International Journal of Information, Control and Computer Sciences
ISSN: 2517-9942
Vol:3, No:12, 2009

Privacy Threats in RFID Group Proof Schemes

HyoungMin Ham, JooSeok Song

***Abstract*—**RFID tag is a small and inexpensive microchip which is capable of transmitting unique identifier through wireless network in a short distance. If a group of RFID tags can be scanned simultaneously by one reader, RFID Group proof could be generated. Group proof can be used in various applications, such as good management which is usually achieved using barcode system. A lot of RFID group proof schemes have been proposed by many researchers. In this paper, we introduce some existing group proof schemes and then analyze their vulnerabilities to the privacy. Moreover, we propose a new attack model, which threats the privacy of user by tracking tags in a group.

***Keywords*—** grouping proof, privacy, RFID, yoking proof

I. Introduction

RFID(Radio-Frequency Identification) tag is a small microchip in which there is an antenna that is capable of transmitting unique identifier of the tag to respond to a query from a reading device, like as RFID reader. RFID tags are applied in various application areas. Using RFID system instead of barcode system is expected to reduce the cost of good management and distribution. In addition, it can be used in other applications in various fields. Due to these advantages, many researchers have been done to improve RFID system.

In 2004, A. Juels proposed a different concept which can be applied to some different applications of RFID system. According to this concept, a pair of RFID tags should be able to generate a proof which can certify that they had been scanned simultaneously by the same reading device. This concept is called "yoking proof [1]". The purpose of the yoking proof is to generate a proof, which can be used to prove that a pair of RFID tags was scanned simultaneously by one reader. It is also required that the proof is verifiable by a trusted entity, possibly an off-line one. It is the practical assumption, which make RFID can be applied to various application fields as contrasted with RFID authentication.

The yoking proof might be useful i.e. when a product and its safety cap must leave the factory together or when a medicine must be dispensed with a leaflet. In these examples, according to the attached tags, we can say that these products are scanned together by one reader at the same time.

Since the first yoking proof was proposed, it is evolved to variable schemes. In 2005, Saito and Sakurai described that the yoking proof is vulnerable to replay attack, and proposed a new scheme using time stamp to solve this problem. In addition, they proposed a new scheme named "Grouping proof [2]" which uses a new entity, named the Pallet tag. Grouping proof is a concept extended from the yoking proof. The purpose of this scheme is to generate a proof which can prove simultaneous existence of a group of tags.

In this paper, we introduce some kind of yoking proof schemes and attacks which related with them. Previous researches introduced some attacks which interfere with completion of the group proof. However, we focus on the privacy issues of group proof. We will compare these schemes and analyze the reason of their vulnerability of privacy.

This paper is organized as follows: In the next section, we present the foundation of yoking and grouping proof such as assumption, requirement and threat. In section 3, we present an overview of related work and provide a brief evaluation of these. In Section 4, we describe a number of two proposed threats against some schemes discussed in Section 3. We will discuss about the cause of vulnerability in Section IV. Section V concludes this paper.

II. Yoking and Grouping proof

We will name the schemes evolved from yoking proof as "Group proof", which implies that a group of tags is scanned simultaneously by one reader. To guarantee this, group proof scheme needs to satisfy the following requirements:

- A group of tags should be scanned by one reader in the same session.
- Tags should be able to generate a proof which can prove that they existed simultaneously.
- The proof should be verifiable by the verifier.

A. Assumptions

We assume the environmental properties of Group Proof as follows:

- The tags are passive, which means they have no power of their own. However, we assume that they are able to perform basic cryptographic operations such as generating pseudo-random number and evaluating MAC functions.
- The tags are passive, which means they have no power of their own. However, we assume that they are able to perform basic cryptographic operations such as generating pseudo-random number and evaluating MAC functions
- RFID readers are potentially untrusted.
- The verifier is a trusted entity that shares some secret information, such as encryption key or seed which is used to generate a random number with the tags.
- RFID tags do not maintain clocks or keep time.

This work was supported by the Korea Science and Engineering Foundation (KOSEF) grant funded by the Korea government (MEST)(2009-0076476)

• This assumption makes the system vulnerable to a reasonable amount of attacks.
• The verifier has a secure channel that links it to the RFID reader authenticated by the verifier.

B. Threats to Group proof

We present five attacks which threats rightful verification of group proof. Three of them are mentioned in other papers and the other two are proposed by us. According to the different purposes of attacks, we classify them in two types. The first one is the attacks causing abnormal completion of group proof without executing legal steps. The second one is about the possibility of privacy problems in group proof. There are some proposed schemes which include the additional consideration of preventing the privacy problem [3][4][5][6]. However, they are still vulnerable to some attacks. To show the vulnerability of these schemes, we propose two attack scenarios, and then discuss the cause of these defects in section.

Illegal-proofing

When the tags communicate with the reader in the same session, the group proof will be generate. This should be verifiable by the verifier. However, the adversary who reuses the message in previous interaction will try to get an acceptable verification from the verifier using some illegal manner, such as a replay attack. The meaning of the Illegal-proofing is all case although some attacks which impair the reliability of the proof, it can present and accept to verifier. The kind of attacks considered in this section will cause some abnormal situation i.e. an adversary can generate an acceptable proof using one message from a tag which was scanned separately in the group and another message which is from a different group. It is possible that the attacker will generate a proof making use of another illegal value, i.e. the tag's response message in the previous session. If the verifier accept the proof and verify it, this scheme will lose the trust of the proof.

There are two kinds of attacks: one is replay attack proposed by [2] and [3], and another is Multi-proof (n) session attack [4] proposed by P.Lopez to [3].

Privacy

Privacy is one of the most important issues in RFID. Based on Juels's proposal, Piramuthu made some improvement on privacy protection and proposed a new scheme. After that, several Group Proof schemes have been proposed continuously. There are some propose schemes which have an additional consideration to prevent the privacy problem like as [3][4][5][6]. However, these schemes, including Piramuthu's, cannot solve the tracing problem. We show this vulnerability in section 4. We will show their vulnerability by using two proposed attack scenarios, and then discuss the cause of this problem in section 4.

III. Related Work

First, we introduce group proof schemes, which concern a pair of tags. The early proposed yoking proof concerns only two tags. Then, some privacy related schemes, which are still concerning a pair of tags is proposed. To address the privacy problem, these schemes considered the anonymity of a tag. However, they cannot solve the traceability problem of a tag. To introduce a number of group proof schemes, we are following as notation shown in TABLE I.

The notations in this paper are shown as the following table.

TABLE I
Notation

Symbol	
V	*Verifier*
R	*RFID Reader*
$A, 1$	*Names of the tag A and tag 1*
T_A, T_1	*Tag A, Tag 1*
ID_A, ID_1	*ID of the tag A and 1*
r_A, r_1	*Random Numbers of the tag A and tag 1*
t	*Specific time duration*
c_A	*Counter of tag A*
X_A	*Symmetric Secret Key of tag A*
$MAC_X(m)$	*MAC of m using key X*
P_{AB}, P_n	*Group Proof*

A. Yoking-proof

Yoking proof proposed by A.Juels could prove that two tags could be scanned within the range of one reader simultaneously. A couple of tag can generate a proof which is verified to verifier even though the reader is untrusted. To guarantee existence of tags, A.Juels used to bind their responses. But generally, tags cannot interact with each other. To overcome this limitation, a reader is used as a communication medium between tags.

Moreover, Juels's scheme relied on the assumption that RFID tags always terminate a session which doesn't complete within a specific time bound. This protocol is illustrated in Fig.1

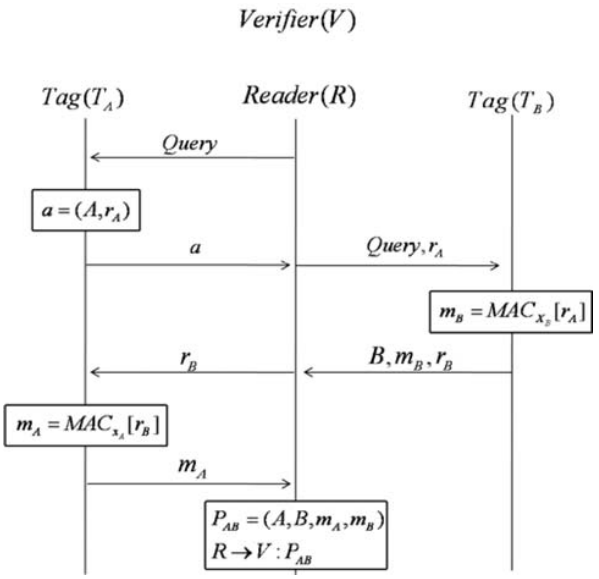

Fig. 1 Yoking-proof protocol

B. Yoking Proof with Time Stamps

Original yoking proof is vulnerable to replay attack. Saito and Sakurai pointed out this problem and described it. Moreover, Saito and Sakurai proposed a new scheme, which used a time stamp to solve this problem. However, Saito and Sakurai's scheme still has a vulnerability to a kind of the replay attack. Their protocol is illustrated in Fig.2.

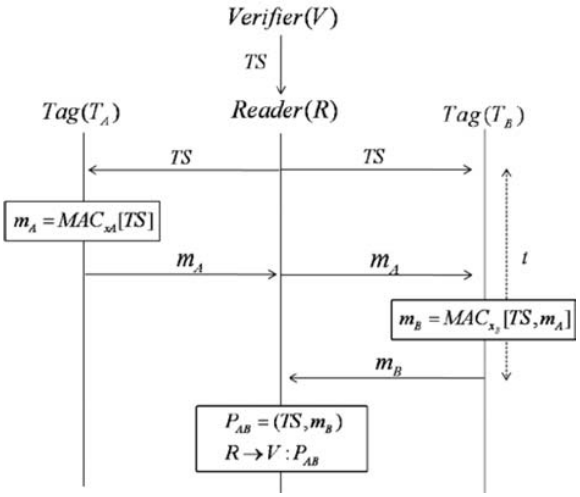

Fig. 2 Yoking proof using time stamp

C. Modified Yoking Proof

S.Piramuthu proposed a scheme based on Juels's yoking protocol which could against replay attack. However, to generate the response of a tag, this protocol uses a counter of the tag instead of the seed *r*, which is sent from the verifier. Moreover, this protocol also concerns about privacy and tracking problem when tag's static identifier is transmitted through the wireless channel in a way of plaintext. This protocol is illustrated in Fig.3.

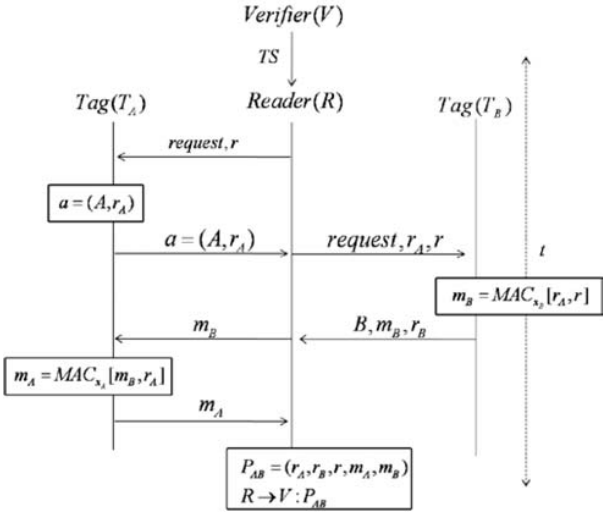

Fig. 3. The Modified Yoking Proof

D. Clumping Proof

Pedro.P.Lopez et al. presented a new proof for scanning tag simultaneously, named Clumping Proof, and proposed multi-proofs (n) session attack [4] which was to show the weakness of Piramuthu's protocol. Clumping proof solved the multi-proofs (n) session attack and provided privacy against tracking. The proposed proof is illustrated in Fig.4.

Since, yoking proof was considered with just two tags, to address this problem, these schemes considered with anonymity of a tag. However, these proposed schemes cannot address the privacy problem, which is the tracing a tag.

From E to G, we introduce group proof schemes, which concern more two tags. The group proof has a flexibility, which can overcome to limit how many a number of tags are acceptable. Also, it has a probability, which can extend to rather differential application area. Since, grouping proof was proposed by Sakurai, a number of schemes preventing privacy problems have been propose. However, like the kind of group proof schemes concerning two tags, these proposed schemes cannot solve the privacy problem completely.

E. Grouping Proof

Group proof is another yoking proof extended by Saito and Sakurai, the adjective of Group proof is to prove that two or more tags can present in the range of a RFID reader simultaneously.

A. Juels left an open problem in his paper that is how to generate a proof for larger group of tags for the future research. And then, Saito and Sakurai presented group proof scheme using Timestamp and Pallet tag. In this protocol, a parameter named Pallet Tag (PT) was introduced. PT could be a large metal plate or flat wooden pallet by which some products could be lifted or moved. PT had more computing resources than normal tags, which made it enough to meet the requirement of the protocol. Prior to running the protocol, it is assumed that the Verifier have shared the secret keys with the tags and PT in security. This protocol is shown in Fig.5.

F. Generalized yoking

L. Bolotnyy and G. Robins generalized A.Juels' protocol by developing a proof, which ensured that a group of tags are read within a certain time period for preventing replay attack. And they modify the requirement of the ″yoking-proof″ to maintain privacy, and present an anonymous yoking protocol. This protocol is shown in Fig.6.

G. Grouping Proof by Y. Lien et al.

Various protocols [2][3][4] have been proposed based on A. Juels' scheme which require to keep those message sent by each tags to generate proof in order. Y.Lien et al. referred to the order-independent problem as specific term, and presented order-independent protocols. Also, they tried solving a tracing issue, one of the privacy problems, by hiding the transferred identity of tags.

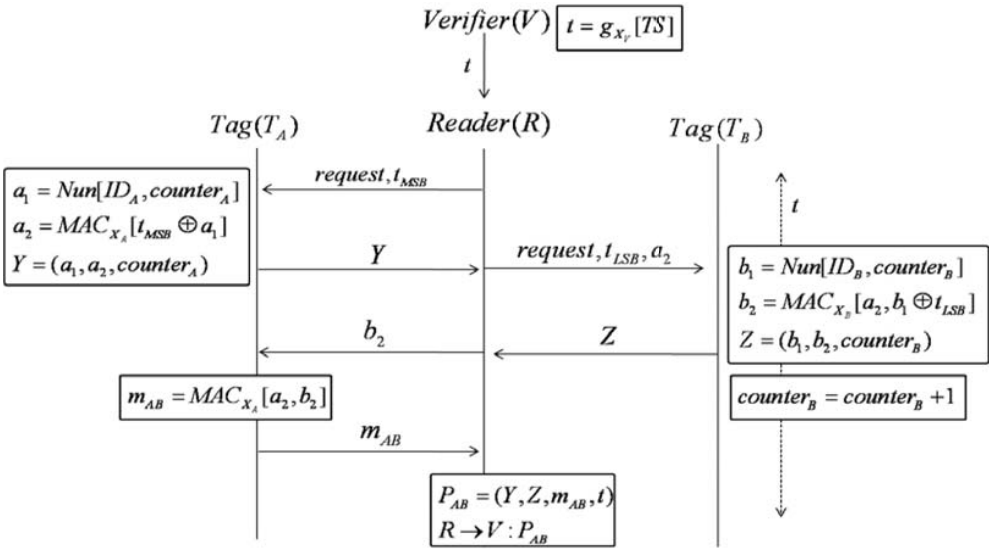

Fig. 4 Clumping proof

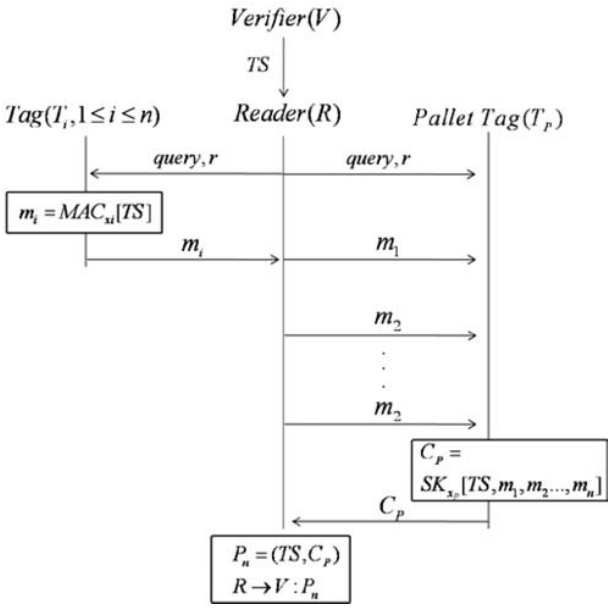

Fig.5 Grouping proof

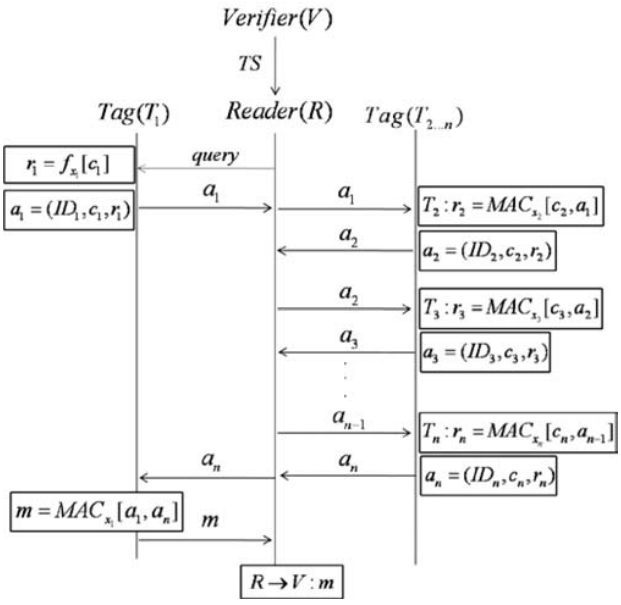

Fig.6 Generalized yoking proof

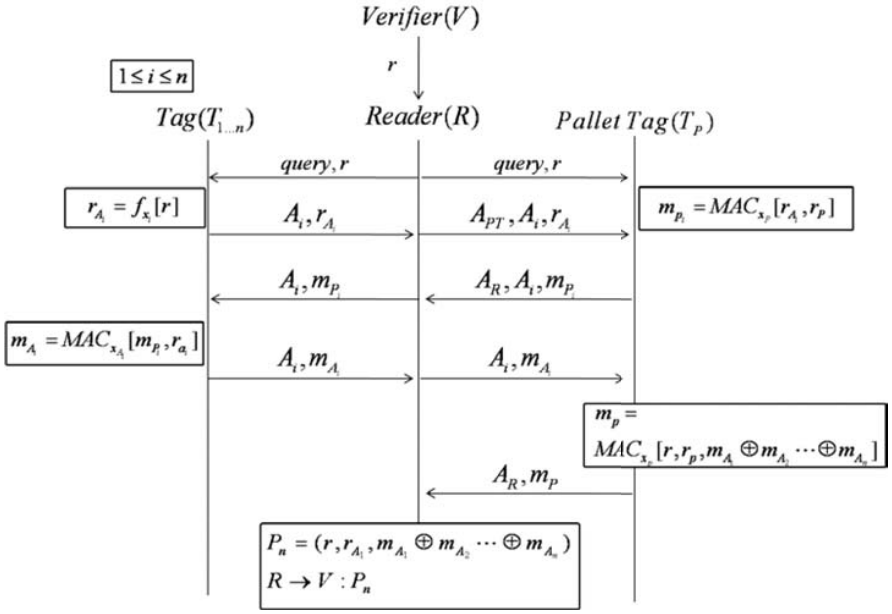

Fig. 7 Reading Order Independent Grouping proof

However, their protocols still cannot guarantee privacy perfectly. This protocol is shown in Fig.7.

Since, grouping proof proposed by Sakurai, in other to prevent privacy problem, there are some schemes have been proposed. However, these proposed schemes cannot address the privacy problem like a kind of group proof schemes for two tags.

IV. Privacy threat: traceability

These proposed attacks allow the adversary to trace the user who has a group of tags and to distinguish a particular tag in the group. Before explaining our scenarios, we firstly define the attack model as follows.

The adversary aimed at tracing the target tag. It is able to collect necessary messages through some previous normal sessions. But we do not concern the case that the adversary physically captures a tag to modify or analyze the data. Also, we assume that an adversary can gain all message of the tags in the wide area by collaborating readers.

We briefly introduce the two proposed scenarios as follows.

Scenario 1

Step 1: An adversary repeats sending a message from previous sessions to the target tag

Step 2: The tag replies with a message which includes the counter of the tag in clear.

Step 3: The adversary can modify the counter of the tag in one direction and use it to identify the target tag.

Scenario 2

Step 1: An adversary repeats sending messages from previous sessions to the target tag

Step 2: The tag replies with a message which includes received messages from the adversary in clear.

Step 3: The adversary can identify and use it to trace the target tag.

We will apply these scenarios to some existing schemes to show if they have privacy problem or not.

A. Clumping proof

If an adversary can trace a response message, which is transmitted by a tag, a user's location privacy problem may occur. In other words, transmitting the same value or distinguishable value from the tag may cause its mobile path to be exposed. Thus, responses from the same tag must not be linkable to each other. It is called unlinkability[7].

The scheme proposed by Pedro.P.Lopez et al. is designed to satisfy the unlinkability from other tags. To trace unlinkable tag, the adversary can apply the first scenario to this scheme.

We assume that the adversary can make sure that there are no tags belonging to other groups in the range of their reader to increase the success rate of the attack.

The process of scenario is the following steps.

1) The adversary repeatedly sends a query message to T_a, which is one of the pair of tags. The adversary can increase the tag's counter by doing this.

2) If the adversary can tell which reply message is sent by T_a among the tags, he can anticipate T_a's next counter contained in the following message.

3) Repeating the same process, he increases the counter of T_b, which is the other one of the pair of tags.

The point of this scenario is to include some predictable value

in the unpredictable new response message of the tag. The potentially untrusted adversary has favorable conditions to prepare for performing this scenario. Consequently, the adversary can distinguish the response of the target tag and then trace its location. However, we need to pay attention to the fact that the counter may be increased one by one in one particular direction. Therefore, it is possible that the counter of the target tag can collide with the counter of another tag from a different pair. But group proof involves more than one tag, which means that the adversary can compare the counter of the target tag with that of other tags. This could improve the traceability of the target tag. In conclusion, it is possible for the adversary to trace a group of tags in this scheme. In other words, it cannot completely protect the user's privacy.

B. Order-independent group proof

This scenario make an adversary can trace a specific group of tag as sending messages which are gathered from some later points in time.

In this scheme, Y. Lien et al. assumed that all tags in a group have a specific order. To trace the group of tags, the adversary should choose the tag which received the very first query from the reader as the target.

The process of scenario is the following steps.

1) A verifier V generates the random number r and sends it to R who is the adversary. He broadcasts random number r in a group.
2) All tags in the group generate r_{Ai} with r which is received from *V* and xi which is their secret key, and then reply with the generated r_{Ai}.
3) After the predefined time *t*, if all tags are initiated, the adversary broadcasts r in the group.
4) All tags in the group generate r_{Ai} which is the same with the previous r_{Ai} and then reply with it.
5) The adversary can trace to the tags by repeatedly executing step 2 and 3.

The author assumed in his paper that A_i, the ID of the tag, changes every time after a successful verification. He claimed it is secure enough to protect the tags from being traced.

However, according to this scenario, the adversary can trace a specific tag in a group without the knowledge of A_i.

C. Discuss about their vulnerabilities

According to scenario mentioned above, the adversary will gain the same response or identify the increased counters from the target tag. Moreover, it can cause the privacy problem, since the users are traced by an unauthorized reader. More serious thing is that this problem can be applied to other proposed schemes like as [3][5]. The point of this problem is that compromising data in group proof schemes may do not any effect verifying the proof, but it can be used to tracing the tag. In other words, group proof schemes mention above do not satisfy the confidentiality. We compare a result that shows a relation of the privacy and confidentiality of group proof schemes in Table.2. We can expect that a group proof scheme, which satisfied confidentiality can prevent the privacy problem.

TABLE II
COMPARISON OF GROUP PROOF SCHEMES

	Illegal proofing	Traceability	Confidentiality
Yoking proof	X	X	X
Yoking proof using time stamp	X	X	X
Piramuthu's scheme	X	X	X
Clumping proof	O	X	X
Grouping proof	O	X	X
Generalized yoking	O	X	X
Order-independent group proof	O	X	X

IV. CONCLUSION

In this paper, we introduced RFID Group Proofs to prove that two or more tags may be scanned in the range of one reader. Also, we revealed their vulnerabilities. Since S.Piramuthu presented his new scheme to address privacy problem, several group proof schemes have been proposed continuously. However, according to the analysis of this paper, it can be concluded that these schemes are not enough in relation to the security.

REFERENCES

[1] A. Juels, "Yoking – Proofs for RFID tags," First International Workshop on pervasive Computing and Communication Security, 2004.
[2] J. Saito and K. Sakurai, "Grouping proof for RFID tags," In 19th International Conference on Advanced Information Networking and Applications 2005, volume 2, pages 621-624, March 2005.
[3] S. Piramuthu, "On Existence Proofs for Multiple RFID Tags," IEEE International Conference on Pervasive Services (ICPS'06), June 2006.
[4] P. Peris-Lopez, J.C. Hernandez-Castro, J.M. Estevez-Tapiador, and A. Ribagorda, "Solving the simultaneous scanning problem anonymously: clumping proofs for RFID tags," In Third International Workshop on Security, Privacy and Trust in Pervasive and Ubiquitous Computing, SecPerl07, Istambul, Turkey, 2007.
[5] L. Bolotnyy and G. Robins, "Generalized Yoking Proofs for a Group of RFID Tags," International Conference on Mobile and Ubiquitous Systems, July 2006.
[6] Yuanhung Lien, Xuefei Leng, Mayes, K. Jung-Hui Chiu, "Reading order independent grouping proof for RFID tags," Intelligence and Security Informatics, 2008. ISI 2008. pp.128-136, 17-20 June 2008.
[7] Sangjin KIM, Jihwan LIM, Jaehong HAN, Heekuck OH, "Efficient RFID Search Protocols Using Counters," IEICE TRANSACTIONS on Communications, Vol.E91-B , No.11, pp.3552-3559, November 2008