Palestine Journal of Mathematics

Vol 14(2)(2025) , 456–466

An Efficient Pairing Free Certificateless Digital Signature Scheme based on Elliptic Curve

Deepika Gautam, Sunil Prajapat, Pankaj Kumar and Manoj Kumar Patel

Communicated by Manoj Patel

MSC 2020 Classifications: Primary 33C20; Secondary 33C65.

Keywords and phrases: Elliptic Curve, Certificateless Signature Scheme, Digital Signature, Identity Based Signature Scheme, Discrete Logarithm Problem.

Abstract: With the escalating universality of smartphones, smart homes, and internet services, it has become pivotal to resolve the privacy and security snags of the modern era. Composed with the advantages of digital signature, certificateless cryptographic primitive seems to be the feasible cryptographic tool for the arising issues and is considered a fundamental building block. Certificateless cryptography has obliterated the prerequisite for certificates and the key escrow dilemmas. Certificateless cryptography is an amalgamation of the Identity based and the public key cryptographic primitive. In this paper, we have proposed a pairing-free certificateless signature scheme on the premise of elliptic curve cryptography. Most existing schemes are either based on bilinear pairing operations or the map to point hash functions. Lamentably, these schemes have excessive computational expenses and are more time-consuming than the elliptic curve scalar point multiplication. The proposed scheme does not employ any of these operations and prominently cuts down the required computational cost and desirable time prerequisite, which formulates the scheme more efficiently. Also, the proposed scheme is to be secure under the existential forgery on adaptive chosen message and identity attack. Finally, after the performance analysis, the proposed scheme is found to be more secure and efficient than the existing scheme.

1 Introduction

In the recent epoch, the speedy evolution of wireless technology, such as smartphones, wearable devices, and smart roadway systems, has gained attention. This has not only facilitated the people to connect but also connected the object with the object and living with the object through information exchange, providing a better livelihood. Because of the exposure of the devices in public networks, security catastrophe to the contents of the communication has increased. Hence, dealing with threats like tempering, eavesdropping, and identity theft is crucial during the transmission of collective data. The digital signature is a cryptographic primitive for accomplishing integrity, nonrepudiation, and message authentication [5]. For the amalgamation of the individual with digital data, a digital signature is an approach that can be corroborated via a third party other than the receiver himself. Both digital signature and public-key cryptography (PKC) together are regarded as valuable and essential tools for achieving information security. In PKC, there is a duo of keys (public and private keys) for every distinct user; the public key is available on the public channel, while the private key is kept secret. PKC involves a trusted third party for binding the public key and the user corresponding to Identity, titled public key infrastructure (PKI). The Certificate Authority in PKI is accountable for distributing, stowing, and issuing certificates. Certificates in PKI links the public key and the entity's Identity together. Later, the problem of management, storage, and the revocation of the certificates in the PKC has arisen.

The inherited certificate supervision dilemma in the PKC was rectified when Shamir [8] projected a new cryptographic primitive termed as identity-based cryptography (ID-BC) in 2003. The entity's unique Id is conceded as the user's public key; on the other hand, the private key is reckoned by a trusted third party named as PKG (private key generator) in the PKC. The PKG reckons the private key using a master secret key of himself and the entity's unique ID, i.e., the entity's public key. ID-BC overcomes the need for the certificate; however, PKG can be malicious and easily falsify the entity's signature. This has given birth to a new problem termed the key escrow problem. After this, many schemes were proposed on the premise of the various signature primitives to solve the problem of the ID-BC, like threshold cryptography and group signature.

In 2006, Al-Riyami and Peterson were the first to broach the concept of certificateless cryptography (CLC) [1]. In the approach of CLC, a partial private key is required for the generation of the private key. and The duo of the key, i.e., private key plus public key, is generated by the user himself using his partial private key. A personage KGC is accountable for the computation and the secure transmission of the partial private key of the user through the open public channel to the user. Here, public keys are either made available in a public directory or the partial private key transmitted with ciphertext/signatures in a protected manner [9]. In this way, the weakness of the ID-BC and PKC are overcome concurrently. This made the CLC more efficient and the optimum unification of both ID-BC and the PKC. Hence, CLC is and can be regarded as a fundamental building block of cryptography [9].

1.1 Motivation and the contribution

Voluminous novel certificateless signature schemes have been proposed in the past years. Regrettably, some of these schemes are either found to be vulnerable to various attacks or have a high computational expanse, are time-consuming. Many schemes are formulated by taking bilinear pairing and the map-to-point hash functions as their premises. Later it was found that the map-to-point hash functions and the pairing are complex and have a very high computational expanse than the elliptic curve point multiplication. The Implementation of the elliptic curve operation is also less strenuous than the bilinear

pairing operation and map-to-point functions [14]. Some applications like smart cards, mobile phones, and wearable devices sometimes work on a low bandwidth environment, low storage, and computability, and desire for a short and efficient signature [13]. All these necessities made the pairing-free certificateless signature scheme the superlative alternative. Furthermore, the premise of the beforementioned, we have proposed a robust scheme based on elliptic curve cryptography and pairing-free certificateless cryptography. Our contributions are as follows:

(i) Using the elliptic curve cryptography, a certificateless signature scheme is presented. Also, as required, we have not employed the scheme's bilinear pairing and map-to-point hash functions. This approach offers improved efficiency while ensuring the desired level of security.

(ii) The scheme has been demonstrated secure over the random oracle model for the adaptive chosen message and identity attacks. This investigation proves the stability and dependability of our approach in real-world cryptographic situations.

(iii) The proposed work is also compared with the existing works and found to be more protected and efficient compared to these works. This assessment demonstrates the improved security and effectiveness of our method in comparison to earlier works, significantly advancing the field.

1.2 Outline of the paper

The remaining paper is systematized in the following way: Section 2 highlights a review of the existing novel works under the related work. Section 3 illuminates the complexity assumption and the elliptic curve cryptography; section 4 describes the system model of CLC and the security of the CLC. In section 5, a robust pairing-free certificateless signature scheme is proposed. Security proof of the proposed scheme for the attack model of CLC is portrayed in section 6. In section 7, the proposed scheme's performance evaluation with the various schemes has been presented. At last, we have a conclusion and future scope in section 8.

2 Related Work

The conception of PKC is first broached by Diffie and Hellman. Later many works were introduced, but it had a certificate management crisis. Shamir was the first to solve this problem efficiently in 1986 by portraying the concept of ID-BC [8]. This cryptosystem has been found with a new catastrophe, i.e., a key escrow problem. The certificate supervision and key escrow crises were solved concurrently by the certificateless cryptography work broached by Al-Riyami and Peterson in 2003 [1]. Nonetheless, Huang et al. [16] showed the evidence for the vulnerability of Al-Riyami and Peterson's work against the Type I adversary or public key replacement attack also projected an improved scheme. Following Al-Riyami and Peterson's work, numerous new works are presented. Yum and Lee were the first to come up with a generic CLS [12]. Regrettably, their work was found to be vulnerable to the key replacement attack by Hu et al. [15]. Huang et al. [3] categorized adversaries in their work into three categories, i.e., strong adversary, normal adversary, and super adversary, on the premise of their ability.

In 2015, for VANETs, Horng et al. [2] presented work on CLAS schemes utilizing conditional privacy preservation. They proved their work under the random oracle model was unforgeable for adaptive chosen message and identity attacks. On the other hand, Li et al. [7] provided that the work given by Horng et al. [2] is unresistant in opposition to malicious but passive KGC attacks. Kumar et al. [6] projected a new work on the CLAS scheme for healthcare wireless sensor networks. They affirmed that the scheme is insusceptible in antagonism to adaptive chosen messages and identity attacks under the random oracle model provided. However, their work is later disclosed to be susceptible in resistance to signature forgery attacks by Wu et al. [10]. He also proposed an enhanced scheme to resolve the weakness. Several researchers have done several works on the premise of pairing operations and map-to-point hash functions. As these schemes had high computational costs and time consumption, several schemes were proposed later without employing pairing and map-to-point operations.

He et al. [4] projected an efficient CLS scheme without using a pairing operation in 2011. Unfortunately, their work was observed to be vulnerable in opposition to strong Type 2 adversaries by Tsai et al. [17]. Using batch verification as their supported scheme, Kamil and Ogundoyin [5] brought the CLS without bilinear pairing for an ad hoc network in 2019. In their work, they have provided shreds of evidence of the vulnerability of the [18, 29, 30, 31, 32, 33, 34, 35] scheme. However, Zhao et al. [19] and Xin ye et al. [20] showed that their scheme could not oppose the forgery attack and coalition attack, respectively. They have also presented the improved vehicle ad hoc network scheme against the respective attacks. Yeh et al. [21] broached the scheme for IoT-Based Mobile Payments on the premise of elliptic curve cryptography. [22] demonstrated a compact certificateless signature scheme for the healthcare wireless network. However, [21] and [22] both are proved to be insecure by the Shim [9]. He has asserted the evidence that [21] is forgeable in opposition to Type I and Type II adversaries, while [22] is insecure against the universal forgery attack.

For VANETs, Ming and Cheng [23] projected a capable certificateless conditional privacy-preserving approach. They employed batch verification as a supported signature verification scheme and averred that their scheme was safe from security attacks. Thumbur et al. [24] have broached the pairing-free certificateless signature scheme for the VANET while using the aggregate as their supporting scheme for the environment. Recently, a secure and competent certificateless signature scheme has been provided by Xiang et al. [11] for the Internet of Things. They analyzed the Jia et al. [25] scheme and proved the vulnerability of their scheme in opposition to type II strong adversary.

3 Preliminaries

(i) *Elliptic curve cryptography (ECC):*
This technique is relied on the elliptic curves over finite fields and was brought to light via Neal Koblitz and Victor Miller in 1985. ECC gained prominence because of the suitable and short size of the signature and the public key compared to the others and is relevant for usage in real-life scenarios like VENET and FANET etc. Security of ECC is depend on the complexity of the elliptic curve discrete logarithm problem. Elliptic curves are useful to execute the cryptographic schemes and helpful to present its cluster arrangement.

A cubic non-singular curve, $E_q(s,t)$ is defined as the elliptic curve over the field Z_q is a set of the solutions $(s,t) \in Z_q \times Z_q$ (where q is the prime number) of the equation $t^2 = s^3 + cs + d$ and $4c^3 + 27d^2 \mod p \neq 0$ with a special point (∞), labelled as the point at infinity. Here t, s, c, d belongs to Z_q. The set $E = \{(s,t)|t^2 = s^3 + cs + d$, where s, t, c, d belongs to $K.\} \cup \{\infty\}$ under the addition operation forms an abelian group. Scalar point multiplication is reckoned as $\alpha P = P + P + ...P(\alpha$ times) over an elliptic curve. A point P is said to have an order n if for some positive integer n; $nP = \infty$.

(ii) *Elliptic curve discrete logarithm problem (ECDLP):* For a given generator P of group E_q and $Q = aP$ belonging to the group E_q such that $a \in Z_q$, the ECDLP is to determine an integer 'a' through the provided probabilistic polynomial time (PPT).

4 System Model and Scheme Framework

The system model of the CLS is formed by three entities, i.e., the key generation canter (KGC), the signer, and the verifier. KGC is the personage who is amenable to the spawning of the system parameters and the partial private key of the user; the signer is a personage who invokes the signature on the provided message, and the verifier is a personage who verifies the signature on the received message. The scheme framework of the CLS consists of six notches as limned underneath:

(i) Setup: KGC is accountable for operating this notch or the algorithm. Using the security parameter as input, KGC calibrates system parameters and his public key as well as master secret key as output. In this notch, system parameters are on the public channel as well the master secret key is stifled secret.

(ii) Partial key generation: After taking the ID of the individual as input for this notch, KGC calibrates the partial private key for the user and uses his private key plus the system parameters to calibrate it. As the output of this notch, the partial private key is handed out securely to the respective user by KGC.

(iii) Secret value generation: A random value is carefully chosen and is a stifled secret by the user. This notch is operated by the user ID himself.

(iv) Key generation: The user corresponding to ID is accountable for operating this notch or algorithm. The intake is the partial private key, and the secret values of this notch, which are used to calibrate the duo of the key for himself, i.e., his private plus public key as the output.

(v) Signature generation: For the given message, the user corresponding to the identity ID calibrates the signature using his private key, partial private key, secret value, and the system parameters as intakes for the notch.

(vi) Signature verification: After receiving the message with the signature and the system parameter as the input for this notch, the verifier or the receiver corroborates the validity of the signature. The verifier outputs the true if the signature is valid; otherwise, false.

4.1 Security model of CLS

The security model of the CLS relies on the ECDLP over the random oracle model. In CLS adaptive chosen message and identity attacks are considered powerful, so the security model of CLS is given in accordance with it. Our CLS attack model has mainly two types of attackers: Type I Adversary and Type II Adversary with different capabilities. Type I Adversary is an outsider attacker while Type II Adversary is an insider or the malicious KGC. Type I Adversary is a personage who has the authority to change the original public key with the new public key chosen by himself but has no access to the KGC's master secret key. On the other hand, Type II Adversary is the personage with the capabilities of getting access to the master secret key of the KGC but has no authority to change the original public key of the user.

The unforgeability against the adaptive chosen message and identity attack of the CLS scheme is shown by a challenge-response game played between the adversary and the challenger γ. There are two games defined on the premises of the different adversaries i.e., Game I and Game II respectively for the Type I Adversary and Type II Adversary. During this challenger and response game, some queries are requested by the adversary to the challenger. These queries are as depicted underneath:

(i) Hash Query: Adversary request for the hash value corresponding to any input and in respond challenger γ returns the hash value to the adversary.

(ii) Request (ID_i): Adversary can demand the public key corresponding to user ID_i, so he asks the Request (ID_i) query. Then in respond to this request γ grants the full public key to adversary.

(iii) Partial-Private-Key-Request-Query: With respect to user ID_i partial private key is demanded by the adversary from the γ (challenger) and in reply the partial private key is presented.

(iv) Secret-Value-Request-Query: With respect to ID_i, secret value is asked by the adversary and in respond γ (challenger) outputs the secret value.

(v) Public-Key- Replacement-Request-Query: Substitution of the previous public key by the new public key, selected by the adversary on his own, requested by the adversary. In reply the γ (challenger) swap the existing public key with new public key associated to user ID_i.

(vi) Signature-Request-Query: Corresponding to selected message m_i the adversary asks for the signature for signer's identity ID_i,. In response, the γ (challenger) generate the signature and produce the pair of messages–signature to adversary.

CLS security model defines the two games as depicted below:

(i) **Game I** In this game, γ (challenger) and super Type I adversary A_1 interact with each other and play the game for the presented scheme.

- Stage-1 (Setup): The Setup step is carried off by the γ (challenger) and computes the system parameters and the secret master key (msk) of his own. His msk is kept secret him but outputs the system parameters to adversary A_1.

- Stage-2 (Queries): Adversary A_1 request for the Hash-query, Request (ID_i) Query, Partial-Private-Key-Request-Query, Secret-Value-Request-Query, Public-Key-Replacement-Request-Query and Signature-Request-Query from the γ (challenger).
- Stage-3 (Forgery): In the last stage forgery, forged pair of message and signature is presented by the adversary A_1 on the m_i (message).

Conditions to win the game:

a. If corresponding to user ID_i, the forged signature is valid for message m_i.
b. In the midst of game with respect to identity ID_i, the m_i (message) has not at all been put forward in front of Request Signature oracle.
c. To Secret-Value-Request-Query along with the oracle Partial-Private-Key-Request-Query, the identity ID_i has never been proposed.

(ii) **Game II** In this game, γ (challenger) and super Type 2 adversary A_2 interact with each other and play the game for the presented scheme.

- Stage-1 (Setup): The Setup step is carried off by the γ (challenger) and γ computes the system or public parameters and the secret master key (msk) of his own. He outputs the system or public parameters and the msk (master secret key) to adversary A_2.
- Stage-2 (Queries): Adversary A_2 request for the Hash-Query, Request ID_i Query, Partial-Private-Key-Request-Query, Secret-Value-Request-Query, and Signature-Request-Queries from the γ (challenger).
- Stage-3 (Forgery): In the last stage forgery, forged pair of message and signature is presented by the adversary A_2 on the m_i (message).

Conditions to win the game:

a. If corresponding to user ID_i, the forged signature is valid for message m_i.
b. In the midst of game corresponding to identity ID_i, the m_i (message) has not at all been put forward in front of Request Signature oracle.
c. To Secret Value Request Queries along with the oracle Public-Key-Replacement-Request-Query, the identity ID_i has never been proposed.

Definition 4.1. If there are no polynomial bound time adversary A_1 and A_2 who can succeed Game I and II respectively, a CLS scheme with a non-negligible gain is probably safe and sound.

5 Our Proposed Certificateless Scheme

5.1 Setup

(i) Upon taking k as security parameter and a prime number q of k-bit and generate the generator P of additive cyclic group G.
(ii) KGC randomly picks $s \in Z_q^*$ as his msk (master secret key) and output the $P_{pub} = sP$ as his public key.
(iii) KGC go for the hash functions $H_1 : 0,1^* \to Z_q^*$, $H_2 : 0,1^* \to Z_q^*$, $H_3 : 0,1^* \to Z_q^*$.
(iv) Outputs the public parameters $\varphi = \{F(q), G, P, P_{pub}, H_1, H_2, H_3\}$

5.2 Partial key generation

For the user ID_i , KGC does as follow:

(i) Select $t_i \in Z_q^*$, and compute $T_i = t_i P$ and $h_1 = H_1(ID_i, P_{pub}, T_i)$.
(ii) Calculate $S_i = t_i + h_1 s \mod q$.

Partial key for the user is given by $D_i = (T_i, S_i))$.

5.3 Secret value generation

(i) User ID_i opt a random number $x_i \in Z_q^*$ and kept it secret.

5.4 Key generation

(i) Using the partial key D_i and the secret value x_i user ID_i compute his private key pair $p_i = (S_i, x_i)$.This pair is kept secret by the user.
(ii) User ID_i, compute $X_i = x_i P$ and output his public key pair PK_i as $PK_i = (T_i, X_i)$.

5.5 Signature generation

Corresponding to the message $m_i \in \{0,1\}^*$, user ID_i calculates the signature as shown below:

(i) Select $r_i \in Z_q^*$ and evaluate $R_i = r_i P$.
(ii) Determine $h_2 = H_2(ID_i, PK_i, R_i, m_i)$, $h_3 = H_3(ID_i, PK_i, T_i, m_i)$.
(iii) Compute $\rho_i = S_i + h_2(r_i + h_3 x_i)$.

Output the signature on the message $m_i \in \{0,1\}^*$ as $\mu = (\rho_i, R_i)$ pair.

5.6 Signature verification

Authenticity of the signature μ is verified by the verifier is the following equation

$$\rho_i P = T_i + h_1 P_{pub} + h_2(R_i + h_3 X_i).$$

If the equation above holds the signature on $m_i \in 0, 1^*$ is valid, otherwise not.

5.7 Correctness

This validates the relationship of signature, public key of the signer and the original message and determine the validity and accuracy of the generated signature.

$$\begin{aligned}
\rho_i P &= \{[S_i + h_2(r_i + h_3 x_i)]P\} \\
\rho_i P &= [S_i P + h_2(r_i P + h_3 x_i P)] \\
\rho_i P &= [(t_i + h_1 s)P + h_2(r_i P + h_3 x_i P)] \\
\rho_i P &= [(t_i P + h_1 s P) + h_2(r_i P + h_3 x_i P)] \\
\rho_i P &= [(T_i + h_1 P_{pub}) + h_2(R_i + h_3 X_i)] \\
\rho_i P &= T_i + h_1 P_{pub} + h_2(R_i + h_3 X_i).
\end{aligned}$$

6 Security Proof

Theorem 6.1. *Under the ECDL assumption, the proposed CLS scheme is unforgeable in opposition of Type I Adversary A_1 in random oracle model.*

Proof. In the proposed CLS scheme, for the adversary A_1, who can break the scheme in time t with ϵ probability, there exist an algorithm γ that can solve the ECDLP $(P, Q = sP)$ for s with non-negligible probability. In this game γ act as challenger and interact with the A_1, as depicted below:

- Setup: The challenger γ picks a random number $s \in Z_q^*$ as a master secret key for KGC and set $P_{pub} = sP$ as the public key of the KGC. The challenger γ publishes the public parameters $\varphi = \{F_q, G, P, P_{pub}, H_1, H_2, H_3\}$. For the consistency and the quick response, γ maintains some lists as below:
  - (i) $L_{H_1}^{List}$: The list contains the tuples $(ID_K, P_{pub}, T_K, l_1)$.
  - (ii) $L_{H_2}^{List}$: The list contains the tuples $(ID_K, PK_K, R_K, m_K, l_2)$.
  - (iii) $L_{H_3}^{List}$: The list contains the tuples $(ID_K, PK_K, T_K, X_K, m_K, l_3)$.
  - (iv) L_C^{List}: The list contains the tuples (ID_K, PK_K, D_K, x_K).
- H_1 query: When A_1 ask a H_1 query on ID_K the challenger γ checks for the $L_{H_1}^{List}$, if the tuple $(ID_K, P_{pub}, T_K, l_1)$ is found then sends the l_1 to the adversary. Otherwise, γ selects the random value $l_1 \in Z_q^*$ and update to it list $L_{H_1}^{List}$ and send the l_1 in the response of the query to the A_1.
- H_2 query: When A_1 ask a H_2 query on ID_K the challenger γ checks for the $L_{H_2}^{List}$, if the tuple $(ID_K, PK_K, R_K, m_K, l_2)$ is found then sends the l_2 to the adversary. Otherwise, γ selects the random value $l_2 \in Z_q^*$ and update it to list $L_{H_2}^{List}$ and send the l_2 in the response of the query to the A_1.
- H_3 query: When A_1 ask a H_3 query on ID_K the challenger γ checks for the $L_{H_3}^{List}$, if the tuple $(ID_K, PK_K, T_K, X_K, m_K, l_3)$ is found then sends the l_3 to the adversary. Otherwise, γ selects the random value $l_3 \in Z_q^*$ and update it to list $L_{H_3}^{List}$ and send the l_3 in the response of the query to the A_1.
- Request ID_K : Upon receiving the Request ID_K query, γ then selects the numbers $a_K, b_K, x_K \in Z_q^*$ and sets $T_K \leftarrow a_K.P - b_K P_{pub}$, $S_K \leftarrow a_K, h_1 \leftarrow b_K$ and computes the $X_K = x_K.P$. Now γ does as follows:
  - (i) If $ID_K \neq ID^*$, then γ outputs $D_K = (T_K, S_K)$, private key $P_K = (S_K, x_K)$ and the public key $PK_K = (T_K, X_K)$. Finally, γ, updates the tuples (ID_K, PK_K, D_K, x_K) to list L_C^{List} and $(ID_K, P_{pub}, T_K, l_1)$ to list $L_{H_1}^{List}$.
  - (ii) If $ID_K = ID^*$, then γ outputs $D_K = (T_K, \perp)$, private key $P_K = (\perp, x_K)$ and the public key $PK_K = (T_K, X_K)$. In response to this query sends the public key $PK_K = (T_K, X_K)$ to the adversary.
- Partial Private Key Request Query: Adversary A_1 ask for the Partial Private Key Query, then γ responds as follows:
  - (i) If $ID_K = ID^*$ then γ aborts the session.
  - (ii) If $ID_K \neq ID^*$, then γ looks in the list L_C^{List} for the tuple (ID_K, PK_K, D_K, x_K) and outputs the D_K to the adversary.
- Secret Value Request Query: Adversary A_1 ask for the Secret Value Request Query for ID_K, then γ responds as follows:
  - (i) If $ID_K = ID^*$ then γ aborts the session.
  - (ii) If $ID_K \neq ID^*$, then γ looks in the list L_C^{List} for the tuple (ID_K, PK_K, D_K, x_K) and output the x_K to the adversary A_1. Otherwise, γ ask for the Request ID_K query and returns the x_K accordingly.

- Public Key Replacement Request Query: Adversary A_1 ask for the Public Key Replacement Request Query corresponding with ID_K to swap the primary public key PK_K with a new public key $PK_K^{'}$. In response to this query γ updates the PK_K with $PK_K^{'}$ in the tuple (ID_K, PK_K, D_K, x_K) to $(ID_K, PK_K^{'}, D_K, x_K)$.
- Signature Request Query: Adversary A_1 ask for the Signature Request Query on (m_K, ID_K) to the challenger γ. To this query request γ looks for the L_C^{List} for the tuple (ID_K, PK_K, D_K, x_K) and does as follows:
  (i) If $ID_K = ID^*$ then γ aborts the session.
  (ii) Otherwise, γ randomly selects $\rho_K \in Z_q^*$ and computes $R_K = h_2^{-1}(\rho_K P - T_K - h_1 P_{pub}) - h_3 X_K$ and in response of the query returns the (ρ_K, R_K) duo to the adversary.
- Forgery: Adversary A_1 yield a valid but a forged signature (ρ_K, R_K) on the message m_K and the identity ID_K. According to Forking lemma, A_1 can falsify another validate signature (ρ_K^*, R_K) with different hash function h_1^* but with same random tape on the same message m_K. Thus γ writes as $\rho_K P = T_K + h_1 P_{pub} + h_2(R_K + h_3 X_K)$ and $\rho_K^* P = T_K + h_1^* P_{pub} + h_2(R_K + h_3 X_K)$, and subtracting them we have

$$\rho_K^* P - \rho_K P = T_K + h_1^* P_{pub} + h_2(R_K + h_3 X_K) - (T_K + h_1 P_{pub} + h_2(R_K + h_3 X_K))$$
$$(\rho_K^* - \rho_K)P = T_K + h_1^* P_{pub} + h_2(R_K + h_3 X_K) - T_K - h_1 P_{pub} - h_2(R_K + h_3 X_K)$$
$$(\rho_K^* - \rho_K)P = (h_1^* - h_1)P_{pub}$$
$$\frac{(\rho_K^* - \rho_K)}{(h_1^* - h_1)} P = P_{pub}$$
$$\frac{(\rho_K^* - \rho_K)}{(h_1^* - h_1)} P = s.P$$
$$\frac{(\rho_K^* - \rho_K)}{(h_1^* - h_1)} = s$$

Hence, γ computes the $s = \frac{(\rho_K^* - \rho_K)}{(h_1^* - h_1)}$ as the solution of the ECDLP for the random instance $(P, Q = sP)$. □

Theorem 6.2. *Under the ECDL assumption, the proposed CLS scheme is unforgeable in opposition to Type II Adversary A_2 in random oracle model.*

Proof. In the proposed CLS scheme, for the adversary A_2, who can break the scheme in time t with ϵ probability, there exist an algorithm γ that can solve the ECDLP $(P, X_K = x_K P)$ for x_K with non-negligible probability. In this game γ act as challenger and interact with the A_2, as depicted below:

- Setup: The challenger γ picks a random number $s \in Z_q^*$ as a master secret key for KGC and set $P_{pub} = sP$ as the public key of the KGC. The challenger γ publishes the public parameters $\varphi = \{F_q, G, P, P_{pub}, H_1, H_2, H_3\}$ and his master secret key to adversary A_2.
  For the consistency and the quick response, γ maintains some lists $L_{H_1}^{List}, L_{H_2}^{List}, L_{H_3}^{List}$ and L_c^{List} as illustrated before in the Theorem 6.1.
- Request ID_K : Upon obtaining the Request ID_K query of the adversary A_2, γ rejoinder as depicted below:
  (i) If $ID_K \neq ID^*$, γ selects the $t_K, x_K \in Z_q^*$ and computes $X_K = x_K.P$ and then sets $T_K = t_K.P$. Then the partial private key computed as $S_K = t_K + h_1 s \mod q$. Then γ outputs $D_K = (T_K, S_K)$, private key $P_K = (S_K, x_K)$ and the public key $PK_K = (T_K, X_K)$. Finally, γ updates the tuples (ID_K, PK_K, D_K, x_K) to list L_C^{List} and $(ID_K, P_{pub}, T_K, l_1)$ to list $L_{H_1}^{List}$.
  (ii) If $ID_K = ID^*$, γ selects the $t_K, x_K \in Z_q^*$ and computes $X_K = x_K.P$ and then sets $T_K = t_K.P$ and output partial private key $D_K = (T_K, \perp)$, private key $P_K = (\perp, x_K)$ and the public key $PK_K = (T_K, X_K)$. After this, in response to this query γ sends the public key $PK_K = (T_K, X_K)$ to the adversary A_2.
- Hash queries: Corresponding to this theorem hash queries are similar to those of the mentioned in previous Theorem 6.1.
- Partial-Private-Key-Request-Query: Adversary A_2 request for the Partial-Private-Key-Request-Query for the ID_K, then γ responds as stated: Firstly, γ looks for the list L_c^{List} in search of the tuple (ID_K, PK_K, D_K, x_K). If the tuple is found then output the D_K, otherwise, go for the Request ID_K query and outputs the D_K accordingly to the adversary A_2.
- Secret-Value-Request-Query: Adversary A_2 request for the Secret-Value-Request-Query with the ID_K, then γ retorts as stated:
  (i) If $ID_K = ID^*$, then γ stops the session.
  (ii) If $ID_K \neq ID^*$, then γ looks in the L_C^{List} for the tuple (ID_K, PK_K, D_K, x_K) outputs the x_K to the adversary A_2. Otherwise, go for the Request ID_K query and outputs the x_K accordingly to the adversary A_2 in response.
- Signature-Request-Query: Corresponding to this theorem Signature-Request-Query is similar to query mentioned in previous Theorem 6.1.

- Forgery: Adversary A_2 yield a valid but a forged signature (ρ_K, R_K) on the message m_K and the identity ID_K. Accordingly with the Forking lemma, A_2 can falsify another validate signature (ρ_K^*, R_K) with different hash function h_2^* but with same random tape on the same message m_K. Thus γ writes as $\rho_K P = T_K + h_1 P_{pub} + h_2(R_K + h_3 X_K)$ and $\rho_K^* P = T_K + h_1 P_{pub} + h_2^*(R_K + h_3 X_K)$, and subtracting them we have

$$\rho_K^* P - \rho_K P = T_(K) + h_1 P_{pub} + h_2^*(R_K + h_3 X_K) - (T_K + h_1 P_{pub} + h_2(R_K + h_3 X_K))$$

$$(\rho_K^* - \rho_K)P = h_2^*(R_K + h_3 X_K) - h_2(R_K + h_3 X_K)$$

$$(\rho_K^* - \rho_K)P = (h_2^* - h_2)(R_K + h_3 X_K)$$

$$\frac{(\rho_K^* - \rho_K)}{(h_2^* - h_2)} P = R_K + h_3 X_K$$

$$\frac{(\rho_K^* - \rho_K)}{(h_2^* - h_2)} P - R_K = h_3 X_K$$

$$h_3^{-1}[\frac{(\rho_K^* - \rho_K)}{(h_2^* - h_2)} P - r_K P] = x_K P$$

$$h_3^{-1}[\frac{(\rho_K^* - \rho_K)}{(h_2^* - h_2)} - r_K]P = x_K P$$

$$x_K = h_3^{-1}[\frac{(\rho_K^* - \rho_K)}{(h_2^* - h_2)} - r_K]$$

Hence, γ computes the $x_K = h_3^{-1}[\frac{(\rho_K^* - \rho_K)}{(h_2^* - h_2)} - r_K]$ as the solution of the ECDLP for the random instance P, X_K. □

7 Efficiency Analysis

In this section, we are going to discuss the efficiency of the proposed scheme by comparing the scheme with the pre-existing well-known scheme. For the evaluation, experimental data from Xiang et al [11] are taken as the support. Here, MIRACL software on Pentium IV is being used for the evaluation of the various cryptographic operation., We have used an additive group G of order q over a non-singular elliptic curve $E : y^2 = x^3 + ax + b \mod q$, where $a, b \in Z_q^*$ and both prime numbers p and q are of the length of 160 bits for obtaining a 1024 bits RSA algorithm level reliable security. Execution time of various cryptographic operations for instance bilinear pairing addition, elliptic curve scalar multiplication, hash function and elliptic addition are delineated below in Table 1. We have analysed the computational evaluation of various existing schemes with our proposed scheme in Table 2 on the premise of the Table 1. Comparison is carried out on the premises of some parameters i.e., cost during the signature phase as well as the verification phase, their hard problem security of the scheme, and pairing or pairing free schemes.

Table 1. Execution time of the cryptographic operations is depicted below.

S.no	Operations	Symbols	Time (ms)
1.	Bilinear pairing multiplication	T_{bpm}	1.6722
2.	Bilinear pairing addition.	T_{bpadd}	0.0069
3.	Elliptic scalar multiplication	T_{em}	0.4420
4.	Elliptic addition.	T_{eadd}	0.0018
5.	Hash function	T_h	0.0001
6.	Inverse function	T_{inv}	0.1888
7.	Modular operation.	T_{mod}	0.0011
8.	Map to point function	T_{mtp}	4.4060

Table 2. Comparative table for the various scheme based on computational cost.

S.No	Scheme	Signature phase	Verification Phase	Pairing Free	Secure	Attack	Hard problem
1.	Kumar et al [6]	$4T_{em} + 2T_{eadd} + 3T_h = 1.7719ms$	$4T_{em} + 3T_{eadd} + 4T_h = 1.7738ms$	No	No	Coalition attack	CDH
2.	Yang et al [28]	$4T_{bpm} + 2T_{bpadd} + 3T_h = 6.7029ms$	$3T_{bpm} + T_{bpadd} + 4T_h = 5.0239ms$	No	No	Coalition attack	CDH
3.	Malhi et al [29]	$4T_{bpm} + 2T_{bpadd} + T_h = 6.7027ms$	$3T_{bpm} + T_{bpadd} + 2T_h = 5.0237ms$	No	No	Coalition attack	CDH
4.	Yeh [21]	$1T_{em} + 1T_h = 0.4421ms$	$4T_{em} + 3T_{eadd} + 1T_h = 1.7735ms$	Yes	No	Type1 & type2 adversary	ECDLP
5.	Ming and Cheng [23]	$3T_{em} + 2T_h = 1.3262ms$	$4T_{em} + 3T_{eadd} + 3T_h = 1.7737ms$	Yes	Yes	-	ECDLP
6.	Gayathri et al. [27]	$3T_{em} + 1T_{eadd} + 2T_h = 1.328ms$	$5T_{em} + 4T_{eadd} + 2T_h + 1T_{inv} = 2.4062ms$	Yes	Yes	-	ECDLP
7.	Liu et al. [26]	$2T_{em} + 3T_h = 0.8843ms$	$4T_{em} + 3T_{eadd} + 3T_h = 1.7737ms$	Yes	No	Type 2 adversary	ECDLP
8.	Our scheme	$1T_{em} + 2T_h = 0.4422ms$	$4T_{em} + 3T_{eadd} + 3T_h = 1.7737ms$	Yes	Yes	-	ECDLP

Scheme [6, 28, 29] are pairing based schemes while the other schemes in the table are pairing free scheme. Computational evaluation carried out using the Table 1 for various schemes. For Gayathri et al. [27] scheme the computational cost for the

signature phase is reckoned as $3T_{em} + 1T_{eadd} + 2T_h = 1.328ms$ and $5T_{em} + 4T_{eadd} + 2T_h + 1T_{inv} = 2.4062ms$ for the verification phase using the Table 1. Similarly, Yang et al [28] $4T_{bpm} + 2T_{bpadd} + 3T_h = 6.7029ms$ and the $3T_{bpm} + T_{bpadd} + 4T_h = 5.0239ms$ for the signature and the verification phase respectively. For our proposed scheme $1T_{em} + 2T_h = 0.4422ms$ and $4T_{em} + 3T_{eadd} + 3T_h = 1.7737ms$ are the computational cost for the signature phase and the verification phase respectively. Likewise, the cost is calculated for the other schemes in Table 2. It can be lucidly

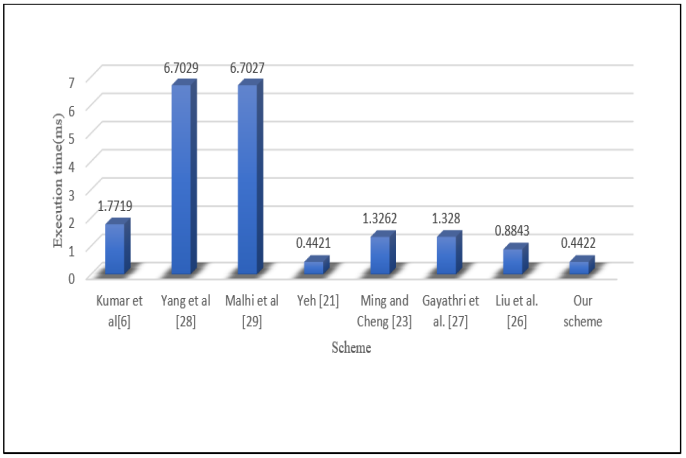

Figure 1. Computational cost for the signature phase.

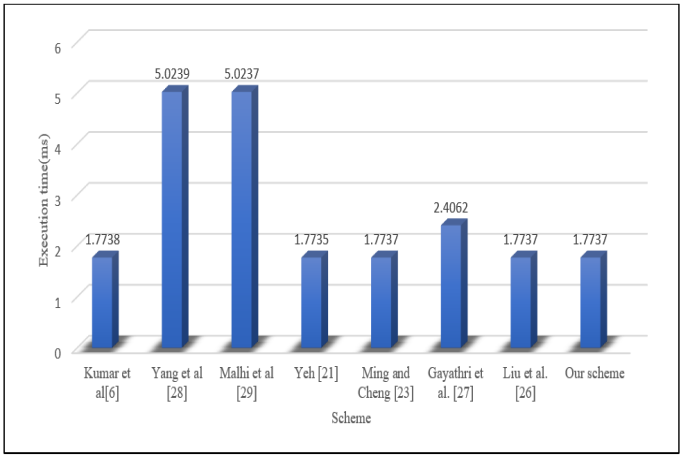

Figure 2. Computational cost for the verification phase.

observed from the Figure 1 and the Figure 2 that for the pairing-based schemes [6, 28, 29] have higher computational cost comparatively of those of the pairing free scheme in the signature phase as well as for the verification phase. Cost for the signature and verification phase in the Yeh [21] scheme is lesser than the proposed scheme but it is not secure against the type I and the type II adversary. Since proposed scheme has security against the both types of attacks, the proposed scheme is more competent compared to the Yeh [21]. The verification cost for the Ming and Xheng et al [23] and the Liu et al [26] is equal to the proposed scheme but their cost on the signature phase is higher than the proposed schemes, so proposed scheme is better than both schemes.

7.1 Energy consumption for the signature

We have analysed the energy consumption of various existing schemes with our proposed scheme. We have computed the energy consumption using the $E_c = C_t P$ [6]. Here E_c represent the energy consumption, C_t represent the total computational time of the signature and P represents the CPU's maximum power. Total computational time of the signature (C_t) is calculated by sum of computational cost for the signature phase and the verification phase. The maximum power of CPU is $38.9W$. Table 3 represents the comparison is carried out on the premises of energy consumption of signature. Energy consumption is calculated by the formula aforementioned. Clearly, total computation cost C_t of the proposed scheme is $2.2159ms$ $(0.4422ms + 1.7737ms = 2.2159ms)$. So, the energy consumption is $86.1986mJ$ $(2.2159ms 38.9W = 86.1986mJ)$. Likewise, the energy consumption is calculated for the other schemes in Table 3. It can be lucidly observed from the Figure 3 and Figure 4 that pairing-based schemes [6, 28, 29] have higher total computation cost and energy consumption comparatively of those of the pairing free scheme. Total computation cost and energy consumption of the Yeh [21] scheme is lesser than the proposed scheme but the it is not secure against the type I and the type II adversary. Since proposed scheme has

Table 3. Energy consumption of various schemes.

S.No	Scheme	Total computation cost for the signature (ms)	Energy consumption for the signature (mJ)
1.	Kumar et al [6]	3.5457	137.9278
2.	Yang et al [28]	11.7268	456.1725
3.	Malhi et al [29]	11.7264	466.7107
4.	Yeh [21]	2.2156	86.1868
5.	Ming and Cheng [23]	3.0999	120.5862
6.	Gayathri et al. [27]	3.7342	145.2604
7.	Liu et al. [26]	2.658	105.7884
8.	Our scheme	2.2159	86.1986

security against the both types of attacks, the proposed scheme is more competent compared to the Yeh [21]. Lucidly, from the above discussion, the proposed scheme has better efficiency in terms of computational cost, energy consumption and the security.

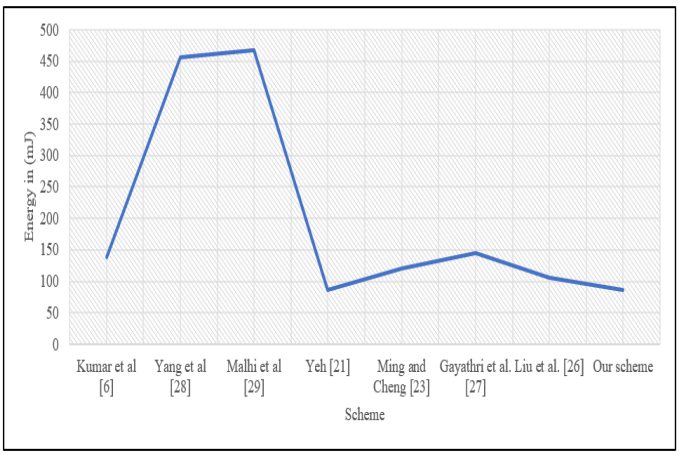

Figure 3. Energy consumption for the signature.

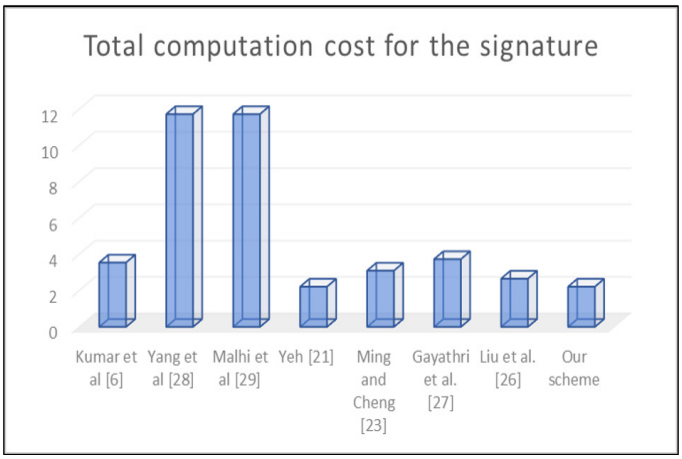

Figure 4. Total computation cost the signature.

8 Conclusion

We have broached a pairing-free certificateless signature scheme. Due to the countenance of certificateless cryptography, it has no key management and certificate management issues. The proposed scheme neither employs the bilinear operation nor the map-to-point hash function, which reduces the computational cost and time consumption. The security of the proposed scheme is based on the ECDLP problem on the random oracle model. In this paper, we have given the security analysis of the proposed scheme against the Type I and the Type II adversary over the random oracle model, which makes our scheme's security features stronger. At last, the efficiency analysis demonstrates that the proposed scheme has a lower computational

cost and energy consumption and provides more security than the other well-known existing scheme. Hence it makes the proposed scheme more efficient and secure and is applicable for the limited bandwidth communication, storage space, and computational cost areas.

References

[1] S.S. Al-Riyami and K.G. Paterson, *Certificateless public key cryptography*, In International Conference on the Theory and Application of Cryptology and Information Security, Springer, Berlin, Heidelberg, pp. 452–473, (2003).

[2] S. Horng, P. Tzeng, X. Huang, T. Wang, M.K. Li, and M.K. Khan, *An efficient certificateless aggregate signature with conditional privacy-preserving for vehicular sensor networks*, Information Sciences, **317**, 48–66, (2015).

[3] Y. Huang, W. Mu, D.S. Susilo, and W. Wu, *Certificateless Signature Revisited*, Proceedings of the ACISP'07, LNCS 4586, Springer-Verlag, Berlin, 308–322, (2007).

[4] D. He, J. Chen, and R. Zhang, *An efficient and provably-secure certificateless signature scheme without bilinear pairings*, International Journal of Communication Systems, **25**, 1432–1442, (2012).

[5] I.A. Kamil and S.O. Ogundoyin, *An improved certificateless aggregate signature scheme without bilinear pairings for vehicular ad hoc networks*, Journal of Information Security and Applications, **44**, 184–200, (2019).

[6] P. Kumar, K. Saru, V. Sharma, A.K. Sangiah, J. Wei, and X. Li, *A certificateless aggregate signature scheme for healthcare sensor network*, Sustainable Computing: Informatics and Systems, **18**, 80–89 (2018).

[7] J. Li, H. Yuan, and Y. Zhang, *Cryptanalysis and Improvement of Certificateless Aggregate Signature with Conditional Privacy-Preserving for Vehicular Sensor Networks*, IACR, Technical Report, EPrint, [Online] Available: https://eprint.iacr.org/2016/692, (2016).

[8] A. Shamir, *Identity-based cryptosystems and signature schemes*, Workshop on the Theory and Application of Cryptographic Techniques, Springer, Berlin, Heidelberg, 47–53, (1984).

[9] K.A. Shim, *Cryptanalysis of two signature schemes for IoT-Based Mobile Payment and Healthcare wireless Medical Sensor Networks*, IEEE Access, **8**, 167203–167208, (2020).

[10] L. Wu, Z. Xu, D. He, and X. Wang, *New certificateless aggregate signature scheme for healthcare multimedia social network on cloud environment*, Secure Communications Networks, **2018**, 2595273, (2018).

[11] D. Xiang, X. Li, J. Gao, and X. Zhang, *A secure and efficient certificateless signature scheme for Internet of Things*, Ad Hoc Networks, **124**, 102702, (2022).

[12] D.H. Yum and P.J. Lee, *Generic construction of certificateless signature*, Australasian Conference on Information Security and Privacy, Springer, Berlin, Heidelberg, 200–211, (2004).

[13] L. Zhang and F. Zhang, *A new certificateless aggregate signature scheme*, Computer Communications, **32**, 1079–1085, (2008).

[14] S.K. Islam and G.P. Biswas, *Provably secure and pairing-free certificateless signature scheme using elliptic curve cryptography*, International Journal of Computer Mathematics, **11**, 2244–2258, DOI: 10.1080/00207160.2013.776674, (2013).

[15] B.C. Hu, D.S. Wong, Z. Zhang, and X. Deng, *Key replacement attack against a generic construction of certificateless signature*, Australasian Conference on Information Security and Privacy, Springer, Berlin, Heidelberg, 235–246, (2006).

[16] X. Huang, W. Susilo, Y. Mu, and F. Zhang, *On the security of certificateless signature schemes*, International Conference on Cryptology and Network Security, Springer, Berlin, Heidelberg, 13–25, (2005).

[17] J.L. Tsai, N.W. Lo, and T.C. Wu, *Weaknesses and improvements of an efficient certificateless signature scheme without using bilinear pairings*, International Journal of Communication Systems, **27**, 1083–1090, DOI: 10.1002/dac.2388, (2014).

[18] J. Cui, J. Zhang, H. Zhong, R. Shi, and Y. Xu, *An efficient certificateless aggregate signature without pairings for vehicular ad hoc networks*, Information Sciences, **451**, 1–15, DOI: 10.1016/j.ins.2018.03.060, (2018).

[19] Y. Zhao, Y. Hou, L. Wang, S. Kumari, M.K. Khan, and H. Xiong, *An efficient certificateless aggregate signature scheme for the Internet of Vehicles*, Transactions on Emerging Telecommunications Technologies, **31**, p. e3708, DOI: 10.1002/ett.3708, (2020).

[20] X. Ye, G. Xu, X. Cheng, Y. Li, and Z. Qin, *Certificateless-based anonymous authentication and aggregate signature scheme for vehicular ad hoc networks*, Wireless Communications and Mobile Computing, **2021**, 6677137, DOI: 10.1155/2021/6677137 (2021).

[21] K.H. Yeh, *A secure transaction scheme with certificateless cryptographic primitives for IoT-based mobile payments*, IEEE Systems Journal, **12**, 2027–2038, DOI: 10.1109/JSYST.2017.2668389, (2018).

[22] N.B. Gayathri, G. Thumbur, P.R. Kumar, M.Z.U. Rahman, and P.V. Reddy, *Efficient and secure pairing-free certificateless aggregate signature scheme for healthcare wireless sensor networks*, IEEE Internet of Things Journal, **6**, DOI: 10.1109/JIOT.2019.2927089, (2019).

[23] Y. Ming and H. Cheng, *Efficient certificateless conditional privacy-preserving authentication scheme in VANETs*, Mobile Information Systems, **2019**, 7593138, DOI: 10.1155/2019/7593138, (2019).

[24] G. Thumbur, G.S. Rao, P.V. Reddy, N.B. Gayathri, D.K. Reddy, and M. Padmavathamma, *Efficient and secure certificateless aggregate signature-based authentication scheme for vehicular ad hoc networks*, IEEE Internet of Things Journal, **8**, 1908–1920, DOI: 10.1109/JIOT.2020.3019304, (2020).

[25] X. Jia, D. He, Q. Liu, and K.K.R. Choo, *An efficient provably-secure certificateless signature scheme for Internet-of-Things deployment*, Ad Hoc Networks, **71**, 78–87, DOI: 10.1016/j.adhoc.2018.01.001, (2018).

[26] J. Liu, L. Wang, and Y. Yu, *Improved security of a pairing-free certificateless aggregate signature in healthcare wireless medical sensor networks*, IEEE Internet of Things Journal, **7**, 5256–5266, DOI: 10.1109/JIOT.2020.2979613, (2020).

[27] N.B. Gayathri, G. Thumbur, R.K. Rao, and P.V. Reddy, *Efficient and secure pairing-free certificateless directed signature scheme*, Journal of King Saud University-Computer and Information Sciences, **33**, 225–234, DOI: 10.1016/j.jksuci.2018.02.016, (2021).

[28] X. Yang, C. Chen, T. Ma, Y. Li, and C. Wang, *An improved certificateless aggregate signature scheme for vehicular ad hoc networks*, In 2018 IEEE 3rd Advanced Information Technology, Electronic and Automation Control Conference (IAEAC) 2334-2338. IEEE 2018.

[29] G. Thakur, S. Prajapat, P. Kumar, A. K. Das, and S. Shetty, *An efficient lightweight provably secure authentication protocol for patient monitoring using wireless medical sensor networks*, IEEE Access, (2023).

[30] S. Prajapat, P. Kumar, S. Kumar, A. K. Das, S. Shetty, and M. S. Hossain, *Designing high-performance identity-based quantum signature protocol with strong security*, IEEE Access, (2024).

[31] S. Prajapat, A. Rana, P. Kumar, and A. K. Das, *Quantum safe lightweight encryption scheme for secure data sharing in Internet of Nano Things*, Computers and Electrical Engineering, **117**, 109253,(2024).

[32] S. Prajapat, P. Kumar, and V. Sharma, *An Efficient CL-Signature scheme over NTRU Lattices*, in Proc. 2022 4th Int. Conf. Adv. Comput., Commun. Control Netw. (ICAC3N), 1220–1224, (2022).

[33] S. Prajapat, P. Kumar, and S. Kumar, *A privacy preserving quantum authentication scheme for secure data sharing in wireless body area networks*, Cluster Computing, 1–17, (2024).

[34] G. Thakur, M. S. Obaidat, P. Sharma, S. Prajapat, and P. Kumar, *An efficient provably secure authentication and key agreement protocol for satellite communication networks*, Security and Privacy, p. e404, (2024).

[35] G. Thakur, S. Prajapat, P. Kumar, and C. M. Chen, *A Privacy-Preserving Three-Factor Authentication System for IoT-Enabled Wireless Sensor Networks*, J. Syst. Archit., **154**, 103245, 2024.

Author information

Deepika Gautam, Srinivasa Ramanujan Department of Mathematics Central University of Himachal Pradesh, Dharamshala (H.P), 176215, India.
E-mail: gautamdeepika1999@gmail.com

Sunil Prajapat, Srinivasa Ramanujan Department of Mathematics Central University of Himachal Pradesh, Dharamshala (H.P), 176215, India.
E-mail: sunilprajapat645@gmail.com

Pankaj Kumar, Srinivasa Ramanujan Department of Mathematics Central University of Himachal Pradesh, Dharamshala (H.P), 176215, India.
E-mail: pkumar240183@gmail.com

Manoj Kumar Patel, Department of Mathematics, NIT Nagaland, Chumukedima, Nagaland, India.
E-mail: mkpitb@gmail.com

Received: 2024-08-01
Accepted: 2024-10-01