ESRAS

An efficient and secure ultra-lightweight RFID authentication scheme for low-cost tags

Shariq, Mohd; Singh, Karan; Lal, Chhagan; Conti, Mauro; Khan, Tayyab

DOI
10.1016/j.comnet.2022.109360

Publication date
2022

Document Version
Final published version

Published in
Computer Networks

Citation (APA)
Shariq, M., Singh, K., Lal, C., Conti, M., & Khan, T. (2022). ESRAS: An efficient and secure ultra-lightweight RFID authentication scheme for low-cost tags. *Computer Networks*, *217*, Article 109360. https://doi.org/10.1016/j.comnet.2022.109360

Computer Networks 217 (2022) 109360

Contents lists available at ScienceDirect

Computer Networks

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

ESRAS: An efficient and secure ultra-lightweight RFID authentication scheme for low-cost tags

Mohd Shariq [a,c], Karan Singh [a], Chhagan Lal [b,*], Mauro Conti [b,c], Tayyab Khan [a]

[a] School of Computer and Systems Sciences, JNU, New Delhi, India
[b] Department of Intelligent Systems, TU Delft, Netherlands
[c] Department of Mathematics, University of Padova, Italy

ARTICLE INFO

Keywords:
RFID
IoT
Authentication
Rank
Security and privacy

ABSTRACT

Internet of Things (IoT) technologies rapidly evolve and are used in many real-life applications. One of the core technologies used in various IoT applications is Radio Frequency IDentification (RFID) technology. RFID wirelessly and uniquely identifies the tagged objects without a direct line of sight. However, the research community had reported privacy and security-related concerns in RFID systems, where an adversary may tamper, eavesdrop, add, delete, or even modify the transmitted messages over an insecure communication channel.

To address the issues mentioned above, we propose an Efficient, Secure, and practical ultra-lightweight RFID Authentication Scheme (ESRAS), which uses rank operation for low-cost tags. We utilize a simplistic bitwise exclusive-OR, circular left rotation, and a newly proposed ultra-lightweight rank operation to provide high security at low cost. The analysis of ESRAS concerning its security and performance shows that it effectively resists several known attacks and is relatively superior to the existing schemes regarding the computational and storage costs. Moreover, ESRAS shows more suitability for low-cost RFID tags and can be executed in a multimedia big data environment.

1. Introduction

Internet-of-Things (IoT) is an umbrella keyword that covers several aspects associated with the extension of the Internet [1]. Over the past years, among various new technologies, IoT has emerged as a major topic researched in academia and industry, aiming to benefit society. IoT technology enables physical objects to exchange and collect data through the Internet [2]. The devices are embedded with various technologies and entities like RFID tags, actuators, sensors, and network connectivity for communicating with the external environment or other devices [3]. RFID technology is rapidly growing and becoming more popular with contactless technology. It has seen a tremendous increase in its applications used in the Automatic Identification and Data Capturing (ADIC) of any targeted object(s) with no direct line-of-sight or contact [4]. In addition to this, it can read the data remotely and automatically through radio frequency signals. One of the first uses of RFID was seen during World War Second in Identify Friend or Foe (IFF) aircraft systems [5]. Since then, several traditional automatic identification technologies have been used in various applications. These techniques include barcode recognition, biometric identification, optical character recognition, and magnetic card identification systems. However, these technologies are still unsatisfactory due to their several limitations. For example, the barcode system needs a direct line-of-sight contact between tags and readers for object identification and storing a small amount of data. While a biometric identification system is expensive for specific purposes, the optical character recognition cost is too high, and magnetic card identification needs close contact to identify an object. In contrast, RFID has numerous advantages over these traditional identification technologies. Therefore, RFID is considered one of the prominent technology in the twenty-first century [6,7]. RFID technology is widely used in various real-life applications such as e-libraries, e-payment, animal identification, personnel identification, smart healthcare systems, human implantation, access control, and Internet of Vehicles (IoV), etc [8–10].

RFID systems typically contain three main components: tags, readers, and backend servers. Each RFID tag has two key elements: a silicon microchip and an antenna. The microchip stores and processes data, while an antenna transmits and receives data to the RFID reader via radio signals [11]. The RFID tags consist of mainly three categories

[*] Corresponding author.
E-mail addresses: shariq99ansari@gmail.com (M. Shariq), karancs12@gmail.com (K. Singh), c.lal@tudelft.nl (C. Lal), mauro.conti@unipd.it (M. Conti), tayyabkhan.cse2012@gmail.com (T. Khan).

https://doi.org/10.1016/j.comnet.2022.109360
Received 29 October 2021; Received in revised form 8 August 2022; Accepted 5 September 2022
Available online 16 September 2022

such as active, semi-active, and passive. Nowadays, primarily passive tags are being used because these are relatively cheaper as compared to active tags. Also, they have no battery and get charged through Radio Frequency (RF) waves from the RFID reader. Instead, the active tags get power, are charged with their battery or energy sources, and transmit signals periodically. The semi-active tags get power and are charged with internal energy sources [11]. Accordingly, the RFID tags can be operated at the three different types of frequency ranges, which includes the low-frequency range (LF: 125 kHz to 134 kHz, reading range: ∼10 cm), high-frequency range (HF: 13.56 MHz, reading range: ∼1 m), and ultra-high frequency range (UHF: 860 to 960 MHz, reading range: 10 to 15 m) [12]. The RFID reader consists of three components: RF signal generator, microcontroller, and receiver or signal detector. It is used to read/write the secret information of the tags over an insecure communication channel and further transmit it into the database of the backend server [13–15]. The RF signal generator produces radio waves, and an antenna is used to transmit them. Also, the reader receives feedback signals which come from the tag. The receiver/signal detector processes the information which is sent by the RFID tags. The backend server is connected with the reader and stores the associated secret information of the tags affixed to objects.

Typically, RFID authentication protocols can be classified into four categories depending upon the supported operations on the tags, the computational cost of the tags, and cryptographic primitives employed on the tags [16].

- **Full-fledged protocols** These support classical cryptographic primitives such as one-way hashing, symmetric/asymmetric encryption, and even private/public key algorithms [17,18].
- **Simple protocols** These provide support for one-way cryptographic hash and Random Number Generator (RNG) on the tags [19,20].
- **Lightweight protocols** These support RNG and Cyclic Redundancy Check (CRC) checksum on the tags. On the other hand, these protocols do not employ hash functions [21,22].
- **Ultra-lightweight protocols** These support bitwise AND, OR, and XOR operations on the tags. Besides, the RNG cannot be employed on the tags [23–25].

As one of the key technologies used in several IoT domains, the main idea behind RFID is to provide secure and reliable access to the information or messages exchanged over secure channels. The sensitive information associated with particular things or objects should be securely delivered over RFID systems. In an RFID system, mutual authentication is considered one of the primary security requirements that should be accomplished between tag and server over a secure communication channel. RFID authentication schemes must always be secure, efficient, and robust against well-known malicious security attacks [26]. However, several security attacks and privacy issues may occur while exchanging messages between tags and readers. Our proposed scheme satisfies various security and privacy requirements to ensure robust, efficient, and secure RFID communications. Besides, the RFID tags are resource-constrained devices with less computing power, limited computational resources, and low memory space. Therefore an RFID system typically cannot withstand the traditional known cryptographic primitives/algorithms, namely symmetric key and asymmetric key cryptographic techniques. To overcome such issues, our proposed authentication scheme exploits bitwise exclusive-OR (⊕), circular left rotates, and newly proposed ultra-lightweight rank operations to encrypt data instead of hash functions, ensuring less computational and storage overheads on the tags while supporting a higher level of security. In addition, the proposed scheme meets essential security requirements and protects from various security attacks.

To establish a secure RFID authentication system, we present the key objectives, which can be regarded as the main criteria for designing our proposed scheme. These objectives are as follows.

(1) Accomplish mutual authentication between communicating entities.
(2) Achieve forward security.
(3) Resist several known attacks like tag tracking, disclosure, and de-synchronization.
(4) Minimize the storage and communication cost on tags with higher efficiency.

The key contributions of our proposed scheme are as follows.

(1) We propose an efficient and secure ultra-lightweight RFID authentication scheme suitable in IoT scenarios. In particular, we exploit bitwise exclusive-OR (⊕), circular left rotates $Rot(\cdot,\cdot)$, and newly proposed ultra-lightweight rank $Rank(\cdot,\cdot)$ operations for minimizing the computational overhead on tags.
(2) The proposed scheme accomplishes mutual authentication and provides resistance against several attacks, including de-synchronization and tag location tracking attacks.
(3) We implement our proposed scheme, and a performance comparison has been made with the other similar existing schemes to show that our scheme greatly overcomes the storage and communication cost of tags while maintaining the key security requirements.

In Section 2, we describe previous schemes along with their limitations. The notations used and preliminaries are given in Section 3. The methodology of our proposed efficient and secure ultra-lightweight RFID authentication scheme using rank operation for low-cost tags is detailed in Section 4. Next, the informal security analysis is presented following the ESRAS's performance evaluation in Section 5. Section 6 provides the results obtained using Scyther simulation and the performance evaluation. Finally, Section 7 provides the concluding remark.

2. Related work

RFID is considered a promising technology for ubiquitous environments, allowing almost every object to be wirelessly identified via Radio Frequency (RF) waves. Over the past decades, researchers have proposed many schemes to achieve secure communication for safeguarding RFID systems from several known attacks and privacy concerns. However, it is difficult to ensure security and privacy requirements in low-cost RFID systems because of insecure communication among tags and readers. Next, we discuss relevant state-of-the-art RFID authentication schemes with their pros and cons as shown in Table 1.

Peris-Lopez et al. [41–43] presented a class of Ultra-lightweight protocols called UMAP. The protocols are chronological, Ultra-lightweight, lightweight, minimalist, and efficient mutual authentication protocols namely, LMAP [41], M^2AP [42], and EMAP [43], respectively. These protocols utilized simple bitwise OR, exclusive-OR (⊕), and *sum mod* operations to achieve a low-cost computation cost. Also, all these operations were efficient and cost-effective for passive RFID tags. However, Wang-Li [24] and Li-Deng [25] showed that the families of UMAP protocols were insecure against the full disclosure and the de-synchronization attacks.

In [44], an enhancement of RAPP [31] to fix the security weaknesses of the de-synchronization attack on RAPP. The protocol utilizes XOR (⊕), permutation $Per(\cdot,\cdot)$, and build-in CRC-16 operations on the tag. Besides, the protocol utilizes a secret key backup mechanism to improve security functionalities with no increment in performance cost. The protocol provides security against tag tracing, replay, secret disclosure, and de-synchronization attacks. Later on, the protocol in [45] pointed out that the shared secret key between $\mathcal{T}$ and $\mathcal{BS}$ can be easily obtained by an adversary. Thus, the protocol [44] is insecure against de-synchronization attacks.

Table 1
Comparison among various RFID authentication schemes.

References	Classes	Primitives	Strengths	Shortcomings
[6]	Lightweight	XOR, $Rot(\cdot,\cdot)$, $Per(\cdot,\cdot)$, $E(\cdot)_k/D(\cdot)_k$	The scheme uses fewer resources on tags which is better suited for low-cost RFID systems.	Insecure against tag tracking, traceability, anonymity, disclosure, impersonation, de-synchronization, and replay attacks.
[27] SCHEME I	Lightweight	XOR, $PRNG(\cdot)$, $h(\cdot)$, g_t	The reader remotely connects with the backend server by employing 4G and 5G technology to increase the mobility of RFID systems.	Vulnerable to traceability attacks.
[27] SCHEME II	Lightweight	Square and Modulo operations ($x^2 \equiv k\ mod\ n/m$)	The Rabin algorithm only performs square and modulo operations to raise a higher level of security for the public key level.	Vulnerable to tag impersonation attacks.
[28]	Lightweight	ECC-based $E(\cdot)_k/D(\cdot)_k$, $f(x)$, (k,n)-SS	The scheme shows strong computational efficiency for RFID systems.	Lack of authenticity of the tag to server.
[29]	Lightweight	XOR, $Rot(\cdot,\cdot)$, $Inv(\cdot,\cdot)$, 2^m $(+)$	The scheme improves efficiency and enhances a higher level of security for resource-constrained RFID systems.	The scheme does not take advantage of computation, communication, and storage costs.
[30]	Lightweight	XOR, $PRNG(\cdot)$, $En(X)$	The scheme is well-suitable for low-cost passive tags.	Vulnerable to de-synchronization and secret disclosure attacks.
[31]	Ultralightweight	XOR, $Rot(\cdot,\cdot)$, $Per(\cdot,\cdot)$	The scheme avoids unbalanced OR and AND operations.	Insecure against de-synchronization attacks.
[32]	Ultralightweight	XOR, $Mer(\cdot,\cdot)$, $Sep(\cdot,\cdot)$	The scheme is well-suitable for low-cost RFID tags.	Vulnerable to de-synchronization and replay attacks.
[33]	Ultralightweight	XOR, $Per(\cdot,\cdot)$, build-in $CRC-16$ function	The scheme used a secret key backup technology to improve security features.	Vulnerable to de-synchronization attacks.
[34]	Ultralightweight	XOR, $modulo\ 2^L$ $(+)$, Reverse Rotation (RR)	The scheme used a sub-key and sub-index mechanism for the key updating phase.	Vulnerable to secret disclosure attacks and reader impersonation attacks.
[35]	Ultralightweight	XOR, CRC, Syndrome decoding	The scheme requires fewer resources on RFID tags which makes it more suitable for passive tags.	Vulnerable to tag traceability attacks and tag impersonation attacks.
[36]	Ultralightweight	XOR, $Rot(\cdot,\cdot)$, $K_c(X)$	The scheme strongly avoids unbalanced AND, OR operations and proposes $K_c(X)$.	Vulnerable to impersonation and de-synchronization attacks.
[37]	Ultralightweight	XOR, $Rot(\cdot,\cdot)$	The scheme ensures data confidentiality, integrity, and tag anonymity features.	Vulnerable to secret disclosure and de-synchronization attacks.
[38]	Ultralightweight	XOR, $Rot(\cdot,\cdot)$, $Con(\cdot,\cdot)$	The scheme provides stronger security also better suited for low-cost passive RFID tags.	Vulnerable to impersonation and de-synchronization attacks.
[39]	Ultralightweight	XOR, $PRNG(\cdot)$, $Rot(\cdot,\cdot)$, $f(x)$, modulo 2^m $(+)$	The scheme is more suitable for resource-constrained RFID systems.	Lack of security simulation tools including AVISPA, CryptoVerif, Scyther, etc.
[40]	Ultralightweight	XOR, $Rot(\cdot,\cdot)$, $Mix(\cdot,\cdot)$	The scheme is very attractive to low-cost RFIDs.	The scheme consumes high storage overhead on the tag.

In [38], a new succinct and Ultra-lightweight RFID authentication protocol called SLAP is presented. The protocol uses simple exclusive-OR, circular left rotate $Rot(\cdot,\cdot)$, and conversion $Con(\cdot,\cdot)$ operations. The passive tags were suitable for implementation using these operations. The conversion operation ensures a security guarantee of the RFID system associated with these properties, including sensibility, full confusion, irreversibility, and low complexity. In addition, the protocol is insecure against replay, traceability, and de-synchronization attacks. Later, Safkhani and Bagheri [46] presented a protocol [38] that is still vulnerable to de-synchronization attacks. However, the protocol in [47] also pointed out that the protocol [38] is not secure under impersonation attacks.

In [36], an Ultra-lightweight RFID protocol called KMAP. To prevent unbalanced logical AND and OR operations, the protocol uses simple exclusive-OR ($\oplus$), circular left rotate $Rot(\cdot,\cdot)$, and pseudo-Kasami code (K_c) operations. Besides, the protocol resists replay, de-synchronization, and full disclosure attacks. Later on, Safkhani and Bagheri [46] pointed out that the protocol in [36] is not secure against de-synchronization attacks. After that, the protocol in [47] pointed out that the protocol [36] is not secure under impersonation attacks.

In [37], a novel Ultra-lightweight protocol is introduced for IoT devices by employing RFID tags. The protocol utilizes exclusive-OR and circular left rotation. The protocol is secure under de-synchronization, tag tracking, and disclosure attacks and ensures data confidentiality, integrity, and tag anonymity properties. Later on, Wang et al. [48] pointed out that the shared secret key between $\mathcal{T}$ and $\mathcal{BS}$ can be obtained by an adversary. Hence, the protocol [37] is vulnerable to de-synchronization and disclosure attacks.

Zheng et al. [49] proposed a mobile RFID authentication scheme for the smart campus. The scheme employs one-way hash $H(\cdot)$, XOR ($\oplus$), and series operation ($\|$). It also guarantees known security features such as counterfeit, eavesdropping, tag location tracking, replay, Main-In-The-Middle (MITM), Denial-of-Service (DoS), and de-synchronization attacks. Later on, Safkhani and Vasilakos [50] pointed out that the scheme is susceptible to tag traceability, tag impersonation, and replay attacks.

In [39], Shamir's $(2, n)$ scheme is proposed using an Ultra-lightweight authentication protocol called UMAPSS. The scheme utilizes a polynomial $f(x)$, $sum\ mod\ (2^m)$, $PRNG(\cdot)$, and $Rot(\cdot,\cdot)$ on the tag. The scheme can ensure known security functionalities, including mutual authentication, integrity, tag anonymity, untraceability, data confidentiality, forward security, and can also resist several security attacks.

In [27], two RFID-based protocols are presented using a one-way hash and Rabin Public Key (RPK) cryptosystem. The hashing protocol utilizes a secure one-way hash $h(\cdot)$, PRNG function, secret keys, and index grouping (g_t) on the RFID tag. In the hashing protocol, the index grouping number associated with the last successful authentication and the key groups associated with the previous three successful authentications are stored in the database. Later on, the hash-based protocol is susceptible to tag traceability attacks reported in [51]. In contrast, in RPK-based protocol, RPK is a symmetric cryptographic approach that utilizes operations of square and modulo such that $(x^2 \equiv k\ mod\ n/m)$. Such operations verify the Rabin encryption algorithm process and resist replay, tag tracking, and DoS attacks. Subsequently, the protocol is susceptible to tag impersonation attacks reported in [51].

In [29], a lightweight authentication protocol for passive RFID tags is introduced. The scheme uses inverse operations, XORing, circular shift, and addition modulo $2^q(+)$. The protocol guarantees several security features, including mutual authentication, location privacy or untraceability, data integrity, tag anonymity, data confidentiality, forward security, and resisting known attacks.

Xiao et al. [30] presented a block cipher-based RFID authentication protocol called LRSAS. The protocol uses some operations such as simple bitwise XORing ($\oplus$), $PRNG(\cdot)$, and SKINNY encryption algorithm. The SKINNY algorithm comprises three phases: setup, round function, and key updating. The protocol guarantees known security functionalities, including confidentiality, integrity, forward security, tag tracking, de-synchronization, and tag impersonation attacks. Later, Trinh et al. [52] reported that the protocol is susceptible to de-synchronization and secret disclosure attacks.

3. Preliminaries

We present the procedure of rank operation and circular rotation operations in this section. To achieve higher security, simple bitwise exclusive-OR, circular left and right, and newly proposed Ultra-lightweight $Rank(X, Y)$ operation are used while designing an efficient and secure Ultra-lightweight RFID authentication scheme named ES-RAS. Table 2 shows all the necessary parameters with their description.

Table 2
Notations and their descriptions.

Notations	Description
$\mathcal{T}, \mathcal{R}, \mathcal{BS}$	RFID tag, reader, backend server
ID	Static identification number of each RFID tag
IDS	Index pseudonym stored in the tag and the database
R_1, R_2	Pseudo random numbers generated at reader
K_1, K_2	Pre-shared secret keys of tags shared with the backend server
$Rank(X, Y)$	Rank operation between strings X and Y
$Rank(X\ or\ Y)$	Number of 1's presents in string X or Y
$nullity(X\ or\ Y)$	Number of 0's presents in string X or Y
$Rot(X, Y)$	Circular left rotation of X by $rank(Y)$
lsb	Least significant bit
msb	Most significant bit
T_h	Threshold used to limit the size of each substring
$\oplus$	Bitwise XOR operator
$? =$	Comparison operator

3.1. Circular left rotate operation

The proposed scheme uses two circular left and right rotation operations. In general, the rotation operation can be denoted $Rot(X, Y)$. However, $Rot(X, Y)$ does left rotate string X by $rank(y)$ mod L bits, where L denotes the bit length of X. The rank of X or Y is defined as the number of 1's presented in string X or Y. For example, considering X and Y are two 8-bit length strings as follows:

$X = 01011100,\ \ Y = 10110100.$

Now, we compute the left rotate operation on X and Y as follows: $Rot(X, Y) =$ String X is left rotated by $rank(Y)$, where $rank(Y) = 4$. Now, $wt(Y)(mod\ 8) = 4\ mod\ 8 = 4$. Hence, $Rot(X, Y) = Rot(X, 4) = 11000101$.

3.2. Definition of rank and nullity

The rank and nullity of the string are defined as the number of 1's and 0's present in the given strings. Suppose that X and Y are the given strings, the $rank$ and $nullity$ of X and Y can be defined as

$rank(X\ or\ Y) =$ Number of 1's presents in string X or Y.

$nullity(X\ or\ Y) =$ Number of 0's presents in string X or Y.

Considering X and Y are two n-bit length strings can be defined as,

$$X = x_1 x_2 \dots x_n, \quad x_i \in \{0, 1\}, i = 1, 2, \dots, n.$$

$$Y = y_1 y_2 \dots y_n, \quad y_j \in \{0, 1\}, j = 1, 2, \dots, n.$$

$$\begin{aligned} Rank(X, Y) &= Z = z_1 z_2 \dots z_n \\ &= \sim X'' \oplus \sim Y'',\ \ z_k \in \{0, 1\}, k = 1, 2, \dots, n. \end{aligned}$$

To achieve full confusion, a new rank $Rank(X, Y)$ operation is used for hiding the information presented in the X and Y. The new proposed Ultra-lightweight $rank$ operation consists of four steps: rank and nullity, grouping, swapping, and composition. To better understand this operation, an example is illustrated below. We are assuming that X and Y are two 32-bit strings. Assuming the value of the threshold is $T_h = 6$.

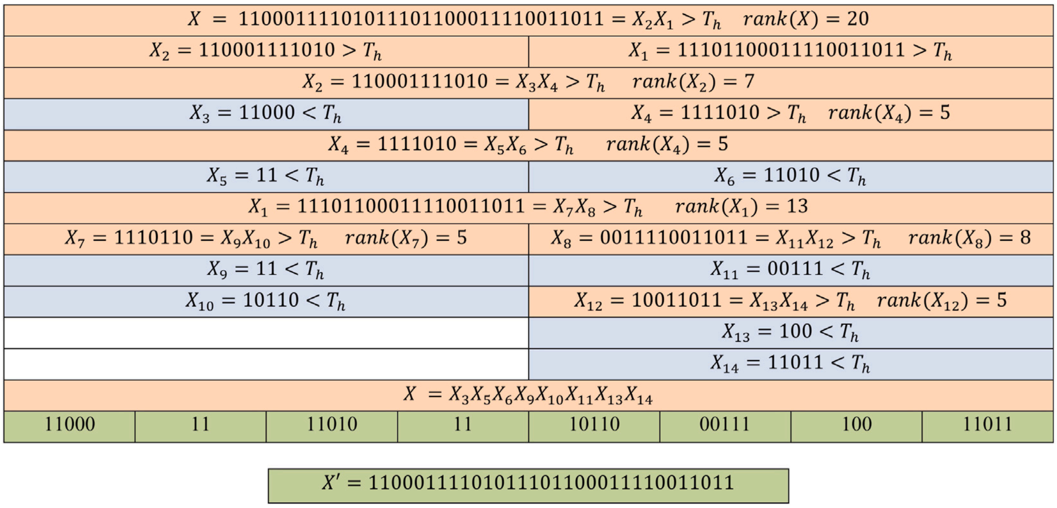
$X = 11000111101011101100011110011011.$

$Y = 10111101110101100011110111000010.$

All used operations are Ultra-lightweight. Thus these can be easily implemented on resource-constrained, low-cost RFID tags. The computational complexity of the rank operation depends on the threshold T_h value. If the value of T_h is small, the confusion will become greater. Therefore, we will suggest a larger value of T_h than 5.

Step 1: **Rank and nullity** Find the rank and nullity of both strings X and Y with respect to 1's and 0's that appear in the given strings.

$rank(X) =$ Number of 1's presents in $X = 20$ and



$X\ =\ 110001111010111011000111110011011 = X_2X_1 > T_h \quad rank(X) = 20$

$X_2 = 110001111010 > T_h$	$X_1 = 111011000111110011011 > T_h$

$X_2 = 110001111010 = X_3X_4 > T_h \quad rank(X_2) = 7$

$X_3 = 11000 < T_h$	$X_4 = 1111010 > T_h \quad rank(X_4) = 5$

$X_4 = 1111010 = X_5X_6 > T_h \quad rank(X_4) = 5$

$X_5 = 11 < T_h$	$X_6 = 11010 < T_h$

$X_1 = 111011000111110011011 = X_7X_8 > T_h \quad rank(X_1) = 13$

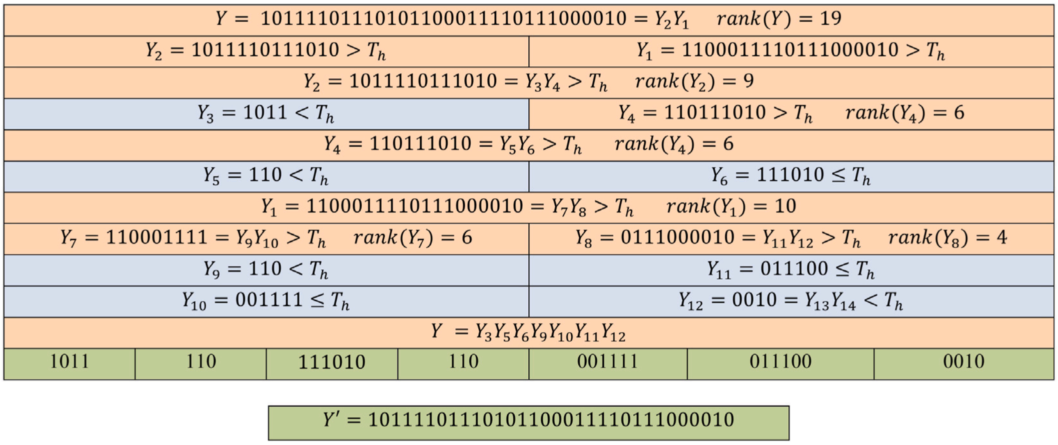
$X_7 = 1110110 = X_9X_{10} > T_h \quad rank(X_7) = 5$	$X_8 = 0011110011011 = X_{11}X_{12} > T_h \quad rank(X_8) = 8$
$X_9 = 11 < T_h$	$X_{11} = 00111 < T_h$
$X_{10} = 10110 < T_h$	$X_{12} = 10011011 = X_{13}X_{14} > T_h \quad rank(X_{12}) = 5$
	$X_{13} = 100 < T_h$
	$X_{14} = 11011 < T_h$

$X\ = X_3X_5X_6X_9X_{10}X_{11}X_{13}X_{14}$

11000	11	11010	11	10110	00111	100	11011

$X' = 110001111010111011000111110011011$

Fig. 1. Computation on string X.



$Y =\ 1011110111010110001111011100010 = Y_2Y_1 \quad rank(Y) = 19$

$Y_2 = 1011110111010 > T_h$	$Y_1 = 110001111011100010 > T_h$

$Y_2 = 1011110111010 = Y_3Y_4 > T_h \quad rank(Y_2) = 9$

$Y_3 = 1011 < T_h$	$Y_4 = 110111010 > T_h \quad rank(Y_4) = 6$

$Y_4 = 110111010 = Y_5Y_6 > T_h \quad rank(Y_4) = 6$

$Y_5 = 110 < T_h$	$Y_6 = 111010 \leq T_h$

$Y_1 = 110001111011100010 = Y_7Y_8 > T_h \quad rank(Y_1) = 10$

$Y_7 = 110001111 = Y_9Y_{10} > T_h \quad rank(Y_7) = 6$	$Y_8 = 0111000010 = Y_{11}Y_{12} > T_h \quad rank(Y_8) = 4$
$Y_9 = 110 < T_h$	$Y_{11} = 011100 \leq T_h$
$Y_{10} = 001111 \leq T_h$	$Y_{12} = 0010 = Y_{13}Y_{14} < T_h$

$Y\ = Y_3Y_5Y_6Y_9Y_{10}Y_{11}Y_{12}$

1011	110	111010	110	001111	011100	0010

$Y' = 1011110111010110001111011100010$

Fig. 2. Computation on string Y.

Table 3
Divided strings X' and Y'.

$X' =$	110001111010111011100	011110011011	$nullity(X) = 12$
$Y' =$	1011110111010110001	1110111000010	$nullity(Y) = 13$

Table 4
Swapping on X' and Y'.

$X'' =$	011110011011	110001111010111011100
$Y'' =$	1110111000010	1011110111010110001

$nullity(X) =$ Number of 0's presents in $X = 12$.

$rank(Y) =$ Number of 1's presents in $Y = 19$ and

$nullity(Y) =$ Number of 0's presents in $Y = 13$.

***Step 2:* Grouping** First, all the given strings (i.e., X and Y) are divided into several small blocks by using the rule of segmentation, which is based on the $rank(X)$ and $rank(Y)$, respectively. In particular, a parameter threshold T_h is used to limit the size of each substring. Let us consider that $rank(X)$ is m such that $m \leq n$, so the two substrings of X after division are given as $X_1 = x_n x_{n-1} \dots x_{m+2} x_{m+1}$, $X_2 = x_m x_{m-1} \dots x_2 x_1$. Then, the division operation on substrings X_1 and X_2 will be continued by using the same segmentation rule based on their $rank(X)$ until the length of all the substrings $X_j (j \leq n)$ are less than the threshold T_h. Similarly, the same rule is performed on string Y divided into $Y_k (k \leq n)$ by using the same segmentation rule. The computations on strings X and Y are shown in Figs. 1 and 2.

***Step 3:* Swapping** In Table 3, we divide the above-obtained strings X' and Y' into two blocks according to $nullity(X)$ and $nullity(Y)$ given in $Step$ 1, respectively. After that, we perform a swap operation on both parts to obtain X'' and Y'' as shown in Table 4.

***Step 4:* Composition** To compute the final computation of the rank operation, we first perform $not(\sim)$ operation on X'' and Y''. Thereafter, the simple bitwise exclusive-OR operation is performed between them. Then, we have

$\sim X'' = 1000011001000011100001010001001 1.$

$\sim Y'' = 0001000111101010000100010100111 0.$

$$Rank(X,Y) =\sim X'' \oplus \sim X''.$$

Therefore, $Rank(X,Y) = 10010111101010011001010001011101.$

$rank(Rank(X,Y)) = 17$ and $nullity(Rank(X,Y)) = 15$.

The aforementioned rank operation is well-suitable and can be easily realized in low-cost RFID tags. The proposed rank operation has four major properties, which are as follows:

- **Full confusion** For each given input, they are confused by the other one and have no predicted or fixed bit produced by the rank operation. Therefore, an adversary cannot obtain one bit of useful or even sensitive information from the output to predict the input.

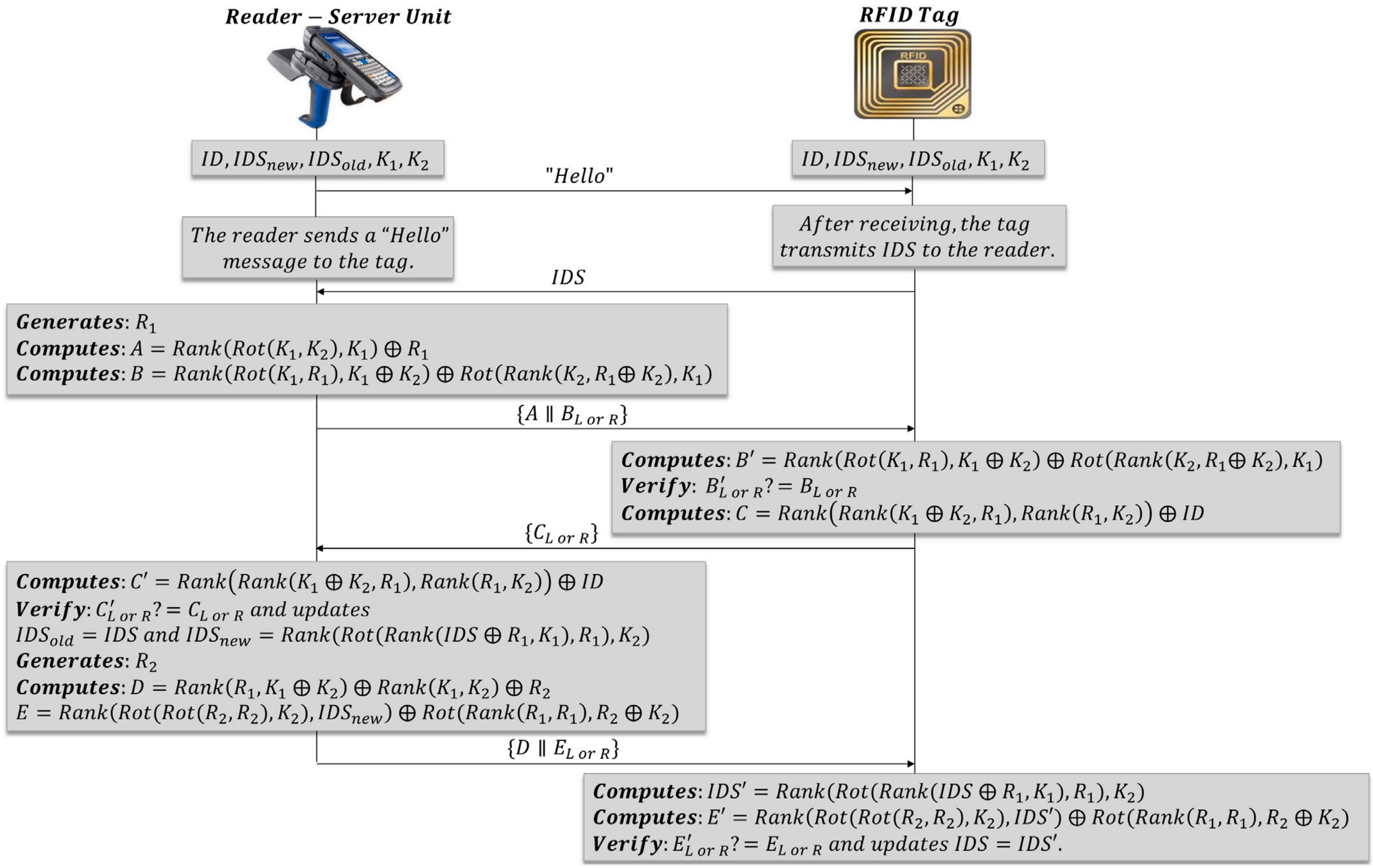

$Reader - Server\ Unit$
$RFID\ Tag$
$ID, IDS_{new}, IDS_{old}, K_1, K_2$
$ID, IDS_{new}, IDS_{old}, K_1, K_2$
"Hello"
The reader sends a "Hello" message to the tag.
After receiving, the tag transmits IDS to the reader.
IDS
Generates: R_1
Computes: $A = Rank(Rot(K_1, K_2), K_1) \oplus R_1$
Computes: $B = Rank(Rot(K_1, R_1), K_1 \oplus K_2) \oplus Rot(Rank(K_2, R_1 \oplus K_2), K_1)$
$\{A \parallel B_{L\ or\ R}\}$
Computes: $B' = Rank(Rot(K_1, R_1), K_1 \oplus K_2) \oplus Rot(Rank(K_2, R_1 \oplus K_2), K_1)$
Verify: $B'_{L\ or\ R} ?= B_{L\ or\ R}$
Computes: $C = Rank(Rank(K_1 \oplus K_2, R_1), Rank(R_1, K_2)) \oplus ID$
$\{C_{L\ or\ R}\}$
Computes: $C' = Rank(Rank(K_1 \oplus K_2, R_1), Rank(R_1, K_2)) \oplus ID$
Verify: $C'_{L\ or\ R} ?= C_{L\ or\ R}$ and updates
$IDS_{old} = IDS$ and $IDS_{new} = Rank(Rot(Rank(IDS \oplus R_1, K_1), R_1), K_2)$
Generates: R_2
Computes: $D = Rank(R_1, K_1 \oplus K_2) \oplus Rank(K_1, K_2) \oplus R_2$
$E = Rank(Rot(Rot(R_2, R_2), K_2), IDS_{new}) \oplus Rot(Rank(R_1, R_1), R_2 \oplus K_2)$
$\{D \parallel E_{L\ or\ R}\}$
Computes: $IDS' = Rank(Rot(Rank(IDS \oplus R_1, K_1), R_1), K_2)$
Computes: $E' = Rank(Rot(Rot(R_2, R_2), K_2), IDS') \oplus Rot(Rank(R_1, R_1), R_2 \oplus K_2)$
Verify: $E'_{L\ or\ R} ?= E_{L\ or\ R}$ and updates $IDS = IDS'$.

Fig. 3. Proposed ESRAS scheme.

- **Irreversibility** For two given inputs, they can be confused by each other based on their rank, bit's position, and values. An adversary cannot obtain, predict, or even recover the other input if it knows one of the two inputs and the corresponding output in the rank operation.
- **Sensibility** The corresponding output of the rank operation will be completely different only if one bit is changed in one of the two given inputs.
- **Low complexity** The rank operation utilizes only simple XOR and circular left rotate operations. These operations are elementary to use as well as cost-effective for a passive tag implementation.

4. Proposed scheme

The proposed scheme consists of two phases: initialization and authentication.

4.1. Valid assumptions considered

The underlying assumptions on which the proposed scheme operates are as follows:

(1) An adversary can mimic a genuine tag or reader.
(2) An adversary can tamper, modify, intercept, add, and/or even delete messages during the messages exchanged among RFID components.
(3) The communication channel is considered to be secure between $\mathcal{R}$ and $\mathcal{BS}$ as well as insecure between $\mathcal{T}$ and $\mathcal{R}$, i.e., all attacks are possible.
(4) The backend server is a fully trusted entity; an adversary cannot reveal the tags' information.

4.2. Initialization phase

This phase defines some underlying statements, which are as follows:

(1) Initially, the manufacturer stores a unique static identification number ID and an index IDS in each tag's internal memory.
(2) For each $\mathcal{T}$, the manufacturer stores two secret keys K_1 and K_2, a new and old pseudonym IDS_{new} and IDS_{old} in $\mathcal{BS}$. Initially, $IDS_{old} = IDS$ and $IDS_{new} = Null$.
(3) Each reader consists of two $PRNG(\cdot)$.
(4) The tag and the reader have limitations of computing resources. In contrast, the backend server has no such limitations.
(5) The other relevant tag's information is stored at $\mathcal{BS}$.

4.3. Authentication phase

Fig. 3 shows the detailed process of the authentication phase of ESRAS scheme which is executed in the following steps.

Step 1: $M_1 : \mathcal{R} \rightarrow \mathcal{T} : \{“Hello”\}$.
The reader $\mathcal{R}$ initiates an authentication session by sending a "$Hello$" message to $\mathcal{T}$.

Step 2: $M_2 : \mathcal{T} \rightarrow \mathcal{R} : \{IDS\}$.
After receiving, $\mathcal{T}$ sends an index pseudonym IDS to $\mathcal{R}$.

Step 3: $M_3 : \mathcal{R} \rightarrow \mathcal{T} : \{A \parallel B_{L\ or\ R}\}$.
Upon receiving IDS, $\mathcal{R}$ uses the received IDS as an index to search the secrets of tags in the backend server database. If it finds a match in the database, then $\mathcal{R}$ generates a L-bit pseudo-random number R_1 and computes A and B. After that, $\mathcal{R}$ sends the messages $A \parallel B_{L\ or\ R}$ to $\mathcal{T}$, where B_L and B_R represent the left and right half of the string B,

respectively. The B_L or B_R of string B is transmitted to the tag based on the rank of B (if $Rank(B)$ is odd, then sent B_L, else sent B_R).

- Computes $A = Rank(Rot(K_1, K_2), K_1) \oplus R_1$.
- Computes $B = Rank(Rot(K_1, R_1), K_1 \oplus K_2) \oplus Rot(Rank(K_1, R_1 \oplus K_2), K_2)$.

Step 4: *$M_4 : \mathcal{T} \rightarrow \mathcal{R} : \{C_{L\ or\ R}\}$.*

After receiving $A \parallel B_{L\ or\ R}$, the tag extracts R_1 from A by XORing $Rank(Rot(K_1, K_2), K_1)$ with A. After that, the tag computes a local value of B' and verifies whether $B'_{L\ or\ R}? = B_{L\ or\ R}$, if so, then $\mathcal{T}$ authenticates $\mathcal{R}$ as a legitimate reader and computes the response message C. $\mathcal{T}$ sends the response message $C_{L\ or\ R}$ to $\mathcal{R}$, where C_L and C_R represent the left and right half of the string C, respectively.

- Extracts $R_1 = Rank(Rot(K_1, K_2), K_1) \oplus A$.
- Compute $B' = Rank(Rot(K_1, R_1), K_1 \oplus K_2) \oplus Rank(Rot(K_1, R_1 \oplus K_2), K_2)$.
- Verify $B'_{L\ or\ R} = B_{L\ or\ R}$
- Computes $C = Rank(Rank(K_1 \oplus K_2, R_1), Rank(R_1, K_2)) \oplus ID$.

Step 5: *$M_5 : \mathcal{R} \rightarrow \mathcal{T} : \{D \parallel E_{L\ or\ R}\}$.*

Upon receiving $C_{L\ or\ R}$, $\mathcal{R}$ computes a local value of C' and verifies whether $C'_{L\ or\ R}? = C_{L\ or\ R}$, if so, then $\mathcal{R}$ authenticates $\mathcal{T}$ as a legitimate tag $\mathcal{T}$ and update its index pseudonyms IDS_{old} and IDS_{new} in the database. After that, the reader generates L-bit pseudo-random number R_2 and computes the response messages D and E. The reader $\mathcal{R}$ sends the response messages $D \parallel E_{L\ or\ R}$ to the tag $\mathcal{T}$ where E_L and E_R represent the left and right half of the string E, respectively.

- Computes $C' = Rank(Rank(K_1 \oplus K_2, R_1), Rank(R_1, K_2)) \oplus ID$.
- Verify $C'_{L\ or\ R}? = C_{L\ or\ R}$ and updates the index $IDS_{old} = IDS$ and $IDS_{new} = Rank(Rot(Rank(IDS \oplus R_1, K_1), K_2))$.
- Computes $D = Rank(R_1, K_1 \oplus K_2) \oplus Rank(K_1, K_2) \oplus R_2$.
- Computes $E = Rank(Rot(Rot(R_2, R_2), K_2), IDS_{new}) \oplus Rot(Rank(R_1, R_1), R_2 \oplus K_2)$.

Step 6: *Verification at Tag.*

After receiving $C \parallel D_{L\ or\ R}$, the tag extracts R_2 from D by XORing $Rank(R_1, K_1 \oplus K_2) \oplus Rank(K_1, K_2)$ with D. The tag computes IDS' and the local value of E' and subsequently verifies whether $E'_{L\ or\ R}? = E_{L\ or\ R}$, if so, the tag successfully authenticates the reader as a legitimate reader and updates its index pseudonym.

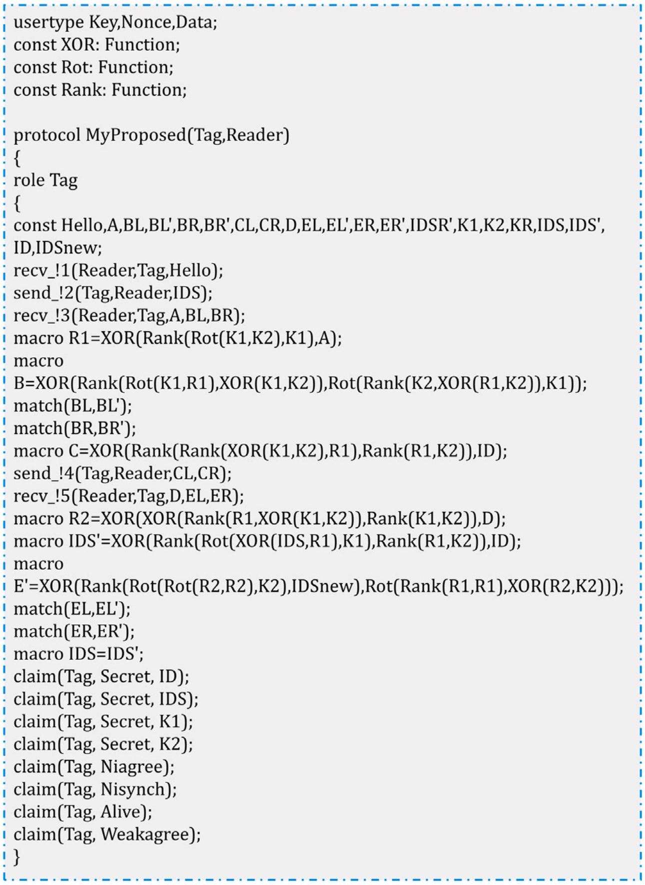
- Extracts $R_2 = Rank(R_1, K_1 \oplus K_2) \oplus Rank(K_1, K_2) \oplus D$.
- Computes $IDS' = Rank(Rot(Rank(IDS \oplus R_1, K_1), R_1), K_2)$.
- Computes $E' = Rank(Rot(Rot(R_2, R_2), K2)), IDS_{new} \oplus Rot(Rank(R_1, R_1), R_2 \oplus K_2)$.
- Verify $E'_{L\ or\ R}? = E_{L\ or\ R}$ and updates the index $IDS = IDS'$.

5. Analysis and evaluation

The security analysis and the performance evaluation of ESRAS are illustrated in Tables 5 and 6. We have compared our proposed scheme with various existing Ultra-lightweight RFID authentication schemes. These schemes are URASP [8], IOLAS [29], LRSAS [30], RAPP [31], RAPLT [32], KMAP [36], Tewari–Gupta [37], SLAP [38], LMAP [41], M^2AP [42], EMAP [43], LPCP [44], SASI [53], David–Prasad [54], Gossamer [55], RRAP [56], RCIA [57], and URMAP [58], respectively.

5.1. Informal security analysis

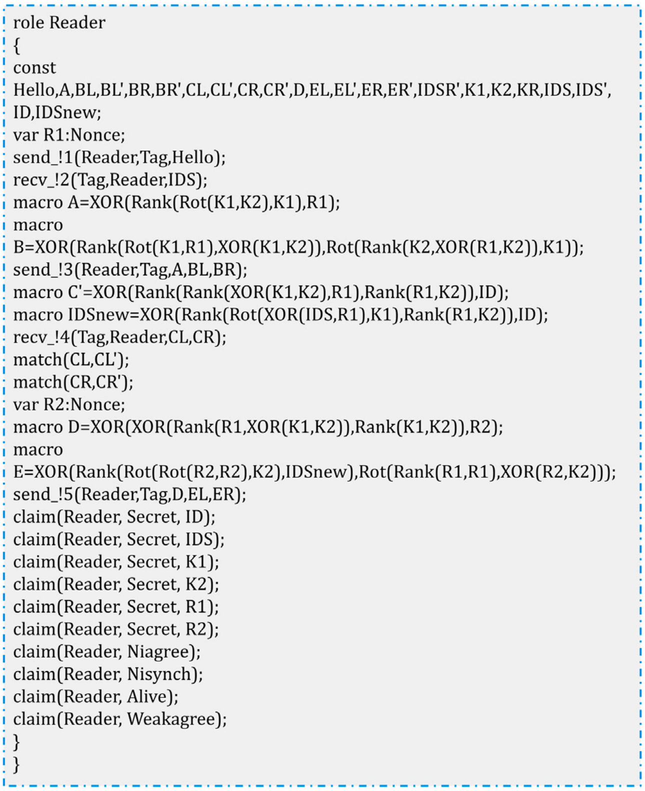
The comparative informal security and privacy analysis of ESRAS are illustrated in Table 5.



```
usertype Key,Nonce,Data;
const XOR: Function;
const Rot: Function;
const Rank: Function;

protocol MyProposed(Tag,Reader)
{
role Tag
{
const Hello,A,BL,BL',BR,BR',CL,CR,D,EL,EL',ER,ER',IDSR',K1,K2,KR,IDS,IDS',
ID,IDSnew;
recv_!1(Reader,Tag,Hello);
send_!2(Tag,Reader,IDS);
recv_!3(Reader,Tag,A,BL,BR);
macro R1=XOR(Rank(Rot(K1,K2),K1),A);
macro
B=XOR(Rank(Rot(K1,R1),XOR(K1,K2)),Rot(Rank(K2,XOR(R1,K2)),K1));
match(BL,BL');
match(BR,BR');
macro C=XOR(Rank(Rank(XOR(K1,K2),R1),Rank(R1,K2)),ID);
send_!4(Tag,Reader,CL,CR);
recv_!5(Reader,Tag,D,EL,ER);
macro R2=XOR(XOR(Rank(R1,XOR(K1,K2)),Rank(K1,K2)),D);
macro IDS'=XOR(Rank(Rot(XOR(IDS,R1),K1),Rank(R1,K2)),ID);
macro
E'=XOR(Rank(Rot(Rot(R2,R2),K2),IDSnew),Rot(Rank(R1,R1),XOR(R2,K2)));
match(EL,EL');
match(ER,ER');
macro IDS=IDS';
claim(Tag, Secret, ID);
claim(Tag, Secret, IDS);
claim(Tag, Secret, K1);
claim(Tag, Secret, K2);
claim(Tag, Niagree);
claim(Tag, Nisynch);
claim(Tag, Alive);
claim(Tag, Weakagree);
}
```

Fig. 4. SPDL specification for the Tag role.



```
role Reader
{
const
Hello,A,BL,BL',BR,BR',CL,CL',CR,CR',D,EL,EL',ER,ER',IDSR',K1,K2,KR,IDS,IDS',
ID,IDSnew;
var R1:Nonce;
send_!1(Reader,Tag,Hello);
recv_!2(Tag,Reader,IDS);
macro A=XOR(Rank(Rot(K1,K2),K1),R1);
macro
B=XOR(Rank(Rot(K1,R1),XOR(K1,K2)),Rot(Rank(K2,XOR(R1,K2)),K1));
send_!3(Reader,Tag,A,BL,BR);
macro C'=XOR(Rank(Rank(XOR(K1,K2),R1),Rank(R1,K2)),ID);
macro IDSnew=XOR(Rank(Rot(XOR(IDS,R1),K1),Rank(R1,K2)),ID);
recv_!4(Tag,Reader,CL,CR);
match(CL,CL');
match(CR,CR');
var R2:Nonce;
macro D=XOR(XOR(Rank(R1,XOR(K1,K2)),Rank(K1,K2)),R2);
macro
E=XOR(Rank(Rot(Rot(R2,R2),K2),IDSnew),Rot(Rank(R1,R1),XOR(R2,K2)));
send_!5(Reader,Tag,D,EL,ER);
claim(Reader, Secret, ID);
claim(Reader, Secret, IDS);
claim(Reader, Secret, K1);
claim(Reader, Secret, K2);
claim(Reader, Secret, R1);
claim(Reader, Secret, R2);
claim(Reader, Niagree);
claim(Reader, Nisynch);
claim(Reader, Alive);
claim(Reader, Weakagree);
}
}
```

Fig. 5. SPDL specification for the Reader role.

Table 5
Security and privacy comparison among various Ultra-lightweight authentication schemes.

Scheme ↓ ⟶	Mutual authentication	Forward security	Resistance to tag tracking	Resistance to de-synchronization attacks	Resistance to disclosure attacks	Security of the diffusion function
URASP [8]	Yes	❋	Yes	Yes	Yes	Yes
IOLAS [29]	Yes	Yes	❋	Yes	❋	❋
LRSAS [30]	Yes	Yes	Yes	Yes	❋	❋
RAPP [31]	No	Yes	No	No	Yes	Yes
RAPLT [32]	No	Yes	No	No	Yes	❋
KMAP [36]	Yes	❋	Yes	No	Yes	No
Tewari–Gupta [37]	Yes	Yes	Yes	No	No	No
SLAP [38]	Yes	Yes	Yes	No	Yes	Yes
LMAP [41]	❋	No	No	No	No	❋
M^2AP [42]	❋	No	No	No	No	❋
EMAP [43]	❋	No	No	No	No	❋
LPCP [44]	Yes	❋	Yes	No	Yes	❋
SASI [53]	❋	No	No	No	No	❋
David–Prasad [54]	❋	No	No	❋	No	❋
Gossamer [55]	❋	No	No	No	Yes	Yes
R^2AP [56]	Yes	Yes	Yes	Yes	Yes	No
RCIA [57]	Yes	❋	Yes	No	Yes	No
URMAP [58]	Yes	❋	Yes	❋	Yes	Yes
Ours	Yes	Yes	Yes	Yes	Yes	Yes

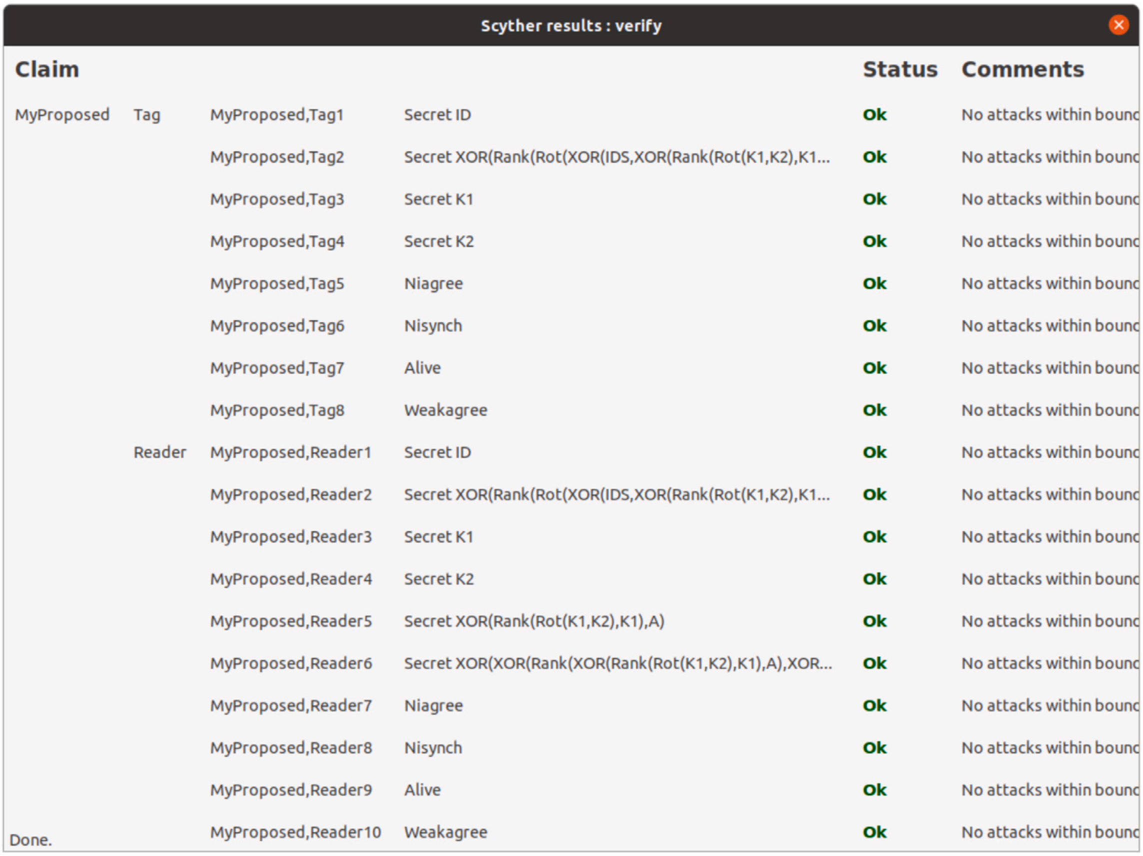
Acronyms Yes: Denotes satisfied; No: Denotes not satisfied; ❋: No discussion.

Table 6
Performance comparison among various Ultra-lightweight authentication schemes.

Scheme ↓ ⟶	Computational operations on the tag side	Total no. of messages for mutual authentication	Communication messages generated on tag	Storage cost on tag
URASP [8]	$\oplus, Per, Rot$	$4L$	$1.5L$	$4L$
IOLAS [29]	$\oplus, Rot, Inv, +$	$4L$	$2L$	$5L$
LRSAS [30]	$\oplus, En(X)$	$5L$	$2L$	$3L$
RAPP [31]	$\oplus, AND, OR, Rot, Per$	$5L$	$2L$	$5L$
RAPLT [32]	$\oplus, Mer, Sep$	$4L$	$3L$	$5L$
KMAP [36]	$\oplus, Rot, K_c$	$4L$	$2L$	$7L$
Tewari–Gupta [37]	$\oplus, Rot$	$4L$	$2L$	$7L$
SLAP [38]	$\oplus, Rot, Con$	$4L$	$1.5L$	$7L$
LMAP [41]	$\oplus, OR, +$	$4L$	$2L$	$6L$
M^2AP [42]	$\oplus, AND, OR, +$	$4L$	$3L$	$6L$
EMAP [43]	$\oplus, AND, OR$	$4L$	$3L$	$6L$
LPCP [44]	$\oplus$, Rot,CRC-16	$5L$	$2L$	$5L$
SASI [53]	$\oplus, OR, Rot, +$	$4L$	$2L$	$7L$
David–Prasad [54]	$\oplus, AND$	$5L$	$3L$	$5L$
Gossamer [55]	$\oplus, Rot, MixBits, +$	$4L$	$3L$	$7L$
R^2AP [56]	$\oplus, Rot, Rec$	$5L$	$2L$	$5L$
RCIA [57]	$\oplus, Per, R_h$	$4L$	$2L$	$7L$
URMAP [58]	$\oplus,\ Per - XOR$	$4L$	$2L$	$5L$
Ours	$\oplus, Rot, Rank$	$5L$	$1.5L$	$5L$

Acronyms L: Number of bits stored in each parameter.

- **Mutual authentication:** It implies that genuine tags and readers need to authenticate each other. In the ESRAS scheme, the reader–server unit authenticates the genuine tag by comparing the left or right half of the transmitted messages that are $B'_{L\ or\ R} ? = B_{L\ or\ R}$ and $E'_{L\ or\ R} ? = E_{L\ or\ R}$. Likewise, the genuine tag authenticates the server by comparing the left or right half of the transmitted message $C'_{L\ or\ R} ? = C_{L\ or\ R}$. Therefore, the property of mutual authentication is established between tag and server.
- **Resistance to tag tracking:** The tag's ID or its secrets are not revealed in the ESRAS scheme. Moreover, it uses the index pseudonym IDS. The IDS and the shared secret keys K_1 and K_2 are updated during each successful protocol run. Besides, the update operations also involve random numbers, so the tag will be anonymous to the adversary. This way, the adversary cannot track the response messages A, B, C, D, and E involving random numbers. In addition, we are not using any unbalanced operations during the update process, so the adversary cannot track the location of the tags through IDS.
- **Forward security:** It ensures securing past communications from a tag if the tag gets compromised by an adversary. Considering an adversary can access the tag, it cannot determine the previous secrets such as random numbers, index pseudonyms, and keys from the tag. Now, considering an adversary can determine the IDS and keys of the tag. However, the adversary still cannot determine the previous secrets as different values of the IDS and keys are used after a successful protocol run. Hence, the adversary cannot compromise the previously communicated information from the same tag.
- **Resistance to de-synchronization attacks:** The shared secret cannot be de-synchronized among tag and reader through an adversary. The tag and the readers will use different random numbers to update the shared secret in each authentication phase. Therefore, the adversary cannot modify or even change the response messages to change the values of R_1 and R_2. Hence, the proposed scheme successfully prevents the de-synchronization attack.
- **Resistance to disclosure attacks:** The adversary can slightly modify the messages from the reader and send them to the tag to verify the correctness of modifications. It is quite difficult to disclose the secrets (i.e., K_1 and K_2) even if the adversary knows $Rank(Rot(K_1, K_2), K_1)$. In our proposed scheme, the tag performs



Scyther results : verify

Claim				Status	Comments
MyProposed	Tag	MyProposed,Tag1	Secret ID	Ok	No attacks within bound
		MyProposed,Tag2	Secret XOR(Rank(Rot(XOR(IDS,XOR(Rank(Rot(K1,K2),K1...	Ok	No attacks within bound
		MyProposed,Tag3	Secret K1	Ok	No attacks within bound
		MyProposed,Tag4	Secret K2	Ok	No attacks within bound
		MyProposed,Tag5	Niagree	Ok	No attacks within bound
		MyProposed,Tag6	Nisynch	Ok	No attacks within bound
		MyProposed,Tag7	Alive	Ok	No attacks within bound
		MyProposed,Tag8	Weakagree	Ok	No attacks within bound
	Reader	MyProposed,Reader1	Secret ID	Ok	No attacks within bound
		MyProposed,Reader2	Secret XOR(Rank(Rot(XOR(IDS,XOR(Rank(Rot(K1,K2),K1...	Ok	No attacks within bound
		MyProposed,Reader3	Secret K1	Ok	No attacks within bound
		MyProposed,Reader4	Secret K2	Ok	No attacks within bound
		MyProposed,Reader5	Secret XOR(Rank(Rot(K1,K2),K1),A)	Ok	No attacks within bound
		MyProposed,Reader6	Secret XOR(XOR(Rank(XOR(Rank(Rot(K1,K2),K1),A),XOR...	Ok	No attacks within bound
		MyProposed,Reader7	Niagree	Ok	No attacks within bound
		MyProposed,Reader8	Nisynch	Ok	No attacks within bound
		MyProposed,Reader9	Alive	Ok	No attacks within bound
Done.		MyProposed,Reader10	Weakagree	Ok	No attacks within bound

Fig. 6. Scyther simulation result of our scheme.

masking (XORing operation) between the tag's unique identification number ID and $Rank(Rank(K_1 \oplus K_2, R_1), Rank(K_1, K_2))$. Therefore, it is impossible to disclose without knowing secrets. Hence, ESRAS resists the disclosure attack.

5.2. Performance evaluation

The performance evaluation of ESRAS is done in terms of computation, communication, and storage cost for each tag. The tags have limited computation capability and memory in comparison to the reader and server in RFID systems. However, the tags' performance can be evaluated with no limitations in the hardware environments of the backend database and reader. Therefore, any authentication scheme considers the computational complexity of an RFID system. Table 6 illustrates the performance comparison of ESRAS with several considerable Ultra-lightweight RFID authentication schemes.

- **Computation cost:** It consists of the types of Ultra-lightweight primitives that are required for each tag. The proposed scheme does not utilize CRC, hash function, pseudo-Kasami code $K_c(X)$, and encryption $E(\cdot)_k$/decryption $D(\cdot)_k$ algorithm. In ESRAS scheme, only simple bitwise exclusive-OR ($\oplus$), and circular left rotation $Rot(X, Y)$, and a newly proposed Ultra-lightweight rank $Rank(X, Y)$ operations have been utilized.
- **Communication cost:** The numbers of transmitted messages by the tag in each authentication session. The tag transmits a total of one and a half communication messages. All the used parameters have L bits. Thus, the communication cost generated on the tag is $1.5L$ bits.
- **Storage cost:** The shared elements and the static tag ID are stored in the tag's memory space. In the ESRAS scheme, a total of five strings, including its unique ID, the two entries for index pseudonym IDS, and two shared secret keys (i.e., K_1 and K_2) are stored on the tag. Hence, the storage of each tag is $5L$ bits.

6. Scyther simulation of our proposed scheme

Scyther is a GUI-based automatic tool to verify security protocols [59]. The Scyther tool checks whether the proposed protocol is secure under security attacks. The experimental setup is simulated by using Scyther installed on the Linux platform with Ubuntu v20.04. The command "scyther-gui.py" is used to open the window for opening and editing files. The Scyther input language is Security Protocol Description Language (SPDL), used for writing the protocol specification or description. The SPDL is case sensitive, where xyz.spdl is not the same as XYZ.spdl. Programs or SPDL descriptions of protocols are saved with a .spdl extension. A pre-defined set of claim events are in Scyther, such as Secret, $session - keyreveal$, Niagree, Nisynch, Alive, and Weakagree. Moreover, a sequence of events is used, which includes sending or receiving. Figs. 4 and 5 show the SPDL specification of the roles of tag and reader. From Fig. 6, the result status OK indicates that there are no possible attacks within bounds which means that the proposed ESRAS scheme strongly resists all possible active and passive (i.e., replay and Man-In-The-Middle) attacks.

7. Conclusion

Since security and privacy are two key concerns in RFID systems, several issues such as eavesdropping, tampering, and modifications may occur over a communication channel while transmitting messages. Considering these security flaws, we proposed an efficient and secure Ultra-lightweight RFID authentication scheme (ESRAS). We have utilized the simple bitwise exclusive-OR, circular left rotate, and newly proposed Ultra-lightweight rank operations to provide higher security with fewer computation and communication costs of tags. The rank operation has four major security properties: full confusion, irreversibility, sensibility, and low complexity. The security analysis demonstrates that our ESRAS scheme is resistant to possible security attacks. The performance evaluation demonstrates that ESRAS requires less storage cost and computation overhead than existing schemes. The Scyther results show that our scheme has no possible attacks within bounds. Furthermore, our scheme shows superiority for low-cost RFID systems and can be realized in several real-world domains.

CRediT authorship contribution statement

Mohd Shariq: Conception and design of study, Analysis and/or interpretation of data, Writing – original draft, Writing – review & editing. **Karan Singh:** Conception and design of study, Analysis and/or interpretation of data, Writing – original draft, Writing – review & editing. **Chhagan Lal:** Conception and design of study, Analysis and/or interpretation of data, Writing – original draft, Writing – review & editing. **Mauro Conti:** Conception and design of study, Analysis and/or interpretation of data, Writing – original draft, Writing – review & editing. **Tayyab Khan:** Conception and design of study, Analysis and/or interpretation of data, Writing – original draft, Writing – review & editing.

Declaration of competing interest

The authors declare the following financial interests/personal relationships which may be considered as potential competing interests: Chhagan Lal reports was provided by Delft University of Technology.

Data availability

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

Acknowledgments

All authors approved the version of the manuscript to be published.

References

[1] Daniele Miorandi, Sabrina Sicari, Francesco De Pellegrini, Imrich Chlamtac, Internet of things: Vision, applications and research challenges, Ad Hoc Netw. 10 (7) (2012) 1497–1516.

[2] Manik Lal Das, Pardeep Kumar, Andrew Martin, Secure and privacy-preserving rfid authentication scheme for internet of things applications, Wirel. Pers. Commun. 110 (1) (2020) 339–353.

[3] Negin Dinarvand, Hamid Barati, An efficient and secure RFID authentication protocol using elliptic curve cryptography, Wirel. Netw. 25 (1) (2019) 415–428.

[4] Nasrollah Pakniat, Ziba Eslami, Cryptanalysis and improvement of a group RFID authentication protocol, Wirel. Netw. 26 (5) (2020) 3363–3372.

[5] Kai Fan, Wei Jiang, Hui Li, Yintang Yang, Lightweight RFID protocol for medical privacy protection in IoT, IEEE Trans. Ind. Inf. 14 (4) (2018) 1656–1665.

[6] Kai Fan, Qi Luo, Kuan Zhang, Yintang Yang, Cloud-based lightweight secure RFID mutual authentication protocol in IoT, Inform. Sci. 527 (2020) 329–340.

[7] Kai Fan, Qi Luo, Hui Li, Yintang Yang, Cloud-based lightweight RFID mutual authentication protocol, in: 2017 IEEE Second International Conference on Data Science in Cyberspace (DSC), IEEE, 2017, pp. 333–338.

[8] Mohd Shariq, Karan Singh, Pramod Kumar Maurya, Ali Ahmadian, Muhammad Rezal Kamel Ariffin, URASP: An ultralightweight RFID authentication scheme using permutation operation, Peer-to-Peer Netw. Appl. 14 (6) (2021) 3737–3757.

[9] Mohd Shariq, Karan Singh, Mohd Yazid Bajuri, Athanasios A Pantelous, Ali Ahmadian, Mehdi Salimi, A secure and reliable RFID authentication protocol using digital schnorr cryptosystem for IoT-enabled healthcare in COVID-19 scenario, Sustainable Cities Soc. 75 (2021) 103354.

[10] Mohd Shariq, Karan Singh, Pramod Kumar Maurya, Ali Ahmadian, David Taniar, AnonSURP: an anonymous and secure ultralightweight RFID protocol for deployment in internet of vehicles systems, J. Supercomput. 78 (6) (2022) 8577–8602.

[11] Debiao He, Sherali Zeadally, An analysis of RFID authentication schemes for internet of things in healthcare environment using elliptic curve cryptography, IEEE Internet Things J. 2 (1) (2014) 72–83.

[12] Pramod Kumar Maurya, Satya Bagchi, A secure PUF-based unilateral authentication scheme for RFID system, Wirel. Pers. Commun. 103 (2) (2018) 1699–1712.

[13] Tianjie Cao, Xiuqing Chen, Robin Doss, Jingxuan Zhai, Lucas J Wise, Qiang Zhao, RFID ownership transfer protocol based on cloud, Comput. Netw. 105 (2016) 47–59.

[14] Pramod Kumar Maurya, Satya Bagchi, Cyclic group based mutual authentication protocol for RFID system, Wirel. Netw. 26 (2) (2020) 1005–1015.

[15] Mehdi Hosseinzadeh, Jan Lansky, Amir Masoud Rahmani, Cuong Trinh, Masoumeh Safkhani, Nasour Bagheri, Bao Huynh, A new strong adversary model for RFID authentication protocols, IEEE Access 8 (2020) 125029–125045.

[16] Alaauldin Ibrahim, Gokhan Dalkılıc, Review of different classes of RFID authentication protocols, Wirel. Netw. 25 (3) (2019) 961–974.

[17] Shingo Kinoshita, Miyako Ohkubo, Fumitaka Hoshino, Gembu Morohashi, Osamu Shionoiri, Atsushi Kanai, Privacy enhanced active RFID tag, Cognit. Sci. Res. Pap. Univ. Sussex CSRP 577 (2005) 100.

[18] Sandeep Kumar, Christof Paar, Are standards compliant elliptic curve cryptosystems feasible on RFID, in: Workshop on RFID Security, Citeseer, 2006, pp. 12–14.

[19] Hung-Yu Chien, Secure access control schemes for RFID systems with anonymity, in: 7th International Conference on Mobile Data Management (MDM'06), IEEE, 2006, p. 96.

[20] Jeongkyu Yang, Jaemin Park, Hyunrok Lee, Kui Ren, Kwangjo Kim, Mutual authentication protocol for low-cost RFID, in: Workshop on RFID and Lightweight Crypto, WRLC, 2005, pp. 17–24.

[21] Julien Bringer, Hervé Chabanne, Emmanuelle Dottax, A Lightweight Authentication Protocol Secure against Some Attacks, IEEE Computer Society, Washington, DC, USA.

[22] Hung-Yu Chien, Che-Hao Chen, Mutual authentication protocol for RFID conforming to EPC class 1 generation 2 standards, Comput. Stand. Interfaces 29 (2) (2007) 254–259.

[23] Hung-Yu Chien, Chen-Wei Huang, Security of ultra-lightweight RFID authentication protocols and its improvements, Oper. Syst. Rev. 41 (4) (2007) 83–86.

[24] Ticyan Li, Guilin Wang, Security analysis of two ultra-lightweight RFID authentication protocols, in: IFIP International Information Security Conference, Springer, 2007, pp. 109–120.

[25] Tieyan Li, Robert Deng, Vulnerability analysis of EMAP-an efficient RFID mutual authentication protocol, in: The Second International Conference on Availability, Reliability and Security (ARES'07), IEEE, 2007, pp. 238–245.

[26] Hoorin Park, Heejun Roh, Wonjun Lee, Tagora: A collision-exploitative RFID authentication protocol based on cross-layer approach, IEEE Internet Things J. 7 (4) (2020) 3571–3585.

[27] Lijun Gao, Lu Zhang, Feng Lin, Maode Ma, Secure RFID authentication schemes based on security analysis and improvements of the USi protocol, IEEE Access 7 (2019) 8376–8384.

[28] Yanxiao Liu, Qindong Sun, Yichuan Wang, Lei Zhu, Wenjiang Ji, Efficient group authentication in RFID using secret sharing scheme, Cluster Comput. 22 (4) (2019) 8605–8611.

[29] Yali Liu, Xinchun Yin, Yongquan Dong, Keke Huang, Lightweight authentication scheme with inverse operation on passive rfid tags, J. Chin. Inst. Eng. 42 (1) (2019) 74–79.

[30] Liang Xiao, He Xu, Feng Zhu, Ruchuan Wang, Peng Li, SKINNY-based RFID lightweight authentication protocol, Sensors 20 (5) (2020) 1366.

[31] Yun Tian, Gongliang Chen, Jianhua Li, A new ultralightweight RFID authentication protocol with permutation, IEEE Commun. Lett. 16 (5) (2012) 702–705.

[32] Il-Soo Jeon, Eun-Jun Yoon, A new ultra-lightweight RFID authentication protocol using merge and separation operations, Int. J. Math. Anal. 7 (52) (2013) 2583–2593.

[33] Lijun Gao, Maode Ma, Yantai Shu, Yuhua Wei, An ultralightweight RFID authentication protocol with CRC and permutation, J. Netw. Comput. Appl. 41 (2014) 37–46.

[34] Kai Fan, Nan Ge, Yuanyuan Gong, Hui Li, Ruidan Su, Yintang Yang, An ultra-lightweight RFID authentication scheme for mobile commerce, Peer-to-Peer Netw. Appl. 10 (2) (2017) 368–376.

[35] Pramod Kumar Maurya, Joydeb Pal, Satya Bagchi, A coding theory based ultralightweight RFID authentication protocol with CRC, Wirel. Pers. Commun. 97 (1) (2017) 967–976.

[36] Umar Mujahid, Muhammad Najam-ul Islam, Shahzad Sarwar, A new ultralightweight RFID authentication protocol for passive low cost tags: KMAP, Wirel. Pers. Commun. 94 (3) (2017) 725–744.

[37] Aakanksha Tewari, B.B. Gupta, Cryptanalysis of a novel ultra-lightweight mutual authentication protocol for IoT devices using RFID tags, J. Supercomput. 73 (3) (2017) 1085–1102.

[38] Hanguang Luo, Guangjun Wen, Jian Su, Zhong Huang, SLAP: Succinct and lightweight authentication protocol for low-cost RFID system, Wirel. Netw. 24 (1) (2018) 69–78.

[39] Yali Liu, Martianus Frederic Ezerman, Huaxiong Wang, Double verification protocol via secret sharing for low-cost RFID tags, Future Gener. Comput. Syst. 90 (2019) 118–128.

[40] Atul Kumar, Ankit Kumar Jain, Mutual authentication protocol for low cost passive tag in RFID system, Int. J. Inform. Technol. (2021) 1–7.

[41] Pedro Peris-Lopez, Julio Cesar Hernandez-Castro, Juan M Estévez-Tapiador, Arturo Ribagorda, LMAP: A real lightweight mutual authentication protocol for low-cost RFID tags, in: Proc. of 2nd Workshop on RFID Security, Vol. 6, 2006.

[42] Pedro Peris-Lopez, Julio Cesar Hernandez-Castro, Juan M Estevez-Tapiador, Arturo Ribagorda, M^2AP: a minimalist mutual-authentication protocol for low-cost RFID tags, in: International Conference on Ubiquitous Intelligence and Computing, Springer, 2006, pp. 912–923.

[43] Pedro Peris-Lopez, Julio Cesar Hernandez-Castro, Juan M Estevez-Tapiador, Arturo Ribagorda, EMAP: An efficient mutual-authentication protocol for low-cost RFID tags, in: OTM Confederated International Conferences "on the Move to Meaningful Internet Systems", Springer, 2006, pp. 352–361.

[44] Lijun Gao, Maode Ma, Yantai Shu, Yuhua Wei, An ultralightweight RFID authentication protocol with CRC and permutation, J. Netw. Comput. Appl. 41 (2014) 37–46.

[45] Mete Akgün, M. Ufuk Çağlayan, On the security of recently proposed RFID protocols, IACR Cryptol. ePrint Arch. 2013 (2013) 820.

[46] Masoumeh Safkhani, Nasour Bagheri, Generalized desynchronization attack on UMAP: Application to RCIA, KMAP, SLAP and SASI+ protocols, IACR Cryptol. ePrint Arch. 2016 (2016) 905.

[47] Paolo D'Arco, Roberto De Prisco, Design weaknesses in recent ultralightweight RFID authentication protocols, in: IFIP International Conference on ICT Systems Security and Privacy Protection, Springer, 2018, pp. 3–17.

[48] King-Hang Wang, Chien-Ming Chen, Weicheng Fang, Tsu-Yang Wu, On the security of a new ultra-lightweight authentication protocol in IoT environment for RFID tags, J. Supercomput. 74 (1) (2018) 65–70.

[49] Lijuan Zheng, Chunlei Song, Ning Cao, Zhaoxuan Li, Wenfeng Zhou, Jianyou Chen, Lili Meng, A new mutual authentication protocol in mobile RFID for smart campus, IEEE Access 6 (2018) 60996–61005.

[50] Masoumeh Safkhani, Athanasios Vasilakos, A new secure authentication protocol for telecare medicine information system and smart campus, IEEE Access 7 (2019) 23514–23526.

[51] Mehdi Hosseinzadeh, Omed Hassan Ahmed, Sarkar Hasan Ahmed, Cuong Trinh, Nasour Bagheri, Saru Kumari, Jan Lansky, Bao Huynh, An enhanced authentication protocol for RFID systems, IEEE Access 8 (2020) 126977–126987.

[52] Cuong Trinh, Bao Huynh, Jan Lansky, Stanislava Mildeova, Masoumeh Safkhani, Nasour Bagheri, Saru Kumari, Mehdi Hosseinzadeh, A novel lightweight block cipher-based mutual authentication protocol for constrained environments, IEEE Access 8 (2020) 165536–165550.

[53] Hung-Yu Chien, SASI: A new ultralightweight RFID authentication protocol providing strong authentication and strong integrity, IEEE Trans. Dependable Secure Comput. 4 (4) (2007) 337–340.

[54] Mathieu David, Neeli R. Prasad, Providing strong security and high privacy in low-cost RFID networks, in: International Conference on Security and Privacy in Mobile Information and Communication Systems, Springer, 2009, pp. 172–179.

[55] Pedro Peris-Lopez, Julio Cesar Hernandez-Castro, Juan ME Tapiador, Arturo Ribagorda, Advances in ultralightweight cryptography for low-cost RFID tags: Gossamer protocol, in: International Workshop on Information Security Applications, Springer, 2008, pp. 56–68.

[56] Xu Zhuang, Yan Zhu, Chin-Chen Chang, A new ultralightweight RFID protocol for low-cost tags: R^2AP, Wirel. Pers. Commun. 79 (3) (2014) 1787–1802.

[57] Umar Mujahid, Muhammad Najam-ul Islam, M. Ali Shami, RCIA: A new ultralightweight RFID authentication protocol using recursive hash, Int. J. Distrib. Sens. Netw. 11 (1) (2015) 642180.

[58] Madiha Khalid, Umar Mujahid, M Najam-ul Islam, Hongsik Choi, Imtiaz Alam, Shahzad Sarwar, Ultralightweight resilient mutual authentication protocol for IoT based edge networks, J. Ambient Intell. Humaniz. Comput. (2021) 1–12.

[59] C. Cremers, Scyther tool, 2021, http://www.cs.ox.ac.uk/people/cas.cremers/scyther/. [Online; Accessed on March 10, 2021].

MOHD SHARIQ received his B.Tech. degree in Computer Science and Engineering from Gautam Buddha Technical University, India, and M.Tech. degree in Computer Science and Technology from the School of Computer and Systems Sciences, JNU, New Delhi, India in 2017. He has submitted his Ph.D. thesis in the School of Computer and Systems Sciences, JNU, New Delhi. His primary research interests include RFID security protocols design, security and privacy, lightweight RFID authentication, and information security. He has published several research papers in reputed journals.

KARAN SINGH received the Engineering degree (Computer Science & Engineering) from Kamala Nehru Institute of Technology, Sultanpur, UP, India. He is the M.Tech. (Computer Science & Engineering) and Ph.D. (Computer Science & Engineering) from Motilal Nehru National Institute of Technology UP, India. He worked at Gautam Buddha University, UP, India. Currently, he is working with the School of Computer & Systems Sciences, Jawaharlal Nehru University, New Delhi. His primary research interests are in Computer network, Network security, Multicast communication, IoT, and Body Area network. He is the supervisor of many research scholars. He is a reviewer of Springer, Taylor & Francis, Elsevier Journals and IEEE Transactions. He is an Editorial Board Member of Journal of Communications and Network (CN), USA. He published 70+ research papers in refereed journals and good conferences. He organized the workshops, conference sessions, and training. Dr. Singh worked as General Chair of the international conference (Qshine 2013) at Gautam Buddha University, India. Recently he organized a conference ICCCS 2018 at Dronacharya College of Engineering, Gurgaon and a special session in 2nd ICGCET 2018 at Denmark.

CHHAGAN LAL received the Ph.D. degree in computer science and engineering from the Malaviya National Institute of Technology, Jaipur, India, in 2014. He is currently working as a Postdoctoral Research Fellow of the Delft University of Technology, The Netherlands. Previously, he was a Postdoctoral Fellow of the Department of Mathematics, University of Padua, Italy, where he was part of the SPRITZ Research Group. He was a Postdoctoral Research Fellow of Simula Research Laboratory, Norway. His current research areas include applications of blockchain technologies, security in software-defined networking, and Internet-of-Things networks. During his Ph.D, he was awarded the Canadian Commonwealth Scholarship under the Canadian Commonwealth Scholarship Program to work in the University of Saskatchewan, Saskatoon, SK, Canada.

MAURO CONTI received the Ph.D. degree from the Sapienza University of Rome, Italy, in 2009. He is a Full Professor with the University of Padua, Italy. He is also affiliated with TU Delft and the University of Washington, Seattle. After his Ph.D., he was a Postdoctoral Researcher with Vrije Universiteit Amsterdam, The Netherlands. In 2011, he joined as an Assistant Professor with the University of Padua, where he became an Associate Professor in 2015, and a Full Professor in 2018. He has been Visiting Researcher with GMU, UCLA, UCI, TU Darmstadt, UF, and FIU. His research is also funded by companies, including Cisco, Intel, and Huawei. His main research interest is in the area of security and privacy. In this area, he published more than 400 papers in topmost international peer-reviewed journals and conferences. He has been awarded the Marie Curie Fellowship by the European Commission in 2012, and a Fellowship by the German DAAD in 2013. He is an Area Editor-in-Chief for IEEE COMMUNICATIONS SURVEYS AND TUTORIALS, and he has been an Associate Editor for several journals, including IEEE COMMUNICATIONS SURVEYS AND TUTORIALS, IEEE TRANSACTIONS ON DEPENDABLE AND SECURE COMPUTING, IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, and IEEE TRANSACTIONS ON NETWORK AND SERVICE MANAGEMENT. He was a Program Chair for TRUST 2015, ICISS 2016, WiSec 2017, and ACNS 2020, and a General Chair for SecureComm 2012, SACMAT 2013, CANS 2021, and ACNS 2022. He is a Senior Member of ACM. He is a member of the Blockchain Expert Panel of the Italian Government. He is Fellow of the Young Academy of Europe.

TAYYAB KHAN received the Engineering degree in Computer Science & Engineering from Gautam Buddh Technical University, UP, India. He has completed his M.Tech. and PHD in Computer Science & Engineering from the school of computer and systems sciences, JNU New Delhi, India in OCT 2016 from the school of computer and systems sciences, JNU New Delhi, India. He has published various research papers in reputed journals. His primary research interests are in the Trust modeling, wireless sensor network, Body sensor networks, Network security, Multicast communication. He published many research papers in refereed journals and good conferences. He organized the workshops, conference sessions, and training.