The ISC Int'l Journal of Information Security
ISeCure

January 2026, Volume 18, Number 1 (pp. 91–98)
http://www.isecure-journal.org

Efficient Certificateless Multi-Signcryption Scheme for Secure Group Communications

Swapna Gurram [1], N.B. Gayathri [2,*], Gowri Thumbur [3] and T. Siva Nageswara Rao [1]

[1] *Department of Mathematics, Vallorapalli Nageswara Rao Vignana Jyothi Institute of Engineering and Technology, Hyderabad, India*
[2] *Department of Mathematics and Computer Science, Sri Sathya Sai Institute of Higher Learning, Anantapur, India*
[3] *Department of ECE, Gitam University, Andhra Pradesh, India*

ARTICLE INFO.

Article history:
Received: April 23, 2025
Revised: October 08, 2025
Accepted: January 05, 2026
Published Online: January 07, 2026

Keywords:
Multi-Signcryption, Certificateless Signcryption, Public Verifiability, Elliptic Curve, ECCDHP, ECDLP.

Type: Research Article

doi: 10.22042/isecure.2026.518405.1223

ABSTRACT

Confidentiality, unforgeability, and public verifiability are essential for secure multi-party communications. These communications play a vital role in real-world applications such as decentralized financial transactions, e-commerce, cloud computing, and web services, where authentication and privacy preservation are very important. In conventional cryptosystems, individual signcryption performed by each participant significantly increases the unsigncryption cost for the receiver. Multi-signcryption offers an efficient alternative by allowing multiple signers to jointly signcrypt a single message. This paper proposes a novel certificateless multi-signcryption scheme that eliminates the certificate management problem of traditional public key infrastructures and avoids the key escrow problem of identity-based cryptography. To reduce the computational cost associated with bilinear pairings over elliptic curves, the proposed scheme is designed in a pairing-free environment. This scheme achieves constant-time verification in the unsigncryption phase and is independent of the number of signers. Security is formally proven under the hardness assumptions of the Elliptic Curve Computational Diffie–Hellman Problem (ECCDHP) and the Elliptic Curve Discrete Logarithm Problem (ECDLP). The proposed scheme ensures confidentiality, unforgeability, and public verifiability, and it attains significantly lower computational costs than existing schemes. Hence, the proposed scheme can be used for secure group communications in resource-constrained environments where high performance is essential.

1 Introduction

Public key cryptography (PKC) relies on two fundamental requirements: confidentiality and authentication. Encryption guarantees confidentiality, whereas digital signatures ensure authentication. Usually, these objectives are achieved either by encrypting a message and then signing the ciphertext, or by signing a message before encrypting it. However, both approaches incur significant computational and communication overhead. To address this, Zheng [1] introduced a new technique called signcryption, which

[*] Corresponding author.

Email addresses: swapnacrypto@gmail.com, gayatricrypto@gmail.com, gthumbur@gitam.edu, shivathottempudi@gmail.com

ISSN: 2008-2045 © 2026 ISC. All rights reserved.

integrates digital signature and encryption into a single logical step. The basic idea behind signcryption is to simultaneously encrypt the plaintext and generate the signature, instead of following the traditional sequential method. As the cost of signcryption is much lower than the combined cost of encryption and digital signature, it reduces the overall cost associated with performing these operations separately. Extending this concept to multi-party communications can significantly reduce both computational and communication costs for users.

Multi-signcryption combines multiple digital signatures into a single encrypted message, producing one compact signcryption text. This allows multiple parties to perform signcryption simultaneously. Secure multi-party communication has many applications, such as banking, healthcare, and academia. It plays a significant role in real-world applications, including decentralized finance, e-commerce, transaction authorization, and privacy-preserving transactions (e.g., on Ethereum). Additionally, multi-signcryption enhances the security of cloud-based and web applications. In e-voting systems, multi-signcryption techniques ensure voter integrity through encryption, while the use of multiple signatures prevents tampering during ballot access. Similarly, in military and other high-priority government applications, multi-signcryption safeguards national security by securing the transfer of classified information between authorized parties. In many real-world applications, it is often necessary to transmit multiple digital signatures on a single message to a single recipient in an authenticated manner. However, if each sender in a group performs signcryption independently, it results in high computational overhead and increased communication costs.

2 Related Work

In 1997, Zheng [1] proposed the first digital signcryption scheme to improve computational and communication efficiency. Later, in 2004, Baek *et al.* [2] presented a security model for Zheng's scheme in the context of traditional public-key cryptography (PKC) and proved its security. To overcome the challenges related to certificate management in traditional PKC, Shamir [3] introduced a new paradigm known as identity-based cryptography (IDBC), where the public key of a user is derived from a unique identity. Subsequently, several signcryption schemes [4, 5] were proposed within the IDBC framework. The first identity-based signcryption scheme was proposed by Malone-Lee [6]. Later, many identity-based signcryption schemes appeared in the literature [7], including hybrid, aggregate, ring, proxy, and multi-signcryption schemes. In multi-signcryption schemes, if each sender in a group executes signcryption independently, it results in high computational and communication costs at both the sender's and the receiver's ends. To avoid these excessive computations, Zhang *et al.* [8] introduced a novel multi-signcryption scheme in 2009. This scheme provides secure encryption for multiple senders and supports multiple signatures on a single message, regardless of the number of users. Multi-signcryption schemes also allow unsigncryption to be performed at the cost of a single unsigncryption operation. In the same year, Selvi *et al.* [9] proved that the scheme proposed by Zhang *et al.* [8] is insecure and forgeable, and they proposed a new scheme to address these issues in a multi-user setting. However, the schemes presented in [8] and [9] do not provide public verifiability. To overcome this limitation, Swapna *et al.* [10] proposed a signcryption scheme with public verifiability in 2014. All these schemes are based on bilinear pairings over elliptic curves in the identity-based cryptography setting. Subsequently, several studies have focused on improving the security and efficiency of multi-signcryption schemes in the identity-based framework [5, 7–9, 11–13]. In 2013, Khullar *et al.* [14] presented an identity-based multi-receiver signcryption scheme over elliptic curves. In 2015, Qi *et al.* [15] designed an efficient identity-based multi-signcryption scheme that optimizes group communication. In 2018, Tanwar and Kumar [16] proposed a secure multi-signcryption scheme with public verifiability in the identity-based framework. In 2019, Zhao *et al.* [17] proposed a broadcast signcryption scheme for vehicular communications. In 2025, Singh *et al.* [18] proposed a secure multi-proxy multi-signcryption scheme using bilinear pairings for secure e-commerce applications. All the above schemes are based on the identity-based setting. However, identity-based cryptography suffers from the key escrow problem. To overcome this limitation, Al-Riyami and Paterson [19] introduced the notion of certificateless public key cryptography in 2003, which eliminates the certificate management problem of traditional public key infrastructure schemes [1, 4] as well as the key escrow problem inherent in identity-based signature schemes [5, 7–10]. In the certificateless setting, the key generation centre (KGC) generates a partial private key for each user, while the user independently generates the full private key. The first certificateless multi-signcryption scheme without pairings was proposed by Ding [20] in 2014. However, this scheme is not based on elliptic curves and therefore cannot be considered truly pairing-free, as it is constructed over a multiplicative group with 1024-bit keys. In 2018, Wu *et al.* [21] proposed a secure certificateless multi-signcryption scheme in the standard model. In 2024, Swapna *et al.* [22] presented an efficient certificateless multi-signcryption scheme using bilinear pairings over elliptic curves. In the same year, Long *et al.* [23]

and Xu *et al.* [24] proposed certificateless signcryption schemes for wireless body area networks and the Internet of Vehicles, respectively. All the above signcryption schemes are based on bilinear pairings in identity-based and certificateless settings, and the computation of these bilinear pairings is not efficient. To address this efficiency concern, we focus on designing a multi-signcryption scheme in a pairing-free environment. Motivated by this, we propose a new certificateless multi-user signcryption scheme for secure group communications without bilinear pairings. The security of the proposed scheme is analyzed in the random oracle model.

Our Contributions

To the best of our knowledge, there is no existing work in the literature that addresses multi-signcryption in a certificateless setting without bilinear pairings on elliptic curves. To bridge this gap, we propose a certificateless multi-signcryption (CL-MSC) scheme that does not rely on bilinear pairings. We present the framework of the CL-MSC scheme and prove its security based on the hardness assumptions of the Elliptic Curve Computational Diffie–Hellman Problem (EC-CDHP) and the Elliptic Curve Discrete Logarithm Problem (ECDLP). The proposed scheme achieves public verifiability, confidentiality, and unforgeability. Furthermore, we analyze the efficiency of the proposed scheme in terms of both computational and communication costs and compare it with existing multi-signcryption schemes. The rest of the paper is structured as follows. Section 3 presents the mathematical preliminaries, complexity assumptions, the formal model of the CL-MSC scheme, and its security requirements. Section 4 describes the proposed scheme in detail. The security analysis is provided in Section 5.2. In Section 5.3, we compare the efficiency of the proposed scheme with existing schemes and demonstrate its superiority. Finally, Section 6 concludes the paper.

3 Preliminaries

In this section, we present the mathematical preliminaries and define the computational hard problems [25]. We also describe the formal model of the CL-MSC scheme along with its security model.

3.1 Computational hard problems

*Elliptic Curve Group:*An elliptic curve E over a prime finite field F_p is defined by an equation $y^2 = x^3 + ax + b\,(modp)$ where $a, b \in F_p^*$ and $27b^2 + 4a^3 \neq 0$. Then $G = \{(x, y)/x, y \in F_p, E(x, y) = 0\} \cup \{\mathcal{O}\}$ is the additive elliptic curve group where $\mathcal{O}$ is the point at infinity [25].

Definition 1. Let us consider the points on the elliptic curve form an additive cyclic group G and Q be the generator of G. Determine $abQ \in G$, where $a, b \in F_p^*$, from the given occurrence (Q, aQ, bQ) with a known parameter Q is termed as Elliptic Curve Computational Diffie-Hellman Problem (ECCDHP).

Definition 2. Let us consider the points on the elliptic curve form an additive cyclic group G and Q be the generator of G. According to the ECCDHP assumption in G, no one can solve the ECCDHP in G with a non-negligible advantage in a probabilistic polynomial time.

Definition 3. Let us consider the points on the elliptic curve form an additive cyclic group G and Q be the generator of G. Let $a \in F_p^*$ be selected at random and kept confidential. The Elliptic Curve Discrete Logarithmic Problem (ECDLP) is to compute a from $aQ \in G$.

Definition 4. Let us consider the points on the elliptic curve form an additive cyclic group G and Q be the generator of G. According to the ECCDHP assumption in G, no one can solve the ECDLP in G with a non-negligible advantage in a probabilistic polynomial time.

3.2 Formal Model for proposed CL-MSC Scheme

Here, we define the CL-MSC scheme model through a flowchart, as shown in Figure 1. The scheme consists of the following algorithms: Setup, Partial Private Key (PPK) Generation, Private and Public Key Generation, Multi-Signcryption, and Unsigncryption. Each of these algorithms is described in detail below.

3.3 Security requirements for CL-MSC Scheme

The basic security requirements of signcryption are unforgeability and confidentiality. Achieving these two properties simultaneously is challenging and complex. We assume that R denotes the receiver, and S_i, for $i = 1, 2, ..., n$, denote the signers. The proposed CL-MSC scheme is designed to satisfy key security requirements [7, 26], including confidentiality, unforgeability, and public verifiability.

- *Confidentiality:* Retrieving the plain-text m is infeasible for any intruder, and it is also infeasible to derive the receiver's private key from the signcryption text σ.
- *Unforgeability:* No intruder can generate a valid signature on behalf of any member of the signer group.
- *Public Verifiability:* The authenticity of the CL-MSC scheme can be verified by any third party

without knowledge of the original message or the receiver's private key.

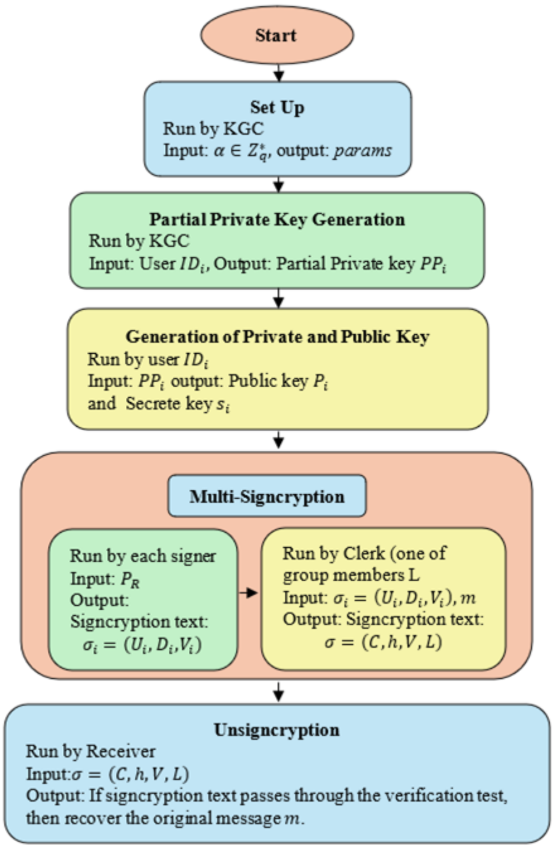
Start
Set Up
Run by KGC
Input: $\alpha \in Z_q^*$, output: *params*
Partial Private Key Generation
Run by KGC
Input: User ID_i, Output: Partial Private key PP_i
Generation of Private and Public Key
Run by user ID_i
Input: PP_i output: Public key P_i
and Secrete key s_i
Multi-Signcryption
Run by each signer
Input: P_R
Output:
Signcryption text:
$\sigma_i = (U_i, D_i, V_i)$
Run by Clerk (one of
group members L
Input: $\sigma_i = (U_i, D_i, V_i), m$
Output: Signcryption text:
$\sigma = (C, h, V, L)$
Unsigncryption
Run by Receiver
Input:$\sigma = (C, h, V, L)$
Output: If signcryption text passes through the verification test,
then recover the original message m.

Figure 1. CL-MSC Scheme

Table 1. Notations and their Meanings

Notation	Meanings
$G = \langle P \rangle$	Cyclic group G with generator P
k, α	Security parameter, Master secret key
params	System Public parameters
KGC	Key Generation Center
ID_i, ID_R	Identity of the user i and receiver R
H_i	Collision-resistant hash functions
d_i	Partial private key of the user i
P_i, s_i	Public key and Secret key of the user i
m, C	Message, Ciphertext
σ	Signcryption text

4 Design of CL-MSC Scheme

This section presents the proposed multi-signcryption scheme in a certificateless setting on elliptic curves, without the use of bilinear pairings. The scheme involves five core algorithms: Setup, Partial Private Key (PPK) Generation, Private and Public Key Generation, Multi-Signcryption, and Unsigncryption, described as follows.The basic notations used in the scheme are summarized in Table 1.

Set-Up:

KGC runs this algorithm by choosing an additive cyclic group G with the generator P, prime order $q = 2^n$, security parameter k, and the message space $m \in \{0,1\}^n$. KGC also defines the following hash functions, $H_1 : G \times \{0,1\}^* \to Z_q^*$, $H_2 : G \to \{0,1\}^n$, $H_3 : \{0,1\}^* \to Z_q^*$. The KGC chooses his secret key $\alpha \in_R Z_q^*$ and calculates $P_{pub} = \alpha P$. Finally, KGC publishes $params = \{k, n, q, Z_q^*, P, P_{pub}, H_1, H_2, H_3\}$ as the public parameters.

PPK Generation:

KGC chooses $\mu_i \in_R Z_q^*$ and then computes $X_i = \mu_i P$ and $d_i = \mu_i + \alpha H_{1i}(X_i, ID_i, P_{pub})$ with the user's identity ID_i. Using the secure channel, KGC sends the PPK pair $PP_i = (X_i, d_i)$ to the user.

Generation of Private and Public Keys:

After receiving the PPK pair (X_i, d_i) through secure channel, User verifies $d_i P = X_i + h_{1i} P_{pub}$ where $h_{1i} = H_{1i}(X_i, ID_i, P_{pub})$. He accepts the pair (X_i, d_i) if it is true. The User sets the full public key as $P_i = (X_i, R_i)$ where $R_i = \lambda_i P$, sets the private key as $s_i = (d_i, \lambda_i)$, where the user randomly selects $\lambda_i \in Z_q^*$.

Multi-Signcryption Scheme:

Each sender with an identity ID_{S_i} in the list L of n members executes this algorithm with the receiver's identity ID_R, the receiver's public key (X_R, R_R), and m is the message to generate signcryption text σ_i. Each sender performs the following steps.

(1) Each sender chooses $u_i \in_R Z_q^*$ and computes $D_i = u_i(X_R + R_R + h_{1R} P_{pub})$ and $U_i = u_i P$.
(2) Send (U_i, D_i) through the secure channel to all other senders in the group.
(3) Each sender computes $D = \sum_{i=1}^{n} D_i, U = \sum_{i=1}^{n} U_i$, after receiving (U_i, D_i) from the others, and encrypts the message m by $C = m \oplus H_2(D)$ and then computes $h = H_3(C, U, D, P_{ID_R}, L)$.
(4) Each sender generates the signature by computing $V_i = \frac{u_i}{\lambda_{S_i} h + d_{S_i}}$ and then sends it to the clerk (one of the members from the list L) along with the values U, D, and C. Once receiving (V_i, U, D, C) from all the senders, the clerk verifies whether U, D, and C values are the same; if so, then the clerk computes $V = \sum_{i=1}^{n} V_i$. Finally, output the resultant signcryption text $\sigma = (C, h, V, L)$ and send it to the receiver R.

Unsigncryption

The receiver with an identity ID_R executes this algorithm with ID_{S_i} as the identity of the sender, the public key of the sender $P_{ID_{S_i}}$, and the signcryption text σ. To verify the signcryption text and decrypt the messages, the receiver carries out the following steps.

(1) Compute $U^{'} = V(hR_S + X_S + h_{1S}P_{pub})$.
(2) Computes $D^{'} = (\lambda_R + d_R)U^{'}$
(3) Compute $h^{'} = H_3(C, U^{'}, D^{'}, P_{ID_R}, L)$.
(4) Accept the message m iff $h^{'} = h$, and retrieve the message m as $m = C \oplus H_2(D^{'})$.

5 Analysis of CL-MSC scheme

The correctness of our CL-MSC scheme, Security, and Efficiency analysis are discussed in this section.

5.1 Correctness of CL-MSC Scheme

The correctness of the CL-MSC scheme is shown by the following equations.

$U^{'} = V(hR_S + X_S + h_{1S}P_{pub})$
$= \sum_{i=1}^{n} V_i(hR_{S_i} + X_{S_i} + P_{pub}h_{1S_i}(X_{S_i}, ID_{S_i}, P_{pub}))$
$= \sum_{i=1}^{n} \frac{u_i}{\lambda_{S_i}h+d_{S_i}}(hR_{S_i}+X_{S_i}+P_{pub}h_{1S_i}(X_{S_i}, ID_{S_i}, P_{pub}))$
$= \sum_{i=1}^{n} \frac{u_i}{\lambda_{S_i}h+d_{S_i}}(h\lambda_{S_i}+\mu_{S_i}+\alpha h_{1S_i}(X_{S_i}, ID_{S_i}, P_{pub}))P$
$= \sum_{i=1}^{n} \frac{u_i}{\lambda_{S_i}h+d_{S_i}}(h\lambda_{S_i} + d_{S_i})P$
$= \sum_{i=1}^{n} u_iP$
$= \sum_{i=1}^{n} U_i = U$.

The signature is verified $h^{'} = h$ iff $U^{'} = U$.

5.2 Security Analysis of CL-MSC Scheme

The security parameters of the proposed CL-MSC scheme, like confidentiality, unforgeability, and public verifiability, are discussed in this section.

- *Confidentiality:* Without knowledge of D, no one can decrypt the message, since it needs the receiver's private key.
  $D^{'} = (\lambda_R + d_R)U$
  $= \sum_{i=1}^{n}(\lambda_R + d_R)u_iP$
  $= \sum_{i=1}^{n}(\lambda_RP + d_RP)u_i$
  $= \sum_{i=1}^{n}(R_R+X_R+P_{pub}H_{1R}(X_R, ID_R, P_{pub}))u_i$
  $= \sum_{i=1}^{n} D_i = D$.
  An intruder must solve ECDLP to obtain the receiver's private key, but this is infeasible due to security parameters. Therefore, the confidentiality of this scheme relies on the infeasibility of solving the ECDLP in probabilistic polynomial time.
- *Unforgeability:* Any sender in the group L, as well as any outside adversary who is not involved in the protocol execution, cannot forge the proposed CL-MSC signature. Since the CL-MSC scheme utilizes the private keys of all participating signcrypters, no individual signer in the group can independently generate a valid signcryption. Furthermore, the clerk in the signcrypter group L, who is responsible for combining the individual signatures, may attempt to select values λ_i and D_i before computing V such that $h' = h$ holds for a forged message m. By doing so, the clerk is effectively attempting to solve the inversion problem, which can be reduced to the Elliptic Curve Computational Diffie–Hellman Problem (ECCDHP) and the Elliptic Curve Discrete Logarithm Problem (ECDLP) in the group G. Hence, the clerk cannot forge the proposed CL-MSC scheme. Since the remaining signers in group L possess fewer capabilities than the clerk, they are also unable to forge a valid signcryption.

  Finally, an external intruder who does not participate in the CL-MSC protocol cannot forge the scheme, even if all individual signatures are available, because forging a valid signcryption requires knowledge of all users' private keys. A formal security proof for the unforgeability of the proposed scheme follows the same approach as that proved by Swapna et al. [26]. Therefore, the proposed CL-MSC scheme is unforgeable.
- *Public Verifiability:* Public verifiability refers to the ability to verify the authenticity of a signcrypted test without knowledge of the original message. In the proposed CL-MSC scheme, any third party can verify the authenticity of the signcryption in the event of a dispute between the sender and the receiver.

5.3 Efficiency Analysis of CL-MSC Scheme

This section presents a comparison of the proposed CL-MSC scheme with existing schemes in the literature. To the best of our knowledge, there is no multi-signcryption scheme without bilinear pairings in the certificateless setting; therefore, we limit our comparison to identity-based signcryption schemes. The efficiency of the proposed CL-MSC scheme is compared with the schemes in [8–10]. The computational cost is evaluated based on the experimental results reported in [27–29], where various cryptographic operations are implemented using the MIRACL library. The results are summarized in Table 2.

Table 2. Running Time of Cryptographic Operations and its Notations

Notation	Descriptions and running time
T_P	Running time for computation of one pairing $\approx 87T_{ML}$
T_{PE}	Running time for computation of pairing based exponentiation $\approx 43.5T_{ML}$
T_{SM}	Running time for computation of one scalar multiplication $\approx 29T_{ML}$
T_{PA}	Running time for computation of one point addition $\approx 0.12T_{ML}$

The methods used to perform the mathematical operations and their transformations are also presented in Table 2. The analysis considers a cyclic

Table 3. Security Notions

Scheme	Conf.	Unfor.	P.V	No. K.E.P.	W.P
[8]	✓	✓	×	×	×
[9]	✓	✓	×	×	×
[10]	✓	✓	✓	×	×
[OURS]	✓	✓	✓	✓	✓

group G defined over an elliptic curve, specifically a Koblitz curve of the form $E : y^2 = x^3 + ax + b \pmod p$, defined over the field $\mathbb{Z}_q^*$. The length of the points in group G is approximately 320 bits, and the size of q is approximately 160 bits. The proposed CL-MSC scheme is compared with related schemes using various security parameters, including confidentiality (Con.), unforgeability (Unforg.), public verifiability (P.V.), absence of the key escrow problem (No K.E.P.), and pairing-free construction (W.P.), as shown in Table 3. The comparison demonstrates that only the proposed scheme provides confidentiality, unforgeability, and public verifiability in a certificateless setting without bilinear pairings. Furthermore, Table 4 shows that the proposed scheme incurs very low computational costs during both the signcryption and unsigncryption phases compared to existing schemes. In addition, the verification process during unsigncryption is independent of the number of signers. For the same message length and the same number of group members in the list L, the communication cost of the proposed scheme is $|G|+|\mathbb{Z}_q^*|= 480$ bits, which is more efficient than the existing schemes in [8–10], which require $2|G|= 640$ bits. Figure 2 illustrates the running time of the signcryption algorithm, showing that the proposed CL-MSC scheme achieves significantly lower computational time compared to existing schemes, with a running time of $(58.36n + 28.64)T_{ML}$ for n users. Similarly, Figure 3 shows that the running time of the unsigncryption algorithm is independent of the number of signers and is equal to $116.24T_{ML}$. Finally, Figure 4 presents the total running time of the proposed CL-MSC scheme, which is $4230.02T_{ML}$ for 70 users. From a computational perspective, the proposed CL-MSC scheme is more efficient, particularly as the number of users in the network increases.

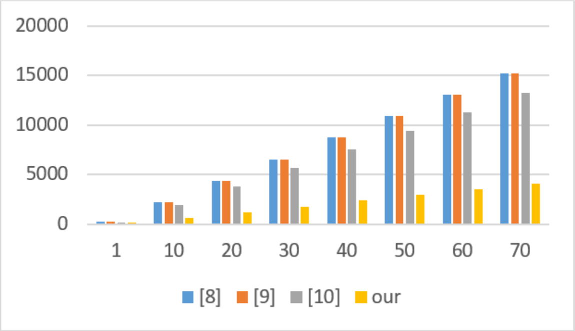

Figure 2. Running Time of Signcryption Algorithm

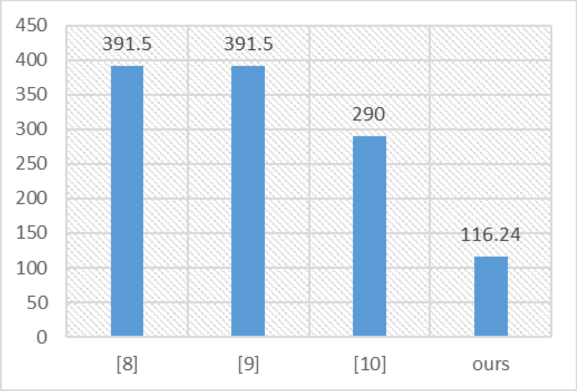

Figure 3. Running Time of Unsigncryption Algorithm

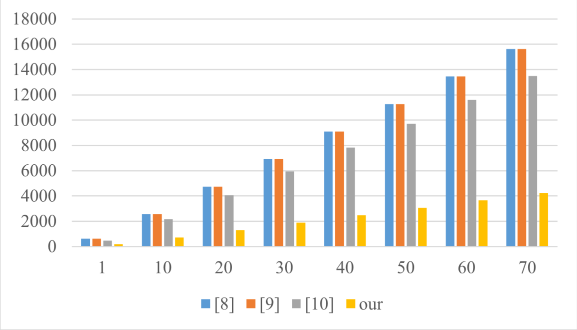

Figure 4. Total Running Time of CL-MSC Scheme

6 Conclusion

In this paper, we propose a certificateless multi-signcryption scheme for secure group communications without bilinear pairings. The proposed CL-MSC scheme achieves essential security properties, including confidentiality, unforgeability, and public verifiability, under standard elliptic curve hardness assumptions. By eliminating bilinear pairings, the scheme significantly reduces computational and communication overhead compared to existing identity-based and certificateless multi-signcryption schemes. The security of the proposed scheme was analyzed in the random oracle model, and its efficiency was evaluated through a detailed comparison with related schemes. Owing to its lightweight design and strong security guarantees, the proposed CL-MSC scheme is suitable for practical applications such as secure group communications, e-commerce, and resource-constrained environments.

References

[1] Yuliang Zheng. Digital signcryption or how to achieve cost(signature + encryption) ¡ cost(signature) + cost(encryption). In *Advances in Cryptology - CRYPTO '97*, pages 165–179.

Table 4. Total Running Time of CL-MSC Scheme

Scheme	Multi-Signcryption	Unsigncryption	Total time	Total cost in T_{ML}
[8]	$3nT_{SM} + nT_{PE} + nT_P$	$T_{PE} + 4T_P$	$3nT_{SM} + (n+1)T_{PE} + (n+4)T_P$	$211.5n + 391.5$
[9]	$3nT_{SM} + nT_{PE} + nT_P$	$T_{PE} + 4T_P$	$3nT_{SM} + (n+1)T_{PE} + (n+4)T_P$	$211.5n + 391.5$
[10]	$2nT_{SM} + nT_{PE} + nT_P$	$T_{SM} + 3T_P$	$(2n+1)T_{SM} + nT_{PE} + (n+3)T_P$	$184.5n + 290$
[OURS]	$(1+2n)T_{SM} + 3(n-1)T_{PA}$	$2T_{PA} + 4T_{SM}$	$(2n+5)T_{SM} + (3n-1)T_{PA}$	$58.36n + 144.88$

Springer, Berlin, Heidelberg, 1997.

[2] Joonsang Baek, Jan Newmarch, Reihaneh Safavi-Naini, and Willy Susilo. A survey of identity-based cryptography. In *In Proc. of the 10th Annual Conference for Australian Unix User Group*, pages 95–102, 2004.

[3] Adi Shamir. Identity-based cryptosystems and signature schemes. In *Advances in Cryptology: Proceedings of CRYPTO 84*, pages 47–53. Springer, Berlin, Heidelberg, 1985.

[4] Chandana Gamage, Yuliang Zheng, and Jussipekka Leiwo. An efficient scheme for secure mesasage transmission using proxy-signcryption. In *In Proc. 22nd Australasian Computer Science Conference (ACSC)*, pages 420–431, Auckland, New Zealand, 1999.

[5] Fagen Li, Yong Yu, Xudong Luo, and Feng Huang. A survey of identity-based signcryption. *IETE Technical Review*, 28(3):265–272, 2011.

[6] John Malone-Lee. Identity-based signcryption. Cryptology ePrint Archive, Report 2002/098, 2002.

[7] Padmalaya Nayak, P. Vasudeva Reddy, and G Swapna. Security issues in iot applications using certificateless aggregate signcryption schemes: An overview. *Internet of Things*, 21:100641, 2023.

[8] Jianhong Zhang, Yixian Yang, and Xinxin Niu. A novel identity-based multi-signcryption scheme. *Computer communications*, 32(1):14–18, 2009.

[9] S. S. D Selvi, G. P. Sarathy, and S. Sarath Kumar. Breaking and fixing of an identity-based multi-signcryption scheme. In *Provable Security: Second International Conference, ProvSec 2008, Guiyang, China, October 15-17, 2008. Proceedings*, pages 61–75. Springer, Berlin, Heidelberg, 2009.

[10] G. Swapna and P. Vasudeva Reddy. Efficient identity based multi-signcryption scheme with public verifiability. *Journal of Discrete Mathematical Sciences and Cryptography*, 17(2):181–190, 2014.

[11] Yu Zhou, Zeng Li, Feng Hu, and Fagen Li. Identity-based combined public key schemes for signature, encryption, and signcryption. In P Chandra, D Giri, F Li, S Kar, and D Jana, editors, *Information Technology and Applied Mathematics, Advances in Intelligent Systems and Computing*, volume 699, pages 1–10. Springer, Singapore, 2019.

[12] SSD Selvi, SS Vivek, J Shriram, S Kalaivani, and CP Rangan. Identity based aggregate signcryption schemes. In B Roy and N Sendrier, editors, *Progress in Cryptology – INDOCRYPT 2009, LNCS*, volume 5922, pages 378–397. Springer, Berlin, Heidelberg, 2009.

[13] Y Sun, Cong Xu, Fagen Li, and Yong Yu. Identity based multi-proxy multi-signcryption scheme for electronic commerce. In *Proc. of the 2009 Fifth International Conference on Information Assurance and Security*, pages 281–284, Xi'an, China, 2009.

[14] Shruti Khullar, V Richhariya, and Vandana Richhariya. An efficient identity based multi-receiver signcryption scheme using ecc. *International Journal of Advancements in Research & Technology*, 2(4):189–194, Apr 2013.

[15] Z H Qi, H C Yang, and H Huang. An efficient identity-based multi-signcryption scheme. In *Proc. of the International Conference on Computer Information Systems and Industrial Applications*, pages 308–310. Atlantis Press, 2015.

[16] Sunil Tanwar and Ashwani Kumar. Extended identity based multi-signcryption scheme with public verifiability. *Journal of Information and Optimization Sciences*, 39(2):503–517, 2018.

[17] Yu Zhao, Yan Wang, Yixi Liang, Haiyang Yu, and Yang Ren. Identity-based broadcast signcryption scheme for vehicular platoon communication. *IEEE Transactions on Industrial Informatics*, 19(6):7814–7824, Jun 2023.

[18] T Singh, R Ali, and Varsha Tyagi. An efficient identity based multi-proxy multi-signcryption scheme for electronic commerce using bilinear pairing. *Procedia Computer Science*, 259:1592–1601, 2025.

[19] Samad S Al-Riyami and Kenneth G Paterson. Certificateless public key cryptography. In *Proc. Adv. Cryptol. (ASIACRYPT)*, volume 2894, pages 452–473, 2003.

[20] Ya Ding. Certificateless multi-signcryption scheme without pairing. *Applied Mechanics and Materials*, 599-601:1435–1438, 2014.

[21] Xiangdong Wu, Min Zhang, and Shengjie Zhu.

Certificateless multi-signcryption scheme in standard model. *International Journal of Grid and Utility Computing*, 9(2):120–127, 2018.

[22] G Swapna, G Naga Malleswari, Gowri Thumbur, and T Kusuma. Efficient certificateless multi-signcryption scheme using elliptic curves. *Journal of Computational Analysis and Applications (JoCAAA)*, 33(08):2207–2216, 2024.

[23] W Long, Li Deng, Junjie Zeng, Yang Gao, and Tingyi Lu. An efficient certificateless anonymous signcryption scheme for wban. *Sensors*, 24(15):4899, 2024.

[24] Gang Xu, X Yin, and Xiang Li. Lightweight and secure multi-message multi-receiver certificateless signcryption scheme for the internet of vehicles. 2024.

[25] Neal Koblitz, Alfred J Koblitz, and Alfred J Menezes. Elliptic curve cryptography: The serpentine course of a paradigm shift. *Journal of Number Theory*, 131(5):781–814, 2011.

[26] G. Swapna, K.A. Ajmath, and Gowri Thumbur. An efficient pairing-free certificateless signcryption scheme with public verifiability. *Journal of Mathematical and Computer Science*, 11:24–43, 2021.

[27] Kun Ren, Wenjing Zhang, Feng Zhang, Ting He, Chan Kim, and Kiseok Lee. On broadcast authentication in wireless sensor networks. *IEEE Transactions on Wireless Communications*, 6(11):4136–4144, 2007.

[28] Xi Cao and Zhen-Guo Cao. A pairing-free identity-based authenticated key agreement protocol with minimal message exchanges. *Information Sciences*, 180(15):2895–2903, 2010.

[29] Song-Yong Tan, Meng-Chow Lim, and Ming-Theng Chia. Java implementation for pairing-based cryptosystems. In *Computational Science and Its Applications – ICCSA 2010: 10th International Conference, Fukuoka, Japan, March 23-26, 2010. Proceedings, Part IV*, volume 6016 of *Lecture Notes in Computer Science*, pages 188–198. Springer, Berlin, Heidelberg, 2010.

Swapna Gurram is an Assistant Professor in the Department of Mathematics at VNR Vignana Jyothi Institute of Engineering and Technology, Hyderabad, India. She received her M.Sc., M.Phil., and Ph.D. degrees in Mathematics from Andhra University, India. She has over 18 years of academic and research experience. Her research interests include cryptography and information security, with a particular emphasis on designing efficient and secure cryptographic algorithms. Dr. swapna is a Life Member of the Andhra Pradesh and Telangana State Mathematics Society.

N. B. Gayathri is an Assistant Professor in the Department of Mathematics and Computer Science (DMACS) at Sri Sathya Sai Institute of Higher Learning, Anantapur Campus, India. She received her M.Sc., M.Phil., and Ph.D. degrees in Mathematics from Andhra University, India. She has more than 15 years of academic and research experience. Her research interests focus on cryptography and information security, particularly the development of efficient and secure cryptographic algorithms. She has also completed a funded research project under the Women Scientist Scheme of the Department of Science and Technology, Government of India. Dr. Gayathri serves as a reviewer for several journals and is a Life Member of the Indian Mathematical Society.

Gowri Thumbur (Senior Member, IEEE) received the B.Tech. degree in Electronics and Communication Engineering from Nagarjuna University, Guntur, India, in 2000, and the M.Tech. degree in Digital Systems and Computer Electronics from Jawaharlal Nehru Technological University, Anantapur, India, in 2005. She received the Ph.D. degree in Electronics and Communication Engineering, with a specialization in Signal Processing, from Jawaharlal Nehru Technological University, Kakinada, India, in 2017. She is currently an Associate Professor in the Department of Electronics and Communication Engineering, GITAM School of Technology, GITAM University, Vishakhapatnam, India. Her research interests include signal processing, VLSI design, digital image processing, and information security.

T. Siva Nageswara Rao earned his M.Sc. degree in Mathematics from Nagarjuna University and his Ph.D. degree from Rayalaseema University. He is currently serving as an Assistant Professor in the Department of Mathematics at Vallurupalli Nageswara Rao Vignana Jyothi Institute of Engineering and Technology (VNR VJIET), Hyderabad, Telangana, India.