IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received February 21, 2021, accepted March 24, 2021, date of publication March 29, 2021, date of current version April 6, 2021.

Digital Object Identifier 10.1109/ACCESS.2021.3069429

RFID Authentication Scheme Based on Hyperelliptic Curve Signcryption

USMAN ALI[1,2], (Graduate Student Member, IEEE), MOHD YAMANI IDNA BIN IDRIS[3], (Member, IEEE), MOHAMAD NIZAM BIN AYUB[1], INSAF ULLAH[4], IHSAN ALI[1], TARAK NANDY[1], (Graduate Student Member, IEEE), MUKTAR YAHUZA[1], (Graduate Student Member, IEEE), AND NAUMAN KHAN (Graduate Student Member, IEEE) [1]

[1]Department of Computer System and Technology, Faculty of Computer Science and Information Technology, University of Malaya, Kuala Lumpur 50603, Malaysia
[2]Department of Computer Science, University of Swat, Saidu Sharif 19130, Pakistan
[3]Center for Research in Mobile Cloud Computing, University of Malaya, Kuala Lumpur 50603, Malaysia
[4]Department of Computer Science, Hamdard Institute of Engineering and Technology, Islamabad 44000, Pakistan

Corresponding authors: Usman Ali (usmanali838@ieee.org), Mohd Yamani Idna Bin Idris (yamani@um.edu.my), and Mohamad Nizam Bin Ayub (nizam_ayub@um.edu.my)

This work was supported in part by the University of Malaya Impact Oriented Interdisciplinary Research Grant under Grant IIRG003 (A,B,C)-19IISS, and in part by the Ministry of Higher Education Malaysia Fundamental Research Grant Scheme (FRGS) under Grant FP055-2019A.

ABSTRACT The implementation of efficient security mechanisms for Radio Frequency Identification (RFID) system has always been a continuous challenge due to its limited computing resources. Previously, hash-based, symmetric-key cryptography-based and elliptic curve cryptography based security protocols were proposed for RFID system. However, these protocols are not suitable because some of them failed to fulfil the RFID security requirements, and some of them produce high computational overhead. Recently researchers have focused on developing an efficient security mechanism based on Hyper Elliptic Curve Cryptography (HECC) which provides high security with 80 bits lower-key size. In this paper, we propose an efficient RFID authentication scheme (RFID-AS) based on hyperelliptic curve Signcryption. The proposed RFID-AS provides the required security features for the RFID system as well as security from potential attacks. We validated the security of proposed RFID-AS by using formal security analysis techniques, such as the Real-Or-Random (ROR) model and Automated Validation of Internet Security Protocols and Applications (AVISPA). Furthermore, the results reveal that the computational, communication and storage overheads of the proposed RFID-AS is much less than the other recently proposed schemes. Compared to the most recently published work based on ECC Signcryption, our scheme is 70% efficient in terms of computational overhead, 42.7% efficient in terms of communication overhead, and 57.7% efficient in terms of storage overhead. Therefore, the proposed RFID-AS is more efficient as compared to the recently published work in this domain. Hence, it is an attractive solution for resource-limited devices like RFID tags.

INDEX TERMS Hyperelliptic curve cryptography, RFID, authentication protocol, AVISPA.

I. INTRODUCTION

The rapidly evolving computing age has enabled all sorts of possibilities to automate processes and recognize items that have now become crucial components of computing due to the fact it saves time and produces minimal errors as they pave the way to substantial productivity benefits. As of now, bar codes, voice recognition, optical character recognition, smart cards, magnetic stripes, chip cards, biometrics, and RFID are among the multitude of technologies that have been developed to incorporate Automatic Identification and Data Capture (AIDC). RFID has been proved to be the most popular AIDC technology in recent years [1]. According to Jia *et al.* [2], the use of RFID has grown exponentially with the development of IoT, as the core technology behind it. RFID is a wireless communication technology

The associate editor coordinating the review of this manuscript and approving it for publication was Shaohua Wan.

TABLE 1. Classification of RFID tags [5], [6].

Specification	Active Tags	Semi Passive Tags	Passive Tags
Cost	High	High	Low
Size	Large	Large	Small
Storage	Read/write memory	Read/write memory	Read memory
Power	Integrated battery	Internal chip battery	Surrounding signal
Distance	1000 m	100 m	5 m
Lifespan	10 years	10 years	Unlimited
Tag Signal	High	High	Low
Required Signal	Low	Low	High
Application	Environmental and logistic	Real-time tracking	Identification

using radio frequency electromagnetic signals to detect and identify objects bearing tags [3]. There are three main communication components in an RFID system, namely: server, tag (transponder) and reader (Interrogator), as shown in Figure 1. In an RFID system, the basic communication session begins when the reader broadcasts radio waves to interrogate the tag and the tag responds to the reader's signal. RFID tags are classified into three distinct types: active tags, semi-passive tags and passive tags as shown in Table 1. An active tag carries onboard power-source that keeps the tag active to transfer its data to an even larger range while a semi-passive tag has a minuscule onboard power-source; however, it only activates the tag in the presence of a nearby RFID reader. On the other hand, a passive tag has no onboard power-source. It can obtain the power required for activating the tag from the nearby RFID reader.

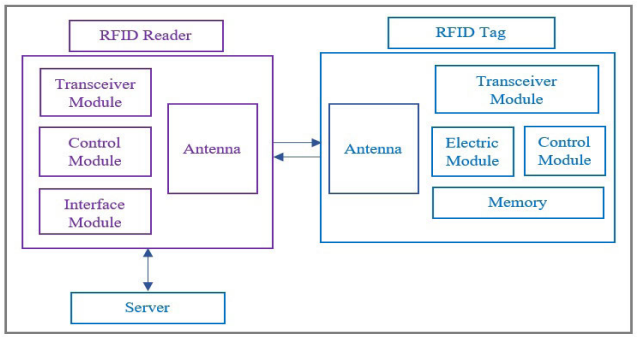


FIGURE 1. Communication components of an RFID System.

In general, an RFID tag contains a unique ID number, location information, object description such as price, date, etc. The ID helps the server to identify the tag distinctively in the presence of many tags. When a tag-carrying object enters the RFID reader region, its data is collected wirelessly and sent to the server for storage and user application requirements.

Khattab *et al.* [4] have discovered that when compared to various parameters, RFID outperforms other AIDC techniques, including data density, machine readability, human readability, cost, reading speed, range, moisture effect, and distraction of sight. However, RFID systems have some limitations, including less storage capacity and low processing speed of the tag. With such inadequate computational resources, designing and implementing security schemes that provide security features has been very demanding. Furthermore, the information is being transmitted between tags and readers wirelessly and is susceptible to attacks by the eavesdropper and illegitimate reader due to insecure wireless channels.

Several authors have addressed security concerns and challenges for RFID. Guizani *et al.* [7] and Kannouf *et al.* [8] presented an overview of RFID system threats and attacks. Khattab *et al.* [9] carried out a detailed analysis of RFID system attacks. They categorized RFID attacks into particularly three types: physical attacks, device attacks, and channel attacks. To prevent physical attacks, it is possible to avoid tag alteration or tampering by establishing a protected zone around the device using the device's sealed tamper-resistant case. Additionally, by using spread spectrum technologies and antenna polarization, the jamming attack can be countered. Furthermore, using a strong cryptographic scheme, the device attacks and other channel attacks can be prevented. Consequently, the cryptographic scheme must fulfill an RFID system's security requirements such as authentication, confidentiality, non-repudiation, integrity, anonymity, forward security, availability, and scalability. The cryptographic schemes that are prospective candidates to protect any information system are Symmetric Key Cryptography (SKC) [10], [11], RSA based cryptography [12], [13], Elliptic Curve Cryptography (ECC) [14], [15], and Hyper Elliptic Curve Cryptography (HECC) [16], [17]. A comparison of these cryptographic systems based on various aspects has been presented in Table 2.

It can be observed from Table 2 that SKC based schemes have a big issue with key distribution, while RSA based schemes have high computational cost due to modular exponential computation. ECC-based schemes perform better than the RSA, while HECC performs better than ECC by providing the same security features with less computation cost, communication overhead, and memory requirement.

HECC based schemes require less storage, smaller key size, quicker in key generation. They produce smaller ciphertext as compared to other Public Key Cryptography (PKC) schemes. Due to these features, HECC is an attractive cryptographic scheme to offer security for systems having limited computational resources such as RFID. Zheng [18] introduces the concept of Signcryption, which combines encryption as well as authentication in a single logical step. Before the actual advent of Signcryption, the technique was to use encryption-then-signature to achieve secrecy and authentication. Zheng showed that Signcryption saves 50% of computing time and 85% of communication costs compared to the process of signature-then-encryption.

A. MOTIVATION AND CONTRIBUTION

Providing security in all fields of computing and communication has always been a priority. However, implementing efficient and appropriate RFID system security mechanisms has been a continuous challenge because of limited computing resources. RFID system requires a security mechanism, that minimizes computational, communication and storage overhead. Recently Singh *et al.* [19] suggested Elliptic Curve Signcryption based RFID authentication protocol. The security and efficacy of their proposed protocol are based on ECC. Even though ECC utilizes 160-bit small keys and fewer parameter sizes as compared to RSA however, 160-bit key size is still not well suited for resource-limited devices like RFID tags. ECC has higher computation overhead and generates excessive communication cost compared to HECC having 80-bits key size [20] that generates less communication and computational cost than ECC. Hence, their proposed protocol does not fulfill performance efficiency because their scheme generates excessive communication overhead computational overhead. Furthermore, there is no verification of the security of their proposed method by using any verification tools such as Scyther and AVISPA. It is crucial to design authentication protocol, to eliminate all the above limitations, and to fulfill the security requirements of resource-limited RFID systems. We describe our main contributions as following.

- We designed an RFID authentication scheme (RFID-AS) based on hyperelliptic curve Signcryption
- We have shown that our scheme provides the required security features such as: authentication, confidentiality, non-repudiation, integrity, anonymity, forward security, availability and scalability.
- We have shown that our scheme provides security against replay, man-in-the-middle (MiM), impersonation, cloning, location tracking, desynchronization, Denial of Service (DoS), and key compromise attacks.
- The results of proposed RFID-AS confirm its efficiency in terms of Computational, Communication and Storage overhead.
- We validated our proposed scheme's security by using formal security analysis techniques,such as the Real-Or-Random (ROR) model and Automated Validation of Internet Security Protocols andApplications (AVISPA).

B. STRUCTURE OF THE PAPER

The rest of the paper is organized as follows. Section 2 overviews the related work. Section 3 discusses the system model. Section 4 explains the proposed authentication scheme. Section 5 demonstrates the proof of the correctness of the proposed protocol. Section 6 provides security analysis. Section 7 shows the comparative analysis. Section 8 provides the conclusion and finally, section 9 provides the future work.

II. RELATED WORK

Due to the lower computational capability of RFID tags, protection and privacy have been the main concern for RFID systems. Over the years, several security solutions providing various security features have been suggested. However, a great deal of emphasis has been placed on the design of secure authentication schemes for RFID. Also, several ECC-based schemes have been suggested in recent years, as ECC-based solutions are comparatively better than RSA and other PKC schemes. Gódor *et al.* [21] suggested ECC-based RFID authentication, which provides confidentiality and authentication while providing resistance against replay attacks. They also measured the computational time of various operations in the protocol. However, several required security attributes were not enforced in this scheme, and it could not deter DoS attacks. Lee *et al.* [22] revealed the problems of un-traceability and anti-counterfeiting in RFID systems. They proposed a protection framework that offered several security features but failed to meet mutual authentication, scalability, and resistance to desynchronization attacks. Safkhani *et al.* [23] suggested authentication scheme that provides security against tag impersonation attack. However, their scheme is susceptible to other attacks. Safkhani *et al.* [24] also suggested a hash-based scheme for mutual authentication. However, their scheme is computationally inefficient as the server needs to check all the entries in the database. Peris-Lopez *et al.* [25] suggested grouping proofs based protocol to safeguard tag impersonation attacks. However, this protocol suffers from concurrency attack. Liu *et al.* [26] proposed ECC-based RFID authentication, which reduces RFID tag computation cost and provides mutual authentication, confidentiality, and anonymity. The protocol was capable of defending against desynchronization attacks, counterfeit attacks, and replay attacks. Liao *et al.* [27] suggested an RFID authentication protocol based on an elliptic curve that utilizes secure challenge-response and ID-verifier messages to be transferred. However, their protocol suffers from a key compromise attack where the key contained in the tag can be recovered by an attacker. Zhao [28] proposed an improved authentication protocol that is safer and powerful than the Liao scheme. However, Farash [29] showed that the Zaho scheme unsuccessful in offering forward security. Chou [30] categorized the RFID authentication schemes as ultra-lightweight, lightweight, simple, and full-fledged. Chou

stated that full-fledged authentication schemes are attractive because non-full-fledged authentication schemes are susceptible to tracking and desynchronization attacks. Chou also suggested an ECC-based authentication scheme and asserted that it also offers forward anonymity and scalability in addition to location privacy and mutual authentication, while also offering security against DoS, replay, and MiM attack. Farash [31] has shown that the Chou scheme failed to provide forward secrecy, confidentiality, and mutual authentication. Furthermore, Chou protocol was proven to have failed to protect against tracking attacks, cloning attacks, and impersonation and attacks. Farash also suggested an enhanced authentication scheme that can address impersonation, tracking attacks, MiM attacks, and offer mutual authentication, confidentiality, and forward secrecy. However, this protocol's total computational time takes an even greater amount than existing RFID authentication schemes. Zhang *et al.* [32] suggested an ECC-based scheme, which provides session initiation anonymity. Conversely, Lu *et al.* [33] revealed that Zhang *et al.* protocol failed to offer mutual authentication. Lu *et al.* also suggested an updated authentication protocol to resolve the security vulnerabilities of the Zhang scheme. Mehmood *et al.* [34] exposed that Lu *et al.* protocol is unable to protect the user's identity and does not provide resistance against masquerade attack. Mehmood *et al.* also suggested an enhanced mutual authentication scheme that provides anonymity, forward confidentiality, mutual authentication, forward protection, and session key privacy. Additionally, their scheme provides security against masquerade, replay, and MiM attacks. Feng *et al.* [35] suggested an ECC-based RFID security scheme that provides resistance against Dos, tracking, impersonation, and replay attacks. They asserted that their proposed scheme requires less communication overhead, storage costs, and processing time. Chen *et al.* [36] analyzed several ECC-based full-fledged RFID authentication schemes. They pointed out that some of these schemes have privacy and security drawbacks, while some schemes produce high communication costs. Chen *et al.* also suggested two authentication schemes and stated that their schemes are efficient and secure. Shen *et al.* [37], revealed that the Chen *et al.* protocol is susceptible to spoofing attacks and replay attacks. Alamr *et al.* [38] proposed an RFID authentication scheme using ECC based Diffie-Hellman key exchange concept to compute the secret key. This key, in turn, is utilized for the messages to be encrypted. Their protocol provides mutual authentication, confidentiality, anonymity, privacy and offers resistance to replay, impersonation, and MiM attacks. Qian *et al.* [39] suggested a lightweight RFID security protocol using ECC encryption and simple operations such as bitwise AND, XOR, etc. This scheme decreases the tag computation cost, as it does not use the operation of the elliptic curve scalar multiplication. However, this scheme is restricted to providing confidentiality, authentication, and forward secrecy only. Bagheri *et al.* [40] proposed anti-collision RFID protocol. However, their protocol does not guarantee that all the tags are identified. Zheng *et al.* [41] suggested ECC-based RFID authentication that provides privacy, forward security, scalability, anonymity, and mutual authentication. Their protocol also offers resistance against DoS attacks, internal attacks, and tracking attacks. Chiou *et al.* [42] proposed an authentication protocol. However, in this protocol, the tag must perform five elliptic curve scalar multiplication (ECSM) operations, which increase computational cost. Therefore, this scheme is computationally inefficient and not appropriate for RFID systems. Liu *et al.* [43] proposed a security scheme for mobile RFID systems and mentioned that their approach is more efficient and can withstand all known attacks. Conversely, by observing the authentication stage of the protocol, it can be determined that the tag must execute four ECSM operations, which increases the tag computation cost. Therefore, this scheme is computationally inefficient and not appropriate for RFID systems. A lightweight RFID protection protocol for medical privacy was proposed by Fan *et al.* [44] and stated that it ensures confidentiality and secure authentication. This scheme is based on a simple operation such as XOR operation, hash computation, displacement operation, and cross operation. However, Aghili *et al.* [45] carried out a thorough review of the Fan *et al.* scheme and exposed that it is susceptible to secret information disclosures and impersonation attacks. Dinarvand *et al.* [46] suggested an ECC-based RFID authentication scheme that achieves authentication, non-repudiation, confidentiality, integrity, anonymity, forward security, availability, and scalability. Furthermore, their protocol is secure against tracking, de-synchronization, server spoofing, and replay attacks. Recently Singh *et al.* [19] proposed an RFID authentication protocol based on Elliptic Curve Signcryption. They also demonstrated that the computation cost and communication overhead of their proposed scheme is less than others. As the security and efficiency of the authentication, protocols described in the above literature are based on an elliptic curve, using 160-bits key size, which generates excessive communication overhead as compared to the hyperelliptic curve with 80-bits lower-key size as shown in Table 2. Even though ECC utilizes 160-bit small keys and fewer parameter sizes as compared to RSA but still the 160-bit key size is not well suited for resource-limited devices like RFID tags.

III. SYSTEM MODEL

This section describes the system architecture and threat model for the proposed scheme.

A. SYSTEM ARCHITECTURE

Primarily, an RFID system comprises three main communication components, namely a server, tag, and a reader as shown in Figure 2. In an RFID system, the basic communication session begins when the reader broadcast radio signal and the tag responds to the reader's signal. In the proposed RFID-AS, server and reader are communicating through a secure wired channel while the tag and reader are communicating through an insecure wireless channel. The server is a central database device that manages information related to the tags

TABLE 2. Comparison of different cryptographic schemes.

Evaluation parameters	Cryptographic Primitives			
	SKC	RSA	ECC	HECC
Computational cost	low	very high	high	lower than ECC
Communication overhead	low	very high	low	lower than ECC
Order of no of key	$O(n^2)$	$O(n)$	$O(n)$	$O(n)$
Key distribution	big problem	simple	simple	simple
Key bits for same security level	80 bit	1024 bit	160 bit	80 bit
Speed of key generation	speedy	very slow	speedy	speedy than ECC
Complexity	$O(n)$	$O(n^3)$	$O(n^2)$	$O(n^2)$
Memory requirement	very less	very large	Less	less than ECC

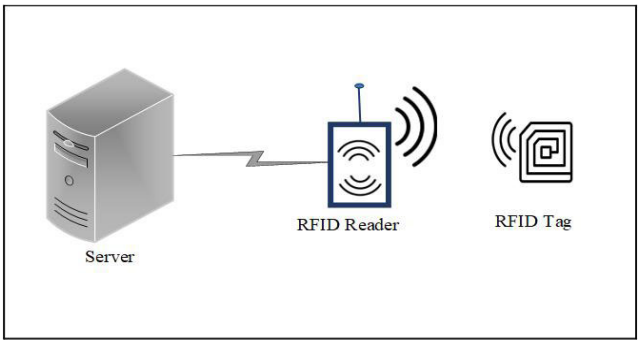


FIGURE 2. Schematic diagram of RFID system.

and reader. The reader collects the information of the tag and forwards it to the server to authenticated the tag.

B. THREAT MODEL

We considered Dolve–Yao threat model [47] for our proposed scheme. In this model the adversary has full control over the communication channel between tag and reader, and can thereby intercept, analyze, modify messages (as far as he knows the session key) and can replay the messages to the tag and reader.

IV. PROPOSED SCHEME

In this section, the background information required in the designing of the proposed scheme is first explained. Next, the working of the proposed authentication scheme is described in detail.

A. BACKGROUND DETAILS

Hyper elliptic Curve cryptography (HECC): Hyperelliptic curves (HEC) are algebraic curves with genus $g > 1$ [16]. HEC are also known as generalized form of elliptic curves (EC) that have g=1. The difference between HECC and ECC is group operation. Unlike the EC, the points on the HEC cannot form a group; rather it generates an additive Abelian group, derived from the divisor class group. HEC of genus 2 with 80-bits field size can be constructed to attain similar security as 160-bits ECC [20]. A HEC of g=2 over $F(2^m)$, is a set of solution (x, y) $\in$ [$F(2^m)$ x $F(2^m)$] and is given by the equation (1):

$$E : y^2 + h(x)y = f(x) \tag{1}$$

where [x,y] $\in$ $F(2^m)$, h(x) $\in$ $F(2^m)$ [x] is a polynomial with degree $deg(h)?g$ and f(x) $\in$ $F(2^m)$ [x] is a monic polynomial of degree $deg(f) = 2g + 1$. Additional requirements for the curve is it must be non-singular curve. A divisor D as shown in equation (2), is a finite formal sum of scalar multiples of points in curve E.

$$D = \sum(m_p[P]) \tag{2}$$

where $m_p \in$ Z, and [P] represent points on the hyperelliptic curve E.

B. PROPOSED AUTHENTICATION SCHEME

Our proposed RFID authentication scheme (RFID-AS) is based on HEC Signcryption and is consisted of three phases: Setup, Authentication, and Update. The flowchart of our proposed scheme is shown in Figure 3. it is assumed that the data transmission from reader to server and vice versa is secure due to wired channel, whereas the data transmission from reader to tag and vice versa is insecure due to insecure wireless channel.

Table 3 shows the symbols and notations used to describe the scheme. The scheme is applicable to passive tag, semi-active tag and active tag.

1) SETUP PHASE

The server in the Setup phase, performs the following operations to select and assign initial values to system parameters.

i Selects a hyperelliptic curve $E : y^2 + h(x)y = f(x)$ with the curve parameters $\{F_q, F_q^*$, q, x, y, D$\}$.
ii Selects a unique identifier T_{id} for each tag such as T_{id} =i.D, where i $\in$ {1, q–1} is a random integer.
iii Selects a random integer $T_{pn} \in_R$ {1, q–1}, as the unique pseudonym for each tag.

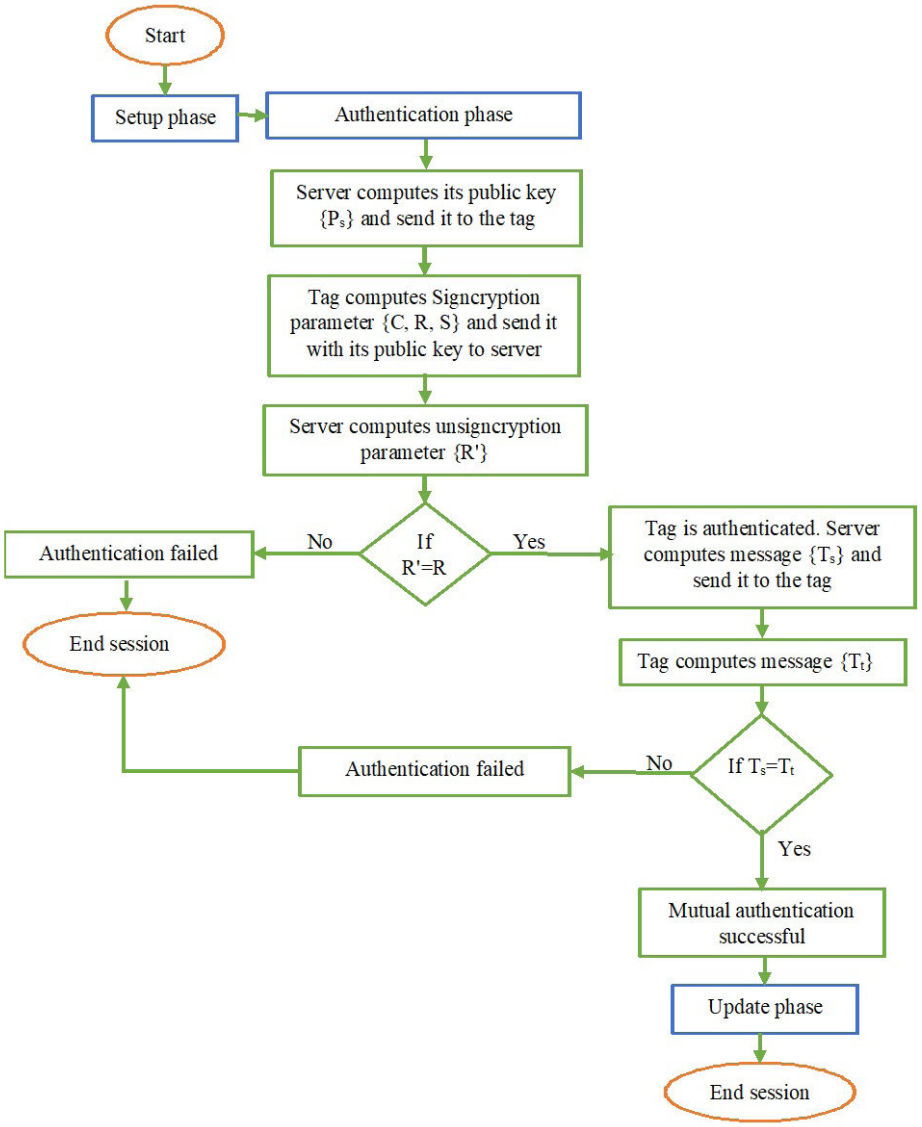


FIGURE 3. Flowchat of the proposed scheme.

iv Selects a unique identifier X_{id} for server such as X_{id} =j.D, where j $\in$ {1, q–1} is a random integer.
v Selects a one-way hash function
vi The server stores $\{T_{id}, T_{pn}\}$ for every tag in its database.
vii The server also stores $\{T_{id}, T_{pn}, X_{id}\}$ and $\{F_q, F_q^*$, q, x, y, D$\}$, in the memory of each tag.

2) AUTHENTICATION PHASE

The tag and server simultaneously authenticate each other by using the concept of signcryption-unsigncryption, in which authentication and confidentiality attributes are implemented together. The tag performs the signcryption operation while the server performs the unsigncryption operation. The complete work flow of the protocol has been presented in Figure 4. The following steps carried out in this phase:

1) For every session, the server initializes its private key V_s with a random number $\in$ {1, q–1}. The server then compute public key P_s as and shown in Eq (3) and send it to the tag:

$$P_s = V_s D \tag{3}$$

2) The tag after receiving $\{P_s\}$, performs the Signcryption operation to obtain its Signcryption parameters C, R and S as follows:
   i For every session the tag initialize its private key V_t with random integer $\in$ {1, q–1} and compute its public key P_t as:

$$P_t = V_t D \tag{4}$$

   ii The tag computes its secret key K as:

$$K = hash(V_t P_s \oplus X_{id}) \tag{5}$$

TABLE 3. Symbols and notations used in the protocol.

Notation	Description
E	Hyperelliptic curve: $y^2+h(x)y = f(x)$
F_q	Finite prime field of size $q = 2^{80}$
F_q^*	Algebraic closure of F_q
x, y	curve parameters
D	Divisor of HEC
V_s	Server private key
V_t	Tag private key
P_s	Server public key
P_t	Tag public key
T_{id}	Tag unique identifier
T_{pn}	Tag unique pseudonym
X_{id}	Server identifier
K	Secret Key
E_k	Encryption using K
D_k	Decryption using K
$hash$	One-way hash function

iii The tag encrypt its pseudonym to obtain the first Signcryption parameter C as:

$$C = E_K(T_{pn}) \tag{6}$$

iv The tag apply hash function to the XOR of tag-identifier and tag-pseudonym to obtain second Signcryption parameter R as:

$$R = hash(T_{pn} \oplus T_{id} \oplus X_{id}) \tag{7}$$

v After computing R, the tag can now obtain its third Signcryption parameter S as:

$$S = (V_t/(V_t + R))modq \tag{8}$$

vi The tag then sends C, R, S and P_t to the server.

3) The server performs the unsigncyption operation after receiving the Signcryption parameters C, R, S and tag public key P_t.

i Computes its secret key K' as:

$$K' = hash(S.V_s(P_t + R.D) \oplus X_{id}) \tag{9}$$

ii Decrypts C by using K' to obtain first unsigncrypted parameter T'_{pn} as:

$$T'_{pn} = D_{K'}(C) \tag{10}$$

iii Search its database to find the corresponding tag identifier T_{id} and if it is not found then the session is terminated, otherwise the second unsigncrypted parameter R' is computed as:

$$R' = hash(T'_{pn} \oplus T_{id} \oplus X_{id}) \tag{11}$$

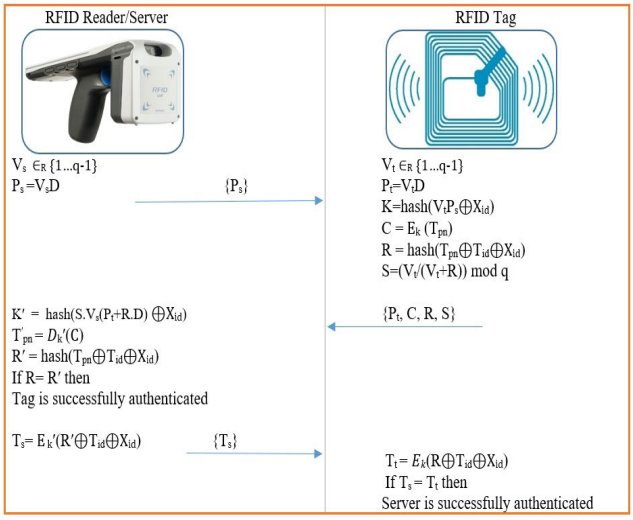


FIGURE 4. Proposed RFID authentication protocol.

iv If $R = R'$, then server authenticate tag successfully, If $R \neq R'$ then authentication failed and session is terminated.

v After tag authentication, the server computes authentication message $\{T_s\}$ as:

$$T_s = E_{K'}(R' \oplus T_{id} \oplus X_{id}) \tag{12}$$

and sends $\{T_s\}$ to the tag.

4) Once the tag receive the authentication message $\{T_s\}$, it computes T_t as:

$$T_t = E_K(R \oplus T_{id} \oplus X_{id}) \tag{13}$$

If $T_s = T_t$, then server authentication by tag is successful and if $T_s \neq T_t$, then authentication is unsuccessful and session is dismissed.

3) UPDATE PHASE

Upon successful mutual authentication of tag and server, both of them must update the value of T_{pn}, so that it can be protected from desynchronization attack and unauthorized usage. The tag updates the T_{pn} by performing the following operation:

$$T_{pn}^{new} = (K \oplus T_{id} \oplus T_{pn} \oplus X_{id}) \tag{14}$$

The server updates the Tpn by performing the following operation:

$$T_{pn}^{new} = (K' \oplus T_{id} \oplus T'_{pn} \oplus X_{id}) \tag{15}$$

V. PROOF OF CORRECTNESS

The accuracy of our proposed RFID-AS is based on the fact that the same secret key has been produced by both parties in authentication phase. According to Eq. (5), the tag computes its secret key as shown below.

$K = hash(V_tP_s \oplus X_{id})$, where $P_s = V_sD$

$K = hash(V_tV_sD \oplus X_{id})$.

According to Eq. (9), the server computed its secret key as shown below.

$K' = hash(S.V_s(P_t + R.D) \oplus X_{id})$, where $P_t = V_t D$.

$K' = hash(S.V_s(V_t D + R.D) \oplus X_{id})$

$K' = hash(S.V_s.D(V_t + R) \oplus X_{id})$ where $S = (V_t/(V_t + R))modq$

$K' = hash(V_t/(V_t + R).V_s.D(V_t + R) \oplus X_{id})$

$K' = hash(V_t.V_s.D \oplus X_{id}) = K$

Since $K = K'$, hence the proposed scheme correctness is verified.

VI. SECURITY ANALYSIS

Definition 1 (Collision-Resistant Cryptographic One-Way Hash Function H(.)): "It is a mathematical function reperesented by $H(.)$, that accepts a variable-length input string and produces a n-bits fixed-length output string i.e. $H(.) : \{0, 1\}^* \rightarrow \{0, 1\}^n$. According to the definition of $H(.)$, it is infeasible to produce the input string, given the output string, and for the same input string, it will always produce the same output".

Definition 2 (Hyper Elliptic Curve Discrete Logarithm Problem (HECDLP)): "According to HECDLP, it is computationally hard to compute an integer $d \in \{1, \ldots q-1\}$ given D and $p = d.D$, where q $\approx 2^{80}$".

A. FORMAL SECURITY ANALYSIS THROUGH ROR MODEL

We have used the Real-Or-Random (ROR) model [48] for the formal security analysis of our proposed (RFID-AS). According to this model, an active adversary A tries to target the communication among the participants by simulating real (actual) attacks using "Execute, Send, Reveal and Test queries". In the proposed RFID-AS, the participants are tag T_i and reader R and the corresponding participant instances are represented as π_{T_i} and π_R respectively. We assume that A interact with $\pi_i = (\pi_{T_i}, \pi_R)$, where π_i, represent an instance of executing participant. The queries initiated by the adversary A, are described below:

Execute query: This query enables A to intercept (eavesdrop) all the messages exchanged between π_{T_i} and π_R.

Send query: In this query A can send a message Msg to π_i, and receive a response from π_i accordingly.

Reveal query: This query enables A to extract the current session key between π_{T_i} and π_R.

Test query: In this query A request π_i for the session key K and π_i reply with an outcome c, where c represents a random bit.

Furthermore, $H(.)$ is also modeled as a random oracle and is accessible to all the participants including the adversary A. We provide the proof of the existence of semantic security (secret session key security) in our proposed RFID-AS, by applying Theorem 1 as described below.

Theorem 1: Suppose an adversary A, running in a polynomial time pt, tries to obtain the current session key between π_{T_i} and π_R, using the games G_1, G_2 and G_3. Then, A's advantage in breaking the semantic security to extract the session key K between π_{T_i} and π_R in the proposed RFID-AS can be written as:

$$Adv_A^{RFID-AS}(pt) \leq (q_h^2/|hash| + 2.Adv_A^{HECDLP}(pt)$$

where the variables q_h, $|hash|$ and $Adv_A^{HECDLP}(pt)$, represent the number of hash queries, the range space of $H(.)$ and the non-negligible winning advantage of breaking HECDLP respectively.

Proof: We provide the proof of Theorem 1, by considering three games $G_i (i = 1, 2, 3)$. In each game A tries to guess the correct bit c by using the Test query. Suppose $wins_A^{G_i}$, is an event where A can guess the random bit c correctly, then the advantage for A in winning a game is given as:

$$Adv_{A,G_i}^{RFID-AS}(pt) = Pr[wins_A^{G_i}]$$

Game G1: This game is considered to be identical to the actual protocol executing under the ROR model. According to this game, the following output is obtained.

$$Adv_A^{RFID-AS}(pt) = |2Adv_{A,G_1}^{RFID-AS} - 1| \tag{16}$$

Game G2: In this game, the adversary A perform an eavesdropping attack by using the Execute query to break the secret session key security. The adversary A intercept all the messages communicated between π_{T_i} and π_R, which are: $m1 = Ps$, $m2 = Pt$, C, R, S and $m3 = Ts$. As a next step, A needs to perform the Reveal and Test queries to check whether the derived session key, acquired from the communication between π_{T_i} and π_R, is original or randomly selected. The secret session key between π_{T_i} and π_R can be produced as: $K = hash(V_t.P_s \oplus X_{id}) = hash(S.V_s(P_t + R.D) \oplus X_{id}) = K'$. To derive this session key, A needs to know the secret information V_t, V_s and X_{id}. It means that only eavesdropping of $m1$, $m2$ and $m3$ will not increase the winning probability for A. Hence, it is hard to distinguish between G_1 and G_2 as shown in the following equation:

$$Adv_{A,G_2}^{RFID-AS} = Adv_{A,G_1}^{RFID-AS} \tag{17}$$

Game G3: This game is modeled as an active attack which simulates the Send and Hash query. It is clear from G2 that the eavesdropped messages $mi (i = 1, 2, 3)$ between π_{T_i} and π_R do not lead to any hash collision because the information in these messages are protected by $H(.)$ and HECDLP. The variables V_s and V_t involved in P_s and P_t are protected by HECDLP, and the variables $T_p n$, $T_i d$ and $X_i d$ involved in R are protected by $H(.)$. Furthermore, G_2 and G_3 are indistinguishable except G_3, simulates Hash and Send queries and solving the HECDLP. The advantage of solving HECDLP is $Adv_A^{HECDLP}(pt)$ and according to birthday paradox, the collision probability of using hash oracle query is $(q_h^2)/2|hash|$. Overall, we can obtain the following outcome.

$$|Adv_{A,G_2}^{RFID-AS} - Adv_{A,G_3}^{RFID-AS}| \leq (q_h^2)/2|hash| + Adv_A^{HECDLP}(pt) \tag{18}$$

Now all the queries are executed by A and is only left in guessing the correct bit c, this results in the following output.

$$Adv_{A,G_3}^{RFID-AS} = 1/2 \tag{19}$$

Using equations 16 and 17, the following result is obtained.

$$1/2.Adv_A^{RFID-AS}(pt) = |Adv_{A,G_1}^{RFID-AS} - 1/2| = |Adv_{A,G_2}^{RFID-AS} - 1/2| \quad (20)$$

Using equations 19 and 20, the following result is obtained.

$$1/2.Adv_A^{RFID-AS}(pt) = |Adv_{A,G_2}^{RFID-AS} - Adv_{A,G_3}^{RFID-AS}| \quad (21)$$

Similarly, using equations 18 and 21, the following result is obtained.

$$1/2.Adv_A^{RFID-AS}(pt) \leq (q_h^2/2|hash| + Adv_A^{HECDLP}(pt) \quad (22)$$

We can obtain the following result by multiplying equation 22 by "2".

$$Adv_A^{RFID-AS}(pt) \leq (q_h^2)/|hash| + 2.Adv_A^{HECDLP}(pt)$$

B. FORMAL SECURITY VERIFICATION USING AVISPA

We implemented and validated the proposed scheme using the AVISPA simulation tool [49]. AVISPA is integrated with SPAN to provide a user interface. The architecture of the AVISPA tool has been shown in Figure 5. AVISPA tool operates under two validation states, namely: SAFE and UNSAFE. The output of the simulation is a SAFE state if a cryptographic scheme provides resistance against the MiM attack. The simulation's output is an UNSAFE state if a cryptographic scheme is not able to withstand the MiM attack. The role oriented language for writing cryptographic schemes in AVISPA is called High-Level Protocol Specification Language (HLPSL) [50]. We used software tools such as SPAN (version: SPAN-Ubuntu-10.10-light_1) and Oracle VM Virtual Box (version: 5.2.0.118431). The HLPSL source code of the proposed scheme contains four roles: role server, role tag, role session, and role environment as shown in Table 4, 5, 6, 7 respectively. AVISPA uses a special identifier i for the intruder. We used two backends of the AVISPA tool: OFMC and ASTE to validate our proposed scheme. The simulation result of the proposed protocol by using ATSE and OFMC back-end of AVISPA tool shows that the proposed protocol is safe as shown in Figure 6a and Figure 6b respectively.

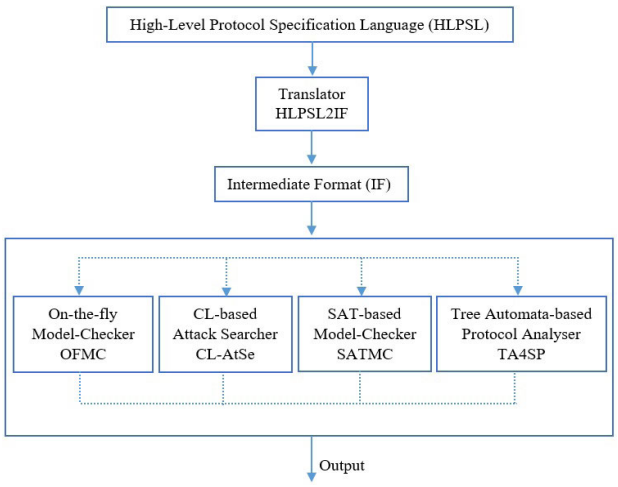


FIGURE 5. Architecture of the AVISPA tool [49].

TABLE 4. HLPSL code for Server.

```
role Server(S,T:agent,
Ps,Pt:public_Key,Hash:hash_func,
SND,RCV:channel(dy))
played_by S def=
local
State: nat,
Na,Na1,Nb,Nb1,Tid,Tpn,Xid:text,
K1,R1:message
init
State := 0
transition
1.State  =0/\RCV(start) =|>
  State':=1/\SND(S.T)
2.State  =1/\RCV(T.{Nb'}_Ps) =|>
  State':=2/\Na1' :=new()/\Xid :=new()
    /\Na' :=Ps.Na1'/\SND(S.{Na'.Xid}_Pt)
    /\K1' :=Hash(xor((Na'.Nb'),Xid))
    /\secret(K1',sec_1,{S,T})
3.State =2/\RCV(T.{Tpn'.Tid'.Xid'}_K1)=|>
  State':=3/\SND(S.{Tpn'}_K1)
    /\witness(S,T,auth_1,Tpn')
    /\R1':=Hash(xor(Tpn',Tid',Xid))
    /\request(S,T,auth_2,R1')
end role
```

C. INFORMAL SECURITY ANALYSIS

The following assumptions are considered while performing the informal security analysis.

i. The tag identifier T_{id}, tag pseudonym T_{pn}, and server identifier X_{id}, are known only to the server and the tag.

ii. For every session, fresh random values for V_s and V_t are selected by the server and the tag, respectively.

iii. The encryption algorithm E_K is secure enough that an adversary is incapable of two decrypt the ciphertext C.

1) AUTHENTICATION

In each session the tag should authenticate the server and vice versa, so that to ensure secure communication in RFID system.

Tag authentication: Once the server obtains the Signcryption text {C, R, S} from the tag, it computes the key K' for decryption of ciphertext C to acquire the tag pseudonym T'_{pn}. The server searches its database to find the tag unique identifier T_{id} corresponding to T'_{pn}. The server computes R' and compare it with R obtained from the tag. If $R' = R$, then the server authenticates the tag successfully. Suppose an attacker pretends to be a valid tag. In that case, it must produce an accurate value of R, but the value of R depends

TABLE 5. HLPSL code for Tag.

```
role Tag(S,T:agent,
Ps,Pt:public_key,Hash:hash_func,
SND,RCV:channel(dy))
played_by T def=
local
State: nat,
Na,Na1,Nb,Nb1,Tid,Tpn, Xid: text,
K1,R2: message
init
State := 0
transition
1.State  =0/\RCV(S.T) =|>
  State':=1/\Nb1':=new()
/\Nb':=Pt.Nb1'/\SND(T.{Nb'}_Ps)
2.State =1/\RCV(S.{Na'.Xid'}_Pt) =|>
  State':=2/\K1':=Hash(xor((Na'.Nb), Xid'))
    /\Tpn':=new()/\Tid':=new()
    /\SND(S.{Tpn'.Tid'.Xid'}_K1)
3.State =2/\RCV(T.{Tpn}_K1) =|>
  State':=3/\request(S,T,auth_1,Tpn)
    /\ R2':=Hash(xor(Tid,Tpn,Xid'))
    /\ secret(R2',sec_2,{S,T})
    /\ witness(T,S,auth_2,R2')
end role
```

TABLE 6. HLPSL code for Session role.

```
role session(S,T:agent,
Ps,Pt:public_key,
Hash:hash_func)
def=
local
SA,RA,SB,RB: channel(dy)
composition
 role_Server(S,T,Ps,Pt,
             Hash,SA,RA) /\
 role_Tag(S,T,Ps,Pt,
          Hash,SB,RB)
end role
```

on T_{id} and X_{id}, and only legitimate tag and server know this, thus any illegitimate tag or reader cannot produce the correct value of R.

Server authentication: The tag computes $\{T_t\}$, after it has received the message $\{T_s\}$ from the server. The message $\{T_s\}$ computed by the server depends on tag identifier T_{id} and server identifier X_{id} such that only legitimate tag and server know this. Additionally, $\{T_s\}$ is an encrypted message and an adversary is not able to find the shared secret key to decrypt the message $\{T_s\}$. The tag authenticates the server successfully if $T_s = T_t$. An adversary pretending itself to be a valid server must produce the correct message $\{T_s\}$. However $\{T_s\}$ depends on T_{id} and X_{id}, and only legitimate tag and server know this, thus it is impossible for an unauthorized server to produce the correct message $\{T_s\}$.

TABLE 7. HLPSL code for Environment role.

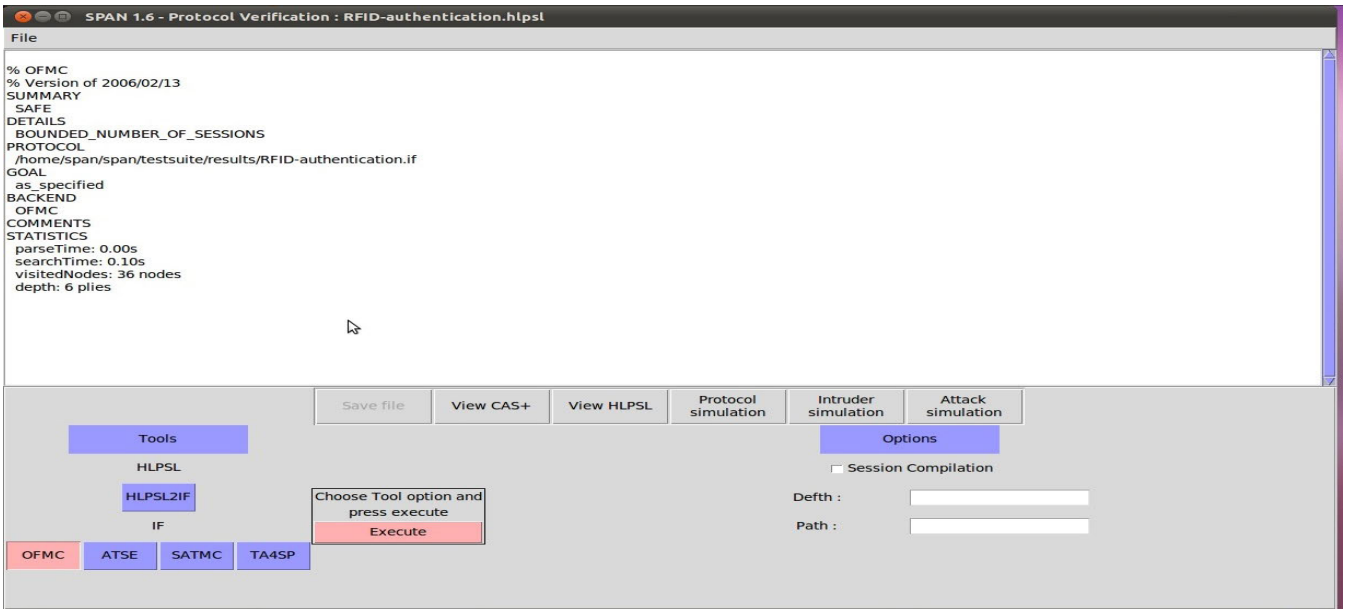
```
role environment()
def=
const
s,t: agent,
ka,kb: public_key,
h: hash_func,
sec_1,sec_2:protocol_id,
auth_1,auth_2:protocol_id
intruder_knowledge={s,t,h,ka,kb}
composition
session(s,t,ka,kb,h)
/\ session(s,i,ka,kb,h)
/\ session(i,t,ka,kb,h)
end role
goal
secrecy_of sec_1
    authentication_on auth_1
    secrecy_of sec_2
    authentication_on auth_2
end goal
environment()
```

2) CONFIDENTIALITY

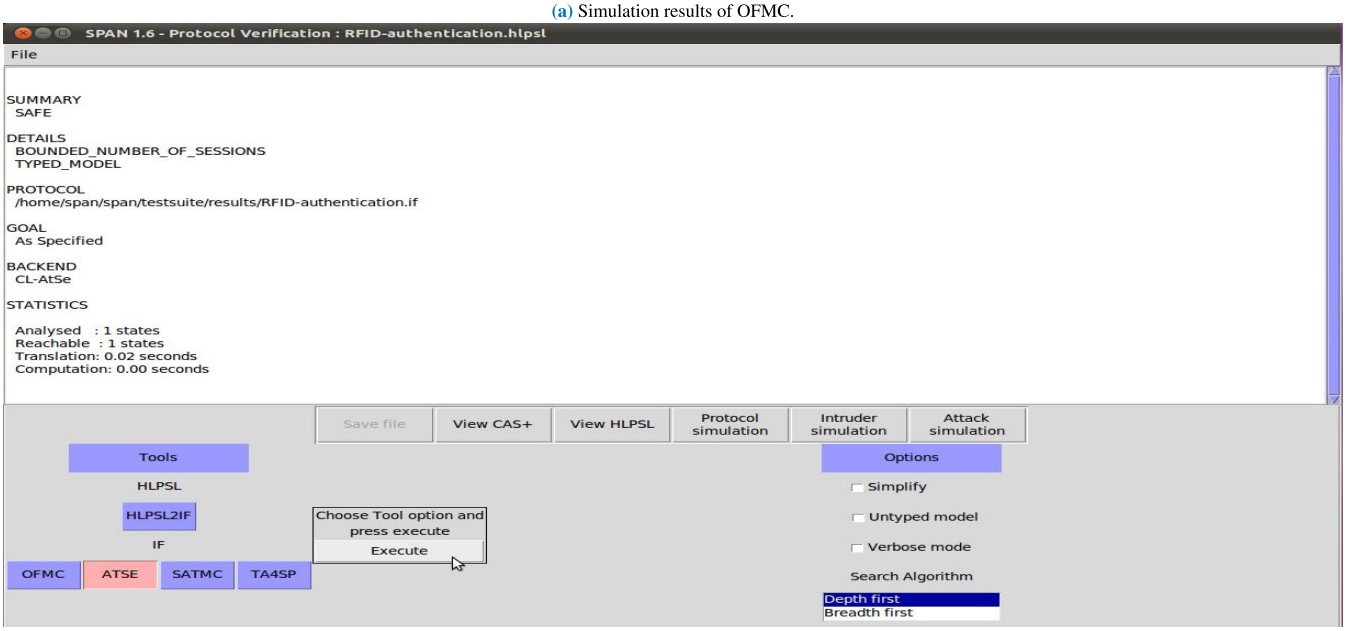
Confidentiality is the assurance to keep the information secret during the transmission. In the proposed RFID-AS, the first message is the server public key $\{P_s\}$ sent to the tag and since it is a public parameter and known to all, so it can be submitted as plaintext. The second message sent to the server is the Signcryption parameters $\{C, R, S\}$ and tag public key $\{P_t\}$. As $\{P_t\}$is a public parameter and is known to all so it can be transmitted as plaintext. All the three Signcryption parameters $\{C, R, S\}$ reveals no information. The adversary is unable to decrypt the ciphertext C because it requires private key V_t of the tag and server identifier X_{id} to produce the secret key K. According to the property of HECDLP, an adversary cannot compute V_t, given P_t and D. Furthermore, server identifier X_{id} is only known to legitimate tag and server. Similarly, Adversary A cannot obtain any information from R and S because R is computed from one-way hash function and its reverse is impossible to compute and S is obtained using R. The third message sent to the tag is $\{T_s\}$ which is encrypted message and an adversary cannot obtain any information from this because it requires a secret key K and an adversary is unable to produce it due to the property of HECDLP. Therefore, confidentiality attributes are successfully provided by the proposed RFID-AS.

3) NON-REPUDIATION

The value of R and S, sent to the server by the tag depends on the tag identifier T_{id} and server identifier X_{id}. Similarly, the $\{T_s\}$ message sent to the server's tag also depends on



(a) Simulation results of OFMC.



(b) Simulation results of ATSE.

FIGURE 6. Simulation results.

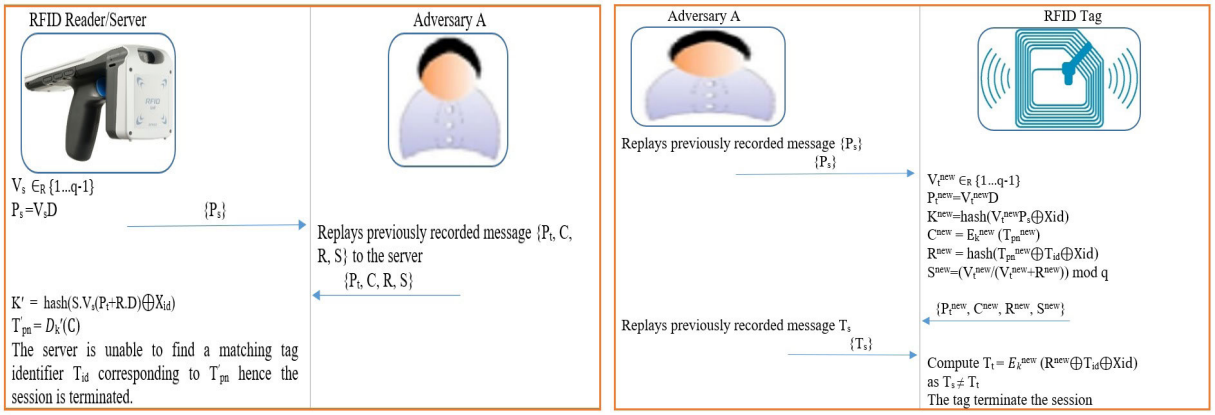
the tag identifier T_{id} and server identifier X_{id}. Based on Assumption 1, if $R = R'$ then the tag would not repudiate that the message was sent by it to the server and if $T_s = T_t$, then the server would not repudiate that the message was sent by it to the tag.

4) INTEGRITY

An adversary can't have two messages that have the identical message digest [41]. It means that for adversary A having an output of hash function can never determine the input message. Suppose an adversary alters any value in $\{C, R, S\}$, it can easily be identified by the server. The K value will not be equal to the K value created by the tag, which causes the server to generate R incorrectly. In this situation, authentication fails and the server terminates the session. Similarly, it can be easily identified if an Adversary alters $\{T_s\}$ received by the tag from the server. It would not be the same as computed by the tag, in this situation, the authentication fails and the tag terminates the session. In the proposed RFID-AS, data integrity during transmission is thus guaranteed.

5) ANONYMITY

In the proposed RFID-AS, the tag sends the secret information: tag identity T_{id}, tag pseudonym T_{pn} and server identifier



(a) Server resistance against replay attack

(b) Tag resistance against replay attack.

FIGURE 7. Resistance against replay attack.

X_{id} in the form of a signcrypted message. Further, the security of T_{pn} is maintained by using encryption and the security of T_{id} and X_{id} is maintained by using a hash function to the result obtained from the XOR operations between T_{pn}, T_{id} and X_{id}. To obtain the confidential information T_{pn}, T_{id} and X_{id}, the adversary needs the secret key K, which is not possible for him to calculate due to HECDLP. Similarly, the secrecy of T_{id} and X_{id} is preserved in the message $\{T_s\}$ sent by the server to the tag by performing XOR operations between R', T_{id} and X_{id} and then encrypting the result using the key K'. The adversary needs to decrypt to get the value of T_{id} and X_{id}, which is not possible because the key K' is not known and is not possible for him to calculate due to HECDLP. Therefore the proposed RFID-AS offers tag anonymity.

6) FORWARD SECURITY

Suppose the Adversary A, somehow manages to know the tag pseudonym T_{pn}. In that case, it may not be able to retrieve previous messages, due to the messages $\{T_s\}$ and {C, R, S}, solely dependent on the secret key computed by tag and server, which subsequently depends on the random numbers V_s and V_t generated by the server and the tag respectively for each session. The proposed RFID-AS therefore offers forward security as the adversary yet is unable to get and use the past messages later.

7) AVAILABILITY

The tag identifier T_{id} and server identifier X_{id} remains the same during the entire communication of tag and server, and the adversary is unable to reach it. In addition, the tag pseudonym T_{pn} that is sent to the server is updated for each session. The updating of tag pseudonym T_{pn} for both the server and the tag ensures that both have the same T_{pn} at all times. The proposed RFID-AS, therefore, offers availability and prevents de-synchronization.

8) SCALABILITY

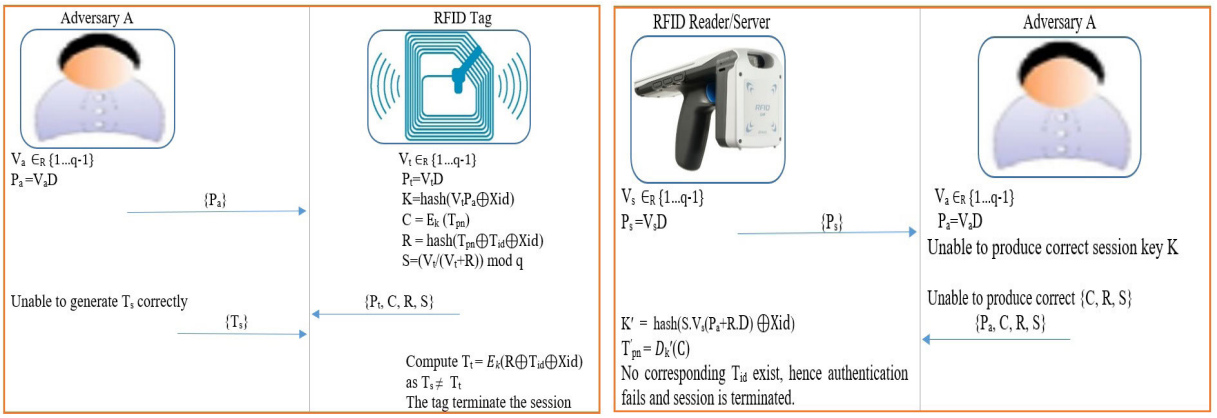
The server searches and find tag identifier T_{id} in its database corresponding to the tag pseudonym T_{pn} obtained from the tag. So no linear search is needed for the server to know each tag's identity [31]. The server consumes O(1) amount of time to search for the corresponding tag in the proposed RFID-AS, consequently saving enormous computational workload as total tags in the system increases. Thus, the proposed RFID-AS, as a result, offers scalability.

9) SECURITY AGAINST REPLAY ATTACK

An adversary eavesdropping on the communication channel can obtain the past messages $\{P_s\}$, $\{P_t, C, R, S\}$ and $\{T_s\}$, communicated between tag and server. The adversary then can replay these messages to create an unauthorized effect. In our proposed scheme, the tag pseudonym T_{pn} value is a private random number and for every new session, T_{pn} is updated to T_{pn}^{new}. Therefore in the new session the adversary is unable to use the previously recorded messages.

i If an adversary pretending to be a valid tag and send to the server the pre-recorded message $\{P_t\}$ and $\{C, R, S\}$, then the server perform the following computation:
It computes the secret key as $K' = hash(S.V_s(P_t + R.D) \oplus X_{id})$ and Decrypts the ciphertext to find the tag pseudonym $T'_{pn} = D_{k'}(C)$. The server is unable to find a corresponding tag identifier T_{id} because $T'_{pn} \neq T_{pn}^{new}$ and dismisses the session. The resistance of the server replay attack is shown in Figure 7a.

ii If Adversary A pretending to be a valid server and transmit to the tag the pre-recorded messages $\{P_s\}$ and $\{T_s\}$, then the tag performs the following computations.
Initialize its private key $V_t^{new} \in_R \{1 \ldots q-1\}$.
compute $P_t = V_t^{new} D$.
Compute its secret key $K^{new} = hash(V_t^{new} P_s \oplus X_{id})$.
Compute the ciphertext $C = E_{K^{new}}(T_{pn})$.
Compute $R^{new} = hash(T_{pn} \oplus T_{id} \oplus X_{id})$.
Compute $S^{new} = (V_t/(R^{new} + V_t))modq$.
Compute $T_t^{new} = E_{k^{new}}(R^{new} \oplus T_{id} \oplus X_{id})$.
Evidently, $T_t^{new} \neq T_s$ because in the new session the tag used V_t^{new} and the modified tag pseudonym T_{pn}^{new}, rather than V_t and T_{pn}, that were used in the former sessions. Thus, the server authentication fails and the tag



(a) Resistance against server impersonation attack.

(b) Resistance against tag impersonation attack.

FIGURE 8. Resistance against impersonation attack.

terminates the session. The resistance of the tag replay attack is shown in Figure 7b.

10) SECURITY AGAINST CLONING ATTACK

According to Liao *et al.* [27], the RFID authentication protocol is susceptible to cloning attacks when a group of tags uses the same secret key in the authentication process. The proposed RFID-AS uses no stored secret key in the tag memory. Each session's new key is produced dynamically therefore, the adversary is not capable to extract the confidential data to clone a tag. Even if the adversary can obtain a specific tag identifier T_{id} for a set of tags, it is not capable of obtaining tag pseudonym T_{pn} for the same tags, as T_{pn} is not fixed and is updated in every session.

11) SECURITY AGAINST LOCATION TRACKING ATTACK

An adversary is unable to retrieve tag identifier T_{id} and server identifier X_{id} transferred between tag and server due to secure communication in our proposed scheme. Whenever the tag transmit $\{C, R, S\}$, the adversary would be unable to retrieve T_{id} and X_{id}, because it has to solve the computationally difficult HECDHP for computing the secret key. Likewise, the attacker can not decrypt when the server transmits $\{T_s\}$ to the tag due to the secret key K of the server and tag. Moreover, in producing the messages, private random numbers are used. The attacker will, therefore not access the location information, hence security against location tracking attack has been guaranteed.

12) SECURITY AGAINST DESYNCHRONIZATION ATTACK

The adversary in the desynchronization attack prevents updating certain confidential information during tag server communication in an ongoing session. The adversary tries to intercept the messages and it is possible that the server failed to update the tag pseudonym in its database while the tag updates its pseudonym in its memory [46]. In our proposed scheme, the server stores the previous value of tag pseudonym T_{pn} as well as the modified value of tag pseudonym T_{pn}^{new} to avoid the desynchronization attack. When the server receives $\{C, R, S\}$ from the adversary, the server decrypts C and decides whether the decrypted value is a previous tag pseudonym T_{pn} or a modified tag pseudonym T_{pn}^{new}. But since the adversary has no correct values for T_{pn} and T_{pn}^{new}. Hence the adversary is unable to perform the de-synchronization of shared secret due to data integrity and mutual authentication provided by the proposed scheme.

13) SECURITY AGAINST DoS ATTACK

It has already been shown that while updating the tag pseudonym T_{pn}, the proposed scheme ensures availability and can also prevent de-synchronization attack. Furthermore, updating of the Tag Pseudonym T_{pn} between tag and server is the only synchronous update. Hence security against the DoS attack has been guaranteed.

14) SECURITY AGAINST IMPERSONATION ATTACK

An adversary eavesdropping on the communication channel can impersonate a valid server or tag.

i Server impersonation attack is also known as server spoofing attack in which an adversary tries to mimic the behavior of a valid server. In doing so adversary A, chooses a random integer V_a, then calculates $P_a = V_aD$ and sends $\{P_a\}$ to the valid tag. The tag then produces the message $\{P_t, C, R, S\}$ and sends it to A. However, A is unable to find X_{id} and compute the secret key K and in turn, is unable to generate the message $\{T_s\}$ correctly and therefore unequal to the tag generated $\{T_t\}$. Thus, the tag finishes the session due to the fact $T_s \neq T_t$. The Adversary A therefore unsuccessful to mimic the behavior of a server and thus security against the server impersonation attack has been guaranteed as shown in Figure 8a.

ii The tag impersonation attack is also known as a tag masquerade attack in which an adversary tries to mimic the behavior of a valid tag. The adversary A, when receives $\{P_s\}$ from a valid server, generate the message

TABLE 8. Comparison of computational overhead.

Protocol	Tag	Server	Total
Singh et al. [19]	2 ECSM	3 ECSM	5 ECSM
Alamar et al. [38]	4 ECSM	5 ECSM	9 ECSM
Zheng et al. [41]	3 ECSM	4 ECSM	7 ECSM
Dinarvand et al. [46]	3 ECSM	3 ECSM	6 ECSM
Proposed RFID-AS	***1 HECDM***	***2 HECDM***	***3 HECDM***

TABLE 9. Comparison of computational overhead.

Protocol	Computational Overhead (sec)			Proposed scheme efficiency
	Tag	Server	Total	
Singh et al. [19]	0.128	0.192	0.32	**70%**
Alamar et al. [38]	0.256	0.32	0.576	**83%**
Zheng et al. [41]	0.192	0.256	0.448	**78.6%**
Dinarvand et al. [46]	0.192	0.192	0.384	**75%**
Proposed RFID-AS	***0.032***	***0.064***	***0.096***	———

$\{P_a\}$ and $\{C, R, S\}$ and send it to the server. Since the adversary is unable to obtain the tag identifier T_{id} and server identifier X_{id}, this is because only legitimate tag and server know it and therefore the message $\{C, R, S\}$ sent by the adversary is incorrect. The valid server when receiving this incorrect message $\{C, R, S\}$ from the adversary, decrypt the ciphertext C to compute R', but since $R \neq R'$, hence the authentication fails and the session is terminated. Thus security against the tag impersonation attack has been guaranteed as shown in Figure 8b.

15) SECURITY AGAINST MiM ATTACK

An adversary in the MiM attack tries to modify the messages transmitted from the tag to the server and vice versa. The adversary pretending itself as a legitimate party and sends the modified messages to either tag or server [30]. As shown in section 6.2.6, the security against server and tag impersonation attacks is guaranteed and no illegitimate tag or server initiates and completes the session successfully. Thus, security against the MiM attack has also been guaranteed.

16) SECURITY AGAINST KEY COMPROMISE ATTACK

Since the server and the tag randomly generate private keys V_s and V_t for each session, that are used to produce the secret key K and an adversary is unable to generate this secret key due to HECDLP. Hence security against the key compromise attack has been guaranteed.

VII. COMPARATIVE ANALYSIS

The proposed scheme's efficiency has been evaluated by measuring the common performance parameters that include computational, communication and storage overhead. This section provides the analysis of these overheads as well as the comparison of the results with the existing schemes.

A. OVERHEAD ANALYSIS

1) COMPUTATIONAL OVERHEAD

The computational overhead of an authentication scheme depends on the time consumed by various operations performed by the protocol during its execution. In the ECC based RFID authentication protocol, the computational time is related to the number of elliptic curve scalar multiplication (ECSM) operation. Similarly, in HECC based RFID authentication protocol, the computational time is related to the number of hyperelliptic curve Division multiplication (HECDM) operations. The time consumed by other operations in an authentication scheme is very small compared to the execution time of ECSM or HECDM and therefore can be ignored. According to [21] the time to compute a single ECSM operation is 0.064 s on a 5 MHz tag. Thus, we can assume the time to compute a single HECDM to be 0.032 s due to 80-bits key and parameter size which is half of the key and parameters size used in 160-bits ECC [51]. In the proposed RFID authentication scheme, the tag executes one HECDM operation and the server executes two HECDM operations. Therefore, the tag execution time is 0.032 s and the server execution time is 0.064 s. Therefore, the total time consumed by the server and tag together is 0.096 s. Tables 8 and 9 compare the computation overhead with the current schemes [19], [27], [38], [41], [46]. Table 9 also provides the percentage improvement efficiency of the proposed scheme. A graphical representation of the comparison is also shown in Figure 9.

TABLE 10. Comparison of Communication overhead.

Protocol	Communication Overhead (bits)			Proposed scheme efficiency
	Tag	Server	Total	
Singh et al. [19]	736	576	1312	**42.7%**
Alamr et. al. [38]	640	960	1600	**53%**
Zheng et. al. [41]	640	640	1280	**41.2%**
Dinarvand et.al. [46]	800	640	1440	**47.8%**
Proposed RFID-AS	***544***	***208***	***752***	———

TABLE 11. Comparison of storage overhead.

Protocol	Storage overhead (bits)			Proposed scheme efficiency
	Tag	Server	Total	
Singh et al. [19]	1760	1120+640m	2880+640m	**57.7%**
Alamr et. al. [38]	1920	1120+320m	3040+320m	**32.6%**
Zheng et. al. [41]	2080	1760+320m	3840+320m	**38.9%**
Dinarvand et.al. [46]	1920	1120+800m	3040+800m	**64.9%**
Proposed RFID-AS	***1040***	***640+240m***	***1680+240m***	———

TABLE 12. Comparison of security requirements and potential to counter various attacks.

Protocol	Security Attributes								Resistance against attacks								FSV
	MA	CO	NR	IN	AV	FS	AN	SC	LC	MiM	CL	RP	IM	DoS	DE	KC	
Singh et al. [19]	Y	Y	Y	Y	Y	Y	Y	N	Y	Y	Y	Y	Y	Y	Y	Y	N
Alamr et. al.[38]	Y	Y	Y	N	Y	Y	N	N	Y	Y	Y	Y	Y	N	N	Y	N
Zheng et. al. [41]	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	N
Dinarvand et.al. [46]	Y	Y	Y	Y	Y	Y	Y	N	Y	Y	Y	Y	Y	Y	Y	Y	N
Proposed RFID-AS	**Y**	**Y**	**Y**	**Y**	**Y**	**Y**	**Y**	**Y**	**Y**	**Y**	**Y**	**Y**	**Y**	**Y**	**Y**	**Y**	**Y**

MA-Mutual authentication, CO-Confidentiality, NR-Non Repudiation, IN-integrity, AV-Availability, FS-Forward security, AN-Anonymity, SC-Scalability, LC-location tracking attack, MiM-Man in the middle attack, CL-Cloning attack, RP-Replay attack, IM-Impersonation attack, DoS-Denial of service attack, DE-De-synchronization attack, KC-Key compromise attack, FSV-Formal Security Validation, N- Security functionality not satisfied. Y- Security functionality satisfied.

2) COMMUNICATION OVERHEAD

Communication overhead depends on the size and the number of messages communicated between the two entities during the execution of a protocol. In the proposed scheme, three messages $\{P_s\}$, $\{P_t, C, R, S\}$, and $\{T_s\}$ are transferred between server and tag. We assumed, 128-bit AES for encryption that produces 128-bit ciphertext, while SHA-256 for a hash function, that produces 256 bits output. The communication cost of the tag to send the message $\{P_t, C, R, S\}$, is $128+256+80+80 = 544$ bits. While the communication cost of the server to send the messages $\{P_s\}$ and $\{T_s\}$ is $80 + 128 = 208$ bits. The total communication cost of tag and server is 752 bits. Table 10 presents a comparison of the communication overhead and improvement in efficiency from the current schemes [19], [38], [41], [46]. A graphical analysis of this comparison is also shown in Figure 10.

3) STORAGE OVERHEAD

The tag is required to store hyperelliptic curve parameters $\{F_q, F_q^*, q, x, y, D\}$, server public key P_s, tag's private key V_t, tag's public key P_t, server identifier X_{id}, tag's unique id T_{id} and the unique pseudonym of the tag T_{pn} and T_{pn}^{new}. Since 80-bit HECC has been used, the size of each curve parameter is 80 bits. So the storage cost of the tag can be calculated as: $80+80+80+80+80+80+80+80+80+80+80+80+80 = 1040$ bits. The server is required to store system parameters $\{F_q, F_q^*, q, x, y, D\}$, server private key V_s, server identifier X_{id}, tag unique identifier T_{id}, tag unique pseudonym T_{pn}, and T_{pn}^{new}. It is assumed that the system has m number of tags, so the storage cost of the server can be calculated as: $80+80+80+80+80+80+80+80+80m+80m+80m = 640+240m$ bits. Table 11 presents comparison of the storage overhead and improvement in efficiency from the current

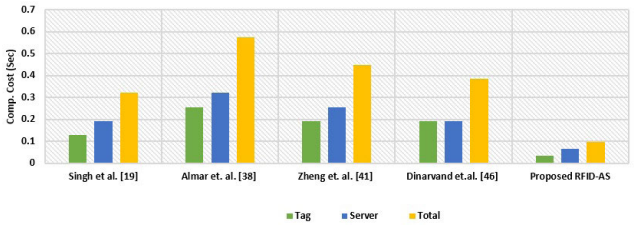


FIGURE 9. Comparison of computational overhead.

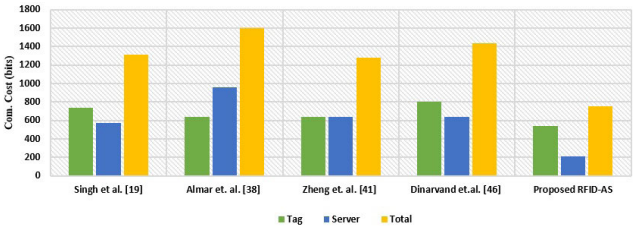


FIGURE 10. Comparison of communication overhead.

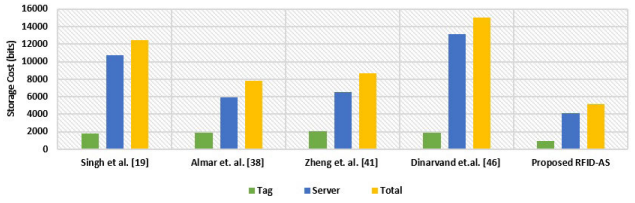


FIGURE 11. Comparison of storage overhead.

schemes [19], [38], [41], [46]. A graphical analysis of the comparison for the number of tags $m = 15$, is also shown in Figure 11.

B. COMPARISON OF SECURITY FUNCTIONALITIES

In this section the security requirements shown in section 6.1 and the potential to counter various attacks shown in section 6.2 are compared with the existing schemes [19], [38], [41], [46] as shown in Table 12.

VIII. CONCLUSION

RFID technology has become very popular due to less expense and improved speed. However implementation of the security and privacy mechanism is a major problem for RFID tag due to its lower computational capacity. Previously, the researchers suggested hash-based, SKC-based, and ECC-based for RFID systems. However, some of these protocols failed to achieve complete security requirements and some protocols have high computational overhead. In this paper, we proposed a hyperelliptic curve Signcryption based RFID authentication scheme. The security and efficiency of the proposed scheme are based on 80-bit HEC as compared to 160-bit ECC. The proposed scheme achieves security requirements for the RFID systems such as authentication, confidentiality, non-repudiation, integrity, anonymity, forward security, availability, and scalability. Additionally, the proposed scheme can also provide security against replay, MiM, impersonation, cloning, location tracking, desynchronization, DoS, and key compromise attacks. Furthermore, the security of the proposed scheme is validated by using the AVISPA tool. The results of the performance parameters of the proposed scheme have been compared with most recent RFID authentication protocols In terms of computation, communication, and storage overhead. Compared to the most recent protocol, our proposed scheme improves 70% computational overhead, 42.7% communication overhead, and 57.7% storage overhead. Thus the proposed scheme is more efficient and provides enhanced security as compared to the existing schemes, therefore, the proposed scheme is an attractive solution for resource-limited devices like RFID systems.

IX. FUTURE WORK

In the future, we are planning to conduct a practical test to measure performance.

REFERENCES

[1] R. Want, "An introduction to RFID technology," *IEEE Pervasive Comput.*, vol. 5, no. 1, pp. 25–33, Jan./Mar. 2006.
[2] X. Jia, Q. Feng, T. Fan, and Q. Lei, "RFID technology and its applications in Internet of Things (IoT)," in *Proc. 2nd Int. Conf. Consum. Electron., Commun. Netw. (CECNet)*, Apr. 2012, pp. 1282–1285.
[3] J. Yu and L. Chen, *Tag Counting and Monitoring in Large-Scale RFID Systems*. Cham, Switzerland: Springer, 2019, doi: 10.1007/978-3-319-91992-8.
[4] A. Khattab, Z. Jeddi, E. Amini, and M. Bayoumi, "Introduction to RFID," in *RFID Security*. Cham, Switzerland: Springer, 2017, pp. 3–26, doi: 10.1007/978-3-319-47545-5.
[5] C. Swedberg, "Iotera develops active RFID tag with 4-mile read range," *RFID J.*, 2014. Accessed: Nov. 28, 2020. [Online]. Available: https://www.rfidjournal.com/iotera-develops-active-rfid-tag-with-4-mile-read-range-2
[6] P. N. Roque, "Performance analysis of effective range and orientation of UHF passive RFID," M.S. thesis, 2008. [Online]. Available: https://scholar.afit.edu/etd/2741
[7] S. Guizani, "Security applications challenges of RFID technology and possible countermeasures," in *Proc. Int. Conf. Comput., Manage. Telecommun. (ComManTel)*, Apr. 2014, pp. 291–297.
[8] N. Kannouf, Y. Douzi, M. Benabdellah, and A. Azizi, "Security on RFID technology," in *Proc. Int. Conf. Cloud Technol. Appl. (CloudTech)*, 2015, pp. 1–5.
[9] A. Khattab, Z. Jeddi, E. Amini, and M. Bayoumi, "Rfid security threats and basic solutions," in *RFID Security*. Cham, Switzerland: Springer, 2017, pp. 27–41.
[10] M. Ågren, "On some symmetric lightweight cryptographic designs," Ph.D. dissertation, Dept. Elect. Inf. Technol., Fac. Eng., Lund Univ., Lund, Sweden, 2012. [Online]. Available: https://portal.research.lu.se/ws/files/5271313/3159359.pdf
[11] H. Delfs, H. Knebl, and H. Knebl, *Introduction to Cryptography*, vol. 2. Berlin, Germany: Springer, 2002, doi: 10.1007/978-3-662-47974-2.
[12] R. L. Rivest, A. Shamir, and L. Adleman, "A method for obtaining digital signatures and public-key cryptosystems," *Commun. ACM*, vol. 26, no. 1, pp. 96–99, Jan. 1983.
[13] W. P. Wardlaw, "The RSA public key cryptosystem," in *Coding Theory and Cryptography*. Berlin, Germany: Springer, 2000, pp. 101–123, doi: 10.1007/978-3-642-59663-6_6.
[14] N. Koblitz, "Elliptic curve cryptosystems," *Math. Comput.*, vol. 48, no. 177, pp. 203–209, 1987.
[15] A. J. Menezes, P. C. Van Oorschot, and S. A. Vanstone, *Handbook of Applied Cryptography*. Boca Raton, FL, USA: CRC Press, 2018.
[16] N. Koblitz, "Hyperelliptic cryptosystems," *J. Cryptol.*, vol. 1, no. 3, pp. 139–150, Oct. 1989.
[17] T. Wollinger, J. Pelzl, and C. Paar, "Cantor versus Harley: Optimization and analysis of explicit formulae for hyperelliptic curve cryptosystems," *IEEE Trans. Comput.*, vol. 54, no. 7, pp. 861–872, Jul. 2005.
[18] Y. Zheng, "Digital signcryption or how to achieve cost (signature & encryption) cost (signature)+ cost (encryption)," in *Proc. Annu. Int. Cryptol. Conf.* Berlin, Germany: Springer, 1997, pp. 165–179, doi: 10.1007/BFb0052234.
[19] A. K. Singh and B. Patro, "Elliptic curve signcryption based security protocol for RFID," *KSII Trans. Internet Inf. Syst.*, vol. 14, no. 1, 2020, doi: 10.3837/tiis.2020.01.019.

[20] J. Pelzl, T. Wollinger, J. Guajardo, and C. Paar, "Hyperelliptic curve cryptosystems: Closing the performance gap to elliptic curves," in *Proc. Int. Workshop Cryptograph. Hardw. Embedded Syst.* Berlin, Germany: Springer, 2003, pp. 351–365, doi: 10.1007/978-3-540-45238-6_28.
[21] G. Godor, N. Giczi, and S. Imre, "Elliptic curve cryptography based mutual authentication protocol for low computational capacity RFID systems–performance analysis by simulations," in *Proc. IEEE Int. Conf. Wireless Commun., Netw. Inf. Secur.*, Jun. 2010, pp. 650–657.
[22] Y. K. Lee, L. Batina, D. Singelee, B. Preneel, and I. Verbauwhede, "Anti-counterfeiting, untraceability and other security challenges for RFID systems: Public-key-based protocols and hardware," in *Towards Hardware-Intrinsic Security*. Berlin, Germany: Springer, 2010, pp. 237–257, doi: 10.1007/978-3-642-14452-3_11.
[23] M. Safkhani, N. Bagheri, M. Naderi, Y. Luo, and Q. Chai, "Tag impersonation attack on two RFID mutual authentication protocols," in *Proc. 6th Int. Conf. Availability, Rel. Secur.*, Aug. 2011, pp. 581–584.
[24] M. Safkhani, P. Peris-Lopez, J. C. Hernandez-Castro, N. Bagheri, and M. Naderi, "Cryptanalysis of cho's protocol, a hash-based mutual authentication protocol for rfid systems," *IACR Cryptol. ePrint Arch.*, vol. 2011, p. 331, Jun. 2011.
[25] P. Peris-Lopez, M. Safkhani, N. Bagheri, and M. Naderi, "RFID in eHealth: How to combat medication errors and strengthen patient safety," *J. Med. Biol. Eng*, vol. 33, pp. 363–372, Jan. 2013.
[26] Y.-L. Liu, X.-L. Qin, C. Wang, and B.-H. Li, "A lightweight RFID authentication protocol based on elliptic curve cryptography," *J. Comput.*, vol. 8, no. 11, pp. 2880–2887, Nov. 2013.
[27] Y.-P. Liao and C.-M. Hsiao, "A secure ECC-based RFID authentication scheme using hybrid protocols," in *Proc. Adv. Intell. Syst. Appl.*, vol. 2. Berlin, Germany: Springer, 2013, pp. 1–13, doi: 10.1007/978-3-642-35473-1_1.
[28] Z. Zhao, "A secure RFID authentication protocol for healthcare environments using elliptic curve cryptosystem," *J. Med. Syst.*, vol. 38, no. 5, p. 46, May 2014.
[29] M. S. Farash, O. Nawaz, K. Mahmood, S. A. Chaudhry, and M. K. Khan, "A provably secure RFID authentication protocol based on elliptic curve for healthcare environments," *J. Med. Syst.*, vol. 40, no. 7, p. 165, Jul. 2016.
[30] J.-S. Chou, "An efficient mutual authentication RFID scheme based on elliptic curve cryptography," *J. Supercomput.*, vol. 70, no. 1, pp. 75–94, Oct. 2014.
[31] M. S. Farash, "Cryptanalysis and improvement of an efficient mutual authentication RFID scheme based on elliptic curve cryptography," *J. Supercomput.*, vol. 70, no. 2, pp. 987–1001, Nov. 2014.
[32] Z. Zhang, Q. Qi, N. Kumar, N. Chilamkurti, and H.-Y. Jeong, "A secure authentication scheme with anonymity for session initiation protocol using elliptic curve cryptography," *Multimedia Tools Appl.*, vol. 74, no. 10, pp. 3477–3488, May 2015.
[33] Y. Lu, L. Li, H. Peng, and Y. Yang, "A secure and efficient mutual authentication scheme for session initiation protocol," *Peer Peer Netw. Appl.*, vol. 9, no. 2, pp. 449–459, Mar. 2016.
[34] Z. Mehmood, G. Chen, J. Li, L. Li, and B. Alzahrani, "A robust ECC based mutual authentication protocol with anonymity for session initiation protocol," *PLoS ONE*, vol. 12, no. 10, Oct. 2017, Art. no. e0186044.
[35] L. Feng and X. Yao, "RFID system mutual authentication protocols based on ECC," in *Proc. IEEE 12th Int. Conf Ubiquitous Intell. Comput., IEEE 12th Int. Conf Autonomic Trusted Comput., IEEE 15th Int. Conf Scalable Comput. Commun. Associated Workshops (UIC-ATC-ScalCom)*, Aug. 2015, pp. 1644–1649.
[36] Y. Chen and J.-S. Chou, "ECC-based untraceable authentication for large-scale active-tag RFID systems," *Electron. Commerce Res.*, vol. 15, no. 1, pp. 97–120, Mar. 2015.
[37] H. Shen, J. Shen, M. K. Khan, and J.-H. Lee, "Efficient RFID authentication using elliptic curve cryptography for the Internet of Things," *Wireless Pers. Commun.*, vol. 96, no. 4, pp. 5253–5266, Oct. 2017.
[38] A. A. Alamr, F. Kausar, and J. S. Kim, "Secure mutual authentication protocol for RFID based on elliptic curve cryptography," in *Proc. Int. Conf. Platform Technol. Service (PlatCon)*, Feb. 2016, pp. 1–7.
[39] Q. Qian, Y.-L. Jia, and R. Zhang, "A lightweight RFID security protocol based on elliptic curve crytography," *IJ Netw. Secur.*, vol. 18, no. 2, pp. 354–361, 2016.
[40] N. Bagheri, P. Alenaby, and M. Safkhani, "A new anti-collision protocol based on information of collided tags in RFID systems," *Int. J. Commun. Syst.*, vol. 30, no. 3, p. e2975, Feb. 2017.
[41] L. Zheng, Y. Xue, L. Zhang, and R. Zhang, "Mutual authentication protocol for RFID based on ECC," in *Proc. 7 IEEE Int. Conf. Comput. Sci. Eng. (CSE), IEEE Int. Conf. Embedded Ubiquitous Comput. (EUC)*, vol. 2, Jul. 2017, pp. 320–323.
[42] S.-Y. Chiou, W.-T. Ko, and E.-H. Lu, "A secure ECC-based mobile RFID mutual authentication protocol and its application," *Int. J. Netw. Secur.*, vol. 20, no. 2, pp. 396–402, Mar. 2018.
[43] G. Liu, H. Zhang, F. Kong, and L. Zhang, "A novel authentication management RFID protocol based on elliptic curve cryptography," *Wireless Pers. Commun.*, vol. 101, no. 3, pp. 1445–1455, Aug. 2018.
[44] K. Fan, W. Jiang, H. Li, and Y. Yang, "Lightweight RFID protocol for medical privacy protection in IoT," *IEEE Trans. Ind. Informat.*, vol. 14, no. 4, pp. 1656–1665, Apr. 2018.
[45] S. F. Aghili and H. Mala, "Security analysis of an ultra-lightweight RFID authentication protocol for m-commerce," *Int. J. Commun. Syst.*, vol. 32, no. 3, p. e3837, Feb. 2019.
[46] N. Dinarvand and H. Barati, "An efficient and secure RFID authentication protocol using elliptic curve cryptography," *Wireless Netw.*, vol. 25, no. 1, pp. 415–428, Jan. 2019.
[47] D. Dolev and A. Yao, "On the security of public key protocols," *IEEE Trans. Inf. Theory*, vol. IT-29, no. 2, pp. 198–208, Mar. 1983.
[48] M. Abdalla, P.-A. Fouque, and D. Pointcheval, "Password-based authenticated key exchange in the three-party setting," in *Proc. Int. Workshop Public Key Cryptogr.* Berlin, Germany: Springer, 2005, pp. 65–84, doi: 10.1007/978-3-540-30580-4_6.
[49] A. Armando, D. Basin, Y. Boichut, Y. Chevalier, L. Compagna, J. Cuéllar, P. H. Drielsma, P. C. Héam, O. Kouchnarenko, J. Mantovani, and S. Mödersheim, "The AVISPA tool for the automated validation of Internet security protocols and applications," in *Proc. Int. Conf. Comput. Aided Verification*. Berlin, Germany: Springer, 2005, pp. 281–285, doi: 10.1007/11513988_27.
[50] Y. Chevalier, L. Compagna, J. Cuellar, P. H. Drielsma, J. Mantovani, S. Mödersheim, and L. Vigneron, "A high level protocol specification language for industrial security-sensitive protocols," in *Proc. Workshop Specification Automated Process. Secur. Requirements*, 2004, pp. 1–13.
[51] I. Ullah, N. Amin, J. Khan, M. Rehan, M. Naeem, H. Khattak, S. Khattak, and H. Ali, "A novel provable secured signcryption scheme *PSSS*: A hyper-elliptic curve-based approach," *Mathematics*, vol. 7, no. 8, p. 686, Jul. 2019.

USMAN ALI (Graduate Student Member, IEEE) received the B.S. degree in computer system engineering from the Ghulam Ishaq Khan (GIK) Institute of Engineering Sciences and Technology, Pakistan, in 2011, and the M.S. degree in computer engineering from the National University of Sciences and Technology (NUST), Islamabad, Pakistan, in 2015. He is currently pursuing the Ph.D. degree in computer science with the University of Malaya, Malaysia. His research interests include information security, lightweight authentication, and privacy.

MOHD YAMANI IDNA BIN IDRIS (Member, IEEE) received the B.E., M.Sc., and Ph.D. degrees in electrical engineering from the University of Malaya, Kuala Lumpur, Malaysia. He is currently an Associate Professor with the Department of Computer Systems, Faculty of Computer Science and Information Technology, University of Malaya. He is the author of a book, more than 110 articles in reputable journals, and more than 20 inventions. His research interests include information security, embedded systems (system on chip and FPGA), image processing and computer vision, digital forensics, surveillance systems, digital signal processing (speech processing and bio-signals), and wireless sensor networks.

MOHAMAD NIZAM BIN AYUB is currently a Senior Lecturer with the Department of Computer Systems, Faculty of Computer Science and Information Technology, University of Malaya, Kuala Lumpur, Malaysia.

INSAF ULLAH received the M.S. degree in computer sciences from the Department of Information Technology, Hazara University Mansehra, Pakistan, where he is currently pursuing the Ph.D. degree in computer sciences. He is currently a Lecturer with the Department of Computer Sciences, Hamdard University, Islamabad. His research interests include network security, UAVs/drones, information centric networking (ICN), named data networking (NDN), the IoT, IIoT, wireless sensor networks (WSN), wireless body area networks (WBAN), and cryptography.

IHSAN ALI received the M.S. degree in computer system engineering from the Ghulam Ishaq Khan Institute of Engineering Sciences and Technology, in 2008. He is currently pursuing the Ph.D. degree with the Faculty of Computer Science and Information Technology, University of Malaya, Kuala Lumpur, Malaysia. He has been actively involved in research and teaching activities for the last ten years in the different country, including Saudi Arabia, USA, Pakistan, and Malaysia. He is currently an Active Research Associate with the Centre for Mobile Cloud Computing Research, Faculty of Computer Science and Information Technology, University of Malaya. He has authored or coauthored more than 40 high impact research journal articles, including a highly reputable IEEE COMMUNICATIONS SURVEYS AND TUTORIALS and *IEEE Communication Magazine*. His research interests include wireless sensor networks (WSNs), robotics in WSNs, sensor cloud, fog computing, the IoT, and ML/DL in WSN. He has served as a Technical Program Committee Member for several well-known conferences, including the IWCMC 2017-2018, AINIS 2017, Future 5V 2017, ICACCI-2018, INAIT2019, DiCES-N19, CCNC2020, ICCAIS2020, and CSNT2020. He has an Organizer of the special session on fog computing in Future 5V 2017. He is an Active Reviewer of *Computers and Electrical Engineering*, the *KSII Transactions on Internet and Information Systems*, *Mobile Networks and Applications*, the *International Journal of Distributed Sensor Networks*, the *Journal of Advanced Transportation*, the IEEE TRANSACTIONS ON INTELLIGENT TRANSPORTATION SYSTEMS, *Computer Networks*, IEEE ACCESS, *Wireless Communications and Mobile Computing*, and *IEEE Communication Magazine*.

TARAK NANDY (Graduate Student Member, IEEE) received the M.Tech. degree in computer science and engineering from the West Bengal University of Technology, India. He is currently pursuing the Ph.D. degree with the University of Malaya, Malaysia. He is currently serving as a Graduate Research Assistant in computer system and technology with the University of Malaya. His major research interests include vehicular communication, the IoT, cyber-physical security, machine learning, authentication, and privacy.

MUKTAR YAHUZA (Graduate Student Member, IEEE) received the B.Eng. degree in computer engineering from Bayero University Kano, Nigeria, in 2010, and the M.Sc. degree in computer information and engineering from the International Islamic University Malaysia (IIUM), in 2015. He is currently pursuing the Ph.D. degree in computer science with the University of Malaya, Malaysia. His research interests include information security, Internet of drones security and privacy, lightweight authentication and privacy, and image processing.

NAUMAN KHAN (Graduate Student Member, IEEE) received the master's degree from the University of Electronic Science and Technology of China, in 2016, where his research area was software-defined networking. He is currently pursuing the Ph.D. degree in computer science with the University of Malaya, Kuala Lumpur. He was working as a Network Engineer for more than three years in local and international IT companies. He is currently a Lecturer with the University of Malakand, Pakistan, and sponsored for the Ph.D. degree through the Higher Education Commission of Pakistan, Faculty Development Program. He is a CISCO (CCNA and CCNP), Microsoft certified. His research interests include software-defined networking, network security, and the Internet of Things.