Peer-to-Peer Networking and Applications (2025) 18:317
https://doi.org/10.1007/s12083-025-02128-z

RESEARCH

Authentication protocol for RFID-enabled TMIS: An LCD code-based approach

Haradhan Ghosh[1] · **Pramod Kumar Maurya**[2,3] · **Satya Bagchi**[1]

Received: 25 January 2025 / Accepted: 17 September 2025 / Published online: 30 October 2025

Abstract
Radio frequency identification (RFID) is a wireless technology used to identify objects without line-of-sight contact. RFID technology has many applications in the medical field because it ensures security and reliability. Telecare medical information systems (TMIS) have recently received prominent attention in healthcare systems. The combination of an RFID system and TMIS gives various advantages, like reducing administrative costs, improving the quality of services, keeping accurate medical records, etc. Through TMIS, the patient's medical information is transferred via radio waves in the RFID system. Due to wireless communication, there are many security and privacy issues associated with TMIS systems, such as private data leakage, traceability attacks, replay attacks, man-in-middle attacks, etc. To ensure secure communication in TMIS, we introduce a lightweight mutual authentication protocol by employing LCD code properties. The protocol's formal security is done using BAN logic and the Scyther tool. We show that tags untraceability and sensitive information protection are preserved using Juels and Weis's privacy model. In addition, we analyze the performance of the protocol in terms of processing, transmission, and storage costs.

Keywords RFID systems · Authentication protocol · Linear codes · Security · Privacy · TMIS

1 Introduction

In recent years, e-health and telemedicine services have become more popular. With e-Health and telemedicine services, people can access medical facilities such as primary care consultations, psychotherapy, remote monitoring, treatment, and emergency services. Through the development of TMIS, people can consult doctors online, bringing about substantial improvements. Instead of going to the hospital, people can access telemedicine services from the convenience of their own homes because people may be affected by other patients in the hospital. Patients and doctors are more at ease with the treatment approach because of TMIS's procedures. The TMIS is helpful for various healthcare services that are required due to the current demand in the healthcare sector. These programmes offer patients at-home support for private healthcare. The network's technological advancement has improved healthcare services. As a result, the patient can access medical services via electronic devices. One of the popular research topics in IoT healthcare applications is RFID-based identification for the TMIS domain. An RFID system can peruse and store data precisely, so it assumes an extraordinarily significant part in the development of TMIS. The RFID system makes the hospital's workflow [33] more automated, supplies patients with additional advantages with more clinical choices, and reduces medical costs.

RFID technologies are useful for low-cost devices that identify assets via radio waves [14, 15]. An RFID system comprises the following elements [26]; RFID reader, RFID tags, and a back-end server. Tags are electronic microchips usually containing private and fundamental data about the items. The reader attempts to constantly lay out an

✉ Haradhan Ghosh
hg.20ma1104@phd.nitdgp.ac.in

Pramod Kumar Maurya
pramod.maurya@bmu.edu.in

Satya Bagchi
sbagchi.maths@nitdgp.ac.in

[1] School of Mathematical Sciences, National Institute of Science Education and Research Bhubaneswar, Bhubaneswar 752050, India

[2] Department of Mathematics, National Institute of Technology Durgapur, Durgapur 713209, India

[3] School of Engineering and Technology, BML Munjal University, Gurugram 122413, India

association with the tag to separate the data from it. The server receives a tag's associated information via a reader for processing. RFID enables higher levels of security than traditional barcodes, as RFID tags are more sensitive and resourceful than barcodes. RFID is being used in a variety of healthcare settings, including counting regions following clinical resources, newborn and patient-recognized proof, clinical treatment following, consent, and patient tracking. In an RFID-enabled TMIS system [5, 22, 41], patient identification is given by a wearable device that contains a tag. The tag could contain relevant data for clinical staff to obtain blood classification, date of birth, sensitivities, and prescriptions. A nurse can retrieve the patient's records from the tag using a reader. The information is then sent to a server so that doctors can view the patient record's remotely, which makes it easier for them to keep an eye on each patient.

With the TMIS [7], sensitive information is shared among doctors, patients, insurance companies, etc. However, the interconnection nature of TMIS creates several privacy and security issues, such as unauthorized access to patient records, valuable financial information, insurance information, etc. Nowadays, protecting healthcare data is vital considering the number of cyber-criminals launched malicious attacks. To overcome security and privacy concerns, TMIS requires a mechanism that only authorized persons can access sensitive information. Authentication is an excellent way to check the authenticity of a person who wants to access sensitive information. An effective RFID authentication protocol helps in preserving privacy in the TMIS system. Therefore, it becomes very vital and appealing to build RFID ultralightweight protocols with high-security functionalities at low expenses in TMIS.

1.1 Motivation

Researchers have presented many authentication protocols [9, 20, 27, 29, 36, 38, 42] by using some cryptographic primitives. However, due to the computational and storage costs in TMIS, they are unsuitable for tiny powered tags. Additionally, an adversary can intercept, alter, or tamper with a patient's sensitive data over a wireless channel. For this reason, there are many protocols [5, 6, 18, 28] where common security attacks can occur over the channel. Therefore, it is difficult to formulate a TMIS protocol that is both practical and reasonable. With LCD codes over a finite field, we have developed a secure and trustworthy RFID authentication protocol for inexpensive tags that can address present TMIS problems.

The primary objectives of the proposed protocol are given below:

1. To achieve common verification between the tag and the server via the reader.
2. To preserve tag anonymity and tag location privacy.
3. To conquer known attacks like disclosure, de-synchronization, traceability, etc.
4. To optimize storage cost, communication cost and computation cost.

1.2 Our contribution

Based on LCD codes, the present work provides a mutual authentication mechanism over TMIS. The following is a summary of the most important contributions.

1. To reduce the computational cost, we only used the left shift operator, concatenation, bitwise operations, and fundamental properties of LCD codes over finite fields.
2. The Scyther tools and BAN principles are used to evaluate the basic security.
3. By applying Juels and Weis model, we prove that our protocol preserves tags untraceability.
4. Our protocol is compared to some similar protocols regarding communication and computational costs.

2 Related work

In this decade, several RFID authentication protocols have been designed for security purposes. Many authors have proposed authentication protocols, but they are unsuitable for resource-constrained tags due to their high computational storage costs and other various reasons. So, it is not easy to present a safe and identifying RFID protocol in TMIS. Therefore, we have discussed some existing related protocols with their leverages and shortcomings.

Sun et al. [35] presented an RFID-based protocol using the integration of barcodes and RFID tags. This protocol demonstrated a compelling and safe patient care environment for preventing the danger of medication blunders. Later, Huang and Ku [17] designed an RFID grouping proof protocol for the medication well-being of inpatients. This protocol becomes lightweight as it is used the pseudo-random number generator (PRNG) and cyclic redundancy code (CRC). Chien et al. [8] proved that the protocol [17] suffers from replay attacks and de-synchronizations. Then, they proposed two RFID protocols, one for the online case and another for the offline case, to improve medication security.

Tian et al. [37] represented an RFID-based protocol using permutation operation, XOR, a circular left rotation on tags. Later, Ahmadian et al. [1] performed the cryptanalysis of [37] and demonstrated the security weakness in contrast to the de-synchronization attack. Wu et al. [40] suggested a novel password enable authentication protocol in TMIS, attracting many researchers in this field. In this protocol, the authors have used symmetric cryptography and discrete

logarithm problem as cryptographic primitives. The password change phase cannot be verified using this protocol.

In light of coding theory, Maurya et al. [24] presented an ultralightweight authentication protocol. The protocol used CRC and syndrome decoding techniques for better security, privacy, and low computational costs. Also, they compared their protocol with some related protocols in terms of security and computational costs and showed that the protocol provides better security with much less computational cost. Aghili and Mala [2] show that the protocol [24] is defenceless against tag impersonation and tag traceability attacks.

Fan et al. [11] proposed an RFID-based ultralightweight authentication protocol using left rotation, random number generators, XOR, and concatenation operations. The protocol [11], however, is not ideal for dealing with rogue RFID tags or cloud providers. After that, Fan et al. [12] suggested an RFID-based protocol for healthcare protection in the IoT. The protocol used cross operation, rotation, and bit-wise XOR to provide the authentication. Later, Khan et al. [21] addressed some security flaws of the protocol [12], which include tag anonymity and traceability attacks.

Salem and Amin [30] proposed an RFID protocol for a secure TMIS based on the El-Gamal cryptosystem. Also, they analyze the formal security by AVISPA tools. However, this protocol has an excessively high storage expense. Maurya and Bagchi [25] designed a group-based protocol for RFID systems utilizing left shift and modulo operations.

Shariq and Singh [31] proposed a lightweight RFID protocol that incorporates the properties of vector space. Utilizing BAN logic, the protocol's accuracy has been completed. Wang et al. [39] designed an ultralightweight RFID protocol for the protection of medical privacy in modern life using Bit-Crossing XOR and cyclic shift operations. Later, Gao and Lu's [13] designed an ultralightweight authentication protocol in a passive RFID system. This protocol used bitwise XOR and circular left-rotation operations and verified security using GNY (Gong, Needham, and Yahalom) logic.

Chander and Gopalakrishnan [5] suggested a TMIS authentication method to lessen the computational burden on mobile nodes with limited resources. Using the Scyther and AVISPA tools, the authors analyze the security of the protocol. This protocol, however, is liable to modification and impersonation attacks. Kumar et al. [22] designed an ultralightweight RFID authentication protocol for healthcare systems to improve medication safety for patients. The protocol employs reformation operation, bitwise XOR, and circular left–right rotations. The formal security analysis of the protocol is performed by the Scyther tool.

Studying the existing approaches, we observe that each one has certain drawbacks or may not be appropriate for a low-cost tag. Accordingly, we presented a reliable and efficient authentication protocol for TMIS for low-cost tags.

3 Preliminaries

In this section, we discussed some preliminaries about LCD codes and their properties.

3.1 Linear codes

Suppose p is a prime and $\mathbb{F}_q$ is a finite field, where q is a power of p. A linear code D of length n is a subspace of $\mathbb{F}_q^n$. It is denoted by $D = [n, k]$, where k represents the dimension of the subspace. An element of the code D is called a codeword. As D is a subspace, there exists a basis $b_1, b_2, \ldots, b_k$. A matrix whose rows generate the codeword of D is known as a generator matrix G. The dual or orthogonal code of D is denoted by $D^{\perp}$, and is defined as $D^{\perp} = \{b \in \mathbb{F}_q^n : a \cdot b = 0 \ \forall a \in D\}$. A parity-check matrix H of D is the generator matrix of $D^{\perp}$. A linear code D is called a linear complementary dual (LCD) code if D meets $D^{\perp}$ trivially [23].

Lemma 3.1 *Let D be a linear code over $\mathbb{F}_q$ with G and H, then D becomes an linear complementary dual code if and only if $\begin{pmatrix} G \\ H \end{pmatrix}$ is invertible [23].*

3.2 Secret codeword recovery

Let $D = [n, k]$ be an LCD code over $\mathbb{F}_q^n$ with G and H. Let $X = x_1 x_2 \ldots x_n$ be a codeword of D and $Y^T = G \cdot X^T$. We assume that X is a secret codeword that we have to find out. Suppose we know G, H, and the value of Y^T. Using these parameters, we can get a secret codeword X as follows.

As we know

$$G \cdot X^T = Y^T \tag{3.1}$$

The system of equations' solution set (3.1) forms an affine space with associated vector space $D^{\perp}$. Because D is an LCD code, the system of Eq. 3.1 admits a unique solution in D. We can get a unique solution by solving the following linear system.

$$\begin{pmatrix} G \\ H \end{pmatrix} X^T = \begin{pmatrix} Y^T \\ 0 \end{pmatrix}.$$

4 Proposed protocol

The proposed protocol is split into two parts, the first of which presents the initialization phase and the second of which presents the authentication phase. The notation

definitions are given in Table 1, and the flow diagram of the proposed protocol is given in Fig. 1. The notations K_R and K_L denote the right and left parts of K, respectively. If the number of bits in *K* is *n*, then K_R is the first $\frac{n}{2}$ bits and K_L is the last $\frac{n}{2}$ bits of *K*. The same meaning applies to all other parameters used in the proposed protocol in left (*L*) or right (*R*) form.

4.1 Assumption

The proposed protocol operates under the accompanying important suppositions listed below:

1. The random number(s) is/are generated by the legitimate tag ($\mathcal{T}$) and the legitimate reader ($\mathcal{R}$).
2. An adversary in the system can fake a correct $\mathcal{R}$ or a valid $\mathcal{T}$.
3. An adversary has the ability to block, adjust, or even tamper with all messages during communication.
4. The connecting channel is considered to be secure between $\mathcal{R}$ and the back-end server ($\mathcal{S}$).
5. The back-end server is regarded as trustworthy, and the communication route between $\mathcal{R}$ and the $\mathcal{S}$ is safe.
6. The connecting channel is considered insecure between $\mathcal{T}$ and $\mathcal{R}$.

4.2 Initialization phase

1. Because the basis of a linear space is not unique, neither is the generator matrix of a linear code. As a result, we must indicate which generating matrix is utilized. Regarding this, the manufacturer chooses an LCD code $D = [n, k]$. The initiator stores an arbitrary but fixed generator matrix *G* and a corresponding parity check matrix *H* on the server.

Table 1 Proposed protocol employs notations and explanations

Notation	Explanation
D	An LCD code.
G	A generator matrix of *D*.
H	A parity-check matrix of *D*.
IDS	Index pseudonym of a tag.
ID	Tag's unique identifying number.
$r_1,\ r_2$	Random number produced by a reader.
K	Tag's secret key.
K_R	First $\frac{n}{2}$ bits of *K*.
K_L	Last $\frac{n}{2}$ bits of *K*.
$\ll$	Circular left shift operator.
$\|\|$	Concatenation.
$\oplus$	Exclusive-or operator.

2. The initiator chooses a unique codeword *ID* from *D* and assigns it as a tag's distinctive identifying number. In addition, it calculates a vector $Y = (y_1, y_2, \ldots, y_k)$, where $y_i = g_i \cdot ID^T$. Here, g_i is the i^{th} row of *G*. The initiator stocks *Y* to the tag's memory and chooses a key *K* and a pseudonym *IDS* for each tag, where *IDS* works as an index in the database.
3. The initiator stores *ID*, *K* and *IDS* for each $\mathcal{T}$ with the server ($\mathcal{S}$). In addition, for each $\mathcal{T}$, $\mathcal{S}$ stores a new pseudonym IDS_{new}. Initially, IDS_{new} is *NULL*. The communication route between $\mathcal{R}$ and $\mathcal{S}$ is thought to be secure. Thus, $\mathcal{R}$ and $\mathcal{S}$ may be regarded as a single entity.

4.3 Authentication phase

This phase consists of the following steps.

1. Whenever a tag ($\mathcal{T}$) enters the scan area of a reader ($\mathcal{R}$), $\mathcal{T}$ gets a message from $\mathcal{R}$.
2. Then $\mathcal{T}$ transmits its *IDS* to $\mathcal{R}$.
3. After getting *IDS* from $\mathcal{T}$, $\mathcal{R}$ performs the following steps:
   - $\mathcal{R}$ match *IDS* with stored IDS_{old} and IDS_{new}. If a match is made, $\mathcal{R}$ retrieves $\mathcal{T}$'s pairing values *K* and *ID*.
   - After that, $\mathcal{R}$ generates two nonce r_1, r_2 and sends $\alpha = r_1 \oplus K$ and $\beta = r_2 \oplus K$ to $\mathcal{T}$.
4. $\mathcal{T}$ extracts r_1 and r_2 from α and β respectively. $\mathcal{T}$ calculates $\gamma = Y^T \oplus ((r_{1_L} \parallel K_R) \ll wt(r_{2_R} \parallel K_L))$ and transmits γ to $\mathcal{R}$.
5. Upon receiving γ from $\mathcal{T}$, $\mathcal{R}$ performs the following steps:
   - $\mathcal{R}$ calculates $Y'^T = \gamma \oplus ((r_{1_L} \parallel K_R) \ll wt(r_{2_R} \parallel K_L))$ and solves the system of linear equations $\begin{pmatrix} G \\ H \end{pmatrix} X^T = \begin{pmatrix} Y'^T \\ 0 \end{pmatrix}$ and get a unique solution $X = (x_1, x_2, \ldots, x_n)$.
   - $\mathcal{R}$ checks whether fetched *ID* is the same as *X* or not. If it holds, $\mathcal{R}$ authenticates $\mathcal{T}$.
   - After that, $\mathcal{R}$ calculates $\zeta = (Y^T \ll wt(r_1)) \oplus ((r_{2L} \parallel (K_L \ll wt(X_R))) \ll wt((r_{1R} \parallel (K_R \ll wt(X_L)))))$ and transmits it to $\mathcal{T}$, also updates $IDS_{new} = ((IDS_{current} \oplus r_2) \ll wt(Y'^T \oplus r_1))$.
6. After receiving ζ from $\mathcal{R}$, $\mathcal{T}$ performs the following steps:

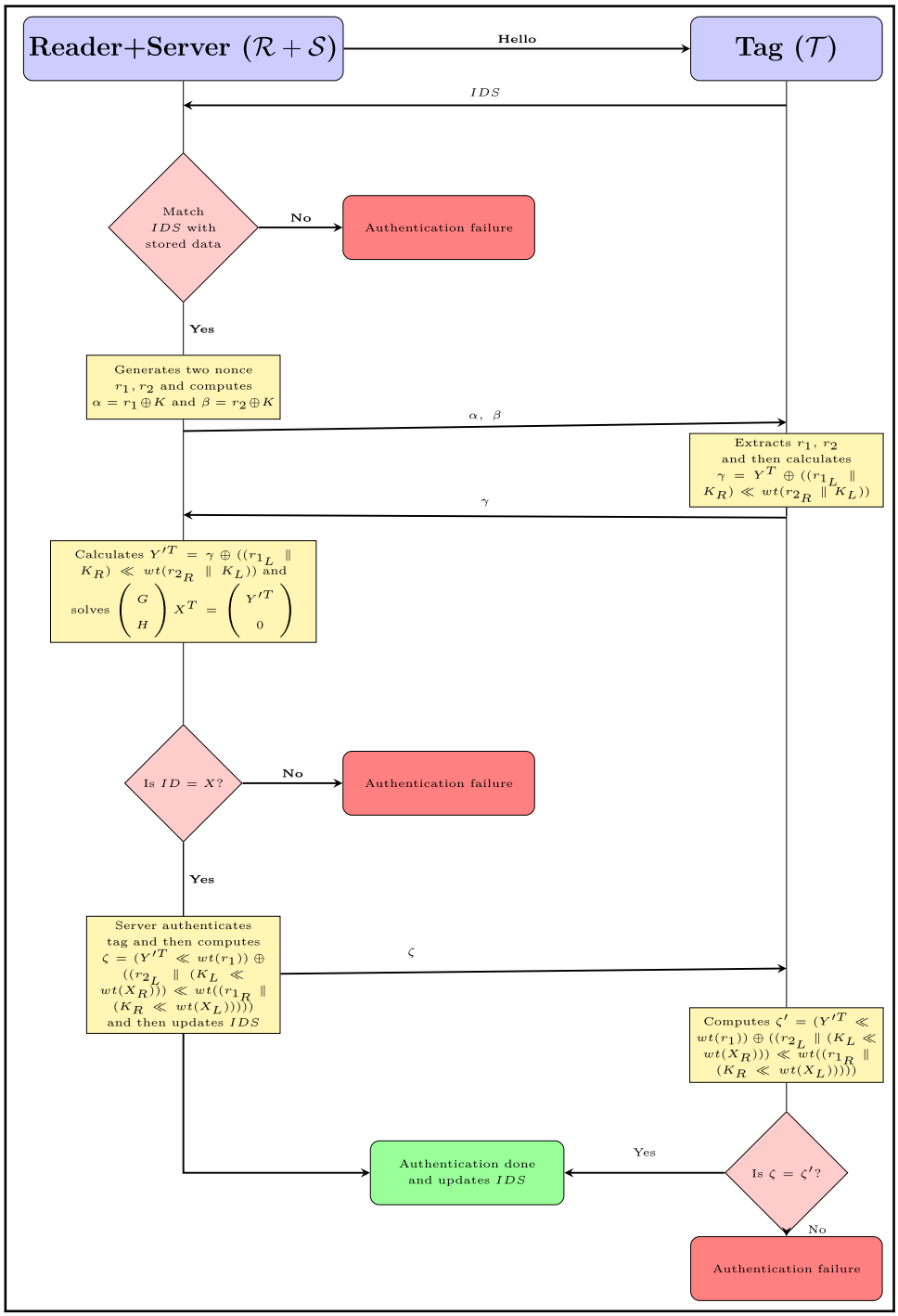

Fig. 1 Flow diagram of the proposed protocol

- $\mathcal{T}$ calculates $\zeta' = (Y^T \lll wt(r_1)) \oplus ((r_{2L} \parallel (K_L \lll wt(X_R))) \lll wt((r_{1R} \parallel (K_R \lll wt(X_L)))))$.
- Checks whether ζ' is the same as receiving ζ or not. If so, $\mathcal{T}$ verifies $\mathcal{R}$ and revises $IDS = ((IDS_{current} \oplus r_2) \lll wt(Y'^T \oplus r_1))$.

5 Security analysis

In this section, we analyze the security features of the proposed protocol by applying formal methodologies and informal techniques.

5.1 Formal security analysis

This section demonstrates formal security by using the following models.

5.1.1 Juel and Weis model

Juel and Weis [19] model is a challenge-response model in which the attacker tempers pseudonym numbers and shared keys after executing the model. This model comprises a system of *n* tags T_i and one reader *R*. Different messages are utilized by the adversary ($\mathcal{A}$): (a) The **SetKey** message assigns a new secret key to the tag. The tag receives the **SetKey** message and modifies the last key value to an unrestricted secret key. (b) The **TagInit** message is utilized to start the current session of the tag and end the prior session, and (c) The **ReaderInit** is utilized to introduce an ongoing session to a reader *R*. In this experiment, the objective of $\mathcal{A}$ is to differentiate between two distinct tags within the bounds of their computational capability and functionality-call bounds. $\mathcal{A}$ is capable of executing, sending, corrupting, and testing requests.

- **Execute**(*R*, *T*, *i*): This query is a passive attack in which $\mathcal{A}$ listens in on the actual protocol execution between *R* and *T* in session *i*.
- **Send**(P_1, P_2, *i*, *m*): $\mathcal{A}$ sends any message *m* when two parties, P_1 and P_2 are communicating in a protocol session *i*.
- **Corrupt**(*T*, *k*): An adversary $\mathcal{A}$ controls the secret key *k* of the tag *T* through this query.
- **Test**(T_1, T_2, *i*): $\mathcal{A}$ has to assume the bit $b \in \{0, 1\}$ correctly in order to succeed based on an identity Id_b which is picked out of $\{Id_1, Id_2\}$ for a session *i*. This query awards consent to testing the thought for untraceability.

Our suggested protocol is deemed secure against untraceability if and only if $\mathcal{A}$'s benefit in predicting the value of *b* is marginal. The objects and the adversary $\mathcal{A}$ must participate in the game. The adversary's objective is to find the right tag, and both need to be fresh. The privacy model in the game is implemented in the following stages.

- **Learning phase**: $\mathcal{A}$ initialized an Execute query so that $\mathcal{A}$ can eavesdrop to authenticate the session between reader and tags and obtain the authentication variables γ and ζ of the proposed protocol.
- **Challenge phase**: In this phase, $\mathcal{A}$ chooses fresh tags T_0, T_1 with identifiers Id_0, Id_1. $\mathcal{A}$ then sends a Test query and consequently, $\mathcal{A}$ is given a challenge to test identifier $Id_b = \{Id_0, Id_1\}$. We consider the least significant bits (LSB), so $b = Id_{bLSB}$.
- **Guessing phase**: The accurate guess of $\mathcal{A}$ is

$$Adv_{\mathcal{A}}(t) = |Pr[\mathcal{A}\ wins] - \frac{1}{2}|,$$

where *t* represents the security parameter. The adversary $\mathcal{A}$ outputs a guess $b' \equiv \gamma_{LSB} \oplus \zeta_{LSB}$, which is derivable as,

$$Adv_{\mathcal{A}}(k) = |Pr[b' = b] - \frac{1}{2}| = |Pr[\gamma_{LSB} \oplus \zeta_{LSB}] - \frac{1}{2}|.$$

Now, $\gamma = Y^T \oplus ((r_{1_L} \parallel K_R) \ll wt(r_{2_R} \parallel K_L))$ and $\zeta = (Y^T \ll wt(r_1)) \oplus ((r_{2L} \parallel (K_L \ll wt(X_R))) \ll wt((r_{1R} \parallel (K_R \ll wt(X_L)))))$ are still uncertain because Y^T, K are all balanced in the proposed protocol. Also, the use of two nonce r_1 and r_2 makes γ, ζ uncertain; therefore, it is difficult for $\mathcal{A}$ to compute left shift operation. Moreover, during the game, $\mathcal{A}$ cannot infer the *K* and *IDS* values as *IDS* updates in each session by using r_1 and r_2. Thus, $Adv_{\mathcal{A}}(k) < \epsilon(k)$, some of insignificant function $\epsilon(\cdot)$. Hence, the proposed protocol cannot reveal sensitive information to the adversary $\mathcal{A}$. Consequently, the proposed protocol does not vulnerable to traceability attacks.

5.1.2 Formal security verification by Scyther tool simulation

In this section, we executed our proposed protocol on the Scyther tool for security verification. The Scyther tool is an automatic tool for verifying and analyzing the security properties of security protocols. The scyther tool is built with many novel features, such as multi-protocol analysis, analyzing security protocols by providing a class of attacks, unbound checking, etc., with state-of-the-art performance. It uses protocol descriptions in security protocol description language (SPDL) and tests the security claims of the protocols in different situations. In addition, the Scyther tool automatically creates security claims for a protocol and check them against these claims.

To write protocol descriptions in SPDL, we have to describe the protocol's behaviour in terms of its role. The communication agents perform a role. In our model, we consist of two communication agents, tag and reader. Each role specification consists of a sequence of events performed by the network agents, such as macro, send, receive, claim, etc. The role specification of the agent tag is shown in Fig. 2. It shows that the tag describes cryptographic primitives in terms of symbols like XOR, Hammingweight, Rot, etc., by using *const* keyword. It constructs messages using *macro* keyword. The tag transmits a message that contains *IDS* to the reader when it comes to the reader's reading spectrum through $send_1$ function. The tag receives *beta* and *gamma* by using $recv_2$ function from the reader. Upon receiving, the tag sends *gamma* to the reader and receives *zai* from the reader using $send_3$ and $recv_4$ functions, respectively. Similarly, the role descriptions of

Fig. 2 The tag's role specification

```
Scyther: Description of the Proposed protocol in SPDL.spdl
File Verify Help
Protocol description Settings
 1 protocol Proposed(Tag,Reader){
 2 role Tag{
 3 const IDi,Ki,Y,IDS,alpha,beta,gamma,zai;
 4 const XOR: Function;
 5 const Concatenate: Function;
 6 const Rot: Function;
 7 const Hammingweight: Function;
 8 const Left: Function;
 9 const Right:Function;
10 fresh r1,r2: Nonce;
11 macro alpha'=XOR(r1,Ki);
12 macro beta'=XOR(r2,Ki);
13 macro gamma'=Rot(XOR(Y,Concatenate(Left(r1),Right(Ki))),
14 Hammingweight(Concatenate(Right(r2),Left(Ki))));
15 macro zai'=Rot(XOR(Rot(Y,Hammingweight(r1)),
16 Concatenate(Left(r2),Rot(Left(Ki),Hammingweight(Right(IDi)))))
17 ,Hammingweight(Rot(Right(Ki),Hammingweight(Left(IDi)))));
18 match(zai,zai');
19 send_1(Tag,Reader,IDS);
20 recv_2(Reader,Tag,alpha',beta');
21 send_3(Tag,Reader,gamma');
22 recv_4(Reader,Tag,zai');
23 claim(Tag, Secret, IDi);
24 claim(Tag, Secret, Ki);
25 claim(Tag, Secret, Y);
26 claim(Tag, Niagree);
27 claim(Tag, Nisynch);
28 claim(Tag, Alive);
29 claim(Tag, Weakagree);
30 }
```

the reader are shown in Fig. 3. Each role specification concludes with a list of claim events. Claim events such as *secret*, *Niagree*, *Alive*, *Weakagree* are security properties we want to verify in the proposed protocol. The Scyther tool simulation result is shown in Fig. 4. It demonstrates the validity of the proposed protocol and has no vulnerability within the bounds.

5.1.3 BAN logic proof

This subsection presents the correct proof of our proposed protocol by utilizing BAN logic [4]. The BAN logic is a technique that verifies the correctness of security protocols. It works on beliefs and knowledge and derives new beliefs from existing beliefs to verify the trustworthiness of network agents. The notations of BAN logic are shown in Fig. 5.

Rules The BAN logic uses the following rules:

*Rule*1 : $\frac{U|\equiv U \overset{s}{\leftrightharpoons} V, U \triangleleft \{M\}_s}{U|\equiv V|\sim M}$. *Rule*1 says that suppose U believes that s is a secret shared between U and V, and if U receives a message M that is encrypted by the secret s, then U believes that V has sent the message M.

*Rule*2 : $\frac{U|\equiv \#M_1}{U|\equiv \#M_1, M_2}$. *Rule*2 says that if U believes that a statement M_1 is fresh, U then accepts a communication that contains M_1, $\{M_1, M_2\}$ is also fresh.

```
Scyther: Description of the Proposed protocol in SPDL.spdl
File Verify Help
Protocol description Settings
31 role Reader{
32 const IDi,Ki,Y,IDS,alpha,beta,gamma,zai;
33 const XOR: Function;
34 const Concatenate: Function;
35 const Rot: Function;
36 const Hammingweight: Function;
37 const Left: Function;
38 const Right:Function;
39 fresh r1,r2: Nonce;
40 macro alpha'=XOR(r1,Ki);
41 macro beta'=XOR(r2,Ki);
42 macro gamma'=Rot(XOR(Y,Concatenate(Left(r1),Right(Ki))),
43 Hammingweight(Concatenate(Right(r2),Left(Ki))));
44 macro zai'=Rot(XOR(Rot(Y,Hammingweight(r1)),
45 Concatenate(Left(r2),Rot(Left(Ki),Hammingweight(Right(IDi))))),
46 Hammingweight(Rot(Right(Ki),Hammingweight(Left(IDi)))));
47 recv_1(Tag,Reader,IDS);
48 send_2(Reader,Tag,alpha',beta');
49 recv_3(Tag,Reader,gamma');
50 macro DIi=XOR(gamma', Rot(Concatenate(Left(r1),Right(Ki))
51 ,Hammingweight(Concatenate(Right(r2),Left(Ki)))));
52 match(IDi,DIi);
53 send_4(Reader,Tag,zai');
54 claim(Reader, Secret, IDi);
55 claim(Reader, Secret, Ki);
56 claim(Reader, Secret, Y);
57 claim(Reader, Niagree);
58 claim(Reader, Nisynch);
59 claim(Reader, Alive);
60 claim(Reader, Weakagree);
61 }
62 }
```

Fig. 3 The reader's role specification

Fig. 4 Scyther tool result

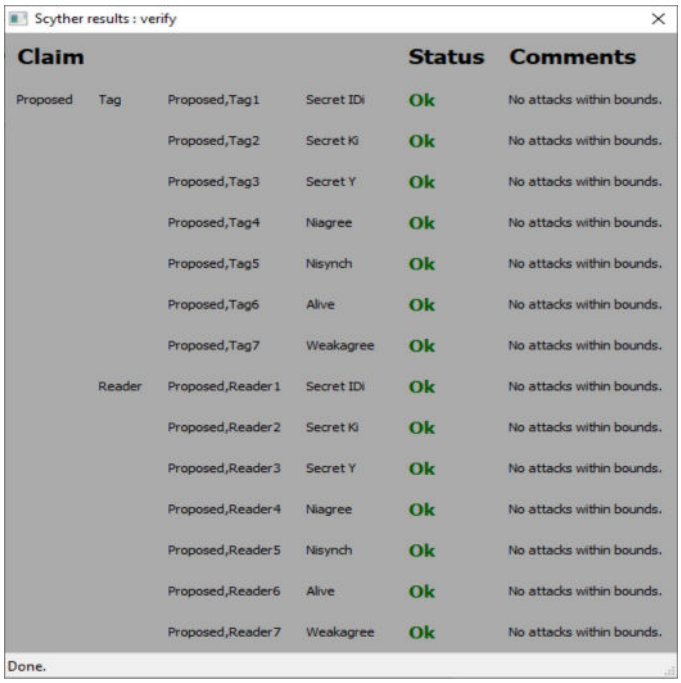

Fig. 5 BAN logic notations

$U \mid\equiv M$:	The network entity U believes that statement M is true.
$U \triangleleft M$:	U receives a statement M from another network entity.
$U \mid\sim M$:	U has sent a message containing M.
$\#M$:	M is fresh.
$U \overset{M}{\leftrightharpoons} V$:	M is a secret key shared in between U and V.
$U \overset{M}{\leftrightarrow} V$:	M is a shared statement between two network entities U and V.
$M \vdash M_1$:	M can drive M_1.

Now, we analyze the suggested protocol's correctness evidence by using the BAN logic symbols and rules. We divide the correctness proof into different parts as below. In the analysis, R indicates for a network agent reader, and T indicates for a network agent tag.

1. **Protocol descriptions:** The descriptions of the messages transmitted between a tag and a reader are as follow.
    1. $T \rightarrow R$: $\{IDS, \gamma\}$
    2. $R \rightarrow T$: $\{\alpha, \beta, \zeta\}$
2. **Protocol idealizations:** It presents the descriptions of the transmitted messages in the BAN logic terminology.
    1. $T \rightarrow R$: $R \triangleleft \{IDS, \gamma\}$
    2. $R \rightarrow T$: $T \triangleleft \{\alpha, \beta, \zeta\}$
3. **Initial assumptions:** The initial assumptions are as follows.
    1. $T \mid\equiv \#r_1, \#r_2$
    2. $R \mid\equiv R \overset{ID,K}{\leftrightharpoons} T$

3. $\mathrm{T} \mid\equiv T \overset{ID,K}{\rightleftharpoons} R$
4. $\mathrm{T} \mid\equiv T \overset{IDS}{\leftrightarrow} R$

4. **Protocol goals:** The security goals are as below.

1. $\mathrm{R} \mid\equiv T \mid\sim \gamma$
2. $\mathrm{T} \mid\equiv R \mid\sim \zeta$
3. $\mathrm{T} \mid\equiv \#\gamma$

5. **Proof process:** In this part, we demonstrate the proof process of the security goals. From idealization (*a*), we get

$$\begin{array}{ll} R & \triangleleft\{IDS, \gamma\} \\ R & \triangleleft\{\gamma\} \\ \Rightarrow R & \triangleleft\{Y^T \oplus ((r_{1_L} \parallel K_R) \ll wt(r_{2_R} \parallel K_L))\} \\ \Rightarrow R & \mid\equiv Y^T \\ \Rightarrow R & \mid\equiv g_i.ID^T \end{array} \tag{5.1}$$

From *Rule*1 and Eq. 5.1, we get

$R \mid\equiv T \mid\sim \gamma.$

Thus, goal 1 is achieved. According to protocol idealization (*b*), we get

$$\begin{array}{ll} T & \triangleleft\{\alpha, \beta, \zeta\} \\ \Rightarrow T & \mid\equiv r_1 \; and \; r_2 \quad (extracts \; from \; \alpha \; and \; \beta) \\ T & \triangleleft\zeta \\ \Rightarrow T & \mid\equiv (Y'^T \ll wt(r_1)) \oplus ((r_{2_L} \\ & \parallel (K_L \ll wt(X_R))) \ll wt((r_{1_R} \parallel (K_R \ll wt(X_L))))) \end{array} \tag{5.2}$$

From *Rule*1 and Eq. 5.2, we get

$T \mid\equiv R \mid\sim \zeta$

Hence, protocol goal 2 is proved. From idealization (*a*), we get

$$T \quad \mid\sim \gamma \tag{5.3}$$

From *Rule*2 and Eq. 5.3, we get

$T \mid\equiv \#\gamma$

Hence, goal 3 is proved.5.2 Informal security analysis

This section offers an informal discussion of the proposed protocol's security aspects. We demonstrate that our protocol can withstand many known assaults. Table 2 compares different comparable authentication protocols in terms of security analysis.

1. Confidentiality- All the transmitted messages are in the form of ciphertext in the proposed protocol. Therefore, it is challenging for an adversary to extricate the values *ID* and *K* from the transmitted message γ due to the shift operation from the left half.
2. Integrity- The secret values (*ID*, *K*) of the protocol are only known by the tag and the server. These values are used to compute γ and ζ, which are transmitted between two entities. Therefore, if an adversary attacks the authentication process by changing the sent values, the process will be halted, and the attacks can be effortlessly distinguished. Therefore, it is impossible to send secret values directly during communication; rather, our improved protocol guarantees the security of the sent secret data.
3. Impersonation attack- In our protocol, the initiator assigns a unique identity and *IDS* for each tag. In each session, random numbers and *IDS* are updated. So, if an adversary eavesdrops on a session, he/she cannot get the identity of the tag and the secret value *K*.

Table 2 Security performance comparison

Protocol	[34] (2015)	[36] (2017)	[30] (2020)	[10] (2021)	[3] (2021)	[32] (2022)	[5] (2022)	[22] (2023)	Proposed
Private data leakage	✓	×	✓	✓	✓	×	×	ND	×
Confidentiality	×	×	×	×	×	×	×	×	×
Integrity	×	×	×	×	×	✓	×	×	×
Traceability attack	✓	×	×	×	×	×	×	×	×
Mutual authentication	×	×	×	×	×	×	×	×	×
De-synchronization attack	✓	✓	×	×	×	×	×	×	×
Man-in-middle attack	×	✓	×	×	✓	×	×	ND	×
Replay attack	×	×	×	×	×	×	×	×	×
Tag anonymity	ND	✓	×	×	×	×	×	×	×
Impersonation attack	×	×	✓	×	✓	×	✓	×	×
Disclosure attack	✓	✓	×	×	×	×	✓	×	×

ND - Not Discussed, ✓ - Vulnerable, × - Not Vulnerable

Therefore, the adversary cannot impersonate an honest tag. Additionally, if the adversary wants to imitate as an honest server, he/she should start a substantial verification reaction in the type of ζ. Since random numbers are refreshed in every session, and *K* is a secret value, the adversary cannot deliver a valid request on behalf of the server. So, the proposed protocol prevents server impersonation attacks.

4. De-synchronization- For each tag, we keep two pseudonyms on the server side. IDS_{old} utilized in the previous effective authentication session, and IDS_{new} which is utilized in the current session. If an adversary changes the sent messages, the server only updates the *IDS*, but the tag does not update. Then, in the later authentication process, as soon as the tag sends its *IDS* to the server, the server matches *IDS* with the IDS_{new}, but it does not match. So, the server compares *IDS* with IDS_{old}, and the process continues for authentication. Hence, the proposed protocol can stand up to de-synchronization attacks.
5. Replay attack- By replying, an adversary can utilize the intercepted data to confirm that the tag is a legitimate one. In the proposed protocol, the value of γ depends on the nonce r_1 and r_2, which are different in different sessions. Therefore, the adversary may eavesdrop on an authentication session and collect data, but the protocol will terminate when he/she tries to replay older messages.
6. Man-in-middle attack- It is an active eavesdropping, where the adversary starts independent connections with the reader or the tag and transfers messages between them. Though the adversary intercepts the values γ and ζ, if he/she is unknown, the values *K* and *IDS*, the man-in-middle attack cannot be completed. Accordingly, our proposed protocol can oppose this kind of attack.
7. Disclosure attack- In the proposed protocol, the secrets are *K* and *ID*. To resist the disclosure of the secrets, the tag utilizes a left shift operator between the values of *K*, r_1 and r_2, which are different in each session. The authentication protocol is, therefore, not compromised by any secret disclosure.
8. Mutual authentication- In our protocol, the server authenticates the tag by comparing *X* and *ID*. The tag also authenticates the server by comparing the received value ζ and the calculated value ζ'. Hence, both the valid tag and the server are authenticated.
9. Anonymity- Since there is no plain message transmitted across the channel, the key component can ensure security. To protect the tag's privacy, we used left shift operations and random numbers in the proposed protocol in each authentication session so that an adversary cannot trace the tag's location. Also, the legitimate tag and reader provide these random numbers. As a result, the tag's identity cannot be tracked by an adversary.
10. The leakage of short-term secret attack- If an adversary knows the temporary secrets r_1 and r_2, he/she cannot calculate Γ or ζ because he/she does not know the values *ID* and *K* of the tag. Thence, our protocol can defend against the leakage of short-term secret attacks.
11. Collaborative attack mitigation: While collaborative attacks typically involve multiple compromised tags or readers sharing information to breach system security, our protocol inherently limits the effectiveness of such strategies. The protocol ensures that each tag maintains a unique secret key and identity that is not shared or derivable across tags. Furthermore, session-based randomness (via fresh nonces r_1, r_2) and pseudonym updates prevent one tag from leveraging knowledge of another. We have elaborated on these safeguards to emphasize their resistance to collusion-based inference.
12. Denial of service (DoS) attack resilience: Although DoS attacks aim to overwhelm or disrupt system functionality rather than compromise data confidentiality, our protocol minimizes the impact of such attacks by using lightweight computations (only shift and XOR operations) and efficient session handling. Additionally, the server's $O(1)$ search complexity and the dual-pseudonym mechanism (IDS_{old} and IDS_{new}) allow rapid recovery from session mismatches without requiring heavy computation or manual resets, which can otherwise be exploited in DoS scenarios. We have included a brief description of these resilience features in the informal security analysis.
13. Resistance to lost tag attacks: In practical RFID deployments, the risk of lost or stolen tags is a critical security concern. The protocol incorporates several mechanisms to enhance security, particularly in the event of a lost RFID tag. It enforces mutual authentication between the tag and the reader, ensuring that an adversary cannot impersonate a lost tag without also being authenticated by the server. The tag's confidential parameters, such as its secret key (*K*) and identity (*ID*), are never transmitted in plaintext; instead, communication relies on random nonces (r_1, r_2) and secure cryptographic operations like bitwise manipulation and circular shifts. Additionally, the pseudonym (*IDS*) is dynamically updated after each session, rendering any previously captured pseudonym obsolete and useless for replay attacks. On the server side, monitoring mechanisms are in place to track both the old and new pseudonyms (IDS_{old} and IDS_{new}). If a tag presents an outdated or mismatched pseudonym, common in cases of cloning or loss, the server can detect the inconsistency and deny access or flag the event. Together, these strategies significantly reduce the risk of unauthorized access or misuse due to lost RFID tags.

Table 3 Computation cost comparison

Protocol	Entity	[34] (2015)	[36] (2017)	[30] (2020)	[10] (2021)	[3] (2021)	[32] (2022)	[5] (2022)	[22] (2023)	Proposed
Rot/ Ref/ Cro/	T	×	4 (Rot)	2 (ME), 1 (FM)	3 (ChM)	×	3 (Cro), 2 (Rot)	×	2 (Rot), 4 (Ref)	5 (Rot)
SSLE/ FMI/ ChM	R+S	×	4 (Rot)	1 (ME), 1 (FMI), 1 (FM)	4 (ChM)	×	3 (Cro), 2 (Rot)	×	2 (Rot), 4 (Ref)	5 (Rot), 1 (SSLE)
Hash	T	5	×	2	6	4	×	9	×	×
	R+S	6	×	2	4	6	×	9	×	×
No. of PRNG	T	1	×	2	2	1	×	1	×	×
	R+S	1	2	1	1	2	2	2	2	2
Required memory	T	2L	7L	4L	3L	5L	4L	2L	4L	3L
Searching Complexity		$O(N)$	$O(N)$	$O(1)$	$O(N)$	$O(1)$	$O(1)$	$O(N)$	$O(1)$	$O(1)$

T - Tag-side, R - Reader-side, S - Server-side, Cro - Cross operation, Ref- Reformation, Rot - Rotation, ChM- Chaotic map, SSLE - Solving System of Linear Equations, FMI - Field Multiplicative Inverse, FM - Field Multiplication

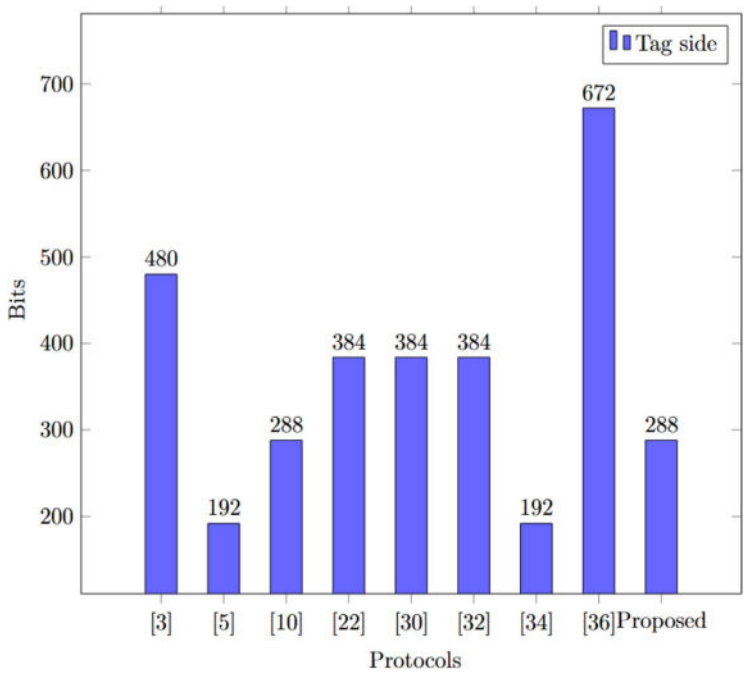

Fig. 6 Storage cost analysis

6 Performance analysis

In this portion, we assess the effectiveness of the proposed protocol's storage, computational, and communication costs by contrasting it and some related protocols [3, 5, 10, 22, 30, 32, 34, 36].

6.1 Storage cost analysis

The tag's memory is exceptionally restricted compared with the reader and the server. In the proposed protocol, we stored ID, K, and IDS, which are 3L bits of memory on the tag side. Every parameter length is $L = 96$ bits according to RFID EPCglobal, so the tag side storage of the proposed protocol is 288 bits, which is less than some existing protocols except [5] and [34], as mentioned in Table 3. However, both the protocols are vulnerable to various attacks, as shown in Table 2. Moreover, the storage cost analysis is given graphically in Fig. 6.

6.2 Computational cost analysis

To lower the processing cost, we do not employ ECC, hash function, and modular exponentiation because these cryptographic primitives have high computational costs. We used only 2 pseudo-random numbers, circular shift operations, and bitwise operations. Hence, our protocol is more effective and can be implemented for low-cost tags in RFID systems. Table 3 shows the computation cost of the proposed protocol and other comparable protocols.

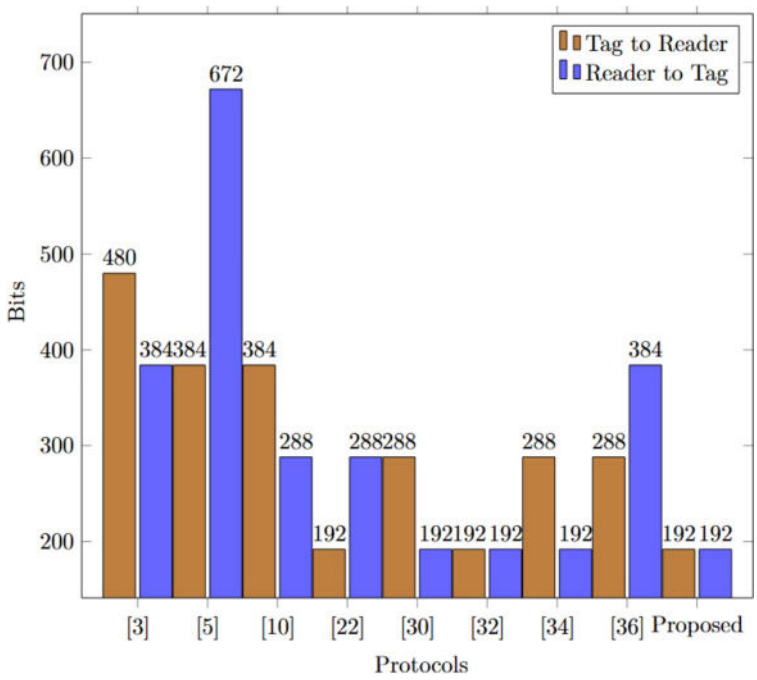

Fig. 7 Communication cost analysis

6.3 Communication cost analysis

In the proposed protocol, the tag transmitted two messages *IDS* and γ to the reader. Hence, the total communication cost is $2L$ bits. Considering $L = 96$, the total communication cost from the tag to the reader is $2 \times 96 = 192$ bits, and the total transmission expense from the reader to the tag is 192 bits. We give a graphical comparison of our protocol with some associated RFID-based protocols in Fig. 7. The graph shows our proposed protocol has minimal communication costs comparing the associated protocols.

6.4 Server inquiry difficulty

The search complexity of the proposed authentication protocol is commonly measured by the back-end server when it searches for a match record in its database. The back-end server only matches the ID string *IDS* and the tag identity *ID* with the database once during a single search attempt during the authentication phase. Therefore, the search complexity is constant, i.e., $O(1)$, which gives better scalability.

6.5 The Benefits of the suggested protocol

RFID adaption is one of the integrated information technologies in medicine and healthcare. RFID technology is becoming more and more prevalent for a variety of applications, including TMIS. Through a wireless channel, RFID technology in healthcare can verify the validity of patients and doctors. However, because these services are provided through an unsecured channel, this system is subject to a variety of assaults [3, 5, 10].

To address privacy and security concerns, we developed a mutual authentication mechanism based on the features of LCD codes and circular left shift operations. The benefits of the suggested protocol are as follows-

1. The suggested protocol uses only 3 rotation operations on the tag side. Hence, the protocol is suitable for low-cost RFID tags.
2. The tag-side storage is $3L$-bits which is small compared to the other protocols except [5, 34].
3. The proposed protocol used the server search complexity $O(1)$ for better scalability.
4. The communication cost between tag and reader is $2L$-bits, which is comparatively less than other related protocols, as shown in Figure 7.
5. The Scyther simulation tool performs the security verification, as shown in Fig. 4. These findings show that the proposed protocol is immune to certain potential attacks.

6.6 Discussion

Additionally, practical issues like signal interference, prevalent in hospital settings due to metal surfaces, wireless congestion, or electromagnetic noise, are acknowledged as physical-layer concerns. While these factors may affect communication reliability, the protocol's use of dynamic pseudonyms and session-based randomization ensures that disrupted sessions do not compromise security. In future implementations, these challenges can be further mitigated by integrating error detection mechanisms and collision-avoidance techniques at the system level. We also recognize the growing impact

of emerging technologies such as quantum computing [16]. Although our current design prioritizes efficiency in classical environments, we plan to extend the protocol by incorporating lightweight post-quantum cryptographic primitives, such as lattice-based or code-based constructions, to withstand quantum attacks. Exploring hybrid designs that balance quantum resistance with minimal resource overhead will be a key direction for future work, ensuring the protocol remains secure and scalable in next-generation IoT and healthcare infrastructures.

7 Conclusion

We have given in this article an ultralightweight authentication RFID-based protocol for healthcare systems. We have used LCD codes, shift operators, and some basic operations to avoid high computation costs. We have shown that the proposed protocol could prevent various vulnerabilities and ensure mutual authentication. We used the BAN logic and Scyther simulation tools to demonstrate the formal security verification. Using the Juels and Weis model, we have shown that our protocol is safe against tag untraceability. In addition, performance evaluations reveal that the suggested protocol is more cost-effective for storage, communication, and computation. As a result, healthcare settings can benefit from implementing our protocol. It is also a real-world application that uses online treatment to protect humans from attackers. To improve the protocol's efficiency, we will consider developing a lattice-based key agreement protocol for TMIS in future work.

Acknowledgements The authors would like to thank the anonymous reviewers for their valuable comments and suggestions to improve the quality of the paper.

Author Contributions The authors H. Ghosh and P. Maurya conceived the idea and wrote the manuscript. P. Maurya prepared all figures, and H. Ghosh prepared all tables in the manuscript. S. Bagchi contributed an overview and overall organisation. All authors reviewed the results and approved the final version of the manuscript.

Funding The CSIR-HRDG, India, for providing financial support for this work, is appreciated by the paper's first author.
The Science and Engineering Research Board (SERB), Government of India, provides additional funding for this work (grant number MTR/2021/000611).

Data Availability No datasets were generated or analysed during the current study.

Declarations

Ethical Approval Not applicable.

Consent for publication Not applicable.

Competing interests The authors declare no competing interests.

References

1. Ahmadian Z, Salmasizadeh M, Aref MR (2013) Desynchronization attack on rapp ultralightweight authentication protocol. Inf Process Lett 113(7):205–209
2. Aghili SF, Mala H (2020) Tracking and impersonating tags in a crc-based ultralightweight rfid authentication protocol. Peer-to-Peer Netw Appl 13(3):816–824
3. Alzahrani BA, Irshad A, Albeshri A, Alsubhi K (2021) A provably secure and lightweight patient-healthcare authentication protocol in wireless body area networks. Wirel Pers Commun 117(1):47–69
4. Burrows M, Abadi M, Needham RM (1989) A logic of authentication. Proc R Soc London, A Math. Phys. Sci. 426(1871):233–271
5. Chander B, Gopalakrishnan K (2022) A secured and lightweight rfid-tag based authentication protocol with privacy-preserving in telecare medicine information system. Comput Commun 191:425–437
6. Chaudhry SA, Naqvi H, Khan MK (2018) An enhanced lightweight anonymous biometric based authentication protocol for tmis. Multimed Tools Appl 77:5503–5524
7. Chen Y, Chen J (2022) An efficient and privacy-preserving mutual authentication with key agreement protocol for telecare medicine information system. Peer-to-Peer Netw Appl 15:516–528
8. Chien HY, Yang CC, Wu TC, Lee CF (2011) Two rfid-based solutions to enhance inpatient medication safety. J Med Syst 35(3):369–375
9. David M, Prasad NR (2009) Providing strong security and high privacy in low-cost RFID networks. In: Schmidt AU, Lian S (eds) Security and privacy in mobile information and communication systems. MobiSec 2009. Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering, vol 17. Springer, Berlin, Heidelberg
10. Dharminder D, Kundu N, Mishra D (2021) Construction of a chaotic map-based authentication protocol for tmis. J Med Syst 45(8):1–10
11. Fan K, Wang W, Jiang W, Li H, Yang Y (2018) Secure ultra-lightweight RFID mutual authentication protocol based on transparent computing for IoV. Peer-to-Peer Netw Appl 11:723–734
12. Fan K, Jiang W, Li H, Yang Y (2018) Lightweight RFID protocol for medical privacy protection in IoT. IEEE Trans Industr Inform 14(4):1656–1665
13. Gao M, Lu Y (2022) URAP: a new ultra-lightweight RFID authentication protocol in passive RFID system. J Supercomput 78:10893–10905
14. Gope P, Amin R, Islam SH, Kumar N, Bhalla VK (2018) Lightweight and privacy-preserving RFID authentication scheme for distributed IoT infrastructure with secure localization services for smart city environment. Future Gener Comput Syst 83:629–637
15. Ghosh H, Maurya PK, Bagchi S (2023) Linear complementary pair of codes based lightweight RFID protocol. Comput Commun 208:79–88
16. Ghosh H, Maurya PK, Bagchi S, Dwivedi AD (2025) Lightweight RFID-enabled authentication protocol in post-quantum environment. Comput Electr Eng 124:110367
17. Huang HH, Ku CY (2009) A RFID grouping proof protocol for medication safety of inpatient. J Med Syst 33(6):467–474
18. Jin C, Xu C, Zhang X, Zhao J (2015) A secure RFID mutual authentication protocol for healthcare environments using elliptic curve cryptography. J Med Syst 39:24
19. Juels A, Weis SA (2009) Defining strong privacy for RFID. ACM Trans Inf Syst Sec (TISSEC) 13(1):1–23
20. Khalid M, Mujahid U, Najam-ul-Islam M (2018) Cryptanalysis of ultralightweight mutual authentication protocol for radio frequency identification enabled internet of things networks. Int J Distrib Sens Netw 14(8)

21. Khan MA, Ullah S, Ahmad T, Jawad K, Buriro A (2023) Enhancing security and privacy in healthcare systems using a lightweight RFID protocol. Sensors 23(12):5518
22. Kumar A, Singh K, Shariq M, Lal C, Conti M, Amin R, Chaudhry SA (2023) An efficient and reliable ultralightweight RFID authentication scheme for healthcare systems. Comput Commun 205:147–157
23. Ling S, Xing C (2004) Coding Theory, 1st edn. Cambridge University Press
24. Maurya PK, Pal J, Bagchi S (2017) A coding theory based ultralightweight RFID authentication protocol with CRC. Wirel Pers Commun 97(1):967–976
25. Maurya PK, Bagchi S (2020) Cyclic group based mutual authentication protocol for RFID system. Wirel Netw 26:1005–1015
26. Maurya PK, Bagchi S (2023) Quadratic residue-based unilateral authentication protocol for RFID system. Multimed Tools Appl 82(11):16533–16554
27. Mir O, Nikooghadam M (2015) A secure biometrics based authentication with key agreement scheme in telemedicine networks for e-health services. Wirel Pers Commun 83(4):1–23
28. Qi M, Chen J (2018) New robust biometrics-based mutual authentication scheme with key agreement using elliptic curve cryptography. Multimed Tools Appl 77:23335–23351
29. Safkhani M, Bagheri N (2016) Generalized desynchronization attack on UMAP: application to $RCIA$, $KMAP$, $SLAP$ and $SASI^+$ protocols. Cryptology ePrint Archive, Paper 2016/905
30. Salem FM, Amin R (2020) A privacy-preserving RFID authentication protocol based on El-Gamal cryptosystem for secure TMIS. Inf Sci 527:382–393
31. Shariq M, Singh K (2021) A novel vector-space-based lightweight privacy-preserving RFID authentication protocol for IoT environment. J Supercomput 77:8532–8562
32. Shariq M, Singh K, Maurya PK, Ahmadian A, Taniar D (2022) Anonsurp: an anonymous and secure ultralightweight RFID protocol for deployment in internet of vehicles systems. J Supercomput 78:8577–8602
33. Shokouhifar M (2021) Swarm intelligence RFID network planning using multi-antenna readers for asset tracking in hospital environments. Comput Netw 198:108427
34. Srivastava K, Awasthi AK, Kaul SD (2015) A hash based mutual RFID tag authentication protocol in telecare medicine information system. J Med Syst 39:153
35. Sun PR, Wang BH, Wu F (2008) A new method to guard inpatient medication safety by the implementation of RFID. J Med Syst 32(4):327–332
36. Tewari A, Gupta BB (2017) Cryptanalysis of a novel ultralightweight mutual authentication protocol for IoT devices using RFID tags. J Supercomput 73:1085–1102
37. Tian Y, Chen G, Li J (2012) A new ultralightweight RFID authentication protocol with permutation. IEEE Commun Lett 16(5):702–705
38. Wang K, Chen C, Fang W (2018) On the security of a new ultralightweight authentication protocol in IoT environment for RFID tags. J Supercomput 74:65–70
39. Wang X, Fan K, Yang K, Cheng X, Dong Q, Li H, Yang Y (2022) A new RFID ultra-lightweight authentication protocol for medical privacy protection in smart living. Comput Commun 186:121–132
40. Wu ZY, Lee YC, Lai F, Lee HC, Chung Y (2012) A secure authentication scheme for telecare medicine information systems. J Med Syst 36(3):1529–1535
41. Xiao L, Xie S, Han D, Liang W, Guo J, Chou WK (2021) A lightweight authentication scheme for telecare medical information system. Connect Sci 33(3):769–785
42. Zhuang X, Zhu Y, Chang C (2018) Security issues in ultralightweight RFID authentication protocols. Wirel Pers Commun 98:779–814

Haradhan Ghosh 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, India, in 2019. He is pursuing a Ph.D. in the Department of Mathematics at NIT Durgapur, India. He is a life member of the Cryptology Research Society of India (CRSI). His research interests include RFID security, post-quantum cryptography, information security, and coding theory.

Pramod Kumar Maurya Pramod Kumar Maurya received his MSc in Mathematics from University of Allahabad, India, 2011. He has completed MTech in Computer Science and Data Processing from IIT Kharagpur, India, 2014. He received his PhD in Mathematics from NIT Durgapur, India. He is currently working as an Assistant Professor III in the School of Engineering and Technology, BML Munjal University, Haryana, India. His research interests include identity authentication, RFID security, and information security.

Satya Bagchi Satya Bagchi received his BSc and MSc in Mathematics from the University of Kalyani, West Bengal, India, respectively, in 2002 and 2004. He received his PhD in Mathematics from the same university in 2013. He is currently an Associate Professor at the Department of Mathematics, National Institute of Technology, Durgapur, India. His current research interests are in algebraic coding theory, RFID security protocol design, and cryptography. He is a life member of the Cryptology Research Society of India (CRSI); Indian Mathematical Society, India; Ramanujan Mathematical Society, India; Indian Statistical Institute, India; and Operational Research Society of India.

Terms and Conditions

Springer Nature journal content, brought to you courtesy of Springer Nature Customer Service Center GmbH (“Springer Nature”).
Springer Nature supports a reasonable amount of sharing of research papers by authors, subscribers and authorised users (“Users”), for small-scale personal, non-commercial use provided that all copyright, trade and service marks and other proprietary notices are maintained. By accessing, sharing, receiving or otherwise using the Springer Nature journal content you agree to these terms of use (“Terms”). For these purposes, Springer Nature considers academic use (by researchers and students) to be non-commercial.
These Terms are supplementary and will apply in addition to any applicable website terms and conditions, a relevant site licence or a personal subscription. These Terms will prevail over any conflict or ambiguity with regards to the relevant terms, a site licence or a personal subscription (to the extent of the conflict or ambiguity only). For Creative Commons-licensed articles, the terms of the Creative Commons license used will apply.
We collect and use personal data to provide access to the Springer Nature journal content. We may also use these personal data internally within ResearchGate and Springer Nature and as agreed share it, in an anonymised way, for purposes of tracking, analysis and reporting. We will not otherwise disclose your personal data outside the ResearchGate or the Springer Nature group of companies unless we have your permission as detailed in the Privacy Policy.
While Users may use the Springer Nature journal content for small scale, personal non-commercial use, it is important to note that Users may not:

1. use such content for the purpose of providing other users with access on a regular or large scale basis or as a means to circumvent access control;
2. use such content where to do so would be considered a criminal or statutory offence in any jurisdiction, or gives rise to civil liability, or is otherwise unlawful;
3. falsely or misleadingly imply or suggest endorsement, approval , sponsorship, or association unless explicitly agreed to by Springer Nature in writing;
4. use bots or other automated methods to access the content or redirect messages
5. override any security feature or exclusionary protocol; or
6. share the content in order to create substitute for Springer Nature products or services or a systematic database of Springer Nature journal content.

In line with the restriction against commercial use, Springer Nature does not permit the creation of a product or service that creates revenue, royalties, rent or income from our content or its inclusion as part of a paid for service or for other commercial gain. Springer Nature journal content cannot be used for inter-library loans and librarians may not upload Springer Nature journal content on a large scale into their, or any other, institutional repository.
These terms of use are reviewed regularly and may be amended at any time. Springer Nature is not obligated to publish any information or content on this website and may remove it or features or functionality at our sole discretion, at any time with or without notice. Springer Nature may revoke this licence to you at any time and remove access to any copies of the Springer Nature journal content which have been saved.
To the fullest extent permitted by law, Springer Nature makes no warranties, representations or guarantees to Users, either express or implied with respect to the Springer nature journal content and all parties disclaim and waive any implied warranties or warranties imposed by law, including merchantability or fitness for any particular purpose.
Please note that these rights do not automatically extend to content, data or other material published by Springer Nature that may be licensed from third parties.
If you would like to use or distribute our Springer Nature journal content to a wider audience or on a regular basis or in any other manner not expressly permitted by these Terms, please contact Springer Nature at

onlineservice@springernature.com