Ultra-Lightweight Mutual Authentication and Ownership Transfer Protocol with PUF for Gen2 v2 RFID Systems

Hsin-Han Huang, Lo-Yao Yeh, and Woei-Jiunn Tsaur

***Abstract*— Radio Frequency Identification (RFID) is used to replace bar code system. RFID is more powerful than bar code system but it suffers from the weakness of wireless communication. Security issues in RFID systems include tag or reader impersonation, replay attack, eavesdropping, location privacy, forward and backward un-traceability. Appling traditional security mechanism such as MD4, MD5, SHA 256 or AES directly on RFID is impossible due to the hardware limitation of a passive tag. Thus, many studies try to design all new protocols about mutual authentication and ownership transfer on RFID system. Physical unclonable function (PUF) is a new hardware security device that could make their protocols tinier. In order to keep location privacy of tag, most of these works will not use tag's unique identification. Instead, they will use a temporary identification once and update it individually each run. However, in this way, their works will suffer from de-synchronization between the tag and reader, if an attacker blocks some messages. In this paper, we propose protocols about mutual authentication and ownership transfer with PUF that can significantly alleviate this issue because the de-synchronization attacks will not happen in our mutual authentication protocol. On the other hand, our protocol also can be compatible with EPC Gen2v2 standard easily. Besides, our simple and robust methods have better performance.**

***Index Terms*—RFID; PUF; mutual authentication; ownership transfer**

I. Introduction

Radio Frequency IDentification, RFID, can be used to replace bar code system in identification technology. It can provide the same or even more functions than bar code system. Hence, RFID can be applied not only in logistics and supply chain management, but also in some new domains like health care, materials management, objects tracking, etc. RFID uses radio frequency, RF, as communication media instead of optical. This allows RFID can identify multiple targets at the same time without touching. However, due to the weakness of wireless communication, RFID also suffers from security issues.

Manuscript received January 27, 2016; revised February 10, 2016.

Hsin-Han Huang is with Institute of Computer Science and Engineering, National Chiao Tung University, Hisnchu, Taiwan (email: hsinhanhuang.cs01g@g2.nctu.edu.tw).

Lo-Yao Yeh is with National Center for High-performance Computing, National Applied Research Laboratories, Taichung, Taiwan (email: lyyeh@narlabs.org.tw).

Woei-Jiunn Tsaur is with Department of Information Management, Da-Yeh University, Changhua, Taiwan (email: wjtsaur@mail.dyu.edu.tw).

The RFID system consists of tags and reader/back-end-database. Tag with unique identification is deployed on target goods. The reader has more detailed information of tags, and indexes them based on their unique identifications. One reader queries the targeted tag by unsafe radio frequency, but communicates other readers in the safer wire communication with powerful security mechanism. For the purpose of large-scale and wide range applications, tags are limited in cost, size, processing capacity, storage size and non-battery assisted. This kind of tag is also called passive tag. The EPC Gen2v2 standard [1] specifies the requirements of commercially available tags, and only support some restricted operations like cyclic redundancy check, pseudo random number generator and EXOR.

Security issues in RFID system deserve more than a passing notice. Take logistics and supply chain management for example. The standard shipping map comprises manufacturing, transportation, distribution center, delivery and retail. The owner of goods/tag may change intensively, so does the ownership between tag and reader. The handoff of ownership must make sure that the privacy among previous and current owners is isolated. During the ownership holding period, the tag and reader still have to authenticate each other before communicating to avoid the impersonation attack. After successful mutual authentication, we can prevent messages from eavesdropping.

On the other hand, to control the power of reader's antenna for limiting the communication range may reduce the risk of attack. However, inadequate power will cause useless message. That is say, as distance from the reader increases, the number of messages needed to be resent cloud goes up. If the authentication mechanism is complex, the system performance will degenerate very fast due to additional transmission. Hence, striking a balance between security and communication range, and between simple and robust authentication is quite important.

Hardware limitation of a Gen2v2 tag makes the security problems became even more complicated. There is no more than 2,000 hardware gates available can be used for security in passive tag. However, traditional security mechanism like MD4, MD5, SHA 256 and AES cannot be adopted on RFID system directly due to the gate numbers of implementation. Thus, many studies make a new start on designing tiny protocol about mutual authentication and ownership transfer. Physical unclonable function, PUF, is a hardware [4] that makes the use of the race condition in gates and wires to produce the unique identification. That is, for every challenge,

ISBN: 978-988-14047-6-3
ISSN: 2078-0958 (Print); ISSN: 2078-0966 (Online)

a PUF can produce a unique correspond response which differs from other PUF's even if they share same in physical structure. With this feature, some studies [2, 4, 5, 7, and 8] already apply PUF in their design to make their mutual authentication dexterous. On the other hand, both tag and reader do not use tag's unique identification directly in order to avoid tracing of tags. They use temporary tag identification, and update it individually after successful authentication. In this way, if an attacker blocks massages, temporary tag identification will not be consistent between tag and reader, namely de-synchronization.

Based on these research foundations, our protocol also takes advantage of PUF in mutual authentication and ownership transfer. Several pairs of <challenge/response> produced by PUF on tag are preloaded on trusted third party, TTP, then will be released to the reader partially later. Furthermore, temporary tag identification will also be generated by TTP. In ownership transfer, TTP will release partial pairs of <challenge/response> with temporary tag identification to the reader, but only temporary tag identification to tag. By this way, the ownership can be provided as needed just like a service. On the other hand, mutual authentication bases on the fact that only the right tag and reader will share the same pairs of challenge/response and temporary tag identification. The proposed protocol in mutual authentication will not only immune normal attacks (such as eavesdrop, tag/reader impersonation, relay attack, and Man in the Middle), but also alleviate the problem of de-synchronization. In ownership transfer, it can still keep location privacy and forward/backward untracebility.

Our contributions are listed as follows:

1. By leveraging PUF, our authentication mechanism is more simple and robust.
2. The issue of de-synchronization between tag and reader can be significantly alleviated because only ownership transfer/update protocol is possible to be attacked.
3. Our protocol is the first work to combine PUF and can be compatible with EPC Gen2v2 standard.

The rest of this paper is organized as follows. More information about related work is given in Section II. Concrete protocols including mutual authentication and ownership transfer are given in Section III. Analysis of proposed protocols about security issues is given in Section IV. We demonstrate the elegant and robust about proposed protocols in Section V. Finally, this work is concluded in Section VI.

II. Related work

We first denote challenge as c, corresponding response as r, PUF function as p(.), and p(c) will equal to r. Each challenge will have a unique response produced by PUF, and [4][8] use this feature to verify tag. PUF on tag can produce distinct pairs of <challenge/response>, {(c, r)}, then server stores these data for authentication in advance. Obviously, only the correct tag can answer the right response to the challenge. Subsequently, [6] and [9] make some improvements. Pairs of <challenge/response> are not stored in server beforehand, but are provided by tag directly. After successful mutual authentication, tag will offer server new (c, r) for next run. Obviously, their works will not work in ownership handoff. Moreover, there is a problem of de-synchronization in these ways. [2] also tries to take PUF in their mutual authentication. But, [5] shows that there still exist some problems in secret disclosure attack, traceability attack, reader impersonation attack and de-synchronization attack on [2].

The work of [7] makes use of PUF as a mask generator to keep messages exchanged from sight. In addition, the tag and reader use temporary tag id instead of unique tag id in communication. After successful authentication, the tag and reader update temporary tag id individually to avoid the traceability attack. Their protocols about authentication can also immune most attacks. Unfortunately, if an attacker blocks some of messages, this method will suffer from de-synchronization attack.

In [3], pairs of challenge and response produced by PUF on tag also be preloaded on server. These data are organized in the form of (tag-id, {c- p(c)-p(p(c))-p(p(p(c)))}), called key-chain. Reader can download few key-chain from server for authentication dynamically. During authentication, tag and reader use one key-chain as session key to verify each other. In fact, a successful authentication needs 5 messages in communication. Also, it is difficult to be applied in the scenario of ownership transfer, let alone be applied in supply chain.

Trusted third party, TPP, is introduced by [11] for their ownership transfer. TTP controls the ownership handoff and makes sure the forward/backward un-traceability between readers. In the phase of mutual authentication, linear feedback shift register, LFSR, and PUF are used to generate mask and update the temporary tag id each run. In each successful run, the tag id and shared key are updated individually. Overall, [11] needs 4 messages in mutual authentication and 2 messages in ownership transfer. However, [10] pointed out there is still message blocking attack, de-synchronization attack, and the misuse of LFSR problems in authentication; besides, ownership transfer cannot avoid attack on traceability of tag.

TTP also be adopted by [12] for their ownership transfer. Their mutual authentication customized "authentication" message to be compatible with EPC Gen2v2 standard. Their work also suffers from de-synchronization attack.

III. Proposed method

A. Pre-condition/Assumption

We assume that the following pre-conditions and assumptions in the RFID system. Each tag is a passive one, so the processing capacity, storage size and hardware complexity of a tag is strictly limited. All tags are non-battery assisted, and draw power from readers. Furthermore, they only support operations such as cyclic redundancy check, pseudo random number generator and EXOR that are specified by EPC Gen2v2. Tag with PUF attached on goods has its unique identification named EPC (or PIN). Every tag shares its EPC only with TTP. All previous and current owners of the tag will know nothing about EPC.

Reader communicates with tags in unsecure wireless channel. On the other hand, reader links other readers or TTP

ISBN: 978-988-14047-6-3
ISSN: 2078-0958 (Print); ISSN: 2078-0966 (Online)

in secure wire with traditional security mechanism such as TLS. A reader has the ownership of one tag for some time period. While only an ownership subsists, the reader can authenticate, query, and exchange information with the tag.

TTP will keep all information about each tag in detail. The information includes the unique identification named EPC (or PIN), pairs of <challenge/response> generated by the PUF embedded in the tag, and the current owner for every tag. TTP will not only verify the reader, but also control the ownership handoff between them. Instead of using unique identification of tag, TTP will release a temporary identification to the tag and reader for communicating, called TempID.

B. Mutual Authentication

The reader broadcasts (TempID ⊕ r') and its corresponding challenge c' to all Tags. Each tag computes the response r" by its PUF. Only the target tag can get the correct r', then decode its TempID. Now, target tag knows this reader has the correct TempID and the pair of <challenge/response>. Therefore, the reader has authenticated. Other non-target tags will not calculate the right response r" or get its TempID, so it ignores this broadcast.

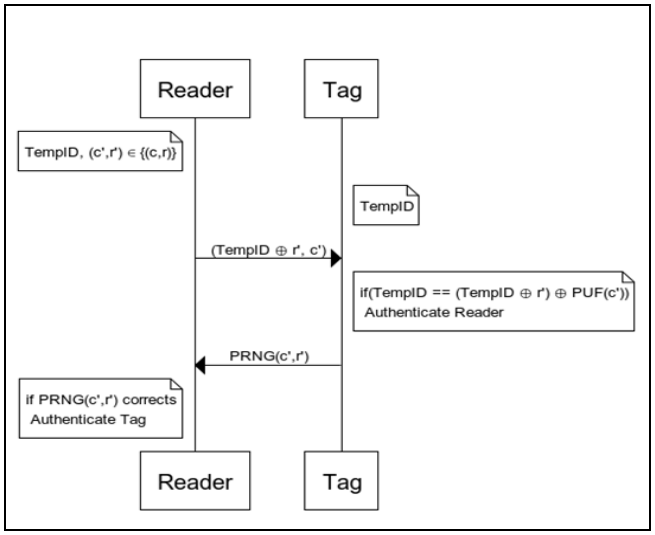

Fig 1 Protocol of mutual authentication

After authenticating the reader, the target tag will return message PRNG(c', r') to reader. Only the target tag knows the right response r' as well as calculates the correct PRNG(c', r'). If so, the reader authenticates the tag. Otherwise, the reader will terminate the connection. Finally, the (c',r') serves as the session key to encode the following communication.

Both the tag and reader will time out and return from their security state to normal state, if each of them does not receive any expect message in time. To be compatible with EPC Gen2v2 standard [1], all we need is to customize our protocol in "Authenticate" message.

C. Ownership Transfer/Update

The reader may run out of his pairs of <challenge/response> for some target tags, or the reader may try to get the new ownership of some tags. Anyway, if the reader needs to have or renew the ownership of some tags, it should submit ownership transfer/update to TTP.

The reader should hand in his pairs of <challenge/response> to TTP, if has. TTP checks eligibility of the request and reader. After successful verification, TTP will return the reader new pairs of <challenge/response>, and new TempID of the target tag. In the same time, TTP also makes the tag update his own TempID. In the last stage of ownership transfer/update, TTP will cross out all pairs of <challenge/response> that are released to the old reader, as shown in Figure 2. It is worth to mention, the desynchronization problem may occur in the ownership transfer/update protocol. Fortunately, [14] also states that the denial of service, DoS, attack is usually not under consideration in ownership transfer protocol.

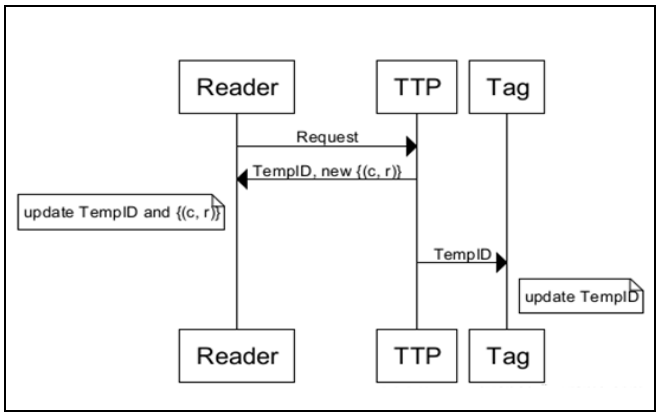

Fig 2 Protocol of ownership transfer/update

IV. SECURITY ANALYSIS

1. Tag/reader impersonation: In mutual authentication, the pair (c', r') and TempID only be shared by both the right reader and tag. A counterfeit reader cannot generate the right (TempID ⊕ r'); on the other hand, a counterfeit tag will not produce the right r' and corresponding PRNG(c', r').

2. Replay attack/eavesdrop: An attacker will not be able to generate the correct r', even if he knows c' by eavesdropping. After authenticating each other, both the reader and tag will use (c', r') as the session key to encode their communication. If someone tries to replay message (TempID ⊕ r', c') or PRNG(c', r') to be authenticated, he will still get nothing useful ever after.

3. De-synchronization problem: In our protocol, both the reader and tag will not update TempID or some shared key individually after each successful communication. Hence, there is no de-synchronization problem in mutual authentication phase. Only in ownership transfer/update phrase, both the reader and tag will update their shared TempID generated by TTP.

4. Location privacy: The message that contains identification of target tag, TempID, is masked by r'. This masker, r', only be used once in a communication, and will be changed next run. Consequently, there is no way to lock target tag and trace its location.

5. Forward/Backward un-traceability: Although the previous and current owners will have correct pairs of (c', r') for the same tag, only the current owner shares the right TempID with this tag. The previous and current owners will not be

ISBN: 978-988-14047-6-3
ISSN: 2078-0958 (Print); ISSN: 2078-0966 (Online)

disturbed.

6. Windowing problem: Tag has only one TempID at the same time. Hence, there is only one reader can be the owner.

V. EVALUATION

This evaluation will show that how the required numbers of massages in a security mechanism influences the performance of mutual authentication.

In [12], authors reveal the relationship between distance and successful OT messages. As distance between the reader and tag increasing, the power received from reader decreasing and so are successful messages. In other words, the probability of a message to be received successfully is inversely proportion to the distance between them.

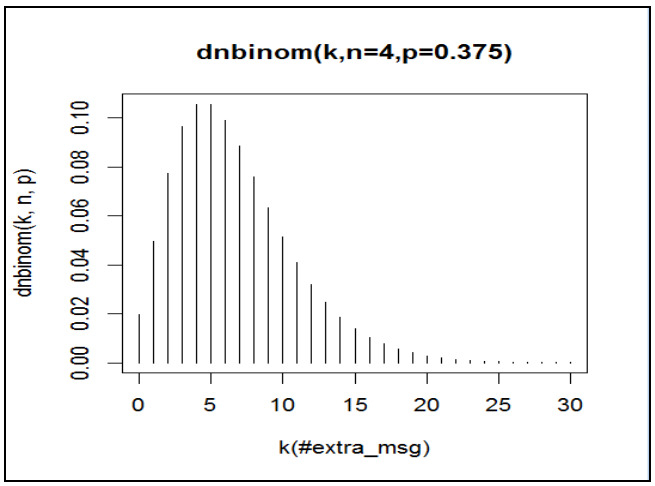

Fig 3 Distribution of additional messages with 4 successful messages

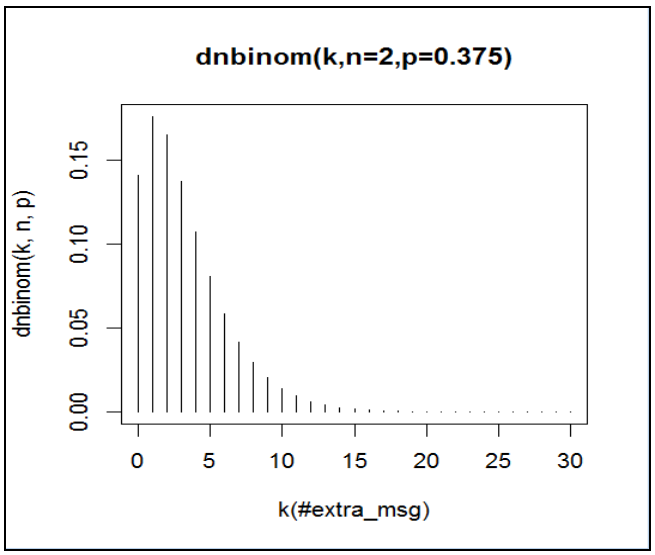

Fig 4 Distribution of additional messages in our work (with 2 successful messages)

In the definition of negative binomial distribution, every trial will successes or fails, but final trial must success. The successful numbers of trials are given, but total numbers of trials needed are a distribution can be modeled by negative binomial distribution.

Without loss of generality, we refer [12] and can assume the probability be 0.375 of a successful message in the distance 2.5 m. In [11], completing the mutual authentication needs 4 successful messages to be exchanged. On the other hand, our protocol only needs 2 messages. We show the difference of performance between them by negative binomial distribution.

To complete mutual authentication, figure 3 and 4 show the relationship between the probability, y - axis, and exact number of messages needed to be resend, x-axis. Figure 3 shows the distribution of resend messages in [11]. In most cases, it only needs extra 5 messages to complete mutual authentication. However, in the worst case, 25 additional messages are needed. Figure 4 shows the situation of our work. In most cases, 1 extra message is need. In the worst case, no more than 17 additional messages are needed. This is why we claim our protocol is simple and robust.

VI. CONCLUSION

In this paper, we leverage physical unclonable function, PUF, in our mutual authentication mechanism. By this way, the protocol of our mutual authentication is more simple and robust. Consequently, the issue of de-synchronization between tag and reader can be alleviated. Our protocol can be compatible with EPC Gen2v2 standard by embedding in “authentication” message.

REFERENCES

[1] R. Air, I. Protocol, and M. Version, “EPC TM Radio-Frequency Identity Protocols Generation-2 UHF RFID Specification for RFID Air Interface,” pp. 1–152, 2013.

[2] R. Bassil, W. El-Beaino, A. Kayssi, and A. Chehab, “A PUF-based ultra-lightweight mutual-authentication RFID protocol,” 2011 Int. Conf. Internet Technol. Secur. Trans., vol. 1, no. June, pp. 495–499, 2011.

[3] Y. Xu and Z. He, “Design of a Security Protocol for Low-Cost RFID,” 2012 8th Int. Conf. Wirel. Commun. Netw. Mob. Comput., pp. 1–3, 2012.

[4] S. Devadas, E. Suh, S. Paral, R. Sowell, T. Ziola, and V. Khandelwal, “Design and Implementation of PUF-Based ‘Unclonable’ RFID ICs for Anti-Counterfeiting and Security Applications,” IEEE Int. Conf. RFID, pp. 58–64, 2008.

[5] M. Safkhani, N. Bagheri, and M. Naderi, “Security Analysis of a PUF based RFID Authentication Protocol,” ePrint Arch., pp. 1–10, 2011.

[6] Y. S. Lee, Y. Park, S. Lee, T. Kim, and H. J. Lee, “RFID mutual authentication protocol with Unclonable RFID-tags,” Int. Conf. Mob. IT Converg., pp. 74–77, 2011.

[7] Z. He and L. Zou, “High-Efficient RFID Authentication Protocol Based on Physical Unclonable Function,” 2012 8th Int. Conf. Wirel. Commun. Netw. Mob. Comput., pp. 1–4, 2012.

[8] D. Jiang and C. N. Chong, “Anti-counterfeiting using phosphor PUF,” in 2nd International Conference on Anti-counterfeiting, Security and Identification, 2008, pp. 59–62.

[9] K. Lars, Y. Zhen, W. Yawen, and G. Yong, “Lightweight secure search protocols for low-cost RFID systems,” Proc. - Int. Conf. Distrib. Comput. Syst., pp. 40–48, 2009.

[10] X. Kardas, S., X. Akgu, M. N, M. S. Kiraz, and H. Demirci, “Cryptanalysis of Lightweight Mutual Authentication and Ownership Transfer for RFID Systems,” Light. Secur. Priv. Devices, Protoc. Appl. (LightSec), 2011 Work., pp. 20–25, 2011.

[11] L. Kulseng, Z. Yu, Y. Wei, and Y. Guan, “Lightweight mutual authentication and ownership transfer for RFID systems,” Proc. - IEEE INFOCOM, 2010.

[12] Haifeng Niu and S. Jagannathan, “‘A Gen2v2 Compliant RFID authentication and ownership management protocol”, Proc. of the IEEE Conference on Local Computer Networks, pp. 331-336, September

ISBN: 978-988-14047-6-3
ISSN: 2078-0958 (Print); ISSN: 2078-0966 (Online)