**Noname manuscript No.**
(will be inserted by the editor)

# Cyclic group based mutual authentication protocol for RFID system

**Pramod Kumar Maurya · Satya Bagchi**



Received: date / Accepted: date

**Abstract** Widespread deployment of RFID system arises security and privacy concerns of users. There are several proposals are in the literature to avoid these concerns, but most of them provides reasonable privacy at the cost of search complexity on the server side. The search complexity increases linearly with the number of tags in the system. Some schemes use a group based approach to solve the search complexity problem. In this paper, we proposed a group based authentication protocol for RFID system which is based on some characteristics of cyclic groups. The scheme uses only bitwise XOR and mod operation for the computational work. Also, the scheme does not use any pseudo-number generator on the tag-side. We use two benchmark metric based on anonymity set to measure the privacy level of the system when some tags are compromised by an adversary. We present some simulation results which show that the scheme preserves high level of privacy and discloses very less amount of information when some tags are compromised. Furthermore, it's formal and informal analysis shows that our scheme preserves information privacy as well as un-traceability and also withstand against various well known attacks.

**Keywords** RFID system · Cyclic group · Anonymity · Authentication protocol · Security · Privacy.

## 1 Introduction

RFID technology is becoming most promising technology in industries to improve the efficiency of tracking and managing goods. Because of its convenience and low-cost, we encounter this technology in various applications like supply chain management, logistics, access control, manufacturing, e-health, passport verification etc [8] [20] [5] [15].

RFID system is made up with three entities: tags, readers, and back-end server. Each tag comprises with a microchip for storing and processing data, and an antenna for receiving and transmitting data. The server stores all the information about the tags and connected with the readers via a secure channel while the readers communicate with the tags over an insecure channel [19] [7] [4] [9].

P. K. Maurya
Department of Mathematics
National Institute of Technology Durgapur
Burdwan, India.
E-mail: pramod_kumar22490@hotmail.com

S. Bagchi
Department of Mathematics
National Institute of Technology Durgapur
Burdwan, India.
E-mail: satya5050@gmail.com

With the widespread adoption of RFID system in our daily life, security and privacy concerns are also arise critically [2] [6] [18]. We can use cryptography tool to avoid these concerns but the main obstacle to deploy these tools in RFID system is tight constraints on power, memory and computational capability on the tags.

To enhance the security and privacy of the RFID system and reduce the computational complexity, researchers have been proposed a large number of authentication schemes. Here, we describe some tree-based and group-based authentication schemes related to RFID system. In 2004, Molnar and Wagner [12] proposed a tree-based approach for symmetric key authentication scheme. The scheme reduces its identification complexity from linear to logarithmic. However, it violates the privacy of the other tags when some tags are compromised by an adversary. In 2005, Nohara et al. [13] proposed a similar kind of authentication scheme. The scheme provides higher privacy than [12] in case of one tag is compromised. Buttyán et al. [3] proposed an optimal key trees for tree-based private authentication scheme in 2006. They used different branching factors at different levels of the tree to enhancing the privacy level of the scheme. Also, they introduce a benchmark metric for measuring privacy level of the system when some tags are compromised. In 2007, Avoine et al. [1] developed a group based symmetric key authentication scheme. They improve the trade-off between scalability and privacy by dividing the tags into a number of groups. Also, they analyze the privacy level of the system by using privacy metric when a single tag is compromised as well as any number of tags are compromised. The main draw back of the scheme is to decrease the privacy level when more tags are compromised. In 2017, Rahman et al. [16] developed a secure anonymous private authentication scheme which is similar to [1] except that the scheme used different technique to provide better privacy and ensure more security. They used privacy metric same as in [1] to measure the privacy level of the system. Also, the scheme used information leakage metric based on shannon information theory [17] to measure the information leakage in bits of the system when some tags are compromised.

After reviewing the work done, we would like to propose a similar kind of group based authentication scheme. The scheme uses some different kind of techniques to improve privacy and minimize computational cost.

Rest of the paper is organized as follows: In Section 2, we discuss preliminaries and details of our system model. We present adversary model in Section 3. Group based authentication scheme for RFID system is proposed in Section 4. The formal and informal analysis are given in Section 5. Section 6 illustrates the performance of the proposed scheme. In Section 7, we measure the level of privacy of the system when some tags are compromised by an adversary. We discuss simulation results in Section 8. Finally, conclusions are made in Section 9.

## 2 Preliminaries and System Model

In this section, we give brief overview of a cyclic group [10] and using it's properties, we develop our RFID system model. In this system model, we assume that a reader and the server communicate with each other via a secure communication channel. For simplicity, we assume that the reader and the server are combined into one entity, called reader.

Suppose $G$ be a nonempty set together with an operation $*$ that combines any two elements of $G$ is in $G$. The set $G$ together with this operation is a group if it holds group's law. The order of a group $G$ is the total number of elements in the group. It is denoted by $|G|$. Let $H$ be a subset of a group $G$. We say that $H$ is a subgroup of $G$ if it is itself a group under the operation of $G$.

**Definition 2.01** *A group $G$ is called cyclic if there exists an element $a \in G$ such that $G =< a >= \{a^n \mid n \in \mathbb{Z}\}$. The element $a$ is called a generator of $G$.*

Some important characteristics of cyclic groups are as follows:

1. Suppose $G =< a >$ be a cyclic group of order $n$. Then $G =< a^k >$ iff $gcd(k, n) = 1$.
2. Every subgroup of a cyclic group is cyclic.
3. Suppose $G =< a >$ be a cyclic group of order $n$. The order of any subgroup of $G$ is a divisor of $n$.
4. For each positive divisor $k$ of $n$, the group $G$ has exactly one subgroup of order $k$ denoted by $< a^{n/k} >$.

| Subgroup | Index | Tag | Storage data |
|---|---|---|---|
| $H_1 =< a_1 >$ | $i_1$ | $T_{1i_1}$ | $[ID_{1i_1}, K_{1i_1}, r_{1i_{1_{old}}}, r_{1i_{1_{new}}}]$ |
| | $i_2$ | $T_{1i_2}$ | $[ID_{1i_2}, K_{1i_2}, r_{1i_{2_{old}}}, r_{1i_{2_{new}}}]$ |
| | $\vdots$ | $\vdots$ | $\vdots$ |
| | $i_{\|H_1\|-1}$ | $T_{1i_{\|H_1\|-1}}$ | $[ID_{1i_{\|H_1\|-1}}, K_{1i_{\|H_1\|-1}}, r_{1i_{(\|H_1\|-1)_{old}}}, r_{1i_{(\|H_1\|-1)_{new}}}]$ |
| $\vdots$ | $\vdots$ | $\vdots$ | $\vdots$ |
| $H_m =< a_m >$ | $i_1$ | $T_{mi_1}$ | $[ID_{mi_1}, K_{mi_1}, r_{mi_{1_{old}}}, r_{mi_{1_{new}}}]$ |
| | $i_2$ | $T_{mi_2}$ | $[ID_{mi_2}, K_{mi_2}, r_{mi_{2_{old}}}, r_{mi_{2_{new}}}]$ |
| | $\vdots$ | $\vdots$ | $\vdots$ |
| | $i_{\|H_m\|-1}$ | $T_{mi_{\|H_m\|-1}}$ | $[ID_{mi_{\|H_m\|-1}}, K_{mi_{\|H_m\|-1}}, r_{mi_{(\|H_m\|-1)_{old}}}, r_{mi_{(\|H_m\|-1)_{new}}}]$ |
| $\vdots$ | $\vdots$ | $\vdots$ | $\vdots$ |

**Table 1** The server look-up table

We construct a system model for RFID system with the help of above mentioned characteristics of cyclic groups. For this, we choose a cyclic group $G =< a >$ of order $n$ and find its some subgroups $H_i =< a_i >$, $i = 1, 2, \ldots$, where $a_i = a^{n/k}$ for some positive divisor $k$, according to our requirement using characteristics 4. According to characteristics 4, if $a_i$ and $a_j$ are generators of two different subgroups $H_i$ and $H_j$ respectively, then $a_i$ and $a_j$ are distinct elements in $G$. For the system model, with each element of $H_i$ except the identity element, we assign a tag together with some secret parameters. Additionally, if $H_p$ is the highest order subgroup (say, $|H_p| = P$) and $H_{p-1}$ is the second highest order subgroup (say, $|H_{p-1}| = Q$) in the system. Then we utilize only $Q$ number of elements of $H_p$ to assign tags in such a way so that the value of $i$ (which is used as an index in server look-up table) is same in both the subgroups.

We made a look-up table for the server which is shown in Table 1. From the Table 1, we can see that with each element $a_j^i$ in $H_j =< a_j >$, a tag $T_{ji}$ is assigned and $i$ is used as a index in the look-up table for the tag $T_{ji}$. The server stores a unique identification number $ID_{ji}$ and a secret key $K_{ji}$ to the tag $T_{ji}$. It also shows that two nonce $r_{ji_{old}}$ and $r_{ji_{new}}$ are associated with the tag $T_{ji}$. Initially, we take $r_{ji_{old}} = 0$ and $r_{ji_{new}}$ be a nonce.

For each tag $T_{ji}$ which is associated with an element $a_j^i$ in $H_j$, we store inverse of $a_j^i$ in $H_j$, i.e. $(a_j^i)^{-1}$, and $i$ in the tag's internal memory. We also store a unique identification number $ID_{ji}$, a secret key $K_{ji}$, and a nonce $R_4$ inside the tag's memory. Initially, $R_4$ is same as $r_{ji_{new}}$ which is stored in the server's look-up table for tag $T_{ji}$.

## 3 Adversary Model

In this section, we present the ability of an adversary $\mathscr{A}$. The adversary is capable to interact with the RFID system $S$ and also, eavesdrops, intercepts, and modifies any transmitted message between any reader and any tag in the system. Our adversarial model is similar to the model proposed by

Juels and Weis [11] with some modifications to meet our requirement. $\mathscr{A}$ is also able to send the following queries to an oracle.

1. SendTag$(m, T_{ji}) \rightarrow m'$
   The adversary $\mathscr{A}$ may send a message $m$ to the tag $T_{ji}$ which responds with message $m'$.
2. SendReader$(m, R) \rightarrow m'$
   $\mathscr{A}$ can intract with a reader $R$ by sending a message $m$. The reader $R$ responds with message $m'$.
3. DrawTags$(S)$
   The adversary has access to a set of tags at any time from the system with this oracle query.
4. Corrupt$(T_{ji})$
   $\mathscr{A}$ is able to access the volatile memory as well as non volatile memory of a tag $T_{ji}$.

We also bound the adversary $\mathscr{A}$ to use SendTag and SendReader queries by $r$ and $t$ respectively. $\mathscr{A}$ can performs $s$ number of computational steps. At a time, $\mathscr{A}$ is able to send Corrupt message to atmost $(n-2)$ number of tags where $n$ is the total number of tags obtained from DrawTags query.

### 3.1 Privacy Experiment

We denote privacy experiment for an RFID system $S$ by $EXP^{priv}_{\mathscr{A},S}[k, n, r, s, t]$, where $r$, $s$, and $t$ represent the capability of an adversary to use SendTag, computations steps and SendReader respectively. Also, $k$ represents a security parameter. An RFID authentication protocol is considered to be private if no adversary has significant advantage in this experiment.

The main goal of the adversary in the experiment is to distinguish between two different tags with in its computational and interaction limits. The experiment is composed in three phases as follows:

1. Learning Phase: The adversary $\mathscr{A}$ interacts with the system $S$ and inqueries oracle queries without exceeding its bound and analyze them.
2. Challenging Phase: $\mathscr{A}$ selects two uncorrupted tags from the pool obtained by Drawtags oracle. $\mathscr{A}$ randomly selects any one from them. The adversary evaluates oracles on that particular tag.
3. Guessing Phase: $\mathscr{A}$ outputs a guess bit $b$. $\mathscr{A}$ is expected to produce 1 if he succeeds, otherwise 0.

$EXP$ succeed if $b = 1$.

### 3.2 Privacy Definition [$(r, s, t)$-privacy]

According to Juels and Weis [11], an RFID authentication protocol with security parameter $k$ is $(r, s, t)$-private if

$$Pr[EXP^{priv}_{\mathscr{A},S}[k, n, r, s, t] \textit{ succeeds in guessing } b] \leq \frac{1}{2} + \frac{1}{poly(k)},$$

where $poly(k)$ is any polynomial function of $k$.

## 4 Process

In this section, we propose a group based authentication protocol which works under all circumstances required for RFID systems. Used notations in this protocol are given in Table 2, and proposed protocol is shown in Figure 1. The work flow of the proposed scheme is as follows:

| Notation | Description |
|---|---|
| $G =< a >$ | A finite cyclic group. |
| $H_j =< a_j >$ | A subgroup of the group $G$ with generator element $a_j$. |
| $(a_j^k)^{-1}$ | Inverse element of $a_j^k$ in the subgroup $H_j$. |
| $R_m : m = 1, 2, 3$ | Nonce generated by the reader. |
| $K_{ji}$ | Secret key of a tag $T_{ji}$ associated with the $i^{th}$ element of a subgroup $H_j$. |
| $ID_{ji}$ | Unique identification number of the tag $T_{ji}$. |
| $\oplus$ | Exclusive-or operation. |

**Table 2** Notations and symbols used in proposed scheme

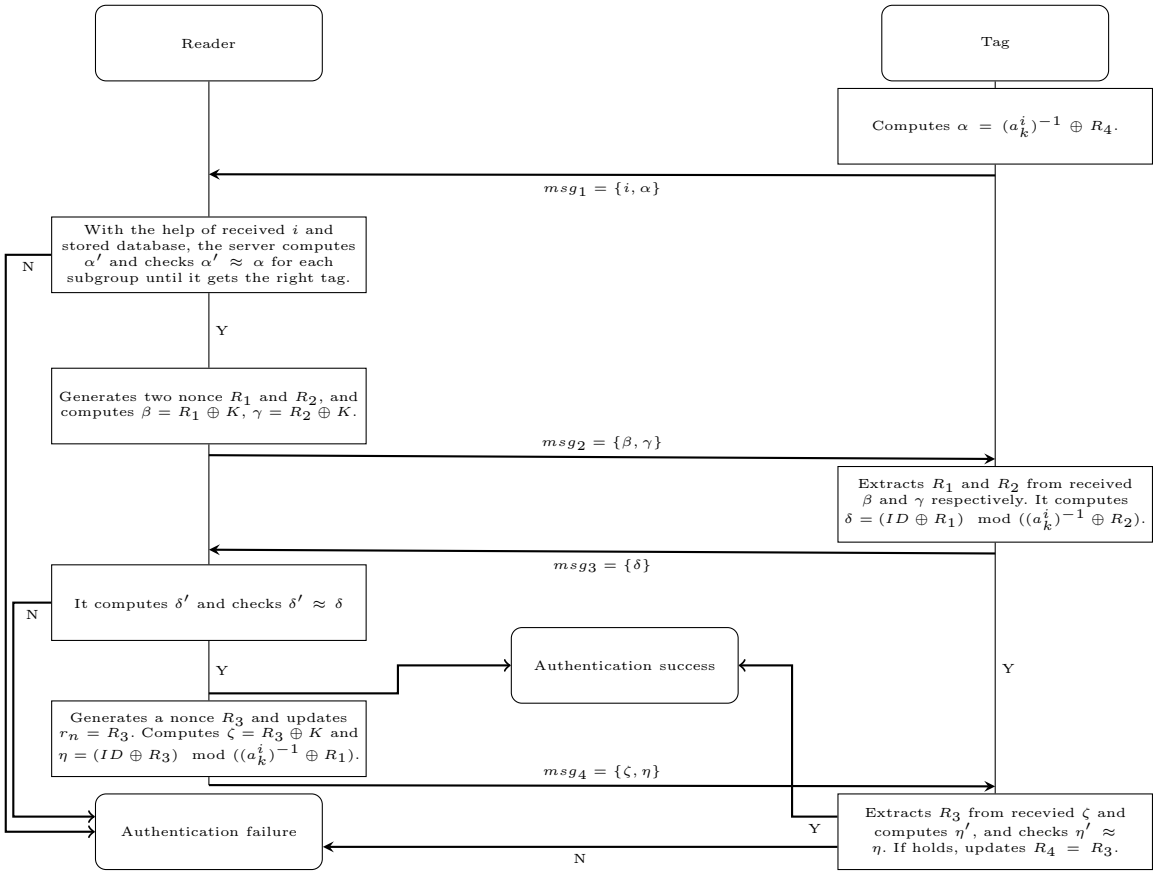


**Fig. 1** Proposed Mutual Authentication Protocol

1. $msg_1 : T_{ki} \rightarrow R : \{i, \alpha\}$
   The tag $T_{ki}$ computes $\alpha = (a_k^i)^{-1} \oplus R_4$ and forms a request message $msg_1 = \{i, \alpha\}$. The tag sends $msg_1$ to a reader $R$.
2. $msg_2 : R \rightarrow T_{ki} : \{\beta, \gamma\}$
   After receiving the tag's request message $msg_1$, the reader uses $i$ as an index (as in Table 1) to performs the following steps for all the subgroups until it finds the right tag:
   (a) It calculates the inverse of $a_k^i$ in $H_k$, where $a_k$ is the generator of subgroup $H_k$.
   (b) The reader computes $\alpha' = (a_k^i)^{-1} \oplus r_{ki_{old}}/r_{ki_{new}}$ and checks whether $\alpha'$ is equal to the received $\alpha$ or not. If so, it gets the right tag $T_{ki}$ (say) inside the subgroup $H_k$. If fails, the reader terminates the protocol.
   (c) The reader generates two nonce $R_1$ and $R_2$, and computes $\beta = R_1 \oplus K_{ki}$, $\gamma = R_2 \oplus K_{ki}$, where $K_{ki}$ is the secret key of the tag $T_{ki}$. The reader forms a response message $msg_2 = \{\beta, \gamma\}$ and transmits it to the tag.

3. $msg_3 : T_{ki} \rightarrow R : \{\delta\}$
   Upon receiving the response message $msg_2$, the tag $T_{ki}$ extracts $R_1$ and $R_2$ from $\beta$ and $\gamma$ respectively with the help of its secret key $K_{ki}$. It computes $\delta = (ID_{ki} \oplus R_1) \mod ((a_k^i)^{-1} \oplus R_2)$ and send $\delta$ inside the response message $msg_3 = \{\delta\}$ to the reader.
4. $msg_4 : R \rightarrow T_{ki} : \{\zeta, \eta\}$
   After receiving message $msg_3$ from the tag $T_{ki}$, the reader calculates $\delta' = (ID_{ki} \oplus R_1) \mod ((a_k^i)^{-1} \oplus R_2)$ for the tag $T_{ki}$ and checks whether $\delta'$ is equal to the received $\delta$ or not. If it holds, the reader authenticates the tag $T_{ki}$ otherwise terminates the session. If tag's authentication succeed, the reader generates a nonce $R_3$ and assigns $r_{ki_{old}} = r_{ki_{new}}$, and $r_{ki_{new}} = R_3$. Simultaneously, also computes $\zeta = R_3 \oplus K_{ki}$, $\eta = (ID_{ki} \oplus R_3) \mod ((a_k^i)^{-1} \oplus R_1)$ and forms a response message $msg_4 = \{\zeta, \eta\}$. It sends $msg_4$ to the tag $T_{ki}$.
5. Upon receiving message $msg_4$, the tag $T_{ki}$ extracts $R_3$ from $\zeta$ and calculates $\eta' = (ID_{ki} \oplus R_3) \mod ((a_k^i)^{-1} \oplus R_1)$. The tag checks whether $\eta'$ is equal to the received $\eta$ or not. If so, the tag authenticates the reader and updates $R_4 = R_3$ for further communication.

## 5 Security and Privacy Analysis

In this section, we present formal and informal analysis of our proposed scheme with respect to above mentioned adversary model. The formal analysis shows that the proposed scheme preserves privacy and un-traceability. Also, it's informal analysis shows that the proposed scheme is secure against various well-known attacks.

### 5.1 Formal Security Analysis

**Theorem 1** *The proposed scheme attains information privacy with respect to a adversary $\mathscr{A}$.*

*Proof* We assume that the proposed scheme does not preserve information privacy. So the success probability of the adversary to win experiment is non-negligible. $\mathscr{A}$'s privacy game is composed in three phases as follows:

- Learning Phase: The adversary gets a set of $n$-tags by querying DrawTags oracle. $\mathscr{A}$ can send any oracle queries to a tag $T_i$ (say) without exceeding its computation bound and analyze them. $\mathscr{A}$ can use Corrupt oracle to atmost $n-2$ tags.

$$T_i \leftarrow \text{DrawTag}(S)$$
$$msg_1 = \{i, \alpha\} \leftarrow \text{SendTag}(init, T_i)$$
$$msg_2 = \{\beta, \gamma\} \leftarrow \text{SendReader}(msg_1, R)$$
$$msg_3 = \{i, \delta\} \leftarrow \text{SendTag}(msg_2, T_i)$$
$$msg_4 = \{\zeta, \eta\} \leftarrow \text{SendReader}(msg_3, R)$$
$$\{i, (a_j^i)^{-1}, K, ID, R\} \leftarrow \text{Corrupt}(T_i).$$

- Challenge Phase: The adversary $\mathscr{A}$ selects two uncorrupted tags say, $T_i$ and $T_j$, from the set of tags obtained by DrawTags query as its challenge tags. Let $T_0^* = T_i$, $T_1^* = T_j$, and $b \in \{0, 1\}$. $\mathscr{A}$ randomly selects $T_b$ among them and analyze all queries run on it. Note that $\mathscr{A}$ is not able to use Corrupt oracle on that particular tag $T_b$.

$$msg_1 = \{i, \alpha\} \leftarrow \text{SendTag}(init, T_b)$$
$$msg_2 = \{\beta, \gamma\} \leftarrow \text{SendReader}(msg_1, R)$$
$$msg_3 = \{i, \delta\} \leftarrow \text{SendTag}(msg_2, T_b)$$
$$msg_4 = \{\zeta, \eta\} \leftarrow \text{SendReader}(msg_3, R).$$

- Guess Phase: Eventually, the adversary outputs a guess bit $b'$ for the corresponding tag.

The adversary wins the experiment if $b' = b$. It is possible only when the adversary knows all the secrets stored in $T_b$'s internal memory as well as the mother group $G$. So our assumption is wrong. Hence the proposed scheme preserves the information privacy with respect to $\mathscr{A}$.

**Theorem 2** *The proposed scheme provides un-traceability with respect to the adversary* $\mathscr{A}$.

*Proof* Let us assume that the proposed scheme is traceable. i.e. the adversary can trace a tag at any time. This means $\mathscr{A}$ is able to distinguish between two tags. We show that our assumption is wrong with the help of $\mathscr{A}$'s privacy game which is as follows:

- Learning Phase: $\mathscr{A}$ uses DrawTags query for the system $S$ and gets access to $n$-tags. For all the tags, $\mathscr{A}$ sends SendTag and SendReader queries to get transmitted information among a reader and tags. The adversary analyzes all the transmitted message. The adversary can use Corrupt query for atmost $n-2$ tags because the goal of the privacy game is to distinguish between two uncorrupted tags.

$$\begin{gathered} T_i \leftarrow \text{DrawTag}(S) \\ msg_1 = \{i, \alpha\} \leftarrow \text{SendTag}(init, T_i) \\ msg_2 = \{\beta, \gamma\} \leftarrow \text{SendReader}(msg_1, R) \\ msg_3 = \{i, \delta\} \leftarrow \text{SendTag}(msg_2, T_i) \\ msg_4 = \{\zeta, \eta\} \leftarrow \text{SendReader}(msg_3, R) \\ \{i, (a_j^i)^{-1}, K, ID, R\} \leftarrow \text{Corrupt}(T_i). \end{gathered}$$

- Challenge Phase: The adversary selects two uncorrupted tags $T_i$ and $T_j$ to which it did not send Corrupt query in the learning phase. $\mathscr{A}$ randomly selects $T_b : b \in \{i, j\}$ among them. The adversary queries all the oracle queries except Corrupt query to the tag $T_b$ and evaluates them.

$$\begin{gathered} msg_1^* = \{i, \alpha\} \leftarrow \text{SendTag}(init, T_b) \\ msg_2^* = \{\beta, \gamma\} \leftarrow \text{SendReader}(msg_1^*, R) \\ msg_3^* = \{i, \delta\} \leftarrow \text{SendTag}(msg_2^*, T_b) \\ msg_4^* = \{\zeta, \eta\} \leftarrow \text{SendReader}(msg_3^*, R). \end{gathered}$$

- Guess Phase: $\mathscr{A}$ outputs a guess bit $b'$.

The adversary wins the game if $b' = b$ but it is possible only when if

$$Pr[msg_1^* = msg_1] = 1$$

Since the message $msg_1$ depend upon the tag's nonce $R_4$ which is different in each protocol run. So our assumption is wrong. Hence the adversary is unable to trace the tag.

## 5.2 Informal Security Analysis

### *5.2.1 Replay Attack Resistance*

An adversary can eavesdrops the wireless channel and keeps all the transmitted messages between a reader and a tag. The adversary uses these message into another session to disguise itself as the tag or the reader to deceive the other one. In the proposed scheme, it is infeasible for an adversary to forge messages as a valid tag/reader because each transmitted message incorporates a fresh nonce in each authentication session which can not be get by the adversary (since the nonce XOR with some other secret parameters). This makes all the replayed message by the adversary are illegal message. Thus the scheme prevents strongly the replay attack.

*5.2.2 De-synchronization Attack Resistance*

For each tag, the server stores two nonce $r_{old}$ and $r_{new}$ in its database to save the scheme from the de-synchronization attack. The server also updates these values after a successful authentication session. An adversary intercepts or modified any transmitted message in one session in such a way so that a tag does not update the value of stored nonce. The server can authenticate the legitimate tag by its old value stored in database into another session. So it is not possible for an adversary to de-synchronize the scheme.

*5.2.3 Man-in-Middle Attack Resistance*

An adversary is unable to act as a middle man in between a reader and a tag because it is infeasible for the adversary to intercepts any transmitted message without knowing the secret key, unique identification number, and knowledge about the cyclic group. The probability of guessing or calculating these values from the transmitted message is negligible because a fresh nonce is used in each transmitted message.

## 6 Performance Analysis

In this section, we present efficiency of our proposed scheme in terms of tag computation, server computation, and storage, as described in Table 3. The proposed scheme's search complexity is $O(\gamma)$ which is same as in Avione et al. [1] but better than Rahman et al. [16]. During the authentication phase, the scheme performs only bit-wise XOR operation whereas schemes of Avoine et al. and Rahman et al. perform symmetric key encryption and decryption. Also, the proposed scheme does not use any pseudo number generator function for generating nonce on the tag-side. It uses nonce generated by the reader. We assume that all the parameters used in the proposed scheme are $L$-bits long. On the tag side, our scheme keeps five items. Thus the storage cost is $5L$ bits. The proposed scheme also provides mutual authentication among a reader and tags. When we compare with [1] and [16] in terms of computation, the proposed scheme performs very less computation which is optimal for the real world tiny powered tags.

| Protocol | Entity | Avoine [1] | Rahman [16] | Proposed protocol |
|---|---|---|---|---|
| Symmetric encryption/ decryption | T | 2 | 2 | × |
| | R | 2 | 2 | × |
| Search complexity | R | $O(\gamma)$ | $O(\gamma + \|\pi\|)$ | $O(\gamma)$ |
| No. of PRNG | T | 1 | 1 | × |
| Required memory | T | $3L$ | $(m+2)L$ | $5L$ |
| Mutual authentication | | × | × | ✓ |

$\gamma$- Total number of groups in the system.
$|\pi|$ - Total number of secret keys of a tag associated with the identifier $ID_x$.
$m$ - Number of identifier is assigned to each tag.

**Table 3** Computation cost performance comparison

## 7 Measurement of Privacy

In this section, we analyze the privacy level of our proposed scheme in terms of anonymity set and data leakage in bits. For the anonymity sets, we use privacy metric introdued by [3]. Also, we use

another metric says information leakage for data leakage proposed by shannon [17] and used in [14] [16] to measure the information (in bits) disclosed by the proposed scheme when some tags are compromised.

Both the metric use disjoint partition sets of tags for observation. When some tags are compromised, the set of all tags are partitioned in such a way so that the adversary can not distinguish the tags that belong to the same partition but she can distinguish the tags belong to different partitions. Here, $|P_i|$ denotes the size of such partition $P_i$ and $\frac{|P_i|}{N}$ is the probability that a randomly chosen tag belongs to partition $P_i$.

### 7.1 Level of privacy based on anonymity set

The level of privacy $\Re$ based on anonymity set is characterized as average anonymity set size normalized with the total number of tags $N$ [3] [1] [16].

$$\Re = \frac{1}{N}\sum_i |P_i|\frac{|P_i|}{N} = \frac{1}{N^2}\sum_i |P_i|^2. \tag{1}$$

In the proposed scheme, if a tag is compromised, it does not leak any information about the subgroup in which it belongs. For this reason, the adversary can not distinguish between two tags whether they belongs to same subgroup or not. So, if $\mathbb{C}$ is the total number of compromised tags in the whole system, we partitioned the system into $\mathbb{C}$ number of anonymity sets with size 1 and one another anonymity set of size $(N - \mathbb{C})$. Using equation 1, the level of privacy $\Re$ achieved by our scheme is

$$\Re = \frac{1}{N^2}\{\mathbb{C} + (N - \mathbb{C})^2\}, \tag{2}$$

where $N$ is the total number of tags in the system and $\mathbb{C}$ is the total number of compromised tags in the system.

### 7.2 Level of privacy based on information leakage in bits

According to Rahman et al. [16], if an adversary partitioned a system with $N$ tags into $k$ disjoint sets, then the information leakage in bits can be expressed as follows:

$$\mathbb{I} = \sum_{i=1}^{k} \frac{|P_i|}{N} \log_2 \left(\frac{N}{|P_i|}\right). \tag{3}$$

In the proposed scheme, if $\mathbb{C}$ is the total number of compromised tags in the system. Then we partitioned the system with $N$ tags into $\mathbb{C}$ anonymity sets of size 1 and one another anonymity set of size $(N - \mathbb{C})$. According to our partitions, the information leakage in bits is as follows

$$\mathbb{I} = \frac{\mathbb{C}}{N} \log_2 N + \frac{(N - \mathbb{C})}{N} \log_2 \left(\frac{N}{N - \mathbb{C}}\right). \tag{4}$$

## 8 Experimental Results

In this section, we compare our scheme with Avoine et al. [1] and Rahman et al. [16] using a matlab simulation. The simulation is done using the expressions (1) - (4). In the simulation, we assume that the system has $N = 2^{10}$ number of tags and all the tags are divided into 32 groups. We choose range of compromised tags from 0 to 600. In the proposed scheme, it is not necessary to take same number

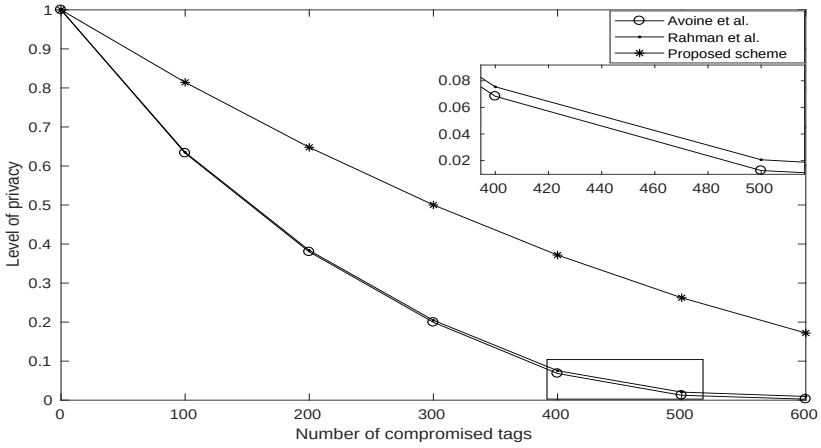


**Fig. 2** Level of privacy of the system based on anonymity set

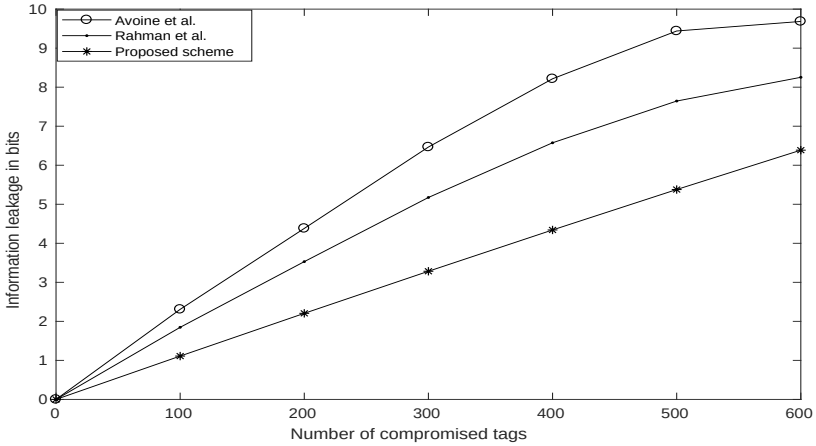


**Fig. 3** Level of privacy of the system based on information leakage in bits

of tags in each groups. In the simulation, we run 100 simulations for each value of compromised tags $\mathbb{C}$ in the system. In each simulation run, compromised tags are chosen uniformly random from the groups of all tags. Finally, we average all the obtained values over all simulation runs. The simulation results are shown in Figure 2 and Figure 3. The simulation results of the Figure 2 shows that the privacy level achieved by the proposed scheme is 94.42% and 98.43% better than Rahman et al. and Avoine et al. respectively, when $\mathbb{C}$ becomes 600 in a similar setup. According to simulation result shown in Figure 3, the proposed scheme discloses 22.62% and 34.05% less information than Rahman et al. and Avoine et al. respectively when $\mathbb{C}$ becomes 600. Thus the proposed scheme achieves higher improvement in terms of privacy level and information leakage than the other schemes, when some tags are compromised by an adversary.

## 9 Conclusion

In this paper, we have proposed a group based authentication scheme for RFID system based on a cyclic group. The detailed formal analysis shows that it preserves information privacy and un-traceability. The informal analysis shows that the scheme resists various existing attacks. The

performance analysis illustrates that the scheme uses very less resources on tags to performs computational work and storage data. The experimental results show that our scheme preserves high level privacy when some tags are compromised. Thus, the analysis and prominent features conclude that the scheme is secure and efficient for a low-cost RFID system.

**Conflict of Interest:** The author P K Maurya thanks to MHRD, India, for financial support of his research.

## References

1. Avoine, G., Buttyant, L., Holczer, T., Vajda, I.: Group-based private authentication. In: IEEE International Symposium on a World of Wireless, Mobile and Multimedia Networks, pp. 1–6 (2007)
2. Avoine, G., Coisel, I., Martin, T.: Untraceability model for RFID. IEEE Transactions on Mobile Computing, 13(10), pp. 2397–2405 (2014)
3. Buttyán, L., Holczer, T., Vajda, I.: Optimal Key-Trees for Tree-Based Private Authentication. Springer Berlin Heidelberg (2006)
4. Cao, T., Chen, X., Doss, R., Zhai, J., Wise, L.J., Zhao, Q.: RFID ownership transfer protocol based on cloud. Computer Networks, 105, pp. 47 – 59 (2016).
5. Chien, H.Y.: Secure access control schemes for RFID systems with anonymity. In: 7th International Conference on Mobile Data Management (MDM'06), pp. 1–4 (2006).
6. Chien, H.Y.: SASI: A new ultralightweight RFID authentication protocol providing strong authentication and strong integrity. IEEE Transactions on Dependable and Secure Computing, 4(4), pp. 337–340 (2007).
7. Cho, J.S., Jeong, Y.S., Park, S.O.: Consideration on the brute-force attack cost and retrieval cost: A hash-based radio-frequency identification (RFID) tag mutual authentication protocol. Computers & Mathematics with Applications, 69(1), pp. 58 – 65 (2015)
8. Dimitriou, T.: Key evolving RFID systems: Forward/backward privacy and ownership transfer of RFID tags. Ad Hoc Networks, 37(Part 2), pp. 195 – 208 (2016).
9. Gao, L., Ma, M., Shu, Y., Wei, Y.: An ultralightweight RFID authentication protocol with CRC and permutation. Journal of Network and Computer Applications, 41(0), pp. 37 – 46 (2014)
10. Gallian, J.A.: Contemporary abstract algebra. Cengage Learning (2016).
11. Juels, A., Weis, S.A.: Defining strong privacy for RFID. ACM Trans. Inf. Syst. Secur., 13(1), pp. 7:1–7:23 (2009).
12. Molnar, D., Wagner, D.: Privacy and security in library RFID: Issues, practices, and architectures. In: Proceedings of the 11th ACM Conference on Computer and Communications Security, CCS '04, pp. 210–219. ACM (2004).
13. Nohara, Y., Inoue, S., Baba, K., Yasuura, H.: Quantitative evaluation of unlinkable id matching schemes. In: Proceedings of the 2005 ACM Workshop on Privacy in the Electronic Society, WPES '05, pp. 55–60. ACM (2005).
14. Nohl, K., Evans, D.: Quantifying Information Leakage in Tree-Based Hash Protocols Information and Communications Security: 8th International Conference, ICICS, pp. 228–237 (2006).
15. Maurya, P.K., Pal, J., Bagchi, S.: A coding theory based ultralightweight RFID authentication protocol with CRC. Wireless Personal Communications, 97(1), pp. 967–976 (2017).
16. Rahman, F., Hoque, M.E., Ahamed, S.I.: Anonpri: A secure anonymous private authentication protocol for RFID systems. Information Sciences, 379, pp. 195 – 210 (2017).
17. Shannon, C.E.: A mathematical theory of communication. SIGMOBILE Mob. Comput. Commun. Rev., 5(1), pp. 3–55 (2001).
18. Srivastava, K., Awasthi, A.K., Kaul, S.D., Mittal, R.C.: A hash based mutual RFID tag authentication protocol in telecare medicine information system. Journal of Medical Systems, 39(1), pp. 1–5 (2014).
19. Tian, Y., Chen, G., Li, J.: A new ultralightweight RFID authentication protocol with permutation. IEEE Communications Letters, 16(5), pp. 702–705 (2012)
20. Wang, J., Floerkemeier, C., Sarma, S.E.: Session-based security enhancement of RFID systems for emerging open-loop applications. Personal and Ubiquitous Computing, 18(8), pp. 1881–1891 (2014).