Cryptanalysis of Two Recent RFID Authentication Protocols

Sülayman KARDAŞ
Batman Üniversitesi, Mühendislik- Mimarlık Fakültesi, Bilgisayar Mühendisliği Bölümü, Batman.
skardas@gmail.com

ABSTRACT
EPCglobal introduced Electronic Product Code (EPC) for identifying objects and trace them in a wide network area. EPCglobal and ISO confirmed EPC Class-1 Generation-2 (EPC-C1G2) that includes the requirements of lightweight RFID tags. However, these class of tags are vulnerable to some inevitable attacks such as tracking, cloning and data leakage. Recently, numerous authentication protocols have been proposed for RFID systems. Many of them suffers from either the security and privacy issues or identification efficiency. Yeh et al. and Lo and Yeh proposed two mutual authentication protocols conforming to EPC-C1G2 standard. They claim their protocols provide forward secrecy against strong adversary. In this paper, we prove that both protocols do not satisfy this security objective. Moreover, we point out the potential counter measures in order to enhance the security of above protocols.

Keywords: RFID, EPCglobal, privacy, security, attack.

İki Yeni RFID Kimlik Protokollerin Kripto Analizi

ÖZET

EPCglobal nesneleri tanımlamak ve geniş bir ağ alanında onları takip edebilmek için Elektronik Ürün Kodu (EPC) tanımladı. EPCglobal ve ISO hafifsıklet RFID etiketlerin gereksinimlerini içeren EPC Klas 1 Nesil-2 (EPC - C1G2) standardını doğruladı. Fakat bu etiketler takip edilebilme, klonlama ve veri sızıntısı gibi saldırılara karşı savunmasızdırlar. Son zamanlarda, RFID sistemleri için çeşitli kimlik doğrulama protokolleri yayınlandı. Birçoğu güvenlik ve gizlilik sorunları veya kimlik tanımlama verimliliği sıkıntısı çekmektedir. Yeh ve ark. ve Lo ve Yeh EPC-C1G2 standardına uygun iki adet karşılıklı kimlik doğrulama protokollerini önerdi. Her iki öneride de protokollerin güçlü düşmana karşı ileri gizliliği sağladığı iddia edilmektedir. Bu makalede, her iki protokolün de güvenlik hedeflerini sağlamadığı kanıtlanmaktadır. Ayrıca, yukarıdaki protokollerinin güvenliğini geliştirmek amacıyla potansiyel karşı tedbirler önerildi.
Anahtar Kelimeler: RFID, EPCglobal, mahremiyet, güvenlik, saldırı.

1. Introduction

Radio Frequency IDentification (RFID) is a common way of remote object identification by means of small, lightweight and inexpensive RFID tags. It is also a way of remotely storing and retrieving the data that may contain information about the labelled object such as prices, height/weight, location and etc. A typical RFID system involves of three core components: the transponder (RFID tag/label), the transceiver (RFID reader) and the back-end database. RFID readers are usually composed of an RF module, a control unit, and a coupling element in order to interrogate the tags by means

of RF communication [12]. There are three classes of tags; passive, semi-active and active labels. Passive labels have no internal power source and use the electromagnetic power emitted by RFID reader. Nevertheless, semi-passive tags possess a battery that supplies its own microchip but they use the power, produced by the reader, during communication. In contrast, active tags have an internal power source and use this power in the microchip processor and in communication. Since passive tags are the cheapest ones, they are used in wide range of area, especially, in logistics and retailer industry. The back-end database usually stores all required information for a tag. It is assumed that an adversary can eavesdrop and modify the communications between reader and labels, but the interactions between the reader and the back-end database are protected.

RFID systems have been standardized, in which the physical and the link layers that include anti-collision mechanism, air interface, communication protocols and security functions [12]. EPCglobal, which guides the development of industry and produced the electronic product code (EPC) in order to support the usage of RFID, and the International Standards Organizations (ISO) are two significant organizations. These organizations provide standards for communications between RFID tags and readers. In February 2005, the EPCglobal published EPC Class-1 Generation-2 (EPC-C1G2) specification that defines functionality and operations of a RFID system [1]. In EPC-C1G2 specifications, the low cost passive RFID tag is defined and the tags include 16-bit Pseudo-Random Number Generator and 16-bit Cyclic Redundancy Check (CRC) function on-chip, which are discussed below in detail. Moreover, it supports a kill PIN with 32-bit to make the tag unusable permanently and a sleeping PIN with 32-bit to make tag temporarily unusable. Furthermore, the tags also support 32-bit access PIN to read/write any data in secure mode. However, it is pointed out in [6], [7], [14] that in EPC-C1G2 specification, little attention is paid on security threats and there are several weaknesses that would harm its global popularity. Killing a tag does not work in some cases. For instance, the customer service would require the information of product, which had been killed before. Moreover, it is possible to extract the PIN while eavesdropping a honest communication between a legitimate reader and the victim tag. In order to mitigate these security risks, several security protocols have been designed to improve security level of the RFID systems. Nonetheless, many of the proposed

protocols do not conform to EPC-C1G2 specification because they involve either a hash function or an encryption function [4]. On the other hand, the schemes that support of EPC-C1G2 standard have several security weaknesses [4], [14]. Therefore, the security is still an open problem in the EPC-C1G2. In 2010, Yeh et al. [21] and Lo and Yeh [10] have also suggested two new authentication scheme that conforms to the EPC-C1G2 standard yet. The authors claim that the proposed protocols ensure user privacy include forward secrecy and tag privacy. Nevertheless, in this paper, we show that in contrast to the claims these security objectives are not met.

This paper is organized as follows. Firstly, we briefly discuss some proposed protocols and their weaknesses in Section 2. In Section 3, we describe Yeh et al. 's protocol and prove that their protocol does not satisfy forward secrecy. Section 4 describes Lo and Yeh's RFID authentication protocol and our attack on this protocol in detail. Section 5 concludes the paper.

2. Related Work

In this section, we fleetingly discuss some security schemes designed for EPC-C1G2 specification with their security weaknesses.

In 2003, a set of ultra-lightweight authentication protocols for low-cost RFID tags and the security analysis are firstly proposed by Vajda et al. [19]. Thereafter, Juels [5] comes up with the concept of the minimalist cryptography. Next year, Juels [7] presents that combat skimming attacks against EPC tags conformed EPC-C1G2 UHF standard but his proposals are vulnerable to active attacks and eavesdropping. Some recent proposals [17], [18] have presented that RFID protocols can be vulnerable to Denial of Service (DoS) attack.

Karthikeyan and Nesterenko employ a simple matrix multiplication in their security scheme. In the scheme, the security relies on the difficulty of recovering multiplier from the product of two matrices [8]. Their system does not require any computationally expensive cryptographic mechanism. However, their protocols cannot resist tracking and replay attacks [9].

Duc et al. introduce a synchronization - based authentication protocol for the EPC-C1G2 specification [14]. It utilizes two simple cryptographic primitives, a Cyclic Redundancy Code (CRC) function and a pseudo random number generator (PRNG).

Even though the scheme exhibits efficient computational complexity, it does not provide resistance against replay attacks and the synchronization between the tag and the reader could be easily broken down [4].

Chien and Chen proposed an improved the scheme that is invented by [8], [14] to make privacy and security issues stronger [4]. Unfortunately, in the scheme, an adversary can easily accomplish replay attack and the scheme does not provide forward untracebility of the tags [11], [16]. In addition, the attacker can impersonate the tags and the reader, and this scheme does not provide location privacy [16].

Burmester and Medeiros [2] prove that Duc et al.'s protocol [13], Chien and Chen's protocol [4] are vulnerable to replay and synchronization attacks, although both them claim that the protocols support to intractability and uncloneability whilst conforming to EPC-C1 G2. After analyzing these protocols, they propose a mutual authentication RFID protocol, which achieves strong anonymity.

Peris-Lopez et al. [16] propose a robust and efficient FRID authentication protocol, called Gossamer, after a series of ultra-lightweight RFID protocols. In their work, they also present security analysis of the Ultralightweight Mutual Authentication Protocols (UMAP) and claim that ultra-lightweight protocols need to have a non-triangular function to increase the security. Hernandez-Castro et al. [3] analyze an ultra-lightweight authentication protocol, achieving Strong Authentication and Strong Integrity (SASI) for lightweight RFID labels and shows that non-triangular function is a necessary but it is not lonely sufficient condition for secure a low-cost protocol.

Yeh and Lo [20] recently claim that very popular lightweight authentication protocols [2, 15] are vulnerable to a desynchronization attack. In their analysis, it is shown that an adversary can extract the secret key by performing a series of challenge and response operations. They also propose an enhanced key update mechanism to defend the desynchronization attack. There are also some other recently published authentication protocols for RFID systems [22-24] but these protocols are not applicable to EPCglobal standard.

3. Yeh et al.'s Authentication Protocol

We borrowed the notations and authentication steps of the protocol defined in [21].

3.1. Notations

- EPC_s : EPC codes are divided into six 16-bit blocks. Then, the six blocks are XORed to get EPC_s.
- DATA : the corresponding information for the tag.
- K_i : the tag's secret authentication key.
- P_i : the tag's access key.
- K_{old} : the old secret key used for authentication.
- K_{new} : the new secret key used for authentication.
- P_{old} : the old access key.
- P_{new} : the new access key.
- C_i : i-th tag's database index.
- C_{old} : i-th tag's old database index.
- C_{new} : i-th tag's new database index.
- RID : Reader ID number.
- $\oplus$: XOR operation.
- $H(.)$: Hash function.

3.2. Yeh et al.'s protocol

Initialization*:* The manufacturer chooses three random nonce P_0, K_0, C_0 for each tag and stores these values in the tag's non-volatile memory ($P_i = P_0,\ K_i = K_0,\ C_i = C_0$) and the corresponding entry in the server's database ($P_{new} = P_{old} = P_0,\ K_{new} = K_{old} = K_0, C_{new} = C_{old} = C_0$).

The Authentication: The authentication steps are depicted in Figure 1. The steps are also described in detail as follows.

1) First of all, the legitimate reader generates a random nonce (N_R) and sends it to the tag.

2) Upon getting N_R, the tag generates a random number (N_T) and calculates following three authentication messages $M1 = PRNG(EPC_s \oplus N_R) \oplus K_i$, $D = N_T \oplus K_i$, and $E = N_T \oplus PRNG(C_i \oplus K_i)$. Then, it sends the quadruple message ($M1,\ D,\ C_i,\ E$) to the reader.

3) The reader calculates the authentication message $V = H(RID \oplus N_R)$ and sends it together with N_R and the messages (M_1, D, C_i, E) to the server.

4) Upon getting $(M1, D, C_i, E, N_R, V)$, the server does following operations in the

database:

a) For each RID value in the database, it calculates $H(RID \oplus N_R)$ with N_R and compares the product with the received V in order to detect a correct matching and verify the reader.

b) In case of $C_i = 0$, the database sequentially selects an entry $(K_{old}, P_{old}, C_{old}, K_{new}, P_{new}, C_{new}, RID, EPC_s, DATA)$, calculates the values $I_{old} = M1 \oplus K_{old}$ and $I_{new} = M1 \oplus K_{new}$, and checks whether I_{old} or I_{new} is equal to $PRNG(EPC_s \oplus N_R)$. As soon as an equality is found, set value X as old or new in keeping with which authentication key (K_{new} or K_{old}) is used during the computation. In case of $C_i \neq 0$, C_i is used for index to find the matching entry in the database. If the entry is found by using C_{old}, set X as old; otherwise set X as new if the entry field C_{new} matches up. Then verify M1, so as to check if it is equal to $PRNG(EPC_s \oplus N_R) \oplus K_X$.

c) Retrieves K_X from the matching entry, XOR it with the received D to obtain N_T, and checks whether the received E is equal to $N_T \oplus PRNG(C_x \oplus K_i)$. If the two values are not equal to each other, then the protocol aborts.

d) Calculates $M2 = PRNG(EPC_s \oplus N_T) \oplus P_X$ and $Info = DATA \oplus RID$, then sends them to the reader.

e) If $X = new$, then update the entry ($K_{old} = K_{new}$, $P_{old} = P_{new}$) and $K_{new} = PRNG(K_{new})$ and $P_{new} = PRNG(P_{new})$. If $X = old$, then update C_{new} as $PRNG(N_T \oplus N_R)$.

5) The reader XORs RID with the received Info to obtain DATA, and sends M2 to the tag.

6) The tag XORs P_i with the received M2. If the computed value is equal to $PRNG(EPC_s \oplus N_T)$, then the authentication is finished successfully and finally the secrets are updated as follows: $K_{i+1} = PRNG(K_i)$, $P_{i+1} = PRNG(P_i)$, and $C_{i+1} = PRNG(N_T \oplus N_R)$.

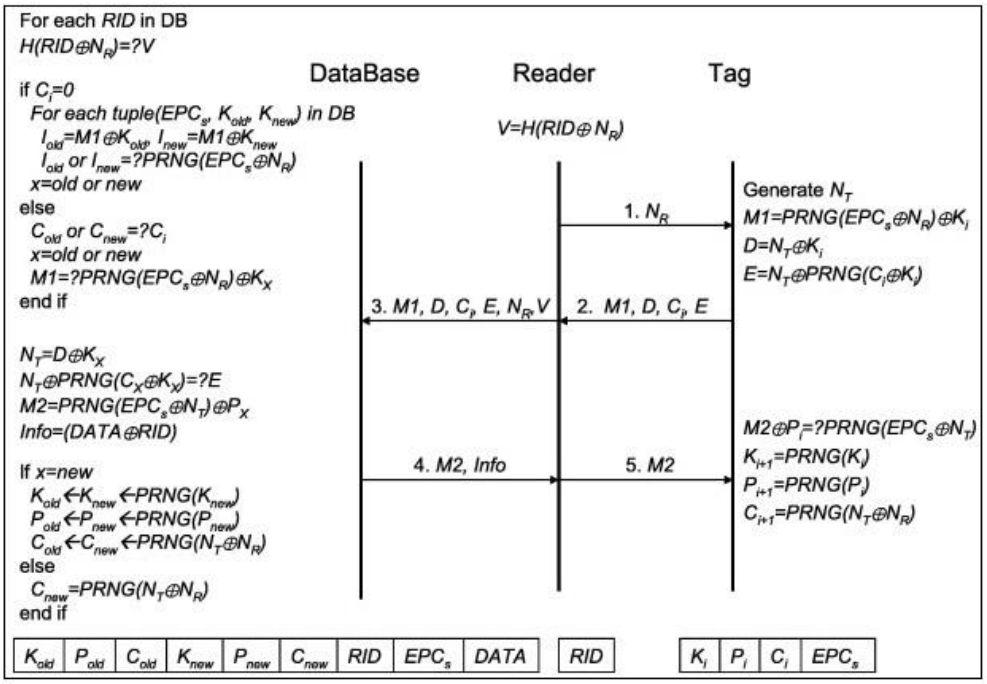

Figure 1. Yeh et al.'s proposed protocol [21]

3.3. Attacks on the Yeh et al.'s protocol

The authors claim that the proposed protocol provides forward secrecy against a strong adversary. However, with the following attack, we show that their protocol does not satisfy this privacy feature.

***Attack*:** Let an adversary A corrupt tag $\mathrm{T_i}$ at time t and retrieve the secrets $\mathrm{P, K, C}$ and $\mathrm{EPC_s}$. Assume that A has already recorded all transactions between tag T_i and the reader ($\mathrm{N_R, M1, D, C_i, E,}$ and $\mathrm{M2}$) at time t', where t' < t. We next show that A will reveal the secrets of the session $\mathrm{P_i, K_i}$ by the use of $\mathrm{EPC_s}$.

a. A first computes $\mathrm{PRNG(EPC_s \oplus N_R)}$ by the use of $\mathrm{EPC_s}$ and the nonce $\mathrm{N_R}$ and extracts K_i by XORing M1 and $\mathrm{PRNG(EPC_s \oplus N_R)}$.

b. Then, A extracts N_T by XORing the message D and K_i.

c. A computes $\mathrm{PRNG(EPC_s \oplus N_T)}$.

d. Finally, A extracts P_i by XORing $\mathrm{M2}$ and $\mathrm{PRNG(EPC_s \oplus N_T)}$.

It is clearly seen that the adversary A can easily reach all the secrets used in the session which belongs to tag T_i. Therefore, we conclude that Yeh et al.'s protocol does not provide forward secrecy. In the protocol, the use of constant EPC makes the protocol weaker against the strong adversary. Moreover, it is not easy to adopt forward secrecy with simple cryptographic primitives such as XOR and PRNG with small

entropy. Hence some strong cryptographic primitives such as one-way hash function, strong PRNG should be utilized. In the next section, we describe Lo and Yeh's [10] proposed RFID authentication protocol. The authors claim that their protocol provides forward secrecy, however; we show a feasible attack on the protocol.

4. Lo and Yeh's Authentication Protocol

Lo and Yeh [10] claim that they introduce a secure communication protocol for tag authentication and data access authorization in EPC Gen-2 compliant RFID systems. The proposed protocols adopt a process-oriented design to exploit the memory space at tag and back-end servers more efficiently while providing data confidentiality and mutual authentication. They also prevent threats of tag tracing and secrecy disclosure. However, we show that the proposed protocol does not prevent threats of any secrecy disclosure. The notations and detailed protocol steps are first described as follows.

4.1. Notations

- EPC_x : 96-bit unique EPC code stored at tag *x*.
- EPC_{x_DB} : 96 - bit unique EPC code stored at back-end server.
- K_x : The secret key shared by tag x and back-end server.
- flag : It represents whether previously session is safely terminated ($flag = 0$) or not ($flag = 1$).
- $ObjectData$: *Optional* information of tagged object.

4.2. Lo and Yeh's Protocol

The owner of the system performs an initial setup for each tag in order to store three values ($EPC_x, K_x,$ flag). A unique 96-bit EPC number is assigned to EPC_x for each tag Tag_x. This value is also assigned to EPC_{x_DB} stored at database. K_x is randomly generated from PRNG at the server and it is stored at both Tag_x and the database. The flag is initially set as 0. After each successful protocol, the secret K_x value is updated at the tag side and the server side. The authentication scheme is summarized in Figure 2 and Figure 3. The protocol steps are also described as follows.

Case 1: previous session is safely terminated* (flag = *0, Figure 2).

1. An legitimate Reader chooses a random nonce (N_1) and sends it to Tag_x.

2.Upon getting N_1, Tag_x chooses a random number (N_2) and calculates the authenticated response message, $M_1 = (EPC_x||N_1||N_2||CRC(EPC_x||N_1||N_2)) \oplus PRNG(K_x \oplus N_2)$. Tag_x sends flag, M_1 and N_2 to the reader. It also set flag $= 1$.

3.Upon receiving M_1 and N_2, the reader sends these messages along with message N_1 to the server.

4. The server sequentially retrieves the pair of K_{x_DB} and EPC_{x_DB} from each entry in the database. The server computes $M_1 \oplus PRNG(K_{x\_DB} \oplus N_2)$ and $CRC(EPC_{x\_DB}||N_1||N_2)$, and tries to find the match entry in the back-end database according to $(M_1 \oplus PRNG(K_{x\_DB} \oplus N_2) = EPC_{x\_DB}||N_1||N_2||CRC(EPC_{x\_DB}||N_1||N_2)$. Server repeats this verification step as soon as it finds a match record; otherwise, it drops this authentication steps. If server finds the match entry, it chooses two random nonce N_3 and N_4 and calculates $M_2 = (EPC_{x\_DB}||N_1||N_2||CRC(EPC_{x\_DB}||N_4)) \oplus PRNG(K_{x\_DB} \oplus N_3)$. Server updates the shared secret key $K_{x\_DB} = PRNG(K_{x\_DB} \oplus N_4)$, then it sends N_3, M_2 and ObjectData to the reader with the help of a protected channel.

5. The legitimate reader reaches ObjectData and sends the pair of N_3 and M_2 to tag Tag_x.

6. Upon receiving M_2 and N_3, Tag_x first verifies if the values of $M_2 \oplus PRNG(K_x||N_3)$ and $EPC_x||N_4||CRC(EPC_x||N_4)$ are equal in which N_4 is derived from $M_2 \oplus PRNG(K_x||N_3)$. If this verification is successful, then Tag_x updates its secret value $K_x = PRNG(K_x \oplus N_4)$ and updates $flag$ value as 0.

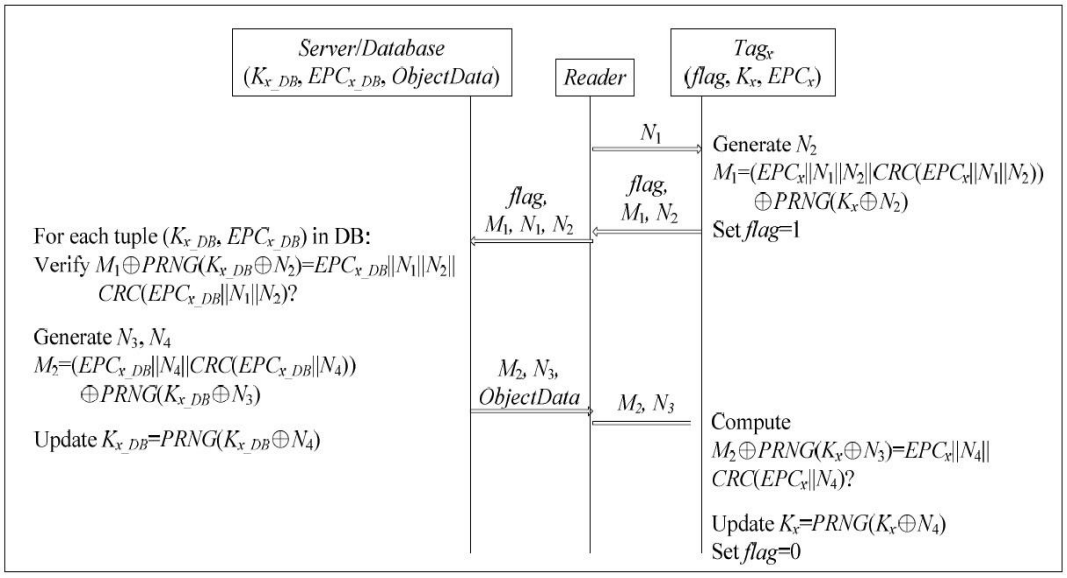

Figure 2. Lo and Yeh's protocol: previous session is safely terminated (flag = 0) [10]

Case 2: previous session is safely terminated* (flag = 1, *Figure 3).

- ✓ The legitimate reader chooses a random nonce (N_1) and sends it to Tag_x.
- ✓ As soon as receiving N_1, Tag_x chooses a random number (N_2) and computes $M_1 = (EPC_x||K_x||N_1||N_2||CRC(EPC_x||K_x||N_1||N_2) \oplus PRNG(EPC_x \oplus N_2)$. Tag_x sends flag, M_1 and N_2 to the reader.
- ✓ After receiving M_1 and N_2, the reader forwards these messages along with message N_1 to the server.
- ✓ The server sequentially retrieves the pair of K_{x_DB} and EPC_{x_DB} from the database. The server calculates $M_1 \oplus PRNG(K_{x\_DB} \oplus N_2)$ and $CRC(EPC_{x\_DB}||N_1||N_2)$, and tries to find a match entry in the back-end database according to $(M_1 \oplus PRNG(EPC_{x\_DB} \oplus N_2) = EPC_{x\_DB}||K_x||N_1||N_2||CRC(EPC_{x\_DB}||K_x||N_1||N_2))$. Server repeats this verification step until it finds a match record in the database; otherwise, it aborts this step. If server finds the match entry, it chooses two random nonce N_3 and N_4 and calculates $M_2 = (EPC_{x\_DB}||N_1||N_2||CRC(EPC_{x\_DB}||N_3)) \oplus PRNG(K_x \oplus N_3)$. Server updates the shared secret key $K_{x\_DB} = PRNG(K_{X\_DB} \oplus N_4)$, then it sends N_3, M_2 and ObjectData to the reader with the help of a protected channel.
- ✓ The reader reaches ObjectData and forwards message N_3 and M_2 to tag Tag_x.
- ✓ Upon receiving M_2 and N_3, Tag_x first verifies if the values of $M_2 \oplus$

$\mathrm{PRNG}(\mathrm{K_x}||\mathrm{N_3})$ and $\mathrm{EPC_x}||\mathrm{N_4}||\mathrm{CRC}(\mathrm{EPC_x}||\mathrm{N_4})$ are identical in which $\mathrm{N_4}$ is retrieved from $\mathrm{M_2} \oplus \mathrm{PRNG}(\mathrm{K_x}||\mathrm{N_3})$. If this verification is successful, then $\mathrm{Tag_x}$ updates its secret value $\mathrm{K_x} = \mathrm{PRNG}(\mathrm{K_x} \oplus \mathrm{N_4})$ and updates the flag as 0.

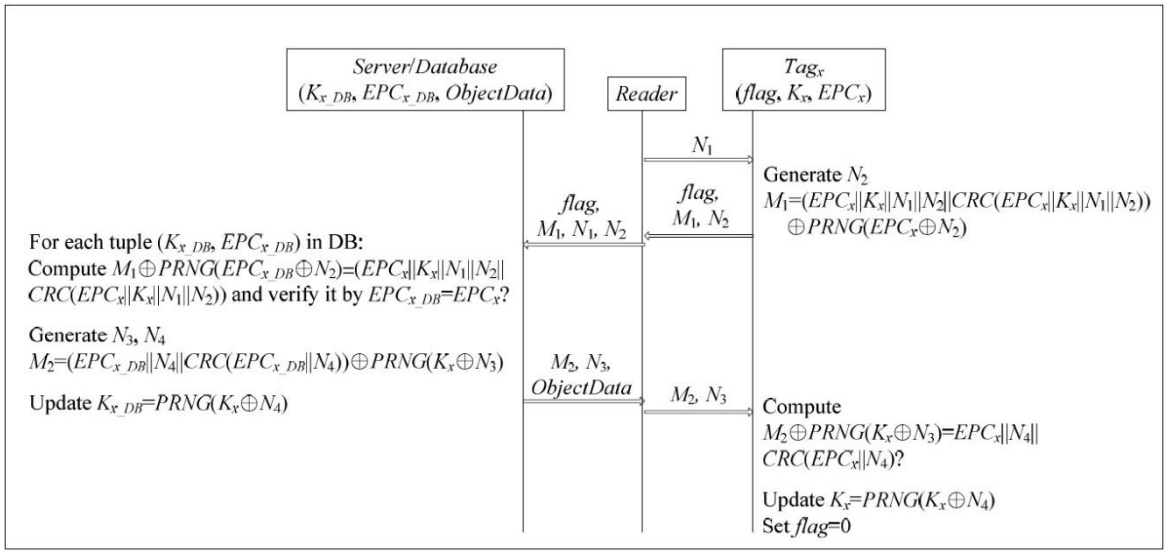

Figure 3. Lo and Yeh's protocol: previous session is not safely terminated (flag = 1) [10]

4.3. Attacks on the Lo and Yeh's protocol

The authors claim that their proposed protocol achieves forward secrecy against the secret disclosure of the tag. That is, if a tag is corrupted by an adversary, the adversary cannot trace back the trajectory of the tag because of key updating mechanism used in the protocol. Nevertheless, we show that their protocol does not satisfy this feature of privacy properly. The attack on this protocol is described as follows. Let A be the adversary who compromises a legitimate tag $\mathrm{Tag_x}$.

- The adversary *A* compromises tag $\mathrm{Tag_x}$ at time t and retrieves $\mathrm{EPC_x}$, $\mathrm{K_x}$ and flag. $\mathrm{EPC_x}$ value will be enough to trace back because $\mathrm{EPC_x}$ is fixed value for all transactions.
- Let *A* have already recorded a transaction between $\mathrm{Tag_x}$ and the reader at time t' where t' < t. The adversary derives $\mathrm{K_x}$ value of this transaction according to value of flag.
  - If flag is zero, then she derives $\mathrm{K_x}$ as follows. The bit length of random nonce $\mathrm{N_1}$ is 16. A have already recorded $\mathrm{N_1}$, $\mathrm{N_2}$ from the transactions and $\mathrm{EPC_x}$ from corruption. *A* first calculates

$M_1 \oplus (EPC_x||N_1||N_2||CRC(EPC_x||N_1||N_2))$. The key space of K_x is very small, ($2^{16} = 65536$), because of EPCglobal C1 Gen standard. Therefore, *A* try all possible value of K_x in order to find the K_x that gives $PRNG(K_x \oplus N_2)$. After deriving K_x, A may also verify K_x by computing message $M_2 \oplus PRNG(K_x \oplus N_3)$.

- If flag is 1, A simply computes $PRNG(EPC_x \oplus N_2)$ and XORs this value with M_1, then she finally derive K_x. She will also verify whether this K_x is correct in the computation of message M_2 by help of N_3.

In this protocol, using a fixed EPC makes the protocol weaker against the strong adversary. The use of small PRNG with small entropy also makes the protocol weaker against any passive attack. The brute-force must not computationally feasible to search whole space for any secrets used in the protocol. Hence, a strong PRNG or one-way hash function should be used to provide forward secrecy while providing authentication.

5. Conclusion

Nowadays, there are many critical RFID applications used in our daily lives. The reputation of security and privacy concerns has been progressively growing for RFID systems. The design of appropriate lightweight security protocols for lightweight RFID system is still a big challenge because of their restricted constrains. It is known that the EPC-C1G2 standard supports only simple cryptographic primitives (PRNG and CRC) for RFID tags. In order to achieve privacy and security for this standard, Yeh et al. [21] and Lo and Yeh [10] have recently proposed two new authentication protocols. They also claim that their protocol provides security against strong adversarial, such as forward security. In this paper, we established two simple attacks against these EPCglobal enabled RFID authentication protocols. The severity of our attacks shows the insecure design of the protocols.

References

1. EPCglobal. http://www.epcglobalinc.org/, 2009.
2. M. Burmester and B. de Medeiros. The Security of EPC GeN_2 Compliant RFID Protocols. In *ACNS*, pages 490-506, 2008.
3. J. C. H. Castro, J. M. Estevez-Tapiador, P. Peris-Lopez, and J.-J. Quisquater. Cryptanalysis of the SASI Ultralightweight RFID Authentication Protocol with Modular Rotations. *CoRR*, abs/0811.4257, 2008.

4. 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.

5. A. Juels. Minimalist Cryptography for Low-Cost RFID Tags. In *SCN*, pages 149-164, 2004.

6. A. Juels. RFID Security and Privacy: A Research Survey, 2005.

7. A. Juels. Strengthening EPC Tags Against Cloning. In *WiSe 05: Proceedings of the 4th ACM workshop on Wireless security*, pages 67-76. ACM Press, 2005.

8. S. Karthikeyan and M. Nesterenko. RFID Security without Extensive Cryptography. In *SASN '05: Proceedings of the 3rd ACM workshop on Security of ad hoc and sensor networks*, pages 63-67, New York, NY, USA, 2005. ACM.

9. C. H. Lim and T. Kwon. Strong and Robust RFID Authentication Enabling Perfect Ownership Transfer, Conference on Information and Communications Security IC_İCS 06, 2006, pages = 1-20, Springer-Verlag.

10. N. Lo and K.-H. Yeh. A Secure Communication Protocol for EPCglobal Class 1 Generation 2 RFID Systems. *Advanced Information Networking and Applications Workshops, International Conference on*, 0:562-566, 2010.

11. N. W. Lo and K.-H. Yeh. An Efficient Mutual Authentication Scheme for EPCglobal Class-1 generation-2 RFID System. In *EUC'07: Proceedings of the 2007 conference on Emerging direction in embedded and ubiquitous computing*, pages 43-56, Berlin, Heidelberg, 2007. Springer-Verlag.

12. P. Lopez. *Lightweight Cryptography in Radio Frequency Identification (RFID) Systems.* PhD thesis, Computer Science Department, Carlos III University of Madrid, 2008.

13. D. Nguyen, D. Jaemin, P. Hyunrok, and L. K. Kim. Enhancing Security of EPCglobal Gen-2 RFID Tag against. In Third Conference Software Computing and Intelligent Systems (SCIS '06), 2006.

14. D. Nguyen Duc, J. Park, H. Lee, and K. Kim. Enhancing Security of EPCglobal Gen-2 RFID Tag against Traceability and Cloning. In *Symposium on Cryptography and Information Security*, Hiroshima, Japan, January 2006.

15. P. Peris-Lopez, J. C. Hernandez-Castro, J. M. Estevez-Tapiador, and A. Ribagorda. Advances in Ultralightweight Cryptography for Low- cost RFID Tags: Gossamer Protocol. In K.-I. Chung, K. Sohn, and M. Yung, editors, *Workshop on Information Security Applications - WISA'08,* volume 5379 of *Lecture Notes in Computer Silence*, pages 56-68, Jeju Island, Korea, September 2008. Springer.

16. P. Peris-Lopez, J. C. Hernandez-Castro, J. M. Estevez-Tapiador, and A. Ribagorda. Cryptanalysis of a Novel Authentication Protocol Conforming to EPC-C1G2 Standard. *Comput. Stand. Interfaces*, 31(2):372-380, 2009.

17. B. Song and C. J. Mitchell. RFID Authentication Protocol for Low-cost Tags. In V. D. Gligor, J.-P. Hubaux, and R. Poovendran, editors, *Proceedings of the 1st ACM Conference on Wireless Network Security - WiSec'08,* pages 140-147, Alexandria, Virginia, USA, March-April 2008. ACM, ACM Press.

18. B. Sun, Y. Xiao, C.-C. Li, H.-H. Chen, and T. A. Yang. Security Co-existence of Wireless Sensor Networks and RFID for Pervasive Computing. *Computer Communications*, 31(18):4294-4303, 2008.

19. I. Vajda and L. Buttyan. Lightweight Authentication Protocols for Low-Cost RFID Tags. In *Second Workshop on Security in Ubiquitous Computing - Ubicomp 2003*, Seattle, Washington, USA, October 2003.

20. K.-H. Yeh and N. Lo. Improvement of Two Lightweight RFID Authentication Protocols. *Information Assurance and Security Letters*, 1:6, 2010.

21. T.-C. Yeh, Y.-J. Wang, T.-C. Kuo, and S.-S. Wanga. Securing RFID Systems Conforming to EPC Class 1 Generation 2 Standard. Elsevier, 2010.

22. N. Chikouche, F. Cherif, P.-L. Cayrel, and M. Benmohammed. Improved RFID authentication protocol based on randomized McEliece cryptosystem. International Journal of Network Security, 17(4):413–422, July 2015.

23. T. Dimitriou. Key evolving RFID systems: Forward/backward privacy and ownership transfer of RFID tags. Ad Hoc Networks, September 2015.

24. U. Mujahid, M. Najam-ul Islam, and A. Shami. RCIA: A new ultralightweight RFID authentication protocol using recursive hashing. International Journal of Distributed Sensor Networks, December 2014.