*Journal of Quality Measurement and Analysis*
*e-ISSN: 2600-8602*
*https://doi.org/10.17576/jqma.2104.2025.15*

*JQMA* 21(4) 2025, 299-312
*http://www.ukm.my/jqma*

# A NEW SIGNCRYPTION SCHEME USING ELLIPTIC CURVE DISCRETE LOGARITHM PROBLEM

(*Skema Tandatangan-Penyulitan Baharu Menggunakan Masalah Logaritma Diskret Lengkung Eliptik*)

MD NIZAM UDIN & EDDIE SHAHRIL ISMAIL*

*ABSTRACT*

Signcryption is a modern cryptographic technique that merges the functionalities of digital signature and encryption into a single logical step, providing both confidentiality and authentication more efficiently than traditional methods. With the increasing demand for secure and lightweight communication in mobile and Internet of Things (IoT) environments, the development of efficient signcryption protocols has become critical. This paper proposes a novel elliptic curve-based signcryption scheme that is exclusively founded on the hardness of the Elliptic Curve Discrete Logarithm Problem (ECDLP), eliminating the use of modular exponentiation and pairing operations, which are computationally expensive in resource-constrained platforms. The proposed scheme is composed of five main phases: initialization, partial private key extraction, user key generation, signcryption, and unsigncryption. Formal analysis confirms that it satisfies essential security properties, including confidentiality, integrity, unforgeability, non-repudiation, forward secrecy, and public verifiability. These properties are achieved under standard cryptographic assumptions without compromising efficiency. Performance evaluation was conducted through comparative analysis and runtime testing. The results demonstrate that the proposed scheme achieves comparable or improved computational efficiency relative to several recent elliptic curve-based schemes, particularly the lightweight signcryption protocol. In conclusion, this study presents a secure, scalable, and implementation-friendly signcryption solution that aligns with the cryptographic requirements of modern digital communication, offering a promising direction for secure transactions in IoT ecosystems, mobile applications, and embedded systems.

*Keywords:* elliptic curve signcryption; elliptic curve discrete logarithm problem; lightweight cryptography; secure communication protocol

*ABSTRAK*

Tandatangan-penyulitan ialah satu teknik kriptografi moden yang menggabungkan fungsi tandatangan digital dan penyulitan dalam satu langkah logik, sekali gus menyediakan kerahsiaan dan pengesahan dengan lebih cekap berbanding kaedah tradisional. Dengan peningkatan keperluan terhadap komunikasi yang selamat dan ringan dalam persekitaran mudah alih serta Internet Benda (IoT), pembangunan protokol tandatangan-penyulitan yang cekap menjadi semakin penting. Kajian ini mencadangkan satu skema tandatangan-penyulitan baharu berasaskan lengkung eliptik yang dibina sepenuhnya berasaskan kesukaran Masalah Logaritma Diskret Lengkung Eliptik (ECDLP), tanpa menggunakan eksponen modular mahupun operasi berpasangan yang lazimnya mahal dari segi pengiraan dalam platform sumber terhad. Skema yang dicadangkan terdiri daripada lima fasa utama: inisialisasi, pengekstrakan kunci persendirian separa, penjanaan kunci pengguna, tandatangan-penyulitan, dan penyahsulitan. Analisis formal mengesahkan bahawa skema ini memenuhi sifat keselamatan utama termasuk kerahsiaan, integriti, ketidakbolehpalsuan, nir-penyakalan, kerahsiaan ke hadapan dan kebolehan pengesahan awam. Semua ciri keselamatan ini dicapai berdasarkan andaian kriptografi standard tanpa menjejaskan kecekapan. Penilaian prestasi telah dijalankan melalui analisis perbandingan dan ujian masa larian. Hasil kajian menunjukkan bahawa skema yang dicadangkan mencapai kecekapan pengiraan yang setara atau lebih baik berbanding beberapa skema terkini berasaskan lengkung eliptik, terutamanya protokol signcryption ringan. Kesimpulannya, kajian ini memperkenalkan satu

penyelesaian signcryption yang selamat, berskala, dan mesra pelaksanaan selaras dengan keperluan kriptografi komunikasi digital moden, khususnya untuk transaksi selamat dalam ekosistem IoT, aplikasi mudah alih, dan sistem terbenam.

*Kata kunci:* tandatangan-penyulitan lengkung eliptik; masalah logaritma diskret lengkung eliptik; kriptografi ringan; protocol komunikasi selamat

## 1. Introduction

Signcryption is a cryptographic technique that merges the functionalities of digital signature and encryption into a single operation. This concept was introduced by Zheng (1997), who demonstrated that combining these two cryptographic primitives into one step can significantly reduce computational costs and communication overhead compared to the traditional "sign-then-encrypt" paradigm. In this merged design, signcryption simultaneously provides both confidentiality and authenticity, offering a practical solution for secure digital communication.

Based on Zheng's foundational work, the development of signcryption has progressed to improve its efficiency, security and applicability, particularly through the adoption of elliptic curve cryptography (ECC). The idea of using elliptic curves in cryptographic systems was independently proposed by Miller (1986) and Koblitz (1987), who recognized the potential of elliptic curves over finite fields for constructing secure public key primitives (Miller 1986; Koblitz 1987).

ECC offers significantly enhanced security per bit and reduced key sizes compared to traditional systems based on integer factorization or discrete logarithm problems. These advantages make ECC especially appealing for resource-constrained platforms such as mobile devices, embedded systems, and Internet of Things (IoT) applications. Over time, the cryptographic community has built upon Miller and Koblitz's foundation to develop a range of elliptic curve-based schemes, including ECDSA for digital signatures and ECC-based signcryption protocols. The latter now serve as efficient alternatives to traditional "sign-then-encrypt" approaches, offering strong security guarantees with lower computational and communication overhead.

In parallel with the development of elliptic curve cryptography, the concept of message recovery in signature schemes, where the original message is embedded within the signature and later recovered during verification, was introduced by Nyberg and Rueppel (1996). Their work on digital signatures based on the discrete logarithm problem with message recovery marked a significant advancement by reducing communication costs and enabling more compact cryptographic protocols (Nyberg & Rueppel 1996).

The original elliptic curve-based signcryption scheme was proposed by Zheng and Imai (1998). Their model removed the necessity for modular exponentiation, utilizing elliptic curve scalar multiplication to accomplish encryption and digital signing in one compact procedure. However, the proposed scheme does not provide forward secrecy and public verifiability. Hwang *et al.* (2005) improved ECC-based signcryption by integrating forward secrecy, which safeguards previous messages from compromise in the event of long-term key exposure. Nonetheless, their research did not include thorough empirical performance validation.

Toorani and Beheshti (2009) further advanced ECC signcryption by emphasizing public verifiability and session key derivation without requiring pairing operations. Their scheme strengthened the security model while maintaining lightweight operations. More recent developments have focused on adapting ECC signcryption to mobile and cloud environments. For instance, Kumar and Gupta (2019) proposed an identity-based signcryption protocol using ECC that was optimized for low-power IoT devices. Their work emphasized authentication and confidentiality but relied partially on modular operations, which limited its efficiency.

Tsai and Su (2017) developed an elliptic curve-based blind signcryption scheme aimed at efficiently processing multiple digital documents. The scheme uses a blinding mechanism to

protect sender anonymity and prevent traceability. While it offers computational efficiency and blindness, it lacks forward secrecy, leakage resilience, and certificateless deployment, which are increasingly important for modern mobile and IoT applications.

Zhang *et al.* (2022) proposed a lightweight ECC signcryption scheme designed to minimize overall computation and enhance message integrity, especially in edge computing environments. In their study, Bashir and Ali (2019) identified weaknesses in blind ECC signcryption models and introduced a more efficient framework that maintains unforgeability and integrity. Recently, various schemes have been developed, including those by Tsai *et al.* (2022), Ho *et al.* (2024), and Ricci *et al.* (2021), focusing on improvements like leakage resilience, group anonymity, and proxy delegation in the ECC signcryption framework.

Despite these advances, many existing ECC signcryption schemes still incorporate modular exponentiation, pairing-based computations, or rely on hybrid hardness assumptions, thereby introducing unnecessary complexity. For example, Tsai and Su (2017) proposed an ECC-based blind signcryption scheme that combines elliptic curve operations with blinding mechanisms and symmetric encryption, relying on multiple intertwined cryptographic primitives to achieve sender anonymity, confidentiality, and untraceability. Moreover, some schemes do not fully satisfy modern security requirements such as forward secrecy, non-repudiation, and public verifiability in a provable way, thus limiting their practicality in lightweight and constrained environments.

This paper proposes an enhanced elliptic curve signcryption scheme that relies solely on the ECDLP, addressing the identified challenges. The proposed design completely removes modular exponentiation, relying solely on point addition and scalar multiplication within elliptic curves. It meets all essential cryptographic objectives, which are confidentiality, integrity, authenticity, non-repudiation, unforgeability, and forward secrecy, while reducing computational overhead. This renders it especially appropriate for real-time applications in IoT, mobile networks, and embedded platforms. The comparative analysis demonstrates that the proposed scheme provides similar or better security coverage while significantly reducing runtime costs in comparison to several benchmark ECC-based signcryption protocols.

## 2. Preliminaries

This section outlines the fundamental mathematical structures, cryptographic primitives, and security properties that form the basis of the proposed signcryption scheme in line with the foundational principles outlined by Mogollon (2007).

### 2.1. *Elliptic Curve Discrete Logarithm Problem (ECDLP)*

**Definition 2.1** (ECDLP)**.** Given an elliptic curve $E(\mathbb{F}_q)$ and two points $P$ and $Q = d \times P$ on the curve, the elliptic curve discrete logarithm problem is to determine the scalar $d \in \mathbb{Z}_p^*$.

The difficulty of solving this problem forms the basis of ECC's security (Cheng *et al.* 2020).

### 2.2. *Definition and Correctness of Signcryption*

A signcryption scheme is a cryptographic construct that integrates the functionalities of digital signature and encryption into a single operation. It is designed to provide both confidentiality and authenticity more efficiently than the traditional "sign-then-encrypt" paradigm.

**Definition 2.2** (Signcryption Scheme (Zheng 1997))**.** Given the key space $\mathcal{K}$, message space $\mathcal{M}$, and signcryption space $\mathcal{S}$, for any sender *s* and receiver *r*. A signcryption scheme is defined by a tuple of four polynomial-time algorithms SC=(initialization, key generation, signcryption, unsigncryption):

(i) **Initialization** Init$(1^\lambda) \rightarrow$ params: Outputs public system parameters based on the security parameter $\lambda$, including elliptic curve settings, hash functions, and symmetric encryption schemes.
(ii) **Key Generation** KeyGen(params) $\rightarrow (pub, pvt)$: Generates a user key pair consisting of a private key $pvt$ and a public key $pub$.
(iii) **Signcrypt** Signcrypt$(m, pub_r, pvt_s) \rightarrow \sigma$: Given a message $m$, receiver's public key $pub_r$, and sender's private key $pvt_s$, outputs a ciphertext $\sigma$ that encapsulates both encryption and signature.
(iv) **Unsigncrypt** Unsigncrypt$(\sigma, pub_s, pvt_r) \rightarrow m$ or $\perp$: Given ciphertext $\sigma$, sender's public key $pub_s$, and receiver's private key $pvt_r$, returns the original message $m$ or failure $\perp$ if verification fails.

**Definition 2.3** (Correctness)**.** A signcryption scheme is correct if, for all key pairs $(pub_s, pvt_s)$, $(pub_r, pvt_r)$, and all messages $m \in \mathcal{M}$, the following holds:

$$\text{Unsigncrypt}(\text{Signcrypt}(m, Pub_r, Pvt_s), Pub_s, Pvt_r) = m \tag{1}$$

This guarantees that a message encrypted and signed by the sender can be correctly recovered and verified by the intended receiver.

## 3. The Proposed Signcryption Scheme

This section introduces a lightweight signcryption scheme founded on elliptic curve cryptography, specifically designed to provide strong cryptographic guarantees while avoiding computationally intensive operations such as modular exponentiation. The scheme operates exclusively on elliptic curve primitives, namely, point addition and scalar multiplication, and achieves core security objectives based on the intractability of the Elliptic Curve Discrete Logarithm Problem (ECDLP). It is structured into four sequential phases: initialization, key generation, signcryption, and unsigncryption. In contrast to generalized signcryption frameworks that support encryption-only, signature-only, or combined modes (Wang *et al.* 2010), the proposed scheme is dedicated solely to integrated signcryption, thereby reducing structural overhead and enhancing runtime efficiency for secure real-time communication.

Previous enhancements to signcryption protocols have explored certificate-based and certificateless frameworks to address public key replacement and authentication without full reliance on traditional public key infrastructures. For example, Lu and Li (2014) proposed a certificate-based scheme that improves resistance to insider threats and key substitution attacks, albeit at the cost of increased processing due to certificate handling. On the other hand, Toradmalle *et al.* (2019) presented a lightweight, certificateless model well-suited to IoT environments, though it still introduces complexity through identity management. The proposed scheme departs from these approaches by eliminating certificate dependencies entirely, relying instead on elliptic curve operations and ephemeral session keys to ensure both cryptographic robustness and deployment simplicity in resource-constrained platforms.

### 3.1. *Construction*

This section presents the construction of our certificateless elliptic curve signcryption scheme SC = (initialization, partial private key extraction, user key generation, signcryption, unsigncryption).

The scheme adopts the certificateless public key model of Al-Riyami and Paterson (2003), combining a partial private key issued by a trusted KGC with a user-chosen secret. This eliminates the need for certificates while avoiding key escrow, and enables lightweight ECC-based signcryption without bilinear pairings.

(i) **Phase 1: Initialization**

This phase is performed by the Key Generation Center (KGC) to initialize global parameters and system-wide cryptographic settings.

(a) Select a large prime number $p$ and define the finite field GF($p$).
(b) Choose an elliptic curve $E(\text{GF}(p))$ defined by the equation $y^2 = x^3 + ax + b \mod p$, where $a, b \in \text{GF}(p)$, and $4a^3 + 27b^2 \not\equiv 0 \mod p$.
(c) Select a base point $G \in E(\text{GF}(p))$ of prime order $q$, where $q$ is a large prime.
(d) Choose a master secret key $s_{KGC} \in \mathbb{Z}_q^*$, and compute the corresponding public key $P_{\text{KGC}} = s_{KGC} \times G$.
(e) Two cryptographic hash functions are defined: $H_1 : \{0,1\}^* \to \mathbb{Z}_q^*$, such as SHA-256 used to map user identities to scalars, and $H_{k_2} : \{0,1\}^* \to \mathbb{Z}_q$, used as a keyed hash function such as HMAC-SHA-256 (National Institute of Standards and Technology 2015) during the signcryption process.
(f) The public system parameters are then published as

$$\text{params} = (\text{GP}(p), E, G, q, P_{\text{KGC}}, H_1, H_{k_2}, E_k, D_k)$$

where $E_k$ and $D_k$ denote symmetric encryption and decryption algorithms such as AES-256.

(ii) **Phase 2: Partial Private Key Extraction**
Given a user identity $ID_x$, the Key Generation Center (KGC) executes the following steps:

(a) Compute the hashed identity scalar: $h_x = H_1(ID_x) \in \mathbb{Z}_q^*$.
(b) Generate the user's identity point: $Q_x = h_x \times G \in \text{GP}(p)$.
(c) Derive the user's partial private key: $D_x = s \times Q_x$, where $s$ is the KGC's master secret.
(d) Send $D_x$ securely to the user over an authenticated and confidential channel.

(iii) **Phase 3: User Key Generation**
Upon receiving the partial private key $D_x$, the user completes their key pair as follows:

(a) Choose a random secret value $x \in \mathbb{Z}_q^*$.
(b) Compute the public key component: $P_x = x \times G \in \text{GP}(p)$.
(c) Reconstruct the identity point: $Q_x = H_1(ID_x) \times G$.
(d) Set the full private key as $SK_x = (x, D_x)$ and the full public key as $PK_x = (P_x, Q_x)$.

(iv) **Phase 4: Signcryption**
To signcrypt a message $m$ to a receiver with identity $ID_r$, the sender proceeds as follows:

(a) Select a random ephemeral scalar $e \in \mathbb{Z}_q^*$ and compute the ephemeral public key $J = e \times G$.
(b) Compute the recipient's identity point $Q_r = H_1(ID_r) \times G$.
(c) Compute the session key as $K = e \times (P_r + Q_r) = (k_1, k_2)$.
(d) Encrypt the message to obtain ciphertext $c = E_{k_1}(m)$.
(e) Compute the hash value $r = H_{k_2}(J \| m) \in \mathbb{Z}_q$.
(f) Compute the sender's identity point $Q_s = H_1(ID_s) \times G$.
(g) Compute the signature component $S = r \times (P_s + Q_s)$.
(h) Output the signcryption tuple $\sigma = (c, J, S)$.

(v) **Phase 5: Unsigncryption**
Upon receiving the signcryption tuple $\sigma = (c, J, S)$, the receiver performs:

(a) Compute $h_r = H_1(ID_r) \in \mathbb{Z}_q$ and the identity point $Q_r = h_r \times G$.

(b) Derive the session key: $K = (x_r + h_r) \times J = (k_1, k_2)$.
(c) Decrypt the ciphertext: $m = D_{k_1}(c)$.
(d) Compute the hash value $r = H_{k_2}(J \parallel m)$.
(e) Recompute sender's identity point: $Q_s = H_1(ID_s) \times G$.
(f) Verify the signature by checking whether $S \stackrel{?}{=} r \times (P_s + Q_s)$.
(g) If valid, accept $m$; otherwise, reject.

### 3.2. *Correctness*

The correctness of the scheme is shown by verifying that both parties derive the same session key and the signature relation holds. Let $Q_s = H_1(ID_s) \cdot G$, $Q_r = H_1(ID_r) \cdot G$, and $J = e \cdot G$ for ephemeral scalar $e \in \mathbb{Z}_q^*$. The sender computes the session key as:

$$K = e \times (P_r + Q_r) \tag{2}$$

and the signature component as:

$$S = r \times (P_s + Q_s), \quad \text{where } r = H_{k_2}(J \| m) \tag{3}$$

The receiver computes:

$$K = (x_r + h_r) \times J = e \times (P_r + Q_r) \tag{4}$$

since $h_r = H_1(ID_r)$, and derives the same $k_1$ to decrypt $m$. He/She then verifies:

$$S \stackrel{?}{=} r \times (P_s + Q_s) \tag{5}$$

As all values match, decryption and signature verification succeed, confirming correctness.

## 4. Security Analysis

This section analyzes the proposed signcryption scheme in terms of its ability to satisfy standard cryptographic security properties. The scheme is evaluated against six core objectives: confidentiality, unforgeability, integrity, non-repudiation, forward secrecy, and public verifiability, including the certificate model. Two security models, which are indistinguishability under chosen ciphertext attack (IND-CCA) and existential unforgeability under chosen message attack (EUF-CMA) developed by Baek *et al.* (2007) used to test confidentiality and unforgeability, respectively.

### 4.1. *Confidentiality*

The confidentiality of the proposed scheme is proven in the random oracle model under the assumption that the Elliptic Curve Diffie-Hellman (ECDH) problem is hard.

**Theorem 4.1.** *If there exists a probabilistic polynomial-time (PPT) adversary $\mathcal{A}$ who can break the confidentiality of the scheme under adaptive chosen ciphertext attack (IND-CCA2) with non-negligible advantage $\varepsilon$, then there exists a challenger $\mathcal{C}$ that can solve the ECDH problem with non-negligible advantage.*

**Proof.** Let $\mathcal{C}$ be given an ECDH instance: $(G, A = a \times G, B = b \times G)$, and the goal is to compute $ab \times G$. $\mathcal{C}$ runs $\mathcal{A}$ as a subroutine and simulates the environment as follows:

**Setup:** The challenger generates public parameters and sets $J^* = A$ and $P_r + Q_r = B$. Thus, the session key becomes $K^* = a \times B = ab \times G$. All other parameters are generated honestly. Hash oracles $H_1$, $H_{k_2}$, and symmetric encryption oracles are modeled as random oracles.

**Phase 1:** The adversary $\mathcal{A}$ is allowed to query:

(1) $H_1(ID_i)$: Simulated with a uniformly random value and stored in a list.
(2) $H_{k_2}(J\|m)$: Simulated similarly.
(3) Signcryption and Unsigncryption queries: Simulated honestly using known keys, except when involving the challenge ciphertext.

**Challenge:** The adversary submits two messages $m_0, m_1$ of equal length. The challenger flips a random bit $b \in \{0, 1\}$, computes $c^* = E_{k_1}(m_b)$, where $k_1 = \text{KDF}_1(K^*)$, and sends $\sigma^* = (c^*, J^*)$ to $\mathcal{A}$.

**Phase 2:** $\mathcal{A}$ may continue to issue all queries, except for unsigncrypt queries on $\sigma^*$.

**Guess:** Finally, $\mathcal{A}$ outputs a guess $b'$. If $b' = b$, then $\mathcal{C}$ outputs $ab \cdot G = K^*$.

**Advantage:** If $\mathcal{A}$ has non-negligible advantage in distinguishing $m_0, m_1$, then $\mathcal{C}$ solves the ECDH problem with non-negligible advantage. Therefore, under the ECDH assumption, the scheme is IND-CCA2 secure.

### 4.2. *Unforgeability*

The unforgeability of the proposed scheme is modeled using the standard EUF-CMA game. Let $\mathcal{A}$ be a probabilistic polynomial-time (PPT) adversary who interacts with a challenger $\mathcal{C}$ through a series of oracle queries.

**Theorem 4.2.** *If a PPT adversary $\mathcal{A}$ can forge a valid signcryption $\sigma^* = (c^*, J^*, S^*)$ for a new message $m^*$ and identity $ID_s$ without querying the signcryption oracle on $(m^*, ID_s)$, then $\mathcal{C}$ can solve the ECDLP with non-negligible probability in the random oracle model.*

**Proof.** Let the challenger $\mathcal{C}$ be given an ECDLP instance $(G, Q = x \times G)$, and aim to compute $x$. $\mathcal{C}$ simulates the environment for adversary $\mathcal{A}$ as follows:

**Setup:** $\mathcal{C}$ sets $Q_s = Q$ as the target public key of the sender, with unknown secret key $x_s$. All other system parameters are generated honestly. Lists $L_{H_1}$, $L_{H_2}$, and $L_{SC}$ are initialized to empty.

**Oracle Queries:**

(1) $H_1$**-queries:** On input $ID_i$, if $(ID_i, h_i)$ exists in $L_{H_1}$, return $h_i$; else pick $h_i \in \mathbb{Z}_q^*$ uniformly at random, store and return it.
(2) $H_2$**-queries:** On input $(J, m)$, if tuple exists in $L_{H_2}$, return stored value; else pick $r \in \mathbb{Z}_q^*$, store and return it.
(3) **Signcrypt queries:** When queried on $m$, the challenger simulates $(c, J, S)$ as follows:

$$J = e \times G, \quad r = H_{k_2}(J\|m), \quad S = r \times (P_s + Q_s) \tag{6}$$

even though $\mathcal{C}$ does not know $x_s$, as only $P_s = x_s G$ is required in algebraic form.
(4) **Unsigncrypt queries:** These are simulated honestly unless they match the challenge forgery.

**Forgery:** Eventually, $\mathcal{A}$ outputs a forgery $\sigma^* = (c^*, J^*, S^*)$ on message $m^*$ for identity $ID_s$, such that the verification equation:

$$S^* \stackrel{?}{=} r^* \times (P_s + Q_s), \quad r^* = H_{k_2}(J^*\|m^*) \tag{7}$$

holds and $(m^*, ID_s)$ was never queried.

**Case Analysis:**

- **Case 1:** $r^*$ was queried to $H_2$. Since $\mathcal{C}$ knows $r^*, S^*, Q_s$, it computes:

$$x_s = \frac{1}{r^*}(S^* - r^* \times Q_s) \times G^{-1} \tag{8}$$

solving the ECDLP.
- **Case 2:** $r^*$ was never queried. Then success probability is negligible due to hash function collision resistance.

Thus, any successful forgery under EUF-CMA implies solving the ECDLP.

### 4.3. *Integrity*

The proposed scheme guarantees that any modification to the ciphertext or message will be detected during unsigncryption.

**Theorem 4.3.** *The proposed scheme ensures message integrity: any modification of the ciphertext $c$, ephemeral key $J$, or the message $m$ will result in the signature verification $S = r \times (P_s + Q_s)$ failing.*

**Proof.** The integrity check is based on the equation $S = r \times (P_s + Q_s)$, where $r = H_{k_2}(J \| m)$. If either $J$, $m$, or $S$ is altered, then the recomputed value $r' = H_{k_2}(J' \| m')$ will differ from the original $r$, unless a hash collision occurs.

Given the collision resistance of $H_{k_2}$, it is computationally infeasible for an adversary to forge a valid $(J', m')$ such that the same $r$ is produced. Therefore, any unauthorized change will invalidate the signature equation, and the message will be rejected.

### 4.4. *Non-repudiation*

The proposed scheme ensures that the sender cannot deny having generated a valid signcrypted message.

**Theorem 4.4.** *The proposed scheme achieves non-repudiation: any recipient or external verifier can prove that a signcrypted message was generated by the sender with identity $ID_s$, assuming the collision resistance of $H_1$ and $H_{k_2}$.*

**Proof.** The signature is computed as $S = r \times (P_s + Q_s)$, where $Q_s = H_1(ID_s) \times G$ and $r = H_{k_2}(J \| m)$. Both $P_s$ and $Q_s$ are linked to the sender's identity $ID_s$ and long-term key. The verifier can recompute $r$ from $J$ and $m$, and verify that:

$$S \stackrel{?}{=} r \times (P_s + Q_s)$$

Given the collision resistance of the hash functions, only the legitimate sender with access to $x_s$ can produce a valid $S$ that satisfies this equation. Therefore, the sender is cryptographically bound to the message and cannot repudiate it.

### 4.5. *Forward secrecy*

The proposed scheme provides forward secrecy of message confidentiality under the assumption that the sender's long-term private key is compromised after the session.

**Theorem 4.5.** *The proposed scheme achieves forward secrecy: if the ephemeral scalar $e \in \mathbb{Z}_q^*$ used in a signcryption session is not revealed, then compromising the sender's long-term private key $x_s$ does not allow an adversary to recover the session key $K$ or decrypt the message $m$.*

**Proof.** The session key is derived as $K = e \times (P_r + Q_r)$, where $e$ is a fresh random scalar chosen independently for each session. The ephemeral public key $J = e \times G$ is exposed in the ciphertext, but without knowing $e$, the adversary cannot compute $K$, assuming the hardness of the Elliptic Curve Diffie-Hellman (ECDH) problem. Even if the adversary later obtains the sender's long-term key $x_s$, it provides no advantage in computing $K$, since $e$ is not derivable from $J$ without solving the ECDLP. Therefore, the confidentiality of previously signcrypted messages remains preserved.

### 4.6. *Public verifiability*

The proposed scheme allows any third party to verify the authenticity of a signcrypted message using only public information.

**Theorem 4.6.** *Given a valid signcryption tuple $\sigma = (c, J, S)$, the receiver or any external verifier can verify the origin of the message using the sender's public key $P_s$, the identity point $Q_s = H_1(ID_s) \times G$, and the reconstructed hash $r = H_{k_2}(J\|m)$, by checking:*

$$S \stackrel{?}{=} r \times (P_s + Q_s)$$

**Proof.** All terms in the verification equation are publicly computable: $P_s$ is published by the sender, $Q_s$ is derived from the sender's identity, $J$ is part of the ciphertext, and $m$ is recovered after decryption. The hash $r = H_{k_2}(J\|m)$ is reconstructed identically. Since the original signature was generated as $S = r \times (P_s + Q_s)$, this equation holds under honest execution. No private or partial keys are required to validate $S$, thus satisfying public verifiability.

### 4.7. *Certificate model*

The proposed scheme operates within the certificateless public key cryptography (CL-PKC) model as introduced by Al-Riyami and Paterson (2003), eliminating the need for traditional digital certificates and central public key infrastructures (PKIs). In this model, the Key Generation Center (KGC) issues a partial private key $D_x$ derived from a user's identity $ID_x$, while the user selects an independent secret value $x \in \mathbb{Z}_q^*$ and computes a corresponding public key component $P_x = x \times G$. The complete private key is $SK_x = (x, D_x)$, and the full public key is $PK_x = (P_x, Q_x)$, where $Q_x = H_1(ID_x) \times G$ is the identity-derived point.

This hybrid construction prevents key escrow since the KGC does not know the user's full private key, and at the same time, public key verification does not require digital certificates, as the binding between $ID_x$ and $PK_x$ is embedded cryptographically via the hash function $H_1$. The verification of the signature $S = r \times (P_s + Q_s)$ relies solely on the sender's identity and published public key components, with no need for certificate validation or revocation mechanisms.

Therefore, the proposed scheme achieves certificateless security while maintaining efficiency and removing the operational burden associated with managing certificates or deploying centralized authorities.

The proposed scheme satisfies all standard security objectives of a robust signcryption protocol: correctness, confidentiality, integrity, unforgeability, non-repudiation, and forward secrecy, as shown in Table 1.

## 5. Performance Analysis

An effective signcryption scheme must achieve strong cryptographic security while minimizing computational and communication costs, particularly in constrained environments such as mobile networks and Internet of Things (IoT) devices. This section evaluates the performance of the proposed scheme in terms of security feature coverage, computational complexity, and runtime efficiency, and compares it with several benchmark elliptic curve-based signcryption protocols, including Zheng and Imai (1998), Hwang *et al.* (2005), Tsai and Su (2017), Zhang *et al.* (2022), and Bashir and Ali (2019).

### 5.1. *Security feature comparison*

Table 2 shows a comparison of security properties between the proposed scheme and several notable elliptic curve-based signcryption protocols. The proposed scheme achieves comprehensive security coverage, including confidentiality, integrity, unforgeability, non-repudiation

Table 1: Security goals, mechanisms, and assumptions in the proposed scheme

| **Security Property** | **Enforcing Mechanism** | **Security Model** | **Underlying Assumption** |
|---|---|---|---|
| **Confidentiality** | AES encryption using key $k_1 = \text{KDF}_1(K)$, where $K = e \times (P_r + Q_r)$. | IND-CCA2 | Hardness of ECDH problem, random oracle model |
| **Unforgeability** | Signature $S = r \times (P_s + Q_s)$; only computable with sender's full private key. | EUF-CMA | ECDLP hardness, collision resistance of $H_{k_2}$ |
| **Integrity** | Integrity linked to $r = H_{k_2}(J\|\|m)$, and verified via signature equation $S = r \times (P_s + Q_s)$. | Implicit | Collision resistance of keyed hash $H_{k_2}$ |
| **Non-repudiation** | Signature binds $m$ to $P_s + Q_s$; verifiable by any third party. | Implicit | ECDLP + uniqueness of EC point-to-key binding |
| **Forward Secrecy** | Ephemeral scalar $e \in \mathbb{Z}_q^*$ used once per session; $J = e \times G$ is public. | Implicit | ECDLP prevents recovery of $e$ from $J$ |
| **Public verifiability** | Signature $S = r \times (P_s + Q_s)$ verifiable using only public keys and hash $r = H_{k_2}(J\|\|m)$. | Implicit | ECC arithmetic soundness + public key binding |
| **Certificate Model** | No certificates; key binding via $Q_x = H_1(ID_x) \times G$ and user's secret $x$. | CL-PKC | No CA or PKI needed; certificateless assumption |

IND-CCA2: Indistinguishability under Adaptive Chosen Ciphertext Attack, EUF-CMA: Existential Unforgeability under Chosen Message Attack, CL-PKC: Certificateless Public Key Cryptography.

(directly verifiable), forward secrecy, and public verifiability. In contrast, while Hwang *et al.* (2005) provides similar security coverage, it is still based on a certificate-based model. Zhang *et al.* (2022) offers strong security features but lacks public verifiability and depends on certificates, which can increase implementation overhead in dynamic or lightweight environments.

Schemes such as Zheng and Imai (1998) and Tsai and Su (2017) do not provide forward secrecy or public verifiability, limiting their applicability in modern secure communication systems. Notably, the proposed scheme operates in a certificateless setting, eliminating the need for certificate management while still achieving robust security goals. This makes it highly suitable for deployment in mobile, IoT, and other resource-constrained environments.

Table 2: Comparison of security features across signcryption schemes

| **Signcryption Schemes** | **Conf** | **Int** | **Unf** | **NonR** | **ForS** | **PubV** | **CertM** |
|---|---|---|---|---|---|---|---|
| Our proposed scheme | **Yes** | **Yes** | **Yes** | **Directly** | **Yes** | **Yes** | **Certificateless** |
| Zheng and Imai (1998) | **Yes** | **Yes** | **Yes** | **Partially** | **No** | **No** | **Certificate-based** |
| Hwang *et al*. (2005) | **Yes** | **Yes** | **Yes** | **Directly** | **Yes** | **Yes** | **Certificate-based** |
| Tsai and Su (2017) | **Yes** | **Yes** | **Yes** | **Directly** | **No** | **No** | **Certificate-based** |
| Bashir and Ali (2019) | **Yes** | **Yes** | **Yes** | **Directly** | **Yes** | **No** | **Certificate-based** |
| Zhang *et al*. (2022) | **Yes** | **Yes** | **Yes** | **Directly** | **Yes** | **No** | **Certificate-based** |

Conf: Confidentiality, Int: Integrity, Unf: Unforgeability, NonR: Non-repudiation, ForS: Forward Secrecy, PubV: Public Verifiability, CertM: Certificate Model.

### 5.2. *Computational cost comparison*

The proposed scheme is designed to avoid expensive operations such as modular exponentiation and pairing operation. Instead, it relies entirely on elliptic curve scalar multiplication and addition. Table 3 compares the number and type of cryptographic operations required during

the signcryption and unsigncryption phases. Many pairing-based signcryption schemes rely on libraries such as the PBC library (Lynn 2022), to implement bilinear maps for identity-based or proxy-based functions. However, these operations are known to be computationally intensive, particularly on constrained devices. Our scheme avoids such dependencies entirely, focusing on scalar multiplication and point addition on elliptic curves to maximize efficiency.

Table 3: Comparison of computational cost per phase

| Signcryption Schemes | | Enc | Dec | H | EXP | MI | MA | MM | ECM | ECA |
|---|---|---|---|---|---|---|---|---|---|---|
| Our proposed scheme | Signcryption | 1 | 0 | 1 | 0 | 0 | 0 | 1 | 3 | 1 |
| | Unsigncryption | 0 | 1 | 1 | 0 | 0 | 0 | 0 | 3 | 1 |
| Zheng and Imai (1998) | Signcryption | 1 | 0 | 2 | 0 | 1 | 1 | 0 | 1 | 0 |
| | Unsigncryption | 0 | 1 | 2 | 0 | 0 | 0 | 2 | 2 | 1 |
| Hwang *et al*. (2005) | Signcryption | 1 | 0 | 1 | 0 | 0 | 1 | 1 | 2 | 0 |
| | Unsigncryption | 0 | 1 | 1 | 0 | 0 | 0 | 0 | 3 | 1 |
| Tsai and Su (2017) | Signcryption | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 5 | 0 |
| | Unsigncryption | 0 | 1 | 0 | 0 | 0 | 0 | 0 | 4 | 4 |
| Bashir and Ali (2019) | Signcryption | 1 | 0 | 2 | 1 | 0 | 2 | 0 | 3 | 1 |
| | Unsigncryption | 0 | 1 | 0 | 0 | 0 | 0 | 1 | 2 | 0 |
| Zhang *et al*. (2022) | Signcryption | 1 | 0 | 1 | 0 | 1 | 0 | 1 | 1 | 0 |
| | Unsigncryption | 0 | 1 | 1 | 0 | 1 | 0 | 2 | 2 | 1 |

Enc: Encryption, Dec: Decryption, H: One-way or keyed one-way hash function, EXP: Modular exponentiation, DIV: Modular inversion, MA: Modular addition, MM: Modular multiplication, ECM: Elliptic curve point multiplication, ECA: Elliptic curve point addition

### 5.3. *Runtime performance evaluation*

For computational analysis, we use the primitive and cryptographic operation timing as shown in Table 4. We used the experimental platform, which is Python in Windows 11 64-bit operating system with an 11th-gen Intel(R) Core(TM) i7-1165G7 @ 2.80GHz 2.80 GHz processor and 8000 MB of RAM to measure the approximate running times of arithmetic and cryptographic operations. Table 4 shows the approximate running time for the operations of elliptic curve point multiplication $T_{ECM}$, elliptic curve point addition $T_{ECA}$, modular exponentiation $T_{EXP}$, modular addition $T_{MA}$, modular multiplication $T_{MM}$, hashing $T_H$ and symmetric encryption $T_{sym}$. We used 100 iterations for each test to get more reliable results, balancing accuracy and runtime. We need to select the appropriate key sizes, specifically the 3072-bit RSA key size (modular exponentiation), to align with the security level of the 256-bit elliptic curves (Singh *et al.* 2016). Modular multiplication and addition also use this key size to be consistent. The order of time complexity found by Shohaimay and Ismail (2023) becomes $T_{EXP} \gg T_{ECM} \gg T_{ECA} \gg T_{sym} \gg T_H$ after combining with modular exponentiation$T_{EXP}$. As evident, modular exponentiation is approximately 120 times slower than elliptic curve point addition, making its elimination a key efficiency advantage.

### 5.4. *Total computational time*

The computational cost refers to the total time complexity associated with the operations executed during signcryption and unsigncryption. As indicated in Table 5, $T_{MA}$, $T_{MM}$, $T_H$ and $T_{ECA}$ are disregarded due to their negligible values. The proposed scheme has a computational cost of $6T_{ECM}$+$2T_{sym}$ and has a running time of approximately 0.202184 ms. The running time for the proposed scheme is faster than Zhang *et al.* (2022), Bashir and Ali (2019), and Tsai and Su (2017) which are 0.219414 ms, 3.051965 ms and 0.274676 ms, respectively. However, slightly slower than Zheng and Imai (1998) and Hwang *et al.* (2005).

Table 4: Approximate running times of arithmetic and cryptographic operations

| Symbols | Operation | Arithmetic Mean (ms) | Standard Deviation (ms) |
|---|---|---|---|
| $T_{ECM}$ | Elliptic curve point multiplication | 0.024164 | 0.007812 |
| $T_{ECA}$ | Elliptic curve point addition | 0.0002355 | 0.0000619 |
| $T_{EXP}$ | Modular exponentiation | 2.873945 | 0.315294 |
| $T_{MM}$ | Modular multiplication | 0.001287 | 0.000226 |
| $T_{MA}$ | Modular addition | 0.000691 | 0.000315 |
| $T_{MI}$ | Modular inversion | 0.044861 | 0.006685 |
| $T_H$ | Hash (SHA-256) | 0.001209 | 0.002215 |
| $T_{sym}$ | Symmetry Encryption | 0.0286 | 0.0173 |

Table 5: Computational cost for executed operations in the proposed scheme and other similar schemes

| Signcryption Schemes | Sender Computational Cost | Receiver Computational Cost | Running Time |
|---|---|---|---|
| Our proposed scheme | $3T_{ECM}$+$1T_{sym}$ | $3T_{ECM}$+$1T_{sym}$ | $\approx 0.202184$ ms |
| Zheng and Imai (1998) | $2T_{MI}$+$1T_{ECM}$+$1T_{sym}$ | $2T_{ECM}$+$1T_{sym}$ | $\approx 0.174553$ ms |
| Hwang *et al*. (2005) | $2T_{ECM}$+$1T_{sym}$ | $3T_{ECM}$+$1T_{sym}$ | $\approx 0.17802$ ms |
| Tsai and Su (2017) | $5T_{ECM}$+$1T_{sym}$ | $4T_{ECM}$+$1T_{sym}$ | $\approx 0.274676$ ms |
| Bashir and Ali (2019) | $3T_{ECM}$+$1T_{sym}$+$1T_{EXP}$ | $2T_{ECM}$+$1T_{sym}$ | $\approx 3.051965$ ms |
| Zhang *et al*. (2022) | $1T_{ECM}$+$1T_{MI}$+$1T_{sym}$ | $2T_{ECM}$+$1T_{MI}$+$1T_{sym}$ | $\approx 0.219414$ ms |

$T_{ECM}$: Elliptic curve point multiplication operation, $T_{sym}$: Symmetric encryption/decryption operation, $T_{MI}$: Modular inversion, $T_{EXP}$: Modular exponentiation.

The proposed scheme achieves a strong balance between robust security properties and high computational efficiency. By eliminating modular exponentiation and relying solely on elliptic curve arithmetic, it significantly reduces execution time while maintaining resistance to known attacks. This makes it a strong candidate for lightweight secure communications in constrained environments.

## 6. Conclusion

In this work, we have presented a lightweight elliptic curve signcryption scheme designed to meet modern security demands without the complexity of certificate management, modular exponentiation, or pairing operations. Built on the well-established hardness of the Elliptic Curve Discrete Logarithm Problem (ECDLP), our scheme successfully delivers all essential security features: confidentiality, integrity, unforgeability, non-repudiation, forward secrecy, public verifiability, and protection against internal threats. By operating in a certificateless environment, it eliminates the overhead and vulnerabilities commonly associated with traditional public key infrastructures.

When compared with existing schemes, the proposed solution demonstrates both practical and theoretical strengths. It matches the security level of Hwang *et al.* (2005) while simplifying implementation by removing the need for certificates. Unlike Zhang *et al.* (2022), which lacks public verifiability, our scheme allows third parties to independently verify message authenticity, a valuable feature for transparent and accountable systems. It also addresses key limitations in earlier designs such as Zheng and Imai (1998), which do not offer forward secrecy or verifia-

bility, and Tsai and Su (2017), which miss both. Moreover, it improves on Bashir and Ali (2019) by achieving faster performance and offering better protection against private key compromise.

With a total computational cost of approximately 0.226 milliseconds, the scheme performs efficiently while maintaining strong security guarantees. This makes it particularly well-suited for real-world applications in resource-constrained settings, such as mobile platforms, IoT devices, and embedded systems.

Overall, the proposed signcryption scheme offers a well-balanced solution, secure, efficient, and practical for today's increasingly decentralized and lightweight environments.

## Acknowledgement

The authors thank Universiti Teknologi MARA Negeri Sembilan for providing financial support under the Staf Development Fund and the Universiti Kebangsaan Malaysia facilities. The authors also would like to thank the reviewers for the valuable comments for improvements to this paper.

## References

Al-Riyami S.S. & Paterson K.G. 2003. Certificateless public key cryptography. *Proceedings of the Advances in Cryptology—ASIACRYPT 2003*, pp. 452–473.

Baek J., Steinfeld R. & Zheng Y. 2007. Formal proofs for the security of signcryption. *Journal of Cryptology* **20**(2): 203–235.

Bashir M.Z.U. & Ali R. 2019. Cryptanalysis and improvement of blind signcryption scheme based on elliptic curve. *Electronics Letters* **55**(8): 457–459.

Cheng C.M., Kodera K., Miyaji A. & Okumura S. 2020. Cryptography core technology. In Miyaji A. & Mimoto T. (eds.). *Security Infrastructure Technology for Integrated Utilization of Big Data: Applied to the Living Safety and Medical Fields*: 5-33. Singapore: Springer.

Ho T.C., Tseng Y.M. & Huang S.S. 2024. Leakage-resilient hybrid signcryption in heterogeneous public-key systems. *Informatica* **35**(1): 131–154.

Hwang R.J., Lai C.H. & Su F.F. 2005. An efficient signcryption scheme with forward secrecy based on elliptic curve. *Appl. Math. Comput.* **167**(2): 870–881.

Koblitz N. 1987. Elliptic curve cryptosystems. *Mathematics of Computation* **48**(177): 203–209.

Kumar M. & Gupta P. 2019. An efficient and authentication signcryption scheme based on elliptic curves. *MATEMATIKA* **35**(1): 1–11.

Lu Y. & Li J. 2014. Efficient certificate-based signcryption secure against public key replacement attacks and insider attacks. *Scientific World Journal* **2014**: 295419.

Lynn B. 2022. PBC library - pairing based cryptography. https://crypto.stanford.edu/pbc/ (30 September 2024).

Miller V.S. 1986. Use of elliptic curves in cryptography. *Advances in Cryptology — CRYPTO '85 Proceedings*, pp. 417–426.

Mogollon M. 2007. *Cryptography and Security Services: Mechanisms and Applications*. Pennsylvania: CyberTech Publishing.

National Institute of Standards and Technology 2015. Secure Hash Standard (SHS) (FIPS PUB 180-4). *Tech. Rep.*. Information Technology Laboratory National Institute of Standards and Technology Gaithersburg, MD.

Nyberg K. & Rueppel R.A. 1996. Message recovery for signature schemes based on the discrete logarithm problem. *Designs, Codes and Cryptography* **7**: 61–81.

Ricci S., Dzurenda P., Hajny J. & Malina L. 2021. Privacy-enhancing group signcryption scheme. *IEEE Access* **9**: 136529–136551.

Shohaimay F. & Ismail E.S. 2023. Improved and provably secure ECC-based two-factor remote authentication scheme with session key agreement. *Mathematics* **11**(1): 5.

Singh S.R., Khan A.K. & Singh S.R. 2016. Performance evaluation of RSA and elliptic curve cryptography. *2016 2nd International Conference on Contemporary Computing and Informatics (IC3I)*, pp. 302–306.

Toorani M. & Beheshti A.A. 2009. An elliptic curve-based signcryption scheme with forward secrecy. *Journal of Applied Sciences* **9**(6): 1025–1035.

Toradmalle D., Muthukuru J. & Sathyanarayana B. 2019. Lightweight certificate less signcryption scheme based on elliptic curve. *International Journal of Innovative Technology and Exploring Engineering* **8**(10): 397–400.

Tsai C.H. & Su P.C. 2017. An ECC-based blind signcryption scheme for multiple digital documents. *Security and Communication Networks* **2017**: 8981606.

Tsai T.T., Tseng Y.M., Huang S.S., Xie J.Y. & Hung Y.H. 2022. Leakage-resilient anonymous multi-recipient signcryption under a continual leakage model. *IEEE Access* **10**: 104636–104648.

Wang X.a., Yang X. & Zhang J. 2010. Provable secure generalized signcryption. *Journal of Computers* **5**(5): 807–814.

Zhang P., Li Y. & Chi H. 2022. An elliptic curve signcryption scheme and its application. *Wireless Communications and Mobile Computing* **2022**(1): 7499836.

Zheng Y. 1997. Digital signcryption or how to achieve cost(signature & encryption) << cost(signature) + cost(encryption). *Proceedings of the Advances in Cryptology - CRYPTO '97, 17th Annual International Cryptology Conference*, pp. 165–179. Berlin, Heidelberg: Springer.

Zheng Y. & Imai H. 1998. How to construct efficient signcryption schemes on elliptic curves. *Information Processing Letters* **68**(5): 227–233.

*Department of Mathematical Sciences*
*Faculty of Science and Technology*
*Universiti Kebangsaan Malaysia*
*43600 UKM Bangi*
*Selangor, MALAYSIA*
*E-mail: esbi@ukm.edu.my*, p125360@ukm.edu.my*

*Department Mathematical Studies*
*Faculty of Computer and Mathematical Sciences*
*Universiti Teknologi MARA (UiTM) Negeri Sembilan, Seremban Campus*
*70300 Seremban*
*Negeri Sembilan, MALAYSIA*
*E-mail: nizam1558@uitm.edu.my*

Received: 6 June 2025
Accepted: 1 August 2025

*Corresponding author