MARP: Mobile Agent for RFID Privacy Protection

Soo-Cheol Kim, Sang-Soo Yeo, and Sung Kwon Kim

Chung-Ang University,
221 Huk-Suk-dong, Dong-Jak-gu, Seoul, Korea
{sckim, ssyeo}@alg.cse.cau.ac.kr
skkim@cau.ac.kr

Abstract. Recently many researchers in various fields has noticed RFID system. RFID system has many advantages more than other automatic identification system. However, it has some consumer privacy problems, such as location tracking and disclosure of personal information. Most of related works have focused on the cryptographic scheme for the RFID tag and the reader. In this paper, a proxy agent scheme using personal mobile device for the privacy protection. Our MARP, mobile agent for RFID privacy protection, has strong cryptographic modules with a powerful CPU and battery system and guarantees more high-level security than other protection schemes. MARP acquires a tag's secrete information partially and becomes the proxy agent of the tag which is in its sleep mode. All readers can communicate with MARP instead of the tag and can attempt authentication with MARP. Since the tag should have only one hash module in the environment of MARP, we can use the existing tag hardware with slight modification for protection consumer's privacy in RFID system.

1 Introduction

RFID(Radio Frequency Identification) system, which uses radio frequency for contactless communications, is considered as an extended one of smart card system. RFID system differs form smart card system in manufacturing cost, application field and transmission distance. Generally a smart card has security key, biometrics, financial account information or traffic ticket values and its cost may be several dollars [1]. On the other hand, an RFID tag is embedded in every good in a market and it costs a few dimes. Moreover, an RFID tag can be recognized omnidirectionally by interrogators in a few meters.

In this paper, we address RFID system and its privacy problems. As we mentioned above, RFID is a technology that automatically identifies an object by reading the information stored in an RFID tag in a contactless method using radio frequency. The information is stored in an RFID tag, composed of an antenna and an IC chip, which is then attached to the object to be identified. The information is recognized through an RFID reader. It is expected that RFID system will replace the barcode system in the near future and help in drastic innovation of logistics and distribution industries [1, 2, 3, 4].

J. Domingo-Ferrer, J. Posegga, and D. Schreckling (Eds.): CARDIS 2006, LNCS 3928, pp. 300–312, 2006.

However, the fact that the RFID system allows the wireless data communication without physical contact raises a new issue. Currently, an RFID tag responds to any reader. That means anyone with a reader can read the information in the tag, potentially violating the privacy of the owner of the object with the RFID tag [5]. The privacy violation problem can be viewed in terms of information leak and location tracking.

First, information leakage deals with the fact that the direct identification information of the unique ID of the tag can be transmitted to anyone and everyone with the reader. Since a personal object can reflect the owner's life style, income level, consumption inclination and physical condition, violation of privacy due to tag information leakage should be considered significant [6].

Second, the location tracking is the problem caused by the tags always sending the same information. That can be used by the adversary with illicit purpose to track the location of the specific tag owner. It is like embedding a cheap positioning system to a tag. Of course, tracking the location or moving path of the tag owner without the approval would be serious privacy violation [7].

There have been many studies of the schemes to protect the privacy. The most simple and definite method is the *Kill command* [8]. Other methods include reader authentication using hash functions and protection of the user privacy using the *blocker tag* [9, 10]. *RFID Guardian* method using a specific device is similar to MARP in concept [11, 12]. However, all of the above mentioned method cannot completely protect the privacy [13].

We propose a new method that ensures high level privacy protection using a special mobile agent device. The concept of MARP is for a special mobile device to manage the tags and gather some of the information embedded in the tag to substitute its role. MARP can provide the high level cryptographic services that are unable in the low price tags.

The rest of the paper is organized as follows. Section 2 describes a few well-known RFID privacy protection methods. Section 3 describes the brief introduction of the RFID system and the required assumptions for the proposed scheme. Section 4 describes MARP in details, separated into the initial setup phase, the privacy protection phase and the authentication phase. And the main scheme using MARP is also explained. Section 5 describes the analysis for the proposed scheme. Section 6 presents the conclusions.

2 Related Work

The most extreme way to protect the privacy in RFID system is to destroy the RFID tag attached to an object or disable its functionality using the *Kill command*. The *Kill command* is a basic function included in all EPC tags [4, 7, 8]. The tag function is removed by entering a special secret code value (PIN) to prevent tag information leakage and tracking. Although it is the simplest and surest way to protect the privacy, it is not a recommended approach since it also loses all the potential advantages for using the RFID system.

Weis proposed the hash based metaID method [7]. Tag can be either in locked or unlocked mode, and only the authenticated reader can unlock a tag. When

a tag is in the locked mode, all functions except transmission of the metaID of the tag are disabled. The metaID based method allows identification of a unique ID only by the authenticated reader. However, it does not solve the problem of location tracking since a tag in locked mode always transmits the same metaID value. Weis proposed another scheme, "Randomize hash-lock" in [7]. In this scheme, the tag has a hash function and a PRNG(pseudo-random number generator). This scheme satisfies indistinguishability, but has some security holes in reader-tag communication and very heavy load in the back-end server [13, 14].

Juels proposed the *"blocker tag"* method [9, 10]. The *blocker tag* method uses a type of defense shield to protect the tag. The *blocker tag* always responds in both 0 and 1 to the reader inquiry. Therefore it hides its existence and forces the reader to give up trying to recognize the tag. The privacy is protected by preventing the reader to recognize the tag ID through a type of interference. However, the blocker tag presents the risk of being misused, and selective blocking is not possible.

Golle proposed a scheme using re-encryption [15]. In this scheme, the Reader and the tag have to compute ElGamal public key cipher. And the tag must be re-encrypted very Frequently. However, this scheme can be attacked through various security vulnerability.

There are other methods of arbitrating the communication between the reader and tag using the mobile device [11, 12, 16, 17]. This device protects the privacy with high capacity memory and calculation capability. The device mainly has four functions: 1) monitoring of the new tag or reader, 2) managing the key on behalf of the tag, 3) controlling the access by the tag or reader, and 4) authenticating if the reader is legitimate on behalf of the tag.

3 The RFID System for MARP

An RFID system generally consists of RFID tag, RFID reader and back-end server. For the proposed system in this paper, there is additional personal privacy protection agent (MARP) that arbitrates the communication between the reader and tag, and the trusted public key management center. Fig.1 shows that the RFID system for MARP.

- **RFID Tag** *Transponder* — A tag is attached to a certain object with its unique identification. In general, it consists of the IC chip and antenna. When the reader sends an inquiry, the tag responds with its own internal data or the result of calculation using the data. An RFID tag can be either an active tag or passive tag. The passive tag, which has not own battery for reducing the manufacturing cost, receivers reader's query through radio signal and sends its answer to reader using harvested energy from the electromagnetic field of the reader's radio signal. The system proposed in this study assumes a hash enabled passive tag.
- **RFID Reader** *Transceiver*— A reader is the device that transmits RF signal to the tag and receive the response from the tag. Its role is to send an inquiry

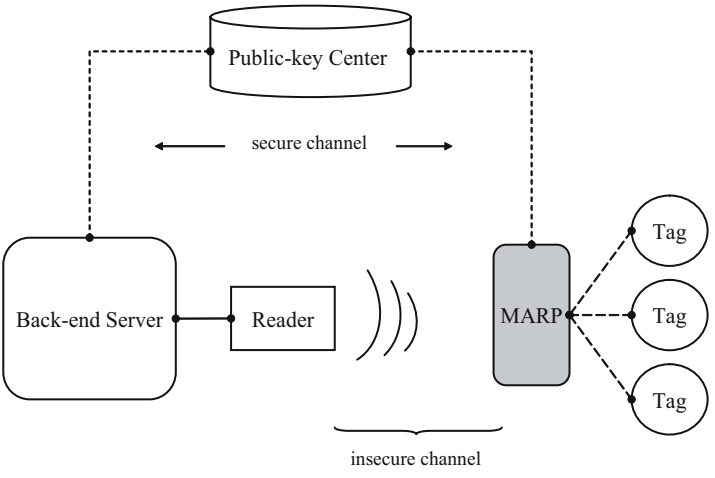

Fig. 1. The RFID system for MARP

to the tag, receive the data from the tag and then identifies it using its own subsystem or external back-end system. For this study, the readers are assumed to be in a certain group [18] and contain the group ID as well as the group individual key and public key. In the proposed scheme, the access authority to the tags is classified by the group ID.

- **Reader Subsystem** — The data processing subsystem is attached to the reader and retrieves appropriate information from its own database or external database server according to the data obtained by the reader. Generally, the data processing subsystem is considered as a pard of reader.
- **Back-end Server** — The back-end server is a server system that processes the tag related data sent by the reader. The back-end server has the tag related information in a database. The answer of the tag is transmitted securely to the back-end server through authenticated reader and it is used to identify the tag. The back-end server must be trusted and must have the capability to process every query from a lot of readers concurrently.
- **MARP** *(Mobile Agent for RFID Privacy Protection)* — This is the key part of the proposed scheme. MARP is a compact battery-powered mobile device, such as Personal Digital Assistants (PDA) or cellular phones. It has the role of gathering the secret information of tag and functioning on behalf of the tag. In this study, each MARP has the individual key and public key. It is also assumed that the reader can easily differentiate tag from MARP.
- **Trusted Public-key Center** — MARP scheme utilizes authentication using the public key. Since each reader group and MARP has the public key pair, a trusted third party public key distribution center is needed to manage them.

4 Mobile Agent for RFID Privacy Protection

This section describes MARP scheme proposed in this study. MARP is a mobile device with high performance capability, memory and high calculation capability. An RFID user will carry around MARP to register the tags to MARP and then use it to represent the tags.

The key to MARP is to secure some of the tag's secret information and use it to authenticate the tag. MARP registers all user tags, record them in the database and perform the mutual authentication to provide the tag information appropriate for the reader class.

4.1 Term Definition

- $h()$: the one-way hash function algorithm.
- Uid_t : the unique identifier of the tag t.
- Key_t : the secrete value of the tag t.
- PIN_t : mode change key of the tag t.
- Rid_g : identifier of reader group g.
- K_d^g : private key of reader group g.
- K_e^g : public key of reader group g .
- K_d^m : private key of MARP m.
- K_e^m : public key of MARP m.
- $\|$: concatenation.
- $\oplus$: exclusive-OR.

4.2 Initial Setup Phase

Before performing MARP scheme, there is certain preparation needed. Each tag must contain the PIN_t. Only those MARP having the key can register the tag and toggles it between sleep and wake modes. If a store has the tagged items for sale, the store DB will contain PIN_t of each tagged item. After the item is sold, PIN_t will be transferred to MARP of the buyer who registers the item.

A reader is assigned with a specific group ID. It has the authority to read the tag only with the group ID. It is a type of classification. For an example, when scanning the tags for the purpose of advertising similar to spam mail, the

Table 1. Data states in the RFID system for MARP

Back-end Server	Reader	MARP	Tag
Uid_t Key_t	Rid_g K_d^g K_e^g	K_d^m K_e^m	Uid_t Key_t PIN_t
Rid_g		Rid_g K_e^g	
K_d^g K_e^m		Uid_t $h(Key_t)$ PIN_t	

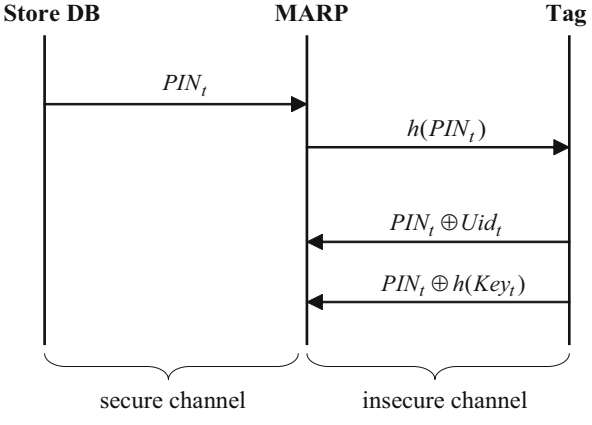

Fig. 2. Initial setup phase

legal regulation may force the reader to have the group ID such as SPAM. Then the users who do not want the spam scan will prevent access by the SPAM group readers. With the group ID and the group public key, readers can also be authenticated for their legitimacy.

For secure communication, MARP also has the individual ID and public key. Therefore, a trusted public key distribution center is needed to manage the public keys. Each MARP contains the reader group ID's it manages and can attain the reader group public key through the public key distribution center.

In terms of the data for each RFID system component, the server contains the tag related information (tag ID, secret data, and PIN_t) and reader group related information (reader group ID and reader group public key). It can also attain MARP public key through the trusted public key authentication center. The reader must contain its own group ID, public key and individual key. MARP contains its own information (public key and individual key) as well as the information of the reader group (ID and public key) with the access authority. It must also contain the information (ID, hashed secret data and PIN_t) of the

tags it controls. The tag contains its own ID, secret data and PIN_t. Table 1 shows that the data states in proposed RFID system MARP fist needs to gather tag's secret data before it represents a tag. When a tagged item is purchased at a store, the PIN_t of the tag will be transferred to MARP which gathers the tag data and puts the tag in sleep mode using the PIN_t. Collecting the secret data of the tag is simple. The hashed PIN_t is sent to the tag in a short distance. (It is assumed that the tag can be registered only within a short distance for security purpose.) The tag confirms validity of the information and then sends its secret data (ID and hashed secret key) by first XORing with PIN_t. The data transmission is secure since wiretapping the data alone cannot decode the secret tag information. Fig.2 shows that the tag registration protocol in the proposed system.

Detailed Protocol.

1. Store DB send PIN_t to MARP.
   - Store DB $\longrightarrow$ MARP : PIN_t.
2. The hashed PIN_t is sent to the tag in as short distance.
   - MARP $\longrightarrow$ Tag : $h(PIN_t)$.
3. The tag confirms validity of the information and then sends its secret data (ID and hashed secret key) by first XORing with PIN_t.
   - Tag : computes PIN_t from received $h(PIN_t)$.
   - Tag : authenticates MARP.
   - Tag $\longrightarrow$ MARP: $PIN_t \oplus Uid_t$, $PIN_t \oplus h(Key_t)$.

4.3 Privacy Protect Phase(Tag Sleep Mode)

Once the secret information of the tag is stored in MARP, the tag is put into sleep mode. This mode allows MARP to act on behalf of the tag and is the most typical mode of the proposed scheme. In this mode, data communication occurs only between MARP and the reader. The mutual authentication process consists of 5 steps, and the procedure and communication protocol of each step is as follows(Fig.3):

Detailed Protocol.

1. The reader sends an inquiry along with the group ID and a random number which are signed by the reader group individual key to MARP.
   - Reader $\longrightarrow$ MARP : $Query \parallel E_{K_d^g}(Rid_g \parallel R_r)$.

2. MARP checks the signature to identify the reader group ID before generating another random number. Both random numbers are signed with its own individual key and encrypted with the reader group public key then securely sent to the reader.
   - MARP : checks the signature to identify the reader group ID.
   - MARP : generate random number. R_m.
   - MARP $\longrightarrow$ Reader : $a_1 = E_{K_e^m}(E_{K_d^g}(R_r \parallel R_m)$.

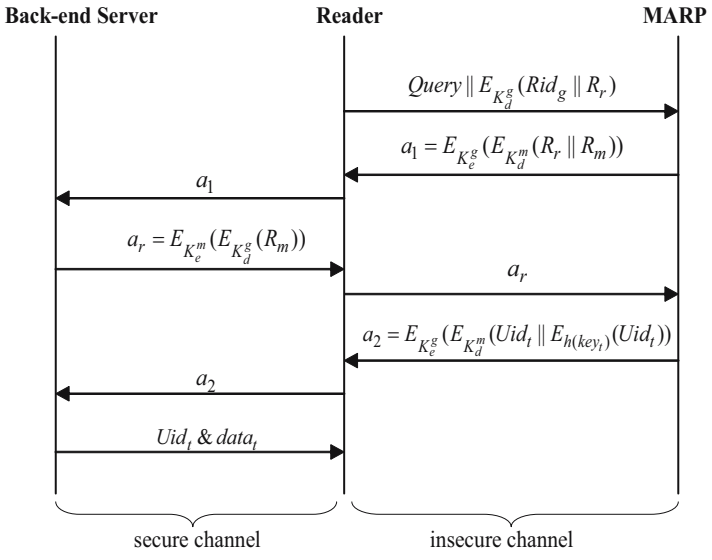

Fig. 3. Privacy protection phase

3. The reader transmits the received information to the server. The server checks the signature to attain MARP ID. After that, the server signs the random number sent by MARP with its own individual key, encrypts it with MARP public key and re-sends it.
   - Reader ⟶ Server : a_1.
   - Server : checks the signature to attain MARP ID and R_m.
   - Server → Reader → MARP : $a_r = E_{K_e^m}(E_{K_d^g}(R_m))$.
4. Once MARP receives the information from the reader and confirms it, the mutual authentication is completed. After that, MARP only transfers the approved tag data using the keys on the device.
   - MARP : confirms information, the mutual authentication is completed.
   - MARP → Reader → Server : $a_2 = E_{K_e^g}(E_{K_d^m}(Uid_t \| E_{h(key_t)}(Uid_t))$.
5. The server decrypts the received information and transfers the concerned information to the reader.
   - Server : decrypts the received information.
   - Server ⟶ Reader: Uid_t & $data_t$.

4.4 Authentication Phase(Tag Wake Mode)

This mode is used for the certain cases which require inspection of the illicitly altered tag by MARP. If the tag is to transfer the raw secret data to MARP, its counterfeiting or alteration can be done very easily. A canceled tag may act as if it has the secret information or sends the information of another tag. Therefore, the data is hashed with a simple scheme. To verify the tag, the tag authentication using the tag's secret data all it's needed. The tag validation protocol consists of three steps as follows(Fig.4):

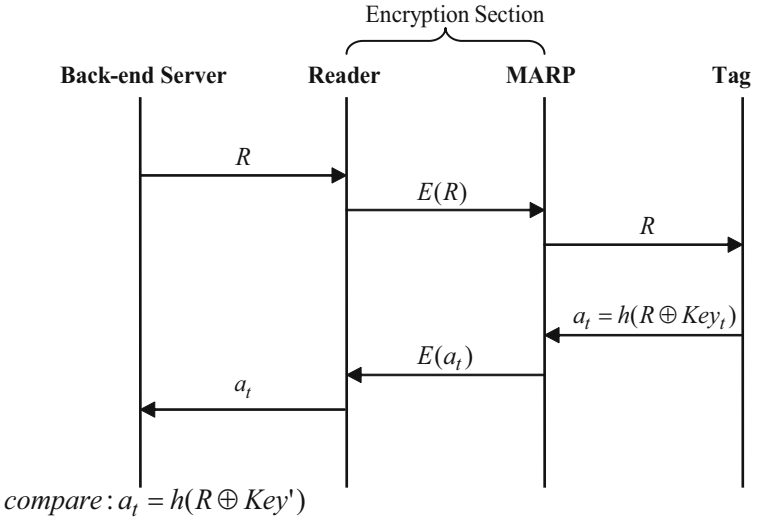

Fig. 4. Authentication phase

Detailed Protocol.

1. The server generates a random number and sends it to MARP which puts the tag in wake mode and sends the random number to it using PIN_t.
   - Server : generates a random number.
   - Server → Reader → MARP: $E_{K_d^g}(R)$.
   - MARP : puts the tag in wake mode to it using PIN_t.
   - Tag ⟶ MARP : R.
2. Awaken tag XOR's the received random number with its own secret data, hashes it and sends it to MARP. MARP transfers the received data to the server.
   - Tag → MARP → Reader → Server : $a_t = h(R \oplus Key_t)$.
3. The server compares the information from the tag with its own and authenticates the tag if they are in agreement.
   - Server : compares $a_t = h(R \oplus Key')$.
   - Server : authenticates Tag.

4.5 Main Scheme

Authentication between the tag and MARP, between MARP and reader, and between the server and tag are separately described above. It is now needed to consider each step collectively. The main scheme is not MARP acting on behalf of the tag using the sleep or wake mode. It is carried out in the shape of the tags being depended upon MARP. If the sleep mode of the tag is used, MARP can alter the tag at any time. Therefore, authentication step is needed time to time. However, what if the authentication step is carried out in each operation?

First of all, the tag should not react to any scan by the readers once it is affiliated with MARP. It may only communicate with MARP that know its

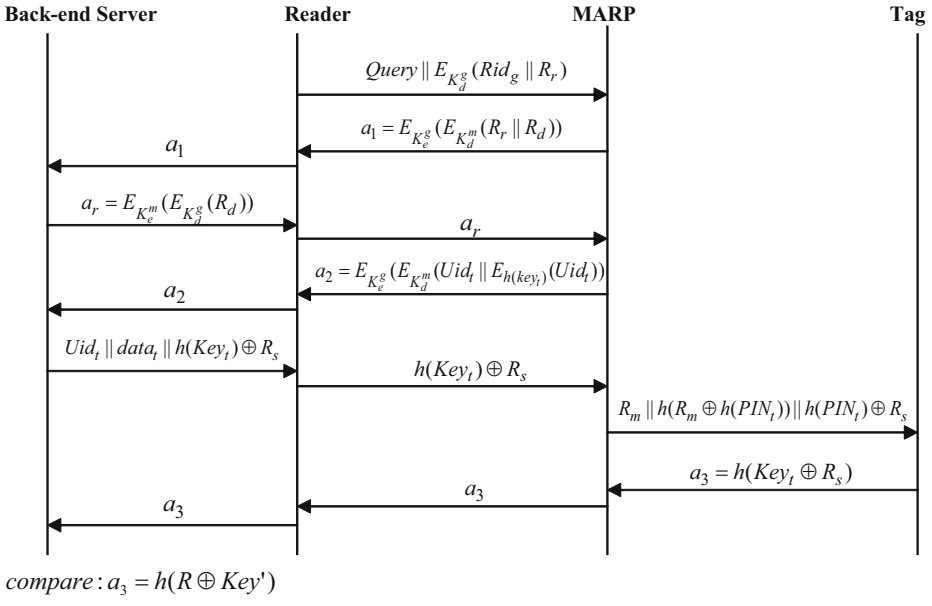

Fig. 5. Main scheme using MARP

PIN_t. It's a type of master-slave relation. Since the tag will not respond to an inquiry unless an accurate PIN_t is provided, it will not be recognized by any readers with the PIN_t. Employing that, authentication using the secret data can be requested to the tag for each communication.

There is some change as the authentication protocol is added at the later part of the above mentioned scheme. The server can calculate the tag ID and the related data by analyzing the data sent by MARP and send the information to the reader. Fig.5 shows the main scheme using MARP.

Detailed Protocol.

1. At the same time, the hashed secret data is XOR'ed with the random number R_s and sent.
   - Server $\longrightarrow$ Reader : $Uid_t \parallel data_t \parallel (Key_t) \oplus R_s$.
   - Reader $\longrightarrow$ MARP : $h(Key_t) \oplus R_s$.
2. MARP calculates R_s received from the server. It then XOR's the hashed PIN_t with R_s and sends it to the tag. It also sends the key that verifies that it is the tag master. For example, the tag's secret data can be hashed, XOR'ed and sent.
   - MARP : calculates R_s and generate new R_m.
   - MARP $\longrightarrow$ Tag: $R_m \parallel h(R_m \oplus h(PIN_t)) \parallel h(PIN_t) \oplus R_s$.
3. The tag analyzes the information sent by MARP. It responds only after confirming that MARP is its master. If it is, the secret data is added to R

and hashed before being sent to MARP. The server calculates the received response and authenticates the tag.

- Tag : authenticates MARP.
- Tag → MARP → Reader → Server: $h(Key_t \oplus R_s)$.
- Server : authenticates Tag.

4.6 Overall Scenario Using MARP

This scenario presents how MARP can be used in real situation.

- When a good with an RFID tag arrives at a shop, the master of the shop stores the PIN of the RFID tag in the shop's DB.
- When a consumer purchases the good, the PIN of the RFID tag of the good transmitted to the consumer's MARP. There are some feasible methods that sends the PIN information to MARP. One method is that the DB system of the shop prints the PIN on receipt and gives it to the consumer. Another method is that the DB system of the shop communicates the PIN to the consumer's MARP using a secure channel, such like bluetooth or direct cable.
- The consumer register the tag and its PIN in his MARP. The MARP acquires some of the tag's secret information through authentication using the tag's PIN. After the consumer register the tag, he can change the PIN for keeping security. These steps constitutes the initial setup phase.
- After the initial setup phase, the tag is subordinate to the MARP, and ignores any unauthenticated requests. This is master/slave state and only the MARP can read the tag.
- A reader have to communicate with the MARP instead of the tag. In the communication between the reader and the MARP, public key cryptosystem would be used for high level security. Each of them can acquire the other's public key form the public key distribution center. These steps constitutes the main scheme. And in the main scheme, the reader or the back-end server can be assured of the tag's reality through verifying the tag's secret information using the tag involved protocol. This scheme should prevent the MARP from forging the tag.
- During the consumer has the good with the tag at home, he can make the tag normal state and/or can communicate with the MARP.
- If the consumer transfer the good to another user, he have to sends the PIN information of the good to another user. After the new user registers the tag, he must change the PIN of the tag. This prevent the old user from accessing the tag illegally.

5 Analysis

We analyze the proposed scheme in this section. Our scheme is designed for a secure RFID system with low-cost tags. A tag uses its PIN or its hashed PIN as an encryption key in every session for secure communication with a MARP. Since we use hash functions and random numbers in the communication between a back-end server and a MARP, an attacker cannot know the secret information of the tag. And since only authenticated readers and tags can joined to our

communication protocols, our scheme is secure. It is impossible for the attacker to trace the location of the specific tag which sends indistinguishable answers in every query by him.

In MARP scheme, a tag has two phase protocols that are the initial setup phase and main scheme phase. In the initial setup phase, the tag sends only some of its secret information to the MARP. If the tag has already hashed PIN and hashed Key in its memory, it computes only exclusive-OR operation twice. In the main scheme phase, the tag computes two hash operations and two exclusive-OR operations. Eventually, in our MARP scheme, a tag needs to have one hash module and one exclusive-OR module.

In REP scheme of Juels[17], which is a mobile agent scheme using a re-encryption method, a tag must send all of its secret information to the agent. This causes an important security problem that the mobile agent can counterfeit or masquerade after returning or transferring of the item with the tag. On the contrary, in our scheme, MARP obtain only some of secret information of the tag and we have authentication protocol that confirm the reality of the tag. These features should reduce the possibility of forging the tag.

6 Conclusions

This study deals with protection of the privacy for the RFID system. Since the low cost RFID tags have only hundreds bits of memory and thousands of logical gates, the existing privacy protection method typically used in the mobile communication system cannot be used in RFID system. Therefore, many proposals have been made to protect the privacy under the limited resources. We have mentioned those RFID privacy protection schemes and pointed out their weakness.

We proposed MARP as a concept using the external proxy agent device for the privacy protection. MARP attains a part of the secret information of the tags to act on behalf of them. Once the secret information is attained, it communicates with the authenticated reader groups with high level security. The proposed scheme is a unique one that overcomes the built-in limitation of the tags.

Since MARP is an external device, it can be applied without much change to the currently existing RFID system. Furthermore, it has the added benefit of requiring minimum hardware capability in the tag since the privacy protection protocol is processed by the external device. We think that it is feasible to implement MARP on the current mobile devices, since an ordinary cellular phone has some cryptographic modules and a common PDA has almost perfect cryptographic modules except RF communication ability. Now we are implementing MARP on a PDA with Java platform for simulating the our scheme.

Acknowledgement

This work was supported by grant No. R01-2005-000-10568-0 from the Basic Research Program of the Korea Science & Engineering Foundation.

References

1. K. Finkenzeller, *RFID handbook*, John Wiley & Sons, 1999.
2. D. Brock, "The Electronic Product Code - A Naming Scheme for physical Objects", *Auto-ID White Paper*, http://www.autoidlabs.com/whitepapers/MIT-AUTOID-WH-002.pdf , January 2001.
3. H. Knospe and H. Pobl, "RFID Security", *Infomation Security Technical Report*, vol. 9, no. 4, pp. 39-50, Elsevier, 2004.
4. S. Sarma, S. Weis, and D. Engels, "Radio-Frequency Identification: Security Risks and Challenges", *Cryptobytes*, vol. 6 no. 1, pp. 2-9, RSA Laboratories, Spring 2003.
5. G. Avoine and P. Oechslin, "RFID Traceability: A Multilayer Problem", *Financial Cryptography - FC'05*, vol. 3570 of LNCS, pp. 125-140, February 2005.
6. R. Anderson and M. Kuhn, "Low Cost Attacks on Tamper Resistant Devices", *International Workshop on Security Protocols - IWSP*, vol. 1361 of LNCS, pp. 125-135, April 1997.
7. S. Weis, S. Sarma, R. Rivest, and D. Engels, "Security and Privacy Aspects of Low-cost Radio Frequency Identification Systems", *Security in Pervasive Computing - SPC 2003*, vol. 2802 of LNCS, pp. 454-469, March 2003.
8. S. Sarma, S. Weis, and D. Engels, "RFID Systems and Security and Privacy Implications", *Cryptographic Hardware and Embedded Systems - CHES 2002*, vol. 2523 of LNCS, pp. 454-469, August 2002.
9. A. Juels, R. Rivest, and M. Szydlo, "The Blocker Tag : Selective Blocking of RFID Tags for Consumer Privacy", *Computer and Communications Security - ACM CCS 2003*, pp. 27-30, October 2003.
10. A. Juels, J. Brainard, "Soft Blocking : Flexible Blocker Tags on the Cheap", *Workshop on Privacy in the Electronic Society - WPES 2004*, pp. 1-7, October 2004
11. M. Rieback, B. Crispo, and A. Tanenbaum, "RFID Guardian: A Battery-powered Mobile Device for RFID Privacy Management", *Australasian Conference on informaiton Security and Privacy - ACISP 2005*, vol. 3574 of LNCS, pp. 184-194, July 2005.
12. A. Tanenbaum, G. Gaydadjiev, B. Crispo, M. Rieback, D. Stafylarakis, and C. Zhang, "The RFID Guardian Project.", http://www.cs.vu.nl/∼melanie/rfid_guardian/people.html
13. G. Avoine, "Adversarial Model for Radio Frequency Identification", *Cryptology ePrint Archive*, Report 2005/049, http://eprint.iacr.org, 2005.
14. J. Saito, J.C. Ryou and K. Sakurai, "Engancing Privacy of Universal Re-Encryption Scheme for RFID Tags", *Embedded and Ubiquitous Computing - EUC '04*, vol. 3207 of LNCS, pp. 879-890, August 2004.
15. P. Golle, M. Jakobsson, A. Juels, and P. Syverson,"Universal Re-Encryption for Mixnets", *Track on the RSA Conference – CT-RSA '04*, vol. 2964 of LNCS, pp. 163-178, February 2004.
16. S. Konomi, "Personal Privacy Assistants for RFID Users", *International Workshop Series on RFID 2004*, November 2004.
17. A. Juels, P. Syverson, and D. Bailey, "High-Power Proxies for Enhancing RFID Privacy and Utility", *Center for High Assurance Computer Systems - CHACS 2005*, August 2005.
18. X. Gao , Z. Xiang , G. Wang , J. Shen , J. Huang , and S. Song, "An Approach to Security and Privacy of RFID System for Supply Chain", *Conference on E-Commerce Technology for Dynamic E-Business – CEC-East'04*, pp. 164-168, September 2005.