Security Analysis of Fan *et al.* Lightweight RFID Authentication Protocol for Privacy Protection in IoT

Seyed Farhad Aghili and Hamid Mala

Department of Information Technology Engineering, Faculty of Computer Engineering, University of Isfahan, Hezar Jerib St., Isfahan 81746-73441, Iran

{sf.aghili@eng, h.mala@eng}.ui.ac.ir

Abstract. The designers of Radio-Frequency IDentification (RFID) systems have a challenging task for proposing secure mutual authentication protocols for Internet of Things (IoT) applications. Recently, Fan *et al.* proposed a new lightweight RFID mutual authentication protocol in the journal of IEEE Transactions on Industrial Informatics. They claimed that their protocol meets necessary security properties for RFID systems and can be applied for IoT. In this paper, we analyze the security of this protocol and show that it is vulnerable against secret disclosure, reader impersonation and tag traceability attacks. Additionally, we show that in their protocol the anonymity of the tag does not held.

keywords: RFID, IoT, Secret disclosure, Impersonation attack, Anonymity.

1 Introduction

Radio-frequency identification (RFID) is a short range communication technology that is coming to increasing use as an alternative for bar codes in identifying tagged objects. Generally, an RFID system consists of tag and reader, and when involving a large capacity of calculation and information, it also requires a server. The tag usually contains private and important information about the products, and the reader tries to establish a connection with the tag all the times to achieve the information from the tag. Free-space information transfer in RFID system makes it vulnerable against security threats such as eavesdropping. Considering the limitations of tags, we cannot use the advanced crypto primitives such as AES, DES, RSA and SHA1. However, light-weight cryptography is used in the majority of suggested protocols such as light-weight hash functions and logical operations like XOR and bit rotation [1]. Traditionally, an RFID system involves two recommended communication channels:

- The channel between the tag and the reader that can be in two states: forward channel and backward channel in each time. When sending message from the reader to the tag, we have a forward channel but if the message is being sent in reverse, we have a backward channel. The important challenge in this channel is eavesdropping of the messages.
- The channel between the reader and the server is formed when the reader and the server communicate with each other. When an RFID system is employed in an IoT network, this channel is unsecure.

Recently, Fan *et al.* [2] proposed a mutual authentication protocol and claimed that their protocol owned the security properties necessary for RFID systems and is suitable for IoT. In this paper, we show that this protocol has several vulnerabilities. The presented attacks are designed for RFID-based IoT systems.

Paper organization In this paper, the related work is briefly introduced in Section 2. Preliminaries and notations used in this paper are mentioned in Section 3. We briefly describe Fan *et al.* lightweight authentication protocol [2] in Section 4. We analyze the security of Fan *et al.* protocol in Section 5, and propose several attacks against this protocol. Finally, in Section 6 we conclude the paper.

2 Related work

In recent decade, many authentication protocols have been proposed for RFID systems. For example, the HB-family (HB, HB^{+}, HB^{++}, etc.) [3–5] by employing matrix multiplication and some XORs, and the MAP-family (EMAP, M2AP, LMP^{+} and etc.) [6–8] based on bitwise operations like AND, XOR and OR are some of the lightweight authentication protocols proposed in literature. However, these two models have several limitations, weaknesses and vulnerabilities [9–13]. Later, in [14], Kulseng *et al.* proposed a lightweight solution to mutual authentication for RFID systems by using Physically Unclonable Functions (PUFs) and Linear Feedback Shift Registers (LFSRs) which are lightweight operations. However, Kardas [15] showed that their protocol is not resistant against message injection attack, and has several vulnerabilities.

In order to overcome RFID authentication problems, Cheng *et al.* [16] employed Chebyshev chaotic maps. However, Akgun and Caglayan in [17] proposed several attacks like de-synchronization attack and secret disclosure attack against Cheng *et al.* protocol. In 2014, Benssalah *et al.* proposed an improvement to overcome these weaknesses [18]. However in [19], Akgun *et al.* showed that their protocol is vulnerable to tracking, tag impersonation, and de-synchronization attacks.

In [20], Zhu *et al.* proposed a new Authentication protocol for RFID systems in the Internet of things and claimed that their protocol is secure. However, in [21] Erguler showed that Zhu *et al.*'s protocol is vulnerable to de-synchronization, replay and reader impersonation attacks, which are based on reader compromised attack.

In [22], the authors proposed an ultra-lightweight RFID mutual authentication protocol for IoT in a secure manner. However, the authors in [23] illustrate that their protocol cannot satisfy all security issues in RFID-based IoT systems and an attacker can compromise the reader and then execute the denial of service (DoS), reader and tag impersonation and de-synchronization attacks.

Recently, Fan *et al.* proposed a lightweight mutual authentication protocol [2]. They claimed that their protocol owned the security properties necessary for RFID systems and is suitable for universal RFID applications such as IoT. In this paper, we show that this protocol has several vulnerabilities.

3 Preliminaries and notations

In this section we describe the operation of bit cross ($cro(x,y)$), Index Data Table (IDT) and notations used in this paper (Table 1).

Table 1. Notations

Notation	Description
RID	Private ID of the tag
TID	Private ID of the reader
N_R, N_T, N_S	Random numbers generated by the reader, the tag and the server respectively
K_i	The i-th session key
$PRNG(\cdot)$	The Pseudo Random Number Generator function
$cro(x,y)$	The operation of bit cross
$Rot(x,y)$	The operation of rotation, $x = W(y)$
$\oplus$	Exclusive OR operation
$Mark$	The status of the last session
$\|$	Concatenation operation

Definition 1: $cro(x,y)$. Suppose that x and y are two N-bit strings, the corss operation is defined as below:

- $\sim x$ means the not operation on x.
- The odd bits value of $\sim x \| y$ are XORed by the even bits of $\sim y \| x$, and the result is regarded as the odd bits of the final result.

– The even bits of $\sim x||y$ are XORed by the odd bits of $\sim y||x$, and the result is regarded as the even bits of the final result denoted by $cro(x,y)$.

Definition 2: Index Data Table. In Fan *et al.* scheme, the Index Data Table included index value and index content which are unique (Table 2). In every session, the value of key is updated, so the index value is fresh for each session. Moreover, after every successful session, the status of *Mark* changes to "10" from "00".

Table 2. Index Data Table

Index value	Index content
$cro(RID \oplus TID, K_1)$	$Rot(K_1 \oplus TID, K_1 \oplus RID)$
$cro(RID \oplus TID, K_2)$	$Rot(K_2 \oplus TID, K_2 \oplus RID)$
...	...
$cro(RID \oplus TID, K_i)$	$Rot(K_i \oplus TID, K_i \oplus RID)$
$cro(RID \oplus TID, K_{i+1})$	$Rot(K_{i+1} \oplus TID, K_{i+1} \oplus RID)$

4 Fan *et al.* authentication protocol

Recently, Fan *et al.* proposed a lightweight mutual authentication protocol for RFID systems and they claimed that their protocol could be used for the IoT. When an RFID system is applied in the IoT, a significant challenge that must be taken into account by the protocol designer is the potentially insecure channel between the server and the reader.

In Fan *et al.* protocol the three components of the protocol pre-share the tuple $(K_i, cro(\cdot), Rot(\cdot), PRNG(\cdot))$. The protocol, as shown in Fig. 1, runs the following steps.

1. The reader starts the protocol by sending a random number N_R to the tag;
2. Once the tag received this message, generates a random number N_T and sets $Mark = 00$. It then transmits $cro(RID \oplus TID, K_i)||N_T$ to the reader.
3. After receiving the message, the reader obtains N_T and forwards $cro(RID \oplus TID, K_i)||N_R||N_T$ to the server.
4. Once the server received the message, it obtains N_R and N_T and then employs $cro(RID \oplus TID, K_i)$ to find the corresponding index content in the IDT. If it can find a match, it indicates that the last session has been done correctly and the current session is executable. Then the server generates a random number N_S and sends $cro(RID \oplus TID, K_i \oplus N_S)||Rot(K_i \oplus TID, K_i \oplus RID)||N_S \oplus K_i$ to the reader. Otherwise the authentication fails and the protocol will be terminated.

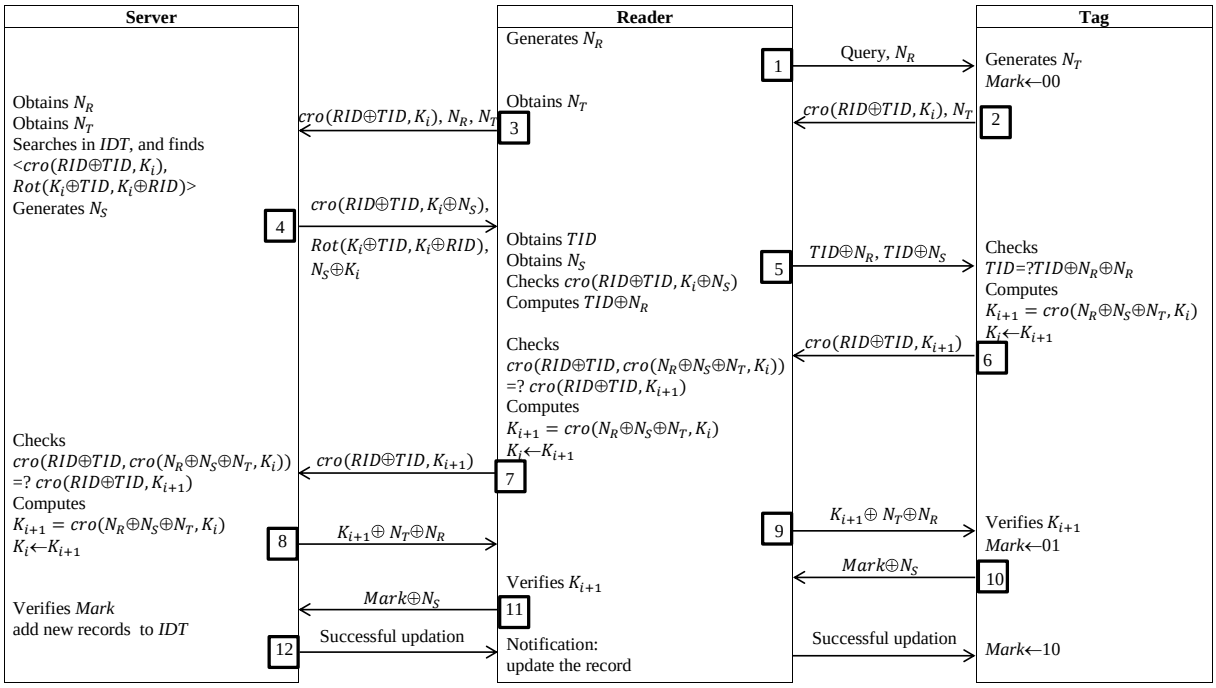

Fig. 1. Fan *et al.* authentication protocol

5. Once the reader received the tuple $(cro(RID \oplus TID, K_i \oplus N_S) \| Rot(K_i \oplus TID, K_i \oplus RID) \| N_S \oplus K_i)$, according to the hamming weight $W(K_i \oplus TID)$ of the rotation operation and $K_i \oplus K_i \oplus TID$ it obtains TID. It then obtains N_S and verifies the value of $cro(RID \oplus TID, K_i \oplus N_S)$ by comparing with the received value. If so, it computes $TID \oplus N_R$ and $TID \oplus N_S$ and sends them to the tag.

6. After receiving this message, the tag obtains N_S and if $TID = TID \oplus N_R \oplus N_R$ holds, it authenticates the server and the reader. Then the tag updates K_i as $K_{i+1} = cro(N_R \oplus N_S \oplus N_T, K_i)$ and sends it to the reader involved in the message $cro(RID \oplus TID, K_{i+1})$. Otherwise the authentication fails.

7. Upon receiving the message $cro(RID \oplus TID, K_{i+1})$, if $cro(RID \oplus TID, cro(N_R \oplus N_S \oplus N_T, K_i)) = cro(RID \oplus TID, K_{i+1})$ holds, the reader updates K_i by the same equation $K_{i+1} = cro(N_R \oplus N_S \oplus N_T, K_i)$ and sends it to the server by the message $cro(RID \oplus TID, K_{i+1})$. Otherwise the protocol will be terminated.

8. Once the server received this message, it does the same checking operation and if it holds, the server updates K_i as $K_{i+1} = cro(N_R \oplus N_S \oplus N_T, K_i)$. It then computes the message $K_{i+1} \oplus N_T \oplus N_R$ and sends it to the reader. Otherwise the connection fails.

9. Upon receiving the message $K_{i+1} \oplus N_T \oplus N_R$, if $K_{i+1} = (K_{i+1} \oplus N_T \oplus N_R) \oplus N_T \oplus N_R$ holds, the reader verifies K_{i+1} and sends the message $K_{i+1} \oplus N_T \oplus N_R$ to the tag for the same verification process. Otherwise the protocol will be terminated.
10. Once the tag accepts the validity of K_{i+1}, it sets $Mark = 01$, indicating the synchronization of K_i is completed. Then the tag computes $Mark \oplus N_S$ and sends it to the server through the reader. Note that in the original work [2], $Mark$ has been defined as a 2-bit string while parameters like N_S are typically larger strings, so their XOR does not make any sense. However, without loss of generality, we assume $Mark$ is some trivial extension of this 2-bit string.
11. After receiving the message $Mark \oplus N_S$, the server obtains the value of $Mark$ and if it is equal to 01, it concludes that the synchronization of K_i is completed. Then the server adds a new record $cro(RID \oplus TID, K_{i+1})$, $Rot(K_{i+1} \oplus TID, K_{i+1} \oplus RID)$ to IDT, after which the notification that the record completes the update is sent to the tag through the reader.
12. Now, the tag sets $Mark = 10$, indicating the authentication protocol is completed.

5 Security analysis of the Fan *et al.* protocol

In this section, we present several attacks against Fan *et al.* protocol. We show that this protocol is vulnerable to secret disclosure, reader impersonation and tag traceability attacks. Moreover, we show that in spite of the designers claim, the protocol fails to protect tag privacy.

Secret disclosure attack In the Fan *et al.* protocol, the adversary starts the attack by eavesdropping the messages of Steps 1, 2 and 9 which are respectively N_R, N_T and $K_{i+1} \oplus N_T \oplus N_R$. It then executes the attack by obtaining the new session key K_{i+1} from the equation $K_{i+1} = (K_{i+1} \oplus N_T \oplus N_R) \oplus N_R \oplus N_T$.

Attack on the anonymity The attacker can eavesdrop the messages of Steps 1 and 5 which are respectively N_R and $TID \oplus N_R$ and jeopardises the anonymity of the target tag by obtaining the identification of the tag TID from the equation $TID = (TID \oplus N_R) \oplus N_R$.

Reader impersonation attack The concept of this attack is that the adversary tries to run a new successful session with the target tag as a legitimate reader. Assume the situation that the attacker has already done

previous attacks and obtained the tag's identification TID and the tag's current key K_i. The presented reader impersonation attack against Fan *et al.* protocol is described as follows:

1. The adversary starts the protocol by sending random number N_{A1} to the tag;
2. The tag generates the random number N_T and sets $Mark = 00$. It then transmits $cro(RID \oplus TID, K_i) \| N_T$ to the adversary.
3. Once the adversary received the message, generates another random number N_{A2} and computes $TID \oplus N_{A1}$ and $TID \oplus N_{A2}$ and sends them to the tag.
4. After receiving this message, the tag obtains N_{A2} and verifies $TID = TID \oplus N_{A1} \oplus N_{A1}$ and authenticates the adversary. Then it updates K_i as $K_{i+1} = cro(N_{A1} \oplus N_{A2} \oplus N_T, K_i)$ and sends it to the adversary in the blind form of $cro(RID \oplus TID, K_{i+1})$.
5. The adversary uses N_{A1}, N_{A2}, N_T and K_i, and computes $K_{i+1} = cro(N_{A1} \oplus N_{A2} \oplus N_T, K_i)$. Then, it sends the message $K_{i+1} \oplus N_T \oplus N_{A1}$ to the tag for the verification process.
6. Upon receiving the message $K_{i+1} \oplus N_T \oplus N_{A1}$, the tag checks if $K_{i+1} = (K_{i+1} \oplus N_T \oplus N_{A1}) \oplus N_T \oplus N_{A1}$ holds. So, the tag verifies K_{i+1} and sets $Mark = 01$, indicating the synchronization of K is completed. Then the tag computes $Mark \oplus N_{A2}$ and sends it to the adversary.
7. After receiving the message, the adversary informs the tag that the updation is successful.
8. Now, the tag sets $Mark = 10$, indicating the authentication protocol is completed.

Tag traceability attack To trace a target tag, it is enough to link two sessions of the protocol in which that tag has been involved. In this subsection, we describe a traceability attack on Fan *et al.* protocol. In this attack, the adversary uses the link of two sessions of the protocol by eavesdropping the message of Step 1 which is $cro(RID \oplus TID, K_i)$. Before the next update of the tag, its session key K_i is unchanged. So, in $cro(RID \oplus TID, K_i)$ message, all of the parameters are constant. Thus, the attacker can use $cro(RID \oplus TID, K_i)$ to distinguish and track tags.

6 Conclusion

In this paper, we showed Fan *et al.* protocol proposed for lightweight RFID systems in IoT is not secure. We proved that their protocol cannot provide all security requirements in RFID systems and it is vulnerable to secret disclosure, reader impersonation and tag traceability attacks. Moreover, we showed that in their protocol the anonymity of the tag does not held. The success probability of presented attacks is “1".

References

1. S. Karthikeyan and M. Nesterenko, "RFID security without extensive cryptography," in *Proceedings of the 3rd ACM workshop on Security of ad hoc and sensor networks*, pp. 63–67, ACM, 2005.
2. K. Fan, W. Jiang, H. Li, and Y. Yang, "Lightweight RFID Protocol for Medical Privacy Protection in IoT," *IEEE Transactions on Industrial Informatics*, vol. 14, no. 4, pp. 1656–1665, 2018.
3. N. J. Hopper and M. Blum, "Secure human identification protocols," in *International Conference on the Theory and Application of Cryptology and Information Security*, pp. 52–66, Springer, 2001.
4. A. Juels and S. A. Weis, "Authenticating pervasive devices with human protocols," in *Annual International Cryptology Conference*, pp. 293–308, Springer, 2005.
5. J. Bringer, H. Chabanne, and E. Dottax, "Hb^{++}: a lightweight authentication protocol secure against some attacks," in *Second International Workshop on Security, Privacy and Trust in Pervasive and Ubiquitous Computing (SecPerU'06)*, pp. 28–33, IEEE, 2006.
6. P. Peris-Lopez, J. C. Hernandez-Castro, J. M. Estevez-Tapiador, and A. Ribagorda, "EMAP: an efficient mutual-authentication protocol for low-cost RFID tags," in *OTM Confederated International Conferences" On the Move to Meaningful Internet Systems"*, pp. 352–361, Springer, 2006.
7. P. Peris-Lopez, J. C. Hernandez-Castro, J. M. Estevez-Tapiador, and A. Ribagorda, "M^2AP: A minimalist mutual-authentication protocol for low-cost RFID tags," in *International Conference on Ubiquitous Intelligence and Computing*, pp. 912–923, Springer, 2006.
8. T. Li, "Employing lightweight primitives on low-cost RFID tags for authentication," in *Vehicular Technology Conference, 2008. VTC 2008-Fall. IEEE 68th*, pp. 1–5, IEEE, 2008.
9. H. Gilbert, M. Robshaw, and H. Silvert, "An active attack against HB+ - A provably secure lightweight authentication protocol," tech. rep., Cryptology ePrint Archive, Report 2005/237, 2005, available at http://eprint. iacr. org/2005/237. pdf.
10. K. Ouafi, R. Overbeck, and S. Vaudenay, "On the security of hb# against a man-in-the-middle attack," in *International Conference on the Theory and Application of Cryptology and Information Security*, pp. 108–124, Springer, 2008.
11. S. Islam, "Security analysis of LMAP using AVISPA," *International Journal of Security and Networks*, vol. 9, no. 1, pp. 30–39, 2014.
12. M. Safkhani, N. Bagheri, M. Naderi, and S. K. Sanadhya, "Security analysis of $lmap^{++}$, an RFID authentication protocol," in *Internet Technology and Secured Transactions (ICITST), 2011 International Conference for*, pp. 689–694, IEEE, 2011.
13. F. Zeng, H. Mu, and X. Wen, "An improved LMAP++ protocol combined with low-cost and privacy protection," in *Advanced Technologies, Embedded and Multimedia for Human-centric Computing*, pp. 847–853, Springer, 2014.

14. L. Kulseng, Z. Yu, Y. Wei, and Y. Guan, "Lightweight mutual authentication and ownership transfer for RFID systems," in *INFOCOM, 2010 Proceedings IEEE*, pp. 1–5, IEEE, 2010.
15. S. Kardas, M. Akgün, M. S. Kiraz, and H. Demirci, "Cryptanalysis of lightweight mutual authentication and ownership transfer for rfid systems," in *Lightweight Security & Privacy: Devices, Protocols and Applications (LightSec), 2011 Workshop on*, pp. 20–25, IEEE, 2011.
16. Z.-Y. Cheng, Y. Liu, C.-C. Chang, and S.-C. Chang, "Authenticated RFID security mechanism based on chaotic maps," *Security and Communication Networks*, vol. 6, no. 2, pp. 247–256, 2013.
17. M. Akgün, T. Uekae, and M. U. Caglayan, "Vulnerabilities of RFID security protocol based on chaotic maps," in *2014 IEEE 22nd International Conference on Network Protocols*, pp. 648–653, IEEE, 2014.
18. M. Benssalah, M. Djeddou, and K. Drouiche, "Security enhancement of the authenticated RFID security mechanism based on chaotic maps," *Security and Communication Networks*, vol. 7, no. 12, pp. 2356–2372, 2014.
19. M. Akgün, A. O. Bayrak, and M. U. ÇaÇğlayan, "Attacks and improvements to chaotic map-based RFID authentication protocol," *Security and Communication Networks*, vol. 8, no. 18, pp. 4028–4040, 2015.
20. W. Zhu, J. Yu, and T. Wang, "A security and privacy model for mobile RFID systems in the internet of things," in *Communication Technology (ICCT), 2012 IEEE 14th International Conference on*, pp. 726–732, IEEE, 2012.
21. I. Erguler, "A potential weakness in rfid-based internet-of-things systems," *Pervasive and Mobile Computing*, vol. 20, pp. 115–126, 2015.
22. K. Fan, Y. Gong, C. Liang, H. Li, and Y. Yang, "Lightweight and ultralightweight RFID mutual authentication protocol with cache in the reader for IoT in 5G," *Security and Communication Networks*, vol. 9, no. 16, pp. 3095–3104, 2015.
23. S. F. Aghili, M. Ashouri-Talouki, and H. Mala, "DoS, impersonation and de-synchronization attacks against an ultralightweight RFID mutual authentication protocol for IoT," *The Journal of Supercomputing*, pp. 1–17, 2017.