Analysis of an RFID Authentication Protocol in Accordance with EPC Standards

Behzad Abdolmaleki
Department of Electrical Engineering
Shahed University
Tehran, Iran
b.abdolmaleki.ir@ieee.org

Hamidreza Bakhshi
Department of Electrical Engineering
Shahed University
Tehran, Iran
bakhshi@shahed.ac.ir

Karim Baghery
Information Systems and Security Lab (ISSL)
Sharif University of Technology
Tehran, Iran
k.baghery.1988@ieee.org

Mohammad Reza Aref
ISSL Lab, Department of Electrical Engineering
Sharif University of Technology
Tehran, Iran
aref@sharif.edu

Received: April 8, 2014-Accepted: February 8, 2015

***Abstract*—In the past few years, the design of RFID authentication protocols in accordance with the EPC Class-1 Generation-2 (EPC C1 G2) standards, has been one of the most important challenges in the information security domain. Although RFID systems provide user-friendly services for end-users, they can make security and privacy concerns for them. In this paper we analyze the security of an RFID mutual authentication protocol which is based on EPC Class-1 Generation-2 standard and proposed in 2013. The designers of protocol claimed that their protocol is secure against different security attacks and provides user privacy. In this paper, we show that unlike their claims, their protocol is not secure against most of the security attacks such as replay attack, the tag's ID exposure, and the spoofing attacks. As a result, their protocol cannot provide security of RFID users in different authentication applications. Finally, in order to prevent the aforementioned attacks and overcome all the existing weaknesses, we apply a modification in the updating procedure of the protocol and propose a strengthened version of it.**

Keywords-Security and Privacy;RFID Authentication protocols; EPC Class-1 Generation-2 standards.

I. INTRODUCTION

Radio Frequency Identification (RFID) technology is increasingly becoming part of our life. This technology is essential underlying technology found in almost every authentication applications such as access control systems, e-passport, public transportation passes, anti-theft cars and etc. [1]-[2]. Furthermore, RFID is a key enabler of the future Internet of Things (IoT) and it has a great economical potential.

RFID technology allows automatic identification of objects with the help of a low cost small electronic chip, called "tag" or "smart tag". RFID tags are "smarter" than the widely known barcodes, which makes RFID easier to use and more efficient than barcodes. The data stored on this "smart tag" can be read by wireless devices, called RFID readers. Generally, RFID systems are composed of three main parts, that third part called back-end server. All information and secret values of all tags are stored in the back-end server. The reader is located among the tag and the back-end server and exchanges data

between them. According to the power of tags, they classified to passive tags, semi-passive tags and active tags. Passive tags do not have supplies power for their computational, and electrical field that generated by the reader supplies their needed power. Tags are called semi-passive if they have battery for their internal circuitry runs. Note that semi-passive tags do not use their power for communication and the reader provides their communications power. In the last group, all needed energy for both internal circuitry run and communication supply by battery [3]-[4].

In the last few years different RFID authentication protocols in accordance with EPC C1 G2 have been proposed [5]-[9]. In 2007, *Chien* and *Chen* [5] proposed an improved authentication protocols for RFID EPC C1 G2 tags. In 2010, *Yeh et al.* [6] analyzed the security and the privacy of *Chien* and *Chen*'s protocol and proposed a strengthened version of their protocol that is based on EPC C1 G2 standard. In 2011, *Habibi et al.* investigated *Yeh et al.*'s protocol against different security and privacy attacks [7]. *Habibi et al.* showed that *Yeh et al.*'s protocol suffers from Reveal secret parameters, impersonation attacks, DoS attack and also it does not provide user privacy [7]. Another one of the newest protocol in this family is *Pang et al.*'s protocol that proposed recently in [8].

In this paper, we will study the security of *Pang et al.*'s protocol and it will be shown that unlike their claims, their protocol have some vulnerabilities and is not secure against most of attacks such as the replay attack, the tag's ID exposure, the spoofing attack.

The rest of this paper is organized as follows: section II, describes some RFID protocol threats. These threats will be used at subsequent sections for security analyzes. Review of *Pang et al.*'s protocol provided in section III. In section IV, vulnerabilities of *Pang et al.*'s protocol described. Finally, conclusions are drawn in Section V.

II. RFID Protocol Threats

In RFID systems and their applications, security problem is one of the most important challenges. In this section, we briefly investigate some of the attacks and threats that RFID systems are vulnerable to them. Some of these attacks and threats as following

A. Information Leakage

In RFID systems, when the tag and the reader want to send message to each other, if the channel between the tag and the reader not be insecure, this communicate can be eavesdrop by adversary. Therefore, this is more important that the designed authentication protocol be secure against eavesdropping. Namely, the sent data between the tag and the reader should not leak any information to nobody [10], [11] .

B. Replay attack

Replay attack occurs when an attacker tries to obtain transmitted message or messages between the tag and the reader using eavesdropping. Consequently, after obtaining the messages by attacker, attacker replays it for the tag or the reader. In other word, the attacker uses obtained messages for impersonate a legitimate reader or a legitimate tag [12].

C. Denial-of-Service attack

Message blocking attack or Denial-of-Service (DoS) attack is one of the different attacks on RFID systems. In this case, the attacker tries to block sent messages between the tag and the reader. DoS attack causes de-synchronization between the tag, the reader and the back-end server and de-synchronization makes the back-end server and the tag could not recognize each other in the next steps [13]-[14]

D. Tag impersonation attack

Tag impersonation attack occurs when an attacker is between a reader and tags, and the attacker tries to impersonate a reader to receive response from tag. The attacker does this work by sending an impersonated query to the tag. Then, an attacker sends the obtained response to the reader to impersonate the tag [10], [15].

III. Review of Pang et al.'s Protocol

In 2013, *Pang et al.* [8] proposed a mutual authentication protocol for RFID systems which is conforming to the EPC C1 G2 standards. In this section, we aim to review their protocol which will be cryptanalyzed in the next section. In review procedure, in order to simply and prevent confusing, the notations of original paper are used that are reported in Table I.

TABLE I. The Notations

Notation	Description
$\mathbf{EPC}_s$	A 96-bit EPC code that build by XORing six 16-blocks of the EPC code.
$\mathbf{K}_i$	The authentication key stored in the tag for database to authenticate the tag at the $(i+1)th$ authentication phase
$\mathbf{P}_i$	The access key stored in the tag for the tag to authenticate the database at the $(i+1)th$ authentication phase
$\mathbf{C}_i$	The database index stored in the tag to find the corresponding record of the tag in the database.
RID	The reader identification number
$\mathbf{K}_{old}$	The old authentication key stored in the database
$\mathbf{K}_{new}$	The new authentication key stored in the database
$\mathbf{C}_{old}$	The old database index stored in the database
$\mathbf{C}_{new}$	The new database index stored in the database
$\mathbf{D}_i$	The detailed information of the tag stored in the database
$(.)'$	For second run of protocol
$\mathbf{H}(.)$	Hash function
$\mathcal{A}$	An attacker
R	The legitimate reader
T	The legitimate Tag
$\oplus$	Bitwise XOR
$\|$	Concatenation operation
$\mathbf{A} \oplus \mathbf{B}$	Message A is XORed with message B
$\mathbf{A} \rightarrow \mathbf{B}$	A forwards a message to B

In *Pang et al.*'s protocol, the reader and the back-end server exchange data over a secure channel but the channel between the tag and the reader is not secure. *Pang et al.*'s protocol consists of two phases that can be described as follows (Shown in Fig. 1)

E. Initialization phase

In this phase, the values of $[K_{old}, C_{old}, K_{new}, C_{new}, EPC_s, D_i]$ that preloaded in the back-end server, set to initial values of K_0 and C_0 that generated randomly by

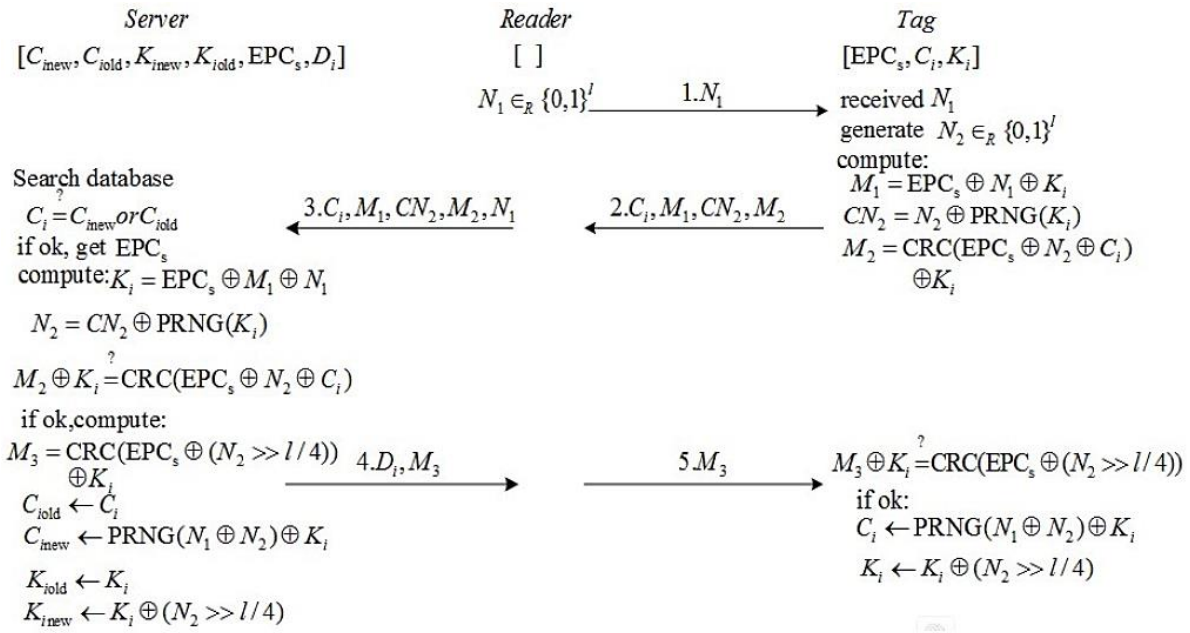


Fig. 1. Pang et al.'s protocol [8].

the manufacturer, $K_{old} = K_{new} = K_0$, $C_{old} = C_{new} = C_0$. Also, the values of $[K_i, C_i, EPC_s]$ that preloaded in the tag, sets to K_0 and C_0 that stored in the back-end server, $K_i = K_0$ and $C_i = C_0$.

F. Authentication phase

In this phase, the authentication will be done in five steps. The stages can be expressed as follows,

1) ***Reader→Tag:*** The reader generates a random number N_1, and sends it to the tag.

2) ***Tag→Reader:*** The tag generates a random number N_2, and computes $M_1 = EPC_S \oplus N_1 \oplus K_i$, $CN_2 = N_2 \oplus PRNG(K_i)$, and $M_2 = CRC(EPC_S \oplus N_2 \oplus C_i) \oplus K_i$ and forward them to the reader.

3) ***Reader → Back-end server:*** The reader receives the transmitted messeges from the tag and forwards $(C_i, M_1, CN_2, M_2, N_1)$ to the back-end server. After receiving messages from the reader, the back-end server performs the following steps,

a) Using the received C_i, the back-end server retrieves the database for matching C_i with C_{old} or C_{new} and picks up EPC_S of the original tag. Then, the back-end server computes K_i by $K_i = EPC_S \oplus N_1 \oplus M_1$. If $K_i = K_{old}$, or K_{new}, the back-end server obtains $N_2 = CN_2 \oplus PRING(K_i)$ and checks whether $M_2 \oplus K_i = CRC(EPC_s \oplus N_2 \oplus C_i)$ or not. This process will continue until a matched tag be founded. Otherwise, the reader receives error message from the back-end server and the protocol aborts.

4) ***Back-end server → Reader:*** This phase can be summarized as follows,

a) After successful authentication, the back-end server computes $M_3 = CRC(EPC_S \oplus (N_2 \gg l/4)) \oplus K_i$, and forwards (D_i, M_3) to the reader.

b) The back-end server updates the secret values as follows,

$$C_{iold} \leftarrow C_i$$
$$C_{inew} \leftarrow PENG(N_1 \oplus N_2) \oplus K_i$$
$$K_{iold} \leftarrow K_i$$
$$K_{inew} \leftarrow K_i \oplus (N_2 \gg l/4).$$

5) ***Reader→Tag:*** The reader receives (D_i, M_3) and forwards M_3 to the tag. Then, the tag computes $CRC(EPC_s \oplus (N_2 \gg l/4)) \oplus K_i$ and checks that $M_3 \oplus K_i = CRC(EPC_s \oplus (N_2 \gg l/4))$ or not.

If they were equal, the tag authenticates the back-end server successfully and updates as following

$$C_i \leftarrow PENG(N_1 \oplus N_2) \oplus K_i$$
$$K_i \leftarrow K_i \oplus (N_2 \gg l/4)$$

Otherwise, the tag stops the session and the protocol aborts.

II. Attacks and Improvements on Pang et al.'s Protocol

In [8], *Pang et al.* claimed that their protocol provide security of RFID users. In this section, the security of *Pang et al.*'s protocol is investigated and it is shown that their protocol have some weaknesses and suffers from replay, DoS, tag impersonation and reader impersonation attacks. Finally, in order to remove these weaknesses and enhancing the security of *pang et al.*'s protocol, the updating of their protocol is modified.

A. Reveal EPC_S

In *Pang et al.*'s protocol, it is referred that EPC_S is constructed from XORing six 16-bit blocks of EPC code, thus the length of EPC_S is 16-bit. Since in authentication phase of protocol, $M_1 = EPC_S \oplus N_1 \oplus K_i$, consequently it can be concluded that the length of N_1, K_i and EPC_S are the same. In *Pang et al.*'s protocol, short length of EPC_S and being fix in all rounds, is one of the weaknesses of their protocol that can be used to get EPC_S. In this way, the attacker can eavesdrop two sessions of protocol, then by some calculations, it can

obtain EPC_S. This attack consists of three stages as follows,

Stage 1) The attacker eavesdrops one successful session of protocol and saves the exchanged messages between the reader, the target tag and the back-end server, including $(C_i, M_1, CN_2, M_2, N_1, M_3)$.

Stage 2) The attacker plays the role of the reader and sends N_1 to the target tag and receives $(C_{i+1}, M_1', CN_2', M_2')$. Then it performs following operations,

$$M_1 = EPC_S \oplus N_1 \oplus K_i$$

$$M_1' = EPC_S \oplus N_1 \oplus K_{i+1}$$

where $K_{i+1} = K_i \oplus (N_2 \gg l/4)$, then

$$M_1 \oplus M_1' = EPC_S \oplus N_1 \oplus K_i \oplus EPC_S \oplus N_1 \oplus K_{i+1}$$
$$= K_i \oplus K_{i+1}$$
$$= K_i \oplus K_i \oplus (N_2 \gg l/4)$$
$$= (N_2 \gg l/4)$$

Stage 3) The attacker omits K_i by XORing M_1, M_3 and N_1, then obtains 16-bit β string.

$$\beta = M_1 \oplus M_3 \oplus N_1$$
$$= EPC_S \oplus N_1 \oplus K_i \oplus CRC(EPC_s \oplus (N_2 \gg l/4)) \oplus K_i \oplus N_1$$
$$= EPC_S \oplus CRC(EPC_s \oplus (N_2 \gg l/4))$$

Stage 4) Since length of EPC_s is 16, thus $EPC_s \epsilon\, U$, that $U = \{u_1, u_2, \dots, u_{2^{16}}\}$. Now, the attacker uses β and $(N_2 \gg l/4)$ that obtained previous stages, and obtains EPC_s using following algorithm,

Algorithm1

$For\ 1 \le i \le 2^{16}$

$Choose\ u_i \in U$

$\alpha = CRC\big(u_i \oplus (N_2 \gg l/4\,)\big) \oplus u_i$

$if\ \ \alpha = \beta\ \ then$

$return\ u_i\ as\ EPC_s$

End

Then, the attacker finds the value of correct EPC_s with maximum 2^{16} run of algorithm1.

In the rest of paper, using the value of EPC_s some practical and important attacks are provided.

B. Tag impersonation attack

In this attack, the attacker tries to impersonate a tag to receive response from the reader. In the following tag impersonation attack has been done on the *Pang et al.*'s protocol. This attack consists of two phases as follows,

Learning phase: In this phase, the attacker is eavesdropper. After one successful run, he/she saved the exchanges data between the reader and the target tag including $(C_i, M_1, CN_2, M_2, N_1)$.

Attack phase: The attacker plays role of the reader and sends N_1 to the target tag and receives $(C_{i+1}, M_1', CN_2', M_2')$, and using EPC_S that obtained in the last attack, performs following operations,

1) Calculates K_i and K_{i+1} as follows,

$$K_i = M_1 \oplus N_1 \oplus EPC_s$$
$$K_{i+1} = K_i \oplus (N_2 \gg l/4\,)$$

2) The attacker plays role of the tag and starts a new session with the reader and receives N_1' from him/her. Then, he/she calculates the following massages and sends them to the reader.

$$M_1' = EPC_s \oplus N_1' \oplus K_{i+1}$$
$$CN_2' = N_2' \oplus PRNG(K_{i+1})$$
$$M_2' = CRC(EPC_s \oplus N_2' \oplus C_{i+1}) \oplus K_{i+1}$$

3) The reader sends received massages to the back-end server. Since M_1' , CN_2' and M_2' calculated correctly, the back-end server admits the attacker and authenticate him/her.

C. Reader impersonation attack

In this subsection we will show that *Pang et al.*'s protocol is also vulnerable to reader impersonation attack. In this attack, the attacker tries to forge a legitimate reader. This attack can be performed as follows,

1) The attacker eavesdrops exchanged data between the target tag and the reader, and calculates EPC_s and K_{i+1} like as previous sections.
2) The attacker starts a new session with the target tag and sends N_1' to him/her. Then, he/she receives $(C_{i+1}, M_1', CN_2', M_2')$ from the tag.
3) Using K_{i+1} and CN_2', the attacker extracts N_2' and computes M_3' as follows and forwards M_3' to the target tag.

$$N_2' = CN_2' \oplus PRNG(K_{i+1})$$
$$M_3' = CRC(EPC_s \oplus (N_2' \gg l/4\,)) \oplus K_{i+1}$$

4) Since N_2' and M_3' calculated correctly, the target tag admits the attacker and authenticates him/her and updates its secret values.

D. DoS attack

At the end of the mentioned reader impersonation attack, the tag updates its secret values as follows,

$$C_i \leftarrow PRNG(N_1' \oplus N_2') \oplus K_i$$
$$K_i \leftarrow K_i \oplus (N_2' \gg l/4\,)$$

and the legitimate reader does not know these values, and the back-end server has updated as follows,

$$C_i \leftarrow PENG(N_1 \oplus N_2) \oplus K_i$$
$$K_i \leftarrow K_i \oplus (N_2 \gg l/4)$$

It can be seen that the stored secret values in the tag and the back-end server are different from each other and they are desynchronized. Hence, in the next session of protocol, the back-end server cannot authenticate the tag.

E. Remove existing weaknesses

In the previous sections, we showed that the updating of *Pang et al.*'s protocol has a weakness that makes it vulnerable to various security attacks. In order to remove these weaknesses, we change the updating of *Pang et al.*'s protocol. More precisely, we modify $K_i \leftarrow K_i \oplus (N_2 \gg l/4)$ as $K_i \leftarrow H(K_i \oplus (N_2 \gg l/4))$, where $H(.)$ is a hash function. It can be seen that with this change, the attacker cannot obtain the secret parameter and perform the mentioned attacks. As a result, the improved version of protocol can provide security and privacy of RFID end-users and is secure against various security and privacy attacks.

IV. Conclusion

In this paper, we investigated the security of an RFID mutual authentication protocol that is conforming to the EPC C1 G2 standard and has been proposed by *Pang et al.* in 2013. The authors analyzed their protocol against various security and privacy attacks and were claimed that the protocol is secure against all attacks and also provide user privacy. It is shown that still there are some flaws on their protocol and it cannot provide secure and confidential communications for RFID users. More precisely, it is shown that their protocol is not secure against secret parameter reveal, reader impersonation attack, tag impersonation and DoS attacks and an adversary can perform these attacks on this protocol. Then, in order to provide security and privacy of RFID users and omit all the mentioned weaknesses on *Pang et al.*'s protocol, we modified updating procedure of their protocol and proposed an improved version of it.

References

[1] C. H. Lim, and T. Kwon, "Strong and robust RFID authentication enabling perfect ownership transfer," *In Proceedings of ICICS '06, LNCS 4307*, pp. 1-20, 2006.

[2] L. Kulseng, Z. Yu, Y. Wei, and Y. Guan, , "Lightweight mutual authentication and ownership transfer for RFID systems," *IEEE INFOCOM*, p. 251–255, 2010.

[3] D. Heyden , "RFID Applications," Fibre2Fashion, 11 February 2014. [Online]. Available: http://www.fibre2fashion.com/industry-article/11/1023/rfid-applications1.asp.

[4] Z. Ahmadian, M. Salmasizadeh, and M. R. Aref, "Recursive linear and differential cryptanalysis of ultralightweight authentication protocols," *IEEE Transactions on Information Forensics and Security*,, vol. 8, no. 7, pp. 1140 - 1151, July 2013.

[5] H. Y. Chien, and C. H. Chen, "Mutual authentication protocol for RFID confirming to EPC Class 1 Generation 2 standards," *Computer Standards & Interfaces*, vol. 29, no. 2, pp. 254-259, 2007.

[6] T.C. Yeh, Y. J. Wang, T. C. Kuo, and S. S. Wang, "Securing RFID systems conforming to EPC Class-1 Generation-2 standard," *Expert Systems with Applications*, vol. 37, no. 12, pp. 7678-7683, 2010.

[7] M. H. Habibi, M. Gardeshi, and M. Alagheband, "Practical attacks on an RFID authentication protocol conforming to EPC C-1 G-2 standard," *Int. Journal of UbiComp (IJU)*, vol. 2, no. 1, pp. 1-13, 2011.

[8] L. Pang, L. He, Q. Pei and Y. Wang, "Secure and efficient mutual authentication protocol for RFID conforming to the EPC C-1 G-2 Standard," in *IEEE Wireless Comm. and Networking Conference*, 2013.

[9] S. M. Alavi, K. Baghery, and B. Abdolmaleki, "Security and privacy flaws in a recent authentication protocol for EPC C1 G2 RFID tags," *Advances in Computer Science : an Int. Journal*, vol. 3, no. 5, pp. 44-52, 2014.

[10] M. H. Habibi, and M. R. Aref, "Attacks on recent RFID authentication protocols," *Journal of Signal Processing Systems, Springer*, pp. 1-13, 2013.

[11] T. Van Deursen, and S. Radomirovic,, "Attacks on RFID protocol," Cryptology ePrint Archive, Report 2008/310, <http://eprint.iacr.org/>, 2008.

[12] M. Safkhani, P. Peris-Lopez, J. C. H. Castro, N. Bagheri, and M. Naderi, "Cryptanalysis of Cho et al.'s Protocol, A Hash-Based Mutual Authentication Protocol for RFID Systems.," *IACR Cryptology ePrint Archive, eprint.iacr.org/2011/331.pdf*, 2011.

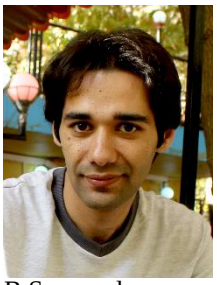
[13] D. Han, and D. Kwon, "Vulnerability of an RFID authentication protocol conforming to EPC Class-1Generation-2 Standards," *Computer Standards & Interfaces*, vol. 31, p. 648–652, 2009.

[14] Y.C.Lee, Y.C.Hsieh, P.S.You, and T.C.Chen, "An Improvement on RFID Authentication Protocol with Privacy Protection," in *Third International Conference on Convergence and Hybrid Information Technology*, , South Korea: Busan, 2008.

[15] M.H. Habibi, M. R. Alaghband, and M. R. Aref, "Attacks on a lightweight mutual authentication protocol under EPC C-1 G-2 standard," *Information Security Theory and practice, LNCS 6633, Springer-Verlag*, pp. 254-263, 2011.

Behzad Abdolmaleki received his B. Sc. degree in physics from university of Kurdistan, Sanandaj, Iran, in 2010,and his M.Sc. degree in Electrical Engineering - Communications Systems from Shahed University Tehran, Iran in 2014. He is working with the Information Systems and Security Lab., ISSL, Department of Electrical Engineering, Sharif University of Technology. Since 2013 he is member of IEEE. His research interests mainly include cryptography, information security, optimization on wireless networks and smart antennas.

Hamidreza Bakhshi was born in Tehran, Iran on April 25, 1971. He received the B.Sc. degree in electrical engineering from Tehran University, Iran in 1992,and his M.Sc. and Ph.D. degree in Electrical Engineering from Tarbiat Modarres University, Iran in 1995 and 2001, respectively. |Since 2010, he has been an Associate Professor of Electrical Engineering at Shahed University, Tehran, Iran. His research interests include wireless communications, multiuser detection, and smart antennas.



Karim Baghery is a research assistant at Information Systems and Security Laboratory (ISSL), Sharif University of Technology, Tehran, Iran. He received his M.Sc. degree in Electrical Engineering - Communications Systems from Shahed University Tehran, Iran in 2014, and the B.Sc. degree in Electrical Engineering-Telecommunication from IAU University, Urmia Branch, Iran, in 2010. During 2012 to 2014 he was working in the Information Theoretic Learning Systems Laboratory (ITLSL), department of electrical engineering, Shahed University, Tehran, Iran. He is Member of IEEE and Reviewer of Wireless Personal Communications journal. His research interests mainly include RFID security, lightweight cryptography, and optimization on wireless networks.

Mohammad Reza Aref received the B.S. degree in 1975 from University of Tehran, Iran, and the M.S. and Ph.D. degrees in 1976 and 1980, respectively, from Stanford University, Stanford, CA, USA, all in electrical engineering.

He returned to Iran in 1980 and was actively engaged in academic affairs. He was a faculty member at Isfahan University of Technology from 1982 to 1995. He has been a Professor of electrical engineering at Sharif University of Technology, Tehran, since 1995, and has published more than 230 technical papers in communications and information theory and cryptography in international journals and conferences proceedings. His current research interests include areas of communication theory, information theory, and cryptography.