A Secure Lightweight Authentication Scheme for RFID Systems in IoT Environment

Received: 30 January 2023; Accepted: 10 March 2023 *Research Article*

Md. Monzur Morshed
Department of Computer Science and Engineering
Daffodil International Univerrsity
Dhaka, Bangladesh
monjur.morshed@diu.edu.bd

Hongnian Yu
School of Computing Engineering and the Built Environment
Edinburgh Napier University
Edinburgh, UK
hongnianyu@uic.edu.cn
0000-0003-2894-2086

Anthony S. Atkins
School of Computing and Digital Technologies Staffordshire University
Stafford, UK
a.s.atkins@staffs.ac.uk
0000-0002-8447-4822

***Abstract*— Radio Frequency Identification (RFID) technology is suitable for IoT applications. RFID is cheap and light weight and hence it is very popular in IoT technology. The concern of research community is the privacy and security issue of RFID system. Due to low storages of RID tag it a challenging research problem to ensure privacy and security such as data visibility, loss, modification, eavesdrop etc. In this paper we propose a new RFID authentication protocol for RFID system. It ensures privacy and security in IOT environment in a more efficient way. To ensure better security we use a different password for each tag and it changes after each authentication process. It also can protect from an unexpected lack of synchronization in case an incomplete authentication is held for any unwanted problem in authentication phase. The proposed protocol shows some relatively superior performance in some aspects of computation and storages.**

Keywords*— RFID security, IoT, privacy, recovery, authentication

I. INTRODUCTION (*HEADING 1*)

Various types of sensors and RFID technology are the essential component in the present deployment of IoT. RFID tags are used in many applications now a days. It is used in automation of automobiles, logistics management, toll collection in roads, animal tracking, etc [1][2]. The RFID tag is used as Electronic Product Code (EPC). It is standardized by EPCglobal Inc [3]. Due to thee small size and low-cost of the RFID tag it is used to identify items or objects automatically. An RFID system typically consists of three components. These are tag, reader and database in the back-end[4].

There are two types of RFID tags: active and passive. Typically passive tags are inexpensive where as active tag contains batteries to power their transmission. An RFID tag comprises a unique code as identity which can be used to identify any item or object. Using this unique code in an RFID tag it is possible to track the tag uniquely. Typically the code and information in RFID tags are transmitted in plaintext. In IoT environment the information in the tags may contain sensitive data. But without proper security protections this system may be less attractive for many practical applications [1]. The main challenge to ensure security is that, employment of traditional cryptography is not applicable in a low-cost, small size and lightweight passive RFID tags[5].

The paper aims the goal to develop a new scheme to solve these issues and to offer an efficient and secure protocol for RFID systems which can overcome from de-synchronization for any incomplete authentication and abnormal termination.

This paper aims to develop a new authentication scheme using a password that is changed after each authentication. The identifier and secret password are exchanged with lightweight encryption and light-weight hash function using random numbers so that the code and secret transmitted by the RFID systems are anonymous. In this way the scheme aims to ensure the privacy and security of RFID systems of the issues outlined above. It specially aims to ensure location privacy and recovery in case of desynchronization discussed above with less computation. The main contributions of the proposed scheme are:

(1) To develop a secure and light weight authentication scheme for RFID system

(2) Resist all known attacks like tracing, impersonation, information leakage etc.

(3) RFID tag identifier and secret password are always encrypted and hashed so that tag ID is never disclosed.

(4) To ensure less computation, storage and lower communication cost.

(5) To ensure synchronization in the case of communication failure.

The rest of the paper is organized as in following sections. In Section II the model for security and privacy for RFID systems and performance criteria are explained for the RFID systems. In Section III related works are outlined. Section IV presented the proposed protocol. In this Section the protocol is also explained together with a recovery example in the case of abnormal termination of the authentication. The performance, privacy and security of the scheme is evaluated in Section V. In Section VI the analysis and the result of simulation are outlined. The conclusion is placed finally in section VII.

II. PRIVACY AND SECURITY OBJECTIVES FOR RFID

To ensure privacy or security of the contents of the RFID tag there are several goals are identified. The objective of security protocols are to keep the data secret and to protect data during the transmission between the tag and the reader from tentative attacks.

- **Information leakage:** Every tag in an RFID system has a unique code and other data that are transmitted to the system. Due to this unique code it can be easily identified and the data may be leaked. To ensure the protection from the leakage of information of both identity and data, an RFID system requires security protection so that unauthorized person or adversary cannot access any information from the tag.
- **Traceability and Location privacy:** Sometimes it is enough to harm if any how it can be tracked or linked with any person to a tag. When a transmitter sends any fixed response to a receiver, an attacker may differentiate and identify the response. After this it may track the location of the user.
- **Mutual authentication**: Authentication of the tag and the reader with each other is done by transmitting their code and other secret with each other. If they are matched with their own information then they authenticate each other.
- **Impersonation and Forward security**: An adversary may collect the code and data during transmission between the tag and the reader. If any data can be identified it can be used to impersonate the tag to exploit in future.
- **Message Interception or denial of service (DoS):** An adversary sometimes may initiate to prevent communication between the tag and the reader. If the adversary is successful to interfere the transmission then it can cause de-synchronization between the server and the tag.

III. Related Works

There are different types of RFID authentication schemes to ensure privacy and security in an RFID system. Many schemes work with static code and few other work with varying code or secret.

In [6, 7, 8] the authors proposed various protocols that work with static codes to ensure security or privacy. The advantage of these schemes in pervasive computing environment is that it is easy to work and manage since it does not face any synchronization challenges. Molnar et al. [6] presented a novel authentication scheme to implement in a library system. To ensure anonymity and privacy it utilizes a pseudorandom number and secret key shared by the tag and the reader. In this scheme the code and the secret are fixed and the random number transmitted in plain text which can be a cause to break the privacy of the tag by the adversary.

In [7] Rhee et al. also outlines a mutual RFID authentication protocol (CRAP). This protocol also used fixed code or identifier suitable in IoT pervasive computing. However, hash functions computations makes the scheme inefficient for a large number of tags in pervasive computing of IoT.

In [8] Choi et al. presented another protocol with static identifier which is hash based low-cost and sized authentication scheme. It is also suitable for pervasive environment like IoT. This scheme is not appropriate to protect from impersonation attack and traceability attack for its counter parameter used in the scheme [9].

Ohkubo et al. [10] presented a privacy scheme for RFID system using a hash chain (HC) method. The method utilized two one-way hash functions to ensure privacy and security. However, it is not suitable in practical situation due to the uses of a large number of hash chains in back-end database.

To ensure the privacy and security of the RFID systems in an effective manner varying coder or secrets are used in some authentication schemes. This paper listed few of the schemes using varying codes and secret for the authentication process presented as follows:

Few of early researchers have also proposed authentication schemes to ensure privacy and security of RFID systems using varying codes or secrets [11, 12, 13, 14]. These are protected against many attacks. Due to varying codes they include the recovery process for accidental de-synchronization or incomplete authentication process. However, the hash function is used from the identifier only. If any authentication phase is incomplete, an unauthorized user can take the responses for the next phase to break the security. Hence the unauthorized user can intentionally use the collected information to use for man-in-the middle attack and it can also be a threat for location privacy.

Chien and Chen [11] presented a mutual authentication protocol to ensure protection from a replay attack. To ensure synchronization this protocol uses a database to store new and previous key values of the tag which can prevent from a DoS attack. The authentication key and access keys are always updated and hence prevent a traceability. However, this protocol is vulnerable to forward and backward traceability. If an adversary can capture the information from a tag it can trace the previous interactions of the tag from previous transmission and the identifier of the tag. By using the immediate previous transaction and identifier it may be possible to recognise any transaction in future.

Another hash-based identifier variation scheme (HIDV) is presented by Henrici et al. [12] which utilizes a hash function to prevent location privacy by altering the identifier after each successful session. However, if any session is terminated incompletely an adversary can use the same hashed response for which it may open the risk for impersonation attack say spoofing.

Lee et al. [13] also proposed an authentication scheme that improves and simplifies the HIDV scheme in security and efficiency. It also has the same limitation as in HIDV scheme that a tag always uses the same hashed response before the next authentication allows tracking the tag.

Dimitriou [15] introduced an RFID authentication scheme to protect the privacy and security. It also protects against cloning of the tag. This scheme also uses the hash function of the id to a reader and it maintains scalability at the server. The back-end server replies the message with the altered new identifier to the tag after receiving the response from the tag. This scheme also has the problem of tracking due to the fact that between valid sessions, the tag id remains the same.

Song and Mitchell [14] presented an authentication scheme for RFID system and also introduced a protocol for an ownership transfer [16] to prevent from all attacks. These protocols show better efficiency in terms of storage and computation. However these are vulnerable to impersonation attack for both the tag side and reader side.

Hoque et al. [17] introduced an authentication protocol that also supports both security, privacy and recovery of id in RFID systems. The protocol also can synchronize the value of tags and readers and thus ensures robustness. This protocol is expensive in as it requires a large number of hash functions and computations.

Cai et al. [18] presented an enhanced version of authentication protocol described in [8] to overcome the limitations by retaining all the security and privacy protections. The modified protocol also uses almost similar storage and computation requirements as in the previous protocol.

Shafiq et al.[19] proposed a new protocol for varying identifier, random number and low-cost operation like XOR, Rot and new function Rank to guarantee privacy and security for the RFID tag and reader. However, the IDS information is transmitted in plaintext which may be tracked by an unauthorized user.

Peris-Lopez et al. in [20–22] proposed various lightweight protocols RFID systems to ensure privacy and security. The protocols outlined in these papers are LMAP, $M2$AP, and EMAP. The protocols are efficient and utilized low-cost operations like bitwise OR, XOR, and $sum\ mod$ operations. However, these protocols are also vulnerable at security attack and de-synchronization [23, 24].

In LPCP [25], an enhanced security scheme of RAPP [26] is proposed to overcome the weakness in security. To improve security performance, the protocol also uses a mechanism of secret key backup. However, the RAPP protocol is still insecure against de-synchronization attacks.

In [27], another new authentication scheme for RFID is proposed. The Ultra-lightweight protocol SLAP uses simple bitwise XOR, rotate with left circular Rot$(\cdot,\cdot)$ and $Con(\cdot,\cdot)$ for conversion operations. For implementation of these operations the inexpensive passive tags were appropriate. However, the protocol is vulnerable against various attacks like traceability, de-synchronization and replay attacks.

Liu et al. [28] utilizes Shamir's $(2, n)$ ultra lightweight scheme UMAPSS for RFID authentication. The scheme can protect the system from the known security problem efficiently.

In [29], a lightweight authentication protocol IOLAS for passive RFID tags is introduced. The scheme can ensure all known security protection efficiently.

In [30] Xiao et al. presented a block cipher-based RFID authentication protocol named LRSAS. The author claimed The protocol guarantees all known security protection efficiently but Trinh et al. [31] reported that the protocol is susceptible to de-synchronization and secret disclosure attacks.

Some other schemes [32][33][34],[35] and [36] use almost similar lightweight encryption and showed relatively better performance but with a cost of compromising few security protections.

An essential research objective is to formulate a security scheme for RFID technology in IoT environment that addresses the issues and solve these problems efficiently with limited capability in computation and storage of an RFID tag.

IV. Our Contribution: A Secure Lightweight Authentication Scheme (SLAS)

In this section, a new scheme (SLAS) is proposed. The notations used in this protocol are as follows:

Notations

h	hash function
l	The length
r_1	First Random number
r_2	Second Random number
ID	Tag Code / Identifier
X	variable Secret
S	Secret number
$A = A_L \| A_R$	
$B = B_L \| B_R$	
$\oplus$	Bitwise XOR
$\|$	Concatenation
$\leftarrow$	Assignment

Tag Initialization

Tag: Each tag contains three fields:

ID: Tag Code/ Identifier
X: Variable Secret
S: Helping Secret

Reader: Reader contains no field. It uses the data from database.

Database Initialization: The database has four fields:
ID: Tag Code/ identifier
X: Variable Secret
S: Helping Secret
X_{prev}: X in previous phase

Operations in SLAS Scheme

If a tag approaches within the range of any reader, the session of authentication scheme is initiated. The scheme is outlined in Fig.1. The steps in the scheme are as follows.

Step 1: A reader generates the first random number (r_1) and transmits a request with it to the tag.

Step 2: With the response from the reader the tag generates second random number (r_2).

It then computes

$$A \leftarrow h(ID \| r_1 \| r_2)$$
$$C \leftarrow X \oplus r_2$$
$$P \leftarrow S \oplus C$$

.

Step 3: The tag replies with the values A_L, C and P to the targeted reader.
The reader transmits this data to its database.

Step 4. The database side then computes

$$P' \leftarrow S \oplus C \quad \text{for all S}$$
$$if \quad P = P' \quad Computes$$

$r_2 \leftarrow X \oplus C$ and $A' \leftarrow h(ID \| r_1 \| r_2)$

if $A'_L = A_L$

ID of *the* tag is authenticated.

For next session

$X_{prev} \leftarrow X$ *and*

$X \leftarrow h(X, r_2)$.

$B \leftarrow h(ID \| X \| r_1 \| r_2)$

else *if* $A'_L \neq A_L$

Computes

$r_2 \leftarrow X_{prev} \oplus C$ and

$A' \leftarrow h(ID \| r_1 \| r_2)$

if $A'_L = A_L$

ID of *the* tag is authenticated.

For next session

$X_{prev} \leftarrow X_{prev}$ *and*

$X \leftarrow h(X_{prev}, r_2)$

$B \leftarrow h(ID \| X \| r_1 \| r_2)$

else ignore the message and

Computes $B \leftarrow unknown$

Step 5. The reader replies with B_R to its tag.

6. *T*he tag then performs the following operations:

$XT \leftarrow h(X, r_2)$ $B' \leftarrow h(ID \| XT \| r_1 \| r_2)$

if $B'_R = B_R$ the tag authenticates and updates

$X \leftarrow XT$

Database *ID, S, X, X_{prev}*		Reader		Tag *ID, X, S*
			Request, r_1	Generate random number r_2 $A \leftarrow h(ID \| r_1 \| r_2)$ $C \leftarrow X \oplus r_2$ $P \leftarrow S \oplus C$
Computes for all S $P' \leftarrow S \oplus C$ *if* $P = P'$ *Computes* $r_2 \leftarrow X \oplus C$ and $A' \leftarrow h(ID \| r_1 \| r_2)$ *if* $A'_L = A_L$ *ID* of *the* tag is authenticated. For next session $X_{prev} \leftarrow X$ *and* $X \leftarrow h(X, r_2)$. $B \leftarrow h(ID \| X \| r_1 \| r_2)$ else *if* $A'_L \neq A_L$ Computes $r_2 \leftarrow X_{prev} \oplus C$ and $A' \leftarrow h(ID \| r_1 \| r_2)$ *if* $A'_L = A_L$ *ID* of *the* tag is authenticated. For next session $X_{prev} \leftarrow X_{prev}$ *and* $X \leftarrow h(X_{prev}, r_2)$ $B \leftarrow h(ID \| X \| r_1 \| r_2)$ else ignore the message and Computes $B \leftarrow unknown$	A_L, C, P ←		A_L, C, P ←	
	B_R →		B_R →	$XT \leftarrow h(X, r_2)$ $B' \leftarrow h(ID \| XT \| r_1 \| r_2)$ *if* $B'_R = B_R$ then the tag authenticates and perform $X \leftarrow XT$

Fig. 1. Proposed SLAS Scheme

V. ANALYSIS AND EVALUATION

In the process of evaluation of the proposed scheme the privacy, security and efficiency are considered for analysis. It was a challenging task to select various existing authentication schemes to compare performance with tour proposed SLAS scheme. The proposed scheme SLAS has been compared with various existing and relatively recent protocols having good performance ultra-lightweight RFID authentication schemes. These selected scheme are URASP [8], ESRAS[19], IOLAS [29], RSAS [30], RAPP [31],RAPLT [32], SLAP [38], LMAP [41], *M*2AP [42], EMAP [43], LPCP [44], David–Prasad [54], RRAP [56], and URMAP [58]. Most of these protocols require relatively lower cost and storage in comparison to other protocols those are not selected.

A. ANALYSIS OF PRIVACY AND SECURITY

To evaluate the privacy and security we selected the threats [19] discussed in section II. It is shown in TABLE II.

Information leakage: In this protocol the information is either transmitted in a hash function. Without knowing the value of ID, X, S an adversary cannot authenticate. The value of ID is always hashed with a function when transmitted.

$$A \leftarrow h(ID \parallel r_1 \parallel r_2)$$
$$C \leftarrow X \oplus r_2$$
$$P \leftarrow S \oplus C$$

The value of X and S are transmitted using XOR but the value of X is updated by a hash function after every authentication phase.

$$X \leftarrow h(X, r_2)$$

The combination of r1 and r2 with X, S and ID produces an unpredictable response so that the adversary cannot access any information. In can only guess with a costly computation with negligible probability $\frac{1}{2^l}$.

Mutual authentication: In the proposed mutual authentication with the tag and reader is done by a very strict privacy and security mechanism. The reader server authenticate by the secure transmitted message part by comparing the expression $A'_L \neq A_L$

The tag also authenticate by the secure transmitted message part by comparing the expression $B'_R = B_R$

In this way the mutual authentication is established in the tag and the reader in a secure way.

Location privacy: The information transmitted by A cannot be tracked with any targeted tag. Two new random numbers r1, r2 are generated in every authentication process and the value of X also updated by using random number and hash function as follows:

$$A \leftarrow h(ID \parallel r_1 \parallel r_2)$$
$$C \leftarrow X \oplus r_2$$
$$P \leftarrow S \oplus C$$
$$X \leftarrow h(X, r_2)$$

In a simulation program the anonymity of the response are tested and found the tracking and location privacy breaking is not possible. Even if an adversary sends the same random number r1 many times it ensures anonymity in each session by transmitting new values of r2 and X.

Impersonation and Forward security: The scheme follows a complete challenge-response method using mutual authentication. Without accessing the value of tag code (ID), two secrets X and S an adversary cannot impersonate.

$$A \leftarrow h(ID \parallel r_1 \parallel r_2)$$

In each session the tag and reader generates new responses of A and B using two fresh random numbers. These are fully indistinguishable from other response in other sessions hence he impersonation are not possible and forward security is ensured.

$$B' \leftarrow h(ID \parallel XT \parallel r_1 \parallel r_2)$$

Message interception: The scheme can recover from the abnormal interruption can be synchronized automatically. If the last transmission is interrupted then in the subsequent authentication session the database side can use the older value Xprev using random numbers to authenticate and synchronous the system.

$$X \leftarrow h(X_{prev}, r_2)$$
$$B \leftarrow h(ID \parallel X \parallel r_1 \parallel r_2)$$

Forward security: The proposed protocol uses varying secret in each successful new session. So the scheme ensures the privacy and security of the past communications in case the tag is compromised by an unauthorized reader. It cannot discover previous secret and random number. Moreover the ID is never transmitted in plain text. Also the adversary cannot get access of future data and secret.

B. EFFICIENCY ANALYSIS

In this paper the communication cost, computation cost and storage cost were chosen for analysis of efficiency. The low-cost small sized tag has very limited computational and communication ability. The objective of the scheme is to minimize storage and computational and communication capacity requirements. By considering these issues the proposed SLAS scheme gives the performance as in Table II.

Computation cost: The proposed scheme does not use CRC, traditional high cost encryptions or decryptions. It uses simple bitwise XOR and lightweight hash function.

Communication cost: Another objective of the RFID authentication scheme is to reduce the communication cost sent by the tag. It denotes the number of transmitted data from the tag side in each authentication phase. It is assumed that all the field have same length of L. In our proposed scheme the communication cost from tag is 2.5L.

Storage Costs: For identification and authentication purpose the tag stores ID, secret and some other shared information. The objective is to optimize the memory space in tag by ensuring all the security issues discussed. The proposed scheme requires a total three parameters including its ID and two secrets X and S. So the storage size requirement in the tag is 3L.Tt requires relatively less storage in tag and in database side than some schemes and offers protection from all threats discussed in section II. The storage cost in the database side is 4L.

TABLE I. SECURITY AND PRIVACY COMPARISON AUTHENTICATION SCHEMES.

Scheme	Mutual authentication	Forward Security	Tracking Prevention	Synchronization	Leakage Protection	Diffusion function Security
URASP [8]	*Yes*	X	*Yes*	*Yes*	*Yes*	*Yes*
IOLAS [29]	*Yes*	*Yes*	X	*Yes*	X	X
LRSAS [30]	*Yes*	*Yes*	*No*	*Yes*	X	X
RAPP [31]	*N*	*Yes*	*No*	*N*	*Yes*	*Yes*
RAPLT [32]	*N*	*Yes*	*No*	*No*	*Yes*	X
SLAP [38]	*Yes*	*Yes*	*Yes*	*No*	*Yes*	*Yes*
LAMP [41]	X	*No*	*No*	*No*	*No*	X
M^2AP [42]	X	*No*	*No*	*No*	*No*	X
EMAP [43]	X	*No*	*No*	*No*	*No*	X
LPCP [44]	*Yes*	X	*Yes*	*No*	*Yes*	X
David-Prasad [54]	X	*N*	*N*	X	*N*	X
R^2AP [56]	*Yes*	*Yes*	*Yes*	*Yes*	*Yes*	*N*
URMAP [58]	*Yes*	X	*Yes*	X	*Yes*	*Yes*
ESRAS[19]	*Yes*	*Yes*	*Yes*	*Yes*	*Yes*	*Yes*
SLAS(Proposed)	*Yes*	*Yes*	*Yes*	*Yes*	*Yes*	*Yes*

Database computation and complexity: The scheme requires less hash function computations in database. It does not computes hash unnecessarily to match the ID rather it initially checks the secret and then verify the hash function.

VI. SIMULATION RESULTS

The following simulations were conducted to verify few aspects of the security.

Scyther Simulation

To test the idea in a simulated environment Scyther Simulation tool is used. It is a GUI-based tool to verify security performance of the protocols [37]. For the experiment Scyther Simulation tool is installed in a Desktop computer in Windows 10 platform. It is suitable for challenge-response authentication system. The language used here is called Security Protocol Description language(SPDL). The basic requirements for this authentication protocol such as random number generation, encryption, hash functions, send response, verifications can be performed. For example a random number can be generated using fresh declaration. In our simulation r1 and r2 and fresh type. For one-way encryption process hash function can be used. Other necessary encryption function can be declared using special predefined type Function. Some popular events are

send to send response
recv to receive response

claim to specify role to model intended security property. Some predefined claims are

Alive to check if it is alive
Secret Secrecy of a parameter is checked
Niagree Non-injective agreement
Nisynch Non-injective synchronisation
Weakagree Weak agreement

match to match pattern

Other than this a macro can be used to simplify and or abbreviation of complex term.

The result of the simulation is given in Fig.3. From the result it is shown that all the status are OK which means under the assumptions of the scheme and the protocol the SLAS is secure from the attacks and it resist all the active and passive threats.

VII. CONCLUSION

In case of a RFID system the security and privacy issue is very a challenging issue due to small memory size and computation capability of the low-cost tag. A novel authentication scheme SLAS has been proposed to protect privacy and security for RFID systems. Several security issues such as information leakage, eavesdrop, tampering, replay attack, modification and tracking are most concerns. Our proposed protocol works on these issue to protect the system using low cost and lightweight RFID. The protocol uses lightweight hash function for computation of identifier and secret using two random numbers. So the transmitted signal is fully protected from information leakage and tracking. It is secured from message interception and location privacy and ensures forward security by changing the secret number after each authentication process. The proposed scheme requires three one-way hash computations and one bitwise XOR function which makes it highly efficient for a large range of security protection in RFID system. The storage requirement for the tag is reasonably less for the overall security protection from all threats. The performance analysis shows that the SLAS scheme is both secure and relatively efficient in comparison to the selected schemes.

```
const XOR:Function;
hashfunction h;

protocol Myproposed(Tag, Reader)
{
   //SPDL part for Tag role
   role Tag
    {
        const  ID,X,X',AL,B,BR,B'R,XT, r1;
        fresh r2:Nonce;
         recv_!1(Reader, Tag, r1);
         macro A=h(ID, r1,r2);
         macro C=XOR(X,r2);
         send_!2(Tag, Reader, AL,C,r2);
         recv_!3(Reader, Tag, BR);
               macro XT=h(X,r2);
               macro B'=h(ID,XT,r1,r2);
               match(B'R,BR);
               claim(Tag, Secret, ID);
               claim(Tag, Secret, X);
               claim(Tag, Secret, r2);
               claim(Tag, Niagree);
               claim(Tag, Nisynch);
               claim(Tag, Nisynch);
               claim(Tag, Alive);
               claim(Tag, Weakagree);
          }

      //SPDL part for Reader role
        role Reader
          {
              const ID, X,Xprev,r2,AL,A'L,BL,BR;
               fresh r1:Nonce;
               send_!1( Reader,Tag, r1);
               recv_!2(Tag,Reader, AL,C,r2);
               macro r2=XOR(X,C);
               macro A'=h(ID, r1,r2);
               match(A'L,AL);
               macro Xprev=X;
               macro X=h(X,r2);
               macro B=h(ID,X,r1,r2);
               send_!3( Reader,Tag,BR);
               claim(Reader, Secret, ID);
               claim(Reader, Secret,X);
               claim(Reader, Secret, r2);
               claim(Reader, Niagree);
               claim(Reader, Nisynch);
               claim(Reader, Alive);
               claim(Reader, Weakagree);
          }
     }
```

Fig. 2. SPDL for the Tag and the Reader

TABLE II. PERFORMANCE COMPARISON AMONG VARIOUS AUTHENTICATION SCHEMES.

Criteria / Scheme	Number of messages (Total)	Communication messages (Tag)	Storage cost (Tag)
URASP [8]	**4*L***	**1.5*L***	**4*L***
IOLAS [29]	**4*L***	**2*L***	**5*L***
LRSAS [30]	**5*L***	**2*L***	**3*L***
RAPP [31]	**5*L***	**2*L***	**5*L***
RAPLT [32]	**4*L***	**3*L***	**5*L***
SLAP [38]	**4*L***	**1.5*L***	**7*L***
LAMP [41]	**4*L***	**2*L***	**6*L***
M^2AP [42]	**4*L***	**3*L***	**6*L***
EMAP [43]	**4*L***	**3*L***	**6*L***
LPCP [44]	**5*L***	**2*L***	**5*L***
David-Prasad [54]	**5*L***	**3*L***	**5*L***
R^2AP [56]	**5*L***	**2*L***	**5*L***
URMAP [58]	**4*L***	**2*L***	**5*L***
ESRAS	**5*L***	**1.5*L***	**5*L***
SLAS(Proposed)	**3L**	**2.5L**	**3L**

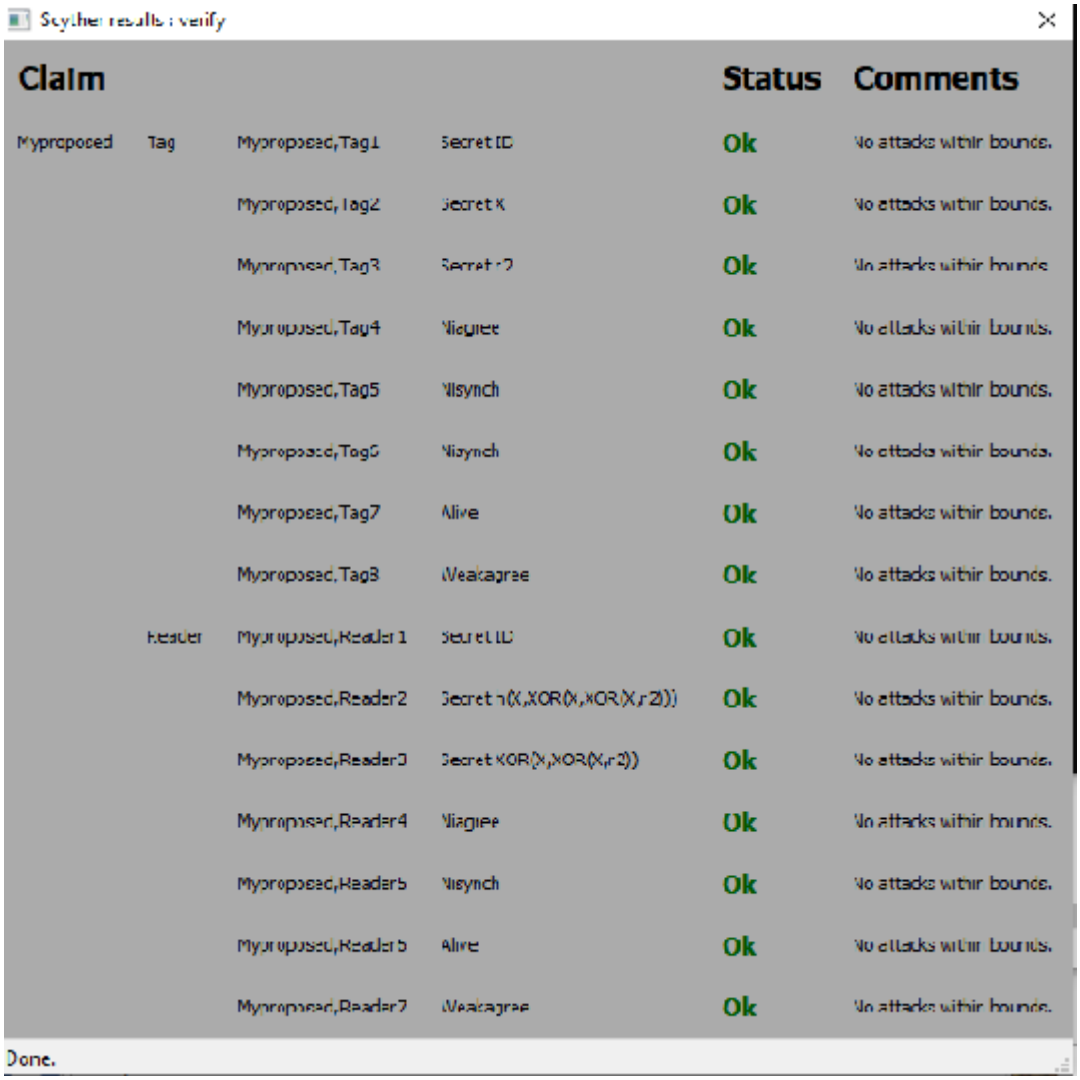

Fig. 3. Scyther Simulation Result for proposed SLAS

REFERENCES

[1] A. Jules,S. Garfinkel, and R. Pappu, "RFID privacy: an overview of problems and proposed solutions," IEEE Security and Privacy. 3(3): 34-43, May/June 2005.

[2] A. Jules, "RFID security and privacy: A research survey," IEEE Journal on Selected Areas in Communication, 24(2), February 2006.

[3] EPCglobal Web site, 2005. Referenced 2005 at http://www.EPCglobalinc.org.

[4] R. Want,"An Introduction to RFID Technilogy," IEEE Pervasive Computing, vol. 5, pp. 25 – 33, 2005.

[5] B. S. Prabhu, X. Su, H. Ramamurthy, C. Chu, R. Gadh, "WinRFID – A Middleware for the enablement of Radio Frequency Identification (RFID) based Applications," UCLA - Wireless Internet for the Mobile Enterprise Consortium (WINMEC)420 Westwood Pl., Los Angeles CA 90095.

[6] D. Molnar and D. Wagner, "Privacy and security in library RFID: Issues, practices, and architectures," In B. Pfitzmann and P. Liu, editors, Conference on Computer and Communications Security - ACM CCS, pages 210–219, Washington, DC, USA, October 2004. ACM Press.

[7] K. Rhee, J. Kwak, S. Kim and D. Won, "Challenge-Response Based RFID Authentication Protocol for Distributed Database Environmnet," SPC 2005, LNCS 3450, pp. 70-84, 2005.

[8] E.Y. Choi, S.M. Lee, D.H. Lee, "Efficient RFID Authentication Protocol for Ubiquitous Computing Environment," Embedded and Ubiquitous Computing, vol.3832, pp.945-954, 2005.

[9] J. Zhi-Wei , S. Xiao-yan, H. Lee and Z. Tao, "A Revised One-way Hash based Low-cost Authentication Protocol In RFID System," Wireless Communications, Networking and Mobile Computing, 2009. WiCom '09. 5th International Conference, Page(s): 1 – 4.

[10] M. Ohkubo, K. Suzki, and S. Kinoshita, "Cryptographic approach to "privacy-friendly" tags.," In RFID Privacy Workshop, MIT, MA, USA, November 2003. http://www.rfidprivacy.us/2003/agenda.php.

[11] H. Chien and C. Chen, "Mutual authentication protocol for RFID conforming to EPC class 1 generation 2 standards," Computer Standards & Interfaces, 29(2):254–259, February 2007.

[12] D. Henrici and P. Muller, "Hash-based enhancement of location privacy for radio-frequency identification devices using varying identifiers," In R. Sandhu and R. Thomas, editors, International Workshop on Pervasive Computing and Communication Security - PerSec 2004, pages 149–153, Orlando, Florida, USA, March 2004. IEEE Computer Society.

[13] S.M. Lee, Y.J. Hwang, D.H. Lee and J.I. Lim, "Efficient Authentication for Low-Cost RFID systems," ICCSA05, vol. 3480 LNCS, pp.619-629, Springer-Verlag, 2005.

[14] B. Song and C. J. Mitchell, "RFID authentication protocol for low-cost tags," In WISEC, pages 140-147, 2008.

[15] T. Dimitriou, "A lightweight RFID protocol to protect against traceability and cloning attacks," In Conference on Security and Privacy for Emerging Areas in Communication Networks - SecureComm, pages 59–66, Athens, Greece, September 2005. IEEE.

[16] B. Song, "RFID Tag Ownership Transfer," In 4thWorkshop on RFID Security (RFIDsec 08), Budaperst, Hungary, July 2008.

[17] M.E. Hoque,F. Rahman, S.I. Ahamed, "Supporting Recovery, Privacy and Security in RFID Systems Using A Robust Authentication Protocol," Proceedings of the 2009 ACM symposium on Applied Computing, SAC'09, Honlulu, Hawaii,USA. pp.1062-1066.

[18] S. Cai, Y. Li, T. Li, R. H. Deng, "Attacks and Improvements to an RFID Mutual Authentication Protocol and its Extensions," WiSec'09, March 16–18, 2009, Zurich, Switzerland.

[19] M. Shafiq, K. Shingh, C. Lal, M. Conti, T. Khan, ESRAS: An efficient and secure ultra-lightweight RFID authentication scheme for low-cost tags. Computer Networks, 217(2022), pp. 1-11.

[20] Pedro Peris-Lopez, Julio Cesar Hernandez-Castro, Juan M Estévez-Tapiador, Arturo Ribagorda, LMAP: A real lightweight mutual authentication protocol for low-cost RFID tags, in: Proc. of 2nd Workshop on RFID Security, Vol. 6, 2006.

[21] Pedro Peris-Lopez, Julio Cesar Hernandez-Castro, Juan M Estevez-Tapiador, Arturo Ribagorda, *M*2AP: a minimalist mutual-authentication protocol for lowcost RFID tags, in: International Conference on Ubiquitous Intelligence and Computing, Springer, 2006, pp. 912–923.

[22] Pedro Peris-Lopez, Julio Cesar Hernandez-Castro, Juan M Estevez-Tapiador, Arturo Ribagorda, EMAP: An efficient mutual-authentication protocol for lowcost RFID tags, in: OTM Confederated International Conferences ''on the Move to Meaningful Internet Systems'', Springer, 2006, pp. 352–361.

[23] Ticyan Li, Guilin Wang, Security analysis of two ultra-lightweight RFID authentication protocols, in: IFIP International Information Security Conference, Springer, 2007, pp. 109–120.

[24] Tieyan Li, Robert Deng, Vulnerability analysis of EMAP-an efficient RFID mutual authentication protocol, in: The Second International Conference on Availability, Reliability and Security (ARES'07), IEEE, 2007, pp. 238–245.

[25] Lijun Gao, Maode Ma, Yantai Shu, Yuhua Wei, An ultralightweight RFID authentication protocol with CRC and permutation, J. Netw. Comput. Appl. 41 (2014) 37–46.

[26] Yun Tian, Gongliang Chen, Jianhua Li, A new ultralightweight RFID authentication protocol with permutation, IEEE Commun. Lett. 16 (5) (2012) 702–705.

[27] Hanguang Luo, Guangjun Wen, Jian Su, Zhong Huang, SLAP: Succinct and lightweight authentication protocol for low-cost RFID system, Wirel. Netw. 24 (1) (2018) 69–78.

[28] Yali Liu, Martianus Frederic Ezerman, Huaxiong Wang, Double verification protocol via secret sharing for low-cost RFID tags, Future Gener. Comput. Syst. 90 (2019) 118–128.

[29] Yali Liu, Xinchun Yin, Yongquan Dong, Keke Huang, Lightweight authentication scheme with inverse operation on passive rfid tags, J. Chin. Inst. Eng. 42 (1) (2019) 74–79.

[30] Liang Xiao, He Xu, Feng Zhu, Ruchuan Wang, Peng Li, SKINNY-based RFID lightweight authentication protocol, Sensors 20 (5) (2020) 1366.

[31] Cuong Trinh, Bao Huynh, Jan Lansky, Stanislava Mildeova, Masoumeh Safkhani, Nasour Bagheri, Saru Kumari, Mehdi Hosseinzadeh, A novel lightweight block cipher-based mutual authentication protocol for constrained environments, IEEE Access 8 (2020) 165536–165550.

[32] Mohd Shariq, Karan Singh, Pramod Kumar Maurya, Ali Ahmadian, Muhammad Rezal Kamel Ariffin, URASP: An ultralightweight RFID authentication scheme using permutation operation, Peer-to-Peer Netw. Appl. 14 (6) (2021) 3737–3757.

[33] Il-Soo Jeon, Eun-Jun Yoon, A new ultra-lightweight RFID authentication protocol using merge and separation operations, Int. J. Math. Anal. 7 (52) (2013) 2583–2593.

[34] Mathieu David, Neeli R. Prasad, Providing strong security and high privacy in low-cost RFID networks, in: International Conference on Security and Privacy in Mobile Information and Communication Systems, Springer, 2009, pp. 172–179.

[35] Xu Zhuang, Yan Zhu, Chin-Chen Chang, A new ultralightweight RFID protocol for low-cost tags: *R*2AP, Wirel. Pers. Commun. 79 (3) (2014) 1787–1802.

[36] Madiha Khalid, Umar Mujahid, M Najam-ul Islam, Hongsik Choi, Imtiaz Alam, Shahzad Sarwar, Ultralightweight resilient mutual authentication protocol for IoT based edge networks, J. Ambient Intell. Humaniz. Comput. (2021) 1–12.

[37] C. Cremers, Scyther tool, 2021, http://www.cs.ox.ac.uk/people/cas.cremers/scyther/. [Online; Accessed on March 10, 2021].