Wireless Networks
https://doi.org/10.1007/s11276-020-02266-7

Cryptanalysis and improvement of a group RFID authentication protocol

Nasrollah Pakniat[1] · Ziba Eslami[2]

© Springer Science+Business Media, LLC, part of Springer Nature 2020

Abstract
In recent years, radio frequency identification (RFID) systems have become popular for identification. The key technology to protect the security of RFID systems is mutual authentication between the tags and the server. To enhance the efficiency of RFID systems, recently, Liu et al. proposed a group authentication protocol based on the concept of secret sharing. In this paper, we show that Liu et al.'s protocol falls short of providing security requirements. More specifically, we prove that in their protocol, authenticity of the tags to the server can not be achieved and on top of that the scheme can not be used more than once. We further propose a group mutual authentication protocol for RFID tags to overcome the mentioned drawbacks and prove that our proposal is secure. The results of analyzing the performance of the proposed protocol and its comparison with existing literature indicate that it outperforms current secure RFID authentication protocols.

Keywords RFID · Mutual authentication · Secret sharing · Cheater identification

1 Introduction

Radio frequency identification system (RFID) is an automatic technology that aids to identify objects, record metadata or control individual targets through radio waves [1, 2]. Typically, RFID systems consist of tags, readers and backend servers. Through broadcasting RF signals, the readers can inquire tags of their identifications and contents. The corresponding data are then read or updated by servers. Due to their low cost, stability and the property of identification without physical contact, RFIDs have been used in many applications, such as access control, file tracking, race timing, supply chain management, and smart labels. The widespread deployment of RFID systems enhances the efficiency and convenience, however, it also introduces potential security threats and risks to our life. Forging of participated entities (either tags or servers) is one key threat. Secure RFID systems, the same as many other similar scenarios [3–5], require a mechanism for mutual authentication whereby qualified tags can recognize qualified servers and vice versa so that any attempt to forge tags or servers is detected. Another threat is disclosure of sensitive data since the co-related information of tags (labeled on products) might be utilized to reveal a user's identity, his location, his movement, or his habits. Therefore, designing a secure RFID authentication solution which is capable of providing both identity privacy (anonymity) and mutual authentication is quite a challenging task. This in turn means employing sophisticated algorithms is inevitable. On the other hand, due to the small storage and low computational capacity of tags [6], most existing RFID authentications adopt lightweight cryptography or hash functions to achieve security [7–22]. Popular tags (like Mifare, Suicard, ISO 15693, EPC Gen2 [20, 23]) have cost pressure from the market and all call for computationally lighter algorithms as well.

Recently, Liu et al. [24] used the concept of secret sharing (SS) to propose an efficient group RFID authentication protocol. Their protocol is a unilateral authentication method so that authentication of the tags to the server is

✉ Nasrollah Pakniat
pakniat@irandoc.ac.ir

Ziba Eslami
z_eslami@sbu.ac.ir

[1] Information Science Research Center, Iranian Research Institute for Information Science and Technology (IRANDOC), Tehran, Iran

[2] Department of Data and Computer Science, Shahid Beheshti University, G.C., Tehran, Iran

Published online: 04 February 2020

done via secret sharing. For the reverse authentication (i.e., authentication of the servers to the tags), the authors suggested employing any existing secure RFID authentication protocol.

1.1 Motivations and contributions

In this paper, first, we consider the security of existing literature on group RFID authentication protocols based on secret sharing and prove that Liu et al.'s [24] protocol falls short of achieving its claims regarding security. In particular, we prove that this protocol doesn't provide authenticity of the tags and furthermore, the scheme is one-time. Then, we proceed to show how secret sharing can be employed to come up with a secure and efficient group RFID protocol with mutual authentication capabilities. In our proposal, mutual authentication, i.e. the authentication of the tags to the server and vice versa, is achieved via secret sharing. We further prove that the proposed protocol provides all the needed security requirements and finally, we show that, using secret sharing for mutual authentication in the proposed protocol, makes it comparably more efficient than other existing secure protocols in the literature.

1.2 Organization of the paper

The rest of this paper is organized as follows. In Sect. 2, we describe related works on group authentication in RFIDs. In Sect. 3, we review Liu et al.'s protocol. We discuss drawbacks of Liu et al.'s protocol in Sect. 4. In Sect. 5, we propose a new secret sharing- based group authentication protocol for RFID. We analyze the security and the performance of the proposed protocol in Sect. 6. Finally, we conclude the paper in Sect. 7.

2 Related works

Many researches have focused on simultaneous authentication of multiple RFID tags. There are schemes based on sequential tag processing and some papers introduced schemes which authenticate all the tags at once. Saito and Sakuri [25] proposed an authentication method using timestamps which was in fact, a scheme for multiple tags authentication. In this scheme, the reader retrieves timestamps from a database and broadcasts it to the each tag. This RFID system uses two types of tags, ordinary and pallets. Yet, this RFID scheme can't resist certain attacks. In 2007, Lin et al. [26] proposed the idea of combining all tags together forming a chain while authenticating them with preserved integrity. But the identity of tags is transmitted in plain which makes this scheme vulnerable to tracing. In addition, this protocol requires reading tags in a specific ordering which makes it inefficient for practical situations. To overcome this impracticality issue, Lien et al. [27] was proposed, assuming that the reader has enough computational power and pallet tags that can merge into the reader. This protocol can be used in some special supply chains. Liu et al. [28] proposed grouping-proofs-based authentication for distributed RFID systems. In this method, tags are divided in several groups which are later checked in sequence. This method handles strong privacy concerns and is resistant to many common types of attacks. Although sequential processing of tags needs them to be ordered in advance. Dhal and Gupta [29] proposed another RFID authentication protocol for multiple tags in 2014, assuming multiple tags are attached to an object with the intention of increasing reader identification probability. In 2015, Shen et al. [30] came up with an improvement for the previous protocol in order to make the RFID system able to ensure object positioning in addition to identifying it. Some more advanced protocols are based on secret sharing routines and hash functions and use both symmetric and asymmetric keys. In some methods with symmetric key such as [31], the transmitted information may be leaked and thus they cannot be used in large scales. With the introduction of elliptic curve cryptography (ECC) in RFIDs [31], asymmetric encryption was employed for authentication of multiple tags. Vaudenay [32] showed that asymmetric key encryption methods are crucial to ensure strong privacy guarantees. This line of research was followed by Batina et al. [33] who provided an ECC-based protocol allowing multiple tags to be authenticated at once. However, [34] and [35] proved vulnerability of this method to man in the middle (MITM), tracing and impersonation attacks. Lin et al. [36] made improvements to Batina et al.'s work, however Ko et al. [37] found that this protocol is also vulnerable to impersonation and tracking attacks. Cheng et al. [31] proposed an ECC based method to be resistant to MITM attacks and to include strong privacy concerns. To protect sensitive information in RFID tags, key distribution techniques were employed initially by Langheinrich and Marti [38]. Their work was mainly based on Shamir's scheme [39] and divided tag IDs into a single secret. Although their protocol was resistant to eavesdropping attacks but later [40] found out that it suffers from scalability issues. Another attempt of using Shamir 's secret sharing was made in [38]. They proposed a distributed process that divides IDs between the tags and the reader as encoded shares and keeps in a tag storage. In their authentication process a combination of secret shares is required to verify the secret key. Later a key distribution method using Ramp secret sharing was proposed in which the size of each share was smaller than the secret itself [41]. Although [42] found that [41] is vulnerable to

tracking and counterfeiting attacks. Cai et al. [42] came up with a scheme able to resist tracking attacks using hash functions. It updates the value of secrets in tags by using hash functions, but this scheme is also vulnerable to tracking attack. To ensure privacy and to prevent tracking attacks, Abughazaleh et al. [43] provided a secret key updating method based on dividing and distributing shares using an addition operator and SHA-3 hash function. In 2018, Liu et al. [24] proposed a scheme based on secret sharing in order to improve efficiency. They also provided a cheater identification procedure to detect forged tags. In this paper, we are mainly concerned with the results of this work. We show that this scheme cannot be used for the same tags more than once. We further point out security issues like its vulnerability to malicious active attackers in subsequent sections.

3 Review of Liu et al.'s protocol

In this section, we review the group RFID authentication protocol proposed by Liu et al. [24]. We first summarize notations in Table 1 and then proceed to provide the details of the scheme.

The details of Liu et al.'s group RFID authentication protocol [24], also depicted in Fig. 1 are as follows:

- *Initialization* In this phase:
  1. $\Gamma.Gen$ is executed to generate sk_S and PK_S as the private and public keys corresponding to the server, respectively.
  2. A threshold value $k(<n)$ is chosen.
  3. The polynomial $f(x) = \sum_{i=0}^{k-1} a_i x^i$ is constructed over Z_q where $a_i (i = 0, \ldots, k-1)$ are some randomly chosen values.
  4. For $i = 1, \ldots, n$: a unique value $x_i \in Z_q$ is assigned to T_i as its identifier and $f_i = f(x_i)$ is computed as its private share.

  At the end of the initialization phase, the server keeps $\{q, k, sk_S\}$ and each tag T_i keeps $\{x_i, f_i, PK_S\}$.
- *Communication-round 1* Each tag T_i computes $C_{1i} = \Gamma.Enc(x_i, PK_S)$ and $C_{2i} = \Gamma.Enc(f_i, PK_S)$ and sends them to the server.
- *Communication-round 2*
  1. After receiving the pair (C_{1i}, C_{2i}) from T_i (for $i = 1, \ldots, n$), the server computes the pair (x_i', f_i') where, $x_i' = \Gamma.Dec(C_{i,1}, sk_S)$ and $f_i' = \Gamma.Dec(C_{i,2}, sk_S)$.
  2. The server then applies the Lagrange interpolation procedure on the computed pairs $((x_i', f_i')$ for $i = 1, \ldots, n)$ to obtain a polynomial $f'(\cdot)$. If the degree of $f'(\cdot)$ is $(k-1)$ then, all the tags are considered verified. Otherwise, assuming that $AuthSS_1, \ldots, AuthSS_{C_n^k}$ are all different subsets of T containing exactly k tags, the forged tags will be identified through the following procedure:
     (a) For $j = 1, \ldots, C_n^k$: The server applies Lagrange interpolation procedure on the pairs obtained by decrypting the provided

Table 1 Notations

Notation	Meaning
$\Gamma = (Gen, Enc, Dec)$	An ECC based asymmetric encryption scheme
sk_S	The secret key of the server
PK_S	The public key of the server
n	The number of the tags
k	The threshold value
$T = \{T_1, T_2, \ldots, T_n\}$	The set of RFID tags
q	A prime number
x_i	The associated identity to T_i. For example it could be the Electronic Product Code (EPC) associated to each tag in EPC C1 G2 standard
E	An elliptic curve group over a prime field
P	Generator of the Elliptic curve E
h	A cryptographic hash function
T_{EM}	Elliptic curve point multiplication operation.
T_{EA}	Elliptic curve addition operation
T_h	Hash computation operation
$T_{mul,q}$	Multiplication operation in the field $\mathbb{Z}_q$

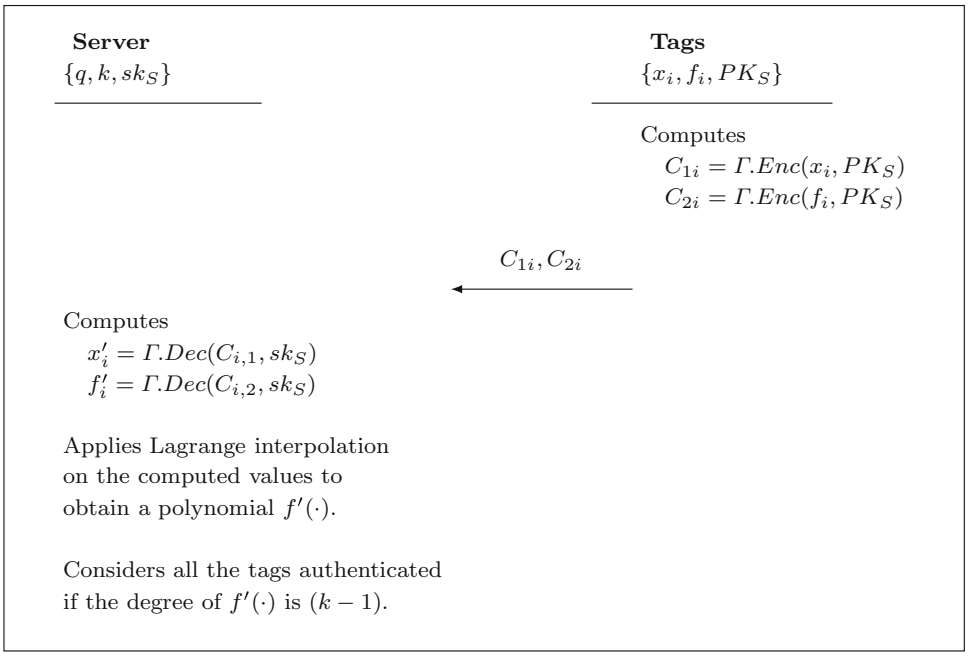

Fig. 1 Liu's et al. group RFID authentication protocol

ciphertexts by all the members of $AuthSS_j$ and computes a polynomial $f'_j(\cdot)$.

(b) Let $f^*(\cdot)$ be the polynomial computed more often the above procedure. Then, for $j = 1, \ldots, C_n^k$: all the members of $AuthSS_j$ would be considered qualified if $f'_j(\cdot)$ is equal to $f^*(\cdot)$.

(c) Let QT be the set of all qualified tags then, the set of forged tags is determined as $FT = T - QT$.

4 Drawbacks of Liu et al.'s group RFID authentication protocol

In the following we provide the main drawbacks of Liu et al.'s protocol [24].

D1. *In Liu et al.'s protocol, an attacker can perform a procedure so that while the valid tags would be identified forged, some fake ones would pass the authentication* The reason for such a claim is that in Liu et al.'s protocol, the server does not keep any information about the shared polynomial $f(\cdot)$. Therefore, knowing the values k, n, PK_S, an attacker $\mathcal{A}$ can generate a new $(k-1)$-th degree polynomial $f_{\mathcal{A}}$, produce a set of fake tags $T_{\mathcal{A}} = \{T'_1, \ldots, T'_n\}$ with $n' > n$, and equip each one with $\{x'_i, f'_i = f_{\mathcal{A}}(x'_i), PK_S\}$. Afterwards, when the tags want to authenticate themselves to the server, $\mathcal{A}$ inserts the forged tags among the valid ones. Now, since the number of the fake tags are more than the valid ones, it is easy to see that the fake tags would be considered authenticated by the server and the valid ones would be considered forged.

D2. *While an RFID authentication protocol should be multi-use, Liu et al.'s protocol is not* In an RFID authentication protocol, the server and the tags should be able to authenticate themselves to each other multiple times. Unfortunately, it can easily be seen that Liu et al.'s protocol can only be used once. If Liu et al.'s protocol were used multiple times to authenticate a group of tags then, an attacker would be easily able to impersonate itself as a valid tag in any future authentication of this group. The reason for such a claim is that the values sent by any tag would be also valid in any future authentication of the same group.

D3. *Liu et al.'s protocol doesn't use all the potentials of secret sharing schemes* In Liu et al. protocol, only the authentication of the tags to the server is done by using the secret sharing schemes. According to the authors, the authentication of the server to the tags can be done by this part of an existing efficient RFID authentication protocol. However, this approach would reduce almost all the efficiency obtained by using the secret sharing schemes. That is because in this way, the tags should keep more secrets to be able to do such a procedure and do some heavy computations to authenticate the server.

In the next section, we propose a new secret sharing-based group RFID authentication protocol that overcomes the above-mentioned drawbacks.

Our idea to overcome issue $D1$ is that the server keeps some information regarding the shared secrets between the tags. To overcome the second issue (i.e.,$D2$), we initiate another secret sharing process to generate the private shares of the tags. The sharing is done in such a way that the values provided by tags to prove their authenticity in one authentication round would become invalid in another authentication round. The proposed protocol overcomes issue $D3$ by using tag's shares from the secret and the exchanged values between the sender and the tags. The details are provided in the next section.

5 The proposed secret sharing-based group mutual authentication protocol for RFIDs

Using the notations provided in Table 1, the proposed group RFID authentication protocol, depicted in Fig. 2, can be described as follows:

- *Initialization* In this phase:
  1. The server will be equipped with a private key $sk_S \in_R Z_q^*$ and the corresponding public key $PK_S = sk_S \cdot P$.
  2. A threshold value $k(<n)$ will be chosen.
  3. The polynomials $f_1(x) = \sum_{i=0}^{k-1} a_i x^i$ and $f_2(x) = \sum_{i=0}^{k-1} b_i x^i$ will be constructed over Z_q where $a_i, b_i \in_R Z_q (i = 0, \ldots, k-1)$.
  4. For $i = 1, \ldots, n$: x_i will be assigned to T_i as its identifier, and $(f_{1i}, f_{2i}) = (f_1(x_i), f_2(x_i))$ will be computed as its private share.

  At the end of this phase, the server keeps $\{q, k, sk_S, P, a_0, b_0\}$ and each tag T_i keeps $\{q, x_i, f_{1i}, f_{2i}, P, PK_S\}$.
- *Communication-round 1* The server chooses $r \in_R Z_q^*$ and sends it to all the tags.
- *Communication-round 2* Each tag T_i:
  1. Chooses $r_i \in_R Z_q^*$.
  2. Computes

$$\begin{aligned} h_i &= f_{1i} + r \cdot f_{2i} (mod q), \\ R_i &= r_i \cdot P, \\ TK_i &= r_i \cdot PK_S, \\ k_{i,1} &= h_i + h(TK_i || 0) (mod q), \\ k_{i,2} &= x_i + h(TK_i || 1) (mod q), \\ k_{i,3} &= r_i + h(TK_i || 2) (mod q). \end{aligned}$$

  3. Sends $(k_{i,1}, k_{i,2}, k_{i,3}, R_i)$ to the server.
- *Communication-round 3* The server:
  1. For $i = 1, \ldots, n$: computes

$$\begin{aligned} TK_i' &= sk_S \cdot R_i, \\ h_i' &= k_{i,1} - h(TK_i || 0) (mod q), \\ x_i' &= k_{i,2} - h(TK_i || 1) (mod q), \\ r_i' &= k_{i,3} - h(TK_i || 2) (mod q), \\ v_i' &= r_i' \cdot h_i' (mod q). \end{aligned}$$

  2. Applies the Lagrange interpolation procedure on the pairs $((x_i', h_i')$ for $i = 1, \ldots, n)$ to obtain a polynomial $h'(\cdot)$. If the degree of $h'(\cdot)$ is $(k-1)$ and the vertical intercept is $a_0 + rb_0$ then, all the tags are considered verified. Otherwise, to find the forged tags, the server:
     (a) Finds SS as a subset of T containing exactly k tags with $h_{SS}(0) = a_0 + rb_0$ where, $h_{SS}(\cdot)$ is the polynomial obtained by applying the Lagrange interpolation procedure on (x'_{B_i}, h'_{B_i}) for $i = 1, \ldots, k$ such that $T_{B_i} \in SS$.
     (b) Sets $UT = T - SS$ as the temporary set of unchecked tags and $QT = SS$ as the initial set of qualified tags.
     (c) For each $T_i \in UT$, sets $QT = QT + \{T_i\}$ if $h_{SS}(x_i') = h_i'$.
     (d) Determines the set of forged tags as $FT = T - QT$.
  3. Sends v_i' back to T_i for each i such that $T_i \in QT$.
- *Communication-round 4* Each tag $T_i \in QT$ checks whether $v_i' = r_i \cdot h_i$ holds or not. If it holds, then the tag accepts the server.

6 Security analysis and performance evaluation

In this section, first we analyze the security of our proposed protocol and then, we evaluate its performance and provide comparisons with other existing protocols.

6.1 Security analysis

In the following parts, we present the security analysis for the proposed protocol. The analysis mainly contains proofs for the provided functionalities by the proposed protocol and its resistance to different attacks.

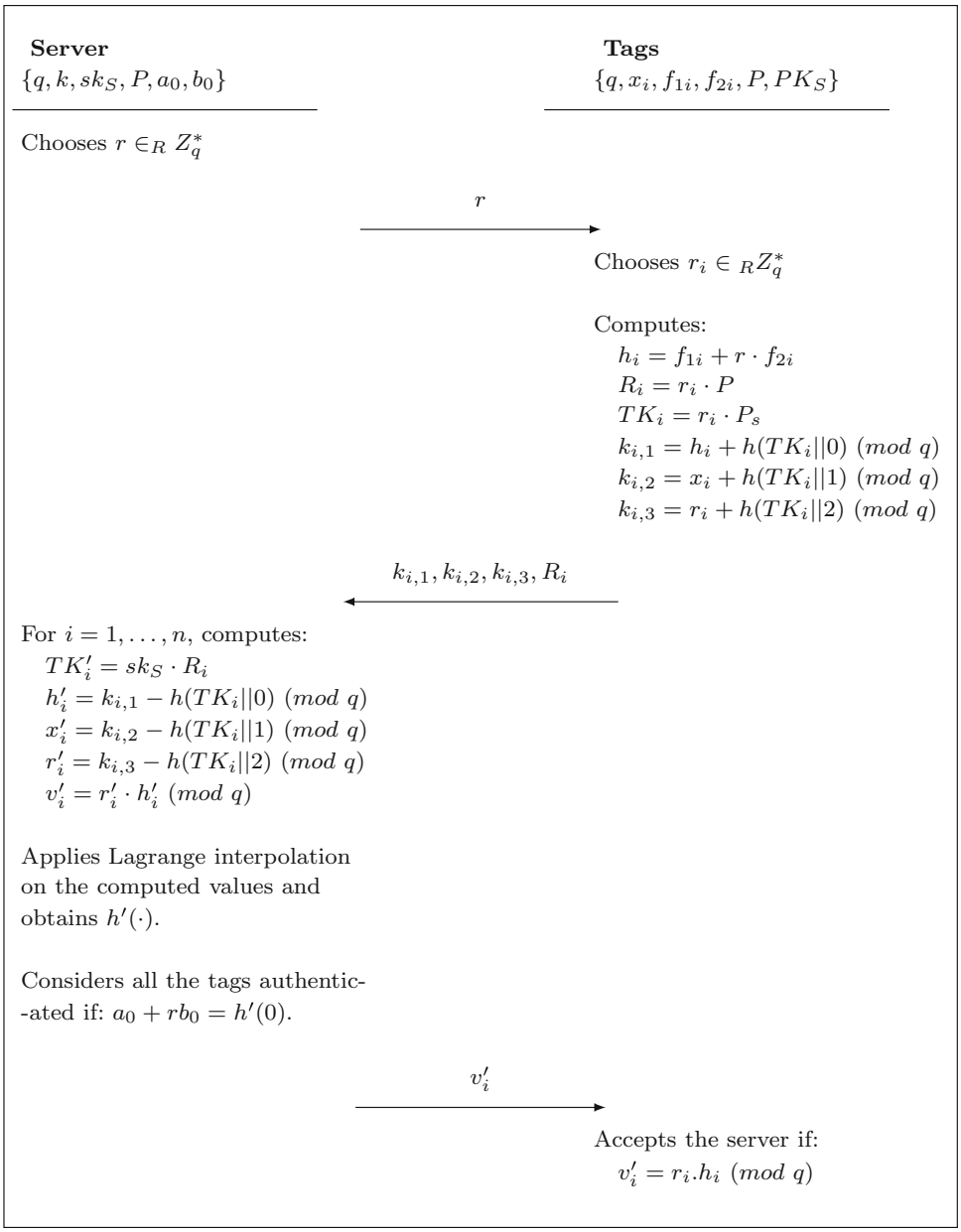

Fig. 2 The proposed secret sharing-based group RFID mutual authentication protocol

6.1.1 Provided functionalities

Mutual authentication First, we provide the proof that the server only accepts non-forged tags. Based on the homomorphic property of the polynomial based secret sharing schemes, the values x_i and h_i provided by the non-forged tags at the end of the communication-round-2 fulfill the following condition:

$h(x_i) = h_i$

where, $h(x) = f_1(x) + r \cdot f_2(x)$. Now,

- with the assumption that there exists k non-forged tags, there would be a subset of tags for which the fixed term of the interpolated polynomial (by using their provided values) would be equal to $a_0 + r \cdot b_0$,
- with the assumption that the number of forged tags won't exceeds $k - 1$, there won't be a subset of tags, containing forged ones, for which the fixed term of the interpolated polynomial (by using their provided values) would be equal to $a_0 + r \cdot b_0$.

Based on the above facts, unless a tag provides valid values (which is impossible to be done by fake tags) at the end of the communication-round-2, it won't be authenticated.

For the reverse authentication, the server authenticates himself to each tag by computing v_i and sending it to the tag T_i and the checking procedure done by the tag in the communication-round-4. The computation cannot lead into

a valid v_i unless the server knows his private key sk_S. Therefore, the tag can validate server's authentication.

Anonymity of the tags In the communication-round-2, each tag chooses a random value $r_i \in \mathbb{Z}_q^*$ which is involved in calculating $(K_{i,1}, K_{i,2}, K_{i,3}, R_i)$, so next time when a new r_i is chosen, all the generated values will be different from the previous time, and somehow they look random. Therefore, an attacker can't bind these values to any tag and can't decide if this tag is the one observed before or not.

Multi-usage Each time the authentication procedure is performed, the server chooses a random $r \in \mathbb{Z}_q^*$ and sends it to all tags. Each tag calculates $h_i = f_{1i} + r \cdot f_{2i}$ so that r is involved in calculating h_i. In each run r is different so h_i will be different for the same tag. For an attacker, in order to impersonate a tag, it needs to use the transcripts that were sent before, but it is impossible to use those information since r is different in each run of the scheme and thus previous information become invalid. Furthermore, each tag involved a random r_i in its values sent to the server. Directly computing r_i from $R_i = r_i.P$ is as hard as solving the elliptic curve version of the Discrete Logarithm Problem. Also, the transmitted data between the tags and the server won't reveal any information about r_i. Therefore we can run the protocol as many times as we wish, safely.

6.1.2 Resistance to different attacks

Resistance to replay attack As explained earlier, during each authentication instance of the proposed protocol, the server chooses a random value $r \in \mathbb{Z}_q^*$ and sends it to all tags. Then, each tag calculates $h_i = f_{1i} + r \cdot f_{2i}$ and somehow, encrypts this value and sends the result along with some other encrypted messages to the server. These messages pass the verification performed by the server only when the same r is used. Using a fresh random value r, during each authentication round by the server, makes it impossible for an attacker to use reply attack to impersonate the tags. Moreover, the authentication of the server to the i-th tag is done by using v_i which is computed as $v_i = h_i \cdot r_i$ where r_i and h_i are unique to each authentication round. Therefore, it is also impossible to use v_is from previous round in a reply attack to impersonate the server.

Resistance to de-synchronization attack In the proposed protocol, the server does not require to keep the secret key of the tags and more importantly, the secret keys are not updated after each authentication round. Therefore, the de-synchronization attack is not applicable to the proposed protocol.

Resistance to traceability attack During each authentication instance of the proposed protocol, all the transmitted messages, including the messages sent back by the server to the tags, are blended with new fresh random values. Furthermore, none of the unbalanced operations is used in the authentication protocol which in many cases may lead to additional security vulnerabilities [46]. Therefore, the proposed protocol is resistant to the traceability attack.

6.2 Performance analysis

In this section, we analyze the performance of the proposed protocol and compare it with the existing ones. To achieve the same security level in comparisons, we assume that in all protocols, an elliptic curve modulo a 160-bit length prime is used. Moreover, to make a fair comparison, it is assumed that (1) the server is required to authenticate n tags in all the considered protocols, and (2) the server's workload for finding a matched tag is also included in the computational cost of the server.

Computational costs are obtained by computing the number of operations performed in each protocol by the tags and the server. To make the comparisons feasible, we ignore light computations and only take into account the most time-consuming operation, i.e., the elliptic curve point multiplication T_{EM}. In the comparisons, we consider 5 MHz tags for which the running time of the point multiplication is 64 ms [21], where ms denotes millisecond. In the proposed protocol, each tag needs to perform $2T_{EM}$ and therefore 128 ms.

Communication costs are obtained by computing the length of the transmitted messages through the authentication process. In the computations, we have ignored the required parameters to describe the elliptic curve and have assumed that the output length of the used hash functions in these protocols is 160 bits. Moreover, the length of each elliptic curve point is assumed to be 320 bits. (Note that each point on the elliptic curve has x and y coordinates and in our case can be represented with 320 bits.) In the proposed protocol, each tag sends the values $k_{i,1}, k_{i,2}, k_{i,3}, R_i$ to the server. Therefore, the communication costs of each tag in the proposed protocol is $3(160) + 320 = 800$ bits. The server broadcasts a random value r in the communication-round 1 and send v_i' to each tag in the communication-round 3. Each of these values have 160 bits length and therefore, the overall communication costs of the server to authenticate n tags is equal to $n(160) + 160 = (161)n$.

The storage space represents the required space to store the data on the tag side and the server side. In the proposed protocol, each tag needs to store $\{q, x_i, f_{1i}, f_{2i}, P, PK_S\}$. Therefore, the required storage space by each tag is $4(160) + 2(320) = 1280$ bits. The server, in the proposed protocol needs to only store $\{q, k, sk_S, P, a_0, b_0\}$ to authenticate all the tags. Therefore, the required storage by

Table 2 Comparisons between the proposed group RFID mutual authentication protocol and the related protocols

	[44]	[45]	[20]	[21]	[24]	Ours
Mutual authentication	No	Yes	Yes	Yes	No	Yes
Anonymity	No	No	Yes	Yes	Yes	Yes
Multi usage	Yes	No	Yes	Yes	No	Yes
Tag's computations	$2T_{EM} = 128$ (ms)	$5T_{EM} = 320$ (ms)	$3T_{EM} = 192$ (ms)	$3T_{EM} = 192$ (ms)	$2T_{EM} = 128$ (ms)	$2T_{EM} = 128$ (ms)
Server's computations	$O(n.(log\ n))$	$O(n.(log\ n))$	$O(n.(log\ n))$	$O(n.(log\ n))$	$O(n.(logn)^2)$	$O(n.(logn)^2)$
Communication costs of the tag (bits)	960	640	960	800	1280	800
Communication costs of the server (bits)	320(n)	640(n)	640(n)	640(n)	–	$160(n+1)$
Tag's storage requirements (bits)	1440	1280	1440	1440	640	1280
Server stroeage requirements (bits)	$800 + 480$(n)	$640 + 480$(n)	$800 + 480$(n)	$800 + 800$(n)	480	1120

the server is independent of the number of the tags and is only $5(160) + 320 = 1120$ bits.

We have also computed these parameters for the related protocols and compared them with our protocol. The results of the comparisons are provided in Table 2. As it can be seen from this table, the proposed protocol, along with the protocols of [20, 21], are the only existing protocols that provide the needed security requirements, i.e., mutual authentication, anonymity and multi-usage. Compared to the protocols of [20] and [21], in the proposed protocol, the computations performed by each tag is reduced by a factor of $\frac{1}{3}$. Moreover, while, the communication costs of the tags in the proposed protocol and that of [21] are equal, the server in the proposed protocol has far less communication costs. In terms of the required storage, while the tags in the proposed protocol and that of [20] require the same amount of storage, the server requires only a fixed amount of storage in the proposed protocol and therefore, our protocol is far more efficient than the other existing protocols in this regard. These advantages are obtained at the cost of an increase in the computational costs at the server side with a factor of $log\ n$. Note that while, the computational complexity of the server in all other protocols is of order $O(n(log\ n))$, in the proposed protocol, it is of order $O(n(logn)^2)$. Considering the described advantages, it can be concluded that the proposed protocol outperforms the existing literature.

7 Conclusion

Recently, Liu et al. proposed a group RFID authentication protocol in which the authentication of the tags to the server is done via secret sharing schemes. The authors claimed that their protocol is secure. However, in this paper, we disprove their claim and show that (1) this protocol doesn't provide authenticity of the tags to the server, and (2) it isn't multi-use. To overcome the mentioned drawbacks, we propose a new group RFID mutual authentication protocol and prove that the proposed protocol provides all the needed security requirements. In the proposed protocol, the authentication of the tags to the server as well as the vise versa are done via secret sharing. The results of analyzing the performance of the proposed protocol and comparison with the existing secure protocols in the literature are provided which demonstrate that our scheme outperforms existing protocols in terms of efficiency.

References

1. Jia, X., Feng, Q., & Ma, C. (2010). An efficient anti-collision protocol for RFID tag identification. *IEEE Communication Letters*, *14*(11), 1014–1016.
2. Jia, X., Feng, Q., Fan, T., & Lei, Q. (2012). RFID technology and its applications in Internet of Things (IoT). In *2012 2nd international conference on consumer electronics, communications and networks (CECNet)* (pp. 1282–1285).
3. Memon, I., Hussain, I., Akhtar, R., & Chen, G. (2015). Enhanced privacy and authentication: An efficient and secure anonymous communication for location based service using asymmetric cryptography scheme. *Wireless Personal Communications*, *84*(2), 1487–1508.
4. Memon, I., Arain, Q. A., Memon, H., & Mangi, F. A. (2017). Efficient user based authentication protocol for location based services discovery over road networks. *Wireless Personal Communications*, *95*(4), 3713–3732.
5. Madhusudhan, R., Hegde, M., & Memon, I. (2018). A secure and enhanced elliptic curve cryptography-based dynamic

authentication scheme using smart card. *International Journal of Communication Systems*, *31*(11), 1–21.
6. Michahelles, F., Thiesse, F., Schmidt, A., & Williams, J. R. (2007). Pervasive RFID and near field communication technology. *IEEE Pervasive Computing*, *6*(3), 94–96.
7. Chien, H. (2007). SASI: A new ultralightweight RFID authentication protocol providing strong authentication and strong integrity. *IEEE Transactions on Dependable and Secure Computing*, *4*(4), 337–340.
8. Avoine, G., Dysli, E., & Oechslin, P. (2006). Reducing time complexity in RFID systems. In *Selected areas in cryptography* (pp. 291–306).
9. Juels, A., & Weis, S. A. (2005). Authenticating pervasive devices with human protocols. *Advances in Cryptology—CRYPTO*, *2005*, 293–308.
10. Cao, T., Shen, P., & Bertino, E. (2008). Cryptanalysis of some RFID authentication protocols. *Journal of Communications*, *3*, 20–27.
11. Yang, J., Park, J., Lee, H., Ren, K., & Kim, K. (2005). Mutual authentication protocol for low-cost RFID. In *Workshop on RFID and lightweight crypto* (pp. 17–24).
12. Liu, Y., Zhong, Q., Chang, L., Xia, Z., He, D., & Cheng, C. (2016). A secure data backup scheme using multi-factor authentication. *IET Information Security*, *11*(5), 250–255.
13. Yeh, T. C., Wu, C. H., & Tseng, Y. M. (2011). Improvement of the RFID authentication scheme based on quadratic residues. *Computer Communications*, *34*(3), 337–341.
14. Liu, Y., Cheng, C., Gu, T., Jiang, T., & Li, X. (2016). A lightweight authenticated communication scheme for smart grid. *IEEE Sensors Journal*, *16*(3), 836–842.
15. Molnar, D., & Wagner, D. (2004). Privacy and security in library RFID: Issues, practices, and architectures. In *Proceedings of the 11th ACM conference on computer and communications security* (pp. 210–219).
16. Chen, Y., Chou, J. S., & Sun, H. M. (2008). A novel mutual authentication scheme based on quadratic residues for RFID systems. *Computer Networks*, *52*(12), 2373–2380.
17. Chien, H. Y. (2013). Combining Rabin cryptosystem and error correction codes to facilitate anonymous authentication with untraceability for low-end devices. *Computer Networks*, *57*(14), 2705–2717.
18. Chien, H. Y., & Laih, C. S. (2009). ECC-based lightweight authentication protocol with untraceability for low-cost RFID. *Journal of Parallel and Distributed Computing*, *69*(10), 848–853.
19. Gòdor, G., & Imre, S. (2011). Elliptic curve cryptography based authentication protocol for low-cost RFID tags. In*IEEE international conference on RFID-technologies and applications, 2011* (pp. 386–393).
20. Chien, H. Y. (2017). Elliptic curve cryptography-based RFID authentication resisting active tracking. *Wireless Personal Communications*, *94*(4), 2925–2936.
21. Dinarvand, N., & Barati, H. (2019). An efficient and secure RFID authentication protocol using elliptic curve cryptography. *Wireless Networks*, *25*(1), 415–428.
22. Gholami, V., & Alagheband, M. R. (2019). Provably privacy analysis and improvements of the lightweight RFID authentication protocols. *Wireless Networks*. https://doi.org/10.1007/s11276-019-02037-z.
23. Global, E. P. C. (2008). EPC radio-frequency identity protocols class-1 generation-2 UHF RFID protocol for communications at 860 MHz–960 MHz. *Version*, *1*, 23.
24. Liu, Y., Sun, Q., Wang, Y., Zhu, L., & Ji, W. (2019). Efficient group authentication in RFID using secret sharing scheme. *Cluster Computing*, *22*(4), 8605–8611.
25. Saito, J., & Sakurai, K. (2005). Grouping proof for RFID tags. In *19th international conference on advanced information networking and applications, AINA 2005*, vol. 2 (pp. 621–624).
26. Lin, C. C., Lai, Y. C., Tygar, J., Yang, C. K., & Chiang, C. L. (2007). Coexistence proof using chain of timestamps for multiple RFID tags. *Advances in Web and Network Technologies, and Information Management*, *4537*, 634–643.
27. Lien, Y., Leng, X., Mayes, K., & Chiu, J. H. (2008). Reading order independent grouping proof for RFID tags. In *IEEE international conference on intelligence and security informatics, 2008* (pp. 128–136).
28. Liu, H., Ning, H., Zhang, Y., He, D., Xiong, Q., & Yang, L. (2013). Grouping proofs-based authentication protocol for distributed RFID systems. *IEEE Transactions on Parallel and Distributed Systems*, *24*(7), 1321–1330.
29. Dhal, S., & Gupta, I. (2014). A new authentication protocol for RFID communication in multi-tag arrangement. In *International conference on computing for sustainable global development (INDIACom), 2014* (pp. 668–673).
30. Shen, J., Tan, H., Chang, S., Ren, Y., & Liu, Q. (2015). A lightweight and practical RFID grouping authentication protocol in multiple-tag arrangements. In *2015 17th international conference on advanced communication technology (ICACT)*.
31. Cheng, S., Varadharajan, V., Mu, Y., & Susilo, W. (2017). An efficient and provably secure RFID grouping proof protocol. In *Proceedings of the Australasian computer science week multiconference* (p. 71).
32. Vaudenay, S. (2007). On privacy models for RFID. In *International conference on the theory and application of cryptology and information security* (pp. 68–87).
33. Batina, L., Lee, Y. K., Seys, S., Singelee, D., & Verbauwhede, I. (2010). Privacy-preserving ECC-based grouping proofs for RFID. In *International conference on information security* (pp. 159–165).
34. Lv, C., Jia, X., Lin, J., Jing, J., & Tian, L. (2011). An efficient group-based secret sharing scheme. In *International conference on information security practice and experience* (pp. 288–301).
35. Hermans, J., & Peeters, R. (2012). Private yoking proofs: Attacks, models and new provable constructions. In *International workshop on radio frequency identification: Security and privacy issues* (pp. 96–108).
36. Lin, Q., & Zhang, F. (2012). ECC-based grouping-proof RFID for inpatient medication safety. *Journal of Medical Systems*, *36*(6), 3527–3531.
37. Ko, W. T., Chiou, S. Y., Lu, E. H., & Chang, H. K. C. (2014). Modifying the ECC-based grouping-proof RFID system to increase inpatient medication safety. *Journal of Medical Systems*, *38*(9), 66.
38. Langheinrich, M., & Marti, R. (2007). Practical minimalist cryptography for RFID privacy. *IEEE Systems Journal*, *1*(2), 115–128.
39. Shamir, A. (1979). How to share a secret. *Communications of the ACM*, *22*(11), 612–613.
40. Lv, C., Jia, X., Lin, J., Jing, J., Tian, L., & Sun, M. (2011). Efficient secret sharing schemes. In *Data management and applications: Secure and trust computing* (pp. 114–121).
41. Juels, A., Pappu, R., & Parno, B. (2008). Unidirectional key distribution across time and space with applications to RFID security. In *USENIX security symposium* (pp. 75–90).
42. Cai, S., Li, T., Ma, C., Li, Y., & Deng, R. H. (2009). Enabling secure secret updating for unidirectional key distribution in RFID-enabled supply chains. In *International conference on information and communications security* (pp. 150–164).
43. Abughazalah, S., Markantonakis, K., & Mayes, K. (2014). Enhancing the key distribution model in the RFID-enabled supply chains. In *2014 28th international conference on advanced information networking and applications workshops* (pp. 871–878).

44. Zhang, X., Li, L., Wu, Y., & Zhang, Q. (2011). An ECDLP-based randomized key RFID authentication protocol. In *2011 international conference on network computing and information security*, vol. 2 (pp. 146–149).
45. Liao, Y. P., & Hsiao, C. M. (2014). A secure ECC-based RFID authentication scheme integrated with ID-verifier transfer protocol. *Ad Hoc Networks*, *18*, 133–146.
46. Avoine, G., Carpent, X., & Hernandez-Castro, J. (2015). Pitfalls in ultralightweight authentication protocol designs. *IEEE Transactions on Mobile Computing*, *15*(9), 2317–2332.

Publisher's Note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

Nasrollah Pakniat has a Ph.D. in Mathematics, graduated in 2015 from Shahid Beheshti University. He received his M.Sc. degree in Computer Science from Shahid Beheshti University in 2011. He holds a B.Sc. degree in Computer Science from Shahid Bahonar University of Kerman in 2008. He began his scientific experience in 2016 as a faculty member in IranDoc. Now he is an assistant professor of Information Science Research Center. His efforts at Irandoc has mainly devoted to development of cryptographic protocols and text mining algorithms. His research interests include cryptography, network security and text mining.

Ziba Eslami received her Ph.D. in Applied Mathematics from Tehran University in 2000. During the academic years 2000–2003, she was a postdoctoral fellow in the Institute for Research in Fundamental Sciences (IPM). She served as a non-resident researcher at IPM during 2003–2005. Currently, she is an associate professor in the Department of Data and Computer Science at Shahid Beheshti University (SBU) in Iran. Her research is primarily centered around cryptography and security of cryptographic protocols.