Authorized Tracking and Tracing for RFID Tags

Ming-Yang Chen[1], Ching-Nung Yang[2] and Chi-Sung Laih[1]

[1]Department of Electrical Engineering,
National Cheng-Kung University, Taiwan
E-mail: cmy@crypto.ee.ncku.edu.tw, laihcs@eembox.ncku.edu.tw
[2]Department of Computer Science and Information Engineering
National Dong Hwa University
E-mail: cnyang@mail.ndhu.edu.tw

Abstract. Radio Frequency Identification (RFID) systems have become popular for identifying not only objects but also persons. For example, in supply chain applications, the company can constantly track the movements of goods. Also, for Body Area Network or Personal Area Work, the tag is used for identifying a person. However, the movements and current locations of goods and a person's activity profiles are the sensitive information and should be kept secret. This paper develops the interaction protocols between readers and tags to address this privacy issue of protecting tagged objects from tracking and tracing by non-authorized readers.

1. Introduction

Radio Frequency Identification (RFID) technology was first introduced at World War II and used to distinguish where the enemy aircrafts are. Typically, RFID system has three basic components: tags, readers and the central IT system. There are already a large number of RFID applications but recently due to the falling prices, RFID technique plays a more important role for identifying and tracking objects. For example, tags can be implanted into the farmed pigs and pinpoint where they are; monitor the temperature of patients wearing ring-like tags; the retailers can automatically manage the tagged goods in the supply chain and etc. In brief, the unique identifier is used to make a "silent" tracing of a person or an object. The word "silent" means that the tracking and tracing is not noticed by the traced objects and can be carried out directly without their intervention. However, the unique identifier in tags makes the objects to be identified and traced and this will reveal the private profile. In this paper, we design an authorized tracking and tracing to achieve the anonymity (the unauthorized readers cannot trace the tagged objects) and meantime the legal central IT system can trace the movements of tagged objects.

The remainder of this paper is organized as follows. In Section 2, we describe previous works and our motivation. In Section 3 we design the proposed schemes. Security analyses and comparison are given in Section 4, and we draw our conclusions in Section 5.

2. Previous Works and Motivation

2.1. Previous Works

In RFID system, the reader retrieves the information of tags and sends back to the backend central IT system. If an attacker intrudes the IT server he can obtain the tracking and tracing profiles of the tagged items and compromise the secrecy. In general, the IT server is rigorously protected but the intruder may use unauthorized readers to scan the tags and successfully trace the tagged items.

Authentication protocol instinctively seems to be a good solution to assure the privacy but it cannot solve the tracking and tracing problem. The reason is that a tag will respond some values when an unauthorized reader requests. Even the value is not the tag's identifier the intruder may trace the specific value and know its location. For example, hash-based and randomized hash-based access controls were proposed in [1-4]. Although the powered tags do not send its identifier or sensitive information, the tagged item is still traced due to the disclosure of a certain value. Hash-chain based protocols were proposed in [5-7] but the unauthorized intruder may trace the specific tag by tracing the hash value. Another hash-based scheme [8] used hash function to protect the identifier but is also useless because the intruder can trace the hash value.

2.2. Motivation

Therefore, preventing the tags from being powered by an unauthorized reader is a complete solution for tracing problem. In [9, 10], the authors use electromagnetic waves to interfere and prevent the intended reading. Also, a flexible blocking instead of all-pass or block all was given in [10]. However, RFID is an international defacto standard for identifying objects. By using this hardware solution [9, 10], only certain readers can read the information from tags. If not all readers can scan and read tags, it is against the wide applications of RFID.

In this paper we first study the tracking and tracing with different depths. Namely, the authorized reader can read out all information including the identifier and track the tag. The unauthorized reader only receives the public information for this tag, e.g., manufacturer, product type for some commercial services, and the authorized reader can read all information. This gives consideration to two both sides: one is the tracking and tracing with certain limits and the other is the basic services for getting public information of tags. Since many tagged items have the same public information, thus the unauthorized reader cannot track the specific tag. Fig. 1 shows a certain type of RFID tag used in our schemes. The memory of tag is categorized into three fields. Field A stores the public information "*a*", the first 60 bits in the identifier EPC-96 tag (a read only memory). Field B, the last 36 bits in EPC-96 tag, stores the unique private information "*b*" such as the serial number. Field C is an extra memory block and stores some secret parameters.

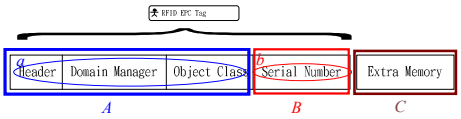

Fig. 1. Three fields in memory of RFID tag: Fields A, B and C, Field A: the public information "*a*", Field B: the private information "*b*", Field C: secret parameters.

3. The Propose Schemes

First we define the notations used in this paper: $h^m(\cdot)$ is performing the hash function m times; "||" is the concatenation of two words; $\oplus$ is the exclusive OR operation; $\{\cdot\}_K$ and $\{\cdot\}_K^{-1}$ are the encryption and decryption for a symmetric cipher with the secret key K. Note that in our proposed schemes, the low-cost tag performs the easy computation such as hash function and exclusive OR operation. The symmetric encryption/decryption is only required at the reader side.

3.1. Scheme A

Detail steps of Scheme A are shown in Fig. 2. When issued from the dealer (the central IT system), the tags store the EPC code (a, b). Also Field C stores two secret values k_0, k_1 and a counter value j (the initial value is j=1). The dealer then distributes the secret value k_0 to all authorized readers in a secret channel. When requesting, the reader sends a random number x. The powered tag computes $P_j = b \oplus h^j(k_1)$, $R_j = h^j(k_0, x)$, $V_{j+1} = h^{j+1}(k_0, x)$ (for verification later), and then sends back (a, j, P_j, $R_j \oplus k_1$) to the reader. The counter value increases by 2, i.e., j=j+2 (Note: since $V_{j+1} = h^{j+1}(k_0, x)$ $h^{j+1}(k_0, x)$ will be used in Step (7) for verification). The reader uses k_0, j, x to determine k_1, and obtains $b = P_j \oplus h^j(k_1)$. Then, sends back the EPC code (a, b) to the central IT system to check the effectiveness of this EPC code. Afterwards, the reader selects a new secret value k_2 and responds ($b \oplus h^{j+1}(k_0, x)$, $k_0 \oplus k_2$), where the first term is used for verifying whether the reader is authorized or not and the second term is used for updating the previous k_1. After the successful verification the k_1 is updated by k_2 and j is reset to 1; otherwise the value of k_1 is unchanged.

The unauthorized reader can only obtain the public information when it requests the tag. However, if the tag is continuously scanned by unauthorized readers the invalid verification results in the unchanged k_1 but at this time the counter increases and the different value of j make P_j and R_j different. So, the intruder could not trace the value P_j and R_j for this tag. When the tag is powered by an authorized reader, the k_1 is updated and j is reset to 1. Scheme A needs to share a secret value k_0 between readers and tags. Since all tags share the same k_0, thus the secrecy will be compromised by the tag-loss attack which will be discussed in Section 4. A modified

scheme without pre-sharing a secret k_0 between authorized readers and tags is given in the next sub section.

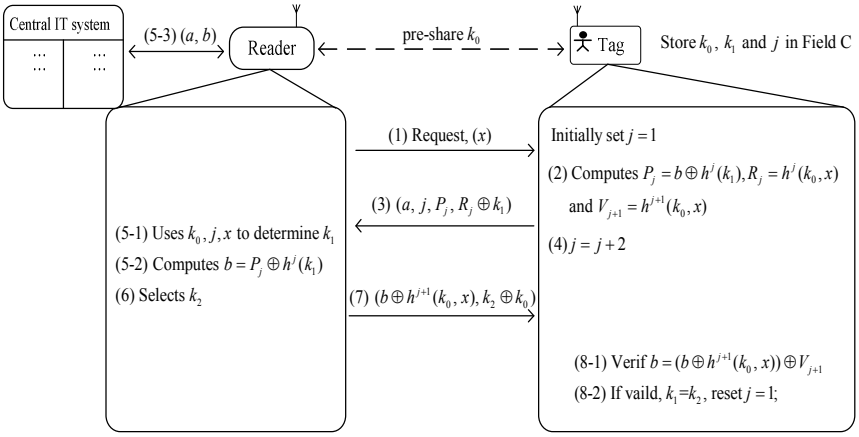

Fig. 2. Scheme A: the reader and tag pre-share a secret value.

3.2. Scheme B

Fig. 3 shows an enhanced scheme without pre-sharing the secret value between readers and tags by using the symmetric cipher at the reader side but it only uses simple hash function and exclusive OR operation at the tag side. The dealer first distributes the secret key K to all the authorized readers. When issuing the tag, the dealer prepares l pairs (k_i, c_i), where $c_i = \{a \| k_i\}_K$, i=1, …, l, and these secret pairs are all different for different tags. Store them in the Field C and the maximum l is according to the memory size of Field C. When requesting, the reader sends a random number x. The powered tag computes $P_i = b \oplus h(a, k_i, x)$ and then sends back (a, P_i, c_i) to the reader. Then, increases i by one. The reader decrypts $\{c_i\}_K^{-1} = (a \| k_i)$ and obtains $b = h(a, k_i, x) \oplus P_i$. Then, like Scheme A, sends back the EPC code (a, b) to the central IT system. Afterwards, the reader selects a new secret value k_i', encrypts $c_i' = \{a \| k_i'\}_K$, and responds $(b \oplus k_i, (k_i' \| c_i') \oplus h(k_i))$. The first term is used for verification of an authorized reader, and the second term is for updating the new secret pair (k_i', c_i'). If pass the verification, then overwrite (k_i, c_i) by (k_i', c_i').

When the tag is powered, it always uses the different pair (k_i, c_i) for each request. The reason is that if the reader is authorized, the (k_i, c_i) will be updated after the successful verification. However, for the unauthorized reader the value i is different for each unauthorized scanning, and thus the unauthorized reader cannot trace the value (a, P_i, c_i) for a tag. In both schemes A and B, if unauthorized readers only scan but do not make the response (Step (7) in Figs. 2 and 3), at this time the tag cannot

verify. This situation does not compromise our authorized tracing ability due to Step (4) in Figs. 2 and 3, i.e., "j=j+2" and "i=i+1" (we update i and j immediately after finishing Step (3) no matter the reader responds Step (7) or not).

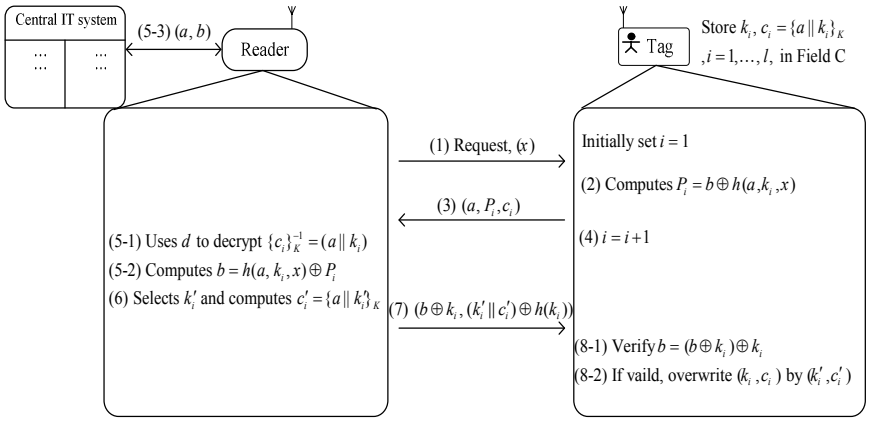

Fig. 3. Scheme B: readers and tags do not pre-share a secret value by using symmetric encryption/decryption at the reader side.

Although we do not need the pre-shared secret value in Scheme B, however the unauthorized tracing resistance ability is only "l" times. After using up all the pre-stored secret pairs this scheme will repeat to use the same (k_i, c_i) and may be traced according to the reused c_i. In fact, some manufactures, e.g., AWID [11] and STMicroelectonics [12], provide tags with the large extra memory. For example, the Prox-Linc MT and SRIX4K have 2K and 4K user-definable bits, respectively. So, suppose the public information a is 32 bits and secret value k_i is 32bits. The ciphertext c_i=$\{a\| k_i\}_K$ is 64bits (e.g., by DES encryption). Each pair (k_i, c_i) needs 96 bits to store. When using 2K and 4K memory for Field C, we have 21 and 42 secret pairs. Typically, 42 secret pairs may have the sufficient resistance for the unauthorized scanning. The detail analysis for the resistance ability of unauthorized requests is given below.

Suppose that the authorized requesting probability in the RFID-based environment is p_a and the unauthorized requesting probability is p_u=(1−p_a) and the repeated requests are independent. Therefore a possible requesting sequence within n independent requests is $\overbrace{p_i \cdot \ldots \cdot p_i}^{n}$, where p_i may be p_u or p_a.

Then the probability distribution of Scheme B, the number of unauthorized request x in n independent requests, is $D_B(x; n, p_u)=\binom{n}{x} p_u^x p_a^{n-x}$. Thus, when storing l secret pairs in tag the resistance ability of unauthorized tracking and tracing is defined as $R = \left(\sum_{i=0}^{l} \binom{n}{i} p_u^i p_a^{n-i} \right)$ (Note: the summation of the probabilities for all possible

requesting sequence that do not exhaust the secret pairs within n independent requests).

Example 1: For n=5, l=2 and p_a=p_u=1/2, the resistance ability R for Scheme B is calculated below.

$$R = \sum_{i=0}^{2} \binom{5}{i} p_u^i p_a^{n-i} = \binom{5}{0} p_a^5 + \binom{5}{1} p_u^1 p_a^4 + \binom{5}{2} p_u^2 p_a^3$$
$$= p_a^5 + 5p_u^1 p_a^4 + 10 p_u^2 p_a^3.$$

There are 16 sequences in all possible 32 requesting sequences for n=5. When p_a=p_u=1/2, R=16/32=50%. The average number of secret pairs sent by the reader for making up the balance of secret pairs in the tag for these 16 sequences is:

$$\sum_{i=0}^{2} \binom{5}{i} \times (5-i) \Big/ 16 = \big(1\times 5 + 5\times 4 + 10\times 3\big)/16 = 3.43.$$

(Note: the reader does not send anything for the unauthorized request). □

Considering l=42 (4K bits extra memory) and p_a=p_u=1/2, the value n=77 can achieve 80% resistance ability. The next scheme enhances Scheme B to achieve the stronger resistance ability for storing same secret pairs in tags.

3.2. Scheme C

Similar to Scheme B, except that the reader should make up a deficiency of l secret pairs when scanned by an authorized reader. Fig. 4 shows Scheme C. In Step (6), the authorized reader prepares i secret pairs, (k_1, c_1), (k_2, c_2), …, (k_i, c_i), where the value i is obtained from Step (3). These i secret pairs are encrypted by XOR-ing $h(k_0)$, …, $h^i(k_i)$, respectively, and sent to the tag.

The analysis for the resistance ability of unauthorized requests is given below. Scheme C will be out of action only for the l continuous unauthorized requests. For discussing the case, consider the following specified order ending at the x continuous unauthorized requests in n independent requests, $\overbrace{p_i \cdot \ldots \cdot p_i \cdot p_a}^{n-x \text{ previous requests}} \cdot \overbrace{p_u \cdot \ldots \cdot p_u}^{x}$, where the probability p_i may be p_a or p_u and the lengths of continuous unauthorized requests in the previous requesting sequence are no larger than l. The probability of above requesting sequence denoted as $P(x; n, p_u)$ is the probability that the tag is scanned continuously by unauthorized readers x times at the last x requests, and the previous (n–x) requests have no larger than l continuous requests. The value $P(x; n, p_u)$ is shown in the following theorem.

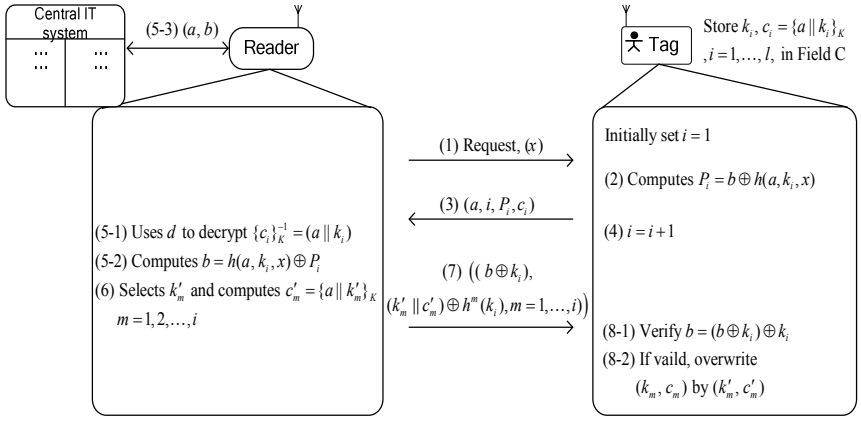

Fig. 4. Scheme C: enhance the resistance ability of the unauthorized requesting by making up a deficiency of l secret pairs in the tag.

Theorem: $P(x;\ n,\ p_u) = \sum_{(n_0, n_1, \ldots, n_l) \in S_x} \binom{N}{n_0, n_1, \ldots, n_l} \times p_a^{(n_0 + n_1 \ldots + n_l)} \times p_u^{(n_1 + 2n_2 + \ldots + ln_l) + x}$, where $(n_0,\ n_1,\ \ldots,\ n_l) \in S_x$ are all possible numbers satisfying $n - x = \left(\sum_{i=0}^{l} (i+1) \times n_i \right)$, and $N = (n_1 + n_2 + \ldots + n_l)$.

Proof: To derive the theorem, we proceed with a multinomial-like distribution. We define a single authorized request as event E_0 with probability $p_0 = p_a$, one unauthorized request followed by an authorized request as event E_1 with probability $p_1 = (p_u \times p_a)$, …, l unauthorized requests followed by an authorized request as event E_l with probability $p_l = \left(p_u^l \times p_a \right)$. Let the outcomes for E_i be n_i, $i \in [0,\ l]$, and $n - x = \left(\sum_{i=0}^{l} (i+1) \times n_i \right)$. Then the probability of the $(n-x)$ previous requesting sequence is calculated as follows.

Let S_x be a set include all possible non negative integers $(n_0,\ n_1,\ \ldots,\ n_l)$ satisfying $n - x = \left(\sum_{i=0}^{l} (i+1) \times n_i \right)$. If the outcomes $n_0 + n_1 + \ldots + n_l = N$, then the number of partitions of N items into $(l+1)$ groups is $\binom{N}{n_0, n_1, \ldots, n_l}$ and the probability of the $(n-x)$ previous requesting sequence $\text{Prob}\left\{ \overbrace{p_i \cdot \ldots \cdot p_i \cdot p_a}^{n-x \text{ previous requests}} \right\}$ is:

$$\text{Prob}\left\{ \overbrace{p_i \cdot \ldots \cdot p_i \cdot p_a}^{n-x \text{ previous requests}} \right\} = \sum_{(n_0, n_1, \ldots, n_l) \in S_x} \binom{N}{n_0, n_1, \ldots, n_l} \times p_0^{n_0} \times p_1^{n_1} \times \ldots \times p_l^{n_l}$$

$$= \sum_{(n_0,n_1,\ldots,n_l)\in S_x} \binom{N}{n_0,n_1,\ldots,n_l} \times p_a^{(n_0+n_1\ldots+n_l)} \times p_u^{(n_1+2n_2+\ldots+ln_l)}.$$

So, $P(x;\ n,\ p_u)$ is $P(x;\ n,\ p_u)=\text{Prob}\left\{\overbrace{p_i\cdot\ldots\cdot p_i\cdot p_a}^{n-x \text{ previous requests}}\right\}\times p_u^x = \sum_{(n_0,n_1,\ldots,n_l)\in S_x} \binom{N}{n_0,n_1,\ldots,n_l}$

$\times\ p_a^{(n_0+n_1\ldots+n_l)} \times p_u^{(n_1+2n_2+\ldots+ln_l)+x}$.

The proof is completed. □

For Scheme C, when storing l secret pairs in tags the resistance ability of unauthorized tracking and tracing is the summation of the probabilities for all possible requesting sequence that the length of continuous unauthorized requests is no more than l, i.e., $R=\left(\sum_{x=0}^{l} P(x;\ n,\ p_u)\right)$.

Example 2: For n=5, l=2 and p_a=p_u=1/2, the resistance ability R of Scheme C is calculated as follows.

The probabilities are, respectively, $P(2;\ 5,\ p_u)= p_a^3 p_u^2 + p_a^1 p_u^4 + 2\ p_a^2 p_u^3$, $P(1;\ 5,\ p_u)= p_a^4 p_u^1 + 3\ p_a^2 p_u^3 + 3\ p_a^3 p_u^2$ and $P(0;\ 5,\ p_u)= p_a^5 + 4\ p_a^4 p_u^1 + 6\ p_a^3 p_u^2 + 2\ p_a^2 p_u^3$ (Detail calculations of all probabilities $P(x;\ n,\ p_u)$, x=0, 1, 2, please see full version). Thus, the resistance ability $R= p_a^5 + 5\ p_a^4 p_u^1 + 10\ p_a^3 p_u^2 + 7\ p_a^2 p_u^3 + p_a^1 p_u^4$. When p_a=p_u=1/2, R=24/32=75%. Consider the number of secret pairs sent by the reader for making up the balance in these 24 sequences. The average number of secret pairs for this example is $\left(\sum_{x=0}^{l} |S_x| \times (5-x)\right) \Big/ \left(\sum_{x=0}^{l} |S_x|\right) = (13\times 5 + 7\times 4 + 4\times 3)/24 = 4.37$. (Note: the dealer will send 5(=1+2+2) secret pairs for the requesting sequence $(p_a\cdot p_u\cdot p_a\cdot p_u\cdot p_a)$, and 3(=1+2) secret pairs for the requesting sequence $(p_a\cdot p_u\cdot p_a\cdot p_u\cdot p_u)$.) □

From Examples 1 and 2, Scheme C has the strong resistance ability against the unauthorized request (the resistance ability is enhanced from 50% to 75%) and the average number 4.37 is slightly larger than 3.43 in Scheme B.

4. Security Analyses and Comparison

Some attacks: reply attack, man in the middle attack and tag-loss attack are applied to examine the security of our proposed schemes.

Reply attack: The random number x sent by the readers in our proposed schemes is used for preventing the replay attack. The responses R_j (Step (3) in Scheme A) and R_i (Step (3) in Scheme B and Scheme C) are calculated using the nonce x and thus the values will be different each time. Considering Step (7), Scheme A uses $b\oplus h^{j+1}(k_0, x)$, and Schemes B and C use $b\oplus k_i$ to encrypt the private information b.

The nonce x in Scheme A and the k_i in Schemes B and C are used only once. Therefore, the proposed scheme can resist the replay attack except that the nonce x is reused. However, the reused number attack can be avoided by choosing the sufficient length of x.

Man in the middle attack: Modification may be done in Step (3) and Step (7). First, considering that the intruder modifies the content in Step (3), our proposed schemes check the correctness of the EPC code (a, b) by querying the central IT system. If the response of the central IT system is invalid, then the readers stop proceeding. Second, consider the modification in Step (7). For Scheme A, an intruder may arbitrarily modify the second term in $(b \oplus h(k_0, j+1), k_2 \oplus k_0)$ and meantime pass the verification. Then, the tag XOR-ing the second term to obtain k_1' and overwrites k_1. This situation will not compromise the secrecy because the tag computes $P_j = b \oplus h^j(k_1')$ and the intruder does not know k_1' even he had modified the $(k_2 \oplus k_0)$. It is evident that in Step (7) of Schemes B and C, the intruder cannot pass the verification since the private information b is encrypted by $b \oplus k_i$, where k_i is used only once.

Tag-loss attack: Tags are in general not tamper resistant and therefore all information stored in tags can be retrieved. The attacker could buy a tag manufactured by a specific company. In Scheme A, the attacker has the secret values k_0, k_1 and thus he can trace all tags with the same k_0 according the known $R_j = h^j(k_0, x)$ in this 4-tuple $(a, j, P_j, R_j \oplus k_1)$ (Step (3) in Fig. 2). For Schemes B and C, there are no same secrets shared by different tags like k_0 in Scheme A. Even if the attacker retrieves the l secret pairs (k_i, c_i) in a specific tag he cannot track and trace other tags.

In this paper, we design three schemes to avoid the unauthorized tracking and tracing for RFID tags. Each scheme has its advantage. Table 1 summarizes the detail comparison among these three schemes.

Table 1. Comparison of the proposed schemes

comparison items			Scheme A	Scheme B	Scheme C
pre-shared secret values			YES	NO	NO
connect to central IT system			YES	YES	YES
resistance for attack	reply attack		YES	YES	YES
	man in the middle attack		YES	YES	YES
	tag-loss attack		NO	YES	YES
computation complexity[#2]	reader	E/D[#1]	NO	2	$(i+1)$[#3]
		Hash	3	2	$(i+1)$[#3]
		XOR	4	3	$(i+2)$[#3]
	tag	Hash	3	1	$(i+1)$[#3]
		XOR	2	2	$(i+2)$[#3]
memory size of tag			low	high[#4]	medium[#4]

#1: symmetric encryption/decryption

#2: the computation complexity is evaluated for a successful request and verification

#3: the value i is the previous i continuous unauthorized requests

#4: for the same resistance ability the secret pairs in Scheme C is less than Scheme B

5. Conclusions

In this paper, we divide the EPC code into the public and private information where the public information is privacy-free and used for some commercial services while the private information is a unique serial number of a specific tag. For providing the authorized tracking and tracing, the public information can be scanned by any readers but the private information is only retrieved by authorized readers. Scheme A can resist the unauthorized requests and only store a few secrets in memory; however it needs pre-sharing a secret value between authorized readers and tags and also is compromised by tag-loss attack. Schemes B and C do not need sharing a secret value but the resistance ability depends on the number of secret pairs store in tags, and they also require encryption/decryption at the reader side. Moreover, only simple operations: hash functions and exclusive OR operations are used at the tag side for our proposed schemes.

6. References

[1] S. A. Weis, "Security and Privacy in Radio-Frequency Identification Devices," Master's thesis, Massachusetts Institute of Technology, Cambridge, MA 02139, May 2003.

[2] S. E. Sarma, S. A. Weis, and D. W. Engels, "RFID Systems and Security and Privacy Implications," *In Workshop on Cryptographic Hardware and Embedded Systems*, *Lecture Notes in Computer Science*, volume 2523, pages 454–470, 2002.

[3] S. E. Sarma, S. A. Weis, and D. W. Engels, "Radio Frequency Identification: Risks and Challenges," *CryptoBytes (RSA Laboratories)*, 6(1), Winter/Spring 2003.

[4] S. A. Weis, S. E. Sarma, R. L. Rivest, and D. W. Engels, "Security and Privacy Aspects of Low-Cost Radio Frequency Identification Systems," *In Security in Pervasive Computing*, *Lecture Notes in Computer Science*, volume 2802 , pages 201–212, 2004.

[5] M. Ohkubo, K. Suzuki, and S. Kinoshita, "Cryptographic approach to a privacy friendly tag," *In RFID Privacy Workshop*, MIT, 2003.

[6] M. Ohkubo, K. Suzuki, and S. Kinoshita, "Efficient Hash-Chain Based RFID Privacy Protection Scheme," *In Ubiquitous Computing (UBICOMP)*, September 2004.

[7] S. Kinoshita, Ohkubo, M., Hoshino, F., Morohashi, G., Shionoiri, O. and Kanai. A, "Privacy Enhanced Active RFID Tag," *In 1st International Workshop on exploiting context histories in smart environments*, 2005.

[8] D. Henrici and P. Muller, "Hash-based Enhancement of Location Privacy for Radio-Frequency Identification Devices using Varying Identifiers," *In Pervasive Computing and Communications (PerCom), IEEE Computer Society*, pages 149–153, 2004.

[9] A. Juels, R. L. Rivest, and M. Szydlo, "The Blocker Tag: Selective Blocking of RFID Tags for Consumer Privacy," *In Computer and Communications Security*, pages 103–111, ACM Press, 2003.

[10] A. Juels and J. Brainard, "Soft Blocking：Flexible Blocker Tags on the Cheap," In Workshop on Privacy in the Electronic Society (WPES), 2004.

[11] AWID, available at http://www.awid.com.

[12] STMicroelectonics, available at http://www.st.com/rfid.