International Journal of Security and Its Applications
Vol. 12, No. 6 (2018), pp.1-12
http://dx.doi.org/10.14257/ijsia.2018.12.6.01

Security Analysis of an Ownership Transfer Protocol

Gelare Oudi Ghadim[1], Farokhlagha Moazami[1] and Shabnam Saderi Oskuiee[1]

[1]*Shahid Beheshti University, Cyberspace Research Institute*
Tehran, Iran
g.oudiqadim@mail.sbu.ac.ir, f_moazemi@sbu.ac.ir,
S.saderioskuiee@mail.sbu.ac.ir

Abstract

One of the important features of RFID systems is secure ownership transfer of the RFID tag. In many application of RFID tag, the owner of a tag might be changed many times. The main aspect of an ownership transfer protocol is security and efficiency. Recently, a scheme for ownership transfer based on Physically Unclonable Function (PUF) and a simple XOR that can be implemented on passive tags easily, has been proposed. The authors claim that their protocol offers tag anonymity, untraceability and forward untraceability for the new owner and the tag, resistant against desynchronization attack and replay attack. In this paper, we will analyze the security of the proposed protocol and will show that this protocol is vulnerable to forward traceability, impersonation, anonymity and traceability attack.

Keywords: *RFID; ownership transfer; security; attacks*

1. Introduction

Radio Frequency Identification (RFID) systems are used for detection or identification of people and objects. The main advantage of this technology is automatic detection of a large number of non-contacting objects and collecting information. Entrance systems, health-care, supply- chain management, measuring traffic, passport and credit cards can be mentioned as RFID applications.

A typical RFID system will include tags, readers and backend server. In RFID systems the information about detecting and identifying the objects will be saved on passive tags. Passive tags do not have internal battery to power themselves and they use the electromagnetic signal from the reader as the power source. Because the communication between the readers and the tags is wireless and insecure, a malicious attacker can perform some attacks to collect information and disruption in protocol. As a result, to prevent any complication, the readers and the tags should authenticate each other before any communication and data exchange.

Beside authentication, sometimes it is necessary to transfer ownership of the tag from one to another and this transfer may happen frequently in tags lifetime. Secure and efficient ownership transfer is an important aspect in RFID systems. Overall, an ownership Transfer protocol must protect the old and new owner's privacy. The new owner must be able to authenticate the tag and only the new owner can query the tag after ownership has been transferred. In a secure ownership transfer, an attacker should not be able to distinguish and track the tag. The anonymity of the tag is important, therefore the ID of the tag needs to be protected from the adversary. Also, a secure ownership transfer protocol must ensure that an attacker cannot impersonate any entity, be authenticated as a legitimate entity and communicates with other entities. As another security issue, an

Received (June 3, 2018), Review Result (October 1, 2018), Accepted (October 7, 2018)

ISSN: 1738-9976 IJSIA

attacker should not be able block messages transmitted between the tag and the backend server and protocol is out of synchronization.

A lot of works have been done in secure data and ownership transferring. Proposed protocols have weaknesses hence research in this area continues to this day. In past, researchers used symmetric cryptographic functions and asymmetric cryptographic functions to design protocols that provide better privacy and security [1, 2]. Due to the limited memory and computational power of passive tags, these tags are not able to use the standard cryptographic functions, so RFID ownership transfer protocols must use low-cost cryptographic primitives like pseudorandom number generators (PRNG), cyclic redundancy check (CRC) functions, physically unclonable functions (PUF), linear feedback shift register (LFSR) functions and bitwise operations, *etc*. Therefore, the protocols proposed by Feldhofer *et al.*, [1] and Kumar *et al.*, [2] not suitable and practical for passive RFID tags.

Many RFID ownership transfer protocols based on hash and keyed encryption functions have been proposed [3-8]. However, they all have some drawbacks. In 2007, Osaka *et al.*, [3] proposed an ownership transfer protocol with a TTP. Kapoor and Piramuthu *et al.*, [9] have been shown that in the protocol proposed by Osaka *et al.*, [3], an attacker by blocking the first message was sent by the reader to the tag (N_R) and send $N_R=0$ to the tag, can lead him/her to track the tag. Also this protocol suffers from desynchronization attack and cannot provide integrity. Chen *et al.*, [10] uses a hash function to verification the received key in the tag side to provide integrity and prevent desynchronization attack. However, in this improved protocol an attacker can still track the tag and lead him/her to desynchronization [9, 15]. Song *et al.*, [4] proposed a scheme for ownership transfer that transfers the ownership and updates the secret keys. Authors in [11] and [12] have been shown that the authentication protocol proposed by Song *et al.*, [4] is not secure against tracking the tag, desynchronization attack and an attacker can compromise the forward secrecy by capturing the tag and knowing the random number of the tag. Also authors in [11] have shown that the secret update protocol is vulnerable to desynchronization attack. Also Kapoor *et al.*, [9] has been shown that an attacker by blocking the messages was sent by the new owner and replies these messages to the current owner can perform ownership transfer protocol.

Also several lightweight RFID ownership transfer protocols that uses low-cost primitive cryptography have been proposed [13-18]. These protocol also suffer from security flaws. Kulseng *et al.*, [13] proposed a lightweight mutual authentication and ownership transfer protocol that uses a combination of PUF and LFSR. Kardas *et al.*, [19] have been shown that the mutual authentication protocol by Kulseng *et al.*, [13] is not secure against desynchronization attack when an attacker injects a random number to message was sent by the tag. Also their ownership transfer protocol does not provide privacy of the tag and the new owner against the old owner because after successful ownership transfer, the old owner still knows the tag's ID and using this ID, the old owner can identify the tag. Niu *et al.*, [14] proposed an ownership transfer and authentication protocol that uses XOR and a 16-bit PRNG. Safkhani *et al.*, [20] have been shown that in the proposed protocol in paper [14], the old owner with knowing K_M^1 can compromise the new owner's privacy and take control of the tag after ownership transfer. Sundaresan *et al.*, [15] have been proposed an ownership transfer protocol for multi-tag multi-owner that uses a simple XOR and a 128-bits PRNG function and provides good privacy for owners separately. Munilla *et al.*, [21] have been shown that this protocol is vulnerable against replay, forward traceability, desynchronization and tracking attacks. In this paper, we focus on lightweight ownership transfer protocols.

In 2016, Zhang *et al.*, [22] proposed a lightweight ownership transfer protocol that can be used in passive tags easily. This protocol is based on a Physically Unclonable Function (PUF) and a simple XOR that can be implemented on passive tags easily. A physical unclonable function is a physical entity that is embodied in a physical structure and is

easy to evaluate but hard to predict. Further, an individual PUF device must be easy to make but practically impossible to duplicate, even given the exact manufacturing process that produced it. In this respect, it is the hardware analog of a one-way function. Today, PUFs are usually implemented in integrated circuits and are typically used in applications with high security requirements.

In this paper, we will discuss security aspects of Zhang *et al.*, protocol and we will show that the protocol does not protect forward untraceability since the old owner is able to disclosure the new secrets have been established between the tag and the new owner. Therefore, the old owner is able to communicate with the tag after the ownership is transferred and hence the privacy of the new owner and the tag is compromised. Also, in this protocol, an attacker can impersonate S_{new} and does ownership transfer with the tag instead of the new owner. Finally, we will show that the protocol does not provide tag anonymity and tag untraceability since the tag's ID can be revealed by the attacker. Also, when ID of the tag is revealed by the attacker then the attacker can impersonate the tag.

The rest of the paper is organized as follows. We briefly review the ownership transfer protocol proposed by Zhang *et al.*, in Section 2. The vulnerabilities of this protocol are identified in Section 3. Finally, we conclude the paper in Section 4.

2. Review of Zhang et al.'s Protocol

In this section, we describe Zhang et al.'s protocol. Zhang et al. proposed a lightweight ownership transfer protocol using PUF function that can be implemented on passive low-cost tags. At first step, the old owner authenticates the tag to find and check its legitimacy. Secondly, the old owner passes all the tags information through a cable channel to the new owner. Finally, the new owner and the tag mutually authenticate each other. In fact, Zhang et al.'s protocol has three phases: mutual authentication between the old owner and the tag, ownership transfer phase and mutual authentication between the new owner and the tag. In the tag memory, they put one status bit f, if f=1 then the tag will accept ownership transfer and when the status bit is 0, the tag is in its own normal mode.

2.1. Mutual Authentication between the Old Owner and the Tag

In the mutual authentication phase of Zhang et al.'s protocol, the old reader first send a query command *OTHello* that the tag changes the status bit f to 1 at the end of the successful mutual authentication. This phase has two steps as follows:

2.1.1. Tag Identification: The reader sends *OTHello* to the tag and the tag sends ID_S to the reader. After receiving ID_S, the reader uses ID_S to search the backend database. If the ID_S doesn't match with ID_S^{new} but the ID_S matches with ID_S^{old}, then the reader uses ID_S^{old}, this means that in the last session, the tag could not update the data.

2.1.2. Mutual Authentication: Figure 1 illustrates the mutual authentication phase that is explained as follows:

Reader → Tag

- Reader generates a 96-bit random number n
- Using keys (G_n, G_{n+1}), Reader calculates:

$$A = ID_S \oplus G_{n+1} \oplus n \quad (1)$$

$$B = (G_n \oplus n) + G_{n+1} \quad (2)$$

$$X = \mathrm{ROT}(B, n) \oplus B \quad (3)$$

– Send A||X to the tag

Tag → Reader

– Tag when receives A||X calculates M and N and extracts n′, B′ and X′ as follows:

$$M = \text{PUF}(G_{\text{n}}) \tag{4}$$

$$N = \text{PUF}(M) \tag{5}$$

$$n' = ID_{\text{S}} \oplus M \oplus A \tag{6}$$

$$B' = (G_{\text{n}} \oplus n') + M \tag{7}$$

$$X' = \text{ROT}(B', n') \oplus B' \tag{8}$$

– Compare X to X′, if they are unequal, the tag sends a fail signal to the reader, else calculates:

$$D = M \oplus N \oplus n' \tag{9}$$

$$C = (IDT + ID_S) \oplus (n' + N) \tag{10}$$

$$Y = \text{ROT}(C, n') \oplus C \tag{11}$$

– Send D||Y to the reader.

Reader → Tag

– After the reader receives D||Y, calculates:

$$N' = D \oplus n \oplus G_{\text{n+1}} \tag{12}$$

$$C' = (IDT + ID_{\text{s}}) \oplus (n + N') \tag{13}$$

$$Y' = \text{ROT}(C', n) \oplus C' \tag{14}$$

– Compare Y to Y′, if they are unequal, the reader sends a fail signal to the tag, else the mutual authentication is successful and sends the success signal to the tag.

Update pseudonym and keys

– The reader:

$G_{\text{n}}^{\text{old}} = G_{\text{n}}$, $G_{\text{n}}^{\text{new}} = G_{\text{n+1}}$, $G_{\text{n+1}}^{\text{old}} = G_{\text{n+1}}$, $G_{\text{n+1}}^{\text{new}} = N'$,
$ID_{\text{S}}^{\text{old}} = ID_{\text{S}}$, $ID_{\text{S}}^{\text{new}} = N' + n + ID_{\text{S}}$.

– The tag:

$G_{\text{n}} = G_{\text{n+1}}$, $G_{\text{n+1}} = N$, $ID_{\text{S}} = N + n' + ID_{\text{S}}$.

2.2. Ownership Transfer Phase

After successful mutual authentication, the status bit of the tag changes to 1 and the tag can execute the ownership transfer protocol. The old owner sends the information about the tag to the new owner through a secure channel. In this session, we consider the old server and the reader as a whole and represent with S_{old}, we also represent the new server and the reader with S_{new}.

At first, S_{old} using its reader to send a query *Hello* to the tag and the tag sends ID_S to S_{old}. S_{old} receives ID_S and uses this ID_S to search in the old backend database for {ID_S, G_n, G_{n+1}, IDT} and sends them to the new server of the new owner.

Details of this phase are shown in Figure 2 that is explained as follows:

S_{new}→ S_{old}

– S_{new} receives tag secrets, generates a random number R and calculates:

$$E = ID_{\text{S}} \oplus R \tag{15}$$

$$F = G_{\text{n}} \oplus G_{\text{n+1}} \oplus R \tag{16}$$

$$U = \mathrm{ROT}(F, R) \oplus F \quad (17)$$

– Send E||U to S_{old}.

$S_{old} \rightarrow$ Tag

– S_{old} Sends E||U to the tag.

Tag$\rightarrow S_{old}$

– Tag extracts R′ and calculates:

$$R' = E \oplus ID_S \quad (18)$$

$$F' = G_n \oplus G_{n+1} \oplus R' \quad (19)$$

$$U' = \mathrm{Rot}(F', R') \oplus F' \quad (20)$$

– Compare U to U′, if they are equal, the received message is correct and the tag calculates:

$$J = G_n \oplus R' \quad (21)$$

$$K = \mathrm{PUF}(J) \quad (22)$$

$$S = J \oplus K \quad (23)$$

$$T = (IDT + ID_S) \oplus (R' + K) \quad (24)$$

– Send S||T to S_{old}.

$S_{old} \rightarrow S_{new}$

– S_{old} sends S||T to S_{new}.

$S_{new} \rightarrow S_{old}$

– S_{new} when receive S||T, calculates K′ and T′:

$$K' = S \oplus R \oplus G_n \quad (25)$$

$$T' = (IDT + ID_S) \oplus (R + K') \quad (26)$$

– Compare T to T′, if they are unequal, S_{new} drops the received message and sends a fail signal to S_{old}, else S_{new} updates its secret and sends a success signal to S_{old}.

$$G_n = G_n \oplus R \quad (27)$$

$$G_{n+1} = K' \quad (28)$$

$$ID_S = ID_S + R + K' \quad (29)$$

$S_{old} \rightarrow$ Tag

– S_{old} sends a success signal or fail signal to the tag.

Tag

– If the tag receives the success signal, it updates keys and pseudonym and meanwhile the tag sets the status bit f to 0.

$$G_n = J \quad (30)$$

$$G_{n+1} = K \quad (31)$$

$$ID_S = ID_S + R' + K \quad (32)$$

– If the tag receives the fail signal, it doesn't update keys and pseudonym and the status bit f remains 1.

2.3. Mutual Authentication between the New Owner and the Tag

After successful ownership transfer, S_{new} and the tag have new shared secrets which S_{old} doesn't know these secrets. Then, only the new owner can perform mutual authentication with the tag.

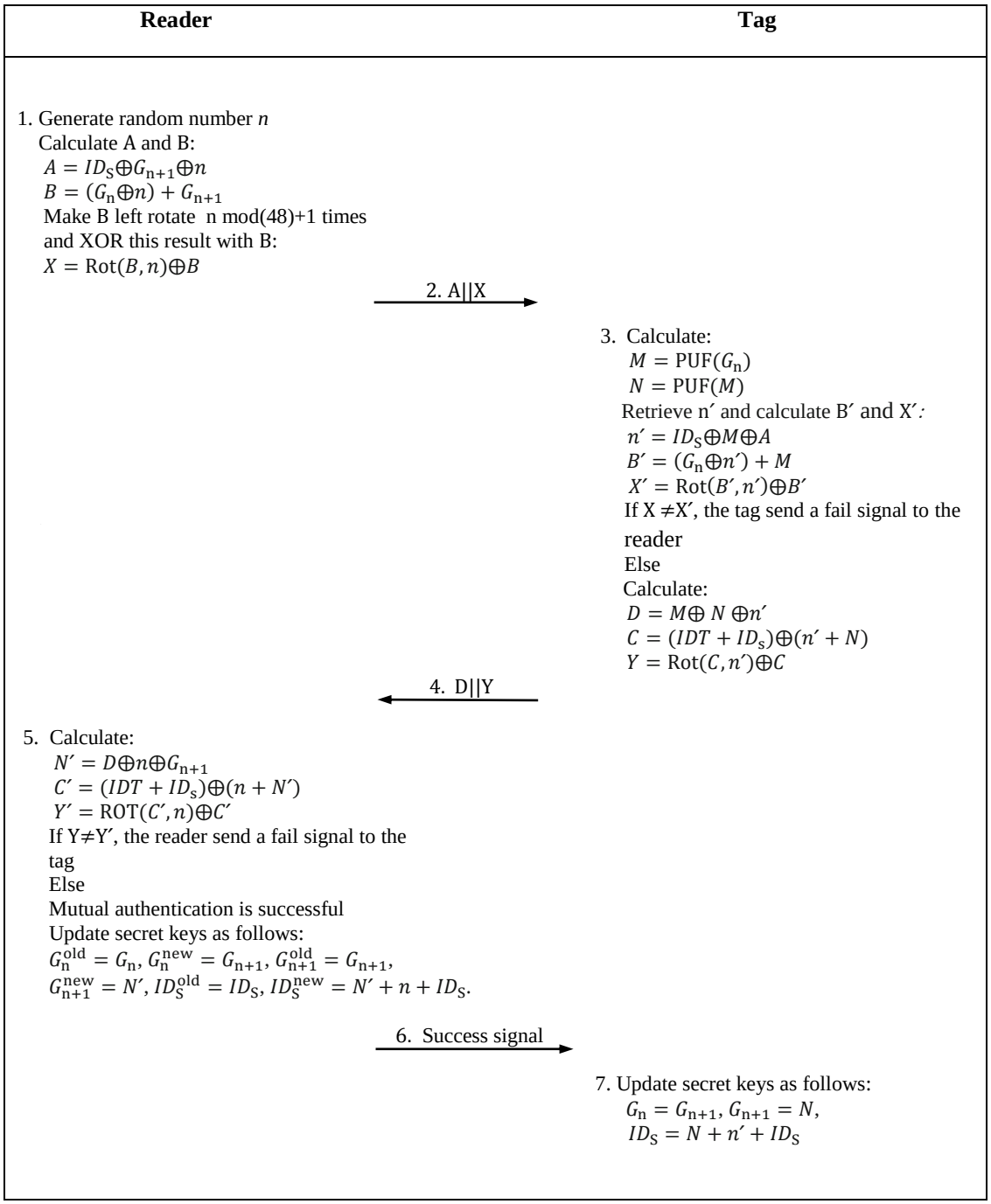

Figure 1. Mutual Authentication Protocol

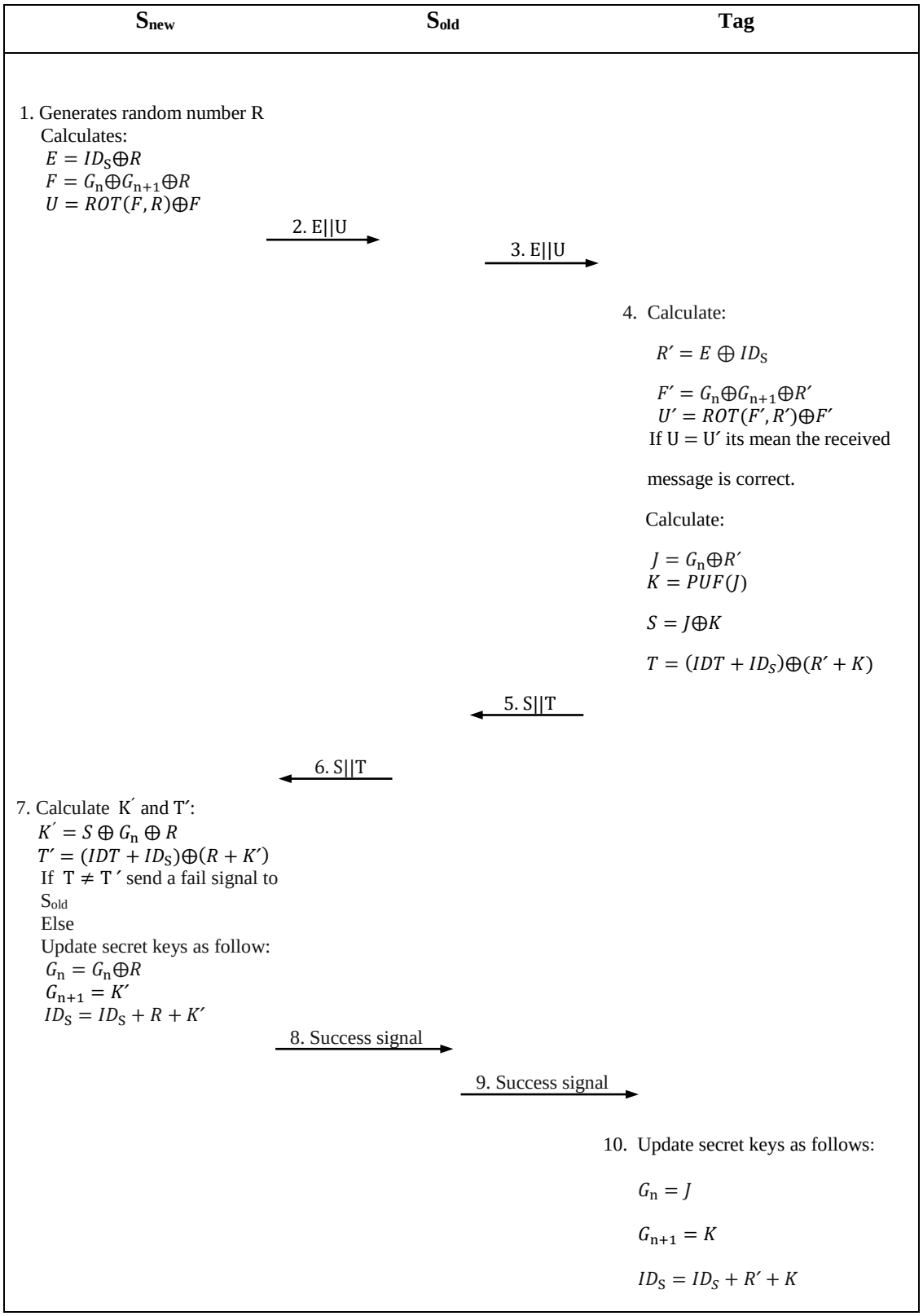

Figure 2. Ownership Transfer Protocol

3. Security Analysis

In this section, we will analyze the most important vulnerabilities in Zhang *et al.*, protocol.

3.1. Forward Traceability Attack

Providing forward untraceability means, the old owner after successful ownership transfer cannot communicate and trace the tag. Therefore, the old owner should not have any information about the new secrets between the tag and the new owner. In this subsection, we will show that the privacy of the tag and the new owner will be compromised easily by the old owner. In following, the details of the attack will be described.

- **Step 1:** First, the old owner saves all massages that received from the tag and the new owner. Therefore, the old owner knows {E, U, S, T}.
- **Step 2:** The old owner extracts R′ using equation (33) and calculates F′ and U′ according to the equations (34) and (35). Then, the old owner compares U to U′, if they are equal, the old owner has calculated R′ correctly.

$$R' = E \oplus ID_{\mathrm{S}} \tag{33}$$

$$F' = G_{\mathrm{n}} \oplus G_{\mathrm{n+1}} \oplus R' \tag{34}$$

$$U' = \mathrm{ROT}(F', R') \oplus F' \tag{35}$$

- **Step3:** Since the old owner knows the correct value of R, hence the old owner can calculate J′ and K′ according to the equations (36) and (37).

$$J' = G_{\mathrm{n}} \oplus R' \tag{36}$$

$$K' = S \oplus J' \tag{37}$$

With the above discussion, the old owner can calculate J′ and K′, which are the new shared secrets between the new owner and the tag. Hence the old owner can compromise the privacy of the new owner and the tag.

$$G_{\mathrm{n}} = J' \tag{38}$$

$$G_{\mathrm{n+1}} = K' \tag{39}$$

$$ID_{\mathrm{s}}^{\mathrm{new}} = ID_{\mathrm{s}}^{\mathrm{old}} + R' + K' \tag{40}$$

3.2. Impersonation Attack and Attack on anonymity and Traceability

In this subsection, we will show that Zhang *et al.*, protocol cannot prevent an attacker to perform S_{new} impersonation attack. Also, the authors claimed that in their protocol, an attacker cannot distinguish and track the tag. In the sequel, we will show that an attacker is able to obtain the tag's ID so anonymity of the tag is fail and hence the attacker can track the tag. Also, using the tag's ID, attacker can impersonate the tag.

Learning Phase:

Firs, the attacker eavesdrops the mutual authentication phase between the tag and the old reader and after one successful authentication phase, the attacker saves the exchanged messages between the tag and the old reader {A, X, D, Y, ID_S^{old}}. Also, the attacker eavesdrops the ownership transfer phase and obtains $ID_{\mathrm{s}}^{\mathrm{new}}$. Finally, the attacker by blocking E||U, prevents S_{new} from performing ownership transfer phase.

Attack Phase:

- **Step 1:** The attacker by possessing A, D and ID_S^{old}, extracts M⊕n and calculates N according to the equations (41) and (42).

$$M \oplus n = A \oplus ID_S^{old} \quad (41)$$

$$N = M \oplus n \oplus D \quad (42)$$

The attacker has ID_S^{new} and ID_S^{old}, therefore the attacker can calculate a random number n from equation (43) and obtain M by equation (44).

$$ID_S^{new} = ID_S^{old} + N + n \quad (43)$$

$$M = M \oplus n \oplus n \quad (44)$$

- **Step 2:** In the ownership transfer phase, the attacker impersonates S_{new}. To this aim, the attacker generates a new random number r and with knowing M and N, calculates E and U. Then, the attacker sends E||U to S_{old}.

$$E = ID_S^{new} \oplus r \quad (45)$$

$$F = \mathrm{M} \oplus \mathrm{N} \oplus r \quad (46)$$

$$U = \mathrm{ROT}(F, r) \oplus F \quad (47)$$

- **Step 3:** S_{old} sends E||U to the tag and the tag extracts r′ from equation (48). The tag calculates U′ and compares U to U′, if they are equal, the tag calculates J, K and S and send S||T to S_{old}.

$$r' = ID_S^{new} \oplus E \quad (48)$$

$$F' = G_n \oplus G_{n+1} \oplus r' \quad (49)$$

$$U' = \mathrm{ROT}(F', r') \oplus F' \quad (50)$$

$$J = G_n \oplus r' \quad (51)$$

$$K = \mathrm{PUF}(J) \quad (52)$$

$$S = J \oplus K \quad (53)$$

$$T = (IDT + ID_S^{new}) \oplus (r' + K) \quad (54)$$

- **Step 4:** S_{old} sends S||T to the attacker and the attacker can easily obtain K′ and J′, which are shared secrets between the tag and the attacker. In the end, the attacker sends success signal to S_{old}.

$$J' = M \oplus r \quad (55)$$

$$K' = S \oplus J' \quad (56)$$

$$ID_S = ID_S^{new} + r + K' \quad (57)$$

- **Step 5:** S_{old} sends success signal to the tag. After receiving success signal, the tag updates keys and pseudonym and sets the status bit f to 0.

$$G_n = J \quad (58)$$

$$G_{n+1} = K \quad (59)$$

$$ID_S = ID_S + r' + K \quad (60)$$

Therefore, an attacker can impersonate S_{new} and perform successful ownership transfer with the tag. Also, the attacker by knowing K and ID_S^{new}, can easily obtain IDT from equation (54). So the attacker has tag's ID and the anonymity of the tag can be broken.

The attacker now can track the tag since he/she has IDT and in every session can obtain ID_S, n and N, hence can calculate Y and identify the tag. Also, the attacker can impersonate the tag since the attacker has IDT and can update ID_S and obtain ID_S^{new}, G_n and G_{n+1}.

4. Conclusion

Zhang *et al.*, proposed a lightweight ownership transfer protocol that uses PUF functions and can be implemented on passive tags. Protocols that use PUF functions consider as powerful protocols because they can prevent lots of attacks. We discuss the security of Zhang *et al.*, ownership transfer and show that the proposed protocol has some drawbacks. In this protocol, the old owner can easily compromise the new owner's privacy and communicate with the tag after ownership transfer so the protocol doesn't provide forward untraceability. Also, this protocol is vulnerable to impersonation attack and an attacker can easily impersonate S_{new} and performs ownership transfer with the tag instead of S_{new}. Finally, we show that attacker can obtain the tag's ID and so the anonymity of the tag can be compromised by the attacker and the attacker can track the tag. Also, the attacker can impersonate the tag.

References

[1] M. Feldhofer, S. Dominikus and J. Wolkerstorfer, "Strong authentication for RFID systems using the AES algorithm", **(2004)**, pp. 357-370.
[2] S. Kumar, "Elliptic curve cryptography for constrained devices", Ph.D. Dissertation, Ruhr-University Bochum, **(2006)**.
[3] K. Osaka, T. Takagi, K. Yamazaki and O. Takahashi, "An efficient and secure RFID security method with ownership transfer", Proceedings of the International Conference on Computational Intelligence and Security (CIS), LNAI 4456, **(2007)**, pp. 778-787.
[4] B. Song, "RFID tag ownership transfer", In Proceedings of Workshop on RFID Security, Budapest, Hungary, **(2008)**.
[5] G. Kapoor and S. Piramuthu, "Single RFID tag ownership transfer protocols", IEEE Transactions on Systems, Man and Cybernetics, Part C: Applications and Reviews, vol. 42, no. 2, **(2012)**, pp. 164-173.
[6] H. Lei and T. Cao, "RFID protocol enabling ownership transfer to protect against traceability and DoS attacks", The First International Symposium on Data, Privacy and E-Commerce, IEEE Computer Society, **(2007)**, pp. 508-510.
[7] S. Fouladgar and H. Afifi, "A simple privacy protecting scheme enabling delegation and ownership transfer for RFID tags", Journal of Communications, vol. 2, no. 6, **(2007)**, pp. 6-13.
[8] B. Song and C. J. Mitchell, "Scalable RFID security protocols supporting tag ownership transfer", Computer Communications, vol. 34, no. 4, **(2011)**, pp. 556-566.
[9] G. Kapoor and S. Piramuthu, "Vulnerabilities in some recently proposed RFID ownership transfer porotocols", IEEE Commun. Lett, vol. 14, no. 3, **(2010)**, pp. 260-262.
[10] H. Chen, W. Lee, Y. Zhao and Y. Chen, "Enhancement of the RFID security method with ownership transfer", Proceedings International Conference on Ubiquitous Information Management and Communication, **(2009)**, pp. 251-254.
[11] P. Peris-Lopez, J. C, Hernandez-Castro, J. M. Tapiador, T. Li and Y. Li, "Vulnerability analysis of RFID protocols for tag ownership transfer", Computer Networks, vol. 54, no. 9, **(2010)**, pp. 1502-1508.
[12] P. Rizomiliotis, E. Rekleitis and S. Gritzalis, "Security analysis of Song and Mitchell authentication protocol for low-cost RFID tags", IEEE Communications Letter, vol. 13, no. 4, **(2009)**, pp. 274-276.
[13] L. Kulseng, Z. Yu, Y. Wei and Y. Guan, "Lightweight mutual authentication and ownership transfer for RFID systems", In INFOCOM'10: Proceeding of the 29th Conference on Information Communications, **(2010)**, pp. 251-255.
[14] H. Niu, E. Taqieddin and S. Jagannathan, "EPC Gen2v2 RFID standard authentication and ownership management protocol", IEEE Transactions on Mobile Computing, vol. 15, no. 1, **(2014)**, pp. 137-149.
[15] S. Sundaresan, R. Doss, W. Zhou and S. Piramuthu, "Secure ownership transfer for multi-tag multi-owner passive RFID environment with individual-owner-privacy", Computer Communications, vol. 55, **(2015)**, pp. 112-124.

[16] C. L. Chen, Y. C. Huang and J. R. Jiang, "A secure ownership transfer protocol using EPC global Gen-2 RFID", Telecomunication System, vol. 53, **(2013)**, pp. 387-399.
[17] X. Fu and Y. Guo, "A lightweight RFID mutual authentication protocol with ownership transfer", Advances in Wireless Sensor Networks Communications in Computer and Information Science, vol. 334, **(2013)**, pp. 68-74.
[18] R. Doss, Z. Wanlei and Y. Shui, "Secure RFID tag ownership transfer based on quadratic residues", IEEE Transactions on Information Forensics and Security, vol. 8, no. 2, **(2013)**, pp. 390-401.
[19] S. Kardas, M. Akgun, M. Kiraz and H. Demirci, "Cryptanalysis of lightweight mutual authentication and ownership transfer for RFID systems", Workshop on Lightweight Security and Privacy: Devices, Protocol and Applications, **(2011)**, pp. 20-25.
[20] M. Safkhani, H. Jannati and N. Bagheri, "Security analysis of Niu et al. authentication and ownership protocol", IACR Cryptology ePrint Archive 2015:615, **(2015)**, pp. 1-8.
[21] J. Munilla, M. Burmester and A. Peinado, "Attacks on Ownership Transfer Scheme for Multi-tag Multi-owner Passive RFID Environments", Computer Communications 000, **(2016)**, pp. 1-5.
[22] X. Zhang, W. Huang, H. Xu and Y. Wang, "The lightweight ownership transfer protocol using physically unclonable function", International Journal of Security and Its Applications, vol. 10, no. 2, **(2016)**, pp. 115-128.

Authors

Gelare Oudi Ghadim, she is the master student in secure communication and cryptography from Shahid Beheshti University, Tehran, Iran and B.S. degree in communication engineering from Sistan and Baluchestan University, NNN Zahedan, Iran, in 2015. Her researches interested include RFID security and privacy.

Farokhlagha Moazami is an assistant professor at the Cyber Space Research Institute at Shahid Beheshti University, Iran, Tehran, since 2013. She received B.S. and Ph.D. degrees in mathematics from Alzahra University, Tehran, Iran, in 2004 and 2012, respectively and M.S. degree in mathematics from Sharif University of Technology, Iran, Tehran, in 2006. She was a postdoctoral at Sharif University of Technology, Iran, Tehran, from 2012 to 2013. Her main research interests are theoretical and practical aspects of cryptography.

Shabnam Saderi Oskuiee, she is the master student in secure communication and cryptography from Shahid Beheshti University, Tehran, Iran and B.S. degree in communication engineering from Tabriz University, Tabriz, Iran, Zaheda. In 2015, her researches interested include RFID security and privacy.

