Lattice based Ring Signature Scheme for Secure Cloud-based EMR Sharing

Wenxin Hu*, Yidan Chai*†, Xue Chen† , Chao Zheng
North China University of Technology, Beijing, China.
chaicyd@sina.com; chenxuemail0510@163.com

2022 7th International Conference on Computer and Communication Systems (ICCCS) | 978-1-6654-5060-7/22/$31.00 ©2022 IEEE | DOI: 10.1109/ICCCS55155.2022.9845850

***Abstract*—Advances in medical science and technology continue to drive the development of e-healthcare, with Electronic Medical Records (EMRs) consisting of medical information such as patient consultation records and bodily data being gradually popularized in the form of cloud sharing. The sharing of EMR effectively enhances the effectiveness and reliability of healthcare services. However, the highly sensitive EMRs are susceptible to tampering and misuse during the EMR sharing, which poses a tremendous threat to patients' privacy and the security of e-health. Further, EMRs are extremely vulnerable to quantum computing attacks during the process of sharing in cloud, which will be the most significant bottleneck in the advancement of e-healthcare systems. To tackle the foregoing issues, we present a lattice-based ring signature scheme for secure EMR sharing on the cloud. To begin with, we implement EMR sharing with medical cloud. Then, we set a lattice-based ring signature scheme to ensure user anonymity, EMR and signature unforgeability, while resisting quantum attacks. Further, we require all EMR-related users to perform multiparty confirmation signatures on the EMR. In conlusion, the security analysis and performance evaluation indicate that our scheme guarantees correctness, anonymity, and unforgeability, while outperforming other existing schemes.**

***Index Terms*—Lattice, Cryptography, Security, EMR, e-Health.**

I. Introduction

As electronic medical technologies are continuously advancing, EMRs are becoming increasingly prevalent in healthcare systems due to their facilitation. In the field of e-healthcare, the EMR is an efficient and convenient way to record patient medical data and realize information sharing, creating a new way for people to access medical information. To better utilize the value of EMRs, they are required to be saved in the big data storage of medical clouds [1]. However, in the process of sharing EMRs in the cloud, their security and privacy face huge challenges, which greatly hinder the development and popularity of e-healthcare.

The issue of user privacy and data security [14],[16],[19],[20] is increasingly being taken seriously. To protect the security of EMRs, some scholars choose to utilize the classical digital signatures [15],[17]. Among them, [15] chooses attribute-based signatures in healthcare to assure the data security in e-health. In addition, some scholars propose using the technology of blockchain to control the access and management of EMRs, such as [9],[10],[11]. While these schemes provide a certain degree of information security for EMRs, nonetheless they disregard the privacy and security challenges posed by quantum attacks as well as multi-party signing and access to EMRs.

With the advent of quantum computing, quantum simulation [33-36] and quantum communication [30-32], more and more quantum computers and algorithms have emerged, posing a serious threat to classical cryptography. The existing EMR privacy protection systems are no longer able to counter quantum attacks, and thus existing the risk of privacy and information leakage. Threatened by the Shor algorithm [22], which has the ability to compute polynomial-time mathematical decompositions as well as discrete logarithmic decompositions. Many attackers use the Grover algorithm [12] to extract the user's keys to complete transactions in informal ways. To address these problems, lattice-based cryptography [13],[18] has been proposed, which is not only resistant to quantum computing attacks but also more efficient and less expendable than other post-quantum cryptography [23].

Furthermore, classical digital signatures are unable to resist quantum attacks, but strongly protect and verify the authenticity of data, thus preventing forgery and tampering attacks. Ring signatures [21] with a high degree of anonymity no longer have an administrator role, where a group of signatories are allowed to sign messages without revealing the anonymity. In healthcare, ring signature combines decentralization and soundness, which can remove the security risks due to multiple party signatures and efficiently guarantee the privacy of EMR.

Therefore, to address all the above challenges, we propose a lattice-based ring signature scheme for secure cloud-based EMR sharing. Our scheme assures secure EMR sharing, anonymity of users as well as the unforgeability of signatures and EMRs. More critically, our scheme is able to resist external attacks and quantum computing attacks, thus guaranteeing the security of patient EMRs and information from being compromised. Security and experimental evaluation analysis demonstrate that our paper guarantees relevant properties and outperforms other schemes in computational cost.

The major contributions of our paper include:

(1) In our paper, we construct an EMR sharing scheme that combines medical cloud storage and signature technology to maximize the value of EMR.

(2)We devise a ring signature scheme that enables resistance to quantum attacks, while guaranteeing user anonymity, signature and EMR unforgeability.

(3) Our scheme is fully capable of ensuring the security

*Wenxin Hu and Yidan Chai have the same contribution to this work in no particular order.

†Yidan Chai and Xue Chen are the corresponding authors.

of EMRs when signed by multiple parties, thus ensuring the security of information and data during storage and sharing.

(4) Security analysis and performance evaluation indicate that our paper assures anonymity and unforgeability, being resistant to quantum attacks and outperforming other schemes.

The rest of our paper is structured as follows: The preliminary knowledge is introduced in Section II. The challenges and our goals are given in Section III. Section IV elaborates our proposed scheme. Section V and Section VI provide the security analysis and performance evaluation, respectively. Then, we complete the related-paper review in Section VII. Finally, the conclusion is in Section VIII.

II. Preliminaries

Definition 1. Lattice [24]

The n vectors a_1,a_2,$\cdots$,a_n $\in \mathbb{R}^m$, which are linearly independent, form the basis of the lattice L:

$$L(a_1, a_2, \cdots, a_n) = \{\Sigma x_i \cdot a_i | x_i \in \mathbb{Z}\} \tag{1}$$

where the n is rank and the dimension of the lattice L is defined by m with $m \geq n$. A is an $m \times n$ matrix consisting of a set of bases a_1,a_2,$\cdots$,a_n of lattice L. The lattice L is as:

$$L(A) = L(a_1, a_2, \cdots, a_n) = \{\Sigma A \cdot x | x_i \in \mathbb{Z}^m\}. \tag{2}$$

Definition 2. Statistical Distance

Let finite set Ω have 2 random variables X and Y on it. Moreover, the statistical distance $\Delta(X, Y)$ among that is:

$$\Delta(X, Y) = \frac{1}{2}\Sigma_{s\in\Omega}|Pr[X = s] - Pr[Y = s]|. \tag{3}$$

Definition 3. Small Integer Solution(SIS) Problem

The Shortest Vector Problem (SVP), the most famous of the hard problems in the lattice, has the goal of searching for the shortest vector $v \in L \setminus \{0\}$. Combining SVP with an integer lattice is the Small Integer Solution problem (SIS), as follows.

The matrix $A \in \mathbb{Z}_q^{m\times n}$ with the real number α, search the vector $t \in \mathbb{Z}^m, t \neq 0, \|t\| \leq \alpha$ to reach the formula $A \cdot t = 0\ mod\ q$.

Theorem 1: Let $m = poly(n)$, $\alpha > 0$, and the modulus $q \geq \alpha \cdot poly(n)$ is large enough, SIS is the worst case and similar to the SVP.

Definition 4. TrapGen Algorithm [25]

Given the modulus $q = poly(n)$, the positive integer m, we have $q \geq 2, m \geq 5n\ log\ q$. The output of $TrapGen(1^n)$ is that the matrix $B \in Z_q^{n\times m}$ and the matrix$A_B \in Z_{n\times m}$. The matrix A_B is the good basis of $L^{\perp}(A) = \{x \in \mathbb{Z}^m : Ax = 0\ mod\ q\}$, such that $\|\tilde{A_B}\| \leq O(\sqrt{n\ log\ q})$.

Definition 5. SamplePre Algorithm [25]

Input the vector $s \in \mathbb{Z}_q^n$ and σ, the matrix $B \in Z_q^{n\times m}$, $A_B \in Z^{n\times m}$ in the Samplepre algorithm. Then, output ϵ is within negligible statistical distance of $D_{L_s^{\perp}(B),\sigma}$ as well as $\epsilon \in \{\epsilon \in Z^m : \|\epsilon\| \leq \sigma\sqrt{m}\}$ like $B\epsilon = s(mod\ q)$ with the overwhelming probability.

Definition 6. Discrete Gaussian Distribution

Let $\rho_{v,\sigma}(\mathbb{Z}^m)$ define as the discrete integral of $\rho_{v,\sigma}$, thus $D_{v,\sigma}^m(x) = \frac{\rho_{v,\sigma}^m(x)}{\rho_{\sigma}^m(\mathbb{Z}^m)}$.

Lemma 1 [27]: For $j \geq 1$, we have $Pr[\| z \| > j\sigma\sqrt{m} : z \leftarrow D_{\sigma}^m] < j^m exp(\frac{m}{2}(1 - k^2))$. Further, for $z \leftarrow D_{\sigma}^m$, $v \in \mathbb{R}^m$, we get

$$Pr[| \langle z, v\rangle | > r] \leq exp(-\frac{r^2}{2 \| v \|^2\ \sigma^2}) \cdot 2. \tag{4}$$

Lemma 2 [27]: For $v \in \mathbb{Z}^m$, if $\sigma = \delta\|v\|$, then

$$Pr[\frac{D_{\sigma}^m(z)}{D_{v,\sigma}^m(z)} < exp(\frac{12}{\delta} + \frac{1}{2\delta^2}) : z \leftarrow D_{\sigma}^m] = 1 - 2^{-100}. \tag{5}$$

III. Threat Models and Design Goals

A. Threat Models

1) EMR Tampering Attacks: Malicious users illegally tamper with information in the patient's EMR or fabricate false data in the EMR, leading to misdiagnosis or treatment errors by physicians.

2) User Privacy Breach Attacks: The malicious user spies on the true identity of the signatory or speculates on his/her behavior, leading to user privacy leakage.

3) Signature Forgery Attacks: A malicious user may threaten the security and reliability of the EMR by forging the required signatures.

4) Quantum Computing Attacks: EMR and traditional cryptographic signatures are hardly resistant to future quantum computing attacks, leading to privacy and security issues.

B. Design Goals

1) Authenticity of EMRs: The integrity and unforgeability of the EMR is critical in healthcare, hence we have to ensure the authenticity of the EMR.

2) Anonymity of Users: During the sharing process of EMR, the anonymity of users must be guaranteed to prevent the issue of privacy leakage of users.

3) Multi-party Confirmation: The EMR requires the signature of each relevant entity to ensure the authenticity, security, and traceability of the EMR.

4) Unforgeability of Signatures: Signing the EMR is a vital measure to guarantee the secure sharing of the EMR, thus it is crucial to ensure that the signature is unforgeability.

5) Resisting Quantum Computing Attacks: Our scheme demands the ability to resist quantum computing attacks in order to achieve superior level of EMR shared security.

IV. Our Proposed Scheme

A. Overall

For secure EMR sharing, we set a lattice-based ring signature scheme for multiparty signatures [18]. As shown in Fig. 1, the EMR is generated during the treatment of a patient by a doctor. Subsequently, we require the patient and the doctor to sign and confirm the EMR and then transmit it to the hospital, which signs and uploads it to the medical cloud to ensure the authenticity and unforgeability of the EMR, thus enabling secure EMR sharing. Our design goals are guaranteed by the nature of our signature scheme.

The specific ring signature scheme that can resist quantum attacks will be introduced in four parts: Setup, Key Extraction, Signature Generation, Signature Verification.

B. Setup

We performed setup of the lattice-based ring signature scheme, as Algorithm 1, and obtained the public parameters.

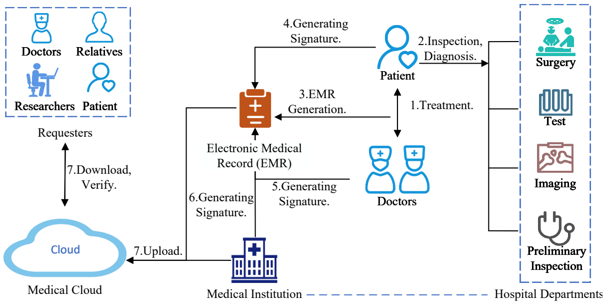

Fig. 1. System Model.

Algorithm 1 $Setup(q, n, m, H))$

Output: Prime number q, Positive integer m, n, Hash function $H : \{0, 1\}^*$

```
Set $q \geq 3$, which $q$ is the prime number.
Set positive integers $n \geq 64$ and $m \geq 5n\ log\ q$
Set positive integers $a$ and $b$.
$H : \{0, 1\}^* \leftarrow \{v \in \{-1, 0, 1\}^a, \|v\|_1 \leq b\}$.
```

C. Key Extraction

We set the ring as R, containing l members, and for all EMR related users $i \in [l]$, we execute Algorithm 2 to obtain the public and secret keys. The matrix Z_i is randomly chosen in the $Z_q^{n\times a}$ and the matrix A_i is computed by $TrapGen(1^n)$. Then, the algorithm $SamplePre$ runs a times with the positive integer d. In our Key-Extraction process, $A_iS_i = Z_i$, which $S_i \in \{-d, \cdots, 0, \cdots, d\}^{m\times a}$

Algorithm 2 $Key - Extraction(1^n, R, l)$

Input: Security parameter n, Ring R, Ring members l
Output: Secret key sk_i, Public key pk_i

```
Set the public polynomial $p_i \in Z_q^{n\times m}$.
for $i \in [l]$ in $R$ do
    $s_i, e_i \leftarrow Z_q^{n\times m}$
    Execute $TrapGen(1^n)$
    $z_i \leftarrow p_is_i + e_i$ (mod $q$), where $A_iS_i = Z_i$.
    $sk_i \leftarrow (s_i, e_i)$
    $pk_i \leftarrow z_i$
end for
Return $sk_i, pk_i$
```

D. Signature Generation

After the EMR-related users obtain the key pairs, the EMR requires a signature. We set the EMR to message μ_{EMR} and the signer to U_{H_i}.

The concrete signature generation algorithm is shown in Algorithm 3. We have to explain that the y_j is randomly chosen by discrete normal distribution D_σ^m,which σ is the standard deviation.

Algorithm 3 $Signature - Generation(S_{H_i}, R, \mu_{EMR}, l)$

Input: Secret key of the signatory sk_{H_i}, Ring R, Ring members l, Public polynomial p_i, Message μ_{EMR}
Output: Signature $(v_i : i \in [l], h)$

```
for $i \in [l]$ in $R$ do
    Randomly chosen $y_i \leftarrow R_q$
    $t = \{t_0, t_1, \cdots, t_n\}$
    for $i \in \{0, 1, \cdots, n\}$ do
        $t_i \leftarrow p_iy_i + e_i$ (mod $q$)
    end for
    $h' \leftarrow hash(\lfloor t\rceil\|\mu)$
    $h \leftarrow F(h')$
    if $i = H_i$ then
        $v_{H_i} \leftarrow (y_{H_i} + s_{H_i}h)p_{H_i}$
    else
        $v_i \leftarrow p_iy_i + z_ih$
    end if
    $e' \leftarrow D_\sigma^m$
    $w \leftarrow t_i - e'h$(mod $q$)
end for
Return $Sig \leftarrow (v_i : i \in [l], h)$
```

E. Signature Verification

For the verification of the signature on EMR μ_{EMR}, we must to input the EMR μ_{EMR}, and the signature $Sig \leftarrow (v_i : i \in [l], h)$. Through the Algorithm 4, if the signature is valid, we will accept it. Otherwise, we reject it.

Algorithm 4 $Signature - Verification(Sig, R, \mu_{EMR}, l)$

Input: Signature $Sig \leftarrow (v_i : i \in [l], h)$, Ring R, message μ_{EMR}, Ring members l
Output: Accept or Reject

```
for $i \in [l]$ in $R$ do
    $h \leftarrow F(h')$
    $w \leftarrow v_i - z_ih$ (mod $q$)
    $h* \leftarrow hash(\lfloor w\rceil\|\mu_{EMR})$
    if $h' = h*$ then
        Return Accept
    else
        Return Reject
    end if
end for
```

V. Security Analysis

Our security analysis is based on a random oracle model. Our proposed signature scheme applied to EMR ensures the security of its sharing process. Our scheme effectively guarantees the anonymity of the user, the authenticity of the EMR, the unforgeability of the signature, and the resistance to quantum attacks.

A. Correctness

Due to the properties of the trapdoor function [26], our scheme is correctness. In our scheme, the signature $Sig \leftarrow (v_i : i \in [l], h)$ is generated by the EMR-related user U_{H_i}. For $\sigma \in R$, We let $S_{H_i}h$ equal to the random vector v. The distribution of $v_{H_i} = S_{H_i}h + y_{H_i}$ is with statistically distance $\frac{2^{-\omega(logm)}}{M}$ of D_σ^m. Therefore, we have $Pr[|v| > 2\sigma\sqrt{m}; v \leftarrow D_\sigma^m] < 2^{-m}$ for all $v_i(i \in [l])$.

To conclude, the correctness is as follow:

$$\begin{aligned}\sum_{i\in[l]} A_i v_i - Z_i h &= A_{H_i} v_{H_i} - Z_i + \sum_{i\in[l]\setminus\{H_i\}} A_i v_i \\ &= A_{H_i} S_{H_i} h + A_{H_i} y_{H_i} - Z_i h + \sum_{i\in[l]\setminus\{H_i\}} A_i y_i \\ &= \sum_{i\in[l]} A_i y_i \end{aligned} \tag{6}$$

B. Anonymity

Theorem 2 (Anonymity): In our scheme, n is the security parameter. The polynomial-time adversary A wins the anonymous game $Game_{Anony}$ in a negligible probability. Therefore, our scheme guarantees anonymity.

Proof of Theorem 2: Given an adversary A and a challenger C in the anonymous game $Game_{Anony}$.

Setup: The challenger $C \in \mathbb{Z}_q^{n\times k}$ obtains $A_i \in \mathbb{Z}_q^{n\times m}$, $C \in \mathbb{Z}_q^{n\times k}$, and $B_i \in \mathbb{Z}_q^{m\times m}$. B_i is a good basis of lattice $L_q^{\perp}(A_i)$, by l times of running $TrapGen(1^\lambda)$ and matrix Z_i which is chosen uniformly at random from $\mathbb{Z}_q^{n\times k}$. After that, outputs matrix $S_i \in \{-d, \cdots, 0, \cdots, d\}^{m\times k}$ as the algorithm by running k times, thus satisfies $A_i S_i = Z_i$. Challenger C finally gives the public key pk_i for all $i \in [l]$. And also, keeps the secret key sk_i from being revealed.

Signing queries: A makes a signature query with ring $L = \{A_i\}_{i\in[l]}$ and a EMR μ_{EMR} to C. Then, C answers with the result of $Sign(pk, sk, \mu_{EMR})$.

Secret Key queries: Adversary A adaptability queries the secret key of the index $i \in l$, replies with S_i.

Challenge phase: The adversary A asks for the ring signature of message μ'_{EMR} with the index of $i_0, i_1 \in [l]$. Then, C randomly chooses $b \in \{0, 1\}$ and generates the ring signature and outputs the final answer $Sig \leftarrow (v_i : i \in [l], h)$.

Guess phase: A outputs guessed b' of a random bit b which $b \in \{0, 1\}$. There are two cases of $Sig \leftarrow (v_i : i \in [l], h)$. On the one hand, challenge signature is generated by the secret key S_{ib} of the index member i_b. Then, we have $v_{i_b} = S_{i_b}h + y_{i_b}$ with the probability $min(\frac{D_\sigma^m(v_{i_b})}{MD_{S_{i_b},h,\sigma}^m(v_{i_b})}, 1)$ and output the sign $Sig \leftarrow (v_i : i \in [l], h)$. On the other hand, if we utilize another method to obtain v_{i_b} which are chosen uniformly and randomly over D_σ^m with probability of $\frac{1}{M}$ which $M = O(l)$ and output the sign $Sig \leftarrow (v_i : i \in [l], h)$. By Lemma 1 and 2, the $\frac{2^{-\omega(logm)}}{M}$ is the statistical distance of the above algorithms.

Let X_{i_b} represent the signature received by the S_{i_b} and randomly chosen v_{i_b} from D_σ^m with the probability of $\frac{1}{M}$. Other remaining $(v_i : i \in [l] \setminus \{i_b\})$ is chosen from D_σ^m directly. We then set Y to denote the distribution $Sig \leftarrow (v_i : i \in [l], h)$. Applying the rejection sampling, for i_0, i_1, we calculate:

$$\begin{aligned}\Delta(X_{i_0}, X_{i_1}) &\leq \Delta(X_{i_0}, Y) + \Delta(X_{i_1}, Y) \\ &\leq 2 \cdot \frac{2^{-\omega(logm)}}{M} = \frac{2^{-\omega(logm)+1}}{M}.\end{aligned} \tag{7}$$

Thus, signature X_{i_0} is indistinguishable with signature X_{i_1} with overwhelming probability, and it means that almost no malicious adversary has the ability to guess the correct bit b. Consequently, we have to say this ensures the unconditional anonymity of our proposed scheme.

C. Unforgeability

Our lattice based ring signature scheme must achieve unforgeability to ensure a secure EMR sharing process.

Theorem 3: For the $n > 64$ and $m > 5n\ log\ q$, we randomly chosen $s \leftarrow \{-d, \cdots, 0, \cdots, d\}^m$, and there existing an another s' satisfy $As = As'$ with probability $1 - 2^{-100}$.

Proof of Theorem 3: Due to the range of A, there are q^n elements s that unable collide with any other elements in $\{-d, \cdots, 0, \cdots, d\}^m$, consisting of $(2d + 1)^m$ elements. The probability of choosing a element that did not collide with other element is at most $\frac{q^n}{(2d+1)^m} < 2^{-100}$.

The statistical distance between algorithms 5 and 6 is negligible. Due to the polynomial-time forger F succeeds in forging is not negligible when it executes s queries to the signing oracle and h queries to the random oracle H. Then, the polynomial-time algorithm able to solve the SIS problem with non-negligible probability $= \frac{\delta^2}{2(h+s)}$ when $\alpha = (4\sigma + 2dk)\sqrt{ml}$.

```
Algorithm 5 ($m$,$L = \{A_i\}_{i\in[l]}, Hi$)
1: $\forall i \in [l]$, sample random vector, $y_i \leftarrow D_s^m$
2: $h \longleftarrow \{t : t \in \{-1, 0, 1\}^a, \|t\|_1 \leq a\}$
3: $\forall i \in [l]$, if $i \neq H_i$, sets $v_i = y_i$; if $i = H_i$, sets $v_j = S_j h + y_j$
   with probability $min(\frac{D_\sigma^m(v_{H_i})}{MD_{S_{H_i}h,\sigma}m(v_{H_i})}, 1)$
4: Outputs $(v_i : i \in [l], h)$
5: Program $H(\sum_{i\in[l]} A_i z v_i - Z_i h, L, m) = h$
```

```
Algorithm 6 ($m$,$L = \{A_i\}_{i\in[l]}, H_i$)
1: $h \longleftarrow \{t : t \in \{-1, 0, 1\}^a, \|t\|_1 \leq a\}$
2: $v_i \leftarrow D_s^m$, for all $i \in [l], v_i \leftarrow D_s^m$, with probability $\frac{1}{M}$
3: Outputs $(v_i : i \in [l], h)$
4: Program $H(\sum_{i\in[l]} A_i v_i - Z_i h, L, m) = h$
```

Theorem 4: The statistical distance of Algorithm 2 and Algorithm 3 will be $\varepsilon = sh \cdot 2^{-nl+1} + s^2 \cdot 2^{-nl+1}) + s \cdot \frac{2^{-100}}{M}$. For that, we denote D as the distinguisher, the advantage is negligible.

Proof of theorem 4: Given matrix $A_i = \lfloor A_i \| I \rfloor$, $y_i = \lfloor y_{i,1} \| y_{i,0} \rfloor$ and $t \in Z_q^n$, we have:

$$
\begin{aligned}
&Pr[\sum_{i\in[l]} A_i y_i = z; y_i \leftarrow D_\sigma^m] \\
&= Pr[[y_{1,1}\|y_{2,1}\|\cdots\|y_{l,1}] = (t - \sum_{i\in[l]} \bar{A}_i y_{i,0}); y_i \leftarrow D_\sigma^m] \\
&= maxPr[y_1 = z; y_1 \leftarrow D_\sigma^{nl}] \\
&\le 2^{-nl+1} \qquad (8)
\end{aligned}
$$

Due to Lemma 1 and Lemma 2, the probability collision is $2^{-nl+1} \cdot h + 2^{-nl+1} \cdot s$. After s queries, the probability is $s(h+s) \cdot 2^{-nl+1}$. Therefore, after most s times, the statistical distance is at most $\frac{2^{-\omega(logm)}}{M} \cdot s$.

Consequently, the statistical distance between ring signing algorithm with Algorithm 3 is

$$s(h+s) \cdot 2^{-nl+1} + \frac{2^{-\omega(logm)}}{M} \cdot s. \qquad (9)$$

Theorem 5: The forger F makes s signing oracle queries and h random oracle queries, and $A = [A_1\|A_2\|\cdots\|A_l] \leftarrow Z_q^{n\times ml}$. Existing an algorithm able to compute the vector $v \in Z^{ml}, v \neq 0$, to $Av = 0$ and $\|v\| \leq (4\sigma + 2dk)\sqrt{ml}$ with probability is

$$(\frac{1}{2} - 2^{-100})(\delta - \frac{1}{\mid D_H \mid})(\frac{\delta - \frac{1}{|D_H|}}{t} - \frac{1}{|D_H|}). \qquad (10)$$

Proof of Theorem 6: Given D_H is the range of the random oracle, and choose $T \in Z_q^{n\times k}$ randomly. Given t is the number of times of the random oracle programming when the forger attacked and $t = h + s$. Moreover, lets r_i, $i \in [l]$ as the response of the random oracle, and $i_0 \in [l]$ is index of signer. Through theorem 3, we know that existing another S'_{i_0} such that all the columns of S'_{i_0} are the same as S_{i_0} except for column k with probability $1 - 2^{-100}$, and $AS_{i_0} = AS'_{i_0}$. If $z'_{i_0} - z_{i_0} + S_{i_0}c' - S_{i_0}c = 0$ and $z'_{i_0} - z_{i_0} + S_{i_0}c' - S_{i_0}c = 0$, but the forger can not distinguish whether we use S_{i_0} or S'_{i_0}.

Obviously, we get $z'_{i_0} - z_{i_0} + S_{i_0}c' - S_{i_0}c \neq 0$ with the probability at least $\frac{1}{2}$, consequently we find a non-zero v with probability $(\frac{1}{2} - 2^{-100})(\delta - \frac{1}{|D_H|})(\frac{\delta - \frac{1}{|D_H|}}{t} - \frac{1}{|D_H|})$.

VI. Performance Evaluation

In this section, we compare our scheme with other lattice based ring signature schemes [28],[29] in terms of computational overhead. Our experiment performed 50 times signature generation and verification simulations on Windows 10 to validate data stability values with AMD Ryzen 7 5800H with Radeon Graphics 3.20 GH processor, 16GB RAM. For the accuracy of the experiment, we conducted the evaluation on signature generation and verification overhead using EMR data sizes that approximated those in real healthcare scenarios.

As shown in Fig. 2, Wang et al [28] performed a lattice extension under the bonsai tree model, however, this increases the dimensionality of the lattice and its signature and verification overheads are heavy. The scheme of Tian et al [29] is strongly unforgeable and robust, and has lower overheads than [28]. However, our scheme is lower than both of [28],[29] in signature and verification overhead, providing high efficiency while guaranteeing resistance to quantum attacks.

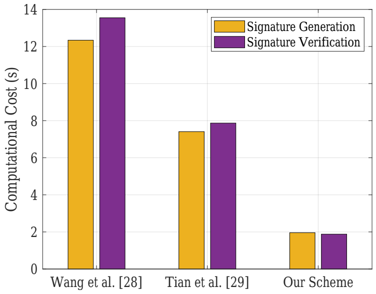

Fig. 2. Comparison of Signature Generation and Verification Overhead.

VII. Related Work

To protect the security of EMRs, scholars have proposed various schemes. The signature algorithms effectively protect the privacy of EMRs. For example, [2] used XML signatures, based on open standards, to help with encryption and privacy protection. Su et al. [3] created a signature scheme based on attribute revocation, which implements attribute revocation with the KUNodes algorithm to protect privacy and ensure EMR security. However, the computational storage and system overhead consumed is heavy. [4] used an aggregated signature scheme based on unpaired certificates, which has a more robust performance compared to the traditional schemes. The paper [5] proposes an improved certificate-free aggregated signature scheme that is significantly reduces the cost of communication. However, it lacks the security of multi-party processing EMR.

In addition, some scholars have realized the security protection of EMR with the help of fingerprint recognition technology or based on other protocols and algorithms. For example, [6] applied fingerprint recognition to EMR access privileges to provide secure authentication of EMR, which greatly diminishes the influence of keys. [7] proposed a web-based EMR system that is based on the premise of HIPAA-related content and is able to effectively protect the information of individual visits. However, that can be easily cracked by hackers. Tasatanattakool et al. [8] proposed a user authentication algorithm and role-based access control to protect the privacy of patient EMR through a user authentication algorithm.

Furthermore, some scholars reach control access of EMR using blockchain. For example, Nirjhor et al. [9] used blockchain on the basis of IPFS and combined it with CAS. However, its key expiration date is too long resulting in a lack of security. A GAC-PSPR scheme based on the blockchain proposed by [10], which can ensure that EMR is not modified arbitrarily and achieve secure access. Wu et al. [11] designed a dynamic access control framework based on the LDP policy to ensure privacy and security. Crucially, the security of EMR is vulnerable to quantum attacks, which has become a severe barrier to the development of e-healthcare security.

Acknowledgment

This work was supported by the National Natural Science Foundation of China Grants No. 12175002, the National

Natural Science Foundation of Beijing Municipality Grants No. 1222020, and NCUT Talents Project and Special Fund for C.Z.

VIII. CONCLUSION

In this paper, we propose a secure cloud-based EMR sharing scheme utilizing the lattice-based ring signature. Most of the existing EMR secure sharing schemes require only one party signature, which carries the risk of EMR forgery and misuse, besides, they are unable to resist quantum computing attacks. To solve the above challenges, this paper designs a EMR sharing scheme in which multiple parties sign the EMR and upload it to the medical cloud. We set a lattice-based ring signature to ensure the privacy of users, the unforgeability of EMRs and signatures,while resisting quantum attacks, thus achieving a superior level of EMR sharing security. The security analysis and performance evaluation indicate that our scheme achieves the established goals and outperforms existing schemes.

REFERENCES

[1] K. Sudheep and S. Joseph, “Review on Securing Medical Big Data in Healthcare Cloud,” in *2019 5th International Conference on Advanced Computing & Communication Systems (ICACCS)*, pp. 212-215, 2019.

[2] G. Hsieh and R. Chen, “Design for a secure interoperable cloud-based Personal Health Record service,” in *4th IEEE International Conference on Cloud Computing Technology and Science Proceedings*, pp. 472-479, 2012.

[3] Q. Su, R. Zhang, R. Xue and P. Li, “Revocable Attribute-Based Signature for Blockchain-Based Healthcare System,” in *IEEE Access*, vol. 8, pp. 12788-127896, 2020.

[4] G. K. Verma, B. B. Singh, N. Kumar, O. Kaiwartya and M. S. Obaidat, “PFCBAS: Pairing Free and Provable Certificate-Based Aggregate Signature Scheme for the e-Healthcare Monitoring System,” in *IEEE Systems Journal*, vol. 14, no. 2, pp. 1704-1715, 2020.

[5] J. Liu, L. Wang and Y. Yu,“Improved Security of a Pairing-Free Certificateless Aggregate Signature in Healthcare Wireless Medical Sensor Networks,” in *IEEE Internet of Things Journal (IoTJ)*, vol. 7, no. 6, pp. 5256-5266, 2020.

[6] Y. Shin, Y. Lee, W. Shin and J. Choi, “Designing Fingerprint-Recognition-Based Access Control for Electronic Medical Records Systems,” in *22nd International Conference on Advanced Information Networking and Applications - Workshops (aina workshops 2008)*, pp. 106-110, 2008.

[7] S. Khadka, “Privacy, security and storage issues in medical data management,” in *2012 Third Asian Himalayas International Conference on Internet*, pp. 1-5, 2012.

[8] P. Tasatanattakool and C. Techapanupreeda, “User authentication algorithm with role-based access control for electronic health systems to prevent abuse of patient privacy,” in *2017 3rd IEEE International Conference on Computer and Communications (ICCC)*, pp. 1019-1024, 2017.

[9] M. K. I. Nirjhor, M. A. Yousuf and M. S. Mhaboob, “Electronic Medical Record Data Sharing Through Authentication and Integrity Managemen-t,” in *2021 2nd International Conference on Robotics, Electrical and Signal Processing Techniques (ICREST)*, pp. 308-313, 2021.

[10] G. Wu and Y. Wang, “The security and privacy of blockchain-enabled EMR storage management scheme,” in *2020 16th International Conference on Computational Intelligence and Security (CIS)*, pp. 283-287, 2020.

[11] G. Wu, S. Wang, Z. Ning and B. Zhu, “Privacy-Preserved EMR Information Publishing and Sharing: A Blockchain-Enabled Smart Healthcare System,” in *IEEE Journal of Biomedical and Health Informatics*, 2021.

[12] L. K. Grover, “A fast quantum mechanical algorithm for database search[J],” in *Proceedings of the Twenty-Eighth Annual ACM Symposium on Theory of Computing*, no. 8, pp. 212-219, 1996.

[13] P. K. Pradhan, S. Rakshit and S. Datta, “Lattice Based Cryptography : Its Applications, Areas of Interest & Future Scope,” in *2019 3rd International Conference on Computing Methodologies and Communication (ICCMC)*, 2019.

[14] 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*, early access, 2022.

[15] J. Liu, L. Wang and Y. Yu, Improved Security of a Pairing-Free Certificateless Aggregate Signature in Healthcare Wireless Medical Sensor Networks, IEEE Internet Things J., vol. 7, no. 6, pp. 5256-5266, 2020.

[16] 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 *WCNC 2022*, early access, 2022

[17] Y. Cheng, S. Xu, M. Zang and W. Kong, “LPPA: A Lightweight PrivacyPreserving Authentication Scheme for the Internet of Drones,” in *ICCT 2021*, pp. 656-661, 2021.

[18] S. Xu, X. Chen, C. Wang, Y. He, K. Xiao and Y. Cao, “A Lattice-Based Ring Signature Scheme to Secure Automated Valet Parking,” in *WASA 2021*, vol. 12938, pp. 70-83, 2021.

[19] S. Xu, X. Chen and Y. He, “EVchain: An Anonymous Blockchain-Based System for Charging-Connected Electric Vehicles,” *Tsinghua Sci. Technol.*, vol. 26, no. 6, pp. 845-856, 2021.

[20] Y. Cheng, S. Xu, M. Zang, S. Jiang and Y. Zhang, “Secure Authenticati on Scheme for VANET Based on Blockchain,” in *ICCC 2021*, pp. 1526-1531, 2021.

[21] R. L. Rivest, A. Shamir, Y. Tauman, How to leak a secret, International Conference on the Theory and Application of Cryptology and Information Security (2001) 552-565.

[22] P. W. Shor, “Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer,” SIAM review, pp. 303-332, 1999.

[23] J. Hostein, J. Pipher, J. H. Silverman, “Nss: An ntru lattice-based signature scheme,” pp. 211-228, 2001.

[24] M. Ajtai, “Generating hard instances of lattice problems,” in *the twenty-eighth annual ACM symposium on Theory of computing*, pp. 99-108, 1996.

[25] 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*, no. 10, pp. 197-206, 2008.

[26] J. H. Yang and C. C. Chang, “An ID-based remote mutual authentication with key agreement scheme for mobile devices on elliptic curve cryptosystem,” in *Computers & security*, vol. 28, no. 3-4, pp. 138-143, 2009.

[27] V. Lyubashevsky, “Lattice signatures without trapdoors,” in *EUROCRYPT*, pp. 738-755, 2012.

[28] F. H. Wang, Y. P. Hu and C. X. Wang, “A Lattice-based Ring Signature Scheme from Bonsai Trees [J],” in *Journal of Electronics & Information Technology*, vol. 32, no. 2, pp. 2400-2403, 2010.

[29] M. M. Tian, L. S. Huang and W. Yang, “Efficient Lattice-Based Ring Signature Scheme[J],” in *Chinese Journal of computers*, vol. 35, no. 4, pp. 713-717, 2012.

[30] Chao Zheng. “Quantum remote sensing secure direct communication,” *Proc. SPIE 11128, Infrared Remote Sensing and Instrumentation XXVII*, 111280R, 2019.

[31] Chao Zheng*, Guofei Long, “Quantum secure direct dialogue using Einstein-Podolsky-Rosen pairs,” *Science China Physics, Mechanics & Astronomy*, vol. 57, no. 7, pp. 1238-1243, 2014.

[32] Guilu Long, Chuan Wang, Fuguo Deng, Chao Zheng, “Quantum Secure Direct Communication,” *Conference on Coherence and Quantum Optics*, pp. M6-42, 2013.

[33] Chao Zheng and Daili Li, “Distinguish between typical non Hermitian quantum systems by entropy dynamics,” *Scientific Reports*, vol. 12, no. 1, pp. 1-10, 2022.

[34] Chao Zheng, “Quantum simulation of PT-arbitrary-phasesymmetric systems,” *EPL*, vol. 136, no. 3, p. 30002, 2021.

[35] Chao Zheng, “Universal quantum simulation of singlequbit nonunitary operators using duality quantum algorithm,” *Scientific Reports*, vol. 11, no. 1, pp. 1-14, 2021.

[36] Chao Zheng, Jin Tian, Daili Li, Jingwei Wen, Shijie Wei, Yansong Li, “Efficient quantum simulation of an anti-P-pseudo-Hermitian two-level system,” *Entropy*, vol. 22, no. 8, p. 821, 2020.