ACSIJ Advances in Computer Science: an International Journal, Vol. 3, Issue 6, No.12 , November 2014
ISSN : 2322-5157
www.ACSIJ.org

ACSIJ
WWW.ACSIJ.ORG

Vulnerabilities and Improvements on HRAP+, a Hash-Based RFID Authentication Protocol

Seyed Mohammad Alavi[1], Behzad Abdolmaleki[2], and Karim Baghery[3]

[1] Imam Hossein Comprehensive University
Tehran, Iran
malavi@ihu.ac.ir

[2] Information Systems and Security Lab (ISSL), Sharif University of Technology
Tehran, Iran
b.abdolmaleki.ir@ieee.org

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

Abstract

In the last decade, Radio Frequency Identification (RFID) systems are employed in many authentications and identifications applications. In RFID systems, in order to provide secure authentication between RFID users, different authentication protocols proposed. In 2011, *Cho et al.* proposed a hash-based mutual RFID authentication protocol (HRAP). They claimed that HRAP protocol provides secure communication between RFID users and also it can provide users privacy. In that year, *Habibi et al.* investigated the security and privacy of HRAP protocol and showed that HRAP protocol has some weaknesses. Then, *Habibi et al.* proposed an improved version of HRAP protocol ($HRAP^+$) that eliminates all weaknesses of HRAP protocol. In this study, we cryptanalyze the $HRAP^+$ protocol and we show that there are some flaws in $HRAP^+$ protocol still. It is shown that, an attacker can perform tag impersonation, server impersonation, and replay attacks with success probability greater than $\frac{1}{4}$. Then, in order to omit all mentioned weaknesses, we propose an improved version of $HRAP^+$ protocol. Security analysis shows that the improved protocol can improve the performance of $HRAP^+$ protocol. In addition, we compare the security of the proposed protocol with some hash-based protocols that proposed recently.

Keywords: *RFID authentication protocols, $HRAP^+$ protocol, Security, Impersonation Attack.*

1. Introduction

RFID systems are increasingly becoming part of our daily life. In many of our daily routines, without realizing it, we use RFID technology that use radio waves for automatic identification applications [1]. RFID technology also is used in different objects for different applications. Mainly, RFID systems consist of three main parts including Tag, Reader and Back-end-server or Database (Shown in Fig. 1). The data included in RFID tags that often are identification numbers, can be collected by the wireless reader. Also the reader can perform some logic processors and change the content of RFID tags. The third part of RFID systems that contains all secret information of tags, is back-end server or database. The reader located between the tags and the back-end server and exchanges data between them. In each run of RFID system, the database performs some certification and authentication processes and provides access to the data [2]. In some applications, communication channels between the readers and the database is insecure [3]. But in some cases, communication channels between the readers and the database is secure [4].

Due to nature of wireless communication between tags and readers, these channels can be eavesdropped by an adversary. As a results, although these systems provide many useful services, they can dangerous for security and the privacy of end-users. In the last few years, in order to protect RFID users against different security and privacy attacks

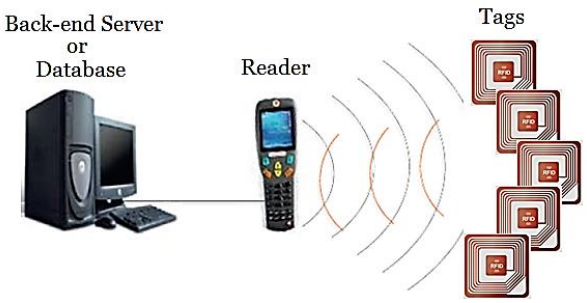

Fig. 1. A System model of RFID systems

and provide secure communication between them, different RFID authentication protocols have been proposed [5-10]. Although, all proposed protocols have been presented to provide security and privacy of end-users, in some cases it is shown that the proposed protocols have some weaknesses and suffer from various attacks. So in order to increase the security and privacy of the proposed protocols, lots of literature focused in cryptanalyze of RFID authentication protocols [5-14].

In 2011, in order to provide secure communication for RFID users, *Cho et al*. proposed a hash-based mutual RFID authentication protocol [5] which referred as HRAP protocol in this paper. In HRAP protocol, communication channel between the reader and the database is secure. *Cho et al.* analyzed the security and the privacy of HRAP protocol and claimed that their protocol can provide security and privacy of RFID users. In that year, *Habibi et al.* [6] cryptanalyzed HRAP protocol and showed that still the security and the privacy of HRAP protocol has some problems and is not secure against desynchronization attack, traceability and backward traceability attacks. Then, *Habibi et al.* applied some changes in the structure of tag message (M_1) and proposed an improved version of HRAP protocol (HRAP$^+$). *Habibi et al*. present some security and privacy analysis for HRAP$^+$ protocols and claimed that HRAP$^+$ protocol eliminates all weaknesses of HRAP protocol and is resistance against various attacks.

In this study, we cryptanalyze the HRAP$^+$ protocol and we show that although *Habibi et al*. tried to omit all weaknesses of HRAP protocol, still HRAP$^+$ protocol has some security problems and is vulnerable against tag impersonation, server/reader impersonation and replay attacks. In the HRAP$^+$ protocol, the structure of *RID* has a problem that makes it vulnerable against the mentioned attacks. In this paper, it is shown that how an attacker can use this weakness and impersonate the tag, the back-end server or the reader. Mentioned attacks are based on an assumption that is reasonable in many cases. Duo to this assumption, the success probability of mentioned attacks is greater than $\frac{1}{4}$ that are given in the section 3 with more details.

Furthermore, in order to increase the performance of HRAP$^+$ protocol and provide security and privacy of RFID users, we propose an improved version of HRAP$^+$ protocol. We analyze the security of the proposed protocol and we show that with our modifications all weaknesses of HRAP$^+$ protocol removed. Also we compare the security of proposed protocol with some hash-based protocols that proposed recently. Our comparisons, show that the proposed protocol has sufficient security and privacy and is resistance against all attacks.

The rest of paper is organized as follows: HRAP$^+$ protocol is introduced in section 2. In section 3, some attacks on HRAP$^+$ protocol presented. In section 4, we apply some changes in HRAP$^+$ protocol and propose an improved version of it. The security of proposed protocol is analyzed in section 5, and it is shown that all weaknesses of HRAP$^+$ protocol are omitted. Also in this section the security analysis of proposed protocol are compared with some similar protocols that are hash-based and proposed in recent years. Finally, we conclude this paper in section 6.

<table>
<tr><th colspan="2">Server / Reader $(ID_{old}, S_{old}, ID_{new}, S_{new})$</th><th>Tag (ID_k, S_j)</th></tr>
<tr><td rowspan="2">For each tuple of (ID_{old}, S_{old}) and (ID_{new}, S_{new})
Generates β and obtains R_t^i and RID_i
Verify $\alpha_i \stackrel{?}{=} h(ID_k^i \oplus R_r^i \oplus R_t^i \oplus RID_i)$
Calculates $\theta = h(\beta_i \parallel RID_i)$ and sends it to the tag and updates its secret values as follows:
If $ID = ID_{new}$
$S_{old} \leftarrow S_{new} \leftarrow h(S_{new} \parallel RID_i)$
$ID_{old} \leftarrow ID_{new} \leftarrow h(ID_{new} \parallel S_j)$
If $ID = ID_{old}$
$S_{new} \leftarrow h(S_{new} \parallel RID_i)$
$ID_{new} \leftarrow h(ID_{new} \parallel S_j)$</td><td>$R_r^i \stackrel{(1)}{\rightarrow}$</td><td rowspan="2">Generates R_t^i Randomly
$RID_i = (R_t^i - R_t^i mod S_j + 1)_{[0:47]} \parallel (R_t^i + S_j - R_t^i mod S_j)_{[48:95]}$
$\alpha_i = h(ID_k^i \oplus R_r^i \oplus R_t^i \oplus RID_i)$
$\beta_i = ID^i_{k\,[48:95]} \parallel S_{j\,[0:47]}$</td></tr>
<tr><td>$\stackrel{(2)}{\leftarrow} (\alpha_i, \beta_i \oplus R_t^i)$</td></tr>
<tr><td>$\theta \stackrel{(3)}{\rightarrow}$</td><td>Calculates $h(\beta_i \parallel RID_i)$
If $(\theta == h(\beta_i \parallel RID_i))$ server is legitimate and the tag updates:
$S_{j+1} \leftarrow h(S_j \parallel RID_i)$
$ID_{i+1} \leftarrow h(ID_i \parallel S_j)$</td></tr>
</table>

Fig. 2. The HRAP$^+$ protocol [6].

2. The HRAP+ Protocol

In [6], *Habibi et al.* proposed an improved version (HRAP+) of HRAP protocol that proposed by *Cho et al.* in [5]. HRAP+ protocol is similar to HRAP protocol and consists of three phases. The structure of HRAP+ protocol is illustrated in Fig. 2. The notation that are used in HRAP+ protocol are provided in Table 1.

Table 1. The Notations of HRAP+ Protocol

Notations	Description
S_j	The communications key shared by server and tag
ID_k	The group identification code of the kth tag
R_i	A random number
$h(.)$	Hash function
$\|$	Concatenation operation
$A \oplus B$	Message A is XORed with message B
$A \stackrel{?}{=} B$	Compare whether A is equal to B or not

3. Security Analysis of HRAP+ Protocol

In this section, the security of HRAP+ protocol is analyzed. It is shown that security of HRAP+ protocol has some weaknesses and dose not resist against tag impersonation, reader impersonation and replay attacks. All attacks performed with two assumptions and the success probability of attacks are greater than "$\frac{1}{4}$" that in the rest of paper will be explained with more details.
According to the authentication phase of HRAP+ protocol, the value of RID is defined as follows,

$$RID = \left(R_t - R_t \bmod S_j + 1\right)_{[0:47]} \| \left(R_t + S_j - R_t \bmod S_j\right)_{[48:95]} \quad (1)$$

now if $R_t < S_j$, the value of RID_i in (1) can be rewritten as follows,

$$RID = (R_t - R_t + 1)_{[0:47]} \| \left(R_t + S_j - R_t\right)_{[48:95]} = (1)_{[0:47]} \| \left(S_j\right)_{[48:95]} \quad (2)$$

Note that, when $R_t < S_j$, $R_t \bmod S_j = R_t$.

3.1 Tag Impersonation Attack

This attack can be performed in two phases as follows,
Learning phase: In round i th of protocol, the attacker eavesdrops exchanged data between the tag and the server and obtains R_r^i, $R_t^i \oplus \beta$ and α.
Attack phase: In round $(i+1)$th of protocol, when the server send a request message R_r^{i+1}, the attacker impersonate the tag and responses with α and $R_t^i \oplus \beta \oplus R_r^i \oplus R_r^{i+1}$ to the server. Then, the server performs following operations,

- For each tuple of (ID_k, S_j), the server generates β and obtains $R_t^{i+1} = R_t^i \oplus R_r^i \oplus R_r^{i+1}$ and RID_{i+1}.
- Then the server uses the values ID_k^i, R_r^{i+1}, R_t^{i+1} and RID_{i+1} and checks that $\alpha \stackrel{?}{=} h\left(ID_k^i \oplus R_r^{i+1} \oplus R_t^{i+1} \oplus RID_{i+1}\right)$. According to mentioned assumptions $R_t^i < S_j$ and $R_t^{i+1} < S_j$, we can write $RID_{i+1} = (1)_{[0:47]} \| \left(S_j\right)_{[48:95]} = RID_i$.
- Since $RID_{i+1} = RID_i$, the server authenticates the attacker as a legitimate tag.

Proof:

$$h\left(ID_k^i \oplus R_r^{i+1} \oplus R_t^{i+1} \oplus RID_{i+1}\right) = h\left(ID_k^i \oplus R_r^{i+1} \oplus R_t^i \oplus R_r^i \oplus R_r^{i+1} \oplus RID_{i+1}\right)$$

$$= h\left(ID_k^i \oplus R_t^i \oplus R_r^i \oplus RID_i\right) = \alpha \quad (3)$$

Lemma 1: For two numbers λ and μ that are random numbers from set $\chi = \{0,1,\dots,2^n - 1\}$ and $\mu > 1$, the probability of inequality $\lambda < \mu$ is greater than $\frac{1}{2}$.
Proof: Provided in appendix.

Lemma 2: For three numbers λ, μ and κ that are random numbers from set $\chi = \{0,1,\dots,2^n - 1\}$ and $\mu > 1$, the probability of inequality $\lambda \oplus \kappa < \mu$ is greater than $\frac{1}{2}$.
Proof: Provided in appendix.

According to the *Lemma 1* and *Lemma 2*, the inequalities $R_t^i < S_j$ and $R_t^{i+1} < S_j$ hold with probability greater than $\frac{1}{2}$. Therefore, this attack will be successful with probability greater than $\frac{1}{4}$.

3.2 Server Impersonation and Reply Attacks

In this section, we aim to show that in HRAP+ protocol, an attacker can perform replay attack and impersonate the server. This attack can be summurized as follows,

- Firstly, the attacker eavesdrops first session of protocol and obtains $h(\beta_i \| RID_i)$. Also in this session, the attacker blocks third phase of protocol (transmit message from the server to the tag). As a result the tag dose not update its secret values.
- Now, the attacker acts as a legitimate server and sends a random number R_{Att} to the target tag.

- In response, the tag generate a random number R_t^{i+1} and calculates $R_t^{i+1} \oplus \beta_{i+1}$ and $\alpha_{i+1} = h(ID_k^i \oplus R_{Att} \oplus R_t^{i+1} \oplus RID_{i+1})$, then sends them to the attacker.
- Then, the attacker sends eavesdropped message $h(\beta_i \parallel RID_i)$ to the target tag.
- Since the tag dose not its secret values, $\beta_{i+1} = \beta_i = ID_{k_{[48:95]}} \parallel S_{j_{[0:47]}}$. Using assumptions $R_t^i < S_j$ and $R_t^{i+1} < S_j$, it can be result that $RID_{i+1} = (1)_{[0:47]} \parallel (S_j)_{[48:95]} = RID_i$. As a result $h(\beta_{i+1} \parallel RID_{i+1}) = h(\beta_i \parallel RID_i)$ and the tag authenticate the attacker as a legitimate server.

In this attack also, according to the *Lemma 1* and *Lemma 2*, the inequalities $R_t^i < S_j$ and $R_t^{i+1} < S_j$ hold with probability greater than $\frac{1}{2}$, as a result the attacker will impersonate the server with probability greater than $\frac{1}{4}$.

4. Improved Version of HRAP⁺ Protocol

In the last section we showed that due to structure of $RID_i = (R_t - R_t \bmod S_j + 1)_{[0:47]} \parallel (R_t + S_j - R_t \bmod S_j)_{[48:95]}$. an attacker could perform tag impersonation, reply attack, and server impersonation attack on HRAP⁺ protocol. In this section, in order to omit mentioned weaknesses of HRAP⁺ protocol, we propose an improved version of HRAP⁺ protocol (Shown in Fig. 3). In the improved protocol, we changed the structure of RID, indeed we protect RID via a one-way hash function. The improved protocol can be summarized in two phases as follows.

4.1 Initial Phase

In this phase, some secret values such as ID_k and S_j are stored in the specific tag. Also a one-way hash function is saved in all tags. In the server, for each specific tag, the values ID_{old}, ID_{new}, S_{old} and S_{new} are stored. Like as all tags, the server uses a one-way hash function in authentication procedures.

4.2 Authentication Phase

The authentication of proposed protocol is similar to HRAP⁺ protocol and consists of three phases. This phase can be expressed as follows.

1. Like as HRAP⁺ protocol, the server generate a random number R_r^i and sends it to the target tag.
2. Firstly, the tag generates random number R_t^i. Then the tag uses R_t^i and calculates messages RID_i, α_i and β_i as follows, and send α_i and $\beta_i \oplus R_t^i$ to the server.

$$RID_i = h(R_t^i \oplus S_j)$$

$$\alpha_i = h(ID_k^i \oplus R_r^i \oplus R_t^i \oplus RID_i)$$

$$\beta_i = h\left(ID_{k_{[48:95]}}^i \parallel S_{j_{[0:47]}}\right)$$

3. In order to authenticate the tag, the server performs following operations,
   - For each tuple of (ID_k, S_j), the server generates β and obtains R_t^i and RID_i.
   - Then the server uses the values ID_k^i, R_r^i, R_t^i and RID_i and checks that $\alpha \stackrel{?}{=} h(ID_k^i \oplus R_r^i \oplus R_t^i \oplus RID_i)$. If they were the same, the server computes $\theta = h(\beta_i \parallel RID_i)$ and sends it to the target tag.

Server / Reader $(ID_{old}, S_{old}, ID_{new}, S_{new})$		**Tag** (ID_k, S_j)
For each tuple of (ID_{old}, S_{old}) and (ID_{new}, S_{new}) generates β and obtains R_t^i and RID_i Verify $\alpha_i \stackrel{?}{=} h(ID_k^i \oplus R_r^i \oplus R_t^i \oplus RID_i)$ Calculates $\theta = h(\beta_i \parallel RID_i)$ and sends it to the tag and updates its secret values as follows: If $ID = ID_{new}$ $S_{old} \leftarrow S_{new} \leftarrow h(S_{new} \parallel RID_i)$ $ID_{old} \leftarrow ID_{new} \leftarrow h(ID_{new} \parallel S_j)$ If $ID = ID_{old}$ $S_{new} \leftarrow h(S_{new} \parallel RID_i)$ $ID_{new} \leftarrow h(ID_{new} \parallel S_j)$	$R_r^i \xrightarrow{(1)}$ $\xleftarrow{(2)} (\alpha_i, \beta_i \oplus R_t^i)$ $\theta \xrightarrow{(3)}$	Generates R_t^i Randomly $RID_i = h(R_t^i \oplus S_j)$ $\alpha_i = h(ID_k^i \oplus R_r^i \oplus R_t^i \oplus RID_i)$ $\beta_i = h\left(ID_{k_{[48:95]}}^i \parallel S_{j_{[0:47]}}\right)$ Calculates $h(\beta_i \parallel RID_i)$ If $(\theta == h(\beta_i \parallel RID_i))$ server is legitimate and the tag updates: $S_{j+1} \leftarrow h(S_j \parallel RID_i)$ $ID_{i+1} \leftarrow h(ID_i \parallel S_j)$

Fig. 3. Improved version of HRAP⁺ protocol.

- After that, the server updates its secret values similar to HRAP+, otherwise aborts the protocol.
- The tag calculates $h(\beta_i \| RID_i)$ and compares with received message from the server. If they were the same, the tag authenticate the server and updates its secret values similar to HRAP+ protocol.

5. Security Analysis of Proposed Protocol

In the last session we proposed an improved version of HRAP+ protocol that removes mentioned weaknesses. It this subsection, we aim to analyze the security and the privacy of proposed protocol against various attacks.

5.1 Tag and Server Impersonations Attacks

In section 3, we showed that the main weakness of HRAP+ protocol is the structure of $RID = \left(R_t - R_t \text{mod} S_j + 1\right)_{[0:47]} \| \left(R_t + S_j - R_t \text{mod} S_j\right)_{[48:95]}$, that makes HRAP+ vulnerable against impersonation attacks. In proposed protocol, we changed the structure of RID completely as follows,

$$RID_{new} = h\left(R_t^i \oplus S_j\right) \quad (4)$$

where $h(.)$ is a one-way hash function. As it can be seen, with this changes, since the values of R_t^i and S_j change in each run of protocol, and the attacker dose not access to them directly, so the attacker cannot perform impersonation attacks.

5.2 Replay Attack

In this attack, the attacker tries to perform impersonation attacks to access exchanged messages, modify, and even delete them. In the proposed protocol, we applied some changes in the structure of exchanged data between the tag and the reader, indeed we changed $\beta = ID_{k\,[48:95]}^i \| S_{j\,[0:47]}$ to $= h\left(ID_{k\,[48:95]}^i \| S_{j\,[0:47]}\right)$. Also, we changed the structure of secret value RID that provided in (4). It can be seen that with these changes, the attacker cannot perform replay attack. Note that, with new values of β and RID, if somehow the attacker obtains the random number R_t, he/she cannot extract secret keys S_j and ID_k.

Furthermore, the structure of the proposed protocol is similar to HRAP+ protocol, as a result the proposed protocol is secure against other attacks like as HRAP+ protocol. More analysis about other attacks provided in [6].
In order to more evaluation of the security and the privacy of the proposed protocol, in Table 2, the security and the privacy of proposed protocol compared with some hash-based protocols that proposed in the last few years. It can be seen, that with applied new changes in the proposed protocol, all weakness of HRAP+ protocol have been omitted.

Table 2. Security Analysis of Some Hash-based Protocols

Protocols / Attacks	*Wei et al.* [7]	HRAP [5]	HRAP+ [6]	Improved HRAP+
Tag Impers.	×	×	×	✓
Replay Attack	✓	✓	×	✓
Reader Impers.	×	×	×	✓
DoS Attack	×	×	✓	✓
Traceability	×	✓	✓	✓

✓: Secure ×: Insecure

6. Conclusions

In this paper, the security of HRAP+ that is an improved version of HRAP protocol, is analyzed. We showed that although the designer of HRAP+ tried to remove all weaknesses of HRAP protocol, still HRAP+ protocol has some security problems and is not resist against tag impersonation, server impersonation and replay attacks. Mentioned attacks were based on an assumption that in many cases is reasonable. Duo to this assumption, the success probability of mentioned attacks was greater than $\frac{1}{4}$. Furthermore, we presented an improved version of HRAP+ protocol that removed weaknesses of HRAP+ protocol. In order to more evaluation we analyzed the security of proposed protocol and also we compared the security analysis of the proposed protocol with some hash-based protocol that are in the same family and proposed recently.

Appendix

Proof of Lemma 1:

$$A \coloneqq \{(\lambda,\mu) | 0 \le \lambda \le 2^n, 2 \le \mu \le 2^n, and\ \lambda < \mu\}$$

$$= \bigcup_{\mu=2}^{2^n-1} \{(\lambda,\mu) | \lambda = 0,1,\dots,\mu\},$$

and

$$S \coloneqq \{(\lambda,\mu) | 0 \le \lambda \le 2^n, 2 \le \mu \le 2^n\}$$

as a result,

$$Pr[(\lambda,\mu) \in A] = \frac{|A|}{|S|}$$

$$= \frac{\frac{2^n(2^n+1)}{2} - 3}{2^n(2^n-2)}$$

$$= \frac{1}{2} + \frac{3}{2(2^n - 2)} - \frac{3}{2^n(2^n - 2)} \geq \frac{1}{2}$$

Proof of Lemma 2:

$A_{(\lambda,\mu)} \coloneqq \{(\lambda, \mu, \kappa) |\ \kappa = \lambda \oplus r\ where\ \ 0 \leq \psi \leq \mu\}$

Thus, for each $(\kappa, \lambda, \mu) \in A_{(\lambda,\mu)}$ there exist an ψ such that

$$\lambda \oplus \kappa = \lambda \oplus \lambda \oplus \psi = \psi \leq \mu$$

Now, let

$$A \coloneqq \bigcup_{0 \leq \lambda \leq 2^n, 2 \leq \mu \leq 2^n} A_{(\lambda,\mu)}$$

Hence, for total numbers (λ, μ, κ) such that $\lambda \oplus \kappa \leq \mu$ and $\mu > 1$ we have

$$|A| = \sum_{\mu=2}^{2^n-1} \sum_{\lambda=0}^{2^n-1} |A_{(\lambda,\mu)}| = \sum_{\mu=2}^{2^n-1} \sum_{\lambda=0}^{2^n-1} (\mu + 1)$$

$$= 2^n \sum_{\mu=2}^{2^n-1} (\mu + 1)$$

$$= 2^n \left(\frac{2^n(2^n + 1)}{2} - 3 \right)$$

On the other hand,

$$S \coloneqq \{(\kappa, \lambda, \mu) | 0 \leq \lambda, \mu \leq 2^n - 1, 2 \leq \kappa \leq 2^n - 1\},$$

$$|S| = 2^n 2^n (2^n - 2)$$

Now, the probability that for random κ, λ and $\mu > 1$, $\lambda \oplus \mu < \kappa$ is equal with

$$Pr[(\kappa, \lambda, \mu) \in A] = \frac{|A|}{|S|}$$

$$= \frac{1}{2} + \frac{3}{2(2^n - 2)} - \frac{3}{2^n(2^n - 2)} > \frac{1}{2}$$

References

[1] G. D. Vecchia, M. Esposito, "A knowledge-based approach for detecting misuses in RFID systems, designing and deploying RFID applications". http://www.intechopen.com/books/designing-and-deploying-rfid-applications/aknowledge-based-approach-for detecting-misuses-in-rfid-systems.

[2] B. Song and C. J. Mitchell, "Scalable RFID security protocols supporting tag ownership transfer," *Journal of Computer Communications*, vol. 34, pp. 556-566, 2011.

[3] T. C. Yeh, Y. J. Wanga, T. Ch. Kuo, and S. S. Wanga, "Securing RFID systems conforming to EPC Class 1 Generation 2 standard," *Exp. Sys. with Appl.*, vol. 37, p. 7678–7683, 2010.

[4] M. Asadpour, and M. T. Dashti, "A privacy-friendly RFID protocol using reusable anonymous tickets," in *10th International Conference on Trust, Security and Privacy in Computing and Communications*, Changsha , 2011.

[5] J.-S.Cho, S.-S. Yeo, and S. K. Kim, "Securing against brute-force attack: A hash-based RFID mutual authentication protocol using a secret value," *Computer Communication*, vol. 34, pp. 391-397, 2011.

[6] M. H. Habibi, M. R. Aref, and Di Ma, "Addressing flaws in RFID authentication protocols," in *12th International Conference on Cryptology, Springer Berlin Heidelberg*, India, 2011.

[7] C.-H. Wei, M.-S. Hwang, and A. Y. Chin., "A mutual authentication protocol for RFID," *IT Professional*, vol. 13, no. 2, pp. 20-24, 2011.

[8] M. Safkhani, N. Bagheri,S. K. Sanadhya, M. Naderi , and H. Behnam, "On the security of mutual authentication protocols for RFID systems: The case of Wei et al.'s protocol". In *6th International Workshop on Data Privacy Management and Autonomous Spontaneus Security*, 2012.

[9] G. Avoine, and X. Carpent, "Yet another ultralightweight authentication protocol that is broken". In *Workshop on RFID Security- RFIDSec'12*, Nijmegen, 2012.

[10] Z. Sohrabi-Bonab, M. Alagheband, and M. R. Aref, "Traceability analysis of quadratic residue-based RFID authentication protocols," in *11th Annual International Conference on Privacy, Security and Trust (PST)*, Tarragona, 2013.

[11] M. Safkhani, P. Peris-Lopez, J. C. Hernandez-Castro, and N. Bagheri, "Cryptanalysis of the Cho et al. protocol: A hash-based RFID tag mutual authentication protocol," *Journal of Computational and Applied Mathematics*, vol. 259, pp. 571-577, 2014.

[12] 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 International Journal (ACSIJ)*, vol. 3, no. 5, pp. 44-52, 2014.

[13] M. Mohammadi, M. Hosseinzadeh and M. Esmaeildoust, "Analysis and improvement of the lightweight mutual authentication protocol under EPC C-1 G-2 standard," *Advances in Computer Science : an International Journal (ACSIJ)*, vol. 3, no. 2, pp. 10-16, 2014.

[14] M. R. Alagheband, and M. R. Aref, "Unified privacy analysis of new found RFID authentication protocols," *Security and Communication Networks*, vol. 6, no. 8, pp. 999-1009, 2013.