IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Date of publication xxxx 00, 0000, date of current version xxxx 00, 0000.

*Digital Object Identifier 10.1109/ACCESS.2017.DOI*

# An Enhanced Authentication Protocol Suitable for Constrained RFID Systems

**MEHDI HOSSEINZADEH[1,2] MOHAMMAD REZA SERVATI[3], AMIR MASOUD RAHMANI[4], MASOUMEH SAFKHANI[3,5], JAN LANSKY [6], RENATA JANOSCOVA[6], OMED HASSAN AHMED[7], JAWAD TANVEER[8,*], SANG-WOONG LEE [9,*],**

[1] 1Institute of Research and Development, Duy Tan University, Da Nang, Vietnam
[2]School of Medicine and Pharmacy, Duy Tan University, Da Nang, Vietnam (e-mail: mehdihosseinzadeh@duytan.edu.vn)
[3]Department of Computer Engineering, Shahid Rajaee Teacher Training University, Tehran, Iran, Postal code: 16788-15811 (e-mail: mohammadreza.servati75@gmail.com, Safkhani@sru.ac.ir)
[4]Future Technology Research Center, National Yunlin University of Science and Technology, Yunlin, Taiwan (e-mail: rahmania@yuntech.edu.tw)
[5]School of Computer Science, Institute for Research in Fundamental Sciences (IPM), P. O. Box 19395-5746, Tehran, Iran
[6]Department of Computer Science and Mathematics, Faculty of Economic Studies, University of Finance and Administration, Prague, Czech Republic (e-mail:{lansky,janoscova}@mail.vsfs.cz)
[7]Department of Information Technology, University of Human Development Sulaymaniyah, Iraq (e-mail:Omed.hassan@uhd.edu.iq)
[8]Department of Computer Science and Engineering Sejong University Seoul 05006 Korea (e-mail: jawadtanveer@sejong.ac.kr)
[9]Pattern Recognition and Machine Learning Lab, Department of AI Software, Gachon University, Seongnam 13557, Korea (e-mail: slee@gachon.ac.kr)

Corresponding authors: Jawad Tanveer (E-mail: jawadtanveer@sejong.ac.kr) and Sang-Woong Lee (E-mail: slee@gachon.ac.kr)

The result was created through solving the student project “Security analysis and developing lightweight ciphers and protocols” using objective oriented support for specific university research from the University of Finance and Administration, Prague, Czech Republic. Authors thank Michal Merta, and Zdeněk Truhlář for their help with the research connected with the topic of the article.

## ABSTRACT

RFID technology offers an affordable and user-friendly solution for contactless identification of objects and individuals. However, the widespread adoption of RFID systems raises concerns regarding security and privacy. Vulnerabilities such as message tampering, interception, and eavesdropping pose significant risks to the integrity of the system. This study examines the effectiveness of two recently proposed ultra-lightweight RFID authentication protocols, URASP and KUAJB, in addressing these security challenges.
Surprisingly, our findings reveal that both URASP and KUAJB protocols are susceptible to secret disclosure attacks, despite their claims of providing robust security. Consequently, the development of a truly ultra-lightweight protocol that ensures adequate security becomes a formidable task. As a potential solution, the enhancement of the URASP protocol through the integration of a simple cryptographic primitive is suggested to bolster its security measures.

**INDEX TERMS** RFID; Ultra-lightweight; Permutation; Secret Disclosure Attack; Quark Hash Function

## I. INTRODUCTION

RFID technology is extensively employed across various industries, such as manufacturing, supply chains, and healthcare, owing to its affordability and energy efficiency. Moreover, it is recognized as a highly promising technology for the Internet of Things (IoT). Device authentication is one of the most important challenges when it comes to security and privacy in RFID systems. Due to RFID tags’ limited computational capabilities, which prevent them from carrying out sophisticated cryptographic primitives, the implementation of well-known authentication methods is constrained. Several lightweight authentication techniques have been put out to address this problem, such as the one described in [1], which makes use of a pseudo-identifier SID and a secret key $x$ that is given by the administrator to each valid tag. The suggested system has been security assessed against various RFID attacks and guarantees the secret data’s secrecy, integrity, and authenticity.

Researchers have developed several security approaches, which can be divided into four main categories: full-fledged, simple, lightweight, and ultra-lightweight, to solve the security and privacy concerns in RFID systems. Different cryptography operations can be used without limitations by full-fledged security mechanisms. Schemes that support hash functions and pseudo-random number generators (PRNGs) to build security protocols are under the simple category. Security protocols can be built using lightweight cryptographic primitives like the cyclic redundancy check

(CRC), the pseudo-random number generator (PRNG), and other procedures. The bit-wise operations XOR, OR, Rotate, and similar ones are the only ones allowed by the ultra-lightweight protocols. Although creating security protocols that are only extremely lightweight is exciting, researchers have discovered numerous security flaws in them, and there are few such schemes in use [2, 3, 4, 5].

As shown in Figure 1, an RFID system is made up of three main parts: a tag, a reader, and a back-end server that stores and manages data from the tag and reader. Based on how they are powered, tags can be divided into three categories: active, semi-active, and passive tags. Passive tags, which are the least expensive tags, can only communicate with a reader's signal. Active tags are powered by internal batteries. Semi-active tags can utilize either a reader's signal or its battery [6].

Ultra-high frequency passive tags are frequently employed in a variety of applications, operate between 860 and 960 MHz. Additionally, there are numerous common attacks on inexpensive RFID tags, such as response injection attacks, unauthorized cloning, unauthorized deactivating, and tracked without authorization. For more information, see Table 1.

### A. OUR CONTRIBUTIONS

This paper's main contribution can be summarized as follows:

- This paper illustrates a secret disclosure attack against two recent authentication protocols, i.e. Sharigh et al. [7] protocol (URASP) and Khan et al. [8] protocol (KUAJB from now).
- This paper addresses [7]'s authentication protocol security flaw and suggests a new authentication protocol. In order to keep the proposed protocol lightweight, lightweight hash functions such as Quark hash function [9] have been used instead of conventional hash functions such as SHA-3.
- Security of authentication protocols is always demonstrated through informal and formal security analysis. Comparing our proposed scheme with similar recent protocols reveals that our proposed protocol outperforms its predecessors, the URASP protocol, in terms of security or effectiveness.
- The analyzes carried out in this paper involves formal tools such as Scyther and ProVerif and a wide range of informal discussions against the resistance of the proposed authentication scheme against different active and passive attacks.

### B. PAPER ORGANIZATION

The body of this essay is organized as follows: The related work in this field is summarized in Section II. The preliminaries and basic definitions used in this paper are stated in Section III. Section IV briefly explains URASP and KUAJB authentication schemes. The security analysis of those authentication schemes is explained in Section V, which is actually secret value disclosure attacks against the discussed protocols. Section VI introduces a new authentication scheme, and Section VII analyzes security of this scheme using both formal and informal methods. Section VIII evaluates how well this approach worked and the conclusion is presented in Section IX.

## II. RELATED WORK

In this section, many authentication schemes, such as lightweight, ultra-lightweight, and simple are reviewed. Furthermore, as with other authentication protocols (i.e., full-fledged), these authentication protocols must provide all required security properties. A modern authentication protocol for Medical Wireless Sensor Networks (MWSN) was proposed by [10] and they believed their own scheme satisfied all security requirements. However, [11] made the observation that the proposed protocol in [10] is vulnerable to privileged attacks. Additionally, that protocol does not protect user anonymity. After that [11] presented a modification to their authentication scheme. Although, [12] drew attention to the improvement's flaws, which include a lack of password identification and vulnerability to a de-synchronization attack. [13] also revealed that the proposed protocol in [11] had a few additional security flaws, such as vulnerability to offline password guessing and user impersonation.

[14] proposed a XOR and Rotation operations based protocol. However, some researchers such as [15, 5, 16] demonstrated that their protocol is weak and vulnerable to secret disclosure and de-synchronization attacks. In addition, [15] suggested a modified version of [14] scheme, but [17] reveals that [15]'s scheme suffers from secret disclosure for instance.

A cloud-assisted authentication scheme for Telecare Medical Information Systems (TMIS) was asserted by [18] and they thought their scheme was secure against well-known privacy and security attacks. While [19] showed that their authentication scheme is insecure and susceptible to security issues such as impersonation and patient anonymity contradiction attacks. Also, another authentication scheme for healthcare systems was suggested by [20], while, [21] presented convincing impersonation and replay attacks for their protocol. Furthermore, [22] proposed a protocol for device identification in residential automation systems with a smart grid. However, [23] showed that [22]'s protocol suffers from stolen smart devices, impersonation, and session key exposure, and also is unable to provide a secure authentication mechanism.

Also, [24] developed a lightweight authentication scheme for wearable devices. After that, [25] illustrated that their protocol is insecure and vulnerable to privileged insiders, compromised sensing devices, and de-synchronization attacks. [26] asserted a lightweight protocol and claimed it to be a secure protocol, however [27] showed that their scheme is not secure and suspicious to key compromise, replay, and impersonation attacks. Also, two respectively ultra-lightweight and lightweight schemes were proposed by [28] and [29]. Whereas, [30] illustrated that [28]'s scheme is suspect to secret disclosure and de-synchronization

TABLE 1: Types of RFID attacks

| Attacks | Explanation |
|---|---|
| Tag tracking | By sending authentication requests to the tag as a trustworthy reader and assessing the tag's response messages, the tag could be traced. |
| Forgery | Every time a valid tag's identity information is intercepted, an attacker can pose as a genuine tag and ask the valid reader for confirmation. |
| Replay | By intercepting RFID session data in an effort to verify the target object, the intruder can send stolen info to authorized members in the later times. |
| De-synchronization | In this attack, one of the authentication sides only updates secret shared values and so the other side cannot validate it for the subsequent round of authentication, as a result, the ensuing phases are halted. |
| Data confidentiality contradiction | Securing the communication message before transmission is crucial to preventing the leakage of critical and secret information, as an attacker may get crucial information through maliciously listening in on session messages between authorized users. In the absence of a key value, an attacker will not be able to decrypt the communication message or identify the secret value. |
| Data integrity contradiction | The integrity of data prevents data from being altered while in transit. Data integrity and data origin authentication are both parts of data authentication. The recipient can be certain that the data has not been changed if there is a data integrity preservation mechanism. In the symmetric key cryptography a method which is used to offer message authentication is the message authentication code(MAC). |
| User privacy contradiction | RFID security protocols are required to ensure that user data is protected and to stop attacker from intercepting the RFID tag. To secure and privacy-preserving RFID authentication, numerous authentication methods and protocols have been put forth. To prevent information leakage or falsification by unauthorized users, it is crucial to maintain privacy and confidentiality of all crucial messages in the system throughout communication. |
| Forward/Backward secrecy contradiction | Given that the long-term key kept on the tag was obtained by an attacker through a variety of illicit means. If the past/future session keys are computed only using these long-term secret values, it does not satisfy the forward/backward secrecy property. Because the attacker knowing that the long-term secret values, can compute the past/future session keys. Therefore, in order to guarantee the RFID system's forward/backward secrecy, for example, the shared session key values must be also connected to the random numbers generated in its time. |

attacks. Regarding the proposed protocol in [29], it suffers from tag impersonation and de-synchronization attack, given that required parameters can be extracted from the tag's response. As another authentication scheme, [31] suggested an ultra-lightweight authentication scheme for medical privacy, while [32] showed drawbacks in their protocol such as vulnerability against reader impersonation, secret disclosure, and tag traceability attacks, and they proposed a new authentication scheme called SecLap. However, [33] demonstrated that the SecLap protocol is vulnerable to the secret disclosure attack for instance. [34] proposed a claimed to be secure ECC-based protocol for IoT medical systems, whereas [35] demonstrated that [34]'s protocol is not secure and is vulnerable to a variety of attacks such as traceability, de-synchronization, and integrity contradiction. Furthermore, using encryption and decryption algorithms, [36] proposed an authentication mechanism for RFID-based IoT devices. Another ultra-lightweight protocol called ESRAS has been proposed by Shariq et al. [37]. The proposed scheme aims to achieve confusion and diffusion by using an ultra-lightweight operation termed $Rank(X, Y)$ as the heart of non-linearity, where $X$ and $Y$ are strings of bits, and the function is conducted using bitwise operations efficiently. However, latter [30] demonstrated that this protocol, similar to many other ultra-lightweight protocols, suffers from various attacks, including secret disclosure attacks and de-synchronization. In [38] Safkhani et al. proposed a generalized framework for the security analysis of any two-party authentication protocol in which a protocol party does not contribute to the session randomness and updates the shared parameters to avoid traceability. They have shown that such a protocol suffers from de-synchronization attacks. They applied the attack to several known ultra-lightweight protocols and also proposed a generalized scheme called GIMAP to avoid such attacks, supported by a concrete example. Inspired by [39], the proposed protocol employs $\chi per(\cdot)$ as the source of

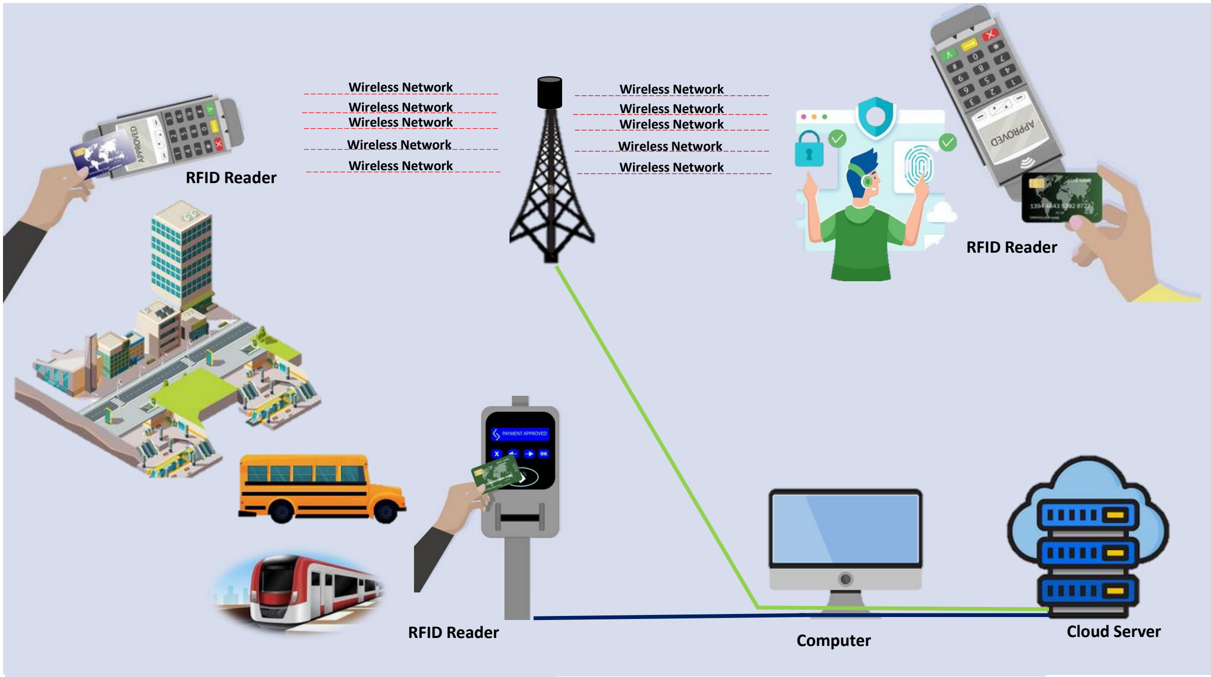


FIGURE 1: A typical architecture of an RFID system

non-linearity. However, the protocol's tag sends a parameter $IDS$ which is constant as long it does not participate in a successful session. It shows that this protocol is a target for conditional traceability. Khan et al. [8] recently proposed a protocol to solve the anonymity and traceability difficulties in existing ultra-lightweight protocols. This protocol which we call it KUAJB (the first letters of the designers' last name) benefits from Cross Operation called $Cro(x,y)$ as the source of non-linearity, which has been already introduced in [40]. Similar to $Rank(X,Y)$ function in [41], $Cro(x,y)$ is also very efficient in hardware and can be implemented using bit-wise operations efficiently. Although they claimed security against various attacks, however, in this paper we show its security flaws. Another protocol that has been recently proposed inspired by the mentioned $Cro(x,y)$ function, is AnonSURP [41]. It also belongs to ultra-lightweight RFID protocols. However, in this protocol, the shared parameters are updated after each successful session and the reader is the only entity that contributes to the session freshness by generating two random numbers $R_1$ and $R_2$, see [41, Sec 5:Fig. 4] for more details. Hence, it is a clear victim for the generalized de-synchronization attack proposed in [38], an interested reader can refer to [38] and we omit details of the attack in this paper due to its simplicity. Recently, [7] proposed an ultra-lightweight authentication scheme, and they claimed that their protocol addressed all security issues. However, we show that their protocol is also not secure against a secret disclosure attack, and we use it as a basis to introduce a new lightweight authentication scheme that is resistant to well-known attacks. Table 2 illustrates a summary of the reviewed authentication schemes.

## III. PRELIMINARIES

This section describes the notations and preliminaries used in this paper. The notations used throughout the paper are represented in Table 3.

Because the permutation function used in [7] has been exposed to the URASP's vulnerability to secret value discovery attacks, we will explain the permutation operation and left rotation operation used in [7] briefly here.

### A. PERMUTATION OPERATION

We revisit the permutation operation proposed by Tian *et al.* in [42], and then revisit an improved version of it in [7]. Furthermore, Figure 2 illustrates an example of this operation.

**Definition** Given two $l$-bit strings $X$ and $Y$, where:

$$X = x_1x_2...x_l,\ x_i \in \{0,1\},\ i = 1,2,...,l$$

$$Y = y_1y_2...y_l,\ y_j \in \{0,1\},\ j = 1,2,...,l$$

Let the hamming weight of $Y$, $wt(Y)$, is $m$ $(0 \leq m \leq l)$ and

$$y_{k_1} = y_{k_2} = ... = y_{k_m} = 1$$

$$y_{k_{m+1}} = y_{k_{m+2}} = ... = y_{k_l} = 0$$

where $1 \leq k_1 < k_2 < ...k_m \leq l$ and $1 \leq k_{m+1} < k_{m+2} < ...k_l \leq l$. Then, $Per(X,Y)$ is defined as follows:

$$Per(X,Y) = x_{k_1}x_{k_2}...x_{k_m}x_{k_l}x_{k_{l-1}}...x_{k_{m+2}}x_{k_{m+1}}$$

The authors of [7] point out some flaws in the preceding permutation and present a new permutation operation that

TABLE 2: A recap of related works

| **References** | Feature | **Weaknesses** |
|---|---|---|
| [10] | Lightweight | 1) Anonymity<br>2) Insider attack<br>3) Off-line guessing attacks |
| [11] | Lightweight | 1) De-synchronization attack<br>2) User impersonation attack<br>3) Off-line guessing attacks |
| [18] | Lightweight | De-synchronization attack |
| [14] | Lightweight | 1) De-synchronization attack<br>2) Secret disclosure attack |
| [15] | Ultra-lightweight | 1) De-synchronization attack<br>2) Secret disclosure attack |
| [37] | Ultra-lightweight | Secret disclosure attack |
| [41] | Ultra-lightweight | De-synchronization attack |
| [38] | Lightweight | Conditional traceability attack |
| [20] | Lightweight | 1) Replay attack<br>2) Impersonation attack |
| [22] | Lightweight | 1) Impersonation attacks<br>2) Stolen smart card attack<br>3) Session key disclosure attack |
| [24] | Lightweight | 1) Privileged-insider attack<br>2) Compromise sensing device attack<br>3) De-synchronization attack |
| [26] | Lightweight | 1) Key compromise impersonation attack<br>2) Replay attack<br>3) Impersonation attack |
| [28] | Ultra-lightweight | 1) De-synchronization attack<br>2) Secret disclosure attack |
| [29] | Ultra-lightweight | 1) Impersonation attack<br>2) De-synchronization attack |
| [32] | Lightweight | 1) Traceability attack<br>2) Personal disclosure attack |
| [34] | ECC-based | 1) Traceability attack<br>2) Integrity contradiction attack<br>3) De-synchronization attack |
| [35] | ECC-based | Energy consuming |

works as follows:

$$Per_{new}(X,Y) = Per_{old}(X \oplus Y, Y)$$

Where $Per_{old}$ represents Tian *et al.*'s permutation. For more information, please see [7].

### B. ROTATION OPERATION

We will discuss the left rotation operation utilized in [7] in this part. $Rot(X,Y)$ indicates that the string $X$ is rotated to the left by $wt(Y)\ (mod\ l)$ bits.

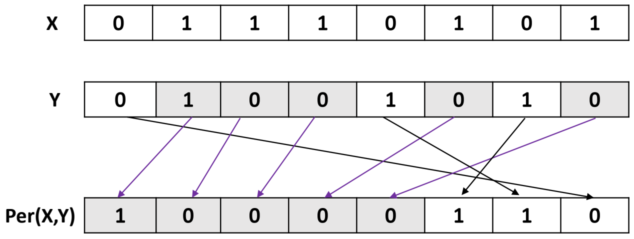


FIGURE 2: The $Per(X,Y)$ operation

## IV. EVALUATED PROTOCOLS

### A. URASP PROTOCOL

URASP comprises two stages: startup and authentication. Furthermore, Figure 3 demonstrates [7]'s authentication scheme.

#### 1) Initialization phase

During this phase, legitimate entities share some basic values that will be used later in the authentication step, as follows:

1) In each tag, $SA$ stores a unique identity $ID$, secret keys $K$, $K'$, and an index pseudonym $IDS$.
2) $SA$ also saves $ID$, $K$, $IDS_{new}$, and $IDS_{old}$ in the server for each tag. We start with $IDS_{new} = Null$ and $IDS_{old} = IDS$.
3) $SA$ stores $K$ in each reader for each tag.

#### 2) Authentication phase

The URASP protocol conducts the following stages during the authentication phase:

1) step 1: $\mathcal{R} \rightarrow \mathcal{T} : \{Query, \alpha, \beta\}$: The reader chooses two random numbers i.e. $R_1$ and $R_2$, calculates $\alpha =$

TABLE 3: Used notations in this paper

| Notation | Description |
|---|---|
| $SA$ | System Administrator in [7] |
| $T$ | Tag |
| $R$ | Reader |
| $A$ | Adversary |
| $ID$ | Tag's unique identifier in [7] |
| $IDS$ | Tag's pseudonym in [7] |
| $IDS_{newrR}, IDS_{newL}$ | The right half and left half of $IDS_{new}$ in [7] |
| $K$ | Tag's secret value in [7], also given to the reader |
| $K'$ | The tag's secret value in [7], also known to the server |
| $R_1, R_2, R_3$ | Random numbers |
| $\|$ | Concatenation operation |
| $\oplus$ | Exclusive-or (XOR) operation |
| $H(.)$ | Cryptographic one-way hash functions |
| $Per(X, Y)$ | Permutation function in [7] |
| $wt(Y)$ | $Y$'s Hamming weight |
| $R_R$ | Random Nonce of Reader in [8] |
| $R_S$ | Random Number of Server in [8] |
| $R_T$ | Random Number of Tag in [8] |
| $R_{ID}$ | Reader $ID$ in [8] |
| $TID$ | Tag's ID in [8] |
| $K_{SR}$ | Pre-shared Key between Server and Reader in [8] |
| $K_{RT}$ | Pre-shared Key between Reader and Tag in [8] |
| $K$ | Current Session Number in [8] |
| $K_{new}$ | Next Session Number in [8] |
| $Cro(x, y)$ | Cross Operation in [8] |
| $Rot(x, y)$ | Rotation Operation, $x \ll wt(y)$ in [8] |

$R_1 \oplus K$ and $\beta = R_2 \oplus K$, and sends $(Query, \alpha, \beta)$ to the tag.

2) step 2: $\mathcal{T} \to \mathcal{R} : \{IDS, \gamma_L\}$: Using its key $K$, the tag extracts $R_1$ and $R_2$ from received $\alpha$ and $\beta$. Then the tag computes $\gamma = Per(Rot(Rot(ID \oplus R_1, R_2), K), K \oplus R_2)$ and sends $(IDS, \gamma_L)$ to the reader (If $wt(\gamma)$ is even, it sends $\gamma_R$).
3) step 3: $\mathcal{R} \to \mathcal{BS} : \{IDS, R_1, R_2, \gamma_L\}$: Over a secure channel, the reader sends $(IDS, R_1, R_2, \gamma_L)$ to the server.
4) step 4: $\mathcal{BS} \to \mathcal{T} : \{\gamma_R\}$: The server pulls $ID$ and $K$ from the database based on the received $IDS$ and then conducts the following actions:
    a) computes $\gamma' = Per(Rot(Rot(ID \oplus R_1, R_2), K), K \oplus R_2)$.
    b) determines whether $\gamma'_L \overset{?}{=} \gamma_L$. If this is the case, the server authenticates the tag and changes $IDS_{old} = IDS$ and $IDS_{new} = Per(Rot(Rot(IDS, K \oplus R_1), R_2 \oplus ID), ID \oplus K)$.
    c) computes $\delta = Per(Rot(Per(\gamma'_R, IDS_{newR}), R_2), \gamma'_L \oplus IDS_{newL} \oplus K_R)$.
5) Tag verification. The tag does the following to authenticate the server:
    a) finds $IDS' = Per(Rot(Rot(IDS, K \oplus R_1), R_2 \oplus ID), ID \oplus K)$.
    b) finds $\delta' = Per(Rot(Per(\gamma_R, IDS'), R_2), \gamma_L \oplus IDS' \oplus K_R)$.
    c) determines whether $\delta'_R \overset{?}{=} \delta_R$. If that's the case, the tag authenticates the server and modifies the index $IDS = IDS'$.

### B. KUAJB PROTOCOL

KUAJB authentication includes several steps between the reader, the tag, and the server. All communications are over public channels and accessible by the adversary. The steps of the protocol are as follows, also depicted in Figure 4.

1) The reader generates a random number $R_R$ and computes $N'_R = R_R \oplus K_{RT}$ and sends it to the tag as $M_1$, where $K_{RT}$ is a pre-shared key between the tag and the reader.
2) The tag extracts $R_R = N'_R \oplus K_{RT}$, generates a random number $R_T$ and sets $mark = 00$ to indicate the start of the session. Next, it computes $N'_T = R_T \oplus K_{RT}$ and Cro$(RID \oplus TID, K)$ and sends them to the reader.
3) The reader extracts $R_T = N'_T \oplus K_{RT}$, computes $N''_R = R_R \oplus K_{SR}$, $N''_T = R_T \oplus K_{SR}$ and Cro$(RID \oplus TID, K)$ and sends them as $M_3$ to the server.

| Server | $Message$ | Reader | $Message$ | Tag |
|---|---|---|---|---|
| | | Generates $R_1$ and $R_2$, calculates $\alpha = R_1 \oplus K$ and $\beta = R_2 \oplus K$; $M_1 : \{Query, \alpha, \beta\}$ | | |
| | | | $\xrightarrow{\{M_1\}}$ | Using its key $K$, extracts $R_1$ and $R_2$ from received $\alpha$ and $\beta$. Then the tag computes $\gamma = Per(Rot(Rot(ID \oplus R_1, R_2), K), K \oplus R_2)$ and sends $(IDS, \gamma_L)$ to the reader (If $wt(\gamma)$ is even, it sends $\gamma_R$); $M_2 : \{IDS, \gamma_L/\gamma_R\}$ |
| | | Over a secure channel, the reader sends $(IDS, R_1, R_2, \gamma_L)$ to the server; $M_3 : \{IDS, R_1, R_2, \gamma_L\}$. | $\xleftarrow{\{M_2\}}$ | |
| The server pulls $ID$ and $K$ from the database based on the received $IDS$ and computes $\gamma' = Per(Rot(Rot(ID \oplus R_1, R_2), K), K \oplus R_2)$, determines whether $\gamma'_L \overset{?}{=} \gamma_L$ to authenticate the tag and changes $IDS_{old} = IDS$ and $IDS_{new} = Per(Rot(Rot(IDS, K \oplus R_1), R_2 \oplus ID), ID \oplus K)$ and compute $\delta = Per(Rot(Per(\gamma'_R, IDS_{newR}), R_2), \gamma'_L \oplus IDS_{newL} \oplus K_R)$; $M_4 : \{\gamma_R\}$ | $\xleftarrow{\{M_3\}}$ | | | |
| | $\xrightarrow{\{M_4\}}$ | | | |
| | | | $\xrightarrow{\{M_4\}}$ | Computes $IDS' = Per(Rot(Rot(IDS, K \oplus R_1), R_2 \oplus ID), ID \oplus K)$ and $\delta' = Per(Rot(Per(\gamma_R, IDS'), R_2), \gamma_L \oplus IDS' \oplus K_R)$, verifies whether $\delta'_R \overset{?}{=} \delta_R$ to authenticates the server and do the update $IDS = IDS'$. |

FIGURE 3: URASP authentication scheme proposed by [7]

4) The server extracts $R_R = N''_R \oplus K_{SR}$ and $R_T = N''_T \oplus K_{SR}$. It also searches the ID table IDT to find a record for $Cro(TID \oplus RID, K)$. Next, it generates a random number $R_S$ and computes $N'_S = R_S \oplus K_{SR}$, $\text{Cro}\,(RID \oplus TID, N'_S \oplus K)$, $\text{Rot}(K \oplus TID, RID \oplus K)$, and $K \oplus N'_S$ and sends them as $M_4$ to the reader over a public channel.
5) The reader extracts $R_S = N'_S \oplus K_{SR}$ and $wt(K \oplus TID)$ and verifies the received token from the server to authenticate it. It then sends $TID \oplus R_R$ and $N''_S = R_S \oplus K_{RT}$ as $M_5$ to the tag over a public channel.
6) The tag extracts $R_S = N''_S \oplus K_{RT}$ and verifies the received token to authenticate the reader. Next, it updates the session number $K$ as $K_{new} = \text{Cro}\,(N_R \oplus N_R \oplus N_T, K)$ and sends $\text{Cro}\,(TID, K_{new} \oplus RID)$ as $M_6$ to the reader.
7) The reader verifies the received $\text{Cro}\,(TID, K_{new} \oplus RID)$ to authenticate the tag and also update $K$ to $K_{new}$. It then sends $\text{Cro}\,(TID, K_{new} \oplus RID)$ as $M_7$ to the server.
8) The server also verifies the received $\text{Cro}\,(TID, K_{new} \oplus RID)$ to authenticate the tag and also update $K$ to $K_{new}$. It then sends $K_{\text{new}} \oplus R_T \oplus R_R$ as $M_8$ to the reader.
9) The reader verifies the received token and sends $K_{new} \oplus R_T \oplus N_R$ as $M_9$ to the tag.
10) The tag also verifies the received token from the reader to make sure that $K$ is synchronized and sets $Mark = 01$. It also computes $Mark \oplus R_S$ and sends it to the reader as $M_{10}$.
11) The reader also forwards the received message to the server as $M_{11}$.
12) The server extracts and verifies $Mark = 01$ to store a new record $\{\text{Cro}\,(RID \oplus TID, K_{\text{new}}),\ \text{Rot}\,(K_{\text{new}} \oplus TID, K_{\text{new}} \oplus RID)\}$ in its index table IDT.
13) Finally the tag sets $Mark = 10$ after receiving a notification that indicates the authentication has been accomplished successfully.

## V. ON THE SECURITY OF URASP AND KUAJB

### A. CRYPTANALYSIS OF URASP

This section takes a closer look at URASP. We will expose some flaws in this protocol. The attacker $\mathcal{A}$ does the following:

1) sends $\alpha = 0$ and $\beta = 0$ to the RFID tag and receives $\{IDS, \gamma_L\}$ while preventing communication and updating between the tag and the reader. So $K = R_1$, $K = R_2$, and $\gamma = Per(Rot(Rot(ID \oplus K, K), K), 0)$. We show it as $\overleftarrow{z}$ because $Per(z, 0)$ is actually a rearrangement of $z$ from MSB to LSB. This results in $\gamma = \overleftarrow{Rot(Rot(ID \oplus K, K), K)} = \overleftarrow{Rot(ID \oplus K, 2K)}$.
2) Again, the adversary sends $\alpha = 1$ and $\beta = 0$ to RFID tag and receives $\{IDS, \gamma_L\}$ while he prevents communication between tag and reader and updating. So, we have $K = R_1 \oplus 1$, $K = R_2$, $\gamma = Per(Rot(Rot(ID \oplus K \oplus 1, K), K), 0) = \gamma = \overleftarrow{Rot(Rot(ID \oplus K \oplus 1, K), K)} = \overleftarrow{Rot(ID \oplus K \oplus 1, 2K)}$.

Because the attacker in both situations knows $\gamma_L$, the value of $ID \oplus K$ will almost surely leak, signaling a disclosure attack with a success rate of "1" and the complexity of three protocol executions.

| Server | $Message$ | Reader | $Message$ | Tag |
|---|---|---|---|---|
| | | Generates $R_R$ and computes $M_1 : \{N'_R = R_R \oplus K_{RT}\}$ | | |
| | | | $\xrightarrow{\{M_1\}}$ | $R_R = N'_R \oplus K_{RT}$, generates a random number $R_T$ and sets $mark = 00$, computes $M_2 : \{N'_T = R_T \oplus K_{RT}; \mathrm{Cro}(RID \oplus TID, K)\}$ |
| | | $R_T = N'_T \oplus K_{RT}$, computes $M_3 : \{N''_R = R_R \oplus K_{SR}, N''_T = R_T \oplus K_{SR}; \mathrm{Cro}(RID \oplus TID, K)\}$ | $\xleftarrow{\{M_2\}}$ | |
| $R_R = N''_R \oplus K_{SR}$ and $R_T = N''_T \oplus K_{SR}$; finds a record for $Cro(TID \oplus RID, K)$; generates $R_S$ and computes $M_4 : N'_S = R_S \oplus K_{SR}; \mathrm{Cro}\left(RID \oplus TID, N'_S \oplus K\right); \mathrm{Rot}(K \oplus TID, RID \oplus K); K \oplus N'_S\}$ | $\xleftarrow{\{M_3\}}$ | | | |
| | $\xrightarrow{\{M_4\}}$ | $R_S = N'_S \oplus K_{SR}$ and $wt(K \oplus TID)$ and verifies the received token from the server and computes $M_5 : \{TID \oplus R_R; N''_S = R_S \oplus K_{RT}\}$ | | |
| | | | $\xrightarrow{\{M_5\}}$ | $R_S = N''_S \oplus K_{RT}$ and verifies the received token. Updates the session number $K$ as $K_{new} = \mathrm{Cro}\left(N_R \oplus N_R \oplus N_T, K\right)$ and computes $M_6 : \{\mathrm{Cro}\,(TID, K_{new} \oplus RID)\}$ |
| | | Verifies the received $\mathrm{Cro}\,(TID, K_{new} \oplus RID)$ to authenticate the tag and also update $K$ to $K_{new}$. It then computes $M_7 : \{\mathrm{Cro}\,(TID, K_{new} \oplus RID)\}$ | $\xleftarrow{\{M_6\}}$ | |
| Verifies the received $\mathrm{Cro}\,(TID, K_{new} \oplus RID)$ to authenticate the tag and also update $K$ to $K_{new}$. It computes $M_8 : \{K_{\text{new}} \oplus R_T \oplus R_R\}$ | $\xleftarrow{\{M_7\}}$ | | | |
| | $\xrightarrow{\{M_8\}}$ | Verifies the received token and computes $M_9 : \{K_{new} \oplus R_T \oplus N_R\}$ | | |
| | | | $\xrightarrow{\{M_9\}}$ | Verifies the received token to make sure that $K$ is synchronized and sets $Mark = 01$ and computes $M_{10} : \{Mark \oplus R_S\}$ |
| | | The reader also forwards the received message to the server as $M_{11} : \{Mark \oplus R_S\}$. | $\xleftarrow{\{M_{10}\}}$ | |
| Verifies $Mark = 01$ to store a new record $\{\mathrm{Cro}\,(RID \oplus TID, K_{\text{new}}),\ \mathrm{Rot}\,(K_{\text{new}} \oplus TID, K_{\text{new}} \oplus RID)\}$ in its index table IDT. | $\xleftarrow{\{M_{11}\}}$ | | | |
| | | | | Sets $Mark = 10$ after receiving a notification that indicates the authentication has been accomplished successfully. |

FIGURE 4: KUAJB authentication scheme proposed by [8]

Because the attacker knows $\gamma_L$ in both cases, the value of $ID \oplus K$ will almost certainly leak, indicating a secret disclosure attack with the success probability of "1" and also the complexity of three runs of the protocol.

### B. CRYPTANALYSIS OF KUAJB

The designer of KUAJB claimed security against various attacks and verified its security formally and informally. However, in this section, we show that this protocol has important security flaws, by proposing an efficient secret disclosure attack. Recall from subsection IV-B all communications take place over public channels and are accessible by the adversary. Hence, we can assume the adversary has access to all transferred messages, i.e. $M_1, \ldots, M_{11}$, where:

$$\begin{aligned}
M_1 &: \{N'_R = R_R \oplus K_{RT}\} \\
M_2 &: \{N'_T = R_T \oplus K_{RT}\} \\
M_3 &: \{N''_R = R_R \oplus K_{SR}, N''_T = R_T \oplus K_{SR}; \\
&\quad \mathrm{Cro}(RID \oplus TID, K)\} \\
M_4 &: \{N'_S = R_S \oplus K_{SR}; \mathrm{Cro}\,(RID \oplus TID, N'_S \oplus K)\,; \\
&\quad \mathrm{Rot}(K \oplus TID, RID \oplus K); K \oplus N'_S\} \\
M_5 &: \{TID \oplus R_R; N''_S = R_S \oplus K_{RT}\} \\
M_6 &: \{\mathrm{Cro}\,(TID, K_{new} \oplus RID)\} \\
M_7 &: \{\mathrm{Cro}\,(TID, K_{new} \oplus RID)\} \\
M_8 &: \{K_{\text{new}} \oplus R_T \oplus R_R\} \\
M_9 &: \{K_{new} \oplus R_T \oplus N_R\} \\
M_{10} &: \{Mark \oplus R_S\} \\
M_{11} &: \{Mark \oplus R_S\}
\end{aligned}$$

Now, let the adversary to do the following computations, given $M_1$, $M_2$ and $M_8$:

$$\begin{aligned} M_1 \oplus M_2 \oplus M_8 &= N'_R \oplus N'_T \oplus K_{\text{new}} \oplus R_T \oplus R_R \\ &= R_R \oplus K_{RT} \oplus R_T \oplus K_{RT} \oplus K_{\text{new}} \\ &\quad \oplus R_T \oplus R_R \\ &= K_{\text{new}} \end{aligned}$$

which is expected to be a secret parameter. In addition, $M_{10} : \{Mark \oplus R_S\}$ and it is clear to the adversary that $Mark = 01$ in this stage. Hence:

$$01 \oplus \ Mark \oplus R_S = 01 \oplus 01 \oplus R_S = R_S$$

On the other hand, $M_5 : \{TID \oplus R_R; N''_S = R_S \oplus K_{RT}\}$ and given $R_S$ the adversary can extract $K_{RT}$ as:

$$N''_S \oplus R_S = R_S \oplus K_{RT} \oplus R_S = K_{RT}$$

Similarly, the adversary also can extract the following secret parameters:

$$\begin{aligned} M_1 &\rightarrow N'_R \oplus K_{RT} = R_R \\ M_2 &\rightarrow N'_T \oplus K_{RT} = R_T \\ M_3 &\rightarrow N''_R \oplus R_R = K_{SR} \\ M_5 &\rightarrow TID \oplus R_R \oplus R_R = TID \end{aligned}$$

Following the description of $Cor(x, y)$ form [40], given $Cro(x, y)$ and $y$ it is possible to determine $x$. Hence, the adversary can also extract $RID$, the only remain parameter, from $M_6$ : $\{\text{Cro}\,(TID, K_{new} \oplus RID)\}$ for instance. Even if we consider $Cro(x, y)$ as a random function, then any malicious tag has access to $RID$. Hence the protocol also suffers from an insider attack, despite the designer's claim.

## VI. IMPROVED PROTOCOL

This section provides a brief overview of the proposed protocol. The proposed protocol same as its predecessor is divided into two phases: initialization and authentication. It worth noting that in order to keep the proposed protocol lightweight, instead of normal hash functions, we have used Quark hash function [9]. Quark is a lightweight hash function designed based on the sponge construction and has a multitude of types such as D-QUARK, U-QUARK, and S-QUARK. Compared to the D-QUARK and the S-QUARK, the U-QUARK is lighter than the S-QUARK and D-QUARK. Therefore, we used the U-QUARK hash function in the proposed protocol structure.

### A. INITIALIZATION PHASE

This phase shares some initial values between legitimate entities that will be used later in the authentication phase. The system administrator $SA$ performs the following actions:

1) In each tag, $SA$ stores a unique identity $ID$, secret keys $K, K'$, and an index pseudonym $IDS$.
2) $SA$ saves $ID$, $K'$, $IDS_{new}$, and $IDS_{old}$ in the server for each tag. We start with $IDS_{new} = Null$ and $IDS_{old} = IDS$.
3) $SA$ stores a counter value $Count = 0$ in each reader.

### B. AUTHENTICATION PHASE

During the authentication phase, following Figure 5, the improved protocol performs the following steps:

1) step 1: $\mathcal{R} \rightarrow \mathcal{BS} : \{Hello\}$: The reader sends a hello to the server.
2) step 2: $\mathcal{BS} \rightarrow \mathcal{R} : \{R_1\}$: The server generates and sends a random value $R_1$ to the reader.
3) step 3: $\mathcal{R} \rightarrow \mathcal{T} : \{Hello, R_1\}$: The reader sends a hello along $R_1$ to the tag.
4) step 4: $\mathcal{T} \rightarrow \mathcal{R} : \{R_2, \alpha, IDS\}$: After receiving $\{Hello, R_1\}$ messages, the tag generates another random value $R_2$, computes $\alpha = H(R_2 \oplus K \| ID \oplus R1)$ and sends $(R_2, \alpha, IDS)$ to the reader.
5) step 5: $\mathcal{R} \rightarrow \mathcal{BS} : \{R_2, \alpha, IDS\}$: The reader sends the received message to the server.
6) step 6: $\mathcal{BS} \rightarrow \mathcal{T} : \{\beta'\}$: Based on the received $IDS$, the server retrieves $ID$ and $(K, K')$ from its database and performs the following actions:
   a) Determines whether $\alpha \overset{?}{=} H(R_2 \oplus K \| ID \oplus R1)$to authenticate the tag.
   b) If the tag has been authenticated, the server computes $\beta = H(R_2 \| K \| ID \| R_1)$ and sends through the reader to the tag. Then it updates the tag's indexes as $IDS_{old} = IDS$ and $IDS_{new} = H(IDS \| R_2 \| R_1 \| K')$.
7) Tag verification. The tag does the following to authenticate the server:
   a) Verifies whether $\beta \overset{?}{=} H(R_2 \| K \| ID \| R_1)$to authenticate the server.
   b) If the server has been authenticated, the tag updates its index as $IDS = H(IDS \| R_2 \| R_1 \| K')$.

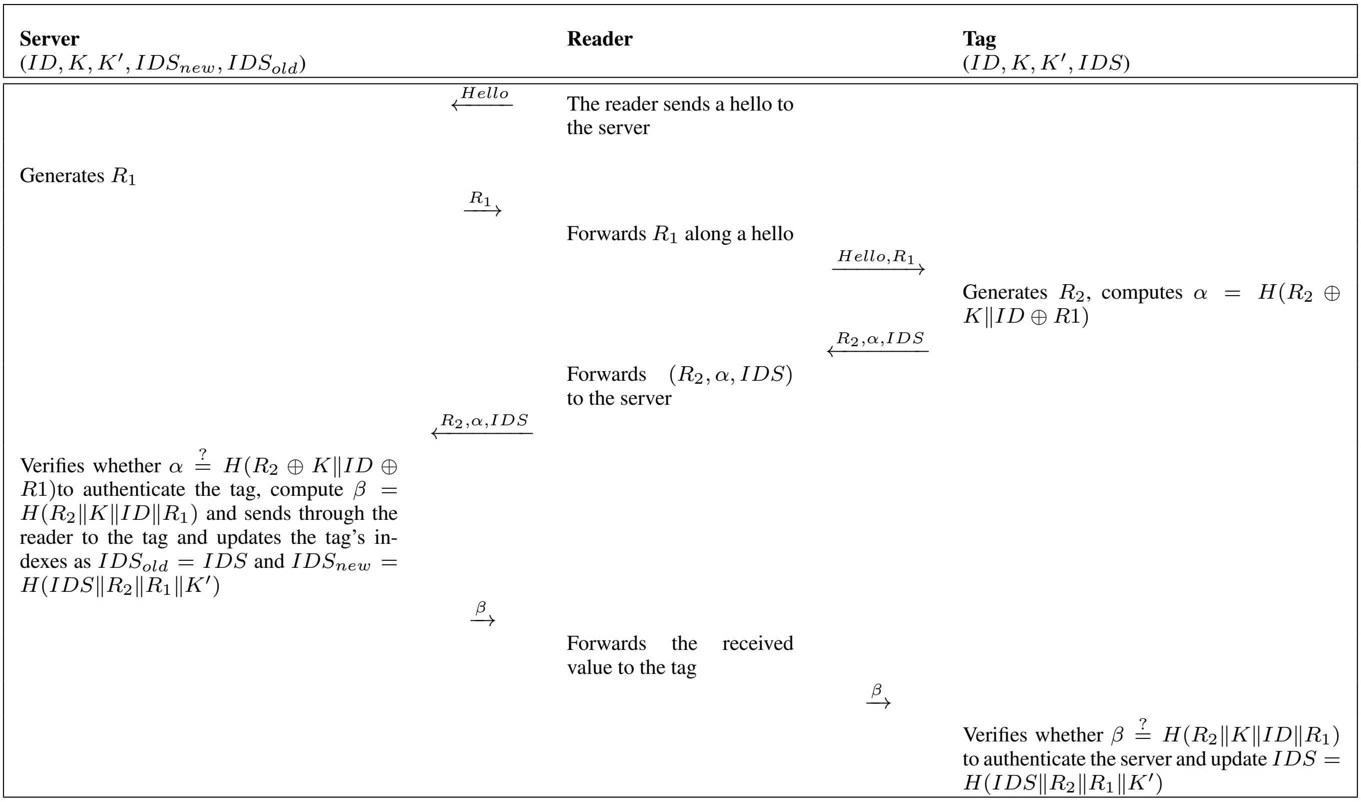
## VII. SECURITY ANALYSIS OF THE IMPROVED PROTOCOL

### A. FORMAL SECURITY ANALYSIS

We evaluated the proposed protocol's security from a formal viewpoint. Numerous formal methods for evaluating the reliability of a cryptographic protocol have already been developed. GNY logic and BAN logic are examples of manual processes, while Scyther and ProVerif are examples of automated methods. Scyther and ProVeirf were chosen from among them to formally simulate the suggested scheme and validate its protection.

#### 1) Through Scyther

This section gives formal security confirmation of our protocol using the Scyther tool, which is widely used. It is a verification tool that is used to formally evaluate security schemes, security requirements, and security flaws. Scyther's adversary model is predetermined and based on the Dolev-Yao model. Scyther ensures that the suggested protocol's



**Server** $(ID, K, K', IDS_{new}, IDS_{old})$

**Reader**

**Tag** $(ID, K, K', IDS)$

$\xleftarrow{Hello}$ The reader sends a hello to the server

Generates $R_1$

$\xrightarrow{R_1}$ Forwards $R_1$ along a hello

$\xrightarrow{Hello, R_1}$ Generates $R_2$, computes $\alpha = H(R_2 \oplus K \| ID \oplus R1)$

$\xleftarrow{R_2, \alpha, IDS}$ Forwards $(R_2, \alpha, IDS)$ to the server

$\xleftarrow{R_2, \alpha, IDS}$

Verifies whether $\alpha \overset{?}{=} H(R_2 \oplus K \| ID \oplus R1)$to authenticate the tag, compute $\beta = H(R_2 \| K \| ID \| R_1)$ and sends through the reader to the tag and updates the tag's indexes as $IDS_{old} = IDS$ and $IDS_{new} = H(IDS \| R_2 \| R_1 \| K')$

$\xrightarrow{\beta}$ Forwards the received value to the tag

$\xrightarrow{\beta}$

Verifies whether $\beta \overset{?}{=} H(R_2 \| K \| ID \| R_1)$ to authenticate the server and update $IDS = H(IDS \| R_2 \| R_1 \| K')$

FIGURE 5: Proposed scheme

secret information is safe from the adversary during protocol execution. Compared to other simulation tools such as AVISPA, ProVerif, and others, the Scyther simulation is now very prevalent for authentication protocols. The AVISPA tool includes a role-based language called HLPSL, which, after execution, shows whether the protocol is secure or not. If it is secure, it indicates the protocol is resistant to man-in-the-middle and replay attacks. Other security threats are not taken into account, e.g. password guessing. It is normal for an intruder to find security assaults extremely difficult if sensitive and critical data cannot be found during protocol execution or from the protocol explanation. We established three basic functions in the Scyther tool for security verification of the proposed protocol: Tag, server, and reader.

Security verification results show that the suggested scheme is secure, and Figure 6 confirms this validation. Figure 7 also shows our implementation codes in SPDL. It worth noting that in this paper we use the compromise-0.9.2 version of Scyther, while the v1.1.3 version has the same verification result as well and Table 4 shows the security claims of the Scyther tool.

#### 2) Through ProVerif

ProVerif is a software application that allows for automated reasoning about the security features of cryptographic protocols. It is capable of validating security aspects like authentication, process equivalency, and confidentiality. The program has been used to examine the implementations of cryptographic protocols such as the Transport Layer Security (TLS) protocol. ProVerif can prove various security features for an unbounded message space and an infinite number of sessions by supporting a wide range of cryptographic primitives. ProVerif was used to simulate and test the security of the suggested authentication strategy, and the results in Figure 10 also shows a security flaw of the [7]'s protocol. It is worth noting that Figure 9 demonstrates that our proposed scheme is secure and efficient against a wide range of attacks, which is an important aspect for authentication protocols.

### B. STRUCTURAL CRYPT-ANALYSIS

Ahmadian et al. [44] proposed two structural crypt-analysis methods: RLC (Recursive Linear Cryptanalysis) and RDC (Recursive Differential Cryptanalysis).

**RDC:** In RDC, the adversary efforts to learn secret variables by manipulating and gaining responses for cipher texts over multiple sessions. It operates on the principle of calculating linear equations between public value differences. In our protocol, however, each session authentication includes an independently generated random nonce. Even if the adversary obtains responses from the tag for different sessions, the randomness introduced by the nonces prevents them from deducing linear relationships between the sessions' outputs.

**RLC:** The RLC primarily uses the T-function's intrinsic weak diffusion properties to try to construct a linear matrix

TABLE 4: Scyther tool security claims

| Claims | Description |
|---|---|
| $Secrecy$ | Secrecy implies that no particular confidential data is made available to the adversary and that, even if it is conveyed across an insecure channel, there are many degrees of secrecy with discernible limits. |
| $Aliveness$ | According to the description, the targeted communication partner has really carried out an incident anytime a person meets a role description up until the claim incident and feels he is communicating with a trustworthy agent. |
| $Weakagree$ | In order to prevent one of the communication partners from being generated by the attacker, the communication partners must certify that they are interacting with one another. |
| $Nisynch$ | According to [43], non-injective synchronization means that roles carry out receiving and transmitting events in the prescribed order and with the relevant primary content. |
| $Niagree$ | Non-injective consensus on messages, according to [43], signifies that the sender and receiver agree on the private values transmitted, and the findings of the study corroborate this assumption. |

of known and unknown variables, then solves the matrix to obtain the unknown parameters. Nevertheless, RLC will not be useful in the proposed scheme because we utilize non-T functions (Clock) in our message architecture, which prohibits attackers from computing the linear matrix.

## C. INFORMAL SECURITY ANALYSIS

### 1) Mutual authentication

Mutual authentication is a crucial characteristic in verification schemes that transmit sensitive data to ensure data security. It is also important in RFID systems to ensure security and privacy, and security protocols can be developed to offer reader authentication to tags. In the proposed authentication scheme, mutual authentication occurs between the valid tag and the server, as well as vice versa. The server authenticates the valid tag by making comparisons between the received $\alpha$ and the locally computed one, while the valid tag similarly verifies the server by comparing the $\beta$ with the computed version. As a result, both the valid tag and the server must verify each other.

### 2) Confidentiality

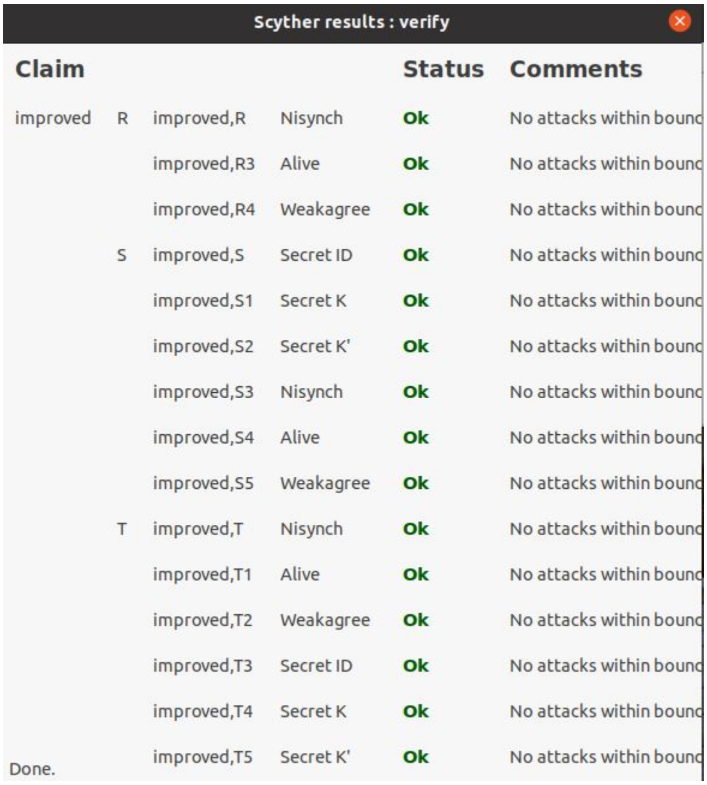
Various authentication techniques have been proposed to ensure the security of RFID systems, including schemes that use pseudo-random number generators (PRNG) and cryptographic algorithms to protect the secret information stored inside the tags and ensure confidentiality, integrity, and authentication. These schemes are designed to resist common types of attacks on RFID tags, such as unauthorized disabling, cloning, and tracking, and to ensure the privacy and security of the system. Some proposed schemes use one-way hash operations, bit-wise exclusive-OR operations, and synchronized shared secrets to achieve mutual authentication and resist known attacks. These schemes have been proposed for various applications, including medical environments, where the security and privacy of patient information are critical. In the proposed protocol, the transferred values over the public channel are $IDS$,$R_1$, $\alpha = H(R_2 \oplus K \| ID \oplus R1)$, $R_2$ and $\beta = H(R_2 \| K \| ID \| R_1)$ and the secrets are $(ID, K, K')$. The adversary has no chance to determine those values without converting the has function, which is infeasible.

### 3) Tag location privacy

RFID systems are prone to a variety of security concerns, such as passive eavesdropping, active interference, unauthorized tracking, and others. As a result, a secure RFID system should enable mutual authentication while also preventing unwanted tracking. Cryptographic algorithms and secret key management are at the heart of the proposed approaches for secure RFID authentication. If the exchanged messages remain static during each authentication session, a malicious user can use unauthorized readers to follow the tag's location. However, in the proposed authentication technique, the response message calculated by the tag consists of a pseudo-random number generated in each authentication process by the genuine tag and a valid reader, exclude $IDS$ which is updated after each successful session. As a result, an adversary cannot determine the location of the tags even if they eavesdrop on the channel and collect data transferred between the tag and the reader.

### 4) De-synchronization attack

To prevent de-synchronization attacks, the suggested authentication method keeps two pseudonyms for each tag on the server: $IDS_{old}$, which is a record from a previously finished authentication session, and $IDS_{new}$, which is utilized in the current session. If an attacker intercepts or modifies the delivered messages, the server matches the $IDS$ supplied by the tag to its previously saved $IDS_{new}$ throughout the next authentication session. If the $IDS$ is not identical to $IDS_{new}$ owing to a prior authentication session that was not completed, the server checks it against the prior pseudonym, $IDS_{old}$, and proceeds with the authentication process.



Scyther results : verify

| Claim | | | | Status | Comments |
|---|---|---|---|---|---|
| improved | R | improved,R | Nisynch | Ok | No attacks within bound |
| | | improved,R3 | Alive | Ok | No attacks within bound |
| | | improved,R4 | Weakagree | Ok | No attacks within bound |
| | S | improved,S | Secret ID | Ok | No attacks within bound |
| | | improved,S1 | Secret K | Ok | No attacks within bound |
| | | improved,S2 | Secret K' | Ok | No attacks within bound |
| | | improved,S3 | Nisynch | Ok | No attacks within bound |
| | | improved,S4 | Alive | Ok | No attacks within bound |
| | | improved,S5 | Weakagree | Ok | No attacks within bound |
| | T | improved,T | Nisynch | Ok | No attacks within bound |
| | | improved,T1 | Alive | Ok | No attacks within bound |
| | | improved,T2 | Weakagree | Ok | No attacks within bound |
| | | improved,T3 | Secret ID | Ok | No attacks within bound |
| | | improved,T4 | Secret K | Ok | No attacks within bound |
| | | improved,T5 | Secret K' | Ok | No attacks within bound |

Done.

FIGURE 6: The security verification results of improved authentication scheme through compromise-0.9.2 version of Scyther tool

#### 5) Impersonation attack

RFID authentication systems attempt to increase security by preventing timing attacks and delivering low-cost solutions. An attacker eavesdropping on a session in which a tag generates a response message using random numbers $R_1$, $R_2$ and the tag's identification number $ID$ would be unable to spoof the tag using $\alpha$ and $\beta$ because each authentication session uses unique random numbers.

#### 6) Replay attack

Replay attacks occur when an attacker intercepts certain authentication communications between the tag and the reader and then replays these messages in an authentication session in order to authenticate as a genuine tag. The proposed authentication method, on the other hand, is resistant to replay attacks because it uses one-time pad random numbers and checks data before transmission, making it impossible for an attacker to use the same information to authenticate a tag as genuine.

#### 7) Man In the Middle (MITM) attack

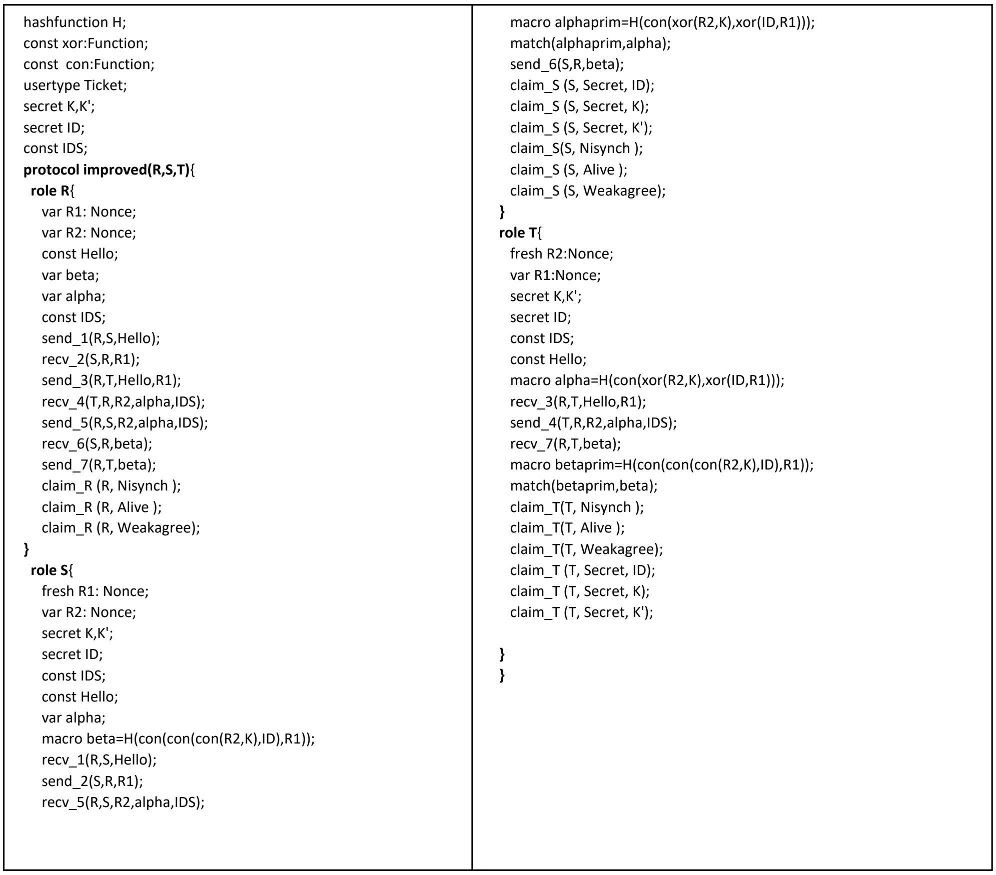
MITM attacks attempt to evade mutual authentication and are only successful if the attacker impersonates each endpoint effectively enough to satisfy authentication. Secure cryptographic systems provide some sort of message authentication, commonly employing key-agreement protocols, and have been created to authenticate the certificate authority (CA). Given that both the tag and the server contribute to the computed responses, $\alpha = H(R_2 \oplus K\|ID \oplus R1)$ and $\beta = H(R_2\|K\|ID\|R_1)$, a MITM adversary has no chance to do impersonation without the knowledge of $ID, K$ or $K'$ in practice.

### D. VHDL IMPLEMENTATION

VHSIC Hardware Description Language (VHDL) is a powerful language used for simulating and representing the architecture and functionality of digital systems. Designers can utilize VHDL to represent digital systems at various levels of abstraction, ranging from high-level system behavior to low-level implementation details such as logic gates. VHDL serves as a valuable tool for digital design verification, documentation, and design entry. It enables designers to accurately describe the behavior and structure of complex digital systems, facilitating the design process and allowing for extensive testing and analysis. In our work, we have simulated the QUARK hash function as a fundamental component of our proposed authentication scheme. Simulation results obtained using the ModelSim application, as depicted in Figures  11 and  12, demonstrate the effectiveness and feasibility of this hash function.

## VIII. PERFORMANCE ANALYSIS

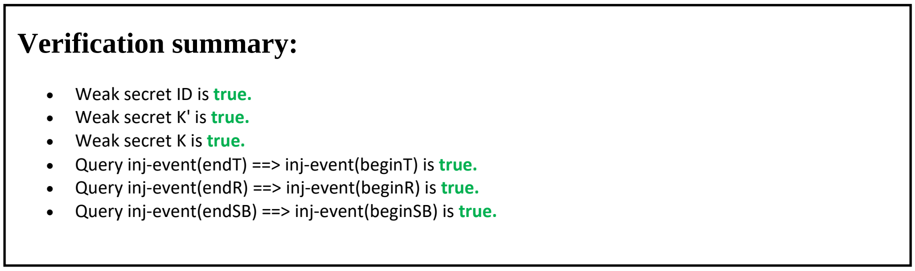
The suggested authentication technique was compared to other systems in terms of security and functionality aspects,



```
hashfunction H;
const xor:Function;
const  con:Function;
usertype Ticket;
secret K,K';
secret ID;
const IDS;
protocol improved(R,S,T){
 role R{
   var R1: Nonce;
   var R2: Nonce;
   const Hello;
   var beta;
   var alpha;
   const IDS;
   send_1(R,S,Hello);
   recv_2(S,R,R1);
   send_3(R,T,Hello,R1);
   recv_4(T,R,R2,alpha,IDS);
   send_5(R,S,R2,alpha,IDS);
   recv_6(S,R,beta);
   send_7(R,T,beta);
   claim_R (R, Nisynch );
   claim_R (R, Alive );
   claim_R (R, Weakagree);
}
 role S{
   fresh R1: Nonce;
   var R2: Nonce;
   secret K,K';
   secret ID;
   const IDS;
   const Hello;
   var alpha;
   macro beta=H(con(con(con(R2,K),ID),R1));
   recv_1(R,S,Hello);
   send_2(S,R,R1);
   recv_5(R,S,R2,alpha,IDS);
   macro alphaprim=H(con(xor(R2,K),xor(ID,R1)));
   match(alphaprim,alpha);
   send_6(S,R,beta);
   claim_S (S, Secret, ID);
   claim_S (S, Secret, K);
   claim_S (S, Secret, K');
   claim_S(S, Nisynch );
   claim_S (S, Alive );
   claim_S (S, Weakagree);
 }
 role T{
   fresh R2:Nonce;
   var R1:Nonce;
   secret K,K';
   secret ID;
   const IDS;
   const Hello;
   macro alpha=H(con(xor(R2,K),xor(ID,R1)));
   recv_3(R,T,Hello,R1);
   send_4(T,R,R2,alpha,IDS);
   recv_7(R,T,beta);
   macro betaprim=H(con(con(con(R2,K),ID),R1));
   match(betaprim,beta);
   claim_T(T, Nisynch );
   claim_T(T, Alive );
   claim_T(T, Weakagree);
   claim_T (T, Secret, ID);
   claim_T (T, Secret, K);
   claim_T (T, Secret, K');

 }
 }
```

FIGURE 7: SPDL implementation of our proposed scheme



**Verification summary:**

- Weak secret ID is **true.**
- Weak secret K' is **true.**
- Weak secret K is **true.**
- Query inj-event(endT) ==> inj-event(beginT) is **true.**
- Query inj-event(endR) ==> inj-event(beginR) is **true.**
- Query inj-event(endSB) ==> inj-event(beginSB) is **true.**

FIGURE 8: The security verification outcome of the proposed system using the Proverif tool

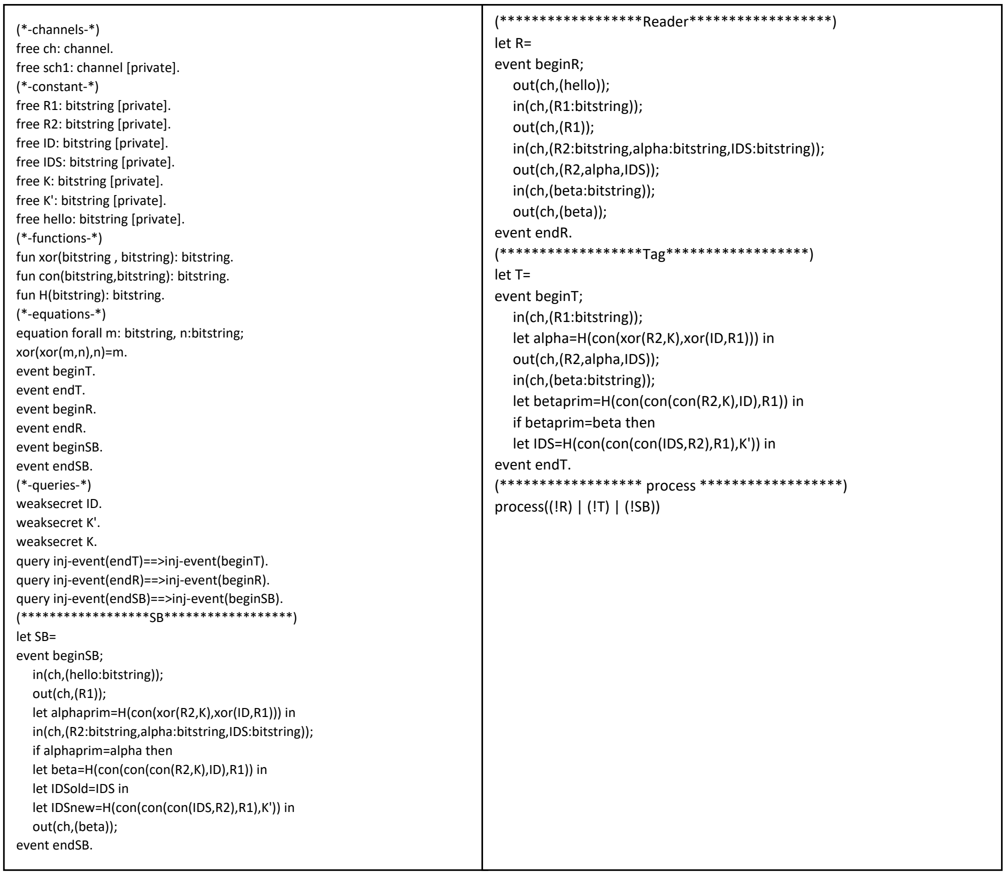
computation and communication costs [[45, 46, 47, 7]]. According to the performance evaluation, the suggested authentication technique increases the efficiency and security of RFID communication networks. Other studies compared the functionality, computational cost, and communication cost of proposed authentication approaches to those of other comparable state-of-the-art schemes. Tools such as E3C have been proposed for quantifying the computing and transmission costs of authentication and key exchange protocols.

### A. SECURITY COMPARISON

The proposed authentication scheme was compared to recent protocols in terms of security requirements, and Table 5 summarizes the security properties of the proposed scheme and protocols from the literature [[45, 46, 47, 48, 7]]. The linked methods were discovered to have numerous security weaknesses against various security attacks such as impersonation, disclosure, and de-synchronization. Other research has shown security issues in password-based remote user authentication techniques using smart cards.

### B. COMPUTATIONAL COST COMPARISON

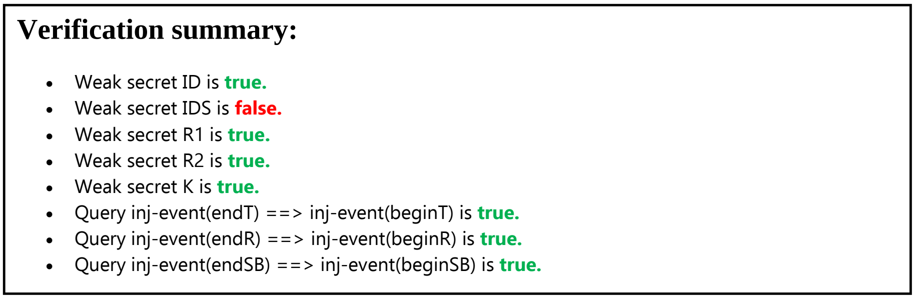
In Table 6, the computational cost of the proposed authentication scheme was determined and compared to various protocols [[45, 46, 47, 7, 48]]. It is important to mention that the execution time of the rotation operation, permutation



```
(*-channels-*)
free ch: channel.
free sch1: channel [private].
(*-constant-*)
free R1: bitstring [private].
free R2: bitstring [private].
free ID: bitstring [private].
free IDS: bitstring [private].
free K: bitstring [private].
free K': bitstring [private].
free hello: bitstring [private].
(*-functions-*)
fun xor(bitstring , bitstring): bitstring.
fun con(bitstring,bitstring): bitstring.
fun H(bitstring): bitstring.
(*-equations-*)
equation forall m: bitstring, n:bitstring;
xor(xor(m,n),n)=m.
event beginT.
event endT.
event beginR.
event endR.
event beginSB.
event endSB.
(*-queries-*)
weaksecret ID.
weaksecret K'.
weaksecret K.
query inj-event(endT)==>inj-event(beginT).
query inj-event(endR)==>inj-event(beginR).
query inj-event(endSB)==>inj-event(beginSB).
(*****************SB*****************)
let SB=
event beginSB;
   in(ch,(hello:bitstring));
   out(ch,(R1));
   let alphaprim=H(con(xor(R2,K),xor(ID,R1))) in
   in(ch,(R2:bitstring,alpha:bitstring,IDS:bitstring));
   if alphaprim=alpha then
   let beta=H(con(con(con(R2,K),ID),R1)) in
   let IDSold=IDS in
   let IDSnew=H(con(con(con(IDS,R2),R1),K')) in
   out(ch,(beta));
event endSB.
```

```
(*****************Reader*****************)
let R=
event beginR;
   out(ch,(hello));
   in(ch,(R1:bitstring));
   out(ch,(R1));
   in(ch,(R2:bitstring,alpha:bitstring,IDS:bitstring));
   out(ch,(R2,alpha,IDS));
   in(ch,(beta:bitstring));
   out(ch,(beta));
event endR.
(*****************Tag*****************)
let T=
event beginT;
   in(ch,(R1:bitstring));
   let alpha=H(con(xor(R2,K),xor(ID,R1))) in
   out(ch,(R2,alpha,IDS));
   in(ch,(beta:bitstring));
   let betaprim=H(con(con(con(R2,K),ID),R1)) in
   if betaprim=beta then
   let IDS=H(con(con(con(IDS,R2),R1),K')) in
event endT.
(***************** process *****************)
process((!R) | (!T) | (!SB))
```

FIGURE 9: ProVerif implementation code of the improved protocol



**Verification summary:**

- Weak secret ID is **true.**
- Weak secret IDS is **false.**
- Weak secret R1 is **true.**
- Weak secret R2 is **true.**
- Weak secret K is **true.**
- Query inj-event(endT) ==> inj-event(beginT) is **true.**
- Query inj-event(endR) ==> inj-event(beginR) is **true.**
- Query inj-event(endSB) ==> inj-event(beginSB) is **true.**

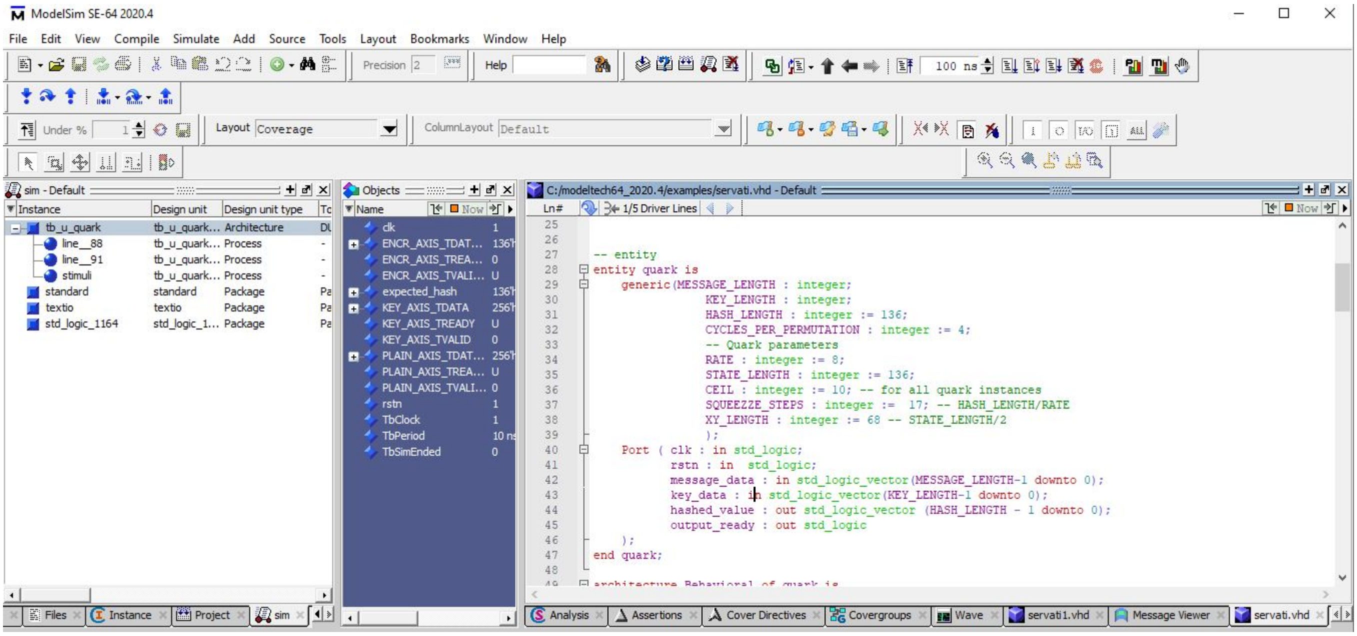
FIGURE 10: The security verification results of URASP through ProVeirf tool

operation, and Cross operation, denoted as $T_{Rot}$, $T_{Per}$, and $T_{Cro}$ respectively, are very small and can be disregarded. These operations are defined in [7] and [8] protocols.

[9] recommended the QUARK hash function for RFID infrastructure owing to its high performance and inexpensive cost. To keep the protocol lightweight, the suggested protocol uses the U-QUARK hash function instead of standard hash functions. The U-QUARK hash function was lighter than the D-QUARK and S-QUARK, according to [9]. The hash function ($T_h$) took 0.5ms to complete, but the encryption and decryption procedure ($T_{E/D}$) took 8.7ms. The Quark hash took 0.002892 ms to complete. As demonstrated in Table 6, the suggested authentication system outperforms competing protocols. Table 6 demonstrates that the proposed protocol has a significantly lower execution time compared to other designs that employ conventional hash functions, owing to the utilization of Quark lightweight hash function.

### C. COMMUNICATION COSTS COMPARISON

In Table 7 and Figure 13 the communication costs of the proposed authentication technique and other current schemes were estimated and compared. The suggested authentication technique is less expensive in terms of communication than comparable protocols. Each scheme's communication cost was calculated using a 160-bit identity, a 160-bit secret key, a 32-bit timestamp, and 64-bit random numbers. The hash


ModelSim SE-64 2020.4
File Edit View Compile Simulate Add Source Tools Layout Bookmarks Window Help
sim - Default
Objects
C:/modeltech64_2020.4/examples/servati.vhd - Default
Analysis
Assertions
Cover Directives
Covergroups
Wave
servati1.vhd
Message Viewer
servati.vhd

| Instance | Design unit | Design unit type |
|---|---|---|
| tb_u_quark | tb_u_quark... | Architecture |
| line__88 | tb_u_quark... | Process |
| line__91 | tb_u_quark... | Process |
| stimuli | tb_u_quark... | Process |
| standard | standard | Package |
| textio | textio | Package |
| std_logic_1164 | std_logic_1... | Package |

```
-- entity
entity quark is
    generic(MESSAGE_LENGTH : integer;
                KEY_LENGTH : integer;
                HASH_LENGTH : integer := 136;
                CYCLES_PER_PERMUTATION : integer := 4;
                -- Quark parameters
                RATE : integer := 8;
                STATE_LENGTH : integer := 136;
                CEIL : integer := 10; -- for all quark instances
                SQUEEZZE_STEPS : integer :=  17; -- HASH_LENGTH/RATE
                XY_LENGTH : integer := 68 -- STATE_LENGTH/2
                );
    Port ( clk : in std_logic;
            rstn : in  std_logic;
            message_data : in std_logic_vector(MESSAGE_LENGTH-1 downto 0);
            key_data : in std_logic_vector(KEY_LENGTH-1 downto 0);
            hashed_value : out std_logic_vector (HASH_LENGTH - 1 downto 0);
            output_ready : out std_logic
    );
end quark;
```

FIGURE 11: Implementation of Quark hash function in VHDL

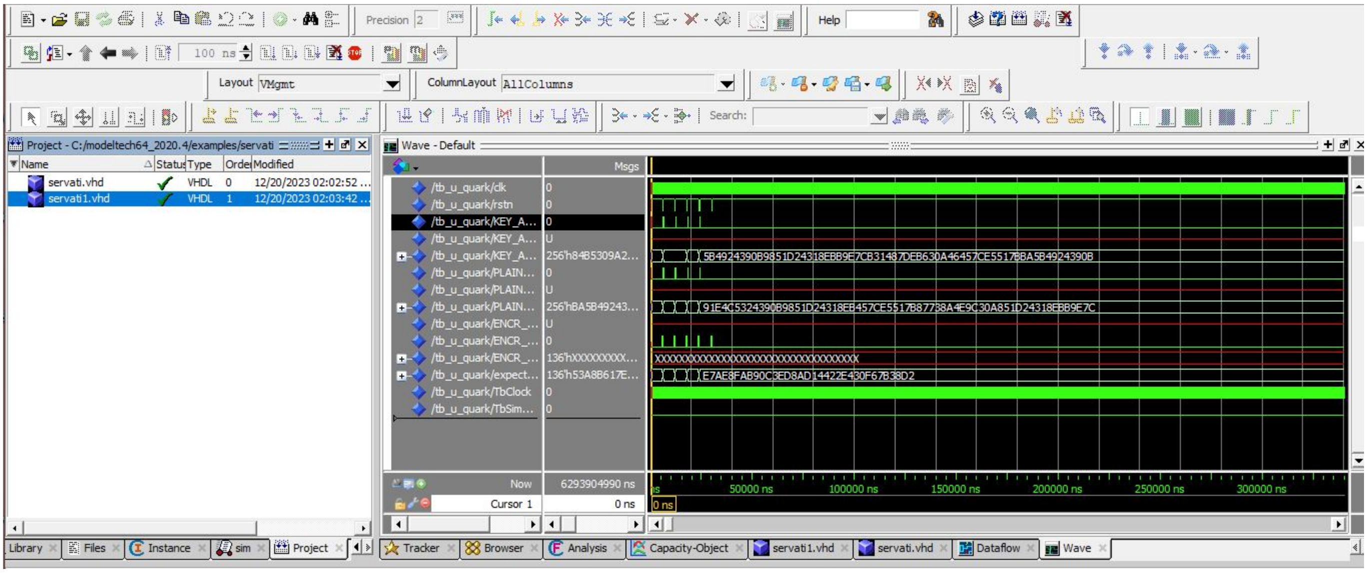

Project - C:/modeltech64_2020.4/examples/servati
Wave - Default
servati.vhd VHDL 0 12/20/2023 02:02:52
servati1.vhd VHDL 1 12/20/2023 02:03:42
/tb_u_quark/clk
/tb_u_quark/rstn
/tb_u_quark/KEY_A...
/tb_u_quark/PLAIN...
/tb_u_quark/ENCR_...
/tb_u_quark/expect...
/tb_u_quark/TbClock
/tb_u_quark/TbSim...
5B4924390B9851D24318EBB9E7CB31487DEB630A46457CE5517BBA5B4924390B
91E4C5324390B9851D24318EB457CE5517B87738A4E9C30A851D24318EBB9E7C
E7AE8FAB90C3ED8AD14422E430F67B38D2
Now 6293904990 ns
Cursor 1 0 ns
50000 ns
100000 ns
150000 ns
200000 ns
250000 ns
300000 ns

FIGURE 12: Implementation results of QUARK hash function in VHDL

function's 160-bit message digest (SHA-1) and 256-bit symmetric cryptographic encryption and decryption (AES-256) were also employed. In [48],[7] and [8] protocols, since the exclusive-or value of the key and random number are sent in the insecure channel, the minimum bit length of the random number, secret keys, and pseudonym values is considered 160 bits. It should be noted that the designers of [7] and [8] protocols did not determine length of the parameters used in their protocol. As you can see in Table  7, the proposed protocol is in a good position in terms of the number of rounds and communication costs in comparison with recent similar protocols due to the complete security it provides.

The comparison of storage costs on the limited capacity side of the examined protocols is shown in Table 8 and Figure 14 which indicate that the storage expenses of the suggested protocol are reasonable when compared to other similar protocols.

## IX. CONCLUSION

Several ultra-lightweight authentication techniques have been proposed over the years; however, all of those protocols are insecure and are frequently prone to various attacks that include secret disclosure, de-synchronization, and impersonation. These techniques rely on limited bit-wise operations

TABLE 5: A comparison of the proposed authentication scheme's security with current comparable schemes

| Protocols | Year | $A_1$ | $A_2$ | $A_3$ | $A_4$ | $A_5$ | $A_6$ | $A_7$ | $A_8$ |
|---|---|---|---|---|---|---|---|---|---|
| [45] | 2018 | ✓ | ✓ | ✓ | ✓ | ✗ | ✓ | ✓ | ✓ |
| [46] | 2019 | ✗ | ✓ | ✗ | ✓ | ✓ | ✗ | ✗ | ✓ |
| [47] | 2019 | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✗ |
| [49] | 2019 | ✗ | ✗ | ✗ | ✓ | ✓ | ✗ | ✗ | ✗ |
| [48] | 2022 | ✗ | ✗ | ✓ | ✓ | ✓ | ✓ | ✓ | ✗ |
| [7] | 2021 | ✓ | ✗ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| [8] | 2023 | ✓ | ✗ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| Proposed scheme | | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |

$A_1$: Replay attack; $A_2$: Secret disclosure attack;
$A_3$: Tag anonymity contradiction attack; $A_4$: De-synchronization attack;
$A_5$: Data confidentiality contradiction attack; $A_6$: MITM attack
$A_7$: Impersonation attack; $A_8$: Privilege insider attacks

TABLE 6: Computational cost of the proposed protocol vs current comparable protocols (in milliseconds)

| Protocols | Overall cost | Operation Type | Execution cost |
|---|---|---|---|
| [45] | $8T_h$ | Standard Hash | $4ms$ |
| [46] | $8T_h + 2T_{E/D}$ | Standard Hash | $21.4ms$ |
| [47] | $29T_h$ | Standard Hash | $14.5ms$ |
| [49] | $36T_h$ | Standard Hash | $18ms$ |
| [48] | $9T_h$ | Standard Hash | $4.5ms$ |
| [7] | $8T_{Per} + 10T_{Rot}$ | Ultra lightweight | Negligible |
| [8] | $12T_{Cro} + 2T_{Rot}$ | Lightweight | Negligible |
| Proposed scheme | $6T_h$ | Lightweight QUARK Hash | $0.017352ms$ |

TABLE 7: Communication cost comparison of the suggested scheme with recent similar protocols

| Protocols | Total Communication Cost in bits | No. of Messages |
|---|---|---|
| [45] | 1536 | 5 |
| [46] | 2720 | 4 |
| [47] | 2208 | 4 |
| [49] | 3360 | 4 |
| [48] | 2560 | 4 |
| [7] | 1280 | 5 |
| [8] | 1760 | 11 |
| Proposed scheme | 1248 | 7 |

such as AND, OR, and XOR, which are insufficient to offer a fully robust security protocol. In this paper, we demonstrate how to use URASP and KUAJB protocols security flaws to launch a secret disclosure attack against them. Furthermore, we provide a new improved protocol that can withstand various security attacks by leveraging lightweight hash functions such as QUARK. Despite having higher computation and storage costs than URASP and KUAJB protocols, the improved protocol is more resistant to a variety of security risks.

## REFERENCES

[1] F. Zhu, P. Li, H. Xu, and R. Wang, "A novel lightweight authentication scheme for RFID-based healthcare systems," Sensors, vol. 20, no. 17, p. 4846, 2020.

[2] D. Henrici and P. Muller, "Hash-based enhancement of location privacy for radio-frequency identification devices using varying identifiers," in IEEE Annual Conference on Pervasive Computing and Communications Workshops, 2004. Proceedings of the Second, pp. 149–153, IEEE, 2004.

[3] J. Yang, J. Park, H. Lee, K. Ren, and K. Kim, "Mutual authentication protocol for low-cost RFID," in Workshop on RFID and lightweight crypto, pp. 17–24, WRLC, 2005.

[4] J. Daemen, S. Hoffert, M. Peeters, G. V. Assche, and R. V. Keer, "Xoodyak, a lightweight cryptographic scheme," IACR Trans. Symmetric Cryptol., vol. 2020, no. S1, pp. 60–87, 2020.

[5] M. Khalid, U. M. Khokhar, and M. Najam-ul-Islam, "Cryptanalysis of ultralightweight mutual authentica-

TABLE 8: Storage cost comparison of the suggested scheme with recent similar protocols

| Protocols | Constrained resource side's capacity in bits |
|---|---|
| [45] | 320 |
| [46] | 640 |
| [47] | 320 |
| [49] | 640 |
| [48] | 480 |
| [7] | 480 |
| [8] | 480 |
| Proposed scheme | 640 |

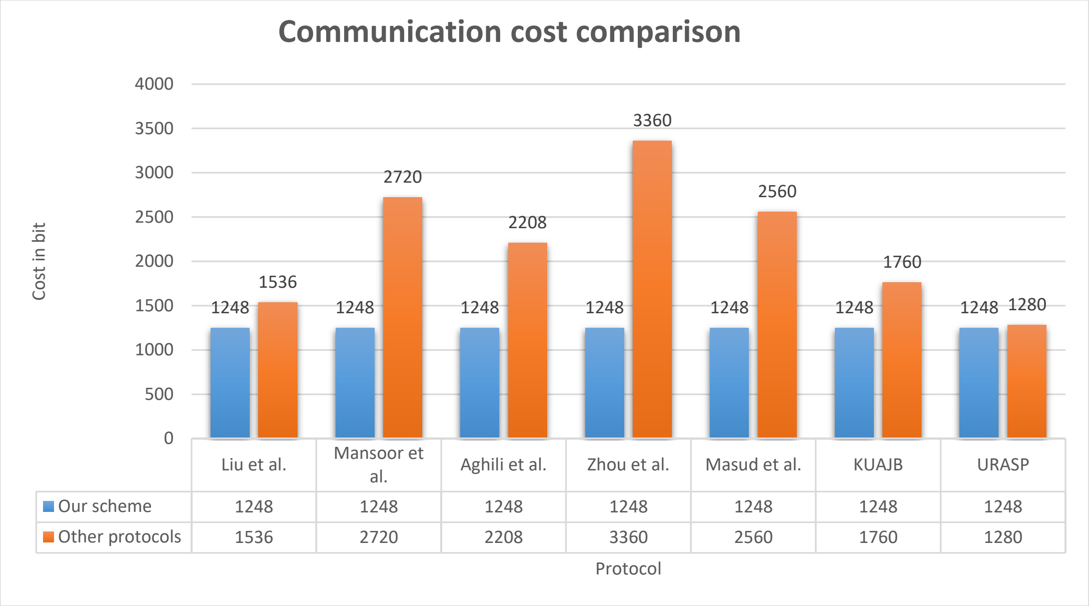


FIGURE 13: Communication cost of the proposed scheme with recent similar protocols

tion protocol for radio frequency identification enabled internet of things networks," Int. J. Distributed Sens. Networks, vol. 14, no. 8, 2018.

[6] L. Xie, Y. Yin, A. V. Vasilakos, and S. Lu, "Managing RFID data: challenges, opportunities and solutions," IEEE communications surveys & tutorials, vol. 16, no. 3, pp. 1294–1311, 2014.

[7] M. Shariq, K. Singh, P. K. Maurya, A. Ahmadian, and M. R. K. Ariffin, "URASP: an ultralightweight RFID authentication scheme using permutation operation," Peer-to-Peer Netw. Appl., vol. 14, no. 6, pp. 3737–3757, 2021.

[8] M. A. Khan, S. Ullah, T. Ahmad, K. Jawad, and A. Buriro, "Enhancing security and privacy in healthcare systems using a lightweight RFID protocol," Sensors, vol. 23, no. 12, p. 5518, 2023.

[9] J.-P. Aumasson, L. Henzen, W. Meier, and M. Naya-Plasencia, "Quark: a lightweight hash," Journal of cryptology, vol. 26, pp. 313–339, 2013.

[10] P. Kumar, S.-G. Lee, and H.-J. Lee, "E-sap: Efficient-strong authentication protocol for healthcare applications using wireless medical sensor networks," Sensors, vol. 12, no. 2, pp. 1625–1647, 2012.

[11] D. He, N. Kumar, J. Chen, C.-C. Lee, N. Chilamkurti, and S.-S. Yeo, "Robust anonymous authentication protocol for health-care applications using wireless medical sensor networks," Multimedia Systems, vol. 21, no. 1, pp. 49–60, 2015.

[12] X. Li, J. Niu, S. Kumari, J. Liao, W. Liang, and M. K. Khan, "A new authentication protocol for healthcare applications using wireless medical sensor networks with user anonymity," Security and Communication Networks, vol. 9, no. 15, pp. 2643–2655, 2016.

[13] F. Wu, L. Xu, S. Kumari, and X. Li, "An improved and anonymous two-factor authentication protocol for health-care applications with wireless medical sensor networks," Multimedia Systems, vol. 23, no. 2, pp. 195–205, 2017.

[14] A. Tewari and B. B. Gupta, "Cryptanalysis of a novel ultra-lightweight mutual authentication protocol for IoT

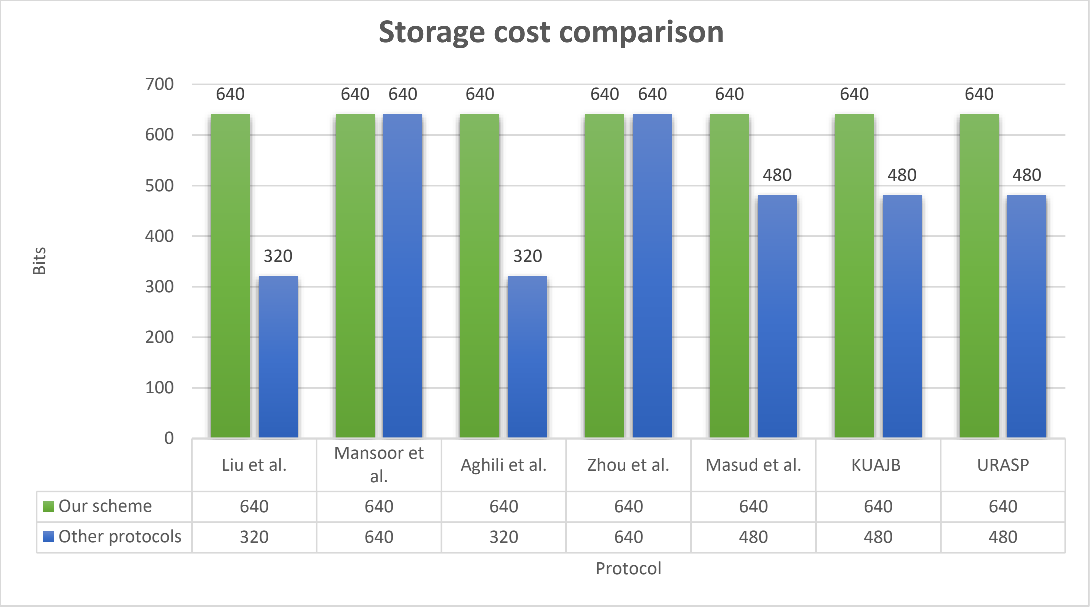


FIGURE 14: Storage cost of the proposed scheme with recent similar protocols

devices using RFID tags," The Journal of Supercomputing, vol. 73, no. 3, pp. 1085–1102, 2017.

[15] K.-H. Wang, C.-M. Chen, W. Fang, and T.-Y. Wu, "On the security of a new ultra-lightweight authentication protocol in IoT environment for RFID tags," The Journal of Supercomputing, vol. 74, no. 1, pp. 65–70, 2018.

[16] S. Huang, C. Tsai, and T. Hwang, "Comment on "cryptanalysis of a novel ultralightweight mutual authentication protocol for IoT devices using RFID tags"," in Proceedings of the 2018 International Conference on Data Science and Information Technology, DSIT 2018, Singapore, July 20-22, 2018, pp. 23–27, ACM, 2018.

[17] J. H. Khor and M. Sidorov, "Weakness of ultra-lightweight mutual authentication protocol for iot devices using RFlD tags," in 2018 Eighth International Conference on Information Science and Technology (ICIST), pp. 91–97, IEEE, 2018.

[18] C.-T. Li, D.-H. Shih, and C.-C. Wang, "Cloud-assisted mutual authentication and privacy preservation protocol for telecare medical information systems," Computer methods and programs in biomedicine, vol. 157, pp. 191–203, 2018.

[19] D. Kumar, H. S. Grover, and Adarsh, "A secure authentication protocol for wearable devices environment using ECC," J. Inf. Secur. Appl., vol. 47, pp. 8–15, 2019.

[20] L. Zheng, C. Song, N. Cao, Z. Li, W. Zhou, J. Chen, and L. Meng, "A new mutual authentication protocol in mobile RFID for smart campus," IEEE Access, vol. 6, pp. 60996–61005, 2018.

[21] M. Safkhani and A. Vasilakos, "A new secure authentication protocol for telecare medicine information system and smart campus," IEEE Access, vol. 7, pp. 23514–23526, 2019.

[22] A. Xiang and J. Zheng, "A situation-aware scheme for efficient device authentication in smart grid-enabled home area networks," Electronics, vol. 9, no. 6, p. 989, 2020.

[23] J. Oh, S. Yu, J. Lee, S. Son, M. Kim, and Y. Park, "A secure and lightweight authentication protocol for IoT-based smart homes," Sensors, vol. 21, no. 4, p. 1488, 2021.

[24] A. Gupta, M. Tripathi, T. J. Shaikh, and A. Sharma, "A lightweight anonymous user authentication and key establishment scheme for wearable devices," Computer Networks, vol. 149, pp. 29–42, 2019.

[25] R. Hajian, S. ZakeriKia, S. H. Erfani, and M. Mirabi, "SHAPARAK: scalable healthcare authentication protocol with attack-resilience and anonymous key-agreement," Computer Networks, vol. 183, p. 107567, 2020.

[26] Z. Xu, C. Xu, H. Chen, and F. Yang, "A lightweight anonymous mutual authentication and key agreement scheme for WBAN," Concurrency and computation: Practice and experience, vol. 31, no. 14, p. e5295, 2019.

[27] B. A. Alzahrani, A. Irshad, A. Albeshri, and K. Alsubhi, "A provably secure and lightweight patient-healthcare authentication protocol in wireless body area networks," Wireless Personal Communications, vol. 117, no. 1, pp. 47–69, 2021.

[28] X. Wang, K. Fan, K. Yang, X. Cheng, Q. Dong, H. Li, and Y. Yang, "A new RFID ultra-lightweight authentication protocol for medical privacy protection in smart living," Computer Communications, vol. 186, pp. 121–

132, 2022.

[29] B. Chander and K. Gopalakrishnan, "A secured and lightweight RFID-tag based authentication protocol with privacy-preserving in telecare medicine information system," Computer Communications, 2022.

[30] M. R. Servati, M. Safkhani, S. Ali, M. H. Malik, O. H. Ahmed, M. Hosseinzadeh, and A. H. Mosavi, "Cryptanalysis of two recent ultra-lightweight authentication protocols," Mathematics, vol. 10, no. 23, 2022.

[31] K. Fan, S. Zhu, K. Zhang, H. Li, and Y. Yang, "A lightweight authentication scheme for cloud-based RFID healthcare systems," IEEE Network, vol. 33, no. 2, pp. 44–49, 2019.

[32] S. F. Aghili, H. Mala, P. Kaliyar, and M. Conti, "SecLAP: Secure and lightweight RFID authentication protocol for medical IoT," Future Generation Computer Systems, vol. 101, pp. 621–634, 2019.

[33] M. Safkhani, S. Rostampour, Y. Bendavid, and N. Bagheri, "Iot in medical & pharmaceutical: Designing lightweight RFID security protocols for ensuring supply chain integrity," Computer Networks, vol. 181, p. 107558, 2020.

[34] V. Sureshkumar, R. Amin, V. Vijaykumar, and S. R. Sekar, "Robust secure communication protocol for smart healthcare system with FPGA implementation," Future Generation Computer Systems, vol. 100, pp. 938–951, 2019.

[35] M. R. Servati and M. Safkhani, "ECCbAS: an ECC based authentication scheme for healthcare IoT systems," Pervasive and Mobile Computing, vol. 90, p. 101753, 2023.

[36] V. Kumar, R. Kumar, A. A. Khan, V. Kumar, Y.-C. Chen, and C.-C. Chang, "RAFI: Robust authentication framework for IoT-based RFID infrastructure," Sensors, vol. 22, no. 9, 2022.

[37] M. Shariq, K. Singh, C. Lal, M. Conti, and T. A. Khan, "ESRAS: an efficient and secure ultra-lightweight RFID authentication scheme for low-cost tags," Comput. Networks, vol. 217, p. 109360, 2022.

[38] M. Safkhani, S. Rostampour, Y. Bendavid, S. Sadeghi, and N. Bagheri, "Improving RFID/IoT-based generalized ultra-lightweight mutual authentication protocols," J. Inf. Secur. Appl., vol. 67, p. 103194, 2022.

[39] M. Adeli, N. Bagheri, S. Sadeghi, and S. Kumari, "$\chi$perbp: a cloud-based lightweight mutual authentication protocol," Peer Peer Netw. Appl., vol. 16, no. 4, pp. 1785–1802, 2023.

[40] K. Fan, W. Jiang, H. Li, and Y. Yang, "Lightweight RFID protocol for medical privacy protection in IoT," IEEE Trans. Ind. Informatics, vol. 14, no. 4, pp. 1656–1665, 2018.

[41] M. Shariq, K. Singh, P. K. Maurya, A. Ahmadian, and D. Taniar, "AnonSURP: an anonymous and secure ultralightweight RFID protocol for deployment in internet of vehicles systems," J. Supercomput., vol. 78, no. 6, pp. 8577–8602, 2022.

[42] Y. Tian, G. Chen, and J. Li, "A new ultralightweight RFID authentication protocol with permutation," IEEE Communications Letters, vol. 16, no. 5, pp. 702–705, 2012.

[43] G. Lowe, "A hierarchy of authentication specifications," in Proceedings 10th Computer Security Foundations Workshop, pp. 31–43, IEEE, 1997.

[44] Z. Ahmadian, M. Salmasizadeh, and M. R. Aref, "Recursive linear and differential cryptanalysis of ultralightweight authentication protocols," IEEE Transactions on Information Forensics and Security, vol. 8, no. 7, pp. 1140–1151, 2013.

[45] B. Liu, B. Yang, and X. Su, "An improved two-way security authentication protocol for RFID system," Information, vol. 9, no. 4, p. 86, 2018.

[46] K. Mansoor, A. Ghani, S. A. Chaudhry, S. Shamshirband, S. A. K. Ghayyur, and A. Mosavi, "Securing IoT-based RFID systems: A robust authentication protocol using symmetric cryptography," Sensors, vol. 19, no. 21, p. 4752, 2019.

[47] S. F. Aghili, H. Mala, M. Shojafar, and P. Peris-Lopez, "LACO: lightweight three-factor authentication, access control and ownership transfer scheme for e-health systems in IoT," future generation computer systems, vol. 96, pp. 410–424, 2019.

[48] M. Masud, G. S. Gaba, K. Choudhary, M. S. Hossain, M. F. Alhamid, and G. Muhammad, "Lightweight and anonymity-preserving user authentication scheme for iot-based healthcare," IEEE Internet of Things Journal, vol. 9, no. 4, pp. 2649–2656, 2022.

[49] L. Zhou, X. Li, K.-H. Yeh, C. Su, and W. Chiu, "Lightweight IoT-based authentication scheme in cloud computing circumstance," Future Generation Computer Systems, vol. 91, pp. 244–251, 2019.

MEHDI HOSSEINZADEH received the B.S. degree in computer hardware engineering from Islamic Azad University, Dezfol Branch, Iran, in 2003, and the M.Sc. and Ph.D. degrees in computer system architecture from the Science and Research Branch, Islamic Azad University, Tehran, Iran, in 2005 and 2008, respectively. He is the author/coauthor of more than 250 publications in technical journals and conferences. His research interests include SDN, information technology, data mining, big data analytics, e-commerce, e-marketing, and social networks.

MOHAMMAD REZA SERVATI is a highly accomplished researcher and computer scientist specializing in the field of privacy and security in resource-constrained environments. He completed his Master's degree in Computer Engineering from Shahid Rajaee Teacher Training University, where he excelled with an exceptional grade of A. During his Master's studies, Mohammad Reza focused his research efforts on authentication protocols, ranging from lightweight to full-fledged, ultra-lightweight, and simple protocols. He extensively evaluated these protocols using formal verification techniques, including proveif, Avispa and scyther, as well as manual methods such as BAN or RoR. His research uncovered vulnerabilities in several protocols, leading him to propose a robust and secure scheme that demonstrated resilience against passive and active attacks, while maintaining reasonable computational and communication costs. Mohammad's contributions in the field of privacy and security have been recognized through the publication of papers in renowned journals and conferences.

AMIR MASOUD RAHMANI received his BS in computer engineering from Amir Kabir University, Tehran, in 1996, the MS in computer engineering from Sharif University of Technology, Tehran, in 1998, and the PhD degree in computer engineering from IAU University, Tehran, in 2005. Currently, he is a Professor in the Department of Computer Engineering. He is the author/co-author of more than 350 publications in technical journals and conferences. His-research interests are in the Internet of things, cloud/fog computing, and evolutionary computing.

MASOUMEH SAFKHANI received the Ph.D. degree in Electrical Engineering from the Iran University of Science and Technology, in 2012, with the security analysis of RFID protocols as her major field. She is currently an Associate Professor with the Computer Engineering Department, Shahid Rajaee Teacher Training University, Tehran, Iran. Her current research interests include the security analysis of lightweight and ultra-lightweight protocols, targeting constrained environments, such as RFID, the IoT, VANET, and WSN. She is the author/co-author of over 70 technical articles in information security and cryptology in major international journals and conferences.

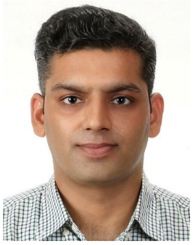
JAN LANSKY received the M.S. and Ph.D. degrees in computer science (software systems) from Charles University, Prague, Czech Republic, in 2005 and 2009, respectively. Since March 2009, he has been a Professor with the Department of Computer Science and Mathematics, Faculty of Economic Studies, University of Finance and Administration, Prague, where he has also been the Head of the Department, since September 2014. His research interests include crypto currencies, text compression, and databases.

RENATA JANOSCOVA graduated from the Lviv polytechnic National University in 1990 and received the Ph.D degree in 2009 there (Slovak Academy of Sciences and Comenius University in Bratislava). She has been working as an Assistant Professor with the Department of Computer Science and Mathematics, Faculty of Economic Studies, University of Finance and Administration, Prague, Czech Republic since September 2020. In her work, she focuses on Applied Informatics (Information Systems), CAQ – Computer Aided Quality, use of networks for distance education and Data Mining.She is a reviewer in the Scopus journal Acta Informatica Pragensia. She is a member of TK 37 Information Technologies and TK 71 Applications of statistical methods, within Slovak Office of Standards, Metrology and Testing (ÚNMS SR).

OMED HASSAN AHMED is the Head of the Information Technology Department at the College of Science and Technology, University of Human Development, in northern Iraq. He has been a distinguished faculty member at this institution since 2013. Dr. Ahmed's academic credentials include:

- A B.Sc. in Information Technology from Teesside University, UK.
- A Higher National Diploma (HND) in Information Technology, also from Teesside University, UK.
- An MSc in Computer Science from Newcastle University, UK.
- A PhD in Computer Science from Huddersfield University, UK.

With his robust educational background and vast experience, Dr. Ahmed is a significant contributor to the disciplines of Information Technology and Computer Science.



JAWAD TANVEER attained a Bachelor of Science (B.S.) degree in telecommunication and networking from COMSATS University Islamabad, Pakistan, in 2012. He then pursued a Master of Science (M.S.) degree in information security from Riphah International University, Islamabad, Pakistan, which he successfully obtained in 2017. His academic journey culminated with the completion of a Doctor of Philosophy (Ph.D.) degree in the field of Optical Engineering at Sejong University, Seoul, South Korea, in 2022. Prior to that, he served as a teaching associate at the Department of Computer Science, COMSATS University Islamabad, Pakistan, from April 2012 to February 2019. He currently holds the position of Assistant Professor within the Department of Computer Science and Engineering at Sejong University. His areas of research focus encompass Next Generation Wireless Networks, the integration of artificial intelligence (AI) in unmanned aerial vehicle (UAV) assisted wireless networks (UAWN), mmWave technology, secure routing protocols, and wireless positioning technologies.

SANG-WOONG LEE received the B.S. degree in electronics and computer engineering and the M.S. and Ph.D. degrees in computer science and engineering from Korea University, Seoul, South Korea, in 1996, 2001, and 2006, respectively. From June 2006 to May 2007, he was a Visiting Scholar with the Robotics Institute, Carnegie Mellon University. From September 2007 to February 2017, he was a Professor with the Department of Computer Engineering, Chosun University, Gwangju, South Korea. He is currently a Professor with the School of Computing, Gachon University, Seongnam, South Korea. His current research interests include face recognition, computational aesthetics, machine learning, medical imaging analysis, and AI-based applications.