Cryptanalysis of Cho *et al.*'s Protocol, A Hash-Based Mutual Authentication Protocol for RFID Systems

Masoumeh Safkhani[1], Pedro Peris-Lopez[2], Julio Cesar Hernandez-Castro[3], Nasour Bagheri[4] and Majid Naderi[1]

[1] Electrical Engineering Department, Iran University of Science and Technology, Tehran, Iran, {M_Safkhani,M_Nderi}@iust.ac.ir

[2] Information Security and Privacy Lab, Delft University of Technology, Delft, The Netherlands, P.PerisLopez@tudelft.nl

[3] School of Computing of Portsmouth University, UK, Julio.Hernandez-Castro@port.ac.uk

[4] Electrical Engineering Department, Shahid Rajaee Teacher Training University, Tehran, Iran, Nbagheri@srttu.edu

Abstract. Radio frequency identification systems need protocols to provide confidentiality, user privacy, mutual authentication and etc. These protocols should resist active and passive attacks such as forgery, traceability, replay and desynchronization attacks.

In this paper we cryptanalysis a hash based RFID mutual authentication protocol which has been recently proposed by Cho *et al.* More precisely, we present the following attacks on this protocol:

1. **Desynchronization attack**: the success probability of attack is "1" while the attack complexity is one run of protocol.
2. **Tag impersonation attack**: the success probability of attack is "$\frac{1}{4}$" for two runs of protocol.
3. **Reader impersonation attack**: the success probability of attack is "$\frac{1}{4}$" for two runs of protocol.

Keywords: RFID, Authentication, Desynchronization Attack, Tag Impersonation Attack, Reader Impersonation Attack.

1 Introduction

Radio Frequency Identification (RFID) technology is a new wireless technology that has a great capability to find many applications an influence many aspects of life in the near future. It has already been used in libraries, e-passports, manufacturing, inventory control, supply chain management, e-health and so on. The tag, the reader and the back-end data base are three basic components of an RFID system. Tags are connected to the objects that are supposed to be identified through radio frequency signals by the reader. The back-end data base mainly aids the reader by an extra storage spaces and further computational capability. That extra storage space can be used to keep the information of all tags that can be accessed by the reader. However, the main problem that impacts RFID system application is data security which may waives all its benefits. For example, an RFID system may lead to privacy problems for the object which is supposed to be identified through the tag. Hence, the end users need a guarantee to be sure that they will not be spoofed by any non-ligament reader, their data will remain secure, receive a reliable service and etc. On the other hand, it should not be possible for any invalid tag to spoof an authenticated reader as a legitimate tag. To address these requirements, several RFID mutual authentication protocols [1–18] have already been proposed in the literatures, the security of many of them has already been violated [19–30].

Recently Cho *et al.* has proposed a hashed based mutual authentication protocol [15] and claimed that their protocol completely solves the privacy concerns [31] and forgery concerns [32, 33] of RFID systems. However, we show that their protocol does not satisfy the claimed requirement. More precisely, we present tag impersonation, reader impersonation and desynchronization attacks on this protocol. All attacks have the high success probability and negligible complexity.

The rest of the paper is organized as follows: In section § 2 we describe some notations and preliminaries that used thorough this paper. We briefly review Cho *et al.* 's protocol in section § 3. Our desynchronization, tag impersonation and reader impersonation attacks are presented in sections § 4, § 5 and § 6 respectively. Concluding remarks are presented in Section § 7.

2 Preliminaries

The notations that used through of this paper are as follows:

- ID_k: Identifier of the k^{th} tag.
- $h(.)$: One way hash function.
- $||$: A concatenation operation.
- $\oplus$: Exclusive-or operation.
- s: An 96-bit secret value which is shred between tag and back-end server.
- s_j: A secret value used in the j^{th} session.
- $DATA$: Tag's related information.
- RID_i: An 96-bit Group ID of random number.
- R_r: Random number generated by reader.
- R_t: Random number generated by tag.
- α: Message generated by tag for authentication.
- β: Blind factor.
- $X_{(a:b)}$: A fraction of value X includes the a^{th}-bit to the b^{th}-bit.
- X^i: Parameter X related to the i^{th} tag.

3 Cho *et al.*'s RFID Hash-based Mutual Authentication Protocol

Recently, Cho *et al.* [15] proposed a mutual authentication protocol for RFID systems. The proposed protocol uses a one way hash function in its structure and expected to provide enough security against various attacks. In addition, they randomize each session of mutual authentication by employing two random values R_r and R_t, respectively generated by the reader and the tag and a value denoted by RID_i which is supposed to be dependent on R_t. Since the secret value of tag s_j get updated at each successful run of protocol, to avoid the desynchronization attack the back-end database keeps a record of two latest secret value of tag denoted by s_{old} and s_{new} respectively. The protocol, see also Fig. 1, works as follows:

1. The reader generates a random number R_r and sends *request* along with R_r to the tag.
2. As the tag receives the message, it generates another random number R_t and does as follows:

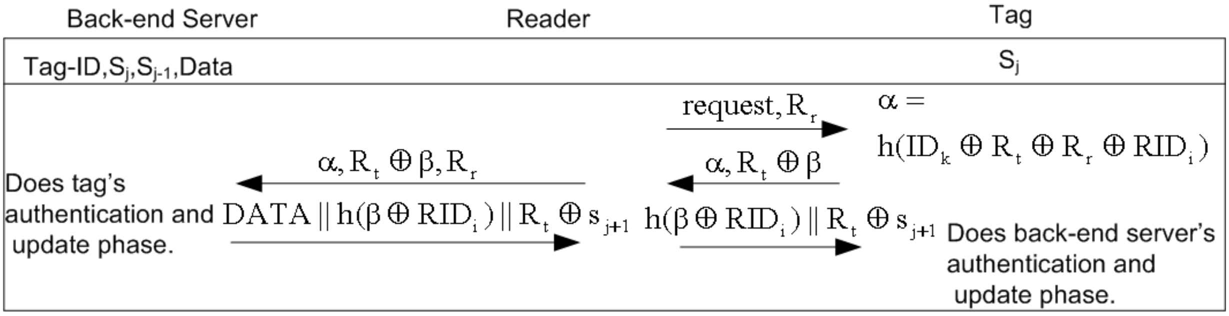

Fig. 1. The Cho *et al.*'s hash-based RFID Mutual Authentication Protocol.

(a) It computes $RID_i = (R_t - R_t \bmod s_j + 1)_{(0:47)} || (R_t + s_j - R_t \bmod s_j)_{(48:95)}$, $\alpha = h(ID_k \oplus R_t \oplus R_r \oplus RID_i)$ and $\beta = (s_j)_{(0:47)} || (ID_K)_{(48:95)}$.
(b) It sends α and $R_t \oplus \beta$ to the reader.

3. As the reader receives α and $R_t \oplus \beta$, passes them to the back-end data base.
4. To authenticate the tag and update the secret value s, the back-end data base does as follows:
   (a) for any record i on its data base (the i^{th} record includes $(ID_k^i, s_{old}^i, s_{new}^i, Data^i)$ of a tag) it computes β for each tuple (ID_k^i, s_{old}^i) and (ID_k^i, s_{new}^i), extracts R_t from $R_t \oplus \beta$ for any computed β, calculates RID_i' and $\alpha' = h(ID_k \oplus R_t \oplus R_r \oplus RID_i')$.
   (b) If it finds a match between the received α and a retrieved α', it will authenticate the tag and updates its record. Assuming that (ID_k^i, s_j^i) is a tuple for which tag i has been authenticated, the back-end data base will authenticate the record of the authenticated tag as follows:
      – it assigns s_j^i to s_{old}^i,
      – generates a new secret value s_{j+1} and assigns it to s_{new}^i.
   (c) The back-end data base generates $DATA || h(\beta \oplus RID_i) || R_t \oplus s_{j+1}$ and sends it to the reader.
5. The reader passes $h(\beta \oplus RID_i) || R_t \oplus s_{j+1}$ to the tag.
6. The tag extracts $h(\beta \oplus RID_i)$ from the received value and verifies it to whether authenticate the reader.
7. If the tag authenticated the reader it extracts s_{j+1} from $R_t \oplus s_{j+1}$ and updates its secret value s_j to s_{j+1}.

The authors have claimed several security properties for the protocol [15, Section 6.] including but not limited to the following properties:

– resistance against the desynchronization attack.
– resistance against the spoofed reader attack, in which the adversary sends intended or meaningless request and tries to $h(\beta \oplus RID_i)$ to be authenticated by the tag.
– resistance against the spoofed tag attack, in which the adversary tries to generate a valid α to be authenticated by the reader.

However, in the following sections we present several attacks on this protocol that contradicted the above mentioned authors' claims.

4 Desynchronization Attack

Cho *et al.* [14] claim that their protocol is resistant against the desynchronization attack. More precisely, the authors state that the protocol prevents the problem of desynchronization via keeping a record of *old* secret value s to avoid from get desynchronized when tag does not receive the last message of protocol properly. However, we observed a flaw on the protocol that can be used to desynchronize the tag and the reader easily. To desynchronize the tag T_i and the reader R the adversary can follow the steps described below:

1. Eavesdrop one session of protocol.
2. Change the last message that sent by R to T_i from $h(\beta \oplus RID_i)||R_t \oplus s_{j+1}$ to $h(\beta \oplus RID_i)||R_t \oplus s_{j+1} \oplus \Delta$, for $\Delta \neq 0$.
3. The tag authenticates the reader based on the received $h(\beta \oplus RID_i)$ and assigns $s_{j+1} \oplus \Delta$ to s_{j+1}.

Following the above attack the secret value contained in T_i is set to $s_{j+1} \oplus \Delta$ while the stored values on R are s_j and s_{j+1} and the reader has no record of $s_{j+1} \oplus \Delta$. Hence, R never authenticates T_i in the next sessions of protocol. The success probability of our desynchronization attack is “1” and the complexity of attack is only one run of protocol.

5 Tag Impersonation Attack

Cho *et al.* [14] claim that it would not be possible for the adversary to generate a tuple α and $\beta \oplus R_t$ such that the reader authenticate the adversary as a valid Tag. More precisely, the authors state that to generate a valid α and $\beta \oplus R_t$ and impersonate the tag, the adversary at least requires to find the secret values s_j and ID_k that are protected by $h(.)$. However, we present a rather simple attack which can impersonate a legitimate tag without any knowledge of the secret values s_j and ID_k. Our attack is based on this fact that for $a < b$ we can state that:

$$a \ mod \ b \equiv a$$

Given this fact and assuming that $R_t < s_j$ we have:

$$RID_i = (R_t - R_t \ mod \ s_j + 1)_{(0:47)}||(R_t + s_j - R_t \ mod \ s_j)_{(48:95)} = (1)_{(0:47)}||(s_j)_{(48:95)}$$

which independents on R_t. Now, we use this observation on the tag impersonation attack which its steps are described below:

1. Adversary eavesdrops one session of protocol and obtains R_r, α, $R_t \oplus \beta$, where assuming that $R_t < s_j$ then $RID_i = (1)_{(0:47)}||(s_j)_{(48:95)}$.
2. On the next session of protocol, when the reader sends *request* along with R'_r, adversary impersonates the tag and replies with the tuple α and $R_t \oplus \beta \oplus R_r \oplus R'_r$.
3. The back-end server uses the tuple (ID_k, s_j) of the tag to generate β and extracts $R'_t = R_t \oplus R_r \oplus R'_r$ and RID'_i.
4. The back-end data base uses the extracted R'_t and RID'_i to verify whether $\alpha \stackrel{?}{=} h(ID_k \oplus R'_t \oplus R'_r \oplus RID'_i)$.

5. If $R'_t < s_j$ then $RID'_i = (1)_{(0:47)} || (s_j)_{(48:95)} = RID_i$ and we have:

$$h(ID_k \oplus R'_t \oplus R'_r \oplus RID'_i) = h(ID_k \oplus R_t \oplus R_r \oplus R'_r \oplus R'_r \oplus RID_i) = h(ID_k \oplus R_t \oplus R_r \oplus RID_i) = \alpha$$

6. Since $\alpha = h(ID_k \oplus R'_t \oplus R'_r \oplus RID'_i)$ the back-end data base authenticates the adversary as a legitimate tag.

The adversary will be succeed in its attack if the assumptions are correct. For random selection of R_t and R_r, the success probability of each assumption is "$\frac{1}{2}$". Hence the total probability of the above tag impersonation attack is "$\frac{1}{4}$" and the complexity of attack is two runs of protocol.

Remark 1. The above attack works as long as the tag has not updated its secret value s. However, when the adversary does the eavesdropping phase at step 1. of the above attack, if it blocks the last message of protocol, on which the reader sends $h(\beta \oplus RID_i) || R_t \oplus s_{j+1}$ to the tag, then the attack can be applied even after one updating of secret value s. The reason comes from this property of protocol that the back-end data base keeps a record of s_{old}.

6 Reader Impersonation Attack

The authors [14] claim that the proposed protocol is very secure against an intended request because the adversary has no control on the generated R_t and the related RID_i that are changed every session, even if the secret value s has not been updated. However, we present an attack which can impersonate a legitimate reader without any knowledge of the secret values s_j and ID_k and any control over the generated R_t. Our attack is based on the given observation that for $R_t < s_j$ one can state that:

$$RID_i = (1)_{(0:47)} || (s_j)_{(48:95)}$$

which is independent on R_t. The proposed reader impersonation attack is as bellow:

1. Adversary eavesdrops one session of protocol and obtains R_r, α, $R_t \oplus \beta$ and $h(\beta \oplus RID_i) || R_t \oplus s_{j+1}$, where for $R_t < s_j$ one can state that:

$$RID_i = (1)_{(0:47)} || (s_j)_{(48:95)}$$

2. It blocks the last message from the reader to the tag, $h(\beta \oplus RID_i) || R_t \oplus s_{j+1}$. Hence, the tag does not update its secret value s.
3. Adversary supplants a legitimate reader and sends *request* with the stored R_r to the tag and receives tag's response, α' and $R'_t \oplus \beta'$, where $\beta' = \beta$ because the secret value s has not been updated.
4. For $R'_t < s_j$ we can state that:

$$RID'_i = (1)_{(0:47)} || (s_j)_{(48:95)} = RID_i$$

5. The adversary replies to the tag with $h(\beta \oplus RID_i) || \Delta$, where Δ can be any random value.
6. For the given assumptions, $h(\beta \oplus RID_i) = h(\beta' \oplus RID'_i)$ and the tag authenticates the adversary as a legitimate reader.

The adversary will be succeed in its attack if the assumptions are correct, i.e. $R_t < s_j$ and $R'_t < s_j$. For random selection of R_t and R'_t, the success probability of each assumption is "$\frac{1}{2}$". Hence, the total probability of the above reader impersonation attack is "$\frac{1}{4}$" and the complexity of attack is eavesdropping one run of protocol and supplant a session following it.

Remark 2. The given attack desynchronizes the tag from the reader, because after the supplanted run of protocol the tag updates its secret value s to $s_j = R'_t \oplus \Delta$ which the legitimate reader has no knowledge of it.

7 Conclusion

In this paper we analyzed the security of Cho *et al.* mutual authentication protocol which is a hash based protocol to be employed in RFID systems. We demonstrated desynchronization, tag impersonation and reader impersonation attacks on this protocol. The success probability of these attacks are "1", "$\frac{1}{4}$" and "$\frac{1}{4}$" respectively and the complexity of each attack is at most two runs of protocol.

References

1. S. Weis. *Security and Privacy in Radio Frequency Identification Devices*. Masters Thesis, Massachusetts Institute of Technology (MIT), 2003.
2. Stephen A. Weis, Sanjay E. Sarma, Ronald L. Rivest, and Daniel W. Engels. Security and Privacy Aspects of Low-Cost Radio Frequency Identification Systems. In *International Conference on Security in Pervasive Computing-SPC 2003*, volume 2802 of *Lecture Notes in Computer Science*, pages 201–212, 2004.
3. Kinoshita S. Ohkubo M., Suzuki K. Hash-chain based forward-secure privacy protection scheme for low-cost RFID. In *Proc. of the 2004 Symposium on Cryptography and Information Security (SCI 2004)*, pages 719–724, 2004.
4. Yiyuan Luo, Qi Chai, Guang Gong, and Xuejia Lai. A lightweight stream cipher WG-7 for RFID encryption and authentication. In *GLOBECOM*, pages 1–6. IEEE, 2010.
5. Pedro Peris-Lopez, Julio Cesar Hernandez-Castro, Juan M. Estevez-Tapiador, and Arturo Ribagorda. EMAP: An Efficient Mutual Authentication Protocol for Low-Cost RFID Tags. In *OTM Federated Conferences and Workshop: IS Workshop – IS'06*, volume 4277 of *Lecture Notes in Computer Science*, pages 352–361, Montpellier, France, November 2006. Springer-Verlag.
6. Chien Hung-Yu. SASI: A New Ultralightweight RFID Authentication Protocol Providing Strong Authentication and Strong Integrity. *IEEE Transactions on Dependable and Secure Computing*, 4(4):337–340, December 2007.
7. Pedro Peris-Lopez, Julio César Hernández Castro, Juan M. Estévez-Tapiador, and Arturo Ribagorda. LMAP:A Real Lightweight Mutual Authentication Protocol for Low cost RFID tags. In *RFIDSec*, 2006.
8. Pedro Peris-Lopez, Julio César Hernández Castro, Juan M. Estévez-Tapiador, and Arturo Ribagorda. Advances in Ultralightweight Cryptography for Low-Cost RFID Tags: Gossamer Protocol. In Kyo-Il Chung, Kiwook Sohn, and Moti Yung, editors, *WISA*, volume 5379 of *Lecture Notes in Computer Science*, pages 56–68. Springer, 2008.
9. Alireza Sadighian and Rasoul Jalili. AFMAP: Anonymous Forward-Secure Mutual Authentication Protocols for RFID systems. In Rainer Falk, Wilson Goudalo, Eric Y. Chen, Reijo Savola, and Manuela Popescu, editors, *The Third IEEE International Conference on Emerging Security Information, Systems and Technologies(SECURWARE 2009)*, pages 31–36, Athens, Greece, 2009. IEEE Computer Society.
10. Alireza Sadighian and Rasool Jalili. FLMAP: A fast lightweight mutual authentication protocol for RFID systems. In *ICON*, pages 1–6. IEEE, 2008.
11. Lars Kulseng, Zhen Yu, Yawen Wei, and Yong Guan. Lightweight Mutual Authentication and Ownership Transfer for RFID systems. In *The proceedings of IEEE INFOCOM 2010*, pages 1–5, March 2010.
12. R.Rivest-D. Engels S.Weis, S.Sarma. Security and privacy aspects of low-cost radio frequency identification systems. In *1st International Conference on Wierless Communications, Networking and mobile computing 2007(WiCom 2007)*, pages 2078–2080, 2007.

13. Hung-Yu Chien. Secure access control schemes for RFID systems with anonymity. In *Mobile Data Management*. IEEE Computer Society, 2006.
14. Meng-Lin Tsai Yu-Yi Chen and Jinn-Ke Jan. The design of RFID access control protocol using the strategy of indefinite-index and challenge -response. In *Computer Communication*, volume 34, pages 250–256, 2011.
15. Sang-Soo Yeo Jung-Sik Cho and Sung Kwon Kim. Securing against brute-force attack: A hash-based RFID mutual authentication protocol using a secret value. In *Comput.Commun,doi:10.1016/j.comcom.2010.02.029*, 2010.
16. Tzu-Chang Yeh, Chien-Hung Wu, and Yuh-Min Tseng. Improvement of the rfid authentication scheme based on quadratic residues. *Computer Communications*, 34(3):337–341, 2011.
17. Dang Nguyen Duc and Kwangjo Kim. Defending rfid authentication protocols against dos attacks. *Computer Communications*, 34(3):384–390, 2011.
18. Chiu Chiang Tan, Bo Sheng, and Qun Li. Secure and serverless RFID authentication and search protocols. *IEEE Transactions on Wireless Communications*, 7(4):1400–1407, 2008.
19. Mihály Bárász, Balázs Boros, Péter Ligeti, Krisztina Lója, and Dániel Nagy. Passive Attack Against the M2AP Mutual Authentication Protocol for RFID Tags. In *First International EURASIP Workshop on RFID Technology*, Vienna, Austria, September 2007.
20. Tianjie Cao, Elisa Bertino, and Hong Lei. Security analysis of the sasi protocol. *IEEE Trans. Dependable Sec. Comput.*, 6(1):73–77, 2009.
21. Julio C Hernandez-Castro, Juan M E Tapiador, Pedro Peris-Lopez, and Jean-Jacques Quisquater. Cryptanalysis of the SASI Ultralightweight RFID Authentication Protocol with Modular Rotations. Technical Report arXiv:0811.4257, Nov 2008.
22. Raphael C.-W. Phan. Cryptanalysis of a New Ultralightweight RFID Authentication Protocol - SASI. *IEEE Transactions on Dependable and Secure Computing*, 99(1), 2008.
23. Tieyan Li and Robert H. Deng. Vulnerability Analysis of EMAP - An Efficient RFID Mutual Authentication Protocol. In *Second International Conference on Availability, Reliability and Security – AReS 2007*, Vienna, Austria, April 2007.
24. Mihály Bárász, Balázs Boros, Péter Ligeti, Krisztina Lója, and Dániel Nagy. Passive Attack Against the M2AP Mutual Authentication Protocol for RFID Tags. In *First International EURASIP Workshop on RFID Technology*, Vienna, Austria, September 2007.
25. Masoumeh Safkhani, Majid Naderi, and Nasour Bagheri. Cryptanalysis of AFMAP. *IEICE Electronics Express*, 7(17):1240–1245, 2010.
26. Masoumeh Safkhani, Majid Naderi, and Habib Rashvand. Cryptanalysis of AFMAP. *International Journal of Computer & Communication Technologys*, 2(2):182–186, 2010.
27. Masoumeh Safkhani, Nasour Bagheri, Majid Naderi, Yiyuan Luo, and Qi Chai. Tag impersonation attack on two RFID mutual authentication protocols. In *FARES*, 2011.
28. Masoumeh Safkhani, Majid Naderi, Nasour Bagheri, and Somitra Kumar Sanadhya. Cryptanalysis of some protocols for RFID systems. Cryptology ePrint Archive, Report 2011/061, 2011. `http://eprint.iacr.org/`.
29. Masoumeh Safkhani, Nasour Bagheri, and Majid Naderi. Cryptanalysis of Chen *et al.*'s RFID access control protocol. Cryptology ePrint Archive, Report 2011/194, 2011. `http://eprint.iacr.org/`.
30. Nasour Bagheri, Masoumeh Safkhani, Majid Naderi, and Somitra Kumar Sanadhya. Security analysis of $LMAP^{++}$, an RFID authentication protocol. Cryptology ePrint Archive, Report 2011/193, 2011. `http://eprint.iacr.org/`.
31. A.Jules. RFID security and privacy: a reserch survey. In *Selected Areas in Communications*, volume 24, pages 381–394, 2006.
32. T.Dimitriou. A lightweight RFID protocol to protect against traceability and cloning attacks. In *in Proceedings of SecureComm'05*, pages 59–66, 2005.
33. H.Lee-K.Ren-K.Kim J.Yang, J.Park. Mutual authentication protocol for low-cost RFID. In *In proceedings of the Workshop on RFID and Lightweight Cryptography*, pages 17–24, 2005.