Cryptanalysis of improved Yeh *et al.* 's authentication Protocol: An EPC Class-1 Generation-2 standard compliant protocol

Masoumeh Safkhani[1], Nasour Bagheri[2], Somitra Kumar Sanadhya[3], Majid Naderi[1]

[1] Electrical Engineering Department, Iran University of Science and Technology, Tehran, Iran{M_Safkhani, M_Naderi}@iust.ac.ir
[2] Electrical Engineering Department, Shahid Rajaee Teacher Training University, Tehran, Iran NBagheri@srttu.edu
[3] Institute of Information Technology (IIIT), Delhi, New Delhi, India, Somitra@iiitd.ac.in.

Abstract. EPC class 1 Generation 2(or in short term EPC-C1 G2) is one of the most important standards for RFID passive tags. However, the original protocol known to be insecure. To improve the security of this standard, several protocols have been proposed compliant to this standard. In this paper we analyze the improved Yeh *et al.* 's protocol by Yoon which is conforming to EPC-C1 G2 standard and is one of the most recent proposed protocol in this field. We present several efficient attacks against this protocol. Our first attack is a passive attack that can retrieve all secret parameters of the tag on the cost of eavesdropping only one session of protocol between the tag and a legitimate reader (connected to the back-end database) and $O(2^{16})$ evaluations of *PRNG*-function in off-line . Although the extracted information are enough to mount other relevant attacks (e. g. such as traceability, tag impersonation, reader impersonation, and desynchronization attacks) and would be enough to rule out any security claim for this protocol, to highlight other weaknesses of the protocol we present another tag impersonation attack with the complexity of two runs of protocol and the success probability of "1". In addition, we show a straight forward way to trace the tag as long as it has not updated its secret values.

keywords: RFID, EPC-C1 G2, Mutual Authentication, Secret Disclosure, Tag/Reader Impersonation, Traceability.

1 Introduction

RFID technology can potentially be employed almost everywhere. A typical RFID system includes a reader and a number of tags, which may range from the battery-powered ones with Wi-Fi capabilities, to the low-cost ones that are constrained in resources with even no internal power. The tag includes some information related to the tag holder. The tag can be read/modified by the reader which is normally supported by a back-end database.

Low-cost RFID can be a good replacement for the barcodes that are currently the most extended identification systems. The main advantages of RFID over barcodes are as follows [17]:

- Tag's data can be read automatically, even without line of sight and without physical contact , at a distance of several meters and at a rate of hundreds of times per second.
- It provides unequivocal identification for each tagged item, while a barcode only specifies the category of the labeled product.

However, security and privacy concerns are the main concern in the rapid and wide spread application of this distinguished technology.

There are several interconnected standards for RFID systems. Among them, ISO and EPC global have played the main role. In 2004 [7, 8], the Electronic Product Code Class-1 Generation-2 specification (EPC-C1 G2 in short) was announced by EPC Global which also has been ratified by ISO [11] and published as an amendment to ISO/IEC18000-6. This standard is an important milestone for the standardization of low-cost RFID tags. However, the later security analysis that carried out on the EPC-C1 G2 specification have demonstrated important security flaws in this standard [1, 16]. This is motivated researchers to try to propose EPC-compliant schemes, trying to correct the weaknesses and improve its security level, analyze the security of EPC-compliant schemes, or improve the vulnerable schemes [2–6, 9, 10, 12–15, 17–22]. Among them, one of the most recent proposals following this approach is an improvement to the Yeh *et al.* 's protocol [21] proposed by Yoon [22], which is the main concern of this paper. Yoon [22] has analyzed the security to the Yeh *et al.* 's protocol and proposed an improved protocol as a treatment for the Yeh *et al.* 's protocol. However, in this paper we show that they were not success in their attempt and the proposed protocol is really weak.

Paper Organization : In § 2 some preliminaries and notations are introduced. We describe improved Yeh *et al.* 's protocol in § 3. The secret parameter disclosure attack is presented in § 4. § 5 and § 6 describe the tag impersonation and the traceability attacks respectively. Finally, in § 7 we present the conclusion remarks.

2 Preliminaries

Through the paper, we use the following notation:

- EPC_s: The 96 bits of EPC code are divided into six 16-bit blocks and then these six blocks are XORed to give EPC_s.
- $DATA$: The corresponding information for the tag kept in the back-end database.
- K_i: The authentication key stored in the tag for database to authenticate the tag at the $(i+1)^{th}$ phase of authentication.
- P_i: The access key stored in the tag for the tag to authenticate the back-end database at the $(i+1)^{th}$ phase of authentication.
- K_{old} and K_{new}: The old and new authentication key stored in the back-end database respectively.
- P_{old} and P_{new}: The old and new access key stored in the back-end database respectively.
- C_i: The index of the record of the tag's information in back-end database stored in the tag.
- C_{old} and C_{new}: The old and new back-end database index stored in the back-end database respectively.
- X: The value kept as either *new* or *old* to show which key in the record of the back-end database is matched with the one of the tag.

- $B \longleftarrow A$: Assign the value of A to B.
- N_T and N_R: The random numbers that generated by the tag and the reader respectively.
- $\oplus$: Exclusive-or operation.
- RID: The reader identification number.
- $H(.)$: Hash function.

It must be noted that the output length of the available $PRNG$-function of EPC-C1 G2 has 16-bit length. We also use this assumption implicitly in our analysis in the rest of this paper.

3 Protocol Description

In this section we give a brief description of improved Yeh *et al.* 's protocol. This protocol has two phases: the initialization phase and the $(i+1)^{th}$ authentication phase which is described as follow:

Initialization Phase: In this phase, the manufacture generates random values for K_0, P_0 and C_0 respectively and sets the values of the record in the tag, i. e. $K_i = K_0, P_i = P_0, C_i = C_0$ and the corresponding record in the back-end database, i. e. $K_{old} = K_{new} = K_0, P_{old} = P_{new} = P_0, C_{old} = C_{new} = 0$.

Authentication Phase: The authentication phase of the improved Yeh *et al.* 's protocol at its $(i+1)^{th}$ run is as follow:

1. The reader generates a random number N_R and sends it to the tag.
2. On reception the message, the tag generates a random number N_T, computes $M1, D, E$ as below and sends $M1, D, C_i$, and E to the reader:
   $M1 \longleftarrow PRNG(EPC_s \oplus N_R \oplus N_T) \oplus K_i$
   $D \longleftarrow N_T \oplus K_i$
   $E \longleftarrow N_T \oplus PRNG(C_i \oplus K_i)$
3. Once the reader receives the message, computes $V = H(RID \oplus N_R)$ and forwards $M1, D, C_i, E, N_R, V$ to the back-end database.
4. On receiving the message, the back-end database performs the operations that described as follows:
   - For each stored RID in the database, computes $H(RID \oplus N_R)$ and compares it with the received V. In the case of equality, the back-end database authenticates the reader.
   - If $C_i = 0$, which means that it is the first access to the tag, iteratively:
     - Picks up an entry (K_{old}, P_{old}, C_{old}, K_{new}, P_{new}, C_{new}, RID, EPS_s, $DATA$) stored in itself,
     - Verifies whether $M1 \oplus K_{old} \stackrel{?}{=} PRNG(EPC_s \oplus N_R \oplus D \oplus K_{old})$. If "Yes" marks X as *old*.
     - Verifies whether $M1 \oplus K_{new} \stackrel{?}{=} PRNG(EPC_s \oplus N_R \oplus D \oplus K_{new})$. If "Yes" marks X as *new*.
   - If $C_i \neq 0$, uses C_i as an index to find the corresponding record in the database. If the record is found in its records for the field C_{old}, mark X as *old*, otherwise if it is in its records for the field C_{new} mark X as *new*.
   - Verifies whether $PRNG(EPC_s \oplus N_R \oplus D \oplus K_X) \oplus K_X \stackrel{?}{=} M1$. If "No" the protocol aborts.

- Verifies whether $N_T \oplus PRNG(C_X \oplus K_X) \stackrel{?}{=} E$. If "No" the protocol aborts.
- Computes $M_2, Info$, and MAC as follows and forwards them to the reader:
  $M2 \longleftarrow PRNG(EPC_s \oplus N_T) \oplus P_X$
  $Info \longleftarrow DATA \oplus RID$
  $MAC \longleftarrow H(DATA \oplus N_R)$

- If $X = new$, updates the database as follows:
  $K_{old} \longleftarrow K_x$,
  $K_{new} \longleftarrow PRNG(K_X)$,
  $P_{old} \longleftarrow P_x$,
  $P_{new} \longleftarrow PRNG(P_X)$.
  $C_{new} \longleftarrow PRNG(N_T \oplus N_R)$.

- If $X = old$, updates the database as follows:
  $C_{new} \longleftarrow PRNG(N_T \oplus N_R)$.

5. On receiving the message, reader verifies whether $H(Info \oplus RID \oplus N_R) \stackrel{?}{=} MAC$. If "Yes" forwards $M2$ to the tag; otherwise the protocol aborts.
6. On receiving the message, the tag does as follows:
   - Verifies whether $PRNG(EPC_s \oplus N_T) \stackrel{?}{=} M2 \oplus P_i$. If "No" the protocol aborts.
   - Authenticates the back-end database.
   - Updates the contents kept inside as follows:
     $K_{i+1} \longleftarrow PRNG(K_i)$,
     $P_{i+1} \longleftarrow PRNG(P_i)$.
     $C_{i+1} \longleftarrow PRNG(N_T \oplus N_R)$.

4 Secret Parameters Disclosure

In this section we present an efficient and passive attack that retrieves any secret parameters of the tag include EPC_s, K_i, and P_i. The adversary does as follows:

1. Eavesdrops one session of protocol and stores all transferred messages include: $N_R, C_i, M1 = PRNG(EPC_s \oplus N_R \oplus N_T) \oplus K_i, D = N_T \oplus K_i, E = N_T \oplus PRNG(C_i \oplus K_i), M2 = PRNG(EPC_s \oplus N_T) \oplus P_X$
2. $\forall\ i = 0\ \ldots\ N_d$ does as follows:
   - $K_i \longleftarrow i$,
   - $N_T \longleftarrow D \oplus K_i$,
   - If $E = N_T \oplus PRNG(C_i \oplus K_i)$ then returns K_i and N_T.
3. For the returned value of K_i and N_T from Step 2 and $\forall\ i = 0\ \ldots\ N_d$ does as follows:
   - $EPC_s \longleftarrow i$,
   - If $M1 = PRNG(EPC_s \oplus N_R \oplus N_T) \oplus K_i$ then returns EPC_s.

4. For the returned value of K_i and N_T from Step 2 and EPC_s from Step 3 and $\forall\ i = 0\ \ldots\ N_d$ does as follows:
   - $P_X \longleftarrow i$,
   - If $M2 = PRNG(EPC_s \oplus N_T) \oplus P_X$ then returns P_X.
5. Returns the following values:
   (a) $P_{old} = P_i$,

   (b) $P_{new} = PRNG(P_i)$,

   (c) $K_{old} = K_i$,

   (d) $K_{new} = PRNG(K_i)$,

   (e) $C_{old} = C_i$,

   (f) $C_{new} = PRNG(N_T \oplus N_R)$,

The complexity of the given attack is eavesdrop one session of protocol between the tag and a legitimate reader and 3×2^{16} evaluation of the $PRNG$-function. However, the adversary succeeds in its attack if it comes up with only one pre-image in each of Steps 2, 4, 3 of the given attack(it must be noted that the existence of at least one pre-image in each step is guaranteed). Otherwise, it should repeat the attack several times to come up with a unique solution. In that case, an efficient approach can be the blocking of the transferred $M2$ in the last Step of the protocol to avoid the secret parameters updating. In this case two runs of protocol should be fairly enough to extract all given parameters.

Remark 1. Given all secret parameters of the tag, it would be easy to apply the following attacks on the protocol with the success probability of "1" and the cost of one run of protocol:

1. Traceability attack,
2. Tag impersonation attack,
3. Reader impersonation attack,
4. Desynchronization attack

However, to show other weaknesses of the protocol we present other possible attacks on the protocol at the rest of the paper.

5 Tag Impersonation Attack

Tag impersonation attack is a forgery attack that leads to identifying spoofed tags by a legitimate reader. In this section we show how an adversary can deceive the reader to authenticate it as a legitimate tag. For our tag impersonation attack the adversary, which is an active adversary, can follows the steps described below:

Phase 1 (Learning): Adversary Eavesdrop one successful run of protocol and stores transferred messages between the reader and the legitimate tag include N_R, $M1$, D, C_i, E.
At the end of this phase the records related to this tag in the back-end database include (K_{old}, P_{old}, C_{old}, K_{new}, P_{new}, C_{new}, RID, EPS_s, $DATA$) and the tag record includes (K_{new}, P_{new}, C_{new},, EPS_s,), where:
$K_{new} = PRNG(K_{old})$,
$P_{new} = PRNG(P_{old})$,
$C_{new} = PRNG(N_T \oplus N_R)$,
$M1 = PRNG(EPC_s \oplus N_R \oplus N_T) \oplus K_{old}$,
$D = N_T \oplus K_{old}$,
$E = N_T \oplus PRNG(C_{old} \oplus K_{old})$.

Phase 2 (Impersonation): To impersonate the legitimate tag, the adversary waits until the reader initiates a new session of protocol, where:

1. The reader generates a random number N'_R and sends it to the tag.
2. On reception N'_R, the adversary replies with $M'1$, D', C'_i, E' where :
   (a) $M'1 = M1 = PRNG(EPC_s \oplus N'_R \oplus N_T) \oplus K_{old}$
   (b) $C'_i = C_{old}$
   (c) $D' = D \oplus N_R \oplus N'_R = N_T \oplus K_i \oplus N_R \oplus N'_R$
   (d) $E' = E \oplus N_R \oplus N'_R = N_T \oplus PRNG(C_{old} \oplus K_{old}) \oplus N_R \oplus N'_R$
3. Once the reader receives the message, computes $V = H(RID \oplus N_R)$ and forwards $M'1$, D', C'_i, E', V to the back-end database.
4. On receiving the message, the back-end database proceeds as follows:
   – For each stored RID in the database, computes $H(RID \oplus N_R)$ and compares it with the received V. Since the adversary has not manipulated the transferred message from the reader to the back-end database, the back-end database authenticates the reader.
   – We assume that $C'_i \neq 0$, then back-end database uses $C'_i = C_i$ as an index to find the corresponding record in the database. The record is found in its records for the field C_{old} hence back-end database marks X as old.
   – Verifies whether $PRNG(EPC_s \oplus N'_R \oplus D' \oplus K'_{old}) \oplus K_{old} \stackrel{?}{=} M'1$, where

$$PRNG(EPC_s \oplus N'_R \oplus D' \oplus K_{old}) \oplus K_{old} =$$

$$PRNG(EPC_s \oplus N'_R \oplus D \oplus N_R \oplus N'_R \oplus K_{old}) \oplus K_{old} =$$

$$PRNG(EPC_s \oplus N_R \oplus D \oplus K_{old}) \oplus K_{old} = M1 = M'1.$$

   – Verifies whether $N'_T \oplus PRNG(C'_{old} \oplus K'_{old}) \stackrel{?}{=} E'$, where:

$$N'_T = D' \oplus K_{old} = N_T \oplus N_R \oplus N'_R \Rightarrow$$

$$N'_T \oplus PRNG(C_{old} \oplus K_{old}) =$$

$$N_T \oplus N_R \oplus N'_R \oplus PRNG(C_{old} \oplus K_{old}) = E'$$

- Authenticates the adversary as a legitimate reader and computes $M'_2, Info$ and MAC as follows and forwards them to the reader:
  $M'2 \longleftarrow PRNG(EPC_s \oplus N'_T) \oplus P'_{old}$
  $Info \longleftarrow DATA \oplus RID$
  $MAC \longleftarrow H(DATA \oplus N'_R)$

- Since $X = old$, updates the back-end database as follows:
  $C'_{new} \longleftarrow PRNG(N'_T \oplus N'_R)$.

5. On receiving the message, reader verifies whether $H(Info \oplus RID \oplus N_R) \stackrel{?}{=} MAC$ which it is and it forwards $M2$ to the tag.

Following the given attack, the adversary would be authenticated by the back-end database with the probability of "1" while the complexity of attack is only two runs of protocol.

6 Traceability Attack

In this section we show that the improved Yeh *et al.* 's protocol puts at the risk the location privacy of tags' holders because it is possible to track tags with the probability of '1'(between two successful runs of authentication protocol). The following properties of the protocol are enough to trace tag, as long as it does not updated its internal values:

1. When the reader or possibly the adversary $\mathcal{A}$, which supplants a legal reader in a mutual authentication session, sends a random number N_R to the tag, it will responds with $M1, D, C_i$, where C_i is the tag's index in the back-end database and will remain fixed as long as the tag does not participant in a successful run of protocol to update its internal values.
2. Given that the tag's reply to the reader's (or adversary) query includes D and E where:

$$D = N_T \oplus K_i,$$

$$E = N_T \oplus PRNG(C_i \oplus K_i)$$

It can be see that if $\mathcal{A}$ computes Y as follows:

$$Y \longleftarrow D \oplus E = N_T \oplus K_i \oplus N_T \oplus PRNG(C_i \oplus K_i) = K_i \oplus PRNG(C_i \oplus K_i)$$

then Y is only depends on K_i and C_i and as long as the tag has not updated they will remain fixed. Hence, Y can be used as a measure to trace T_i.

7 Conclusions

In this paper we have analyzed the security of improved Yeh *et al.* 's protocol, proposed by Yoon, which is conforming to EPC-C1 G2 standard and is one of the most recent proposed protocol in this field. Our main attack was a passive attack which can retrieve all secret parameters of the tag efficiently. Actually, the cost of this attack is eavesdropping only one session of protocol between

the tag and a legitimate reader and $O(2^{16})$ *PRNG*-function evaluation in off-line. To show other weaknesses of the protocol, we also presented a tag impersonation attack with the complexity of two runs of protocol and the success probability of "1" and two ways to trace the tag as long as it has not updated its secret values. This study has shown that the proposed protocol does not reach the claimed security. More precisely, it does not provide any security level. Hence, it could not be a good successor for the current EPC- C1 G2 standard, despite of the designer expectation.

References

1. D. V. Bailey and A. Juels. Shoehorning security into the EPC tag standard. In R. D. Prisco and M. Yung, editors, *SCN*, volume 4116 of *Lecture Notes in Computer Science*, pages 303–320. Springer, 2006.
2. M. Burmester and B. de Medeiros. The security of EPC gen2 compliant RFID protocols. In S. M. Bellovin, R. Gennaro, A. D. Keromytis, and M. Yung, editors, *ACNS*, volume 5037 of *Lecture Notes in Computer Science*, pages 490–506, 2008.
3. M. Burmester, B. de Medeiros, J. Munilla, and A. Peinado. Secure EPC gen2 compliant radio frequency identification. In P. M. Ruiz and J. J. Garcia-Luna-Aceves, editors, *ADHOC-NOW*, volume 5793 of *Lecture Notes in Computer Science*, pages 227–240. Springer, 2009.
4. C.-L. Chen and Y.-Y. Deng. Conformation of EPC class 1 generation 2 standards RFID system with mutual authentication and privacy protection. *Eng. Appl. of AI*, 22(8):1284–1291, 2009.
5. H.-Y. Chien and C.-H. Chen. Mutual authentication protocol for RFID conforming to EPC class 1 generation 2 standards. *Computer Standards & Interfaces*, 29(2):254–259, 2007.
6. E. Y. Choi, D. H. Lee, and J. I. Lim. Anti-cloning protocol suitable to EPCglobal class-1 generation-2 RFID systems. *Computer Standards & Interfaces*, 31(6):1124–1130, 2009.
7. Class-1 generation 2 UHF air interface protocol standard version 1.2.0, Gen2, 2008. http://www.epcglobalinc.org/standards/.
8. EPC Tag data standar dversion 1.4.2008. http://www.epcglobalinc.org/standards/. Yearly report on algorithms and keysizes, Technical Report D.SPA.13Rev.1.0,ICT-2007-216676,. In *Gen2*. ECRYPT, 2010.
9. M. H. Habibi, M. R. Alaghband, and M. R. Aref. Attacks on a lightweight mutual authentication protocol under EPC C-1 G-2 standard. In C. A. Ardagna and J. Zhou, editors, *WISTP*, volume 6633 of *Lecture Notes in Computer Science*, pages 254–263. Springer, 2011.
10. M. H. Habibi, M. Gardeshi, and M. R. Alaghband. Practical attacks on a RFID authentication protocol conforming to EPC C-1 G-2 standard. 2(1):1–13, Feb. 04 2011. Comment: 13 page, International Journal of Ubicomp.
11. Information technologyRadio frequency identification for item management. Part 6:parameters for air interface communications at 860 MHz to 960MHz .http://www.iso.org. 2005.
12. G. Jin, E. Y. Jeong, H.-Y. Jung, and K. D. Lee. RFID authentication protocol conforming to EPC class-1 generation-2 standard. In H. R. Arabnia and K. Daimi, editors, *Security and Management*, pages 227–231. CSREA Press, 2009.
13. J. G. Kim, W. J. Shin, and J. H. Yoo. Performance analysis of EPC class-1 generation-2 RFID anti-collision protocol. In O. Gervasi and M. L. Gavrilova, editors, *ICCSA (3)*, volume 4707 of *Lecture Notes in Computer Science*, pages 1017–1026. Springer, 2007.
14. N.-W. Lo and K.-H. Yeh. An efficient mutual authentication scheme for EPCglobal class-1 generation-2 RFID system. In M. K. Denko, C.-S. Shih, K.-C. Li, S.-L. Tsao, Q.-A. Zeng, S.-H. Park, Y.-B. Ko, S.-H. Hung, and J. H. Park, editors, *EUC Workshops*, volume 4809 of *Lecture Notes in Computer Science*, pages 43–56. Springer, 2007.
15. P. Peris-Lopez, J. C. H. Castro, J. M. Estévez-Tapiador, and A. Ribagorda. Cryptanalysis of a novel authentication protocol conforming to EPC-C1G2 standard. *Computer Standards & Interfaces*, 31(2):372–380, 2009.
16. P. Peris-Lopez, J. C. Hernandez-Castro, J. M. Estevez-Tapiador, and A. Ribagorda. RFID specification revisited. In *The internet of things:From RFID to The Next-Generation Pervasive Networked Systems*, pages 311–346. Taylor & Francis Group, 2008.
17. P. Peris-Lopez, J. C. Hernandez-Castro, J. E. Tapiador, and J. C. A. van der Lubbe. Cryptanalysis of an EPC class-1 generation-2 standard compliant authentication protocol. *Eng. Appl. of AI*, 24(6):1061–1069, 2011.
18. P. Peris-Lopez, T. Li, and J. C. Hernandez-Castro. Lightweight props on the weak security of EPC class-1 generation-2 standard. *IEICE Transactions*, 93-D(3):518–527, 2010.

19. P. Peris-Lopez, T. Li, J. C. Hernandez-Castro, and J. E. Tapiador. Practical attacks on a mutual authentication scheme under the EPC class-1 generation-2 standard. *Computer Communications*, 32(7-10):1185–1193, 2009.
20. K.-H. Yeh and N.-W. Lo. Improvement of an EPC gen2 compliant RFID authentication protocol. In *IAS*, pages 532–535. IEEE Computer Society, 2009.
21. T.-C. Yeh, Y.-J. Wang, T.-C. Kuo, and S.-S. Wang. Securing RFID systems conforming to EPC class 1 generation 2 standard. *Expert Syst. Appl*, 37(12):7678–7683, 2010.
22. E.-J. Yoon. Improvement of the securing RFID systems conforming to EPC class 1 generation 2 standard. *Expert Systems with Applications*, In Press, Corrected Proof:–, 2011.