A Lightweight Heterogeneous Signcryption Scheme Seamlessly Compatible for Multi-Infrastructure IoT Environments

Nimra Bari, Ghulam Abbas, *Senior Member, IEEE*, Abdul Waheed, Akhtar Badshah, Ziaul Haq Abbas, and Muhammad Waqas, *Senior Member, IEEE*

***Abstract*—The Internet of Things (IoT) interconnects vast numbers of sensors and devices that operate under different cryptographic infrastructures, making secure cross-domain communication essential. Most existing signcryption schemes are designed for a single infrastructure or, at best, two fixed ones, which limits applicability in heterogeneous and evolving IoT deployments. To address this need, we introduce LH3SC, a seamless elliptic-curve heterogeneous signcryption scheme that supports three infrastructures: certificateless cryptography, public key infrastructure, and identity-based cryptography, with a CLC sender. LH3SC enables devices across these domains to communicate securely without major architectural changes. The security analysis establishes IND-CCA2 confidentiality and EUF-CMA unforgeability, and the performance evaluation demonstrates lower computation and communication costs than representative schemes. These properties make LH3SC suitable for resource-constrained IoT settings, including healthcare automation, smart grids, and other distributed systems that require seamless cross-domain security.**

***Index Terms*—Certificateless Cryptography, Elliptic Curve Cryptography, Identity-based Cryptography, Public Key Infrastructure, Signcryption, Seamless Communication.**

I. Introduction

A. Motivation

The Internet of Things (IoT) is reshaping everyday life through a vast mesh of interconnected entities, including sensors, devices, gateways, and cloud servers, that often operate under different security infrastructures and trust domains [1]–[3]. This decentralization, combined with diverse communication protocols, exposes IoT deployments to significant security and privacy risks, including data breaches and unauthorized access [4]–[6]. To ensure secure communication, cryptographic mechanisms are essential. The three primary infrastructures are: public key infrastructure (PKI) [7], [8], which relies on a certificate authority (CA) but introduces management challenges; identity-based cryptography (IBC) [9], [10], which eliminates certificates but suffers from the key escrow problem; and certificateless cryptography (CLC) [11], which addresses these limitations but remains vulnerable to insider attacks due to its dependence on a semi-trusted key generation center (KGC). Early research focused on achieving efficient and simple homogeneous signcryption schemes [12]–[20], mostly based on a single cryptographic framework. These schemes apply to a closed environment where all devices belong to the same security domain. This approach is limited because it cannot support the diversity and multi-vendor nature of the modern IoT world, where devices from distinct domains must be able to communicate with each other. To address this limitation, heterogeneous signcryption performs a crucial role [13], [21]–[23] in supporting the quality and safety of communication in two distinct cryptographic infrastructures. Despite this progress, most existing heterogeneous solutions are developed for a fixed number of infrastructures, which restricts scalability and prevents seamless integration of new devices employing other cryptographic schemes. In real-world IoT environments, the different types of infrastructures usually accommodate various types of nodes. For example, CLC environments typically use lightweight sensors and wearables [14]–[16]. However, resource-rich systems in automotive and business devices typically use PKI [17], [18], and identity-oriented systems like healthcare IoT and telecom use IBC [19], [20].

Consequently, infrastructures such as CLC, PKI, and IBC often operate side by side in the same environment and are required to interoperate securely [24]. However, most existing solutions do not provide truly seamless cross-infrastructure interoperability, particularly in scenarios involving resource-constrained devices.

To overcome this limitation, we propose a lightweight heterogeneous signcryption model that enables secure and efficient communication across multiple cryptographic infrastructures. The key challenge lies in striking an appropriate balance between security and efficiency. Stronger security guarantees typically introduce additional computational and communication overhead, which may be unsuitable for IoT and WBAN gateways with limited resources. On the other hand, overly lightweight designs may weaken resistance against adaptive attacks. These practical trade-offs form the foundation and motivation for the balanced framework presented in this work.

N. Bari is with the Faculty of Computer Science and Engineering, GIK Institute of Engineering Sciences and Technology, Topi 23640, Pakistan (email:nimra.bari@giki.edu.pk).

G. Abbas and Z. H. Abbas are with Telecommunications and Networking (TeleCoN) Research Center, GIK Institute of Engineering Sciences and Technology, Topi 23640, Pakistan (e-mail:abbasg@giki.edu.pk, ziaul.h.abbas@giki.edu.pk).

A. Waheed is with the Department of Computer Science, CECOS University of IT and Emerging Sciences, Hayatabad, Peshawar 25000, Pakistan (e-mail: abdul@netlab.snu.ac.kr).

A. Badshah is with the Department of Software Engineering, University of Malakand, Dir Lower 18800, Pakistan (e-mail: akhtarbadshah@uom.edu.pk).

M. Waqas is with the School of Computing and Mathematical Sciences, Faculty of Engineering and Science, University of Greenwich, United Kingdom (e-mail: engr.waqas2079@gmail.com).

(Corresponding author: Abdul Waheed and Muhammad Waqas.)

B. Novelty and Contributions

In this work, we present LH3SC, an elliptic-curve-based heterogeneous signcryption framework that enables secure communication across three major cryptographic infrastructures, CLC, PKI, and IBC, within a unified design. The key contributions of this paper are summarized as follows:

- First, we develop a seamless ECC-based heterogeneous signcryption scheme in which a CLC sender can securely communicate with receivers in CLC, PKI, or IBC environments, removing fixed-pair limitations of prior heterogeneous constructions.
- Second, by integrating CLC, PKI, and IBC into a single coherent framework (with a CLC sender), the proposed design supports practical cross-domain deployment in heterogeneous IoT ecosystems (e.g., smart grids and healthcare systems) where different trust models coexist.
- Third, we formally prove the security of the proposed LH3SC scheme, establishing EUF-CMA unforgeability under the ECDLP assumption and IND-CCA2 confidentiality under the ECCDH assumption within the defined adversarial model.
- Finally, we thoroughly evaluate the LH3SC scheme, and the results show that it outperforms representative schemes in computation and communication costs.

C. Paper Organization

The remainder of this article is organized as follows. The related work is provided in Section II. Section III briefly describes the necessary cryptographic background and preliminaries. In Section IV, we define the security model adopted in this work. The proposed LH3SC scheme is then detailed in Section V. A comprehensive security analysis is presented in Section VI, followed by performance evaluation and comparative analysis in Section VII. Finally, this article is concluded in Section VIII.

II. Related Work

Recent years have seen many signcryption schemes tailored to different cryptographic infrastructures. These efforts generally fall into two groups: homogeneous schemes that stay within one cryptographic setting, and heterogeneous schemes that enable communication across different infrastructures. We next review representative work from both categories.

A. Homogeneous Signcryption

Homogeneous signcryption schemes focus on secure communication within the same cryptographic framework, optimizing a single infrastructure for improved performance and security [25], [26]. The authors in [27] proposed a CLC-based homogeneous signcryption scheme for the Internet of Health Things (IoHT) using hyperelliptic curve cryptography (HECC). Similarly, Kasyoka *et al.* [28] introduced a secure, pairing-free CLC-based signcryption scheme for healthcare systems. For edge computing-based VANETs, Yang *et al.* [29] presented a pairing-free CLC-based online-offline signcryption scheme with batch verification. A multimode CLC-based ring signcryption scheme was proposed by Zhan *et al.* [30], and a certificateless aggregate signcryption scheme was introduced in [12].

Several homogeneous methods aim to maximize security and efficiency within a single infrastructure. Li *et al.* [31] proposed a pairing-free certificateless signcryption scheme that dynamically generated a self-generation mechanism to reduce computational overhead. Similarly, Rao *et al.* [32] developed a lightweight certificateless aggregate signcryption scheme for IIoT, without the expensive bilinear pairing operations. To ensure high security, Wu *et al.* [33] introduced a certificateless batch-verifying signcryption for vehicle-to-vehicle (V2V) communications. Gong *et al.* [34] proposed SLIM, a multi-authority attribute-based signcryption scheme that transfers the majority of the calculations to an edge server, minimizing costs for IoT devices. [35] The authors presented a certificate-based signcryption based on HECC to overcome key escrow and key distribution problems in IIoT. Kuang *et al.* [36] designed a signcryption signature scheme with a policy based on attributes of the ciphertext. Signcryption with an equality test for zero-trust IoT frameworks, enabling secure data comparison without decryption [37], [38].

B. Heterogeneous Signcryption

Heterogeneous signcryption schemes enable secure communication across various cryptographic infrastructures, which is crucial for interoperability in complex environments, such as the Internet of Vehicles (IoV) and the Industrial Internet of Things (IIoT) [39], [40].

Some researchers have proposed CLC-to-PKI signcryption schemes. Ali *et al.* [41] introduced a CLC–PKI hybrid encryption scheme based on bilinear pairings and batch unsigncryption, allowing vehicles to verify a range of messages at the same time. Ali *et al.* [42] also proposed a fog computing-based CLC–PKI signcryption scheme for IoV. Chen *et al.* [43] proposed a CLC–PKI signcryption scheme for secure communication, while Niu *et al.* [23] proposed two heterogeneous schemes for 5G network slices. Tseng *et al.* [22] proposed a CLC-to-PKI scheme with constant decryption complexity PKI scheme, which is appropriate for resource-constrained IoT devices.

Cao *et al.* [44] introduced a CLC-to-IBC online-offline heterogeneous signcryption scheme with public verification to trace malicious activity. Jin *et al.* [21] proposed a CLC-to-IBC heterogeneous signcryption scheme for IIoT, and Jin *et al.* [45] developed an online-offline CLC-to-IBC signcryption scheme to reduce online computation overhead. Yu *et al.* [46] presented a lattice-based bidirectional heterogeneous signcryption scheme for IBC-to-CLC communication using hash functions and matrix operations.

Xie *et al.* [47] proposed an IBC-to-CLC signcryption scheme for IIoT. To facilitate secure CLC— PKI communication, the authors of [48] developed a hyperelliptic curve-based heterogeneous signcryption scheme for IoT. Yang *et al.* [49] introduced a heterogeneous multi-receiver aggregate signcryption scheme for PKI-to-CLC infrastructure, reducing computational load on vehicles and improving edge node efficiency. Brown *et al.* [50] proposed a CLC-to-IBC

This article has been accepted for publication in IEEE Internet of Things Journal. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/JIOT.2026.3679417

TABLE I
COMPARATIVE ANALYSIS OF HOMOGENEOUS AND HETEROGENEOUS SIGNCRYPTION SCHEMES

Reference	Contribution	Cryptographic Technique	Challenges / Limitations
Homogeneous Signcryption Schemes			
Rao et al. [32]	Lightweight IIoT aggregate signcryption	CLC	Low-resource limitation
Wu et al. [33]	Batch-verifying V2V signcryption	CLC	Batch computation overhead
Zhan et al. [30]	Multimode ring signcryption	CLC	Ring operation complexity
Gong et al. [34]	Multi-authority IoT signcryption (SLIM)	CLC	Edge dependency
Ullah et al. [35]	HECC certificate-based signcryption	Certificate-based	Key distribution issues
Kuang et al. [36]	Attribute-based equality-test signcryption	CLC	Equality test overhead
Ullah et al. [27]	Anonymous IoHT signcryption	CLC	High computation
Li et al. [31]	Streamlined smart terminal signcryption	CLC	Limited flexibility
Yang et al. [49]	Online/offline VANET signcryption	CLC	Edge processing cost
Kasyoka et al. [50]	Efficient WSN signcryption	CLC	Sensor overhead
Heterogeneous Signcryption Schemes			
Chen et al. [43]	Online/offline IoV signcryption	CLC + PKI	Resource-constrained nodes
Cao et al. [44]	Offline/online VANET signcryption	CLC + PKI	Edge computation
Jin et al. [45]	IoT online/offline signcryption	CLC + PKI	Computation overhead
Ali et al. [42]	CLC-PKI fog computing IoV	CLC + PKI	Edge overhead
Yu et al. [46]	Lattice-based network signcryption	Lattice + CLC	Matrix operation cost
Xie et al. [47]	IBC-CLC multi-receiver IoT signcryption	IBC + CLC	Computation overhead
Ullah et al. [48]	Access control IoT signcryption	CLC + PKI	Verification cost
Yang et al. [49]	Efficient VANET mutual signcryption	CLC + PKI	limited flexibility
Brown et al. [50]	CLC-to-IBC WSN signcryption	CLC + IBC	Scalability issues
Jiao et al. [51]	Lattice-based VANET signcryption	Lattice + CLC	High computation
Yang et al. [52]	PKI-to-IBC equality test IoV	PKI + IBC	Equality test cost
Jin et al. [53]	CLC-to-PKI equality test IoV	CLC + PKI	Verification/blockchain cost

Note: CLC = Certificateless Cryptography, IBC = Identity-Based Cryptography, PKI = Public Key Infrastructure, Lattice = Lattice-based Cryptography.

scheme based on the bilinear Diffie—Hellman assumption and the ROM for secure channels.

Finally, several advanced heterogeneous schemes focus on additional features and compatibility, such as Jiao *et al.* [51] proposed a lattice-based heterogeneous CLC-to-IBC signcryption scheme for secure bidirectional vehicular communication. Yang *et al.* [52] introduced a PKI-to-IBC communication architecture for IoV, enabling multi-ciphertext equality checking. Jin *et al.* [53] presented a heterogeneous signcryption scheme with equality testing and blockchain integration, allowing a cloud server to verify ciphertext equality without decryption for enhanced security and reliability.

Current heterogeneous signcryption systems have multiple practical shortcomings, such as being based on bilinear pairings, having limited interoperability, not usually being larger than two cryptographic infrastructures, and not fully supporting public verifiability and forward secrecy security properties. In contrast to these schemes, the given LH3SC scheme does not rely on bilinear pairings to minimize the computational cost and allows unified and smooth communication between the CLC, PKI, and IBC environments under the same signcryption system without altering the native forms of key management, while providing security.

III. PRELIMINARIES

A. Network Model

The LH3SC scheme operates in a heterogeneous IoT environment, as shown in Fig. 1. It consists of three main

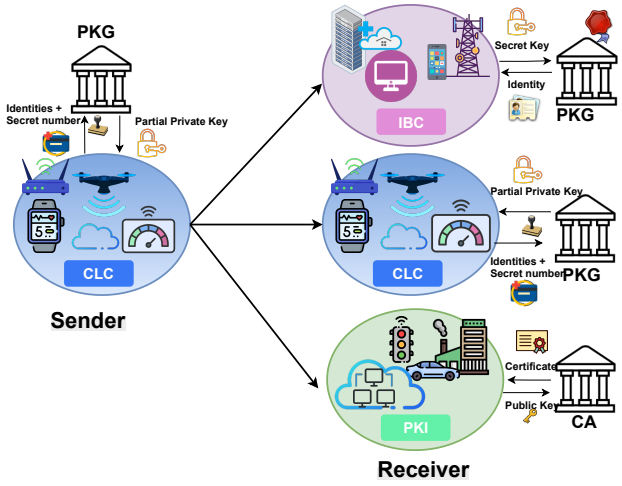

Fig. 1. Network model of the proposed LH3SC scheme

entities: a sender, a receiver, and a trusted authority (TA). The TA initializes and maintains the master secret key and the corresponding public key, acting as a Key Generation Center (KGC) or a Registration Authority (RA). The sender is a resource-constrained IoT device within the CLC infrastructure that generates keys and performs signcryption, while the receiver can belong to the CLC, PKI, or IBC infrastructure. Each cryptographic infrastructure is managed by its own trusted authority, and these authorities function independently of one another. It has no centralized global authority managing

all domains, and it is more realistic as a multi-domain trust environment, associated with heterogeneous deployments of IoT. In this context, a sender who uses a CLC-based system can signcrypt information safely on behalf of a receiver who is a part of another cryptographic infrastructure. This design allows to provide easy inter-operability and flexible and cross-infrastructure communication without interfering with security.

B. Elliptic Curve Cryptography

Elliptic Curve Cryptography (ECC) is a lightweight and secure public-key cryptosystem defined over a finite field $\mathbb{F}_q$, where q is a prime Number. An elliptic curve E over $\mathbb{F}_q$ is defined in Equation (1):

$$y^2 \equiv x^3 + ax + b \pmod{q}, \quad a, b \in \mathbb{F}_q \tag{1}$$

with the points on E, along with the point at infinity O, forming an additive cyclic group $\mathbb{G}$ of prime order q. Each entity selects a private key $u \in \mathbb{Z}_q^*$ and computes the corresponding public key $U = uP$, where P is a generator of $\mathbb{G}$ [27], [29].

The security of ECC depends on the computational hardness of several well-known mathematical problems:

Definition 1 (elliptic curve discrete logarithm problem (ECDLP))**.** *Given two points P and $U = uP$ in $\mathbb{G}$, with $u \in \mathbb{Z}_q^*$, the ECDLP states that it is computationally impossible to compute u, i.e., the discrete logarithm of U to the base P.*

Definition 2 (elliptic curve computational Diffie-Hellman problem (ECCDH))**.** *Given P, $U = uP$, and $V = vP$ in $\mathbb{G}$, where $u, v \in \mathbb{Z}_q^*$, the ECCDH problem consists of computing in Equation (2).*

$$C = uvP. \tag{2}$$

Definition 3 (gap elliptic curve computational Diffie–Hellman problem (Gap-ECCDH))**.** *same as ECCDH, but when the adversary is provided with access to a Decisional Diffie-Hellman (DDH) oracle that, on input (P, A, B, C), decides whether $C = abP$.*

Definition 4 (Elliptic Curve Decision Diffie–Hellman Problem (ECDDH))**.** *Let P be a generator of a cyclic group $\mathbb{G}$ of prime order q, and let $U = uP$ and $V = vP$ be public keys corresponding to private keys $u, v \in \mathbb{Z}_q^*$. The ECDDH problem is to determine whether a given point $C \in \mathbb{G}$ is the valid shared secret uvP or a randomly chosen element $C' \in \mathbb{G}$:*

$$(P, U, V, C = uvP) \quad vs. \quad (P, U, V, C'),$$

where C' is uniformly sampled from $\mathbb{G}$.

C. Security Requirements

The LH3SC scheme is designed to meet the following security and operational requirements:

- Message confidentiality: The plaintext is hidden from unauthorized parties.
- Message authentication: The receiver can verify the sender's claimed identity.
- Message integrity: Any modification, insertion, or deletion of content is detectable.
- Non-repudiation: The sender cannot deny generating a valid signcrypted message.
- Unforgeability: An adversary cannot produce a valid signcryption without the sender's secret key.
- Public verifiability: Third parties can verify authenticity without the sender's private key.
- Resistance to common attacks: The design mitigates impersonation, message modification, and man-in-the-middle attacks.
- Replay protection: Freshness is enforced via timestamps (resolution ≤ 1 ms) to prevent reuse.
- Forward secrecy: Past session keys remain secure even if long-term keys are compromised.

IV. Security Model

LH3SC security relies on two core goals: confidentiality and unforgeability. We model three types of adversaries to reflect different threat scenarios. The sender operates in a CLC environment, while the receiver may be in PKI, IBC, or CLC.

Consider an additive cyclic group $\mathbb{G}$ of prime order q generated by P, where the ECDLP is assumed to be hard.

Type-I Adversary ($\mathcal{A}_I$): Does not know the master secret key but can substitute the user's public key in the system.

Type-II Adversary ($\mathcal{A}_{II}$): Knows the master secret key but cannot substitute or modify public keys.

The confidentiality game (IND-CCA2) can be played against an adversary with either Type-I or Type-II capabilities. The specific restrictions for each adversary type within the confidentiality game are described in game 02.

Game 01: Unforgeability against a Type-I Adversary ($\mathcal{A}_I$)

This game models EUF-CMA for an adversary who can substitute public keys.

Setup: The challenger $\mathcal{C}$ uses security parameter ℓ to generate the parameters of system params, which include the master public key M_{pub}. $\mathcal{C}$ gives params to $\mathcal{A}_I$. $\mathcal{C}$ also generates a key pair for the target receiver, which may be from PKI, IBC, or CLC, denoted as $(R_{\text{pub}}, R_{\text{pri}})$. The adversary $\mathcal{A}_I$ is given R_{pri}.

Query Phase: The adversary $\mathcal{A}_I$ is allowed to adaptively issue the following queries:

- Private Key Query $(\mathcal{Q}_{pri})$: For any identity except the target sender identity ID_S^*.
- Public Key Query $(\mathcal{Q}_{pub})$: For any identity.
- Public Key Replacement Query: Allowed for any identity.
- Signcryption Query $(\mathcal{Q}_{sc})$: For any tuple $(m, ID_S, R_{\text{pub}})$, the challenger returns a valid signcryption σ.
- Unsigncryption Query $(\mathcal{Q}_{usc})$: Allowed for any ciphertext.

Forgery: The adversary $\mathcal{A}_I$ outputs a forgery $(\sigma^*, ID_S^*, R_{\text{pub}}^*)$ and wins the game if:

1) $\mathsf{Unsigncrypt}(\sigma^*, R_{\text{pri}}, S_{\text{pri}}^*)$ outputs a valid message m^*;
2) $\mathcal{A}_I$ did not query the private key for ID_S^*;
3) $\mathcal{A}_I$ did not query the signcryption oracle for the pair (m^*, ID_S^*).

Game 02: Unforgeability against a Type-II Adversary ($\mathcal{A}_{II}$)

This game models EUF-CMA for an adversary who knows the master secret key.

Setup: The challenger $\mathcal{C}$ runs the setup algorithm, gives params and the master secret key M_{sec} to $\mathcal{A}_{II}$. $\mathcal{C}$ also generates the receiver's key pair $(R_{\text{pub}}, R_{\text{pri}})$. The adversary $\mathcal{A}_{II}$ is given R_{pri}.

Query Phase: $\mathcal{A}_{II}$ can adaptively issue the following queries:

- Private Key Query $(\mathcal{Q}_{pri})$: Allowed for any user identity ID except the target sender identity ID_S^*.
- Public Key Query $(\mathcal{Q}_{pub})$: Allowed for any identity.
- Signcryption Query $(\mathcal{Q}_{sc})$: For $(m, ID_S, R_{\text{pub}})$, $\mathcal{C}$ returns a valid signcryption σ.
- Unsigncryption Query $(\mathcal{Q}_{usc})$: Allowed for any ciphertext.

Restriction: $\mathcal{A}_{II}$ is not allowed to substitute public keys.

Forgery: $\mathcal{A}_{II}$ outputs a forgery $(\sigma^*, ID_S^*, R_{\text{pub}})$. $\mathcal{A}_{II}$ wins if:

1) $\mathsf{Unsigncrypt}(\sigma^*, R_{\text{pri}}, S_{\text{pri}^*})$ returns a valid message m^*.
2) $\mathcal{A}_{II}$ did not query the private key for ID_S^*.
3) $\mathcal{A}_{II}$ did not query the signcryption oracle for the pair (m^*, ID_S^*).

Definition 5. *The scheme is EUF-CMA secure against a Type-II adversary if, for any PPT adversary$\mathcal{A}_I$ and $\mathcal{A}_{II}$, the advantage is shown in Equation (3) is negligible.*

$$\mathbf{Adv}_{\mathcal{A}_{II}}^{EUF\text{-}CMA}(\ell) = \Pr[\mathcal{A}_{II} \text{ wins Game 01}] \tag{3}$$

Game 03: IND-CCA2 Confidentiality Resistance against an Adversary with Type-I or Type-II Capabilities

This game ensures semantic security under the adaptive IND-CCA2 security model. The adversary, denoted $\mathcal{A}$, can be instantiated with either Type-I or Type-II capabilities.

Setup: The challenger $\mathcal{C}$ runs the setup algorithm and gives params to $\mathcal{A}$. If $\mathcal{A}$ is a Type-II adversary, $\mathcal{C}$ also provides the master secret key M_{sec}. $\mathcal{C}$ generates a key pair for the target sender $(S_{\text{pub}}, S_{\text{pri}})$ and the target receiver $(R_{\text{pub}}, R_{\text{pri}})$, where the receiver will be from PKI, IBC, or CLC. Crucially, R_{pri} is NOT given to $\mathcal{A}$.

Phase 1: $\mathcal{A}$ may issue queries adaptively:

- Private Key Query $(\mathcal{Q}_{pri})$: Allowed for any user identity ID except the target receiver ID_R.
- Public Key Query $(\mathcal{Q}_{pub})$: Allowed for any identity.
- Public Key Replacement $(\mathcal{Q}_{pubR})$: Only allowed if $\mathcal{A}$ has Type-I capabilities. The adversary may substitute any public key except the target receiver's public key R_{pub}.
- Signcryption Query $(\mathcal{Q}_{sc})$: For $(m, ID_S, R_{\text{pub}^*})$, $\mathcal{C}$ returns a valid signcryption σ.
- Unsigncryption Query $(\mathcal{Q}_{usc})$: For any ciphertext σ under R_{pub} except the future challenge ciphertext σ^*.

Challenge: $\mathcal{A}$ submits two messages (m_0, m_1) fo same size and the sender's identity ID_S. $\mathcal{C}$ randomly picks a bit $b \in \{0, 1\}$, signcrypts m_b using S_{pri} and R_{pub} to generate the challenge ciphertext σ^*, and returns σ^* to $\mathcal{A}$.

Phase 2: $\mathcal{A}$ can continue to issue queries as in Phase 1, subject to the following restrictions:

TABLE II
NOTATIONS USED IN THE LH3SC SCHEME

Symbol	Description
B, C	Ephemeral ECC public key, shared secret
C_{add}	Cyclic additive ECC group
H_1, H_2, H_3	Hash functions
ID_I, ID_C, ID_P	Identities in IBC, CLC, PKI
$ID_{\text{S}}, ID_{\text{R}}$	Identity of sender/receiver
$I_{\text{pri/pub}}, C_{\text{pri/pub}}, P_{\text{pri/pub}}$	Private/public keys in IBC, CLC, PKI
K	Symmetric session key
$M_{\text{sec}}, M_{\text{pub}}$	Master secret/public key
m, t	Plaintext IoT data, timestamp
$P, q, \mathbb{Z}_q^*$	Generator point, group order, multiplicative group
P_{ars}	Partial key
RA, KGC	Registration authority, key generation center
$R_{\text{pri}}, R_{\text{pub}}$	Receiver's private/public key
$S_{\text{pri}}, S_{\text{pub}}$	Sender's private/public key
X, L, σ	Masked message, signature, ciphertext
$\vartheta, \perp$	Authentication tag, invalid output

- It cannot query the private key of ID_R.
- It is not allowed to make an unsigncryption query for the challenge ciphertext σ^* under the target receiver's key R_{pub}.
- If $\mathcal{A}$ has Type-I capabilities, it cannot substitute the public key R_{pub} at any point during the game (Phase 1 or Phase 2).

Guess: $\mathcal{A}$ outputs a guess $b' \in \{0, 1\}$. The advantage of the adversary is defined as in Equation (4):

$$\mathbf{Adv}_{\mathcal{A}}^{\text{IND-CCA2}}(\ell) = \left|2 \cdot \Pr[b' = b] - 1\right|. \tag{4}$$

Definition 6. *The scheme is IND-CCA2 secure if for any PPT adversary $\mathcal{A}$ (with either Type-I or Type-II capabilities), the advantage $\mathbf{Adv}_{\mathcal{A}}^{IND\text{-}CCA2}(\ell)$ is negligible.*

In Game 01 and Game 02 (unforgeability), the adversary is assumed to possess the receiver's private key R_{pri}, and the objective is to validate the authenticity of the message. In contrast, in Game 03 (confidentiality), the adversary does not have access to R_{pri}, and the goal is to ensure that the message content remains secret.

V. Proposed Scheme

This section introduced the LH3SC scheme, which is constructed using ECC and integrates three distinct infrastructures: CLC, PKI, and IBC. The notations employed throughout the scheme are summarized in Table II. The scheme is mainly divided into phases, namely, Setup, Public/Private Key Generation, Signcryption, and Unsigncryption. as illustrated in Fig. 2.

A. Setup Phase

In the initialization phase, the RA or KGC selects a master secret key $M_{\text{sec}} \in \mathbb{Z}_q^*$ and computes the master public key as

$$M_{\text{pub}} = M_{\text{sec}} \cdot P$$

where P is the generator of the additive cyclic group C_{add} defined over the elliptic curve. Here, M_{sec} must remain strictly

This article has been accepted for publication in IEEE Internet of Things Journal. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/JIOT.2026.3679417

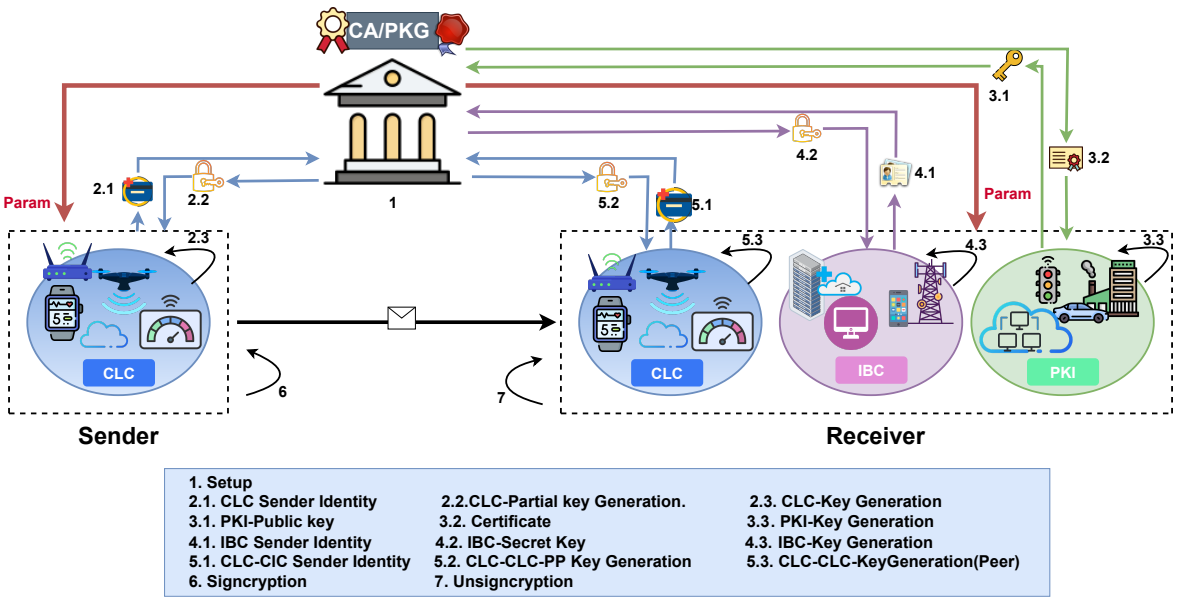

Fig. 2. Architecture of the LH3SC scheme.

confidential, while M_{pub} is made publicly available.

The RA/KGC then sets and publishes the global system parameters in (5):

$$\text{params} = (H_1, H_2, H_3, q, P, M_{\text{pub}}) \tag{5}$$

where H_1, H_2, and H_3 are secure one-way hash functions modeled as random oracles. All three infrastructures (CLC, PKI, and IBC) use these parameters as the basis for key generation and subsequent cryptographic operations.

B. CLC Key Generation

In the CLC setting, the RA issues each user a partial private key derived from the user's identity. For a sender with identity ID_C, the RA computes

$$P_{ars} = H_1(ID_C \| M_{\text{sec}}) \pmod q,$$

where $P_{ars} \in \mathbb{Z}_q^*$. This binds the partial key to both the user identity and the RA's master key.

The RA sends P_{ars} securely to the user, who then selects an independent random secret $\gamma_s \in \mathbb{Z}_q^*$ to limit the impact of RA compromise. The complete private and public keys are computed as in (6):

$$C_{\text{pri}} = (P_{ars} + \gamma_s) \bmod q, \quad C_{\text{pub}} = C_{\text{pri}} \cdot P. \tag{6}$$

Thus, the full key pair $(C_{\text{pri}}, C_{\text{pub}})$ combines RA-issued and user-chosen randomness, reducing key escrow risk.

C. PKI Key Generation

In the PKI setting, each node generates its own key pair. It picks a random scalar $\partial \in \mathbb{Z}_q^*$ and computes, as in (7),

$$P_{\text{pri}} = \partial, \quad P_{\text{pub}} = \partial \cdot P. \tag{7}$$

The public key P_{pub} is then certified by the RA acting as a certification authority (CA). This certificate links the key to the node's identity and helps prevent impersonation and man-in-the-middle (MITM) attacks.

D. IBC Key Generation

In the IBC setting, user identities map directly to public key material. For a node with identity ID_I, the KGC first evaluates

$$h_g = H_1(ID_I) \in \mathbb{Z}_q^*.$$

Using this value, the private key is computed as

$$I_{\text{pri}} = M_{\text{sec}} \cdot h_g,$$

The public key is obtained as

$$I_{\text{pub}} = h_g \cdot M_{\text{pub}}.$$

Since $M_{\text{pub}} = M_{\text{sec}} \cdot P$, the pair can also be expressed compactly as in Equation (8)

$$I_{\text{pri}} = M_{\text{sec}} \cdot H_1(ID_I), \quad I_{\text{pub}} = H_1(ID_I) \cdot M_{\text{pub}}. \tag{8}$$

This approach removes the need for certificates, but it introduces inherent key escrow because the KGC holds the master secret key and can therefore reconstruct any user's private key.

E. Signcryption

In the signcryption phase, the sender encrypts and authenticates a message m using its private key C_{pri}, the receiver's public key R_{pub}, and a timestamp t. For freshness, the sender first samples a random scalar $\alpha \in \mathbb{Z}_q^*$ and computes:

$$B = \alpha \cdot P.$$

Using the receiver's public key, the shared secret is established as

$$C = \alpha \cdot R_{\text{pub}},$$

where R_{pub} represents P_{pub}, I_{pub}, or C_{pub} in the PKI, IBC, and CLC settings, respectively. The session key is then derived by hashing the pair (C, B) as

$$K = H_2(C \,\|\, B).$$

Because R_{pub} varies by receiver and α is fresh each time, the session key K (and the tag ϑ below) is unique per session, supporting confidentiality, integrity, and

non-repudiation across sessions. Although the long-term infrastructure keys remain static in PKI, CLC, and IBC, the per-session randomness α ensures session-key freshness and limits the impact of key compromise, offering weak forward secrecy against long-term key exposure. The plaintext is then masked with the session key:

$$X = m \oplus K.$$

To ensure integrity and authenticity, the sender computes the tag as

$$\vartheta = H_3(X \,\|\, ID_C \,\|\, ID_R \,\|\, C_{\text{pub}} \,\|\, R_{\text{pub}} \,\|\, B \,\|\, t),$$

which cryptographically binds the message, sender identity, and session parameters. Finally, the signature component is computed as

$$L = (\vartheta \cdot C_{\text{pri}} + \alpha) \bmod q.$$

The complete ciphertext is therefore expressed in Equation (9).

$$\sigma = (\vartheta, X, L, B, t). \tag{9}$$

F. Unsigncryption

During unsigncryption, the receiver recovers the plaintext and checks authenticity from the ciphertext $\sigma = (X, L, B, t)$. It first derives the shared secret using its private key R_{pri} and the received value B, as follows.

$$C' = P_{\text{pri}} \cdot B \quad \text{(PKI)}, \quad C' = I_{\text{pri}} \cdot B \quad \text{(IBC)},$$

$$C' = C_{\text{pri}} \cdot B \quad \text{(CLC)}.$$

Using (C', B), the session key is reconstructed as

$$K = H_2(C' \,\|\, B).$$

The original message is then obtained as

$$m = X \oplus K.$$

For integrity checking, the receiver recomputes

$$\vartheta = H_3(X \,\|\, ID_C \,\|\, ID_R \,\|\, C_{\text{pub}} \,\|\, R_{\text{pub}} \,\|\, B \,\|\, t),$$

and checks the correctness condition in Equation (10).

$$L \cdot P \stackrel{?}{=} \vartheta \cdot C_{\text{pub}} + B. \tag{10}$$

If the equality holds, the message is accepted; otherwise, the receiver outputs $\perp$, indicating an authentication or integrity failure.

G. Consistency Proof

The correctness of the LH3SC scheme is demonstrated through two properties: (1) consistency of the derived symmetric key between sender and receiver, and (2) correctness of the signature verification equation. We prove both for all communication modes: CLC-CLC, CLC-PKI, and CLC-IBC.

Assumption: All operations are performed in the additive cyclic group C_{add} defined over the elliptic curve, where scalar multiplication is commutative.

1) Symmetric Key Consistency

Let $\alpha \in \mathbb{Z}_q^*$ be a randomly selected ephemeral secret by the sender and $B = \alpha P$ be the ephemeral public key.

a) Case 1: CLC-CLC

The sender computes the shared secret $C = \alpha \cdot C_{\text{pub}}$. The receiver computes:

$$C' = C_{\text{pri}} \cdot B = (C_{\text{pri}} \bmod q) \cdot (\alpha P) = \alpha (C_{\text{pri}} \cdot P) = \alpha \cdot C_{\text{pub}} = C$$

Thus, both derive the same symmetric key $K = H_2(C \,\|\, B)$.

b) Case 2: CLC-PKI

The sender computes:

$$C = \alpha \cdot P_{\text{pub}} = \alpha \cdot (P_{\text{pri}} \cdot P)$$

The receiver computes:

$$C' = P_{\text{pri}} \cdot B = P_{\text{pri}} \cdot (\alpha \cdot P) = \alpha \cdot (P_{\text{pri}} \cdot P) = C$$

Hence, $K = H_2(C \,\|\, B)$ is consistent.

c) Case 3: CLC-IBC

The sender computes:

$$C = \alpha \cdot I_{\text{pub}} = \alpha \cdot (H_1(ID_I) \cdot M_{\text{pub}})$$

The receiver computes:

$$\begin{aligned} C' &= I_{\text{pri}} \cdot B = (M_{\text{sec}} \cdot H_1(ID_I)) \cdot (\alpha \cdot P) \\ &= \alpha \cdot H_1(ID_I) \cdot (M_{\text{sec}} \cdot P) \quad \text{(by commutativity)} \\ &= \alpha \cdot H_1(ID_I) \cdot M_{\text{pub}} = C \end{aligned}$$

Thus, $C = C'$ and key derivation are consistent.

2) Signature Correctness

Let ϑ be the hash-based authentication tag. The sender generates the signature:

$$L = (\vartheta \cdot C_{\text{pri}} + \alpha) \bmod q$$

The receiver verifies the signature using the equation.

$$L \cdot P \stackrel{?}{=} \vartheta \cdot C_{\text{pub}} + B$$

Expanding the left-hand side

$$L \cdot P = (\vartheta \cdot C_{\text{pri}} + \alpha) \cdot P = \vartheta \cdot (C_{\text{pri}} \cdot P) + \alpha \cdot P = \vartheta \cdot C_{\text{pub}} + B$$

This confirms that the signature verification equation holds for all communication types.

VI. Security Analysis

The LH3SC scheme is designed for lightweight deployment in heterogeneous IoT environments. Accordingly, we analyze security in the random-oracle model (ROM), a standard assumption for resource-constrained IoT and WBAN signcryption. The reductions show EUF-CMA security against Type-I/Type-II adversaries and IND-CCA2 security (Section IV) under standard elliptic-curve hardness assumptions. The proofs are not claimed to be tight in the standard model, reflecting the typical trade-off between rigorous reductions and efficiency in lightweight heterogeneous signcryption.

A. Formal Security Analysis

Theorem 1 (EUF-CMA Security against Type-I Adversary)**.** *If the ECDLP is hard in $\mathbb{G}$, then in the ROM, the proposed scheme is EUF-CMA secure against any Type-I adversary $\mathcal{A}_I$. Specifically, if $\mathcal{A}_I$ forges a valid signcryption with advantage ϵ after making $\mathcal{Q}_{H_i}$ hash queries and $\mathcal{Q}_{sc}$ signcryption queries, then the reduction algorithm $\mathcal{C}$ solves ECDLP with advantage at least $\frac{\epsilon}{\mathcal{Q}_{ID}\mathcal{Q}_{H_3}}$, where $\mathcal{Q}_{ID}$ is the number of distinct sender*

identities that appear in public-key or signcryption queries, up to a standard abort probability due to guessing the target identity and handling forbidden queries.

Proof. Let $\mathcal{C}$ receive an ECDLP instance $(P, \Gamma = \gamma P)$ and simulate the environment for $\mathcal{A}_I$:

Setup: $\mathcal{C}$ sets $M_{\text{pub}} = aP$ for random $a \in \mathbb{Z}_q^*$, guesses a target sender identity ID^* uniformly from the identities that will appear in public-key or signcryption queries, and sets the corresponding public key to $C^*_{\text{pub}} = \Gamma$.

Oracle Simulations:

- $H_1(ID)$: If $ID = ID^*$, return random $h^* \in \mathbb{Z}_q^*$ and record it; otherwise return a fresh random value and answer consistently on repeats.
- $H_3(X\|ID_C\|ID_R\|C_{\text{pub}}\|R_{\text{pub}}\|B\|t)$: Return a fresh random $\vartheta \in \mathbb{Z}_q^*$ on first query and answer consistently on repeats.
- Signcryption Query $(m, ID_S, R_{\text{pub}})$: If $ID_S \neq ID^*$, respond using the real signcryption algorithm. If $ID_S = ID^*$, $\mathcal{C}$ aborts (this is a standard reduction restriction since $\mathcal{C}$ does not know C^*_{pri}).
- Private Key Query (ID): If $ID = ID^*$, abort; otherwise return the corresponding private key.
- Public Key Replacement: Allowed for any identity except ID^*; if $\mathcal{A}_I$ replaces C^*_{pub}, $\mathcal{C}$ aborts.

Forgery: When $\mathcal{A}_I$ outputs a valid forgery $\sigma^* = (\vartheta^*, X^*, L^*, B^*, t^*)$ for ID^*, with non-negligible probability the forgery must correspond to a prior H_3 query on $(X^*, ID^*_C, ID^*_R, C^*_{\text{pub}}, R^*_{\text{pub}}, B^*, t^*)$. By the Forking Lemma, $\mathcal{C}$ can rewind the execution to obtain a second accepting forgery with the same (X^*, B^*, t^*) but a different H_3 output ϑ', yielding:

$$L^*P = \vartheta^* C^*_{\text{pub}} + B^*$$
$$L'P = \vartheta' C^*_{\text{pub}} + B^*$$

Subtracting gives $(L^* - L')P = (\vartheta^* - \vartheta')C^*_{\text{pub}}$, so:

$$\gamma = (L^* - L')(\vartheta^* - \vartheta')^{-1} \mod q$$

The success probability accounts for the guessing of the target identity and the Forking Lemma probability:

$$\epsilon' \geq \frac{\epsilon}{\mathcal{Q}_{ID}\mathcal{Q}_{H_3}}(1 - \frac{1}{q}). \tag{11}$$

■

Theorem 2 (EUF-CMA Security against Type-II Adversary)**.** *If ECDLP is hard in $\mathbb{G}$, then the scheme is EUF-CMA secure against a Type-II adversary $\mathcal{A}_{II}$ who knows the master secret key. The reduction is similar to Theorem 1 but with no public key replacement queries and with $\mathcal{A}_{II}$ given M_{sec}.*

Proof. The proof follows Theorem 1 with the following changes. The simulator gives M_{sec} to $\mathcal{A}_{II}$ and answers all private-key queries for $ID \neq ID^*$ using the real key generation. No public key replacement queries are allowed in this game. For the target sender, $\mathcal{C}$ embeds the ECDLP challenge by setting $C^*_{\text{pub}} = \Gamma$ and cannot answer signcryption queries on ID^* (otherwise it would need C^*_{pri}). When $\mathcal{A}_{II}$ outputs a valid forgery for ID^*, the same forking argument on H_3 yields two accepting transcripts and extracts γ from

$$L^*P = \vartheta^* C^*_{\text{pub}} + B^*, \quad L'P = \vartheta' C^*_{\text{pub}} + B^*,$$

thereby solving ECDLP. The key observation is that knowing M_{sec} only reveals the RA/KGC contribution $P_{ars} = H_1(ID_C\|M_{\text{sec}}) \pmod q$; it does not reveal the user secret γ_s, and thus does not allow computing C^*_{pri} from C^*_{pub} without solving ECDLP. ■

Theorem 3 (IND-CCA2 Security)**.** *Suppose the ECCDH is hard in $\mathbb{G}$. In that case, the proposed scheme provides IND-CCA2 security against both Type-I and Type-II adversaries in the ROM.*

Proof. Let $\mathcal{C}$ receive an ECCDH instance $(P, U = aP, V = bP)$ and set the target receiver's public key to $R^*_{\text{pub}} = V$.

Setup: $\mathcal{C}$ generates the target sender's key pair $(S_{\text{pub}}, S_{\text{pri}})$ honestly and provides params to $\mathcal{A}$ (and M_{sec} if $\mathcal{A}$ is Type-II). The receiver's private key R^*_{pri} is unknown to $\mathcal{C}$.

Oracle Simulations:

- $H_2(C\|B)$: $\mathcal{C}$ maintains a list and returns a fresh random value for each new query, answering consistently on repeats.
- Unsigncryption Query $(\sigma, S_{\text{pub}}, ID_R)$: $\mathcal{C}$ verifies the signature equation using public information. If it holds, $\mathcal{C}$ returns $m = X \oplus H_2(C\|B)$ if it has already seen the corresponding $H_2(C\|B)$ query; otherwise it returns $\perp$. This is consistent with the random-oracle simulation and the IND-CCA2 restrictions (no query on the challenge ciphertext under R^*_{pub}).

Challenge Phase: For messages (m_0, m_1), $\mathcal{C}$ chooses random bit ϕ, sets:

$$B^* = U$$
$$C^* = abP \quad \text{(the ECCDH challenge)}$$
$$K^* = H_2(C^*\|B^*)$$
$$X^* = m_\phi \oplus K^*.$$

To construct a valid signcryption, $\mathcal{C}$ selects a fresh timestamp t^*, computes

$$\vartheta^* = H_3(X^* \,\|\, ID^*_S \,\|\, ID^*_R \,\|\, S_{\text{pub}} \,\|\, R^*_{\text{pub}} \,\|\, B^* \,\|\, t^*),$$

and sets $L^* = (\vartheta^* \cdot S_{\text{pri}} + a) \bmod q$. The challenge ciphertext is $\sigma^* = (\vartheta^*, X^*, L^*, B^*, t^*)$.

Analysis: If $\mathcal{A}$ distinguishes σ^* with non-negligible advantage, then with non-negligible probability it must query H_2 on (C^*, B^*); otherwise K^* is information-theoretically hidden. By guessing the correct H_2 query (at most $\mathcal{Q}_{H_2}$), $\mathcal{C}$ can output C^* and solve ECCDH. Thus:

$$\epsilon' \geq \frac{\epsilon}{\mathcal{Q}_{H_2}} - \mathsf{negl}(q). \tag{12}$$

■

B. Informal Security Analysis

Proposition 1 (Confidentiality)**.** *LH3SC is IND-CCA2 secure in the ROM under ECCDH.*

Proof. In LH3SC the message is sent as $m \oplus K$ with $K = H_2(C\|B)$. The values are $C = \alpha R_{\text{pub}}$ (the ECCDH shared secret) and $B = \alpha P$ (the ephemeral public value).

An adversary who only sees (B, R_{pub}) must first recover C to compute K, which is infeasible for any PPT adversary under the ECCDH assumption. Because H_2 is modeled as a random oracle, its output on $(C\|B)$ is pseudorandom, so the mask K is indistinguishable from random. As a result, the distributions of $m_0 \oplus K$ and $m_1 \oplus K$ are indistinguishable for any two challenge messages. Adaptive unsigncryption queries do not reveal K since they require valid signatures, and oracle responses can be fixed consistently without exposing C. Therefore the IND-CCA2 advantage is negligible, and the scheme achieves semantic security under ECCDH. ■

Proposition 2 (Integrity and Authentication)**.** *LH3SC ensures integrity and sender authentication under ECDLP.*

Proof. The tag $\vartheta = H_3(X\|ID_C\|C_{\text{pub}}\|B\|t)$ binds all critical inputs. By collision resistance of H_3, any change to m, ID_C, C_{pub}, B, or t alters ϑ except with negligible probability. The verification equation $L \cdot P = \vartheta \cdot C_{\text{pub}} + B$ can be satisfied only by a sender who knows C_{pri} (otherwise forging L would solve the ECDLP). Therefore, ciphertext integrity and sender authentication hold. ■

Proposition 3 (Unforgeability)**.** *The scheme is EUF-CMA under the ECDLP hardness in the ROM.*

Proof. Forging a valid signcryption requires producing (L, B) that satisfies the verification equation for some message m^*. By the forking lemma extraction technique, this would imply solving the ECDLP for C_{pub}. Even with access to signcryption and unsigncryption oracles, an adversary cannot forge without the sender's private key C_{pri}. ■

Proposition 4 (Non-repudiation)**.** *LH3SC supports non-repudiation via third-party verification.*

Proof. Using only public values, a verifier can recompute $\vartheta = H_3(X\|ID_C\|C_{\text{pub}}\|B\|t)$ and test whether $L \cdot P \stackrel{?}{=} \vartheta \cdot C_{\text{pub}} + B$. If the equation holds, the signature must have been generated with the private key corresponding to C_{pub}, which provides third-party evidence of the sender's involvement. ■

Proposition 5 (Replay Protection)**.** *LH3SC resists replay attacks via timestamps and session randomness.*

Proof. The timestamp t included in ϑ lets the receiver verify freshness. A receiver can also keep a short-term cache of observed (B, t) pairs and discard repeats. With this check and the fresh ephemeral point $B = \alpha P$, each ciphertext is tied to a unique session, so replaying an old ciphertext is rejected even if the plaintext is reused. ■

Proposition 6 (Forward Secrecy)**.** *LH3SC provides partial forward secrecy against long-term key compromise.*

Proof. For each session, the sender samples fresh $\alpha \in \mathbb{Z}_q^*$ and sets $B = \alpha P$ and $C = \alpha R_{\text{pub}}$. The derived session key $K = H_2(C\|B)$ therefore depends on α, which is discarded after the session completes. Thus, even if long-term keys are later exposed, an attacker still cannot reconstruct past session keys without breaking ECCDH to recover α from B. ■

Proposition 7 (Resistance to Key Compromise Attacks)**.** *LH3SC remains secure under master-key exposure and public-key replacement.*

Proof. Type-I adversary (public key replacement): A Type-I adversary can replace public keys but does not know the master secret. In LH3SC, signature verification ties the sender's identity to the public key via ϑ. As a result, swapping a public key alone is not enough to forge a valid signature, because a valid signature still requires the matching private key.

Type-II adversary (master key knowledge): A Type-II adversary may learn the master secret key M_{sec}, which allows computation of partial private keys. However, each user's full private key also depends on their own secret γ_s. Without γ_s, the adversary cannot reconstruct the complete private key. Thus, confidentiality and unforgeability still reduce to the hardness of the ECDLP for the user's private key.

Key escrow resistance: In CLC mode, the RA/KGC issues only the partial private key P_{ars}. Since the user's secret γ_s is never revealed, deriving the full private key C_{pri} is computationally infeasible. This design therefore mitigates the key escrow problem. ■

Proposition 8 (Cross-Domain Compatibility)**.** *LH3SC preserves security across CLC, PKI, and IBC.*

Proof. The security proof does not depend on a specific infrastructure. Across CLC, PKI, and IBC, the scheme uses the same elliptic-curve group and the same hardness assumptions. The only difference is how the receiver's public parameter R_{pub} is obtained or derived in each setting. This variation does not change the core cryptographic steps. The ECCDH-based key agreement and the signature verification are identical in structure and mathematics across all three infrastructures. As a result, in the ROM, the security guarantees carry over uniformly to PKI, IBC, and CLC environments. ■

VII. Comparative Analysis

In this section, we compare the proposed heterogeneous signcryption scheme with prior work in terms of computation and communication cost. We follow standard unit-cost assumptions for basic cryptographic operations and include the sizes of transmitted group elements. These metrics are crucial in constrained environments such as WBANs and other IoT deployments, where efficiency directly affects feasibility.

To keep the comparison fair, we conducted a simulation-based evaluation using a commonly used unit-cost model for scalar multiplication, bilinear pairing, exponentiation, and hash operations. The experiments were implemented in Python with standard cryptographic libraries on a Windows system (Intel Core i7, 8 GB RAM, Windows 11), providing a consistent and reproducible baseline for measuring computational complexity and communication overhead across schemes.

A. Computational Overhead

The analysis of computation cost is done with respect to the average execution time of the basic cryptographic operations

TABLE III
COMPARISON OF COMPUTATIONAL COSTS IN SIGNCRYPTION SCHEMES (MILLISECONDS)

Scheme	Signcryption Time (ms)	Unsigncryption Time (ms)
CLC → CLC		
Zhang and Shi [12]	$3Pm + 3H \approx 1.089$	$2Pm + 4H \approx 0.795$
Yang *et al.* [29]	$3Pm + 1Exp + 3H \approx 1.441$	$2Pm + 4H \approx 0.795$
Zhan *et al.* [30]	$5Pm + 5H \approx 1.814$	$3Pm + 3H \approx 1.089$
Kasyoka *et al.* [28]	$2Pm + 1Exp + 2H \approx 1.078$	$2Pm + 1Exp + 2H \approx 1.078$
Ullah *et al.* [27]	$3Pm + 3H \approx 1.089$	$2Pm + 3H \approx 0.795$
LH3SC (CLC → CLC)	$2Pm + 3H \approx 0.760$	$2Pm + 2H \approx 0.726$
CLC → IBC		
Cao *et al.* [44]	$4Pm + 4H \approx 1.452$	$4Pm + 4H \approx 1.452$
Jin *et al.* [21]	$2Pm + 1Exp + 3H \approx 1.113$	$3Bp + 2Pm + 1Exp + 2H \approx 11.313$
Brown *et al.* [50]	$1Pm + 1Bp + 1Exp + 2H \approx 4.162$	$3Bp + 2H \approx 10.304$
Jin *et al.* [45]	$6Pm + 1Exp + 3H \approx 2.426$	$2Bp + 4Pm + 1Exp + 4H \approx 8.627$
LH3SC (CLC → IBC)	$2Pm + 3H \approx 0.760$	$2Pm + 2H \approx 0.726$
CLC → PKI		
Ali *et al.* [41]	$1Exp + 2Pm + 3H \approx 1.113$	$2Bp + 2H \approx 6.892$
Ali *et al.* [42]	$3Pm + 2H \approx 1.054$	$2Pm + 2H \approx 0.726$
Chen *et al.* [43]	$2Pm + 4H \approx 0.795$	$3Pm + 3H \approx 1.089$
Niu *et al.* [23]	$4Pm + 3H \approx 1.417$	$3Pm + 3H \approx 1.089$
Jin *et al.* [53]	$2Exp + 3Pm + 3H \approx 1.794$	$1Exp + 3Bp + 2Pm + 4H \approx 11.382$
LH3SC (CLC → PKI)	$2Pm + 3H \approx 0.760$	$2Pm + 2H \approx 0.726$

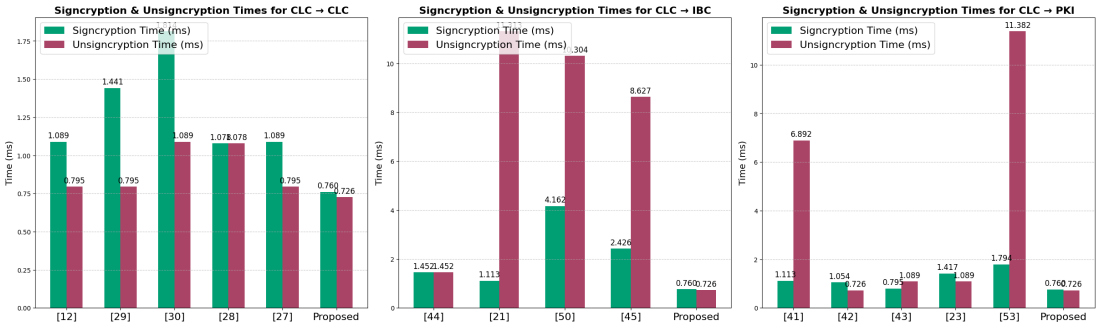

Fig. 3. Computational overhead comparison of existing and LH3SC schemes.

in milliseconds (ms): bilinear pairing (Bp) takes about 3.411ms, exponentiation (Exp) takes about 0.353 ms, point multiplication (Pm) takes about 0.328 ms, and hash operation (H) takes about 0.035 ms. These unit costs are used in the computation of the total computational overhead by adding the weighted cost of every operation in the various protocol phases, as shown in Table III and Fig. 3. The interaction types identified in the analysis are certificateless-to-certificateless (CLC–CLC), certificateless-to-public-key (CLC–PKI), and certificateless-to-identity-based (CLC–IBC) communications. The LH3SC scheme minimizes the use of bilinear pairings, which are the most computationally intensive operations in most existing schemes. For example, some related protocols require up to five bilinear pairings in the signcryption step, resulting in a computational cost of about 18.9 ms. By contrast, LH3SC relies primarily on point multiplications and hash functions, which significantly reduces computational overhead. Specifically, the signcryption phase takes about 0.76 ms, which is faster than the top performers. Its lightweight nature also means that it has been possible to run most cryptographic operations efficiently using few resources. The unsigncryption phase takes about 0.726 ms, making the scheme about 6 times faster than the bilinear pairing schemes. These improvements are particularly beneficial to IoT devices with severe computational and power requirements. The LH3SC scheme can reduce the number of bilinear pairings and maximize the use of point multiplications and hash functions, which provide this scheme with a strong level of security and a high level of efficiency, hence making it extremely appropriate for large-scale heterogeneous IoT applications.

B. Communication Overhead

The communication overhead of cryptographic schemes is a critical factor in their practical deployment, especially in computationally limited environments. The communication overhead of each scheme is measured in bits, based on the

TABLE IV
COMPARISON OF COMMUNICATION COSTS IN SIGNCRYPTION SCHEMES (BITS)

Scheme	Sender's Private Key	Receiver's Private Key	Public Key	Signcryption	Unsigncryption
CLC → CLC					
Zhang and Shi [12]	$2Z_p \approx 320$	$2Z_p \approx 320$	$2G_1 \approx 640$	$2G_1 + G_2 + 4Z_p \approx 2304$	$2G_1 + 2G_2 + 4Z_p \approx 3328$
Yang *et al.* [29]	$2Z_p \approx 320$	$2Z_p \approx 320$	$2G_1 \approx 640$	$2G_1 + 4Z_p \approx 1280$	$2G_1 + 4Z_p \approx 1280$
Zhan *et al.* [30]	$2Z_p \approx 320$	$2Z_p \approx 320$	$2G_1 \approx 640$	$2G_1 + G_2 + 4Z_p \approx 2304$	$2G_1 + 2G_2 + 4Z_p \approx 3328$
Kasyoka *et al.* [28]	$2G_1 + 3Z_p \approx 1120$	$2G_1 + 2Z_p \approx 960$	$G_1 + Z_p \approx 480$	$4G_1 + 5Z_p \approx 2080$	$2G_1 + 3Z_p \approx 1120$
Ullah *et al.* [27]	$3G_1 + 3Z_p \approx 1440$	$3G_1 + 2Z_p \approx 1280$	$2G_1 + Z_p \approx 800$	$3G_1 + 2G_2 + 3Z_p \approx 3488$	$2G_1 + 2G_2 + 3Z_p \approx 3168$
LH3SC scheme	$Z_p \approx 160$	$Z_p \approx 160$	$2G_1 \approx 640$	$2G_1 + 3Z_p \approx 1120$	$2G_1 + 2Z_p \approx 960$
CLC → IBC					
Cao *et al.* [44]	$2G_1 + 2Z_p \approx 960$	$1G_1 + 3Z_p \approx 480$	$G_1 + Z_p \approx 320$	$4G_1 + 7Z_p \approx 2400$	$2G_1 + 4Z_p \approx 1280$
Jin *et al.* [21]	$G_1 + 2Z_p \approx 640$	$G_1 + Z_p \approx 480$	$2G_1 \approx 640$	$2G_1 + G_2 + 5Z_p \approx 2464$	$2G_1 + 3G_2 + 3Z_p \approx 4192$
Brown *et al.* [50]	$2G_1 + Z_p \approx 800$	$1G_1 \approx 320$	$1G_1 \approx 320$	$2G_1 + G_2 + 2Z_p \approx 1984$	$3G_2 + Z_p \approx 3232$
Jin *et al.* [45]	$G_1 + 2Z_p \approx 640$	$G_1 + Z_p \approx 480$	$2G_1 \approx 640$	$3G_1 + G_2 + 7Z_p \approx 3104$	$2G_1 + 3G_2 + 4Z_p \approx 4352$
LH3SC scheme	$Z_p \approx 160$	$Z_p \approx 160$	$2G_1 \approx 640$	$2G_1 + 3Z_p \approx 1120$	$2G_1 + 2Z_p \approx 960$
CLC → PKI					
Ali *et al.* [41]	$2G_1 + 3Z_p \approx 1120$	$1G_1 + 1Z_p \approx 480$	$2G_1 \approx 640$	$2G_1 + 1G_2 + 2Z_p \approx 1984$	$2G_2 + 1Z_p \approx 2208$
Ali *et al.* [42]	$2G_1 + 3Z_p \approx 1120$	$2G_1 + 1Z_p \approx 800$	$G_1 \approx 320$	$2G_1 + G_2 + 2Z_p \approx 1984$	$2G_2 + 1Z_p \approx 2208$
Chen *et al.* [43]	$3G_1 + 2Z_p \approx 1280$	$G_1 + Z_p \approx 480$	$2G_1 + 1Z_p \approx 800$	$5G_1 + 7Z_p \approx 2720$	$4G_1 + 5Z_p \approx 2080$
Niu *et al.* [23]	$1Z_p \approx 160$	$G_1 + 4Z_p \approx 960$	$2G_1 + Z_p \approx 800$	$6G_1 + 6Z_p \approx 2880$	$4G_1 + 3Z_p \approx 1760$
Jin *et al.* [53]	$2G_1 + 4Z_p \approx 1280$	$2G_1 + 2Z_p \approx 960$	$2G_1 + 2Z_p \approx 960$	$3G_1 + 7Z_p \approx 2080$	$3G_2 + 3Z_p \approx 3552$
LH3SC scheme	$Z_p \approx 160$	$Z_p \approx 160$	$2G_1 \approx 640$	$2G_1 + 3Z_p \approx 1120$	$2G_1 + 2Z_p \approx 960$

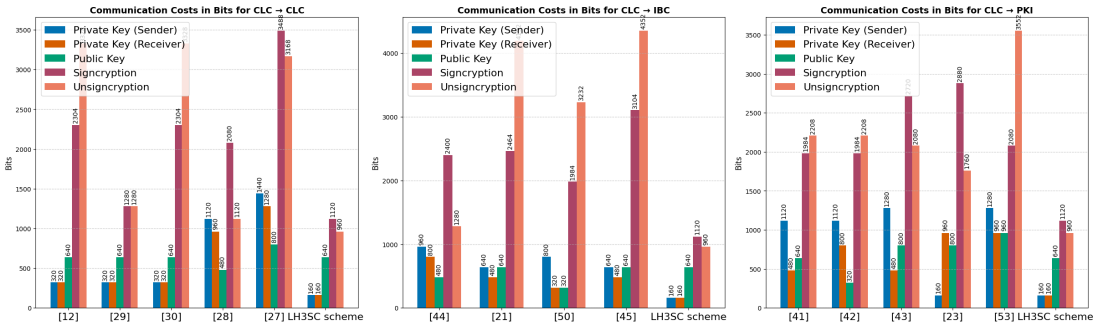

Fig. 4. Communication overhead of existing and LH3SC schemes.

TABLE V
COMPARISON OF SECURITY FEATURES AMONG SCHEMES

Scheme	$\mathcal{F}_1$	$\mathcal{F}_2$	$\mathcal{F}_3$	$\mathcal{F}_4$	$\mathcal{F}_5$	$\mathcal{F}_6$	$\mathcal{F}_7$	$\mathcal{F}_8$
Zhang and Shi [12]	✓	✓	✓	×	×	✓	✓	×
Yang *et al.* [29]	✓	✓	✓	✓	✓	×	✓	✓
Zhan *et al.* [30]	✓	✓	✓	×	✓	✓	✓	✓
Kasyoka *et al.* [28]	✓	✓	✓	×	✓	✓	✓	×
Ullah *et al.* [27]	✓	✓	✓	×	×	×	×	×
Cao *et al.* [44]	✓	✓	✓	✓	✓	✓	✓	✓
Jin *et al.* [21]	✓	✓	✓	×	✓	×	✓	×
Brown *et al.* [50]	✓	✓	✓	×	✓	×	✓	×
Jin *et al.* [45]	✓	✓	✓	×	✓	✓	✓	×
Ali *et al.* [41]	✓	✓	✓	✓	✓	✓	✓	✓
Ali *et al.* [42]	✓	✓	✓	✓	✓	✓	✓	✓
Chen *et al.* [43]	✓	✓	✓	✓	✓	×	✓	✓
Niu *et al.* [23]	✓	✓	✓	✓	✓	×	✓	✓
Jin *et al.* [53]	✓	✓	✓	×	✓	✓	✓	✓
LH3SC scheme	✓	✓	✓	✓	✓	✓	✓	✓

Note: $\mathcal{F}_1$: Message Confidentiality, $\mathcal{F}_2$: Authentication, $\mathcal{F}_3$: Integrity, $\mathcal{F}_4$: Unforgeability, $\mathcal{F}_5$: Public Verifiability, $\mathcal{F}_6$: Non-repudiation, $\mathcal{F}_7$: Replay Resistance, $\mathcal{F}_8$: Forward Secrecy.

size of group elements and scalars transmitted in ciphertexts and keys. We adopt standard element sizes: $|G_1| = 320$ bits, $|G_2| = 1024$ bits, and $|Z_p| = 160$ bits. For example, a ciphertext consisting of $2G_1 + 1Z_p$ corresponds to $2 \times 320 + 160 = 800$ bits. Table IV and Fig. 4 summarize the communication costs of existing schemes and our proposed construction across heterogeneous settings. The results show that the LH3SC scheme significantly reduces ciphertext and key sizes, achieving a ciphertext size of approximately 1,120 bits and a private key size of only 160 bits, which are smaller than those of most related works mentioned.

Existing schemes, such as those presented by Ali *et al.*, Chen *et al.*, Niu *et al.*, Jin *et al.*, and others, require multiple G_1 and Z_p elements, and in some cases also depend on the larger G_2 group, which leads to higher communication costs. For instance, schemes relying on G_2 incur ciphertext sizes exceeding 2000 bits, whereas our LH3SC scheme completely avoids the use of G_2 elements.

By focusing only on lightweight G_1 and Z_p components, the communication cost is substantially minimized. Moreover, many existing approaches use G_2 and several Z_p terms, resulting in the production of ciphertexts and keys with a length of 1,500–3,000 bits. The LH3SC scheme reduces these values by a large margin. In particular, our scheme will need 1,120 bits of the ciphertext and 160 bits for private keys, which is a significant improvement over the prior works.

Significantly, such compactness does not come at the expense of security, as the scheme is still based on hardness assumptions of ECC that are well established. The scheme is robust by eliminating G_2 operations and reducing redundant Z_p elements, and significantly lowering the communication costs. This makes it the most suitable to use in IoT devices, healthcare applications, and other cases where communication overhead reduction is vital.

C. Security Features Comparison

Beyond efficiency, it is important to assess the security guarantees each scheme provides. Table V compares the main properties: message confidentiality, authentication, integrity, unforgeability, public verifiability, non-repudiation, replay resistance, and forward secrecy. The LH3SC scheme satisfies all of these requirements, achieving a full checkmark for each feature. This underscores the robustness of the construction against common cryptographic threats.

TABLE VI
COMPARISON OF CRYPTOSYSTEM INFRASTRUCTURE ACROSS SCHEMES

Scheme	Homogeneous	Heterogeneous	Seamless
Zhang and Shi [12]	×	✓	×
Yang *et al.* [29]	×	✓	×
Zhan *et al.* [30]	×	✓	×
Kasyoka *et al.* [28]	×	✓	×
Ullah *et al.* [27]	×	✓	×
Cao *et al.* [44]	×	✓	×
Jin *et al.* [21]	×	✓	×
Brown *et al.* [50]	×	✓	×
Jin *et al.* [45]	×	✓	×
Ali *et al.* [41]	✓	×	×
Ali *et al.* [42]	✓	×	×
Chen *et al.* [43]	✓	×	×
Niu *et al.* [23]	✓	×	×
Jin *et al.* [53]	✓	×	×
LH3SC scheme	✓	✓	✓

D. Infrastructure Compatibility

Infrastructure choices can be as limiting as cost or security. PKI brings certificate overhead, IBC avoids certificates but introduces key escrow, and CLC splits the private key between the KGC and the user to mitigate both issues. Our scheme links PKI, IBC, and CLC so devices in different trust domains can communicate without heavy storage or administrative burden. Table VI summarizes which schemes interoperate across cryptosystem types. Overall, LH3SC keeps computation and communication low while still supporting PKI, CLC, and IBC. There are still constraints: the sender must be CLC-based, which limits flexibility for PKI/IBC senders, and the design is mainly one-way. Also, the performance study used a controlled simulation, so real networks and devices may behave differently. Future work will allow PKI/IBC senders, add full bidirectional communication, and test the scheme in more realistic heterogeneous IoT deployments.

VIII. CONCLUSION

In this article, we propose LH3SC, a seamless ECC-based heterogeneous signcryption scheme in which a CLC sender can securely communicate with receivers in CLC, PKI, or IBC environments, removing fixed-pair limitations of prior heterogeneous constructions. Moreover, by integrating CLC, PKI, and IBC into a single coherent framework (with a CLC sender), the proposed design supports practical cross-domain deployment in heterogeneous IoT ecosystems where different trust models coexist. We analyze the security of LH3SC, which ensures IND-CCA2 security under the assumption that ECDHP is hard and EUF-CMA security under the assumption that ECDLP is hard in the ROM. Finally, the performance analysis demonstrates a significant reduction in computational and communication overhead compared to state-of-the-art schemes. For future work, we plan to build a prototype on heterogeneous IoT platforms, measure performance under realistic network conditions, and analyze side-channel and other practical threats, along with extensions to support PKI/IBC senders and fully bidirectional communication.

REFERENCES

[1] J. Y. Khan and M. R. Yuce, *Internet of Things (IoT): systems and applications*. CRC Press, 2019.

[2] F. Zhang, C. Zhang, J. Guan, Q. Zhou, K. Chen, X. Zhang, B. He, J. Zhai, and X. Du, "Breaking the edge: Enabling efficient neural network inference on integrated edge devices," *IEEE Trans. Cloud Comput.*, vol. 13, no. 2, pp. 694–710, 2025.

[3] G. Xu, L. Lei, Y. Mao, Z. Li, X.-B. Chen, and K. Zhang, "CBRFL: A framework for committee-based byzantine-resilient federated learning," *J. Netw. Comput. Appl.*, vol. 238, p. 104165, 2025.

[4] P. Sun, S. Shen, Y. Wan, Z. Wu, Z. Fang, and X.-Z. Gao, "A survey of IoT privacy security: Architecture, technology, challenges, and trends," *IEEE Internet Things J.*, vol. 11, no. 21, pp. 34 567–34 591, Nov 2024.

[5] Y. Chen, S. He, B. Wang, Z. Feng, G. Zhu, and Z. Tian, "A verifiable privacy-preserving federated learning framework against collusion attacks," *IEEE Trans. Mobile Comput.*, vol. 24, no. 5, pp. 3918–3934, 2025.

[6] G. Xu, X. Fan, S. Xu, Y. Cao, K. Zhang, J. Kang, and D. Niyato, "Towards authenticated encrypted search with constant trapdoor for mobile cloud systems," *IEEE Trans. Mobile Comput.*, pp. 1–15, 2025.

[7] M. El-Hajj and P. Beune, "Lightweight public key infrastructure for the internet of things: A systematic literature review," *J. Ind. Inf. Integr.*, vol. 41, p. 100670, 2024.

[8] F. Han, P. Yang, H. Du, and X.-Y. Li, "Accuth$^+$+: Accelerometer-based anti-spoofing voice authentication on wrist-worn wearables," *IEEE Trans. Mobile Comput.*, vol. 23, no. 5, pp. 5571–5588, 2024.

[9] J. Wei, L. Xie, Q. Zhu, Y. Gao, K. Yu, and K.-K. Raymond Choo, "IDTRSC: ID-based traceable ring signcryption framework for data sharing without key escrow," *IEEE Trans. Veh. Technol.*, vol. 74, no. 7, pp. 11 207–11 220, 2025.

[10] P. Yu, W. Huang, R. Zhang, X. Qian, H. Li, and H. Chen, "GuardGrid: A queriable and privacy-preserving aggregation scheme for smart grid via function encryption," *IEEE Internet Things J.*, vol. 12, no. 11, pp. 17 622–17 633, 2025.

[11] S. Xu, X. Chen, Y. Guo, S.-M. Yiu, S. Gao, and B. Xiao, "Efficient and secure post-quantum certificateless signcryption with linkability for IoMT," *IEEE Trans. Inf. Forensics Secur.*, vol. 20, pp. 1119–1134, 2025.

[12] J. Zhang and C. Shi, "An enhanced-security certificateless aggregate signcryption for secure data transmission in resource-constrained networks," *IEEE Internet Things J.*, vol. 12, no. 16, pp. 34 086–34 101, 2025.

[13] D. Wang, Y. Cao, K.-K. R. Choo, Z. Yang, Z. Sun, and H. Cruickshank, "Secure battery swapping: A reservation scheme with conditional privacy-preserving bidirectional heterogeneous aggregate signcryption

and incentive mechanism," *IEEE Trans. Veh. Technol.*, vol. 72, no. 11, pp. 14 087–14 102, 2023.
[14] M. Gupta and B. S. Kumar, "Lightweight secure session key protection, mutual authentication, and access control (LSSMAC) for WBAN-assisted IoT network," *IEEE Sensors J.*, vol. 23, no. 17, pp. 20 283–20 293, 2023.
[15] L. Deng, B. Wang, Y. Gao, Z. Chen, and S. Li, "Certificateless anonymous signcryption scheme with provable security in the standard model suitable for healthcare wireless sensor networks," *IEEE Internet Things J.*, vol. 10, no. 18, pp. 15 953–15 965, 2023.
[16] H. Zhu, C. Jin, Y. Xu, G. Chen, and L. Chen, "Efficient and secure heterogeneous online/offline signcryption for wireless body area network," *Pervasive Mobile Comput.*, vol. 99, p. 101893, 2024.
[17] A. Z. A. Aljarwan and M. A. Bin Ngadi, "Review of certificateless authentication scheme for vehicular ad hoc networks," *IEEE Access*, vol. 13, pp. 100 074–100 094, 2025.
[18] W. Yang, P. Cao, and F. Zhang, "A secure pairing-free certificateless online/offline signcryption scheme with batch verification for edge computing-based VANETs," *IEEE Trans. Veh. Technol.*, vol. 74, no. 1, pp. 1570–1583, 2025.
[19] R. Elhabob, N. Eltayieb, H. Xiong, and S. Kumari, "Equality test on identity-based encryption with cryptographic reverse firewalls for telemedicine systems," *IEEE Internet Things J.*, vol. 12, no. 2, pp. 2106–2121, 2025.
[20] W. Mao, P. Jiang, and L. Zhu, "Locally verifiable batch authentication in IoMT," *IEEE Trans. Inf. Forensics Secur.*, vol. 19, pp. 1001–1014, 2024.
[21] C. Jin, W. Qin, Z. Chen, C. Li, X. Chen, G. Chen, H. Zhang, and J. Weng, "Heterogeneous signcryption scheme from CLC to IBC for IIoT," *Peer-to-Peer Netw. Appl.*, vol. 18, no. 4, p. 181, 2025.
[22] Y.-M. Tseng, T.-C. Ho, T.-T. Tsai, and S.-S. Huang, "AHMRE-SCST: Lightweight anonymous heterogeneous multirecipient encryption with seamlessly compatible system transformation for IoT devices," *IEEE Internet Things J.*, vol. 11, no. 17, pp. 28 508–28 525, 2024.
[23] S. Niu, H. Shao, Y. Hu, S. Zhou, and C. Wang, "Privacy-preserving mutual heterogeneous signcryption schemes based on 5G network slicing," *IEEE Internet Things J.*, vol. 9, no. 19, pp. 19 086–19 100, 2022.
[24] X. Ding, Y. Xu, G. Li, K. Yang, J. Yuan, and J. An, "Design and performance evaluation for BILCM-ID system with improved stopping criterion," *IEEE Trans. Veh. Technol.*, vol. 74, no. 4, pp. 6779–6784, 2025.
[25] T. Peng, B. Gong, C. Guo, A. Badshah, M. Waqas, H. Alasmary, and S. Chen, "An efficient conjunctive keyword searchable encryption for cloud-based IoT systems," *Digit. Commun. Netw.*, vol. 11, no. 4, pp. 1293–1304, 2025.
[26] P. Chen, Y. Song, and Y. Xia, "Adaptively diagnosing system faults in microservice architecture: An autonomous predictive model construction framework," *Future Gener. Comput. Syst.*, p. 108256, 2025.
[27] I. Ullah, A. Alkhalifah, S. U. Rehman, N. Kumar, and M. A. Khan, "An anonymous certificateless signcryption scheme for internet of health things," *IEEE Access*, vol. 9, pp. 101 207–101 216, 2021.
[28] P. N. Kasyoka, M. Kimwele, and S. A. Mbandu, "Efficient certificateless signcryption scheme for wireless sensor networks in ubiquitous healthcare systems," *Wireless Pers. Commun.*, vol. 118, no. 4, pp. 3349–3366, 2021.
[29] W. Yang, P. Cao, and F. Zhang, "A secure pairing-free certificateless online/offline signcryption scheme with batch verification for edge computing-based VANETs," *IEEE Trans. Veh. Technol.*, vol. 74, no. 1, pp. 1570–1583, 2025.
[30] Q. Zhan, M. Luo, and M. Qiu, "An efficient multimode certificateless ring signcryption scheme in VANETs," *IEEE Internet Things J.*, vol. 11, no. 20, pp. 33 508–33 524, 2024.
[31] X. Li, C. Jiang, D. Du, Z. Zhou, M. Fei, L. Wu, and C. Y. Chung, "Cyber-physical power systems: Exploring a streamlined signcryption scheme for resource-limited smart terminals," *IEEE Trans. Ind. Informat.*, vol. 20, no. 7, pp. 9749–9760, 2024.
[32] G. Srinivasa Rao, G. Thumbur, R. B. Amarapu, G. N. Bhagya, and P. V. Reddy, "A new lightweight and secure certificateless aggregate signcryption scheme for industrial internet of things," *IEEE Internet Things J.*, vol. 11, no. 6, pp. 10 563–10 574, 2024.
[33] Q. Wu, L. Zhang, Y. Yang, and K.-K. R. Choo, "Certificateless signature scheme with batch verification for secure and privacy-preserving V2V communications in VANETs," *IEEE Trans. Dependable Secure Comput.*, vol. 22, no. 2, pp. 1448–1459, 2025.
[34] B. Gong, C. Guo, C. Guo, C. Guo, Y. Sun, M. Waqas, and S. Chen, "SLIM: A secure and lightweight multi-authority attribute-based signcryption scheme for IoT," *IEEE Trans. Inf. Forensics Secur.*, vol. 19, pp. 1299–1312, 2024.
[35] I. Ullah, A. Alomari, A. M. Abdullah, N. Kumar, A. Alsirhani, F. Noor, S. Hussain, and M. A. Khan, "Certificate-based signcryption scheme for securing wireless communication in industrial internet of things," *IEEE Access*, vol. 10, pp. 105 182–105 194, 2022.
[36] P. Kuang, X. Zhang, M. Yang, H. Xiong, C. Feng, D. Wu, W. Wang, and A. Wahaballa, "Efficient zero-trust data transmission for consumer electronic using holographic counterparts in internet of things: Ciphertext-policy attribute-based signcryption with equality test," *IEEE Trans. Consum. Electron.*, 2025.
[37] B. Gong, Y. Wu, A. Badshah, and M. Waqas, "Privacy-preserving and traceable certificateless anonymous mutual authentication scheme for IoT," *IEEE Trans. Dependable Secure Comput.*, vol. 22, no. 6, pp. 7508–7520, 2025.
[38] X. Ai, A. Badshah, S. Tu, M. Waqas, and I. Ahmad, "An improved ultra-lightweight anonymous authenticated key agreement protocol for wearable devices," *IEEE Trans. Mobile Comput.*, vol. 24, no. 5, pp. 4543–4557, 2025.
[39] W. Xu, J. Deng, J. Yu, S. Mao, Y. Li, Z. pENG, and B. Xiao, "Blockchain-based verifiable decentralized identity for intelligent flexible manufacturing," *IEEE Internet Things J.*, vol. 12, no. 16, pp. 32 366–32 378, 2025.
[40] Y. Chen, H. Li, Y. Song, and X. Zhu, "Recoding hybrid stochastic numbers for preventing bit width accumulation and fault tolerance," *IEEE Trans. Circuits Syst. I, Reg. Papers*, vol. 72, no. 3, pp. 1243–1255, 2025.
[41] I. Ali, Y. Chen, N. Ullah, M. Afzal, and W. HE, "Bilinear pairing-based hybrid signcryption for secure heterogeneous vehicular communications," *IEEE Trans. Veh. Technol.*, vol. 70, no. 6, pp. 5974–5989, 2021.
[42] I. Ali, Y. Chen, C. Pan, and S. Chen, "Cost-effective and secure scheme for fog computing-enabled internet of vehicles using CLC-to-PKI-based heterogeneous signcryption," *IEEE Trans. Intell. Veh.*, pp. 1–15, 2024.
[43] Z. Chen, C. Jin, G. Chen, Y. Jin, and H. Zong, "A heterogeneous online/offline signcryption scheme for internet of vehicles," *Veh. Commun.*, vol. 43, p. 100635, 2023.
[44] P. Cao, Y. Zheng, W. Yang, and F. Zhang, "An enhanced offline/online heterogeneous signcryption protocol with batch verification for edge computing-based VANETs," *IEEE Trans. Intell. Transp. Syst.*, vol. 26, no. 8, pp. 11 631–11 646, 2025.
[45] C. Jin, H. Zhu, W. Qin, Z. Chen, Y. Jin, and J. Shan, "Heterogeneous online/offline signcryption for secure communication in internet of things," *J. Syst. Archit.*, vol. 127, p. 102522, 2022.
[46] S. Yu, M. Shang, and F. Li, "A lattice-based efficient heterogeneous signcryption scheme for secure network communications," *J. High Speed Netw.*, vol. 30, no. 1, pp. 19–27, 2024.
[47] P. Xie, N. Li, Z. Wang, J. Zhu, and P. Zhang, "An efficient heterogeneous multi-message and multi-receiver signcryption IBC-CLC scheme for industrial internet of things," *Int. J. Netw. Secur.*, vol. 25, no. 2, pp. 324–331, 2023.
[48] I. Ullah, H. Zahid, F. Algarni, and M. A. Khan, "An access control scheme using heterogeneous signcryption for IoT environments," *Comput. Mater. Continua*, vol. 70, no. 3, pp. 4307–4321, 2022.
[49] X. Yang, K. Yao, S. Li, N. Ren, and C. Wang, "Efficient and mutual heterogeneous signcryption schemes for VANETs," *Peer-to-Peer Netw. Appl.*, vol. 18, p. 247, 2025, © The Author(s) 2025, under exclusive licence to Springer Science+Business Media, LLC, part of Springer Nature.
[50] B. Klugah-Brown, J. B. A. Kanpogninge, and X. Qi, "A signcryption scheme from certificateless to identity-based environment for WSNs into IoT," *Int. J. Comput. Appl.*, vol. 120, no. 9, 2015.
[51] J. Jiao, L. Guo, W. Yu, S. Yang, and S. Li, "An efficient lattice-based heterogeneous signcryption scheme for VANETs," *Concurr. Comput. Pract. Exp.*, vol. 37, no. 3, p. e8384, 2025.
[52] X. Yang, S. Li, M. Li, X. Du, and C. Wang, "Heterogeneous signcryption scheme from PKI to IBC with multi-ciphertext equality test in internet of vehicles," *IEEE Internet Things J.*, vol. 11, no. 8, pp. 14 178–14 191, 2024.
[53] C. Jin, W. Qin, Z. Chen, K. Sun, G. Chen, J. Shan, and L. Chen, "Heterogeneous signcryption scheme with equality test from CLC to PKI for IoV," *Comput. Commun.*, vol. 220, pp. 149–159, 2024.