The ISC Int'l Journal of Information Security

July 2016, Volume 8, Number 2 (pp. 155–160)

http://www.isecure-journal.org

Short Paper

A Note on the Security of Two Improved RFID Protocols

Masoumeh Safkhani [1,*], and Nasour Bagheri [2]

[1] *Computer Engineering Department, Shahid Rajaee Teacher Training University, Tehran, Iran*

[2] *Electrical Engineering Department, Shahid Rajaee Teacher Training University, Tehran, Iran*

ARTICLE INFO.

Article history:

Received: 17 March 2016

Revised: 28 May 2016

Accepted: 4 June 2016

Published Online: 23 June 2016

Keywords:

RFID, Authentication Protocol, Desynchronization Attack, Secret Disclosure Attack.

ABSTRACT

Recently, Baghery *et al.* [1, 2] presented some attacks on two RFID protocols, namely Yoon and Jung *et al.* protocols, and proposed the improved version of them. However, in this note, we show that the improved version of the Jung *et al.* protocol suffers from desynchronization attack and the improved version of the Yoon's protocol suffers from secret disclosure attack. The success probability of the desynchronization attack against the improved version of the Jung *et al.* protocol is $(1-2^{-2n})^2$, where n is length of the protocol parameters. The attack can be accomplished with just three runs of the protocol. The success probability of the secret disclosure attack against the improved version of the Yoon's protocol is almost 1, while the complexity is just two runs of the protocol and doing 2^{16} off-line evaluations of PRNG function.

1 Introduction

Baghery *et al.* [1, 2] recently proposed an attempt on enhancing the privacy of two recent authentication schemes for low-cost RFID systems, i.e., Yoon [3] and Jung *et al.* [4] protocols. The first protocol was an enhancement of Yoon's protocol [3], which is an improvement over Yeh *et al.*'s protocol [5] and has already received several security analyses, e.g., see [6, 7].

In this letter, the security of the improved version of the protocols are scrutinized and important security pitfalls are shown.

The rest of the letter is organized as follows: In Section 2, we review the improved Yoon's protocol and present the secret disclosure attack against it. The description of the Jung*et al.* protocol and the desynchronization attack against it are explained in Section 3. Section 4 gives some solutions to address the weaknesses of the protocols against the attacks presented in this letter.Finally the paper concludes in Section 5.

2 On the security of the improved Yoon's protocol

2.1 Protocol Description

As depicted in Figure 1, in this section, using the notation depicted in Table 1, we give a brief description of the improved Yoon's protocol. This protocol has two phases: the initialization phase and the $(i+1)^{th}$ authentication phase which is described as follows:

Initialization Phase: In this phase, the manufacture generates random values for K_0, P_0 and C_0, respectively and sets the values of the record in

* Corresponding author.

Email addresses: safkhani@srttu.edu (M. Safkhani), nbagheri@srttu.edu (N. Bagheri)

ISSN: 2008-2045

$\mathcal{R}_i$:	RFID reader i
$\mathcal{T}_j$:	RFID tag j
DB:	The back-end database
EPC_s:	A 16-bit Electronic Product Code.
$DATA$:	The corresponding information for $\mathcal{T}_j$ kept in DB.
K_i:	The authentication key stored in the tag.
P_i:	The access key stored in the tag.
C_i:	The index of the record of the i^{th} $\mathcal{T}_j$'s information in DB.
K_{old} and K_{new}:	The old and new authentication key of $\mathcal{T}_j$ stored in DB, respectively.
P_{old} and P_{new}:	The old and new access key stored in DB, respectively.
C_{old} and C_{new}:	Respectively the old and new DB index for the i^{th} tag.
$B \longleftarrow A$:	Assign the value of A to B.
N_T and N_3:	The random numbers that generated by the tag.
$\oplus$:	Exclusive-or operation.
RID:	The reader identification number.
$H(.)$:	Hash function.
$HMAC$:	Hash-based Message Authentication Code.
RID_i:	The identification value of an anonymous reader.
T_t:	The identification value (ID) of an anonymous tag T_i.
$A\|\|B$:	Concatenation of strings A and B.

Table 1. Notation

the tag, *i. e.*, K_0, P_0, C_0, and the corresponding record in the back-end database $K_{old} = K_{new} = K_0, P_{old} = P_{new} = P_0, C_{old} = C_{new} = 0$.

Authentication Phase: The authentication phase of the improved Yoon's protocol at its $(i+1)^{th}$ run is as follows:

(1) The reader generates a random number N_R and sends it to the tag.

(2) The tag receives N_R, generates random numbers N_T and N_3, computes M_1, D, C_i, E as below and sends tuple (M_1, D, C_i, E) to the reader:
$M_1 \leftarrow PRNG(EPC_s \oplus N_R \oplus N_T) \oplus K_i$
$D \leftarrow N_T \oplus K_i$
$C_i \leftarrow C_i \oplus N_3$
$E \leftarrow PRNG(N_T) \oplus PRNG(C_i \oplus K_i)$

(3) Once the reader receipts the message, it computes $V = H(RID \oplus N_R)$ and forwards tuple (M_1, D, C_i, E, N_R, V) to the back-end database DB.

(4) DB receives the tuple (M_1, D, C_i, E, N_R, V) and proceeds as follows:
- It verifies whether $H(RID \oplus N_R) \stackrel{?}{=} V$ to authenticate the reader.
- If the reader has been authenticated, for any entry in database it computes $I_X = M_1 \oplus K_X$, for $X \in \{old, new\}$, and checks whether $I_X = PRNG(EPC_s \oplus N_R \oplus D \oplus K_X)$, to determine whether $X = old$ or new. If it finds related record, it verifies whether $E \stackrel{?}{=} PRNG(D \oplus K_X) \oplus PRNG(C_X \oplus K_X)$ to authenticate the tag. If the tag has been authenticated, DB computes the following values and sends $(M_2, Info, MAC)$ to the reader:
$N_T \leftarrow D \oplus K_X$
$M_2 \leftarrow PRNG(EPC_s \oplus N_T) \oplus P_X$
$Info \leftarrow DATA \oplus RID$
$MAC \leftarrow H(DATA \oplus N_R)$
$N_3 \leftarrow C_i \oplus C_X$
- If $X = new$, DB updates its values as follows:
$K_{old} \leftarrow K_{new} \leftarrow PRNG(K_{new} \oplus N_3)$,
$C_{old} \leftarrow C_{new} \leftarrow PRNG(N_T \oplus N_R \oplus P_{new})$,
$P_{old} \leftarrow P_{new} \leftarrow PRNG(P_{new})$.
- Else, DB updates its values as follows:
$K_{new} \leftarrow PRNG(K_{new} \oplus N_3)$,
$C_{new} \leftarrow PRNG(N_T \oplus N_R \oplus P_{new})$.

(5) Once the reader receipts the message, it verifies whether $H(DATA \oplus N_R) \stackrel{?}{=} MAC$. If "Yes" forwards M_2 to the tag; otherwise the protocol aborts.

(6) Once the tag receipts the message, it verifies

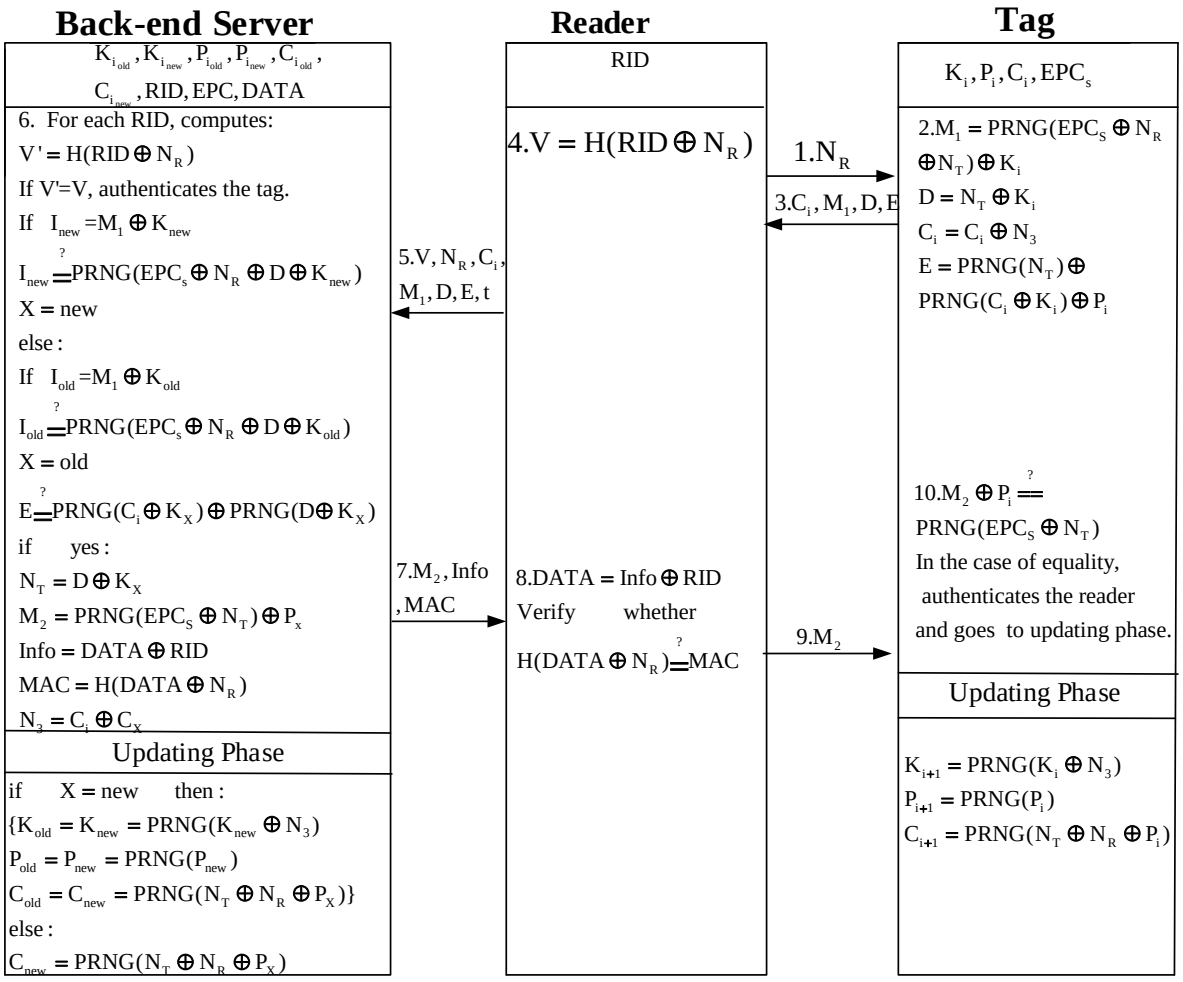

Figure 1. The improved Yoon's protocol[2]

whether $PRNG(EPC_s \oplus N_T) \stackrel{?}{=} M_2 \oplus P_i$ to authenticate DB and update its parameters as follows:

$K_{i+1} \longleftarrow PRNG(K_i \oplus N_3)$,
$C_{i+1} \longleftarrow PRNG(N_T \oplus N_R \oplus P_i)$,
$P_{i+1} \longleftarrow PRNG(P_i)$.

Remark 1. In Step 4, the designers only update C_{new}. However, we consider it as a typo because K_{new} should also be updated; otherwise it will be easy to desynchronize the tag and the reader by just blocking the last message sent from the reader to the tag. In that case, DB has updated the tag's record based on N_3, while the tag has not. In the next session, assuming that the tag generates N_3', DB runs Step 4 but does not update the value of K_{new} while the tag uses N_3' to update its key, which desynchronize the tag and DB with a high probability. Hence, we assumed that in Step 4 of the protocol, DB also updates K_{new}. However, this assumption does not simplify the presented analysis in the next section.

2.2 Secret Disclosure Attack on the Protocol

Designers of the improved protocol based their protocol on the Yoon's protocol which uses a 16-bit PRNG. In addition, they have presented an attack with the complexity of 2^{16} offline computation against the Yoon's protocol. In this section, we show that it is possible to extract all secret parameters of the improved version of the Yoon's protocol with almost the same complexity. To disclose the secrets of the tag, the adversary does as follows:

Learning Phase

- Step 1: Given the target tag T_j, the adversary eavesdrops a session of the protocol between the tag and the reader and stores the following values, but it blocks the reader's feedback to the tag(hence the tag will not update its parameter in this stage):

$M_1 = PRNG(EPC_s \oplus N_R \oplus N_T) \oplus K_i$, $D =$

$N_T \oplus K_i$, $C_i = C_i \oplus N_3$, $E = PRNG(N_T) \oplus PRNG(C_i \oplus K_i)$ and $M_2 = PRNG(EPC_s \oplus N_T) \oplus P_X$

- Step 2: The adversary impersonates the reader and sends N_R to the tag and stores its responses which are as follows: $M_1' = PRNG(EPC_s \oplus N_R \oplus N_T') \oplus K_i$, $D' = N_T' \oplus K_i$, $C_i = C_i \oplus N_3'$ and $E' = PRNG(N_T') \oplus PRNG(C_i \oplus K_i)$

Secret Disclosure Phase

- Step 1: With the complexity of 2^{16}, the adversary finds a value for $\mathcal{X}$ that satisfies $PRNG(\mathcal{X}) \oplus PRNG(\mathcal{X} \oplus \Delta) = M_1 \oplus M_1'$, where $\Delta = D \oplus D'$.

- Step 2: Given $\mathcal{X}$ form **Step 1**, the adversary extracts $K_i = M_1 \oplus PRNG(\mathcal{X})$.

- Step 3: Given K_i form **Step 2**, the adversary extracts $N_T = D \oplus K_i$ and $EPC_s = \mathcal{X} \oplus N_T \oplus N_R$.

- Step 4: Given N_T and EPC_s form **Step 3**, the adversary extracts $P_i = M_2 \oplus PRNG(EPC_s \oplus N_T) = \mathcal{X} \oplus N_T \oplus N_R$.

- Step 5: The adversary can use E and E' to ensure the correctness of the extracted values.

Given the above attack, the adversary knows all sufficient information to impersonate the tag to the reader or the reader to the tag, hence it can be also considered as a tag/reader impersonation attack. In addition, impersonating the reader, the adversary will desynchronize both tag and the reader and it is enough to trace the target tag at any time, given that it will not update its secret parameters through DB any more. Finally, given the value of P_i from **Step 4** and its updating rule which is $P_{i+1} = PRNG(P_i)$, even without desynchronizing the tag and the reader any adversary who has an estimation of the number of the successful communications of the tag and the reader can trace the tag which compromises the tag holder's privacy.

3 On the Security of the Improved Jung *et al.* Protocol

3.1 Protocols Description

As depicted in Figure 2, in this section, using the notation depicted in Table 1, we describe the improved version of the Jung *et al.* protocol [1, 2]. More precisely, the protocol can be described as follows:

PROTOCOL 2: This protocol is composed of five steps:

- Step 1: The RFID reader ($\mathcal{R}_i$) sends $Hello(ID_r)$ to the RFID tag $\mathcal{T}_j$.

- Step 2: The RFID tag $\mathcal{T}_j$ generates a random number N_T and calculates $\alpha = H(ID_t \oplus N_T)$, $\beta = K_i \oplus N_T \oplus C_i$ and $\gamma = HMAC_{ID_t}(T_t, ID_r, N_T)$ and transmits tuple $(\alpha \| \beta \| \gamma \| T_t \| ID_r)$ to the reader $\mathcal{R}_i$.

- Step 3: The RFID reader ($\mathcal{R}_i$) transmits the received tuple to the database (DB).

- Step 4: DB receives the tuple sent by $\mathcal{R}_i$, extracts $I_X = K_X \oplus C_X \oplus \beta$ for each tuple (ID_t, K_X, C_X), where $X \in \{old, new\}$, and verifies whether $H(ID_t \oplus I_X) \stackrel{?}{=} \alpha$. Then it checks whether $\gamma \stackrel{?}{=} HMAC_{ID_t}(T_t, ID_r, I_X)$ to authenticate the tag. If the tag has been authenticated, DB calculates $\Psi = HMAC_{ID_t}(T_t + 1, ID_r, I_X)$ and sends it through the reader to $\mathcal{T}_j$. DB also updates the tag's records as $K_{old} \leftarrow K_{new} \leftarrow H(K_X \oplus N_T)$ and $C_{old} \leftarrow C_{new} \leftarrow H(N_T \oplus ID_r)$.

- Step 5: To authenticate DB, the tag verifies the received value from DB by checking whether $\Psi \stackrel{?}{=} HMAC_{ID_t}(T_t + 1, ID_r, I_X)$. If DB has been authenticated successfully, the tag updates its parameters as $K_{i+1} \leftarrow H(K_i \oplus N_T)$ and $C_{i+1} \leftarrow H(N_T \oplus ID_r)$.

3.2 Desynchronization Attack on the Protocol

Designers of the improved protocol claimed that [2, p.146] since DB keeps a record of both new and old secret parameters of the tag it is not possible to desynchronize $\mathcal{T}$ and DB. However, in this section we present an efficient attack to desynchronize the tag which contradicts the designers' claim. To desynchronize the tag, the adversary does as follows:

Learning Phase

- Step 1: Assuming that the target tag participated in an authentication process, when $\mathcal{T}_j$ transmits tuple $(\alpha \| \beta \| \gamma \| T_t \| ID_r)$ to the reader $\mathcal{R}_i$, the adversary intercepts it but keeps a record of it.

- Step 2: In the next attempt of the reader to authenticate $\mathcal{T}_j$, the tag generates a new random value N_T' and calculates $\alpha' = H(ID_t \oplus N_T')$, $\beta' = K_i \oplus N_T' \oplus C_i$ and $\gamma' = HMAC_{ID_t}(T_t, ID_r, I_X)$ and transmits tuple $(\alpha' \| \beta' \| \gamma' \| T_t \| ID_r)$ to the reader $\mathcal{R}_i$.

- Step 3: $\mathcal{R}_i$ transmits the received tuple to DB.

- Step 4: DB receives the tuple sent by $\mathcal{R}_i$, authenticates the tag, calculates $\Psi = HMAC_{ID_t}(T_t + 1, ID_r, I_X)$ and sends it through the reader to $\mathcal{T}_j$. DB also updates the tag's records as $K_{old} \leftarrow K_{new} \leftarrow H(K_X \oplus N_T')$ and $C_{old} \leftarrow C_{new} \leftarrow H(N_T' \oplus ID_r)$

- Step 5: The tag also authenticates DB successfully and updates its parameters as $K_{i+1} \leftarrow H(K_i \oplus N_T')$ and $C_{i+1} \leftarrow H(N_T' \oplus ID_r)$.

Desynchronization Phase

- Step 1: When the reader tries to communicate with a tag $\mathcal{T}_r$, the adversary impersonates that tag and sends the stored tuple from **Step 1** of the learning phase of this attack to the reader, i.e., $(\alpha \| \beta \| \gamma \| T_t \| ID_r)$, where $\alpha = H(ID_t \oplus N_T)$, $\beta = K_i \oplus N_T \oplus C_i$ and $\gamma = HMAC_{ID_t}(T_t, ID_r, N_T)$. **- Step 3:** $\mathcal{R}_i$ transmits the received tuple to the DB.

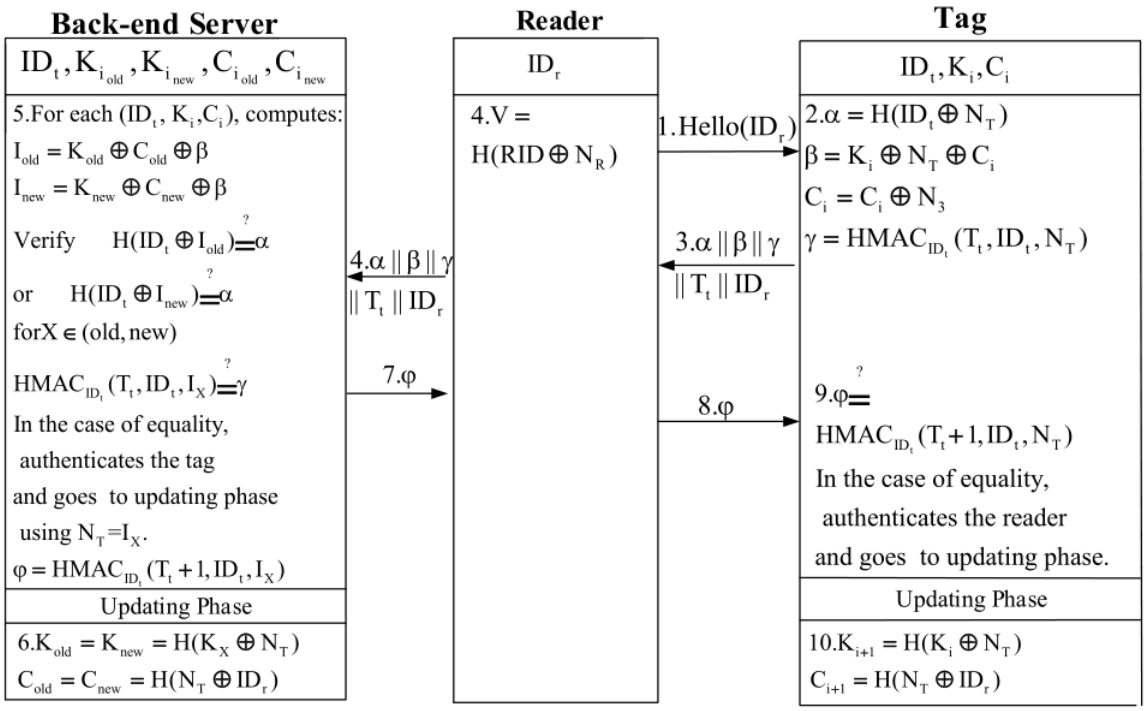

Figure 2. The improved Jung *et al.* protocol[2]

- Step 4: DB receives the tuple sent by $\mathcal{R}_i$, based on the old secret parameters of $\mathcal{T}_j$, authenticates $\mathcal{T}_j$ as the tag, calculates $\Psi'=HMAC_{ID_t}(T_t+1, ID_r, N_T)$ and sends it through the reader to the tag. DB also updates the $\mathcal{T}_j$'s records as $K_{old} \leftarrow K_{new} \leftarrow H(K_X \oplus N_T)$ and $C_{old} \leftarrow C_{new} \leftarrow H(N_T \oplus ID_r)$

At the end of the given procedure, the tag's records of secret parameters are $K_{i+1} = H(K_i \oplus N'_T)$ and $C_{i+1} = H(N'_T \oplus ID_r)$ which does not match any record of the server with the probability of $(1-2^{-2n})^2$, where n is the length of each parameter. Hence, the tag and the database have been desynchronized and they will not authenticate each other henceforth. The success probability of the given attack is $(1-2^{-2n})^2$ while the complexity is just three runs of the protocol. It must be noted, the adversary can impersonate T_j at any time using the stored record $(\alpha\|\beta\|\gamma\|T_t\|ID_r)$, because the server matches it with the *old* parameters of $\mathcal{T}_j$. Hence, the attack can also be considered as a tag impersonation attack.

Remark 2. Although, in the protocol a time stamp T_t is used, however, it does not verify by any party of the protocol. Hence, it cannot prevent the given attack.

4 Recommendations

Our attacks in this letter on the improved version of the Yoon's protocol employs the fact that a 16-bit PRNG can be easily inverted and it may not be feasible to design a secure protocol just using several calls to 16-bit PRNGs. This fact has already been used for security analysis of some other EPC C-1 G-2 compliant protocols, *e.g.,* see [8–10]. Hence, we suggest to use lightweight block ciphers, *e.g.,* SIMON [11], or lightweight PRNGs with longer output, *e.g.,* [12], to improve the security of EPC C-1 G-2 compliant protocols.

The second attack that we have presented in this letter was on the improved version of the Jung *et al.* protocol [4]. The main observation was the fact that a party of protocol, *i.e.,* the reader, does not contribute to the randomness of the messages. This weakness has already been used for example to cryptanalysis of RAPP-protocol [13] also, see [14, 15]. Hence, it should be vital for any protocol to be randomized by all protocol parties.

5 Conclusions

In this letter, we analyzed the security of two recent protocols published in [1, 2] and showed their important security pitfalls.
The vulnerabilities of the analyzed protocols against such simple attacks show that the analyzed protocols were incorrectly designed. Hope our result helps the direction of designing secure protocols for constrain RFID tags and avoiding such flaws in future protocols.

Acknowledgment

This work was supported by Shahid Rajaee Teacher Training University under contract number 7502.

References

[1] Karim Baghery, Behzad Abdolmaleki, Bahareh Akhbari, and Mohammad Reza Aref. Privacy analysis and improvements of two recent rfid authentication protocol. In *International ISC Conference on Information Security and Cryptology (ISCISC), At Tehran, 2014*, pages 137–142, 2014.

[2] Karim Baghery, Behzad Abdolmaleki, Bahareh Akhbari, and Mohammad Reza Aref. Enhancing privacy of recent authentication schemes for low-cost RFID systems. *The ISC International Journal of Information Security*, 7(2):469–491, 2015.

[3] Eun-Jun Yoon. Improvement of the securing RFID systems conforming to EPC class 1 generation 2 standard. *Expert Syst. Appl.*, 39(1): 1589–1594, 2012.

[4] Seung Wook Jung and Souhwan Jung. HMAC-based RFID authentication protocol with minimal retrieval at server. In *Thes Fifth International Conference on Evolving Internet INTERNET 2013*, pages 52–55, 2013.

[5] 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.

[6] Amin Mohammadali, Zahra Ahmadian, and Mohammad Reza Aref. Analysis and improvement of the securing RFID systems conforming to EPC class 1 generation 2 standard. Cryptology ePrint Archive, Report 2013/404, 2013. http://eprint.iacr.org/2013/066.

[7] Masoumeh Safkhani, Nasour Bagheri, Somitra Kumar Sanadhya, and Majid Naderi. Cryptanalysis of improved yeh *et al.*'s authentication protocol: An EPC class-1 generation-2 standard compliant protocol. Cryptology ePrint Archive, Report 2013/404, 2013. http://eprint.iacr.org/2011/426.

[8] Masoumeh Safkhani, Nasour Bagheri, and Majid Naderi. Strengthening the security of EPC C-1 G-2 RFID standard. *Wireless Personal Communications*, 72(2):1295–1308, 2013.

[9] Masoumeh Safkhani, Nasour Bagheri, and Majid Naderi. A note on the security of IS-RFID, an inpatient medication safety. *I. J. Medical Informatics*, 83(1):82–85, 2014.

[10] Mohammad Hassan Habibi, Mahdi R. Alaghband, and Mohammad Reza Aref. Attacks on a lightweight mutual authentication protocol under EPC C-1 G-2 standard. In Claudio Agostino Ardagna and Jianying Zhou, editors, *WISTP 2011*, volume 6633 of *Lecture Notes in Computer Science*, pages 254–263. Springer, 2011.

[11] Ray Beaulieu, Douglas Shors, Jason Smith, Stefan Treatman-Clark, Bryan Weeks, and Louis Wingers. The SIMON and SPECK Families of Lightweight Block Ciphers. Cryptology ePrint Archive, Report 2013/404, 2013. http://eprint.iacr.org/2013/404.

[12] Honorio Martin, Enrique San Millán, Luis Entrena, Julio César Hernández Castro, and Pedro Peris-Lopez. Akari-x: A pseudorandom number generator for secure lightweight systems. In *IOLTS*, pages 228–233. IEEE, 2011. 17th IEEE International On-Line Testing Symposium (IOLTS 2011), 13-15 July, 2011, Athens, Greece.

[13] Yun Tian, Gongliang Chen, and Jianhua Li. A new ultralightweight RFID authentication protocol with permutation. *IEEE Communications Letters*, 16(5):702–705, 2012.

[14] Zahra Ahmadian, Mahmoud Salmasizadeh, and Mohammad Reza Aref. Desynchronization attack on RAPP ultralightweight authentication protocol. *Inf. Process. Lett.*, 113(7):205–209, 2013.

[15] Nasour Bagheri, Masoumeh Safkhani, Pedro Peris-Lopez, and Juan E. Tapiador. Weaknesses in a new ultralightweight rfid authentication protocol with permutation - RAPP. *Security and Communication Networks*, 7(6):945–949, 2014.

Masoumeh Safkhani is an assistant professor at computer engineering department of Shahid Rajaee Teacher Training University (SRTTU). She is the author of more than 30 articles on cryptanalysis of security protocols and cryptography algorithms. Her current research interest includes RFID security, internet of things (IoT) security and searchable encryption. Homepage of the author is available at: http://www.srttu.edu/english-cv-dr-safkhani/.

Nasour Bagheri is an assistant professor at electrical engineering department, Shahid Rajaee Teacher Training University, Tehran, Iran. He is the author of more than 50 articles on information security and cryptology. Homepage of the author is available at: http://www.srttu.edu/english-cv-dr-bagheri/.