International Journal of Security and Its Applications
Vol.7, No.5 (2013), pp.43-52
http://dx.doi.org/10.14257/ijsia.2013.7.5.04

# A Mutual RFID Security Protocol for Wireless Reader

He Jialiang[1] and Xu Zhiqiang[2]
*[1]College of Information and Communication Engineering, Dalian Nationalities University, China
[2]Department of digital media technology, Sichuan College of Media and Communications, China
urchin2012@sina.com; starsep928@yahoo.com.cn

## Abstract

*Wireless readers are used more and more widespread recently, it brings higher design requirements for RFID protocols. In this paper, a mutual RFID authentication protocol for wireless reader that can meet lightweight encryption function structure protection is proposed, this protocol only requires O(1) work to identify and authenticate a tag in the server. The security properties of the proposed protocol are analyzed as well by comparing with the related RFID authentication protocols.*

**Keywords:** *RFID; Authentication Protocol; Wireless reader*

## 1. Introduction

Radio Frequency Identification (RFID) is an automatic identification technology to remotely store and retrieve data[1], and has been used in various application fields. Wireless readers are used more and more widespread, it brings higher design requirements for RFID protocols.

Based on wireless communication, signal broadcasting, and non-symmetry between the forward channel and the backward channel, RFID systems are confronted with many security problems. Due to strictly limited calculation resources, small storage capacity and faint power supply of low-cost tags, it is difficult to apply an ordinary and complicated but safe cryptographic algorithm to a RFID system and these factors are hindering the rapid spread of this technology [3]. Presently, lightweight encryption methods such as Hash, PRNG and CRC are used wildly in design of RFID protocols. Especially, for achieving the balance between security and performance, hash-based methods have been researched and used actively[4].

Lightweight encryption function structure protection[5] is a new security requirement of RFID security protocols. Without increasing hardware cost of RFID tags, but the difficulty that an adversary decrypts lightweight encryption function would increase by optimizing structure of transmission information.

The rest of this paper is organized as follows: in the second section, the related work is introduced; in the third section, a mutual RFID authentication protocol for wireless reader that can meet lightweight encryption function structure protection is proposed; in the fourth section, security properties of the proposed protocol are analyzed; finally, the conclusion of this paper is generalized in the fifth section.

## 2. Related Work

A well designed RFID authentication protocol should meet common security requirements while storage cost, computation cost, traffic cost of each tag should be

ISSN: 1738-9976 IJSIA

minimally controlled. A RFID system should have the ability of handling growing and huge amounts of tags by alleviating workload of the server in addition. Many authentication protocols have been proposed recently [1, 2, 4, 6-12].

An efficient RFID authentication protocol supporting tag ownership transfer[4] is proposed in 2012, let's introduce and analyze this protocol as follows:

**Table 1. The Notations used in this Paper**

| Symbol | Meaning |
|---|---|
| ID | The unique index code of a tag (The length is $l$) |
| IDS | The tags' unique index-pseudonym (The length is $l$) |
| Info | Information of the corresponding tag that stored in the server |
| RID | The unique index code of a reader (The length is $l$) |
| H() | An one-way hash function, H: $\{0,1\}^{l^*} \rightarrow \{0,1\}^{l}$ (The length of output is $l$) |
| $E_k()$ | Symmetry encryption function (The length of output is $l$) |
| PRNG() | The pseudo random number generator (The length of output is $l_R$, usually $l_R < l$) |
| $\oplus$ | XOR operator |
| $\|\|$ | Concatenation operator |
| $M_L$ | The left part of the message M |
| $M_R$ | The right part of the message M |
| R | The random number generated by the reader (The length is $l_R$) |
| T | Temporary value (The length is $l$) |
| F | Failure information of authentication |
| Pre-x | The previous value of x |
| Cur-x | The current value of x |
| $x_i$ | The x value in the (i)th session of this protocol |
| A→B:M | A sends message M to B |

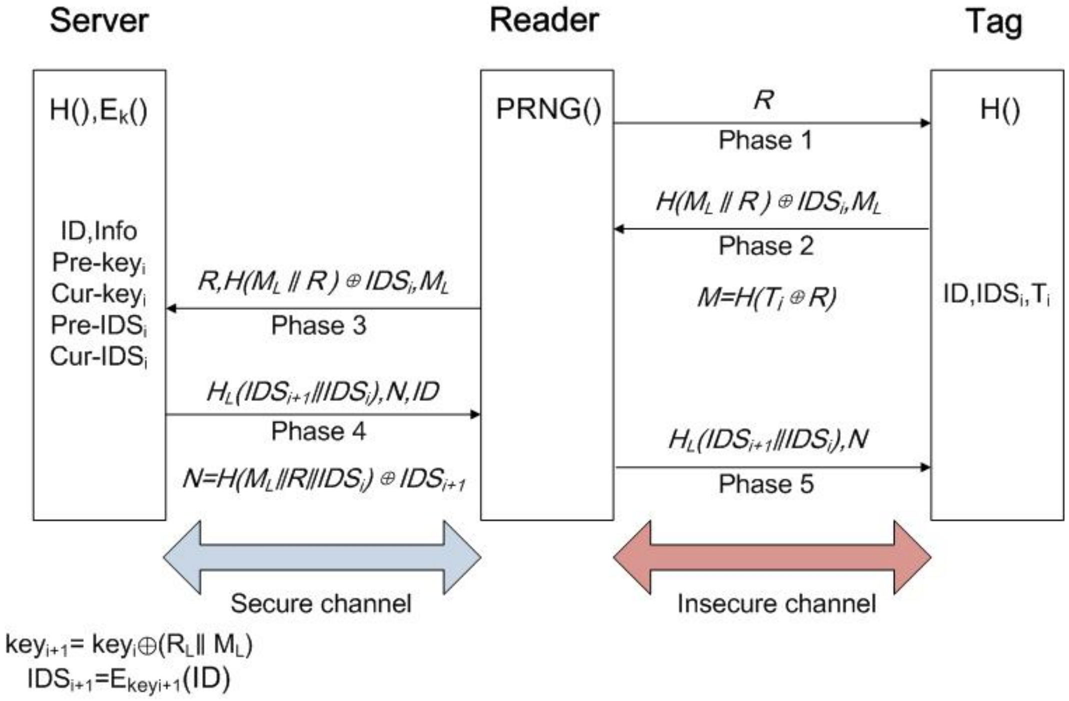

**Figure 1. Original Protocol [4]**

This protocol is an efficient RFID authentication protocol (detailed authentication access refers to [4]), it only requires O(1) work to identify and authenticate a tag in the server by using pseudonym scheme, however, there are some shortcomings of security and performance as follows:

(1)This protocol cannot meet lightweight encryption function structure protection completely. In the phase2, the tag sends $H(M_L \parallel R) \oplus IDS_i$, $M_L$ to the reader through the back channel. As we know, the channel between a reader and a tag is assumed insecure, an adversary can eavesdrop or intercept messages between the reader and the tag. So the adversary can acquire $M_L$, R, and $H(M_L \parallel R) \oplus IDS_i$. In limited authentication access, because the adversary cannot decrypt H() by brute exhaustive search, so this protocol is safe. However, if the adversary eavesdrop or intercept messages in such successive mode, and intercept the message $H_L(IDS_{i+1} \parallel IDS_i)$, N exactly in the phase5 of each authentication access, so the tag cannot update IDS successfully in each access. On this condition, IDS may be taken as a constant value, namely the adversary can get all the input values ($M_L$, R) and the output value ($H(M_L \parallel R) \oplus IDS_i$) of this encryption function H(), if the adversary can collect abundant datum and have strong calculation ability, the cracked possibility of H() would increase.

(2)ID is the most important privacy information for each tag, in this protocol, ID is transmitted from the server and a reader in plaintext, so this protocol is not suitable to wireless connection between the server and a reader, because wireless readers are applied more and more popularly, so the application domains of this protocol are limited.

(3)For wireless connection between the server and a reader, the server should verify and authenticate each authentication application from all readers, only authentication applications from legal readers would be performed, so the server should add a step of verifying and authenticating a reader.

(4)Passive tags have constraint requirements of limited resources, using less computation cost in each tag is an important research object. A tag need not have the capacity of performing concatenation operation and XOR operation at the same time, only XOR operation can achieve calculation outcome of the tag.

Based on this protocol, we proposed a mutual RFID authentication protocol for wireless reader that can meet lightweight encryption function structure protection as follows.

## 3. A New Mutual RFID Authentication Protocol for Wireless Reader

### 3.1. Assumptions

(1)The channel between the server and a reader is assumed insecure for wireless connection; the channel between a reader and a tag is assumed insecure either. We assume that an adversary can observe and manipulate communications between insecure channels.

(2)Tags are passive tags, so the resources of each tag are strictly constrained. In this protocol, each tag only needs to have an one-way hash function H(), XOR operation capability for the reason of hardware cost.

(3)A tag is not vulnerable to compromised with an adversary, that is to say, an adversary cannot acquire the inner information of the tag easily.

(4)The one-way hash function H() is secure enough against brute exhaustive search from an adversary.

### 3.2. Initialization Stage

In this stage, the server and tags store information required to perform authentication. The server should generate a random secret key $k_j$ and calculate $E_{kj}(ID_j)$ for each tag, it initially stores $ID_j$, $Info_j$, Pre-$key_j$(initial value is ‘0’), Cur-$key_j$(initial value is $k_j$), Pre-$IDS_j$(initial value is ‘0’), Cur-$IDS_j$(initial value is $E_{kj}(ID_j)$) of each tag in its database. $ID_j$, IDS(initial value is $E_{kj}(ID_j)$) and $T_0$(initial value may be ‘0’) would be set in the corresponding tag.

### 3.3. The (i +1)th Authentication Access

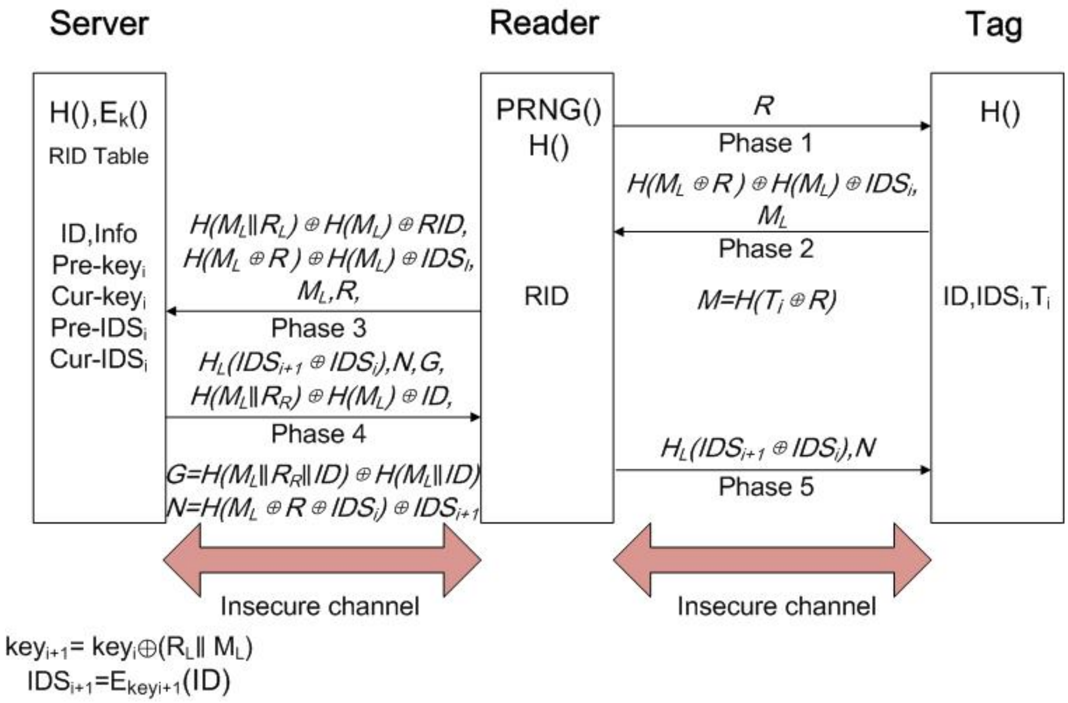

**Figure 2. New Protocol**

The (i+1)th authentication access as follows:

Phase1: The reader generates a random number R and query tags with R.

Phase2: After receiving R, a tag calculates $M = H(T_i \oplus R)$ and $P = H(M_L \oplus R) \oplus H(M_L) \oplus IDS_i$, then sends $H(M_L \oplus R) \oplus H(M_L) \oplus IDS_i$ and $M_L$ back to the reader, subsequently calculates $T_{i+1} = M \oplus P$ and saves $T_{i+1}$ in the memory. Especially, $H(T_i \oplus R)$ is used to substitute pseudo random number of the tag.

Phase3: After receiving $H(M_L \oplus R) \oplus H(M_L) \oplus IDS_i$ and $M_L$ from the tag, the reader would calculate $H(M_L \parallel R_L) \oplus H(M_L) \oplus RID$, and send $H(M_L \oplus R) \oplus H(M_L) \oplus IDS_i$, $H(M_L \parallel R_L) \oplus H(M_L) \oplus RID$, R, $M_L$ to the server.

Phase4: After receiving authentication message from the reader, the server would calculate $RID' = H(M_L \parallel R_L) \oplus H(M_L) \oplus (H(M_L \parallel R_L) \oplus H(M_L) \oplus RID)$, and search whether there exists certain RID* in table RID of the database, which can make RID’ = RID*. If there exists such record, the authentication application would be considered from a legitimate reader, or authentication is failed. The server would calculate $IDS' = H(M_L \oplus R) \oplus H(M_L) \oplus (H(M_L \oplus R) \oplus H(M_L) \oplus IDS_i)$, and search whether there exists certain IDS* in column ‘Cur-

IDS' of the database, which can make IDS' = IDS*. If there exists such record, the tag would be considered as a legitimate tag, then the server calculates $key_{i+1}$ = Cur-key*$\oplus(R_L \| M_L)$ and $IDS_{i+1} = E_{keyi+1}(ID^*)$. In particular, after accomplishing this calculation, the server must search whether there exists IDS" in column 'Pre-IDS' and column 'Cur-IDS', which makes IDS" = $E_{keyi+1}(ID^*)$. If there not exists such record, the server would calculate $H(M_L \| R_R) \oplus H(M_L) \oplus ID$, $H_L(IDS_{i+1} \| IDS_i)$, G = $H(M_L \| R_R \| ID) \oplus H(M_L \| ID)$ and N = $H(M_L \oplus R \oplus IDS_i) \oplus IDS_{i+1}$, then send $H(M_L \| R_R) \oplus H(M_L) \oplus ID$, $H_L(IDS_{i+1} \| IDS_i)$, G and N to the reader and update Pre-key = Cur-key, Cur-key = $key_{i+1}$, Pre-IDS = Cur-IDS, Cur-IDS = $IDS_{i+1}$; if there exists such record, the server must generate such a random key' that can make the value which equals to $E_{key'}(ID^*)$ cannot be found in column 'Pre-IDS' and column 'Cur-IDS', then the server would calculate $H(M_L \| R_R) \oplus H(M_L) \oplus ID$, $H_L(IDS_{i+1} \| IDS_i)$, G = $H(M_L \| R_R \| ID) \oplus H(M_L \| ID)$ and N = $H(M_L \oplus R \oplus IDS_i) \oplus IDS_{i+1}$, then send $H(M_L \| R_R) \oplus H(M_L) \oplus ID$, $H_L(IDS_{i+1} \| IDS_i)$, G and N to the reader and update Pre-key = Cur-key, Cur-key = key', Pre-IDS = Cur-IDS, Cur-IDS = $IDS_{i+1} = E_{key'}(ID^*)$.

If there not exists such IDS* in column 'Cur-IDS' of the database, which can make IDS = IDS*. The server would search whether there exists certain IDS* in column 'Pre-IDS' of the database, which can make IDS = IDS*. If there exists such record, the tag would be considered as a legitimate tag, but in the last authentication access, the tag has not IDS successfully for some reason, so the server calculates $key_{i+1}$ = Pre-key*$\oplus(R_L \| M_L)$ and $IDS_{i+1} = E_{keyi+1}(ID^*)$. In particular, after accomplishing this calculation, the server must search whether there exists IDS" in column 'Pre-IDS' and column 'Cur-IDS', which makes IDS" = $E_{keyi+1}(ID^*)$. If there not exists such record, the server would calculate $H(M_L \| R_R) \oplus H(M_L) \oplus ID$, $H_L(IDS_{i+1} \| IDS_i)$, G = $H(M_L \| R_R \| ID) \oplus H(M_L \| ID)$ and N = $H(M_L \oplus R \oplus IDS_i) \oplus IDS_{i+1}$, then send $H(M_L \| R_R) \oplus H(M_L) \oplus ID$, $H_L(IDS_{i+1} \| IDS_i)$, G and N to the reader and update Cur-key = $key_{i+1}$, Cur-IDS = $E_{keyi+1}(ID^*)$ but Pre-key and Pre-IDS would keep unaltered; if there exists such record, the server must generate such a random key' that can make the value which equals to $E_{key'}(ID^*)$ cannot be found in column 'Pre-IDS' and column 'Cur-IDS', then the server would calculate $H(M_L \| R_R) \oplus H(M_L) \oplus ID$, $H_L(IDS_{i+1} \| IDS_i)$, G = $H(M_L \| R_R \| ID) \oplus H(M_L \| ID)$ and N = $H(M_L \oplus R \oplus IDS_i) \oplus IDS_{i+1}$, then send $H(M_L \| R_R) \oplus H(M_L) \oplus ID$, $H_L(IDS_{i+1} \| IDS_i)$, G and N to the reader and update Cur-key = $key_{i+1}$ = key', Cur-IDS = $E_{key'}(ID^*)$ but Pre-key and Pre-IDS would keep unaltered.

If there is no certain IDS* in column 'Cur-IDS' and column 'Pre-IDS' of the database, which can make IDS = IDS*, the authentication is failed, F would be sent to the reader.

In phase4, only two hash operations would be needed in verifying and authenticating the ID, so the time complexity of hash function calculation achieves O(1).

Phase5: After receiving $H(M_L \| R_R) \oplus H(M_L) \oplus ID$, $H_L(IDS_{i+1} \| IDS_i)$, G and N from the server, the reader would calculate ID' = $H(M_L \| R_R) \oplus H(M_L) \oplus (H(M_L \| R_R) \oplus H(M_L) \oplus ID)$, then calculate $H(M_L \| R_R \| ID') \oplus H(M_L \| ID')$, if calculation outcome equals to received G, the reader would store ID in its memory. Subsequently the reader sends $H_L(IDS_{i+1} \| IDS_i)$, N to the tag. After receiving $H_L(IDS_{i+1} \| IDS_i)$, N from the reader, the tag would calculate IDS = $H(M_L \oplus R \oplus IDS_i) \oplus N$, then calculate $H_L(IDS \| IDS_i)$. If calculation outcome equals to received $H(IDS_{i+1} \| IDS_i)$, then the object of mutual authentication achieves, the tag should update $IDS_{i+1}$ = IDS, otherwise, the authentication is failed.

Comparing with the original protocol[4], new protocol upswings as follow:

(1)In phase2, the tag calculates $H(M_L \oplus R) \oplus H(M_L) \oplus IDS_i$ instead of $H(M_L \| R) \oplus IDS_i$. $M_L$ is updated in each authentication access, so $H(M_L \oplus R)$ and $H(M_L)$ is mutative in each value authentication access, namely $H(M_L \oplus R) \oplus H(M_L)$ is equal to a complicated encryption function for the adversary.

(2)In new protocol, ID is transmitted from the server to a reader under the shield of $H(M_L \| R_R) \oplus H(M_L)$, the reader acquire ID of each legitimate tag by decryption. So this protocol is suitable to wireless connection between the server and a reader.

(3)In new protocol, only XOR operation and one hash function H() are used in a tag, comparing with original protocol, concatenation operation is not used in a tag.

(4)New protocol adds authentication step about RFID reader, only authentication applications from legal readers would be performed by the server.

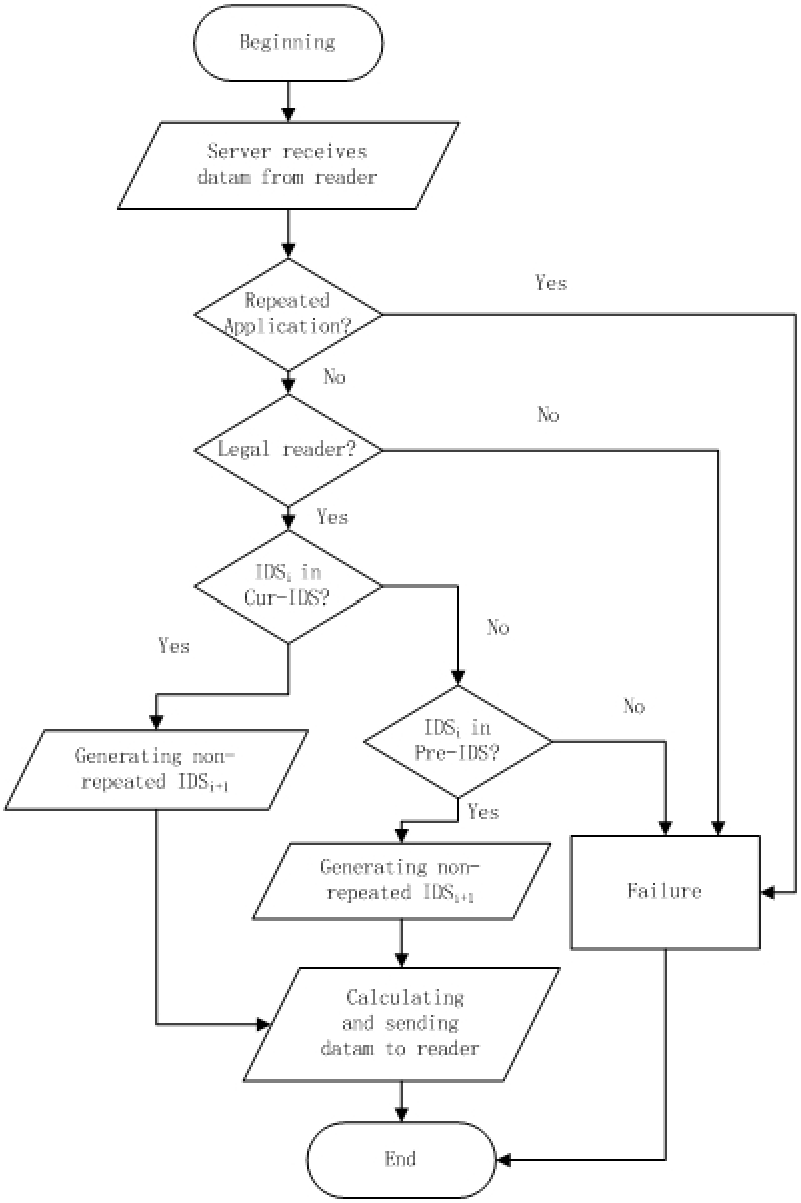
Beginning
Server receives datam from reader
Repeated Application?
Yes
No
Legal reader?
No
Yes
$IDS_i$ in Cur-IDS?
Yes
No
Generating non-repeated $IDS_{i+1}$
$IDS_i$ in Pre-IDS?
No
Yes
Generating non-repeated $IDS_{i+1}$
Failure
Calculating and sending datam to reader
End

**Figure 3. Process of Phase4**

## 4. Security Analysis

(1)Tag untraceability

An adversary can eavesdrop the response message ($H(M_L \oplus R) \oplus H(M_L) \oplus IDS_i, M_L$) from a tag, and analyze the information carefully and try to detect the user location privacy by tracking the tag. Because the tag generates a new substitute random number $M = H(T_i \oplus R)$ during each authentication access, and updates $T_{i+1} = M \oplus (H(M_L \oplus R) \oplus H(M_L) \oplus IDS_i)$ in the phase2, so the adversary cannot determine which tag does the response from the message ($H(M_L \oplus R) \oplus H(M_L) \oplus IDS_i, M_L$). So this protocol can meet tag untraceability.

(2)Tag information protection

ID is stored in the server only and is transmitted from the server to tag through reader, in the transmission process, ID is shield by $H(M_L \| R_R) \oplus H(M_L)$, an adversary cannot calculate $H(M_L \| R_R) \oplus H(M_L)$ so as to cannot acquire ID, so this protocol can meet tag information protection.

(3)Spoofing attack

An adversary feigns a legitimate reader that sends a query with R to tags through the forward channel, and obtains the response of a tag ($H(M_L \oplus R) \oplus H(M_L) \oplus IDS_i, M_L$). In the next authentication access, when a legitimate reader sends query with R', the adversary feigns the tag and responds the legitimate reader with the obtained message ($H(M_L \oplus R) \oplus H(M_L) \oplus IDS_i, M_L$) through the backward channel. However, the reader generates a new random number during each authentication access, namely $R \neq R'$, so the adversary cannot perform tag impersonation.

(4)Replay attack

Replay attack can be prevented in this protocol due to the message transmitted for each session is different. Different value of $H(M_L \oplus R) \oplus H(M_L)$ is utilized in individual session and T that stored in a tag plays a key role in providing different value of $H(M_L \oplus R) \oplus H(M_L)$ to conceal IDS of the tag. An adversary cannot hold H() and then acquire $H(M_L \oplus R) \oplus H(M_L)$, so it is impossible for an adversary to apply replay attack.

(5)Denial of Service (DoS) attack

As pseudonym of a tag (IDS) is mutative, even if loss of message, power failure or loss of connection with the server happens during an authentication access, it would lead to dy-synchronization between the server and the tag, but this protocol could solve this problem in the next authentication access by searching pseudonym IDS in column 'Pre-IDS' and continuing the authentication access. So this protocol can shield DoS attack well.

(6)Forward security

Both the server and the tag store the secret value IDS, and update them in each authentication session. So forward security attacks would be failed because IDS has no relationship with previous sessions.

(7)Backward security

Both the server and the tag store the secret value IDS, and update them in each authentication session; key is stored in the server only, and only the server can perform $E_k()$, so an adversary cannot acquire $E_{key}(ID)$ and forecast behavior of the tag in intending authentication access.

(8)Lightweight encryption function structure protection

This protocol can meet lightweight encryption function structure protection completely. Because either the channel between the server and a reader or the channel between a reader and a tag is assumed insecure, so an adversary can observe and manipulate communications in this protocol. In an integrated tag authentication access, the adversary can eavesdrop $H(M_L \oplus R) \oplus H(M_L) \oplus IDS_i$, $H(M_L \| R_L) \oplus H(M_L) \oplus RID$, $R$, $M_L$, $H(M_L \| R_R) \oplus H(M_L) \oplus ID$, $H_L(IDS_{i+1} \| IDS_i)$, $H(M_L \| R_R \| ID) \oplus H(M_L \| ID)$, $H(M_L \oplus R \oplus IDS_i) \oplus IDS_{i+1}$. Because $M_L$ is updated in each authentication access compulsively, so $H(M_L \oplus R)$ and $H(M_L)$, $H(M_L \| R_L)$ and $H(M_L)$, $H(M_L \| R_R)$ and $H(M_L)$, $H(M_L \| R_R \| ID)$ and $H(M_L \| ID)$ are mutative in each value authentication access, namely $H(M_L \oplus R) \oplus H(M_L)$, $H(M_L \| R_L) \oplus H(M_L)$, $H(M_L \| R_R) \oplus H(M_L)$, $H(M_L \| R_R \| ID) \oplus H(M_L \| ID)$ are all equal to complicated encryption functions for the adversary, it is very difficult to decrypting H() by analyzing these complicated encryption functions for the adversary; in addition, $IDS_i$ and $IDS_{i+1}$ are variables for the adversary, it is difficult to decrypting H() for the adversary by only holding $H_L(IDS_{i+1} \| IDS_i)$ without $IDS_i$ and $IDS_{i+1}$, or by only holding $H(M_L \oplus R \oplus IDS_i) \oplus IDS_{i+1}$, $M_L$, $R$ without $IDS_i$ and $IDS_{i+1}$.

Table 2 indicates a comparison of results among new protocol and related protocols [1, 2, 4, 12] in terms of security.

**Table 2. Comparison of Security**

| Security requirement | [1] | [2] | [4] | [12] | New |
|---|---|---|---|---|---|
| Tag untraceability | X | O | O | O | O |
| Tag information protection | O | O | O | O | O |
| Spoofing attack | O | O | O | X | O |
| Replay attack | O | O | O | O | O |
| DoS attack | O | O | O | X | O |
| Forward security | O | O | O | O | O |
| Backward security | O | O | O | O | O |
| LEFSP | X | X | X | X | O |
| Suitable for wireless reader | X | O | X | O | O |

'O' denotes satisfied, 'X' denotes not satisfied, 'LEFSP' denotes lightweight encryption function structure protection.

## 5. Conclusion

Recently, wireless readers are used more popularly, it brings higher design requirements for RFID protocols. In this paper, a mutual RFID authentication protocol for wireless reader is proposed, this protocol only requires O(1) work to identify and authenticate a tag in the server. The careful security analysis shows that this protocol can resist spoofing attack, replay attack, DoS attack, and meet tag untraceability, tag information protection, forward security, backward security and lightweight encryption function structure protection.

## Acknowledgements

This work was supported in part by Heilongjiang Province Science and Technology Research Grant of the Education Department No. 12533002.

## References

[1] Z. Shijie, Z. Zhen, L. Zongwei and E. C. Wong, "A lightweight anti-desynchronization RFIDauthentication protocol", Information Systems Frontiers, Information Systems Frontiers Press, vol. 12, **(2010)**, pp. 521-528.

[2] H. Jialiang, O. Dantong, B. Tian and Z. Liming, "A Lightweight RFID Authentication Protocol for Mobile Reader", International Journal of Digital Content Technology and its Applications, AICIT, vol. 6, no. 6, **(2012)**, pp. 80-88.

[3] A. Juels, "RFID security and privacy: a research survey", Journal of Selected Areas in Communications, Institute of Electrical and Electronics Engineers, vol. 24, **(2006)**, pp. 381-394.

[4] H. Jialiang, O. Dantong and X. Youjun, "An Efficient RFID Authentication Protocol Supporting Tag Ownership Transfer", International Journal of Advancements in Computing Technology, AICIT, vol. 4, no. 4, **(2012)**, pp. 244-253.

[5] H. Jialiang, O. Dantong, Z. Xi, J. Jinchao and B. Tian, "Lightweight Encryption Function Structure Protection of RFID Security Protocol", Advances in Information Sciences and Service Sciences, AICIT, vol.4, no.7, **(2012)**, pp. 155-162.

[6] B. Song and C. J. Mitchell, "Scalable RFID security protocols supporting tag ownership transfer", Computer Communications, Elsevier, vol. 34, **(2010)**, pp. 556-566.

[7] D. Henrici and P. Müller, "Hash-based enhancement of location privacy for radio-frequency identification devices using varying identifiers", Proceedings of International Workshop on Pervasive Computing and Communication Security - PerSec 2004, **(2004)**, pp. 149-153.

[8] T. Dimitriou, "A lightweight RFID protocol to protect against traceability and cloning attacks", Proceedings of Conference on Security and Privacy for Emerging Areas in Communication Networks-SecureComm 2005, **(2005)**, pp. 59-66.

[9] G. Tsudik, "YA-TRAP: yet another trivial RFID authentication protocol", Proceedings of Fourth IEEE Annual Conference on Pervasive Computing and Communications, **(2006)**, pp. 640-643.

[10] B. Song and C. J. Mitchell, "RFID authentication protocol for low-cost tags", Proceedings of First ACM Conference on Wireless Network Security, **(2008)**, pp. 140-147.

[11] J.-S. Cho, S.-S. Yeo and S. K. Kima, "Securing against brute-force attack: A hash-based RFID mutual authentication protocol using a secret value", Journal of Computer Communications, Computer Communications Press, vol. 34, **(2010)**, pp. 391-397.

[12] C.-H. Wei, M.-S. Hwang and A. Yeh-hao Chin, "A Mutual Authentication Protocol for RFID", Journal of IT Professional, IT Professional Press, vol. 3, **(2011)**, pp. 20-24.

## Authors

**He Jialiang**, born in 1977, received the PhD degree in computer software and theory from Jilin University of China in 2012 and the Master degree in computer application from Jilin University of China in 2004. Now he is an associate professor at College of Information and Communication Engineering, Dalian Nationalities University, China. His papers have been published in some well-known international Journals and IEEE conferences. His main interests include Mobile Internet, Internet of Things, and Intelligent Business Information Processing.

**Xu Zhiqiang**, born in 1981, received the Bachelor degree in communication Engineering from Communication University of China in 2004 and the Master degree in Electronics & Communication Engineering from Communication University of China in 2012. At present, he is an assistant professor of Communication & Media Institute of Sichuan, China. He is experienced the fields of Mobile Internet, Internet of Things, Intelligent Information Processing, *etc.*, he also is a candidate of MSc of Technopreneurship & Innovation Program in Nanyang Technological University in Singapore.