IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received 29 December 2022, accepted 15 January 2023, date of publication 23 January 2023, date of current version 3 February 2023.

Digital Object Identifier 10.1109/ACCESS.2023.3239530

RESEARCH ARTICLE

MDS Code Based Ultralightweight Authentication Protocol for RFID System

PRAMOD KUMAR MAURYA[1], **HARADHAN GHOSH**[2], **AND SATYA BAGCHI**[2]

[1]School of Computer Science and Engineering, Vellore Institute of Technology, Vellore 632014, India
[2]Department of Mathematics, National Institute of Technology at Durgapur, Durgapur 713209, India

Corresponding author: Pramod Kumar Maurya (pramodkumar.maurya@vit.ac.in)

This work is supported by Vellore Institute of Technology, Vellore, India.

ABSTRACT Privacy and security are central issues in the deployment of an RFID system. It is vulnerable to several attacks, such as replay attacks, location tracking, man-in-middle attack, de-synchronization attack, etc., due to the inherent weaknesses of underlying wireless communications. In order to tackle these privacy and security concerns, this paper presents an ultralightweight authentication protocol based on group homomorphism and maximum distance separable (MDS) code. We use group homomorphism properties to make a server lookup table that reduces searching complexity and overcomes scalability issues. We develop an ultralightweight protocol using MDS code properties that employs only bit-wise operators. Formal and informal security analysis of the proposed protocol shows that our proposed protocol resists various attacks. In addition, we use automated security protocol verification tools, AVISPA and Scyther, to validate the security features of the proposed protocol. We demonstrate the correctness proof of the proposed protocol using BAN logic. To measure the level of privacy of the proposed protocol, we use two benchmark metrics to simulate the proposed protocol. The performance analysis indicates that the proposed protocol is efficient for a low-cost environment.

INDEX TERMS Authentication protocol, anonymity set, group homomorphism, MDS code, privacy, RFID system, security.

I. INTRODUCTION

RFID (radio frequency identification) is becoming the most promising technology for automated identification in many IoT applications such as automation, automotive, ticketing, medical, commerce, transport, logistics, etc. Due to low-cost and easy deployment, RFID technology is progressing rapidly in every industry sector. According to IDTechEx's report, the RFID market is expected to reach worth $13.2 billion by 2020 and $186.8 billion in 2026 [10]. Typically RFID system is made up of three components: an RFID tag or smart label, an RFID reader (interrogator), and a back-end server (middle-ware) [21]. An RFID tag consists of a small microchip and an antenna. The tag stores information about the product in which it is embedded. In addition, RFID tags comprise minimal resources with restricted storage capacity. According to the functionality, we can arrange RFID tags into two classifications in general, namely active tag and passive tag. Active tag: these type of tags have their in-built battery for internal processing and data transmission. Passive tag: these types of tags have no in-built power source. Passive tags harvest their power from the interrogator reader by the coupling method [22]. A reader or interrogator is a read/write device that works as a bridge between the back-end server and tags. A middle-ware is a software or database that stores information about the tags and readers and uses this information for various purposes. The workflow of an RFID system is as follows. Whenever a tag comes in the read range of a reader, the tag transmits its information to the reader through a wireless channel. The reader passes the received information to the back-end server via a secure link for validation of the tag.

The associate editor coordinating the review of this manuscript and approving it for publication was Chien-Ming Chen.

A. MOTIVATION

The RFID reader and tag communicate over an insecure wireless channel, so several serious security issues arise, such as tag information leakage, tag location tracking, eavesdropping, de-synchronization attack, replay attack, cloning and spoofing attacks, etc. [23], [24], [43]. RFID tag's data can be read with an anonymous compatible reader without the user's knowledge. When a privacy concern is related to individuals, medical settings, or the military, this can become a national security concern or life-or-death matter. For this reason, overcoming these privacy and security issues associated with the RFID system is essential. So, there is a requirement for powerful security mechanisms to avoid informal admittance to sensitive data while transmitting, storing, and sharing.

B. MAIN CONTRIBUTIONS

The main contributions of this article are as follows-

1) We used the concepts of MDS codes, group homomorphism, and left rotation operations in the proposed protocol to reduce the vulnerabilities.
2) We have designed and implemented the security analysis of the proposed protocol.
3) Formal security verification of the proposed protocol is done using the BAN logic, Scyther simulation, and AVISPA tools.
4) The performance analysis of the proposed protocol is done in terms of security requirements, storage costs, communication costs, and computational costs. The comparison results indicate that the proposed protocol performs better compared to some existing related protocols.

C. ORGANIZATION

The rest of the paper is organized as follows: We review some important research works related to the present topic in Section II. In Section III, we discuss preliminaries that are used in the proposed protocol. We present details of our system model in Section IV. MDS code-based authentication protocol for the RFID system is proposed in Section V. The adversary model is presented in Section VI. In Section VII, we discuss the security and privacy analysis of the proposed protocol. We measure the level of privacy of the protocol in Section VIII. The simulation results are demonstrated in Section IX. BAN logic correctness proof is given in Section X. In section XI, we illustrate the performance of the proposed protocol. We present the conclusions of the paper in Section XII.

II. LITERATURE SURVEY

In the literature, researchers proposed several ultralightweight authentication protocols to resolve security and privacy vulnerabilities associated with the RFID system. Some prominent RFID authentication protocols with their methodology, benefits, and drawbacks are as follows.

In 2006, Lopez et al. [26] presented a minimalist, lightweight authentication protocol for the RFID system. The protocol uses an index pseudonym and four keys. The index pseudonym is used as an index in the database to reduce search complexity. The keys are used to make secure communication between the reader and the tag. The protocol employs only AND, OR, and XOR operators for computational purposes and uses around 300 gates for implementation. The proposed protocol tackles the computation problem that existed in the RFID system very efficiently. However, the protocol suffers from various attacks such as de-synchronization attacks, disclosure attacks, and impersonation attacks.

In 2007, Chien [9] proposed an ultralightweight authentication protocol that employs only simple bit-wise operators on the tag. The author claims that the protocol provides strong privacy and resists several well-known attacks. Unfortunately, the proposed protocol is susceptible to several attacks such as disclosure attacks, DoS attacks, de-synchronization attacks, etc. [6], [7].

Avoine et al. [3] proposed a group-based private authentication protocol by dividing the tags into a number of groups in 2007. In this approach, the proposed scheme achieves a huge improvement in security assurance at the cost of a high computational load.

In 2009, David and Prasad [11] proposed an ultralightweight authentication protocol to reduce computational load significantly without compromising security. The protocol uses only XOR, AND, and NOT operators for computational. In the protocol, the authors use two secret keys to transmit nonces to the tag securely, and the tag extracts the nonce with the help of the keys and uses them to mask the tag's ID. The protocol is very efficient in computational load, but it is susceptible to traceability attacks and disclosure attacks [14].

In 2012, Tian et al. [38] proposed an ultralightweight RFID authentication protocol known as RAPP. The proposed protocol employs a bit-wise operation called permutation to achieve a higher level of privacy and secrecy. The protocol is very efficient in a low-cost environment but does not resist disclosure attacks, traceability attacks, de-synchronization attacks, etc. [24].

Zhuang et al. [42] introduced a reconstruction-based ultralightweight authentication protocol called R^2AP in 2014. The authors introduced a lightweight bit-wise operation, reconstruction, for computational work. The authors give a formal security analysis based on Jules-Weis's un-traceability model to claim that the proposed protocol resists all possible attacks. However, Safkhani [31] highlighted de-synchronization attacks, disclosure attacks, and traceability attacks and challenged its security claims.

Tewari and Gupta [37] proposed a robust ultralightweight authentication protocol to overcome security challenges with the RFID system in 2016. The protocol is efficient in terms of the computational load because it involves only two bit-wise operations, XOR and left rotation. The protocol uses random numbers to mask the tag ID and employs a secret key to hide the transmitted data. In addition to avoiding the de-synchronization attack, the proposed protocol stores current session data as well as previous session data. Unfortunately, the protocol is susceptible to several attacks, namely denial of service attacks, secret disclosure attacks, etc. [16], [32], [39].

In 2016, Luo et al. [19] introduced a succinct and lightweight authentication protocol (SLAP). This protocol is composed only of XOR, left rotation with hamming weight, and a bit-wise operation known as conversion. The security of the protocol depends on the introduced conversion function that possesses irreversibility, full confusion, and sensibility. The protocol uses two secret keys for each tag to transmit data securely over an insecure channel. After successful authentication sessions, it updates the secret keys to resist an un-traceability attack. The protocol guarantees to resist various attacks such as replay attacks, de-synchronization attacks, disclosure attacks, etc. However, Khalid et al. show that the protocol is vulnerable to impersonation attacks and de-synchronization attacks [16], [30].

In 2017, Rahman et al. [28] proposed a secure, anonymous group-based authentication protocol to address the tradeoff between the protection and scalability of RFID systems. The protocol is similar to Avoine et al. [3] except that the protocol uses an alternate grouping technique to accomplish better privacy. This protocol utilized an investigation-based definition to formalize RFID security according to the viewpoint of unlinkability among various RFID tags.

Younis and Abdulkareem [41] proposed a three-pass mutual authentication protocol for RFID systems in 2017. The protocol used PRNG, elliptic curve digital signature algorithm, encryption techniques, and XOR operations. Additionally, this protocol is secure against various known attacks, but the total computational cost is very high compared to some lightweight protocols.

Khor and Sidorov [17] improved the authentication protocol proposed by Tewari and Gupta [37] in 2018. The proposed protocol employs left rotation as well as right rotation with hamming weight to achieve anonymity by mix-up the bits. The authors claim that the protocol overcomes all vulnerabilities presented in Tewari and Gupta's protocol as well as resists all possible attacks. Safkhani and Bagheri [32] presented a full disclosure attack on the protocol proposed by Khor and Sidorov [17].

Qui et al. [27] proposed a robust authentication protocol based on ECC for TMIS in the same year. The protocol fails to prevent replay attacks, user anonymity, impersonation attacks, and password-guessing attacks.

In 2020, Fan et al. [12] proposed an efficient and reliable cloud-based authentication protocol for the RFID system. The authors used bit-wise rotation, permutation, and public-key encryption in the protocol to resist well-known attacks such as tracking, replay, and de-synchronization attacks. The protocol provides higher-level security. However, the protocol is not suitable for the low-cost environment due to the high computational overhead.

Noori et al. [25] proposed an ECC-based scalable RFID authentication protocol for an IoT environment in the same year. The protocol uses ECC, hash function, and random numbers. The scheme attains a higher level of privacy. However, the scheme is not practical for low-cost tags due to the high computational overhead.

In 2021, Shariq and Singh [35] designed a lightweight RFID protocol for passive tags that integrates vector space, linear mapping, basis mechanism, and hash function. The correctness of the protocol has been finished by using BAN logic. The scheme is not secure against impersonation attacks.

Xiao et al. [40] presented a lightweight RFID authentication protocol for TMIS in 2021. The authors used the properties of random numbers, PUF and ECC for a low-cost protocol. The protocol uses the ProVerif tool to test the security attribute, demonstrating that it is safe against various attacks.

In the same year, Agrahari and Varma [1] proposed an RFID authentication protocol for the healthcare environment based on ECC. The protocol uses a hash function, addition and multiplication of elliptic points. Formal security analyses were done by the AVISPA tool, ROR model, and BAN logic.

In 2022, Akleyle and Soyasald1 [2] presented a lattice-based RFID authentication protocol for IoT. They used the hardness of the inhomogeneous small integer solution (ISIS) problem, two hash functions, one permutation matrix, and random numbers. The authors claimed that the protocol could resist post-quantum attacks.

In the same year, Rostampour et al. [29] proposed a lightweight authentication protocol for IoT systems by utilizing an authentication encryption cryptosystem with associated data (AEAD). The formal security of the protocol was shown by using the ROR model and Scyther tool.

After reviewing the work done, we would like to propose an MDS code-based ultralightweight authentication protocol. In our approach, we use the concept of group homomorphism to divide the set of all tags into some clusters. Also, we use some properties of MDS code to minimize computational overhead without compromising the security and privacy of the protocol.

III. PRELIMINARIES

This section overviews group homomorphism and maximum distance separable codes that we will use to construct our system model.

A. GROUP HOMOMORPHISM

Suppose $(Gr, \star)$ and $(Gr', *)$ are two groups with identity elements e and e' respectively. A *group homomorphism* ϕ from Gr to Gr' is a mapping that preserves group operation, i.e., $\phi(a \star b) = \phi(a) * \phi(b)$ for all $a, b \in Gr$ [13]. The *kernel* of a group homomorphism from Gr into Gr' is a subset of Gr defined as

$$\ker \phi = \{g \in Gr : \phi(g) = e'\}.$$

If $| \ker \phi | = t$, then the group homomorphism ϕ is a $t - to - 1$ mapping from Gr onto $\phi(Gr)$. We use this property of group homomorphism to divide the set of all tags into some clusters of the same size in our system model.

B. LINEAR CODE

Let $GF(q)$ be a finite field with q elements. The set $GF(q)^n$ with cardinality q^n forms a vector space over the field $GF(q)$. A linear code C of length n over the field $GF(q)$ is a subspace of the vector space $GF(q)^n$. If C has dimension k, then we say C is a q-ary $[n, k]$ linear code over $GF(q)$ [18]. The hamming distance of two codewords c_1 and c_2, is denoted by $d(c_1, c_2)$ and defined as the number of positions at which the corresponding symbols differ. The minimum distance of the code C is denoted by d and defined as $d = \min\{d(c_1, c_2) \mid c_1 \neq c_2, c_1, c_2 \in C\}$. If a q-ary $[n, k]$ code C has the minimum distance d, then we denote it as q-ary $[n, k, d]$ code over $GF(q)$. A generator matrix G of the code C is a $k \times n$ matrix which spans the code C. A parity check matrix H of order $(n-k)\times n$ with rank $(n-k)$ of the code C which satisfies the following property:

$$C = \{c \in GF(q)^n \mid c \times H^T = 0\},$$

where H^T denotes the transpose of the matrix H.

C. MAXIMUM DISTANCE SEPARABLE CODES

A q-ary $[n, k, d]$ linear code C over $GF(q)$ is said to be a *maximum distance separable* (MDS) code if and only if $d = n-k+1$. MDS codes have many interesting properties. Some of them are as follows.

1) Any k columns of a generator matrix G of the code C are linearly independent.
2) Any $n-k$ columns of a parity-check matrix H of the code C are linearly independent.

D. CONSTRUCTION OF A CODEWORD c FROM l-COORDINATES OF THE CODEWORD c WHERE $l \geq k$

Suppose G is a generator matrix of an MDS code $C = [n, k, d]$ over $GF(q)$ and $\alpha = (\alpha_1, \alpha_2, \ldots, \alpha_k) \in GF(q)^k$. We can generate a codeword c of the code C as follows.

$$c = \alpha \times G$$

implies that

$$(c_1, c_2, \ldots, c_n) = (\alpha_1, \alpha_2, \ldots, \alpha_k) \times G. \qquad \text{(III.1)}$$

We index n columns of the generator matrix G of the code C by $1, 2, \ldots, n$ and write $G = [g_1, g_2, \ldots, g_n]$, where g_i is the i^{th} column of G. Suppose, we know any l-components of a codeword $c \in C$, say, $c_{i_1}, c_{i_2}, \ldots, c_{i_l}$, where $l \geq k$. Then we can construct the whole codeword c by using the following procedure. We make a matrix $G_1 = [g_{i_1}, g_{i_2}, \ldots, g_{i_l}]$ of order $k \times l$ from G. From Equation (III.1), we can write

$$(c_{i_1}, c_{i_2}, \ldots, c_{i_l}) = (\alpha_1, \alpha_2, \ldots, \alpha_k) \times G_1. \qquad \text{(III.2)}$$

By properties of MDS code, the Equation (III.2) has a unique solution because $rank(G_1) = k$. In this way, we can uniquely identify $\alpha = (\alpha_1, \alpha_2, \ldots, \alpha_k)$ from the given $(c_{i_1}, c_{i_2}, \ldots, c_{i_l})$. Hence, we can generate whole codeword $c = \alpha \times G$ using Equation (III.1).

IV. SYSTEM MODEL

We use characteristics of group homomorphism and coding theory to construct a system model. Using the group homomorphism property, we divide the set of all tags in the system into clusters of equal size. The division takes place as follows. Suppose $\mathbb{T}$ is a set of all tags in the system with cardinality p. We choose a group Gr of order p and make a one-to-one correspondence between $\mathbb{T}$ and Gr, i.e., for each element $g \in Gr$, we associate a tag T with it, i.e., $g \leftrightarrow T$. We choose another group Gr' and find a homomorphism ϕ from Gr to Gr' with $|\ker \phi| = t$. So, ϕ is an t-to-1 mapping from Gr to $\phi(Gr)$. Moreover, as we know, with each element $g \in Gr$, there is a unique tag T, which is associated with g. Thus, the t number of tags maps to $g' \in Gr'$ under ϕ. We use the set $\phi(Gr)$ as an index set in the system model. In this way, we divide the set of all tags $\mathbb{T}$ in the system into p/t clusters in which each cluster consists of t number of unique tags.

In addition, we use the properties of maximum distance separable codes, a concept of coding theory, in this system model. For this reason, we choose an MDS code $C = [n, k, d]$ over the field $GF(2)$ and store a fixed generator matrix G of the code C in the database as depicted in Table 1. This system model assumes that reader and server communicate over a secure channel. So, we can consider the reader and the server interchangeable.

The system components used in the system model are as follows.

A. READER

Reader stores all the information about each tag in the system. The reader stores a fixed generator matrix G of the chosen MDS code $C = [n, k, d]$ and group homomorphism ϕ in its database. Table 1 depicts the reader's database lookup table. In Table 1, the symbol $g_{ij} \leftrightarrow T_{ij}$ shows that the tag T_{ij} is associated with the group's element g_{ij}. For each tag T_{ij}, the reader stores a unique codeword ID_{ij} of the code C, a key K_{ij}, and the group element g_{ij} associated with the tag T_{ij} in the database. The reader has a pseudo-random number generator function that generates a pseudo-random number with a hamming weight greater than or equal to k.

B. TAG

In the system model, each tag T_{ij} possesses a unique identification number ID_{ij}, which is a codeword of the code C, a key K_{ij}, and an element $g_{ij} \in Gr$, where g_{ij} is the group element associated with the tag T_{ij} in the system model.

V. PROCESS

This section introduces an MDS code-based ultralightweight authentication protocol according to our system model. The symbols used in the paper are given in Table 2, and the workflow of the proposed authentication protocol is shown in Figure 1.

TABLE 1. The server lookup table.

Generator matrix of the code C	Index (i.e. $\phi(g_{ij}) = g'_j$)	Tag with associate group's element	Storage data
G, ϕ	g'_1	$g_{11} \leftrightarrow T_{11}$	$\{ID_{11}, K_{11}, g_{11}\}$
		$g_{21} \leftrightarrow T_{21}$	$\{ID_{21}, K_{21}, g_{21}\}$
		$\vdots$	$\vdots$
		$g_{t1} \leftrightarrow T_{t1}$	$\{ID_{t1}, K_{t1}, g_{t1}\}$
	g'_2	$g_{12} \leftrightarrow T_{12}$	$\{ID_{12}, K_{12}, g_{12}\}$
		$g_{22} \leftrightarrow T_{22}$	$\{ID_{22}, K_{22}, g_{22}\}$
		$\vdots$	$\vdots$
		$g_{t2} \leftrightarrow T_{t2}$	$\{ID_{t2}, K_{t2}, g_{t2}\}$
	$\vdots$	$\vdots$	$\vdots$
	$g'_{p/t}$	$g_{1p/t} \leftrightarrow T_{1p/t}$	$\{ID_{1p/t}, K_{1p/t}, g_{1p/t}\}$
		$g_{2p/t} \leftrightarrow T_{2p/t}$	$\{ID_{2p/t}, K_{2p/t}, g_{2p/t}\}$
		$\vdots$	$\vdots$
		$g_{tp/t} \leftrightarrow T_{tp/t}$	$\{ID_{tp/t}, K_{tp/t}, g_{tp/t}\}$

TABLE 2. Notations and symbols used in the proposed protocol.

Notation	Description
Gr	A finite group of order p.
Gr'	An another group that is homomorphic to Gr.
ϕ	A homomorphism between Gr and Gr' with $\lvert \ker \phi \rvert = t$.
C	An MDS code.
G	Generator matrix of the code C.
k	Dimension of the code C.
ID_{ij}	Unique identification number of the tag T_{ij} and $ID_{ij} \in C$.
K_{ij}	Key of the tag T_{ij}.
g_{ij}	It is an element of the group Gr that is associated with T_{ij}.
g'_j	An element of the group Gr' such that $\phi(g_{ij}) = g'_j$.
R_1	Pseudo-random number generated by a reader with hamming weight $\geq k$.
$wt(a)$	Hamming weight of a, i.e. number of non-zero positions in the bit-string of a.
R_2	Pseudo-random number generated by a tag.
$\lll$	Circular left shift operator.
$\wedge$	Bitwise AND operator.
$\oplus$	Exclusive-or operator.

The steps of the proposed authentication protocol are as follows.

1) Whenever a tag T_{ij} comes to the read range of a legitimate reader, the reader generates a pseudo-random number R_1 and transmits it to the tag.
2) Upon receiving, the tag generates a pseudo-random number R_2. The tag T_{ij} calculates $\beta = ID_{ij} \wedge R_1$ and $\gamma = \beta \oplus (g_{ij} \lll wt(K_{ij} \oplus R_2))$. It transmits g_{ij} and γ with R_2 to the reader. Here, note down that β contains only l-coordinates of the codeword ID_{ij}, where l is the hamming weight of R_1.
3) After receiving, the reader uses the Table 1 and does the following for each tag T_{ij} in the cluster g'_j (where $g'_j = \phi(g_{ij})$) until it authenticates the tag.

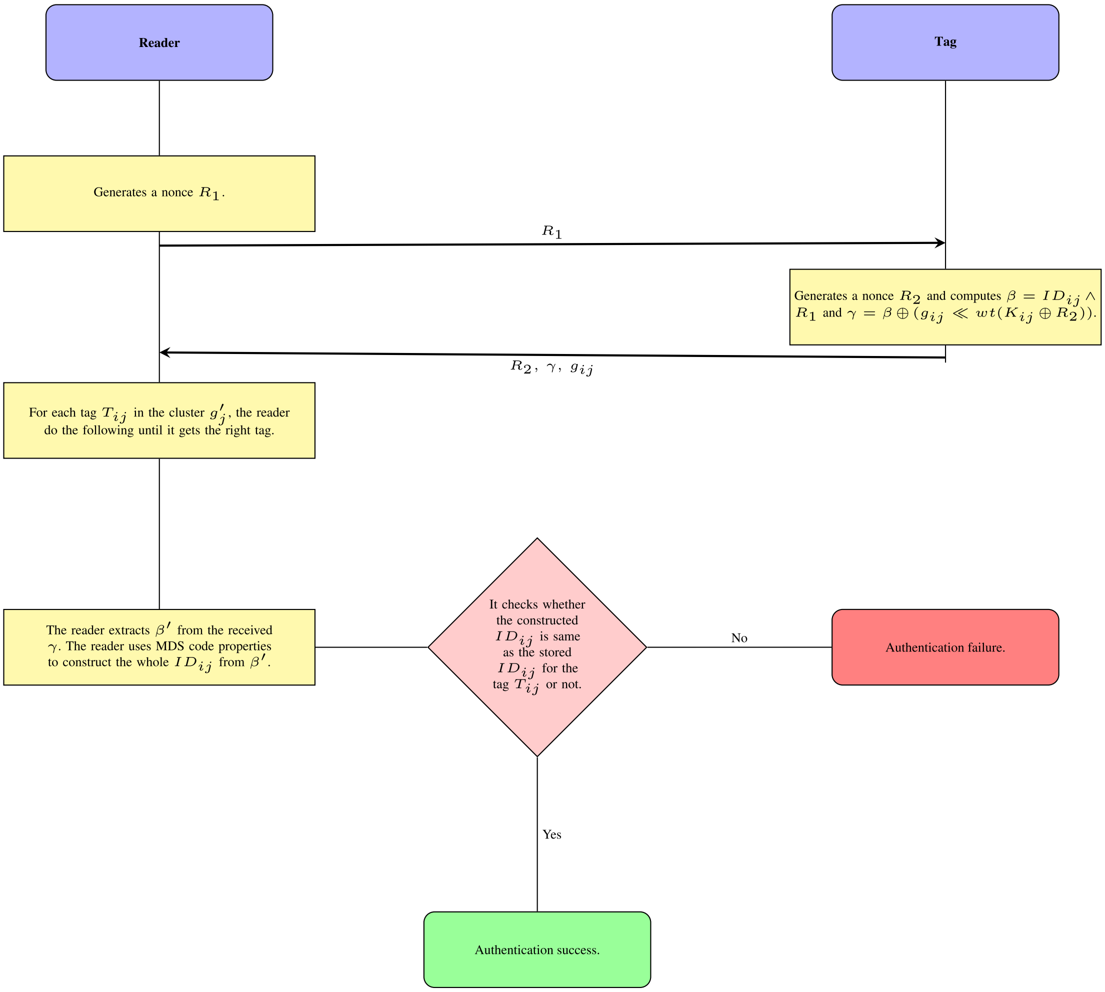

Reader
Tag
Generates a nonce R_1.
R_1
Generates a nonce R_2 and computes $\beta = ID_{ij} \wedge R_1$ and $\gamma = \beta \oplus (g_{ij} \ll wt(K_{ij} \oplus R_2))$.
R_2, γ, g_{ij}
For each tag T_{ij} in the cluster g'_j, the reader do the following until it gets the right tag.
The reader extracts β' from the received γ. The reader uses MDS code properties to construct the whole ID_{ij} from β'.
It checks whether the constructed ID_{ij} is same as the stored ID_{ij} for the tag T_{ij} or not.
No
Authentication failure.
Yes
Authentication success.

FIGURE 1. **Proposed mutual authentication protocol.**

- The reader calculates $\delta = g_{ij} \ll wt(K_{ij} \oplus R_2)$ with the help of stored K_{ij}, and g_{ij} corresponding to the tag T_{ij}.
- It computes $\beta' = \gamma \oplus \delta$.
- The reader uses R_1 to identify the position and value of the coordinates of the codeword ID_{ij} from β' and calculates the whole codeword ID_{ij} by using the generator matrix G of the code C as mentioned in Section III.
- The reader checks the calculated codeword ID_{ij} is the same as the stored codeword for the tag T_{ij}. If it holds, the reader authenticates the tag.

4) If Step 3 does not hold for any tag in the cluster g'_j, the reader terminates the session.

VI. ADVERSARY MODEL

In this section, we define the abilities of an adversary $\mathscr{A}$, which is based on Juel's privacy model [15] with some modifications according to our requirements. Suppose an adversary has abilities to issue the following queries.

•SETKEY: The adversary can corrupt any tag by using this oracle query. We can not use any corrupt tag as a challenge tag in our privacy experiment.

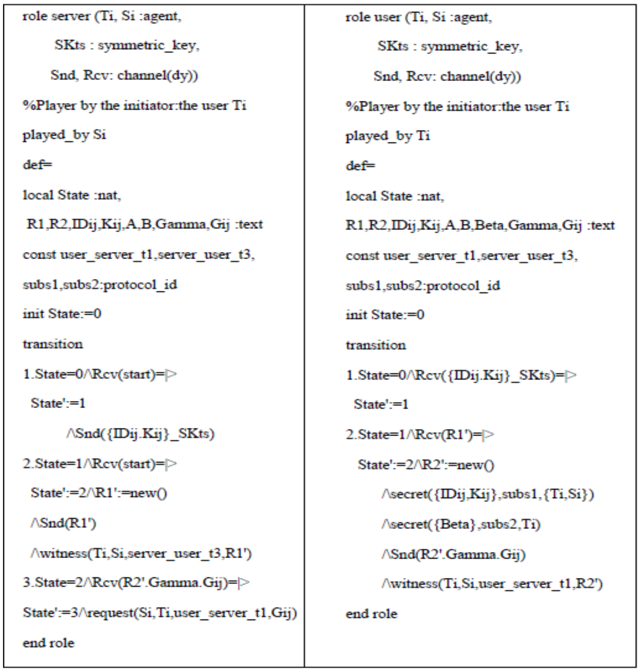
•TAGINIT: By using this oracle query, $\mathscr{A}$ can initialize a protocol session with a tag. After the protocol session initialization, the adversary can communicate with the tag as a challenge-response methodology.

•READERINIT: The adversary can initialize a new protocol session with a reader by issuing this oracle query. Then, $\mathscr{A}$ can transmit and receive a message from the reader.

Here, we parametrized the adversary by applying some restrictions on the ability of the adversary. $\mathscr{A}$ can issue r number of READERINIT messages and t number of TAGINIT query. In addition, $\mathscr{A}$ can perform s number of computation steps. The adversary is able to send SETKEY query at most $(n-2)$ tags at any time, where n is the total number of tags in the system.

A. PRIVACY EXPERIMENT $Exp^{priv}_{\mathscr{A}}[r, S, t]$

In this section, we define the adversary's privacy game that the adversary used to mount an attack on the system. The main goal of the privacy game is to distinguish between two uncorrupted tags. In the game, the system is considered private if the adversary has no significant advantage. We can divide the privacy game into three phases as follows.



```
role server (Ti, Si :agent,
      SKts : symmetric_key,
     Snd, Rcv: channel(dy))
%Player by the initiator:the user Ti
played_by Si
def=
local State :nat,
 R1,R2,IDij,Kij,A,B,Gamma,Gij :text
const user_server_t1,server_user_t3,
subs1,subs2:protocol_id
init State:=0
transition
1.State=0/\Rcv(start)=|>
 State':=1
        /\Snd({IDij.Kij}_SKts)
2.State=1/\Rcv(start)=|>
 State':=2/\R1':=new()
 /\Snd(R1')
 /\witness(Ti,Si,server_user_t3,R1')
3.State=2/\Rcv(R2'.Gamma.Gij)=|>
State':=3/\request(Si,Ti,user_server_t1,Gij)
end role
```

```
role user (Ti, Si :agent,
      SKts : symmetric_key,
     Snd, Rcv: channel(dy))
%Player by the initiator:the user Ti
played_by Ti
def=
local State :nat,
R1,R2,IDij,Kij,A,B,Beta,Gamma,Gij :text
const user_server_t1,server_user_t3,
subs1,subs2:protocol_id
init State:=0
transition
1.State=0/\Rcv({IDij.Kij}_SKts)=|>
 State':=1
2.State=1/\Rcv(R1')=|>
  State':=2/\R2':=new()
      /\secret({IDij,Kij},subs1,{Ti,Si})
      /\secret({Beta},subs2,Ti)
      /\Snd(R2'.Gamma.Gij)
      /\witness(Ti,Si,user_server_t1,R2')
end role
```

FIGURE 2. Role specification for the tag Ti and server Si in the proposed protocol.

1) LEARNING PHASE

The adversary can issue READERINIT query and TAGINIT query to any number of readers and tags without exceeding its functionality-calls limit. $\mathscr{A}$ can also issue $(n-2)$ SETKEY calls to corrupt tags.

2) CHALLENGING PHASE

In this phase, the adversary performs the following steps.

1) $\mathscr{A}$ selects two uncorrupted tags say T_i and T_j.
2) Let $b \in \{i, j\}$ and provides $\mathscr{A}$ to access T_b.
3) $\mathscr{A}$ issues TAGINIT calls to initialize a protocol session with the tag T_b. After that, the adversary communicates with the tag by using the challenge-response technique and performs some computation without exceeding s overall steps.

Guessing Phase The adversary comes with a guess bit b'. $Exp_{\mathscr{A}}^{priv}$[r, s, t] succeeds if $b = b'$.

VII. SECURITY AND PRIVACY ANALYSIS

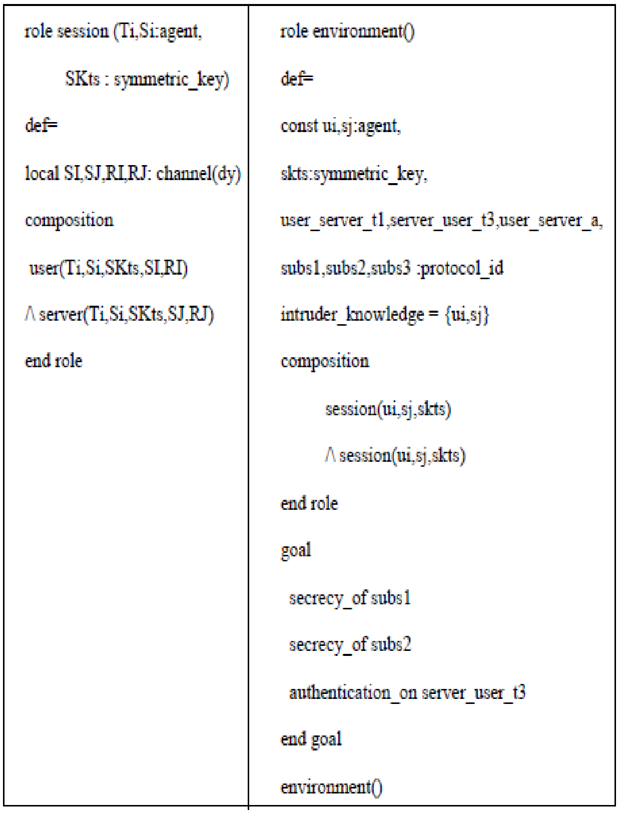
A. FORMAL SECURITY ANALYSIS

Theorem 1: The proposed protocol attains information privacy.

Proof: In this proof, we perform the privacy experiment $Exp_{\mathscr{A}}^{priv}$[r, s, t] for the proposed scheme to evaluate the information privacy of the scheme. In the privacy game, an adversary $\mathscr{A}$ chooses a tag randomly from the set of target tags. The adversary performs the oracle queries with the selected tag and try to guess the tag.

The adversary performs the privacy experiment as follows.

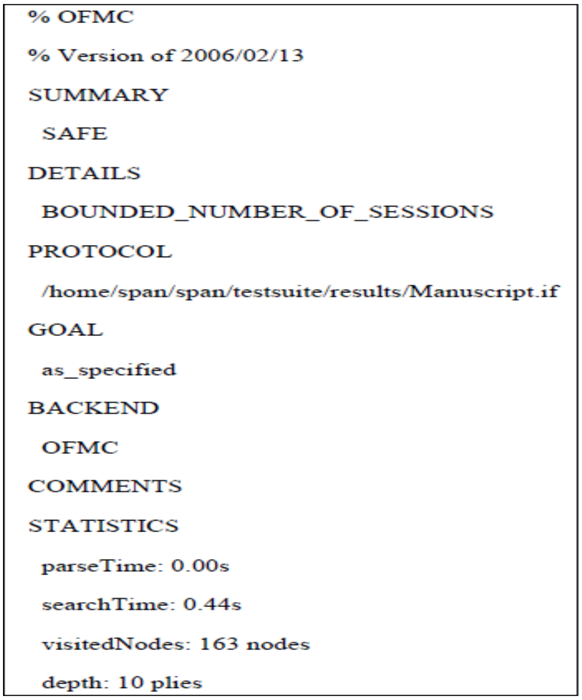
- Learning Phase: The adversary $\mathscr{A}$ interacts with a legitimate reader $\mathscr{R}$ by sending REDERINIT query to it. $\mathscr{A}$ sends TAGINIT query to n tags to initialize protocol sessions with them.
- Challenging Phase: The adversary sends SETKEY query to corrupt $(n-2)$ tags. $\mathscr{A}$ selects the remaining



```
role session (Ti,Si:agent,
     SKts : symmetric_key)
def=
local SI,SJ,RI,RJ: channel(dy)
composition
 user(Ti,Si,SKts,SI,RI)
/\ server(Ti,Si,SKts,SJ,RJ)
end role
```

```
role environment()
def=
const ui,sj:agent,
skts:symmetric_key,
user_server_t1,server_user_t3,user_server_a,
subs1,subs2,subs3 :protocol_id
intruder_knowledge = {ui,sj}
composition
      session(ui,sj,skts)
      /\ session(ui,sj,skts)
end role
goal
 secrecy_of subs1
 secrecy_of subs2
 authentication_on server_user_t3
end goal
environment()
```

FIGURE 3. Role specification for goal and environment in the proposed protocol.



```
% OFMC
% Version of 2006/02/13
SUMMARY
  SAFE
DETAILS
  BOUNDED_NUMBER_OF_SESSIONS
PROTOCOL
  /home/span/span/testsuite/results/Manuscript.if
GOAL
  as_specified
BACKEND
  OFMC
COMMENTS
STATISTICS
  parseTime: 0.00s
  searchTime: 0.44s
  visitedNodes: 163 nodes
  depth: 10 plies
```

FIGURE 4. The result of the analysis using OFMC of the proposed protocol.

two uncorrupted tags, say $\mathscr{T}_0$ and $\mathscr{T}_1$, as target tags. The adversary randomly chooses one tag from selected target tags, say $\mathscr{T}_b$, $b \in \{0, 1\}$. $\mathscr{A}$ interacts with $\mathscr{T}_b$ and gets the following information.

$$\text{TAGINIT}(\mathscr{T}_b) \to (R_2, \gamma, g_{ij}).$$

- Guessing Phase: The adversary comes with an output bit b for the tag $\mathscr{T}_b$.

It is not possible to guess correctly $\mathscr{T}_b$ is either $\mathscr{T}_0$ or $\mathscr{T}_1$ with the help of eavesdropped message (R_2, γ, g_{ij}). Hence, the adversary can not succeed in his privacy game. Therefore, the proposed protocol preserves information privacy. □

Theorem 2: The proposed protocol attains un-traceability.

Proof: We prove that the proposed scheme preserves un-traceability by use of the privacy experiment $Exp_{\mathscr{A}}^{priv}$[r, s, t]. In the experiment, $\mathscr{A}$ intercepts the transmitted messages of one session between a tag and the reader. In future sessions, the adversary tries to trace the tag on the ground of the intercepted messages.

The adversary executes the privacy experiment as follows.

- Learning Phase: The adversary interacts with a legitimate reader and n- number of tags through REDERINIT and TAGINIT queries, respectively. The adversary chooses a tag $\mathscr{T}_i$ from the set of n uncorrupted tags and interacts with it by TAGINIT query.

$$\text{TAGINIT}(\mathscr{T}_i) \to (R_2, \gamma, g_{ij}).$$

- Challenging Phase: The adversary corrupts $n - 2$ tags by sending SETKEY query to them and chooses the remaining two uncorrupted tags, say $\mathscr{T}_0$ and $\mathscr{T}_1$, as target tags. $\mathscr{A}$ randomly selects one tag, say $\mathscr{T}_b$, $b \in \{0, 1\}$, from above two uncorrupted tags. The adversary interacts with $\mathscr{T}_b$ and gets the following information.

$$\text{TAGINIT}(\mathscr{T}_i) \to (R_2', \gamma', g_{ij}').$$

- Guessing Phase: The adversary outputs a bit b for the tag $\mathscr{T}_b$.

The adversary can win the privacy game only if

$$Pr(\gamma' = \gamma) - \tfrac{1}{2}, \text{ is not negligible.}$$

But $\gamma' \neq \gamma$ because γ' contains two nonces R_1 and R_2, which are different in each authentication session. Hence, The adversary can not precisely trace a tag in the proposed protocol. □

B. INFORMAL SECURITY ANALYSIS

In this subsection, we present an informal security analysis of the proposed protocol.

1) REPLAY ATTACK RESISTANCE

RFID system works over a wireless channel. An adversary can easily eavesdrop on all the transmitted messages over the wireless channel and uses them to disguise himself as a legitimate reader or a tag. In the proposed protocol, it is not feasible for an adversary to use the previous session's transmitted data (R_2, γ, g_{ij}) in the current authenticated session to prove himself as a legitimate tag. Because γ contains two nonces (R_1, R_2), which are different in each authentication session, this makes all the replayed messages illegal.

2) DE-SYNCHRONIZATION ATTACK RESISTANCE

Since an adversary can interrupt all the transmitted messages between reader and tag. So, the adversary can create a de-synchronization between a reader and a tag by interrupting some transmitted messages such that one of the two fails to update the data value. Our proposed protocol strongly resists the de-synchronization attack because it does not update any value during the authentication session.

3) MAN-IN-MIDDLE ATTACK RESISTANCE

In the proposed protocol, it is infeasible for an adversary to modify transmitted data to disguise himself as a legitimate tag to deceive the reader. The reason is that the transmitted message γ comprises two nonce and some static secret information. Without knowing this secret information, the adversary can not modify the transmitted data to prove himself as a legitimate tag.

4) IMPERSONATION ATTACK RESISTANCE

An adversary can not impersonate a tag without knowing the secret information stored in the tag's memory. In the proposed protocol, it is not possible to extract the secret information from the transmitted message (R_2, γ, g_{ij}). Hence, the proposed protocol does not susceptible to an impersonation attack.

5) TAG ANONYMITY RESISTANCE

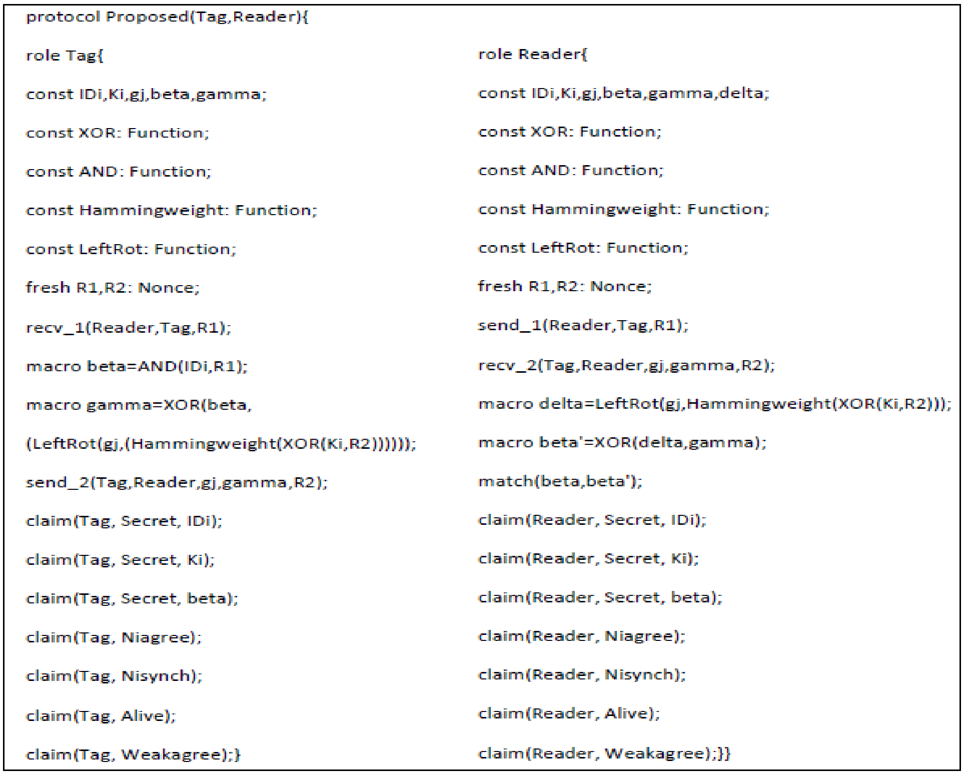
Tag anonymity ensures that the identity of the tag is not revealed to everyone. In the proposed protocol, the tag's identity is ID_{ij}, which is a codeword of the code C. This identity is transmitted by the tag using the cipher text γ with the help of β, K_{ij}, and the random number R_2. Also, the value β changes in each session because of the random number R_1 generated by the reader. Hence, the random numbers help to hide the tag's identity from the adversary.

6) FORWARD SECURITY RESISTANCE

Forward security makes sure that the information currently being transferred cannot be employed to track back the information that was previously transmitted. Any secret information containing those numbers is generated at random in each session. Even if the adversary manages to acquire the tag identity ID_{ij} in some way, they will still be unable to determine the conversations that preceded it because it involves a random number, left rotation, and a key value K_{ij}. Therefore, the adversary cannot predict future calculations using physical attacks. Hence, the proposed protocol ensures perfect forward security.

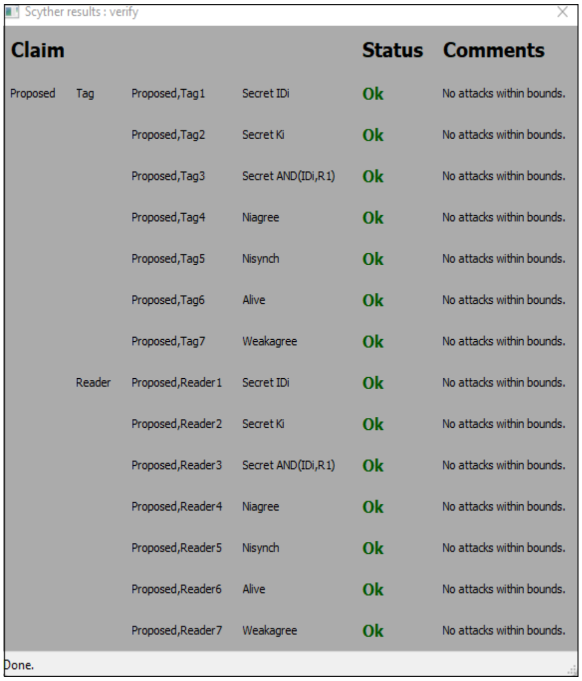
C. SIMULATION OF THE PROPOSED PROTOCOL USING AVISPA TOOL

AVISPA is a tool that automatically validates internet security-sensitive protocols and applications. It provides a



```
protocol Proposed(Tag,Reader){

role Tag{

const IDi,Ki,gj,beta,gamma;

const XOR: Function;

const AND: Function;

const Hammingweight: Function;

const LeftRot: Function;

fresh R1,R2: Nonce;

recv_1(Reader,Tag,R1);

macro beta=AND(IDi,R1);

macro gamma=XOR(beta,

(LeftRot(gj,(Hammingweight(XOR(Ki,R2))))));

send_2(Tag,Reader,gj,gamma,R2);

claim(Tag, Secret, IDi);

claim(Tag, Secret, Ki);

claim(Tag, Secret, beta);

claim(Tag, Niagree);

claim(Tag, Nisynch);

claim(Tag, Alive);

claim(Tag, Weakagree);}

role Reader{

const IDi,Ki,gj,beta,gamma,delta;

const XOR: Function;

const AND: Function;

const Hammingweight: Function;

const LeftRot: Function;

fresh R1,R2: Nonce;

send_1(Reader,Tag,R1);

recv_2(Tag,Reader,gj,gamma,R2);

macro delta=LeftRot(gj,Hammingweight(XOR(Ki,R2)));

macro beta'=XOR(delta,gamma);

match(beta,beta');

claim(Reader, Secret, IDi);

claim(Reader, Secret, Ki);

claim(Reader, Secret, beta);

claim(Reader, Niagree);

claim(Reader, Nisynch);

claim(Reader, Alive);

claim(Reader, Weakagree);}}
```

FIGURE 5. Role specification of the proposed protocol under Scyther tool.



Claim				Status	Comments
Proposed	Tag	Proposed,Tag1	Secret IDi	Ok	No attacks within bounds.
		Proposed,Tag2	Secret Ki	Ok	No attacks within bounds.
		Proposed,Tag3	Secret AND(IDi,R1)	Ok	No attacks within bounds.
		Proposed,Tag4	Niagree	Ok	No attacks within bounds.
		Proposed,Tag5	Nisynch	Ok	No attacks within bounds.
		Proposed,Tag6	Alive	Ok	No attacks within bounds.
		Proposed,Tag7	Weakagree	Ok	No attacks within bounds.
	Reader	Proposed,Reader1	Secret IDi	Ok	No attacks within bounds.
		Proposed,Reader2	Secret Ki	Ok	No attacks within bounds.
		Proposed,Reader3	Secret AND(IDi,R1)	Ok	No attacks within bounds.
		Proposed,Reader4	Niagree	Ok	No attacks within bounds.
		Proposed,Reader5	Nisynch	Ok	No attacks within bounds.
		Proposed,Reader6	Alive	Ok	No attacks within bounds.
		Proposed,Reader7	Weakagree	Ok	No attacks within bounds.

Done.

FIGURE 6. The simulation result of the proposed protocol under the Scyther tool.

modular and expressive formal language (HLPSL) for specifying protocols and their security properties. HLPSL is a role-based formal language that allows the specification of intruder models, complex security properties, and cryptographic primitives with algebraic properties. AVISPA tool is made up of four back-ends. OFMC, CL-AtSe, SATMC, and TA4SP. We use the OFMC mode in this simulation to validate our proposed protocol. The role specification of the tag T_i and the server Si in HLPSL is depicted in Figure 2. Initially, the server shares secret information with the tag by using the command $Snd(\{IDij.Kij\}_S Kts)$. Later, whenever the tag comes in the read range of the server, it transmits a nonce by the command $Snd(R1')$. After receiving, the tag generates a nonce by the command $R2' = new()$ and calculates B', A'. The tag sends $Snd(R2'.A'.Gij)$ to the server. The server receives these data by $Rcv(R2'.A'.Gij)$ and validates the tag. The role of the session, environment and goal in HLPSL is depicted in Figure 3. The goal *secrecy of subs*1 represents the sensitive data $(IDij, Kij)$ is only known to Ti and Si. The simulation result of the proposed protocol is shown in Figure 4. It shows that the proposed protocol is safe under OFMC mode back-ends.

D. SIMULATION OF THE PROPOSED PROTOCOL USING SCYTHER TOOL

The scyther tool is a prominent and broadly acknowledged tool used for checking the correctness of security protocol. To use the Scyther tool, the description of the proposed protocol should be written in SPDL (security protocol description language). The tool provides an option to generate security claims and verify against these claims automatically. The proposed protocol has two communication agents: tag and reader. In the role specification of tag and reader, we comprise a sequence of events like *macro*, *send*, *recv*, *claim*, etc. The role specification of the tag and reader is shown in 5. At the end of each role specification, the claim events like *Niagree*, *Alive*, *Nisynch*, and *Weakagree* are stated as security properties. The Scyther tool checks the validity of the claim events internally. If it does not find any attack against claim events, it shows the result "OK". The resulting window of the proposed scheme is shown in Figure 6. The simulation result shows that the tool did not find any attack in the proposed scheme. Hence, the scheme preserves the claimed security features.

VIII. MEASUREMENT OF PRIVACY

This section characterizes the level of privacy of the proposed protocol in terms of anonymity set and data leakage. For the privacy measurement, we used two privacy metrics given in the papers [5] and [34]. Both metric utilizes disjoint partition sets of tags for perception. At the point when a few tags are compromised, the arrangement of all tags is parcelled in such a manner so that the adversary ($\mathcal{A}$) can not recognize the tags that have a place with a similar partition, yet the adversary can recognize the tags belong to different partitions. Here, $|\mathcal{P}_i|$ denotes the size of such partition $\mathcal{P}_i$ and $\frac{|\mathcal{P}_i|}{T}$ is the probability that a randomly chosen tag belongs to partition $\mathcal{P}_i$, T stands for the total number of tags in the system.

A. LEVEL OF PRIVACY BASED ON ANONYMITY SET

The level of privacy R based on the anonymity set is characterized as the average anonymity set size normalized with the total number of tags T [3], [28]. The level of privacy R is

$$R = \frac{1}{T}\sum |\mathcal{P}_i|\frac{|\mathcal{P}_i|}{T} = \frac{1}{T^2}\sum |\mathcal{P}_i|^2 \qquad \text{(VIII.1)}$$

In the proposed protocol, if a tag is compromised, it releases no data about the cluster to which it belongs. Consequently, $\mathcal{A}$ can not recognize two tags regardless of whether they belong to a similar partition. So, if C is the total number of compromised tags in the system, we partitioned the system into C number of anonymity sets with size 1 and another anonymity set of size $(T - C)$. Using equation VIII.1, the level of privacy R achieved by our protocol is

$$R = \frac{1}{T^2}\{C + (T - C)^2\}. \qquad \text{(VIII.2)}$$

B. LEVEL OF PRIVACY BASED ON INFORMATION LEAKAGE IN BITS

If $\mathcal{A}$ partitioned a system with T tags into d disjoint sets, then the information leakage in bits is given by [28]

$$I = \sum_{i=0}^{d} \frac{|\mathcal{P}_i|}{T}\log_2\left(\frac{T}{|\mathcal{P}_i|}\right). \qquad \text{(VIII.3)}$$

Therefore, according to our partition, the information leakage in bits for the proposed protocol is given by

$$I = \frac{C}{T}\log_2 T + \frac{(T-C)}{T}\log_2\left(\frac{T}{T-C}\right). \qquad \text{(VIII.4)}$$

IX. EXPERIMENTAL RESULTS

This section presents a Matlab simulation of the proposed protocol to measure privacy and data leakage. We take a system of $N = 2^{12}$ number of tags and then divide all tags into 32 clusters. For the system setup, We choose a group $\mathbb{Z}_{2^{12}}$ and associate each element of the group to a tag in the system as referred to in Section IV. We choose another group $\mathbb{Z}_{2^7}$ and define a group homomorphism $\phi : \mathbb{Z}_{2^{12}} \rightarrow \mathbb{Z}_{2^7}$ such that $\phi(x) = 36x\ (mod\ 2^7)$. The order of the kernel in ϕ is 128, i.e., $|\ker\ \phi| = 128$. Due to this, we get a 128-to-1 mapping from $\mathbb{Z}_2^{12}$ to $\mathbb{Z}_2^{7}$. Thus, we divide all tags in the system into 32 clusters and in each cluster, we have 128 tags. The order of the Image in ϕ is 32, i.e., $|Image\ \phi| = 32$. We use each element of $Image(\phi)$ as an index in our system, as shown in Table 1.

In the simulation, we randomly choose a range of compromised tags from 0 to 900. For each value of compromised tags, we run 100 simulations. We find the average of all the simulation runs and measure the privacy and data leakage by using *VIII*.2 and *VIII*.4, respectively. The simulation result of the privacy measurement is shown in Figure 7. The simulation result of Figure 7 shows that the proposed protocol attains higher privacy even if a large number of tags are compromised. The simulation result of the data leakage is shown in Figure 8. It shows that the proposed protocol does not disclose more information about the system while a large number of tags are compromised. With the conclusion of the simulation results, we claim that the proposed protocol achieves a higher level of privacy and discloses a small amount of data even if a large number of tags are compromised in the system.

The security performance of the proposed scheme is compared with some well-known works [8], [9], [12] [17], [19], [20], [33], [36], [37], [38], [42], in Table 3. This table depicts that many of them are not secured against one or more attacks except [12], [33], and [36]. However, these schemes require high computational overhead to withstand all well-known attacks, whereas the proposed scheme achieves the same level of security and privacy with minimal computational overhead, as discussed in section XI.

X. BAN LOGIC PROOF

In this section, we demonstrate formal security proof of our proposed protocol by using BAN logic. The BAN logic is a logical method based on belief, and knowledge [1], [35]. By using BAN logic, we derive new beliefs from known beliefs. Some well-known BAN logic symbols and rules used in this paper are as follows.

Symbols:

1) $X \mid\equiv Y$: X believes that statement Y is true.

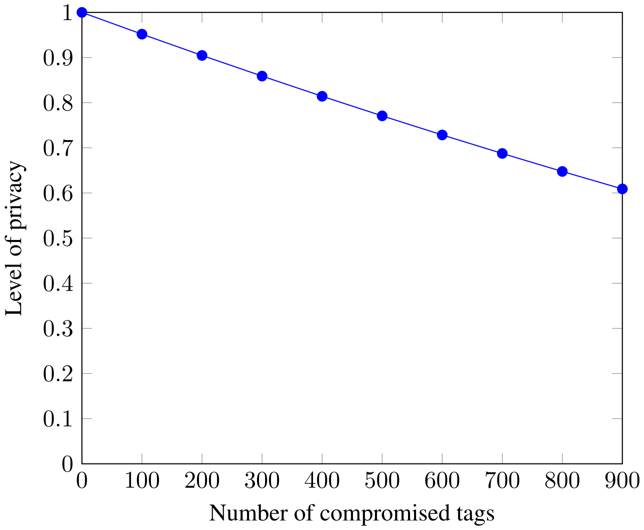


FIGURE 7. Level of privacy of the system based on anonymity set.

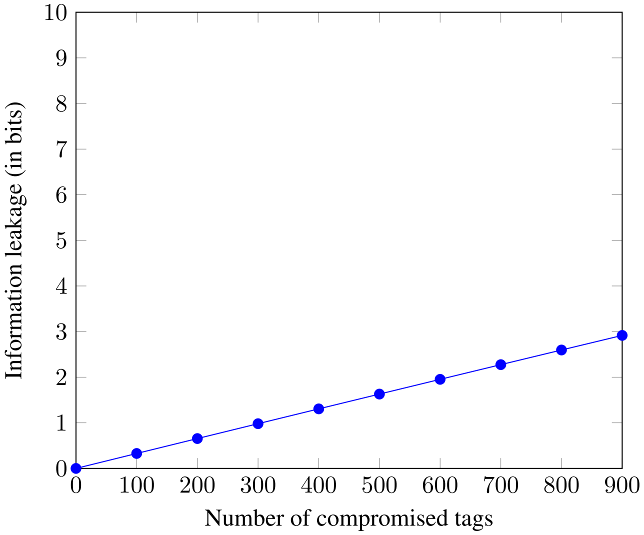


FIGURE 8. Level of privacy of the system based on information leakage in bits.

2) $X \lhd Y$: X receives a message that contains a statement Y from a network agent Z.
3) $X \;|\!\sim\; Y$: X has sent a message that contains Y to a network agent Z.
4) $\#X$: X is fresh.
5) $X \leftrightarrow YZ$: Y is a secret shared between X and Z.
6) $X \overset{Y}{\leftrightharpoons} Z$: Y is a shared statement between X and Z.
7) $X \vdash Y$: X can drive Y.

Rules:

Rule 1: $\frac{X|\equiv X \overset{Y}{\leftrightharpoons} YZ, X \lhd Y}{X|\equiv Z|\sim Y}$.

Rule 1 says that if a network agent X believes that Y is a shared secret between X and Z and receives a message Y, then X believes that Z has sent the message Y.

Rule 2: $\frac{X|\equiv \#R}{X|\equiv \#M,R}$.

Rule 2 means that if an entity X believes that a message R is fresh, then X believes that a message that contains R, i.e., $\{M, R\}$, is also fresh.

The BAN logic correctness proof is divided into five parts as below. In the proof, R stands for a reader, and T stands for a tag.

A. PROTOCOL DESCRIPTION

This subsection describes the messages transmitted between a reader and a tag.

1) R → T: $\{R_1\}$
2) T → R: $\{R_2, \gamma, g_{ij}\}$

B. PROTOCOL IDEALIZATION

Here, we rewrite protocol descriptions into BAN logic syntax.

1) R → T: T $\lhd \{R_1\}$
2) T → R: R $\lhd \{R_2, \gamma, g_{ij}\}$

C. INITIAL ASSUMPTION

Initial assumptions of the proposed protocol are as follows.

1) R $|\equiv \#R_2$
2) T $|\equiv \#R_1$
3) R $|\equiv R \leftrightarrow K_{ij}, ID_{ij}T$
4) R $|\equiv R \leftrightharpoons g_{ij}T$

D. PROTOCOL GOAL

The security goals of the proposed protocol are as follows.

1) T $|\equiv \#\gamma$
2) R $|\equiv T \;|\!\sim ID_{ij}$

E. PROOF PROCESS

From protocol idealization 1 and initial assumption 1, we can get

$$\begin{aligned}
&T \lhd R_1, T \;|\equiv \#R_1, \mathit{and}\\
&T \;|\equiv \gamma\\
&\vdash T \;|\equiv \beta \oplus (g_{ij} \ll wt(K_{ij} \oplus R_2)),\\
&\vdash T \;|\equiv (ID_{ij} \wedge R_1) \oplus\\
&(g_{ij} \ll wt(K_{ij} \oplus R_2)),\\
&\vdash T \;|\equiv \#((ID_{ij} \wedge R_1) \oplus\\
&(g_{ij} \ll wt(K_{ij} \oplus R_2))),\\
&(\mathit{by\ using\ \ Rule\ 2})\\
&\vdash T \;|\equiv \#\gamma
\end{aligned}$$

Hence, protocol goal 1 is proved.

According to initial assumptions 3, 4 and protocol idealization 2, we can get

$$\begin{aligned}
&R \lhd \{R_2, \gamma, g_{ij}\}, R \leftrightarrow K_{ij}, ID_{ij}T,\\
&R \lhd \{R_2, \gamma, g_{ij}\}\\
&\vdash R \lhd \{R_2, \beta \oplus (g_{ij} \ll wt(K_{ij}\\
&\oplus R_2)), g_{ij}\},\\
&\vdash R \lhd \beta,\\
&\vdash R \lhd ID_{ij}\\
&\vdash R \;|\equiv T \;|\sim ID_{ij}, \quad (\mathit{by\ using\ Rule\ 1})
\end{aligned}$$

Hence, protocol goal 2 is proved.

TABLE 3. Security performance comparison.

Protocol	SASI [9]	RAPP [38]	R^{2}AP [42]	SLAP [19]	Tewari [37]	Maurya [20]	Khor [17]	Fan [12]	Shariq [36]	Shamshad [33]	Chander [8]	Proposed
Private data leakage	✓	✓	✓	×	✓	×	✓	×	×	×	×	×
De-synchronization attack	✓	✓	✓	✓	✓	×	×	×	×	×	×	×
Impersonation attack	✓	×	×	✓	×	✓	×	×	×	×	✓	×
Traceability attack	✓	✓	✓	×	×	✓	×	×	×	ND	×	×
Tag anonymity	×	×	×	×	✓	×	×	×	×	×	×	×
Forward security	×	×	×	×	×	×	×	ND	×	×	×	×

✓- Vulnerable, ×- Not vulnerable, ND= Not defined.

TABLE 4. Computation cost performance comparison.

Protocol	Entity	SASI [9]	RAPP [38]	R^{2}AP [42]	SLAP [19]	Tewari [37]	Maurya [20]	Khor [17]	Fan [12]	Shariq [36]	Shamshad [33]	Chander [8]	Proposed
Reconstruction/Conversion/HF/SM	T	×	11 (Permutations)	14 (Reconstruction)	9 (Conversion)	×	1 (CRC)	×	2 (HF)	1 (ME), 1 (MI), 3 (HF)	2 (EPM)	9 (HF)	×
/Permutation/MM/MI/ME/EPM	R+S	×	11 (Permutations)	14(Reconstruction)	9(Conversion)	×	1 (MM), 1 (CRC)	×	2 (HF)	1 (ME), 1 (MI), 3 (HF), 1 (SM)	2 (EPM)	9 (HF)	2(MM)
Bit- Rotation with w(t)	T	2	2	4	2	6	×	9	1	×	×	×	1
	R+S	2	2	5	2	6	×	9	1	×	×	×	1
E()/D()	T	×	×	×	×	×	×	×	1	×	×	×	×
	R+S	×	×	×	×	×	×	×	4	×	3	×	×
No. of PRNG	T	×	×	×	×	×	1	1	×	2	1	1	1
	R+S	2	2	2	1	2	1	3	1	1	2	2	1
No. of basic operations	T	16	17	13	9	11	2	13	3	4	15	15	3
(OR, AND, XOR, Addition)	R+S	12	17	13	9	11	2	12	6	4	12	41	2
Searching complexity		$O(N)$	$O(N)$	$O(N)$	$O(N)$	$O(N)$	$O(1)$	$O(1)$	$O(1)$	$O(N)$	$O(N)$	$O(1)$	$O(1)$
No. of authentication steps		4	5	5	4	4	2	4	4	3	4	7	2
Communication overhead	$T \rightarrow R$	$4L$	$2L$	$5L$	$3L$	$2L$	$2L$	$3L$	$3L$	$3L$	$2L$	$2L$	$3L$
	$R \rightarrow T$	$7L$	$4L$	$3L$	$4L$	$3L$	$1L$	$3L$	$2L$	$4L$	$4L$	$4L$	$1L$
Required memory	T	$7L$	$4L$	$5L$	$7L$	$7L$	$2L$	$5L$	$3L$	$4L$	$8L$	$2L$	$3L$

T - Tag-side, R - Reader-side, S - Server-side, MM - Matrix multiplication, E()/D()-Symmetric key encryption/Decryption, ME- Modular exponentiation, MI= Modular inverse, HF= Hash function, SM- Scalar multiplication, EPM= Elliptic curve point multiplication.

XI. PERFORMANCE ANALYSIS

In this section, we compare computation efforts (given in Table 4) of our proposed protocol with some other related protocols [8], [9], [12], [17], [19], [20], [33], [36], [37], [38], [42].

It is mandatory that a cryptographic protocol be liberated from security attacks with sensible complexities like computation and communication costs as well as storage costs. From Table 4, it can be easily observed that our proposed protocol performs extremely fewer computational operations than the others without sacrificing its security features. Subsequently, these features make our proposed protocol more suitable for a low-cost RFID system in comparison to other existing protocols. The details of the performance analysis are as follows.

A. COMPUTATION COST

Table 4 shows the computational cost of the proposed scheme along with the other related protocols. The protocol (SASI) [9] used total 28 basic operations, two PRNG, and four bit-wise operations. Tian et al. [38] (RAPP) protocol used total 22 permutation operations, four bit-wise operations, 34 basic operations. Zhuang et al. [43] (R^2AP) protocol used total 28 reconstruction operations, nine bit-wise operations, two PRNG, and 26 basic operations. Luo et al. [19] (SLAP) protocol used total 18 conversion operations, four bit-wise operations, and 18 basic operations. Tewari and Gupta [37] used a total 12 bit-wise operations, two PRNG, and 22 basic operations. Maurya et al. [20] protocol employed one cyclic redundancy check (CRC), one PRNG, one matrix multiplication, and four basic operations. Khor et al. [17] protocol used total 18 bit-wise operations, four PRNG, and 25 basic operations. Fan et al. [12] protocol used two bit-wise operations, five encryption/decryption operations, one PRNG, and nine basic operations. Shariq et al. [36] protocol used high computational modular operations, six hash functions, three PRNG, and eight basic operations.

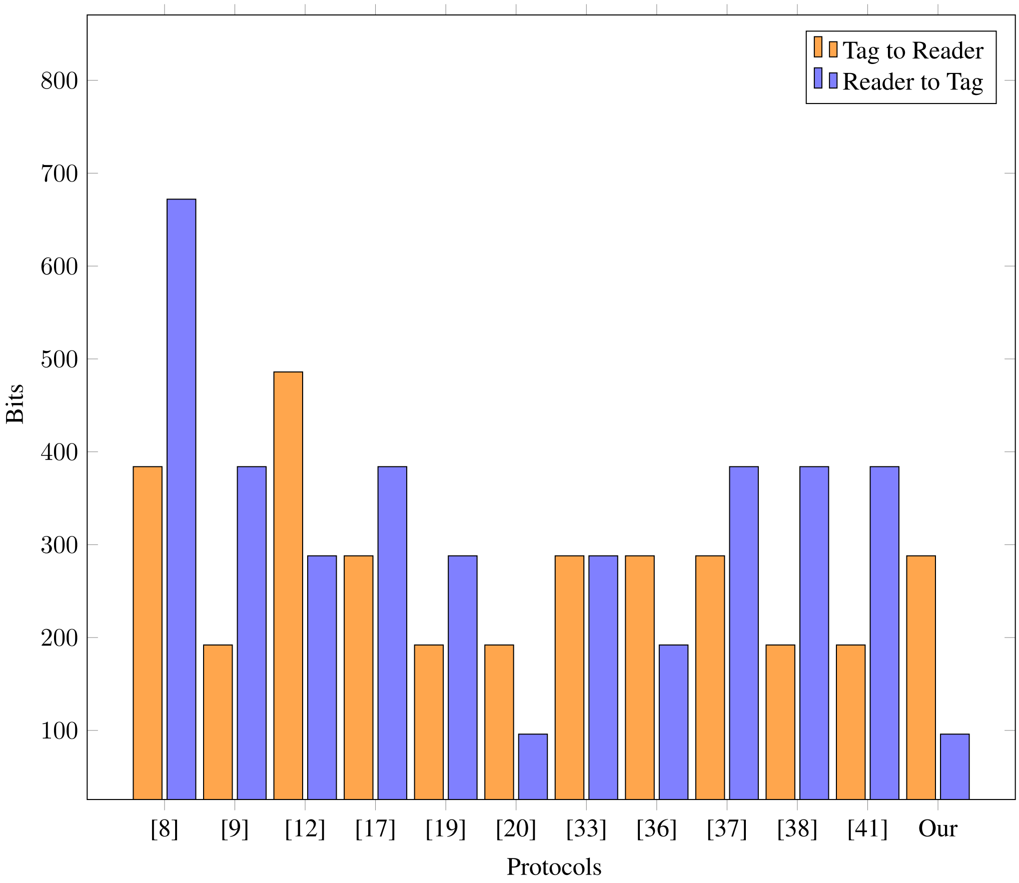


FIGURE 9. Communication cost analysis.

Shamshad et al. [33] protocol used a total of four elliptic curve point multiplication, three encryption/decryption operations, three PRNG, and 27 basic operations. Chander and Gopalakrishnan [8] protocol used a total of 18 hash functions, 3 PRNG, and 56 basic operations. Additionally, in a large-scale environment, a protocol is unsustainable if its search complexity is $O(N)$. The proposed protocol has a searching complexity of $O(1)$, but some related protocols have a complexity of $O(N)$, as shown in Table 4.

In contrast, the proposed protocol does not employ any specific operation like hash function, elliptic curve point operation, modular operation, CRC, permutation, and encryption/decryption operations. In our approach, the tag involves only one hamming weight-based left rotation, three basic operations, and one PRNG. These operations are very low-cost and easily be implemented in low-cost passive tags. On the server side, the proposed protocol employs only two matrix multiplication, one hamming weight-based left rotation, three basic operations and one PRNG to authenticate a tag. Therefore, the computation cost of the proposed protocol is less compared to the related existing protocols given in Table 4.

B. COMMUNICATION COST

In the proposed protocol, we assume that all the parameters are of length $L(=96)$ bits. The reader sends L bits message to the tag, and the tag sends $3L$ bits message to the reader in the proposed scheme. Following that, the proposed protocol's communication cost from reader to tag is 96 bits and from tag to reader is $3L = 3 \times 96 = 288$ bits. Thus, the total communication cost of the proposed scheme is 384 bits. A graphical representation of communication cost comparison from tag to reader and reader to tag is shown in Figure 9. According to this representation, it indicates that the communication cost of the proposed protocol is lower than the other protocols except the protocol [20]. But this protocol is vulnerable to impersonation attacks and traceability attacks. Consequently, the proposed protocol is more suitable than the other protocols.

C. STORAGE COST

The key information stored in the tag may be stolen by an adversary, so less key storage in the tag memory can bring higher security to the RFID system. In the proposed protocol, each tag requires only $3L$ bits for storing its static secret information, where L denotes the length of each parameter used in this protocol. We give a graphical representation of the storage costs in Figure 10 by considering $L = 96$. The storage requirement of the proposed protocol is less than the other protocols except that Chander and Gopalakrishnan [8] and Maurya et al. [20] protocols. Maurya et al.'s [20] protocol suffers from impersonation and traceability attacks, and Chander and Gopalakrishnan's [8] protocol used more

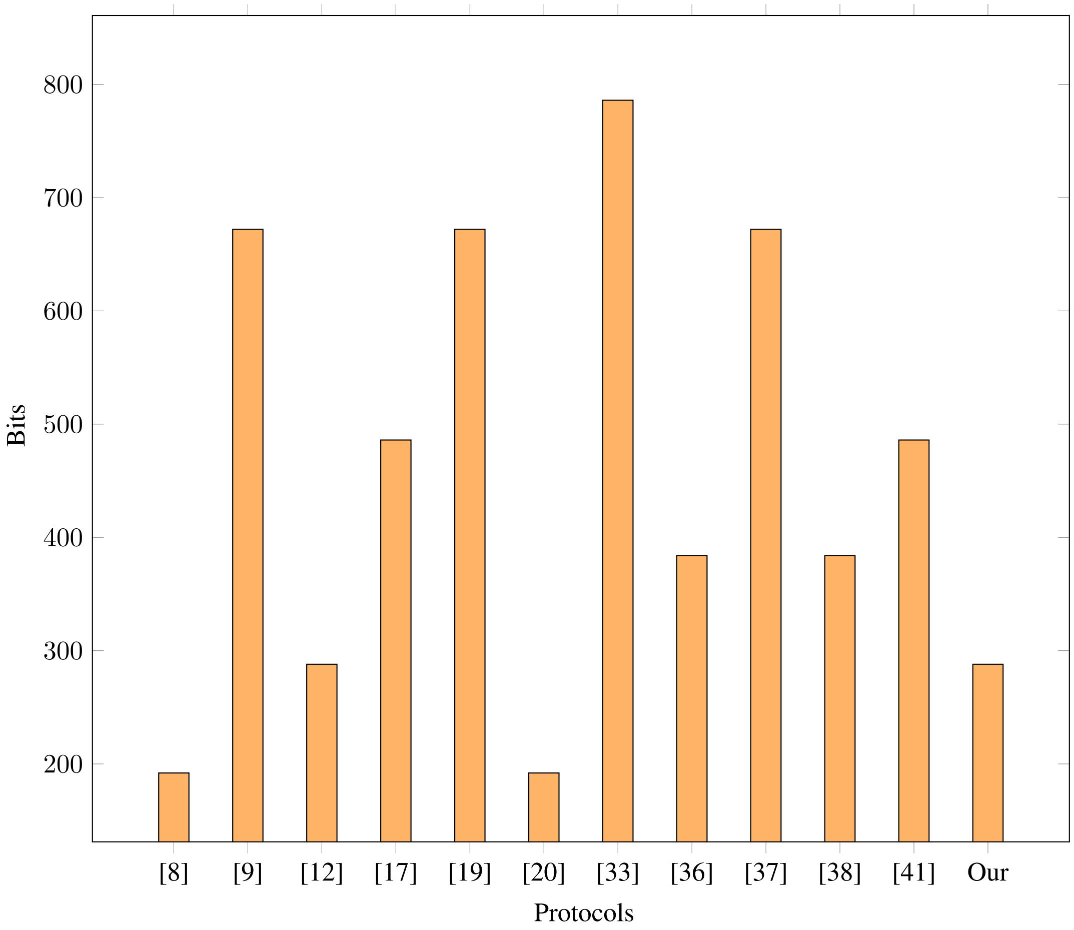


FIGURE 10. Storage cost analysis.

computation compared to the proposed protocol. Therefore, the proposed protocol is more efficient and can be suitable for RFID systems with limited costs.

XII. CONCLUSION

This paper proposes an ultralightweight authentication protocol for an RFID system based on MDS code. The protocol uses properties of MDS codes and group homomorphism to reduce computational costs without compromising security features. We have analyzed the security features of the proposed protocol under a random oracle model, which shows that the protocol preserves information privacy as well as untraceability. The informal security analysis of the proposed protocol shows that the protocol resists all possible well-known threats. The simulation results of the proposed protocol under AVISPA and Scyther tools show that the protocol is safe against various attacks. The simulation result of the measurement of the level of privacy shows that the protocol attains a higher level of privacy and discloses a very small amount of information when some tags are compromised in the system. We demonstrate the correctness of the proposed protocol by using BAN logic. The performance analysis of the proposed protocol illustrates that the protocol employs only bit-wise operators on the tag side to perform computational work. The rigorous analysis of the proposed protocol confirms that the proposed protocol achieves all desirable security features under the resource constraints environment of the RFID system.

REFERENCES

[1] A. K. Agrahari and S. Varma, “A provably secure RFID authentication protocol based on ECQV for the medical Internet of Things,” *Peer Peer Netw. Appl.*, vol. 14, no. 3, pp. 1277–1289, May 2021.

[2] S. Akleylek and M. Soysaldı, “A new lattice-based authentication scheme for IoT,” *J. Inf. Secur. Appl.*, vol. 64, Feb. 2022, Art. no. 103053.

[3] G. Avoine, L. Buttyant, T. Holczer, and I. Vajda, “Group-based private authentication,” in *Proc. IEEE Int. Symp. World Wireless, Mobile Multimedia Netw.*, Jun. 2007, pp. 1–6.

[4] Q. U. Ain, Y. Mahmood, U. Mujahid, and M. Najam-ul-Islam, “Cryptanalysis of mutual ultralightweight authentication protocols: SASI & RAPP,” in *Proc. Int. Conf. Open Source Syst. Technol.*, Dec. 2014, pp. 136–145.

[5] L. Buttyán, T. Holczer, and I. Vajda, *Optimal Key-Trees for Tree-Based Private Authentication*. Berlin, Germany: Springer, 2006.

[6] T. Cao, E. Bertino, and H. Lei, “Security analysis of the SASI protocol,” *IEEE Trans. Depend. Secure Comput.*, vol. 6, no. 1, pp. 73–77, Jan. 2009.

[7] J. C. Hernandez-Castro, J. M. E. Tapiador, P. Peris-Lopez, and J.-J. Quisquater, “Cryptanalysis of the SASI ultralightweight RFID authentication protocol with modular rotations,” 2008, *arXiv:0811.4257*.

[8] B. Chander and K. Gopalakrishnan, “A secured and lightweight RFID-tag based authentication protocol with privacy-preserving in telecare medicine information system,” *Comput. Commun.*, vol. 191, pp. 425–437, Jul. 2022.

[9] H.-Y. Chien, "SASI: A new ultralightweight RFID authentication protocol providing strong authentication and strong integrity," *IEEE Trans. Depend. Secure Comput.*, vol. 4, no. 4, pp. 337–340, Oct./Dec. 2007.

[10] R. Das, *RFID Forecasts, Players and Opportunities 2016–2026*. Cambridge, U.K.: IDTechEx, 2019.

[11] M. David and N.-R. Prasad, "Providing strong security and high privacy in low-cost RFID networks," in *Proc. Int. Conf. Secur. Privacy Mobile Inf. Commun. Syst.* (Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering), vol. 17. Berlin, Germany: Springer, 2009.

[12] K. Fan, Q. Luo, K. Zhang, and Y. Yang, "Cloud-based lightweight secure RFID mutual authentication protocol in IoT," *Inf. Sci.*, vol. 527, pp. 329–340, Jul. 2020.

[13] J.-A. Gallian, *Contemporary Abstract Algebra*. Boston, MA, USA: Cengage Learning, 2016.

[14] J.-C. Hernandez-Castro, P. Peris-Lopez, R. C. W. Phan, and J. M. E. Tapiador, "Cryptanalysis of the David-Prasad RFID ultralightweight authentication protocol," in *Radio Frequency Identification: Security and Privacy Issues* (Lecture Notes in Computer Science), vol. 6370. Berlin, Germany: Springer, 2010.

[15] A. Juels and S. A. Weis, "Defining strong privacy for RFID," *ACM Trans. Inf. Syst. Secur.*, vol. 13, no. 1, pp. 1–23, Oct. 2009.

[16] M. Khalid, U. Mujahid, and M. Najam-ul-Islam, "Cryptanalysis of ultralightweight mutual authentication protocol for radio frequency identification enabled Internet of Things networks," *Int. J. Distrib. Sensor Netw.*, vol. 14, no. 8, Aug. 2018, Art. no. 155014771879512.

[17] J. H. Khor and M. Sidorov, "Weakness of ultra-lightweight mutual authentication PRotocol for IoT devices using RFlD tags," in *Proc. 8th Int. Conf. Inf. Sci. Technol. (ICIST)*, Jun. 2018, pp. 91–97.

[18] S. Ling and C. Xing, *Coding Theory*. Cambridge, U.K.: Cambridge Univ. Press, 2004.

[19] H. Luo, G. Wen, J. Su, and Z. Huang, "SLAP: Succinct and lightweight authentication protocol for low-cost RFID system," *Wireless Netw.*, vol. 24, no. 1, pp. 69–78, 2018.

[20] P. K. Maurya, J. Pal, and S. Bagchi, "A coding theory based ultralightweight RFID authentication protocol with CRC," *Wireless Pers. Commun.*, vol. 97, no. 1, pp. 967–976, Nov. 2017.

[21] P. K. Maurya and S. Bagchi, "A secure PUF-based unilateral authentication scheme for RFID system," *Wireless Pers. Commun.*, vol. 103, no. 2, pp. 1699–1712, 2018.

[22] P. K. Maurya and S. Bagchi, "Cyclic group based mutual authentication protocol for RFID system," *Wireless Netw.*, vol. 26, no. 2, pp. 1005–1015, Feb. 2020.

[23] B. Mbarek, M. Ge, and T. Pitner, "An efficient mutual authentication scheme for Internet of Things," *Internet Things*, vol. 9, pp. 100–106, 2020.

[24] U. Mujahid, G. Unabia, H. Choi, and B. Tran, "A review of ultralightweight mutual authentication protocols," *Int. J. Electr. Comput. Eng.*, vol. 14, no. 4, pp. 96–101, 2020.

[25] D. Noori, H. Shakeri, and M. Niazi Torshiz, "Scalable, efficient, and secure RFID with elliptic curve cryptosystem for Internet of Things in healthcare environment," *EURASIP J. Inf. Secur.*, vol. 2020, no. 1, pp. 1–11, Dec. 2020.

[26] P. Peris-Lopez, J. Hernandez-Castro, J. Estevez-Tapiador, and A. Ribagorda, "M2AP: A minimalist mutual-authentication protocol for low-cost RFID tags," in *Proc. Int. Conf. Ubiquitous Intell. Comput.*, vol. 4159. Wuhan, China, Sep. 2006, pp. 912–923.

[27] S. Qiu, G. Xu, H. Ahmad, and L. Wang, "A robust mutual authentication scheme based on elliptic curve cryptography for telecare medical information systems," *IEEE Access*, vol. 6, pp. 7452–7463, 2018.

[28] F. Rahman, M. E. Hoque, and S. I. Ahamed, "AnonPri: A secure anonymous private authentication protocol for RFID systems," *Inf. Sci.*, vol. 379, pp. 195–210, Feb. 2017.

[29] S. Rostampour, N. Bagheri, Y. Bendavid, M. Safkhani, S. Kumari, and J. J. P. C. Rodrigues, "An authentication protocol for next generation of constrained IoT systems," *IEEE Internet Things J.*, vol. 9, no. 21, pp. 21493–21504, Nov. 2022.

[30] M. Safkhani and N. Bagheri, "Generalized de-synchronization attack on UMAP: Application to RCIA, KMAP, SLAP and SASI$^+$ protocols," Cryptol. ePrint Arch., Tech. Rep. 2016/905, 2016. [Online]. Available: https://eprint.iacr.org/2016/905

[31] M. Safkhani, "Cryptanalysis of R^{2}AP, an ultralightweight authentication protocol for RFID," *J. Electr. Comput. Eng. Innov.*, vol. 6, no. 1, pp. 107–114, 2018.

[32] M. Safkhani and N. Bagheri, "Cryptanalysis of two recently proposed ultralightweight authentication protocol for IoT," 2019, *arXiv:1907.11322*.

[33] S. Shamshad, M. F. Ayub, K. Mahmood, S. Kumari, S. A. Chaudhry, and C.-M. Chen, "An enhanced scheme for mutual authentication for healthcare services," *Digit. Commun. Netw.*, vol. 8, no. 2, pp. 150–161, Apr. 2022.

[34] C. E. Shannon, "A mathematical theory of communication," *ACM SIGMOBILE Mobile Comput. Commun. Rev.*, vol. 5, no. 1, pp. 3–55, Jan. 2001.

[35] M. Shariq and K. Singh, "A novel vector-space-based lightweight privacy-preserving RFID authentication protocol for IoT environment," *J. Supercomput.*, vol. 77, no. 8, pp. 8532–8562, Aug. 2021.

[36] M. Shariq, K. Singh, M. Y. Bajuri, A. A. Pantelous, A. Ahmadian, and M. Salimi, "A secure and reliable RFID authentication protocol using digital schnorr cryptosystem for IoT-enabled healthcare in COVID-19 scenario," *Sustain. Cities Soc.*, vol. 75, Dec. 2021, Art. no. 103354.

[37] A. Tewari and B. B. Gupta, "Cryptanalysis of a novel ultra-lightweight mutual authentication protocol for IoT devices using RFID tags," *J. Supercomput.*, vol. 73, no. 3, pp. 1085–1102, Mar. 2017.

[38] Y. Tian, G. Chen, and J. Li, "A new ultralightweight RFID authentication protocol with permutation," *IEEE Commun. Lett.*, vol. 16, no. 5, pp. 702–705, May 2012.

[39] K.-H. Wang, C.-M. Chen, W. Fang, and T.-Y. Wu, "On the security of a new ultra-lightweight authentication protocol in IoT environment for RFID tags," *J. Supercomput.*, vol. 74, no. 1, pp. 65–70, 2018.

[40] L. Xiao, S. Xie, D. Han, W. Liang, J. Guo, and W.-K. Chou, "A lightweight authentication scheme for telecare medical information system," *Connection Sci.*, vol. 33, no. 3, pp. 769–785, Jul. 2021.

[41] M. I. Younis and M. H. Abdulkareem, "ITPMAP: An improved three-pass mutual authentication protocol for secure RFID systems," *Wireless Pers. Commun.*, vol. 96, no. 1, pp. 65–101, Sep. 2017.

[42] X. Zhuang, Y. Zhu, and C. C. Chang, "A new ultralightweight RFID protocol for low-cost tags: R2AP," *Wireless Pers. Commun.*, vol. 79, no. 3, pp. 1787–1802, Jul. 2014.

[43] X. Zhuang, Y. Zhu, C.-C. Chang, and Q. Peng, "Security issues in ultralightweight RFID authentication protocols," *Wireless Pers. Commun.*, vol. 98, no. 1, pp. 779–814, Jan. 2018.

PRAMOD KUMAR MAURYA received the M.Sc. degree in mathematics from the University of Allahabad, India, in 2011, the M.Tech. degree in computer science and data processing from IIT Kharagpur, India, in 2014, and the Ph.D. degree in mathematics from NIT Durgapur, in 2019. He is currently working as an Assistant Professor with the School of Computer Science and Engineering, Vellore Institute of Technology (VIT), Vellore, India. His research interests include identity authentication, RFID security, and information security.

HARADHAN GHOSH received the B.Sc. degree in mathematics from The University of Burdwan, West Bengal, India, in 2017, and the M.Sc. degree in mathematics from Visva-Bharati University, West Bengal, in 2019. He is currently pursuing the Ph.D. degree with the Department of Mathematics, NIT Durgapur, India. His research interests include RFID security, cryptographic protocol, and coding theory.

SATYA BAGCHI received the B.Sc., M.Sc., and Ph.D. degrees in mathematics from the University of Kalyani, West Bengal, India, in 2002, 2004, and 2013, respectively. He is currently an Associate Professor with the Department of Mathematics, National Institute of Technology at Durgapur, Durgapur, India. His current research interests include RFID security protocol design, cryptography, and coding theory. He is a Life Member of the Cryptology Research Society of India (CRSI).