Enhancing Privacy of Universal Re-encryption Scheme for RFID Tags

Saito, Junichiro
Kyushu University

Ryou, Jae-Cheol
Division of Electrical and Computer Engineering

Sakurai, Kouichi
Kyushu University

出版情報：Proc. of Int. Conf. on Embedded and Ubiquitous Computing(EUC 2004). 1, pp.879-890, 2004-08. Springer
バージョン：
権利関係：

Enhancing privacy of Universal Re-encryption scheme for RFID tags

Junichiro SAITO[1], Jae-Cheol Ryou[2] and Kouichi SAKURAI[1]

[1] Kyushu University
6-10-1 Hakozaki, Higashi-ku, Fukuoka, 812-8581, Japan
saito@itslab.csce.kyushu-u.ac.jp
sakurai@csce.kyushu-u.ac.jp
[2] Division of Electrical and Computer Engineering
Chungnam National University
220 Gung-dong, Yuseong-gu, Daejeon, 305-764, Korea
jcryou@home.cnu.ac.kr

Abstract. A Radio-Frequency-Identification (RFID) tag is a small and cheap device which is combined in IC chip and an antenna for radio communications. It emits an ID in response to a query from a radio communication device called as a reader. For this reason, the RFID tag is used for management of goods and it is used as a substitute for a bar code. However, RFID system may infringe on a consumer's privacy because it has a strong tracing ability. Although ID of a RFID tag can be encrypted, it is possible to pursue an object by tracing specific information. Therefore, we discuss the privacy protection using universal re-encryption proposed by Golle, Jakobsson, Juels and Syverson. Since the system does not protect a modification of the information on RFID tags, it can be exploited by an attacker. Therefore we point out two attacks using modification of the information on RFID tags. Moreover, we offer two proposed schemes for addressing the problem.

1 Introduction

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 [1–5]. 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 paper [1, 6]. 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 open, so it is used for management of goods [1, 6]. 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 foodstuffs, and a closet will be able to offer a few of the enticing possibilities of its contents [1]. Moreover the European Central Bank (ECB) has proposed to embeded RFID tags in Euro banknotes [2]. By using identification combined ID on RFID tags and serial number printed on banknotes, it is expected to prevent forgery or money laundering.

1.1 Privacy problem

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 [4, 9]. 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 [4]. For this reason, there are some problems such as a retail store pursues a consumer and the circulation information on goods are revealed.

1.2 Related works

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 [5]. 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 [2]. 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 ciphertext from the re-encrypted ciphertext [7]. 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 the case of re-encryption. In that case, the attacker will be possible to trace the RFID tag relevant to the public key [7]. Although you may consider to make 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 results

In the paper, we discuss RFID system using Universal Re-encryption based on ElGamal proposed by Golle et al [7]. By using Universal Re-encryption, we can re-encrypt ciphertext without knowledge of a public key [7]. This property is suitable for RFID system. However, since the system can not protect a modification of the information on RFID tags, it can be exploited by an attacker. According to [7], an attacker may alter the information on RFID tags to the contents which cancel re-encryption. Moreover, we point out that an attacker may alter the information to the ciphertext encrypted by the attacker's public key.

To avoid these attacks, we propose two schemes. One is the Re-encryption protocol with a check. This scheme checks the information written in a RFID tag. The proposed scheme prevents infringement of the location privacy by the modification of the information on a RFID tag.

Next, we propose the re-encryption protocol using a one-time pad for anonymity in RFID tags. In order to prevent modification of the information on RFID tags, we introduce the simple access control using hash function. Moreover, the protection capability from infringement of location privacy can be effective because a RFID tag re-encrypt its ID information by using a one-time pad. Moreover, a reader updates a one-time pad on a RFID tag in order to prevent from spoiling its effect.

Furthermore, we discuss the security of our methods from a viewpoint of privacy protection.

2 RFID system using Universal Re-encryption

2.1 Universal Re-encryption

Unlike the usual re-encryption scheme, Universal Re-encryption does not need knowledge of a public key in the case of re-encryption, but re-encryption is performed by determining a random number. Moreover, re-encryption does not need the information about plaintext unlike encryption. The ciphertext which was processed re-encryption repeatedly can be once decrypted to the original plaintext using the private key.

Furthermore, universal re-encryption has semantic secrecy required for the privacy protection [7]. This property is fulfilled in the case of processing of re-encryption, and it means that the information about the original ciphertext isn't leaked at all from the re-encrypted ciphertext. These properties are effective in privacy protection of RFID tags [7].

2.2 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 for reading ID information, a reader for re-encryption, and an attacker. The owner always possesses the reader which can process re-encryption. Moreover, if the property of universal re-encryption is used in the case of re-encryption, then trusted third party, such as a bank and a public institution, can process re-encryption procedure as a service [7]. 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 for reading ID information**: This emits a query to a RFID tag and receives ID information (ciphertext C). Then, it asks to a database by an existing authentication scheme, and acquires the information about the item in which the RFID tag was attached. And it offers service, a function, etc. based on the ID information.
- **Reader for re-encryption**: This emits a query to a RFID tag and receives ID information (ciphertext C). It is asked to a database by an existing authentication scheme, and receives new ciphertext C'. 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 [7].
- **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.

2.3 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 $r = (k_0, k_1)$.

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

  Ciphertext C is written in a RFID tag.

– **Decryption**: The reader for reading ID information receives ciphertext C from a RFID tag, and sends to a database. A database calculates decryption algorithm described as follow.

> 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. And a database searches the information on a RFID tag using its ID, and transmits it to the reader for reading ID information.

– **Re-encryption**: The reader for re-encryption derives ciphertext $C = [(\alpha_0, \beta_0); (\alpha_1, \beta_1)]$ from a RFID tag, and sends it to a database. A database selects random number $r' = (k_0', k_1')$. And a database 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 reader for re-encryption.

3 Security analysis

In the RFID system using universal re-encryption, since the RFID tag can be written by an attacker, he can exploit it using a reader which can rewrite the contents of a RFID tag. Golle et al. pointed out that an attacker may alter the information on RFID tags to the contents which cancel re-encryption. Moreover, we introduce that an attacker may alter the information on RFID tags to the ciphertext encrypted by the attacker's public key. We show two attacks exploiting these problems.

– **attack (1)**: The contents of a RFID tag are rewritten to the ciphertext C_A encrypted by the attacker's public key $y_A = {g_A}^{x_A}$.

$$\begin{aligned} C_A &= [(\alpha_0, \beta_0); (\alpha_1, \beta_1)] \\ &= [(m_A y_A, g_A); (y_A, g_A)]. \end{aligned}$$

A trusted third party re-encrypts the ciphertext C_A to the new ciphertext ${C_A}'$ using random number $r = (k_0, k_1)$.

$$
\begin{aligned}
{C_A}' &= [(\alpha_0 \alpha_1^{k_0}, \beta_0 \beta_1^{k_0}); (\alpha_1^{k_1}, \beta_1^{k_1})] \\
&= [(m_A {y_A}^{k_0}, {g_A}^{k_0}); ({y_A}^{k_1}, {g_A}^{k_1})].
\end{aligned}
$$

Even if re-encryption is performed, the attacker can decrypt the new ciphertext ${C_A}'$ using the attacker's private key x_A.

$$
\begin{aligned}
m &= \alpha_0 \alpha_1^{k_0} / (\beta_0 \beta_1^{k_0})^{x_A} \\
&= m_A {y_A}^{k_0} / ({g_A}^{k_0})^{x_A} \\
&= m_A.
\end{aligned}
$$

– **attack (2)**: When rewritten by the contents which cancels re-encryption, an attacker may rewrite the ciphertext C to the new ciphertext like $C_A = [(\alpha_0, \beta_0); (\alpha_1, \beta_1)] = [(\alpha_0', \beta_0'); (1, 1)]$ described in [7]. Even if it re-encrypt the ciphertext C_A to the new ciphertext ${C_A}'$ using random number $r = (k_0', k_1')$, the new ciphertext ${C_A}'$ do not change as follow.

$$
\begin{aligned}
{C_A}' &= [(\alpha_0 \alpha_1^{k_0'}, \beta_0 \beta_1^{k_0'}); (\alpha_1^{k_1'}, \beta_1^{k_1'})] \\
&= [(\alpha_0, \beta_0); (\alpha_1, \beta_1)] \\
&= C_A.
\end{aligned}
$$

Such attacks pass through the key check of a cryptosystem. In addition, the key check is performed as follows.

$$
m_1 = \alpha_1 / \beta_1^x.
$$

When m_1 is 1, it passes the key check. There is the following in the value which passes along this check.

1. If $\alpha_1 = y^r$ and $\beta_1 = g^r$, then $y = g^x$
2. $\alpha_1 = \beta_1 = 1$
3. If x is even, then $(\alpha_1, \beta_1) = (1, -1)$
4. If x is odd, then $(\alpha_1, \beta_1) = (-1, -1)$

In the case of 2 to 4, a ciphertext does not change, or since a ciphertext changes regularly, it is used for an attack.

By the attack (1), since an attacker can decrypt the information on a RFID tag, he can trace a specific RFID tag by pursuing the information which he can decrypt. Moreover, by the attack (2), since it does not change even if the information on a RFID tag is re-encrypted, an attacker can trace it.

4 Our proposed schemes

We offer two schemes for addressing the concerns of the attacks described above.

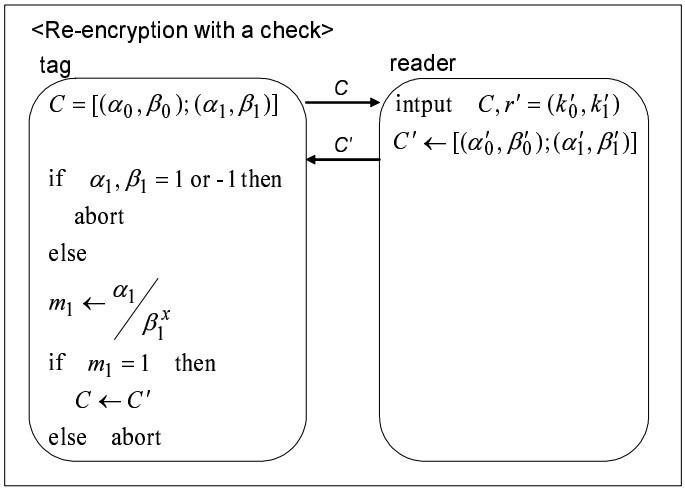

Fig. 1. Re-encryption with a check

4.1 Re-encryption protocol with a check

In order to solve the modification problem which is explained in Section 3, we propose the re-encryption protocol with a check which checks the contents by a RFID tag when re-encryption is performed. In our scheme, authentication of a reader is not performed. But a part of decryption procedure is performed by a RFID tag for checking the contents of the information sent from a reader in the case of re-encryption. Therefore, a RFID tag possesses the private key x. In our system, the model and other algorithms is the same as the section 2.

Protocol. Our protocol is described as follows. A RFID tag performs the following procedure after the re-encryption in the subsection 2.3.

- **Check of re-encryption**: A RFID tag receives new ID information (Re-encrypted ciphertext) $C = [(\alpha'_0, \beta'_0); (\alpha'_1, \beta'_1)]$. If α'_1 or β'_1 is 1 or -1, the re-encryption fails, and the contents of a RFID tag does not change. Compute $m_1 = \alpha'_1 / \beta'^x_1$, if $m_1 = 1$, then rewrite the contents of a RFID tag to C.

The protocol of the re-encryption with this scheme is shown in Fig. 1. When the check of re-encryption has gone wrong, the information on a RFID tag does not change.

In our scheme, the attack (2) is prevented by checking whether α'_1 or β'_1 is 1. Next, the contents of α' and β' which is the information about the key of encryption are checked using a private key. In other words, it is checked whether the ciphertext encrypted by the public key $y = g^x$. Thereby, the attack (1) can be prevented.

Analysis of the proposed scheme. Only the contents written in the scheme are checked instead of authentication of a reader. Therefore, the contents cannot be altered although an attacker can derive the information on a RFID tag. Since the information is encrypted, the attacker can not understand it. Moreover, since this scheme checks some contents written in, it can suppress the calculation by a RFID tag.

However, only the portion which is not checked may be altered. If the contents of a RFID tag are altered, the function of our scheme will be spoiled. The following is a change of the information on the RFID tag at the time of an attack to the scheme. Let $C = [(\alpha_0, \beta_0); (\alpha_1, \beta_1)]$ be a ciphertext in the RFID tag.

- **Attack against our scheme**: An attacker derives the ciphertext $C = [(\alpha_0, \beta_0); (\alpha_1, \beta_1)]$, following ciphertext C_A is written in the RFID tag using message m_A which the attacker set up.

$$\begin{aligned} C_A &= [(\alpha'_0, \beta'_0); (\alpha'_1, \beta'_1)] \\ &= [(m_A, m_A); (\alpha_A, \beta_A)]. \end{aligned}$$

  Since (α_A, β_A) of this ciphertext C_A is (α_1, β_1) itself received from the RFID tag or the contents processed the suitable re-encryption procedure, this writing cannot be prevented by our scheme.
- **Re-encryption by a trusted third party**: A trusted third party get a ciphertext $C = [(\alpha_0, \beta_0); (\alpha_1, \beta_1)] = [(m_A, m_A); (\alpha_A, \beta_A)]$. Compute C' using random number $r' = (k'_0, k'_1)$ and ciphertext C, and write it to a RFID tag.

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

  The ciphertext C' cannot be decrypted without the private key x.

Since the information on a RFID tag differs from the original contents, the identification ability of a RFID system will be spoiled. However, it is impossible for an attacker to decrypt re-encrypted ciphertext C', so he cannot trace the specific RFID tag by the semantic security of Universal Re-encryption. Therefore, location privacy is protected.

4.2 Re-encryption protocol using a one-time pad

We introduce the Re-encryption protocol using a one-time pad. In the RFID system using this scheme, it prevents revealing ID information of a RFID tag by encryption, and the information on a RFID tag is changed by using Universal Re-encryption, so location privacy is protected. Moreover, it is possible to change ID frequently by using the memory called one-time pad in a RFID tag. A RFID

tag changes its ID information using one-time pad. The one-time pad is renewed by a reader for updating one-time pad. Therefore, a RFID tag does not pay the calculation cost of generating the one-time pad.

Model of the scheme. In the system, it is necessary to classify a reader. The components of the system are shown below.

- **RFID tag**: A RFID tag saves a one-time pad Δ for changing ID information, ID information which are encrypted (ciphertext C), secret information S, and session number i. A RFID tag transmits ID information to a query from a reader. Re-encryption of ID information is performed by Universal Re-encryption. Moreover, it authenticates a reader by access key X using the Hash Function at the time of updating a one-time pad. A RFID tag saves secret information S and session number i, and access key X is generated by hash value $X = h(S, i, \Delta)$. A RFID tag possesses Hash Function h at this time.
- **Database**: A database has private key x for ID information (ciphertext C) on a RFID tag, the information on the item relevant to the RFID tag, ID information, access key $X = h(S, i, \Delta)$ for updating one time pad and Hash Function h. Secret information S of the access key for updating a one-time pad and session number i are saved securely by an existing access control scheme. Moreover, it is necessary to use an existing authentication scheme for accessing them.
- **Reader for reading ID information**: This emits a query to a RFID tag and receives ID information (ciphertext C). Then, it asks to a database by an existing authentication scheme, and obtains the information about the item to which the RFID tag is attached. And it offers a service, a function and etc. based on the ID information.
- **Reader for updating a one-time pad**: This emits a query to a RFID tag and receives ID information (ciphertext C). It asks to a database by an existing authentication scheme, and receives access key X and new one-time pad Δ'. Then, it updates the one-time pad of the RFID tag. Using Universal Re-encryption, if a reader for updating a one-time pad saves ID information and the value of a one-time pad, it becomes difficult to trace a RFID tag by semantic security when the next re-encryption is performed by another reader [7]. However, the reader for updating a one-time pad has to process updating a one-time pad correctly.

Unlike the existing system, our scheme has two readers because of the difference in the degree of secrecy of the information to treat.

Protocol. Our scheme follows the following procedures. And the procedure of key generation, encryption and decryption are the same as the RFID system using Universal Re-encryption in section 2.3. Then a database saves the secret key x generated by key generation.

– **Generate one-time pad**: A database generates a one-time pad Δ from ciphertext C of a RFID tag and random number $r = (l_1, ..., l_{2n})$.

$$\Delta = [({\alpha_1}^{l_1}, {\beta_1}^{l_1}), ..., ({\alpha_1}^{l_{2n}}, {\beta_1}^{l_{2n}})].$$

In the state of the first stage, the one-time pad Δ and ciphertext C are written in a RFID tag by a reader. After that, a one-time pad is updated by the reader for updating a one-time pad.

– **Re-encryption**: Whenever a RFID tag emits ID information to the query from a reader, it re-encrypts ciphertext C. In that case, a RFID tag choose 2 sets of element $[({\alpha_1}^{l_k}, {\beta_1}^{l_k}), ({\alpha_1}^{l_{k+1}}, {\beta_1}^{l_{k+1}})](k = 1, 2, ..., n)$ from one time pad Δ. And the RFID tag obtains new ciphertext C' re-encrypted by the following calculation.

$$\begin{aligned} C' &= [(\alpha'_0, \beta'_0); (\alpha'_1, \beta'_1)] \\ &= [(\alpha_0 \alpha_1^{l_k}, \beta_0 \beta_1^{l_k}); (\alpha_1 \alpha_1^{l_{k+1}}, \beta_1 \beta_1^{l_{k+1}})]. \end{aligned}$$

Since the element of a one time pad is a $2 * n$ set, re-encryption is possible n times. After carrying out n times re-encryption, the element of the one-time pad will be reused. Thereby, although the security by re-encryption will be spoiled, this is avoided by updating the one-time pad shown below.

– **Update one-time pad**: The reader for updating a one-time pad emits a query to a RFID tag, and gets ciphertext C. It sends ciphertext C to a database and requires the new one-time pad for updating. By decrypting ciphertext C, a database searches secret information S. And according to the generation procedure of a one-time pad, a database generates new one-time pad Δ' using ciphertext C. Access key $X = h(S, i, \Delta')$ is generated from new one-time pad Δ', secret information S and session number i. The reader for updating a one-time pad receives one-time pad Δ' and access key X, and transmits to a RFID tag. The RFID tag calculates access key $X = h(S, i, \Delta')$ by the same calculation as a database. If the access key X accords with the received access key, the RFID tag updates a one-time pad and saves next session number $i' = i + 1$.

About the case where ID information is drawn out by the reader for reading ID information and the reader for updating a one-time pad, the situation of each communication is shown in Fig. 2.

Analysis of the proposed scheme. In the scheme, the RFID tag performs multiplication on ElGamal and calculation of a hash value. Moreover, it is possible to apply flexibly by changing the size of a one-time pad according to the capacity of a RFID tag. The contents written with a reader are authenticated using a Hash Function. Therefore, the modification of the information on the RFID tag by the attacker can be prevented. Moreover, since the scheme has

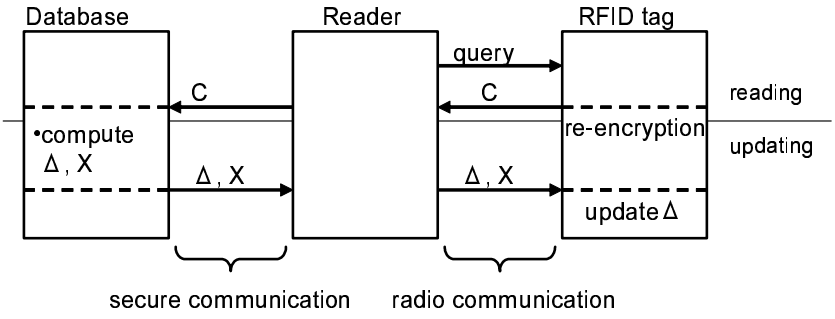

Fig. 2. communication with a reader

high anonymity, it has high protection capability to infringement of the location privacy by long-term tracing of a RFID tag and short-term tracing.

However, since secret information is centralized on the database, its employment and management become important. Furthermore, in order to request updating a one-time pad for a third party, they have to fulfill the character stated by the model of the system. Moreover, detecting modification of a RFID tag is possible although it cannot protect to the alteration of the one time pad in the tampering of a RFID tag.

4.3 Comparison

We propose two schemes for addressing the problems in Universal Re-encryption. Re-encryption protocol with a check can check a modification of the information on a RFID tag. However, since it checks a part of contents, an attacker can alter the other contents. Moreover, the calculation cost of RFID tags is too much. On the other hand, in the Re-encryption protocol using a one-time pad, the calculation cost of RFID tags is reduced by performing some calculations by a database. But restrictions of its model are more severe. That is, since a database authenticates a reader in the case of updating a one-time pad, a reader must update it in the right procedure.

Our proposed schemes are well adapt to management of goods for consumers. If a consumer has a closet which can read RFID tags, it will be able to offer a few of the enticing possibilities of its contents. Moreover, if the closet can update RFID tags, whenever clothes are stored in the closet, the content of the RFID tag attached to the clothes is changed. So he don't need to worry about infringement of location privacy.

You may consider a private key is shared and symmetric key cryptosystem is used. In this case, although a ciphertext is made to change using a random number etc., it is necessary to take synchronization for the value between databases. Since our proposal uses Universal Re-encryption, it can decrypt ciphertext to

plaintext at once without taking synchronization. Therefore, it is possible to reduce the cost of processing on database.

Moreover, it is necessary to manage the private key of each RFID tag safely in a database by the method using the symmetric key cryptosystem. However, by our proposal system using Universal Re-encryption, a database should manage only one private key safely. Therefore, management cost can also be reduced.

5 Conclusion

In this paper, we point out the problems of RFID system using Universal Re-encryption. Moreover, we propose two schemes for addressing them. As a future work, we will evaluate and compare the cost of implementation of our proposed schemes.

6 Acknowledgments

This work was done during the Core University Program on Next Generation Internet between Kyushu University and Chungnam National University supported by Japan Society for the Promotion of Science and by Korea Science and Engineering Foundation. The second author was supported in part by ITRC program of the Ministry of Information and Communication, Korea. And we would like to thank Kenji Imamoto for many useful discussions.

References

1. A. Juels. Privacy and Authentication in Low-Cost RFID Tags. In submission. 2003. http://www.rsasecurity.com/rsalabs/staff/bios/ajuels/index.html
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. S. E. Sarma, S. A. Weis, and D. W. Engels. RFID systems, security and privacy implications. Technical Report MIT-AUTO-WH-014, AutoID Center, MIT, 2002.
4. S. E. Sarma, S. A. Weis, and D. W. Engels. Radio-frequency-identification security risks and challenges. *Security Bytes*, 6(1), 2003.
5. 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. To appear. http://citeseer.nj.nec.com/weis03security.html
6. 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
7. P. Golle, M. Jakobsson, A. Juels, and P. Syverson. Universal re-encryption for mixnets, To be presented at RSA 2004, Cryptographer's Track. http://crypto.stanford.edu/~pgolle/
8. Finkerseller. K, "RFID Handbook",Carl Hanser Verlag Munchen, September 2002.
9. D. McCullagh. RFID tags: Big Brother in small pachkages. *CNet*, 13 January 2003. Available at http://news.com.com/2010-1069-980325.html.