2 *encryptions*, 1 *signing and verification*	3 *encryptions and proofs*, 1 *proof*
TRR		$2n$ *verifications and encryptions*	
Administrator		1 *multiplication*	
Each mix-center	$(m-1)$ *encryptions and proofs*		
The last mix-center	*n decryptions and verifications*		
Talliers		$t\cdot n$ *multiplications*	
LA,RA,NA			$3n+3n+2n$ *encryptions and* $2n$ *decryptions*

In this section, we compare communication and computational complexity of our voting scheme with those of [LK02] and [BFPPS01]. Let n and m present the number of voters and authorities (mix-centers of our system or talliers of [LK01]). [BEPPS01] consists of three authorities which are Local authority (LA), Regional authority (RA), and National authority (NA). Table 3 and table 4 present computational complexities, and numbers of the rounds of communication complexities, in these voting systems. In [LK02] of table 3, TRR means tamper-resistant randomizer and and t means the number of authorities in (t,n) threshold encryption.

Table 4. Communication complexities of our scheme, [LK02] and [BFPPS01]

	Our scheme	[LK02]	[BFPPS01]
Voter's authentication	$2n$	n	$3n$
Voting	n	$4n$	$3n+3n$
Mixing	$n(m-1)$		
Counting	n	$1+t\cdot n$	$10n$

6 Conclusions

In this paper, we propose mix net e-voting system which satisfies robustness and privacy as well as receipt-freeness and universal verifiability. Indeed, Sako et al. proposed e-voting system with receipt-freeness and universal verifiability using mix-net. But, Michels and Horster pointed out that Sako et al.'s scheme has problems against robust-ness and privacy. These problems are caused by a factor to achieve universal verifiability. we introduce firstly E-voting Sheet, and use Overwritable Bulletin Board. For achieving universal verifiability, we use proof-ES, Proof-Mixing and Proof-Counting. Also, our e-voting systems can be used regardless of a number of candidates as well as is similar to a real voting method.

ACKNOWLEDGEMENT

The research was partly supported by the Grant-in-Aid for Creative Scientific Research No.14GS0218 (Head of Researchers : Prof. Hiroto Yasuura, System LSI Research center, Kyushu University) 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 first author was also supported by Grant for Non-Japanese Researcher of Foundation for C&C Promotion (This foundation is maintained with the donations from NEC Corp.).

References

[Abe98] M.Abe,"Universally Verifiable Mix-net with Verification Work IndESendent of the Number of Mix-servers", Eurocrypt'98, pp437-447, 1998.

[BCC88] G.Brassared, D.Chaum and C.Crépeau, "Minimum DisclosurESroofs of Knowledge", Journal of Computer and System Science, Vol.37, pp159-189, 1988.

[BFPPS01] O.Baudron, P.A. Fouque, D.Pointcheval, G.Poupard, J.Stern " Practical Multi-Candidate Election System" ACM 2001.

[BT94] J. Benaloh and D.Tuinstra, "Receipt-Free Secret-Ballot Elections", Proc. of STOC'94, pp544-553, 1994.

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

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

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

[Cha81] D.Chaum, "Untraceable electronic mail return address and digital pseudonyms," Com-munication of the ACM, Vol.24, No.2, pp84-88, 1981.

[CM96] R.Cramer, M.Franklin, B, Schoenmakers, M.Yung "Multi-Authority Secret-Ballot Elec-tions with Linear Work" EUROCRYPT '96, LNCS1070, Springer-Verlag, Berlin Heidelberg 1996.

[DE82] Denning, Dorothy Elization "Cryptography and Data security" Addision-Wesley Publish-ing Company, 1982

[DK00] Y.Desmedt and K.Kurosawa, "How to break a practical MIX and design a new one", Eurocrypt' 2000

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

[GJJS04] P.Golle, M. Jakobsson, A.Juels and P.Syverson, "Universal Re-encryption for Mixnets", CT-RSA 2004, LNCS 2964, pp163-178, 2004.

[Hersch97] M.A.Herschberg, " Secure Electronic Voting Over the World Wide Web", Master Thesis in Electronic Engineering and Computer Science, Massachusetts Institute of Technol-ogy, 1997

[Hirt01] M. Hirt, "Multi-Party computation: Efficient Protocols, General Adversaries, and Vot-ing", Ph.D. Thesis, ETH Zurich, RESrint as vol. 3 of ETH Series in In-formation Security and Cryptology, Hartung-Gorre Verlag, Konstanz, 2001.

[HS00] M.Hirt and K.Sako, "Efficient receipt-free voting based on homomorphic encryption", Eurocrypt 2000, LNCS 1807, pp539-556, 2000.

[Ja98] M.Jakobsson,"A practical MIX", Eurocrypt'98 pp448-461, 1998.

[Ja99] M.Jakobsson,"Flash Mixing" PODC'99, pp83-89, 1999.

[JJ02] A.Juels, M.Jakobsson "Coercion-resistant Electronic Elections" http://ESrint.iacr.org/2002/165/, Nov,2002

[JM98] M.Jakobsson and D.M'Raihi, "Mix-based Electronic Payments", SAC'98. pp.157-173, 1998

[JSI96] M.Jakobsson, K.Sako, R. Impagliazzo "Designated Verifier Proofs and Their Applica-tion" CRYPTO'96, LNCS 1109, pp. 186-200. Springer-Verlag, 1996

[LK00] B.C. Lee, and K.J. Kim, " Receipt-free electronic voting through collaboration of voter and honest verifier" Proceeding of JW-ISC2000, pages 101 · 08, Jan. 25-26, 2000, Okinawa, Japan.

[LK02] B.C. Lee, and K.J. Kim,"Receipt-Free Electronic Voting Scheme with a Tamper-Resistant Randomizer" ICISC2002, vol.5, No.1 pp405-pp422, 2002

[MH96] M.Michels and P.Horster, "Some remarks on a receipt-free and universally verifiable Mix-type voting scheme," Asiacrypt'96, pp125-132, 1996.

[MK00] M.Mitomo and K.Kurosawa, "Attack for Flash Mix", Asiacrypt2000, pp.192-204, LNCS1976, 2000.

[Oka97] T.Okamoto, "Receipt-Free Electronic Voting Scheme for Large Scale Elections", Security Protocols Workshop, 1997.

[OMAFO99] M.Ohkubo, F.Miura, M.Abe, A. Fujioka, T.Okamoto "An Improvement on a Practi-cal Secret Voting Scheme" ISW'99, LNCS 1729, pp225-234, 1999.

[Pfi95] B.Pfitzmann, "Breaking an efficient anonymous channel",LNCS950, Advances in Cryptol-ogy, Proc. of Eurocyrpt'94, Springer-Verlag, pp332-340, 1995

[PIK93] C.Park, K.Itoh and K.Kurosawa," All/nothing election scheme and anonymous channel", Eurocrypt'93, 1993.

[SK95] K.Sako and J.Kilian, "Receipt-Free Mix-type Voting Scheme", Proceeding of Eurocrypt'95, LNCS921, Springer-Verlag, pp393-403,1995.

APPENDIX

A. Designated-Verifier Universal Re-encryption Proof (Proof –Mixing)

We modified Designated-Verifier Re-encryption proof for universal re-encryption. The modified proof is used the proof of the re-encrypted bidding prices by the auction issuer and the auctioneer. Let $[(x_0,y_0),(x_1,y_1)]=[(my^{a_1},g^{a_1});(y^{a_2},g^{a_2})]$ be an original encrypted ElGamal ciphertext by universal re-encryption scheme for the message m and a random encryption factor $(a_1,a_2)\in Z_q^2$, and $[(x_0',y_0'),(x_1',y_1')]=[(x_0x_1^{a_1'},y_0y_1^{a_1'});(x_1^{a_2'},y_1^{a_2'})]$ be a re-encrypted ciphertext by a prover. The prover wants to prove that (x_0',y_0') and (x_1',y_1') have exponents a_1' and a_2' without exposing the values a_1' and a_2'. We suppose that a public key $y_u=g^{s_u}$ is a public key of the verifier.

Like [CLK03], the verifier can open the commitment F freely with his private key s_u in the modified designated-verifier re-encryption proof. That is, he can compute another pair $r'+s_ut'=r+s_ut$ such that holds.

Prover **Verifier**

$k_1,k_2,r,t\in Z_q^2$

Compute

$[(a,b)(c,d)]=$

$[(y^{k_1},g^{k_1}),(y^{k_2},g^{k_2})]$

$F=g^ry_u^t$

$S=H(a,b,c,d,F,x_0',y_0',x_1',y_1'),$

$T=k_1-a_1-a_2a_1'$

$U=k_2-a_2a_2'$

(r,t,S,T,U) ⟶

Accept the proof if

$S=(y^Tx_0',\ g^Ty_0',\ y^Ux_1',\ g^Uy_1',\ g^ry_u^t,\ x_0',\ y_1',\ x_1',\ y_1')$

B. E-voting Schemes

In this appendix, we explain goals and techniques of several e-voting systems.

E-voting scheme	Cryptography Techniques	Goals
[FOO93]	- Blind signature - Bit-commitment	- Fairness - Security
[SK95]	- Mix-type anonymous Channel (Universal Verifiability)	- Receipt-Free - Universal Verifiability
[CM96]	- Hiding/ Indistinguishable Protocol - Threshold Scheme - Homomorphic encryption	- Privacy - Universal Verifiability - Robustness
[CRG97]	- Threshold Scheme - Homomorphic encryption - ElGamal cryptosystem	- Privacy - Universal Verifiability - Robustness
[OMAFO 099]	- Mix-net - Blind-signature	- Walk away - Unreusability Verifiability
[BFPPS 01]	- ZKIP - Paillier cryptosystem	- Privacy - Verifiability - Robustness