International Journal of Security and Its Applications
Vol. 10, No. 12 (2016), pp.399-408
http://dx.doi.org/10.14257/ijsia.2016.10.12.33

A Secure Ownership Transfer Protocol Supporting Face to Face Transactions for RFID Tag

Lyu Xin-mei[1] and Zhang Tao[2]

[1] *College of special education, Zhengzhou Institute of Technology, Zhengzhou, China*
[2] *School of Computer and Communication Engineering, Zhengzhou University of Light Industry, Zhengzhou, China*
lxmresearch@126.com

Abstract

RFID tag will experience multiple owners in its lifetime. Tag ownership transfer protocol is a hot research issue. It was proposed a secure tag ownership transfer protocol which supports face to face transactions. In this protocol, it uses two keys. One is used to authenticate entity; the other is used to implement tag ownership transfer. We analyzed the protocol security by using GNY logic. The result indicates that old owner authenticates the tag. The new owner and tag share a new key with the help of TTP. Moreover, the protocol resists replay attack, man-in-the-middle attack, desynchronization attack and tracking attack. It provides forward security and backward security about the tag information.

Keywords*: Ownership Transfer; Protocol; GNY Logic; RFID*

1. Introduction

RFID(Radio Frequency Identification) is an automatic identification technology without physical contact. It is very popular in some domains, such as supply chain management, healthcare, animal monitoring, etc. Typically, RFID system is composed of a tag, a reader and a backend database. A tag is attached to an object and stores the information about the object. A reader forwards the messages sent by tag to backend database and vice versa. A backend database stores the information about tag and provides some services, such as authentication and authorization. The structure of RFID system is illustrated as Figure1. A tag has limited computation resource. It can't implement some complicated cryptography algorithms. Hence, it is difficult to protect the information security of RFID system.

The security issues of RFID system have been concerned[1,2]. Tag ownership transfer is one of the security issues. A tag may experience multiple owners during its lifetime. It is important to securely transfer the ownership of tag from the previous owner to the next owner. The procedure of ownership transfer not only provides authentication and resist to replay attack, man-in-the-middle attack, etc., but also has its unique security requirements. The secret shared by the previous owner and tag should be updated, and then sent to the next owner, which protects the forward security. The next owner and tag also update the secret received, which protects the backward security.

The rest of the paper is organized as follows. It analyzes some ownership transfer protocols in the next section. Afterwards, we proposed our protocol and analyzed it by using GNY logic. The last section contains conclusions and suggestions for the next work.

ISSN: 1738-9976 IJSIA

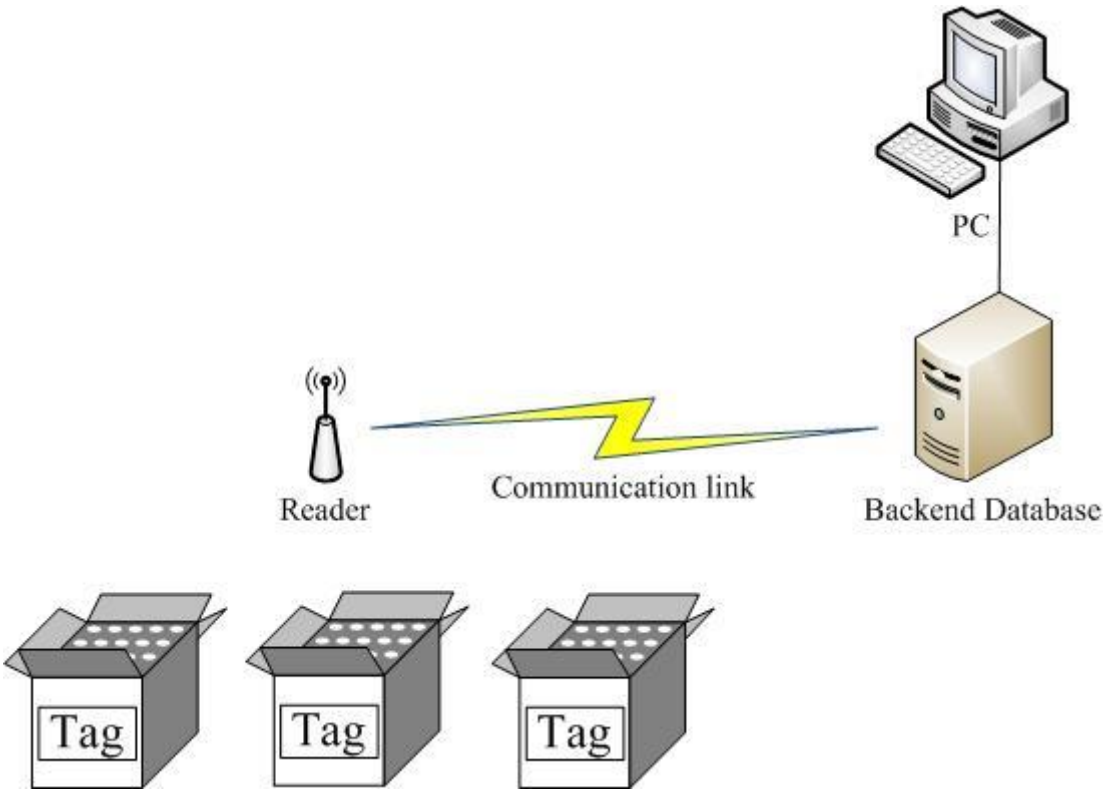


Figure 1. Structure of RFID System

2. Security Requirements

RFID protocols are vulnerable to some attacks, such as replay attack, man-in-the-middle attack, desynchronization attack, tracking attack, etc. Hence, they should fulfill the following security requirements to protect the tag ownership transfer.

- Authentication

It is necessary for owners and tag to implement authentication. In many cases, they implement mutual authentication, while sometimes they fulfill one way authentication, that is, the owners verify the tag identification. Afterwards, they are able to carry on the tag ownership transfer.

- Resistance to replay attack

An adversary is able to intercept the messages exchanged among owners and tag, and replay them, which is replay attack. It usually adds random numbers in the protocol to resist replay attack.

- Resistance to man-in-the-middle attack

An adversary may be able to insert or modify messages transmitted among owners and tag without being found, which is man-in-the-middle attack. It usually uses some cryptography algorithms to protect the messages in order to resist man-in-the-middle attack.

- Resistance to desynchronization attack

Desynchronization attack is a special attack, which is common for RFID protocols. An adversary could interfere with the messages exchanged by owners and tag, which causes desynchronization of the secrets respectively stored in the owners and tag. That is, the secrets stored in owners and tag are different. If owners use the secrets to verify tag, or

vice versa, they will fail. Hence, it is necessary for owners and tag to contain a resynchronization scheme.

- Resistance to tracking attack

In some cases, an adversary could track a tag. For example, the responses of tag are linkable, or distinguishable from those of other tags. An adversary can track the tag by eavesdropping these responses. Therefore, the protocol should break the link and provide indistinguishability.

- Forward security and backward security

Forward security and backward security are two important secure properties. In an ownership transfer protocol, both owners and tag update the secrets. New owner should not obtain the secrets shared by tag and old owner, which protects forward security. Old owner also should not obtain the secrets shared by tag and new owner, which protects backward security.

3. Related Work

RFID system has a characteristic, that is, a tag has limited computation resource, while a reader and a backend database have sufficient computation resource. It generates that a tag is not able to implement complicated cryptography algorithms, while a reader and a database can implement such algorithms. In the tag ownership transfer protocol, we consider that an owner contains reader and backend database. That is, an owner also can implement complicated cryptography algorithms. It is generally assumed the channels between owners and tag are insecure, while the channels among other entities, for example, the channel between old owner and new owner, are secure for the convenience of research because old owner and new owner have sufficient computation resource.

Some researchers have proposed research results. Earlier research results include the protocol proposed by Molnar D. *et al*[3]. The protocol is based on a tree of secrets. It introduces two methods for ownership transfer, soft killing and increasing the tag counter.

Wei Zhou proposed a hierarchical tag ownership transfer protocol in supply chains[4], which is illustrated as Figure2. In the protocol, there is a new entity, renter. The renter will have a sub-key when it rents an item. The main key will be changed when the tag ownership is transferred to a new owner.

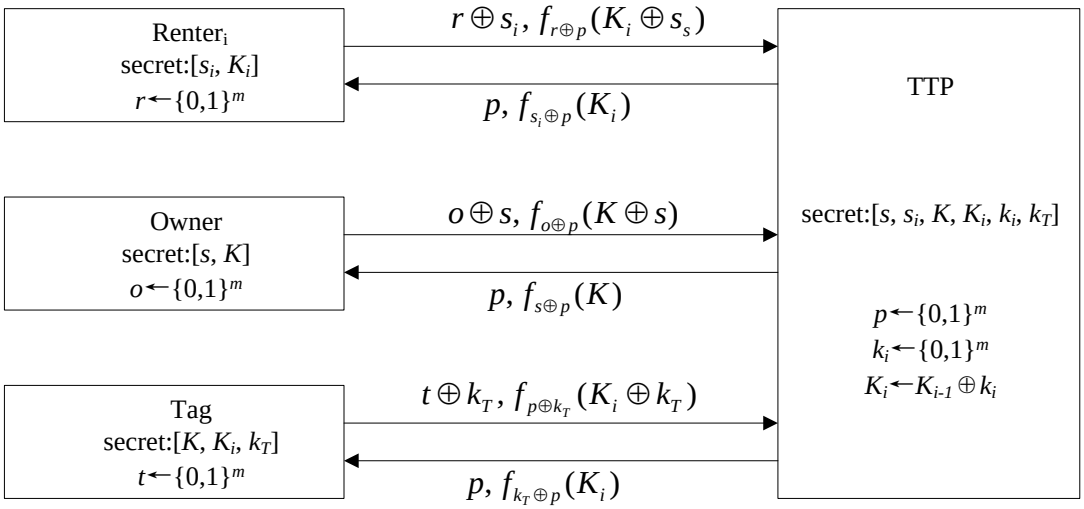


Figure 2. Ownership Transfer Protocol Proposed by Wei

It was proposed a RFID authentication protocol which supports ownership transfer [5]. It is divided into six phase, initialization, synchronized identification phase, update phase, desynchronized identification phase, controlled delegation phase and ownership transfer phase.

It was proposed two RFID tag ownership transfer schemes, the closed loop scheme and open loop scheme[6]. Both of them adapt to the computation constraints of EPC Class-1 Gen-2 passive RFID tag.

Kapoor and Piramuthu proposed two tag ownership transfer protocols[7]. One contains trusted third party(TTP), the other doesn't contains TTP. The two protocols are illustrated as Figure3 and Figure4. Both of the protocols need to use encryption function to protect confidential information.

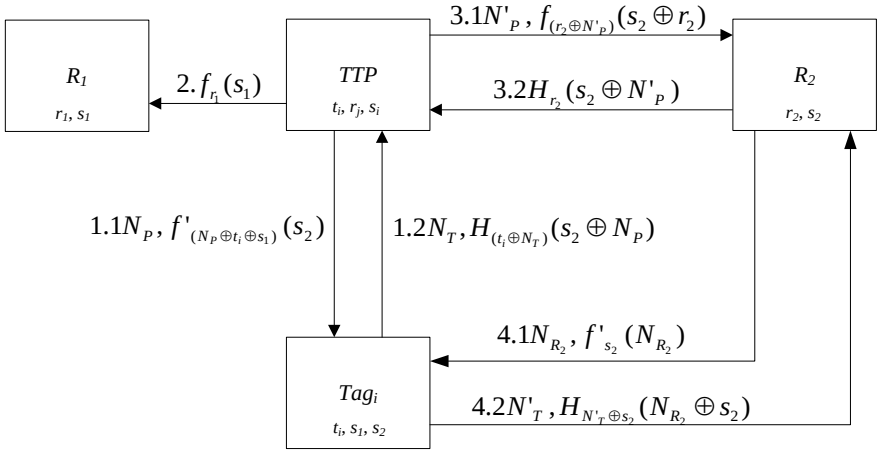


Figure 3. Ownership Transfer Protocol with TTP Proposed by Kapoor and Piramuthu

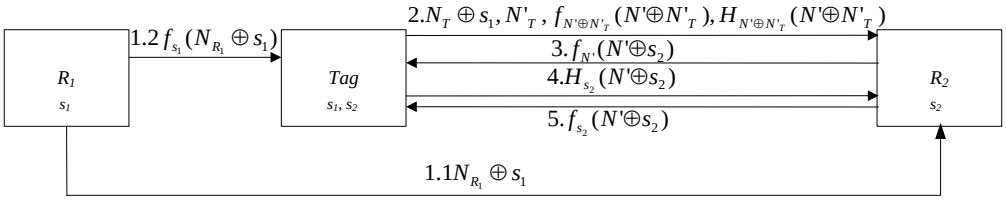


Figure 4. Ownership Transfer Protocol without TTP Proposed by Kapoor and Piramuthu

4. Protocol Description

In some scenarios, the buyer and seller are in the same place. That is, it is face to face transactions. The buyer pays the seller for the object attached by a tag. The seller transfers the ownership of the object to the buyer. Accordingly, the tag ownership also should be transferred to the buyer. It is illustrated as Figure5. Hence, the seller is the old owner of tag, while the buyer is the new owner. The protocol in this paper is suitable for such scenario.

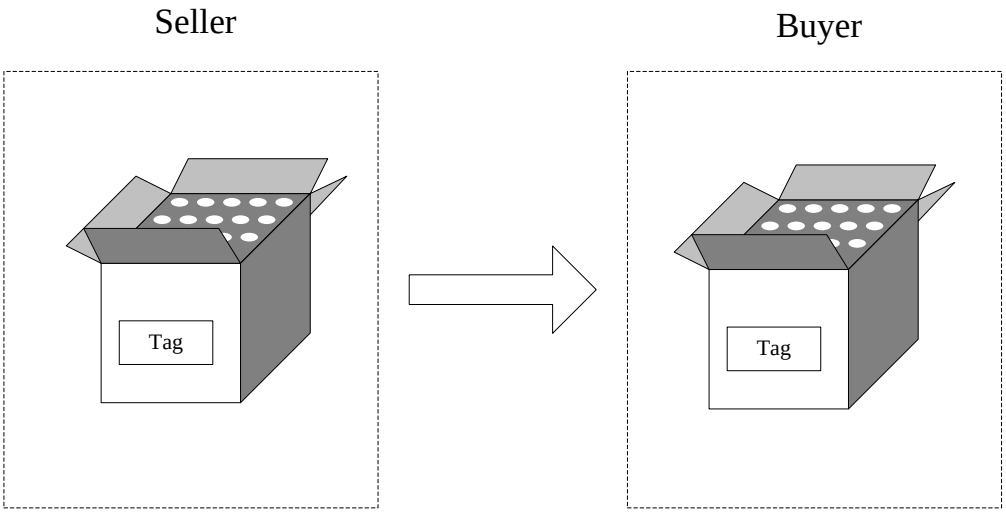


Figure 5. Scenario of Our Protocol

In this paper, it contains four entities, tag, old owner, new owner and trusted third party(TTP). New owner and old owner are in the same place. They are able to communicate with tag directly, while TTP communicates with tag with the help of new owner. New owner pays old owner for the object attached by the tag. Afterwards, old owner hands the object to new owner and implements tag ownership transfer. Old owner is able to eavesdrop on the messages transmitted by new owner and tag because they are not beyond the interception scope of old owner. Moreover, old owner obtains the key shared by new owner and tag, which is used to negotiate a new key shared by new owner and tag. Hence, it is necessary that TTP attends and protects the procedure of tag ownership transfer.

There are two keys in our protocol, k_a and k_u. The former is used to authenticate tag and owners, which is shared by the tag, owners and TTP; the latter is used to update the key and transfer the tag ownership from old owner to new owner, which is shared by the tag and TTP. The notations in Table.1 are used in the protocol.

Table 1. Notations

Notation	Meaning
r	random number generated by an entity, such as tag, old owner, new owner or TTP
ID_{OO}	identification of old owner
ID_{NO}	identification of new owner
k_a	a key which is used to authenticate tag or owners
k_u	a key which is used to update key and transfer tag ownership
a,b	concatenation of variable a and b
$\oplus$	xor operation
$H(x)$	one way hash function of variable x, such as MD5 and SHA

The protocol is illustrated as Figure6. It is assumed that the new owner has paid for the object attached by the tag and the old owner has decided to transfer the tag ownership to new owner.

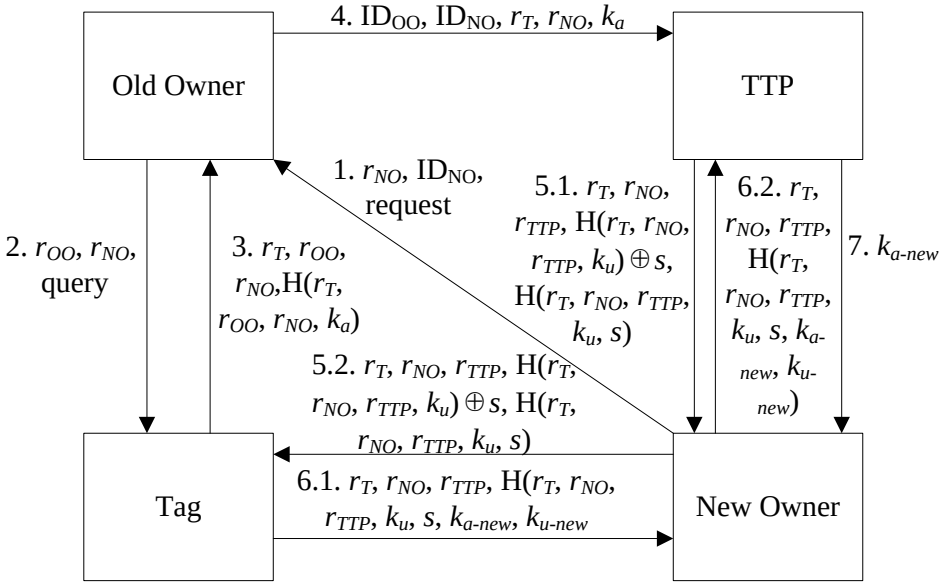


Figure 6. Ownership Transfer Protocol with TTP

1)New owner has bought an object. It wants to obtain the tag ownership. It generates a random number r_{NO} and sends it with an ownership obtain request to the old owner. That is, it sends {r_{NO}, ID_{NO}, request} to the old owner.

2)After receiving the request, old owner generates a random number r_{OO}. It sends {r_{OO}, r_{NO}, query} to tag.

3)Tag generates a random number r_T and computes H(r_T, r_{OO}, r_{NO}, k_a). It sends {r_T, r_{OO}, r_{NO}, H(r_T, r_{OO}, r_{NO}, k_a)} to old owner.

4)Old owner searches its database to find a proper k_a which meets the requirement of H(r_T, r_{OO}, r_{NO}, k_a). If such k_a doesn't exist, the protocol will end. Otherwise, old owner authenticates the tag and decides to transfer the tag ownership to the new owner through TTP. It sends {ID_{OO}, ID_{NO}, r_T, r_{NO}, k_a} to TTP in a secure way.

5)TTP searches its database to find a two-tuple (ID_{OO}, k_a) which is same with the one received. If such two-tuple doesn't exist, the protocol will end. If it finds such (ID_{OO}, k_a), TTP will know the old owner wants to transfer the tag ownership to the new owner. TTP generates a random number r_{TTP} and a secret s. The secret will be used to generated two new keys for the new owner and tag. TTP computes H(r_T, r_{NO}, r_{TTP}, k_u) ⊕ s and H(r_T, r_{NO}, r_{TTP}, k_u, s). It sends {r_T, r_{NO}, r_{TTP}, H(r_T, r_{NO}, r_{TTP}, k_u) ⊕ s, H(r_T, r_{NO}, r_{TTP}, k_u, s)} to tag through the new owner. Afterwards, it updates $k_{a\text{-}new}$ =H(k_a, s) and $k_{u\text{-}new}$ =H(k_u, s). It is important for the TTP that the previous keys, k_a and k_u, should also be stored. If the protocol suffers from desynchronization attack, it will use the previous keys to resynchronize the status.

6)Tag computes H(r_T, r_{NO}, r_{TTP}, k_u) and further obtains s. It uses the H(r_T, r_{NO}, r_{TTP}, k_u, s) received to check the correctness of s computed. If it isn't correct, the protocol will end. Otherwise, it verifies that the secret s computed is right. It updates the k_a and k_u as follows:

$k_{a\text{-}new}$ =H(k_a, s)

$k_{u\text{-}new}$ =H(k_u, s)

Tag computes H(r_T, r_{NO}, r_{TTP}, k_u, s, $k_{a\text{-}new}$, $k_{u\text{-}new}$) and sends {r_T, r_{NO}, r_{TTP}, H(r_T, r_{NO}, r_{TTP}, k_u, s, $k_{a\text{-}new}$, $k_{u\text{-}new}$)} to the TTP through the new owner.

7)TTP checks whether the massage received is correct or not by using $k_{a\text{-}new}$ and $k_{u\text{-}new}$ computed by itself. If it is not correct, the protocol will end. Otherwise, the tag ownership transfer succeeds. TTP sends $k_{a\text{-}new}$ to the new owner in a secure way.

8)New owner receives the new authentication key, $k_{a\text{-}new}$. It uses the key to communicate with tag.

5. Protocol Analysis

GNY logic is a logic analysis method which is used to analyze the protocol security. It generally contains three steps, formal description, initial assumption and reasoning procedure. The protocol should be formalized in the first step, which is helpful for the analysis to the protocol. In the second step, it sets some initial assumptions according to the protocol. It reasons and analyzes the protocol security based on the reasoning rules predefined. In the procedure of reasoning, NO, OO and T respectively represents new owner, old owner and tag. It is assumed that the channels between tag and owners are insecure, while other channels are secure. The expressions and inference rules of GNY logic are in keeping with the paper achieved by Gong *et al*[8]. In this paper, it proposed some rules, including being-told rules, possession rules, freshness rules, recognizability rules, message interpretation rules and rationality rule.

5.1. Formal Description of Protocol

M1: $OO \lhd * r_{NO}$, $*ID_{NO}$, *request

M2: $T \lhd *r_{OO}$, $*r_{NO}$, *query

M3: $OO \lhd *r_T$, r_{OO}, $*r_{NO}$, $*H(r_T, r_{OO}, r_{NO}, k_a)$

M4: $TTP \lhd *ID_{OO}$, $*ID_{NO}$, $* r_T$, $*r_{NO}$, $*k_a$

M5: $T \lhd r_T$, $*r_{NO}$, $*r_{TTP}$, $*(s)_{H(r_T, r_{NO}, r_{TTP}, k_u)}$, $*H(r_T, r_{NO}, r_{TTP}, k_u, s)$

M6: $TTP \lhd *r_T$, $*r_{NO}$, r_{TTP}, $*H(r_T, r_{NO}, r_{TTP}, k_u, s, k_{a\text{-}new}, k_{u\text{-}new})$

M7: $NO \lhd * k_{a\text{-}new}$

5.2. Initial Assumptions

A1: $OO \ni k_a$

A2: $OO| \equiv T \xleftrightarrow{k_a} OO$

A3: $OO| \equiv \# r_{OO}$

A4: $T \ni k_u$

A5: $T| \equiv T \xleftrightarrow{k_u} TTP$

A6: $T| \equiv \# r_T$

A7: $TTP \ni (k_u, s, k_{a\text{-}new}, k_{u\text{-}new})$

A8: $TTP| \equiv T \xleftrightarrow{k_u} TTP$

A9: $TTP| \equiv \# r_{TTP}$

5.3. Security Properties and Inference Procedure

G1: $OO| \equiv T \ni k_a$ (M3, A1, A2, A3, I3, I6)

G2: $T \ni s$ (M5, A4, P6)

G3: $T| \equiv TTP \ni k_u$ (M5, A4, G2, A5, A6, I3, I6)

G4: T|≡TTP~ s (M5, A4, G2, A5, A6, I3, I7)

G5: TTP|≡T∋(k_u, s, $k_{a\text{-}new}$, $k_{u\text{-}new}$) (M6, A7, A8, A9, I3, I6)

From the above analysis and reasoning, it shows that the old owner authenticates the tag in the protocol. That is, the old owner verifies that the tag has the key, k_a. Afterwards, the tag authenticates the TTP. It obtains the secret s generated by the TTP and believes the secret is sent by the TTP. TTP believes the tag obtains k_u, s, $k_{a\text{-}new}$ and $k_{u\text{-}new}$. The key, $k_{a\text{-}new}$, is shared by the tag, new owner and TTP. When the new owner receives $k_{a\text{-}new}$, it will use the key to communicate with the tag after the procedure of ownership transfer. The key, $k_{u\text{-}new}$, is shared by the tag and TTP. It is used to update $k_{a\text{-}new}$ and transfer the tag ownership to the next owner.

In addition, the protocol resists some kinds of attacks. It resists replay attack because it uses random numbers to protect the freshness of messages. The old owner, new owner and tag generate random numbers to resist replay attack. The protocol resists man-in-the-middle attack because the messages is protected by hash function and confidential information. Hash function is unidirectional. An adversary will not infer the secret if it eavesdrops on the messages. The protocol resists desynchronization attack. If it is suffered desynchronization attack, it will resynchronize the status through the TTP. The protocol also protects the user's location privacy. An adversary can not track the tag's holder even if it eavesdropped on the messages.

The protocol supports face-to-face transactions, which is one of its advantages. The old owner and new owner is able to carry out a face-to-face transactions. The new owner pays for the object attached by the tag via cash, credit card or other methods to the old owner. The Old owner will implement the tag ownership transfer immediately when it receives the payment. In the protocol, the TTP separates the old owner from new owner. The new owner isn't able to obtain the secrets shared by the old owner and tag, which provides forward security about the tag information. The TTP generates a secret and sends it to the tag. According to the secret, both of them compute the new keys, $k_{a\text{-}new}$ and $k_{u\text{-}new}$. The old owner can not obtain the new keys, which provides backward security about the tag information.

6. Conclusion

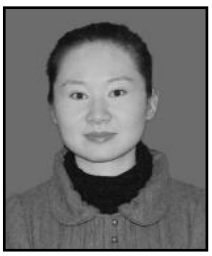
We proposed a secure ownership transfer protocol for RFID tag, which supports face to face transactions. We also analyzed its security by using a logic analysis method, namely, GNY logic. The result indicates the protocol provides authentication. The TTP shares the new keys, $k_{a\text{-}new}$ and $k_{u\text{-}new}$, with the tag and sends the new key, $k_{a\text{-}new}$, to the new owner. The new owner will use $k_{a\text{-}new}$ to communicate with the tag. Moreover, the protocol resists replay attack, man-in-the-middle attack, desynchronization attack and tracking attack. It provides forward security and backward security about the tag information. Next we will research how to further reduce the computation amount.

References

[1] Sarma S.E, Weis S.A, Engels D.W.. RFID systems and security and privacy implications. Lecture Notes in Computer Science. 2523 (**2003**)
[2] Weis, S. A., Sarma, S. E., Rivest, R. L., Engels, D. W. Security and privacy aspects of low-cost radio frequency identification systems. Lecture Notes in Computer Science. 2802 (**2004**)
[3] Molnar D, Soppera A, Wagner D. A scalable, delegatable pseudonym protocol enabling ownership transfer of RFID tags. 12th International Workshop on Selected Areas in Cryptography, (**2005**) August 11-12; Kingston, Canada

[4] Zhou W., Yoon E.J., Piramuthu S. Hierarchical RFID tag ownership and transfer in supply chains. 10th Workshop on E-Business, (**2011**) December 4; Shanghai, China
[5] Fernandez-Mir, A., Trujillo-Rasua, R., Castella-Roca, J., Domingo-Ferrer, J. A scalable RFID authentication protocol supporting ownership transfer and controlled delegation. Lecture Notes in Computer Science. 7055 **(2012)**
[6] Doss R, Zhou W, Yu S. Secure RFID tag ownership transfer based on quadratic residues. IEEE Transactions on Information Forensics and Security.2,8 (**2013**)
[7] Kapoor G, Piramuthu S. Single RFID tag ownership transfer protocols. IEEE Transactions on Systems, Man, and Cybernetics, Part C: Applications and Reviews. 2, 42 **(2012)**
[8] Gong L, Needham R, Yahalom R. Reasoning about belief in cryptographic protocols. IEEE Computer Society Symposium on Research in Security and Privacy, **(1990)** May 7-9; Oakland, Canada.

Authors



Lyu Xin-mei. She is a lecturer in the College of special education, Zhengzhou Institute of Technology. Her current research interests include different aspects of Information Security. She has published more than 5 research papers.

Zhang Tao. He received his Master Degree in Instrument science and technology from Zhengzhou University in 2006. He is now a lecturer in the School of Computer and Communication Engineering, Zhengzhou University of Light Industry. His research interest mainly focuses on Smart Sensor Networks. He has published more than 10 research papers in journals and conferences.