Review on RFID Identity Authentication Protocols Based on Hash Function

Yang Bing[1,a], Liu Baolong[2,b] and Chen Hua[3,c]

[1,2,3] School of Computer Science and Engineering, Xi'an Technological University,

Xi'an 710021, China,

Email:[a]1769579475@qq.com,[b] 24503148@qq.com

Abstract. Radio frequency identification (RFID) is one of the key technologies of Internet of Things, which have many security issues in an open environment. In order to solve the communication problem between RFID tags and readers, security protocols has been improved constantly as the first choice. But the form of attack is also changing constantly with the development of technology. In this paper we classify the security protocols and introduce some problems in the recent security protocols.

Keywords: RFID, protocol, Hash, authentication, attack

1. RFID System Introduction

Radio Frequency Identification (RFID) is a non-contact automatic identification technology, it uses Radio Frequency signal to complete the automatic identification to obtain relevant information of target acquisition, at the same time complete the exchange of information among the target objects, having a wide range of applications among Internet of things. RFID is widely used in the fields of access control, logistics, monitoring, tracking, anti-counterfeiting, identification, security, military, and medical treatment because of its non-contact, fast identification of moving objects, high identification efficiency, can work in harsh environment and convenient operation and so on, But at the same time caused a lot of security issues.

A typical radio frequency identification system consists of a reader (Reader), a tag (Tag), and an antenna (antenna), as shown in Fig.1. In the physical configuration, the tag consist of the RFID front end, the antenna, identity information, the digital baseband for storing information and processing protocols, As a result, the tag can store identity information, usually placed on objects that require authentication. Reader and tag communicate through the radio interface with the background database connection. In the RFID system, the implementation of the label data is the key to information retrieval, we can obtain the label information in the back-end database to understand the special information of the product. The product information needs certification, logistics records and key information management can be saved in the end database.

There are two main defense methods in the face of RFID system security issues: passive detection (physical methods) and active defense (security protocol). As passive detection reduces the utilization

of tags, there are some difficulties to implement, so some active security mechanisms (security authentication protocols) are preferred. The second part introduces the attack model and security requirements of the RFID system. The third part introduces the classical security protocol of the RFID system. The fourth part introduces the research status of the classic protocol. The last part is the summary.

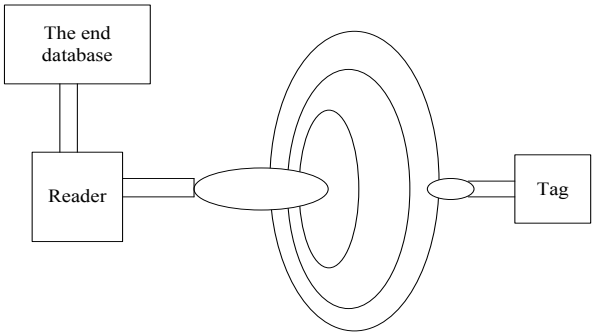

Figure.1 RFID system

2. RFID Attack Model and Security Requirements

2.1 Attack Model Introduction.

RFID systems are vulnerable to suffer attack of various forms, because RFID readers and tags transmit information by wirelessly. RFID security protocols as a solution to security threats, the various forms of attack will be introduced firstly.

● ***Personate Attack.*** A clone tag attack that allows the reader to believe that the received data is from a legitimate tag. An attacker can create an authenticated tag through entering the appropriate format data in a blank tag.

● ***Replay Attacks.*** An effective data transfer is recorded by the attacker and maliciously repeated or sent back between the tag and the reader in an insecure channel between the tag and the reader. Such as a device (not necessarily a tag), masquerading as a trusted entity, and playing back a tag response message to the reader. Another way is to maliciously replay legitimate readers' requery to the tag, aims to retrieve the tag' s private information, in order to avoid this happening, the response of each tag and the reader must be unique in every round.

● ***Tracking Attacks.*** This attack is considered the most important prevention attack which can cause a significant loss of privacy to the label holder. It is easily to be tracked if any information can be connected to a given tag. Thus updating information can prevent such attacks after each successful authentication.

● ***Man-in-the-Middle Attack and Information Disclosure.*** The attacker controls the flow of information by replaying or modifying information between the tag and the reader, at the same time the reader and tag do not detect any anomalies in this attack.

● ***DOS Attacks.*** Similar to tracking attacks, this attack is a major concern in RFID systems. These attacks are easy to achieve, but difficult to prevent. One method is that an attacker maliciously collides with a tag, causing the reader to load more data than they can handle; the other is an attacker blocks

messages that are transmitted between the tag and the reader. The attack could cause desynchronize messages between the tag and the reader.

● ***Forward Attack.*** A system is belong to forward security means the current label response message eavesdropped by the attacker is not linked the previous response message.

2.2 Introduction to security requirements.

In an RFID system, the reader sends a response message received from the tag to the backend database. The database would compare feedback information received from the label, while the database needs to send the news to the label passed the authentication, the label also must carry on the authentication to the database' s identity. In the mutual authentication process, the forgery data must be prohibited from being authenticated. However we must find an effective way to prevent the attacker from modifying the authentication information because the wireless channel between the tag and the reader. In the design of RFID authentication protocol, we must consider the following aspects of the security requirements:

● ***Confidentiality.*** Electronic tags can only send messages to valid readers and can not reveal any valuable information to attackers during system operations. Once the attacker has access to valuable information, the identity of the label information may be leaked. Therefore, a complete RFID security solution must be able to ensure that the information contained in the label can only authorize the reader to access.

● ***Indistinguishability.*** The output value of the tag is required for each authentication is not the same and not directly linked the tag ID value. If an attacker can distinguish a specific output from a target tag, thus the tag can be tracked, that is so-called the anonymity of the tag.

● ***Authenticity.*** It refers to the prohibition of false electronic tags to deceive the reader or server.

● ***Forward Security.*** If an attacker obtains the privacy information of the tag, the tag cannot be tracked. That is, although the adversary obtains the tag' s output information but couldn' t contact the previous round of information.

● ***Efficiency.*** Though efficiency is not included in the security requirements, passive tags in the protocol need to operate hash function XOR operation and so on. Thus efficiency is a necessary factor to consider in the design of security protocols.

3. Introduction to Classic Security Protocols

3.1 Hash—lock protocol.

Hash-lock protocol [2] is proposed by Sarma et al. in order to avoid information disclosure and tracking, in which use meta ID to replace the real tag ID, the protocol flow shown in Figure.2. In this protocol, the tag does not have a dynamic refresh mechanism and the meta ID remains unchanged during the authentication process, further more the tag ID is transmitted in plain text over an unsecured channel. Thus Hash-lock protocol is vulnerable to fake attacks, replay attacks and tracking -positioning attacks.

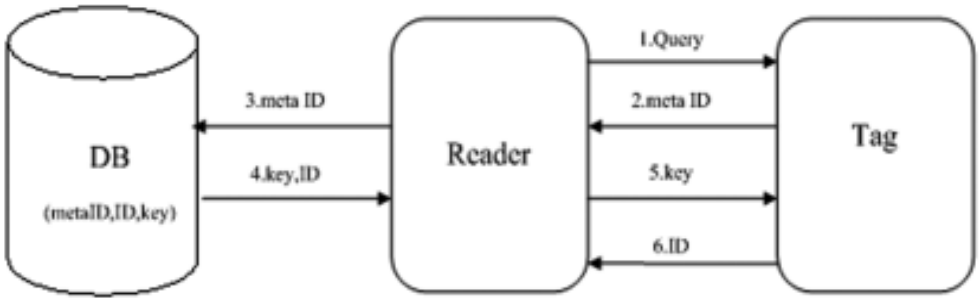

Figure.2 Hash—lock protocol

3.2 Randomized Hash—lock protocol.

In order to solve the problem of position tracking in Hash-lock protocol, Weis et al proposed Randomized Hash-lock protocol [3], using query-reply mechanism of the random number, the protocol flow shown in Figure.3. In this protocol, a pseudo-random number generator is used to increase the amount of label operation within the allowable range of label cost. Tag ID remains unchanged, and the plaintext is still sent between the tag and the reader, causing this protocol is vulnerable to counterfeit attacks, replay attacks, were tracking attacks. In order to validate each tag, the reader must effectively compute the hash value of the each tag ID stored in the back-end database, the resources consumed by the whole authentication process are huge, it is easy to cause DOS attack, and does not apply to a large number of label attestation.

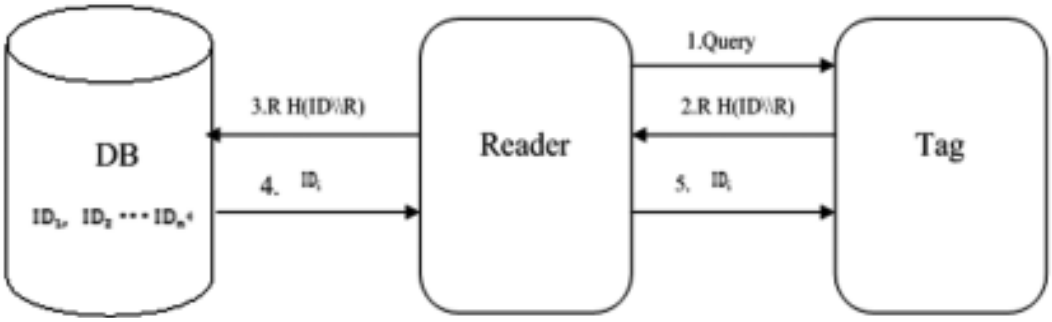

Figure.3 Randomized Hash—lock protocol

3.3 Hash—chain protocol.

Hash-chain protocol [1] is proposed by Ohkubo et al., which is also based on the challenge-response mechanism, the protocol flow shown in Figure.4. Tag and the back-end database share an initial secret value. The protocol resolves the forward security problem when the reader sends an authentication request to the tag, and the tag sends a different response. But in the protocol only reader authenticate the identity of the tag, the tag does not authenticate the identity of the reader, so it is vulnerable to personate attacks and replay attacks. Meanwhile Back-end database' s search work is huge, for each round needs to look up $m \times n$ times, where m is the chain length, n is the number of ID. And ID space is large under normal circumstances, such as up to 128 bits. To ensure randomness, where m should be large enough, as a result it is easily to lead DOS attacks.

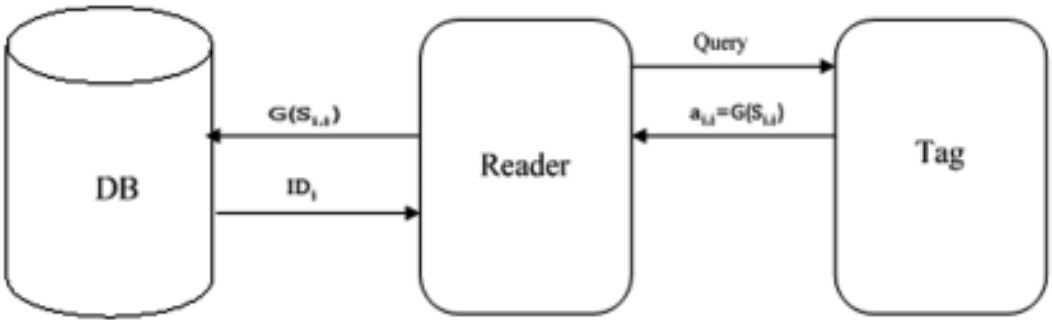

Figure.4 Hash—chain protocol

4. Research Status of Security Protocols

The existing security protocols are divided into four categories, the first type proposed improved protocol respectively security protocol based on the shortcomings of Hash-lock protocol for the study, which also divided into four specific cases, the first section summarized respectively; next type proposed protocol based on the shortcomings of the Randomized Hash-lock protocol; the third type proposed improvement protocol based on Hash-chain protocol; the last type is based on the above three basis protocol, taking into account the safety and efficiency and cost of the label factors fully, proposed comprehensive protocol. The following will be introduced respectively.

4.1 Security protocols based on Hash - lock protocol.

For the shortcoming of the Hash-lock protocol, Lee [15] proposed protocol keep using meta ID instead of the real tag ID value in the original protocol, meanwhile using semi-random access control (SRAC), which provides mutual authentication and good security to prevent tracking attacks, fake attacks, DOS attacks, but in the case that the attacker eavesdropped and playback Meta ID, tags can also be successfully authenticated by legitimate readers, thus the protocol does not have anti-replay attacks. Subsequently, a low-cost RFID authentication protocol (LCAP protocol) was proposed in [14], which uses the challenge-response scheme to ensure the positional privacy of the tag holders. However, if the attacker eavesdropped the current label response, message could be inferred the previous message tags responded and sent, and the protocol cannot provide forward security. Choi et al. [17] proposed an improvement scheme based on the protocol [14] in which the labels are grouped and the back-end database is assigned to each group index also saved in the tag. The shared key and an initialization value and the like are stored in the tags and database.

This protocol does not reveal the tag’s privacy information, using random numbers and counter variables to ensure location privacy, anti-trace attack and impersonation attack, but it is not completely safe. The attacker can derive the previous response information by tapping the response message of the current label, so it doesn’t provide forward security. In [18], an improved scheme is proposed by Choi et al. Taking account into forward security and synchronization attacks, it provides forward security but doesn’t authenticate the reader identity regretful.

One improvement protocol is a serverless system and the two entities involved in authentication are tags and readers. Tan et al. [8] pointed that if the reader and the back-end database couldn’t create a secure and continuous network connection, RFID systems would not be used, if that will limit the application

of RFID systems in remote areas. Thus a server-free security authentication protocol is proposed. In which the back-end database is used as the certification authority (CA) to write the label's secret value into the tag and initialize it, and the reader must obtain authorization from the CA to access a specific set of tags. As well each legitimate reader downloads the authenticated access table from the CA. This protocol is not a strict authentication protocol and cannot guarantee the anonymity of the tag ID, because the communication between the reader and the CA is considered to be secure.

In the references [10,11,12] proposed some protocols based on the Tan et al. Protocol and successfully resist major attack models, including tracking, eavesdropping, and clone attacks. In the scheme [10, 11] achieved mutual authentication and symmetric key setting are implemented, but symmetric key may cause other problems. In scheme [11], the reader and the tag share the key in other states, and the reader identifies the tag with a random number, meanwhile dynamic information must be synchronized between the reader and the tag in order to successfully operate the system. In this case, an attacker can initiate a asynchronous attack to break the synchronization and face the problem of asynchronization.

At the same time, Ha et al. [19] also proposed a serverless security authentication protocol, each tag needs to maintain a state parameter SYNC, that is, the state protocol, but it is well known that the security protocol in RFID is stateless, , each tag and reader does not need to maintain any status information, and the management of the status values in the tags is cumbersome in the communication session. For example, the attacker will be very easy to get the label to protect privacy information after the label's calculation error will change the SYNC value. In this case, the attacker can re-set the state value to 0 when the tag in the session does not successfully end the communication, causing the tag to not work properly. The protocol has a forward privacy threat, and the protocol's security depends on the tag ID during the update session to provide the forward privacy service. Two kinds of attack means are listed in the reference [20] aimed at protocol [19], can destroy its forward privacy, an improved stateless value is proposed in addition, but it is also a serverless security protocol.

One kind of improved scheme is just to consider the forward security. In reference [9], the back-end database and the label share the shared key. The reader only transmits the tag and the back-end database. The tag ID value is not updated, but the key value is updated after each successful authentication.

Other improved scheme does not consider the synchronization problem. In reference [4, 5, 6], some improved methods based on Hash-lock protocol are proposed. The new protocols avoid the tracking attack when the reader accesses the tag receive different response message every round. There are still security flaws. For example, the label ensures the cost and security, but it is not a good solution to the synchronization problem of the label and database in reference [6].

4.2 Security protocols based on Randomized Hash—Lock protocol.

Because of its practicality, there are rarely improved protocols based on Randomized Hash-Lock protocol. The practicality is that the mutual authentication process is completed by only two exchanges of information. Compared other security protocols, mutual authentication cannot be completed by two exchanges of information, at least three to four steps are required to exchange information, and just only one-sided authentication is required such as Tan et al. [8]. Compared to reference [16] maintains the previous authentication step, only transmits the tag ID value to the original protocol in the last step. The improved protocol adds a hash function to the reader and the transmitted message is a hash function consisting of random number and tag ID value, this improved security significantly but at the

same time have high memory consumption, just for only for small networks. Future research may look for a scheme that keeps authenticating each other during the communication process, not just at the beginning of the session, since the authenticated tag is unlocked and its risk of being deceived by the reader can be significantly reduced.

4.3 Security protocols based on Hash—chain protocol.

ID tag in the Hash-chain protocol is dynamically updated, also known as dynamic ID authentication protocol. For it does not authentication the identity of the reader, so this is vulnerable to personate attacks and replay attacks and its back-end database search work is huge and other shortcomings. Thus reference [24] combined with three-way handshake agreement, proposed to create a two-way authentication method serial number in the communication time to encrypt information, but the agreement belongs to the serverless system.

Reference [13] pointed out that Luo et al.' s protocol used two hash functions to update the key value. The reader only communicated the communication between the tag and the back-end server, and almost omitted the reader in the protocol. The counter will also increment the tag value after each round of authentication. When the server sends a request for authentication to the tag, the tag responds to the counter, the counter hashes and the shared key, after the backend server verifies that the random number of sessions is used as the encryption key. However if the count value of one tag is significantly different from the count value of the surrounding tag, the attacker can track the tag according to the count value of the tag in this protocol. In addition if the attacker sends a query request to the tag and the count and key values of the tag are not changed by a valid server, the tag would respond to the same value and attacker can track this tag. Or if an attacker listens to a second session and changes the response value, it is considered to be valid by the tag, and then the tag responds with a message sent by the attacker to the reader. The reader surely cannot decrypt the message. If a lot of tags are attacked, the protocol would suffer DOS attack. At the same time it also analyzed the protocol of Lee et al. specific about the attacker' s personate tag to send a message to the reader, eavesdrops the random number s sent by the reader to the tag, and changes the value to 0, eavesdrops the tag' s return value, and modifies the sending reader, so the agreement is vulnerable to personate attacks.

There are improved protocol based on Hash Chain protocol In reference [21, 22], for example, reference [22] uses a hash function to approximate the randomness, the protocol does not change the secret value in the hash chain, only a hash function to achieve the dynamic update of the label to reduces the huge amount of queries in the backend database in the original protocol meanwhile its time complexity decreases from $O(m \times n)$ to $O(m+n)$. However, the two protocols only improve the security flaws of the original protocol, but the back-end database has exhaustive search and large number of hash operations in verifying the identity of the tags and readers and the efficiency is not obviously improved, so it is not suitable for large tags to be widely used.

4.4 Comprehensive improvement protocols.

In the design of the protocol, the tag only could bears a lower calculation cost, just including the hash function and the random number operation. so the authentication server part of the protocol undertakes a lot of computation and low efficiency. After studying these protocols, in order to overcome this shortcoming, the researchers have done a lot of work can be divided into three general types.

The first type is about the hash value of the ID and other information sent by the tag [3] and the server can pre-calculate and store the hash value to the backend database. Upon receiving the label response message, the server can find the tag ID stored in itself. In general a protocol requires O (1) computational efficiency to validate a tag, using an efficient hash map instead of traversing all tag ID operations. These protocols have a good reliability and anti-traceability, however an attacker can intercept messages sent from the server and then replay the messages to the tag. By comparing the response messages of the tags, the attacker can track the target tag because the response message is fixed before the successful authentication.

The second type of the improved protocols based on tree, packet and shared key idea in order to overcome the deficiency of tag tracking attacks in the first class, hence these protocols improve the key search efficiency of the server and reduce complexity from linear to logarithm, but these agreements are vulnerable to compromise attacks. Based on the tree protocol, such as reference [24], using the tag as a leaf node in the tree, and the key assigned to the internal node. The server stores all the keys and each tag also stores its own key and the associated key $O(\log N)$ from the leaf node to the root node.

During the authentication process, the tag would respond with a hash of the $O(\log N)$ key and a random number, and the server can verify the root key value of the tag. However, tree-based protocols are vulnerable to compromise attacks because each tag shares a set of keys with other tags in the tree structure. Similarly Group-based protocols are also vulnerable to compromise attacks since each group’ s labels share a single key. For example, in reference [25], the tag shares a protection key with the server, and the tag sends the hash value of the protection key to the server that can calculate the hash value during the authentication process. However the protection key in the protocol is shared in the label is known so it is vulnerable to compromise attacks.

Reference [27] proposed a protocol for passive tags but only consider the forward security, and the label of the agreement is too large, which does not meet the low-cost requirements.

Table 1 Security of different protocols

Security attributes	Personate attacks	Replay attacks	Tracking attacks	DOS attacks	Forward security
literature[1]	✓	✓	×	○	✓
literature[2]	✓	✓	✓	×	○
literature[3]	✓	✓	✓	○	✓
literature[14]	×	×	×	○	×
literature[15]	×	✓	×	×	✓
literature[17]	×	×	×	○	×
literature[18]	✓	○	○	○	✓
literature[19]	○	○	○	✓	×
literature[8]	○	✓	○	✓	✓

×: does not exist ○: partially exist ✓: exist

5. Conclusion

This paper first introduces the attack types and security requirements of RFID system recently, and the three classical protocols including Hash-lock protocol, Randomized Hash—lock protocol and Hash-chain protocol based on Hash function, as well as the problems of these protocols including improved protocol based on classical protocols would be illustrated in Table 1. For these shortcomings, the existing security protocols are divided into four categories, of which the first three are based on the improvement of three classic protocols, the last one is based on three classic protocol solutions moreover considering the safety and Efficiency and the cost of tag. However there are a variety of problems in security protocols, including security flaws, efficiency issues, and non-compliance with large-scale tags. At present, there is no good security protocol is recognized as safe, feasible, efficient and so on, the future work is still gathered in how to design a reliable, safe and efficient RFID security protocol.

Sponsors or Supporters

This work is partially supported by Science & Technology Program of Weiyang District of Xi'an City with project "201609", the Science & Technology Program of Department of Shaanxi Education with project "15JK1350".

References

[1] Ohkubo M, Suzuki K, Kinoshta S, "Hash-chain based for-ward-secure privacy protection scheme for low-cost RFID" Proceedings of the 2004 Symposium on Cryptogra-phy and Information Security. Berlin: Springer-Verlag,2004,pp.719-724.

[2] Sarma S, Weis S, Engels D, "RFID systems and security and privacy implications," Proc of the 4th Int Work-shop on Cryptographic Hardware and Embedded Systems. Berlin: Springer, 2002,pp. 454-469.

[3] Weis S A, Sarma S E, Rivest R L, "et al.Security and privacy aspects of low-cost radio frequency identification systems," Proc of the 1st Security in Pervasive Com-putting.Berlin: Springer, 2003,pp.201-212.

[4] Taoyuan, Zhou Xideng, "Mobile mutual authentication protocol based on hash function," Journal of Computer Applications, 2016, 36 (3),pp.657 - 660.

[5] Hou Jinhuan, Ding Fuqiang, "New things RFID security protocol analysis and design of," electronic technology and software engineering, 2015.

[6] Zhao Ting, Wang Jian, "Dynamic RFID authentication protocol," 2010 Hash function of the National Communications Security Conference on.

[7] Guo Wei, "Improvement of HASH Chain Protocol in RFID," second national information security protection technology conference proceedings, 2013, 6, 21.

[8] C. Tan, B. Sheng, and Q. Li, "Secure and serverless rfid authentication and search protocols," vol. 7, no. 4, april 2008, pp. 1400 - 1407.

[9] Minghui Wang, Yongzheng Tang, Fang Shi, Junhua Pan, "An effective RFID authentication protocol," 2012 2nd International Conference on Consumer Electronics, Communications and Networks (CECNet), pp.141 – 144.

[10] Tan C., Sheng B., and Li Q., "Severless search and authentication protocols for RFID," In Proceedings of the Fifth Annual IEEE International Conference on Pervasive Computing and Communications(PerCom '07), New York, USA. pp. 3-12 .
[11] Ahamed, S. I., Rahman, F., and Hoque, M., Kawsar, E, and Nakajima,T, "YA-SRAP: Yet another serverless RFID authentication protocol," In Proceedings of the 4th IET International Conference on Intelligent Environment (IE08). Seattle, USA. pp. 1-8,2008.

[12] Feng Zebo, Wu Xiaoping, Liu Haohan, "RFID security authentication protocol a new free end database," Journal of Naval University of engineering, 2015,02,pp.32-36.

[13]Selwyn Piramuthu, "RFID mutual authentication protocols," Decision Support Systems, Vol.50, Issue 2, January 2011, pp.387-393.

[14] Su Mi Lee, Young Ju Hwang, Dong Hoon Lee, Jong In Lim, "Efficient Authentication for Low-Cost RFID Systems," Lecture Notes in Computer Science. Berlin, vol.3480, pp. 619-627,2005.

[15] Yong Ki Lee, Ingrid Verbauwhede, "Secure and Low-cost RFID Authentication Protocols," Proceedings of the 2nd IEEE Workshop on Adaptive Wireless Networks, 2005.

[16] Kaleb Lee, "A Two-Step Mutual Authentication Protocol Based on Randomized Hash- Lock for Small RFID Networks," 2010 Fourth International Conference on Network and System Security, pp. 527 – 533.

[17] Eun Young Choi, Su Mi Lee, Dong Hong Lee, "Efficient RFID Authentication Protocol for Ubiquitous Computing Environment," Embedded and Ubiquitous Computing, vo1.3832, pp.945-954, 2005.

[18] He Lei, Lu Xin-mei, Jin Song-he, Cai Zeng-yu, "A One-way Hash based Low-cost Authentication Protocol with Forward Security in RFID System," 2010 2nd International Asia Conference on Informatics in Control, Automation and Robotics (CAR 2010)[2],pp.269 – 272.

[19] J. H. Ha, S. J. Moon, J. Y. Zhou, and J. C. Ha, "A new formal proof model for RFID location privacy," in: S. Jajodia and J. Lopez, editors, Proceedings of 13th European Symposium on Research in Computer Security – ESORICS'08, LNCS 5283, Springer – Verlag, pp. 267 – 281,2008.

[20] Da-Zhi Sun, Ji-Dong Zhong, "A hash-based RFID security protocol for strong privacy protection," IEEE Transactions on Consumer Electronics (2012) Vol.58, Issue: 4, pp.1246 – 1252.

[21] Liang Huan qi, "Research of Mutual Authentication Protocol for RFID Based on Hash Function and Public Key," South China University of Technology, 2012.

[22] Jianliang Meng, Ze Wang, "A RFID Security Protocol Based on Hash Chain and Three-Way Handshake," 2013 International Conference on Computational and Information Sciences,pp.1463 – 1466.

[23] Yanfei Liu, Sha Feng, "Scalable Lightweight Authentication Protocol with Privacy Preservation," 2014 Tenth International Conference on Computational Intelligence and Security, pp.474 – 478.

[24] T. Li, W. Luo, Z. Mo, and S. Chen, "Privacy-preserving RFID authentication based on cryptographical encoding," IEEE INFOCOM,2012, pp. 2174-2182.

[25] G. Avoine, L. Buttyan, T. Holczer, and I. Vajda, "Group-Based Private Authentication," IEEE International Symposium on World of Wireless, Mobile and Multimedia Networks, 2007, pp. 1-6.

[26] Prosanta Gope and Tzonelih Hwang, "A realistic lightweight authentication protocol preserving strong anonymity for securing RFID system," Computers & Security, Vol.55, November 2015, pp.271-280.

[27] Prajnamaya Dass, Hari Om, "A secure authentication scheme for RFID Systems," Procedia Computer Science, Vol.78, 2016, pp. 100-106.

[28] Jung-Sik Cho, Young-Sik Jeong and Sang Oh Park, "Consideration on the brute-force attack cost and retrieval cost: A hash-based radio-frequency identification (RFID) tag mutual authentication protocol," Computers & Mathematics with Applications, Vol.69, Issue 1, January 2015, pp. 58-65.

[29] Dang Nguyen Duc and Kwangjo Kim, "Defending. RFID authentication protocols against DoS attacks," Computer Communications, Vol.34, Issue 3, 15 March 2011, pp. 384-390.