Wireless Pers Commun (2018) 103:1699–1712
https://doi.org/10.1007/s11277-018-5875-2

A Secure PUF-Based Unilateral Authentication Scheme for RFID System

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

Published online: 21 May 2018

Abstract Privacy and security concerns are significant barrier for RFID deployment in many applications in modern day world. The implementation of authentication schemes which provide reasonable security under the resource constraints of tiny-powered RFID tags are an efficient way to avoid these concerns. In this paper, we present physical unclonable function based unilateral authentication protocol for RFID system. In addition, we use error-correcting code properties to enhance security of the proposed scheme. Use of error-correcting code also reduces computational cost of the proposed scheme drastically. Security and privacy analysis indicates that the proposed scheme resists various attacks. Cost analysis shows that the scheme outshines the existing protocols in terms of storage requirement, computational operations, and communication cost.

Keywords RFID system · Error-correcting code · PUF · Hash function · Authentication protocol · Security · Privacy

1 Introduction

RFID technology is a fast growing ubiquitous tool in automatic identification applications due to their relatively low-cost and ease to deployment. RFID does not use line-of-sight contact for identification. It is rewritable and also reusable. For this reason, peoples think about this technology is a successor of bar-code. Due to unique feature of RFID system, it is used in many consumer applications such as business specification applications and medical industries etc. In a typical RFID system, there are three components: RFID tags, RFID reader, and Back-end server. RFID tag is a small microchip with an antenna. Tag

✉ Satya Bagchi
satya.bagchi@maths.nitdgp.ac.in; satya5050@gmail.com

Pramod Kumar Maurya
pramod_kumar22490@hotmail.com

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

stores information about an object where it is attached. Generally, RFID tags have no own power source. They receive their power from the electromagnetic field generated by a nearby reader. When tags are powered by a nearby reader, they engage in authentication and transmit data over wireless channel. The back-end server stores secret parameters and other information associated with objects in which a tag is attached.

Internationally, there are three standardization bodies for RFID system: International Organization for Standardization (ISO), EPCglobal, and Telecommunication Standardization Sector of the International Telecommunications Union (ITU-T). According to the standards, RFID system works with different radio frequency ranges. According to frequency ranges, we can classify RFID system into three types: LF RFID system (124–135 KHz), HF RFID system (13.56–433 MHz) and UHF RFID system (900–2.45 GHz).

The communication channel between RFID tags and a reader is wireless. So all the threats associated with wireless channel are also exist in RFID system. It can lead serious breach of security and privacy of users. Here we describe some major types of attacks against RFID system [5, 6].

- *Replay attack* In this attack, an adversary keeps transmitted messages between a reader and a tag in one session. In the later sessions, the adversary uses these information to authenticate herself as a legitimate tag.
- *De-Synchronization Attack* An adversary changes the secret key stored in tag's memory and server database (DB) by intercepting transmitted messages. So that the tag's key stored in its internal memory would not be same as the tag's key stored in DB.
- *Disclosure Attack* In this attack, an adversary tries to get the secret information from the transmitted message between a legitimate reader and legitimate tags.
- *Location Tracking* An adversary tracks the location of an object in which a tag is attached without any knowledge of object's owner.
- *Denial-of-Service (DoS)* Attack An adversary makes tags unavailable for legitimate readers.
- *Impersonation Attack* In this attack, an adversary masquerades herself as a trusted reader/tag.

In the literature, researchers have proposed many authentication protocols for safeguarding RFID system from the above mentioned threats. According to cryptosystem used in RFID authentication schemes, we can divide them into two types: public key cryptosystem (PKC) based authentication schemes and non-public key cryptosystem (NPKC) based schemes. PKC based RFID authentication schemes mostly based on elliptic curve cryptosystem. These kind of schemes provide high security but use more resources for operation computations. For this reason, these schemes are not suitable for tiny-powered tags. On the other hand, NPKC based RFID authentication schemes mainly based on one-way hash function, cyclic redundancy check (CRC), physical unclonable function (PUF), and permutations etc. These type of schemes perform well under the resource constraints of tiny-powered tags. In recent years, researchers have proposed several NPKC based authentication schemes for RFID system that utilize characteristics of PUF to achieve low computational cost and high level of security. Here, we discuss some of PUF-based authentication schemes which are related to our works.

In 2004, Ranasinghe et al. [14] introduced a PUF-based authentication scheme for RFID system. In the scheme, the issuer stores a set of challenge-response pairs in the database (DB). A reader which is connected to the DB uses these pairs to authenticate a tag. The main drawback of this scheme is that the used challenge-response pairs are not reusable for further authentication sessions.

Tuyls and Batina [17] proposed an authentication approach for RFID system in 2006. The scheme uses PUF to reconstruct the secret key whenever it is needed instead of storing it in the tag's internal memory. The scheme withstands physical cloning attacks as well as cloning attack against active/passive adversaries.

In 2009, Kulseng et al. [10] proposed an authentication scheme which uses PUF and linear feedback shift register (LFSR) for authentication and key updation. The scheme consists of two phases: offline setup phase and online search phase. In the setup phase, the issuer assigns some secret informations to all the tags and readers. In the search phase, tags exchange their secrets with a reader for authentication.

In 2010, Sadeghi et al. [15] introduced a destructive-privacy preserving authentication scheme based on PUF. The scheme uses PUF as temper-evident key storage to reconstruct the tag authentication key whenever it is needed. The scheme provides untraceability of tags against adversaries that permanently destroy a tag by physically attacking on it.

Bassil et al. [4] introduced an ultralight-weight authentication scheme for RFID system in 2011. The scheme uses light operations such as bitwise AND, OR, XOR, left and right circular shift in addition to PUF for computation during authentication execution. Unfortunately, the scheme vulnerable under secret discloser attack, traceability attack, reader impersonation attack and de-synchronization attack [16].

In 2012, a PUF-based authentication scheme for offline RFID system has been introduced by Kardas et al. [8]. The scheme utilizes PUF and hash function to achieve destructive-privacy even in case of compromised reader attacks.

Jung and Jung [6] proposed a hash message authentication code (HMAC) based scheme in 2013. The scheme uses a response which is generated by PUF as a secret key of HMAC rather than sending the response against a corresponding challenge.

In 2015, Akgün and Çağlayan [3] introduced an authentication scheme which utilized PUF to achieve higher level privacy with constant identification time. The scheme uses PUF as a secure storage to keep secrets of a tag. The scheme uses only one master key shared between all the tags and readers. With the master key and utilization of PUF, the scheme also solve the scalability issue in RFID system.

In 2017, Kaul and Awasthi [9] proposed an efficient threshold RFID authentication scheme based on PUF. The scheme uses threshold secret sharing method to resist tag compromising attack and also enhance shared control of the secrets among multiple tags.

The contents of this paper are organized as follows. We give a brief description of error-correcting codes and physical unclonable function in Sect. 2. We describe RFID system model in Sect. 3. In Sect. 4, we elaborate ability of an adversary in adversary model. We present classes of adversaries in Sect. 5. Unilateral authentication scheme is proposed in Sect. 6. We analyse security and privacy parameters of the proposed protocol in Sect. 7. In Sect. 8, we give cost analysis of the proposed scheme. Finally, we present conclusion in Sect. 9.

2 Preliminaries

In this section, we describe error-correcting codes of coding theory and physical unclonable function which are used in our proposed scheme.

2.1 Error-Correcting Code

Error-correcting codes are methods for correcting errors from a message when it is transmitted over a noisy channel [12]. Generally, it is denoted by $C = [n, k, d]$. Algebraically C is a k-dimensional subspace of a vector space $\mathbb{F}^n$ over a finite field $\mathbb{F}$. The elements of C are called codewords. The generator matrix G of the code C is a $k \times n$ matrix with rank k whose rows form a basis of the subspace C. Hamming distance of two codewords c_i and c_j is denoted by $d(c_i, c_j)$ and defined as the number of places the codewords differ. The minimum distance of a code C is $d = min\{d(c_i, c_j) : c_i, c_j \in C, i \neq j\} = min\{wt(c_i) : c_i \in C, c_i \neq 0\}$, where $wt(c_i)$ is weight of c_i. The code C always re-constructs a codeword from a noisy word which having at most t-bit errors, where $t = \lfloor \frac{d-1}{2} \rfloor$.

Error correction from a noisy word can be performed by any known decoding method. In these methods, we pick a unique codeword from C which is closest to a received noisy word in terms of Hamming distance. Figure 1 depicts that the condition for correcting at most t-bit errors using decoding method. Inside the sphere, each codeword can be depicted as a point and all noisy words w_i such that $d(w_i, c_j) \leq t$ lies within the sphere centered at the codeword $c_j \in C$ with radius t.

2.2 Physical Unclonable Function

Physical unclonable function (PUF) is a challenge-response unclonable noisy function in which the mapping between a challenge and the corresponding response depends on noise such as temperature, voltage supply, aging, and electromagnetic interference etc. PUF behaves like a random function because its responses are unpredictable for same challenge.

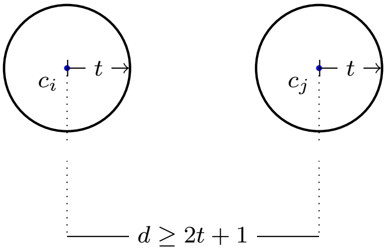
We adopt error-correcting code properties with in PUF function for authentication. For a PUF tag, PUF gives a response w for a challenge $c \in C$ which satisfies $d(w, c) \leq t$, where t is the error correcting capability of the code C. That is

$$\mathrm{PUF}(c) = w, \text{ such that } d(w, c) \leq t.$$

3 System Model

In this section, we describe our system model which is same as Vaudenay privacy model [18] except some modifications according to our requirements. It is shown as follows:

Fig. 1 Decoding spheres



3.1 SetupServer$(1^{\lambda}) \rightarrow (G, DB)$

It generates a secret generator matrix G based on the security parameter λ. For initialization of tags, it generates a code $C = [L, k, d]$ whose generator matrix is G and assigns a codeword c with a unique identification number *EPC* to each tag. It generates a database (DB) in which tag's related all secret information are stored.

3.2 SetupReader$(1^{\lambda}) \rightarrow (K)$

It generates a secret key K based on the security parameter λ and also shares this secret key K with all legitimate tags.

3.3 SetupTag$(EPC)^{\lambda} \rightarrow (K, c, S)$

This oracle generates a tag which has a unique identification number *EPC*, a secret key K, and a unique codeword c of the code C. This oracle also generates updateable memory state S. For each legitimate tag, the pair (c, *EPC*) is stored in DB of the server and the secret key K is shared with all legitimate readers.

3.4 IdentTag $(\sharp) \rightarrow out$

It is an interactive authentication protocol $\sharp$ between a tag, a reader, and the server. If the server authenticates the tag, then $out = EPC$ otherwise $out = \perp$.

4 Adversary Model

The basic components of an RFID system communicate each other over wireless channel. It is easy to eavesdrop the wireless channel and get sensitive information transmitted over the channel. In this model, we consider a tag as drawn tag or free tag according to accessibility of the tag by an adversary ($\mathscr{A}$) i.e. if a tag is inside the reading range of $\mathscr{A}$, then it is considered as drawn tag otherwise it is a free tag.

The following oracles are represent the abilities of $\mathscr{A}$:

4.1 CreateTag^{b} (*EPC*)

$\mathscr{A}$ uses a unique identification number *EPC* to create a tag. This oracle queries SetupTag$(EPC)^{\lambda}$ to create (K, c, S) to the tag. The created tag is legitimate if $b = 1$ and a fake if $b = 0$.

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

$\mathscr{A}$ can access a set of tags which are chosen randomly from the set of free tags with probability distribution *distr*. The drawn tag $vtag_i$ is legitimate or not according to $b_i = 1$ or 0 respectively.

4.3 Free(*vtag*)

The adversary changes the status of the drawn tag *vtag* to a free tag, so that it is inaccessible by the adversary.

4.4 Launch($\sharp$)

$\mathscr{A}$ initiates a new session of the authentication protocol $\sharp$ at the reader side.

4.5 SendReader$(m, \sharp) \rightarrow m'$

This oracle sends message m to a reader in the protocol execution $\sharp$ and gets the response message m' from the reader.

4.6 SendTag$(m, vtag) \rightarrow m'$

It queries a drawn tag *vtag* by sending message m and gets the response message m' from the tag.

4.7 Result($\sharp$)

If $\mathscr{A}$ succeeds, then the output of this oracle is 1 otherwise $\perp$.

4.8 Corrupt(*vtag*)

This oracle returns the current state of the tag *vtag*. The oracle changes the state of *vtag* from drawn to destroy when *vtag* is no longer used after this oracle call.

5 Adversary Classes

According to Vaudenay privacy model [18], adversaries are divided into five classes depending upon the Corrupt(*vtag*) oracle.

- *Weak* Adversaries of this class can not access Corrupt(*vtag*) oracle.
- *Forward* This class of adversaries can only access more Corrupt(*vtag*) oracle after the first call of Corrupt(*vtag*) oracle.
- *Destructive* Adversaries belong to this class can use only once Corrupt(*vtag*) oracle for *vtag* because after first call of Corrupt(*vtag*) oracle, it destroys the tag (*vtag*).
- *Strong* All the oracles are accessible for this class of adversaries.
- *Narrow* Adversaries of this class can not access Result($\sharp$) oracle.

6 Proposed Scheme

We propose a PUF based unilateral authentication protocol for RFID system. Notations are used in this protocol are defined in Table 1, and our proposed protocol is shown in Fig. 2.

Table 1 Notations and symbols are used in the proposed scheme

Notation	Description
C	The binary code generated by G
c	A codeword of the code C
L	Number of bits in bit-string of each parameter
G	Generator matrix of the code C
k	Dimension of the code C
d	Minimum distance of the code C
R_r	Random number generated by a reader
EPC_i	Unique identification number of ith tag
K	Secret key shared between legitimate tags and legitimate readers
N	Total number of tags in the system
$\|\|$	Concatenation operation
$\oplus$	Exclusive-or operation

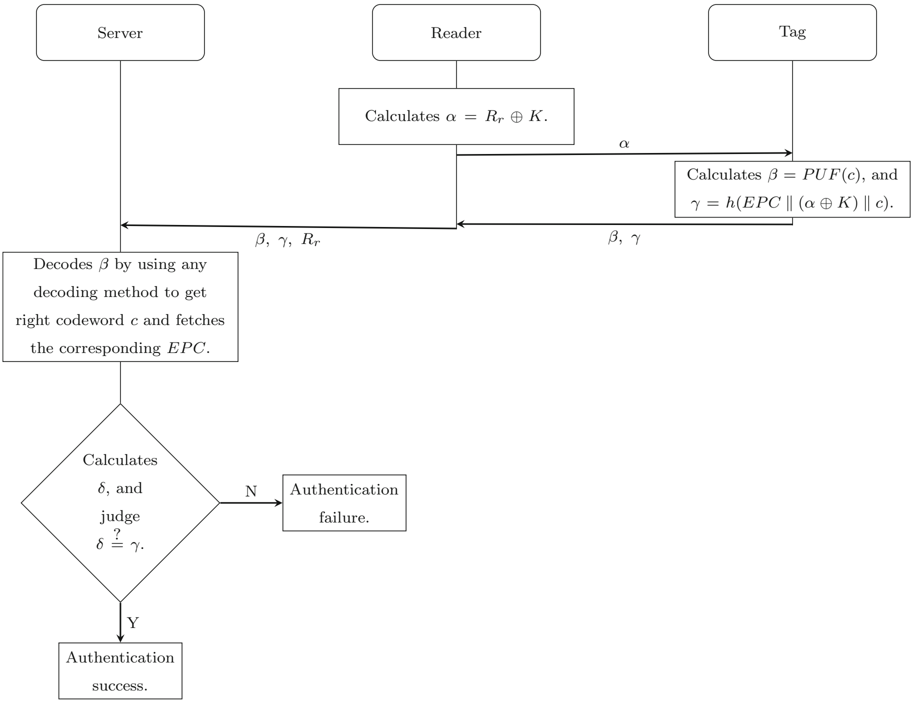

Server
Reader
Tag
Calculates $\alpha = R_r \oplus K$.
α
Calculates $\beta = PUF(c)$, and $\gamma = h(EPC \| (\alpha \oplus K) \| c)$.
$\beta,\ \gamma,\ R_r$
$\beta,\ \gamma$
Decodes β by using any decoding method to get right codeword c and fetches the corresponding EPC.
Calculates δ, and judge $\delta \overset{?}{=} \gamma$.
N
Authentication failure.
Y
Authentication success.

Fig. 2 Proposed authentication protocol

6.1 Assumptions

The proposed protocol works under the following assumptions.

1. Each legitimate tag has its own physical unclonable function (PUF).

2. Every legitimate reader has a pseudo random number generator (PRNG).
3. The server and tags are agreed on a hash function.
4. Communication channel between server and reader is secure.
5. Communication channel between Reader and tag is insecure and their communications are subject to eavesdropping.

6.2 Initialization

1. An initiator (manufacturer) chooses a binary linear code C with generator matrix G of order $k \times L$ with minimum distance d.
2. The generator matrix generates 2^k codewords.
3. The initiator assigns a unique codeword c chosen from these 2^k codewords and an unique identification number EPC to each tag.
4. The initiator assigns a secret key K shared among legitimate tags and legitimate readers.

6.3 Process

The proposed authentication protocol works as follows.

Phase 1 A reader generates a nonce R_r and computes $\alpha = R_r \oplus K$. The reader transmits α to a tag.
Phase 2 After receiving α, the tag computes response messages as follows:

- Calculates $\beta = PUF(c)$.
- Computes $\gamma = h(EPC \| (\alpha \oplus K) \| c)$.

Phase 3 The tag transmits β, γ to the reader.
Phase 4 The reader sends β, γ with R_r to the server.
Phase 5 After receiving β, γ and R_r from the reader, the server computes as follows:

- The server uses any decoding method to get the right codeword c from β.
- It fetches EPC associated with c from the DB.
- Computes $\delta = h(EPC \| R_r \| c)$.
- If $\delta = \gamma$ then the server authenticates the tag otherwise not.

7 Security Analysis

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

Proof Let us assume that $\mathscr{A}$ performs following oracles:

- $\mathscr{A}$ interacts with RFID system and gets access a number of n tags by the DrawTag oracle. i.e.

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

- $\mathcal{A}$ chooses one tag $vtag_i$ from the above drawn tags list and queries a number of oracles for $vtag_i$. i.e.

$$\begin{gathered}\text{Launch}(\sharp)\\ \text{SendReader}(init, \sharp) \to \alpha\\ \text{SendTag}(\alpha,\ vtag_i) \to (\beta,\ \gamma).\end{gathered}$$

Now, To break data privacy, $\mathcal{A}$ needs to know the input data used in the response message $(\alpha,\ \beta,\ \gamma)$. It is infeasible for the adversary to retrieve secret information (i.e. K, EPC, c) used in the $(\alpha,\ \beta,\ \gamma)$ without physically tempered the tag $vtag_i$. □

Theorem 2 *The proposed scheme provides unlinkability with respect to strong adversary* $\mathcal{A}$.

Proof $\mathcal{A}$ performs its experiment as follows:

- $\mathcal{A}$ gets access n tags by querying DrawTag() oracle.

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

- From the drawn tag list, $\mathcal{A}$ chooses two uncorrupted tags $vtag_i$ and $vtag_j$. $\mathcal{A}$ randomly selects $vtag_b$, $b \in \{i,j\}$ among them. The adversary queries a number of oracles on $vtag_b$ and analyze them. i.e.

$$\begin{gathered}\text{CreateTag}(EPC_i) \text{ and } \text{CreateTag}(EPC_j)\\ \text{Select } b \in \{i,j\}\\ \text{drawTag}(EPC_b) \to vtag_b\\ \text{Launch}(\sharp)\\ \text{SendReader}(init, \sharp) \to \alpha'\\ \text{SendTag}(\alpha',\ vtag_b) \to (\beta',\ \gamma')\\ \text{Free}(vtag_b).\end{gathered}$$

- $\mathcal{A}$ terminates the experiment session and outputs a guess bit b'

$$\begin{gathered}\mathcal{A} \text{ succeeds if } b' = 1\\ \text{fails if } b' = 0.\end{gathered}$$

To break unlinkability, $\mathcal{A}$ has to succeed in its experiment. i.e. $\mathcal{A}$ has to determine whether the response message is produced by $vtag_i$ or $vtag_j$. It is infeasible for the adversary to correctly guess the right tag because the proposed scheme uses random number in each response message in each authentication instances. Also, the randomness of PUF enhances the randomization in response messages. Thus it proves the unlinkability property of our proposed scheme. □

7.1 De-Synchronization Attack Resistance

It is infeasible for an adversary to de-synchronize the proposed scheme by interrupting the response message between the reader and the tag. Because secret data (i.e secret key K, unique identification number EPC, and codeword c) are not updated by the server and the tag in any authentication instances.

7.2 Replay Attack Resistance

For replay attack, an adversary collects response message (β, γ) of any authentication session and uses it into later sessions for authentication. In the proposed scheme scenario, when a reader queries a tag by sending newly generated α to the tag, the adversary responds to the reader by sending collected (β, γ) of the previous sessions. The reader transmits this (β, γ) with current session's nonce R_r to the server. The received nonce R_r and nonce used in γ are different. So the server will not verify and terminates the session. The freshness of nonce R_r enables our protocol to prevent replay attack.

7.3 Man-In-Middle Attack Resistance

An adversary acts as a middle man between the reader and the tag only when she knows about the secret parameters. But it is not possible for the adversary to get right codeword c and corresponding unique identification number EPC from response message (β, γ) without any knowledge of K and G.

7.4 Impersonation Attack Resistance

In the proposed scheme, each tag has its own PUF which gives different output for the same input to two different tags. So it is infeasible for the adversary to impersonate a legitimate tag by a fake tag.

8 Cost Analysis

Performance and cost play a very crucial role in an RFID system deployment. The performance of an authentication scheme is expressed in terms of privacy and security. On the other hand, the cost means resources used by the scheme, i.e., required memory storage, communication cost, number of logic gates required for computation etc.

We know that data transmitted from a tag to a reader is much more costly because of the critical power availability on the tag which is harvested from the electromagnetic field of the nearby reader. In Table 2, we present communication cost (in bits) of the proposed scheme with some other schemes [2, 3, 8, 9, 11, 13]. We assume that all the parameters are used in the paper, i.e., EPC, K, R_r, and query/response messages have length L-bits. In Table 2, R $\longrightarrow$ T stands for transmission cost from reader to tag. Similarly, T $\longrightarrow$ R represents transmission cost from tag to reader. In the proposed scheme, a reader's challenge message (α) for a tag requires $1L$ bits and corresponding the tag's response messages (β and γ) requires $2L$ bits. Thus the transmission cost from the reader to the tag (R $\longrightarrow$ T)

Table 2 Communicational cost comparison

Protocol	Kulseng [11]	Kardas [8]	Akgün [3]	Akgün [2]	Maurya [13]	Kaul [9]	Proposed
T $\longrightarrow$ R	$3L$	$2L$	$3L$	$5L$	$2L$	$7L$	$2L$
R $\longrightarrow$ T	$2L$	$4L$	$3L$	$5L$	$1L$	$3L$	$1L$

becomes $1L$ bits and the transmission cost from the tag to the reader (T ⟶ R) becomes $2L$ bits during an authentication session.

In Table 3, we present the computational efforts needed to authenticate a single tag, storage requirement and privacy and security features of the various schemes [2–4, 8, 9, 11, 13] with our proposed scheme. All the schemes [2–4, 8, 9, 11] use PUF function with some other security primitives like hash functions, permutations, cyclic redundancy check (CRC), interpolations, circular shift with modulus (Rot) etc. From the Table 3, it can be easily observed that the storage requirement of the proposed scheme is less than [2–4, 9]; higher than [13]; and same as [8, 11]. Here, we compare our proposed scheme mainly with those schemes that require same or less memory storage on the tag-side in details.

From the Table 3, it can be observed that Kulseng et al.'s [11] storage requirement on the tag-side is $3L$ which is same as the proposed scheme. The scheme [11] performs 2 PUF and 3 PRNG at the tag-side computation during authentication execution which is slightly higher than the proposed scheme. Also, the scheme is vulnerable under message blocking attack, de-synchronization attack and private data leakage [7].

As we can see from the Table 3, Kardas et al. [8] employs 4 hash, 2 PUF and 1 PRNG during an authentication session while the proposed scheme performs 1 hash and 1 PUF at the tag level. Thus Kardas et al. has higher tag level computation as compared to our proposed scheme. In the Kardas et al., the server search complexity is $O(N)$ where N is the total number of tags in the system. This search complexity requires $2N$ number of hash computation in the worst case for a single tag authentication on the server-side. We have removed this problem by employing properties of error-correcting codes in the proposed scheme. The transmission cost from reader to tag (R ⟶ T) is $4L$ bits in the Kardas et al. which is 4-times higher than the proposed scheme. Thus the proposed scheme significantly reduces computational cost and transmission cost and offers same security features as [8].

Both schemes, Maurya et al. [13] and the proposed scheme; utilize some characteristics of coding theory with some other primitives such as hash function, CRC, and physical unclonable function to achieve higher level security with less computation. Table 3 shows that Maurya et al. needs only $2L$ bits for storage requirement on the tag-side which is fewer than the proposed scheme's storage requirement. The server search complexity of Maurya et al. is $O(P)$ where P represents the total number of cosets of the code while the proposed scheme has constant time server search complexity. The scheme proposed by Maurya et al. [13] employs 1 CRC and 1 PRNG at the tag level and has a slightly lower tag level computation as compared to the proposed scheme. However, Maurya et al. is vulnerable under tag impersonation attack and traceability attack [1]. We have overcome these problems by employing PUF and hash computation in the proposed scheme.

9 Conclusion

In this paper, we proposed a PUF based authentication protocol for RFID system. We utilized the properties of error-correcting codes and PUF in the proposed scheme. With the help of these, we reduced the computational cost of the proposed scheme drastically. We analyzed the security features of the proposed scheme in Sect. 7. It shows that the scheme provides high resistance to replay, de-synchronization, tracking, information leakage, and man-in-middle attacks. In Tables 2 and 3, we compared the computational cost of the proposed scheme with some other referred schemes. It shows that the computational cost and the transmission cost of

Table 3 Computation cost performance comparison

Protocol	Entity	Kulseng [11]	Bassil [4]	Kardas [8]	Akgün [3]	Akgün [2]	Kaul [9]	Maurya [13]	Proposed
Decoding method/CRC /Rot/ interpolations/permutations	T	×	5 (Rot)	×	×	8 (Permutations)	×	1 (CRC)	×
	S	×	4 (Rot)	×	×	3 (Permutations)	1 (Interpolation)	1 (Matrix multiplication), 1 (CRC)	1 (Decoding method)
Number of hash	T	×	×	4	4	8	15	×	1
	R + S	×	×	2	4	6	9	×	1
No. of PUFs	T	2	2	2	2	6	4	×	1
No. of PRNG	T	3	×	1	1	2	1	1	×
	R + S	3	2	1	2	2	1	1	1
No. of basic operations	T	4	7	1	4	9	39	3	1
No. of authentication steps		4	4	3	3	4	5	2	2
Server search complexity		$O(1)$	$O(N)$	$O(N)$	$O(1)$	$O(1)$	$O(N)$	$O(P)$	$O(1)$
Required memory	T	$3L$	$4L$	$3L$	$4L$	$7L$	$4L$	$2L$	$3L$
Private data leakage		✓	✓	×	×	×	×	×	×
De-synchronization attack		✓	✓	×	×	×	×	×	×
Impersonation attack		×	✓	×	×	×	×	✓	×
Traceability attack		×	✓	×	×	×	×	✓	×

T Tag-side; *R* reader-side; *S* server-side; *P* total number of cosets of the code C; *N* total number of tags in the system the proposed scheme are relatively low compare to other schemes which provide same security features. Therefore, the proposed scheme performs very well under the resource constraints of tiny-powered tags with high security.

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

Compliance with ethical standards

Conflict of interest The author Pramod Kumar Maurya thanks to MHRD, India for financial support of his research work.

References

1. Aghili, S. F., & Mala, H. (2017). On the security of another CRC based ultralightweight RFID authentication protocol. Cryptology ePrint Archive, Report 2017/1054.
2. Akgün, M., & Çağlayan, M. U. (2016). Towards scalable identification in RFID systems. *Wireless Personal Communications*, *86*(2), 403–421.
3. Akgün, M., & Çağlayan, M. U. (2015). Providing destructive privacy and scalability in RFID systems using PUFs. *Ad Hoc Networks*, *32*, 32–42.
4. Bassil, R., El-Beaino, W., Kayssi, A., & Chehab, A. (2011). A PUF-based ultra-lightweight mutual-authentication RFID protocol. In *2011 international conference for internet technology and secured transactions* (pp. 495–499).
5. Gope, P., & Hwang, T. (2015). A realistic lightweight authentication protocol preserving strong anonymity for securing RFID system. *Computers and Security*, *55*, 271–280.
6. Jung, S. W., & Jung, S. (2013). HRP: A HMAC-based RFID mutual authentication protocol using PUF. In *The international conference on information networking 2013 (ICOIN)* (pp. 578–582).
7. Kardas, S., Akgün, M., Kiraz, M. S., & Demirci, H. (2011). Cryptanalysis of lightweight mutual authentication and ownership transfer for RFID systems. In *2011 workshop on lightweight security privacy: devices, protocols, and applications* (pp. 20–25).
8. Kardas, S., Celik, S., Yildiz, M., & Levi, A. (2012). PUF-enhanced offline RFID security and privacy. *Journal of Network and Computer Applications*, *35*(6), 2059–2067.
9. Kaul, S. D., & Awasthi, A. K. (2017). Privacy model for threshold RFID system based on PUF. *Wireless Personal Communications*, *95*(3), 2803–2828.
10. Kulseng, L., Yu, Z., Wei, Y., & Guan, Y. (2009). Lightweight secure search protocols for low-cost RFID systems. In *29th IEEE international conference on distributed computing systems* (pp. 40–48).
11. Kulseng, L., Yu, Z., Wei, Y., & Guan, Y. (2010). Lightweight mutual authentication and ownership transfer for RFID systems. In *2010 proceedings IEEE INFOCOM* (pp. 1–5).
12. Ling, S., & Xing, C. (2004). *Coding theory*. Cambridge: Cambridge University Press.
13. Maurya, P. K., Pal, J., & Bagchi, S. (2017). A coding theory based ultralightweight RFID authentication protocol with CRC. *Wireless Personal Communications*, *97*(1), 967–976.
14. Ranasinghe, D. C., Engels, D. W., & Cole, P. H. (2004). Security and privacy: Modest proposals for low-cost RFID systems. In *Auto-ID labs research workshop.*
15. Sadeghi, A. R., Visconti, I., & Wachsmann, C. (2010). PUF-enhanced RFID security and privacy. In *Workshop on secure component and system identification (SECSI).*
16. Safkhani, M., Bagheri, N., & Naderi, M. (2011). Security analysis of a PUF based RFID authentication protocol. IACR Cryptology ePrint Archive, Report 2011/704.
17. Tuyls, P., & Batina, L. (2006). RFID-tags for anti-counterfeiting. In D. Pointcheval (Ed.), *Topics in cryptology—CT-RSA 2006. Lecture notes in computer science* (Vol. 3860, pp. 115–131). Berlin: Springer.
18. Vaudenay, S. (2007). On privacy models for RFID. In K. Kurosawa (Ed.), *Advances in cryptology—ASIACRYPT 2007* (Vol. 4833, pp. 68–87). Berlin: Springer.

Publisher's Note

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

Pramod Kumar Maurya received his M.Sc. in Mathematics from University of Allahabad, India, 2011. He has completed M.Tech. in Computer Science & Data Processing from IIT KHARAGPUR, India, 2014. He is currently a research scholar in the Department of Mathematics at NIT DURGAPUR, India. His research interests include identity authentication, RFID security, and information security.

Satya Bagchi received the B.Sc. and M.Sc. Degrees in Mathematics from the University of Kalyani, West Bengal, India, in 2002 and 2004, respectively. He received Ph.D. degree in Mathematics from the same university in 2013. From 2006 to 2007 he was a lecturer, Department of Mathematics, A B N Seal College, Cooch Behar, West Bengal, India. He is currently an Assistant Professor, Department of Mathematics, National Institute of Technology, Durgapur, India. His current research interests are in RFID security protocol design, cryptography and coding theory. Dr Bagchi is a life member of the Cryptology Research Society of India (CRSI).