An efficient and reliable ultralightweight RFID authentication scheme for healthcare systems

Kumar, Anand; Singh, Karan; Shariq, Mohd; Lal, Chhagan; Conti, Mauro; Amin, Ruhul; Chaudhry, Shehzad Ashraf

DOI
10.1016/j.comcom.2023.04.013

Publication date
2023

Document Version
Final published version

Published in
Computer Communications

Citation (APA)
Kumar, A., Singh, K., Shariq, M., Lal, C., Conti, M., Amin, R., & Chaudhry, S. A. (2023). An efficient and reliable ultralightweight RFID authentication scheme for healthcare systems. *Computer Communications*, *205*, 147-157. https://doi.org/10.1016/j.comcom.2023.04.013

Computer Communications 205 (2023) 147–157

Contents lists available at ScienceDirect

Computer Communications

journal homepage: www.elsevier.com/locate/comcom

An efficient and reliable ultralightweight RFID authentication scheme for healthcare systems

Anand Kumar [a], Karan Singh [a], Mohd Shariq [a,c,*], Chhagan Lal [b], Mauro Conti [c], Ruhul Amin [d], Shehzad Ashraf Chaudhry [e,*]

[a] School of Computer and Systems Sciences, Jawaharlal Nehru University, New Delhi 110067, India
[b] Department of Intelligent Systems, CyberSecurity Group, TU Delft, Netherlands
[c] Department of Mathematics, University of Padua, 35131 Padua, Italy
[d] Department of Computer Science and Engineering, NIT, Jamshedpur, Jharkhand, India
[e] Department of Computer Science and Information Technology, College of Engineering, Abu Dhabi University, Abu Dhabi, United Arab Emirates

ARTICLE INFO

Keywords:
ICT
RFID
Ultralightweight
Authentication
Reformation

ABSTRACT

In the era of the Internet of Communication Technologies (ICT), the Internet is becoming more popular and widely used across the world. Radio Frequency IDentification (RFID) has become a prominent technology in healthcare systems for identifying tagged objects. The RFID tags are attached to the billions of different healthcare devices or things in several associated applications. However, RFID tags' security and privacy are regarded as the two biggest concerns. An adversary might eavesdrop, tamper, or even intercept the transmitted messages in RFID systems. Also, the privacy of the users (patients, doctors, and nurses) may breach. In past years, numerous ultralightweight RFID authentication schemes have been proposed in the healthcare sector. However, all these schemes were pointed out as insecure under several known security attacks namely, replay, impersonation, full-disclosure, and de-synchronization attacks. Keeping in view such security flaws, we present an efficient and reliable ultralightweight RFID authentication scheme (ER^2AS) for healthcare systems to enhance patients' medication safety. The scheme employs bitwise XOR, circular left–right rotations, and our proposed ultralighweight *reformation* operation to achieve higher-level security. The security and privacy evaluations demonstrate that ER^2AS scheme resists several known security attacks. The performance analysis also demonstrates that it incurs lower computation and storage overhead on the RFID tags, thus making it practical to be implemented in real-time healthcare environments.

1. Introduction

With the ongoing advancement of Internet Communication and Technologies (ICT) and the rapid development of automated medication systems, RFID is gaining popularity in the healthcare environment to enhance patient medication safety [1–3]. In the pervasive computing infrastructure, RFID has become a core identification technology that uniquely identifies several objects simultaneously over a channel [4]. RFID is being widely used in numerous real-live applications like automatic payment, access control, automatic toll collection, personnel identification, animal identification, human implantation, e-passports, e-healthcare systems, supply chains, and many others [5–10].

Over the years, RFID is becoming more and more prominent in smart healthcare systems and it has various benefits in the healthcare domain such as preventing possible thefts, mitigating human resources, productivity improvement, and reducing cost and time [11–13]. Smart healthcare is becoming an emerging field that provides several facilities such as gaining health monitoring, ease of access, and mobility to users (patients, doctors, nurses, and other medical staff) as shown in Fig. 1. The information associated with patients is stored at the cloud server and can be remotely accessed over the Internet or mobile networks by the users at anytime [14].

In the healthcare environment, patient medication safety is a major concern for global public health. The various goals of patient medication safety are shown in Fig. 2. According to the official statistics, due to the improper identification of patients, there is becoming more mistreatment in the healthcare systems. Considering such medical errors, RFID technology contributes to medical healthcare systems for asset tracking and information tracking of patients [15]. In particular, RFID helps to provide various advantages over healthcare industries such as cost-saving, safety enhancement, and high operational efficiency. Apart from security and privacy, the risks associated with human safety are

* Corresponding author.
E-mail addresses: anand_141@yahoo.com (A. Kumar), karancs12@gmail.com (K. Singh), shariq99ansari@gmail.com (M. Shariq), c.lal@tudelft.nl (C. Lal), mauro.conti@unipd.it (M. Conti), amin_ruhul@live.com (R. Amin), ashraf.shehzad.ch@gmail.com (S.A. Chaudhry).

https://doi.org/10.1016/j.comcom.2023.04.013
Received 28 October 2022; Received in revised form 26 March 2023; Accepted 12 April 2023
Available online 19 April 2023

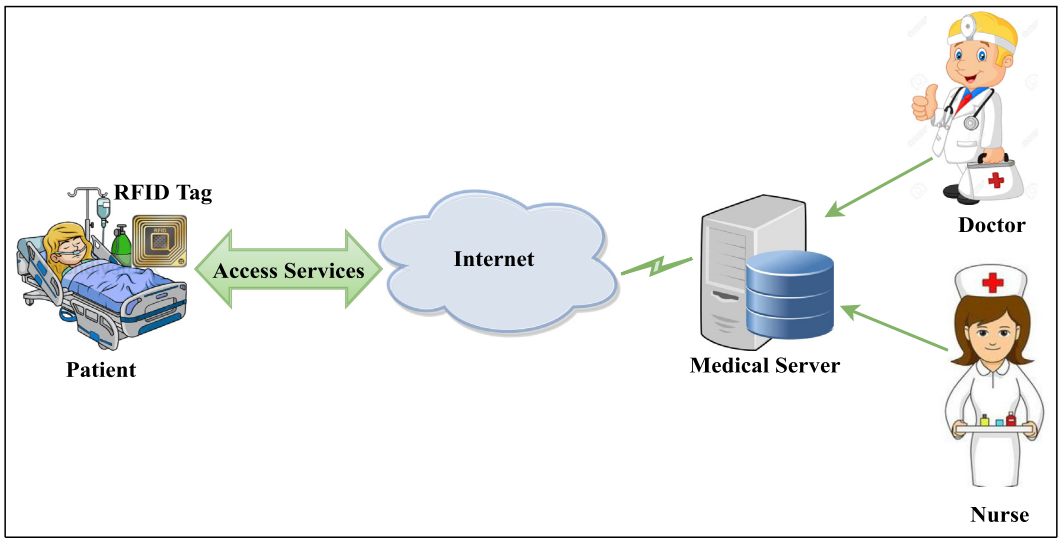

Fig. 1. A typical scenario for the healthcare environment.

the foremost barriers to adopting this technology [16,17]. Furthermore, IoT in healthcare systems brings a lot of facilities such as convenience to physicians and patients in several medical fields, for instance, real-time monitoring, patient medication records, blood bank management, patient information management, medical emergency management, and among others.

The RFID system contains three major components an RFID tag, reader, and a backend server. The tag is a tiny microchip embedded with the object(s). The tags can be categorized in three different ways such as passive, active, and semi-active tags [18–22]. The RFID tags are resource-constraint devices that have limited computing capability and low storage, and also restrict the utilization of cryptographic primitives. The RFID tag operates on three different frequencies namely low, high, and ultra-high frequencies (LF, HF, and UHF), respectively. The LF has a frequency range from 125–134 kHz, low data rate, and can read up to 10 cm, HF has a frequency range of 13.56 MHz, moderate data rate, and can read a range up of to 1 m, and UHF has a frequency range from 860–960 MHz and can read up to 10 to 15 m, respectively [23]. The RFID reader is used to reads data over the tag. The backend server is used to store the sensitive information of the RFID tags [24]. In healthcare systems, the cloud server is used instead of a physical server or backend server because of its storage limitation. Furthermore, the cloud server has several advantages over backend servers such as cost-effectiveness, higher efficiency, better scalability, and disaster recovery [25].

The two secure and insecure communication channels are used during message transmission. A secure communication channel is used between reader and server. On the contrary, an insecure or wireless communication channel is used between tags (for example, patients) and readers (for example, doctors and nurses) [26]. Due to this, security and privacy issues may arise in RFID authentication schemes. Therefore, a safe and secure RFID-based authentication scheme is proposed to protect the patients' data privacy, patient medical records, and his/her associated sensitive medical information. The key objectives of our scheme are summarized as:

- To achieve mutual authentication between $\mathcal{T}$ and $(\mathcal{R} + \mathcal{CS})$.
- To achieve security requirements for RFID Systems.
- To provide resistance against several known attacks.
- To minimize computational operations and storage costs.

1.1. Research gap and motivation

To ensure guarantees of security and privacy is the main contribution to our proposal. Consider that the communication channel between

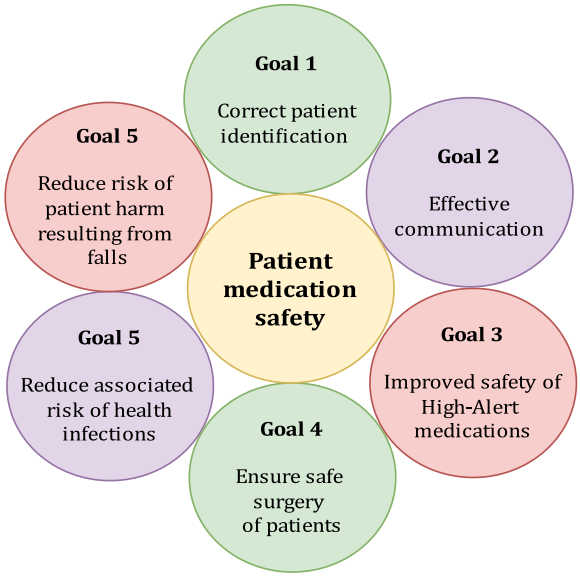

Fig. 2. Patient medication safety goals.

$\mathcal{T}$ and $\mathcal{R}$ is insecure. The RFID system may suffer security attacks and privacy violations during communication. However, the existing state-of-the-art schemes show concerning issues such as disclosure attacks, tag anonymity, impersonation attacks, tag location privacy, and replay attacks, among others [27,28]. To fix the shortcomings of ultra-lightweight primitives used in previous RFID authentication protocols, we have presented a novel reformation $Ref(X, Y)$ method in this paper. The new reformation method has a binary string output corresponding to two binary input strings of the same length. However, the extensive use of T-functions (XOR, AND, and OR) provides low security and can lead to several malicious attacks in the proposed protocol. Therefore, any of the RFID authentication protocol(s) must satisfy various security properties such as eavesdropping, impersonation, loss and message interruption, location tracking, etc.

1.2. Our contribution

The key contribution of our ER^2AS scheme is as follows:

- This paper presents a secure, efficient, and reliable ultralight weight RFID authentication scheme to enhance patients' medication safety. In order to minimize the computational operations on RFID tags, we employ bitwise XOR ($\oplus$), circular left–right $Rot_{(l\ or\ r)}(X, Y)$ rotations, and our proposed ultralightweight reformation $Ref(X, Y)$ operations for encrypting data.
- The security analysis shows our ER^2AS scheme achieves mutual authentication, confidentiality, and location privacy as well as can withstand impersonation, full disclosure, replay, and desynchronization attacks.
- The performance evaluation is carried out with the state-of-the-art existing schemes, which demonstrate that our ER^2AS scheme greatly overcomes the computational operations and storage costs.

1.3. Paper outline

The remaining part of this paper is structured as follows. Section 2 presents the existing literature review. The various notations and preliminaries used are presented in Section 3. Our efficient and reliable RFID authentication scheme for healthcare systems is presented in Section 4. Further, Section 5 evaluated the informal security analysis followed by the performance evaluation. Finally, Section 7 describes the concluding remark.

2. Literature review

Over the past years, numerous RFID authentication schemes have been proposed for safeguarding RFID systems from various security attacks [29]. Table 1 shows the cryptographic primitives, strengths, and limitations of previous state-of-the-art RFID authentication schemes. It is hard to provide all security privacy features because insecure communication is used between tags and readers in low-cost RFID systems. To fix such shortcomings, we have discussed some previous RFID authentication schemes along with cryptographic primitives, strengths, and drawbacks.

Xie et al. [30] adopted a Virtual Private Network (VPN) to build secure backend channels for a cloud-centric RFID authentication protocol in which the database is organized in the form of an encrypted hash table. The protocol uses bitwise XOR ($\oplus$), concatenation, one-way hash $h(\cdot)$, symmetric encryption $E_k(\cdot)$/decryption $D_k(\cdot)$ algorithms, and a $PRNG(\cdot)$. The protocol preserves mutual authentication, pervasive authentication, and tag/reader privacy against the database keeper. Subsequently, Abughazalah et al. [31] proposed an improvement of Xie's scheme [30], and also found that their protocol cannot withstand location tracking, invade tag's privacy, and reader impersonation attacks. Later on, Surekha B et al. [35] found the security weakness of Abughazalah's scheme which does not preserve the tag location privacy feature.

Xiao et al. [32] proposed cloud-RAPIC, a cloud-centric RFID authentication protocol between $\mathcal{R}$ and CS with an insecure communication channel. They use bitwise ($\oplus$), concatenation, one-way hash $h(\cdot)$, symmetric encryption $E_k(\cdot)$/decryption $D_k(\cdot)$, and pseudo-random numbers. The cloud-RAPIC protocol safeguard messages transmitted between participating entities $\mathcal{T}$ and $\mathcal{R}$ without any third party. The protocol meet known security features such as mutual authentication ($\mathcal{R}-\mathcal{T}$ and $\mathcal{R}-S$), forward security, data integrity, data anonymity, and tag location tracking. The protocol also can withstand de-synchronization, replay, and tag/reader impersonation attacks. Later on, Abughazalah et al. [31] found that the cloud-RAPIC [32] protocol cannot withstand location tracking, invade the tag's privacy, and reader impersonation attacks.

Zhenguo Zhao [36] proposed a secure RFID authentication scheme based on Elliptic Curve Cryptography (ECC) that can be deployed in Telecare Medical Information Systems (TMIS). The scheme ensures that the protocol is safe under some security attacks and is more reliable for healthcare systems. The authors showed that their scheme is secure against forward untraceability and more suitable for healthcare environments. However, Farash et al. [37] found that the Zhenguo Zhao [36] scheme showed a security weakness against forward untraceability.

Rahman et al. [29] proposed a privacy-preserving framework for RFID-based healthcare environments. The scheme shows two major concerns for privacy-preserving in RFID-enabled healthcare systems. The primary concern provides an RFID authentication protocol that preserves privacy for monitoring purposes and sensing RFID tags in different ways of identification. The secondary concern provides the healthcare services using tag ID, where a privacy-preserving access control system is used to prevent unauthorized access to the secret information. The framework also solves the trade-off problem between privacy and scalability in RFID systems. Data security, privacy, and access are the paramount factors for RFID adoption in healthcare systems.

Fan et al. [27] introduced a lightweight RFID-based scheme for medical healthcare domain in IoT environment. The scheme employs XOR ($\oplus$), concatenation ($\|$), left rotation $Rot(\cdot,\cdot)$, and cross $Cro(\cdot,\cdot)$ operations. The scheme provides privacy protection for individuals or personnel against easily private data leakage by malicious outsiders. They also claimed that their scheme could not achieve all the necessary security features but it can withstand the known security features namely mutual authentication, tag anonymity, forward secrecy, DoS, and replay attacks. Later on, Aghili et al. [38] showed the security flaws of Fan's scheme [27] which is insecure against tag traceability, secret disclosure, and reader impersonation attacks. Moreover, the scheme could not provide the tag anonymity and reader anonymity features.

To fix the shortcomings of Fan's scheme [27], Aghili et al. [38] have introduced an improved version namely, a secure and lightweight RFID scheme for Medical IoT applications named SecLAP. The scheme employs XOR ($\oplus$), concatenation ($\|$), left rotation $Rot_l(\cdot,\cdot)$, circular right rotation $Rot_r(\cdot,\cdot)$, cross $Cro(\cdot,\cdot)$, and a secure and lightweight modular rotate $MRot_K(\cdot,\cdot)$, operations. The scheme provides a security guarantee against tag/reader impersonation, de-synchronization, replay, and tag traceability attacks. However, Safkhani et al. [39] showed the weaknesses of Aghili's scheme [38] which is insecure against partial and full secret disclosure attacks as well as traceability attacks.

Fan et al. [28] introduced a lightweight RFID-based scheme for cloud healthcare systems. In cloud-centered healthcare systems, the sensitive medical information associated with individuals and patients can be compromised through a malicious cloud server, which may lead to a high risk of leakage of the individual's sensitive information. The scheme employs XOR ($\oplus$), left rotation $Rot(\cdot,\cdot)$, PRNGs, and quadratic reSIDuals operations. The scheme resists known security attacks including tag tracking, de-synchronization, and replay attacks. However, Zhu et al. [40] showed that Fan's scheme [28] could not achieve forward secrecy and was susceptible to impersonation attacks.

Xie et al. [41] introduced a secure and enhanced RFID scheme to prevent the leakage of private or sensitive information from the backend database in the healthcare environment. The scheme uses puncturable Pseudo-Random Function (PRF), indistinguishability obfuscation, and encryption $E(\cdot)_k$/decryption $D(\cdot)_k$ by using the symmetric key k. The scheme is secure against various security functionalities namely mutual authentication, data integrity, confidentiality, eavesdropping, MITM, malicious server, and tag tracking attacks. The scheme does not provide formal security verifications using simulation tools such as AVISPA, CryptoVerif, Scyther, etc.

Fan et al. [33] proposed an efficient cloud-based lightweight RFID scheme that employs simple XOR, an improved permutation $Per(\cdot,\cdot)$, and left rotation $Rot(\cdot,\cdot)$ operations. In addition, the timestamps are used to update the secret information of the tags and also ensure the message's freshness. The scheme is safe under replay and de-synchronization attacks. However, Adeli et al. [42] showed that their

Table 1
Cryptographic primitives, strengths and shortcomings of previous RFID authentication schemes.

References	Cryptographic Primitives	Strengths	Limitations
[30]	* Simple bitwise XOR and concatenation operators * One-way cryptographic hash function * Encryption and decryption functions * Pseudo-random number generator	* Provide backward security * Provide security against malicious cloud providers from the leakage of private user data	* Not secured against reader impersonation and tag location tracking attacks * No formal security verification
[31]	* Simple bitwise XOR and concatenation operators * One-way cryptographic hash function * Symmetric encryption and decryption functions * Pseudo-random number generator	* Achieve mutual authentication * Achieve tag data anonymity * Resists replay and de-synchronization attacks	* Does not provide tag location privacy * Not secured against reader impersonation attack * No formal security verification
[32]	* Simple bitwise XOR and concatenation operators * One-way cryptographic hash function * Encryption and decryption functions * Pseudo-random number generators	* Provide forward untraceability * Achieve tag anonymity * Archive mutual authentication from Tag to Reader and Reader to Server	* Does not provide reader location privacy * Does not achieve identity authentication
[27]	* Simple bitwise XOR and concatenation operations * Cross operation * Circular left rotation operation	* Achieve mutual authentication * Resists replay, DoS, and de-synchronization attacks	* Not secured against traceability, reader impersonation, full and partial disclosure attacks * No formal security verification
[33]	* Simple bitwise XOR operation * Improved Permutation operation * Circular left rotation operation	* Achieve mutual authentication * Privacy-preserving	* Does not provide tag anonymity * Does not provide forward and backward security * Not secured against man-in-the-middle, impersonation, secret disclosure, replay, and de-synchronization attacks * No formal security verification
[34]	* Quadratic residues * Zero-knowledge proof * One-way cryptographic hash function * Encryption and decryption functions	* Achieve strong indistinguishability-privacy using random oracles * Implemented in a PC and Raspberry Pi	* No formal security verification using simulation tools such as AVISPA, CryptoVerif, Scyther, etc.
Proposed scheme	* Simple bitwise XOR operation * Bitwise reformation operation * Circular left and right rotation operations	* Achieve mutual authentication * Achieve tag anonymity, forward security, and tag location privacy * Resists impersonation, disclosure, replay, and de-synchronization attacks	* Not known yet

scheme is vulnerable to man-in-the-middle, impersonation, secret disclosure, replay, traceability, de-synchronization attacks, forward–backward security, and anonymity.

Song et al. [34] proposed a quadratic residues-based RFID zero-knowledge authentication protocol named ZKAP. They uses a secure cryptographic hash function $h(\cdot)$, $E(\cdot)_k/D(\cdot)_k$, quadratic residues, and zero-knowledge proof approaches. The protocol achieves strong indistinguishability-privacy using random oracles and is implemented on a PC and Raspberry Pi. However, there is no formal security verification carried out using any simulation tools such as AVISPA, CrptoVerif, Scyther, etc.

3. Preliminaries

The proposed ER^2AS scheme is consists of non-triangular functions such as reformation $Ref(X,Y)$ and circular left and right $Rot_{(l\ or\ r)}(X,Y)$ operations instead of simple T-functions (triangular functions such as XOR, OR, and AND). The notations along with the descriptions is illustrated in Table 2. The reformation, circular left, and right rotation operations are defined as:

3.1. Definition of reformation

We suppose that X and Y are two n-bit length strings, where

$$X = x_{n-1}x_{n-2}\dots x_0, x_i \in \{0,1\}, i = 0,1,2,\dots,n-1,$$
$$Y = y_{n-1}y_{n-2}\dots y_0, y_j \in \{0,1\}, j = 0,1,2,\dots,n-1.$$

The reformation of X with Y is represented as $Ref(X,Y)$, we have

$$Ref(X,Y) = z_{n-1}z_{n-2}\dots z_0, \quad z_i = F_i(x_i,y_i).$$

Table 2
Symbols and their definitions.

Symbol	Definition
$\mathcal{T},\mathcal{R},CS$	Represents RFID tag, reader, and cloud server
K	Represents secret key shared between $\mathcal{T}$ and CS
$Ref(X,Y)$	Represents reformation operation between strings X and Y
$Rot_{(l\ or\ r)}(X,Y)$	Represents circular left and right rotations of X by $wt(Y)$
IDS	Represents index pseudonym stored in the tag and database
ID	Represents static identification number of each RFID tag
n_1, n_2	Represents pseudo random numbers generated at cloud server
$\oplus$	Represents XOR operator
$a \stackrel{?}{=} b$	Represents comparison between a and b
L	Represents length of each bit string in each parameter

where,

$$F(x_i,y_i) = \left\{ \begin{array}{r|l} x_{i-1} \oplus y_i \ mod\ n, & x_i > y_i \\ x_i \oplus y_i \ mod\ n, & x_i = y_i \\ x_i \oplus y_{i-1} \ mod\ n, & x_i < y_i \end{array} \right\}$$

The new proposed reformation of string X with Y is denoted as $Ref(X,Y)$. To better understand this new ultralightweight $Ref(X,Y)$ operation, we now consider the two 8-bit length strings X and Y such that $X = 10010110$ and $Y = 00111001$ as shown in Fig. 3.

3.2. Circular rotation operations

To design our proposed scheme, we use left and right rotation operations denoted as $Rot_l(X,Y)$ and $Rot_r(X,Y)$, respectively. However, $Rot_l(X,Y)$ is represents a left rotation of X by $wt(Y)(mod\ L)$ bits, where Y is the hamming weight of $wt(Y)$ and it can be defined as the number of 1's presents in string Y. So, X itself with the probability of $\frac{1}{L}$ might

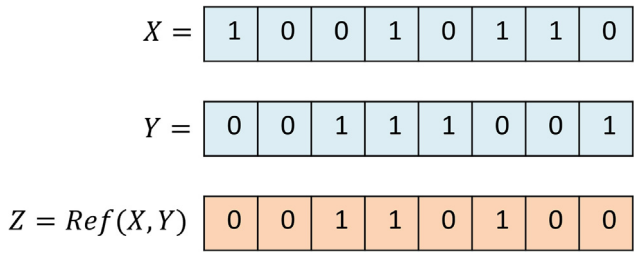

Fig. 3. The reformation $Ref(X, Y)$ operation.

be the outcome of $Rot_l(X, Y)$. Hence, we say the probability distribution is uniform.

- **Left and right rotation operations** Consider X and Y are two 8-bit length strings such that $X = 10110100, Y = 01011100$.
  Now, the left rotation on X and Y can be computed as, $Rot_l(X, Y) = X$ is left rotated by $wt(Y)$, where $wt(Y) = 4$. Then, $wt(Y)(mod\ 8) = 4\ mod\ 8 = 4$. Therefore, $Rot_l(X, Y) = Rot_l(X, 4) =$ 01001011. Now, the right rotation on X and Y can be computed as, $Rot_r(X, Y) = X$ is right rotated by $wt(Y)$, where $wt(Y) = 4$. Then, $wt(Y)(mod\ 8) = 4\ mod\ 8 = 4$. Therefore, $Rot_r(X, Y) = Rot_r(X, 4) =$ 01001011.

4. Proposed scheme

This section mainly consists of initialization and authentication phases. Before initializing the authentication phase, we first provide some important assumptions for our scheme.

4.1. Assumptions considered

We assume some underlying assumptions for designing our proposed scheme as given below:

- **Passive adversary** $\mathcal{P}_{\mathcal{A}}$ The passive adversary $\mathcal{P}_{\mathcal{A}}$ eavesdrops on all communications between RFID components i.e., the tags, readers, and backend server. Besides, $\mathcal{P}_{\mathcal{A}}$ tries to find out some sensitive information or some secret key associated with the targeted tag. However, $\mathcal{P}_{\mathcal{A}}$ cannot alter or even insert any message during the communication.
- **Active adversary** $\mathcal{A}_{\mathcal{A}}$ The active adversary $\mathcal{A}_{\mathcal{A}}$ can insert, modify, alter, inject, or even delete any message instead of eavesdropping. $\mathcal{A}_{\mathcal{A}}$ can also impersonate a legitimate tag or reader by spoofing or replay attack, and causes de-synchronization between tag and backend server by jamming or message interruption. Moreover, $\mathcal{A}_{\mathcal{A}}$ also tries to find out some sensitive information or some secret key associated with the targeted tag same as $\mathcal{P}_{\mathcal{A}}$.
- **Secure communication** The communication is regarded as secure between $\mathcal{R}$ and $\mathcal{CS}$.
- **Insecure communication** The communication is regarded as wireless and insecure between $\mathcal{T}$ and $\mathcal{R}$, where an adversary can easily tap or record the communication data.

4.2. Initialization phase

Before initiating the authentication process, this phase defines some statements for each participating entity listed as:

- Initially, for each tag's memory space, we store an index IDS, a shared secret K, a unique identity ID, reformation, and left–right rotation operations.
- For each tag, a unique identity ID, K, an old IDS_{old} and new IDS_{new} pseudonyms stored in the server. Initially, we say $IDS_{old} = IDS$ and $IDS_{new} = Null$.
- The tag and reader stores a $PRNG(\cdot)$.
- The server stores the same information including all the tag's keys as the tag stores.
- The reformation and circular left–right rotation operations are stored in the memory of the tags.
- The tag and reader contain limited resources, whereas the server has no limitations.

4.3. Authentication phase

In this phase, Fig. 4 puts the whole description of our ER^2AS scheme. The following execution steps of our ER^2AS scheme are given below:

Step 1: $M_1 : \mathcal{R} \rightarrow \mathcal{T} : \{\text{“}Hello\text{”}\}$.

Initially, $\mathcal{R}$ sends a “$Hello$” message to the RFID tag for initializing a new authentication session.

Step 2: $M_2 : \mathcal{T} \rightarrow \mathcal{R} : \{IDS\}$.

After receiving the “$Hello$” message, $\mathcal{T}$ sends an index pseudonym IDS to the RFID reader.

Step 3: $M_3 : \mathcal{R} \rightarrow \mathcal{T} : \{A, B, C_{(L\ or\ R)}\}$.

Upon receiving IDS, $\mathcal{R}$ uses this received IDS as an index to search the secrets of tags in the database of the cloud server. If it finds a match, the reader produces two L-bits random numbers n_1, n_2 and computes the messages A, B, and $C_{(L\ or\ R)}$ (if $wt(C) \approx$ odd sent C_L, else sent C_R). Thereafter, the reader transmits these messages to the tag.

- Computes: $A = Ref(IDS, K) \oplus n_1$.
- Computes: $B = IDS \oplus n_1 \oplus n_2$.
- Computes: $C_{(L\ or\ R)} = Ref(Ref(n_1, n_1), Ref(n_2, n_2))$.

Step 4: $M_4 : \mathcal{T} \rightarrow \mathcal{R} : \{D_{(L\ or\ R)}\}$.

After receiving A, B, and C, $\mathcal{T}$ extracts n_1 from A by XORing $Ref(IDS, K)$ with A and n_2 from B by XORing IDS, n_1, and B. Then, the tag computes a local value of C' and checks whether $C'_{(L\ or\ R)} \stackrel{?}{=} C_{(L\ or\ R)}$, if so, $\mathcal{T}$ authenticates $\mathcal{R}$ as a legitimate reader and updates its index pseudonyms IDS and K in the database. The tag computes the messages D and transmits a corresponding $D_{(L\ or\ R)}$ (if $wt(D) \approx$ odd sent D_L, else sent D_R) to the reader.

- Extracts: $n_1 = A \oplus Ref(IDS, K)$.
- Extracts: $n_2 = B \oplus IDS \oplus n_1$.
- Computes: $C'_{(L\ or\ R)} = Ref(Ref(n_1, n_1), Ref(n_2, n_2))$.
- Verify: $C'_{(L\ or\ R)} \stackrel{?}{=} C_{(L\ or\ R)}$.
- Computes: $D_{(L\ or\ R)} = Rot_r(Ref(Rot_l(IDS_{new}, K_{new}), n_1 \oplus n_2), n_2) \oplus ID$.

Step 5: $M_5 : Verification\ at\ Reader - Server\ Unit$.

Upon receiving $C_{(L\ or\ R)}$, $\mathcal{R}$ computes a local value of D' and checks whether $D'_{(L\ or\ R)} \stackrel{?}{=} D_{(L\ or\ R)}$, if so, $\mathcal{R}$ authenticates $\mathcal{T}$ as a legitimate tag and updates its index pseudonyms IDS and K in the database.

- Computes: $D'_{(L\ or\ R)} = Rot_r(Ref(Rot_l(IDS_{new}, K_{new}), n_1 \oplus n_2), n_2) \oplus ID$.
- Verify: $D'_{(L\ or\ R)} \stackrel{?}{=} D_{(L\ or\ R)}$.

5. Evaluation and analysis

This section comprises comparative security and privacy analysis followed by the performance measured with four different state-of-the-art RFID authentication schemes. All four schemes are proposed by Xie's scheme [30], Abughazalah's scheme [31], Fan's scheme [27], and Aghili's scheme [38], respectively. All existing related schemes shows some pitfalls in terms of their security privacy features as well as computation complexities. Fig. 5 briefly describes the security analysis of our ER^2AS proposed scheme.

Table 3
Comparison of Security and privacy features among various authentication schemes.

Scheme/Feature ↓⟶	Xie's scheme [30]	Abughazalah's scheme [31]	Fan's scheme [27]	Aghili's scheme [38]	Proposed scheme
SF_1	✘	✘	✔	✘	✔
SF_2	✘	✔	✔	✔	✔
SF_3	✘	✔	✔	✔	✔
SF_4	✔	✔	✔	✔	✔
SF_5	✘	✘	✘	✘	✔
SF_6	✔	✘	✔	✔	✔

Acronyms Let us assume that SF_1: Tag anonymity; SF_2: Tag location privacy; SF_3: Secure under impersonation attacks; SF_4: Secure under replay attacks; SF_5: Secure under disclosure attacks; and SF_6: Secure under de-synchronization attacks.

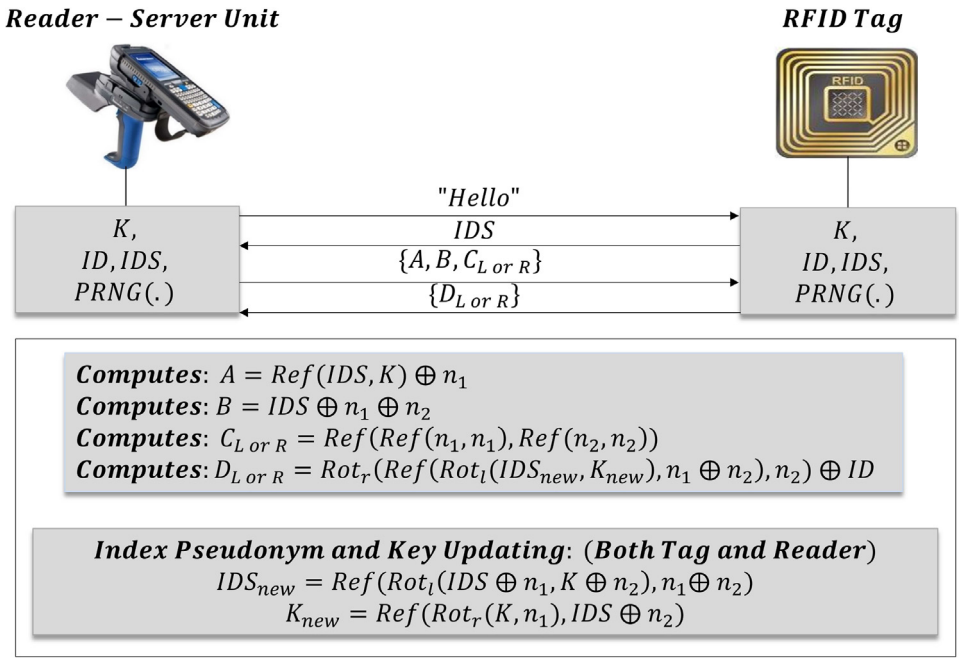

Fig. 4. Efficient and reliable healthcare authentication scheme.

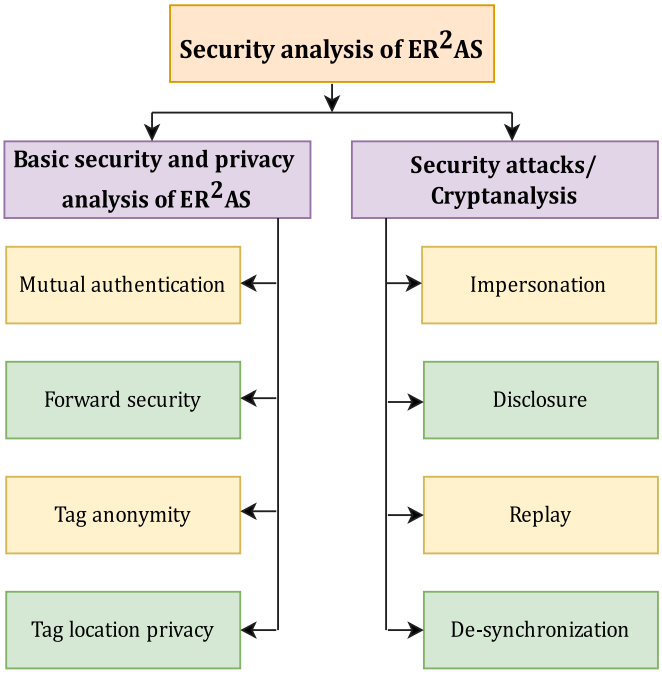

Fig. 5. Security analysis model of our proposed scheme.

5.1. *Informal security analysis*

Table 3 comprises the security and privacy study of ER^2AS mainly analyzes to show the resistance against various known attacks and meet privacy features.

Proposition 1. *ER^2AS preserves mutual authentication.*

Proof. It states that both the legitimate participants used in the scheme successfully authenticate to each other. It is well known that the shared secrets such as IDS, ID, K, random numbers n_1, n_2 are used to compute the response messages A, B, $C_{(L\ or\ R)}$, and $D_{(L\ or\ R)}$. Furthermore, the tag legitimate tag authenticates the legitimate reader by verifying the transmitted messages $C_{(L\ or\ R)}$ with the corresponding local values of $C'_{(L\ or\ R)}$. Similarly, the reader successfully authenticates the tag by verifying the transmitted message $D_{(L\ or\ R)}$ with its local value $D'_{(L\ or\ R)}$. Thus, our ER^2AS scheme preserves the property of mutual authentication. □

Proposition 2. *ER^2AS preserves forward security.*

Proof. In forward security, the previously transmitted messages between tags and servers cannot reveal if the adversary knows the present sensitive data such as shared secret keys and/or random numbers. In ER^2AS, consider an adversary is compromised a tag and retrieves the values of ID, IDS, and K someday, then the adversary still is unable to infer or forge the previous sensitive information as well as secret keys of the same tag, because each updated equations are having two random

Table 4
Comparison of computation operation, communication cost, and communication round.

Scheme ↓⟶	Computation operation	Communication cost	Communication round
Xie's scheme [30]	$\oplus, \|\|, Hash, E_k(\cdot), D_k(\cdot)$	$8L = 8 \times 96 = 768$	10
Abughazalah's scheme [31]	$\oplus, \|\|, Hash, E_k(\cdot), D_k(\cdot), \wedge$	$7L = 7 \times 96 = 672$	7
Fan's scheme [27]	$\oplus, \|\|, Cro(\cdot,\cdot), Rot(\cdot,\cdot)$	$8L = 8 \times 96 = 768$	13
Aghili's scheme [38]	$\oplus, \|\|, Cro(\cdot,\cdot), Rot(\cdot,\cdot), MRot_K(\cdot,\cdot)$	$9L = 9 \times 96 = 864$	9
Proposed scheme	$\oplus, Ref(\cdot,\cdot), Rot_{(l\ or\ r)}$	$3L = 3 \times 96 = 288$	4

numbers. Therefore, the adversary will not compromise the previous messages from the same tag. □

Proposition 3. *ER²AS preserves tag anonymity.*

Proof. The feature of tag anonymity is considered an important feature that prevents identity information tracking and also achieves identity privacy protection for the tags. Thus, an adversary cannot obtain the identities of the tag even if he/she illegitimately accesses the related information. In ER²AS, the tag uses its ID and index pseudonym IDS as the identity, and it does not expose them. The used pseudonym IDS and key K are updated in each successful authentication session run. Therefore, the tag ensures anonymity property. Besides, there is no use of unbalanced operations (OR, AND) in the updating process. Moreover, the adversary does not have an advantage over tag tracking via IDS. Thus, our ER²AS scheme preserves the tag's anonymity property. □

Proposition 4. *ER²AS preserves tag location privacy.*

Proof. Consider an adversary is not permitted to trace the location of a tag or its past location. Therefore, there is an essential need to protect data and protect the privacy related to users or patients. In ER²AS, the tag's responses are changed by employing fresh random numbers n_1, n_2, and the updated tag's values. Thus, the adversary obtains new responses in each authentication session since he/she eavesdrops on a session. Furthermore, the tag's responses are changed because of new fresh random numbers even if the previous authentication session is aborted. □

Proposition 5. *ER²AS resists impersonation attacks.*

Proof. This attack states that the active adversary can impersonate the channel and authenticate himself/herself as a legitimate tag/reader without compromising the secret data. The adversary can compute the tag's response D to impersonate the tag. So, it is infeasible to compute the response messages for an adversary without knowing ID and K. Thus, our ER²AS scheme provides resistance against the impersonation attacks. □

Proposition 6. *ER²AS resits disclosure attacks.*

Proof. The adversary retrieves the shared secrets between the tag and reader in an authentication session run. On the other hand, the passive adversary may eavesdrop the transmitted message over an insecure channel and he/she tries to obtain the updated shared secrets that can be used in the next authentication session. In our proposed scheme, the adversary cannot obtain sensitive information even if he/she has response messages A, B, C, and D. Moreover, the used reformation operation makes it more complex for an adversary to compromise the tag's shared secrets. Thus, our ER²AS scheme is secure against disclosure attacks. □

Proposition 7. *ER²AS resists replay attacks.*

Proof. Suppose an adversary tries to obtain some useful information and he/she can use the same information to authenticate as the legitimate tag. The replay attacks arise in the authentication schemes

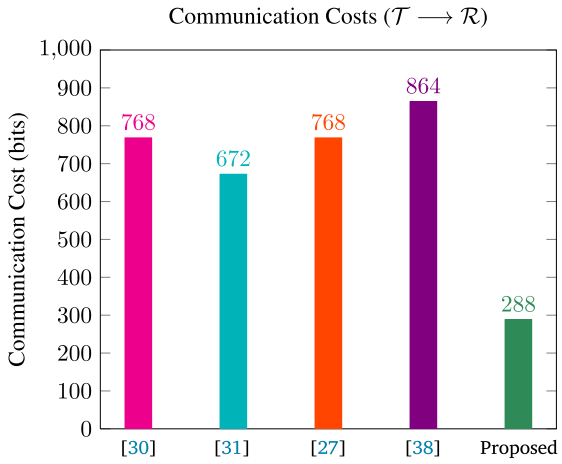

Fig. 6. Communication costs.

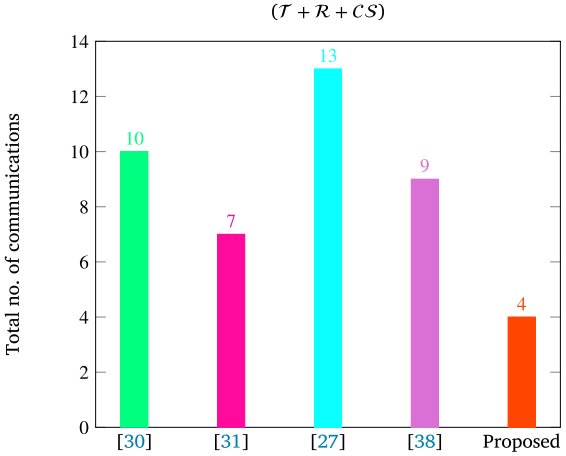

Fig. 7. Communication rounds.

due to random numbers produced by the tag and reader and then utilize these numbers to compute the tag's response D. In ER²AS, the tag will use different random numbers to compute the response D in each authentication session run. If an adversary tries to replay previous messages, then he/she cannot obtain the random numbers. Also, the adversary cannot forge messages as a legitimate tag. Moreover, the tag device does not affect replays of messages. Hence, our proposed ER²AS scheme is secure under replay attacks. □

Proposition 8. *ER²AS resists de-synchronization attacks.*

Proof. The tag does not update its secrets if the last message(s) is/are intercepted in our proposed ER²AS scheme. On the other hand, the reader updates the tag's entries i.e., IDS_{old} and IDS_{new}. To resist the de-synchronization attack, the IDS_{old} and IDS_{new} index pseudonyms

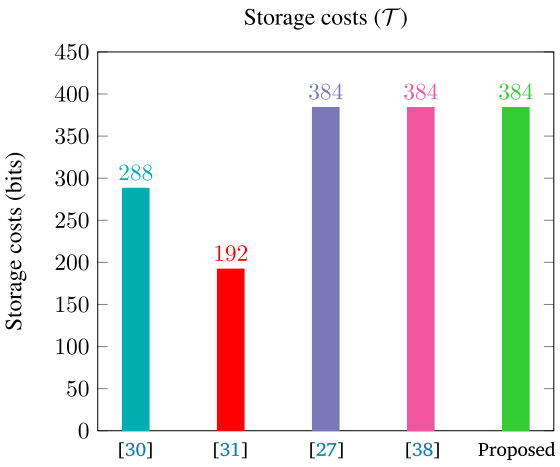

Fig. 8. Storage costs on tag.

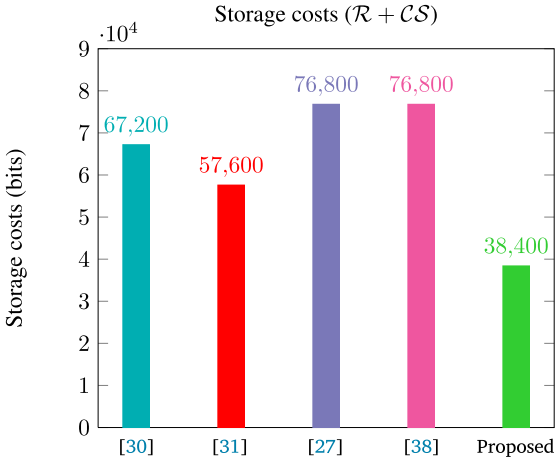

Fig. 9. Storage costs on reader and cloud server.

of shared strings are stored in the reader. Thus, our ER^2AS scheme provides resistance against de-synchronization attacks because the last message(s) is/are sent by the reader. Moreover, the current secrets are only stored in the tag. □

5.2. Performance evaluation

The performance of our ER^2AS scheme has been evaluated and compared with other several existing authentication schemes concerning computation operations, communication costs, and storage costs are shown in Tables 4 and 5, respectively.

- **Computation operation**
  We have utilized bitwise XOR ($\oplus$), circular left and right rotations $Rot_{(r\ or\ l)}(X,Y)$, and reformation $Ref(X,Y)$ operations in our ER^2AS scheme which shows superior performance in terms of computational complexity and storage cost. Hence, our ER^2AS scheme is well preferable for low-cost passive tags.
- **Communication cost**
  It states that the number of transmitted messages is used for mutual authentication. In our proposed scheme, a total of four communication rounds are only used in the whole mutual authentication process. Thus, the communication cost of our scheme is $4L$ bits. Now, we have considered that the length of each parameter for the RFID EPC tag is 96-bit. Then the total communication costs of our ER^2AS scheme is $(3 \times 96) = 288$ bits, which is less than Xie's scheme [30], Abughazalah's scheme [31], Fan's scheme [27], and Aghili's scheme [38] bearing 768 bits, 672 bits, 768 bits, and 864 bits, respectively. In addition, our proposed scheme consumes a total of 4 communication rounds for mutual authentication, which is less than Xie's scheme [30], Abughazalah's scheme [31], Fan's scheme [27], and Aghili's scheme [38] consuming 10, 7, 13, and 9, respectively. In Figs. 6 and 7, the graphical comparison is depicted for communication cost between Tag and reader and total communication cost among tag, reader and cloud server of the proposed scheme with various schemes.

Table 5
Storage cost comparison.

Scheme ↓⟶	Entity	Storage cost
Xie's scheme [30]	$\mathcal{T}$	$3L = 3 \times 96 = 288$
	$\mathcal{R}+\mathcal{CS}$	$7NL = 7 \times 100 \times 96 = 67200$
Abughazalah's scheme [31]	$\mathcal{T}$	$2L = 2 \times 96 = 192$
	$\mathcal{R}+\mathcal{CS}$	$6NL = 6 \times 100 \times 96 = 57600$
Fan's scheme [27]	$\mathcal{T}$	$4L = 4 \times 96 = 384$
	$\mathcal{R}+\mathcal{CS}$	$8NL = 8 \times 100 \times 96 = 76800$
Aghili's scheme [38]	$\mathcal{T}$	$4L = 4 \times 96 = 384$
	$\mathcal{R}+\mathcal{CS}$	$8NL = 8 \times 100 \times 96 = 76800$
Proposed scheme	$\mathcal{T}$	$4L = 4 \times 96 = 384$
	$\mathcal{R}+\mathcal{CS}$	$4NL = 4 \times 100 \times 96 = 38400$

Acronyms
$\mathcal{T}, \mathcal{R}, \mathcal{CS}$: Overhead on the tag, reader, and cloud server, respectively.
N, L: Number of tags stored in RFID systems and bits stored in each parameter, respectively.

- **Storage cost**
  It states that the numbers of key elements and static tag ID are stored in the tag's memory space. In our proposed scheme, a unique ID, an index pseudonym IDS, and a shared secret key K are stored in the tag. Hence, each tag needs the storage of $3L$ bits. Consider an RFID system consisting of a tag population of up to 100 tags (i.e., $N = 100$). For each EPC RFID tag, each parameter is required of 96-bit length (i.e., $L = 96$ bits) corresponding to EPCglobal. Thus, the total storage cost of our scheme is $(4 \times 96) = 384$ bits on the tag which is the same as Fan's scheme [27] and Aghili's scheme [38] i.e., 384 bits and 384 bits, respectively. Although Xie's scheme [30] and Abughazalah's scheme [31] bear less storage cost of 288 bits and 192 bits, respectively than the proposed scheme. In addition, our proposed scheme bears $(4 \times 100 \times 96) = 38400$ bits on the reader and cloud server which is less than Xie's scheme [30], Abughazalah's scheme [31], Fan's scheme [27], and Aghili's scheme [38] bearing 67200 bits, 57600 bits, 76800 bits, and 76800 bits, respectively. The graphical comparisons for storage costs of our ER^2AS scheme with various state-of-the-art schemes as illustrated in Figs. 8 and 9, respectively.
- **Server search cost (scalability)**
  The scalability or server search cost of an RFID authentication scheme is taken into account for searching a match record in a single search attempt from the database. In our scheme, the reader finds the matched record (such as IDS, K) only in a single search from the database. Table 6 shows that our ER^2AS scheme takes $\mathcal{O}(1)$ i.e., constant time to search for a matched record. Hence, our scheme outperforms in terms of scalability.

6. The Scyther tool verification

The Scyther is a widely-accepted automated push-button tool used for formal verification of security protocols. To perform the Scyther simulation of our proposed protocol, we have set up an experimental environment on the Linux operating system, Ubuntu v21.10, an AMD Ryzen 9 5900HX processor of 4.6 GHz, and 16.0 GB of RAM. Considering a perfect cryptography assumption, the adversary cannot obtain any

SPDL code

```
usertype Key,Nonce,Data;
const XOR: Function;
const Rotl: Function;
const Rotr: Function;
const Ref: Function;
protocol MyProposed(Tag,Reader)
{
role Tag
{
const Hello,A,B,CLorR',CLorR,DLorR',DLorR,n1,n2,ID,IDS,IDSnew,K,Knew;
recv_1(Reader,Tag,Hello);
send_!2(Tag,Reader,IDS);
recv_!3(Reader,Tag,A,B,CLorR);
macro n1=XOR(A,Ref(IDS,K));
macro n2=XOR(XOR(B,IDS),n1);
macro CLorR'=Ref(Ref(n1,n1),Ref(n2,n2));
match(CLorR',CLorR);
macro DLorR=XOR(Rotr(Ref(Rotl(IDSnew,Knew),XOR(n1,n2)),n2),ID);
send_!4(Tag,Reader,DLorR);
claim(Tag, Secret, ID);
claim(Tag, Secret, IDS);
claim(Tag, Secret, n1);
claim(Tag, Secret, n2);
claim(Tag, Niagree);
claim(Tag, Nisynch);
claim(Tag, Alive);
claim(Tag, Weakagree);
}
```

Fig. 10. Specification of tag role in SPDL.

SPDL code

```
role Reader
{
const Hello,A,B,CLorR',CLorR,DLorR',DLorR,n1,n2,ID,IDS,IDSnew,K,Knew;
send_!1(Reader,Tag,Hello);
recv_!2(Tag,Reader,IDS);
macro A=XOR(Ref(IDS,k),n1);
macro B=XOR(XOR(IDS,n1),n2);
macro CLorR=Ref(Ref(n1,n1),Ref(n2,n2));
send_!3(Reader,Tag,CLorR);
rec_!4(Tag,Reader,DLorR);
macro DLorR'=XOR(Rotr(Ref(Rotl(IDSnew,Knew),XOR(n1,n2)),n2),ID);
match(DLorR',DLorR);
claim(Reader, Secret, ID);
claim(Reader, Secret, IDS);
claim(Reader, Secret, n1);
claim(Reader, Secret, n2);
claim(Reader, Niagree);
claim(Reader, Nisynch);
claim(Reader, Alive);
claim(Reader, Weakagree);
}
}
```

Fig. 11. Specification of reader-server role in SPDL.

Table 6
Comparison of server search costs among various authentication schemes.

Scheme ↓⟶	Xie's scheme [30]	Abughazalah's scheme [31]	Fan's scheme [27]	Aghili's scheme [38]	Proposed scheme
Server search cost	$\mathcal{O}(N)$	$\mathcal{O}(N)$	$\mathcal{O}(N)$	$\mathcal{O}(N)$	$\mathcal{O}(1)$

Scyther results : verify

Claim				Status	Comments
MyProposed	Tag	MyProposed,Tag1	Secret K	Ok	No attacks within bounds.
		MyProposed,Tag2	Secret ID	Ok	No attacks within bounds.
		MyProposed,Tag3	Secret IDS	Ok	No attacks within bounds.
		MyProposed,Tag4	Secret XOR(A,Ref(IDS,K))	Ok	No attacks within bounds.
		MyProposed,Tag5	Secret XOR(XOR(B,IDS),XOR(A,Ref(IDS,K)))	Ok	No attacks within bounds.
		MyProposed,Tag6	Niagree	Ok	No attacks within bounds.
		MyProposed,Tag7	Nisynch	Ok	No attacks within bounds.
		MyProposed,Tag8	Alive	Ok	No attacks within bounds.
		MyProposed,Tag9	Weakagree	Ok	No attacks within bounds.
	Reader	MyProposed,Reader1	Secret K	Ok	No attacks within bounds.
		MyProposed,Reader2	Secret ID	Ok	No attacks within bounds.
		MyProposed,Reader3	Secret IDS	Ok	No attacks within bounds.
		MyProposed,Reader4	Secret XOR(A,Ref(IDS,K))	Ok	No attacks within bounds.
		MyProposed,Reader5	Secret XOR(XOR(B,IDS),XOR(A,Ref(IDS,K)))	Ok	No attacks within bounds.
		MyProposed,Reader6	Niagree	Ok	No attacks within bounds.
		MyProposed,Reader7	Nisynch	Ok	No attacks within bounds.
		MyProposed,Reader8	Alive	Ok	No attacks within bounds.
		MyProposed,Reader9	Weakagree	Ok	No attacks within bounds.

Fig. 12. Simulation results of our proposed scheme using Scyther tool.

secret information from an encrypted message without knowing its decryption keys. Therefore, we say that all the cryptographic functions are considered perfect. The bounded number of protocol sessions and nonce can be verified by the Scyther tool. In addition, it can characterize the security protocols by producing a finite representation of all possible protocol behaviors. It also provides a Graphical User Interface (GUI) aimed at verifying or understanding a protocol. In Scyther, Python scripting interfaces and command lines make efficient use of it for the verification of large-scale protocols.

The specification or code of a protocol in Scyther can be written in the operational semantics-based Security Protocol Description Language (SPDL). The Scyther allows a set of claim events for the verification of certain claims i.e., some confidential or secret parameters which are used to verify or falsify them. Figs. 10 and 11 show the SPDL code of Tag ($\mathcal{T}$) and Reader-Server ($\mathcal{R}+\mathcal{CS}$) roles, respectively. In Fig. 12, the Scyther tool verification of our proposed protocol shows that there is no attack found within a certain bound. Hence, our protocol provides strong protection against active and passive security attacks.

7. Conclusion and future perspectives

Over the past years, RFID technology is being popular and can be used in various applications across the world. In an RFID system, security and privacy are considered two main concerns. Considering these problems, we proposed an efficient and reliable ultralightweight RFID authentication scheme (ER^2AS) for healthcare systems to enhance patients' medication safety. Our proposed ER^2AS scheme used bitwise XOR, circular left–right operations, and a newly proposed reformation method to resist well-known attacks. The proposed scheme is highly efficient and also achieves higher-level security in comparison to other similar existing schemes. The security and privacy analysis demonstrate that the ER^2AS can withstand impersonation, replay, disclosure, and de-synchronization attacks. Compared to other schemes, the performance analysis demonstrates that our scheme consumes fewer computation operations and storage costs on RFID tags. Therefore, the scheme shows superior performance and is better suited for the healthcare environment. In future studies, we are planning to deploy our ER^2AS scheme in real-time healthcare systems to improve patient medication safety.

CRediT authorship contribution statement

Anand Kumar: Conceptualization, Writing – original draft. **Karan Singh:** Analysis, Supervision. **Mohd Shariq:** Designing original scheme, Experimentation. **Chhagan Lal:** Experimentation, Investigation, Reviewing original and revised drafts. **Mauro Conti:** Supervision, Reviewing original and revised versions. **Ruhul Amin:** Informal analysis, Performance analysis. **Shehzad Ashraf Chaudhry:** Performance analysis and comparisons, Response letter.

Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Data availability

No data was used for the research described in the article.

Acknowledgments

The work of Shehzad Ashraf Chaudhry was supported by the Abu Dhabi University's Office of Research and Sponsored Programs under Grant 19300810.

References

[1] M.L. Das, P. Kumar, A. Martin, Secure and privacy-preserving RFID authentication scheme for Internet of Things applications, Wirel. Pers. Commun. 110 (1) (2020) 339–353.
[2] Z.-Y. Wu, L. Chen, J.-C. Wu, A reliable RFID mutual authentication scheme for healthcare environments, J. Med. Syst. 37 (2) (2013) 1–9.
[3] S.A. Chaudhry, A. Irshad, J. Nebhen, A.K. Bashir, N. Moustafa, Y.D. Al-Otaibi, Y.B. Zikria, An anonymous device to device access control based on secure certificate for internet of medical things systems, Sustainable Cities Soc. 75 (2021) 103322, http://dx.doi.org/10.1016/j.scs.2021.103322.
[4] R. Want, An introduction to RFID technology, IEEE Pervasive Comput. 5 (1) (2006) 25–33.
[5] B. Nath, F. Reynolds, R. Want, RFID technology and applications, IEEE Pervasive Comput. 5 (1) (2006) 22–24.
[6] S. Iyer, RFID: Technology and applications, 2005, IIT Bombay, Presentation.
[7] N. Dinarvand, H. Barati, An efficient and secure RFID authentication protocol using elliptic curve cryptography, Wirel. Netw. 25 (1) (2019) 415–428.
[8] N. Dinarvand, H. Barati, A survey and comparing RFID authentication protocols based on elliptic curve cryptography, Majlesi J. Telecommun. Devices 5 (1) (2016).
[9] M. Shariq, K. Singh, C. Lal, M. Conti, T. Khan, ESRAS: An efficient and secure ultra-lightweight RFID authentication scheme for low-cost tags, Comput. Netw. 217 (2022) 109360.
[10] M. Shariq, K. Singh, A secure and lightweight RFID-enabled protocol for IoT healthcare environment: A vector space based approach, Wirel. Pers. Commun. (2022) 1–25.
[11] D. Dharminder, D. Mishra, X. Li, Construction of RSA-based authentication scheme in authorized access to healthcare services, J. Med. Syst. 44 (1) (2020) 1–9.
[12] W. Yao, C.-H. Chu, Z. Li, The adoption and implementation of RFID technologies in healthcare: A literature review, J. Med. Syst. 36 (6) (2012) 3507–3525.
[13] S. Ajami, A. Rajabzadeh, Radio frequency identification (RFID) technology and patient safety, J. Res. Med. Sci. 18 (9) (2013) 809.
[14] H.-Y. Chien, C.-C. Yang, T.-C. Wu, C.-F. Lee, Two RFID-based solutions to enhance inpatient medication safety, J. Med. Syst. 35 (3) (2011) 369–375.
[15] L. Atzori, A. Iera, G. Morabito, The Internet of Things: A survey, Comput. Netw. 54 (15) (2010) 2787–2805.
[16] W. Yao, C.-H. Chu, Z. Li, The use of RFID in healthcare: Benefits and barriers, in: 2010 IEEE International Conference on RFID-Technology and Applications, IEEE, 2010, pp. 128–134.
[17] M. Haddara, A. Staaby, RFID applications and adoptions in healthcare: A review on patient safety, Procedia Comput. Sci. 138 (2018) 80–88.
[18] M. Shariq, K. Singh, P.K. Maurya, A. Ahmadian, M.R.K. Ariffin, URASP: An ultralightweight RFID authentication scheme using permutation operation, Peer Peer Netw. Appl. 14 (6) (2021) 3737–3757.
[19] M. Shariq, K. Singh, M.Y. Bajuri, A.A. Pantelous, A. Ahmadian, M. Salimi, A secure and reliable RFID authentication protocol using digital schnorr cryptosystem for IoT-enabled healthcare in COVID-19 scenario, Sustainable Cities Soc. 75 (2021) 103354.
[20] M. Shariq, K. Singh, A novel vector-space-based lightweight privacy-preserving rfid authentication protocol for IoT environment, J. Supercomput. 77 (8) (2021) 8532–8562.
[21] M. Shariq, K. Singh, A vector-space-based lightweight rfid authentication protocol, Int. J. Inf. Technol. 14 (3) (2022) 1311–1320.
[22] M. Shariq, K. Singh, P.K. Maurya, A. Ahmadian, D. Taniar, AnonSURP: An anonymous and secure ultralightweight RFID protocol for deployment in internet of vehicles systems, J. Supercomput. 78 (6) (2022) 8577–8602.
[23] P.P. López, D.D.J.C.H. Castro, D.D.A.R. Garnacho, Lightweight Cryptography in Radio Frequency Identification (RFID) Systems, Computer Science Department, Carlos III University of Madrid, 2008.
[24] D. He, S. Zeadally, An analysis of RFID authentication schemes for Internet of Things in healthcare environment using elliptic curve cryptography, IEEE Internet Things J. 2 (1) (2014) 72–83.
[25] M.-G. Avram, Advantages and challenges of adopting cloud computing from an enterprise perspective, Proc. Technol. 12 (2014) 529–534.
[26] F. Wu, L. Xu, S. Kumari, X. Li, A.K. Das, J. Shen, A lightweight and anonymous RFID tag authentication protocol with cloud assistance for e-healthcare applications, J. Ambient Intell. Humaniz. Comput. 9 (4) (2018) 919–930.
[27] K. Fan, W. Jiang, H. Li, Y. Yang, Lightweight RFID protocol for medical privacy protection in IoT, IEEE Trans. Ind. Inform. 14 (4) (2018) 1656–1665.
[28] K. Fan, S. Zhu, K. Zhang, H. Li, Y. Yang, A lightweight authentication scheme for cloud-based RFID healthcare systems, IEEE Netw. 33 (2) (2019) 44–49.
[29] F. Rahman, M.Z.A. Bhuiyan, S.I. Ahamed, A privacy preserving framework for RFID based healthcare systems, Future Gener. Comput. Syst. 72 (2017) 339–352.
[30] W. Xie, L. Xie, C. Zhang, Q. Zhang, C. Tang, Cloud-based RFID authentication, in: 2013 IEEE International Conference on RFID, RFID, IEEE, 2013, pp. 168–175.
[31] S. Abughazalah, K. Markantonakis, K. Mayes, Secure improved cloud-based RFID authentication protocol, in: Data Privacy Management, Autonomous Spontaneous Security, and Security Assurance, Springer, 2014, pp. 147–164.
[32] H. Xiao, A.A. Alshehri, B. Christianson, A cloud-based RFID authentication protocol with insecure communication channels, in: 2016 IEEE Trustcom/BigDataSE/ISPA, IEEE, 2016, pp. 332–339.
[33] K. Fan, Q. Luo, K. Zhang, Y. Yang, Cloud-based lightweight secure RFID mutual authentication protocol in IoT, Inform. Sci. 527 (2020) 329–340.
[34] J. Song, P.-W. Harn, K. Sakai, M.-T. Sun, W.-S. Ku, An RFID zero-knowledge authentication protocol based on quadratic residues, IEEE Internet Things J. (2021).
[35] B. Surekha, K.L. Narayana, P. Jayaprakash, C.S. Vorugunti, A realistic lightweight authentication protocol for securing cloud based RFID system, in: 2016 IEEE International Conference on Cloud Computing in Emerging Markets, CCEM, IEEE, 2016, pp. 54–60.
[36] Z. Zhao, A secure RFID authentication protocol for healthcare environments using elliptic curve cryptosystem, J. Med. Syst. 38 (5) (2014) 1–7.
[37] M.S. Farash, O. Nawaz, K. Mahmood, S.A. Chaudhry, M.K. Khan, A provably secure RFID authentication protocol based on elliptic curve for healthcare environments, J. Med. Syst. 40 (7) (2016) 1–7.
[38] S.F. Aghili, H. Mala, P. Kaliyar, M. Conti, SecLAP: Secure and lightweight RFID authentication protocol for Medical IoT, Future Gener. Comput. Syst. 101 (2019) 621–634.
[39] M. Safkhani, Y. Bendavid, S. Rostampour, N. Bagheri, On designing lightweight RFID security protocols for medical IoT, Cryptol. ePrint Arch. (2019).
[40] F. Zhu, P. Li, H. Xu, R. Wang, A novel lightweight authentication scheme for RFID-based healthcare systems, Sensors 20 (17) (2020) 4846.
[41] S. Xie, F. Zhang, R. Cheng, Security enhanced RFID authentication protocols for healthcare environment, Wirel. Pers. Commun. 117 (1) (2021) 71–86.
[42] M. Adeli, N. Bagheri, S. Sadeghi, S. Kumari, χ perbp: A cloud-based lightweight mutual authentication protocol., IACR Cryptol. ePrint Arch. 2021 (2021) 144.