International Journal of Security and Its Applications
Vol.8, No.3 (2014), pp.21-30
http://dx.doi.org/10.14257/ijsia.2014.8.3.03

Secure Group Ownership Transfer Protocol for Tags in RFID System

Lei He, Yong Gan and Yi-feng Yin

School of Computer and Communication Engineering, Zhengzhou University of Light Industry, Zhengzhou, China
heleiresearch@126.com, yongg@zzuli.edu.cn, yinyifeng@zzuli.edu.cn

Abstract

It was proposed a secure group ownership transfer protocol for tags in RFID system to transfer the ownership of multiple tags simultaneously. Old owner executes authentication and updates secrets of a group of tags. Afterwards, it sends the secrets updated to new owner in a secure way. New owner also implements authentication and update procedure with tags. The protocol was analyzed by using GNY logic. It provides mutual authentication between tags and owners. It resists replay attack, man-in-the-middle attack and desynchronization attack. It also protects forward security, backward security and user's location privacy. Our protocol was implemented and simulated. We obtained experimental data including time cost by tag in the procedure of ownership transfer. It infers that our protocol has much less time cost by tag compared with other protocols.

Keywords: *Group ownership transfer; Protocol; RFID; GNY logic*

1. Introduction

Radio frequency identification (RFID) is an automation identification technology which uses radio signal to transmit data. It has been used in many fields, such as access control, product tracking, logistics management, etc. Compared with barcode, RFID tag can be read or written at a longer distance and much faster. Some retailers and wholesalers has implemented RFID system to manage commodity stocks to reduce cost and improve competitiveness.

In general, a RFID system contains three components, tag, reader and backend database. Tag is attached to the product, person, or animal which is needed to be identified. It contains two parts at least, an integrated circuit and an antenna. The former is responsible for storing and processing information, the latter receives and transmits signal. According to power supply mode, tag is divided into two categories, active tag and passive tag. Active tag has battery to provide power, while passive tag has not battery. Its power comes from electromagnetic induction. Passive tag usually is cheaper than active tag. Reader is mainly responsible for communicating with tag and backend database. It commonly forwards the message to tag or backend database. Backend database stores the information about tag and product which is attached by tag. It provides some services, such as authentication, authorization, etc.

With the development of RFID, its security has been concerned. It is usually assumed that the channel between reader and backend database is secure because they have sufficient computation resource to implement various cryptography algorithms to protect the communication. Correspondingly, it is assumed that the channel between tag and reader is insecure because low-cost tag has limited computation resource. Low-cost

ISSN: 1738-9976 IJSIA

tag can only perform some lightweight cryptography algorithms. In most of existing research results, researchers use some lightweight functions, such as Hash, XOR operation, cyclic shift, *etc*, to protect the security of communication between tag and reader.

Logistics management is an important application area of RFID. During the logistics procedure, object attached by tag may experience multiple owners. It will transfer the access of the tag to new owner (NO) when the object is handed from old owner (OO) to new owner. That is, new owner has access to tag, while old owner does not have the access. New owner and tag share new secrets, which are not known by old owner, to guarantee that only new owner can access the tag and old owner can not access the tag any longer. The procedure of ownership transfer should be protected.

Researchers have proposed some ownership transfer protocols of RFID tag. However, most of these protocols are for single tag. It transfers one tag ownership from old owner to new owner once. It will execute m times protocol when there are m tags which need to be transfered ownership. We assume that it takes old owner t to transfer single tag ownership to new owner. It costs approximately $m*t$ to complete the transfer procedure. In this paper, we propose a secure group ownership transfer protocol for RFID tags. It can transfer m tags ownership from old owner to new owner simultaneously, which greatly improves the efficiency. Moreover, it meets the security requirements mentioned below.

The rest of our paper is organized as follows. We breifly describe secure properties of the group ownership transfer protocol in the following section. Section 3 introduces related work. In Section 4, we propose the secure group ownership transfer protocol. Section 5 analyzes the protocol by using GNY logic. We also implement and simulate our protocol and obtain experimental data in the Section 6. The last section concludes the protocol and provides suggestions for the future work.

2. Security Property

- Authentication(AU)

Authentication provides the confirmation of user’s identification. It is necessary for tag and owner to implement authentication. Sometimes it needs one-way authentication, while sometimes it needs mutual authentication. The former usually refers that owner authenticates tag, while the latter refers that owner and tag mutually confirm the identity. Most of operations executed by owner and tag are based on authentication.

- Resistance to replay attack(RRA)

Replay attack is a common network attack. In the RFID system, it refers that an adversary replay the messages eavesdropped to be authenticaed by tag or owner. It destories the freshness of the messages. It can be resisted by adding fresh random number in the message.

- Resistance to man-in-the-middle attack(RMITMA)

Man-in-the-middle attack is a common network attack, too. In the RFID system, it refers that an adversary has an independent channel in the middle of tag and owner. It modifies the messages obtained and sends them to be authenticated by tag or owner.

- Resistance to desynchronization attack(RDA)

Desynchronization attack is a special attack method in the RFID system. It means that an adversary interferes with the communication between tag and owner when tag or owner nees to update the secrets. It causes that the secrets respectively stored in tag and owner are different. That is, the secrets stored in tag have been updated, while the secrets stored in owner have not been updated, or vice versa.The tag and owner will not implement successfully authentication when they suffer desynchronization attack.

- Location privacy(LA)

It is important for users to protect their location privacy. It is possible the product attached by tag is carried by user everyday. An adversary can make use of the tag to obtain the use's location and track the user.

- Forward security(FS)

Forward security refers that new owner should not infer the secrets shared by tag and old owner from the secrets received from old owner. It requires that old owner updates the secrets shared with tag in a unidirectional way. That is, new owner can't infer the secrets shared by old owner and tag from the secrets received from old owner. Afterwards, old owner sends the secrets updated to new owner.

- Backward security(BS)

Backward security refers that old owner should not infer the secrets shared by tag and new owner from the secres stored by itself. It requires that new owner should update the secrets received from old owner in a secure condition. Especially, old owner can not eavesdrop on the communication between tag and new owner. New owner communicates with tag by using the secrets updated.

3. Related Work

Most of research results is for single tag ownership transfer. One of the early achievements is the protocol proposed by Osaka et al. This protocol is vulnerable to tracking attack and does not provide the user's location privacy. Yoon et al proposed an improved protocol [2] based on the Osaka's protocol. Nevertheless, this protocol is also vulnerable to tracking attack. Jäppinen *et al.*, proposed an improved protocol [3], too. This protocol does not resolve the security problem.

Dimitriou proposed a RFID tag ownership transfer scheme [4]. It uses a keyed pseudo-random function to update the secret shared by tag and owner. It is necessary for old owner and new owner to update the secret in order to protect forward security and backward security.

Song proposed a tag ownership transfer scheme which contains three protocols, ownership transfer protocol, secret update protocol and authorization recovery protocol [5]. Shaohui considered the protocol does not protect the forward security [6].

Periaswamy *et al.*, generated digital fingerprinting of passive tag based on physical unclonable function (PUF) [7]. Furthermore, they proposed an ownership transfer protocol [8]. It transfers tag ownership by heating and cooling tag to change its physical characteristic, further change its digital fingerprinting. However, it is unpredictable for tag to change its physical characteristic by place it in extreme environments repeatedly. It still needs a large number of experiments to verify its effectiveness and stability.

Kapoor *et al.*, proposed two ownership transfer protocols according to the existence of trusted third party (TTP) [9]. One needs TTP, the other does not need TTP. However, both of them use symmetric cryptography algorithm to protect the communication between tag and owner. Hence, tag in these protocols has plenty of computation.

Fern`andez-Mir *et al.*, proposed a scalable RFID authentication protocol supporting ownership transfer [10]. The protocol is divided into six phases, initialization, synchronized identification phase, update phase, desynchronized identification phase, controlled delegation phase and ownership transfer phase. However, desynchronized identification phase can be executed consecutively MAX times, where MAX is a pre-set value. Hence, its value is important for the security of the protocol.

Kardas *et al.*, proposed a RFID authentication protocol supporting ownership transfer [11]. It requires that tag synchronizes with old owner and old owner runs at least two successful authentication protocols to update the secrets before the ownership is transferred. Afterwards, new owner also runs at least two successful authentication protocols to update the secrets. Note that it is necessary for these update procedures to be carried out in a secure environment.

4. Protocol Description

In some cases, it is possible to transfer the ownership of a group of tags simultaneously. A group may contain *m* tags. Most of ownership transfer protocols are for single tag. If old owner transfers the tag ownership one by one to new owner, it will take plenty of time. The time consumed generally is *m* times what it takes to transfer *m* tags ownership simultaneously. In this paper, we propose a secure group ownership transfer protocol for multiple tags. Old owner transfers a group of tags ownership to new owner simultaneously, which increases the efficiency. It is assumed that old owner has *n* groups and every group has *m* tags, which is illustrated as Figure 1.

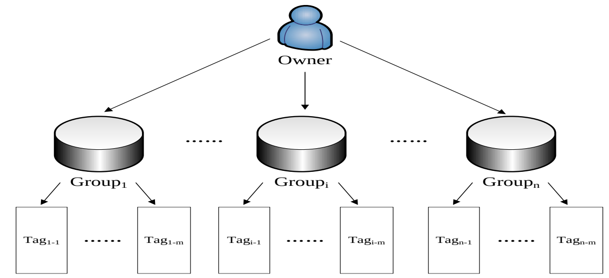

Figure 1. Relationship of Owner and Tags

Tag is assigned a key, *k* and a group identification, *GID*. The tags in the same group have the same group identification, while the key of every tag is different. The notations in Table.1 are used throughout the paper. The protocol is illustrated as Figure 2.

Table 1. Notations

notations	meaning
a, *b*	concatenation of message *a* and *b*
r_i	*i-th* random number
$\mathrm{ID}_{\mathrm{OO}}$	the identification of old owner
$\mathrm{ID}_{\mathrm{NO}}$	the identification of new owner
$k_{i\text{-}p}$	*p-th* key of *i-th* tag in the group
$GID_{j\text{-}q}$	*q-th GID* of the *j-th* group identification
status	a flag bit with length of 2 bits, whose initial value is 00
H(*a*)	one way hash function of message *a*

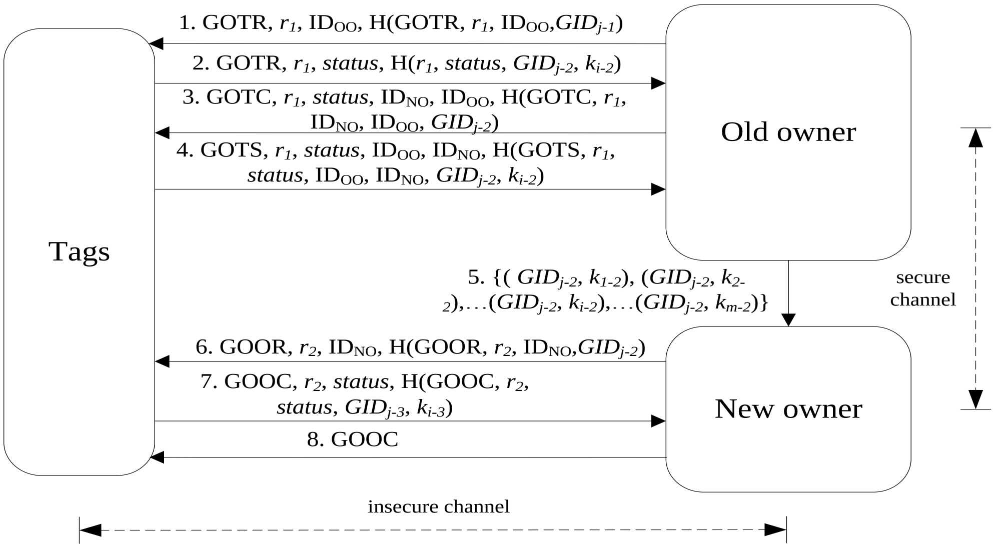
1. GOTR, r_1, $\mathrm{ID_{OO}}$, H(GOTR, r_1, $\mathrm{ID_{OO}}$,GID_{j-1})
2. GOTR, r_1, *status*, H(r_1, *status*, GID_{j-2}, k_{i-2})
3. GOTC, r_1, *status*, $\mathrm{ID_{NO}}$, $\mathrm{ID_{OO}}$, H(GOTC, r_1, $\mathrm{ID_{NO}}$, $\mathrm{ID_{OO}}$, GID_{j-2})
4. GOTS, r_1, *status*, $\mathrm{ID_{OO}}$, $\mathrm{ID_{NO}}$, H(GOTS, r_1, *status*, $\mathrm{ID_{OO}}$, $\mathrm{ID_{NO}}$, GID_{j-2}, k_{i-2})
Old owner
Tags
5. {(GID_{j-2}, k_{1-2}), (GID_{j-2}, k_{2-2}),…(GID_{j-2}, k_{i-2}),…(GID_{j-2}, k_{m-2})}
secure channel
6. GOOR, r_2, $\mathrm{ID_{NO}}$, H(GOOR, r_2, $\mathrm{ID_{NO}}$,GID_{j-2})
7. GOOC, r_2, *status*, H(GOOC, r_2, *status*, GID_{j-3}, k_{i-3})
New owner
8. GOOC
insecure channel

Figure 2. Secure Group Ownership Transfer Protocol

(1)Old owner generates a random number r_1 and broadcasts {GOTR, r_1, $\mathrm{ID_{OO}}$, H(GOTR, r_1, $\mathrm{ID_{OO}}$, GID_{j-1})} to tags, where GOTR is a group ownership transfer request.

(2)Tag checks the value of *status*. If it is 01 or 10, tag thinks it suffers replay attack or the old owner does not receive the correct response in time. It will resend the message last sent. If it is 00, tag checks whether the $\mathrm{ID_{OO}}$ received is the current owner. If it is not the owner, the protocol stops. Otherwise, tag checks whether the message is correct by using $\mathrm{ID_{OO}}$ and *GID* stored by itself. If it is not correct, tag generates a random string and sends it to old owner. Otherwise, it sets *status* =01 and updates *GID* and *k* as follow:

GID_{j-2}=H(GID_{j-1}, r_1, GOTR)

k_{i-2}=H(k_{i-1}, r_1, GOTR)

Tag sends {GOTR, r_1, *status*, H(r_1, *status*, GID_{j-2}, k_{i-2})} to old owner. Note that this step is carried out by many tags simultaneously, which is an important characteristic and reflects this protocol is a group ownership transfer protocol.

(3)If old owner does not receive the correct response from all tags in time, it will start again from the first step. It updates the GID_{j-2} and k_{i-2} in the same way and checks whether the message received is correct. Afterwards, old owner sends {GOTC, r_1, *status*, $\mathrm{ID_{NO}}$, $\mathrm{ID_{OO}}$, H(GOTC, r_1, *status*, $\mathrm{ID_{NO}}$, $\mathrm{ID_{OO}}$, GID_{j-2})} to tags, where GOTC is a group ownership transfer command.

(4)Tag checks whether the message received is correct. If it is not correct, the protocol stops. Otherwise, it sets *status*=10 and replaces $\mathrm{ID_{OO}}$ with $\mathrm{ID_{NO}}$. It sends {GOTS, r_1, *status*, $\mathrm{ID_{OO}}$, $\mathrm{ID_{NO}}$, H(GOTS, r_1, *status*, $\mathrm{ID_{OO}}$, $\mathrm{ID_{NO}}$, GID_{j-2}, k_{i-2})} to old owner, where GOTS is a group ownership transfer successful string.

(5)If the message is correct, old owner think the tag has been prepared for ownership transfer. Otherwise, it will start again from the first step until it receives correct response in time from all tags in the group. It sends {(GID_{j-2}, k_{1-2}), (GID_{j-2}, k_{2-}

$_{2}$),…(GID_{j-2}, k_{i-2}),…(GID_{j-2}, k_{m-2})} to new owner in a secure manner after it verifies that all tags has been ready for ownership transfer.

(6)After new owner receives the message from old owner, it generates a random r_2 and broadcasts {GOOR, r_2, $\mathrm{ID}_{\mathrm{NO}}$, H(GOOR, r_2, $\mathrm{ID}_{\mathrm{NO}}$, GID_{j-2})} to tags, where GOOR is a group ownership obtain request.

(7)Tag checks its status. If the value of status is 00 or 01, it sends {GOOF} to new owner, where GOOF is a group ownership obtaining failure string. If the value of status is 11, it doesn't send response. If the value of status is 10, it checks whether the message received is correct. If it is not correct, the protocol stops. Otherwise, tag updates *GID* and *k* as follow:

GID_{j-3}=H(GID_{j-2}, r_2, GOOR)

k_{i-3}=H(k_{i-2}, r_2, GOOR)

Tag sets status=11 and sends {GOOC, r_2, *status*, H(GOOC, r_2, *status*, GID_{j-3}, k_{i-3})} to new owner, where GOOC is a group ownership obtaining completion string

(8)New owner will resend the message last sent until all tags of the group sends correct response timely. It updates the GID_{j-3} and k_{i-3} in the same way and checks whether the message received is correct. If it is correct, it indicates that the tag has completed the ownership transfer. New owner sends {GOOC} to tags until all tags of the group completes the ownership transfer.

So far, new owner obtains the ownership of tags in the group. The procedure of ownership transfer is completed.

5. Protocol Analysis

GNY logic is a logic analysis method to analyze the security of protocol, which extends BAN logic. We use GNY logic to briefly analyze our group ownership transfer protocol. The analysis includes three steps, formal description, initialization assumptions and reasoning. In order to facilitate analysis, we assume that the channel between tag and owner is insecure because the computation resource of tag is limited, while the channel between old owner and new owner is secure because owners have sufficient computation resource. The expressions and inference rules we used are consistent with the paper achieved by Gong *et al.*, [12].

1. Formal Description of Protocol Messages

M1: T $\triangleleft$ *GOTR, * r_1, * $\mathrm{ID}_{\mathrm{OO}}$, *H(GOTR, r_1, $\mathrm{ID}_{\mathrm{OO}}$, GID_{j-1})

M2: OO $\triangleleft$ GOTR, r_1, * *status*, *H(r_1, status, GID_{j-2}, k_{i-2})

M3: T $\triangleleft$ *GOTC, * r_1, *status*, * $\mathrm{ID}_{\mathrm{NO}}$, *$\mathrm{ID}_{\mathrm{OO}}$, *H(GOTC, r_1, *status*, $\mathrm{ID}_{\mathrm{NO}}$, $\mathrm{ID}_{\mathrm{OO}}$, GID_{j-2})

M4: OO $\triangleleft$ *GOTS, r_1, * *status*, $\mathrm{ID}_{\mathrm{OO}}$, $\mathrm{ID}_{\mathrm{NO}}$, *H(GOTS, r_1, *status*, $\mathrm{ID}_{\mathrm{OO}}$, $\mathrm{ID}_{\mathrm{NO}}$, GID_{j-2}, k_{i-2})

M5: NO $\triangleleft$ (*GID_{j-2}, *k_{1-2}), (*GID_{j-2}, *k_{2-2}),…(*GID_{j-2}, *k_{i-2}),…(*GID_{j-2}, *k_{m-2})

M6: T $\triangleleft$ *GOOR, *r_2, *$\mathrm{ID}_{\mathrm{NO}}$, *H(GOOR, r_2, $\mathrm{ID}_{\mathrm{NO}}$,$GID_{j-2}$)

M7: NO$\triangleleft$ GOOC, r_2, *$status$, *H(GOOC, r_2, $status$, GID_{j-3}, k_{i-3})

M8:T$\triangleleft$ *GOOC

2. Initial Assumptions

A1: T$\ni$ (ID$_{OO}$, GID_{j-1}, k_{i-1})

A2: T$|\equiv$ # GID_{j-1}

A3: T$|\equiv$ T$\xleftrightarrow{GID_{j-1},k_{i-1}}$ OO

A4: OO$\ni$ (r_1, ID$_{OO}$, GID_{j-2}, k_{i-2})

A5: OO$|\equiv$ # r_1

A6: OO$|\equiv$ T$\xleftrightarrow{GID_{j-2},k_{i-2}}$ OO

A7: T$\ni$ (GID_{j-2}, k_{i-2})

A8: T$|\equiv$ # GID_{j-2}

A9: T$|\equiv$ T$\xleftrightarrow{GID_{j-2},k_{i-2}}$ OO

A10: T$|\equiv$ T$\xleftrightarrow{GID_{j-2},k_{i-2}}$ NO

A11: NO$\ni$ (ID$_{NO}$, GID_{j-2}, k_{i-2}, GID_{j-3}, k_{i-3})

A12: NO$|\equiv$ #r_2

A13: NO$|\equiv$ T$\xleftrightarrow{GID_{j-3},k_{i-3}}$ NO

3. Security Objectives and Inference Process

G1: T$|\equiv$ OO ~GOTR (M1, A1, A2, A3, I3, I7)

G2: T$|\equiv$ OO$\ni$ GID_{j-1} (M1, A1, A2, A3, I3, I6)

G3: OO$|\equiv$ T ~ $status$ (M2, A4, A5, A6, I3, I7)

G4: OO$|\equiv$ T$\ni$ (GID_{j-2}, k_{i-2}) (M2, A4, A5, A6, I3, I6)

G5: T$|\equiv$ OO ~GOTC(M3, A7, A8, A9, I3, I7)

G6: T$|\equiv$ OO$\ni$ GID_{j-2} (M3, A7, A8, A9, I3, I6)

G7: OO$|\equiv$ T ~GOTS(M4, A4, A5, A6, I3, I7)

G8: OO$|\equiv$ T$\ni$ ID$_{NO}$ (M4, A4, A5, A6, I3, I6)

G9: T$|\equiv$ NO ~GOOR(M6, A7, A8, A10, I3, I7)

G10: T$|\equiv$ NO$\ni$ GID_{j-2}(M6, A7, A8, A10, I3, I6)

G11: NO$|\equiv$ T~ GOOC(M7, A11, A12, A13,I3, I7)

G12: NO$|\equiv$ T$\ni$ (GID_{j-3}, k_{j-3})(M7, A11, A12, A13, I3, I6)

From the above analysis, we find that this protocol provides mutual authentication between tags and owners. Tags believe that old owner agrees to transfer the ownership to new owner. Old owner believes that tags have updated the secrets, *GID* and *k*, and sends them to new owner. New owner also updates the secrets in the same way. It protects forward security and backward security. Moreover, the protocol resists replay attack and man-in-the-middle attack. It is also resistant against desynchronization attack because it uses a symbol bit, *status*, to guarantee the synchronization of secrets among owners and tags. In addition, an adversary can not obtain the location of tag or track the tag by eavesdropping on the message. The security of our protocol is compared with some research results, which is shown in Table 2. The symbol, “√”, means the requirement is met. The symbol, “×”, indicates the requirement isn’t met. The symbol, “○”, means the security is partially satisfied.

Table 2. Comparison with other Protocols

	AU	RRA	RMITMA	RDA	LA	FS	BS
[1]	√	√	√	√	×	√	√
[2]	√	√	√	√	×	√	√
[3]	√	√	√	√	×	√	√
[4]	√	√	√	√	√	√	√
[5]	√	√	√	√	√	×	√
[9](with TTP)	√	√	√	√	√	√	√
[9](without TTP)	√	√	√	√	√	√	√
[10]	√	√	√	○	√	√	√
[11]	√	√	√	√	√	√	√
Our protocol	√	√	√	√	√	√	√

6. Protocol Implementing and Simulation

Our secure group ownership transfer protocol is implemented and simulated, as well as some other research results. We obtain experimental data, mainly including time cost by tag to carry out ownership transfer. It is shown in Figure 3. Note that the computation time cost is the time of single tag ownership transfer. The computation time cost by tag in our protocol is less, but is not least compared with other research. However, a group of tags implement ownership transfer simultaneously in our protocol. It is important that the time cost by m tags to transfer ownership approximately takes $1/m$ time of other protocols costs. Hence, the cost time of our protocol is much less than other protocols.

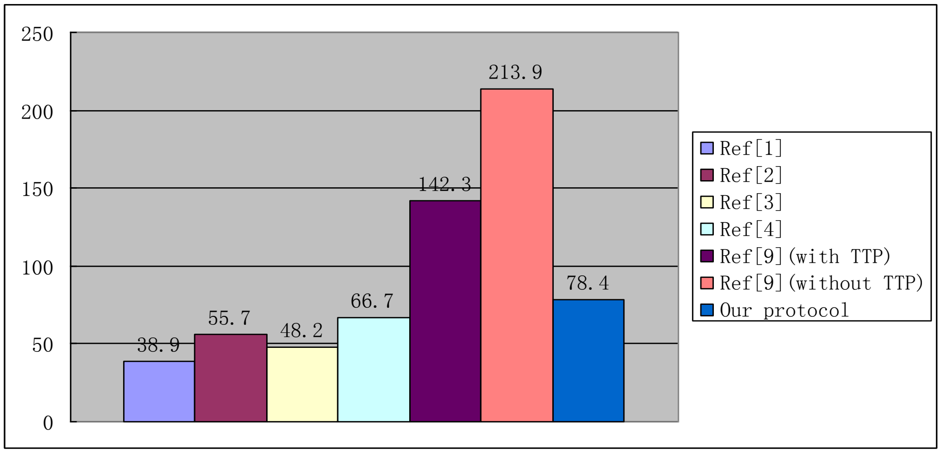

Figure 3. Computation Time Cost by Tag(μs)

7. Conclusion

Most of ownership transfer protocol is for single tag in the RFID system, that is, it transfers ownership of one tag to new owner at a time. In this paper, we propose a secure group ownership transfer protocol of tags in the RFID system. It can transfer the ownership of multiple tags simultaneously. Afterwards, we briefly analyze its security by using GNY logic. The protocol provides mutual authentication between tags and owners. It resists replay attack, man-in-the-middle attack and desynchronization attack. It protects forward security, backward security and user's location privacy. We implement and simulate the protocol and obtain experimental data. The cost time of our protocol is much less than other protocols. Next we will research how to further reduce the computation amount of tag in the procedure of ownership transfer.

Acknowledgements

This paper is sponsored by National Natural Science Foundation of China No. 61340059, 61272038.

References

[1] Osaka K, Takagi T, Yamazaki K, Takahashi, O. An efficient and secure RFID security method with ownership transfer. International Conference on Computational Intelligence and Security, **(2006)** November 3-6; Guangzhou, China.

[2] Yoon E J, Yoo K Y. Two security problems of RFID security method with ownership transfer. IFIP International Conference on Network and Parallel Computing, **(2008)** October 18-21; Shanghai, China

[3] Jappinen P, Hamalainen H. Enhanced RFID security method with ownership transfer. International Conference on Computational Intelligence and Security, **(2008)** December 13-17; Suzhou, China

[4] Dimitriou T. rfidDOT: RFID delegation and ownership transfer made simple. Proceedings of the 4th international conference on Security and privacy in communication networks, **(2008)** September 22-25; Istanbul, Turkey

[5] Song B. RFID tag ownership transfer. Proceedings of Workshop on RFID Security, **(2008)** July 9-11; Budapest, Hungary

[6] Shaohui W. Analysis and design of RFID tag ownership transfer protocol. Proceedings of the International Conference on Informatics, Cybernetics, and Computer Engineering, **(2011)** November 19-20, 2011, Melbourne, Australia.

[7] Periaswamy S C G, Thompson D R, Di J. Fingerprinting RFID tags. Dependable and Secure Computing, IEEE Transactions on. 6, 8 **(2011)**

[8] Periaswamy S C G, Thompson D R, Di J. Ownership Transfer of RFID Tags based on Electronic Fingerprint, **(2008)** July 14-17; Las Vegas, American

[9] 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)**

[10] 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)**

[11] Kardaş, S., Çelik, S., Arslan, A., Levi, A. An efficient and private RFID authentication protocol supporting ownership transfer. Lecture Notes in Computer Science. 8162 **(2013)**

[12] 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

Lei He, received his Master Degree in Cryptography from Southwest Jiaotong 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 wireless network security and cryptography, especially, RFID security. He has published more than 20 research papers in journals and conferences.

Yong Gan, got his Ph.D. in Computer Science and Technology from Xi’an Jiaotong University. He is a professor in the School of Computer and Communication Engineering, Zhengzhou University of Light Industry and dedicated to research computer network and its security. He has published more than 30 research papers in journals and conferences.

Yi-feng Yin, received his Ph.D. from Xidian University in 2009. His PhD work focused on information security and cryptography. He researched the polymorphic cipher and its cryptographic properties for virtual S-box. He is a full-time professor with the School of Computer and Communication Engineering, Zhengzhou University of Light Industry.