Efficient and Secure Post-Quantum Certificateless Signcryption with Linkability for IoMT

Shiyuan Xu, *Graduate Student Member, IEEE,* Xue Chen, *Graduate Student Member, IEEE,* Yu Guo, *Member, IEEE,* Siu-Ming Yiu, *Member, IEEE,* Shang Gao, *Member, IEEE,* and Bin Xiao, *Fellow, IEEE*

***Abstract*—The Internet of Medical Things (IoMT) has gained significant research focus in both academic and medical institutions. Nevertheless, the sensitive data involved in IoMT raises concerns regarding user validation and data privacy. To address these concerns, certificateless signcryption (CLSC) has emerged as a promising solution, offering authenticity, confidentiality, and unforgeability. Unfortunately, most existing CLSC schemes are impractical for IoMT due to their heavy computational and storage requirements. Additionally, these schemes are vulnerable to quantum computing attacks. Therefore, research focusing on designing an efficient post-quantum CLSC scheme is still far-reaching. In this work, we propose PQ-CLSCL, a novel post-quantum CLSC scheme with linkability for IoMT. Our proposed design facilitates secure transmission of medical data between physicians and patients, effectively validating user legitimacy and minimizing the risk of private information leakage. To achieve this, we leverage lattice sampling algorithms and hash functions to generate the partial secret key, then employ the sign-then-encrypt method and design a link label. We also formalize and prove the security of our design, including indistinguishability against chosen-ciphertext attacks (IND-CCA2), existential unforgeability against chosen-message attacks (EU-CMA), and linkability. Finally, through comprehensive performance evaluation, our computation overhead is just 5% of other existing schemes. The evaluation results demonstrate that our solution is practical and efficient.**

***Index Terms*—Certificateless Signcryption, Internet of Medical Things, Linkability, Lattice, Information Security, Applied Cryptography.**

I. Introduction

THE Internet of Medical Things, a new concept emerging from the combination of medical sensor devices and the Internet of Things, providing patients with diverse and flexible treatment options [1], [2]. A traditional IoMT scenario consists of three types of entities as depicted in Fig. 1, including patient, medical monitoring device (MMD), and physician [3], [4]. The medical monitoring device worn by the patient transmits data from various body indicators via the Internet to the hospital for storage. Doctors can access the patient's medical health data by accessing the database of patient records, and then use Artificial Intelligence algorithms to analyze the patient's data, point out possible conditions, provide remote treatment, prescribe potential medications, and make near real-time decisions for the patient. As the patient recovers, the doctor can also remotely ask the patient for advice and precautions to prevent the disease.

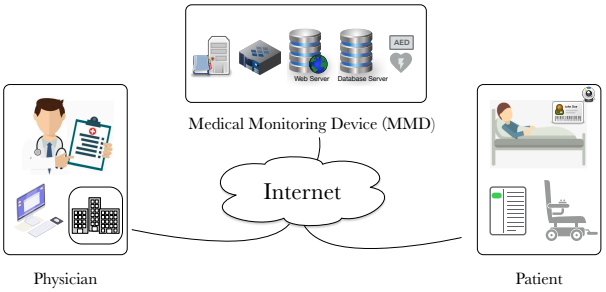

Fig. 1. A Traditional Framework of IoMT.

IoMT provides patients with convenient and reliable healthcare services, enabling them to prevent or treat diseases remotely and in a timely manner [5]. However, the data transmission mode of IoMT can be intercepted or even tampered with by an adversary during the communication process of the patient's medical information data, resulting in the leakage of a large amount of sensitive information such as the patient's personal data [6]. This could lead to doctors making incorrect diagnoses of patients' conditions. For example, if an adversary tampers with the data of medical monitoring devices and sends some worsened physical indicators to the hospital, the doctor may think that the patient's condition has worsened after the analysis and make a wrong diagnosis, thus affecting the patient's health [7]. Therefore, it is significant and challenging to transmit and protect medical data securely.

Numerous scholars have adopted digital signatures [8], [9] and public key encryption [10] to secure data transmissions between medical monitoring devices and users for user authentication and personal information protection. However, directly combining these cryptographic primitives in one scheme will significantly increase the computational and storage overhead, which is impractical for IoMT scenarios. Zheng [11] formalized an innovative primitive, namely signcryption, which can perform both encryption and signature operations. It not only satisfies the authenticity and confidentiality requirements but is also more effective than the traditional 'sign then encrypt'

This work was partially supported by HKU-SCF FinTech Academy, Shenzhen-Hong Kong-Macao Science and Technology Plan Project (Category C Project: SGDX20210823103537030), Theme-based Research Scheme T35-710/20-R, and the National Natural Science Foundation of China under Grants 62102035. (*Corresponding authors*: Yu Guo and Siu-Ming Yiu)

Shiyuan Xu, Xue Chen, and Siu-Ming Yiu are with the Department of Computer Science, School of Computing and Data Science, The University of Hong Kong, Pok Fu Lam, Hong Kong. (E-mail: syxu2@cs.hku.hk, xchen.serena666@connect.hku.hk, smyiu@cs.hku.hk).

Yu Guo is with the School of Artificial Intelligence, Beijing Normal University, Beijing, China. (E-mail: yuguo@bnu.edu.cn).

Shang Gao and Bin Xiao are with the Department of Computing, The Hong Kong Polytechnic University, Hung Hom, Hong Kong. (E-mail: shangjason.gao@polyu.edu.hk, b.xiao@polyu.edu.hk).

or 'encrypt then sign' methodologies. Classical signcryption construction mainly includes two main categories, which are identity-based public key cryptography (IB-PKC) and public key infrastructure (PKI). Nevertheless, PKI-based CLSC schemes require a Certificate Authority (CA) to distribute a large number of certificates to users, resulting in complex management and high storage overhead. In addition, IB-PKC-based primitives face key escrow issues, where the key generation center (KGC) can arbitrarily decrypt the user's message and forge its signature, posing to severe security risks.

To overcome the above-mentioned hindrances, Al-Riyami et al. [12] presented a certificateless public key cryptography (CL-PKC) primitive. Unlike IB-PKC, it introduces the semi-honest KGC with its master secret key, which is only responsible for generating part secret key. Then, Barbosa et al. [13] formalized the concept of CLSC based on bilinear pairing, where a user's secret key consists of a secret key value of its own choice and a partial secret key. Since then, numerous novel CLSC schemes were proposed [14]–[17]. However, these schemes either require significant computational overhead or fail to provide data confidentiality in IoMT scenarios. Besides, most schemes are vulnerable to quantum attacks [18], which makes it still insecure and impractical.

However, there are circumstances where it is crucial to determine if different messages come from the same sender. With the vast amount of medical data available, it is time-consuming for a physician to download and decrypt multiple medical data to determine if they correspond to a specific patient [19]. To bridge the gap, the notion of signature linkability was formalized, where a user generates several messages during a particular event, these messages will be associated with one another [20]. As such, physicians can directly ascertain whether multiple sets of medical data pertain to the same patient, significantly reducing computational overhead. To the best of our knowledge, there does not exist a lattice-based signcryption scheme that provides this property [21]–[29], despite its practical benefits for privacy preservation in IoMT.

A. Our Motivation

IoMT offers patients more reliable and convenient healthcare services, enabling them to receive timely treatment from doctors. However, transmitting medical data in IoMT presents significant security and privacy challenges. For instance, data can be tampered with by malicious adversaries, and patients' sensitive personal information may be leaked. These issues pose a bottleneck to the development of IoMT. Therefore, ensuring the confidentiality and integrity of medical data while achieving quantum safety remains a critical concern.

In our design, we prioritize practicality, efficiency, and security. To get around these concerns, our intuition is to develop a signcryption primitive that simultaneously performs the roles of public key encryption and digital signature. In addition, we incorporate lattice hardness to resist quantum attacks. To simplify the complexity of key management and deployment, a certificateless framework is promising as it avoids the certificate management challenges associated with public key infrastructure (PKI). In terms of security requirements, our design is built to be quantum-resistant and must guarantee confidentiality and unforgeability for medical data. Considering the real-world application, we also incorporate the linkability so that physicians can directly determine whether multiple sets of data are related to the same patient.

B. Our Contribution

We summarize the fourfold contribution to this work below.

- We propose the first post-quantum certificateless signcryption with linkability, named PQ-CLSCL, designed to secure medical data transmission between monitoring devices and users (patients and physicians) in IoMT scenarios. It validates user legitimacy and mitigates the risk of private information leakage while quickly determining if multiple ciphertexts belong to the same patient. To the best of our knowledge, this is the first quantum-safe certificateless signcryption protocol for IoMT.
- The proposed scheme combines lattice-based certificateless signature and public key encryption into a single primitive. It offers several security advantages, including confidentiality, unforgeability, linkability, and authenticity of transmitted data under two types of attacks.
- Our scheme has been proven to satisfy IND-CCA2, EU-CMA, and linkability in the random oracle model (ROM). Through rigorous security analysis, we demonstrate that the IND-CCA2, EU-CMA and linkability of our PQ-CLSCL primitive can be reduced to the hardness of LWE and SIS, respectively. We also give an informal analysis of the Man-in-the-middle attack and Impersonation attack. By conducting a security comparison, our scheme fulfills the properties of IND-CCA2, UF-CMA, quantum resistance, and linkability simultaneously, surpassing the capabilities of prior arts.
- Through comprehensive experiments, we have determined that our signcryption and unsigncryption overheads are 21.067 ms and 10.567 ms, respectively, resulting in a total computation overhead of 31.634 ms. Comparative analysis with other signcryption protocols [21]–[32] reveals that our PQ-CLSCL scheme outperforms the overhead of all other lattice-based solutions. It is worth noting that our signcryption and unsigncryption overheads are only 0.07 to 1.0 times and 0.02 to 1.0 times compared to prior arts, respectively. Our computation overhead is just 0.05 to 1.0 times of existing lattice-based signcryption schemes.

C. Technical Overview

Traditional lattice-based signcryption schemes typically employ the encrypt-then-sign approach [33], [34]. However, it is not suitable for certificateless signcryption. Although Yu et al. [28] proposed a lattice-based certificateless signcryption scheme, the correctness of their construction is subject to debate. Specifically, they used the $\mathbf{SampleD}$ algorithm in their Extract algorithm as described in Section IV.B. However, the input for $\mathbf{SampleD}$ should be a matrix along with a Gaussian parameter s and a center $\mathbf{c}$, rather than $(\bar{\mathbf{A}}, \mathbf{R}, \mathbf{u}_i, s_2)$. Consequently, this discrepancy compromises both the correctness and security of their scheme.

At a high level, we follow the blueprint of the scheme [28] by addressing their problems and then additionally providing the linkability property, which serves as a cornerstone for medical data privacy-preserving in IoMT.

Achieving the lattice-based certificateless signcryption with linkability is not trivial, our approach involves incorporating a hash function H_1 and $\mathbf{SamplePre}$ technique into the partial secret key algorithm to compute $\mathbf{psk}_i$. Then, each user selects a secret value $\mathbf{s}_i$ and combines it with $\mathbf{psk}_i$ to derive its secret key SK_i. Concerning the linkability, we incorporate a link label $\mathbf{l}_S = \mathbf{psk}_S + \mathbf{A}^\top \mathbf{s}_S$ in the ciphertext generation phase. During the ciphertext linkability checking phase, a physician can easily determine if two ciphertexts $\mathbf{c}_1$ and $\mathbf{c}_2$ are from the same patient by comparing the two link labels $\mathbf{l}_1$ and $\mathbf{l}_2$.

D. Outline of This Paper

Section II provides literature reviews to show the recent works. Then, we introduce the preliminary in Section III. After that, our problem formulation is illustrated in Section IV. We elaborate on the proposed PQ-CLSCL primitive in detail in Section V. In Sections VI and VII, we illustrate the security analysis as well as the comprehensive performance evaluation, respectively. Eventually, we conclude this paper.

TABLE I
NOMENCLATURE

Acronym	Description
λ	security parameter
q	prime number
B	error distribution parameter
s	Gaussian parameter
σ	discrete Gaussian distribution parameter
$\mathcal{D}$	discrete normal distribution
H_1, H_2	hash functions
pp	public parameter
(mpk, msk)	master public-secret key pair
ID_i	user's identity
S, U	signcrypt/unsigncrypt users set
$\{S, U\}$	all users set
ID_S, ID_U	signcrypt/unsigncrypt user
$\mathbf{psk}_i$	partial secret key of user ID_i
(PK_i, SK_i)	public-secret key pair of user ID_i
m	medical message
μ_1, μ_2, μ	ciphertext elements
sig, sig'	signature of ciphertext element μ_1
$\mathbf{c}$	final ciphertext of medical message m
$Q_{KG}, Q_{PSK}, Q_{PKR}, Q_{SV}$	query times
$\mathcal{O}_{H_1}^{list}$, $\mathcal{O}_{H_2}^{list}$, $\mathcal{O}_{PK}^{list}$	oracle lists
$\mathcal{B}_i$	simulation algorithms to solve problems
$\mathcal{A}_I / \mathcal{A}_{II}$	two-type adversaries
$\mathcal{C}$	challenger

II. Related Works

A. Signcryption

Signcryption primitives can play the roles of public key encryption and digital signature at the same time, thereby ensuring the confidentiality and integrity of data transmission. These primitives offer a lower communication overhead compared to the traditional sign-then-encrypt scheme. Originally proposed by Zheng et al. [11], signcryption combines signing and encryption algorithms into a single logical step. In 2002, Malone-Lee introduced an identity-based signcryption scheme [35], where the public key can be any string. Subsequently, Barbosa et al. [13] presented the first certificateless signcryption scheme with bilinear pairing, which provides forward secrecy and non-repudiation. Liu et al. later proposed a novel secure certificateless signcryption scheme within a standard model [36], although it was found to be vulnerable to public key replacement attacks. The certificateless signcryption scheme described in [37] meets the requirements for unforgeability and confidentiality. Following this, scholars developed an efficient certificateless online/offline signcryption primitive for edge IoT devices [38]. In 2020, Yu et al. proposed a lattice-based certificateless signcryption scheme [28]. Since then, numerous researchers have focused on designing certificateless signcryption primitives that are resilient to quantum attacks [39], [40]. Recently, several studies have utilized certificateless signcryption to secure message transmission and authentication in the Internet of Vehicles (IoV) [41], [42].

B. Internet of Medical Things

The Internet of Medical Things (IoMT), a combination of medical sensor devices and the IoT [43], offers patients a more accessible and reliable healthcare service. This advancement enables them to seek prompt medical attention for their ailments. However, during the communication and transmission phase of medical data, there are risks of malicious interference from adversaries, or potential leakage of patients' private and personal data [44], [45]. Hence, we necessitate the use of cryptographic techniques to safeguard the confidentiality and integrity of medical data transmission, in which signcryption emerges as a promising candidate. In 2021, Zhang et al. [46] proposed the idea of utilizing the certificateless signcryption scheme to protect data in IoMT. Following this, Chen et al. [2] proposed a paring-free certificateless signcryption scheme for privacy-preserving in IoMT. The low computational and communication overhead of their scheme meets the demands of healthcare data transformation. However, at present, research on practical schemes for protecting healthcare data in the IoMT using signcryption primitive is scarce.

III. Preliminaries

This sector introduces several fundamental knowledge, including the notations utilized in this paper, lattice definition, LWE and SIS hardness, lattice sampling algorithms, and left-over hash lemma. Table I explains the acronym and description used in this paper. In this paper, we use lowercase bold letters to denote vectors ($e.g.$ $\mathbf{a}$) and uppercase bold letters to denote matrices ($e.g.$ $\mathbf{A}$). We denote $\mathbb{Z}$ as the integers. We use $[\mathbf{A}|\mathbf{B}]$ to denote the concatenation of matrices $\mathbf{A}$ and $\mathbf{B}$. We use '$\leftarrow$' to denote sampling values.

Definition 1: A basis of an m-dimensional lattice Λ is an ordered set $\mathbf{B} = (\mathbf{b}_1, \mathbf{b}_2, \cdots, \mathbf{b}_n) \in \mathbb{R}^m$ such that

$$\Lambda = \Lambda(\mathbf{B}) = \{x_1 \cdot \mathbf{b}_1 + x_2 \cdot \mathbf{b}_2 + \cdots + x_n \cdot \mathbf{b}_n | x_i \in \mathbb{Z}\}. \quad (1)$$

Definition 2: Given a positive parameter $\sigma \in \mathbb{R}^+$, a center $\mathbf{c} \in \mathbb{Z}^m$ and any $\mathbf{x} \in \mathbb{Z}^m$, we say that $\mathcal{D}_{\sigma,\mathbf{c}} = \frac{\rho_{\sigma,\mathbf{c}}(\mathbf{x})}{\rho_{\sigma,\mathbf{c}}(\Lambda)}$ for $\forall \mathbf{x} \in \Lambda$ is the discrete Gaussian distribution over Λ: $\rho_{\sigma,\mathbf{c}}(\mathbf{x}) = \exp(-\pi\frac{\|\mathbf{x}-\mathbf{c}\|^2}{\sigma^2})$, where $\mathbf{c}$ is a center and $\rho_{\sigma,\mathbf{c}}(\Lambda) = \sum_{\mathbf{x}\in\Lambda}\rho_{\sigma,\mathbf{c}}(\mathbf{x})$. Note that we need to make sure that $\sigma \leq \alpha s\lambda\sqrt{6l}$ for lattice security.

Definition 3: Given two positive integers n, $\alpha \in (0,1)$, a prime $q = q(n) > 2$, where $\alpha q > 2\sqrt{n}$, and a secret $\mathbf{s} \xleftarrow{\$} \mathbb{Z}_q^n$, we define:

(1) LWE distribution: Uniformly select a matrix $\mathbf{A} \xleftarrow{\$} \mathbb{Z}_q^{n\times m}$, and a sample $\mathbf{e} \leftarrow \Psi_\alpha^m$, outputting $(\mathbf{A}, \mathbf{A}^\top\mathbf{s} + \mathbf{e}) \in \mathbb{Z}_q^{n\times m} \times \mathbb{Z}_q^m$.

(2) Uniform distribution: Uniformly select a matrix $\mathbf{A} \xleftarrow{\$} \mathbb{Z}_q^{n\times m}$ and a vector $\mathbf{x} \xleftarrow{\$} \mathbb{Z}_q^m$, outputting $(\mathbf{A}, \mathbf{x}) \in \mathbb{Z}_q^{n\times m} \times \mathbb{Z}_q^m$.

Lemma 1: Given a vector $\mathbf{x} \leftarrow \mathcal{D}_{\mathbb{Z}^n,s}$ and the inequalities $\|\mathbf{x}\| \leq s\sqrt{n}$ and $|\mathbf{x}| \leq s\omega\sqrt{\log n}$ hold with overwhelming probability if $s \geq \omega\sqrt{\log n}$.

Definition 4: Given a positive integer q, a random matrix $\mathbf{A} \in \mathbb{Z}_q^{n\times m}$, m random vectors $\mathbf{a}_i \in \mathbb{Z}_q^n$, and a real number β ($q > \beta$), find a non-zero integer vector $\mathbf{z} \in \mathbb{Z}^m$ of norm $\|\mathbf{z}\| \leq \beta$ s.t. $\mathbf{Az} = \sum_i^m \mathbf{a}_i \cdot \mathbf{z}_i = 0 \in \mathbb{Z}_q^n$.

Lemma 2: When $\mathbf{c} = 0$, the discrete Gaussian distribution $\mathcal{D}_{\sigma,\mathbf{c}}^m$ can be abbreviated as $\mathcal{D}_\sigma^m$. Given a vector $\mathbf{x} \leftarrow \mathcal{D}_\sigma^m$, it has $\|\mathbf{x}\| \leq 2\sigma\sqrt{m}$ with overwhelming probability. Given a real number $\lambda > 0$ and a vector $\mathbf{g} \in \mathbb{Z}^n$, we have:

$$\Pr[\mathbf{x} \leftarrow \mathcal{D}_\sigma^m : \frac{\mathcal{D}_\sigma^m(\mathbf{x})}{\mathcal{D}_{\sigma,\mathbf{g}}^m(\mathbf{x})} < e^{\frac{1}{2\psi^2}+\frac{12}{\psi}}] > 1 - 2^{-100}, \quad (2)$$

where $\sigma = \psi(\|\mathbf{g}\|)$ and the probability distribution of $\mathcal{D}_\sigma^m$ is

$$\rho_{\sigma,\mathbf{c}}^m(\mathbf{x}) = e^{-(\mathbf{x}-\frac{\mathbf{c}^2}{2\sigma^2})}(2\pi\sigma^2)^{-\frac{m}{2}}. \quad (3)$$

Definition 5: For any lattice Λ and a positive real $\epsilon > 0$, the smoothing parameter $\eta_\epsilon(\Lambda)$ is the smallest real $\sigma > 0$ s.t. $\rho_{1/\sigma}(\Lambda^*\backslash\{0\}) \leq \epsilon$. Note that the Gaussian distribution over lattice has good cryptographic properties when its Gaussian parameter exceeds the smooth parameter.

Theorem 1: [47] Given three integers n, m, and q, where $m \geq 2n\log q$, the $\mathbf{TrapGen}(n, m, q)$ algorithm returns a matrix $\mathbf{A} \in \mathbb{Z}_q^{n\times m}$ and a basis $\mathbf{T} \in \mathbb{Z}_q^{m\times m}$, where $\mathbf{A}$ is statistically close to uniform and $\|\widetilde{\mathbf{T}}\| = \mathcal{O}(\sqrt{n\log q})$.

Theorem 2: [48] Assume that three integers n, $q = \mathsf{poly}(n)$, and $m \geq 5n\log q$.Taking a matrix $\mathbf{A} \in \mathbb{Z}_q^{n\times m}$, a lattice basis $\mathbf{T} \in \mathbb{Z}_q^{m\times m}$ of $\Lambda_q^\perp(\mathbf{A})$ satisfying $\|\mathbf{T}\| \leq O(n\log q)$, and a Gaussian parameter $\sigma \geq \|\widetilde{\mathbf{T}}\| \cdot \omega(\sqrt{\log m})$ as input, the $\mathbf{SamplePre}(\mathbf{A}, \mathbf{T}, \mathbf{v}, \sigma)$ algorithm outputs a vector $\mathbf{x} \in \mathbb{Z}_q^m$, which is statistically close to the distribution $\mathcal{D}_{\Lambda_q^v(\mathbf{A}),\sigma}$ satisfying $\mathbf{Ax} = \mathbf{v} \bmod q$.

Definition 6: A simplified version of the leftover hash lemma includes two universal functions $F = \{f : X \to Y\}$. Given two vectors $\mathbf{x}_1, \mathbf{x}_2 (\mathbf{x}_1 \neq \mathbf{x}_2)$, it always satisfies: $\Pr_{f\leftarrow F}(f(\mathbf{x}_1) = f(\mathbf{x}_2)) = \frac{1}{|Y|}$. Specifically, given a finite addition group $\mathbb{Z}_q^n$, any integer $m \geq 1$, and a matrix $\mathbf{A} \in \mathbb{Z}_q^{n\times m}$, the function $F = \{f_\mathbf{A} : \{0,1\}^m \to \mathbb{Z}_q^n; \mathbf{x} \mapsto f_\mathbf{A}(\mathbf{x}) = \mathbf{Ax}\}$ is two-universal.

IV. Problem Formulation

A. System Models

As elaborated in Fig. 2, our IoMT system involves five entities, namely, medical monitoring device (MMD), gateway, key generation center (KGC), physician, and medical cloud server (MCS).

- **MMD**: MMD is a device that is used to surveil various health indicators of a patient and is usually carried by the patient, e.g. stethoscope holder, sphygmomanometer, continuous positive airway pressure, etc.
- **Gateway**: In an IoMT scenario, the gateway indicates a transfer center, linking the MMD data to the gateway router through short-range radio transceivers.
- **KGC**: KGC is the core infrastructure for public parameter and master public-secret key pairs generation. In addition, it also maintains to calculation of the partial secret keys for MMD-embedded patients and physicians.
- **Physician**: Physician normally refers to the doctor-in-charge or rehabilitation therapist with the responsibility to communicate with the patients through a gateway and also exchange medical information from MCS. There exists a corresponding relationship between a signcrypt ciphertext stored in MCS and the private information of patients. Physicians can obtain the corresponding ciphertext from MCS according to patients' public information.
- **MCS**: MCS is a cloud server and it takes charge of medical data storage. After uploading the data to the MCS by MMD, a physician will diagnose the patient.

B. Threat Models

We make several threat assumptions regarding each entity involved in our design as follows.

- **MMD** is considered as *fully trusted*, and all private medical information is securely exchanged with the KGC and gateway.
- **Gateway** is assumed as *honest-but-curious*. It acts as a communication bond between the MMD and a physician or MCS.
- **KGC** is considered as *semi-honest*, and the master-public-secret key pair together with all partial secret keys are stored in it. For the Type-II adversary $\mathcal{A}_{II}$, it can obtain the master secret key.
- **Physician** is assumed as *fully trusted* in the sense that it keeps the secret key privately and transmits the signcrypted data to the gateway.
- **MCS** is considered as *honest-but-curious*. It used to store the medical signcrypted data honestly while it is curious about the sensitive information from the medical signcrypted data.

C. Formal Definitions of PQ-CLSCL

Our PQ-CLSCL scheme incorporates six algorithms, **Setup**, **Partial secret key Extract**, **KeyGen**, **Signcrypt**, **Unsigncrypt**, and **Link**. We specify the formal definitions as follows.

1) **Setup**(n, λ) : Given a system parameter n and a security parameter λ, this algorithm is executed by KGC and

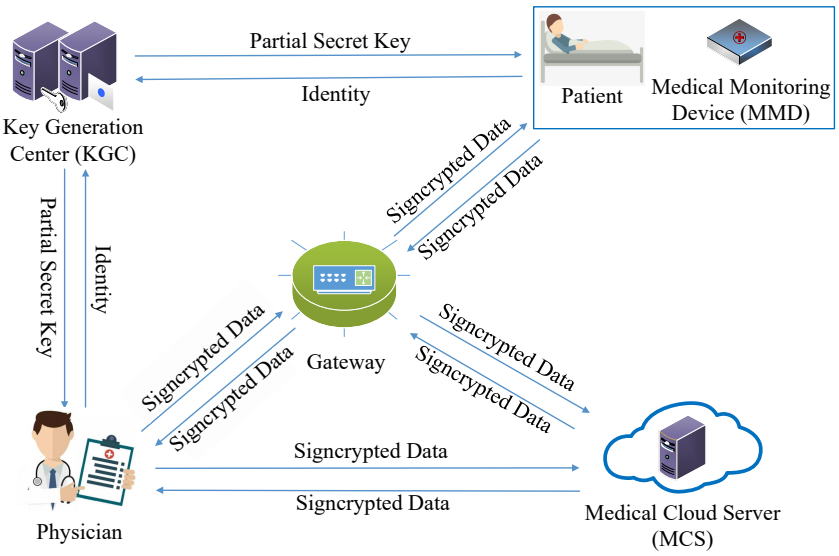

Fig. 2. The System Model of Our Proposed PQ-CLSCL Scheme.

outputs a public parameter pp and a master public-secret key pair (mpk, msk).

2) **Partial secret key Extract**(ID_i, pp) : Given a user with identity ID_i and a public parameter pp, this algorithm returns the user's partial secret key $\mathbf{psk}_i$.
3) **KeyGen**(ID_i, pp) : Given a user with identity ID_i and a public parameter pp, this algorithm calculates a secret key value $\mathbf{s}_i$ as intermediate and publishes a public-secret key pair (PK_i, SK_i) for ID_i.
4) **Signcrypt**$(pp, m, ID_S, ID_U, SK_S, PK_U)$: Given a public parameter pp, a medical message m, a signcrypt user ID_S with its secret key SK_S, and an unsigncrypt user ID_U with its public key PK_U, this algorithm outputs a ciphertext $\mathbf{c}$.
5) **Unsigncrypt**$(pp, \mathbf{c}, ID_S, PK_S, ID_U, SK_U)$: Given a public parameter pp, a ciphertext $\mathbf{c}$, a signcrypt user ID_S and its public key PK_S, and an unsigncrypt user ID_U and its secret key SK_U, this algorithm returns m or $\perp$.
6) **Link**$(\mathbf{c}_1, \mathbf{c}_2, \mathbf{l}_1, \mathbf{l}_2)$: Given two ciphertexts $\mathbf{c}_1, \mathbf{c}_2$ and two link labels $\mathbf{l}_1, \mathbf{l}_2$, this algorithm returns Link or Unlink.

D. Security Models

There are three security prerequisites for a secure PQ-CLSCL scheme, confidentiality, unforgeability, and linkability. Additionally, we need to consider two different types of malicious attackers (Type-I: $\mathcal{A}_I$ and Type-II: $\mathcal{A}_{II}$) interactive with a challenger $\mathcal{C}$ when designing the cryptographic primitive.

1) Security prerequisites
   - Confidentiality: A secure PQ-CLSCL primitive requires to satisfy IND-CCA2, describing through several interactive games between $\mathcal{A}_I$ or $\mathcal{A}_{II}$ together with $\mathcal{C}$.
   - Unforgeability: A requirement for a secure PQ-CLSCL primitive is to achieve EU-CMA, depicting between $\mathcal{A}_I$ or $\mathcal{A}_{II}$ together with $\mathcal{C}$.
   - Linkability: Our primitive also offers the linkability, illustrating between $\mathcal{A}_I$ or $\mathcal{A}_{II}$ together with $\mathcal{C}$.
   - Resistance to the Man-in-the-middle attack: Our PQ-CLSCL primitive can resist the Man-in-the-middle attack in a practical IoMT scenario.
   - Resistance to the impersonation attack: Our PQ-CLSCL primitive can resist the impersonation attack in a practical IoMT scenario.
2) Two types of adversaries
   - Type-I adversaries: A PPT adversary $\mathcal{A}_I$ has the ability to modify a user's public key PK_i but without learning any knowledge about the master secret key msk.
   - Type-II adversaries: A PPT adversary $\mathcal{A}_{II}$ masters the master secret key msk but can't modify a user's public key PK_i.

V. The Design of PQ-CLSCL

In this sector, we begin by illustrating the concrete construction of PQ-CLSCL scheme. Then, we give the parameters setting and the correctness analysis. To facilitate the understanding of our design, we provide two illustrations about the system initialization, and patient registration phases, as well as the ciphertext generation, decryption, and linkability checking phases, as depicted in Fig. 3 and Fig. 4, respectively.

A. Initialization Phase

The KGC initializes the whole system by executing the **Setup** algorithm with the system parameter n and security parameter λ as input, then this algorithm processes the following procedures to generate a public parameter pp and a master public-secret key pair (mpk, msk).

1) The KGC initially calls $q \leftarrow \mathsf{poly}(n)$, where q is a prime number. Then, KGC chooses $\alpha \xleftarrow{\$} \{0,1\}$ randomly.
2) The KGC also defines $\Theta = 2 \cdot n(\lceil \log q \rceil)$. After that, it calculates the error distribution parameter $B = q \cdot \alpha \cdot \omega(\sqrt{\log n})$.

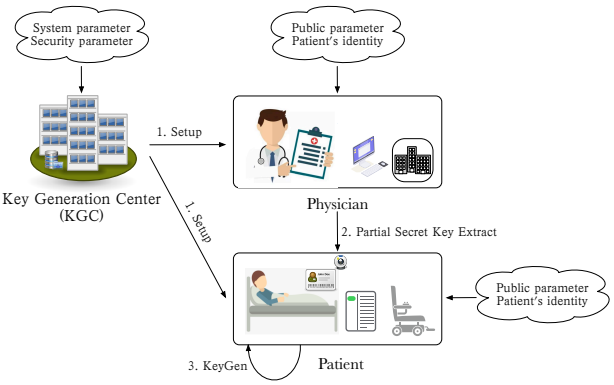

Fig. 3. An Illustration of System Initialization and Patient Registration Phases.

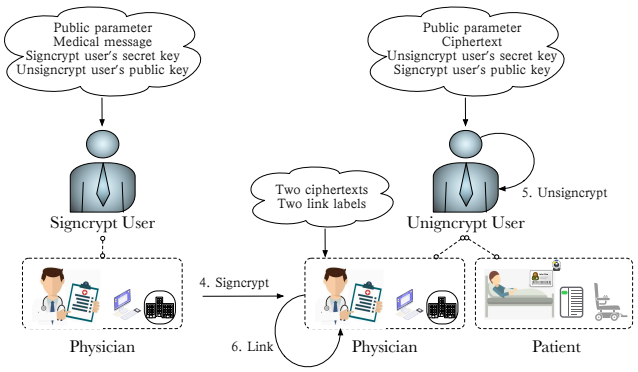

Fig. 4. An Illustration of Ciphertext Generation, Decryption, and Linkability Checking Phases.

3) The KGC sets gadget matrix $\mathbf{G} := \mathbf{I}_n \otimes \mathbf{g}^\top$, $\mathbf{g}^\top = [1, 2, \cdots, 2^{k-1}], k = \lceil \log q \rceil$.
4) The KGC selects two universal hash functions:

$$H_1 : \{0,1\}^* \times \{0,1\}^* \to \mathbb{Z}_q^n; \tag{4}$$

$$H_2 : \mathbb{Z}_q^{2n} \times \{0,1\}^* \to \{-1, 0, 1\}^k. \tag{5}$$

5) Moreover, the KGC executes the $\mathbf{TrapGen}(n, \Theta, q)$ algorithm to calculate $\mathbf{A} \in \mathbb{Z}_q^{n \times \Theta}$ and its basis $\mathbf{T} \in \mathbb{Z}_q^{\Theta \times \Theta}$.
6) In addition to this, KGC calculates a discrete Gaussian distribution $d = 4 \cdot \omega(\sqrt{\log n})$ and defines σ as the discrete Gaussian distribution parameter.
7) After that, the KGC defines master public key $mpk := \mathbf{A}$, master secret key $msk := \mathbf{T}$, and p as the lattice sampling parameter.
8) Ultimately, it returns a public parameter $pp := \{\mathbf{A}, \lambda, d, p, H_1, H_2\}$ and a master public-secret key pair (mpk, msk).

B. User Registration Phase

In the user registration phase, it contains two procedures to generate the public and secret keys for the patient. A medical entity (medical device or physician) firstly calculates and sends the partial secret key $\mathbf{psk}_i$ to the user with identity ID_i. Subsequently, the user calculates the public-secret key pair (PK_i, SK_i) by itself.

1) Generating the partial secret key: We describe the procedure to calculate the partial secret key. After taking a public parameter pp, and a user's identity ID_i as input, a medical entity extracts the partial secret key $\mathbf{psk}_i$ of user ID_i through the following **Partial secret key Extract** algorithm.

1) There are two user sets in the proposed scheme, namely the signcrypt users set and the unsigncrypt users set. We first define the signcrypt users set as $S := \{s_1, s_2, \cdots, s_\ell\}$, where ℓ is the total number of signcrypt users, $i \in [1, \ell]$, and $s_i \in \{0,1\}^*$. Then, we define the unsigncrypt users set $U := \{u_1, u_2, \cdots, u_\kappa\}$, where κ is the total number of unsigncrypt users, $i \in [1, \kappa]$, and $u_i \in \{0,1\}^*$.
2) The KGC calculates $\mathbf{u}_i = H_1(ID_i)$, where $ID_i \in \{S, U\} = \{s_1, s_2, \cdots, s_\ell, u_1, u_2, \cdots, u_\kappa\}$ denotes the general user.
3) The KGC parses $\bar{\mathbf{A}}$ through $\mathbf{A} = [\bar{\mathbf{A}} | \mathbf{G} - \bar{\mathbf{A}} | \mathbf{T}]$. After that, the KGC calls the $\mathbf{SamplePre}(\bar{\mathbf{A}}, \mathbf{T}, \mathbf{u}_i, p)$ algorithm to obtain the partial secret key $\mathbf{psk}_i$ of user ID_i, where $\mathbf{psk}_i \in \mathbb{Z}_q^\Theta$.
4) Ultimately, the KGC sends $\mathbf{psk}_i$ to the user ID_i via a secure private channel.

2) Generating the public-secret key: Now, we move to the second to obtain the public key and secret key of the user. The user first takes a public parameter pp together with its identity ID_i as input to perform the $\mathbf{KeyGen}$ algorithm. After that, it calculates the public-secret key pair (PK_i, SK_i) corresponding to ID_i according to the following steps.

1) The user ID_i chooses a secret value $\mathbf{s}_i \xleftarrow{\$} D_{\mathbb{Z},q\alpha}^n \in \mathbb{Z}_q^n$ randomly and denotes its secret key as $SK_i = (\mathbf{s}_i, \mathbf{psk}_i) \in \mathbb{Z}^n \times \mathbb{Z}^\Theta$.
2) After that, the user ID_i chooses a matrix $\mathbf{M}_i \xleftarrow{\$} \mathbb{Z}_q^{n \times m}$ and a vector $\mathbf{v}_i \xleftarrow{\$} D_{\mathbb{Z},q\alpha}^m \in \mathbb{Z}_q^m$ at random.
3) This algorithm calculates

$$\mathbf{m}_i = \mathbf{M}_i^\top \mathbf{x} + 2\mathbf{v}_i \bmod q \in \mathbb{Z}_q^m, \tag{6}$$

where vector $\mathbf{x} \leftarrow D_\sigma^n$ and $||\mathbf{x}|| \le 2\sigma\sqrt{m}$.
4) Then, this algorithm calculates $PK_i = (\mathbf{m}_i | \mathbf{M}_i^\top) \in \mathbb{Z}_q^{m \times (1+n)}$ as a public key of user ID_i.

C. Ciphertext Generation Phase

In this phase, a signcrypt user ID_S takes a public parameter pp, a medical message m together with its secret key SK_S and the public key PK_U of an unsigncrypt user ID_U as input. Then, the signcrypt user performs the following **Signcrypt** algorithm to generate the ciphertext $\mathbf{c}$ and returns it to the unsigncrypt user.

1) To begin with, a signcrypt user ID_S parses the SK_S as $\mathbf{psk}_S$, $\mathbf{s}_S$ and computes the link label $\mathbf{l}_S$ as $\mathbf{l}_S = \mathbf{psk}_S + \mathbf{A}^\top \mathbf{s}_S \in \mathbb{Z}_q^\Theta$.
2) A signcrypt user ID_S randomly chooses four vectors $\mathbf{r} \xleftarrow{\$} \{0,1\}, \mathbf{w} \xleftarrow{\$} D_{\mathbb{Z},q\alpha}^n, \mathbf{e}_1 \xleftarrow{\$} D_{\mathbb{Z},q\alpha}$, and $\mathbf{e}_2 \xleftarrow{\$} D_{\mathbb{Z},q\alpha}$.
3) It then randomly selects three values $\epsilon_1 \xleftarrow{\$} D_\sigma^l \in \mathbb{Z}^l, \epsilon_2 \xleftarrow{\$} D_\sigma^l \in \mathbb{Z}^l$, and $\epsilon_3 \xleftarrow{\$} D_\sigma^l \in \mathbb{Z}^l$, and also defines a vector $\epsilon = \begin{bmatrix} \epsilon_1 \\ \epsilon_2 \\ \epsilon_3 \end{bmatrix} \in \mathbb{Z}^{3l}$.

4) ID_S calculates two vectors:

$$\mathbf{g} = H_2(\begin{bmatrix} \mathbf{A} & \mathbf{A} & 0 \\ 0 & \mathbf{M}_U & \mathbf{M}_U \end{bmatrix} \epsilon, m), \tag{7}$$

and $\mathbf{t} = SK_S\mathbf{g} + \epsilon \in \mathbb{Z}^{3l}$, where $\epsilon \in \mathbb{Z}^{3l}, m \in \{0,1\}^*$.

5) ID_S calculates a signature $sig = sig' \cdot (0, 0, \cdots, \lceil \frac{q}{2} \rceil)^\top \in \mathbb{Z}_q^n$, where $sig' = \mathbf{t} + \mathbf{g}$ with probability $\mathsf{Prob} \geq \min(\frac{D_\sigma^{3l}(\mathbf{t})}{mD_{\sigma,\omega}^{3l}(\mathbf{t})}, 1)$.

6) Then, the signcrypt user ID_S calculates three ciphertext elements as below.

$$\mu_1 = \mathbf{M}_U\mathbf{r} + sig \in \mathbb{Z}_q^n, \tag{8}$$

$$\mu_2 = \mathbf{A}^\top\mathbf{w} + 2\mathbf{e}_2 \in \mathbb{Z}_q^\Theta, \tag{9}$$

$$\mu = (2\mathbf{v}_U + m + \langle \mathbf{w}, H_1(ID_S, ID_U)\rangle + \langle \mathbf{m}_U, \mathbf{r}\rangle) \bmod q. \tag{10}$$

7) Ultimately, ID_S defines and transmits the final ciphertext $\mathbf{c} = (\mu_1|\mu_2|\mu)$ and the link label $\mathbf{l}_S$ to ID_U.

D. Ciphertext Decryption Phase

The unsigncrypt user ID_U takes a public parameter pp, a ciphertext $\mathbf{c}$ together with its secret key SK_U and the public key PK_S of the signcrypt user ID_S as input. Then, an unsigncrypt user performs the **Unsigncrypt** algorithm to decrypt the ciphertext $\mathbf{c}$ and thereby obtain the medical message m.

1) An unsigncrypt user ID_U calculates

$$m = [\mu - \langle \mu_1, \mathbf{s}_U\rangle - \langle \mu_2, \mathbf{psk}_U\rangle]_q \bmod 2. \tag{11}$$

2) User ID_U calculates

$$\mathbf{g}' = H_2(\begin{bmatrix} \mathbf{A} & \mathbf{A} & 0 \\ 0 & \mathbf{M}_S & \mathbf{M}_S \end{bmatrix} \mathbf{t} - \begin{bmatrix} H_1(ID_S, ID_U) \\ PK_S \end{bmatrix} \mathbf{g}, m). \tag{12}$$

and verifies the two following conditions:

$$||\mathbf{t}|| \leq 2\sigma\sqrt{3l} \text{ and } \mathbf{g}' \stackrel{?}{=} \mathbf{g}. \tag{13}$$

3) If the verification passes, ID_U accepts the medical message m; Otherwise, ID_U outputs $\perp$, namely as the wrong medical message.

E. Ciphertext Linkability Checking Phase

The physician takes two ciphertexts $\mathbf{c}_1$, $\mathbf{c}_2$, and two link labels $\mathbf{l}_1$, $\mathbf{l}_2$ as input. Then, it performs the **Link** algorithm to directly check whether the two ciphertexts are generated by the same signcrypt user.

1) The physician checks if two ciphertexts $\mathbf{c}_1$, $\mathbf{c}_2$ are valid and refuses to answer if one ciphertext is invalid.
2) Then, it outputs 'link' if $\mathbf{l}_1 = \mathbf{l}_2$, and outputs 'unlink' otherwise.

F. Parameters Setting and Correctness Analysis

To enable the proposed scheme correctly and securely, we need to set several parameters as follows. For the security concern, we set $l \geq 5n \log q$. Then, considering the Gaussian parameter and discrete Gaussian distribution parameter, we need to make sure $s \geq \|\mathbf{T}\|\omega(\sqrt{\log n})$ and $\sigma \leq \alpha s\lambda\sqrt{6l}$. We also need to set the lattice sampling parameter $p = \sqrt{7(\mathsf{sv}(\mathbf{T})^2 + 1)}$, where $\mathsf{sv}(\mathbf{T})$ is the singular value of $\mathbf{T}$.

We hereby analyze the correctness of the proposed PQ-CLSCL scheme. Our **Signcrypt** algorithm is statistically indistinguishable from the distribution D_σ^{3l} according to the Lemma 1. In this way, we obtain $||\mathbf{t}|| \leq 2\sigma\sqrt{3l}$ with probability $\mathsf{Prob} \geq \min(\frac{D_\sigma^{3l}(\mathbf{t})}{mD_{\sigma,\omega}^{3l}(\mathbf{t})}, 1)$.

As for the unsigncrypt user ID_U, it has the following equations:

$$\begin{aligned} &\mu - \langle \mu_1, \mathbf{s}_U\rangle - \langle \mu_2, \mathbf{psk}_U\rangle \\ &= (2\mathbf{v}_U + m + \langle \mathbf{w}, H_1(ID_S, ID_U)\rangle + \\ &\quad \langle \mathbf{m}_U, \mathbf{r}\rangle) - \langle \mu_1, \mathbf{s}_U\rangle - \langle \mu_2, \mathbf{psk}_U\rangle \bmod q \\ &= 2(\mathbf{e}_1 + \mathbf{v}_S^\top r - \mathbf{psk}_U^\top \cdot \mathbf{e}_2) + m \bmod q. \end{aligned} \tag{14}$$

If $(\mathbf{e}_1 + \mathbf{v}_S^\top\mathbf{r} - \mathbf{psk}_U^\top \cdot \mathbf{e}_2) < \frac{q}{4}$ holds, then it has $2(\mathbf{e}_1 + \mathbf{v}_S^\top\mathbf{r} - \mathbf{psk}_U^\top \cdot \mathbf{e}_2) < \frac{q}{2}$. Therefore, it makes the following equation succeed:

$$m = [\mu - \langle \mu_1, \mathbf{s}_U\rangle - \langle \mu_2, \mathbf{psk}_U\rangle]_q \bmod 2. \tag{15}$$

For link correctness, a signcrypt user ID_S generates two ciphertexts $\mathbf{c}_1$ and $\mathbf{c}_2$ for messages m_1 and m_2 using the same secret key $sk_S = (\mathbf{psk}_S, \mathbf{s}_S)$ containing two link labels $\mathbf{l}_1 = \mathbf{psk}_S + \mathbf{A}^\top\mathbf{s}_S$ and $\mathbf{l}_2 = \mathbf{psk}_S + \mathbf{A}^\top\mathbf{s}_S$, respectively. Since $\mathbf{l}_1$, $\mathbf{l}_2$ are generated with the same matrix $\mathbf{A}$, if the signcrypt user generates the ciphertexts for the messages m_1, m_2 with the same secret key, then it must be the case that $\mathbf{l}_1 = \mathbf{l}_2$.

VI. Security Analysis

We first analyze the security of the PQ-CLSCL scheme with regard to confidentiality, unforgeability, and linkability. For tight security, our PQ-CLSCL scheme has to prove its security against two categories of adversaries, including Type-I adversary $\mathcal{A}_I$, which is an external entity capable of forging a user's public key; Type-II adversary $\mathcal{A}_I$, which refers to a compromised KGC that possesses the master secret key. We then give the informal analysis to show that our scheme can resist the Man-in-the-middle attack and impersonation attack.

A. Confidentiality

Theorem 3: If there exists a Type-I adversary $\mathcal{A}_I$ who has the ability to break IND-CCA2 of the proposed PQ-CLSCL scheme with a non-negligible advantage Adv_{LWE} in probability-polynomial time, then there exists an algorithm $\mathcal{B}_1$ can solve the LWE hardness within $Q_{KG} + Q_{PSK} + Q_{PKR} + Q_{SV}$ query time, where $Q_{KG}, Q_{PSK}, Q_{PKR}, Q_{SV}$ means $\mathcal{A}_I$ can perform key generation query, partial secret key query, public key replace query, and secret value query, respectively.

Proof Suppose there exists a challenger $\mathcal{C}$ who can perform the algorithm $\mathcal{B}_1$. We finished the security analysis through three games as below.

Game 0: We simulate a real security game for an adversary $\mathcal{A}_I$ between a challenger $\mathcal{C}$. Given a system parameter n, $\mathcal{C}$ initially executes $(pp, (mpk, msk)) \leftarrow \textbf{Setup}(n, \lambda)$. Then, $\mathcal{C}$ sends pp to $\mathcal{A}_I$ and keeps the master secret key msk secret. In this way, $\mathcal{A}_I$ knows nothing about the msk. In addition, the challenger $\mathcal{C}$ maintains three lists $\mathcal{O}_{H_1}^{list}$, $\mathcal{O}_{H_2}^{list}$, and $\mathcal{O}_{PK}^{list}$ to record H_1 oracle, H_2 oracle, and public key oracle, respectively. These lists are initialized empty.

- Query 1 phase: The adversary $\mathcal{A}_I$ performs several queries and the challenger $\mathcal{C}$ will respond the corresponding messages to $\mathcal{A}_I$ as the following paragraphs.
  1) H_1 Query: After obtained the H_1 query of user ID_i from $\mathcal{A}_I$, $\mathcal{C}$ looks up the $\mathcal{O}_{H_1}^{list}$ and returns the corresponding value $\mathbf{Hash}_i^1$ to $\mathcal{A}_I$ if the query $(ID_i, \mathbf{Hash}_i^1)$ has already in the $\mathcal{O}_{H_1}^{list}$; Otherwise, $\mathcal{C}$ selects $\mathbf{Hash}_i^1 \xleftarrow{\$} \mathbb{Z}_q^n$ randomly and inserts $(ID_i, \mathbf{Hash}_i^1)$ into the $\mathcal{O}_{H_1}^{list}$.
  2) H_2 Query: $\mathcal{A}_I$ firstly issues the H_2 query of medical message m, then $\mathcal{C}$ answers the corresponding value $\mathbf{Hash}^2$ to $\mathcal{A}_I$ if this query $(\mathbf{A}, \mathbf{M}_S, \epsilon, m)$ has already in the $\mathcal{O}_{H_2}^{list}$; Otherwise, $\mathcal{C}$ selects $\mathbf{Hash}^2 \xleftarrow{\$} \{-1, 0, 1\}^k$ and inserts $(\mathbf{A}, \mathbf{M}_S, \epsilon, m)$ into the $\mathcal{O}_{H_2}^{list}$.
  3) Public key request Query: After receiving the public key extract query of user ID_i from $\mathcal{A}_I$, $\mathcal{C}$ checks whether it exists $PK_i \in \mathcal{O}_{PK}^{list}$. If it holds, $\mathcal{C}$ will give PK_i to $\mathcal{A}_I$; Otherwise, $\mathcal{C}$ will calculate and give $PK_i \leftarrow (\mathbf{m}_i | \mathbf{M}_i^\top) \in \mathbb{Z}_q^{m \times (1+n)}$ to $\mathcal{A}_I$, and also insert $(\mathbf{ID}_i, *, *, \mathbf{s}_i, \mathbf{m}_i, \mathbf{M}_i, \mathbf{v}_i)$ into the $\mathcal{O}_{PK}^{list}$.
  4) Partial secret key extract Query: After obtaining the partial secret key extract query of user ID_i from adversary $\mathcal{A}_I$, the challenger $\mathcal{C}$ executes $\mathbf{psk}_i \leftarrow$ **Partial secret key Extract**(ID_i, pp). After that, $\mathcal{C}$ sends the $\mathbf{psk}_i$ to $\mathcal{A}_I$ and then inserts $(ID_i, *, \mathbf{psk}_i)$ into the $\mathcal{O}_{PK}^{list}$.
  5) Public key replace Query: $\mathcal{A}_I$ selects and sends a novel public key PK_i' to $\mathcal{C}$. Then, $\mathcal{C}$ retrieves the public key oracle list $\mathcal{O}_{PK}^{list}$ and updates PK_i to PK_i' corresponding to the ID_i.
  6) Secret key extract Query: After getting a query of user ID_i from adversary $\mathcal{A}_I$, $\mathcal{C}$ checks whether $(ID_i, PK_i) \in \mathcal{O}_{PK}^{list}$. If it holds and PK_i has not been replaced, $\mathcal{C}$ executes $SK_i \leftarrow \mathbf{KeyGen}(ID_i, pp)$ for ID_i. Then, $\mathcal{C}$ gives the SK_i to $\mathcal{A}_I$ and inserts (ID_i, SK_i) into the $\mathcal{O}_{PK}^{list}$. Otherwise, $\mathcal{C}$ aborts it.
  7) Signcrypt Query: To begin with, $\mathcal{C}$ chooses $S' \xleftarrow{\$} \{1, 2, \cdots, \lceil q \rceil\}$ at random. In addition, $\mathcal{A}_I$ chooses ID_S, ID_U, and m as the signcrypt user's identity, unsigncrypt user's identity, and a medical message, respectively. When acquiring a signcrypt query from $\mathcal{A}_I$, $\mathcal{C}$ verifies $ID_S \stackrel{?}{=} ID_{S'}$. If it holds, $\mathcal{C}$ processes and sends $\mathbf{c} \leftarrow \mathbf{Signcrypt}(pp, m, ID_S, ID_U, SK_S, PK_U)$ to $\mathcal{A}_I$. Otherwise, $\mathcal{C}$ performs the following operations:
     - $\mathcal{C}$ initially selects $\epsilon \xleftarrow{\$} \mathbb{Z}^{3l}$ and $\mathbf{M}_U \xleftarrow{\$} \mathbb{Z}_q^{n \times m}$.
     - Furthermore, $\mathcal{C}$ calculates
     $$\mathbf{g} = H_2(\begin{bmatrix} \mathbf{A} & \mathbf{A} & 0 \\ 0 & \mathbf{M}_U & \mathbf{M}_U \end{bmatrix} \epsilon, m), \tag{16}$$
     and inserts $(\mathbf{A}, \mathbf{M}_U, \epsilon, \mathbf{g})$ into $\mathcal{O}_{H_2}^{list}$.
     - Moreover, $\mathcal{C}$ calculates the signature $sig' = \mathbf{t} + \mathbf{g} = SK_S \mathbf{g} + \epsilon + \mathbf{g}$, $\mu_1 = \mathbf{M}_U r + sig$, $\mu_2 = \mathbf{A}^\top \mathbf{w} + 2\mathbf{e}_2$, and $\mu = (2\mathbf{v}_U + m + \langle \mathbf{w}, H_1(ID_S, ID_U) \rangle + \langle \mathbf{m}_U, \mathbf{r} \rangle) \bmod q$ accordingly.
     - Ultimately, $\mathcal{C}$ calculates the ciphertext $\mathbf{c} = (\mu_1 | \mu_2 | \mu)$ and sends it to $\mathcal{A}_I$.
  8) Unsigncrypt Query: At the beginning, $\mathcal{A}_I$ selects ID_S, ID_U, and m as the signcrypt user's identity, unsigncrypt user's identity, and a medical message, respectively. When acquiring a signcrypt query from $\mathcal{A}_I$, $\mathcal{C}$ verifies $ID_S \stackrel{?}{=} ID_{S'}$, where $S' \xleftarrow{\$} \{1, 2, \cdots, \lceil q \rceil\}$. If it holds, $\mathcal{C}$ calls and returns m or $\perp \leftarrow \mathbf{Unsigncrypt}(pp, \mathbf{c}, ID_S, PK_S, ID_U, SK_U)$ to $\mathcal{A}_I$; Otherwise, $\mathcal{C}$ manipulates the following steps: (1) $\mathcal{C}$ initially calculates $\mathbf{g}'$ as
     $$H_2(\begin{bmatrix} \mathbf{A} & \mathbf{A} & 0 \\ 0 & \mathbf{M}_S & \mathbf{M}_S \end{bmatrix} \mathbf{t} - \begin{bmatrix} H_1(ID_S, ID_U) \\ PK_S \end{bmatrix} \mathbf{g}, m). \tag{17}$$
     (2) After that, $\mathcal{C}$ calculates
     $$m = [\mu - \langle \mu_1, \mathbf{s}_U \rangle - \langle \mu_2, \mathbf{psk}_U \rangle]_q \bmod 2 \tag{18}$$
     (3) Finally, $\mathcal{C}$ verifies $\mathbf{g}' \stackrel{?}{=} \mathbf{g}$. If the equation holds, $\mathcal{C}$ publishes m to $\mathcal{A}_I$; Otherwise, $\mathcal{C}$ publishes $\perp$ to $\mathcal{A}_I$.
- Challenge phase: The adversary $\mathcal{A}_I$ chooses two different medical messages with same length (m_0, m_1) corresponding to the signcrypt user ID_S^* and unsigncrypt user ID_U^*. In the current query, $\mathcal{A}_I$ is not permitted to obtain SK_i of ID_U^*. At this time, we suppose that $\mathcal{C}$ has finished the H_1 Query, Public key request Query, Partial secret key extract Query, and Secret key extract Query. $\mathcal{C}$ responds to the challenge query as follows.
  1) If $ID_U^* \neq ID_S^{'}$, $\mathcal{C}$ will fail this game.
  2) Otherwise, $\mathcal{C}$ defines a vector $\epsilon^* = \begin{bmatrix} \epsilon_1 \\ \epsilon_2 \\ \epsilon_3 \end{bmatrix} \in \mathbb{Z}^{3l}$, where l is a positive number s.t. $l \geq 5n \log q$ and then selects $b \xleftarrow{\$} \{0, 1\}$ at random. After that, $\mathcal{C}$ computes several equations as below.
  $$\mathbf{g}^* = H_2(\begin{bmatrix} \mathbf{A} & \mathbf{A} & 0 \\ 0 & \mathbf{M}_U & \mathbf{M}_U \end{bmatrix} \epsilon^*, m_b), \tag{19}$$
  $$sig'^* = \mathbf{t}^* + \mathbf{g}^* = SK_S \mathbf{g}^* + \epsilon^* + \mathbf{g}^*, \tag{20}$$
  $$sig^* = sig'^* \cdot (0, 0, \cdots, \lceil \frac{q}{2} \rceil)^\top, \tag{21}$$
  $$\mu_1^* = \mathbf{M}_U \mathbf{r} + sig^* \tag{22}$$
  $$\mu_2^* = \mathbf{A}^\top \mathbf{w} + 2\mathbf{e}_2^* \tag{23}$$
  $$\mu^* = (2\mathbf{v}_U + m_b + \langle \mathbf{w}, H_1(ID_S^*, ID_U^*) \rangle + \langle \mathbf{m}_U, \mathbf{r} \rangle) \bmod q. \tag{24}$$

Ultimately, $\mathcal{C}$ sends the challenge ciphertext $\mathbf{c}^* = (\mu_1^*|\mu_2^*|\mu^*)$ to $\mathcal{A}_I$ and inserts $\mathbf{c}^*$ to $\mathcal{O}_{H_2}^{list}$.

This is the end of Query 1.

- Query 2 phase: In this query, the adversary $\mathcal{A}_I$ can access almost the same queries as in Query 1 except that $\mathcal{A}_I$ is forbidden to access the Partial Secret key extract Query and Secret key extract Query with inputting (ID_i^*, pp) and (ID_S^*, ID_U^*), respectively. Besides, $\mathcal{A}_I$ is also forbidden to access the Unsigncrypt Query by inputting $\mathbf{c}^*$.
- Guess phase: Finally, $\mathcal{A}_I$ outputs a guess b'. Then, $\mathcal{C}$ verifies if $b' \stackrel{?}{=} b$. If it holds, $\mathcal{C}$ will output a solution of the LWE hardness; Otherwise, $\mathcal{C}$ will output $\perp$.

We define $Adv_{\mathcal{A}_I}^{\widehat{\textbf{Game 0}}}(\lambda)$ as the advantage of $\mathcal{A}_I$ wins the $\widehat{\textbf{Game 0}}$.

$\widehat{\textbf{Game 1}}$: This game is identical to $\widehat{\textbf{Game 0}}$, except for $\mathbf{psk}_i$ in the partial secret key extract Query. Concretely, $\mathcal{C}$ chooses $\mathbf{psk}_i \stackrel{\$}{\leftarrow} D_{\mathbb{Z}^\Theta, p\cdot\omega(\log n)}$ randomly and then computes $\mathbf{u}_i = \mathbf{A}\mathbf{psk}_i$. If $\mathbf{u}_i \notin \mathcal{O}_{H_1}^{list}$, $\mathcal{C}$ defines $H_1(ID_i) = \mathbf{u}_i$; If $\mathbf{u}_i \in \mathcal{O}_{H_1}^{list}$, $\mathcal{C}$ recalculates $\mathbf{psk}_i \leftarrow$ **Partial secret key Extract**(ID_i, pp).

We define $Adv_{\mathcal{A}_I}^{\widehat{\textbf{Game 1}}}(\lambda)$ as the advantage of $\mathcal{A}_I$ wins the $\widehat{\textbf{Game 1}}$.

As for $\mathcal{A}_I$, $\widehat{\textbf{Game 1}}$ and $\widehat{\textbf{Game 0}}$ are statistically indistinguishable due to the philosophy of the lattice sampling algorithm. Consequently, we obtain:

$$|Adv_{\mathcal{A}_I}^{\widehat{\textbf{Game 1}}}(\lambda) - Adv_{\mathcal{A}_I}^{\widehat{\textbf{Game 0}}}(\lambda)| \leq \textbf{negl}(\lambda). \tag{25}$$

$\widehat{\textbf{Game 2}}$: This game is identical to $\widehat{\textbf{Game 1}}$, except changing the calculation method of master public key $mpk := \mathbf{A}$. More concretely, we specify the process as follows.

- Setup phase: To begin with, $\mathcal{C}$ executes $pp \leftarrow \mathbf{Setup}(n, \lambda)$ to achieve the randomness for $\mathbf{A}$. Then, $\mathcal{C}$ sends the public parameter pp to $\mathcal{A}_I$.
- Query phase: In $\widehat{\textbf{Game 2}}$, $\mathcal{A}_I$ can nearly access the same queries as in the $\widehat{\textbf{Game 0}}$, excepting two queries.
  1) Partial secret key extract Query: After obtaining the partial secret key extract query of user ID_i from $\mathcal{A}_I$, $\mathcal{C}$ executes $\mathbf{psk}_i \leftarrow$ **Partial secret key Extract**(ID_i, pp) and also obtains $\mathbf{u}_i = H_1(ID_i)$. After that, $\mathcal{C}$ sends the $\mathbf{psk}_i$ to $\mathcal{A}_I$ and then inserts $(ID_i, \mathbf{u}_i, \mathbf{psk}_i)$ into the $\mathcal{O}_{PK}^{list}$.
  2) Public key replace Query: $\mathcal{C}$ replaces $PK_i = (ID_i, \mathbf{u}_i, \mathbf{psk}_i, SK_S\mathbf{g}, \mathbf{m}_i, \mathbf{M}_i, \mathbf{v}_i)$ to $PK_i^{'} = (ID_i, \mathbf{u}_i, \mathbf{psk}_i, *, \mathbf{m}_i, \mathbf{M}_i, *)$.
- Challenge phase: The adversary $\mathcal{A}_I$ selects and also sends two different medical message m_0, m_1 and two users (ID_S^*, ID_U^*) to $\mathcal{C}$. Then, $\mathcal{C}$ performs the following operations to reply $\mathcal{A}_I$.
  - If $ID_U^* = ID_{S'}$, $\mathcal{C}$ has acquired one of the two items $((ID_U^*, \mathbf{u}^*, *, *, *, *, *)$ or $(ID_U^*, \mathbf{u}^*, *, SK_S\mathbf{g}, \mathbf{m}_{S'}, \mathbf{M}', \mathbf{v}'))$, which means the public key $PK_{ID_U^*}$ has been replaced and has not been replaced, respectively.
    - If $PK_{ID_U^*}$ has been replaced, $\mathcal{C}$ verifies the validation of $PK_{ID_U^*}$ as below.
      - If it passes the verification, $\mathcal{C}$ updates $PK_{ID_U^*}$ to $PK_{ID_S'} = (\mathbf{m}_{ID_S'}|\mathbf{M}_{ID_S'}^\top)$. After that, $\mathcal{C}$ chooses $\epsilon \stackrel{\$}{\leftarrow} \mathbb{Z}_q^{n+1}$ and $\varsigma \in \{0,1\}^m$ at random. In addition, $\mathcal{C}$ sends two items $(\mathbf{m}'_{S'}, \mathbf{M}'_{S'}, \epsilon)$ and $(\mathbf{m}'_{S'}, \mathbf{M}'_{S'}, (\varsigma^\top \mathbf{m}'_{S'}|\mathbf{M}'_{S'}\varsigma))$ to $\mathcal{A}_I$. We say that $PK_{ID_S'}$ is valid if $\mathcal{A}_I$ can distinguish $(\mathbf{m}'_{S'}, \mathbf{M}'_{S'}, \epsilon)$ and $(\mathbf{m}'_{S'}, \mathbf{M}'_{S'}, (\varsigma^\top \mathbf{m}'_{S'}|\mathbf{M}'_{S'}\varsigma))$ with overwhelming probability.
      - Otherwise, $\mathcal{C}$ aborts the game.
    - If $PK_{ID_U^*}$ has not been replaced, $\mathcal{C}$ chooses $\epsilon \stackrel{\$}{\leftarrow} \mathbb{Z}_q^{n+1}$ and $\varsigma \stackrel{\$}{\leftarrow} \{0,1\}^m$ randomly. After that, $\mathcal{C}$ sends two items $(\mathbf{m}'_{S'}, \mathbf{M}'_{S'}, \epsilon)$ and $(\mathbf{m}'_{S'}, \mathbf{M}'_{S'}, (\varsigma^\top \mathbf{m}'_{S'}|\mathbf{M}'_{S'}\varsigma))$ to $\mathcal{A}_I$. We say that $PK_{ID_S'}$ is valid if $\mathcal{A}_I$ can distinguish $(\mathbf{m}'_{S'}, \mathbf{M}'_{S'}, \epsilon)$ and $(\mathbf{m}'_{S'}, \mathbf{M}'_{S'}, (\varsigma^\top \mathbf{m}'_{S'}|\mathbf{M}'_{S'}\varsigma))$ with overwhelming probability.

    Finally, $\mathcal{C}$ returns the challenge ciphertext $c^* = (\mu_1^*, \mu_2^*, \mu^*) = (\mu', \mathbf{w}^\top \mathbf{u}_{S'}, \mathbf{M}^\top \mathbf{w} + 2\mathbf{v}_U)$ to $\mathcal{A}_I$.
  - If $ID_U^* \neq ID_{S'}$, $\mathcal{C}$ terminates this game and returns $\perp$ to $\mathcal{A}_I$.
- Guess phase: Ultimately, $\mathcal{A}_I$ outputs a guess b'. Then, $\mathcal{C}$ verifies if $b' \stackrel{?}{=} b$. If it holds, $\mathcal{C}$ will output a solution of the LWE hardness; Otherwise, $\mathcal{C}$ will output $\perp$.

We define $Adv_{\mathcal{A}_I}^{\widehat{\textbf{Game 2}}}(\lambda)$ as the advantage of $\mathcal{A}_I$ wins the $\widehat{\textbf{Game 2}}$.

As for $\mathcal{A}_I$, $\widehat{\textbf{Game 2}}$ and $\widehat{\textbf{Game 1}}$ are statistically indistinguishable according to Theorem 1. Thus, we have:

$$|Adv_{\mathcal{A}_I}^{\widehat{\textbf{Game 2}}}(\lambda) - Adv_{\mathcal{A}_I}^{\widehat{\textbf{Game 1}}}(\lambda)| \leq \textbf{negl}(\lambda). \tag{26}$$

In summary, we say

$$\begin{aligned} &Adv_{LWE} - |Adv_{\mathcal{A}_I}^{\widehat{\textbf{Game 2}}}(\lambda) - \frac{1}{2}| \\ &\leq |Adv_{\mathcal{A}_I}^{\widehat{\textbf{Game 0}}}(\lambda) - Adv_{\mathcal{A}_I}^{\widehat{\textbf{Game 1}}}(\lambda)| + \\ &|Adv_{\mathcal{A}_I}^{\widehat{\textbf{Game 1}}}(\lambda) - Adv_{\mathcal{A}_I}^{\widehat{\textbf{Game 2}}}(\lambda)| \leq \textbf{negl}(\lambda). \end{aligned} \tag{27}$$

□

Theorem 4: If there exists a Type-II adversary $\mathcal{A}_{II}$ who has the ability to break IND-CCA2 of the proposed PQ-CLSCL scheme with a non-negligible advantage Adv'_{LWE} in probabilistic polynomial time, then there exists an algorithm $\mathcal{B}_2$ can solve the LWE hardness within $Q_{KG} + Q_{PSK} + Q_{SV}$ query time, where Q_{KG}, Q_{PSK}, Q_{SV} means $\mathcal{A}_{II}$ can perform key generation query, partial secret key query, and secret value query, respectively.

Proof Suppose there exists a challenger $\mathcal{C}$ who can perform the algorithm $\mathcal{B}_2$. We finished the security analysis below.

- Setup phase: $\mathcal{C}$ executes $(pp, (mpk, msk)) \leftarrow \mathbf{Setup}(n, \lambda)$. Then $\mathcal{C}$ transmits pp and msk to $\mathcal{A}_{II}$.
- Query phase: In this phase, $\mathcal{A}_{II}$ can access almost exactly the same queries as in the former theorem except the

following. Public key request Query: After obtaining this query of user ID_i from $\mathcal{A}_{II}$, $\mathcal{C}$ checks whether $ID_i \stackrel{?}{=} ID_{S'}$. If it holds, $\mathcal{C}$ will update $\mathbf{M}_{ID_{S'}} = \mathbf{M}^*$ and $\mathbf{m}_{ID_{S'}} = \mathbf{m}^*$; Otherwise, $\mathcal{C}$ randomly chooses $\mathbf{M}_i \stackrel{\$}{\leftarrow} \mathbb{Z}_q^{n\times m}$, $\mathbf{v}_i \stackrel{\$}{\leftarrow} D^m_{\mathbb{Z},q\alpha}$, and $SK_i\mathbf{g} \stackrel{\$}{\leftarrow} D^n_{\mathbb{Z},q\alpha}$. Then, $\mathcal{C}$ computes $\mathbf{m}_i = 2\mathbf{v}_i + \mathbf{M}_i^\top SK_i\mathbf{g} \bmod q$. Lastly, $\mathcal{C}$ inserts $(ID_i, \mathbf{m}_i, \mathbf{M}_i, \mathbf{v}_i)$ into the $\mathcal{O}^{list}_{H_1}$ and returns $(ID_i, \mathbf{m}_i, \mathbf{M}_i)$ to the adversary $\mathcal{A}_{II}$.

- Challenge phase: $\mathcal{A}_{II}$ chooses and sends two different medical messages with same length (m_0, m_1) corresponding to the signcrypt user ID^*_S and unsigncrypt user ID^*_U to $\mathcal{C}$. Then, $\mathcal{C}$ verifies if $ID^*_U \stackrel{?}{=} ID_{S'}$.
  1) If the equation holds, $\mathcal{C}$ will terminate the challenge query and return $\perp$;
  2) Otherwise, $\mathcal{C}$ accesses the list $\mathcal{O}^{list}_{H_1}$ and then executes $\mathbf{psk}_{ID_{S'}} \leftarrow$ **Partial secret key Extract**$(ID_{S'}, pp)$. $\mathcal{C}$ also calculates $\mathbf{Hash}^1_{S'} = H_1(ID_{S'})$. Eventually, $\mathcal{C}$ transmits the challenge ciphertext $\mathbf{c}^* = (\mu^*_1|\mu^*_2|\mu^*) = (\mu', \mathbf{w}^\top\mathbf{u}_{S'}, \mathbf{M}^\top\mathbf{w} + 2\mathbf{v}_U)$ to $\mathcal{A}_{II}$.
- Guess: Ultimately, $\mathcal{A}_{II}$ outputs a guess b'. Then, $\mathcal{C}$ verifies if $b' \stackrel{?}{=} b$. If it holds, $\mathcal{C}$ will output a solution of the LWE hardness; Otherwise, $\mathcal{C}$ will output $\perp$. The probability Adv'_{LWE} for this theorem is analogous to the former.

□

B. Unforgeability

Theorem 5: If there exists a Type-I adversary $\mathcal{A}_I$ who has the ability to break EU-CMA of PQ-CLSCL primitive within a non-negligible advantage Adv_{SIS} in probability-polynomial time, then there exists an algorithm $\mathcal{B}_3$ can solve the SIS hardness with probability $Adv_{SIS} = Adv_{A_I} \cdot (1 - 2^{-\omega(\log n)})$.

Proof Assume that there exists a challenger $\mathcal{C}$ who can perform the algorithm $\mathcal{B}_3$ and an adversary $\mathcal{A}_I$ can counterfeit a ciphertext. We finished the security analysis below.

- Setup phase: A challenger $\mathcal{C}$ performs $(pp, (mpk, msk)) \leftarrow \mathbf{Setup}(n, \lambda)$. Then $\mathcal{C}$ sends pp to $\mathcal{A}_I$ and keeps msk in secret. In this way, $\mathcal{A}_I$ knows nothing about the msk. Moreover, the challenger $\mathcal{C}$ maintains three lists $\mathcal{O}^{list}_{H_1}$, $\mathcal{O}^{list}_{H_2}$, and $\mathcal{O}^{list}_{PK}$ to record H_1 oracle, H_2 oracle, and public key oracle, respectively. These lists are initialized empty at the beginning.
- Query phase: The adversary $\mathcal{A}_I$ can access several queries and the challenger $\mathcal{C}$ then replies the corresponding response to $\mathcal{A}_I$. The query regulations are identical to Query 1 in Theorem 4.
- Forge phase: $\mathcal{A}_I$ forges and delivers $\mathbf{c}^* = (\mu^*_1|\mu^*_2|\mu^*)$ of the challenge signcrypt user and unsigncrypt user (ID^*_S, ID^*_U) to $\mathcal{C}$. We say that $\mathcal{C}$ succeeds when the challenge ciphertext is valid. Furthermore, $\mathcal{A}_I$ forges $\mathbf{c} = (\mu_1|\mu_2|\mu)$ of the challenge signcrypt user and unsigncrypt user (ID^*_S, ID^*_U). Accordingly, we have:

$$\begin{bmatrix}\mathbf{A} & \mathbf{A} & 0\\ 0 & \mathbf{M}_U & \mathbf{M}_U\end{bmatrix}\mathbf{t}^* - \begin{bmatrix}H_1(ID^*_S, ID^*_U)\\ PK_{U^*}\end{bmatrix}\mathbf{g}^* = \begin{bmatrix}\mathbf{A} & \mathbf{A} & 0\\ 0 & \mathbf{M}_U & \mathbf{M}_U\end{bmatrix}\mathbf{t}' - \begin{bmatrix}H_1(ID^*_S, ID^*_U)\\ PK_{U^*}\end{bmatrix}\mathbf{g}' \tag{28}$$

We obtain that $\mathbf{M}(\mathbf{t}^* - \mathbf{t}' + \mathbf{psk}_U(\mathbf{g}' - \mathbf{g}^*)) = 0$, where $\mathbf{t}^* \le 2\sigma\sqrt{3l}$, $\mathbf{t}' \le 2\sigma\sqrt{3l}$, $\mathbf{g}' \le \lambda$, and $\mathbf{g}^* \le \lambda$. Consequently, we can say that

$$\frac{\mathbf{t}^* - \mathbf{t}' + \mathbf{psk}_U(\mathbf{g}' - \mathbf{g}^*)}{4} \le s\lambda\sqrt{2l} + 2\sigma\sqrt{2l}$$

is satisfied with overwhelming probability.

Therefore, the probability to solve the SIS hardness is $Adv_{SIS} = Adv_{A_I} \cdot (1 - 2^{-\omega(\log n)})$ since the probability of $\mathbf{t}^* - \mathbf{t}' + \mathbf{psk}_U(\mathbf{g}' - \mathbf{g}^*) = 0$ is less than $(1 - 2^{-\omega(\log n)})$ due to the nature of lattice sampling algorithm [47].

□

Theorem 6: If there exists a Type-II adversary $\mathcal{A}_{II}$ who has the ability to break EU-CMA of the PQ-CLSCL primitive within a non-negligible advantage Adv'_{SIS} in probability-polynomial time, then there exists an algorithm $\mathcal{B}_4$ can solve the SIS hardness with probability $Adv'_{SIS} = Adv_{A_{II}} \cdot (1 - 2^{-\omega(\log n)})$.

Proof Suppose there exists a challenger $\mathcal{C}$ who can perform the algorithm $\mathcal{B}_4$ and an adversary $\mathcal{A}_{II}$ can counterfeit a ciphertext. We finished the security analysis below.

- Setup phase: A challenger $\mathcal{C}$ performs $(pp, (mpk, msk)) \leftarrow \mathbf{Setup}(n, \lambda)$. Then $\mathcal{C}$ sends pp to $\mathcal{A}_{II}$ and keeps msk in secret. In this way, $\mathcal{A}_I$ knows nothing about the msk. Besides, the challenger $\mathcal{C}$ maintains three lists $\mathcal{O}^{list}_{H_1}$, $\mathcal{O}^{list}_{H_2}$, and $\mathcal{O}^{list}_{PK}$, which are identical to the former theorem.
- Query phase: The adversary $\mathcal{A}_{II}$ can access several queries and the challenger $\mathcal{C}$ then replies the corresponding response to $\mathcal{A}_{II}$. The query regulations are the same as the Query phase in Theorem 5.
- Forge phase: $\mathcal{A}_{II}$ forges and delivers $\mathbf{c}^* = (\mu^*_1|\mu^*_2|\mu^*)$ of the challenge signcrypt user and unsigncrypt user (ID^*_S, ID^*_U) to $\mathcal{C}$. We say that $\mathcal{C}$ succeeds when the challenge ciphertext is not $\perp$. Moreover, $\mathcal{A}_{II}$ can also forges $\mathbf{c} = (\mu_1|\mu_2|\mu)$ of the challenge signcrypt user and unsigncrypt user (ID^*_S, ID^*_U). Thus, we have the following equalities:

$$\begin{bmatrix}\mathbf{A} & \mathbf{A} & 0\\ 0 & \mathbf{M}_U & \mathbf{M}_U\end{bmatrix}\mathbf{t}^* - \begin{bmatrix}H_1(ID^*_S, ID^*_U)\\ PK_{U^*}\end{bmatrix}\mathbf{g}^* = \begin{bmatrix}\mathbf{A} & \mathbf{A} & 0\\ 0 & \mathbf{M}_U & \mathbf{M}_U\end{bmatrix}\mathbf{t}' - \begin{bmatrix}H_1(ID^*_S, ID^*_U)\\ PK_{U^*}\end{bmatrix}\mathbf{g}' \tag{29}$$

We acquire that $\mathbf{M}(\mathbf{t}^* - \mathbf{t}' + \mathbf{psk}_U(\mathbf{g}' - \mathbf{g}^*)) = 0$, where $\mathbf{t}^* \le 2\sigma\sqrt{3l}$, $\mathbf{t}' \le 2\sigma\sqrt{3l}$, $\mathbf{g}' \le \lambda$, and $\mathbf{g}^* \le \lambda$. Hence,

$$\frac{\mathbf{t}^* - \mathbf{t}' + \mathbf{psk}_U(\mathbf{g}' - \mathbf{g}^*)}{4} \le s\lambda\sqrt{2l} + 2\sigma\sqrt{2l}$$

is satisfied with overwhelming probability.

To conclude, the probability of solving the SIS hardness is $Adv'_{SIS} = Adv_{A_I} \cdot (1 - 2^{-\omega(\log n)})$ since the probability of $\mathbf{t}^* - \mathbf{t}' + \mathbf{psk}_U(\mathbf{g}' - \mathbf{g}^*) = 0$ is lower than $(1 - 2^{-\omega(\log n)})$ due to the nature of lattice sampling algorithm [47].

□

C. Linkability

Theorem 7: The proposed PQ-CLSCL primitive is linkable if the PQ-CLSCL primitive is unforgeable under the Type-I adversary $\mathcal{A}_I$ attacks based on SIS hardness.

Proof We assume that there exists a Type-I adversary $\mathcal{A}_I$ who tries to break the linkability of the PQ-CLSCL primitive and a challenger $\mathcal{C}$ can respond to queries of $\mathcal{A}_I$.

- Setup phase: A challenger $\mathcal{C}$ performs $(pp, (mpk, msk)) \leftarrow \mathbf{Setup}(n, \lambda)$. Then $\mathcal{C}$ sends pp to $\mathcal{A}_I$ and keeps msk in secret. In this way, $\mathcal{A}_I$ knows nothing about the msk. Moreover, the challenger $\mathcal{C}$ maintains three lists $\mathcal{O}_{H_1}^{list}$, $\mathcal{O}_{H_2}^{list}$, and $\mathcal{O}_{PK}^{list}$ to record H_1 oracle, H_2 oracle, and public key oracle, respectively. These lists are initialized empty at the beginning.
- Query phase: The adversary $\mathcal{A}_I$ can access several queries and the challenger $\mathcal{C}$ then replies the corresponding response to $\mathcal{A}_I$. The query regulations are identical to Theorem 6.
- Unlink phase: $\mathcal{A}_I$ outputs two tuples $(\mathbf{c}_1^* = (\mu_{11}^*|\mu_{21}^*|\mu_1^*), \mathbf{l}_1^*)$ and $(\mathbf{c}_2^* = (\mu_{12}^*|\mu_{22}^*|\mu_2^*), \mathbf{l}_2^*)$, where $\mathbf{c}_i^*$ is ciphertext and $\mathbf{l}_i^*$ is the link label.

Analysis. We assume that $\mathcal{A}_I$ generates two ciphertexts $\mathbf{c}_1^*$, $\mathbf{c}_2^*$ with non-negligible probability while holding only one secret key, and both $\mathbf{c}_1^*$, $\mathbf{c}_2^*$ are valid. Since our PQ-CLSCL scheme satisfies the unforgeability, these two ciphertexts can pass the verification only if the $\mathcal{A}_I$ honestly generates the ciphertexts $\mathbf{c}_1^*$, $\mathbf{c}_2^*$.

When $\mathcal{A}_I$ generates the two ciphertexts, we have two link labels $\mathbf{l}_1^* = \mathbf{psk}_1^* + \mathbf{A}^{\top^*}\mathbf{s}_1^*$, $\mathbf{l}_2^* = \mathbf{psk}_2^* + \mathbf{A}^{\top^*}\mathbf{s}_2^*$ respectively. Since $\mathcal{A}_I$ only has one secret key, then $\mathbf{psk}_1^* = \mathbf{psk}_2^*$ and $\mathbf{s}_1^* = \mathbf{s}_2^*$. Moreover, as the matrix $\mathbf{A}^{\top^*}$ is the same, we get $\mathbf{l}_1^* = \mathbf{l}_2^*$. It shows that the two tuples of $\mathcal{A}_I$ verified by the **Link** algorithm will return 'link', which contradicts the assumption of the linkability game. Therefore, the advantage of $\mathcal{A}_I$ is negligible and our PQ-CLSCL scheme is linkable. □

Theorem 8: The proposed PQ-CLSCL primitive is linkable if the PQ-CLSCL primitive is unforgeable under the Type-II adversary $\mathcal{A}_{II}$ attacks based on SIS hardness.

Proof We assume that there exists a Type-II adversary $\mathcal{A}_{II}$ who tries to break the linkability of the PQ-CLSCL primitive and a challenger $\mathcal{C}$ can respond to queries of $\mathcal{A}_{II}$.

- Setup phase: A challenger $\mathcal{C}$ performs $(pp, (mpk, msk)) \leftarrow \mathbf{Setup}(n, \lambda)$. Then $\mathcal{C}$ sends pp to $\mathcal{A}_{II}$ and keeps msk in secret. In this way, $\mathcal{A}_I$ knows nothing about the msk. Besides, the challenger $\mathcal{C}$ maintains three lists $\mathcal{O}_{H_1}^{list}$, $\mathcal{O}_{H_2}^{list}$, and $\mathcal{O}_{PK}^{list}$, which are identical to the former theorem.
- Query phase: The adversary $\mathcal{A}_{II}$ can access several queries and the challenger $\mathcal{C}$ then replies the corresponding response to $\mathcal{A}_{II}$. The query regulations are the same as Theorem 7.
- Unlink phase: $\mathcal{A}_{II}$ outputs two tuples $(\mathbf{c}_1^* = (\mu_{11}^*|\mu_{21}^*|\mu_1^*), \mathbf{l}_1^*)$ and $(\mathbf{c}_2^* = (\mu_{12}^*|\mu_{22}^*|\mu_2^*), \mathbf{l}_2^*)$, where $\mathbf{c}_i^*$ is ciphertext and $\mathbf{l}_i^*$ is the link label.

Analysis. We assume that $\mathcal{A}_{II}$ generates two ciphertexts $\mathbf{c}_1^*$, $\mathbf{c}_2^*$ with non-negligible probability while holding only one secret key, and both $\mathbf{c}_1^*$, $\mathbf{c}_2^*$ are valid. Since our PQ-CLSCL scheme satisfies the unforgeability, these two ciphertexts can pass the verification only if the $\mathcal{A}_I$ honestly generates the ciphertexts $\mathbf{c}_1^*$, $\mathbf{c}_2^*$.

When $\mathcal{A}_{II}$ generates the two ciphertexts, we have two link labels $\mathbf{l}_1^* = \mathbf{psk}_1^* + \mathbf{A}^{\top^*}\mathbf{s}_1^*$, $\mathbf{l}_2^* = \mathbf{psk}_2^* + \mathbf{A}^{\top^*}\mathbf{s}_2^*$ respectively. Since $\mathcal{A}_I$ only has one secret key, then $\mathbf{psk}_1^* = \mathbf{psk}_2^*$ and $\mathbf{s}_1^* = \mathbf{s}_2^*$. Moreover, as the matrix $\mathbf{A}^{\top^*}$ is the same, we get $\mathbf{l}_1^* = \mathbf{l}_2^*$. It shows that the two tuples of $\mathcal{A}_I$ verified by the **Link** algorithm will return 'link', which contradicts the assumption of the linkability game. Therefore, the advantage of $\mathcal{A}_{II}$ is negligible and our PQ-CLSCL scheme is linkable. □

D. Informal Security Analysis

Theorem 9: The proposed PQ-CLSCL can resist the Man-in-the-middle attack.

Informal Analysis. When each entity sends a request with regard to the public-secret key generation, ciphertext generation, the user has to generate several new random parameters, such as the secret value $\mathbf{s}_i \xleftarrow{\$} D_{\mathbb{Z},q\alpha}^n \in \mathbb{Z}_q^n$, $\epsilon_1 \xleftarrow{\$} D_\sigma^l \in \mathbb{Z}^l, \epsilon_2 \xleftarrow{\$} D_\sigma^l \in \mathbb{Z}^l$, and $\epsilon_3 \xleftarrow{\$} D_\sigma^l \in \mathbb{Z}^l$, etc. As for the ciphertext decryption process, if an adversary tends to launch a Man-in-the-middle attack, it cannot pass the verification procedure. In a nutshell, the proposed PQ-CLSCL scheme possesses the capability to counteract the Man-in-the-middle attack.

Theorem 10: The proposed PQ-CLSCL can resist the impersonation attack.

Informal Analysis. A malicious attacker may attempt to impersonate an unsigncrypt user to decrypt the ciphertext. Regarding this, the attacker must be able to calculate the message $m = [\mu - \langle \mu_1, \mathbf{s}_U \rangle - \langle \mu_2, \mathbf{psk}_U \rangle]_q \bmod 2$. However, the attacker cannot know the value of the user's partial secret key $\mathbf{psk}_U$ as it was generated by the real user. In addition, the user also needs to calculate $\mathbf{g}'$ and checks if $\mathbf{g}' \stackrel{?}{=} \mathbf{g}$ succeed. Therefore, our scheme can protect against impersonation attacks.

VII. Performance Evaluation and Comparison

In this sector, we perform a comparative analysis of our scheme with other existing signcryption schemes [21], [22], [23], [24], [25], [26], [27], [28], [29], [30], [31], [32] in the context of both computational overhead and communication overhead [1]. Specifically, our simulation is conducted on a Dell Alienware M15 R5 laptop in the Win 10 operation system with a processor of AMD Ryzen 7 5800H, Radeon Graphics at 3.20 GHz, and running memory of 16.0 GB with NVME 512 GB SSD. Notably, we only consider the most time-consuming operations in our comparison, such as vector multiplication operation, vector additive operation, scalar multiplication on bilinear pairing group, pairing operation, preimage sampling algorithm, modular inversion operation, and hash-to-point operation. For convenience, all the symbols used in our efficiency analysis are given along with their specific meanings as elaborated in Table II. The running time of the seven operations involved in our compared schemes is shown in Table III, where each data represents the average of 50 iterations.

[1]We omit the computational overhead and communication overhead comparison of schemes [21], [22], [29], and [30] since these schemes are not resistant to quantum attacks (shown in Table VI).

TABLE II
SYMBOLS AND DESCRIPTION OF PERFORMANCE EVALUATION

Symbols	Description
T_{vmul}	The time of vector multiplication operation.
T_{vadd}	The time of vector additive operation.
T_{smul}	The time of scalar multiplication on bilinear pairing group.
T_{pair}	The time of pairing operation.
T_{gs}	The time of Gaussian sampling algorithm.
T_{pis}	The time of pre-image sampling algorithm.
T_{minv}	The time of modular inversion operation.
T_{htp}	The time of hash-to-point operation.
$\|G_{pair}\|$	The length of elements in bilinear pairing group.
$\|Z_q^*\|$	The length of elements in $\|Z_q^*\|$.
$\|m\|$	The size of messages.
$\|n\|$	The security parameter.
$\|q\|$	The large prime.
$\|k\|$	The integer.
$\|l\|$	The number large to $5n \log q$.

A. Communication Overhead Comparison

For the communication overhead, we focus on comparing the size of ciphertext and public key. Table IV shows the theoretical analysis of the public key size and ciphertext size in our scheme and eight other existing schemes [23]–[28], [31], [32]. In our setting, the value of m is lower than the value of Θ. The scheme proposed by Wang et al. [30] is not quantum resistance, so we do not compare their scheme with our scheme in the communication cost.

Regarding the public key size, our scheme is given by $m(n+1)\log q$, significantly lower than the schemes proposed by Yan et al. [25], Yang et al. [27] and Yu, Bai et al. [28]. Although our public key size is slightly higher than those of Li et al. [23], Zhang et al. [24], Sun et al. [26], Yu. Wang et al. [31] and Yu and Shi [32], we offer practicality and linkability. Therefore, the slightly higher overhead is deemed acceptable.

As for ciphertext size, it is evident that our ciphertext size is $2kn\log^2 q$, which is significantly smaller than other lattice-based signcryption schemes [24]–[27]. The ciphertext size of our scheme is nearly equivalent to the schemes proposed by Li et al. [23] and Yu, Bai et al. [28] and slightly larger than the schemes proposed by Yu, Wang et al. [31], and Yu and Shi [32]. As discussed previously, our scheme offers practicality and linkability, which provides higher security compared to their schemes [23], [28], [31], [32]. In a nutshell, our proposed secure post-quantum certificateless signcryption with linkability scheme stands out when compared to existing schemes that can withstand quantum attacks. The public key size of our scheme is lower than several other schemes, and the ciphertext size is significantly smaller than most lattice-based signcryption schemes. Despite having slightly higher public key and ciphertext sizes compared to part of previous schemes, our scheme offers higher security levels due to its practicality and linkability features, which are essential for real-world applications and make the slightly higher overhead acceptable in exchange for these security advantages.

B. Computational Overhead Comparison

For the comparative analysis of computational overhead, we present the theoretical computational values of signcryption and unsigncryption overhead for our primitive and the other six existing mechanisms [23]–[28], [31], [32] in Table V. By combining this analysis with the information in Table III, we can determine that the pre-image sample algorithm has the highest time overhead. However, in our scheme, we have successfully avoided it to minimize the time overhead. Specifically, the signcryption overhead in our scheme consists of four vector multiplication operations and five vector additive operations, while the unsigncryption overhead includes two vector multiplication operations and three vector additive operations. By referring to both Table III and Table V, we can conclude that the time overhead of our protocol is equal to the scheme proposed by Yu, Bai et al. [28] and significantly lower than that of lattice-based schemes [23]–[27], [31], [32].

TABLE III
RUNNING TIMES OF OPERATIONS

Operation	Execution Time (ms)
T_{vmul}	5.183
T_{vadd}	0.067
T_{smul}	1.541
T_{pair}	4.156
T_{gs}	22.575
T_{pis}	33.281
T_{minv}	0.003
T_{htp}	3.739

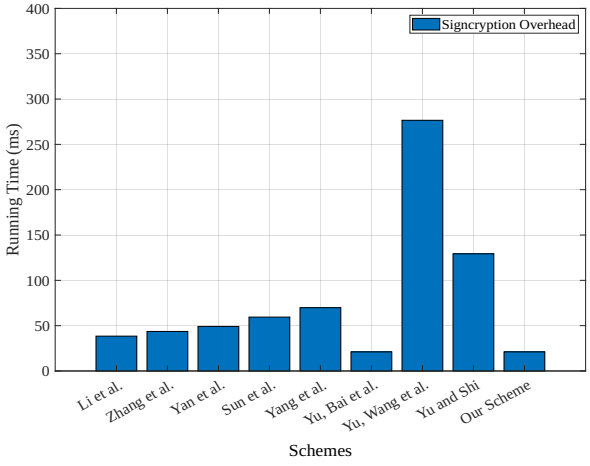

Fig. 5. Approximate Running Time Comparison of Signcryption.

Through the MALTAB experimental platform, we conducted simulation experiments for our scheme and other eight signcryption protocols [23]–[28], [31], [32] to further comprehensively demonstrate the comparison analysis findings in terms of computational overhead. The signcryption overheads of our scheme and other schemes [23]–[28], [31], [32] are shown in Fig. 5. Combining Table III and Table V, we calculate that the signcryption overhead of our scheme is $5\times T_{vadd}+4\times T_{vmul} = 5\times 0.067+4\times 5.183 = 21.067(ms)$. From Fig. 5, we observe that the signcryption time overhead of our scheme is considerably lower than the signcryption schemes [31], [32], slightly lower than existing lattice-based

TABLE IV
COMPARISON OF COMMUNICATION OVERHEAD

Schemes	Public Key Size	Ciphertext Size
Li et al. [23]	$n\Theta \log q$	$n + 6n \log^2 q$
Zhang et al. [24]	$n\Theta \log q$	$796 + 36n^2 \log^3 q$
Yan et al. [25]	$k(k+1)^2\Theta^2 \log^2 q$	$k\Theta n^2 \log^2 q$
Sun et al. [26]	$(\Theta k + 1) \log q$	$2\Theta k^2 n \log^2 q$
Yang et al. [27]	$n\Theta^2 \log q$	$2\Theta^2 n \log^2 q$
Yu et al. [28]	$\Theta(n+1) \log q$	$2kn \log^2 q$
Yu et al. [31]	$nk \log q$	$(l\Theta + k) \log q$
Yu et al. [32]	$n\Theta \log q$	$(\Theta + n) \log q$
Our Scheme	$m(n+1) \log q$	$2kn \log^2 q$

TABLE V
COMPARISON OF COMPUTATIONAL OVERHEAD

Schemes	Signcryption Overhead	Unsigncryption Overhead
Li et al. [23]	$T_{pis} + T_{vmul}$	$2T_{vmul}$
Zhang et al. [24]	$T_{pis} + 2T_{vmul}$	$2T_{vmul}$
Yan et al. [25]	$T_{pis} + 5T_{vadd} + 3T_{vmul}$	$7T_{vadd} + 7T_{vmul}$
Sun et al. [26]	$T_{pis} + 4T_{vadd} + 5T_{vmul}$	$4T_{vadd} + 6T_{vmul}$
Yang et al. [27]	$T_{pis} + 4T_{vadd} + 7T_{vmul}$	$3T_{vadd} + 6T_{vmul}$
Yu et al. [28]	$5T_{vadd} + 4T_{vmul}$	$3T_{vadd} + 2T_{vmul}$
Yu et al. [31]	$(\Theta + 3)T_{vmul} + 5T_{gs} + 3T_{htp} + T_{pis}$	$(2\Theta + 4)T_{vmul} + 3T_{pis} + T_{gs} + 3T_{htp}$
Yu et al. [32]	$(L+2)T_{vmul} + 3T_{htp} + T_{gs} + T_{pis}$	$(L+2)T_{vmul} + 3T_{htp}$
Our Scheme	$5T_{vadd} + 4T_{vmul}$	$3T_{vadd} + 2T_{vmul}$

TABLE VI
PROPERTIES COMPARISON

Schemes	IND-CCA2	UF-CMA	Quantum Resistance	Practicality	Linkability
Yu et al. [21]	✗	✗	✗	✓	✗
Chen et al. [22]	✓	✓	✗	✓	✗
Li et al. [23]	✓	✓	✓	✗	✗
Zhang et al. [24]	✓	✓	✓	✗	✗
Yan et al. [25]	✗	✗	✓	✗	✗
Sun et al. [26]	✓	✓	✓	✗	✗
Yang et al. [27]	✓	✓	✓	✗	✗
Yu et al. [28]	✓	✓	✓	✓	✗
Dai et al. [29]	✓	✓	✗	✓	✗
Wang et al. [30]	✗	✗	✗	✓	✗
Yu et al. [31]	✓	✓	✓	✗	✗
Yu et al. [32]	✓	✓	✓	✗	✗
Our Scheme	✓	✓	✓	✓	✓

signcryption schemes [23]–[27] and equal to scheme [28]. In particular, our signcryption overhead is between 0.07 to 1.00 times of existing schemes [23]–[28], [31], [32].

The comparison of unsigncryption overhead is depicted in Fig. 6. In particular, the unsigncryption overhead of our scheme is essentially the same as schemes [23], [24] and [28]. While the unsigncryption overheads of schemes [25], [26], [27], [31] and [32] are obviously higher than schemes [23], [24], [28] and ours. Especially, the calculation of the unsigncryption cost can also show similar results to the above simulation experiments. The overheads of schemes [23], [24], [28] and our scheme are calculated as $2\times T_{vmul} = 2\times 5.183 = 10.366(ms)$,$2\times T_{vmul} = 2\times 5.183 = 10.366(ms)$, $3\times T_{vadd} + 2 \times T_{vmul} = 3 \times 0.067 + 2 \times 5.183 = 10.567(ms)$, and $3\times T_{vadd} + 2\times T_{vmul} = 3\times 0.067 + 2\times 5.183 = 10.567(ms)$, respectively. Compared with other lattice-based schemes [23]–[28], the overhead of our scheme is 0.02 to 1.0 times that of existing schemes [23]–[28], [31], [32].

A comparative analysis of the overall computational overhead is shown in Fig. 7. Concretely, for our scheme, the computational overhead is $5\times T_{vadd} + 4\times T_{vmul} + 3\times T_{vadd} + 2 \times T_{vmul} = 5 \times 0.067 + 4 \times 5.183 + 3 \times 0.067 + 2 \times 5.183 = 31.634(ms)$. Consequently, incorporating theoretical value calculations and simulation experiments, it is clear that the computational overhead of our scheme is noticeably lower than other lattice-based signcryption schemes [25]–[27], [31], [32], marginally lower than schemes [23], [24], and equal to scheme [28]. In summary, the computational overhead of our

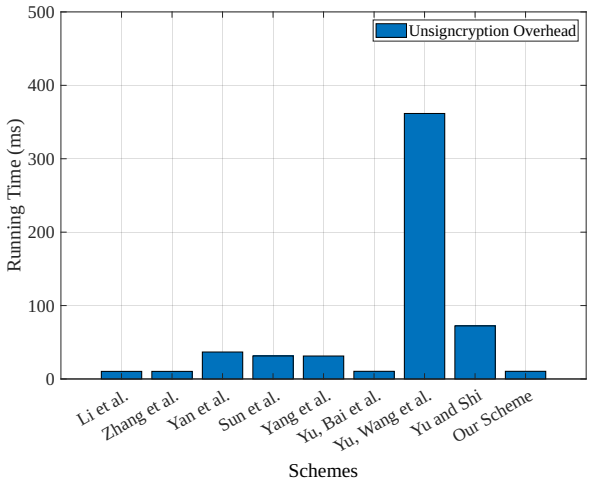

Fig. 6. Approximate Running Time Comparison of Unsigncryption.

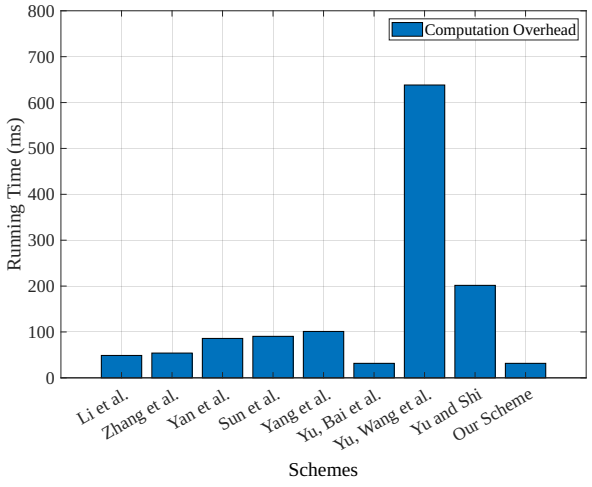

Fig. 7. Approximate Running Time Comparison of Computation Overhead.

scheme is dramatically lower than the other five lattice-based signcryption schemes, being 0.05 to 1.0 times that of all eight schemes [23]–[28], [31], [32]. Due to the additional security of practicality and linkability provided by our scheme, it is acceptable for the computational overhead to be the same as scheme [28].

C. Property Comparison

As far as the security of the scheme is concerned, we mainly consider the five components: IND-CCA2, UF-CMA, quantum resistance, practicality, and linkability. Seen from Table VI, we find that only scheme [21], scheme [25] and scheme [30] fail to meet the security requirements of IND-CCA2 and UF-CMA. For the property of Quantum Resistance, all comparison schemes, except scheme [21], scheme [22] and scheme [30], are capable of resisting quantum attacks. Except for our scheme and scheme [28], all schemes with quantum resistance security are impractical. In addition, only our scheme satisfies the linkability requirement as shown in Table VI. In summary, our scheme guarantees practicality while fulfilling the fullest security requirements.

VIII. Conclusion

In this paper, we propose a novel lattice-based certificateless signcryption primitive with linkability, called PQ-CLSCL. It enables medical data transmission safely in the IoMT while resistant to the quantum computing attacks. We start by presenting the system and security models. After that, we provide a detailed description of our designed scheme. The proposed PQ-CLSCL undergoes rigorous security analysis, demonstrating its satisfaction with IND-CCA2, EU-CMA, and linkability in a quantum setting. We also conduct extensive experimental evaluations and comparisons, which reveal the efficiency of our protocol. These results highlight our superiority compared to most state-of-the-art protocols.

References

[1] W. Mao, P. Jiang, and L. Zhu, "Locally verifiable batch authentication in iomt," *IEEE Transactions on Information Forensics and Security*, 2023.

[2] X. Chen, D. He, M. K. Khan, M. Luo, and C. Peng, "A secure certificateless signcryption scheme without pairing for internet of medical things," *IEEE Internet of Things Journal*, vol. 10, no. 10, pp. 9136–9147, 2022.

[3] X. Chen, S. Xu, T. Qin, Y. Cui, S. Gao, and W. Kong, "Aq–abs: Anti-quantum attribute-based signature for emrs sharing with blockchain," in *2022 IEEE Wireless Communications and Networking Conference (WCNC)*. IEEE, 2022, pp. 1176–1181.

[4] M. Wazid, A. K. Das, S. Shetty, J. J. Rodrigues, and M. Guizani, "Aiscm-fh: Ai-enabled secure communication mechanism in fog computing-based healthcare," *IEEE Transactions on Information Forensics and Security*, vol. 18, pp. 319–334, 2022.

[5] H. Li, K. Yu, B. Liu, C. Feng, Z. Qin, and G. Srivastava, "An efficient ciphertext-policy weighted attribute-based encryption for the internet of health things," *IEEE Journal of Biomedical and Health Informatics*, vol. 26, no. 5, pp. 1949–1960, 2021.

[6] Y. Bao, W. Qiu, P. Tang, and X. Cheng, "Efficient, revocable, and privacy-preserving fine-grained data sharing with keyword search for the cloud-assisted medical iot system," *IEEE Journal of Biomedical and Health Informatics*, vol. 26, no. 5, pp. 2041–2051, 2021.

[7] M. Papaioannou, M. Karageorgou, G. Mantas, V. Sucasas, I. Essop, J. Rodriguez, and D. Lymberopoulos, "A survey on security threats and countermeasures in internet of medical things (iomt)," *Transactions on Emerging Telecommunications Technologies*, vol. 33, no. 6, p. e4049, 2022.

[8] X. Chen, S. Xu, Y. Cao, Y. He, and K. Xiao, "Aqrs: Anti-quantum ring signature scheme for secure epidemic control with blockchain," *Computer Networks*, vol. 224, p. 109595, 2023.

[9] X. Chen, S. Xu, Y. He, Y. Cui, J. He, and S. Gao, "Lfs-as: lightweight forward secure aggregate signature for e-health scenarios," in *ICC 2022-IEEE International Conference on Communications*. IEEE, 2022, pp. 1239–1244.

[10] G. Xu, S. Xu, Y. Cao, F. Yun, Y. Cui, Y. Yu, K. Xiao *et al.*, "Ppseb: a postquantum public-key searchable encryption scheme on blockchain for e-healthcare scenarios," *Security and Communication Networks*, vol. 2022, 2022.

[11] Y. Zheng, "Digital signcryption or how to achieve cost (signature & encryption) cost (signature)+ cost (encryption)," in *Advances in Cryptology—CRYPTO'97: 17th Annual International Cryptology Conference Santa Barbara, California, USA August 17–21, 1997 Proceedings 17*. Springer, 1997, pp. 165–179.

[12] S. S. Al-Riyami and K. G. Paterson, "Certificateless public key cryptography," in *International conference on the theory and application of cryptology and information security*. Springer, 2003, pp. 452–473.

[13] M. Barbosa and P. Farshim, "Certificateless signcryption," in *Proceedings of the 2008 ACM symposium on Information, computer and communications security*, 2008, pp. 369–372.

[14] Y. Zhou, R. Xu, Z. Qiao, B. Yang, Z. Xia, and M. Zhang, "An anonymous and efficient multi-message and multi-receiver certificateless signcryption scheme for vanet," *IEEE Internet of Things Journal*, 2023.

[15] I. Ali, Y. Chen, J. Li, A. Wakeel, C. Pan, and N. Ullah, "Efficient offline/online heterogeneous-aggregated signcryption protocol for edge computing-based internet of vehicles," *IEEE Transactions on Intelligent Transportation Systems*, 2023.

[16] Y. Hou, Y. Cao, H. Xiong, Y. Song, and L. Xu, "An efficient online/offline heterogeneous signcryption scheme with equality test for iovs," *IEEE Transactions on Vehicular Technology*, 2023.

[17] Y. Yang, L. Zhang, Y. Zhao, K.-K. R. Choo, and Y. Zhang, "Privacy-preserving aggregation-authentication scheme for safety warning system in fog-cloud based vanet," *IEEE Transactions on Information Forensics and Security*, vol. 17, pp. 317–331, 2022.

[18] H. Yu and H. Wang, "Lattice-based threshold signcryption for blockchain oracle data transmission," *IEEE Transactions on Intelligent Transportation Systems*, vol. 24, no. 10, pp. 11 057–11 065, 2023.

[19] X. Chen, S. Xu, S. Gao, Y. Guo, S.-M. Yiu, and B. Xiao, "Fs-llrs: Lattice-based linkable ring signature with forward security for cloud-assisted electronic medical records," *IEEE Transactions on Information Forensics and Security*, 2024.

[20] Q. Zhan, M. Luo, and M. Qiu, "An efficient multi-mode certificateless ring signcryption scheme in vanets," *IEEE Internet of Things Journal*, 2024.

[21] H. Yu and B. Yang, "Pairing-free and secure certificateless signcryption scheme," *The Computer Journal*, vol. 60, no. 8, pp. 1187–1196, 2017.

[22] J. Chen, L. Wang, M. Wen, K. Zhang, and K. Chen, "Efficient certificateless online/offline signcryption scheme for edge iot devices," *IEEE Internet of Things Journal*, vol. 9, no. 11, pp. 8967–8979, 2021.

[23] F. Li, F. T. Bin Muhaya, M. K. Khan, and T. Takagi, "Lattice-based signcryption," *Concurrency and Computation: Practice and Experience*, vol. 25, no. 14, pp. 2112–2122, 2013.

[24] X. Zhang, C. Xu, and J. Xue, "Efficient multi-receiver identity-based signcryption from lattice assumption," *International Journal of Electronic Security and Digital Forensics*, vol. 10, no. 1, pp. 20–38, 2018.

[25] J. Yan, L. Wang, M. Li, H. Ahmad, J. Yue, and W. Yao, "Attribute-based signcryption from lattices in the standard model," *IEEE Access*, vol. 7, pp. 56 039–56 050, 2019.

[26] Y. Sun and W. Zheng, "An identity-based ring signcryption scheme in ideal lattice." *J. Netw. Intell.*, vol. 3, no. 3, pp. 152–161, 2018.

[27] X. Yang, H. Cao, W. Li, and H. Xuan, "Improved lattice-based signcryption in the standard model," *IEEE Access*, vol. 7, pp. 155 552–155 562, 2019.

[28] H. Yu, L. Bai, M. Hao, and N. Wang, "Certificateless signcryption scheme from lattice," *IEEE Systems Journal*, vol. 15, no. 2, pp. 2687–2695, 2020.

[29] C. Dai and Z. Xu, "Pairing-free certificateless aggregate signcryption scheme for vehicular sensor networks," *IEEE Internet of Things Journal*, vol. 10, no. 6, pp. 5063–5072, 2023.

[30] Y. Wang, X. Zhang, R. Chen, H.-N. Dai, X. Wang, L. Y. Zhang, and M. Li, "Multireceiver conditional anonymous singcryption for iomt crowdsourcing," *IEEE Internet of Things Journal*, vol. 11, no. 5, pp. 8401–8413, 2024.

[31] H. Yu, W. Wang, and Q. Zhang, "Certificateless anti-quantum ring signcryption for network coding," *Knowledge-Based Systems*, vol. 235, p. 107655, 2022.

[32] H. Yu and J. Shi, "Certificateless multi-source signcryption with lattice," *Journal of King Saud University-Computer and Information Sciences*, vol. 34, no. 10, pp. 10 157–10 166, 2022.

[33] S. Sato and J. Shikata, "Lattice-based signcryption without random oracles," in *Post-Quantum Cryptography: 9th International Conference, PQCrypto 2018, Fort Lauderdale, FL, USA, April 9-11, 2018, Proceedings 9*. Springer, 2018, pp. 331–351.

[34] H. Q. Le, D. H. Duong, P. S. Roy, W. Susilo, K. Fukushima, and S. Kiyomoto, "Lattice-based signcryption with equality test in standard model," *Computer Standards & Interfaces*, vol. 76, p. 103515, 2021.

[35] J. Malone-Lee, "Identity-based signcryption," *Cryptology ePrint Archive*, 2002.

[36] Z. Liu, Y. Hu, X. Zhang, and H. Ma, "Certificateless signcryption scheme in the standard model," *Information Sciences*, vol. 180, no. 3, pp. 452–464, 2010.

[37] S. Miao, F. Zhang, S. Li, and Y. Mu, "On security of a certificateless signcryption scheme," *Information Sciences*, vol. 232, pp. 475–481, 2013.

[38] A. Zhang, L. Wang, X. Ye, and X. Lin, "Light-weight and robust security-aware d2d-assist data transmission protocol for mobile-health systems," *IEEE Transactions on Information Forensics and Security*, vol. 12, no. 3, pp. 662–675, 2016.

[39] H. Yu and J. Shi, "Certificateless multi-source signcryption with lattice," *Journal of King Saud University-Computer and Information Sciences*, vol. 34, no. 10, pp. 10 157–10 166, 2022.

[40] H. Yu, W. Wang, and Q. Zhang, "Certificateless anti-quantum ring signcryption for network coding," *Knowledge-Based Systems*, vol. 235, p. 107655, 2022.

[41] Z. Xie, Y. Chen, I. Ali, C. Pan, F. Li, and W. He, "Efficient and secure certificateless signcryption without pairing for edge computing-based internet of vehicles," *IEEE Transactions on Vehicular Technology*, vol. 72, no. 5, pp. 5642–5653, 2022.

[42] 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 Transactions on Vehicular Technology*, pp. 1–14, 2024.

[43] S. Vishnu, S. J. Ramson, and R. Jegan, "Internet of medical things (iomt)-an overview," in *2020 5th international conference on devices, circuits and systems (ICDCS)*. IEEE, 2020, pp. 101–104.

[44] A. Ghubaish, T. Salman, M. Zolanvari, D. Unal, A. Al-Ali, and R. Jain, "Recent advances in the internet-of-medical-things (iomt) systems security," *IEEE Internet of Things Journal*, vol. 8, no. 11, pp. 8707–8718, 2020.

[45] E. A. Mantey, C. Zhou, J. H. Anajemba, J. K. Arthur, Y. Hamid, A. Chowhan, and O. O. Otuu, "Federated learning approach for secured medical recommendation in internet of medical things using homomorphic encryption," *IEEE Journal of Biomedical and Health Informatics*, 2024.

[46] B. Zhang, "A lightweight data aggregation protocol with privacy-preserving for healthcare wireless sensor networks," *IEEE Systems Journal*, vol. 15, no. 2, pp. 1705–1716, 2020.

[47] D. Micciancio and C. Peikert, "Trapdoors for lattices: Simpler, tighter, faster, smaller." in *Eurocrypt*, vol. 7237. Springer, 2012, pp. 700–718.

[48] C. Gentry, C. Peikert, and V. Vaikuntanathan, "Trapdoors for hard lattices and new cryptographic constructions," in *Proceedings of the fortieth annual ACM symposium on Theory of computing*, 2008, pp. 197–206.

Shiyuan Xu (Graduate Student Member, IEEE) is currently a Ph.D. candidate in the Department of Computer Science at the University of Hong Kong. His research interests include Applied Cryptography, Lattice, Searchable Encryption, and Data Security.
Mr. Xu has published 20+ academic articles in refereed conferences and journals, including IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, IEEE INTERNET OF THINGS JOURNAL, COMPUTER NETWORKS, ACM CIKM, Inscrypt, IEEE ICC, etc. He served as a PC Member of CRYPTO 2024, ASIACRYPT 2024, IEEE MSN 2024, and a Reviewer of IEEE TDSC, IEEE TIFS, IEEE JSAC, ACM WWW, ACM CIKM, DASFAA, etc. He served as a Session Chair of WASA and Inscrypt. He won the Excellent Paper Award of TSINGHUA SCIENCE AND TECHNOLOGY in 2022. He is a Graduate Student Member of IEEE.

Xue Chen (Graduate Student Member, IEEE) is currently a Ph.D. student in the Department of Computer Science at the University of Hong Kong. She received an M.Phil. degree in the Department of Computing at the Hong Kong Polytechnic University in 2024. Her research interests include Applied Cryptography, Lattice, and Data Security.
Miss Xue has published 15+ academic papers in refereed international conferences and journals including IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, COMPUTER NETWORKS, ACM CIKM, Inscrypt, IEEE ICC, etc. She served as a PC Member of IEEE MSN 2024, and a Reviewer of CRYPTO, ASIACRYPT, ACM WWW, INFORMATION SCIENCE, etc. She won the Excellent Paper Award of TSINGHUA SCIENCE AND TECHNOLOGY in 2022. She is a Graduate Student Member of IEEE.

Yu Guo (Member, IEEE) is currently an Associate Professor in the School of Artificial Intelligence at Beijing Normal University. He received a B.E. degree in Software Engineering from Northeastern University, in 2013, an M.Sc. degree in Electronic Commerce, and a Ph.D. degree in computer science from City University of Hong Kong, in 2014 and 2019. He was a Postdoctoral and Research Fellow at the City University of Hong Kong. His research interests include Cloud Computing Security, Privacy-Preserving, and Applied Cryptography.

Dr. Guo has published 40+ academic papers in refereed conferences and articles, including IEEE ICDE, ACM MM, IEEE ICDCS, IEEE/ACM IWQoS, ACM AsiaCCS, ACM CIKM, DASFAA, IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, IEEE TRANSACTIONS ON DEPENDABLE AND SECURE COMPUTING, IEEE TRANSACTIONS ON PARALLEL AND DISTRIBUTED SYSTEMS, IEEE TRANSACTIONS ON COMPUTERS, IEEE TRANSACTIONS ON KNOWLEDGE AND DATA ENGINEERING, IEEE TRANSACTIONS ON SERVICES COMPUTING, etc. He served as a Track Chair of IEEE MSN 2024. He won the Best Paper Award of MMM 2016 and IEEE ICDCS 2020. He is a Member of IEEE.

Shang Gao (Member, IEEE) is currently a Research Assistant Professor in the Department of Computing, at the Hong Kong Polytechnic University. He received a B.S. degree from Hangzhou Dianzi University, in 2010, an M.E. degree from Southeast University, in 2014, and a Ph.D. degree from Hong Kong Polytechnic University, in 2019. After graduation, he worked at Microsoft China for one year. His research interests include Information Security, Applied Cryptography, Blockchain Security, and Zero-knowledge Proofs.

Dr. Gao has published more than 40 papers in top-tier conferences and journals, including IEEE S&P, ACM CCS, IEEE INFOCOM, IEEE ICDCS, IEEE/ACM IWQoS, ACM AsiaCCS, IEEE Globecom, IEEE ICC, IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, IEEE TRANSACTIONS ON DEPENDABLE AND SECURE COMPUTING, IEEE/ACM TRANSACTIONS ON NETWORKING, IEEE TRANSACTIONS ON NETWORK SCIENCE AND ENGINEERING, IEEE TRANSACTIONS ON NETWORK AND SERVICE MANAGEMENT, IEEE INTERNET OF THINGS JOURNAL, IEEE NETWORK, etc. He served as a PC Member of IEEE ICDCS 2022, SecureCom 2023 & 2024. He is a Member of IEEE.

Siu-Ming Yiu (Member, IEEE) is currently a Full Professor and the Associate Director of School of Computing and Data Science at the University of Hong Kong. He received a B.Sc. degree from the Chinese University of Hong Kong in 1988, an M.S. degree from Temple University in 1992, and a Ph.D. degree from The University of Hong Kong in 1996. His research interests are Cryptography and Information Security.

Professor Yiu has published more than 500 papers in top-tier conferences and refereed journals, including NATURE, SCIENCE, EUROCRYPT, ACM SIGMOD, IEEE ICDE, IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, IEEE TRANSACTIONS ON DEPENDABLE AND SECURE COMPUTING, IEEE TRANSACTIONS ON PARALLEL AND DISTRIBUTED SYSTEMS, IEEE TRANSACTIONS ON COMPUTERS, IEEE TRANSACTIONS ON KNOWLEDGE AND DATA ENGINEERING, IEEE TRANSACTIONS ON SERVICES COMPUTING, IEEE TRANSACTIONS ON NEURAL NETWORKS AND LEARNING SYSTEMS, IEEE TRANSACTIONS ON INDUSTRIAL INFORMATICS, IEEE JOURNAL OF BIOMEDICAL AND HEALTH INFORMATICS, etc. His work has been cited over 30000 times on Google Scholar.

He has served as a Steering Committee Member of ASIACRYPT and a General Chair in ASIACRYPT 2017, ICICS 2014, ISC 2014, ProvSec 2014. He was selected for Outstanding Teaching Award by the University in 2009 and won the Teaching Excellence Award in the Department seven times. He also received the Best Teacher Award from the Faculty of Engineering twice. He received two Research Output prizes, one from the department in 2013 and one from the faculty in 2006. He was named on the list of 'Highly Cited Researchers' from Clarivate Analytics as the most influential in the world in 2016, 2017, and 2019 and has been one of the Top 1% of HKU scholars for 12 consecutive years (2011-2022). He is also listed as the World's Top 2% Scientists for career-long impact by Stanford University in 2022. He won the Best Paper Award of ESORICS 2014. He is a Member of IEEE and IACR.

Bin Xiao (Fellow, IEEE) is currently a Full Professor in the Department of Computing, at the Hong Kong Polytechnic University. He was the Dept. Research Committee Chair (DRC Chair) from 2018 to 2021. He received a B.Sc. and M.Sc. degrees from Fudan University, China, and a Ph.D. degree from the University of Texas at Dallas, U.S.A. in 2003. His research interests include AI and Network security, Data Privacy, and Blockchain.

Professor Xiao has published more than 200 technical papers in top-tier conferences and journals, including IEEE S&P, ACM CCS, IEEE INFOCOM, IEEE/CVF CVPR, ACM MM, ICLR, IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, IEEE TRANSACTIONS ON DEPENDABLE AND SECURE COMPUTING, IEEE JOURNAL ON SELECTED AREAS IN COMMUNICATIONS, IEEE/ACM TRANSACTIONS ON NETWORKING, IEEE TRANSACTIONS ON MOBILE COMPUTING, IEEE TRANSACTIONS ON PARALLEL AND DISTRIBUTED SYSTEMS, IEEE TRANSACTIONS ON COMPUTERS, IEEE TRANSACTIONS ON IMAGE PROCESSING, IEEE TRANSACTIONS ON NEURAL NETWORKS AND LEARNING SYSTEMS, IEEE TRANSACTIONS ON INDUSTRIAL INFORMATICS, IEEE TRANSACTIONS ON NETWORK SCIENCE AND ENGINEERING, IEEE TRANSACTIONS ON VEHICULAR TECHNOLOGY, ACM COMPUTING SURVEYS, etc.

Currently, he serves as the Associate Editor of IEEE TRANSACTIONS ON CLOUD COMPUTING and IEEE TRANSACTIONS ON NETWORK SCIENCE AND ENGINEERING. He served as the Associate Editor for ELSEVIER JOURNAL OF PARALLEL AND DISTRIBUTED COMPUTING from 2016 to 2021 and IEEE INTERNET OF THINGS JOURNAL from 2020 to 2023. He is the Chair of the IEEE ComSoc CISTC Committee and IEEE ComSoc distinguished lecturer. He has been the Track Co-Chair of IEEE ICDCS 2022, the Symposium Track Co-Chair of IEEE ICC 2020, ICC 2018, GLOBECOM 2024, GLOBECOM 2017, and the General Chair of IEEE SECON 2018. He is a Fellow of IEEE, a Fellow of AAIA, and a Member of ACM and CCF.