Ultralightweight RFID Reader-Tag Mutual Authentication

Yu-Chung Huang and Jehn-Ruey Jiang

Department of Computer Science and Information Engineering
National Central University
Jhongli City, Taoyuan County, Taiwan, ROC

***Abstract*—In an RFID (Radio Frequency Identification) system, a tag with a unique ID is attached to an object and a reader can recognize the object by identifying the attached tag. With this identified tag ID, the reader can then retrieve the related information of the object from the backend server database. Due to the nature of RF signals, the communication between the reader and tags is vulnerable to attacks, leading to privacy and security weakness. Typical attacks include the forged-tag, forged-server, man-in-the-middle (MitM), tracking, replay, forward secrecy and DoS attacks. Due to the extremely small memory and very limited computation power of tags, some security schemes, like Chien and Chen's scheme, Chen and Deng's scheme, have been proposed to resist these attacks by using ultralightweight operations on tags, such as the random number generation (RNG), the pseudo random number generator (PRNG), the cyclic redundancy check (CRC), and the exclusive-or (XOR) operator. These schemes still have some flaws, though. In this article, we show two mutual authentication schemes using only ultralightweight operations conforming to the EPCglobal Class 1 Generation 2 (EPC C1G2) standard to resist aforementioned attacks and reduce the communication and/or computation overheads. We show comparisons of the two schemes and other related ones, and also show some research directions on designing good RFID reader-tag mutual authentication schemes.**

Keywords—Radio Frequency Identification (RFID), Security, Privacy, Mutual Authentication

I. INTRODUCTION

The RFID (Radio Frequency Identification) technology [1-2] is fundamental in realizing the IoT (Internet of Things) vision [3]; it has been utilized in many applications, such as healthcare, logistic control, supply chain management, and asset tracking, etc. An RFID system consists of tags, a reader and a backend server. A tag with a unique ID is attached to an object and the reader can recognize the object by initiating the identification procedure (or interrogation procedure) to identify the tag ID through wireless communications between the reader and tags. With this identified tag ID, the related information of the object can then be retrieved from the backend server database (or middleware).

Due to the nature of wireless communications, the identification procedure is susceptible to various latent attacks. Typical attacks include the forged-tag, forged-server, denial of service (DoS), replay, man-in-the-middle (MitM), tracking, forward secrecy attacks [4-7]. The RFID system has security and privacy problems in the presence of attacks.

Conventional crytography, such as symmetric and asymmetric encryption/decryption mechanisms, can easily resist the aforementioned attacks. However, general RFID tags, such as the well-known EPCglobal Class 1 Generation 2 (EPC C1G2) tags [8], usually have very low costs and thus have extremely small memory and limited computation power. Therefore, they cannot afford to run general crytography mechanisms [9-10]. For example, only ultralightweight operations, such as the random number generation (RNG), the pseudo random number generator (PRNG), the cyclic redundancy check (CRC), the hash function [11] and the exclusive-or (XOR) operator, are feasible to execute on EPC C1G2 tags.

Several mutual authentication schemes [12-16] have been proposed to resist attacks for RFID systems. By registering tags and readers in the backend server database, they allow a tag and a reader to authenticate each other. Some [12-14] of them use heavy-weight operations on tags; they are thus unsuitable for EPC C1G2 RFID systems. The other schemes [15-16] use only ultralightweight operations on tags; they can therefore be applied to EPC C1G2 tags. Unfortunately, these ultralightweight schemes still suffer from security weaknesses [17]. This motivates us to design ultralightweight schemes to raise the security level of RFID systems conforming to the EPC C1G2 standard.

This article introduces two improved mutual authentication schemes proposed by us in [18] and [19]. The schemes are suitable for EPC C1G2 RFID systems, since they require tags to perform only ultralightweight operations, such as the RNG, PRNG, XOR, and CRC operations. They nevertheless can resist the forged-tag, forged-server, MitM, tracking, replay, forward secrecy and DoS attacks. Moreover, the two schemes have lower communication and/or computation overheads than other related schemes, as demonstrated by the comparisons shown in this paper.

The remainder of the article is organized as follows. Some mutual authentication schemes are introduced in Section II.

Two scheme proposed by us are detailed in Section III. Performance comparisons are presented in Section IV. Finally, some concluding remarks are drawn and future research directions are given in Section V.

II. Related Work

The EPC C1G2 standard [8] is one of the most famous RFID standards. It was adopted by ISO/IEC as an international standard referred to as ISO/IEC 18000-6C. An EPC C1G2 tag is passive and communicates with a reader on the UHF band (800-960 MHz) at the range from 2 m to 10 m depending on the operating environment. It supports the on-chip 16-bit PRNG, 16-bit CRC, and XOR operations.

Many reader-tag mutual authentication schemes [12-16] have been proposed to mitigate the security threats mentioned in Section I by using only ultralightweight operations, such as PRNG, CRC, and XOR, in order to build systems conforming to the EPC C1G2 standard. Below, we describe two of these schemes, Chien and Chen's scheme [15], and Chen and Deng's scheme [16], which are most related to our proposed schemes [18-19].

In Chien and Chen's scheme [15], a tag (denoted by tag_i) shares some private information, such as EPC_i, authentication key K_i and access key P_i with a reader (denoted by $reader_j$). This information is used to build messages M_1 and M_2 in order to prove the authenticity of tag_i and $reader_j$. Unfortunately, since the communication channel between tag_i and $reader_j$ is insecure, the adversary can monitor and modify the message sent through the channel. As shown by Peris-Lopez et al. in [17], Chien and Chen's scheme cannot resist the forged-tag, forged-server, DoS, tracking, and forward secrecy attacks.

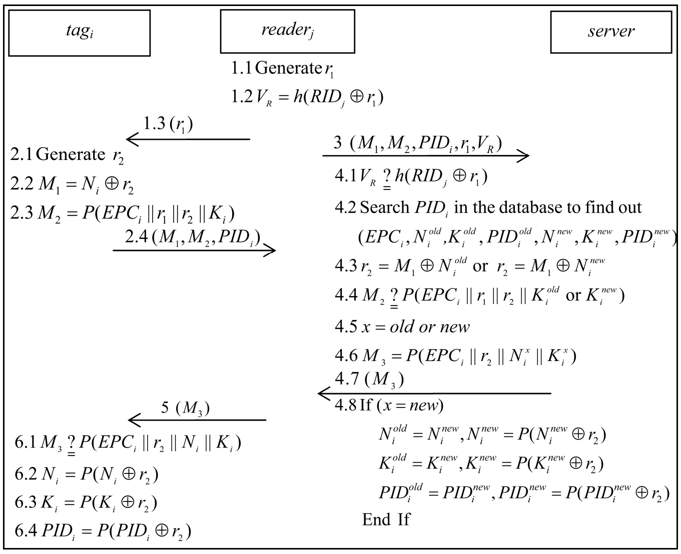
In Chen and Deng's scheme [16], tag_i is associated with a unique EPC code EPC_i, and $reader_j$ is associated with a unique identification IDR_j. To register tag_i, the server randomly selects a nonce N_i and an initial authentication key K_i for tag_i and stores EPC_i, N_i and K_i in tag_i and the server database. To register $reader_j$, the server stores IDR_j in the database. Referring to the CRC security flaw proposed by Peris-Lopez et al. [17], Chen and Deng's scheme is vulnerable to the forged, DoS, and replay attacks. Furthermore, since only tag_i responds to the request message of $reader_j$ according to N_i contained in the message, $reader_j$ needs to poll tags one by one to finish the identification procedure. When a large number of tags are registered on the server, it takes much time for the reader to do the polling.

III. Improved mutual authentication schemes

This section elaborates two improved mutual authentication schemes proposed by us in [18] and [19]. Similar to the schemes mentioned in Section II, the improved schemes assume the communication between the reader and the tags is insecure, but the communication between the reader and the backend server is secure.

A. The First Improvement

We introduce below the first improved scheme proposed in [18]. The scheme, as depicted in Fig. 1, uses only ultralightweight operations, such as the RNG, PRNG and XOR operations. It has two phases, the registration phase and the authentication phase, and can resist more attacks than the schemes introduced in Section II. However, the server needs to seek the information of tag_i in the database for the purpose of authenticating the tag. The seeking is by an exhaustive search since the searching key PID_i changes after successful identification. The seeking leads to some overheads, though.

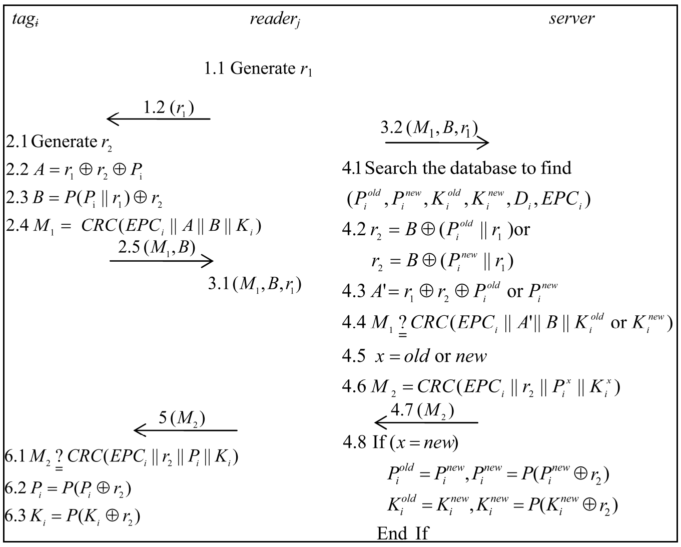


tag_i
$reader_j$
$server$
1.1 Generate r_1
1.2 $V_R = h(RID_j \oplus r_1)$
1.3 (r_1)
2.1 Generate r_2
2.2 $M_1 = N_i \oplus r_2$
2.3 $M_2 = P(EPC_i \| r_1 \| r_2 \| K_i)$
2.4 (M_1, M_2, PID_i)
3 $(M_1, M_2, PID_i, r_1, V_R)$
4.1 $V_R \overset{?}{=} h(RID_j \oplus r_1)$
4.2 Search PID_i in the database to find out
$(EPC_i, N_i^{old}, K_i^{old}, PID_i^{old}, N_i^{new}, K_i^{new}, PID_i^{new})$
4.3 $r_2 = M_1 \oplus N_i^{old}$ or $r_2 = M_1 \oplus N_i^{new}$
4.4 $M_2 \overset{?}{=} P(EPC_i \| r_1 \| r_2 \| K_i^{old}$ or $K_i^{new})$
4.5 $x = old$ or new
4.6 $M_3 = P(EPC_i \| r_2 \| N_i^x \| K_i^x)$
4.7 (M_3)
4.8 If $(x = new)$
$N_i^{old} = N_i^{new}, N_i^{new} = P(N_i^{new} \oplus r_2)$
$K_i^{old} = K_i^{new}, K_i^{new} = P(K_i^{new} \oplus r_2)$
$PID_i^{old} = PID_i^{new}, PID_i^{new} = P(PID_i^{new} \oplus r_2)$
End If
5 (M_3)
6.1 $M_3 \overset{?}{=} P(EPC_i \| r_2 \| N_i \| K_i)$
6.2 $N_i = P(N_i \oplus r_2)$
6.3 $K_i = P(K_i \oplus r_2)$
6.4 $PID_i = P(PID_i \oplus r_2)$

Fig. 1.The process of the first improved mutual authentication scheme [18]

B. The Second Improvement

The second improved scheme proposed in [19] is depicted in Fig. 2. It uses only ultralightweight operations, including the RNG, PRNG, XOR, and CRC, to reduce computation and communication overheads. It is simpler than the first improved scheme; however, it can resist the same number of attacks as the first improvement.



tag_i
$reader_j$
$server$
1.1 Generate r_1
1.2 (r_1)
2.1 Generate r_2
2.2 $A = r_1 \oplus r_2 \oplus P_i$
2.3 $B = P(P_i \| r_1) \oplus r_2$
2.4 $M_1 = CRC(EPC_i \| A \| B \| K_i)$
2.5 (M_1, B)
3.1 (M_1, B, r_1)
3.2 (M_1, B, r_1)
4.1 Search the database to find
$(P_i^{old}, P_i^{new}, K_i^{old}, K_i^{new}, D_i, EPC_i)$
4.2 $r_2 = B \oplus (P_i^{old} \| r_1)$ or
$r_2 = B \oplus (P_i^{new} \| r_1)$
4.3 $A' = r_1 \oplus r_2 \oplus P_i^{old}$ or P_i^{new}
4.4 $M_1 \overset{?}{=} CRC(EPC_i \| A' \| B \| K_i^{old}$ or $K_i^{new})$
4.5 $x = old$ or new
4.6 $M_2 = CRC(EPC_i \| r_2 \| P_i^x \| K_i^x)$
4.7 (M_2)
4.8 If $(x = new)$
$P_i^{old} = P_i^{new}, P_i^{new} = P(P_i^{new} \oplus r_2)$
$K_i^{old} = K_i^{new}, K_i^{new} = P(K_i^{new} \oplus r_2)$
End If
5 (M_2)
6.1 $M_2 \overset{?}{=} CRC(EPC_i \| r_2 \| P_i \| K_i)$
6.2 $P_i = P(P_i \oplus r_2)$
6.3 $K_i = P(K_i \oplus r_2)$

Fig. 2.The process of the second improved mutual authentication scheme [19]

IV. Comparisons

In this section, we show comparisons for the two improved mutual authentication schemes [18-19] and Chien and Chen's scheme [15], and Chen and Deng's scheme [16].

The comparisons are based on the situation where a reader tries to identify a unique tag out of n registered tags.

We first show the comparisons of the communication cost (i.e., the number of bits transmitted) between a tag and a reader. Table I shows the comparison results. Note that in Table I, L_{HELO}, L_{REQ}, and L_{RESP} stand for, respectively, the length (128 bits) of the hello message, the request message and the response message. L_{RND}, L_K and L_{ID} represent the length (128 bits) of the output of the random number generator, the key and the tag identity, respectively. L_{PRNG} and L_{CRC} stand for, respectively, the length (16 bits) of the output of PRNG and CRC operations. Furthermore, L_{CK} stands for the length (128 bits) of the XOR operation result of a key and a CRC output. As shown in Table I, the communication costs of Chien and Chen's, Chen and Deng's schemes, and the first improved scheme are respectively $2L_{RND}+ 2L_{CK}$ (=512 bits), $n(1L_{REQ}+ 1L_{RND}+ 1L_{CRC})+ 1L_{RND}+ 1L_{CR}+ 1L_K+ 1L_{RESP}$ (=272n + 400 bits) and $1L_{ID} + 1L_N + 1L_K + 2L_{PK}$(=640 bits). We can observe that the second improved scheme has a lower communication cost, which is $2L_N+ 2L_{CRC}$ (=288 bits), than the other schemes.

Table II shows computation cost comparisons during the authentication phase. In Table II, T_{XOR}, T_{PRNG}, T_{CRC}, and T_H are the execution time or the computation cost for the XOR, PRNG, CRC and hash function operation, respectively, and n is the number of tag_i. Note that the exclusive-or operation are very low computation-cost operations and the computation costs of other operations are of the ascending order: T_{CRC}, T_{PRNG} and T_H. By Table II, we can observe that the second improved scheme, Chien and Chen's scheme [15] and Chen and Deng's scheme [16] have nearly the same computation cost. Yet, the first improved scheme has lower computation cost than other schemes.

Table III shows the comparisons of the ability to resist various attacks. By Table III, we observe that Chen and Deng's scheme can resist only the MitM attack, and Chien and Chen's scheme suffer from all the aforementioned attacks. The first improved scheme cannot resist the tracking attack, while the second improved scheme can resist all the aforementioned attacks, i.e., the forged-tag, forged-server, MitM, tracking, replay, forward secrecy and DoS attacks.

V. Conclusion

This article shows two improved ultralightweight reader-tag mutual authentication schemes to improve existing schemes for resisting various attacks, such as the forged-tag, forged-server, MitM, tracking, replay, forward secrecy and DoS attacks. The improved schemes use only ultralightweight operators, like the RNG, PRNG, CRC and XOR, on tags to conform to the EPC C1G2 standard. Compared with related schemes, namely Chien and Chen's scheme [15] and Chen and Deng's scheme [16], the improved schemes can resist more attacks and have lower communication and computation costs.

In the future, we plan to design more efficient and more secure RFID reader-tag mutual authentication schemes using only ultralightweight operations. One direction is to use the Rabin algorithm [20] to encrypt (resp., decrypt) messages by executing one multiplication operation on a tag and to decrypt (resp., encrypt) messages by executing one square root operation on a reader. Since a reader has much more resources, such as memory, energy and computation power, than a tag, the asymmetric computation requirements demanded by the Rabin algorithm encryption and decryption are suitable for designing feasible and secure RFID reader-tag mutual authentication schemes.

TABLE I. Communication cost comparisons

Schemes	Communication costs
Chien and Chen's	$2L_{RND} + 2L_{CK}$ (=512 bits)
Chen and Deng's	$n(1L_{REQ}+ 1L_{RND}+ 1L_{CRC}) + 1L_{RND}+ 1L_{CR}+ 1L_K+ 1L_{RESP}$ (=272n+400 bits)
First Improvement	$1L_{HELO}+ 1L_{ID} + 1L_{RND}+ 1L_K + 2L_{PK}$ (=768 bits)
Second Improvement	$1L_{RND} + 11L_{PK} + 2L_{CRC}$ (=288 bits)

Note that L_{HELO}, L_{REQ}, L_{RESP}, L_{PK}, L_{CRC}, L_{CK}, L_{RND} , L_K and L_{ID} are the bit lengths of the hello message, request message, response message, XOR result of a key with a PRNG output, CRC output, XOR result of a key with a CRC output, random number generator output, key and identity, respectively

TABLE II. Computation cost comparisons

Schemes	Computation costs	
	Tag$_i$	**Server**
Chien and Chen's	$2T_{XOR}+ 2T_{CRC} + 1T_{COMP}+ 2T_{PRNG}$	$nT_{VERI} + 1T_{XOR} + 1T_{CRC} + 2T_{PRNG}$ ($T_{VERI}= 2T_{XOR}+ 2T_{CRC}+ 2T_{COMP}$)
Chen and Deng's	$nT_{VERI}+ 4T_{XOR} + 1T_{CRC}$ ($T_{VERI}= 1T_{XOR}+ 1T_{CRC}+ 1T_{COMP}$)	$nT_{VERI} + 3T_{XOR} + 1T_{CRC}$ ($T_{VERI} = 2T_{XOR}+ 1T_{CRC}+1T_{COMP}$)
First Improvement	$6T_{XOR} + 5T_{PRNG}+ 1T_{COMP}$	$((\log n)+1)T_{COMP}+ 1T_H+6T_{XOR}+ 4T_{PRNG}+ 2T_{VERI}$ ($T_{VERI} = 1T_{PRNG}+ 1T_{COMP}$)
Second Improvement	$5T_{XOR} + 1T_{CRC} + 3T_{PRNG}+ 1T_{COMP}$	$nT_{VERI}+5T_{XOR} + 1T_{CRC} + 2T_{PRNG}$ ($T_{VERI} = 1T_{CRC}+ 1T_{COMP}$)

Note that n stands for the number of tags: T_{XOR}, T_{PRNG}, T_{CRC}, T_H, T_{VEFI} and T_{COMP} are the computation costs of the XOR, PRNG, CRC, hash function, verification and comparison operations/procedures, respectively.

TABLE III. Security comparisons

Schemes **Attacks**	Chien and Chen's	Chen and Deng's	First Improvement	Second Improvement
Resistance to the forged-tag attack	No	No	Yes	Yes
Resistance to the forged-server attack	No	No	Yes	Yes
Resistance to the tracking attack	No	No	No	Yes
Resistance to the relay attack	No	No	Yes	Yes
Resistance to the MitM attack	No	Yes	Yes	Yes
Resistance to the forward secrecy attack	No	No	Yes	Yes
Resistance to the DoS attack	No	No	Yes	Yes

References

[1] C. Aggarwal, J. Han, “A Survey of RFID Data Processing,” Managing and Mining Sensor Data, Springer, pp. 349-382, 2013.

[2] A. Grover, H. Berghel, “A Survey of RFID Deployment and Security Issues,” Journal of Information Processing Systems, Vol.7, No.4, pp. 561-580, 2011.

[3] S. Li, L. D. Xu, S. Zhao, “The Internet of Things: a Survey,” Information Systems Frontiers, Vol 17, Issue 2, pp. 243-259, 2015.

[4] M. Alizadeh, M. Zamani, A. R. Shahemabadi, J. Shayan, A. Azarnik, “A Survey on Attacks in RFID Networks,” Open International Journal of Informatics (OIJI). Vol 1, pp. 15-24, 2012.

[5] Z. Liu, D. Liu, L. Li, H. Lin, Z. Yong, “ Implementation of a New RFID Authentication Protocol for EPC Gen2 Standard,” IEEE Sensors Journal, Vol. 15, pp. 1003-1011, February 2015.

[6] R. Doss, S. Sundaresan, W. Zhou, “A practical quadratic residues based scheme for authentication and privacy in mobile RFID systems,” Ad Hoc Networks, Vol. 11, pp. 383-396, January 2013.

[7] Y. P. Liao, C. M. Hsiao, “A secure ECC-based RFID authentication scheme integrated with ID-verifier transfer protocol,” Ad Hoc Networks, Vol. 18, pp. 133-146, July 2014.

[8] EPCglobal web site: http://www.epcglobalinc.org/

[9] C. C. Chang, W. Y. Chen, T. F. Cheng, “A Secure RFID Mutual Authentication Protocol Conforming to EPC Class 1 Generation 2 Standard,” in Proc. of 2014 Tenth International Intelligent Information Hiding and Multimedia Signal Processing (IIH-MSP), pp. 642-645, August. 2014..

[10] M. Safkhani, N. Bagheri, A. Mahani, “On the security of RFID anti-counting security protocol (ACSP),” Journal of Computational and Applied Mathematics, pp. 512-521, 2014.

[11] Z. Shi1, J. Pieprzyk, C. Doche, Y. Xia, Y. Zhang, J. Dai, “A Strong Lightweight Authentication Protocol for Low-cost RFID system,” International Journal of Security and Its Applications, Vol.8, pp. 225-234, 2014.

[12] M. Moessner, G. N. Khan, “Secure authentication scheme for passive C1G2 RFID tags,” Computer Networks, Vol. 56, pp. 273-286, January 2012.

[13] K. Suleyman, C. Serkan, A. Atakan, L. Albert, “An Efficient and Private RFID Authentication Protocol Supporting Ownership Transfer,” Lightweight Cryptography for Security and Privacy, Vol. 8162, pp. 130-141, May 2013.

[14] Y. Liao, C. Hsiao, “A secure ECC-based RFID authentication scheme integrated with ID-verifier transfer protocol,” Ad Hoc Networks, Vol. 18, pp. 133-146, July 2013.

[15] H. Y. Chien, C. H. Chen, “Mutual authentication protocol for RFID confirming to EPC Class 1 Generation 2 standards,” Computer Standards & Interfaces, Vol. 29, pp. 254-259, 2007.

[16] C. L. Chen, Y. Y. Deng, “Conformation of EPC class 1 generation 2 standards RFID system with mutual authentication and privacy protection,” Engineering Applications of Artificial Intelligence, Vol.22, pp. 1284-1291, 2009.

[17] P. Peris-Lopez, J. C. Hernandez-Castro, J. M. Estevez-Tapiador, A. Ribagorda, “Cryptanalysis of a novel authentication protocol conforming to EPC-C1G2 standard,” Computer Standards & Interfaces, vol. 31, pp. 372-380, 2009.

[18] Y. C. Huang, J. R. Jiang, “An Ultralightweight Mutual Authentication Protocol for EPC C1G2 RFID Tags,” in Proc. of 2012 International Symposium on Parallel Architectures, Algorithms and Programming (PAAP'12), pp. 133-140, December 2012.

[19] Y. C. Huang, J. R. Jiang, “Efficient Ultralightweight RFID Mutual Authentication,” in Proc. of 2014 IEEE International Conference on Internet of Things (iThings 2014), pp. 102-108, September 2014.

[20] Wikipedia, Rabin Cryptosystem, http://en.wikipedia.org/wiki/Rabin_cryptosystem, last accessed 2015.