SRTTU

Journal of Electrical and Computer Engineering Innovations
(JECEI)
Journal homepage: http://www.jecei.sru.ac.ir

JECEI

Research paper

RSPAE: RFID Search Protocol based on Authenticated Encryption

M. Eslamnezhad Namin[1]*, M. Hosseinzadeh*[2]*, N. Bagheri*[3,4,*] *A. Khademzadeh*[5]

[1]*Department of Computer Engineering, Science and Research Branch, Islamic Azad University, Tehran, Iran.*

[2]*Health Management and Economics Research Center, Iran University of Medical Sciences, Tehran, Iran.*

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

[4]*School of Computer Science, Institute for Research in Fundamental Sciences (IPM), Tehran, Iran.*

[5]*Iran Telecommunication Research Center, Tehran, Iran.*

Article Info

Article History:
Received 03 July 2017
Revised 13 January 2018
Accepted 16 May 2018

Keywords:
RFID
Secure search
Search protocols
Authenticated encryption

[*]Corresponding Author's Email Address: nbagheri@sru.ac.ir

Extended Abstract

Background and Objectives: Search protocols are among the main applications of RFID systems. Since a search protocol should be able to locate a certain tag among many tags, not only it should be secure against RFID threats but also it should be affordable.

Methods: In this article, an RFID-based search protocol will be presented. We use an encryption technique that is referred to as authenticated encryption in order to boost the security level, which can provide confidentiality and integrity, simultaneously.

Results: Furthermore, since the proposed protocol belongs to the lightweight protocols category, it is appropriate for applications that require many tags and costs must be low. In terms of the security, the analysis results give a satisfactory security level and it is robust against different RFID threats like replay, traceability and impersonation attacks. Using Ouafi-Phan model, BAN and AVISPA, we also checked the security correctness of the suggested protocol.

Conclusion: In this paper, we presented a scalable lightweight RFID search protocol. We employed an encryption technique called Authenticated Encryption (A.E.) to improve the security level of the suggested protocol.

Introduction

RFID is one of noncontact technologies that tries to illuminate human interference and create a smart environment based on wireless systems. Nowadays, it has various applications in different domains like library, passport and object tracking. In an RFID system, each item has an attached tag -to store unique and specific information about it- and a reader which gathers the information of the tag via a wireless connection and sends it to a backend database server to process[1][2].

The search protocol is one of RFID's most significant applications. This application is very useful in the warehouse and supply chain management with a large number of items. By RFID technology, tag search process is accelerated and a stock keeper could find a tagged item with minimum time and high accuracy. The first solution to implement a search process in RFID systems is to assign an identification number to each tag. Protocols based on ALOHA [3][4] and TREE [5][6] are used in this solution. However, these kinds of protocols have an easy and simple solution and could be applicable in some applications; there is a security concern about them. An attacker can trace a tag by its identification number and implement the traceability attack on these protocols. To solve this issue, the researchers tried to use an authentication process to find a specific tag [7][8]. In this process, the reader authenticates all

DOI: 10.22061/JECEI.2019.5186.199

existing tags in its field and understands which one is present this solution gives a satisfactory security level but it is time and power consumption. In a large-scale application, the extensive computational load is burdened on the server by this kind of search technique, with O(N) complexity. In order to have a simple solution with high-level security, search protocols have been proposed.

RFID protocols such as authentication and search could be classified on the basis of a variety of aspects, such as the reader-server communication and the weight of the tag. The protocols are categorized in three classes in terms of the weight of the tag: non-lightweight, lightweight and ultra-lightweight protocols. Only easy functions like shift registers, XOR and AND can be used in ultra-lightweight protocols [9][10][11][12][13]. Hence, this group of protocols could not provide the desired security [14][15][16]. In the lightweight authentication protocols, simple encryption models like cycle redundancy check (CRC) and pseudo random number generator (PRNG) are used [17]. Such protocols have a limitation on resources and the numbers of the gates for security modules, which are accommodated on the tag, are approximately 4500 gates [18]. These protocols are compliant with the EPC standard and can be implemented on the low-cost tags [8]. The third group of protocols to raise the system's security level uses encryption methods such as asymmetric cryptography. For instance, in recent years, some elliptic curve cryptography (ECC)-based protocols have been presented for RFID systems [7][19]. ECC is one of the asymmetric cryptographic methods with a desirable level of security that requires about ten thousand gates to be implemented.[20][21]. Although we achieve an acceptable amount of security by using these functions, they cause the number of accommodated gates on the tag to rise rather than the lightweight protocols. In spite of the fact that security is a key challenge in the RFID search protocols, tag expense is also an effective parameter when implementing the scheme for an implementation with many tags. Therefore, it seems necessary to make trade-off among the amount of security and the price.

Many scientists have been trying to present an effective search protocol in latest years. In 2007, Tan et al. [22] provided various search protocols. In the first protocol that is simplest of them, the reader broadcasts a request, which contains the ID number of the target tag. Then, a tag that its ID matches to the request, responds to the reader. This protocol is susceptible to replay and traceability attacks. To resist the first protocol against the replay attack, the authors proposed that the reader should use a random number in each sending request in the second protocol; the tag stores random numbers that reader has sent in the previous session. If the tag receives the message with a repetitive random number, does not respond. Although this solution could protect the protocol against replay attack, because the tag should store all previous random numbers that were generated by the reader, the implementation of this protocol is difficult. In the third protocol, Tan et al. proposed that for responding to the reader's request, a set of the tags should reply that the first m bit of their ID is similar to the first m bit of the desirable tag ID. In this method, if the tags have structured ID, this protocol has not suitable security levels. In the fourth protocol, the authors proposed that the non-desired tags in the reader's neighborhood should react with the probability of λ. The authors claimed that this approach is resistant against the traceability attack. Although it has been proved in the articles of Safkhani et al. [24] and Dhal et al. [23] that the protocols of Tan et al. are susceptible to the impersonation, the replay and the traceability attacks, many protocols based on protocols of Tan et al [25][26][27][28][29] have been presented.

In 2009, Kulsung et al. presented a search protocol based on PUF and LFSR [29]. In this protocol, if the adversary replays the last transferred message to the tag, the tag responds constant messages; therefore, this protocol is not resistant against the traceability attack [30]. In 2012, Yin and Li proposed a scalable and lightweight search protocol based on Encrypted Credential [28]. This protocol also was not robust against the traceability. In addition, Dhal and Sengupta's protocol [23], the protocol of Zuo et al. [27] and the protocol of Hoque et al. [26] were not resistant against the traceability attack. In the protocol of Kim et al. [25], the protocol of Chun et al. and the protocol of Jialiang et al. [31], the attacker can send a false request, save the answers of the tags and play them back on the reader's valid demand. Therefore, the described protocols could not be robust against the impersonation attack. In the protocol of Lin et al. [17] and the protocol of Sundaresan et al. [32], since the tags' responses are independent of the reader's request, if the adversary stores the tag's response one time, he can impersonate the tag. In Yoon and Youm's protocol [33], the protocol of Won et al. [34] and the protocol of Lee et al. [21], since the target tag always replies to the reader's request, protocols are vulnerable to the traceability. In 2014, Xie et al. [35] presented a secure search protocol to find a lost tag. In the same year, Joen et al. [36] showed that Xie's protocol is vulnerable to the traceability attack. In 2016, by using HMAC hash function, Mita et al. [37][37] presented two authentication and search protocols that both of them are vulnerable to DoS attack [40]. In 2015, Sunderesan et al. [38] presented a tag search protocol using a 128-bit PRNG function that Eslamnezhad et al. [39] proved that it is not resistant against traceability attack and improved it. In 2017, Sunderesan et al. [40] by using a modular and PRNG function presented another search protocol. In this protocol, the reader must be directly linked to the server during a search phase to calculate modular calculations [42].

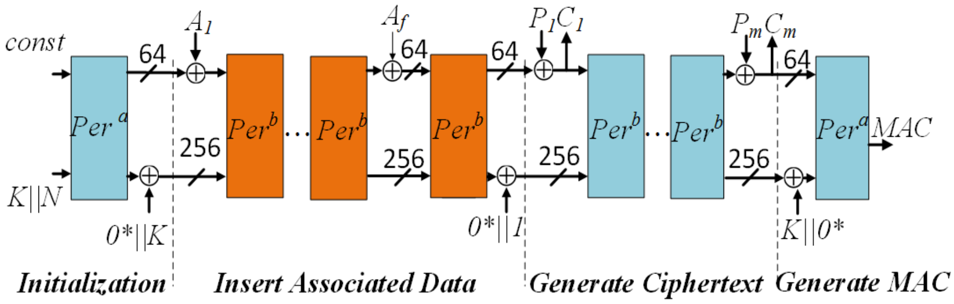


Fig. 1: The Encryption mode of ASCON-128.

In spite of the fact that the famous symmetric and asymmetric encryption methods such as DES [43], AES [44] and ECC [7] could improve the security and privacy level of the tag search protocols, their implementation is sophisticated on the low-cost passive tags [19][43][45].

Given that in low-cost tags the number of gates to implement a security module is roughly 2500 to 4500 gates [29][45][47], using standard algorithms such as RSA and alternative methods such as ECC is practically impossible [48][49][50][51][52]. In addition, AES could be accommodated with 3400 gates [53], although this implementation is inefficient and very slow [40]. Protocols based on PUF and LFSR require approximately 1400 gates but are highly advanced and can ge erate fluctuating outcomes depending on working conditions [41]. In this article, we will suggest a new search protocol which is capable of simultaneously providing confidentiality and integrity. We use authenticated encryption (A.E.) as encryption technique to accomplish this objective. In addition, the suggested search protocol can meet the restriction of low-cost tags in terms of weight.

The main contributions of this paper are:

1. Based on our knowledge in this study, it is the first time that an A.E. encryption is used to present an RFID search protocol for low-price and passive tags.
2. In the proposed protocol in this study, confidentiality and integrity are provided simultaneously.
3. The proposed protocol is a serverless method and suitable for applications with many tags.

Authenticated Encryption

The encryption technique used in the proposed protocol is described in this section. The security of information comprises three key elements: availability, integrity and confidentiality. Confidentiality talks about protecting information from disclosing by unauthorized parties. Integrity refers to protect data from tampering by illegitimate parties and availability guarantees access to information when needed.

Although cryptography methods improve the confidentiality level against various threats such as eavesdropping and disclosing data, if a system wants to provide an acceptable security level, it should satisfy all aspects of security and privacy. For example, a doctor wants to store a medical information of the patient in the medical database. The system should guarantee that the medical information of the patient is kept confidential.

In addition, the system should ensure a person transferring the medical information really is the doctor and the information has not tampered on the channel. Therefore, the system should provide confidentiality and authenticity, simultaneously.

In the mentioned example, suppose that medical records system is used A.E. method. At first, a key $k \in \{0,1\}^{|k|}$ should be shared between the database and the computer of the doctor. When the doctor wants to send the medical records M=(m, AD) to the database on an uncertain channel, the system generates a random number that is called Nonce as $N \in \{0,1\}^n$ and encrypts M by N and k as C=Ek(M, N). It also produces MAC and transmits MAC, N and C to the database. M=Dk(C, N) is decrypted and the integrity of the message is validated by MAC in the database. If the received MAC is valid, the database ensures the sender of the message is a legitimate doctor and stores the record.

The easiest solution to simultaneously prepare confidentiality and integrity is to combine an encryption algorithm and a message authentication code (MAC) function.

In this solution, that is called generic composition [54], not only the efficiency is not acceptable, but also the general combination of functions may cause errors in implementation [55][56]. To solve the mentioned errors, researchers suggested using of block cipher modes and dedicated A.E. algorithms such as AES-GCM[57], CCM-based 802.11i standard [58], GCM-based [59] on NIST standard and six A.E. schemes based on ISO/IEC 19772:2009 standard [60]. Given that basic problems in A.E. schemes and lack of the patent in dedicated A.E. algorithms [61][62][63], in 2014, the CAESAR (Competition for authenticated encryption: Security applicability and robustness) was held by the international cryptologic research community with the objective of offering effective A.E. techniques. Initially 57 designs with different structures, like sponge and stream cipher, were submitted for a number of applications. The main focus of the candidates is to design dedicated A.E. schemes. Given that a dedicated A.E. scheme simultaneously utilizes one module to create a ciphertext and MAC, there is no separated and individual MAC function. In terms of lightweight cryptography scheme, some of the candidate models like NORX [64], ACORN [65], ASCON [66] and JOLTIK [67] have been presented. For more explanation, ASCON algorithm that is a candidate of the final step of CAESAR competition for lightweight applications will be introduced briefly. It is recommended that the reader study the details of ASCON v1.2 in [66]. ASCON is based on sponge construction and uses permutation boxes with 320 bits long. it absorbs 128-bit key, 128-bit Nonce, 64-bit initial vector, and plaintext blocks and generates ciphertext and 128-bit MAC as output. As shown in Fig. 1, four stages are included in the ASCON cryptography process. The internal state is initialized by means of a key, Nonce and a constant value. The second stage is optional and if associated data exists, we can add it to the internal state. Associated data is an additional data that is not encrypted and the receiver will confirm its integrity.

In the third stage, the plain text is absorbed into the The Decryption process in ASCON is similar to the encryption process with the difference that in the third phase the plaintext is swapped with the ciphertext and do not need any additional hardware.

Table 1: The Security Claims of ASCON-128

Claims	Security (bit)
Confidentiality of plaintext	128
Integrity of plaintext	128
Integrity of associated data	128
Integrity of public message number	128

As depicted in Table 2, these lightweight A.E. schemes can meet the passive tag restrictions and involve under 4500 gates in contrast to renowned encryption techniques like ECC, DES and AES [64][65][66][67][68][69]. Therefore, A.E. can be asserted as a suitable encryption model for lightweight tags.

Table 2: Comparison of Lightweight Encryption Schemes

Algorithm	Construction	Parallelizable ENC \ DEC	Security proof	Gate equivalent
acorn	Stream-cipher	Yes	no	2600
ASCON	Sponge	Yes	Yes	2600
NORX	Sponge	Yes	Yes	1386
JOLTIK	Block-cipher	Yes	Yes	2100
DES	Block-cipher	Yes	Yes	2309
Photon	Hash	no	Yes	4362

The Proposed Protocol

As shown in Fig. 2, the new search protocol will be described in this section. Table 3 lists the notations used in this protocol. The suggested protocol consists of two phases: the phase of initialization and the phase of search.

- Initialization phase:

Suppose the channel from the server to the reader is protected. The server first authenticates the reader and stores the legitimate tag information that can be authenticated by the reader as (csi , rtsi, h(Tid, ti)) for i=1 to n in it. In addition, h(Tid, ti) and (cslj, rtsj and rtsj-1) for j=1 to m as the list of legitimate readers are stored in the tags. Furthermore, cs and csl set to zero and rts=rts-1.

- Search phase:

- Step one:

i. Nr is generated randomly by the reader as the nonce.

ii. Increases csj as csj=csj+1.

iii. Calculates M1 as: $M_1 = id_j \oplus N_r \oplus rts_j$.

iv. Encrypts M1 and csj by k as M2=Ek(M1,csj)and broadcasts Nr, M2 and MAC as a search request to the tags accessible in the reader range.

- Step two:

i. Upon receiving search query, each tag decrypts M2 by k and obtains M1 and csj.

ii. It checks id as:

$$id = M_1 \oplus N_r \oplus rts \qquad (1)$$

If above equation does not hold using rts, the tag repeats the comparison by rts-1.

iii. If (1) holds, the tag recognizes the search query is for itself and continues as follow:

A. Compares cs with csl.

B. If $cs \le csl$, this means that the tag receives an expired search query and the replay attack has occurred, then it sets $flag \leftarrow 1$. Otherwise, the authentication process is continued as follow:

A. Equals cs to csl.

B. Generates two random numbers Nt1 and Nt2 as nonce.

C. M3 and M4 are calculated as:

$M_3 = rts \oplus N_{t1} \oplus N_r \oplus id$

$M_4 = E_k(M_3, N_{t2})$

D. Sends Nt1, M4, MAC to the reader.

iv. If flag=1 or (1) does not hold using rts and rts-1, the tag responds to the reader with the probability of λ to harden against the traceability attack.

v. If id is verified by rts, the tag updates rts-1 by rts and rts by Nt2.

- Step three

i. Upon receiving the response of the tag, the reader decrypts it by k and gets M3 and Nt2.

ii. It checks rtsj as:

$$rts_j \overset{?}{=} M_3 \oplus N_{t2} \oplus N_r \oplus id \qquad (2)$$

iii. When (2) is held the tag is there, so rtsj is updated by Nt2 by the reader.

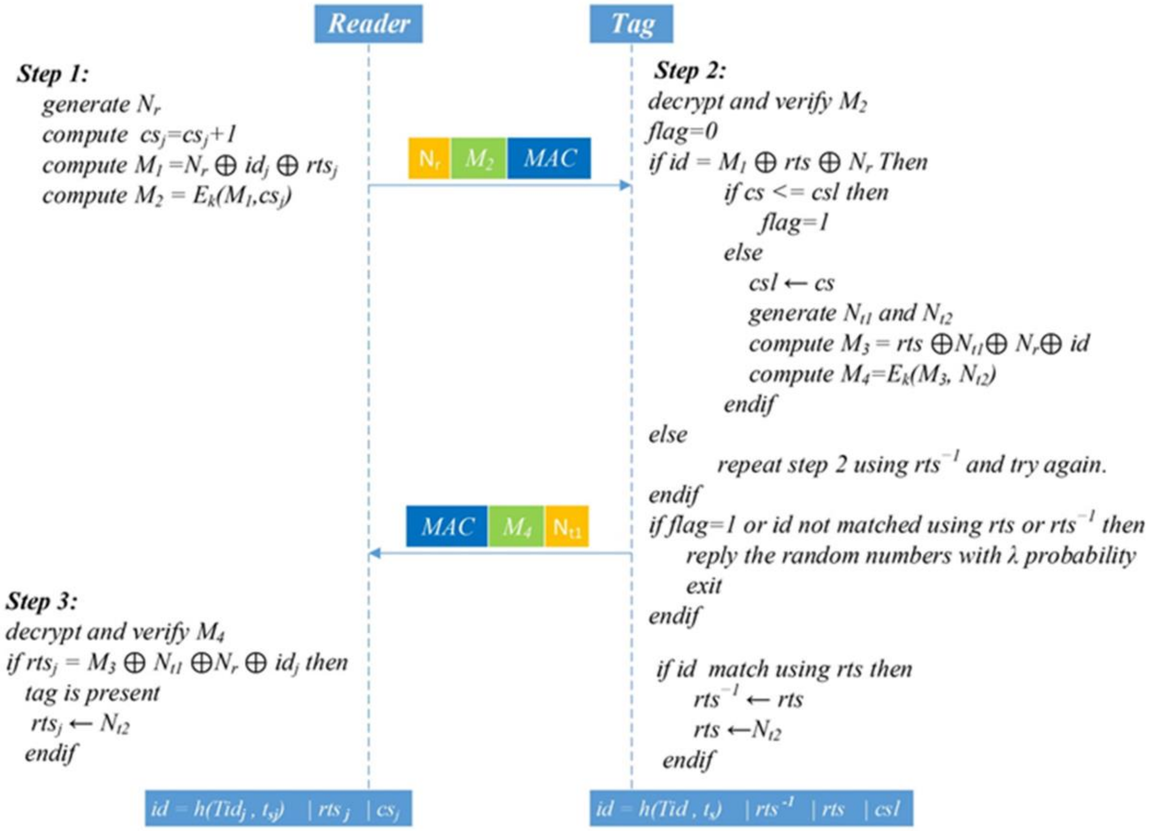

Reader
Tag
Step 1:
generate N_r
compute $cs_j=cs_j+1$
compute $M_1 = N_r \oplus id_j \oplus rts_j$
compute $M_2 = E_k(M_1,cs_j)$
N_r
M_2
MAC
Step 2:
decrypt and verify M_2
flag=0
if $id = M_1 \oplus rts \oplus N_r$ Then
if cs <= csl then
flag=1
else
csl ← cs
generate N_{t1} and N_{t2}
compute $M_3 = rts \oplus N_{t1} \oplus N_r \oplus id$
compute $M_4=E_k(M_3, N_{t2})$
endif
else
repeat step 2 using rts^{-1} and try again.
endif
if flag=1 or id not matched using rts or rts^{-1} then
reply the random numbers with λ probability
exit
endif
MAC
M_4
N_{t1}
Step 3:
decrypt and verify M_4
if $rts_j = M_3 \oplus N_{t1} \oplus N_r \oplus id_j$ then
tag is present
$rts_j \leftarrow N_{t2}$
endif
if id match using rts then
$rts^{-1} \leftarrow rts$
$rts \leftarrow N_{t2}$
endif
$id = h(Tid_j, t_{sj})$ | rts_j | cs_j
$id = h(Tid, t_s)$ | rts^{-1} | rts | csl

Fig. 2: The RSPAE protocol.

Suggested Protocol ‘S Security Analysis

The formal and informal security evaluation of the suggested protocol is provided in the current section. Based on the informal analysis, the robustness of the proposed protocol against some RFID threats will be evaluated.

We use the AVISPA tool and the BAN logic to evaluate the protocol's robustness for formal analysis. In addition, we present a formal proof by using Ouafi-Phan model [70].

It should be noted that the response of the tag is random and there is no information in it about the parameters of the tag.

For this security analysis, we present an adversary model due to various suppositions.

The first assumption is that the adversary can eavesdrop and intercept the transmitted signal between the tags and the reader. Additionally, it can send messages like a reader or a tag, and access to all encryption functions excluding secret parameters.

Table 3: The Notations Used in the Proposed Protocol

Notation	
S	Server
R	Approved portable reader
AL	Access list of the reader
Tid	Tag's Id-number
k	Encryption and decryption key
ts	Each tag's unique secret key
id	The identification of the tag which is calculated on the server as id = h(tid, ts).
rts	Current shared secret between each reader and the tag
rtsr	The rts in the reader-side
rtst	The rts in the tag-side
rts-1	Last shared secret between each reader and the tag
Nr	The random number that the reader generates
Nt1, Nt2	The random number that the tag generates
cs	Current counter value
csl	Last counter value
$\oplus$	Exclusive-OR function (XOR)
m	The number of lawful readers capable of authenticating the tag
flag	Flag is used to indicate the relay attack
$Ps \mid\equiv Xs$	The principal Ps can act if the formula Xs is true.
#Xs	Formula Xs is new and was not previously sent
$Ps \lhd Xs$	Xs sent a message to Ps
Ps|~Xs	Ps once said Xs
Gi	Ith group of the tags around the reader
n	The number of the legitimate tags that the reader has permission to authenticate them.

Informal Security Analysis

A. Dos Attack

In the suggested protocol, asynchronous case for the tag and the reader is possible in the following situations:

$$rts_r \neq rts_t$$

$$cs \leq csl$$

$$rts_t^{-1} \neq rts_t^{-2}$$

We explain how these situations happen and our approaches to resist the protocol against them in the following scenarios.

In the first scenario, the attacker acts as follows:

1. When the reader transmits Nr, M2 and MAC, the adversary eavesdrops the messages.
2. Then intercepts the sending message from the tag

Therefore, rts is changed in the tag-side but rts is not updated in the reader-side. Hence, the type 1 of the desynchronization occurs. To overcome this problem, not only rts is stored, but also the last search round key rts-1 is stored in the tag. As noted earlier, in the proposed protocol, the tag first verifies id by using rts. If the verification is failed, the tag repeats the same process by rts-1. The search protocol will be completed if only one of rts or rts-1 is matched. Note that rts is updated while id is match with the current rts. If the tag uses rts-1 to verify id, it does not update rts. Hence, the proposed solution protects the protocol against DoS attacks.

In the second scenario, to implement the DoS attack, the adversary should be done as follows:

1. He eavesdrops and stores previous search session messages.
2. Computes $cs' = cs \oplus \Delta$ where Δ is a random number.
3. Sends cs', M2 to the tag.

Above scenario causes to change csl to $cs \oplus \Delta$ in the tag-side. Given that, cs in the reader-side are not equal to $cs \oplus \Delta$, the type 2 of the desynchronization is occurred. In the suggested protocol, authenticated encryption is used to prevent such an attack. Since upon receiving the messages, the tag verifies the received messages by checking MAC, if the adversary tampers the messages, the tag detects this manipulation and aborts the session. Therefore, the suggested method is not vulnerable to this attack.

In the third scenario, the adversary intercepts the tag's messages, manipulates them and resends to the reader.

Because M4 and Nt2 is encrypted by A.E. method, if the adversary tampers the messages, the reader detects this manipulation easily. So, the suggested method is not susceptible to this attack.

B. . Reader Location Privacy

In some applications, mobile readers are used. Hence, the adversary has the ability to trace the reader or steal it. If the reader's messages consist of constant values associated with the reader's security parameters, the adversary can trace the reader by eavesdropping the messages. In the proposed protocol, the reader generates Nr randomly, computes M1 and M2 with it and encrypts messages by A.E. method. Accordingly, all the messages generated by the reader are fresh. The probability of the distinguish the reader random query are ($P(win) = 1/2^x$), where x is the length of MAC that based on Table 6, for ASCON, NORX and ACORN, x is 128, 80 and 128 respectively; so, P is negligible. Thus, the reader location privacy attack is not doable on this protocol.

C. Cloning Attack

The aim of the cloning attack is to authenticate a fake tag as a legitimate tag by the adversary. When the reader transmits a fresh message by using cs and Nr to the tags, the adversary as a valid tag should prepare the response based on Nr and cs that have been embedded in the receiving messages. Because the adversary does not have any knowledge about k and rts of the legitimate tag, he cannot forward a valid response to the reader. On the other hand, for spoofing attack, the adversary needs rts, cs and k to make M2 as a search query to fraud the tags. Because all exchange messages in the proposed protocol are encrypted by A.E., it cannot take any information about the secret parameters. Furthermore, since cs is increased in each session if the adversary utilizes the outdated message, it is detected by the tag and the session is aborted. So, our protocol is not susceptible to the cloning attack.

D. *Tag Location Privacy*

In order to protect the tag location privacy, there are various methods such as:

- Tags which are similar for first m bit of their id to the first m bit of the target tag id, answer to the search request of the reader [56].
- To the search request of the reader is reacted with λ probability by the non-target tags [56].

In the proposed protocol, the request of the reader is reacted with λ probability by the non-target tags. Therefore, if the adversary can send a legitimate search query to the tags population because he receives λ responses from them, he cannot detect the existence of the desired tag. On the other hand, to prevent the traceability attack by counting tags' responses [24], we use cs. If the desired tag receives a search query with $\mathrm{cs} \leq \mathrm{csl}$, it does not respond. Therefore, the mentioned attack cannot be implemented on our suggested method.

E. *Physical Security*

This attack is based on the physical access of the adversary to the reader and the tag. As far as the reader is concerned, since the tags' id are saved as hashed form in the reader, the adversary cannot reveal Tid and ts of the tags if the reader security is compromised. On the other hand, a secret key is shared between the reader and the tag by the server, the adversary cannot discover helpful data about other tags by compromise the physical security of the tag. Hence, the proposed protocol has no security issue related to physical security.

F. *Replay Attack*

To implement the replay attack, the attacker saves the transferred messages in one successful session and tries to make a connection to a tag directly by stored messages. When the reader is absent, if the adversary sends the old messages to tag, cs will not be updated. Since it is necessary to increase cs in each session, after receiving the stored message and comparing cs and csl, the tag understands the received message is not fresh and aborts the session. Then, it replies the random numbers with λ probability as the response. Therefore, such an attack on the suggested protocol is not possible.

Formal Security Analysis

G. *AVISPA Tool*

To evaluate and verify the correctness of a security protocol, there are various kinds of automated tools that provide a practical and realistically environment. The aim of this evaluation is to understand that the proposed protocol can perform properly in real condition or not. Automated validation of internet security protocol (AVISPA) is an automated tool that analyzes a security protocol and prepares a report about security issues of the protocol [48].

At the first step of the analysis, we have to model the protocol and the adversary by HLPSL. In the next step, to evaluate the validation of the protocol, AVISPA uses four back-ends as follows:

- TA4SP: Tree automate based on automatic approximations for the analysis of security protocols [72].
- OFMC: On the fly model checker [73].
- SATMC: SAT-based model checker [74].
- CL-ATSE: Constraint logic based-attack searcher [75].

The structure of AVISPA tool has been illustrated in Fig. 3. Because no message is transferred in the initialization phase of RSPAE, in the Fig. 4 only the search phase of the proposed protocol has been shown and formalized by HLPSL. The result of AVISPA is shown in Table 4. In light of utilizing XOR in the proposed protocol, SATMC and TA4SP cannot verify it. So, the outputs of CL-ATSE and OFMC are safe and the outputs of SATMC and TA4SP are INCONCLUSIVE. Therefore, the results of AVISPA analysis confirm that the RSPAE provides authentication and secrecy properties.

H. *BAN Logic*

In this section, a formal method called BAN logic [76] is used to evaluate the security level of the suggested method. Based on the protocol structure, we use the following two rules:

1. Public key rule

$$\mathrm{Pn1}: \frac{\mathrm{Ps} \mid\equiv \mathrm{Qs} \xleftrightarrow{\mathrm{K}} \mathrm{Ps}, \mathrm{Ps} \triangleleft [\ \mathrm{Xs}]_{\mathrm{K}}}{\mathrm{Ps} \mid\equiv \mathrm{Qs} \mid\sim \mathrm{Xs}}$$

2. Believe rule

$$\mathrm{Pn2}: \frac{\mathrm{Ps} \mid\sim (\ \mathrm{Xs},\mathrm{Ys})}{\mathrm{Ps} \mid\sim (\ \mathrm{Xs}\ )}$$

Formal format of the messages in the search phase are as follows:

$$FMn1. \quad R \rightarrow T : N_r, M_2, MAC$$

$$FMn2. \quad T \rightarrow R : N_{t1}, M_4, MAC$$

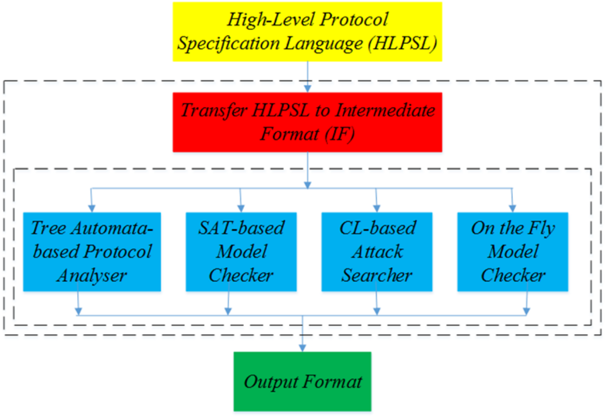

High-Level Protocol Specification Language (HLPSL)
Transfer HLPSL to Intermediate Format (IF)
Tree Automata-based Protocol Analyser
SAT-based Model Checker
CL-based Attack Searcher
On the Fly Model Checker
Output Format

Fig. 3: The structure of AVISPA.

Table 4: AVISPA Results for the RSPAE

Back-end	Summary
TA4SP	INCONCLUSIVE
OFMC	SAFE
SATMC	INCONCLUSIVE
CL-ATSE	SAFE

To evaluate the security level by BAN logic, a protocol has to pass four steps as below:

Idealizing the protocol

In the first step, the formal message of the protocol should be converted to the favorable form of BAN logic. The ideal form of exchange messages in this protocol are:

$\mathrm{IMn1.}\quad \mathrm{T} \lhd \{\mathrm{id}, \mathrm{N_r}, \mathrm{cs}, \mathrm{rts}\}_\mathrm{k}$

$\mathrm{IMn2.}\quad \mathrm{R} \lhd \{\mathrm{id}, \mathrm{N_r}, \mathrm{N_{t1}}, \mathrm{N_{t2}}, \mathrm{rts}\}_\mathrm{k}$

Initiative premises

The initial assumptions of the RSPAE are specified as follows:

$$
\begin{array}{ll}
An1. & R \mid\equiv R \xleftrightarrow{k} T \\
An2. & T \mid\equiv R \xleftrightarrow{k} T \\
An3. & R \mid\equiv T \xleftrightarrow{rts} R \\
An4. & T \mid\equiv T \xleftrightarrow{rts} R \\
An5. & R \mid\equiv T \xleftrightarrow{id} R \\
An6. & T \mid\equiv R \xleftrightarrow{id} T \\
An7. & T \mid\equiv \#(N_{t1}) \\
An8. & T \mid\equiv \#(N_{t2}) \\
An9. & R \mid\equiv \#(N_r) \\
An10. & R \mid\equiv \#(cs)
\end{array}
$$

Establishment of security goals

The RSPAE's security objectives are described as follows:

$\mathrm{Goal\ 1: T \mid\equiv R \mid\sim N_r}$

This implies the tag is confident that the reader produced and transmitted Nr without any interference of the attacker.

$\mathrm{Goal\ 2: R \mid\equiv T \mid\sim N_{t2}}$

This implies the reader is confident that the tag produced and transmitted Nt1 without any interference of the attacker.

Protocol Analysis

According to the previous steps, RSPAE's security evaluation is as follows:

According An2, IMn1 and Pn1: $\mathrm{K1{:}T \mid\equiv R \mid\sim \{cs,id,rts,N_r\}}$ By Pn2 and K1, we obtain K2 as: $\mathrm{K2: T \mid\equiv R \mid\sim N_r}$. Based on An1, IMn2 and Pn1, we compute K3 as: $\mathrm{K3: R \mid\equiv T \mid\sim \{N_{t1}, id, N_{t2}, N_r, rts\}}$. By Pn2 and K3, K4 is inferred as follows: $\mathrm{K3: R \mid\equiv T \mid\sim N_{t2}}$

K2 prove the correctness of Goal1 and K4 prove the correctness of Goal2. Therefore, it can be claimed that in the suggested protocol, messages are exchanged without any interference.

Formal Security Proof

In this section, we evaluate RSPAE's resistance against the traceability attack by a formal proof that proposed by Quafi and Phan [57] and works as follows:

- Learning Phase:

Assuming the existence of the tag T0 in the group G0, the adversary sends an execute query and receives MAC, M2 and Nr from the valid reader and Nt1, M4 and MAC from the tag. In addition, she gathers some noisy response from other members of the group that are sent by λ probability and stores all received messages.

- Challenge phase:

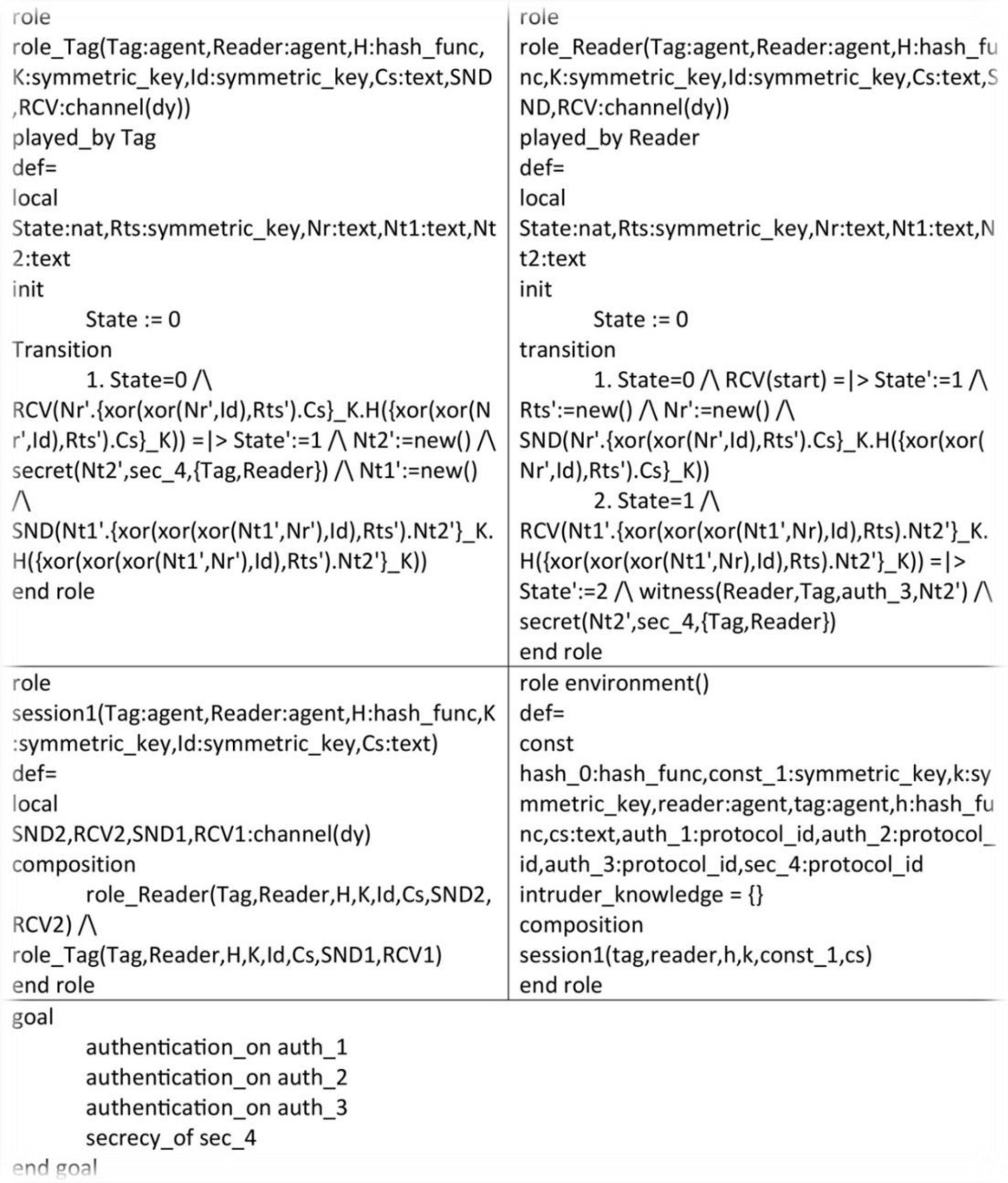
The adversary chooses two fresh groups G0 and G1 as T0 only belongs to G0. Then she sends the test query to them. The challenger generates a random bit $\mathrm{b} \in \{0,1\}$ and delivers responses of Gb to the adversary.

- Guess Phase:

The attacker produces the output b'=0 if she conjectures Gb=G0; otherwise the output will be b'=1. If Pw is the probability of the correct selection of b' by the adversary, the $\mathrm{Adv_A^{Utr}}$ (adversary advantage) is calculated based on the equation 3 and we will show that this amount is negligible.

$$
\begin{aligned}
\mathrm{Adv_A^{Utr}} &= \mid \mathrm{P_w(b' = b) - P_w(random\ coin\ flip)} \mid \\
&= \mid \mathrm{P_w(b' = b)} - \frac{1}{2} \mid
\end{aligned} \tag{3}
$$

Since the untargeted tags in the group Gb respond to the adversary's request by λ probability, to detect of the existence of T0 in this group, the adversary could use the number of responses to successive execution of challenge phase [39].



```
role
role_Tag(Tag:agent,Reader:agent,H:hash_func,
K:symmetric_key,Id:symmetric_key,Cs:text,SND
,RCV:channel(dy))
played_by Tag
def=
local
State:nat,Rts:symmetric_key,Nr:text,Nt1:text,Nt
2:text
init
        State := 0
Transition
        1. State=0 /\
RCV(Nr'.{xor(xor(Nr',Id),Rts').Cs}_K.H({xor(xor(N
r',Id),Rts').Cs}_K)) =|> State':=1 /\ Nt2':=new() /\
secret(Nt2',sec_4,{Tag,Reader}) /\ Nt1':=new()
/\
SND(Nt1'.{xor(xor(xor(Nt1',Nr'),Id),Rts').Nt2'}_K.
H({xor(xor(xor(Nt1',Nr'),Id),Rts').Nt2'}_K))
end role
```

```
role
role_Reader(Tag:agent,Reader:agent,H:hash_fu
nc,K:symmetric_key,Id:symmetric_key,Cs:text,S
ND,RCV:channel(dy))
played_by Reader
def=
local
State:nat,Rts:symmetric_key,Nr:text,Nt1:text,N
t2:text
init
        State := 0
transition
        1. State=0 /\ RCV(start) =|> State':=1 /\
Rts':=new() /\ Nr':=new() /\
SND(Nr'.{xor(xor(Nr',Id),Rts').Cs}_K.H({xor(xor(
Nr',Id),Rts').Cs}_K))
        2. State=1 /\
RCV(Nt1'.{xor(xor(xor(Nt1',Nr),Id),Rts).Nt2'}_K.
H({xor(xor(xor(Nt1',Nr),Id),Rts).Nt2'}_K)) =|>
State':=2 /\ witness(Reader,Tag,auth_3,Nt2') /\
secret(Nt2',sec_4,{Tag,Reader})
end role
```

```
role
session1(Tag:agent,Reader:agent,H:hash_func,K
:symmetric_key,Id:symmetric_key,Cs:text)
def=
local
SND2,RCV2,SND1,RCV1:channel(dy)
composition
        role_Reader(Tag,Reader,H,K,Id,Cs,SND2,
RCV2) /\
role_Tag(Tag,Reader,H,K,Id,Cs,SND1,RCV1)
end role
```

```
role environment()
def=
const
hash_0:hash_func,const_1:symmetric_key,k:sy
mmetric_key,reader:agent,tag:agent,h:hash_fu
nc,cs:text,auth_1:protocol_id,auth_2:protocol_
id,auth_3:protocol_id,sec_4:protocol_id
intruder_knowledge = {}
composition
session1(tag,reader,h,k,const_1,cs)
end role
```

```
goal
        authentication_on auth_1
        authentication_on auth_2
        authentication_on auth_3
        secrecy_of sec_4
end goal
```

Fig. 4: The specification of the RSPAE in HLPSL.

This attack method is not feasible in the RSPEA because if csl in the tag is lower than or equal to cs of the search request, the tag does not respond to the request. The attack is only possible when the adversary is able to decrypt and manipulate the reader's requests. Given that the A.E. based protocols e.g.

Acorn and Acson could provide 128-bit length security messages and values such as Nt1, Nt2 and Nr are fresh and random in a new session, the possibility of the manipulation of the messages by the adversary is very low.

Therefore, it can be claimed that the adversary advantage of the traceability attacks is negligible.

Security and Performance Comparison

In the current section, we compare the suggested protocol with the other protocols in terms of security and efficiency. In Table 5, the efficiency has been compared based on different parameters such as Total transferred bit, The Number of Messages Exchanged and gate equivalent (GE). The tag's weight is an important parameter for comparing the protocol effectiveness. The tag's weight refers to the number of gates that are accommodated in a tag's security module. The fewer the amount of GE a tag has, the lower the cost of implementing the protocol will be. On the other hand, reducing the GE would also lead to a reduction in the protocol's security level. The security module of RSPAE has three principal parts: XOR function, random number generator (RNG) function and A.E. cryptography function.

For a more concise and accurate comparison, we consider three different kinds of A.E. algorithms (NORX, JOLTIK and ACORN) with different features which are shown in Table 6. One effective parameter in an A.E. module's weight is the length of the encrypted message that is called Ek(). Assuming we use NORX8 with 1386 GE to implement the proposed protocol, we need three XOR functions with 3 GE [64] and 32-bit AKARI1B [77] with 922 GE. As a result, the proposed protocol needs 2299 GE to be implemented. For ACORN [65] with 2600 GE, 128-bit AKARI1B is used and a total of 6899 GE are required. Finally, for JOLTIK [67] with 2100 GE, we use 32-bit AKARI1B and need a total of 3028 GE. However, we used a symmetric encryption technique in RSPAE, the findings show that the tag's weight can meet the restriction of passive and lightweight tags. One of the main parameters to compare the efficiency of the RSPAE to other protocols is the number of messages that are exchanged in the protocol. The lower that amount is, the better the consumption energy and the run-time of the protocol will be improved. As shown in Table 6, in the proposed protocol two messages are transferred and TTb = 348. The results prove that even though in the proposed protocol the ciphertext and MAC are transferred together, the TTb is either equal or fewer than other protocols [21][27][34][78].

Despite the fact that there are only two cryptography functions in the proposed protocol, our protocol has fewer TTb and is more secure against various kinds of attacks in comparison to Sundaresan's protocol [78] with zero encryption function.

As mentioned before, in order to prevent invalid readers to have access to a tag, the data of the eligible readers is saved in the memory of tags. Therefore, the number of readers that can save their data in a tag is an important parameter for protocol's scalability. The main required parameters should be stored in each tag are id and (kj, csj, rtsj, rtsj-1) for j=1 to m. We assume that each tag has 8KB memory [79][80]. Given that the number of the readers can be stored in each tag is m= total memory/length (kj, csj, rtsj, rtsj-1), by using NORX, ACORN and Joltik the number of the readers are 372, 127 and 409 respectively. Since ACORN scheme is a candidate in the final step of the CAESAR, we consider it as an encryption scheme of the proposed protocol. However the result of the table 6 does not show the best GE for ACORN, but there are various efficient and lightweight implementations for this secure and lightweight scheme.

As shown in Table 7, the suggested protocol is compared with other protocols based on various attacks. In most of the protocols, an attacker can track tags. To solve this problem, we used tags' random response and counters cs and csl. Hoque et al. [26], Hossain et al. [81] and Sundersan et al. [78] are vulnerable to DoS attack. Because the suggested protocol uses A.E. encryption method and saves additional parameter like rts-1, It is robust against different kinds of DoS attacks. The suggested protocol, using A.E. methods, ensures confidentiality and integrity simultaneously on the side of the reader and on the side of the tags and the protocol is strong against well-known threats to the search procedures such as clone and DoS attacks.

Table 5 and Table 7 demonstrate that the suggested protocol is a scalable and reliable search technique. In addition, for applications with many tags, it is an appropriate solution.

Table 5: Comparison of the RSPAE Performance to Other Protocols

Protocol	Cryptography method	TTb	NME1	NCFR2	NCFT3	GE
Sundersun et al. [78]	PRNG	512	2	-	-	1435
Won et al. [34]	AES-128	640	2	4	4	3400
Zuo et al. [27]	PRNG and Hash-128	320	2	5	5	3143
Lee et al. [21]	ECC	838	4	4	4	14566
RSPAE	AE-NORX	384	2	2	2	2299
RSPAE	AE-JOLTIK	320	2	2	2	3028
RSPAE	AE-ACORN	768	2	2	2	6899

1 The Number of Messages Exchanged.

2 The Number of Cryptography Function on Reader.

3 The Number of Cryptography Function on Tag.

Table 6: Comparison of Lightweight Authenticated Encryption Search Protocols

A.E. algorithm	Nr	k	cs	id	rts	rts-1	MAC	Ek()	TTb*	PRNG GE	Total GE
NORX	32	80	32	32	32	32	80	80	384	922	2299
ACORN	128	128	128	128	128	128	128	128	768	3402	6899
JOLTIK	32	64	32	32	32	32	64	64	320	922	3028

*Total Transfer bits

Table 7: Comparison of Search Protocols

Attack	Tan et al. [22]	Kulseng et al[29]	Kim et al. [25]	Hoque et al. [26]	Won et al. [34]	Hossain et al. [81]	Lee et al. [21]	Sundersun et al. [78]	Zuo et al. [27]	chun et al[82]	Yoon et al. [33]	Yin et al. [47]	Our schema
Replay attack	×	×	✓	✓	✓	✓	✓	✓	×	✓	✓	✓	✓
Clone attack	×	✓	×	✓	✓	✓	✓	×	✓	×	✓	✓	✓
DoS attack	✓	✓	✓	×	✓	×	✓	×	✓	✓	✓	✓	✓
Tag location privacy	✓	×	×	✓	×	×	×	×	×	×	×	×	✓

✓: Resistant

×: Non-Resistant

Conclusion

In this paper, we presented a scalable lightweight RFID search protocol. We employed an encryption technique called Authenticated Encryption (A.E.) to improve the security level of the suggested protocol. The A.E technique will be used for the first time in a search protocol for RFID. The A.E. encryption method can provide confidentiality and integrity, simultaneously. Based on the result of Section 4, the proposed protocol can provide an acceptable security level against different RFID threats and also can resist against manipulating data by unauthorized access. In addition, given the available lightweight algorithms for A.E., we proved that these algorithms could satisfy the limitations of passive tags and need approximately 3000 gates to implement. Therefore, it can be claimed that the proposed protocol is suitable for low-cost and low-power RFID systems. On the other hand, NIST also recently announced a competition for lightweight cryptography, aiming to select standards for hash functions and authenticated encryption schemes. This is another evidence of the significant point behind developing security protocols for constrained environments, e.g., RFID systems, using these primitives.

Our work is also an initial step in this direction for search protocols and we believe there is a long way to go.

Author Contributions

M. Hosseinzadeh, N. Bagheri, and A. Khademzadeh designed and analysed the protocol. M. Eslamnezhad Namin, implemented formally the protocol. M. Eslamnezhad, M. Hosseinzadeh, N. Bagheri, and A. Khademzadeh interpreted the results and wrote the manuscript.

Acknowledgment

The authors would like to thank the anonymous reviewers for their comments which lead to improving the quality of the paper.

Conflict of Interest

The authors declare that there is no conflict of interests regarding the publication of this manuscript.

References

[1] N. Kumar, K. Kaur, S. C. Misra, R. Iqbal, "An intelligent RFID-enabled authentication scheme for healthcare applications in vehicular mobile cloud," Peer-to-Peer Networking and Applications, 9(5): 824–840, 2016.

[2] A. Tewari, B. Gupta, "Cryptanalysis of a novel ultra-lightweight mutual authentication protocol for IoT devices using RFID tags," The Journal of Supercomputing, 73(3): 1085–1102, 2017.

[3] X. Lin, H. Wang, Y. Kwok, B. Chen, M. Dai, L. Zhang, "Exploiting the prefix information to enhance the performance of FSA-based RFID systems," Computer Communications, 56: 108–118, 2015.

[4] D. Litian, W. Zizhong, D. Fu, "An identification algorithm in grouping and paralleling for data-intensive RFID systems," in Proc. International Conference on Big Data Computing and Communications: 337–346, 2015.

[5] Y. C. Lai, L. Y. Hsiao, B. S. Lin, "Optimal slot assignment for binary tracking tree protocol in RFID tag identification," IEEE/ACM Transactions on Networking, 23(1): 255–268, 2015.

[6] X. Yan, Y. Liu, B. Li, X. Liu, "A memoryless binary query tree based successive scheme for passive RFID tag collision resolution," Information Fusion, 22: 26–38, 2015.

[7] C. Jin, C. Xu, X. Zhang, F. Li, "A secure ECC-based RFID mutual authentication protocol to enhance patient medication safety," Journal of medical systems, 40(1): 1-6, 2016.

[8] H. Niu, E. Taqieddin, S. Jagannathan, "EPC GEN2v2 RFID standard authentication and ownership management protocol," IEEE Transactions on Mobile Computing, 15(1): 137–149, 2016.

[9] H. Chien, "SASI: A new ultralightweight RFID authentication protocol providing strong authentication and strong integrity," IEEE Transactions on Dependable and Secure Computing, 4(4): 337–340, 2007.

[10] J. Kang, "Lightweight mutual authentication RFID protocol for secure multi-tag simultaneous authentication in ubiquitous environments," The Journal of Supercomputing, DOI:10.1007/s11227-016-1788-6, 2016.

[11] P. Lopez, J. Castro, J. Estévez-Tapiador, A. Ribagorda, "LMAP: A real lightweight mutual authentication protocol for low-cost RFID tags," in Proc. Workshop on RFID security: 12–14, 2006.

[12] P. Lopez, J. Castro, J. Tapiador, A. Ribagorda, "EMAP: An efficient mutual-authentication protocol for low-cost RFID tags," in Proc. OTM Confederated International Conferences, OTM 2006 Workshops: 352–361, 2006.

[13] K. Wang, C. Chen, W. Fang, T. Wu, "On the security of a new ultra-lightweight authentication protocol in IoT environment for RFID tags," The Journal of Supercomputing, 74(1): 65-70, 2017.

[14] P. Arco and A. Santis, "On ultralight weight RFID authentication protocols," IEEE Transactions on Dependable and Secure Computing, 8(4): 548–563, 2011.

[15] G. Avoine, X. Carpent, B. Martin, "Strong authentication and strong integrity (SASI) is not that strong," in Proc. International Workshop on Radio Frequency Identification: Security and Privacy: 50–64, 2010.

[16] K. Fan, N. Ge, Y. Gong, H. Li, R. Su, Y. Yang, "An ultra-lightweight RFID authentication scheme for mobile commerce," Peer-to-Peer Networking and Applications, 10(2): 368–376, 2016.

[17] D. L. Lin, S. Tsaur, K. Chang, "Lightweight and serverless RFID authentication and search protocol," in Proc. Second International Conference on Computer and Electrical Engineering: 95–99, 2009.

[18] Q. U. Ain, U. Mujahid, M. Najam-ul-islam, "Hardware implementation of ultralight weight cryptographic protocols," presented at the 2015 International Conference on Computing, Communication and Security (ICCCS), Pamplemousses, Mauritius, 2015.

[19] Y. Liao, C. Hsiao, "A secure ECC-based RFID authentication scheme integrated with id-verifier transfer protocol," Ad Hoc Networks, 18: 133-146, 2014.

[20] B. Wang, M. Niset, Y. Ma, H. Nguyen, R. Paul, "Scaling tunneling oxide to 50å in floating-gate logic NVM at 65nm and beyond," in Proc. 2007 IEEE International Integrated Reliability Workshop Final Report: 48–51, 2007.

[21] Y. Ki Lee, L. Batina, D. Singelée, I. Verbauwhede, "Low-cost untraceable authentication protocols for RFID," in Proc. of the third ACM conference on Wireless network security: 55–64, 2010.

[22] C. Tan, B. Sheng, Q. Li, "Secure and serverless RFID authentication and search protocols," IEEE Transactions on Wireless Communications, 7(4): 1400–1407, 2008.

[23] S. Dhal, I. Sengupta, "A new object searching protocol for multi-tag RFID," Wireless Personal Communications, 97(3): 3547-3568, 2017.

[24] M. Safkhani, P. Peris-Lopez, N. Bagheri, M. Naderi, J. Castro, "On the security of tan et al. serverless RFID authentication and search protocols," in Proc. International Workshop on Radio Frequency Identification: Security and Privacy Issues: 1–19, 2013.

[25] Z. Kim, J. Kim, K. Kim, I. Choi, T. Shon, "Untraceable and serverless RFID authentication and search protocols," in Proc. 2011 IEEE Ninth International Symposium on Parallel and Distributed Processing with Applications Workshops: 278–283, 2011.

[26] M. Hoque, F. Rahman, S. Ahamed, J. Park, "Enhancing privacy and security of RFID system with serverless authentication and search protocols in pervasive environments," Wireless Personal Communications, 55(1): 65–79, 2010.

[27] Y. Zuo, "Secure and private search protocols for RFID systems," Information Systems Frontiers, 12(5): 507–519, 2010.

[28] X. Yin, W. Li, "LP0: A RFID authentication protocol for low-cost tags without back-end database," presented at 2012 International Conference on Computer Distributed Control and Intelligent Environmental Monitoring, Hunan, China, 2012.

[29] L. Kulseng, Z. Yu, Y. Wei, Y. Guan, "Lightweight secure search protocols for low-cost RFID systems," presented at the 2009 29th IEEE International Conference on Distributed Computing Systems, Montreal, Canada, 2009.

[30] C. Lv, H. Li, J. Ma, B. Niu, "Vulnerability analysis of lightweight secure search protocols for low-cost RFID systems," International Journal of Radio Frequency Identification Technology and Applications, 4(1): 3–12, 2012.

[31] H. Jialiang, X. Youjun, X. Zhiqiang, "Secure and private protocols for server-less RFID systems," International Journal of Control and Automation, 7(2): 131–142, 2014.

[32] S. Sundaresan, R. Doss, W. Zhou, "A serverless ultra-lightweight secure search protocol for EPC class-1 GEN-2 UHF RFID tags," in Proc. 2012 International Conference on Computer & Information Science (ICCIS), 2: 580–585, 2012.

[33] H. Yoon, H. Youm, "An anonymous search protocol for RFID systems," Journal of Convergence Information Technology, 6(8): 44-50, 2011.

[34] T. Won, J. Chun, D. Lee, "Strong authentication protocol for secure RFID tag search without help of central database," in Proc. 2008 IEEE/IFIP International Conference on Embedded and Ubiquitous Computing, 2: 153–158, 2008.

[35] W. Xie, L. Xie, C. Zhang, Q. Wang, J. Xu, Q. Zhang, C. Tang, "RFID seeking: Finding a lost tag rather than only detecting its missing," Journal of Network and Computer Applications, 42: 135–142, 2014.

[36] S. Jeon, E. Yoon, "An ultra-lightweight RFID seeking protocol for low-cost tags," Applied Mathematical Sciences, 8(125): 6245–6255, 2014.

[37] C. Mtita, M. Laurent, J. Delort, "Efficient serverless radio-frequency identification mutual authentication and secure tag search protocols with untrusted readers," IET Information Security, 10(5): 262–271, 2016.

[38] S. Sundaresan, R. Doss, S. Piramuthu, W. Zhou, "Secure tag search in RFID systems using mobile readers," IEEE Transactions on Dependable and Secure Computing, 12(2): 230–242, 2015.

[39] M. Eslamnezhad Namin, M. Hosseinzadeh, N. Bagheri, A. Khademzadeh, "A secure search protocol for lightweight and low-cost RFID systems," Telecommunication Systems, 67(4): 539–552, 2018.

[40] S. Sundaresan, R. Doss, S. Piramuthu, W. Zhou, "A secure search protocol for low cost passive RFID tags," Computer Networks, 122): 70–82, 2017.

[41] L. Bolotnyy, G. Robins, "Physically unclonable function-based security and privacy in RFID systems," presented at the Fifth Annual IEEE International Conference on Pervasive Computing and Communications (PerCom'07), White Plains, NY, USA, 2007.

[42] C. Mtita, M. Laurent, D. Sauveron, R. Akram, K. Markantonakis, S. Chaumette, "Serverless protocols for inventory and tracking with

a UAV," in Proc. 2017 IEEE/AIAA 36th Digital Avionics Systems Conference (DASC): 1–11, 2017.

[43] Y. Li, J. XIE, Z. MAO, "Secure RFID system based on des encrypt algorithm," Modern Electronics Technique.

[44] M. Feldhofer, S. Dominikus, J. Wolkerstorfer, "Strong authentication for RFID systems using the AES algorithm," in Proc. International Workshop on Cryptographic Hardware and Embedded Systems (CHES 2004): 357–370, 2004.

[45] T. Pham, M. Hasan, H. Yu, "A RFID mutual authentication protocol based on AES algorithm," in Proc. 2012 UKACC International Conference on Control: 997–1002. IEEE, 2012.

[46] R. Doss, W. Zhou, S. Yu, "Secure RFID tag ownership transfer based on quadratic residues," IEEE Transactions on Information Forensics and Security, 8(2): 390–401, 2013.

[47] Y. Huang, C. Yuan, M. Chen, W. Lin, H. Teng, "Hardware implementation of RFID mutual authentication protocol," IEEE Transactions on Industrial Electronics, 57(5): 1573–1582, 2010.

[48] L. Batina, J. Guajardo, T. Kerins, N. Mentens, P. Tuyls, I. Verbauwhede, "An elliptic curve processor suitable for RFID-tags," in Proc. 1st Benelux Workshop on Information and System Security: 1-17, 2006.

[49] A. Juels, S. Weis, "Authenticating pervasive devices with human protocols," in Proc. Annual International Cryptology Conference: 293–308, 2005.

[50] Y. Ki Lee, K. Sakiyama, L. Batina, I. Verbauwhede, "Elliptic-curve-based security processor for RFID," IEEE Transactions on Computers, 57(11): 1514–1527, 2008.

[51] P. Urien, S. Piramuthu, "Elliptic curve-based RFID/NFC authentication with temperature sensor input for relay attacks," Decision Support Systems, 59): 28–36, 2014.

[52] Y. Liao and C. Hsiao, "A secure ECC-based RFID authentication scheme integrated with id-verifier transfer protocol," Ad Hoc Networks, 18: 133–146, 2014.

[53] M. Feldhofer, C. Rechberger, "A case against currently used hash functions in RFID protocols," in Proc. In OTM Confederated International Conferences: 372–381, 2006.

[54] M. Bellare, C. Namprempre, "Authenticated encryption: Relations among notions and analysis of the generic composition paradigm," in Proc. International Conference on the Theory and Application of Cryptology and Information Security: 531–545, 2000.

[55] A. Adomnicai, J. Fournier, L. Masson, "Masking the lightweight authenticated ciphers acorn and ASCON in software," Cryptography and Information Security in the Balkans.

[56] H. Groß, E. Wenger, C. Dobraunig, and C. Ehrenhöfer, "Suit up!–made-to-measure hardware implementations of ASCON," in Proc. 2015 Euromicro Conference on Digital System Design: 645–652, 2015.

[57] G. Zhou, H. Michalik, L. Hinsenkamp, "Efficient and high-throughput implementations of AES-GCM on FPGAs," in Proc. 2007 International Conference on Field-Programmable Technology: 185–192, 2007.

[58] M. Dworkin, "Recommendation for block cipher modes of operation: The CCM mode for authentication and confidentiality," National Institute of Standards and Technology, U.S. department of commerce, Technical report, 2004.

[59] D. McGrew, J. Viega, "The security and performance of the galois/counter mode (GCM) of operation," in Proc. International Conference on Cryptology in India: 343–355, 2004.

[60] S. Cogliani, D. Maimuţ, D. Naccache, R. Canto, R. Reyhanitabar, S. Vaudenay, D. Vizár, "OMD: A compression function mode of operation for authenticated encryption," in Proc. International Conference on Selected Areas in Cryptography: 112–128, 2014.

[61] Y. Niwa, K. Ohashi, K. Minematsu, T. Iwata, "CM security bounds reconsidered," in Proc. International Workshop on Fast Software Encryption: 385–407, 2015.

[62] P. Rogaway, T. Shrimpton, "A provable-security treatment of the key-wrap problem," in Proc. Annual International Conference on the Theory and Applications of Cryptographic Techniques: 373–390, 2006.

[63] M. Saarinen, "Cycling attacks on GCM, GHASH and other polynomial macs and hashes," in Proc. International Workshop on Fast Software Encryption: 216–225, 2012.

[64] S. Neves J. Aumasson, P. Jovanovic, "NORX V2.0,".

[65] H. Wu, "ACORN: A lightweight authenticated cipher,".

[66] C. Dobraunig, M. Eichlseder, F. Mendel, M. Schläffer, "ASCON v1. 2," Submission to the CAESAR Competition.

[67] T. Peyrin, J. Jean, I. Nikolic. 2015, Joltik v1.3, CAESAR Round 2 submission.

[68] J. Guo, T. Peyrin, A. Poschmann, "The photon family of lightweight hash functions," in Proc. Advances in Cryptology (CRYPTO 2011): 222–239, 2011.

[69] G. Leander, C. Paar, A. Poschmann, K. Schramm, "New lightweight DES variants," in Proc. International Workshop on Fast Software Encryption: 196–210, 2007.

[70] K. Ouafi, R. Phan, "Privacy of recent RFID authentication protocols," in Proc. International Conference on Information Security Practice and Experience: 263–277, 2008.

[71] S. Mandal, S. Mohanty, B. Majhi, "Universally verifiable certificateless signcryption scheme for MANET," in Proc. International Conference on Microelectronics, Computing & Communication Systems: 77–89, 2018.

[72] Y. Boichut, P. Héam, and O. Kouchnarenko, "Automatic approximation for the verification of cryptographic protocols," in Proc. AVIS, 2004.

[73] D. Basin, S. Mödersheim, L. Vigano, "OFMC: A symbolic model checker for security protocols," International Journal of Information Security, 4(3): 181–208, 2005.

[74] A. Armando, L. Compagna, "An optimized intruder model for SAT-based model-checking of security protocols," Electronic Notes in Theoretical Computer Science, 125(1): 91–108, 2005.

[75] M. Turuani, "The CL-ATSE protocol analyzer," in Proc. International Conference on Rewriting Techniques and Applications: 277–286, 2006.

[76] M. Burrows, M. Abadi, R. M Needham, "A logic of authentication," in Proc. Royal Society of London A: Mathematical, Physical and Engineering Sciences, 426: 233–271, 1989.

[77] H. Martn, E. Millán, L. Entrena, P. Lopez, J. Castro, "AKARI-x: a pseudorandom number generator for secure lightweight systems," presented at the 2011 IEEE 17th International On-Line Testing, Athens, Greece, 2011.

[78] S. Sundaresan, R. Doss, S. Piramuthu, W. Zhou, "Secure tag search in RFID systems using mobile readers," IEEE Transactions on Dependable and Secure Computing, 12(2): 230-242, 2014.

[79] R. Wessel, "Airbus signs contract for high-memory RFID tags," RFID Journal: 1-2 2010.

[80] D. Dressen, "Large memory RFID system solutions," ATMEL Applications Journal: 48–49.

[81] M. Hossain. S. Ahamed, "Towards a simple secured searching protocol for future RFID applications," presented at the 12th IEEE

International Workshop on Future Trends of Distributed Computing Systems, Kunming, China, 2008.

[82] J. Chun, J. Hwang, D. Hoon Lee, "RFID tag search protocol preserving privacy of mobile reader holders," IEICE Electronics Express, 8(2): 50–56, 2011.

Biographies

Mojtaba Eslamnezhad Namin received the Ph.D. in Computer Systems Architecture from Science and Research Branch, Islamic Azad University, Tehran, Iran in 2017. His current research interests are cryptography, network security, IoT and WSN.

Mehdi Hosseinzadeh was born in Dezful in 1981. He received his B.Sc. in Computer Hardware Engineering from Islamic Azad University, Dezful Branch, in 2003. He also received the M.Sc. and Ph.D. degrees in Computer Systems Architecture from Science and Research Branch, Islamic Azad University, Tehran, Iran in 2005 and 2008, respectively. He is currently an Assistant Professor in Iran University of Medical Sciences, Tehran, Iran and University of Human Development, Sulaimaniyah, Iraq. His research interests are computer arithmetic with emphasis on residue number system, cryptography, network security and e-commerce.

Nasour Bagheri is an associate professor at Electrical Engineering Department, Shahid Rajaee Teacher Training University, Tehran, Iran. He is the author of over 100 articles in information security and cryptology. Homepage of the author is available at: https://sites.google.com/view/nasour-bagheri.

Ahmad KhademZadeh received the B.Sc. degree in applied physics from Ferdowsi University, Mashhad, Iran, in 1969 and the M.Sc. and Ph.D. degrees respectively in Digital Communication and Information Theory and Error Control Coding from the University of Kent, Canterbury, U.K. He is currently the head of Education and National Scientific and Informational Scientific Cooperation Department at Iran Telecom Research Center (ITRC). He was the head of Test Engineering Group and the director of Computer and Communication Department at ITRC. He is also a lecturer at Tehran Universities and he is a committee member of Iranian Computer society and also a committee member of the Iranian Electrical Engineering Conference Permanent Committee. Dr. KhademZadeh has been received four distinguished national and international awards including Kharazmi International Award, and has been selected as the national outstanding researcher of the Iran Ministry of Information and Communication Technology.

How to cite this paper:

M. Eslamnezhad Namin, M. Hosseinzadeh, N. Bagheri, and A. Khademzadeh, "RSPAE: RFID search protocol based on authenticated encryption" Journal of Electrical and Computer Engineering Innovations, 6(2): 185-198, 2018.

DOI: 10.22061/JECEI.2019.5186.199

URL: http://jecei.sru.ac.ir/article_1105.html