Elliptic Curve Signcryption Based Security Protocol for RFID

Anuj Kumar Singh[1*] and B.D.K.Patro[2]
[1] Dr. A.P.J. Abdul Kalam Technical University, Lucknow, (U.P), India
[e-mail: anujbtechcs@gmail.com]
[2] Rajkiya Engineering College, Kannauj, (U.P.), India
[e-mail: bdkpatro@rediffmail.com]
*Corresponding author: Anuj Kumar Singh

Received February 11, 2019; revised July 9, 2019; revised August 12, 2019; accepted September 6, 2019; published January 31, 2020

Abstract

Providing security has been always on priority in all areas of computing and communication, and for the systems that are low on computing power, implementing appropriate and efficient security mechanism has been a continuous challenge for the researchers. Radio Frequency Identification (RFID) system is such an environment, which requires the design and implementation of efficient security mechanism. Earlier, the security protocols for RFID based on hash functions and symmetric key cryptography have been proposed. But, due to high strength and requirement of less key size in elliptic curve cryptography, the focus of researchers has been on designing efficient security protocol for RFID based on elliptic curves. In this paper, an efficient elliptic curve signcryption based security protocol for RFID has been proposed, which provides mutual authentication, confidentiality, non-repudiation, integrity, availability, forward security, anonymity, and scalability. Moreover, the proposed protocol successfully provides resistance from replay attack, impersonation attack, location tracking attack, de-synchronization attack, denial of service attack, man-in-the-middle attack, cloning attack, and key-compromise attack. Results have revealed that the proposed protocol is efficient than the other related protocols as it takes less computational time and storage cost, especially for the tag, making it ideal to be used for RFID systems.

Keywords: RFID, security, elliptic curve, signcryption.

1. Introduction

The rapidly changing computing age has enabled the automation of processes and identification of objects, which have now become very significant parts of computing since they lead to massive benefits in productivity by saving time and reducing errors. Many technologies which have been developed to implement AIDC include optical character recognition, bar codes, smart cards, chip cards, magnetic stripes, biometrics, voice recognition, and Radio Frequency Identification (RFID). RFID [1] has been proven as one of the most prominent technologies used for identification and data capture due to its ability to track moving objects. Furthermore, Jia et al. [2] have mentioned that with the evolution of the Internet of Things (IoT), the usage of RFID has grown exponentially since it is the fundamental technology behind IoT. Khattab et al. [3] have figured out that RFID outperforms other AIDC techniques when compared against different parameters including data density, readability by machine, readability by people, cost, reading speed, range, the effect of moisture, and sight distraction.

1.1 Overview of RFID

RFID is a radio frequency electromagnetic signal based wireless communication technology, which is used to automatically identify objects carrying tags. The two major communicating parties in an RFID system are the tags and the readers. The schematic diagrams of the RFID tag and the reader have been presented in **Fig. 1 (a)** and **Fig. 1 (b)** respectively. Yu and Chen [4] has mentioned that RFID tags can be divided into three categories namely passive tags, active tags, and semi-active tags. A passive tag does not hold a battery and it gets energy from the neighboring RFID reader. In contrast, an active tag holds a battery, which provides sufficient energy to pass its messages to a greater range. A semi-active tag has a small battery on-board but it activates only in the presence of an RFID reader. According to Chetouane [5], the generic architecture of an RFID communication system is based on 3Cs: Context, Capture, and Control, which has been depicted in **Fig. 2**.

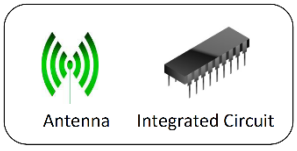

Fig. 1(a). RFID Tag

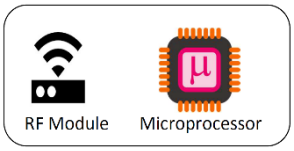

Fig. 1(b). RFID Reader

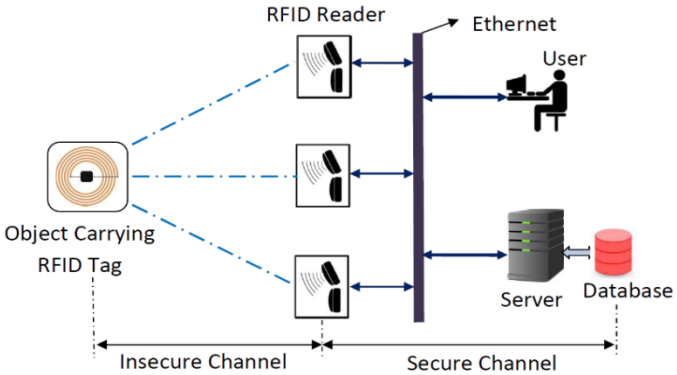

Fig. 2. Generic architecture of RFID system.

The main components of an RFID system are transponder (RFID Tag), transceiver (RFID Reader), antenna, server, and the database. The RFID tag contains a unique identification number, which is stored in the read-only memory of tag. This unique identification number enables the system to recognize the tag idiosyncratically among many tags. When an object carrying transponder enters in the zone of a transceiver its data is captured through the wireless channel by the transceiver and sent to the server for storage and further processing. An

authorized user can access the data stored on the server according to the requirements of the user's applications. An RFID tag generally contains identification information, location information or specification of the object containing the tag, like price, make, date, etc.

1.2 RFID Security Requirements

The four basic security requirements of any communication are confidentiality, integrity, authentication, and non-repudiation. But for communication over the wireless medium, like between RFID tag and the reader, implementation of some more security functionalities is needed. Tan and Wu [6] have pointed out that three key security requirements of RFID are prevention from unauthorized access, prevention from illicit tracking and prevention from skimming. Knospe and Pohl [7] have mentioned confidentiality, availability, authenticity, integrity, and anonymity are the necessary security properties of an RFID system. Dinarvand and Barati [8] figured out that the two additional security features which must also be implemented in the RFID system are forward secrecy and scalability. Therefore, the necessary security requirements of an RFID system are data confidentiality, mutual authentication, data integrity, non-repudiation, availability, tag anonymity, forward secrecy, and scalability.

1.3 RFID Security Challenges

Designing an efficient security mechanism is a big concern for RFID because of the following technical constraints of RFID:
Limited Computing Capability – On an average, the RFID tags possess a processing speed of only a few MIPS, flash memory up to 1MB and RAM up to few 100s KB. With these limited computing resources, it has been very exigent to design and implement security schemes which provide all the necessary security functionalities.
Unreliable Communication – Since the data between tags and reader is transmitted through an insecure wireless channel, it is vulnerable to attacks by unauthorized readers and eavesdroppers. A strong security mechanism should be implemented to prevent the RFID system from these attacks.
Less Power – Since active and semi-active tags operate on a battery which is a limited power source, security schemes should be wisely selected and heavy computations must be avoided.
The two major security challenges in the security of RFID are – first defeating threats and attacks made on to the system using appropriate countermeasures and second using efficient security mechanisms to implement these countermeasures along with necessary security functions.
In [9,10] authors have discussed security issues and challenges for RFID and provides an overview of threats and attacks on RFID systems. A comprehensive study of attacks on RFID has been made by Khattab et al. [11] in which they classified attacks on RFID into three types – physical attacks, system attacks, and channel attacks. The taxonomy of potential attacks on RFID is shown in **Fig. 3**. In Physical attacks, tag modification or tampering can be prevented by building a secure zone around the device or using sealed tamper resistant case for the device. Cloning and reverse engineering can be prevented by using a strong cryptographic fingerprint. The jamming attack can be countered by using spread spectrum technologies and polarization of the antenna. For prevention of other channel attacks and system attacks, design and implementation of appropriate cryptographic schemes is needed.The cryptographic systems which are potential candidates for securing any system are Symmetric Key Cryptosystem, RSA Cryptosystem, Elliptic Curve Cryptosystem, and Pairing Based

Cryptosystem. A comparison of these cryptographic systems has been made on the basis of different aspects and is publicized in **Table 1**.

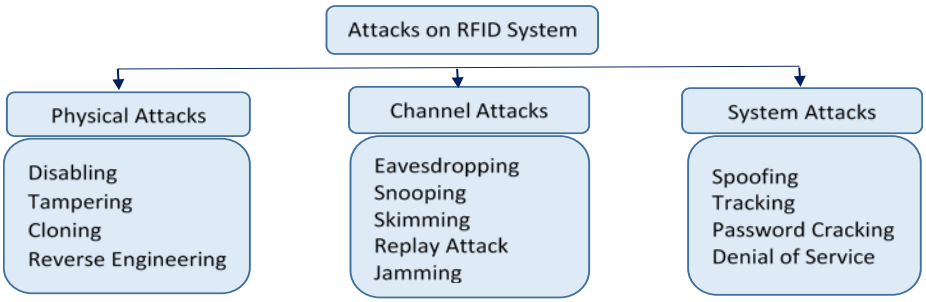

Fig. 3. Taxonomy of attacks on RFID.

By Analyzing **Table 1,** it can be observed that PKC suffers from the problem of key distribution and only provides confidentiality, while RSA consumes high computational cost due to the computation of modular exponentiation. ECC and PBC perform better than RSA in terms of computational cost and security features. Cao and Liu [12] have pointed out that in PBC large size parameters are generated which requires a lot of computing resources and hence PBC is not suited for resource constrained systems like RFID. ECC based security solutions require less key size, produce smaller ciphertext, faster in key generation, quicker in signature verification, and quicker in encryption and decryption as compared to other public key cryptosystems. And due to this reason, ECC is an attractive cryptosystem for providing security to less computationally capable systems like RFID.

Table 1. Comparison of cryptosystems.

Consideration	PKC	RSA	ECC/PBC
Type of Cryptosystem	Symmetric	Asymmetric	Asymmetric
Time of Operations	Reasonable	Very High	Very High
Communication Cost	Reasonable	Very High	Reasonable
No. of Keys (order)	n^2	n	n
Security Features	Co	Co, Au, Nr, Ke	Co, Au, Nr, Ke
Complexity	$O(n)$	$O(n^3)$	$O(n^2)$
Memory Required	Very Less	Huge	Reasonable
Key Size	80	1024	160
Key Generation	Fast	Slow	Fast
Key Exchange	Big Issue	Not an Issue	Not an Issue

PKC-Private Key Cryptosystem, RSA-RSA Cryptosystem, ECC-Elliptic Curve Cryptosystem, PBC-Pairing Based Cryptosystem, Co -Confidentiality, Au -Authentication, Nr –Non-repudiation, Ke – Key Exchange, n-Number of parties

2. Related Work

Security and privacy have been a primary concern for RFID systems due to their less computational capacity. Many security solutions offering different security properties have been proposed over the years. But, a large amount of the emphasis has been given in designing secure authentication protocols for RFID, since majority of applications implement RFID for authentication of objects by the reader or the server. Furthermore, many secure and efficient

protocols based on elliptic curves have been proposed in recent years, since elliptic curve based solutions are suitable for resource constrained applications.

Gódor, Giczi, and Imre [13] suggested an elliptic curve mutual authentication protocol for RFID which provides mutual authentication and forward secrecy, at the same time providing protection from replay attack and tracking attack. The computational time of different operations in the protocol was also analyzed. But, many necessary security attributes were not implemented in this scheme and it was not able to counter DoS attack.

In [14] Liu, Qin, and Wang proposed an authentication protocol for RFID based on ECC, which reduces the computational cost of RFID tag and provides data confidentiality, integrity, tag anonymity, and mutual authentication. The protocol was able to defend against tracking attack, replay attack, counterfeit attack, and desynchronization attack.

Chou [15] classified the RFID security protocols as full-fledged, simple, lightweight, and ultra-lightweight. Chou mentioned that full-fledged security protocols are attractive since non-full-fledged protocols are not scalable and vulnerable to tracking, desynchronization and impersonation attacks. Chou also presented an authentication protocol based on ECC and claimed that in addition to mutual authentication and location privacy it also provides forward secrecy and scalability, at the same time providing protection from DoS, replay, impersonation, and man-in-the-middle attacks.

Farash [16] demonstrated that Chou's authentication protocol [15] fails to provide tag privacy, mutual authentication, and forward secrecy. It was also shown that Chou's protocol failed to defend from impersonation, cloning attacks, and tracking attacks. Farash [16] also proposed an improved protocol which can counter reply, man-in-the-middle, impersonation, and tracking attacks at the same time providing forward secrecy and mutual authentication. But the total computational time of this protocol is higher than existing schemes for a RFID system.

Feng and Yao [17] designed an ECC based mutual authentication protocol for RFID which can resist impersonation, replay, tracking and denial of service attacks. They claimed that the proposed protocol takes less computational time, storage cost and communication overhead.

Alamr, Kausar, and Kim [18] suggested a secure protocol for RFID which uses elliptic curve Diffie-Hellman (ECDH) key exchange scheme to generate the shared secret key. This key is then used to encrypt the messages. This protocol provides resistance from man-in-the-middle attack, impersonation attack, and replay attack while satisfying forward security, mutual authentication, location privacy ,anonymity, and confidentiality.

Qian, Jia, and Zhang [19] proposed a lightweight security protocol for RFID using ECC encryption and basic computations like bitwise XOR, AND etc. Although this protocol reduces tag computation and does not use elliptic curve point multiplication operation, it is limited to provide authentication, confidentiality, forward security, and backward security.

Chen and Chou [20] analyzed some full-fledged RFID protocols based on ECC, and pointed out that few of these have security and privacy weaknesses while other possess high communication cost. They also proposed two protocols and claimed that they are secure and efficient. However, Shen et al. [21] proved that the protocol of Chen and Chou [20] is susceptible to replay attack and server spoofing attack. Shen et al. also proposed an ECC based authentication mechanism for RFID which offers mutual authentication, anonymity, confidentiality, forward secrecy, and untraceability. This mechanism also provides protection from masquerade, server spoofing, and replay attack.

Liao and Hsiao [22] proposed an elliptic curve based RFID authentication protocol which uses the transfer of secure challenge response and ID-verifier messages. Zhao [23] has shown that Liao and Hsiao's protocol [22] endures with key compromise problem where an opponent could retrieve the key stored in the tag. Zhao also developed a authentication scheme and

claimed that it is more secure and efficient than Liao's protocol. Farash et al. [24] demonstrated that Zaho's scheme [23] failed to provide forward security. They designed a new improved RFID authentication mechanism for healthcare surroundings offering forward security, provable security, mutual authentication, and location privacy while protecting from replay, impersonation, and man-in-the-middle attacks.

Lee et al. [25] exposed the issues of untraceability and anti-counterfeting in RFID systems. They also proposed a security scheme for RFID which provided many security features but it fails to satisfy mutual authentication, scalability, and resistance against de-synchronization attack.

Dinarvand and Barati [8] presented an elliptic curve based mutual authentication protocol which offers many security features including mutual authentication, confidentiality, forward security, scalability, anonymity, availability, and integrity. They also proved that the protocol can defend against cloning, replay, de-synchronization, location tracking, masquerade, modification, and server spoofing attacks. Dinarvand and Barati [8] also compared their protocol with the related ones and showed that it takes less computational time and communication cost than others.

Zhang et al. [26] suggested an elliptic curve based scheme with anonymity for session initiation. Lu et al. [27] exposed that Zhang et al.'s scheme [26] fails to provide proper mutual authentication and is susceptible to insider attack. Lu et al. designed a modified authentication scheme overcoming the security weaknesses of Zhang et al.'s scheme. Mehmood et al. [28] proved that the scheme proposed by Lu et al. [27] fails to defend against masquerade attack and cannot protect the user's identity. Mehmood et al. suggested an improved mutual authentication for session initiation which is secure against replay, password guessing, insider, masquerade, stolen verifier, and man-in-the-middle attack. The protocol also offers anonymity, privacy, forward secrecy, mutual authentication, forward security, and session key privacy.

Jin et al. [37] applied elliptic curve cryptography to enhance medication safety of the patient and proposed a secure elliptic curve based authentication protocol for the healthcare environment.

Zheng et al. [38] designed a mutual authentication scheme based on ECC which provides confidentiality, forward security, scalability, mutual authentication, and anonymity. In addition to these security attributes, this protocol provides resistance against system internal attack , camouflage attacks, denial of service attacks, and tracking attacks.

Chiou, Ko, and Lu [39] developed an ECC based mutual authentication protocol for mobile RFID. But, in this protocol five elliptic curve point multiplication operations are to be executed by the tag, which puts a huge computational overhead on the tag. Therefore, this protocol is not suitable for RFID systems.

Fan et al. [40] presented a lightweight RFID security protocol for medical privacy and claimed that it satisfies secure authentication and confidentiality. This scheme utilized only XOR operation, hash computation, displacement operation, and cross operation. However, Aghili and Mala [41] performed a comprehensive security analysis of the protocol presented by Fan et al. and revealed that it is susceptible to server/reader impersonation attack and disclosure of secret information.

Liu et al. [42] designed an elliptic curve based authentication management protocol for mobile RFID systems. They claimed that their protocol can resist all kinds of attacks and is more efficient. However, it can be figured out by studying the authentication phase of the protocol that the tag has to execute four elliptic curve point multiplication operations which increases the tag's computational cost by a huge amount i.e. the Liu et al.'s protocol is computationally inefficient.

3. Preliminaries

3.1 Mathematics of Elliptic Curve

An elliptic curve over finite field is defined by the Weierstrass Equation $y^2 = x^3 + Ax + B$ where $A, B \in F_q$ are constants with the condition $4A^3 + 27B^2 \neq 0$. An elliptic curve denoted by E over finite field F_q is defined by the set of all points (x, y) ϵ F_q X F_q along with a special point ∞ called as point at infinity O. These set of points is given by:

$E(F_q) = \{O\} \cup \{ (x, y) \in F_q \times F_q : y^2 = x^3 + Ax + B \}$

The following laws and operations are satisfied by elliptic curve $E(F_q)$:

1. Identity – For every point $P \in E(F_q), P + O = O + P = P$.

2. Negatives – Let $P = (x, y \in E(F_q)$, then $-P = (x, -y)$ is called as the negative of *P*. And $P + (-P) = O$. Furthermore, $-O = O$.

3. Point Addition – Let $P = (x_1, y_1 \in E(F_q)$ and $Q = (x_2, y_2) \in E(F_q)$ be the two points and $P \neq \pm Q$. The addition of these two points is defined by a third point on $E(F_q), P + Q = (x_3, y_3)$. The coordinates x_3 and y_3 are given by:

$x_3 = \lambda^2 - x_1 - x_2$ and $y_3 = \lambda(x_1 - x_3) - y_1$

where $\lambda = \frac{y_2 - y_1}{x_2 - x_1}$, if $P \neq Q$ and $\lambda = \frac{3{x_1}^2 + A}{2y_1}$, if $P = Q$

4. Point Multiplication – Let $P = (x, y) \in E(F_q)$, then point multiplication is defined by $kP = P + P + \ldots + P$ $(k\ times)$. Where k is an integer.

5. XOR Operation – The XOR operation is the binary bitwise operation which returns a 0 bit when both the input bits are same. This is equivalent to the addition of two bits in radix 2, and discarding the carry bit. In this paper XOR operation of two points on the the elliptic curve has been computed by performing XOR operation between the x -coordinates and the y-coordinates of both the points respectively to give the new point on the elliptic curve.

6. Function F: function F has been used to select only the x-coordinate of the point (x, y) on the elliptic curve, i.e. $F(x, y) = x$.

3.2 Computational Problems based on Elliptic Curve

The security of elliptic curve cryptosystem is based on the three computationally hard problems defined below. For these definitions let $E(F_q)$ be an elliptic curve defined over finite field F_q.

1. ECDLP (Elliptic Curve Discrete Logarithmic Problem) – Given two points $P, Q \in E(F_q)$, it is computationally hard to determine an integer $k \in [1, n-1]$ such that $Q = kP$ [31].

2. ECDHP (Elliptic Curve Diffie-Hellman Problem) – Consider a point $P \in E(F_q)$, and two other points $Q = aP$ and $R = bP$ on E, where a and b are integers. It is computationally hard to determine a point $S = abP$ [32], given P.

3. ECDDHP (Elliptic Curve Decision Diffie-Hellman Problem) – Given a point $P \in E(F_q)$, and three other points $Q = aP$ and $R = bP$, and $S = cP$ on E. It is computationally hard to decide whether $S = abP$ [33].

3.3 Signcryption

Signcryption established by Zheng [29] is a cryptographic primitive which integrate encryption and authentication in a single logical phase. Before the advent of signcryption, to achieve confidentiality and authentication, the approach was to use signature-then-encryption

which first apply the signature and then encrypt the message. In [29] it was shown by Zheng that signcryption saves 50% computational time and 85% communication cost in comparison to signature-then-encryption method. Zheng and Imai [30] proposed the first elliptic curve based signcryption mechanism which consumes 58% less computational time and 40 % less communication overhead in comparison to signature-then-encryption based on ECC. Using elliptic curve with signcryption saves huge computation cost and communication overhead, simultaneously implementing multiple security attributes comprising confidentiality, unforgeability, integrity, authentication, non-repudiation, forward security, secure key exchange, and public verification.

4. Proposed Security Protocol for RFID

In this section, an elliptic curve signcryption based security protocol for RFID has been proposed and explained in detail. The protocol presented here is applicable to passive tags, active tags, and semi-active tags since in this protocol, the first message is initiated by the server. In the proposed security protocol it is presumed that the communication link between the server and the tag is wireless and insecure, while the link between the reader and the server is wired and secure. The notations and symbols used in describing the proposed protocol are listed in **Table 2**. The proposed protocol has been divided into three phases: setup phase, signcryption-unsigncryption phase, and updating phase.

Table 2. Notations and symbols used in the protocol.

Denotation	Symbol
Elliptic curve on finite field F_q defined by $y^2 = x^3 + Ax + B$	E
Finite prime field of size q	F_q
Elliptic curve parameters for E	A, B
Generator of E with order n	G
Two large prime numbers	q, n
Server's private key	v_s
Server's public key	P_s
Randomly selected integer by tag	v
Tag identifier	x_t
Unique pseudonym of tag	ID
Symmetric key encryption with key k	E_k
Symmetric key decryption with key k	D_k

4.1 Setup Phase

In this phase, public keys, private keys, and the system parameters are generated. The following steps are carried out by the server in the setup phase:

1. Selects an elliptic curve $E: y^2 = x^3 + Ax + B$ with the curve parameters $\{q, A, B, G, n\}$.
2. Randomly selects a number $v_s \in Z_n$ which becomes its private key and computes its public key as $P_s = v_s G$.
3. For each tag, the server randomly chooses the unique identifier $x_t \in G$ for the tag on the elliptic curve E.
4. Randomly selects an integer $ID \in Z_n$ which becomes the unique pseudonym for the tag.
5. Hash function $hash: \{0,1\}^* \rightarrow \{0,1\}^l$ is selected by the server.
6. The server saves the pair $\{ID, x_t\}$ for each tag in its database.

7. The server also stores common elliptic curve parameters $\{q, A, B, G, n\}$,the unique identifier x_t and the unique pseudonym ID in the memory of each tag.

4.2 Signcryption-Unsigncryption Phase

In the signcryption-unsigncryption phase, authentication and confidentiality attribute is implemented in the transfer of messages involving the server and the tag. The tag and the server authenticate each other in this phase. The steps carried out in this phase are:
1. A number $v_s \in Z_n$ is selected by the server at random, which becomes its private key. And the server computes $P_s = v_s G$ as its public key. The server sends a message containing its public key $\{P_s\}$ to the tag.
2. Upon receiving the public key $\{P_s\}$ of the server, the tag performs the following operations:
(i) The tag randomly chooses a number $v \in Z_n$.
(ii) Generate the key $k = hash(vP_s \oplus x_t)$.
(iii) Compute the ciphertext $c = E_k\ (ID)$.
(iv) Compute $r = hash(c \oplus k)$.
(v) Calculate $w = (\frac{v}{r})$ and $T = rG$.
(vi) The tag sends the signcrypted text $\{c, T, w\}$ to the server.
3. Upon receiving the signcrypted text $\{c, T, w\}$ the server performs the following computations:
(i) Generate the key $k' = hash(v_s wT \oplus x_t)$.
(ii) Decrypt the ciphertext using key k' as $ID' = D_{k'}(c)$ which is the unique pseudonym of the tag.
(iii) The server searches its database and finds the tag identifier x_t corresponding to the unique pseudonym ID' of tag . If the corresponding tag identifier is not found then the session is terminated by the server.
(iv) Compute $r' = hash(c \oplus k')$.
(v) Calculate $T' = r'G$.
(vi) If $T = T'$, then the server successfully authenticates the tag. Otherwise, the server terminates the session.
(vi) If the authentication of the tag is successful, the server computes $a_s = E_k\ (T' \oplus x_t)$ and sends $\{a_s\}$ to the tag.
4. On receiving $\{a_s\}$, the tag computes $a_s' = E_k\ (T \oplus x_t)$. If $a_s = a_s'$, then the tag successfully authenticates the server. Otherwise, the tag terminates the session. The working of the protocol has been demonstrated in **Fig. 4**.

4.3 Updating Phase

After successfully authenticating each other, the server and the tag must update the unique pseudonym ID of the tag. Since ID of the tag is transmitted as plaintext in the proposed protocol, it is important to update the tag pseudonym so that it can be protected from unauthorized usage and de-synchronization attack. The tag updates the ID as:
$ID^{New} = F(vP_s) \oplus F(x_t) \oplus ID$
The server updates the ID of the tag by performing the following computation:
$ID^{New} = F(v_s wT) \oplus F(x_t) \oplus ID$

5. Proof of Correctness

The correctness of the proposed signcryption based protocol is based on the fact that the tag and the server generate the same key in Step 2 and Step 3 of the protocol respectively, as these keys are used in encryption and mutual authentication between the two parties.

Key generated by the tag in Step 2: $k = hash(vP_s \oplus x_t)$

$= hash(v\, v_s G \oplus x_t) \quad (Since\ P_s = v_s G)$

Key generated by the server in Step 3: $k' = hash(v_s wT \oplus x_t)$

$= hash\left(v_s \left(\frac{v}{r}\right) rG \oplus x_t\right) Since\ w = \left(\frac{v}{r}\right), T = rG)$

$= hash(v_s v\, G \oplus x_t)$

$= k$

Since keys $k\ and\ k'$ are same, hence the correctness of the proposed protocol is verified.

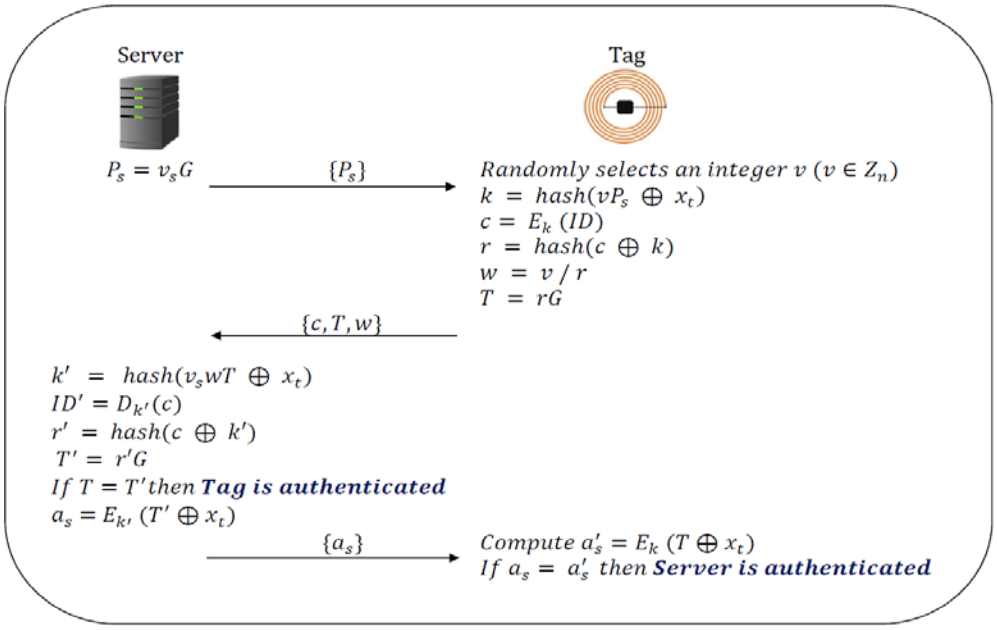

Fig. 4. Proposed Security Protocol for RFID.

6. Security Functions of the Proposed Protocol

The security functionalities of the proposed protocol can be analyzed with respect to two dimensions, the first one is the security attributes implemented by the protocol and the second one is the resistance provided from different attacks.

6.1 Analysis of Security Attributes

As discussed in sub-section 1.2 the security attributes required by an RFID system are confidentiality, mutual-authentication, integrity, non-repudiation, forward security, tag anonymity, and availability. In this sub-section, an analysis of security attributes satisfied by the proposed protocol has been performed. To sustain the security analysis some reasonable assumptions have been made.

Assumption 1*:* The tag id x_t is kept secret between the tag and the server only.

Assumption 2*:* The adversary can obtain common system parameters from a corrupted tag.

Assumption 3: The random numbers v and v_s chosen by the tag and the server respectively are fresh in every session.
Assumption 4: The encryption algorithm E_K is secure enough such that an $Adversary\ A$ is unable to decode ciphertext c.
Assumption 5: If $T = rG$ then the adversary cannot obtain r, given T, due to the strength of ECDLP.

(1) Confidentiality

Confidentiality is the assurance that the messages to be kept secret, must not be readable by the $Adversary\ A$ during the transit. In the proposed protocol, three messages are transferred between the server and the tag. The first one is the public key of server P_s sent by the server to the tag. Since the public key of the server is a public parameter, it can be sent as plaintext. The second message is the signcrypted text $\{c, T, w\}$ sent by the tag to the server. All the three components of the signcrypted text $\{c, T, w\}$ are generated in a way that they do not reveal any secret information to the $Adversary\ A$. The $Adversary\ A$ cannot decrypt c since it needs private quantities v and x_t of the tag to generate the key k. By the property of ECDLP, the $Adversary\ A$ cannot generate r, given T and G. The component w has been produced by dividing private number v of the tag by r. Obtaining w is not possible for adversary as v and r are secretly generated by the tag. The third message is $\{a_s\}$ and without knowing the key k and tag id x_t adversary cannot understand $\{a_s\}$. Therefore, the proposed protocol successfully provides confidentiality attribute.

(2) Mutual Authentication

(i) Authentication of the Tag by the Server - Upon receiving the signcrypted text $\{c, T, w\}$from the tag, the server first generates the key k' and decrypts c to get the tag pseudonym ID'. Then it searches its database to find the matching tag id x_t of the tag. If a matching tag id is found, it calculates r'. Finally the server computes $T' = r'G$. If T' computed by the server is equal to T received within the signcrypted text from the tag, then the server authenticates the tag. The value of T computed by the tag depends upon the value of r and public parameter G as $T = rG$. The value of r calculated by the tag depends upon ciphertext c and key k generated by the tag. In turn, the value of ciphertext c and key k depends upon the secret values v and x_t, where v is the private number generated by the tag and x_t is known only to the tag and the server. If an adversary pretends to be legitimate tag then, it should generate the correct value of T. Since the tag id x_t is only available to the server and the tag, no illegitimate tag can generate the correct value of T. Therefore, the signature generated by the tag is unforgeable.
(ii) Authentication of the Server by the Tag - Upon receiving a_s from the server the tag computes a_s'. If a_s received from the server is equal to the a_s' computed by the tag, then the tag authenticates the server. The value of a_s computed by the server depends upon the tag id x_t which is kept secret between the server and the tag. It is impossible for an illegitimate server to generate the correct value of a_s. Therefore the signature generated by the server is unforgeable.

(3) Integrity

According to the random oracle model, it is not possible for an $Adversary\ A$ to find out two messages which provide the same message digest [36]. If an adversary changes any value in $\{c, T, w\}$ it can be easily detected by the server since the key k' will not be same as key k generated by the tag, which in turn will enable the incorrect generation of T' by the server. The authentication, in this case will fail and the server will terminate the session. Similarly, if an $Adversary\ A$ modifies the message a_s in transit then it can be easily detected because it will not be same as the value of a_s' computed by the tag and the tag will terminate the session. Thus the integrity of the messages is ensured in the proposed protocol.

(4) Non-repudiation

The value of all the three components in the message $\{c, T, w\}$ sent by the tag to the receiver depends upon the tag id x_t. Similarly, the message $\{a_s\}$ sent by the server to the tag is also a function of the tag id x_t. According to *Assumption 1*, if $T = T'$ then the tag cannot deny that it has sent the message and if $a_s = a_s{}'$ then the server cannot deny that it has sent the message.

(5) Forward Security

Even if an $Adversary\ A$ somehow knows the tag id x_t, then also it cannot obtain the previous messages, since the messages $\{c, T, w\}$ and $\{a_s\}$ sent by the tag and the server respectively, depends upon the key generated by both the parties, which in turn depends upon the private random numbers v and v_s chosen by the tag and the server respectively. So the proposed protocol provides forward security as the adversary cannot get the past messages and use them later.

(6) Availability

In the messages sent between the tag and the server, tag id x_t remains same and the adversary cannot access it. Furthermore, the tag pseudonym ID which is transmitted to the server is updated after each session in updating phase explained in sub-section 4.3. Updating the tag pseudonym ID for both the tag and the server ensures that both the server and the tag are always synchronized. Therefore, the proposed protocol offers de-synchronization and meets the availability requirement.

(7) Anonymity

In the proposed protocol the only confidential information of the tag to be transmitted between the server and the tag is tag id x_t. In the signcrypted message sent by the tag to the server, the security of the tag id x_t is maintained by performing XOR operation between the tag id x_t and vP_s. Moreover, the hash function is also applied over the result obtained from XOR operation. To obtain x_t, an adversary needs to know the generated key k and the private random number v of the tag, which is not possible. Similarly in the message $\{a_s\}$ sent by the server to the tag, secrecy of the tag id x_t is maintained by performing XOR operation between the tag id x_t and T' and then encrypting the result of XOR using key k'. To get the value of x_t the adversary needs to decrypt the a_s which is not possible as it doesn't know the key k'. So, the proposed protocol provides tag anonymity.

(8) Scalability

A scalable security protocol for RFID should avoid computational workload in proportion to the number of tags. In step 3 of the protocol, the server searches its database and finds the tag identifier x_t corresponding to the unique pseudonym ID received from the tag. Therefore the server does not require linear search to know the identity of each tag [22]. In the proposed protocol the server takes $O(1)$ time to search the matching tag, thus saving a huge amount of cost as the number of tag increases in the system. Therefore, the proposed protocol provides scalability.

6.2 Analysis of Resistance against Attacks

An RFID security protocol must be able to counter the attacks made on the RFID system. The strength of the proposed RFID security protocol against different attacks, has been analyzed in this sub-section. To model the active and passive attacks launched by the $Adversary\ A$ between the server Ś and the tag T, we consider the attack model given by Ouafi and Phan [35] in which three queries can be generated by the $Adversary\ A$.

Query 1: $Execute(Ś, T, k)$ – For passive attacks, we assume that the $Adversary\ A$ eavesdrops the channel between Ś and T to get honest execution of session k of the protocol.

Query 2: $Send\ (U, V, k, M)$ – For active attacks, the $Adversary\ A$ impersonate a reader $U \in Reader$ (respective tag $U \in Tags$) in some session k of the protocol and sends its chosen message M to an instance of some tag $V \in Tags$ (respective reader $V \in Readers$).
Query 3: $Corrupt(T, K)$ – This query permits the $Adversary\ A$ to obtain the secret K stored on the tag. Since no secret key K is stored on the tag in the proposed protocol, this query can be omitted.

(1) Resistance against Replay Attack

An adversary eavesdropping the channel may pretend to be a legitimate tag or server by replaying the past messages sent between the server and the tag. When an $Adversary\ A$ eavesdrops the messages between the tag and the receiver it can obtain $\{P_s, c, T, w, a_s\}$ and can replay the messages to the server or to the tag to produce an unauthorized effect. In the proposed protocol private random numbers are used and the tag pseudonym ID is updated to ID^{new} after each session, hence the $Adversary\ A$ is unable to use the previously recorded messages in a new session to befool the tag or the server.

(i) If an $Adversary\ A$ tries to pretend to be a legitimate tag and sends the past recorded message $\{c, T, w\}$ to the server, then the server performs the following computations:
Computes the key as $k' = hash(v_s wT \oplus x_t)$
Decrypt the tag pseudonym as $ID' = D_{k'}(c)$
Since $ID' \neq ID^{new}$ the server cannot find a matching x_t and terminates the session.

(ii) If an $Adversary\ A$ tries to pretend to be a legitimate server and sends the past recorded messages $\{P_s\}$ and $\{a_s\}$ to the server, then the tag performs the computations given below.

- Upon receiving $\{P_s\}$ the tag does the following for the new session started by the $Adversary\ A$:
  $Randomly\ selects\ an\ integer\ v^{new}\ (v^{new} \in Z_n)$
  $k^{new} = hash(v^{new} P_s \oplus x_t)$
  $c^{new} = E_{knew}\ (ID^{new})$
  $r^{new} = hash(c^{new} \oplus k^{new})$
  $w^{new} = (v^{new} / r^{new})$
  $T^{new} = r^{new} G$
- Upon receiving $\{a_s\}$ from the $Adversary\ A$ the tag computes
  $a_s^{new} = E_{knew}\ (T^{new} \oplus x_t)$

Clearly, $a_s^{new} \neq a_s$ as the random number v^{new} and the updated tag pseudonym ID^{new} has been used by the tag in the new session, instead of v and ID used in the earlier session. Therefore, the authentication of the server fails and the session is terminated by the tag. The resistance of replay attack by the server and the tag has been demonstrated in **Fig. 5** and **Fig. 6** respectively.

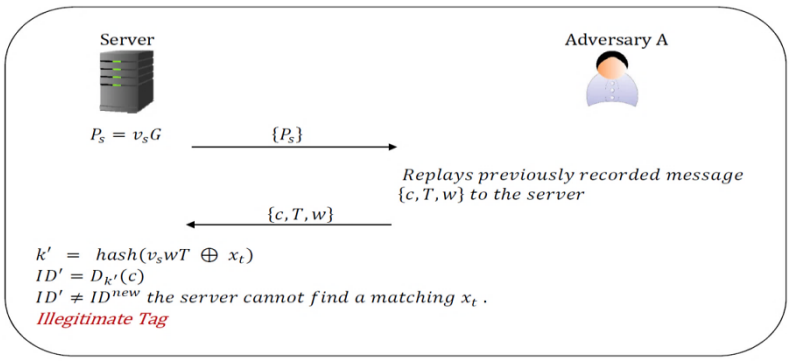

Fig. 5. Resistance against replay attack by the server.

(2) Resistance against Cloning Attack

Liao and Hsiao [22] have mentioned that if the same shared secret key is used in the authentication of a group of tags by the server, it is vulnerable to cloning attack. In the proposed protocol since there is no shared secret key stored on the tag, and the key is generated dynamically by the tag for each session, the adversary cannot steal the secret information to clone the tag. Even if the adversary is able to get unique id x_t for a group of tags, it cannot obtain x_t for other tags, since x_t is a random point chosen in the proposed protocol.

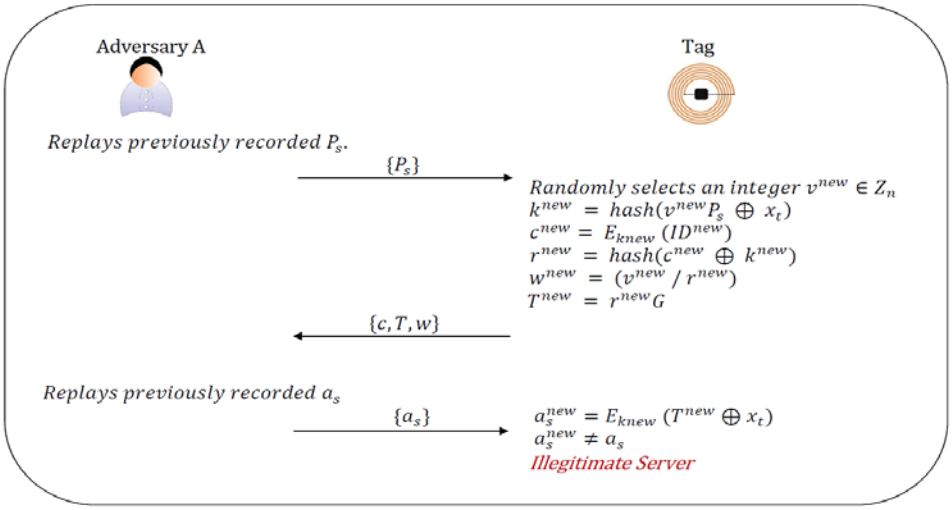

Fig. 6. Resistance against replay attack by the tag.

(3) Resistance against Location Tracking Attack

In our protocol, the messages transmitted between the tag and the server are protected such that an adversary cannot steal the tag id x_t. When the tag sends the message $\{c, T, w\}$ the adversary is unable to extract x_t from this, since it has to solve ECDHP which is computationally hard. Similarly, when the server sends the message $\{a_s\}$ to the tag the attacker cannot decrypt a_s since it is not in the possession of key k' which is privately generated by both the server and the tag. Moreover, private random numbers are used in generating the messages. Therefore, the attacker cannot obtain the location information, and the proposed protocol is secure against location tracking attack.

(4) Resistance against De-synchronization Attack

In the de-synchronization attack, the adversary prevents simultaneous updating of the secret information shared between the server and the tag. When an attacker performs de-synchronization attack and intercepts the messages, it is possible that the server doesn't update the entry of the tag while the tag does it [8]. To thwart de-synchronization attack the server stores both the previous tag pseudonym ID and the updated tag pseudonym ID^{new} in its database. When the adversary transmits the message $\{c, T, w\}$ to the server, the server decrypts the component c and identify that whether the decrypted value is previous tag pseudonym ID or it is the updated tag pseudonym ID^{new}. Moreover, since the proposed protocol provides the mutual authentication and data integrity, the de-synchronization of shared secret cannot be performed by the attacker.

(5) Resistance against DoS Attack

In the proposed protocol, there is no synchronous updating of secret key between the server and the tag. The only synchronous update is updating the tag pseudonym ID. It has already been revealed that the proposed protocol provides availability and can resist

de-synchronization attack in updating the tag pseudonym ID, thus it can withstand DoS attack.

(6) Resistance against Impersonation Attack

An adversary eavesdropping the channel may try to impersonate to be a legitimate tag or server after reading the messages sent between the server and the tag.

(i) In the server impersonating attack, which is also called server spoofing attack, an adversary tries to mimic the behaviour of the server to the tag. In doing this, the $Adversary\ A$ first selects a random number v_a and computes $P_a = v_a G$, then it sends $\{P_a\}$ to the tag. The tag then transmits the message $\{c, T, w\}$ to the $Adversary\ A$. After receiving $\{c, T, w\}$ $Adversary\ A$ cannot generate the key k' correctly and in turn it is not able to generate the message $\{a_s\}$ such that a_s is same as a_s' produced by the tag. Since $a_s \neq a_s{}'$ the tag terminates the session. So, the $Adversary\ A$ fails to mimic the behaviour of the server to the tag and thus our protocol is safe against server impersonating attack. Resistance against server impersonation has been demonstrated in **Fig. 7**.

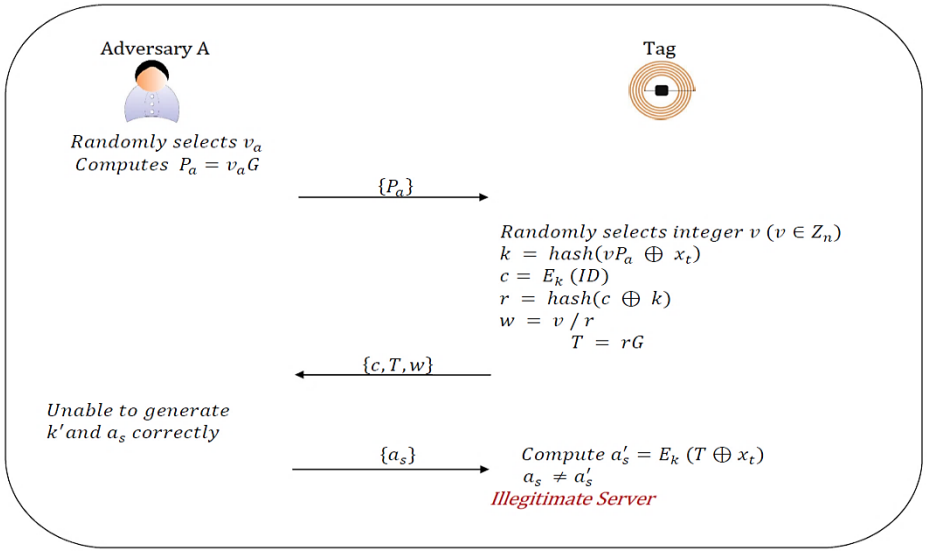

Fig. 7. Resistance against server impersonation attack.

(ii) An attacker may also try to mimic the behaviour of the tag to the server, this kind of impersonation is also known as tag masquerade attack. When the server sends the message $\{P_s\}$ to the $Adversary\ A$, the adversary should create and send the message $\{c, T, w\}$ to the tag. Since the $Adversary\ A$ cannot obtain ID and x_t, it is unable to generate the message $\{c, T, w\}$ correctly. At the server side, when the server decrypts the component c to retrieve ID, it cannot find a matching record in the database and terminates the session. Even if the $Adversary\ A$ uses the ID of the previous session then also it cannot impersonate the server as the protocol is resistant from replay attack. Resistance against tag impersonation has been shown in **Fig. 8**.

(7) Resistance against Man In The Middle (MITM) Attack

In MITM attack, an adversary sits between the tag and the server, and modifies the messages sent from the server to the tag and from the tag to the server, to make tag and server believe that they are communicating with the legitimate party [15]. As discussed in section 6.2 that the proposed protocol is resistant against tag impersonation and server impersonation, hence the proposed protocol can also counter MITM attack.

(8) Resistance against Key Compromise Attack

In a key compromise attack, an attacker somehow obtains the private key of a party and then

impersonate the corrupted party to the other legitimate parties [34]. In the proposed RFID protocol the private keys v and v_s are generated at random by both the tag and the server respectively which are then used in the dynamic generation of the shared key. Even if the attacker somehow knows the long term private key of the tag or the server, it cannot generate the shared secret key correctly since it needs to obtain x_t which is kept secret.

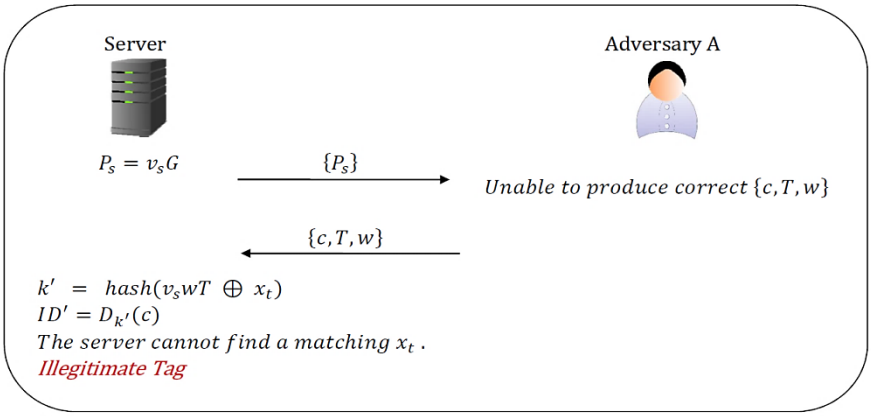

Fig. 8. Resistance against tag impersonation attack.

7. Performance Analysis

In this section, the performance of the proposed RFID security protocol has been analyzed by measuring computational overhead, communication cost, and storage cost taken by the protocol. Moreover, a comparison of security functionalities and the costs have been made in this section to prove that the proposed protocol is efficient than the other schemes mentioned in [8, 18, 22, 23, 26, 37, 38]. It has been assumed that 160 bit ECC has been used and the tag memory is 504 bytes for all the protocols. The proposed protocol uses the SHA-1 algorithm for generating the hash code, and AES-128 algorithm for encryption and decryption.

7.1 Analysis of Computational Cost

The computational time of a security protocol depends upon the time taken by different operations executed by the protocol. The computational time of ECC based RFID protocols is proportional to the number of elliptic curve scalar multiplication (ECSM) operation executed since it is the most complicated and time-consuming operation. The time consumed by other operations is very small in comparison to ECSM operation and therefore can be ignored. It takes 0.064 sec on a 5 MHz tag to compute a single ECSM operation [13]. In the proposed signcryption based RFID protocol three ECSM operations are performed by the server and two ECSM operations are performed by the tag. So, the time consumed by the tag is 0.128 sec, the time taken by the server is 0.192 sec, and the total time taken by the proposed protocol is 0.32 sec. Comparison of computational costs of related protocols have been made and shown in **Table 3**. A graphical representation of the computational time of these protocols has been shown in **Fig. 9(a)**. From **Table 3** and **Fig. 9(a)** it has been revealed that the computational cost of the proposed elliptic curve signcryption based protocol is less than that of the other elliptic curve based protocols.

7.2 Analysis of Communication Cost

Communication cost can be calculated by computing the size of messages exchanged between the tag and the server during the execution of the protocol. In the proposed protocol, three messages $\{P_s\}$, $\{c, T, w\}$, and $\{a_s\}$ are transmitted. Since 160 bit ECC has been used, the size of each elliptic curve point (x, y) is 320 bits. Assuming that 128-bit AES with the 128-bit key has been used for encryption which generates the 128-bit ciphertext. The communication cost of the proposed protocol is computed as:
Tag's communication cost = 256+320+160= 736 (bits)
Server's communication cost = 320+256= 576 (bits)
Total communication cost of the proposed protocol = 1312 (bits)
A comparison of the communication costs of the related protocols has been shown in **Table 4**. **Fig. 9(b)** shows the graphical analysis of the comparison of the communication cost of different RFID protocols.

Table 3. Computational costs of different protocols.

Protocol	Computational cost					
	No. of Elliptic Curve scalar Multiplications			Computational Time (sec)		
	Tag	Server	Total	Tag	Server	Total
Dinarvand [8]	3	3	6	0.192	0.192	0.384
Almar [18]	4	5	9	0.256	0.320	0.576
Liao [22]	5	5	10	0.320	0.320	0.640
Zhao [23]	5	5	10	0.320	0.320	0.640
Zhang [26]	4	2	6	0.256	0.128	0.384
Jin [37]	4	3	7	0.256	0.192	0.448
Zheng [38]	3	4	7	0.192	0.256	0.448
Proposed Protocol	***2***	***3***	***5***	***0.128***	***0.192***	***0.320***

Table 4. Commmunication costs and storage cost of different protocols.

Protocol	Communication cost (bits)			Storage cost (bits)		
	Tag	Server	Total	Tag	Server	Total
Dinarvand [8]	800	640	1440	1920	1120+800m	3040+800m
Almar [18]	640	960	1600	1920	1120+320m	3040+320m
Liao [22]	640	640	1280	1920	1280+800m	3200+800m
Zhao [23]	640	640	1280	1760	1120+480m	2880+480m
Zhang [26]	960	160	1120	1600	1440+480m	2040+480m
Jin [37]	640	640	1280	1600	1120+320m	2720+320m
Zheng [38]	640	640	1280	2080	1760+320m	3840+320m
Proposed Protocol	***736***	***576***	***1312***	***1760***	***1120+640m***	***2880+640m***

7.3 Analysis of Storage Cost

The storage cost indicates the amount of memory space required to store the information on the server and the tag. Although it has been assumed that the tag has limited memory space and the server has the capability of storing a large amount of data in its memory, but the server has to store the data for m number of tags belonging to the system. Therefore, analysis of the storage cost of both the server and the tag has been performed in this sub-section. In the proposed security protocol the tag is required to store system parameters $\{q, A, B, G, n\}$, the public key P_s of the server, tag's unique id x_t and the unique pseudonym of the tag ID. Based on the assumptions the storage cost of the tag is calculated as:

160+160+160+320+160+320+320+160 = 1760 (bits). For the server, it is assumed that there is m number of tags in the system. The server is required to store system parameters $\{q, A, B, G, n\}$, the private key of the server v_s, tag id x_t, the unique pseudonym of the tag ID and ID^{new}. The storage space required by the server can be calculated as: 160+160+160+320+160+160+320m+160m+160m = 1120+640m (bits). Comparison of storage cost consumed by different RFID security protocols has been publicized in **Table 4**. Assuming the value of m=10, a graphical representation of this comparison is shown in **Fig. 9(c)**.

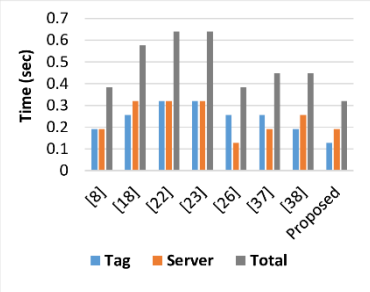

Fig. 9(a). Comparison of computational costs.

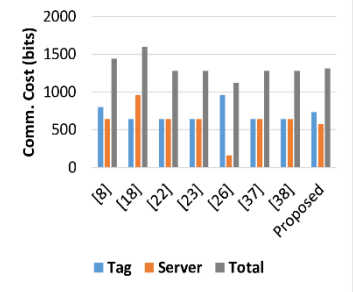

Fig. 9(b). Comparison of communication costs.

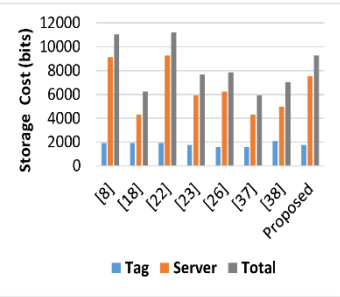

Fig. 9(c). Comparison of storage costs.

7.4 Comparison of Security Functionalities

As mentioned in section 6 of this paper, the proposed signcryption based security protocol provides confidentiality, mutual authentication, integrity, forward security, availability, non-repudiation, anonymity, and scalability which are the necessary security attributes for an RFID system. At the same time, the protocol has the capability to resist replay attack, cloning attack, location tracking attack, de-synchronization attack, denial of service attack, impersonation attack, man-in-the-middle attack, and key compromise attack. The security functionalities of the proposed protocol have been compared with other related protocols and presented in **Table 5**. By analyzing **Table 5**, it has been revealed that the proposed protocol provides all the necessary security attributes, at the same time successfully resisting the security attacks made on an RFID system.

Table 5. Comparison of security functionalities of different protocols

Protocol	Security attributes									Resistance against attacks								
	CO	MU	IN	NR	FW	AV	AN	SC	LO	MI	RP	IM	KE	LC	DO	CL	SS	DE
Dinarvand [8]	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Almar [18]	✓	✓	×	✓	✓	×	✓	×	✓	✓	✓	✓	✓	✓	×	✓	✓	×
Shen [21]	✓	✓	✓	✓	✓	×	✓	×	✓	✓	✓	✓	×	✓	×	×	✓	×
Liao [22]	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	×	×	✓	✓	✓	✓	✓
Zhao [23]	✓	✓	×	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Lee [25]	✓	×	✓	✓	✓	✓	✓	×	✓	✓	✓	✓		✓	×	×	✓	×
Zhang [26]	✓	×	✓	✓	✓	✓	✓	×	✓	✓	✓	✓	✓	✓	×	✓	×	×
Mehmood [28]	✓	✓	✓	✓	✓	×	✓	×	×	✓	✓	✓	✓	×	✓	×	✓	×
Jin [37]	✓	✓	×	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Zheng [38]	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Proposed Protocol	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓

CO-Confidentiality, MU-Mutual authentication, IN-Data integrity, NR-Non Repudiation, FW-Forward security, AV-Availability, AN-Anonymity, SC-Scalability, LO-Location privacy, MI-Man in the middle attack, RP-Replay attack, IM-Impersonation attack, KE-Key compromise attack, LC-location tracking attack, DO-Denial of service attack, CL-Cloning attack, SS-Server spoofing attack, DE-De-synchronization attack. ✓-Security functionality satisfied, × - Security functionality not satisfied.

8. Discussion

This section presents a brief discussion of the results and comparisons made in section 7. The proposed elliptic curve signcryption based protocol has been compared on the basis of computational cost, communication cost, storage cost, and security functionalities with the protocols mentioned in [8, 18, 22, 23, 26, 37, 38]. As depicted from Table 5, the protocols in [18, 22, 23, 26, 37] fail to provide some set of security functionalities and are not found suitable for an RFID system. The proposed protocol and the protocols mentioned in [8, 38] are the only protocols which provide all the necessary security functionalities. From Table 3 and Table 4 it has been realized that both the computational cost and storage cost for the tag in the proposed protocol is less than that of Dinarvand and Barati [8] and Zheng et al. [38]. Furthermore, the tag's computational cost in the proposed protocol is least in all the protocols mentioned in Table 3, which makes it attractive to be used for RFID systems. The tag's communication costs in the proposed protocol is less than Dinarvand and Barati's protocol [8] but more than Zheng et al.'s protocol [38]. Moreover, in the proposed protocol the unique tag pseudonym ID is encrypted and then send through the channel, making the protocol more secure. Since the proposed protocol provides all the necessary security functionalities at the same time taking less computational cost and storage cost for the tag, it is ideal for securing an RFID system.

9. Conclusion

RFID has become very prominent technology due to its advantages of increased speed and less cost than the other comparative techniques. Due to the less computational capability, implementing security and privacy is a big issue for RFID systems. Earlier, elliptic curve protocols have been proposed by the researchers, but in the proposed work signcryption based on the elliptic curve has been utilized to reduce the computational cost, especially for the tag. In the proposed work an elliptic curve signcryption based security protocol has been presented which takes less computational cost and storage cost as compared to other protocols. In addition, the protocol provides all the necessary security functionalities including security attributes and resistance from the attacks on RFID system, as discussed section 6 of the paper. The proposed protocol has been compared with seven other recent ECC based protocols with respect to computational time, communication cost, storage cost, and security functions they provide. The results show that the proposed protocol has low computational overhead, low storage cost for the tag, and provides higher security levels than the other similar protocols. Recent research references have been used in this paper to present the work more effectively before the readers. The proofs, results, and facts presented in this paper are of great importance for the academicians and researchers working in the area of security of RFID.

References

[1] R. Want, "An Introduction to RFID Technology," *IEEE Pervasive Computing*, vol. 5, no. 1, pp. 25-33, 2006. Article (CrossRef Link)

[2] X. Jia, Q. Feng, T. Fan, and Q. Lei, "RFID Technology and its Applications in Internet of Things (IoT)," in *Proc. of 2nd International Conference on Consumer Electronics, Communications and Networks (CECNet)*, pp. 1282-1285, 2012. Article (CrossRef Link)

[3] A. Khattab, Z. Jeddi, E. Amini, and M. Bayoumi, "Introduction to RFID," *Md. Ismail, Md. Sawan (ed.), RFID Security. Analog Circuits and Signal Processing, Springer, AG*, pp. 3-26, 2016. Article (CrossRef Link)

[4] J. Yu and L. Chen, "Introduction," *Tag Counting and Monitoring in Large-Scale RFID Systems, Theoretical Foundations and Algorithm Design, Springer AG*, pp 1-6, 2018. Article (CrossRef Link)

[5] F. Chetouane, "An Overview on RFID Technology Instruction and Application," *IFAC-Papers on- line*, vol. 48, no. 3, pp. 382-387, 2015. Article (CrossRef Link)

[6] C.C. Tan and J. Wu, "Security in RFID Networks and Communications," *L. Chen, J. Ji, Z. Zhang (ed.), Wireless Network Security, Springer, Berlin*, pp. 247-267, 2013. Article (CrossRef Link)

[7] H. Knospe and H. Pohl, "RFID Security," *Information Security Technical Report*, vol. 9, no.4, pp.39-50, 2004. Article (CrossRef Link)

[8] N. Dinarvand and H. Barati, "An Efficient and Secure RFID Authentication Protocol using Elliptic Curve Cryptography," *Wireless Networks*, vol. 25, no. 1, pp. 415-428, 2019. Article (CrossRef Link)

[9] S. Guizani, "Security Applications Challenges of RFID Technology and Possible Countermeasures," in *Proc. of International Conference on Computing, Management and Telecommunications (ComManTel)*, pp. 291-297, 2014. Article (CrossRef Link)

[10] N. Kannouf, Y. Douzi, M. Benabdellah, and A. Azizi, "Security on RFID technology," in *Proc. of International Conference on Cloud Technologies and Applications*, pp. 1-5, 2015. Article (CrossRef Link)

[11] A. Khattab, Z. Jeddi, E. Amini, and M. Bayoum, "RFID Security Threats and Basic Solutions," in *Md. Ismail, Md. Sawan (ed.), RFID Security. Analog Circuits and Signal Processing, Springer, AG*, pp. 27-41, 2017. Article (CrossRef Link)

[12] Z. Cao and L. Liu, "On the Disadvantages of Pairing-Based Cryptography," *IACR Cryptology ePrint Archive*, vol. 2015, pp. 84, 2015. Article (CrossRef Link)

[13] G. Gódor, N. Giczi, and S. Imre, "Elliptic Curve Cryptography Based Mutual Authentication Protocol for Low Computational Capacity RFID Systems - Performance Analysis by Simulations," in *Proc. of IEEE International Conference on Wireless Communications, Networking and Information Security*, pp. 650-657, 2010. Article (CrossRef Link)

[14] Y. Liu, X. Qin, and C. Wang, "A Lightweight RFID Authentication Protocol Based on Elliptic Curve Cryptography," *The Journal of Supercomputing*, vol. 8, no. 11, pp. 2880–2887, 2013.

[15] J. Chou, "An Efficient Mutual Authentication RFID Scheme Based on Elliptic Curve Cryptography," *The Journal of Supercomputing*, vol. 70, no. 1, pp. 75–94, 2014. Article (CrossRef Link)

[16] M.S. Farash, "Cryptanalysis and Improvement of an Efficient Mutual Authentication RFID Scheme Based on Elliptic Curve Cryptography," *The Journal of Supercomputing*, vol. 70, no. 1, pp. 987–1001, 2014. Article (CrossRef Link)

[17] L. Feng and X. Yao, "RFID System Mutual Authentication Protocols Based on ECC," in *Proc. of IEEE 12th International Conference on Ubiquitous Intelligence and Computing and IEEE 12th International Conference on Autonomic and Trusted Computing and 2015 IEEE 15th International Conference on Scalable Computing and Communications and Its Associated Workshops (UIC-ATC-ScalCom)*, pp. 1644-1649, 2015. Article (CrossRef Link)

[18] A. A. Alamr, F. Kausar and J. S. Kim, "Secure Mutual Authentication Protocol for RFID Based on Elliptic Curve Cryptography," in *Proc. of International Conference on Platform Technology and Service (PlatCon)*, pp. 1-7, 2016. Article (CrossRef Link)
[19] Q. Qian, Y. L. Jia and R. Zhang, "A Lightweight RFID Security Protocol Based on Elliptic Curve Crytography," *International Journal of Network Security*, vol. 18, no. 2, pp. 354–361, 2016. Article (CrossRef Link)
[20] Y. Chen and J. S. Chou, "ECC-Based Untraceable Authentication for Large-Scale Active-Tag RFID Systems," *Electronic Commerce Research*, vol. 15, no. 1, pp. 97-120, 2015. Article (CrossRef Link)
[21] H. Shen, J. Shen, M. K. Khan, and J.H. Lee, "Efficient RFID Authentication Using Elliptic Curve Cryptography for the Internet of Things," *Wireless Personal Communications*, vol. 96, no. 4, pp. 5253–5266, 2017. Article (CrossRef Link)
[22] Y.P. Liao and C.M. Hsiao, "A Secure ECC-Based RFID Authentication Scheme Using Hybrid Protocols," in *J.S. Pan, C.N. Yang, C.C. Lin (ed.) Advances in Intelligent Systems and Applications - Volume 2. Smart Innovation, Systems and Technologies, Springer*, vol. 21, pp. 1-13, 2013. Article (CrossRef Link)
[23] Z. Zhao, "A Secure RFID Authentication Protocol for Healthcare Environments using Elliptic Curve Cryptosystem," *Journal of Medical Systems*, vol. 38, no. 5, pp. 1-7, 2014. Article (CrossRef Link)
[24] 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," *Journal of Medical Systems*, vol. 40, no. 7:165, pp. 1-7, 2016. Article (CrossRef Link)
[25] Y.K. Lee, L. Batina, B. Preneel, and I. Verbauwhede, "Anti-counterfeiting, Untraceability and Other Security Challenges for RFID Systems: Public-Key-Based Protocols and Hardware," *A.R. Sadeghi, D. Naccache (ed.), Towards Hardware Intrinsic Security, Springer*, pp. 237-257, 2010. Article (CrossRef Link)
[26] 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 Ccryptography," *Multimedia Tools and Applications*, vol. 74, no. 10, pp. 3477-3488, 2014. Article (CrossRef Link)
[27] Y. Lu, L. Li, H. Peng, and Y. Yang, "A Secure and Efficient Mutual Authentication Scheme for Session Initiation Protocol," *Peer-to-Peer Networking and Applications*, vol. 9, pp. 449-459, 2016. Article (CrossRef Link)
[28] Z. Mehmood, G. Chen G, 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, pp. 1-17, 2017. Article (CrossRef Link)
[29] Y. Zheng, "Digital Signcryption or How to Achieve Cost(Signature & Encryption) ≪ Cost(Signature) + Cost(Encryption)," *Kaliski B.S. (eds) Advances in Cryptology —CRYPTO 1997, Lecture Notes in Computer Science, Springer*, vol. 1294, pp. 165-179, 1997. Article (CrossRef Link)
[30] Y. Zheng and H. Imai, "How to Construct Efficient Signcryption Schemes on Elliptic Curves," *Information Processing Letters*, vol. 68, no. 5, pp. 227 – 233, 1998. Article (CrossRef Link)
[31] K.E. Lauter, and K.E. Stange, "The Elliptic Curve Discrete Logarithm Problem and Equivalent Hard Problems for Elliptic Divisibility Sequences," *Selected Areas in Cryptography, Springer*, pp. 309-327, 2009. Article (CrossRef Link)
[32] I. Shparlinski, "Computational Diffie-Hellman Problem," *Van Tilborg H.C.A., Jajodia S. (eds) Encyclopedia of Cryptography and Security, Springer*, 2011. Article (CrossRef Link)
[33] D. Boneh, "The Decision Diffie-Hellman problem," *Buhler J.P. (eds) Algorithmic Number Theory, ANTS. Lecture Notes in Computer Science, Springer*, vol. 1423, pp. 48-63, 1998. Article (CrossRef Link)
[34] K. Chalkias, F. Baldimtsi, D. Hristu-Varsakelis and G. Stephanides, "Two Types of Key-Compromise Impersonation Attacks against One-Pass Key Establishment Protocols," *J. Filipe, M.S. Obaidat (eds) E-business and Telecommunications, ICETE 2007, Communications in Computer and Information Science, Springer*, vol. 23, pp. 227-238, 2008. Article (CrossRef Link)

[35] K. Ouafi and R.C.W, Phan, "Traceable Privacy of Recent Provably-Secure RFID Protocols," in *Proc. of International conference on applied cryptography and network security*, pp. 479–489, 2008. Article (CrossRef Link)
[36] J. Katz, *The Random Oracle Model*, Digital Signatures, Springer, 2010. Article (CrossRef Link)
[37] C. Jin, C. Xu, X. Zhang and F. Li, "A Secure ECC-based RFID Mutual Authentication Protocol to Enhance Patient Medication Safety," *Journal of Medical Systems*, vol. 40, no. 1, pp. 1-6, 2015. Article (CrossRef Link)
[38] L. Zheng, Y. Xue, L. Zhang and R. Zhang, "Mutual Authentication Protocol for RFID based on ECC," in *Proc. of IEEE International Conference on Computational Science and Engineering (CSE) and IEEE International Conference on Embedded and Ubiquitous Computing (EUC)*, pp. 320–323, 2017. Article (CrossRef Link)
[39] S.Y. Chiou, W. T. Ko, and E. H. Lu, "A Secure ECC-based Mobile RFID Mutual Authentication Protocol and Its Application," *International Journal of Network Security*, vol.20, no.2, pp. 396-402, 2018. Article (CrossRef Link)
[40] K. Fan, W. Jiang, H. Li, and Y. Yang, "Lightweight RFID Protocol for Medical Privacy Protection in IoT," *IEEE Transactions on Industrial Informatics*, vol. 14, no. 4, pp. 1656-1665, 2018. Article (CrossRef Link)
[41] S. F. Aghili, H. Mala, "Security analysis of an ultra-lightweight RFID authentication protocol for m-commerce," *International Journal of Communication Systems*, vol. 32, no. 3, pp. 1-12, 2019. Article (CrossRef Link)
[42] G. Liu, H. Zhang, F. Kong, L. Zhang, "A Novel Authentication Management RFID Protocol Based on Elliptic Curve Cryptography," *Wireless Personal Communications*, vol. 101, no. 3, pp. 1445-1455, 2018. Article (CrossRef Link)

Anuj Kumar Singh is pursuing Ph.D in Computer Science and Engineering from Dr. A.P.J. Abdul Kalam Technical University, Lucknow (India). He is also working as Assistant Professor in Department of Computer Science & Engineering at Amity University Haryana, Gurgaon (India). He passed M.Tech degree with Honours from Panjab University, Chandigarh. He has more than 14 years of teaching experience in technical education. He has published more than 20 research papers in journals and conferences.

Dr. B.D.K. Patro earned Ph.D degree in Computer Science from Institute of Computer and Information Sciences, Dr.B.R.Ambedkar University, Agra (Indis). He is an Associate Professor of Computer Science & Engineering in Rajkiya Engineeirng College, Kannauj (India). He has more than 24 years of experience to teach the undergraduate and postgraduate courses. He has guided 02 Ph.d, guiding 03 Ph.d candidates, supervised 12 M.Tech theis and many Undergraduate projects. He has published more than 30 research papers in journals and conferences.