Multimedia Tools and Applications (2023) 82:16533–16554
https://doi.org/10.1007/s11042-022-14170-7

Quadratic residue-based unilateral authentication protocol for RFID system

Pramod Kumar Maurya[1] · Satya Bagchi[2]

Received: 24 February 2021 / Revised: 14 September 2022 / Accepted: 27 October 2022 /
Published online: 15 November 2022

Abstract

Nowadays, Radio frequency identification (RFID) plays an important role in many real-life applications for remotely identifying objects. RFID system works over a wireless communication environment. Because of this, the RFID system is not secure against various attacks such as user private data leakage, location tracking, and replay attack. To overcome these security flaws, we propose a quadratic residue-based authentication scheme for the RFID system. The scheme uses square root properties of quadratic residue to prevent existing possible attacks. Formal and informal security analysis of the proposed scheme shows that the proposed scheme resists various attacks. In addition, we use BAN logic and Scyther tool to simulate the scheme. The simulation results show that the proposed scheme withstands all possible attacks. Performance evaluation illustrates that the proposed scheme is efficient under a resource-constraints environment. Moreover, the proposed scheme does not store the private information of RFID tags in its database and identifies a tag with constant-time complexity.

Keywords RFID system · Quadratic residue · Square root modulo N · Authentication protocol · Security · Privacy

1 Introduction

RFID is a very valuable technology tool for the automatic identification of objects. Presently, RFID technology is used in many industrial applications for remotely identifying objects such as supply-chain management, access control, transportation, health industries, and automated payment systems. Generally, an RFID system is made up of three

✉ Pramod Kumar Maurya
pramod_kumar22490@hotmail.com

Satya Bagchi
satya5050@gmail.com

[1] School of Computer Science & Engineering, Vellore Institute of Technology, Vellore, Tamil Nadu, India

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

components: an RFID tag, an RFID reader, and a back-end server. The operating principle of an RFID system is that the reader broadcasts radio waves. A nearby tag replies to the reader with the essential information. Then the reader sends the received information to the server for authentication. RFID tags can categorize into two categories: active tags and passive tags. Active tags have in-built batteries for computation and transmission. These tags support computation-intensive algorithms such as symmetric/asymmetric encryption. Passive tags do not have in-built batteries. These tags drive energy from the radio signal emitted by the reader. RFID tags usually contain private and essential information about the products being tagged. Due to high productivity and low cost, RFID becomes a prominent wireless technology in industries and our day-to-day life for tracking and managing goods [2, 8, 10, 15, 22, 31, 32].

Besides the productivity and convenient use of RFID system, there are several serious privacy and security concerns with it due to the wireless communication [23, 24, 30, 33–35, 38]. Due to the insecure wireless networks, the RFID system is susceptible to various attacks such as eavesdropping, spoofing, cloning attack, and man-in-middle attack. To protect the RFID system, the design stage of RFID security schemes should include the following security features:

1. The security scheme should incur low computation and communication costs.
2. The security scheme should prevent de-synchronization attack and denial of service attack.
3. The scheme should ensure user privacy, anonymity, and location privacy.
4. The system should provide forward and backward secrecy.
5. The system should have capabilities to withstand reply attack, cloning attack, and collision attack.

Authentication schemes are considered a possible solution that defense the RFID system against privacy and security threats under the EPC Class-1 Gen-2 standards. In the past few decades, many authentication protocols are proposed by researchers that employ different security primitives such as one-way hash function, elliptic curve cryptography (ECC), permutation, quadratic residue, and encryption/decryption. Some of these protocols are vulnerable to one or more attacks, other protocols are not fit to the RFID resource-constraints environment.

1.1 Our contribution

The key contributions of this article are as follows.

1. We proposed a quadratic residue-based lightweight authentication protocol for the RFID system.
2. To reduce computational overhead and improve security functionality, we utilize only quadratic residue properties and hash function.
3. The security features of the proposed scheme are formally analyzed through the BAN logic and automated security analysis tool, Scyther. In addition, The scheme is also analyzed informally. The rigorous formal-informal analysis shows that the proposed scheme withstands several known attacks.
4. To evaluate the efficiency of the proposed scheme, the performance comparison is carried out with other existing protocols. The comparison demonstrates that the scheme incurs low overhead on the tag side as well as on the server side in comparison to the other existing schemes.

1.2 Paper organization

The contents of this paper are organized as follows. In Section 2, we give a brief description of the existing related works. In Section 3, we describe the capability of an adversary.The unilateral authentication scheme is proposed in Section 4. We demonstrate BAN logic correctness proof of the proposed scheme in Section 5. The security and privacy analysis of the proposed protocol is shown in Section 6. In Section 7, we analyze the performance efficiency of the proposed scheme. Finally, the conclusion is shown in Section 8.

2 Related works

In recent years, several authentication schemes are proposed by researchers to resolve RFID security concerns. Therefore, we discuss some existing schemes with their methodology, advantages, and disadvantages. Researchers widely used hash function as key security primitive in many RFID protocols. A hash-lock based scheme is proposed by Weis et al. [38] in 2004. The scheme employs a hash function to mask the tag's secret before transmitting it to a reader. However, this scheme is not secure from traceability attack and impersonation attack [7]. Tsudik et al. [36] introduced an improvement of the hash-lock scheme in 2006. This scheme introduces timestamp to avoid traceability attack. But later analysis demonstrates that the scheme is susceptible to denial of service attack and reply attack [19]. In 2014, Srivastava et al. [34] introduced a hash-based mutual authentication RFID scheme for telecare information medicine systems. The scheme employs a session key in each authentication round to provide strong privacy. However, Li et al. [20] discovered that the scheme is not secure against impersonation attack and disclosure attack. In addition, Li et al. [20] proposed an improvement of Srivastava's protocol in 2015. However, the enhanced version of Srivastava's protocol is still vulnerable under impersonation attack, traceability attack, and de-synchronization attack [3]. Kaul and Awasthi [17] proposed a threshold authentication protocol in 2017. The scheme achieves strong privacy due to the advantage of physical unclonable function and hash function. Zheng et al. [41] introduced a hash-based scheme for RFID-enabled digital campuses in 2018. The authors claim that the scheme withstands various attacks. However, This scheme is vulnerable to several attacks [29].

Other lightweight primitive such as permutation is also adopted by researchers in many RFID authentication protocols. Some well-known permutation-based schemes are as follows. In 2012, Tian et al. [35] introduced an RFID authentication scheme, RAPP. The scheme employs a new operation called a permutation. However, this scheme is efficient in the low-cost environment but does not resist disclosure attack, traceability attack, and de-synchronization attack [26]. Gao et al. [15] proposed a permutation-based authentication protocol that utilizes cyclic redundancy check and permutation function for computation in 2014. However, this protocol incurs de-synchronization attack [1]. Zhuang et al. [44] proposed a reconstruction-based authentication scheme, R^2AP, in 2014. The authors presented a bit-wise operaton, reconstruction, that is almost the same as permutation operation with some modifications. However, Safkhani [28] highlighted a disclosure attack, traceability attack, and challenged its security claims. Luo et al. [21] introduced a lightweight RFID authentication protocol, SLAP, in 2018. The scheme introduced a conversion function that possesses irreversibility, full confusion, and sensibility. However, Khalid et al. [18] show that the scheme is vulnerable to impersonation attack and de-synchronization attack.

Many quadratic residue-based lightweight authentication protocols are proposed by researchers in recent years. Chen et al. [6] proposed a quadratic residue-based authentication scheme for an RFID system in 2008. The authors utilize quadratic residue properties to resist the scheme against various known attacks. However, Cho and Shen [5] analyze Chen et al.'s scheme and found that the scheme is vulnerable to tag impersonation attack, replay attack, and data privacy attack. Yeh et al. [40] proposed a mutual authentication scheme that is an improved version of Chen et al.'s scheme in 2011. The proposed scheme resists all possible attacks that are found in Chen et al.'s scheme. Doss et al. [12] found that Yeh et al. [40] have some weaknesses. To overcome these weaknesses, Doss et al. [12] proposed a collaborative authentication scheme in 2013. The scheme employs modular squaring and pseudo-random number generator functions to achieve privacy and security. However, this scheme is not secure against replay attack [9]. In 2013, Kardas et al. [16] proposed a unilateral authentication scheme for an RFID system. The scheme employs quadratic residue properties to achieve destructive privacy. The scheme requires a considerable amount of hash operations to authenticate a tag, making the scheme difficult to implement. A quadratic residue-based bilateral authentication scheme is proposed by Chiou et al. [9] in 2018. The scheme uses a virtual ID and time challenge to achieve data privacy. Moreover, the authors simulate the scheme with mobile equipment to demonstrate its efficiency and feasibility. However, the protocol is not secure under traceability attack and data leakage. Zhou et al. [43] introduced a mutual RFID authentication scheme based on quadratic residue for telecare medicine information systems in 2019. The scheme uses a timestamp concept along with characteristics of quadratic residue to attain strong forward privacy. Unfortunately, the scheme is not appropriate for low-cost tags due to the high computational cost. Doss et al. [13] proposed a secure attribute-based authentication protocol to improve security and intelligence in supply chain management in 2020. In this protocol, the authors employ a set of attribute values to identify groups of RFID tags at the same time. The protocol is secure against various well-known attacks at cost of expensive cryptographic primitives such as hash functions, public-key encryption/decryption, pseudo-random number generator (PRNG), and modulus operations.

3 Adversary model

In this section, we present the abilities of an adversary $\mathscr{A}$ in the form of the following oracle queries. In this model, tags are classified into two categories. Tags that belong to the reading range of $\mathscr{A}$ are defined as drawn tags and tags that are not accessible by $\mathscr{A}$ are considered as free tags. The adversary model is based on the Vaudenay privacy model [37] with some modifications.

1. DrawTag$(distr, n) \rightarrow (vtag_1, b_1, vtag_2, b_2, \cdots, vtag_n, b_n)$: $\mathscr{A}$ chooses randomly a set of n tags from the set of free tags with probability distribution $distr$. The drawn tag $vtag_i$ is legitimate if $b_i = 1$.
2. Free$(vtag)$: With this oracle query, $\mathscr{A}$ changes the status of a tag from drawn to free. Thus, the adversary can not access the tag.
3. SendReader$(m) \rightarrow m'$: The adversary sends a message m to a reader. The reader responds with the message m'.
4. SendTag$(m, vtag) \rightarrow m'$: $\mathscr{A}$ sends a message m to a drawn tag $vtag$ by this oracle query. The tag responds with message m'.
5. Result: If $\mathscr{A}$ succeeds, the output of this oracle is 1, otherwise 0.

3.1 Privacy experiment: $Exp_{\mathscr{A}}^{priv}$

The privacy experiment is composed of three phases as described below.

1. Learning Phase: The adversary $\mathscr{A}$ interacts with the system by oracle queries and gets a list of drawn tags.
2. Challenging Phase: $\mathscr{A}$ selects two tags randomly from the drawn tag's list. The adversary tries to distinguish between them.
3. Guessing Phase: The adversary returns 1 if he succeeds, otherwise 0.

4 Proposed scheme

The details of the proposed scheme are given in this section. All the notations are tabulated in Table 1. The flow diagram of the proposed scheme is shown in Fig. 1.

4.1 Assumptions

The following assumptions are necessary for the proposed scheme.

1. An initiator generates two distinct large prime p and q and computes $N = p \times q$. The initiator shares p, q, and N with the server.
2. For each tag, the initiator uniquely chooses a ID and calculates a square root x of ID modulo N. The initiator stores $\{ID, x\}$ to the tag's internal memory.
3. The reader and tags agreed on a pseudo-random number generator (PRNG).
4. The server and tags agreed on a hash function, $h()$.
5. The communication channel between the server and the reader is secure.

4.2 Proposed authentication protocol

The authentication phases of the proposed scheme are as follows.

Phase 1: A reader generates a random number r_1 and transmits it to a tag.

Phase 2: Upon receiving r_1, the tag generates a random number r_2. The tag computes response messages as follows:

Table 1 Notations

Notation	Description
r_1	A random number generated by a reader.
r_2	A random number generated by a tag.
$N = p \times q$	It is a product of two distinct odd primes p and q.
ID	Unique identification number of a tag and it is also a quadratic residue modulo N.
x	A square root of ID modulo N.
$\cdot$	Arithmetic multiplication modulo N.

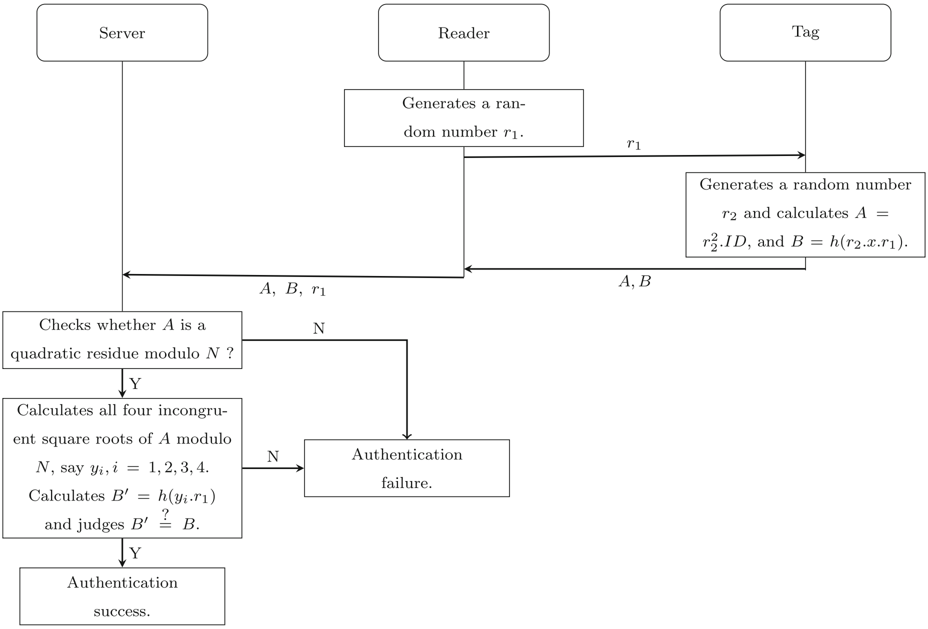

Server
Reader
Tag
Generates a random number r_1.
r_1
Generates a random number r_2 and calculates $A = r_2^2.ID$, and $B = h(r_2.x.r_1)$.
A, B
$A,\ B,\ r_1$
Checks whether A is a quadratic residue modulo N ?
N
Y
Calculates all four incongruent square roots of A modulo N, say $y_i, i = 1,2,3,4$. Calculates $B' = h(y_i.r_1)$ and judges $B' \overset{?}{=} B$.
N
Authentication failure.
Y
Authentication success.

Fig. 1 A quadratic residue based authentication protocol for RFID system

- Calculates $A = r_2^2 \cdot ID$ and $B = h(r_2 \cdot x \cdot r_1)$. The tag transmits A and B to the reader.

Phase 3: The reader forwards A and B along with r_1 to a server.

Phase 4: After receiving a message from the reader, the server authenticates the tag as follows:

- The server checks whether A is a quadratic residue modulo N or not by using stored p and q.
- If A is a quadratic residue modulo N, the server performs as follows:
  - The server computes all four in-congruent square roots modulo N of A (say, $y_1,\ y_2,\ y_3,\ y_4$) with the help of stored p and q. Here, y_i is the same as $r_2 \cdot x_i$, where x_i denotes a square root of ID modulo N.
  - For each y_i, $i = 1, 2, 3, 4$, the server computes $B' = h(y_i \cdot r_1) = h(r_2 \cdot x_i \cdot r_1)$ and checks whether B' is equal to the received B or not.
  - If $B' = B$ for any i, the server authenticates the tag otherwise terminates the authentication session.
- If A is not a quadratic residue modulo N, the server terminates the session.

4.3 Example 1

Suppose an initiator chooses $p = 11$ and $q = 13$. Then $N = p \times q = 143$. Now, the initiator chooses a unique identification number $ID = 23$ for a tag T. It calculates all the distinct square roots of ID modulo N by using p and q. According to quadratic residue properties, there exist only four distinct square roots of ID modulo N. That is, the square roots are 32, 45, 98, and 111. It is convenient to take the square roots of ID modulo N to be a set of the form $S_1 = \{x_1 = 32, x_2 = 45, x_3 = 98, x_4 = 111\}$. Suppose the initiator chooses $x = 45 \in S_1$ for the tag T. With these data, the analytic proof of the proposed scheme is as follows.

Phase 1: A reader generates a random number r_1 (say, $r_1 = 113$) and transmits it to the tag T.

Phase 2: Upon receiving r_1, T chooses a random number r_2 (say, $r_2 = 69$). The tag computes response messages as follows:

$$\begin{aligned} A &= r_2^2 \cdot ID \\ &= (r_2^2 \times ID) \mod N \\ &= (69^2 \times 23) \mod 143 \\ &= 108 \\ B &= h(r_2 \cdot x \cdot r_1) \\ &= h(r_2 \times x \times r_1) \mod N \\ &= SHA-256((69 \times 45 \times 113) \mod 143) \\ &= 434c9b5ae514646bbd91b50032ca579efec8f22bf0b4aac12e65997 \\ &\quad c418e0dd6. \end{aligned}$$

Here, we consider SHA-256 as our hash function $h()$. The tag transmits A and B to the reader.

Phase 3: The reader forwards A and B with r_1 to a server.

Phase 4: After receiving A, B, and r_1 from the reader, the server authenticates the tag as follows:

- The server calculates all distinct square roots of A modulo N by using stored p and q. The square roots of A modulo N are 63, 102, 41, and 80. It is convenient to take the square roots of A modulo N to be a set of the form $S_2 = \{y_1 = 63, y_2 = 102, y_3 = 41, y_4 = 80\}$. Note that S_2 is same as $r_2 \cdot S_1$ as shown below.

$$\begin{aligned} S_2 &= r_2 \cdot S_1 \\ &= r_2 \cdot \{x_1, x_2, x_3, x_4\} \\ &= \{(r_2 \times x_1) \mod N, (r_2 \times x_2) \mod N, (r_2 \times x_3) \\ &\quad \mod N, (r_2 \times x_4) \mod N\} \\ &= \{(69 \times 32) \mod 143, (69 \times 45) \mod 143, (69 \times 98) \\ &\quad \mod 143, (69 \times 111) \mod 143\} \\ &= \{63, 102, 41, 80\} \\ &= \{y_1, y_2, y_3, y_4\} \end{aligned}$$

- For each y_i, $i = 1, 2, 3, 4$, the server computes B' as follows.

$$
\begin{aligned}
B' &= h(y_i \cdot r_1)\\
&= SHA-256(y_i \cdot r_1)\\
B'_1 &= SHA-256(y_1 \cdot r_1)\\
&= b1556dea32e9d0cdbfed038fd7787275775ea40939c146a64\\
&\quad e205bcb349ad02f\\
B'_2 &= SHA-256(y_2 \cdot r_1)\\
&= 434c9b5ae514646bbd91b50032ca579efec8f22bf0b4aac12\\
&\quad e65997c418e0dd6\\
B'_3 &= SHA-256(y_3 \cdot r_1)\\
&= c837649cce43f2729138e72cc315207057ac82599a59be72765\\
&\quad a477f22d14a54\\
B'_4 &= SHA-256(y_4 \cdot r_1)\\
&= eb1e33e8a81b697b75855af6bfcdbcbf7cbbde9f94962ceaec1\\
&\quad ed8af21f5a50f
\end{aligned}
$$

- The server checks whether B'_i is equal to the received B for any i. Here, B'_2 is equal to the received B. Hence, the server authenticates the tag T.

5 BAN logic correctness proof

In this section, we use the BAN logic to verify the correctness of our proposed scheme. The BAN logic is a mechanism that describes the knowledge and beliefs of involved parties in a systematic way and derives new beliefs from the known beliefs. We give the answer to the following questions by using the BAN logic.

- Does the proposed protocol work?
- What does the proposed protocol achieve?

To give correctness proof by using the BAN logic, we need to formalize the scheme by using the BAN logic symbols. Some BAN logic symbols are listed in Table 2.

Table 2 Symbols

Notation	Description
$A \mid\equiv B$	This symbol means the entity A believes statement B is true.
$A \triangleleft B$	The entity A receives a message that contains a statement B.
$A \mid\sim B$	The entity A at some time sent a message including a statement B.
$A \Rightarrow B$	The entity A has jurisdiction over B.
$A\#(B)$	The statement B is fresh.
$A \vdash B$	A imply B.
$\{B\}_k$	The statement B is encrypted under the key k.

Rules: The essential rules that we use in the correctness proof are as below.

1. $\dfrac{P \mid\equiv Q \Rightarrow k,\ P \lhd \{M\}_k}{P \mid\equiv Q \mid\sim \{M\}}$

Rule 1 says that if an entity P believes that an entity Q has jurisdiction over k and receives a message $\{M\}_k$, then P believes that Q has sent the message $\{M\}$.

2. $\dfrac{P \mid\equiv \#(M)}{P \mid\equiv \#(M, X)}$

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

The correctness proof is divided into five parts. Details of each part are given below. In the proof, R stands for a reader, T stands for a tag, and S stands for a back-end server.

5.1 Protocol description

This subsection describes the formal expression of information transmitted between the communication entities in the system.

1. R → T: $\{r_1\}$
2. T → R: $\{r_2^2 \cdot ID, h(r_2 \cdot x \cdot r_1)\}$
3. R → S: $\{r_1, r_2^2 \cdot ID, h(r_2 \cdot x \cdot r_1)\}$

5.2 Protocol idealisation

In this part, the protocol description is given in the BAN logic syntax.

1. R → T: $\{r_1\}$
2. T → R: $\{\{r_2 \sim r_2\}_{ID}, \{r_2 \sim r_1\}_x\}$
3. R → S: $\{r_1, \{r_2 \sim r_2\}_{ID}, \{r_2 \sim r_1\}_x\}$

5.3 Initial assumption

Based on the capabilities of each entity in the proposed scheme, the following assumptions are derived.

1. $S \mid\equiv T \Rightarrow \{ID, x\}$
2. $S \mid\equiv \#(R)$

5.4 Protocol goal

The security goal of the proposed scheme is as follows.

$$S \mid\equiv T \mid\sim \#(\{r_2 \sim r_2\}, \{r_2 \sim r_1\})$$

5.5 Proof process

According to assumption 1 and idealization 3, we get

$$\begin{aligned} &S \mid \equiv T \Rightarrow \{ID, x\}, \quad R \rightarrow S : \{r_1, \{r_2 \sim r_2\}_{ID}, \{r_2 \sim r_1\}_x\} \\ &\quad \vdash\ S \lhd \{r_1, \{r_2 \sim r_2\}_{ID}, \{r_2 \sim r_1\}_x\} \end{aligned} \tag{1}$$

using rule 1 and (1), we get

$$\vdash S \mid\equiv T \mid\sim \{\{r_2 \sim r_2\}, \{r_2 \sim r_1\}\} \tag{2}$$

According to assumption 2, we get

$$\begin{aligned} &S \mid\equiv \#(R) \\ &\quad \vdash \ S \mid\equiv \#(\{r_2 \sim r_2\}, \{r_2 \sim r_1\}) \end{aligned} \tag{3}$$

Therefore from (2) and (3), we get

$$S \mid\equiv T \mid\sim \#\{r_2 \sim r_2\}, \{r_2 \sim r_1\}$$

Hence, our protocol goal is proved.

6 Security and privacy analysis

We analyze the security and privacy features of our proposed scheme in this section.

6.1 Formal analysis

Theorem 1 *The proposed scheme achieves information privacy if $h(.)$ is a one-way hash function.*

Proof Let us assume that the adversary $\mathscr{A}$ performs the following privacy experiment.

- Learning Phase: The adversary interacts with the RFID system by oracle queries. The adversary gets a list of n drawn tags by DrawTag oracle query.

$$DrawTag(distr, n) \rightarrow (vtag_1, b_1, vtag_2, b_2, \ldots, vtag_n, b_n).$$

- Challenging Phase: $\mathscr{A}$ selects two tags, say $vtag_i$ and $vtag_j$ from the above-drawn tags list and changes the status of the remaining tags of the list from drawn to free. The adversary randomly chooses one tag from the previously selected two tags, say $vtag_b$, $b \in \{i, j\}$. $\mathscr{A}$ evaluates all oracle queries on $vtag_b$, i.e.,

$$\text{Free}(vtag_k), \text{ for all } k \in \{1, \ldots, n\} \text{ except } k \neq i \text{ and } k \neq j$$

$$\text{SendReader}(init) \rightarrow r_1$$

$$\text{SendTag}(r_1, \ vtag_b) \rightarrow (A, \ B)$$

$$\text{SendReader}(A, B) \rightarrow b.$$

- Guessing Phase: The adversary returns a bit b for the corresponding tag.

For $\mathscr{A}$, it is not feasible to guess correctly $vtag_b$ is either $vtag_i$ or $vtag_j$, without knowing secret information that is used in the response messages $(A, \ B)$. Also, the extraction of the secret information from the response messages is not possible for the adversary due to the hash function. Thus our proposed protocol attains information privacy. □

Theorem 2 *The proposed scheme is untraceable if $h(.)$ is a one-way hash function.*

Proof Let us assume that our proposed scheme is traceable. So, the success probability to win the privacy experiment is non-negligible. $\mathscr{A}$'s privacy experiment is as follows.

- Learning Phase: The adversary gets access to n tags by DrawTag oracle query. $\mathscr{A}$ can send several oracles queries to a drawn tag. The adversary analyzes the protocol runs between a reader and a chosen drawn tag, say $vtag$.

$$\text{DrawTag}(distr, n) \rightarrow (vtag_1, b_1, vtag_2, b_2, \ldots, vtag_n, b_n)$$

$$\text{SendReader}(init) \rightarrow r_1$$

$$\text{SendTag}(r_1,\ vtag) \rightarrow (A,\ B).$$

- Challenging Phase: The adversary chooses $vtag_i$ and $vtag_j$ as its challenge tags from the drawn tag's list. $\mathscr{A}$ randomly selects one among them, say $vtag_b$, $b \in \{i, j\}$. $\mathscr{A}$ sends response message r_1 which is learned in the learning phase to the tag $vtag_b$, i.e.,

$$\text{SendTag}(r_1,\ vtag_b) \rightarrow (A^\star,\ B^\star)$$

$$\text{SendReader}(A^\star,\ B^\star) \rightarrow b.$$

- Guessing Phase: The adversary outputs a bit b for the corresponding tag.

$\mathscr{A}$ wins the privacy game only if

$$Pr[A^\star = A] = 1 \text{ and } Pr[B^\star = B] = 1.$$

but $A^\star \neq A$ and $B^\star \neq B$ because A and B depend upon pseudo-random numbers r_1 and r_2 which are different in each authentication session. Thus the adversary can not trace $vtag_b$. Hence, our proposed scheme is untraceable. □

6.2 Informal analysis

We present an informal analysis of the proposed scheme in this subsection.

6.2.1 Anonymity

The proposed scheme does not reveal the tag's secret information, i.e., ID and x, to an adversary during transmission. Note that the tag's secret information is used in the local. The unique secrets ID and x can not be inferred from the transmitted message A and B due to the advantage of the integer factorization problem and one-way hash function $h()$. In addition, the tag uses the random number r_2 in the local and it is different in each session. So, an attacker can not retrieve ID from A without knowing the random number r_2. Thus, the proposed scheme provides tag anonymity.

6.2.2 Collision attack resistance

To apply a collision attack in the proposed scheme, an adversary needs to find a number N_1 such that $N_1 \mod N = A \mod N$, where A is the transmitted message. Along with N_1, the adversary needs a square root of N_1. Note that N is stored in the server. So, it is hard for the adversary to find N_1 without knowing N. In addition, if we assume that the adversary knows N_1, then it is still difficult to find a square root of N_1 without knowing the factors of N. Thus, the proposed scheme strongly resists collision attack.

6.2.3 Denial of service attack resistance

Without the protection of a denial of service (DoS) attack, an adversary can cause unauthorized tag disabling, i.e., tags can no longer function properly. In the proposed scheme, the

RFID tag does not update its secret data during authentication. So, the adversary is not able to modify the tag's secret in such a way that the tag no longer functions. Thus, the proposed scheme is not vulnerable under DoS attack.

6.2.4 Forward/Backward secrecy

In the proposed scheme, suppose an adversary cracks a tag and gets all the secret information. Suppose the adversary intercepts the previous session transmitted messages r_1, A and B. However, the adversary can not decode A or B due to the dependence on r_2. To get the value of r_2, the adversary has to find a square root of $A.ID^{-1}$ under modulo N. Without knowing the factors of N, finding a square root under modulo N is computationally equivalent to the integer factorization problem. Thus, by knowing the secret information of the tag, the attacker can not decode the previous session transmitted messages. Similarly, backward secrecy can be proved in which the attacker can not decode the messages transmitted by the tag in the future. Thus, the proposed scheme provides both forward and backward secrecy.

6.2.5 Replay attack resistance

In the proposed scheme, in each authentication session, the transmitted message, i.e., (A, B) composes newly generated random numbers. So, it is not possible for $\mathscr{A}$ to prove itself as a legitimate party by transmitting previous session messages. We can prove our viewpoint as follows. suppose A', B', r_1', and r_2' are old session data and A, B, r_1, and r_2 are current session data. Now, in the current session, whenever the reader queries a tag by sending r_1, $\mathscr{A}$ transmits A' and B' to the reader. The reader forwards these values with r_1 to the server. The server computes all four incongruent square roots of A' (say, $y_i, i = 1, 2, 3, 4$). The server computes local $B' = h(y_i.r_1)$ for each y_i and checks whether any of them is the same as the received B' or not. Unfortunately, the computed local B' is not the same as the received B' because the received B' uses r_1' whereas the computed local B' uses r_1 in its computation. So, the server terminates the session without authenticating the adversary as a legitimate party.

6.2.6 Man-in-middle attack resistance

The proposed scheme resists a man-in-middle attack actively. $\mathscr{A}$ can not fetch the secret data from the transmitted messages. So, $\mathscr{A}$ is not able to manipulate the transmitted messages without knowing the secret data.

6.2.7 De-synchronization attack resistance

The proposed scheme does not update any secret values between the tag and the server. For this reason, there is no possibility of a de-synchronization attack in the scheme.

6.2.8 Cloning attack resistance

$\mathscr{A}$ can not duplicate a pre-existing tag without knowing its secret data. It is not possible for $\mathscr{A}$ to fetch the secret data from the transmitted messages. Hence, the proposed scheme strongly resists a cloning attack.

6.2.9 Scalability

In the proposed scheme, the server does not retrieve the tag's secret data from the database to authenticate a tag. The server authenticates a tag just based on the received data. Thus, the time cost to locate the tag is constant. So, the proposed scheme does not perform exhaustive search operations to authenticate a tag and thus is of scalability.

6.3 Security analysis of the proposed scheme by using Scyther tool

Scyther is an automatic tool for formal analysis, verification, and falsification of security protocols. Scyther performs under the Dolev-Yao attack model. In this model, an adversary has the capabilities to block, eavesdrop, replay, and modify messages sent by honest entities. To simulate the proposed scheme, we use Scyther software version v1.1.3 in our host system. We use the Microsoft Windows 11 operating system, an i-5 processor of 1.6 GHz, and 16.0 GB RAM in the host system. To use the Scyther tool, we have to convert the protocol description into a formal language, known as SPDL language. The SPDL language describes the protocol in role definitions and security properties in terms of claim events. Scyther uses an SPDL language description of the protocol as input and verifies the security claims.

Figure 2 depicts the SPDL language description of our proposed scheme. Here, we consider the server and reader as a single entity, called the reader. In this study, we define two

```
protocol Proposed(Tag,Reader){
role Tag{
const x,A,B,ID;
const Mul: Function;
const Pow: Function;
const Hash : Function;
const SqRoot:Function;
fresh r1,r2: Nonce;
macro C=Hash(Mul(SqRoot(A),r1));
recv_1(Reader,Tag,r1);
macro A = Mul(Pow(r2,2),ID);
macro B =Hash(Mul(r2,x,r1));
send_2(Tag,Reader,A,B);
claim(Tag, Secret, x);
claim(Tag, Secret, ID);
claim(Tag, Niagree);
claim(Tag, Nisynch);
claim(Tag, Alive);
claim(Tag, Weakagree);
}
```

```
role Reader{
const x,A,B,ID;
const Mul: Function;
const Pow: Function;
const Hash : Function;
const SqRoot:Function;
fresh r1,r2: Nonce;
macro A = Mul(Pow(r2,2),ID);
macro B =Hash(Mul(r2,x,r1));
send_1(Reader,Tag,r1);
recv_2(Tag,Reader,A,B);
macro C=Hash(Mul(SqRoot(A),r1));
match(B,C);
claim(Reader, Secret, x);
claim(Reader, Secret, ID);
claim(Reader, Secret, C);
claim(Reader, Niagree);
claim(Reader, Nisynch);
claim(Reader, Alive);
claim(Reader, Weakagree);
}
}
```

Fig. 2 SPDL description of the proposed protocol

roles, Tag and Reader, as shown in Fig. 2. In each role, first, we define the functions such as dot product, hash, exponential, and square root modulo function. We declare pseudo-random numbers, i.e., r1 and r2 by using the fresh declaration. We define macros A, B, and C to simplify the protocol specification. The send and recv events are used for sending and receiving a message, respectively. In the reader role, the reader sends (r1) to a tag and receives (A, B) from the tag. In the tag role, the tag receives (r1) from the reader and sends (A, B) to the reader. At the end of both roles, we used security claim events to model intended security properties. In our claim events, from the tag's point of view, we perform the following claims.

$$claim(Tag, Secret, x)$$
$$claim(Tag, Secret, ID)$$
$$claim(Tag, Niagree)$$
$$claim(Tag, Nisynch)$$
$$claim(Tag, Alive)$$
$$claim(Tag, Weakagree)$$

The claim event with attribute $Secret$ ensures the secrecy of information. More specifically, $claim(Tag, Secret, x)$ means that the message x used in the run remains secret for the role Tag. The claim event with $Niagree$ ensures that the intended communication agents exchange messages in a pre-defined sequence. The attribute $Nisynch$ in the claim event is used to verify that all received messages of an intended receiver are sent by an honest sender. The claim event with attribute $Alive$ ensures that the messages transmitted between intended communication parties are not tampered by an adversary. The attribute $Weakagree$ ensures that an intruder can not disguise a communication agent by imitating any other communication agent. To learn more about the Scyther tool, we refer to [11].

The tool automatically verifies all the claims that are mentioned in Fig. 2. Note that the Scyther tool shows "OK" if it does not find any attack. On the contrary, if it finds an attack, it shows " Fail" for the security claim. Figure 3 depicts the security analysis result of the proposed scheme. The security analysis result shows "OK" for each security claim that is mentioned in Fig. 2. It shows that the Scyther tool can not find any attack against the proposed scheme, which confirms the security of the proposed scheme.

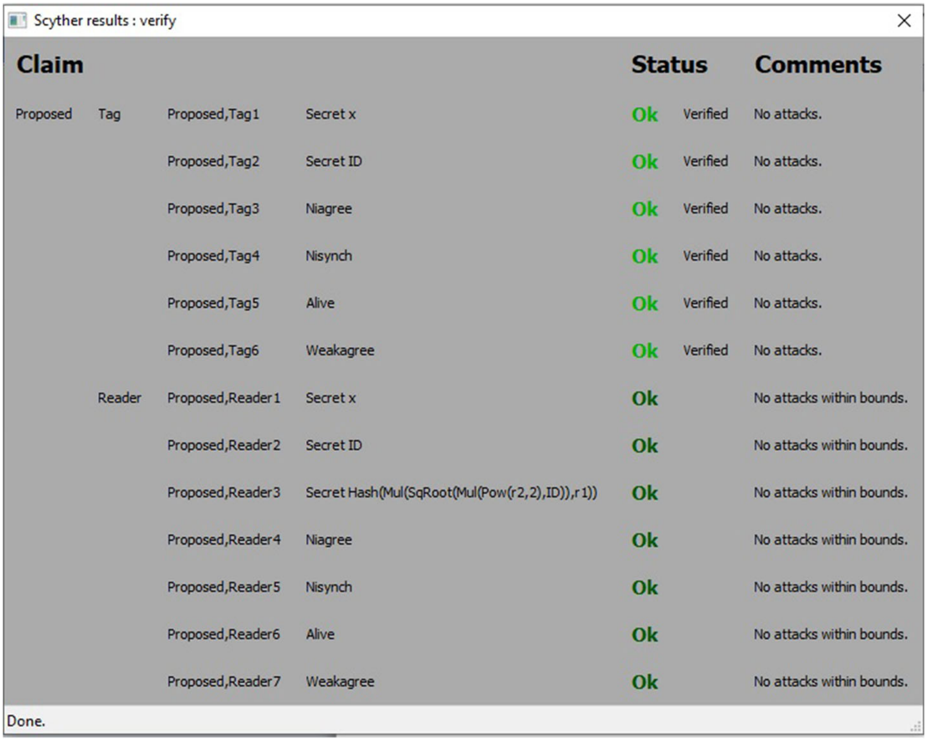
We compare the security performance of the proposed scheme with similar existing protocols, as shown in Table 3. The informal comparison shows that the proposed scheme resists various well-known attacks and preserves various privacy features while the other schemes have one or more weaknesses except Yeh et al. [40] and Doss et al. [13].

7 Performance evaluation

This section presents a performance analysis of the proposed scheme. In addition, this section demonstrates the advantages of the proposed scheme in real-life applications.

7.1 Computation cost analysis

In this subsection, we compare the proposed scheme with some other quadratic residue-based authentication schemes [9, 12, 13, 16, 40, 42, 43] in terms of computation and execution cost. In this comparison, we ignore lightweight operations such as XOR, shift, multiplication, and concatenation operations. In terms of computational operations, a comparison between the proposed scheme and the other quadratic residue-based authentication



Scyther results : verify

Claim				Status		Comments
Proposed	Tag	Proposed,Tag1	Secret x	Ok	Verified	No attacks.
		Proposed,Tag2	Secret ID	Ok	Verified	No attacks.
		Proposed,Tag3	Niagree	Ok	Verified	No attacks.
		Proposed,Tag4	Nisynch	Ok	Verified	No attacks.
		Proposed,Tag5	Alive	Ok	Verified	No attacks.
		Proposed,Tag6	Weakagree	Ok	Verified	No attacks.
	Reader	Proposed,Reader1	Secret x	Ok		No attacks within bounds.
		Proposed,Reader2	Secret ID	Ok		No attacks within bounds.
		Proposed,Reader3	Secret Hash(Mul(SqRoot(Mul(Pow(r2,2),ID)),r1))	Ok		No attacks within bounds.
		Proposed,Reader4	Niagree	Ok		No attacks within bounds.
		Proposed,Reader5	Nisynch	Ok		No attacks within bounds.
		Proposed,Reader6	Alive	Ok		No attacks within bounds.
		Proposed,Reader7	Weakagree	Ok		No attacks within bounds.

Done.

Fig. 3 Simulation result of the proposed protocol

Table 3 Security comparison among various RFID-based authentication protocols

Protocol	Yeh [40] (2011)	Doss [12] (2013)	Kardas [16] (2013)	Zhou [42] (2015)	Chiou [9] (2018)	Zhou [43] (2019)	Doss [13] (2020)	Proposed
SP1	✓	×	✓	×	✓	✓	✓	✓
SP2	✓	✓	✓	×	✓	✓	✓	✓
SP3	✓	✓	✓	✓	✓	×	✓	✓
SP4	✓	✓	✓	×	✓	✓	✓	✓
SP5	✓	✓	✓	×	×	✓	✓	✓
SP6	✓	✓	✓	✓	✓	✓	✓	✓
SP7	✓	✓	✓	✓	✓	✓	✓	✓
SP8	✓	✓	✓	✓	✓	✓	✓	✓
SP9	✓	×	✓	✓	✓	✓	✓	✓
SP10	✓	×	✓	✓	✓	✓	✓	✓
SP11	✓	×	×	✓	×	✓	✓	✓

SP1 - Replay attack resistance, SP2 - Man-in-middle attack resistance, SP3 - De-synchronization attack resistance

SP4 - Cloning attack resistance, SP5 - Anonymity, SP6 - Denial of Service attack resistance, SP7 - Authentication

SP8 - Collision attack resistance, SP9 - Forward secrecy, SP10 - Backward secrecy, SP11 - Un-traceability schemes is listed in Table 4. The proposed scheme does not employ the modulo squaring operation, whereas all the other schemes use it. The proposed scheme performs 1 hash operation on the tag side, while the other similar schemes employ a higher or equal number of hash operations except [12, 13], and [42]. The proposed scheme uses only 1 PRNG operation on the tag side, whereas the other schemes employ a higher or equal number of PRNG operations. On the server side, the proposed scheme performs 4 hash operations (worst case), 1 squaring root solving operation, and 1 PRNG operation, while the other schemes incur a higher computational load on the server side.

In accordance to Zhou et al. [43], the execution time of the cryptographic primitives are as follows: hash function $\approx$ 0.253 ms, pseudo-random number generator $\approx$ 0.021 ms, modular squaring operation $\approx$ 1.896 ms, and square root solving operation $\approx$3.481 ms. According to Mushtag et al. [27], the average execution time for symmetric key encryption/decryption is 15.333 ms. With these results, we estimate the computation cost of the proposed scheme in terms of execution time and compare it with other similar protocols. Table 5 depicts the execution time of all the protocols. In the proposed scheme, the computation cost on the tag side and the server side are 0.274 ms and 4.514 ms receptively. Overall, the total computation cost of the proposed scheme is 4.788 ms. Table 5 shows that the proposed scheme is highly efficient in terms of execution time in comparison to the other schemes. So from the above discussion, we can observe that the proposed scheme uses very few computational resources on the tag side as well as on the server side in comparison to the other quadratic residue-based schemes.

7.2 Communication cost analysis

This section compares the proposed scheme with other similar schemes in terms of communication cost as shown in Fig. 4. Here, “T–>R” means the communication cost from tag to reader, and “ R–>T ” means the communication cost from reader to tag. We assume that each parameter is of length 96-bits. In the proposed scheme, a reader transmits r_1 to a tag. So, the communication cost from the reader to the tag is 96-bits. The tag transmits A and B to the reader in the scheme. Hence, the communication cost from the tag to the reader is 192-bits. Overall, the total communication cost of the proposed scheme is 288-bits, which is fewer or equal in comparison to the other similar schemes as shown in Fig. 4.

7.3 Storage cost analysis

Here, we compare the storage cost of the proposed scheme with other similar protocols. Table 4 lists the storage cost of all the protocols. We assume that the length of each parameter is L-bits. In the proposed scheme, a tag stores 2 parameters: its unique ID and square root x. Thus each tag needs storage of 2L-bits. The server stores 3 parameters: p, q, and N in the proposed scheme. Thus the storage requirement on the server side is 3L-bits. In the proposed scheme, the storage cost on the server side does not depend on the number of tags in the system. This feature reduces the storage cost drastically in the proposed scheme. For instance, suppose L = 96-bits and the number of tags in the system is 1000. On the server side, the storage cost of the proposed scheme is only 288-bits whereas the storage cost of the protocols [9, 12, 16, 40, 42, 43] and [13] is 672000-bits, 1440000-bits, 384000-bits, 576000-bits, 1728000-bits, 1536000-bits and 384000-bits respectively. Thus, the proposed scheme incurs significantly less storage cost on the tag side as well as on the server side in comparison to the other schemes.

Table 4 Computation cost performance comparison

Protocol	Entity	Yeh [40] (2011)	Doss [12] (2013)	Kardas [16] (2013)	Zhou [42] (2015)	Chiou [9] (2018)	Zhou [43] (2019)	Doss [13] (2020)	Proposed
MSO	T	3	4	2	3	2	3	2	×
	R+S	×	4	×	1	4	3	×	×
Number of Hash	T	1	×	3	×	3	3	×	1
	R+S	13 (worst case)	2	18 (worst case)	×	×	14 (worst case)	1	4 (worst case)
SRO	T	×	×	×	×	×	×	×	×
	R+S	3	8	2	2	2	6	2	1
$E_k()/D_k()$	T	×	×	×	×	×	×	×	×
	R+S	×	×	×	×	×	×	4	×
No. of PRNG	T	2	3	1	3	2	1	1	1
	R+S	2	4	1	1	9	2	1	1
Required memory	T	$3L$	$4L$	$2L$	$4L$	$4L$	$4L$	4L	$2L$
	R+S	$7nL$	$15nL$	$4nL$	$6nL$	$18nL$	$16nL$	4nL	$3L$

T - Tag side, R - Reader side, S - Server side, n - Total number of tags in the system, $E_k()/D_k()$-Encryption/Decryption.

MSO - Modulo squaring operation, SRO - Squaring root solving operation, L-bit length of each parameters

Table 5 Computation cost comparison (in milisecond)

protocol	Tag	Server	Total
Yeh [40]	5.983	13.774	19.757
Doss [12]	7.647	36.022	43.669
Kardas [16]	4.572	11.537	16.109
Zhou [42]	5.751	8.879	14.630
Chiou [9]	4.593	14.735	19.328
Zhou [43]	6.468	30.158	36.626
Doss [13]	3.813	68.568	72.381
Proposed	0.274	4.514	4.788

7.4 Advantages of the proposed scheme in real-life applications

RFID technology is widely used in many applications such as access control systems, transport, supply-chain management, and healthcare industries. An access control system is one of the prominent applications that deploy RFID technology to authenticate and restrict

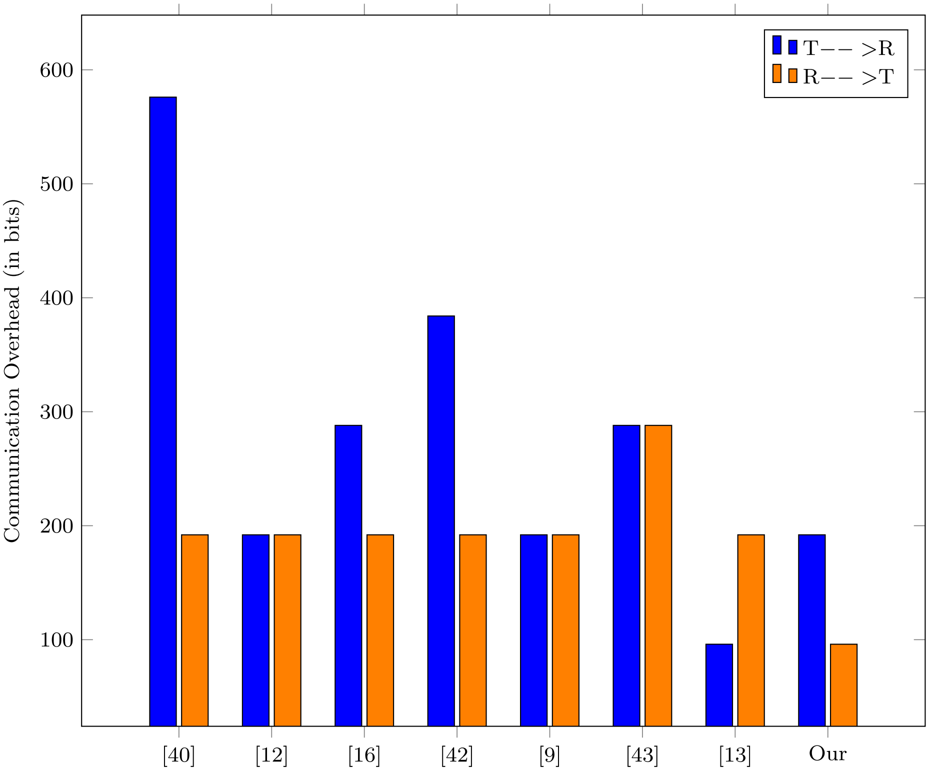


Fig. 4 Communication cost comparison

access to the physical environment like buildings, parking, and homes. Generally, an access control system is made up of two phases: the registration phase and the authentication phase. In the registration phase, a new user registers with the server. During the registration phase, the initiator stores credentials of the user such as unique identification number, password, biometric details, cryptography primitives, etc., in the smart card as well as in the database. The authentication phase comes into the picture when the user wants to access a secured area. At this point, the RFID reader captures a credential that is transmitted by an RFID-enabled smart card and transmits it to the server. The server scans the database for a match with the received data. If a match is found, access is granted to the user. The mechanism requires enough storage and computing power. RFID-based access control system is vulnerable to various attacks due to wireless communication. To overcome privacy and security issues, we can not use classical cryptography due to resource constraints that are existed with RFID. The proposed scheme resolves the privacy and security issues under the resource constraints environment. The advantages of the proposed scheme in RFID-based access control systems are as follows.

1. The proposed scheme performs only 1 hash and 1 PRNG on the tag side. It is suitable for RFID-based access control systems.
2. The scheme requires 2L-bits to store credentials on the tag side. It is appropriate for tiny-power smart cards.
3. The proposed scheme does not store the personal information of a user in the database during the registration phase. It requires 3L-bits of data to check the authenticity of a user. The scheme reduces the memory overhead on the server side drastically.
4. During the authentication phase, the server does not scan the database for a match with the received data.
5. In the worst case, the scheme employs 1 SRO and 4 hash operations to check the authenticity of a user. It is fit for those applications that have limited computational resources on the server side.
6. The proposed scheme is safe against several attacks as discussed in Section 6.

From the above points, we can conclude that the proposed scheme is very efficient in terms of storage and computational overhead. In addition, the scheme provides all the security features that are required in a secure RFID-based access control system.

7.5 Implementation discussion

RFID tags have very limited computational capabilities for security-related tasks. In accordance with Fan et al. [14], RFID tags have only 2500-3000 logic gates for security-related tasks such as authentication. So, if authentication is implementable under the available logic gates, then only it is worthy. The proposed scheme employs 1 PRNG, 1 modulo squaring operation, and 1 one-way hash function on the tag side during the authentication process. Due to the tag's resource constraints, a lightweight security primitive should be adopted. According to Wu et al. [39], a lightweight hash function "LHash" requires only 817 logical gates for implementation. A lightweight PRNG can be implemented only with 761 logic gates [25]. In accordance to Burmester et al. [4], modulo squaring operation can be implemented with < 1000 logic gates. So, the estimated implementation cost of the proposed scheme is $\simeq 2500$ logic gates. Hence, the proposed scheme can be implemented under the RFID environment.

8 Conclusion

In this article, we have proposed a unilateral authentication scheme for the RFID system. The novelty of the proposed scheme is to apply quadratic residue properties in such a way that the scheme withstands various well-known attacks along with minimal computation cost. In addition, The proposed scheme does not store the tag's secret information on the server and a tag can be authenticated by the server without revealing its identity to the server. We have proved the correctness of the proposed scheme by using BAN logic. Formal and informal security analysis shows that the proposed scheme prevents all possible security threats. In addition, we use the Scyther tool to demonstrate that the proposed scheme is secure against various threats. Performance analysis shows that the proposed scheme performs fewer computations on the tag side as well as on the server side in comparison to the other schemes as shown in Table 4. Table 5 shows that the execution time of the proposed scheme is approximately 70% less in comparison to the other similar schemes. The overall analysis shows that the proposed scheme is superior to the other similar existing protocols.

In the future, we will try to implement the proposed scheme. In addition, we will utilize coding theory properties to design post-quantum lightweight authentication schemes for RFID systems.

Data Availability Data sharing not applicable to this article as no datasets were generated or analyzed during the current study.

Declarations

Conflict of Interests The author P K Maurya thanks to VIT Vellore, India for the financial support of his research work.

References

1. Akgun M, Caglayan MU (2013) On the security of recently proposed RFID protocols. Cryptology ePrint Archive
2. Avoine G, Buttyant L, Holczer T, Vajda I (2007) Group-based private authentication. In: IEEE international symposium on a world of wireless, mobile and multimedia networks, pp 1–6
3. Benssalah M, Djeddou M, Drouiche K (2017) Security analysis and enhancement of the most recent RFID authentication protocol for telecare medicine information system. Wirel Pers Commun 96(4):6221–6238
4. Burmester M, De Medeiros B, Motta R (2008) Robust, anonymous RFID authentication with constant key-lookup. In: ACM symposium on information, computer and communications security, Japan, pp 283–291
5. Cao T, Shen P (2008) Cryptanalysis of some RFID authentication protocols. J Commun 3(7):20–27
6. Chen Y, Chou JS, Sun HM (2008) A novel mutual-authentication scheme based on quadratic residues for RFID systems. Comput Netw 52(12):2373–2380
7. Chatmon C, Le T, Burmester M (2006) Secure anonymous RFID authentication protocols. Technical Report TR-060112 Florida State University
8. Chien HY (2007) SASI: a new ultralightweight RFID authentication protocol providing strong authentication and strong integrity. IEEE Trans Dependable Secure Comput 4(4):337–340
9. Chiou S-Y, Chang S-Y (2018) An enhanced authentication scheme in mobile RFID system. Ad Hoc Netw 71:1–13
10. Cho JS, Jeong YS, Park SO (2015) Consideration on the brute-force attack cost and retrieval cost: a hash-based radio-frequency identification (RFID) tag mutual authentication protocol. Comput Math Appl 69(1):58–65
11. Cremers C, Mauw S, Samarin A (2012) Operational semantics and verification of security protocols. Information security and cryptography. Springer, Berlin

12. Doss R, Sundaresan S, Zhou W (2013) A practical quadratic residues based scheme for authentication and privacy in mobile RFID systems. Ad Hoc Netw 11(1):383–396
13. Doss R, Rasua RT, Piramuthu S (2020) Secure attribute-based search in RFID-based inventory control systems. Decis Support Syst 132:113–270
14. Fan K, Kang J, Zhu S, Li H, Yang Y (2019) Permutation matrix encryption based ultralightweight secure RFID scheme in internet of vehicles. Sensors 19(1):152–164
15. Gao L, Ma M, Shu Y, Wei Y (2014) An ultralightweight RFID authentication protocol with CRC and permutation. J Netw Comput Appl 41(0):37–46
16. Kardas S, Celik S, Sariyuce M, Levi A (2013) An efficient and private authentication protocol for RFID systems. J Commun Softw Syst 9(2):128–136
17. Kaul SD, Awasthi AK (2017) Privacy model for threshold RFID system based on PUF. Wirel Pers Commun 95(3):2803–2828
18. 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 14(8)
19. Khan G, Moessner M (2011) Secure authentication protocol for RFID systems. In: Proceedings of 20th international conference on computer communications and networks, pp 1–7
20. Li CT, Weng CY, Lee CC (2015) A secure RFID tag authentication protocol with privacy preserving in telecare medicine information system. J Med Syst 39(8):1–8
21. Luo H, Wen G, Su J (2018) SLAP: succinct and lightweight authentication protocol for low-cost RFID system. Wirel Netw 24:69–78
22. Maurya PK, Pal J, Bagchi S (2017) A coding theory based ultralightweight RFID authentication protocol with CRC. Wirel Pers Commun 97(1):967–976
23. Maurya PK, Bagchi S (2018) A secure PUF-based unilateral authentication scheme for RFID system. Wirel Pers Commun 103(2):1699–1712
24. Maurya PK, Bagchi S (2020) Cyclic group based mutual authentication protocol for RFID system. Wirel Netw 26:1005–1015
25. Melia-Segui J, Garcia-Alfaro J, Herrera-joancomart J (2011) Multiple- polynomial LFSR based pseudorandom number generator for EPC Gen2 RFID tags. In: 37th annual conference of industrial electronics society, pp 3820–3825
26. Mujahid U, Unabia G, Choi H, Tran B (2020) A review of ultralightweight mutual authentication protocols. Int J Electr Comput Eng 14(4):96–101
27. Mushtaq MF, Jamel S, Disina AH, Pindar ZA, Shakir NSA, Deris MM (2017) A survey on the cryptographic encryption algorithms. Int J Adv Comput Sci Appl 8(11)
28. Safkhani M (2018) Cryptanalysis of R_2AP, an ultralightweight authentication protocol for RFID. J Electr Comput Eng Innov 6(1):107–114
29. Safkhani M, Vasilakos A (2019) A new secure authentication protocol for telecare medicine information system and smart campus. IEEE Access 7:23514–23526
30. Sarker IH, Khan AI, Abushark YB, Alsolami F (2022) Internet of Things (IoT) security intelligence: a comprehensive overview, machine learning solutions and research directions. Mob Netw Appl
31. Singh D, Kumar B, Singh S, Chand S (2018) An efficient and secure authentication scheme using Markov chain for wireless sensor networks. In: IEEE 8th international advance computing conference, India
32. Singh D, Kumar B, Singh S (2019) SMAC-AS:MAC Based secure authentication scheme for wireless sensor network. Wirel Pers Commun 107:1289–1308
33. Singh D, Singh S, Kumar B, Chand S (2019) Anonymity preserving authentication and key agreement scheme for wireless sensor networks. In: Futuristic trends in network and communication technologies, communications in computer and information science, Singapore
34. Srivastava K, Awasthi AK, Kaul SD, Mittal RC (2014) A hash based mutual RFID tag authentication protocol in telecare medicine information system. J Med Syst 39(1):1–5
35. Tian Y, Chen G, Li J (2012) A new ultralightweight RFID authentication protocol with permutation. IEEE Commun Lett 16(5):702–705
36. Tsudik G (2006) Ya-trap: yet another trivial RFID authentication protocol. In: Proceedings of the 4th annual IEEE international conference on pervasive computing and communications workshops, IEEE Computer Society, pp 640–648
37. Vaudenay S (2007) On privacy models for RFID. In: Kurosawa K (ed) Advances in cryptology–ASIACRYPT 2007. Lecture Notes in Computer Science, vol 4833. Springer, Berlin, pp 68–87
38. Weis S, Sarma S, Rivest R, Engels D (2004) Security and privacy aspects of low-cost radio frequency identification systems. Security in Pervasive Computing 2802:201–212

39. Wu W, Wu S, Zhang L, Zou J, Dong L (2013) LH ash: a lightweight hash function. In: 9th international conference on information security and cryptology, Guangzhou, pp 291–308
40. Yeh TC, Wu CH, Tseng YM (2011) Improvement of the RFID authentication scheme based on quadratic residues. Comput Commun 34(3):337–341
41. Zheng L, Song C, Cao N, Li Z, Zhou W, Chen J, Meng L (2018) A new mutual authentication protocol in mobile RFID for smart campus. IEEE Access 6:60996–61005
42. Zhou J (2015) A quadratic Residue-Based lightweight RFID mutual authentication protocol with Constant-Time identification. J Commun 10(2):117–123
43. Zhou Z, Wang P, Li Z (2019) A quadratic residue-based RFID authentication protocol with enhanced security for TMIS. J Ambient Intell Humaniz Comput 10:3603–3615
44. Zhuang X, Zhu Y, Chang C (2014) A new ultralightweight RFID protocol for low-cost tags: R2AP. Wirel Pers Commun 79:1787–1802

Publisher's note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.