IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received February 22, 2020, accepted March 9, 2020, date of publication March 17, 2020, date of current version March 27, 2020.

Digital Object Identifier 10.1109/ACCESS.2020.2981503

LDVAS: Lattice-Based Designated Verifier Auditing Scheme for Electronic Medical Data in Cloud-Assisted WBANs

XIAOJUN ZHANG[1,2,3], CHAO HUANG[1], YUAN ZHANG[3], (Member, IEEE), JINGWEI ZHANG[1], AND JIE GONG[1]

[1]Research Center for Cyber Security, School of Computer Science, Southwest Petroleum University, Chengdu 610500, China
[2]Key Laboratory of Financial Mathematics, Putian University (Fujian Province University), Putian 351100, China
[3]School of Computer Science and Engineering, University of Electronic Science and Technology of China, Chengdu 611731, China

Corresponding author: Xiaojun Zhang (zhangxjdzkd2012@163.com)

This work was supported in part by the National Key Research and Development Program of China under Grant 2017YFB0802000, in part by the National Natural Science Foundation of China under Grant 61902327 and Grant 61872060, in part by the Key Laboratory of Financial Mathematics of Fujian Province University (Putian University) under Grant JR201903, in part by the China Postdoctoral Science Foundation Funded Project under Grant 2017M623008, in part by the Youth Scientific and Technology Innovation Team Project of SWPU under Grant 2019CXTD05, and in part by the Sichuan Science and Technology Program under Grant 2018GZ0102.

ABSTRACT Data integrity has become an extremely important security issue in cloud-assisted wireless body area networks (WBANs). As accurate medical diagnostic analysis is heavily based on outsourced electronic medical data in cloud storage, any corrupted data may lead to fateful consequences. Data auditing contributes to medical data integrity verification, but most of existing data auditing schemes are vulnerable to attackers equipped with practical quantum-computing devices, which are very likely to be invented in the near future. Besides, in many scenarios, a patient has no capability to execute medical data integrity verification personally, he/she has to specify a verifier to complete data auditing. To this end, we present an efficient lattice-based designated verifier auditing scheme (LDVAS), which could be well deployed in cloud-assisted WBANs. In particular, LDVAS enables a patient to designate a unique verifier to execute data auditing in post-quantum secure settings, and any others cannot fulfil such task without the approval of the patient. We formally prove the security of LDVAS based on the hardness assumptions of lattice-based problems. The performance evaluation demonstrates the high efficiency and feasibility of LDVAS on the side of the designated verifier.

INDEX TERMS Wireless body area networks, cloud storage, designated verifier auditing, lattice-based problems, post-quantum security.

I. INTRODUCTION

Nowadays, due to the fast development of wireless medical sensors and communication technologies, wireless body area networks (WBANs) have been considered as a key technique for improving the quality of medical and health services [1], [2]. Using wireless medical sensors, the general physiology parameters of patients could be collected, processed, and transmitted to the medical information systems via WBANs. With the sharp increase of electronic medical data generated in WBANs, those real-time massive data need to be stored and processed continuously, and an accurate clinical diagnosis and a timely medical feedback reports are also demanded by patients. Due to the advantages of cloud computing technologies [3], they could be well integrated into WBANs to overcome the inherent weaknesses of traditional WBANs, which brings about a large improvement in medical data storage and processing capabilities.

Cloud-assisted WBANs [4], [5] rely on cloud computing technologies to maintain massive electronic medical data managements for patients, especially for those patients with chronic diseases, the system framework is depicted in Fig. 1. Generally, wireless medical sensor nodes are implanted into a patient's body to periodically monitor and collect important electronic medical data. These medical data are transmitted to a cloud server associated with a medical information system through mobile terminal equipments. As such, based on these critical medical data, a doctor could conduct

The associate editor coordinating the review of this manuscript and approving it for publication was Guangjie Han.

clinical analysis and diagnosis, and provide valuable medical reports.

Despite great benefits on managing massive medical data for patients brought by cloud-assisted WBANs, critical security and privacy concerns in data outsourcing have been raised seriously [6]–[8]. Among those issues, medical data integrity has become the most import one [9]. Since patients with mobile terminal equipments upload electronic medical data to a cloud storage server associated with WBANs, they actually lose physical controlling over the outsourced data. As a result, the cloud server might hide the incidents of the outsourced medical data or tamper with these data for some malicious motivations. Specifically, to save storage space, the cloud server even delete some outsourced medical data which never be accessed. Additionally, an external adversary may tamper with outsourced medical data for economical or malicious purposes. Thus, a doctor is failure to gain authentic and correct medical data, which is likely to prevent patients from being treated accurately, or even lead to severe consequences [10], [11]. Consequently, a periodical integrity checking for outsourced medical data is absolutely essential.

Intuitively, the integrity verification tasks could be completed by patients themselves, but it incurs substantial communication and computation burden for patients to retrieve and check medical data integrity one by one. While public auditing [12] enables patients to resort such tasks to a third-party auditor (TPA). Thus, on behalf of patients, an auditor could periodically check outsourced medical data integrity. Once the auditing task fails, the auditor informs patients in time that electronic medical data may be corrupted, which means that these outsourced data could not be exploited by doctors. Although public auditing brings significant benefits to cloud-assisted WBANs, there are two main hindrances in widely applying public auditing into cloud-assisted WBANs. On the one hand, a majority of existing public auditing schemes [13]–[17] are designed on the traditional cryptographic hardness assumptions. However, according to the research results in [18], with the advent of the quantum computers, the aforementioned public auditing schemes will be threatened. Indeed, the breakthrough research on quantum computers [19] prefigure that the deployment of quantum computers in WBANs is likely to be realized in the near future, which makes post-quantum secure auditing schemes more critical. On the other hand, existing public auditing schemes rely on a third-party auditor to check the data integrity for cloud users, but it requires an impractical assumption that auditors have enough computation capabilities to bear expensive verification costs, such as time-consuming bilinear pairing and modular exponentiation operations. As far as we are concerned, in cloud-assisted WBANs, auditors may simultaneously execute auditing tasks from multiple patients. As such, existing public auditing schemes are confronted with performance bottleneck on the side of an auditor.

In addition to the above hindrances, the deployment of public auditing in cloud-assisted WBANs would face another security challenges. Particularly, we should never ignore the fact that remote public auditing will incur some danger of leaking the privacy to some extent, patients generally consider their medical data very important, these sensitive private information could not be captured by unauthorized parties. In such case, to protect medical data privacy for patients' special purposes, patients could specify a particular verifier to fulfil the remote medical data integrity verification tasks in cloud-assisted WBANs. Additionally, based on the verification process information, a curious third-party auditor may try to recover the primitive medical data of the patients by using powerful computing devices. Accordingly, some feasible technologies need to be employed to prevent the curious TPA from executing such operations.

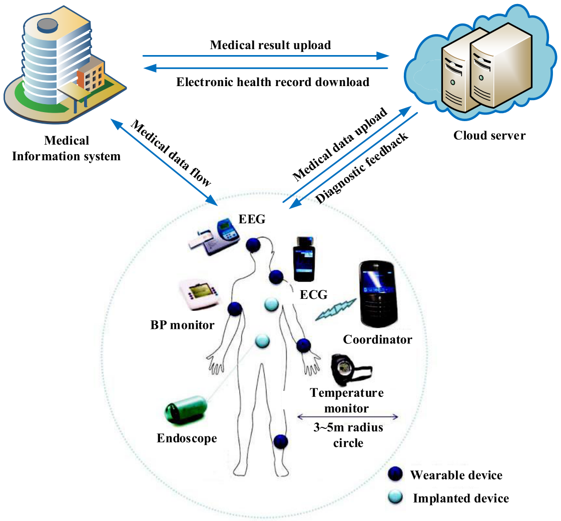


FIGURE 1. System framework of cloud-assisted WBANs.

To address the aforementioned security issues, in this paper, we propose an efficient designated verifier auditing scheme for medical data in cloud-assisted WBANs. Our scheme is constructed on lattice-based cryptography [20], which enjoys very strong security proofs based on worst-case hardness as well as great simplicity.

Specifically, the contributions of this work are elaborated as follows.

- We propose the first lattice-based designated verifier auditing scheme (LDVAS) for electronic medical data in cloud-assisted WBANs, and LDVAS is secure against quantum-computing attacks. We leverage the idea of the construction of a designated verifier signature [21], [22] to design the designated verifier auditing scheme. To be specific, in the auditing delegation phase, a patient as the role of the KGC (Key Generation Centre) in an identity-based system [23], could flexibly generate the private key according to the identity of a designated verifier, and authorize the unique verifier to check the integrity of outsourced medical data.
- We formally prove the security of LDVAS in detail. Particularly, we prove that LDVAS achieves storage

correctness guarantee based on the inhomogeneous small integer solution (ISIS) assumption [24], which means that it is computationally infeasible for a malicious cloud server to generate a forged auditing proof information that could pass the verification phase. LDVAS also preserves the robustness property based on the hardness of the learning with errors (LWE) assumption [24], and thus no one excepts the designated verifier could check the integrity of outsourced medical data. Furthermore, we exploit the GPV signature technique in [25] to guarantee that the curious verifier could not derive the primitive medical data blocks of patients.

- We conduct a comprehensive performance evaluation. Compared with existing schemes, LDVAS is more practical for the high performance requirements in massive medical data processing for cloud-assisted WBANs. In particular, without needing time-consuming cryptographic operations, such as bilinear pairing and modular exponentiation operations, LDVAS enables the designated verifier to fulfil the auditing tasks only through computing simple addition and multiplication operations over a moderate modulus, which could dramatically reduce the integrity verification costs.

The remainder of this paper is organized as follows. We discuss the related work in Section II. In Section III, we present the preliminaries including system model, formal definition, and lattice-based background. Then we propose LDVAS in Section IV. In Section V, we conduct the evaluation of LDVAS in terms of security and performance. Finally, we draw the conclusions in Section VI.

II. RELATED WORK

A. CLOUD STORAGE DATA AUDITING

Recently, with the rapid development of cloud computing, cloud storage technologies have become increasingly prevalent. Simultaneously, many security and privacy issues have emerged, and some feasible cryptographic techniques have been proposed to address these issues [26]–[32]. Among those techniques, cloud storage data auditing has been one of the most important techniques to check the outsourced data integrity.

For the first time, Ateniese *et al.* [33] proposed a provable data possession model which enables a data owner to store data into an untrusted server, and the data owner could check that whether the server possesses the correct data without retrieving an entire data set. In addition, Juels *et al.* [34] presented proofs of retrievability (POR) for large data files. Following up, Shacham and Waters [35] proposed an improved POR model, under the security model as described in [34]. According to the work of Shacham and Waters [35], Wang *et al.* [12] formally presented a pairing-based public auditing scheme for cloud storage, which relies on a third-party auditor (TPA) to fulfil the data integrity verification tasks on behalf of the data owner through challenge and response process. Inspired by the public auditing scheme [12], a majority of public auditing schemes have been proposed, such as [13], [14]. Specifically, those schemes exploit the random masking techniques to prevent the curious TPA from revealing the primitive data blocks of data owners. Moreover, some remote cloud storage data auditing schemes with novel security properties have also been proposed. The public auditing scheme in [36] successfully employs the new indistinguishability obfuscation technique, and it is especially light-weight on the side of the TPA. In the scheme [37], [38], cloud users could specify a unique verifier to conduct the remote data integrity verification, thereby protecting data privacy to some extent. In order to decrease the damage of the user's key exposure in cloud storage data auditing, the scheme in [39] formally defined the secure model of auditing with key-exposure resilience, and proposed a strong key-exposure data auditing for cloud storage. To give assistance to data owners for processing their data in public clouds, the novel proxy-oriented data uploading and remote data integrity checking scheme has also been proposed in [40]. Utilizing biometrics as the fuzzy identity, Li *et al.* [41] have proposed a fuzzy identity-based auditing scheme, which offers the property of error-tolerance, it binds with private key to one identity which will be exploited to verify the correctness of a response auditing proof information generated with another identity, if and only if both identities are sufficiently close. Additionally, some approaches have been proposed to address the issues of medical data integrity in cloud storage [15], [42], [43].

B. LATTICE-BASED CRYPTOGRAPHY AND THE APPLICATIONS IN CLOUDS

Due to the pioneer work in [18], the conventional public key cryptographic algorithms will be broken once the quantum computers come true. Lattice-based cryptography [20] has been termed as the best promising solution of resisting quantum computing, since it enjoys very strong security proofs based on worst-case hardness, relatively efficient implementations, as well as great simplicity. Specifically, because of those excellent properties, the fully homomorphic encryption schemes have been proposed in recent years [44], [45], which enable the cloud computing to arbitrarily compute the encrypted data without recovering any plaintext. In addition, a preimage sampleable function [25] has been designed, which is a basic tool to construct lattice-based signatures to prevent adversaries from tampering with data. Subsequently, using the preimage sampleable function, some novel lattice-based signatures have been proposed in [46], [47]. Furthermore, considering that homomorphic properties have distinguished applications in cloud computing settings, some lattice-based linearly homomorphic signature schemes [48], [49], a fully homomorphic signature [50] and some fully homomorphic message authenticators [51], [52] have also emerged. Attractively, these lattice-based schemes with homomorphic properties could be applied to construct cloud storage auditing schemes with quantum-computing resistance. Based on lattice-based cryptography, the scheme in [53] has addressed the key-exposure problem for data auditing in post-quantum secure cloud storage settings, another post-quantum secure identity-based data outsourcing with public auditing in cloud storage has been proposed in [54]. However, these schemes cannot support the designated verifier integrity checking functionality.

III. PRELIMINARIES

A. SYSTEM MODEL AND FORMAL DEFINITION

Now we introduce the system model of a cloud storage data auditing, as depicted in Fig. 2. There are three different entities: cloud user (patient), cloud server, the designated third-party auditor (TPA).

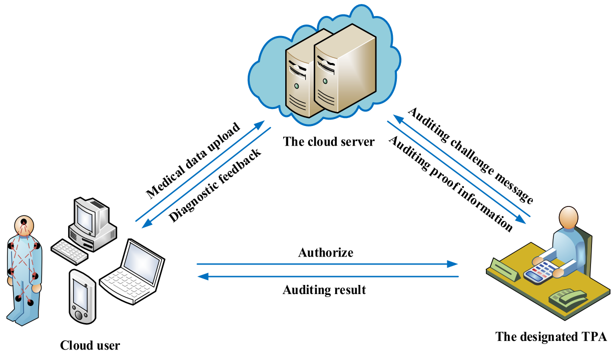


FIGURE 2. System model of cloud storage data auditing.

- Cloud user: As a patient, whose medical data are collected by wireless medical sensors, and are uploaded to a cloud server via wireless body area networks. Specifically, the patient is required to designate a unique TPA to check the outsourced medical data integrity periodically.
- Cloud server: It is equipped with the medical information systems associated with wireless body area networks, and provides with powerful cloud storage and computation resources for patients to create, store, update and request for retrievability.
- The designated TPA: It is a designated verifier, which fulfils the auditing tasks on behalf of patients upon request, and feeds back the auditing results to patients, and detects the medical data corruption as soon as possible.

We provide a formal definition of a cloud storage designated verifier auditing scheme, which consists of the following three phases. They are the system initialization phase, the auditing delegation phase, the challenge-response phase, respectively.

The system initialization phase contains the following three algorithms, called **Setup**, **KeyGen**, and **TagGen**, respectively.

Setup: This is a probabilistic polynomial time algorithm (PPT), which takes as input the common security parameter κ, and outputs the public system parameters.

KeyGen: This is a PPT algorithm which is performed by a cloud server and a patient to set their corresponding public-private key pairs. It takes the public system parameters as inputs, and outputs a public-private key pair $(pk_{patient}, sk_{patient})$ for the patient, and (pk_{cloud}, sk_{cloud}) for the cloud server.

TagGen: This is a PPT algorithm which is performed by the patient, he/she takes as inputs the private key $sk_{patient}$, the medical data file F, and outputs the set of signatures Ψ. Simultaneously, the medical data file tag τ is also produced during this algorithm. Finally, the patient uploads the medical data file F, the file tag τ, and the corresponding set of signatures Ψ to the cloud server associated with wireless body area networks, and deletes them in the local copy.

The auditing delegation phase contains the **VerDesig** algorithm as follows.

VerDesig: This verifier designation algorithm is performed by a patient. Once the patient plans to send a request message for an auditing task to the designated TPA, as the role of the KGC, the patient generates the designated TPA's public-private key pair (pk_{TPA}, sk_{TPA}) by using the patient's private key $sk_{patient}$ and the designated TPA's identity ID_{TPA}. Finally, the patient sends (pk_{TPA}, sk_{TPA}) to the designated TPA via a secure channel, and registers $(ID_{patient}, ID_{TPA}, pk_{TPA})$ into the cloud server simultaneously.

The challenge-response phase for the designated verifier auditing scheme contains the following three algorithms.

GenChal: The is a PPT algorithm which is performed by the designated TPA. It takes as inputs the public system parameters, and outputs an appropriate auditing challenge message $(chal, ID_{TPA})$.

GenProof: The is a PPT algorithm which is performed by the cloud server. It takes as inputs a medical data file F, the corresponding set of signatures Ψ, the medical data file tag τ, and the challenge message $(chal, ID_{TPA})$, outputs a response auditing proof information P to the designated TPA.

VerifyProof: Once receiving the response auditing proof information P from the cloud server, the designated TPA takes *chal* and P as inputs, and outputs true if the integrity of the electronic medical data is verified as correct. Otherwise, it outputs false.

B. DESIGN GOALS

In this paper, we target a designated verifier auditing scheme for medical data in cloud-assisted WBANs, the following objects should be achieved.

- Storage correctness guarantee: The cloud server should keep the outsourced medical data intact. It is computationally infeasible for a malicious cloud server to tamper with the medical data of patients to pass the designated TPA's integrity verification process.
- Robustness: The patient could designate a unique TPA to fulfil the medical data auditing tasks, so that no one excepts the designated TPA could execute the integrity verification of the medical data stored in cloud-assisted WBANs.
- Privacy preservation: Based on the auditing proof information from the cloud server, it is computationally infeasible for a curious designated TPA to recover the

primitive medical data blocks of patients, by using powerful computing devices.

- Quantum-computing resistance. Due to the threats of quantum computers, a practical designated verifier auditing scheme for medical data in cloud-assisted WBANs resisting quantum computing is demanded.
- High performance: It is demanded for a cloud server with a higher efficiency to process massive electronic medical data simultaneously. In addition, to provide with high-quality medical data auditing services in cloud-assisted WBANs, the auditing time and communication costs should be as low as possible on the side of the designated verifier.

C. LATTICE-BASED BACKGROUND

Lattice-based cryptography is secure against quantum-computing attacks, it has very strong security proofs based on worst-case hardness, and has been termed as the best promising post-quantum cryptography. Now we introduce the background of lattice-based cryptography as follows.

Given a positive integer d, $[d]$ denotes the set $\{1, \cdots, d\}$. Given an $n \times m$ matrix $\boldsymbol{A} = [\boldsymbol{a}_1, \cdots, \boldsymbol{a}_m]$, where $\boldsymbol{a}_i$ denotes the i-th column vector of $\boldsymbol{A}$. Define $\|\boldsymbol{a}\|$ as the Euclidean norm of $\boldsymbol{a}$, and $\|\boldsymbol{A}\| = max_{i \in [m]} \|\boldsymbol{a}_i\|$.

Lattices. Let $\boldsymbol{B} = \{\boldsymbol{b}_1, \cdots, \boldsymbol{b}_m\} \subseteq \mathcal{R}^m$ consist of m linearly independent vectors. An m-dimensional lattice Λ generated by $\boldsymbol{B}$ is defined as $\Lambda = \mathcal{L}(\boldsymbol{B}) = \{\boldsymbol{B}z : z \in Z^m\}$.

Here $\boldsymbol{B}$ is a basis of the lattice $\Lambda = \mathcal{L}(\boldsymbol{B})$. Furthermore, denote $\widetilde{\boldsymbol{B}} = \{\widetilde{\boldsymbol{b}}_1, \cdots, \widetilde{\boldsymbol{b}}_m\}$ as its Gram-Schmidt orthogonalization, which is defined iteratively as follows: $\widetilde{\boldsymbol{b}}_1 = \boldsymbol{b}_1$, and for each $i = 2, \cdots, m$, the vector $\widetilde{\boldsymbol{b}}_i$ is the component of $\boldsymbol{b}_i$ orthogonal to span $(\boldsymbol{b}_1, \cdots, \boldsymbol{b}_{i-1})$.

In this paper, our construction will build on integer lattices defined by Ajtai [55].

Definition 1: Given a matrix $\boldsymbol{A} \in Z_q^{n \times m}$ for some integers q, m, n, we define as follows.

$\Lambda_q(\boldsymbol{A}) = \{\boldsymbol{y} \in Z_q^m : \exists \boldsymbol{x} \in Z_q^n, \boldsymbol{y} = \boldsymbol{A}^\top \boldsymbol{x} \; mod \; q\}$.

$\Lambda_q^\perp(\boldsymbol{A}) = \{\boldsymbol{e} \in Z_q^m : \boldsymbol{A}\boldsymbol{e} = 0 \; mod \; q\}$.

$\Lambda_q^{\boldsymbol{y}}(\boldsymbol{A}) = \{\boldsymbol{e} \in Z_q^m : \boldsymbol{A}\boldsymbol{e} = \boldsymbol{y} \; mod \; q\}$.

Observe that $\Lambda_q^{\boldsymbol{y}}(\boldsymbol{A}) = \boldsymbol{t} + \Lambda_q^\perp(\boldsymbol{A}) \; mod \; q$, where $\boldsymbol{t}$ is an arbitrary solution of the equation $\boldsymbol{A}\boldsymbol{t} = \boldsymbol{y} \; mod \; q$. Thus $\Lambda_q^{\boldsymbol{y}}(\boldsymbol{A})$ is the coset of $\Lambda_q(\boldsymbol{A})$.

Discrete Gaussian on Lattices. For any vector $\boldsymbol{u} \in \mathcal{R}^m$, any positive real number $r > 0$, the Gaussian function on $\mathcal{R}^m$ with center $\boldsymbol{u}$ with deviation r is $\rho_{r,\boldsymbol{u}}(\boldsymbol{x}) = exp(-\pi \|\boldsymbol{x} - \boldsymbol{u}\|^2/r^2)$. Denote $\rho_{r,\boldsymbol{u}}(\Lambda) = \sum_{\boldsymbol{x} \in \Lambda} \rho_{r,\boldsymbol{u}}(\boldsymbol{x})$, the discrete Gaussian distribution over Λ with center $\boldsymbol{u}$ and parameter r is $\forall \boldsymbol{x} \in \Lambda$, $\chi = \mathcal{D}_{\Lambda,r,\boldsymbol{u}}(\boldsymbol{x}) = \rho_{r,\boldsymbol{u}}(\boldsymbol{x})/\rho_{r,\boldsymbol{u}}(\Lambda)$.

Hardness problem assumptions on lattices.

Definition 2: The hardness assumption of $LWE_{q,m,\chi}$ problem is defined as follows. For positive integers n, m, q, where $m \geq n$, $q \geq 2$, choose a vector $\boldsymbol{s} \in Z_q^n$, and a discrete Gaussian distribution χ on the Z_q^m, choose a uniform random matrix $\boldsymbol{A} \leftarrow Z_q^{n \times m}$, a random vector $\boldsymbol{y} \leftarrow Z_q^m$, and sample a vector $\boldsymbol{e} \leftarrow \chi$, the distribution $(\boldsymbol{A}, \boldsymbol{A}^\top \boldsymbol{s} + \boldsymbol{e})$ and the distribution $(\boldsymbol{A}, \boldsymbol{y})$ are indistinguishable as described in [24].

Based on the security proof in [24], $LWE_{q,m,\chi}$ is as hard as solving several standard worst-case lattice problems using a quantum algorithm. Moreover, for an LWE instance $(\boldsymbol{A}, \boldsymbol{A}^\top \boldsymbol{s} + \boldsymbol{e})$, provided that we get the knowledge of the trapdoor $\boldsymbol{T}$, with that the Euclidean norm of $\boldsymbol{T}$ is small enough, and $\boldsymbol{e}$ is sampled from a discrete Gaussian distribution χ, thus $\boldsymbol{s}$ could be easily recovered as described in [56]. Note that $\boldsymbol{T}^\top(\boldsymbol{A}^\top \boldsymbol{s} + \boldsymbol{e})(mod \; q) = (\boldsymbol{A}\boldsymbol{T})^\top \boldsymbol{s} + \boldsymbol{T}^\top \boldsymbol{e}(mod \; q) = \boldsymbol{T}^\top \boldsymbol{e}(mod \; q)$, both $\boldsymbol{T}$ and $\boldsymbol{e}$ contain only small entries, each entry of the vector $\boldsymbol{T}^\top \boldsymbol{e}$ is smaller than q and $\boldsymbol{T}^\top \boldsymbol{e}(mod \; q)$ is equal to $\boldsymbol{T}^\top \boldsymbol{e}$. Multiplied by $(\boldsymbol{T}^\top)^{-1}$, we get $\boldsymbol{e}$. Furthermore, we could easily recover $\boldsymbol{s}$.

Definition 3: The inhomogeneous small integer solution assumption of ($ISIS_{q,m,\zeta}$) problem is given as follows. For a prime q, a matrix $\boldsymbol{A} \in Z_q^{n \times m}$, a uniform random vector $\boldsymbol{y} \in Z_q^n$, and a real number ζ, the goal of $ISIS_{q,m,\zeta}$ is to find a nonzero integer vector $\boldsymbol{e} \in Z_q^m$, such that $\boldsymbol{e} \neq 0, \boldsymbol{A}\boldsymbol{e} = \boldsymbol{y} \; mod \; q$ and $0 < \|\boldsymbol{e}\| \leq \zeta$. For any poly-bounded m, $\zeta = poly(n)$, and for any prime $q > \zeta \cdot \omega(\sqrt{n \log n})$, the average-case assumption of $ISIS_{q,m,\zeta}$ is as hard as approximating the assumption of $SIVP$ in the worst case to within certain factors $\gamma(n) = \zeta \cdot \tilde{O}(\sqrt{n})$ in [25].

Preimage sampleable function and lattice basis delegation technique.

Lattice has useful cryptographic applications due to its natural trapdoor characteristic. We first describe an algorithm that generates a uniform random matrix $\boldsymbol{A} \in Z_q^{n \times m}$ and a trapdoor matrix $T_{\boldsymbol{A}} \in Z_q^{m \times m}$, then we describe the preimage sampleable function. Finally, we describe the lattice basis delegation technique.

Definition 4: There is a PPT algorithm **TrapGen**(q,n) [57] that outputs $(\boldsymbol{A} \in Z_q^{n \times m}, T_{\boldsymbol{A}} \in Z_q^{m \times m})$ such that: $\boldsymbol{A}$ is statistically close to a uniform random matrix in $Z_q^{n \times m}$. $T_{\boldsymbol{A}}$ is a basis of $\Lambda_q^\perp(A)$, the Euclidean norm of all the rows in $T_{\boldsymbol{A}}(\|T_{\boldsymbol{A}}\|)$ is bounded by $O(n \log q)$ with all but negligible probability in n.

Definition 5: The preimage sampleable function is defined as follows. Taking as inputs a matrix $\boldsymbol{A} \in Z_q^{n \times m}$, a basis $T_{\boldsymbol{A}} \in Z_q^{m \times m}$ of $\Lambda_q^\perp(\boldsymbol{A})$, a parameter $\sigma \geq \|\widetilde{T_{\boldsymbol{A}}}\| \cdot \omega(\sqrt{\log n})$, and a vector $\boldsymbol{y} \in Z_q^n$, the preimage sampleable function **SamplePre**$(\boldsymbol{A}, T_{\boldsymbol{A}}, \boldsymbol{y}, \sigma)$ [25] outputs a sample $\theta \in Z_q^m$ which is from a distribution that is statistically close to $\mathcal{D}_{\Lambda_q^{\boldsymbol{y}}(\boldsymbol{A}),\sigma}$, where $\mathcal{D}_{\Lambda_q^{\boldsymbol{y}}(\boldsymbol{A}),\sigma}$ is the discrete Gaussian distribution over $\Lambda_q^{\boldsymbol{y}}(\boldsymbol{A})$ with parameter σ.

Agrawal *et al.* [58] have proposed a technique for delegating short lattice basis that enjoys the advantage of keeping the lattice dimension unchanged.

According to [59], there exists a PPT algorithm that takes as inputs an arbitrary basis of m-dimensional lattice Λ and a full-rank set $\boldsymbol{S} = \{\boldsymbol{s}_1, \cdots, \boldsymbol{s}_m\}$ in Λ, outputs a basis $\boldsymbol{T}$ of Λ satisfying $\|\widetilde{\boldsymbol{T}}\| \leq \|\widetilde{\boldsymbol{S}}\|$ and $\|\boldsymbol{T}\| \leq \|\boldsymbol{S}\| \cdot \sqrt{m}/2$.

We describe the distribution $\mathcal{D}_{m \times m}$ as follows. $\mathcal{D}_{m \times m}$ denotes the distribution on a matrix in $Z_q^{m \times m}$, which is defined as $(\mathcal{D}_{Z^m,\sigma_{\boldsymbol{R}}})^m$ conditioned on the resulting matrix being Z_q−invertible that the $\boldsymbol{R}$ matrix mod q is invertible as a matrix in $Z_q^{m\times m}$, here the parameter $\sigma_{\boldsymbol{R}} = \sqrt{n \log q} \cdot \omega(\sqrt{\log m})$.

Finally, we describe the lattice basis delegation algorithm **NewBasisDel** in [58] for $\boldsymbol{B} = \boldsymbol{A}\boldsymbol{R}^{-1}$. The algorithm **NewBasisDel** takes as inputs a rank n matrix $\boldsymbol{A} \in Z_q^{n\times m}$, a Z_q-invertible matrix $\boldsymbol{R}$ sampled from $\mathcal{D}_{m\times m}$, a short basis $T_{\boldsymbol{A}}$ for $\Lambda_q^{\perp}(\boldsymbol{A})$ and parameter $\delta \geq \|\widetilde{T_{\boldsymbol{A}}}\| \cdot \sigma_{\boldsymbol{R}} \sqrt{m} \cdot \omega(\log^{3/2} m)$, and outputs a short basis $T_{\boldsymbol{B}}$ of $\Lambda_q^{\perp}(\boldsymbol{B})$. **NewBasisDel(**$\boldsymbol{A}, \boldsymbol{R}, T_{\boldsymbol{A}}, \delta$**)** proceeds as follows.

(1) Calculate $T'_{\boldsymbol{B}} = \{\boldsymbol{R}\boldsymbol{a}_1, \cdots, \boldsymbol{R}\boldsymbol{a}_m\} \subseteq Z_q^m$, where $T_{\boldsymbol{A}} = \{\boldsymbol{a}_1, \cdots, \boldsymbol{a}_m\} \subseteq Z_q^m$.

(2) Convert $T'_{\boldsymbol{B}}$ into a basis $T''_{\boldsymbol{B}}$ of $\Lambda_q^{\perp}(\boldsymbol{B})$ according to [59].

(3) With the random algorithm **RandBasis**($T''_{\boldsymbol{B}}, \delta$) in [60] to make randomized basis $T_{\boldsymbol{B}}$ of $\Lambda_q^{\perp}(\boldsymbol{B})$ from $T''_{\boldsymbol{B}}$.

IV. CLOUD STORAGE DESIGNATED VERIFIER AUDITING SCHEME FOR MEDICAL DATA IN WBANs

A. OVERVIEW

In this section, we propose a lattice-based designated verifier auditing scheme for electronic medical data in cloud-assisted WBANs. In the proposed scheme, we define a designated verifier as a designated third-party auditor (TPA). To enable the designated TPA to check the integrity of the outsourced medical data stored in a cloud server associated with WBANs efficiently, we utilize a lattice-based linearly homomorphic signature algorithm as a basis tool, to realize the construction of linearly homomorphic authenticators. In particular, we require a patient to perform verifier designation authority. In such case, the patient could flexibly designate a trusted third party to check the outsourced medical data integrity. When the patient wants to check the integrity and correctness of the medical data, as a role of the KGC in an identity-based system, the patient produces the private key according to the identity of the designated TPA, and sends it to the designated TPA via a secure channel. Thus, the designated TPA could execute the subsequent auditing tasks. Furthermore, to guarantee privacy preservation against a curious designated TPA, we take advantage of the preimage sampleable function to produce a signature of a random sample vector, which is termed as random masking. Accordingly, combining linearly homomorphic authenticators with the random masking technique, the scheme could also prevent the designated TPA from recovering the patient's primitive medical data blocks.

B. THE CONSTRUCTION OF LDVAS

The proposed lattice-based designated verifier auditing scheme (LDVAS) for electronic medical data consists of the following three phases: system initialization phase, auditing delegation phase, and challenge-response phase.

The system initialization phase contains the following three algorithms.

Setup: A patient first preprocesses an electronic medical data file F into l medical data blocks $F = \{m_1, m_2, \cdots, m_l\}$, each $m_i \in Z_q^m, 1 \leq i \leq l, F$ could be actually considered as an $m \times l$ matrix. In addition, in order to enable two algorithms **SamplePre** and **NewBasisDel** to execute correctly, the system sets two secure Gaussian parameters σ, δ, respectively, which have been introduced before. For a secure parameter n, the system also sets $params = \{q, m, \widetilde{L}, \mathcal{D}_n, \chi\}$, where $q = poly(n)$, $m \geq \lceil 2n \log q \rceil$, $\widetilde{L} = O(\sqrt{n \log q})$, and $\mathcal{D}_n = \{\boldsymbol{e} \in Z_q^m : 0 < \|\boldsymbol{e}\| \leq \sigma\sqrt{m}\}$, χ is a discrete Gaussian distribution. Finally, the system sets $H_1 : Z_q^{n\times m} \times \{0,1\}^* \rightarrow Z_q^n$, $H_2 : \{0,1\}^* \rightarrow Z_q^n$, $H_4 : Z_q^n \rightarrow Z_q$, $H_5 : Z_q^m \times Z_q^n \rightarrow Z_q^m$ to be four secure collision-resistant hash functions, and sets $H_3 : \{0,1\}^* \rightarrow Z^{m\times m}$ to be a collision-resistant hash function, the output value of H_3 is distributed in $\mathcal{D}_{m\times m}$.

KeyGen: The patient runs **TrapGen**(q, n) to produce a uniform random matrix $\boldsymbol{A} \in Z_q^{n\times m}$ and a basis $T_{\boldsymbol{A}}$ for $\Lambda_q^{\perp}(\boldsymbol{A})$ such that $\|\widetilde{T_{\boldsymbol{A}}}\| \leq \widetilde{L}$. To guarantee the integrity of the unique identity of the medical data file, the patient also selects a light-weight signature algorithm with the corresponding key pair (spk, ssk). Meantime, a cloud server also runs **TrapGen(**q, n**)** to produce a uniform random matrix $\boldsymbol{B} \in Z_q^{n\times m}$ and a basis $T_{cloud} \in Z_q^{m\times m}$ for $\Lambda_q^{\perp}(\boldsymbol{B})$ such that $\|\widetilde{T}_{cloud}\| \leq \widetilde{L}$. Thus, the public parameters are $PK = \{spk, \boldsymbol{A}, \boldsymbol{B}\}$, the secret parameters are $MK = \{ssk, T_{\boldsymbol{A}}, T_{cloud}\}$.

TagGen: For each medical data block $m_i \in Z_q^m$ in the medical data file $F = \{m_1, m_2, \cdots, m_l\}$, with its identity being $id \in \{0,1\}^*$, utilizing the patient's public-private key pair $(\boldsymbol{A}, T_{\boldsymbol{A}})$ and the public key $\boldsymbol{B}$ of the cloud server, the patient produces the signature as follows.

- Compute n vectors $\beta_j = H_1(\boldsymbol{A}\|id\|j) \in Z_q^n$ for $1 \leq j \leq n$.
- Compute $\mu_i = H_2(id\|i) + \boldsymbol{B}m_i \in Z_q^n$, the inner products $h_{i,j} = \langle \mu_i, \beta_j \rangle \in Z_q$ $1 \leq j \leq n$, and parse $h_i = (h_{i1}, \cdots, h_{in})^{\top} \in Z_q^n$.
- Run **SamplePre**($\boldsymbol{A}, T_{\boldsymbol{A}}, h_i, \sigma$) to produce a signature $\theta_i \in Z_q^m$.

Denote the set of signatures by $\Psi = \{\theta_i\}_{1 \leq i \leq l}$. To make sure the integrity of the unique medical data file id, the patient utilizes a light-weight signature algorithm to compute $\tau = id\|SSig_{ssk}(id)$ as the medical data file tag of F, where $SSig_{ssk}(id)$ is the signature of id under the private key ssk. Finally, the patient sends $\{F, \tau, \Psi\}$ to the cloud server and deletes them in the local storage.

The auditing delegation phase contains only the verifier designation **VerDesig** algorithm as follows.

VerDesig: When the patient sends a request message for the auditing task to a designated TPA, with the identity ID_{TPA}, the patient computes $\boldsymbol{R}_{ID_{TPA}} = H_3(ID_{TPA}) \in Z_q^{m\times m}$, $Q_{ID_{TPA}} = \boldsymbol{A}(\boldsymbol{R}_{ID_{TPA}})^{-1} \in Z_q^{n\times m}$, and runs **NewBasisDel(**$\boldsymbol{A}, \boldsymbol{R}_{ID_{TPA}}, T_{\boldsymbol{A}}, \delta$**)** to generate the corresponding private key $T_{ID_{TPA}} \in Z_q^{m\times m}$, where $T_{ID_{TPA}}$ is a random short lattice basis for $\Lambda_q^{\perp}(Q_{ID_{TPA}})$. Then the patient sends $(Q_{ID_{TPA}}, T_{ID_{TPA}})$ to the designed TPA via a secure channel, and registers $(ID_{patient}, ID_{TPA}, Q_{ID_{TPA}})$ into the cloud server.

The challenge-response phase for the designated auditing scheme contains the following three algorithms.

GenChal: Once receiving the request message for designated auditing task from the patient, the designated TPA first retrieves the file tag τ for F, with respect to the scheme we have described in the **TagGen** algorithm, the designated TPA checks the validity of the signature $SSig_{ssk}(id)$ with spk, and then constructs the challenge message $chal$ as follows.

The designated TPA first selects a random c-element subset $\mathcal{I} = \{l_1, \cdots, l_c\}$ of set $\{1, 2, \cdots, l\}$. Then the designated TPA randomly chooses a string $(c_{l_1}, c_{l_2}, \cdots, c_{l_c}) \in \{0, 1\}^c$. The challenge message $chal = \{\{i, c_i\}_{i\in\mathcal{I}}, ID_{TPA}\}$ locates the medical data blocks need to be checked. Finally, the designated TPA sends $chal = \{\{i, c_i\}_{i\in\mathcal{I}}, ID_{TPA}\}$ to the cloud server.

GenProof: Upon receiving challenge message $chal = \{\{i, c_i\}_{i\in\mathcal{I}}, ID_{TPA}\}$, the cloud server looks into $(ID_{patient}, ID_{TPA}, Q_{ID_{TPA}})$ in its database, and computes the aggregate signature $\theta = \sum_{i\in\mathcal{I}} c_i\theta_i$, the aggregate message $\nu = \sum_{i\in\mathcal{I}} c_i m_i$. To blind the aggregation message ν, the cloud server selects a random vector $\boldsymbol{w} \leftarrow Z_q^n$, then runs **SamplePre**$(\boldsymbol{B}, T_{cloud}, \boldsymbol{w}, \sigma)$ to generate the signature $\gamma \in Z_q^m$ of $\boldsymbol{w}$. Then the cloud server executes as follows:

- Compute $\nu' = \gamma + H_4(w)\nu \in Z_q^m$.
- Randomly select a new vector $\xi' \leftarrow Z_q^n$, and compute $H_5(\nu'\|\xi') \in Z_q^m$.
- Select an error vector $\boldsymbol{s} \leftarrow Z_q^m$ according to the discrete Gaussian distribution χ. Compute $\boldsymbol{e} = \theta + H_5(\nu'\|\xi')$, $\xi = Q^{\top}_{ID_{TPA}}\xi' + \boldsymbol{s}$.

Finally, the cloud server sends $P = \{\nu', \boldsymbol{w}, \boldsymbol{e}, \xi\}$ as the response auditing proof information of storage correctness to the designated TPA.

VerifyProof: Using the private key $T_{ID_{TPA}}$, the designated TPA could compute $T^{\top}_{ID_{TPA}}\xi = T^{\top}_{ID_{TPA}}(Q^{\top}_{ID_{TPA}}\xi' + \boldsymbol{s}) = T^{\top}_{ID_{TPA}}\boldsymbol{s}$ *mod q*. Since $T_{ID_{TPA}}$ is a trapdoor basis of $\Lambda_q^{\perp}(Q_{ID_{TPA}})$, whose entries are all sufficiently small and $\boldsymbol{s}$ is an error vector whose entries are also small enough, thus $T^{\top}_{ID_{TPA}}\xi = T^{\top}_{ID_{TPA}}\xi$ *mod q* with an overwhelm probability. Thus the designated TPA could compute $\boldsymbol{s} = (T^{-1}_{ID_{TPA}})^{\top}T^{\top}_{ID_{TPA}}\xi$ *mod q*. And then, the designated TPA gets ξ' from ξ and $\boldsymbol{s}$. Furthermore, the designated TPA computes the aggregate signature $\theta = \boldsymbol{e} - H_5(\nu'\|\xi')$.

The designated TPA proceeds to check the validity of the response auditing proof information as follows.

- Compute n vectors $\beta_j = H_1(\boldsymbol{A}\|id\|j) \in Z_q^n$ for $1 \le j \le n$.
- Compute $\lambda = H_4(\boldsymbol{w})\sum_{i\in\mathcal{I}} c_i H_2(id\|i) - \boldsymbol{w} + \boldsymbol{B}\nu' \in Z_q^n$.
- Compute the inner products $h_{\mathcal{I}j} = \langle\lambda, \beta_j\rangle \in Z_q$, $1 \le j \le n$, and parse $h_{\mathcal{I}} = (h_{\mathcal{I}1}, \cdots, h_{\mathcal{I}n})^{\top} \in Z_q^n$.
- Check the verification equation $H_4(\boldsymbol{w})\boldsymbol{A}\theta = h_{\mathcal{I}}$ and the inequation $0 < \|\theta\| \le c\sigma\sqrt{m}$ whether or not hold.

The correctness of the verification equation is elaborated as follows:

$$\begin{aligned}
H_4(\boldsymbol{w})\boldsymbol{A}\theta &= H_4(\boldsymbol{w})\boldsymbol{A}\sum_{i\in\mathcal{I}} c_i\theta_i = H_4(\boldsymbol{w})\sum_{i\in\mathcal{I}} c_i\boldsymbol{A}\theta_i \\
&= H_4(\boldsymbol{w})\sum_{i\in\mathcal{I}} c_i h_i = H_4(\boldsymbol{w})\sum_{i\in\mathcal{I}} c_i h_i \\
&= H_4(\boldsymbol{w})\sum_{i\in\mathcal{I}} c_i(\langle\mu_i, \beta_1\rangle, \cdots, \langle\mu_i, \beta_n\rangle)^{\top} \\
&= H_4(\boldsymbol{w})(\langle\sum_{i\in\mathcal{I}} c_i\mu_i, \beta_1\rangle, \cdots, \langle\sum_{i\in\mathcal{I}} c_i\mu_i, \beta_n\rangle)^{\top} \\
&= H_4(\boldsymbol{w})(\langle\sum_{i\in\mathcal{I}} c_i\mu_i, \beta_1\rangle, \cdots, \langle\sum_{i\in\mathcal{I}} c_i\mu_i, \beta_n\rangle)^{\top} \\
&= H_4(\boldsymbol{w})(\langle\sum_{i\in\mathcal{I}} c_i H_2(id\|i) + \boldsymbol{B}\nu, \beta_1\rangle, \cdots, \\
&\qquad \langle\sum_{i\in\mathcal{I}} c_i H_2(id\|i) + \boldsymbol{B}\nu, \beta_n\rangle)^{\top} \\
&= (\langle H_4(\boldsymbol{w})\sum_{i\in\mathcal{I}} c_i H_2(id\|i) + \boldsymbol{B}H_4(\boldsymbol{w})\nu, \beta_1\rangle, \cdots, \\
&\qquad \langle H_4(\boldsymbol{w})\sum_{i\in\mathcal{I}} c_i H_2(id\|i) + \boldsymbol{B}H_4(\boldsymbol{w})\nu, \beta_n\rangle)^{\top} \\
&= (\langle H_4(\boldsymbol{w})\sum_{i\in\mathcal{I}} c_i H_2(id\|i) + \boldsymbol{B}(\nu' - \gamma), \beta_1\rangle, \cdots, \\
&\qquad \langle H_4(\boldsymbol{w})\sum_{i\in\mathcal{I}} c_i H_2(id\|i) + \boldsymbol{B}(\nu' - \gamma), \beta_n\rangle)^{\top} \\
&= (\langle H_4(\boldsymbol{w})\sum_{i\in\mathcal{I}} c_i H_2(id\|i) - \boldsymbol{w} + \boldsymbol{B}\nu', \beta_1\rangle, \cdots, \\
&\qquad \langle H_4(\boldsymbol{w})\sum_{i\in\mathcal{I}} c_i H_2(id\|i) - \boldsymbol{w} + \boldsymbol{B}\nu', \beta_n\rangle)^{\top} \\
&= (\langle\lambda, \beta_1\rangle, \cdots, \langle\lambda, \beta_n\rangle)^{\top} \\
&= h_{\mathcal{I}}.
\end{aligned}$$

Therefore the verification equation $H_4(\boldsymbol{w})\boldsymbol{A}\theta = h_{\mathcal{I}}$ holds. On the other hand, since $\theta_i \in Z_q^m$ is a signature of message $m_i \in Z_q^m$, for any $i \in \mathcal{I}$, $0 < \|\theta_i\| \le \sigma\sqrt{m}$ holds, and thus $0 < \|\theta\| = \|\sum_{i\in\mathcal{I}}\theta_i\| \le c\sigma\sqrt{m}$ holds.

V. EVALUATION OF LDVAS

A. STORAGE CORRECTNESS GUARANTEE

In this section, we engage in proving the proposed LDVAS for electronic medical data in cloud-assisted WBANs achieves storage correctness guarantee in the random oracle model. The security proof demonstrates that a malicious cloud server as an adversary cannot cheat the designated TPA, or cannot pass the verification process by providing a forged response auditing proof information. The following theorem proves the idea properly.

Theorem 1: For a malicious cloud server, it is computationally infeasible to generate a forged response auditing proof information that could pass the verification phase in LDVAS.

Proof 1: We assume that there exists an adversary $\mathcal{A}$ (a malicious cloud server) which could generate a forged response auditing proof information passing the verification phase, with a non-negligible probability ε. In the following steps, we will demonstrate how to construct an algorithm $\mathcal{C}$ that could solve the SIS assumption with also a non-negligible probability at least $\varepsilon' \ge \varepsilon$, by running the adversary $\mathcal{A}$ as a subroutine. Here the adversary $\mathcal{A}$ interacts with the challenger $\mathcal{B}$, which plays the role of a patient or a designated TPA.

First of all, the adversary $\mathcal{A}$ is provided with an instance of ISIS assumption $(\boldsymbol{A}, \boldsymbol{y}) \in Z_q^{n\times m} \times Z_q^n$, and tries to find vector θ_k^* using the forged signature of $\mathcal{A}$ such that $0 < \|\theta_k^*\| \leq \sigma\sqrt{m}$ and $\boldsymbol{A}\theta_k^* = \boldsymbol{y}$. In particular, we will give the detailed value of $\boldsymbol{y}$ in the last security proof process. $\mathcal{B}$ also sets five random oracles $\mathcal{O}_{H_1}$, $\mathcal{O}_{H_2}$, $\mathcal{O}_{H_3}$, $\mathcal{O}_{H_4}$, $\mathcal{O}_{H_5}$. To maintain consistency, $\mathcal{B}$ will maintain the corresponding five lists L_1, L_2, L_3, L_4, L_5 which are initialized to be empty.

The challenger $\mathcal{B}$ produces the public parameters $PK = \{spk, \boldsymbol{A}, \boldsymbol{B}\}$, the designated TPA's public key $(ID_{TPA}, Q_{ID_{TPA}})$, and sends them to the adversary $\mathcal{A}$, and $\mathcal{B}$ saves the secret parameters secretly.

$\mathcal{O}_{H_1}$ queries: For a distinct $(\boldsymbol{A}, id, j)$, $\mathcal{B}$ first checks if the value of H_1 was previously defined. If it was, the previously defined value is returned. Otherwise, $\mathcal{B}$ randomly chooses a string from Z_q^n, and stores it into list L_1, then returns it to the adversary $\mathcal{A}$.

The adversary $\mathcal{A}$ executes queries for $\mathcal{O}_{H_2}$, $\mathcal{O}_{H_3}$, $\mathcal{O}_{H_4}$, $\mathcal{O}_{H_5}$ to the challenger $\mathcal{B}$, $\mathcal{B}$ could also answer the queries to $\mathcal{A}$ respectively in a similar way of the querying for $\mathcal{O}_{H_1}$, and meantime $\mathcal{B}$ stores their hash values into list L_2, L_3, L_4, L_5 respectively.

Signing query: The adversary $\mathcal{A}$ queries for $F' = \{m_1', m_2', \cdots, m_l'\}$, its identity is $id' \in \{0, 1\}^*$, as the role of a patient, the challenger $\mathcal{B}$ performs as follows: $\mathcal{B}$ looks into list L_1 to get $(\boldsymbol{A}, id', j, H_1(\boldsymbol{A}\|id'\|j)$ for $1 \leq j \leq n$, and looks into list L_2 to get $(id', i, H_2(id'\|i))$ for $1 \leq i \leq l$. Then $\mathcal{B}$ computes each $\mu_i' = H_2(id'\|i) + \boldsymbol{B}m_i'$, $1 \leq i \leq l$, and computes $h_i' = (h_{i1}', \cdots, h_{in}')^\top$, where $h_{ij}' = \langle\mu_i', H_1(A\|id'\|j)\rangle$, $1 \leq j \leq n$, $1 \leq i \leq l$. For each $i \in \{1, \cdots, l\}$, the challenger $\mathcal{B}$ executes **SamplePre**$(\boldsymbol{A}, T_{\boldsymbol{A}}, h_i', \sigma)$ to generate signature θ_i'. Meanwhile, the challenger $\mathcal{B}$ utilizes a light-weight signature algorithm to compute $\tau' = id'\|SSig_{ssk}(id')$. Finally, $\mathcal{B}$ returns $\{F', \Psi' = \{\theta_1', \cdots, \theta_l'\}, \tau'\}$ to the adversary $\mathcal{A}$.

After querying for polynomial times as above, as the role of the designated TPA, when the challenger $\mathcal{B}$ produces $chal = \{\{i, c_i\}_{i\in\mathcal{I}}, ID_{TPA}\}$ to the adversary $\mathcal{A}$, $\mathcal{A}$ executes as follows.

The adversary $\mathcal{A}$, as the role of a malicious cloud server, may try to initiate tampering attacks in the designated verifier auditing scheme for cloud storage systems. It means that $\mathcal{A}$ could tamper with the patient's medical data m_k as m_k^*, and the patient's signature θ_k as θ_k^* with a non-negligible probability, and $\mathcal{A}$ tries to cheat the designated TPA to believe that the response auditing proof information could pass the verification process. More specially, with the private key T_{cloud}, and the designated TPA's public key $Q_{ID_{TPA}}$, $\mathcal{A}$ performs as follows.

- Select a random vector $\boldsymbol{w} \leftarrow Z_q^n$, and runs **SamplePre**$(\boldsymbol{B}, T_{cloud}, \boldsymbol{w}, \sigma)$ to produce the signature $\gamma \in Z_q^m$ of $\boldsymbol{w}$, then $\mathcal{A}$ outputs the forged aggregate medical data message $\nu'^* = \gamma + H_4(\boldsymbol{w})\cdot(\sum_{i\in\mathcal{I},i\neq k} c_i m_i + c_k m_k^*) \in Z_q^m$.
- Randomly select a new vector $\xi'^* \leftarrow Z_q^n$, and compute $H_5(\nu'^*\|\xi'^*) \in Z_q^m$.
- Select an error vector $\boldsymbol{s}^* \in Z_q^m$ according to the discrete Gaussian distribution χ. Compute the aggregate signature $\theta^* = \sum_{i\in\mathcal{I},i\neq k} c_i\theta_i + c_k\theta_k^*$, then compute $\boldsymbol{e}^* = \theta^* + H_5(\nu'^*\|\xi'^*)$, and $\xi^* = Q_{ID_{TPA}}^\top \xi'^* + \boldsymbol{s}^*$.

Finally, $\mathcal{A}$ sends the forged response auditing proof information $P^* = \{\nu'^*, \boldsymbol{w}, \boldsymbol{e}^*, \xi^*\}$ to the challenger $\mathcal{B}$. Assume that P^* from $\mathcal{A}$ is successfully tampered with, thus it could pass the correct verification equation:

$$H_4(\boldsymbol{w})\boldsymbol{A}\theta^* = (\langle H_4(\boldsymbol{w})\sum_{i\in\mathcal{I}} c_i H_2(id\|i) - \boldsymbol{w} + \boldsymbol{B}\nu'^*, \beta_1\rangle,$$
$$\cdots, \langle H_4(\boldsymbol{w})\sum_{i\in\mathcal{I}} c_i H_2(id\|i) - \boldsymbol{w} + \boldsymbol{B}\nu'^*, \beta_n\rangle)^\top$$

The inequation $0 < \|\theta^*\| = \|\sum_{i\in\mathcal{I}} \theta_i^*\| \leq c\sigma\sqrt{m}$ holds.

For simplicity, suppose $\boldsymbol{E}$ is a matrix such that the j-th row of $\boldsymbol{E}$ is the vector $\beta_j = H_1(\boldsymbol{A}\|id\|j) \in Z_q^n (1 \leq j \leq n)$ in row form. Thus:

$$H_4(\boldsymbol{w})\boldsymbol{A}\theta^* = \boldsymbol{E}(H_4(\boldsymbol{w})\sum_{i\in\mathcal{I}} c_i H_2(id\|i) - \boldsymbol{w} + \boldsymbol{B}\nu'^*).$$

As a matter of fact, the equation $H_4(\boldsymbol{w})\boldsymbol{A}\theta^* = H_4(\boldsymbol{w})\boldsymbol{A}(\sum_{i\in\mathcal{I},i\neq k} c_i\theta_i + c_k\theta_k^*)$ holds. With respect to the combined medical data message $\sum_{i\in\mathcal{I},i\neq k} c_i m_i$ and aggregate signature $\sum_{i\in\mathcal{I},i\neq k} c_i\theta_i$, we could consider that the cloud server has generated a valid response auditing proof information $P_1 = \{\nu_1', \boldsymbol{w}_1, \boldsymbol{e}_1, \xi_1\}$ according to the challenge message $chal = \{\{i, c_i\}_{i\in\mathcal{I},i\neq k}, ID_{TPA}\}$ from the challenger $\mathcal{B}$ as before, where $\boldsymbol{w}_1 \leftarrow Z_q^n$ is another random vector, its signature is γ_1 which is generated by **SamplePre**$(\boldsymbol{B}, T_{cloud}, \boldsymbol{w}_1, \sigma)$, and $\nu_1' = \gamma_1 + H_4(\boldsymbol{w}_1)\sum_{i\in\mathcal{I},i\neq k} c_i m_i$, $\boldsymbol{e}_1 = \sum_{i\in\mathcal{I},i\neq k} c_i\theta_i + H_5(\nu_1'\|\xi_1')$, $\xi_1 = Q_{ID_{TPA}}^\top \xi_1' + \boldsymbol{s}_1$. Thus the following verification equation holds:

$$\begin{aligned} H_4(\boldsymbol{w}_1)\boldsymbol{A} \sum_{i\in\mathcal{I},i\neq k} c_i\theta_i &= \boldsymbol{E}(H_4(\boldsymbol{w}_1) \sum_{i\in\mathcal{I},i\neq k} c_i H_2(id\|i) \\ &\quad - \boldsymbol{w}_1 + \boldsymbol{B}\nu_1') \\ &= \boldsymbol{E}(H_4(\boldsymbol{w}_1) \sum_{i\in\mathcal{I},i\neq k} c_i H_2(id\|i) \\ &\quad - \boldsymbol{w}_1 + \boldsymbol{B}(\gamma_1 + H_4(\boldsymbol{w}_1) \sum_{i\in\mathcal{I},i\neq k} c_i m_i)) \end{aligned}$$

Therefore, we get that:

$$\begin{aligned} H_4(\boldsymbol{w})\boldsymbol{A}\theta^* &= H_4(\boldsymbol{w})\boldsymbol{A}(\sum_{i\in\mathcal{I},i\neq k} c_i\theta_i + c_k\theta_k^*) \\ &= H_4(\boldsymbol{w})\boldsymbol{A} \sum_{i\in\mathcal{I},i\neq k} c_i\theta_i + H_4(\boldsymbol{w})c_k\boldsymbol{A}\theta_k^* \\ &= H_4(\boldsymbol{w})H_4(\boldsymbol{w}_1)^{-1}\boldsymbol{E}(H_4(\boldsymbol{w}_1) \\ &\quad \sum_{i\in\mathcal{I},i\neq k} c_i H_2(id\|i) - \boldsymbol{w}_1 + \boldsymbol{B}(\gamma_1 + H_4(\boldsymbol{w}_1) \\ &\quad \sum_{i\in\mathcal{I},i\neq k} c_i m_i)) + H_4(\boldsymbol{w})c_k\boldsymbol{A}\theta_k^* \end{aligned}$$

Thus, we could get the following equation holds:

$$H_4(\boldsymbol{w})\boldsymbol{A}\theta^* = H_4(\boldsymbol{w})\boldsymbol{E}\sum_{i\in\mathcal{I},i\neq k} c_i H_2(id\|i) + H_4(\boldsymbol{w})\boldsymbol{EB}\sum_{i\in\mathcal{I},i\neq k} c_i m_i + H_4(\boldsymbol{w})c_k\boldsymbol{A}\theta_k^*.$$

Since the adversary $\mathcal{A}'s$ forged response auditing proof information $P^* = \{\nu'^{*}, \boldsymbol{w}, \boldsymbol{e}^*, \xi^*\}$ could pass the verification equation:

$$H_4(\boldsymbol{w})\boldsymbol{A}\theta^* = \boldsymbol{E}(H_4(\boldsymbol{w})\sum_{i\in\mathcal{I}} c_i H_2(id\|i) - \boldsymbol{w} + \boldsymbol{B}\nu'^{*}).$$

According to the above two kinds of expression forms of $H_4(\boldsymbol{w})\boldsymbol{A}\theta^*$, we get that:

$$H_4(\boldsymbol{w})\boldsymbol{E}c_k H_2(id\|k) - \boldsymbol{Ew} + \boldsymbol{EB}\nu'^{*} = H_4(\boldsymbol{w})\boldsymbol{EB}\sum_{i\in\mathcal{I},i\neq k} c_i m_i + H_4(\boldsymbol{w})c_k\boldsymbol{A}\theta_k^*.$$

As described before that $\nu_1' = \gamma_1 + H_4(\boldsymbol{w}_1)\sum_{i\in\mathcal{I},i\neq k} c_i m_i$, where $\gamma_1 \leftarrow$ **SamplePre** $(\boldsymbol{B}, T_{cloud}, \boldsymbol{w}_1, \sigma)$, thus $H_4(\boldsymbol{w})\boldsymbol{EB}\sum_{i\in\mathcal{I},i\neq k} c_i m_i = H_4(\boldsymbol{w})H_4(\boldsymbol{w}_1)^{-1}\cdot(\boldsymbol{EB}\nu_1' - \boldsymbol{EB}\gamma_1) = H_4(\boldsymbol{w})\cdot H_4(\boldsymbol{w}_1)^{-1}(\boldsymbol{E}(\boldsymbol{B}\nu_1' - \boldsymbol{w}_1))$.

Set $\eta = H_4(\boldsymbol{w})H_4(\boldsymbol{w}_1)^{-1}(\boldsymbol{B}\nu_1' - \boldsymbol{w}_1) \in Z_q^n$. Finally, we get that $H_4(\boldsymbol{w})\boldsymbol{E}c_k \cdot H_2(id\|k) - \boldsymbol{Ew} + \boldsymbol{EB}\nu'^{*} = \boldsymbol{E}\eta + H_4(\boldsymbol{w})c_k\boldsymbol{A}\theta_k^*$.

Once receiving $chal = \{\{i, c_i\}_{i\in\mathcal{I},i\neq k}, ID_{TPA}\}$ from $\mathcal{B}$, $\mathcal{A}$ could tamper with the patient's medical data m_k as m_k^*, and forge the patient's signature θ_k as θ_k^* with a non-negligible probability, and $\mathcal{A}$ could further succeed in forging a different response auditing proof $P^* = \{\nu'^{*}, \boldsymbol{w}, \boldsymbol{e}^*, \xi^*\}$, certainly, here $c_k = 1$. Since $H_4(\boldsymbol{w}) = 0$ or $H_4(\boldsymbol{w}_1) = 0$ is negligible, thus the equation holds with a non-negligible probability: $\boldsymbol{A}\theta_k^* = \boldsymbol{E}(H_2(id\|k) - (H_4(\boldsymbol{w}))^{-1}(\boldsymbol{w} - \boldsymbol{B}\nu'^{*} + \eta))$. As the right side of the equation is actually an n-dimension vector in Z_q^n, here for simplicity, we assume it as $\boldsymbol{y}' = \boldsymbol{E}(H_2(id\|k) - (H_4(\boldsymbol{w}))^{-1}(\boldsymbol{w} - \boldsymbol{B}\nu'^{*} + \eta))$. Actually, we see that the adversary (malicious cloud server) could get the n-dimension vector $\boldsymbol{y}'$. And thus, in the beginning of the proof, we could set $\boldsymbol{y} = \boldsymbol{y}' = \boldsymbol{E}(H_2(id\|k) - (H_4(\boldsymbol{w}))^{-1}(\boldsymbol{w} - \boldsymbol{B}\nu'^{*} + \eta))$. It means that the challenge $\mathcal{B}$ is given an instance of ISIS assumption $(\boldsymbol{A}, \boldsymbol{y}') \in Z_q^{n\times m} \times Z_q^n$, there exists an algorithm to output a nonzero vector $\theta_k^* \in Z_q^m$ which satisfies $\boldsymbol{A}\theta_k^* = \boldsymbol{y}' = \boldsymbol{y}$ with a non-negligible probability. However, as described in [25], without the trapdoor basis $T_{\boldsymbol{A}} \in Z_q^{m\times m}$ for $\Lambda_q^{\perp}(\boldsymbol{A})$, the adversary produces a forged signature only with a negligible probability. Thus, based on the forged signature, if $\mathcal{A}$ succeeds in forging the response auditing proof information also with a non-negligible probability $\varepsilon = 1 - 2^{\omega\log n}$, there exists an algorithm $\mathcal{C}$ that could solve the ISIS assumption with a non-negligible probability at least $\varepsilon' = 1 - 2^{\omega\log n}$, this is a contradiction. Consequently, we claim that it is computationally infeasible to produce a forged response auditing proof information that could pass the verification phase based on the hardness of ISIS assumption.

B. ROBUSTNESS

Theorem 2: It is computationally infeasible for any other party excepts a designated TPA to check the integrity of the outsourced medical data stored in the cloud server associated with WBANs.

Proof 2: According to the response auditing proof information $P = \{\nu', \boldsymbol{w}, \boldsymbol{e}, \xi\}$, since $\xi = Q_{ID_{TPA}}^{\top}\xi' + \boldsymbol{s}$ is an LWE instance, by the robustness hypothesis of the LWE assumption, the distribution of ξ is indistinguishable from the uniform random vector in Z_q^m. Thus if any other third party wants to recover ξ' from ξ, he/she has to master the knowledge of the designated TPA's private key. Otherwise, he/she has to solve the LWE assumption. However, it is computationally infeasible according to [24]. Therefore, we conclude that no one excepts the designated TPA could check the integrity of the medical data stored in the cloud server associated with WBANs.

C. PRIVACY PRESERVATION

Theorem 3: Provided with the response auditing proof information $P = \{\nu', \boldsymbol{w}, \boldsymbol{e}, \xi\}$ from a cloud server, it is computationally infeasible for a curious designated TPA to reveal any medical data blocks in the medical data file $F = \{m_1, m_2, \cdots, m_l\}$ of the patient.

Proof 3: Once the aggregate medical data message $\nu = \sum_{i\in\mathcal{I}} c_i m_i$, as a linear combination of elements in medical data blocks, is directly sent to the designated TPA. Provided that it utilizes some powerful computing devices, the curious designated TPA could master the contents of medical data blocks through solving linear combinations. To preserve private medical data blocks from the curious designated TPA, the aggregate medical data message is computed with a random masking as $\nu' = \gamma + H_4(\boldsymbol{w})\nu$. In order to still solve these linear equations, the designated TPA needs to know about the signature $\gamma \in Z_q^m$ of $\boldsymbol{w}$. However, without the trapdoor basis T_{cloud} of the cloud server, the curious designated TPA could never produce the valid signature γ. Therefore, given the response auditing proof information $P = \{\nu', \boldsymbol{w}, \boldsymbol{e}, \xi\}$, with the random masking technique, the curious designated TPA could not directly obtain any linear combination of elements in medical data blocks, or cannot further recover any medical data blocks in the file $F = \{m_1, m_2, \cdots, m_l\}$ by solving linear equations. Thus the privacy-preserving could be guaranteed in cloud-assisted WBANs.

D. PERFORMANCE EVALUATION

Now we conduct a comprehensive performance evaluation of LDVAS compared with existing PPPA in [12], CLPA in [15] and CIPPPA in [43] which have been deployed in cloud-assisted WBANs. Due to the large increase in massive electronic medical data, a cloud sever needs to process these massive data with a high efficiency, we will evaluate the computational costs of the cloud server in LDVAS compared with existing schemes to demonstrate the feasibility of LDVAS.

Specifically, as the key factors that affect the performance of checking the medical data integrity in cloud-assisted WBANs, are actually the communication costs and auditing time, we will demonstrate LDVAS has such performance advantages on the side of the designated auditor in the following comparison.

In the performance evaluation, all the implementations are conducted on a laptop with windows 10 operating system with an Intel Core-i5 CPU and and 8GB DDR3 of RAM. All algorithms are done in the C language and our code uses the MIRACL library version 5.6.1. The elliptic curve is MNT curve, its base field size is 159 bits and its embedding degree is 6. To achieve the security of the hardness of lattice-based assumptions, the parameters m, n, q need to satisfy $m \geq \lceil 2n \log q \rceil$. More specifically, we give an instance of LDVAS, and compare it with existing schemes. We set the security level of the system to be 512 bits, and set $n = 10$, $m = 100$. All the results of implementations are representing 30 trials on average.

First, we conduct the computational costs of generating the response auditing proof on the side of a cloud server. For the computational costs, we denote $Mult$, $mult$, $Pair$, Exp, Add by the running time of an elliptic-curve point multiplication operation, a general multiplication operation, a bilinear pairing operation, a modular exponentiation operation, and an elliptic-curve point addition operation, respectively. We also denote Ha, ha by the running time of a hash-to-point/hash-to-vector operation, and a general hash function operation. In LDVAS, to blind the aggregation message ν, a cloud server selects a random vector $\boldsymbol{w} \leftarrow Z_q^n$, and runs $\mathbf{SamplePre}(\boldsymbol{B}, T_{cloud}, \boldsymbol{w}, \sigma)$ to generate the signature $\gamma \in Z_q^m$ with the private key T_{cloud}. Actually, in this process, γ could be generated by the cloud server without any interacting with the designated verifier, thus γ could be pre-computed by the cloud server. As a result, the actual computational costs of generating the auditing proof on the cloud server side are $(2cm+m+mn) \cdot mult + Ha + ha$. The detailed computational costs on the cloud server side are listed in Table 1. Additional, through the comparison of the computational costs of generating the auditing proof, Fig. 3 gives a more intuitive comparison, with the increase of the number of the challenge data blocks, LDVAS has much less computational costs than existing schemes. Consequently, it is practical for the cloud server in LDVAS with a higher efficiency to process the massive electronic medical data simultaneously.

TABLE 1. Computational costs on the cloud server side.

Scheme	Computational Costs
PPPA	$c \cdot Exp + c \cdot mult$
CLPA	$c \cdot Mult + c \cdot mult$
CIPPPA	$(c+1) \cdot Mult + (c+3) \cdot mult + Ha + ha$
LDVAS	$(2cm + m + mn) \cdot mult + Ha + ha$

Then, we evaluate the auditing time on the side of the designated verifier in LDVAS, compared with existing schemes.

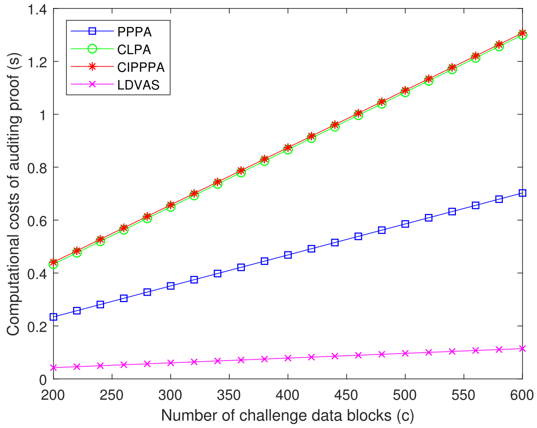


FIGURE 3. The comparison on the cloud server side.

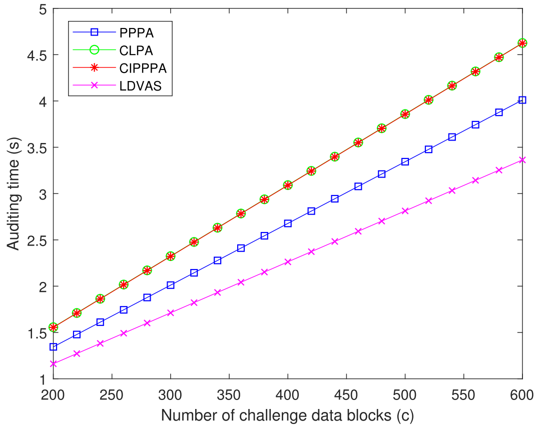


FIGURE 4. The comparison of auditing time.

In detail, according to PPPA, the computational costs of verifying the response auditing proof is $Mult + (c+3) \cdot Exp + 2Pair + c \cdot Ha + ha$. As discussed in [12], since the extra computational costs caused by the random masking is constant: $Mult + 2Exp + ha$, which has nothing to do with the number of sampled data blocks. Also, since bilinear pairing operations are relatively expensive, the extra constant computational costs could be negligible against the overall computational costs of the response auditing proof validation. Therefore, here we set the main auditing time of the auditor to be $c \cdot mult + (c+1) \cdot Exp + 2Pair + c \cdot Ha$ in our implementations. Using the same analytical method, according to CLPA, we could get the computational costs of verifying the response proof is $2Pair + (c+3) \cdot Mult + (c+2) \cdot Add + (c+1) \cdot Ha + 2ha$. According to CIPPPA, the computational costs of verifying the response proof is $3Pair + (c+2) \cdot Mult + (c-1) \cdot Add + c \cdot Ha + ha$. While in the proposed LDVAS, the computational costs of verifying the response proof is $(n+c+1) \cdot Ha + ha + (c+cn+2n+mn) \cdot mult$. As shown in Fig. 4, LDVAS is much more profitable for the designated verifier in auditing time. This is mainly because that our designated verifier auditing scheme is based on lattice, which only needs addition and multiplication operations over

TABLE 2. Communication costs in an auditing task.

Scheme	Challenge message	Auditing proof
PPPA	$c \cdot (\lvert\ell\rvert + \lvert p\rvert)$	$\lvert F\rvert + \lvert G_1\rvert + \lvert G_2\rvert$
CLPA	$c \cdot (\lvert\ell\rvert + \lvert p\rvert)$	$\lvert F\rvert + \lvert G_1\rvert$
CIPPPA	$c \cdot (\lvert\ell\rvert + \lvert p\rvert)$	$\lvert F\rvert + 2\lvert G_1\rvert + \lvert p\rvert$
LDVAS	$c \cdot (\lvert\ell\rvert + 1)$	$\lvert F\rvert + (n + 2m) \cdot \lvert q\rvert$

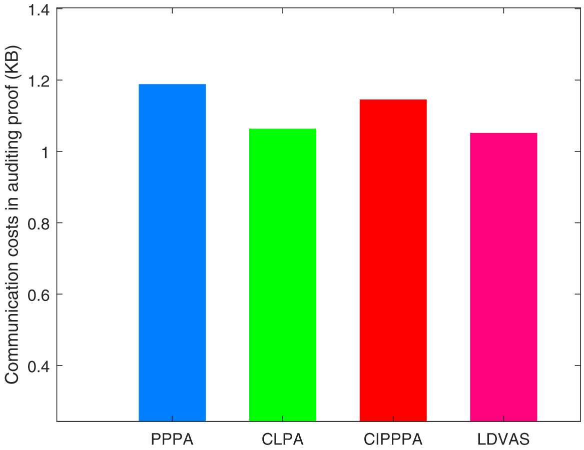


FIGURE 5. Communication costs comparison of auditing proof.

a moderate modulus. The designated verifier could succeed in checking the medical data integrity by computing the limited linearly equations. Furthermore, our scheme enables a patient to designate a specify verifier to fulfil the auditing task, thus guarantees medical data privacy of the patient to some extent.

Finally, we conduct a performance evaluation of the auditing task, which consists of the communication costs and auditing time. For the communication costs, we denote $|\ell|$ by the size of the the number of data blocks, we denote $|q|$, $|p|$ by the bit length of an element in Z_q, Z_p, respectively. In addition, we denote $|F|$ by the bit length of a medical data file, denote $|G_1|$ by the bit length of an element in a cyclic group G_1, and denote $|G_2|$ by the bit length of an element in a bilinear pairing, where $G_1 \times G_1 \rightarrow G_2$. The detailed communication costs between an auditor and a cloud server are listed in Table 2, which include the challenge message and auditing proof. Obviously, we could observe that the communication costs of challenge message in LDVAS are less than other schemes. More specifically, as shown in Fig. 5, the communication costs of auditing proof in LDVAS are also less than existing schemes. Accordingly, compared with existing schemes, the designated verifier of LDVAS has more advantages in communication costs during the auditing task.

Therefore, through the comprehensive performance evaluation of LDVAS compared with existing schemes, we conclude that LDVAS achieves better performance, especially on the side of the designated verifier, which could be more practical for checking the integrity of electronic medical data in post-quantum secure cloud-assisted WBANs.

VI. CONCLUSION

In this paper, we have proposed a lattice-based designated verifier auditing scheme (LDVAS) for electronic medical data in cloud-assisted WBANs, which is secure against quantum-computing attacks. The proposed LDVAS could guarantee that no one excepts a unique designated verifier succeeds in checking the integrity of the outsourced medical data stored in a cloud server associated with WBANs. Based on the hardness of the ISIS assumption, we have proved that a malicious cloud server could not cheat the designated verifier or pass the verification process through generating a forged response proof information. LDVAS could also guarantee the robustness property due to the hardness of LWE assumption. Utilizing the preimage sampleable function to realize the construction of a random masking, LDVAS could prevent the designated verifier from recovering the primitive medical data blocks by solving linear equations. The comprehensive performance evaluation demonstrates that LDVAS has higher performance than existing schemes. More attractively, the designated verifier could fulfil the auditing tasks on behalf on patients with higher computation efficiency. Therefore, LDVAS is quite suitable for the high performance requirements of massive medical data processing even in the post-quantum communication settings. For the future work, we will investigate how to utilize novel lattice-based cryptographic technologies to enhance designated verifier integrity verification for cloud-assisted WBANs in terms of security, performance, and functionality.

REFERENCES

[1] B. Latré, B. Braem, I. Moerman, C. Blondia, and P. Demeester, "A survey on wireless body area networks," *Wireless Netw.*, vol. 17, no. 1, pp. 1–18, Jan. 2011.

[2] R. Cavallari, F. Martelli, R. Rosini, C. Buratti, and R. Verdone, "A survey on wireless body area networks: Technologies and design challenges," *IEEE Commun. Surveys Tuts.*, vol. 16, no. 3, pp. 1635–1657, 3rd Quart., 2014.

[3] B. Singh, S. Dhawan, A. Arora, and A. Patail, "A view of cloud computing," *Commun. ACM*, vol. 53, no. 4, pp. 50–58, 2010.

[4] J. Wan, C. Zou, S. Ullah, C.-F. Lai, M. Zhou, and X. Wang, "Cloud-enabled wireless body area networks for pervasive healthcare," *IEEE Netw.*, vol. 27, no. 5, pp. 56–61, Sep. 2013.

[5] S. Ullah, A. Vasilakos, H.-C. Chao, and J. Suzuki, "Cloud-assisted wireless body area networks," *Inf. Sci.*, vol. 284, pp. 81–83, Nov. 2014.

[6] Y. Zhang, C. Xu, H. Li, K. Yang, J. Zhou, and X. Lin, "HealthDep: An efficient and secure deduplication scheme for cloud-assisted eHealth systems," *IEEE Trans Ind. Informat.*, vol. 14, no. 9, pp. 4101–4112, Sep. 2018.

[7] Y. Zhang, C. Xu, X. Lin, and X. S. Shen, "Blockchain-based public integrity verification for cloud storage against procrastinating auditors," *IEEE Trans. Cloud Comput.*, to be published, doi: 10.1109/TCC.2019.2908400.

[8] Y. Ren, Y. Leng, F. Zhu, J. Wang, and H.-J. Kim, "Data storage mechanism based on blockchain with privacy protection in wireless body area network," *Sensors*, vol. 19, no. 10, p. 2395, May 2019, doi: 10.3390/s19102395.

[9] D. Zissis and D. Lekkas, "Addressing cloud computing security issues," *Future Gener. Comput. Syst.*, vol. 28, no. 3, pp. 583–592, Mar. 2012.

[10] M. Li, W. Lou, and K. Ren, "Data security and privacy in wireless body area networks," *IEEE Wireless Commun.*, vol. 17, no. 1, pp. 51–58, Feb. 2010.

[11] J. Sun, Y. Fang, and X. Zhu, "Privacy and emergency response in e-healthcare leveraging wireless body sensor networks," *IEEE Wireless Commun.*, vol. 17, no. 1, pp. 66–73, Feb. 2010.

[12] C. Wang, S. S. M. Chow, Q. Wang, K. Ren, and W. Lou, "Privacy-preserving public auditing for secure cloud storage," *IEEE Trans. Comput.*, vol. 62, no. 2, pp. 362–375, Feb. 2013.

[13] Y. Wang, Q. Wu, B. Qin, W. Shi, R. H. Deng, and J. Hu, "Identity-based data outsourcing with comprehensive auditing in clouds," *IEEE Trans. Inf. Forensics Security*, vol. 12, no. 4, pp. 940–952, Apr. 2017.

[14] Y. Yu, M. H. Au, G. Ateniese, X. Huang, W. Susilo, Y. Dai, and G. Min, "Identity-based remote data integrity checking with perfect data privacy preserving for cloud storage," *IEEE Trans. Inf. Forensics Security*, vol. 12, no. 4, pp. 767–778, Apr. 2017.

[15] D. He, S. Zeadally, and L. Wu, "Certificateless public auditing scheme for cloud-assisted wireless body area networks," *IEEE Syst. J.*, vol. 12, no. 1, pp. 64–73, Mar. 2018.

[16] H. Yan, J. Li, J. Han, and Y. Zhang, "A novel efficient remote data possession checking protocol in cloud storage," *IEEE Trans. Inf. Forensics Security*, vol. 12, no. 1, pp. 78–88, Jan. 2017.

[17] J. Li, H. Yan, and Y. Zhang, "Efficient identity-based provable multi-copy data possession in multi-cloud storage," *IEEE Trans. Cloud Comput.*, to be published, doi: 10.1109/TCC.2019.2929045.

[18] P. W. Shor, "Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer," *SIAM J. Comput.*, vol. 26, no. 5, pp. 1484–1509, Oct. 1997.

[19] Bloomberg. (2017). *IBM Makes Breakthrough in Race to Commercialize Quantum Computers*. [Online]. Available: https://m.cacm.acm.org/

[20] D. Micciancio and O. Regev, "Lattice-based cryptography," in *Advances in Cryptology—CRYPTO*. Springer, 2006, pp. 131–141.

[21] R. Steinfeld, L. Bull, H. Wang, and J. Pieprzyk, "Universal designated-verifier signatures," in *Advances in Cryptology—ASIACRYPT*. Springer, 2003, pp. 523–542.

[22] W. Susilo, F. Zhang, and Y. Mu, "Identity-based strong designated verifier signature schemes," in *Proc. Australas. Conf. Inf. Secur. Privacy*. Springer, 2004, pp. 313–324.

[23] A. Shamir, "Identity-based cryptosystems and signature schemes," in *Proc. Workshop Theory Appl. Cryptograph. Techn.* Springer, 1984, pp. 47–53.

[24] O. Regev, "On lattices, learning with errors, random linear codes, and cryptography," in *Proc. 37th Annu. ACM Symp. Theory Comput. (STOC)*, 2005, pp. 84–93.

[25] C. Gentry, C. Peikert, and V. Vaikuntanathan, "Trapdoors for hard lattices and new cryptographic constructions," in *Proc. 14th Annu. ACM Symp. Theory Comput. (STOC)*, 2008, pp. 197–206.

[26] H. Qian, J. Li, Y. Zhang, and J. Han, "Privacy-preserving personal health record using multi-authority attribute-based encryption with revocation," *Int. J. Inf. Secur.*, vol. 14, no. 6, pp. 487–497, Nov. 2015.

[27] Y. Ren, Y. Liu, S. Ji, A. K. Sangaiah, and J. Wang, "Incentive mechanism of data storage based on blockchain for wireless sensor networks," *Mobile Inf. Syst.*, vol. 2018, pp. 1–10, Aug. 2018, doi: 10.1155/2018/6874158.

[28] Z. Fu, L. Xia, X. Sun, A. X. Liu, and G. Xie, "Semantic-aware searching over encrypted data for cloud computing," *IEEE Trans. Inf. Forensics Security*, vol. 13, no. 9, pp. 2359–2371, Sep. 2018.

[29] J. Li, H. Yan, and Y. Zhang, "Certificateless public integrity checking of group shared data on cloud storage," *IEEE Trans. Services Comput.*, to be published, doi: 10.1109/TSC.2018.2789893.

[30] X. Fu, X. Nie, T. Wu, and F. Li, "Large universe attribute based access control with efficient decryption in cloud storage system," *J. Syst. Softw.*, vol. 135, pp. 157–164, Jan. 2018.

[31] Y. Zhang, C. Xu, N. Cheng, H. Li, H. Yang, and X. S. Shen, "Chronos+: An accurate blockchain-based time-stamping scheme for cloud storage," *IEEE Trans. Services Comput.*, to be published, doi: 10.1109/TSC.2019.2947476.

[32] Y. Zhang, C. Xu, H. Li, K. Yang, N. Cheng, and X. S. Shen, "PROTECT: Efficient password-based threshold Single-sign-on authentication for mobile users against perpetual leakage," *IEEE Trans. Mobile Comput.*, to be published, doi: 10.1109/TMC.2020.2975792.

[33] G. Ateniese, R. Burns, R. Curtmola, J. Herring, L. Kissner, Z. Peterson, and D. Song, "Provable data possession at untrusted stores," in *Proc. 14th ACM Conf. Comput. Commun. Secur. (CCS)*, 2007, pp. 598–609.

[34] A. Juels and B. Kaliski, "PORs: Proofs of retrievability for large files," in *Proc. ACM Conf. Comput. Commun. Secur. (CCS)*, 2007, pp. 584–597.

[35] H. Shacham and B. Waters, "Compact proofs of retrievability," in *Proc. Int. Conf. Theory Appl. Cryptol. Inf. Secur.* Springer, 2008, pp. 90–107.

[36] Y. Zhang, C. Xu, X. Liang, H. Li, Y. Mu, and X. Zhang, "Efficient public verification of data integrity for cloud storage systems from indistinguishability obfuscation," *IEEE Trans. Inf. Forensics Security*, vol. 12, no. 3, pp. 676–688, Mar. 2017.

[37] S. G. Worku, C. Xu, and J. Zhao, "Cloud data auditing with designated verifier," *Frontiers Comput. Sci.*, vol. 8, no. 3, pp. 503–512, Jun. 2014.

[38] H. Yan, J. Li, and Y. Zhang, "Remote data checking with a designated verifier in cloud storage," *IEEE Syst. J.*, to be published, doi: 10.1109/JSYST.2019.2918022.

[39] J. Yu and H. Wang, "Strong key-exposure resilient auditing for secure cloud storage," *IEEE Trans. Inf. Forensics Security*, vol. 12, no. 8, pp. 1931–1940, Aug. 2017.

[40] H. Wang, D. He, and S. Tang, "Identity-based proxy-oriented data uploading and remote data integrity checking in public cloud," *IEEE Trans. Inf. Forensics Security*, vol. 11, no. 6, pp. 1165–1176, Jun. 2016.

[41] Y. Li, Y. Yu, G. Min, W. Susilo, J. Ni, and K.-K.-R. Choo, "Fuzzy identity-based data integrity auditing for reliable cloud storage systems," *IEEE Trans. Dependable Secure Comput.*, vol. 16, no. 1, pp. 72–83, Jan. 2019.

[42] Y. Ren, J. Shen, Y. Zheng, J. Wang, and H.-C. Chao, "Efficient data integrity auditing for storage security in mobile health cloud," *Peer-to-Peer Netw. Appl.*, vol. 9, no. 5, pp. 854–863, Sep. 2016.

[43] X. Zhang, J. Zhao, C. Xu, H. Li, H. Wang, and Y. Zhang, "CIPPPA: Conditional identity privacy-preserving public auditing for cloud-based WBANs against malicious auditors," *IEEE Trans. Cloud Comput.*, to be published, doi: 10.1109/TCC.2019.2927219.

[44] C. Gentry, A. Sahai, and B. Waters, "Homomorphic encryption from learning with errors: Conceptually-simpler, asymptotically-faster, attribute-based," in *Proc. Annu. Cryptol. Conf.* Springer, 2013, pp. 75–92.

[45] Z. Brakerski and R. Perlman, "Lattice-based fully dynamic multi-key FHE with short ciphertexts," in *Proc. Annu. Int. Cryptol. Conf.* Springer, 2016, pp. 190–213.

[46] X. Boyen and Q. Li, "Towards tightly secure lattice short signature and id-based encryption," in *Proc. Int. Conf. Theory Appl. Cryptol. Inf. Secur.* Springer, 2016, pp. 404–434.

[47] B. Libert, S. Ling, F. Mouhartem, K. Nguyen, and H. Wang, "Signature schemes with efficient protocols and dynamic group signatures from lattice assumptions," in *Proc. Int. Conf. Theory Appl. Cryptol. Inf. Secur.* Springer, 2016, pp. 373–403.

[48] D. Boneh and D. M. Freeman, "Linearly homomorphic signatures over binary fields and new tools for lattice-based signatures," in *Proc. Int. Workshop Public Key Cryptogr.* Springer, 2011, pp. 1–16.

[49] F. Wang, Y. Hu, and B. Wang, "Lattice-based linearly homomorphic signature scheme over binary field," *Sci. China Inf. Sci.*, vol. 56, no. 11, pp. 1–9, Nov. 2013.

[50] S. Gorbunov, V. Vaikuntanathan, and D. Wichs, "Leveled fully homomorphic signatures from standard lattices," in *Proc. 47th Annu. ACM Symp. Theory Comput. (STOC)*, 2015, pp. 469–477.

[51] R. Gennaro and D. Wichs, "Fully homomorphic message authenticators," in *Proc. Int. Conf. Theory Appl. Cryptol. Inf. Secur.* Springer, 2013, pp. 301–320.

[52] D. Fiore, A. Mitrokotsa, L. Nizzardo, and E. Pagnin, "Multi-key homomorphic authenticators," in *Proc. Int. Conf. Theory Appl. Cryptol. Inf. Secur.* Springer, 2016, pp. 499–530.

[53] X. Zhang, H. Wang, and C. Xu, "Identity-based key-exposure resilient cloud storage public auditing scheme from lattices," *Inf. Sci.*, vol. 472, pp. 223–234, Jan. 2019.

[54] X. Zhang, J. Zhao, C. Xu, H. Wang, and Y. Zhang, "DOPIV: Post-quantum secure identity-based data outsourcing with public integrity verification in cloud storage," *IEEE Trans. Services Comput.*, to be published, doi: 10.1109/TSC.2019.2942297.

[55] M. Ajtai, "Generating hard instances of the short basis problem," in *Proc. Int. Colloq. Automata, Lang., Program.* Springer, 1999, pp. 1–9.

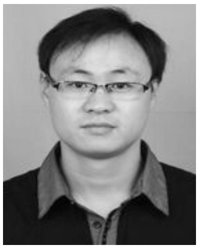
[56] S. D. Gordon, J. Katz, and V. Vaikuntanathan, "A group signature scheme from lattice assumptions," in *Proc. Int. Conf. Theory Appl. Cryptol. Inf. Secur.* Springer, 2010, pp. 395–412.

[57] J. Alwen and C. Peikert, "Generating shorter bases for hard random lattices," *Theory Comput. Syst.*, vol. 48, no. 3, pp. 535–553, 2011.

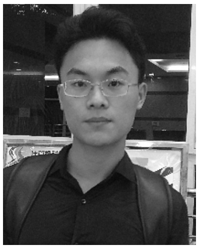
[58] S. Agrawal, D. Boneh, and X. Boyen, "Lattice basis delegation in fixed dimension and shorter-ciphertext hierarchical IBE," in *Proc. Annu. Cryptol. Conf.* Springer, 2010, pp. 98–115.

[59] D. Micciancio and S. Goldwasser, *Complexity of Lattice Problems: A Cryptographic Perspective*, vol. 671. Springer, 2012.

[60] D. Cash, D. Hofheinz, E. Kiltz, and C. Peikert, "Bonsai trees, or how to delegate a lattice basis," in *Proc. Annu. Int. Conf. Theory Appl. Cryptograph. Techn.* Springer, 2010, pp. 523–552.



XIAOJUN ZHANG received the B.Sc. degree in mathematics and applied mathematics from Hebei Normal University, Shijiazhuang, China, in 2009, the M.Sc. degree in pure mathematics from Guangxi University, Nanning, China, in 2012, and the Ph.D. degree in information security from the University of Electronic Science and Technology of China (UESTC), Chengdu, China, in 2015. He was a Research Scholar with the School of Physical and Mathematical Sciences, Nanyang Technological University, Singapore, from 2018 to 2019. He has worked as a Postdoctoral Fellow with UESTC, from 2016 to 2019. He is currently an Associate Professor with the School of Computer Science, Southwest Petroleum University, Chengdu. His research interests include applied cryptography, network security, cloud computing security, and the security and privacy for smart grids.



CHAO HUANG received the B.E. degree in engineering of electronics and information from Southwest Petroleum University, in 2018, where he is currently pursuing the M.S. degree in computer science and technology with the School of Computer Science. His current research interests include cryptography, network security, cloud computing security, and big data security.

YUAN ZHANG (Member, IEEE) received the B.Sc. and Ph.D. degrees from the University of Electronic Science and Technology of China (UESTC), in 2013 and 2019, respectively. He was a Visiting Ph.D. Student with the BBCR Laboratory, Department of ECE, University of Waterloo, Canada, from 2017 to 2019. He is currently an Associate Professor with the School of Computer Science and Engineering, UESTC. His research interests include applied cryptography, data security, and blockchain technology.

JINGWEI ZHANG received the B.E. degree in computer network engineering from Southwest Petroleum University, Chengdu, China, in 2019, where he is currently pursuing the M.S. degree in computer science and technology with the School of Computer Science. His current research interests include cryptography, cloud computing security, and big data security.

JIE GONG received the M.Sc. degree in information security from the University of Electronic Science and Technology of China (UESTC), Chengdu, China, in 1997. He is currently an Associate Professor with the School of Computer Science, Southwest Petroleum University, Chengdu. His research interests include network security, advance computer network technology, and physical information system security.