An Efficient Authentication and Key Agreement Protocol in RFID System

Eun-Jun Yoon[1] and Kee-Young Yoo[2] **

[1] School of Electrical Engineering and Computer Science,
Kyungpook National University,
1370 Sankyuk-Dong, Buk-Gu, Daegu 702-701, South Korea
ejyoon@tpic.ac.kr
[2] Department of Computer Engineering, Kyungpook National University,
1370 Sankyuk-Dong, Buk-Gu, Daegu 702-701, South Korea
yook@knu.ac.kr

Abstract. Due to the very limited computing resource, storing space and electric power supply of tag, it is a great challenge for us to design a practical RFID protocol which is security, efficient and can be used in the low-cost tag. In 2007, He et al. proposed an authentication and key agreement protocol which is used in the process of communication between the low-cost tag and reader. They also proved the security of the protocol through the extended strand space model. This paper presents a more efficient authentication and key agreement protocol for RFID system than He et al.'s protocol. Compare with He et al.'s protocol, the proposed protocol reduces the computational costs as well as protocol communication rounds to agree a shared session key between the reader and the tag.

Keywords: Security protocol, RFID system, Authentication, Key agreement, Session key

1 Introduction

Recently, Radio Frequency Identification (RFID) [1–12] has become a new spotlight technology for supporting ubiquitous computing environments. In the current open network environment, RFID identifies an object by using the radio frequency technology which is a kind of non-contact automatic identification technique. It can automatically read the information from a great deal of tags instantly. Therefore, RFID technology has been widely used by manufacturing management, custody control, management of humans and farm animals, arrangement of books at some libraries, etc.

The important key problem of the current RFID systems is the information security. It means that the current RFID systems have several security problems and challenges. In the normal RFID systems, the communication channel

** Corresponding author: Kee-Young Yoo (yook@knu.ac.kr)
Tel.: +82-53-950-5553; Fax: +82-53-957-4846

between the reader and the backend database is considered to be secure. However, because the communication channel between the RFID tag and the reader is not secure channel, it can be easily attacked by passive or active attackers. Therefore, secure RFID systems must be able to resist any kind of attack, such as wiretap, active attack, tracking etc., and also solve the three basic security problems including secrecy, identification and untraceability [1–4, 12].

In general, RFID tags have very limited computing ability, storing space and electric power supply. Due to these characteristics and a lot of restrictions, it is very difficult to design of the security mechanism of the RFID system. Currently, the most common design method is to use secure one-way hash function, bit-wise exclusive-or (XOR) operation, PRNG (pseudo-random number generator) etc. Up to now, most RFID authentication protocols are based on these cryptographic operations. Therefore, in the RFID system, it is an important challenge to design an efficient and secure protocol which can be used in the low-cost tag [1–4, 12].

In 2007, He et al. [12] proposed an authentication and key agreement (AKA) protocol which is used in the process of communication between the low-cost tag and reader. They also proved the security of the protocol through the extended strand space model [13–15]. This paper presents a more efficient authentication and key agreement (AKA) protocol which is used in the process of communication between the low-cost tag and reader for RFID system than He et al.'s AKA protocol. Compare with He et al.'s AKAP protocol, the proposed AKA protocol reduces the computational costs as well as protocol communication rounds to agree a shared session key between the reader and the tag.

This paper is organized as follows: In Section 2, we briefly review previous He et al.'s AKA protocol. In Section 3, we presents our proposed efficient AKA protocol for RFID system. In Sections 4 and 5, we analyze the security and the efficiency of our proposed AKA protocol, respectively. Finally, our conclusions are presented in Section 6.

2 Review of He et al.'s AKA Protocol

This section reviews He et al.'s AKA protocol [12]. The notations used throughout the paper can be summarized as follows:

- A: the tag.
- B: the reader.
- ID_A: the identity of the tag.
- ID_B: the identity of the reader.
- k_{AB}: the shared key between the reader and the tag.
- S: the shared secret counter between the reader and the tag which increases after authentication.
- SK: the shared session key between the reader and the tag.
- $H(x)$: the secure one-way hash value of x
- $x \oplus y$: the bit-wise XOR operation of x and y.
- M: the plaintext message exchanged between the reader and the tag.

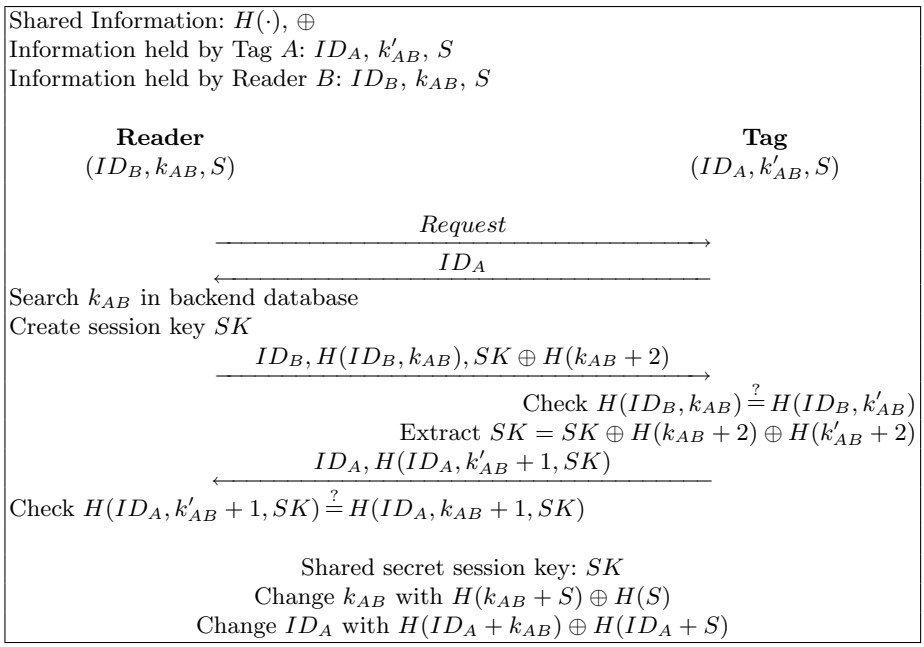

Fig. 1. He et al.'s AKA protocol

He et al.'s AKA protocol is shown in figure 1 and performs as follows:

1. $B \rightarrow A$: *Request*
   B sends request message to A.
2. $A \rightarrow B$: ID_A
   A sends its identity ID_A to B.
3. $B \rightarrow A$: $ID_B, H(ID_B, k_{AB}), SK \oplus H(k_{AB}+2)$
   After receiving ID_A from A, B searches the secret key k_{AB} in the backend database and creates session key SK. Then, B sends out $\{ID_B, H(ID_B, k_{AB}), SK \oplus H(k_{AB}+2)\}$ to A.
4. $A \rightarrow B$: $ID_A, H(ID_A, k'_{AB}+1, SK)$
   After receiving $\{ID_B, H(ID_B, k_{AB}), SK \oplus H(k_{AB}+2)\}$ from B, A computes $H(ID_B, k'_{AB})$ by its saved k'_{AB}. If $H(ID_B, k_{AB}) = H(ID_B, k'_{AB})$, the A successfully authenticates B and calculates $H(k_{AB}+2)$ to get SK; If $H(ID_B, k_{AB})) \neq H(ID_B, k'_{AB})$, authentication fails. Then, A sends out $\{ID_A, H(ID_A, k'_{AB}+1, SK)\}$ to B.
5. After receiving $\{ID_A, H(ID_A, k'_{AB}+1, SK)\}$ from A, B computes $H(ID_A, k_{AB}+1, SK)$ to see whether they are equal or not. If they equal, the authentication and the agreement on SK succeed.
6. After successful agreement on SK, both A and B change k_{AB} with $H(k_{AB}+S) \oplus H(S)$. The following communication adopts encrypt mode, ciphertext $C = M \oplus H(SK)$.

7. After the communication, both A and B change the tag A's identity ID_A with $H(ID_A + k_{AB}) \oplus H(ID_A + S)$ and destroy the SK.

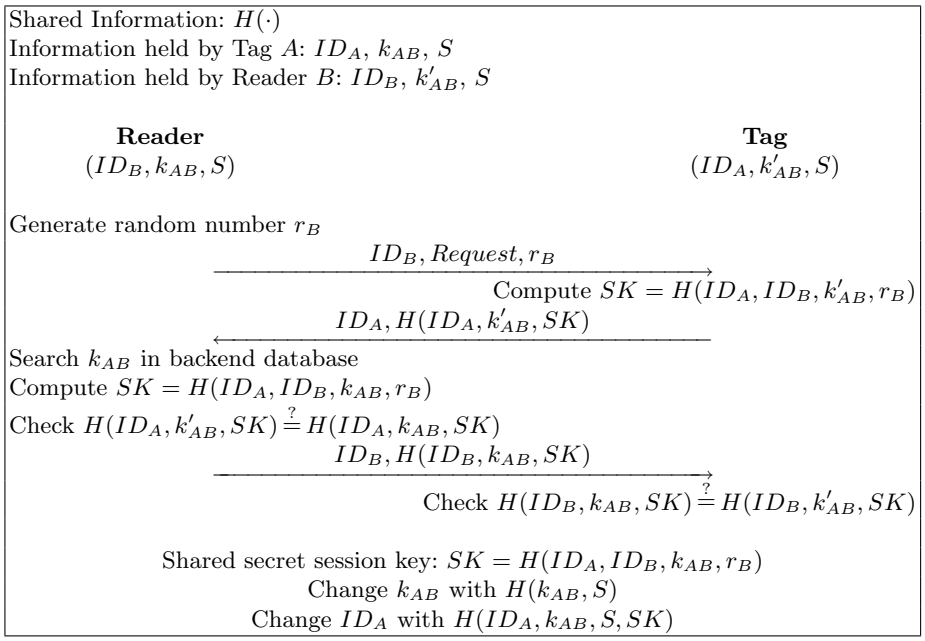

Fig. 2. Proposed AKA protocol

3 Proposed AKA Protocol

This section proposes an efficient AKA protocol than Lie et al.'s AKA protocol. The proposed AKA protocol is shown in figure 2 and performs as follows:

1. $B \rightarrow A$: $ID_B, Request, r_B$
   B generates a random number r_B and sends out a request message $\{ID_B, Request, r_B\}$ to A.
2. $A \rightarrow B$: $ID_A, H(ID_A, k'_{AB}, SK)$
   After receiving request message $\{ID_B, Request, r_B\}$ from B, A computes session key $SK = H(ID_A, ID_B, k'_{AB}, r_B)$ and then sends out $\{ID_A, H(ID_A, k'_{AB}, SK)\}$ to B.
3. $B \rightarrow A$: $ID_B, H(ID_B, k_{AB}, SK)$
   After receiving $\{ID_A, H(ID_A, k'_{AB}, SK)\}$ from A, B searches the secret key k'_{AB} in the backend database and computes session key $SK = H(ID_A, ID_B, k_{AB}, r_B)$. Then, B computes $H(ID_A, k_{AB}, SK)$. If $H(ID_A, k'_{AB}, SK) =$

$H(ID_A, k_{AB}, SK)$, the B successfully authenticates A and agreements session key SK; If $H(ID_A, k'_{AB}, SK) \neq H(ID_A, k_{AB}, SK)$, authentication fails. Finally, B sends out $\{ID_B, H(ID_B, k_{AB}, SK)\}$ to A

4. After receiving $\{ID_B, H(ID_B, k_{AB}, SK)\}$ from B, A computes $H(ID_B, k'_{AB}, SK)$. If $H(ID_B, k_{AB}, SK) = H(ID_B, k'_{AB}, SK)$, the A successfully authenticates B and agreements session key SK; If $H(ID_B, k_{AB}, SK) \neq H(ID_B, k'_{AB}, SK)$, authentication fails.
5. After successful agreement on SK, both A and B change k_{AB} with $H(k_{AB}, S)$. The following communication adopts encrypt mode, ciphertext $C = M \oplus H(SK)$.
6. After the communication, both A and B change the tag A's identity ID_A with $H(ID_A, k_{AB}, S, SK)$ and destroy the SK.

4 Security Analysis

This section provides the proof of correctness of the proposed AKA protocol.

1. *Mutual authentication and key agreement*: In steps 3 and 4, by using the secure one-way hash function $H(\cdot)$ [16], the reader and the tag always verify whether the received massage authentication values ($H(ID_A, k'_{AB}, SK)$ and $H(ID_B, k_{AB}, SK)$) are legal corresponding party's sending message. Therefore, the proposed AKA protocol provides the two-way mutual authentication and guarantees the secrecy of the reader and the tag.
2. *Untraceability*: In step 6, after finish the message communication, both the reader and the tag always change the tag A's identity ID_A with $H(ID_A, k_{AB}, S, SK)$ and then destroy the shared session key SK. Therefore, the proposed AKA protocol ensures the untraceability of the tag.
3. *Computing complexity*: Compared with the Hash-Lock protocol and Hash chain protocol [1–11], the proposed AKA protocol simply uses secure one-way hash function without PRNG(Pseudo-Random Number Generator) on the tag. Only involving one hash function module, it efficiently controls the cost of the tag. The computing complexity in the proposed AKA protocol is at the same level of Hash-Lock protocol. Therefore, the proposed AKA protocol is also suitable for the low-cost RFID system.
4. *Replay attacks*: In steps 5 and 6, both the reader and the tag always change the key k_{AB} and tag's identity ID, the proposed AKA protocol can avoid the replay attacks.

5 Efficiency Analysis

This section discusses the efficiency features of the proposed AKA protocol. The computational costs of the proposed AKA protocol in the reader and the tag are summarized in Table 1.

In He et al.'s AKA protocol, the computational overhead of the reader is 7 hash operations, 3 Bit-wise XOR($\oplus$) operations, and 1 random number generations. The computational overhead of the tag is 7 hash operations and 3 Bit-wise

XOR($\oplus$) operations. He et al.'s AKA protocol needs 4 communication rounds for mutual authentication and session key agreement.

In our proposed AKA protocol, the computational overhead of the reader is 5 hash operations and 1 random number generations. The computational overhead of the tag is 5 hash operations. Our proposed AKA protocol needs 3 communication rounds for mutual authentication and session key agreement.

Obviously, the proposed AKA protocol is more efficient than He et al.'s AKA protocol.

Table 1. Computational costs of the proposed AKA protocol

	Reader	Tag	Communication Rounds
He et al.'s AKA protocol	7 Hash + 3 Xor + 1 Ran	7 Hash + 3 Xor + 0 Ran	4
Proposed AKA protocol	5 Hash + 0 Xor + 1 Ran	5 Hash + 0 Xor + 0 Ran	3

Hash: Hash operation; Xor : Bit-wise XOR($\oplus$) operation;
Ran: Random number generation.

6 Conclusions

This paper presented a more efficient authentication and key agreement (AKA) protocol which is used in the process of communication between the low-cost tag and reader for RFID system than He et al.'s AKA protocol. In the proposed AKA protocol, the numbers of communication rounds are reduced that can be executed in seven messages and three rounds, respectively. As a result, compare with He et al.'s AKA protocol, the proposed AKA protocol has same security and is more computationally efficient and communication round efficient to agree a shared session key between the reader and the tag.

Acknowledgements

Kee-Young Yoo was supported by the MKE(Ministry of Knowledge Economy) of Korea, under the ITRC support program supervised by the IITA(IITA-2008-C1090-0801-0026). Eun-Jun Yoon was supported by the 2nd Brain Korea 21 Project in 2008.

References

1. S.E. Sarma, S.A. Weis, and D.W. Engels, "Radio-frequency Identification : Secure Risks and Challenges," *RSA Laboratories Cryptobytes*, June 2003, pp. 2 - 9.
2. M. Ohkubo, K. Suzuki, and S. Kinoshita, "Hash-chain Based Forward-secure Privacy Protection Scheme for Low-cost RFID," *In :Proceedings of the 2004 Symposium on Cryptography and Information Security (SCIS 2004)*, Sendai, 2004, pp. 719 - 724.
3. G. Avoine and P. Oechslin, "A Scalable and Provably Secure Hash-based RFID Protocol," *In : Proceedings of the 2nd IEEE International Workshop on Pervasive Computing and Communication Security(PerSec 2005)*, Washington. DC, USA, 2005, pp. 110 - 114.
4. Y.B. Zhou and D.G. Feng, "Design and Analysis of Cryptographic Protocols for RFID," *Chinese Journal of Computers*, April 2006, pp. 582 - 589.
5. G. Avoine, E. Dysli, and P. Oechslin, 'Reducing Time Complexity in RFID Systems", *In SAC 2005 of LNCS*, Vol. 3897, Springer-Verlag, 2005, pp. 291-306.
6. S. Kinoshita, F. Hoshino, T. Komuro, A. Fujimura, and M. Ohkubo, "Low-cost RFID Privacy Protection Scheme", *IPSJ*, Vol. 45, No. 8, 2007, pp. 2021-2004.
7. M. Ohkubo, K. Suzuki, and S. Kinoshita, "Cryptographic Approach to "privacy-friendly" tags", *In RFID Privacy Workshop*, 2003.
8. J. Saito and K. Sakurai, "Owner Transferable Privacy Protection Scheme for RFID Tags", *In CSS 2005*, Vol. 2005 of IPSJ Symposium Series, 2005, pp. 283-288.
9. D. G. Han, T. Takagi, H. W. Kim, and K. I. Chung, "New Security Problem in RFID Systems Tag Killing", *In ACIS 2006 of LNCS*, Vol. 3982, Springer-Verlag, 2006, pp. 375-384.
10. K. Rhee, J. Kwak, S. Kim, and D.Won, "Challenge-response based RFID Authentication Protocol for Distributed Database Environment", *In SPC 2005 of LNCS*, Vol. 3450, Springer-Verlag, 2005, pp. 70-84.
11. K. Osaka, T. Takagi, K. Yamazaki, and O. Takahashi, "An Efficient and Secure RFID Security Method with Ownership Transfer", *Computational Intelligence and Security, 2006 International Conference on*, Vol. 2, No. 1, 2006, pp. 1090-1095.
12. L. He, Y. Gan, N.N. Li, and Z.Y. Cai, "A Security-provable Authentication and Key Agreement Protocol in RFID System," *Wireless Communications, Networking and Mobile Computing, 2007 International Conference on*, Vol. 1, No. 1, 2007, pp. 2078 - 2080.
13. F.J.T. Fabrega, J.C. Herzog, and J.D. Guttman, "Strand Spaces: Proving Security Protocols Correct," *Journal of Computer Security*, July 1999, pp. 191 - 230.
14. F.J. Thayer, J.C. Herzog, and J.D. Guttman,"Strand Spaces: Why is a Security Protocol Correct," *In: Proceedings of the 1998 IEEE Symposium on Security and Privacy*, Los Alamitos: IEEE Computer Society Press, 1998, pp. 160 - 171.
15. H.F. Shen, R. Xue, H.Y. Huangn, Z.X. Chen, "Extending the Theory of Strand Spaces," *Journal of Software*, October 2005, pp. 1785 - 1789.
16. B. Schneier, "Applied Cryptography Protocols", *Algorithms and Source Code in C. 2nd edi. John Wiley & Sons Inc.*, 1995.