Security and Privacy in E-voting and RFID System Based on Universal

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

Saito, Junichiro
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：Proc. of the 2005 Symposimu on Cryptography and Information Security. II, pp.907-912, 2005-01. IEICE
バージョン：accepted
権利関係：

SCIS 2005 The 2005 Symposium on Cryptography and Information Security
Maiko Kobe, Japan, Jan.25-28, 2005
The Institute of Electronics, Information and Communication Engineers

Security and Privacy in E-voting and RFID System Based on Universal Re-encryption Mix-net

Yong-Sork HER * Junichiro Saito † Kenji Imamoto ‡ Kouichi Sakurai §

Abstract— Golle *et al.* proposed a universal re-encryption scheme for mix-net in RSA2004. In case of re-encryption, this universal re-encryption does not need a public key, but just uses a random encryption factor. Therefore, the decryption is very simple than that of other re-encryption schemes. In this paper, we apply this universal re-encryption to e-voting system and RFID system which have recently received a lot of attention for privacy and security with the advantage of the universal re-encryption. Furthermore, we analyze security and privacy of our e-voting system and RFID system. In case of e-voting based on the universal re-encryption, it can take the effective computational complexity because the decryption for the counting of voting contents is possible at once. But, it needs the requirement that the tallier is a trusted party. In case of RFID system, a consumer 's privacy can be infringed by a strong tracing ability. Although ID of a RFID tag can be encrypted, it is possible to pursue an object by tracing specific information. We discuss security and privacy of e-voting system and RFID system using the universal re-encryption.

Keywords: E-voting system, RFID system, Universal Re-encryption mix-net, Security, Privacy, Cryptography

1 Introduction

1.1 Motivation

Many e-voting systems have been proposed for secure on-line voting [**?**, **?**, **?**]. 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 construct a receipt to provide the content of his vote. Universal verifiability means that anyone can verify a correctness of election. Sako and Killian[**?**] proposed e-voting system based on a mix-net to solve receipt-freeness and universal verifiability. A mix-net was proposed by Chaum[**?**]. A mix-net is used to apply many applications as anonymous channel. A mix-net takes a list of ciphertexts of users and outputs a permuted list of the plaintexts without revealing the relationship between and . 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-centers is stopped, it should not affect an entire system.
- **Individual Verifiability** : A sender has to check whether or not his message has reached to its destination.

Michels and Horster [**?**] pointed out that Sako-Killian 's scheme has problems of privacy and robustness. These problems give rise to a serious loss on voting system. Golle et al.[**?**] proposed a universal re-encryption public technique that permits the universal re-encryption of ciphertexts. Like standard re-encryption, the universal re-encryption transforms a ciphertext into a new ciphertext with same corresponding plaintext. Moreover, they proposed a mix-net based on their universal re-encryption.

A Radio-Frequency-Identification (RFID) tag is a small and inexpensive device that consists of an IC chip and an antenna which communicate by radio frequency. A radio communication device called as a reader emits a query to RFID tags and reads their ID. Some readers also transmit power to RFID tags when they emit a query. In this case, RFID tags do not have power supply. Therefore RFID tags are expected to be used as a substitute for a bar code in the future [**?**, **?**, **?**, **?**]. In order to use as a bar code, the cost of RFID tags is $0.05\$/unit$, and tags are small as 0.4mm $\times$ 0.4mm and thin enough to be embedded in the papers [**?**, **?**]. For this reason, the processing capacity of a RFID tag is limited. The RFID system using this tag and a reader is used for the automobile object identification. Since the goods attached the RFID tags in a cardboard box can be checked even if the box is not opened, so it is used for management of goods[**?**, **?**]. A RFID tag is attached to goods, and it is expected that its function like a bar code is achieved and it is useful to theft detection. Moreover, after goods are purchased, a RFID system gives a useful function for a consumer. For example, a refrigerator with the reader will be able to recognize expired food-stuffs, and a closet will be able

* Graduate School of Information Science and Electrical Engineering, Kyushu University, ysher@itslab.csce.kyushu-u.ac.jp
† saito@itslab.csce.kyushu-u.ac.jp
‡ imamoto@itslab.csce.kyushu-u.ac.jp
§ Faculty of Information Science and Electrical Engineering, Kyushu University. sakurai@csce.kyushu-u.ac.jp

to offer a few of the enticing possibilities of its contents [?]. Moreover the European Central Bank (ECB) has proposed to embedded RFID tags in Euro banknotes [?]. By using identification combined ID on RFID tags and serial number printed on banknotes, it is expected to prevent forgery or money laundering. The communication between a reader and a RFID tag is performed by radio. So it is simply tapped by an attacker. The reader can simply derive information from the RFID tag and it can be used to infringement of the privacy [?, ?]. Since the RFID tag has unique ID, if the attacker obtains the ID, he can get the information on the object that the tag was attached. For example, the size and the price of clothes, the contents of a wallet, the inventory information on the goods of a store etc. can be leaked. As a result, it infringes on the owner 's privacy. Moreover, the location of the owner can be traced by tracing the information on the specific RFID tag even if the attacker cannot understand the contents of ID. This privacy about owner 's location is called as location privacy [?]. For this reason, there are some problems such as a retail store pursues a consumer and the circulation information on goods is revealed.

1.2 Related works

As above mentioned, many schemes for secure e-voting system have been proposed. Fujioka, Okamoto and Ohta [?] proposed a practical secret voting scheme for large scale elections based on blind signature and bit-commitment. Ohkubo *et al.*[?] upgraded the e-voting scheme of [?] through threshold encryption instead of bit-commitment scheme. Benaloh and Tuinstra [?] 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 [?] 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 heavy cost load can be happened in tallying because of mix-net scheme [?].
Hirt and Sako[?] introduced the efficient receipt-free voting based on homomorphic encryption. To achieve a receipt-freeness, they used schemes of [?] and [?]. Jakobsson[?] proposed a practical mix to achieve privacy, robustness, and verifiability in 1998. He used Blinding I, Blinding II, Unblinding I and Unblinding II. Desmedt and Kurosawa [?] showed an attack such that at least one malicious mix-centers can prevent computing the correct output. And, Jakobsson [?] 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 [?] showed the attack method of Jokobsson 's flash mix under the condition which at most among mix-centers and at most among senders is malicious.
Also, since the communication between a RFID tag and a reader is monitored simply, it applies encryption to the communication, or uses authentication an owner or a specific reader [?]. Since the reader 's capability is not restricted, the reader can encrypt the contents of a RFID tag. However, since the cost of a RFID tag is cheap, the RFID tag has only the limited processing capability. Moreover it is possible that the communication between a RFID tag and a reader is intercepted. Therefore, it is difficult for the RFID tag to authenticate the specific reader. In addition to encrypt the information on the RFID tag, there is an approach of re-encrypting the encrypted information on the RFID tag periodically [?]. Re-encryption means encrypting a ciphertext again. It is performed by using public key cryptography. Even if a ciphertext is re-encrypted repeatedly, we can obtain the plaintext by decrypting only once with using a private key. By using symmetric key cryptography, we must decrypt the re-encrypted ciphertext many times or the reader has to synchronize with the RFID tag. Moreover, if re-encryption has the property of semantic security, it is difficult for an attacker to get the original cipher-text from the re-encrypted ciphertext [?]. Since the information on a RFID tag is changed by re-encryption, it can prevent from tracing the information on the specific RFID tag. Moreover, if the reader processes re-encryption, a RFID tag does not need carry out complicated processing. However, if a reader processes re-encryption with a public key, the owner has to deliver information about the public key for the reader in case of re-encryption. In that case, the attacker will be possible to trace the RFID tag relevant to the public key [?]. Although you may consider making the RFID tag itself process re-encryption, it is difficult for the RFID tag to process re-encryption because its processing capability is restricted.

1.3 Our Contribution

We apply the universal re-encryption public technique for a mix-net which is proposed by Golle *et al.* to an e-voting system and an RFID system. For the re-encryption, this universal re-encryption uses just a random encryption factor, not a public key. Therefore, the application system based on the can get the effective communication complexity in the decryption stage. In this paper, we apply this universal re-encryption to e-voting system and RFID system which have recently received a lot of attention for privacy and security with the advantage of the universal re-encryption. Furthermore, we analyze security and privacy of our e-voting system and RFID system based on the universal re-encryption. Our e-voting system and RFID system consist of each three kinds of participants as follows.
E-voting system : A voter, Mix-centers, Tallier
RFID system : IC tag, Readers, Database
A voter and IC tags play a role as a sender, and mix-centers and readers are mixing-center to shuffle the received data. Tallier and database are authorities to decrypt. Then, mix-centers and readers satisfy confidentiality and untraceability for secure e-voting system

and RFID system. The tallier of an e-voting system satisfies untraceability, not confidentiality. If the tallier satisfies confidentiality, he can trace a voter 's ID. Therefore, it can be happened the privacy of a voter. Also, the database of RFID system does not satisfy confidentiality and untraceability to protect the security of IC tag from the readers.

red When we apply the universal re-encryption public technique to the e-voting system and RFID system, the tallier of the e-voting system does not satisfy untraceability. This problem is caused by the original the universal re-encryption public technique. The universal re-encryption public technique guarantees only external anonymity. But, if the tallier is a trust party and should not collude with other participant, the privacy of a voter can be guaranteed. Moreover, our e-voting system based on the unviersal re-encryption public technique has the excellent computational cost than other e-voting systems based on a mix-net scheme like table 1.

2 The universal re-encryption for Mix-net and Security Analysis

2.1 The universal re-encryption for Mix-net

The outline of Golle *et al.* 's the 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 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.
Decryption (UD) Input is a ciphertext $C = [(\alpha_0, \beta_0); (\alpha_1, \beta_1)]$ under public key y. Verify $\alpha_0, \beta_0, \alpha_1, \beta_1 \in g$; if not, the decryption fails, and a special symbol $\perp$ is output. Compute $m_0 = \alpha_0/\beta_0^x$ and $m_1 = \alpha_1/\beta_1^x$. If $m_1 = 1$, then the output is $m = m_0$. Otherwise, the decryption fails, and a special symbol $\perp$ is output. Note that this ensures a binding between ciphertexts and keys: a given ciphertext can be decrypted only under one given key.
Re-encryption (URe) Input is a ciphertext $C = [(\alpha_0, \beta_0); (\alpha_1, \beta_1)]$ with a random re-encryption factor $r' = (k_0', k_1') \in Z_q^2$. Output is a ciphertext $C' = [(\alpha_0', \beta_0'); (\alpha_1', \beta_1')] = [(\alpha_0 \alpha_1^{k_0'}, \beta_0 \beta_1^{k_0'}); (\alpha_1^{k_1'}, \beta_1^{k_1'}]$, where $k_0', k_1' \in Z_q^2$.
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 Security Analysis

The advantages of the 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 the 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 :

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

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

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

Then, a coercer can get parts of $C^(t-1)$ from C^t as follows.

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

But, if only one mix-center among 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 $V_i(i|i = 1, ..., z)$: A voter casts a vote only by an election rule.
Mix-centers $C_j(j|j = 1, ..., n)$
- Each mix-centers generates a random encryption factor and re-encrypts *Voting Vector* which consists of encrypted voting content.

Tallier
- The tallier generates a public key and a secret key for the encryption of *Voting Vector*.
- He should keep safely the secret key.
- He has not to collude with other people or participants.

- He computes the vote counting.

Bulletin Board *BB*

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

3.2 Model of e-voting

■ **Notation**

m_i : Voting contents of a voter i.
$K_j^i = (k_{j,0}^i, k_{j,1}^i \in Z_q^2)$:Random encryption factor of mix-centers
$C_j (1 \leq j \leq n)$, where $1 \leq i \leq z, k_{j,0}^i \neq k_{j,1}^i$
ζ_j^i : Re-encrypted Voting Vector by mix-centers $C_j (1 \leq j \leq n)$
p, q : Random numbers $(p = 2q + 1)$
H : Hash function such as SHA-1
y_n, x_n : Public keys of the last mix-centers $(y_n = g^{x_n})$

Stage I (Creation of voting vector and Voting stage)

1. The tallier checks whether a voter is a valid voter or not with a voter 's id and signature.
2. A voter V_i chooses a voting content m_i.
3. V_i generates a random encryption factor $k_{0,0}^i, k_{0,1}^i (\in Z_q^2)$, where $k_{0,0}^i \neq k_{0,1}^i$. He computes ζ_0^i with a public key y_n of the tallier as follows.

$$\begin{aligned}\zeta_0^i &= [\![\zeta_{0,0}^i, \zeta_{0,1}^i]\!] = [\![(x_{0,0}^i, y_{0,0}^i)]\!] = [\![x_{0,1}^i, y_{0,1}^i)]\!] \\ &= [\![(m_i y_n^{k_{0,0}^i}, g_n^{k_{0,0}^i}), (y_n^{k_{0,1}^i}, g_n^{k_{0,1}^i})]\!]\end{aligned}$$

4. V_i sends ζ_0^i to the first mix-center.

Stage II (Mixing)

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 as follows.

$$\begin{aligned}\zeta_1^i &= [\![\zeta_{1,0}^i, \zeta_{1,1}^i]\!] = [\![(x_{1,0}^i, y_{1,0}^i), (x_{1,1}^i, y_{1,1}^i)]\!] \\ &= [\![(m_i x_{0,0}^i x_{0,1}^{i\,k_{1,0}^i}, y_{0,1}^{i_{0,0}\,y^{i\,k_{1,0}^i}}), (x_{0,1}^{i\,k_{1,1}^i}, y_{0,1}^{i\,k_{1,1}^i})]\!]\end{aligned}$$

2. Other mix-centers from C_2 to C_{n-1} re-encrypt repeatedly like that of C_1.
3. The last mix-center C_n gets

$$\begin{aligned}\zeta_1^n &= [\![\zeta_{n,0}^i, \zeta_{n,1}^i]\!] = [\![(x_{n,0}^i, y_{n,0}^i), (x_{n,1}^i, y_{n,1}^i)]\!] \\ &= [\![(x_{n-1,0}^i x_{n-1,1}^{i\,k_{n,0}^i}, x_{n-1,0}^i x_{n-1,1}^{i\,k_{n,0}^i}, (x_{n-1,1}^{i\,k_{n,1}^i}, y_{n-1,1}^{i\,k_{n,1}^i})]\!]\end{aligned}$$

Stage III (Counting stage) 1. After the voting time is over, the tallier gets ζ_n^i of a voter as follows.
2. The tallier computes the voting result as follows.

$$x_{n-1,0}^i x_{n-1,1}^{i\,k_{n,0}^i} / (y_{n-1,0}^i y_{n-1,1}^{i\,k_{n,0}^i})^{x_n} = m_i$$

3. The tallier posts the voting result to BB.

$$M = \Sigma_{i=1}^h m_i$$

3.3 Efficiency

The important problem in the application systems based on a mix-net scheme is the efficient proof and decryption methods. Sako and Killian [**?**] proposed cut and choose zero-knowledge proof. This scheme has not only problems of privacy, but also the high load of tallying [**?**, **?**]. Neff [**?**] proposed the polynomial scheme for more efficient proof of correct mixing. However, this scheme has an influence on the computational complexity by the number of mix-center. Jakobsson et al.[**?**] proposed randomized partial checking scheme, and Golle et al. [**?**] proposed optimistic mixing sheme. Table 1shows the computational costs of these systems. Although a mix-net scheme is efficient as an anonymous channel, due to the load of the correctness proof of mixing and decryption, the worth of a mix-net scheme has fallen. Maintaining the effect of the anonymity channel of a mix-net, these problems must be solved in order to use a mix-net scheme. The universal re-encryption mix-net of Golle et al. [**?**] can decrease the computation complexity by decryption. In order to de-crease the computation complexity by a proof of mixing, we use designated-verifier re-encryption proof. In this proof, each mix-center has only $2nk$ for the proof of his mixing like Table 1.

Table 1: Real cost per server (for a total of k servers) of mixing n items using different mixes.

Scheme	Re-encryption	Proof	Decryption
Cut and Choose ZKIP [**?**]	$2n$	$642nk$	$(2+4k)n$
Polynomial Scheme [**?**]	$2n$	$8n(2k-1)$	$(2+4k)n$
Randomized Partial Checking [**?**]	$2n$	$n/2(2k-1)$	$(2+4k)n$
Optimistic Mixing [**?**]	$6n$	$6+12k$	$(5+10k)n$
This paper	$2n$	nk	n

4 RFID System Using the universal re-encryption

4.1 Model of the system

We define a model in the RFID system using Universal Re-encryption based on ElGamal. The model consists of a RFID tag, a database, a reader, and an attacker. If the property of universal re-encryption is used in the case of re-encryption, then third party, such as a bank and a public institution, can process re-encryption procedure as a service. The components of the proposal system are shown below.

- **RFID tag**: A RFID tag emits an ID information (ciphertext C) in response to query from a reader. Its ID information (ciphertext C) is encrypted by universal re-encryption.
- **Database**: A database has private key x for ID information (ciphertext C) on a RFID tag, and the information on the item relevant to the RFID tag. Private key x is saved securely by an existing access control scheme. In addition, it is necessary

to use the existing authentication scheme for accessing this information. Moreover, this also performs calculation of re-encryption of ID information.

- **Reader**: This emits a query to a RFID tag and receives ID information (ciphertext C). And it re-encrypt the cipertext C by using universal re-encryption. Then, it updates the ID information of the RFID tag. Using universal re-encryption, if a reader for re-encryption saved ID information, it becomes difficult for tracing a RFID tag by semantic security when the next re-encryption is performed by another reader.

- **Attacker**: This tries to derive information from a RFID tag and to infringe on an owner's location privacy. Moreover, he alters the information on a RFID tag.

4.2 Protocol of the system

The protocol of Universal Re-encryption based on ElGamal is shown below.

- **Key generation**: Output secret key x and public key ($y = g^x$).

- **Encryption**: Ciphertext $C = [(\alpha_0, \beta_0); (\alpha_1, \beta_1)]$ is generated from the following formulas using message m, public key y, and random number $r = (k_0, k_1)$.

$$\begin{aligned} C &= [(\alpha_0, \beta_0); (\alpha_1, \beta_1)], \\ \alpha_0 &= my^{k_0}, \beta_0 = g^{k_0}, \alpha_1 = y^{k_1}, \beta = g^{k_1}. \end{aligned}$$

  Ciphertext C is written in a RFID tag.

- **Decryption**: A reader receives ciphertext C from a RFID tag, and sends to a database. A database calculates decryption algorithm described as follows.
  Compute $m_0 = \alpha_0/\beta_0^x$ and $m_1 = \alpha_1/\beta_1^x$ using ciphertext $C = [(\alpha_0, \beta_0); (\alpha_1, \beta_1)]$ under public key y from a RFID tag and secret key x. If $m_1 = 1$, then output message $m = m_0$. Otherwise the decryption fails, and a special symbol $\perp$ is output. A given key can be decrypted only under one given key.
  It will get a message m_0 as ID of the RFID tag. Even if ciphertext C is re-encrypted many times, it can return to plaintext by decryption once.

- **Re-encryption**: The reader derives ciphertext $C =$ $[(\alpha_0, \beta_0); (\alpha_1, \beta_1)]$ from a RFID tag. And the reader selects random number $r' = (k'_0, k'_1)$. And it generates new ciphertext C' by calculating the formula described as follow.

$$\begin{aligned} C' &= [(\alpha'_0, \beta'_0); (\alpha'_1, \beta'_1)] \\ &= [(\alpha_0\alpha_1^{k'_0}, \beta_0\beta_1^{k'_0}); (\alpha_1^{k'_1}, \beta_1^{k'_1})]. \end{aligned}$$

  Re-encrypted ciphertext C' is written in a RFID tag by the reader.

5 Security analysis

Here, we analyze security and privacy on our e-voting and RFID system. In section 3 and 4, we proposed simple e-voting system and RFID system based on the universal re-encryption public technique of Golle et al. When we compare e-voting system to RFID system, we can find the common points as follows.
- Votes and tag contents should arrive safely and surely at the destination.
- No one should know the relation between a voter and a vote, and between an IC tag and tag contents.
- The mix-centers should shuffle honestly the contents.
Also, we can find the similar roles by participants in two application systems as table 2. In table 2, there

Table 2: The roles of participants in e-voting system and RFID system.

	E-voting system	RFID system
Sender	Voters	IC tag
Receiver	Tallier	Database
Intermediaries	Mix-centers	Readers

are voters and IC tag such as a sender. The receivers are the tallier of e-voting and the database of RFID system. Also, mix-centers of e-voting system and readers of RFID system shuffle the data which are a vote and tag content. Then, it should keep the following conditions for secure e-voting and RFID system in viewpoints of confidentiality and untraceability. Here,

Table 3: Conditions for secure e-voting and RFID system.

	Mix-centers	Tallier	Readers	Database
Confidentiality	Yes	No	Yes	No
Untraceability	Yes	Yes	Yes	No

Table 4: Security evaluation.

	Mix-centers	Tallier	Readers	Database
Confidentiality	Yes	No	Yes	No
Untraceability	Yes	No	Yes	No

we analyze security and privacy on our e-voting and RFID system using the universal re-encryption public technique of Golle et al. For secure e-voting system and RFID system, it should be satisfied the conditions of table 3. For the intermediaries which are the mix-centers of e-voting system and readers of RFID system, it should be satisfied confidentiality and untraceability. Their roles are just to shuffle the received data. In case of the tallier, he should not have confidentiality, but untraceabiltiy for the counting of voting contents. But, in case of database of RFID system, she should not have confidentiality and untraceability, and saves safely the private key and computes the re-encrypted ID information. So, she should not have confidentiality and untraceabilty.

Internal anonymity VS. External anonymity
red The general mix-net schemes[**?**, **?**, **?**, **?**] satisfy the

inner anonymity in order to prevent an effluence of messages by a malicious mix-center. Although a mix-center proves his mixing, he can know a piece of messages, because he has a public key and a private key to encrypt and decrypt the message. The piece of messages can become proof to guess the original messages. As Golle et al pointed out that the universal re-encryption mix-net guarantees only external anonymity, this mix-net does not satisfy the inner anonymity. Since the message is encrypted under the receiver 's public key, the receiver can decrypt the encrypted message anytime and anywhere as well as trace a message intended for her throughout the mixing process. That is, it does not provide anonymity for senders with respect to the receiver. When this mix-net is applied to application systems such as e-voting system, RFID system and so on, if the receiver is a trust party, the privacy of a sender is guaranteed. In our e-voting system, if the tallier should not collude with other people or other participant, the voter 's privacy can be guaranteed and our e-voting system has the effective computational cost like table 1. Moreover, in the universal re-encryption mix-net, a malicious mix-center can not overflow a piece of votes, because he plays just a role of mixing and has not a public key and a private key.

6 Conclusion

Golle *et al.* proposed the universal re-encryption public technique. In this paper, we apply this universal re-encryption public technique to an e-voting system and a RFID system. Also, we analyze security and privacy of our e-voting system and RFID system based on the universal re-encryption public technique. The universal re-encryption public technique can support security and privacy for the secure RFID system. But, in case of the e-voting, tallier should to be the trusted third party. That is, the tallier should not collude with other people including participants. Also, the tallier should compute honestly the counting of voting contents. Under this condition, the universal re-encryption public technique can support efficiently for the secure e-voting system.

Acknowledgement

The research was partly supported by the Grant-in-Aid for Creative Scientific Research 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'.

References

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

[2] A. Juels and R. Pappu, *Squealing Euros: Privacy Protection in RFID Enabled Banknotes*, In R. Wright, editor, Financial Cryptography '03 Spring-Verlag, 2003.

[3] A. Juels,*Privacy and Authentication in Low-Cost RFID Tags*, In submission. 2003. http://www.rsasecurity.com/rsalabs/staff/bios/ajuels/index.html

[4] A. Juels, R. Rivest, and M. Szydlo, *The Blocker Tag: Selective Blocking of RFID Tags for Consumer Privacy*, In submission. 2003. http://www.rsasecurity.com/rsalabs/staff/bios/ajuels/index.html

[5] A.Neff, *A verifiable secret shuffle and its application to E-voting*, ACM CCS '01, pp.116-125, 2001.

[6] D.Chaum,*Untraceable electronic mail, return addresses, and digital pseudonyms*, In Communications of the ACM, pp84-88, 1981.

[7] D. McCullagh,*RFID tags: Big Brother in small pachkages*, CNet, 13 January 2003. Available at http://news.com.com/2010-1069-980325.html.

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

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

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

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

[12] M.Jakobsson, A.Juels and R.Rivest, *Making Mix Nets Robust for Electronic Voting By Randomized Partial Checking*, USENIX '02, 2002

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

[14] M.Jakobsson,*Flash Mixing*, PODC '99, 1999.

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

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

[17] P.Golle, M. Jakobsson, A.Juels and P.Syverson, *The universal re-encryption for Mix-nets*, CT-RSA 2004, LNCS 2964, pp163-178, 2004.

[18] P.Golle, S.Zhong, D.Boneh, M.Jakobsson and A.Juels, *Optimistic Mixing for Exit-Polls*, Asiacrypt2002, 2002.

[19] 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.

[20] S. A. Weis, S. Sarma, R. Rivest, and D. Engels,*Security and privacy aspects of low-cost radio frequency identification systems*, In First International Conference on Security in Pervasive Computing, 2003.

[21] S. E. Sarma, S. A. Weis, and D. W. Engels,*Radio-frequency-identification security risks and challenges*, Security Bytes, 6(1), 2003.

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