Journal of Cyber Security
DOI:10.32604/jcs.2021.026926
Article

Data Anonymous Authentication for BIoMT with Proxy Group Signature

Chaoyang Li[1,*], Yalan Wang[2], Gang Xu[3], Xiubo Chen[4], Xiangjun Xin[1] and Jian Li[4]

[1]College of Software Engineering, Zhengzhou University of Light Industry, Zhengzhou, 450001, China
[2]Department of Computer Science, University of Surrey, Guildford, Surrey, GU2 7XH, UK
[3]School of Computing Science and Technology, North China University of Technology, Beijing, 100144, China
[4]Information Security Centre, State Key Laboratory of Networking and Switching Technology, Beijing University of Posts and Telecommunications, Beijing, 100876, China
[*]Corresponding Author: Chaoyang Li. Email: lichaoyang@zzuli.edu.cn
Received: 23 October 2021; Accepted: 21 December 2021

Abstract: Along with the increase of wearable medical device, the privacy leakage problem in the process of transmission between these edge medical devices. The blockchain-enabled Internet of Medical Things (BIoMT) has been developed to reform traditional centralized medical system in recent years. This paper first introduces a data anonymous authentication model to protect user privacy and medical data in BIoMT. Then, a proxy group signature (PGS) scheme has been proposed based on lattice assumption. This scheme can well satisfy the anonymous authentication demand for the proposed model, and provide anti-quantum attack security for BIoMT in the future general quantum computer age. Moreover, the security analysis shows this PGS scheme is secure against the dynamical-almost-full anonymous and traceability. The efficiency comparison shows the proposed model and PGS scheme is more efficient and practical.

Keywords: Blockchain-enabled Internet of Medical Things; anonymous authentication; proxy group signature; medical data

1 Introduction

Blockchain technology brings a significant revolution to the traditional centralized system, such as the smart manufacturing, supply chain management, food industry, smart grid, health care and Internet of vehicles [1]. As in traditional healthcare service system, the medical data cannot be shared to other doctors and research institutions, the patient cannot obtain his own electric medical records, the doctor cannot view more medical instance to improve diagnostic level, the medical researcher cannot obtain more medical data resource to develop drugs and medical devices. The emergence of blockchain takes a more promising solution for traditional Internet of Medical Things [2].

Blockchain-enabled Internet of Medical Things (BIoMT) solve the centralized problem in traditional healthcare service system based on blockchain technology [3]. Blockchain makes medical data utilization more transparency and decreases the probability of data tamper. Meanwhile, it improves the data sharing ability and interoperability by aggregating many medical institutions into one BIoMT network. The patient can take personal medical data to see a doctor in different medical institutions, the doctor can view more case resource to improve their diagnostic level, and the researcher can utilize medical data resource to develop the drug and medical device. In recent years, there appear many BIoMT platforms and applications for medical data management and sharing [4–11]. Meanwhile, the increasing of wearable and smart medical devices brings many new problems and challenges for current healthcare service system. BIoMT aggregates the dispersive medical devices to establish a healthcare service network, which can provide more precision and comprehensive treatment for patient [12]. Many daily health data are collected by these devices and uploaded into the BIoMT system, which constructs the basis for patient's

diagnosis and treatment. These data also contain many sensitive information about the patient, which will bring damages for the patient's privacy and property if they are leaked [13,14]. Therefore, in the processes of data processing, how to certify the validity of target doctor, how to guarantee the security of medical data, and how to protect patient's privacy, are very concern aspects of the system users.

Security of medical data and user's privacy are the main challenges for patients and doctors in BIoMT [15]. From the generation to destroy of medical data, it requires the participation of many operators and medical devices. For the security perspective, all the operation records shall be signed by operators and recorded into the blockchain ledger. This can establish a data link for traceability, and provide the evidence for doctor-patient conflict. In order to realize signer's anonymous, the group signature scheme and proxy signature scheme are the common methods to protect the security of signer's privacy. The group signature scheme hides the information of real signers by means of group [16–21], while the proxy signature scheme helps a legal user authorize somebody to sign on behalf of himself [20–24]. By combining the merits of proxy signature and group signature, it can achieve the anonymous authentication of medical data and guarantee the anonymous of signer. Moreover, the anti-quantum attack security is an important property for signature scheme which should be taken more consideration [25–27].

The main contributes of this work are following:

- We construct a data anonymous authentication model for BIoMT, and this model is composed of a proxy group signature scheme and blockchain ledger which can make full protection for medical data from the generation to destroy.
- We propose a proxy group signature (PGS) scheme based on lattice assumption, and this scheme helps to realize the singer's anonymous to public verifier, and the message's anonymous to the signer. Meanwhile, this scheme also can help the BIoMT system resist the quantum attack.
- We present the analysis of ecurity and efficiency, and the results show this PGS scheme is secure and efficient. The PGS can capture the security properties of dynamical-almost-full anonymous and traceability, and it also efficient than similar literature.

2 Data Anonymous Authentication Model

In order to improve the security of storage and management through BIoMT, a data anonymous authentication model has been proposed (Fig. 1). This model utilizes the proxy group signature and blockchain to improve the security of medical data and user's privacy.

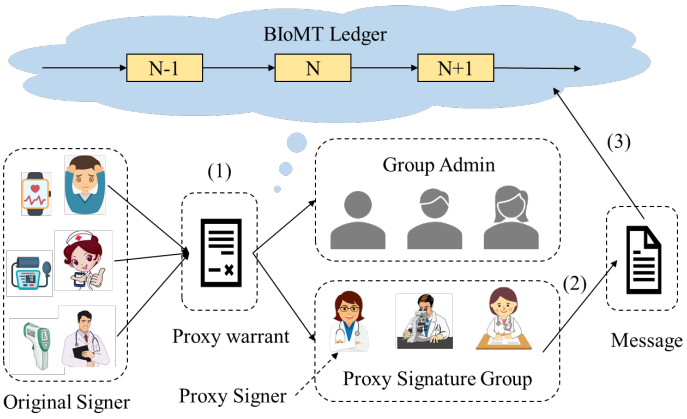

Figure 1: Data Anonymous authentication model

Firstly, this model mainly contains some parties: original signer, proxy signer, group administrator, and proxy signature group, who perform the data management, data signing, and data authentication. The model also contains the proxy warrant, message and BIoMT ledger. Following Table 1 are the descriptions of these items.

Table 1: Parties in data anonymous authentication model

Items	Description
Original Signer	The signer who should perform signing originally.
Proxy Signer	The signer who performs signing on behalf of the original signer.
Proxy Warrant	The certification that the original signer authorizes to the proxy signer.
Group Administrator	The manager who can reveal the correct identity of original and proxy signature from the signature.
Proxy Signature Group	The signers in this group all can perform the proxy signature.
Message	The medical data is going to be signed.
BIoMT Ledger	The public ledger which stores the data transaction and operation records.

Secondly, the data anonymous authentication model mainly contains three parts: agent authorization, proxy group signature, and transaction in BIoMT ledger. Following are the detailed descriptions of these three parts:

(1) *Agent authorization*: The original signer authorizes the proxy signer to exercise the power of signature. Here, the proxy signer should be one legal group member, and the proxy warrant is composed of agent identity, proxy signature warrant, term of agency. The proxy signer is only allowed perform proxy signing in a certain period.

(2) *Proxy group signature*: After the proxy signature group receiving the proxy warrant from the original signer, he first verified the validity of proxy warrant. Then, the proxy signer can represent the proxy signature group to perform signing on the target message on behalf of the original signer. Although the target message is signed by the proxy signer, it contains the private information of original signer, and it will be verified to be legitimate with the original signer's public key. This also proves that the agent authorization is correct and legal.

(3) *Transaction in BIoMT ledger*: This ledger is a public recordation which records the data transaction and the operations of data processing. The general medical data are recorded as the transaction into this ledger, and this management mode can help patients take their own medical data to different medical institutions participated in the BIoMT system. The operations of data processing contain generation, signature, storage, delete, and so on. These records can provide a traceable evidence for the medical dispute.

2.2 Proxy Group Signature Scheme

This section gives the proposed proxy group signature (PGS) scheme. The PGS scheme is designed with lattice assumption $\Re - SIS^{\kappa}_{q,n,m,\beta}$ to improve the security against the quantum attack, where κ is a uniform distribution. In this paper, we simplify the lattice assumption from $\Re$ to $\mathbb{Z}$ with rings $\Re = \mathbb{Z}[x]/(x^n+1)$, but do not decrease the hardness of this lattice assumption $\mathbb{Z} - SIS^{\kappa}_{q,n,m,\beta}$. Then, we utilize the bimodal Gaussian distribution for selecting the random parameters to improve the efficiency of reject sampling . Following seven algorithms are detailed descriptions of the proposed PGS scheme.

Key Gen. $(n,m,q \rightarrow (\{A,B,U_i\} \in \mathbb{Z}_{2q}^{n*m}, \{S_A, S_B, S_{U_i}\} \in \mathbb{Z}_{2q}^{m*n})$: The parameters n,m,q,κ,σ are defined based on the rules where κ is the security parameter and $m = O(n \log q)$. Then, following six steps will generate the system keys:

a) Select a short matrix $S_A \in \mathbb{Z}_{2q}^{m*n}$ as the group master secret key, where $\left\|\tilde{S}\right\| \le O(\sqrt{n \log q})$;

b) Derive the matrix $A \in \mathbb{Z}_{2q}^{n*m}$ such that $AS_A = A(-S_A) = qI_n (\text{mod}\, 2q)$;

c) Select a short matrix $S_B \in \mathbb{Z}_{2q}^{m*n}$ as the tracing manager's (Opener) secret key;

d) Derive the matrix $B \in \mathbb{Z}_{2q}^{n*m}$ such that $BS_B = B(-S_B) = qI_n (\mathrm{mod}\, 2q)$;

e) Generate guest i's key pair (U_i, S_{U_i}) with the same principle;

f) Output the group public key $gpk = (A, B)$, group master secret key $gmsk = S_A$, tracing manager's (opener's) secret key $tmsk = S_B$, guest i's key pair $(upk_i = U_i, usk_i = S_{U_i})$.

Join algorithm $(gpk, gmsk, upk_i, usk_i) \to (mc_i)$: The group guest first creates a registration message, and then the group manager generates a member certificate with a leaving data and time for this group guest. Note that this is a probabilistic polynomial algorithm, so it will restart if it does not derive a valid member certificate.

(1) Group guest performs following five steps:

a) Selects vectors $x_{i_1}, x_{i_2} \leftarrow D_{\sigma_1}^m$, as $D_{\sigma_1}^m$ is the bimodal Gaussian distribution;

b) Computes $y_{i_1} = S_{U_i} x_{i_1}$ and $y_{i_2} = Bx_{i_2}$;

c) Computes $z_i = x_{i_1} + x_{i_2}$;

d) Sets a leaving date and time t_{r_i};

e) Sends $(y_{i_1}, y_{i_2}, z_i, t_{r_i})$ to group manager.

(2) Group manager performs following eight steps:

a) Samples $r_i \leftarrow SampleD(S_A, A, qz_i, \sigma_2)$;

b) Computes $Token_i = A \cdot r_i$ as the revocation token;

c) Computes $c_{i_1} \leftarrow H(Ay_{i_1} \bmod 2q, Token_i)$ with the received y_{i_1};

d) Chooses a random bit $a \in \{0,1\}^n$;

e) Computes $w_{i_1} \leftarrow y_{i_1} + (-1)^a S_A c_{i_1}$;

f) Derives (w_{i_1}, c_{i_1}) with probability $\min(\frac{D_{\sigma_1}^{Token_i}(w_{i_1})}{M_1 D_{c_{i_1}, \sigma_1}^{Token_i}(w_{i_1})}, 1)$; otherwise, restart;

g) Records group guest i's registration information $reg[i] \leftarrow (i, y_{i_1}, t_{r_i}, r_i, 1)$, here "1" represents this Group guest i is active;

h) Outputs the member certificate $mc_i = (w_{i_1}, c_{i_1}, Token_i)$ for GG i.

Delegation generation algorithm $(m, gpk, gmsk, upk_i, usk_i, mc_i) \to (A_P, S_P)$: The original signer first generates a signature warrant to proxy signer, and then the proxy signer generates the proxy public and private keys if this signature warrant is valid. Here, the proxy signer is also the same as group guest, which has the joint and exit mechanisms.

(1) Original signer performs following three steps:

a) Selects vectors $y_{i_3} \leftarrow D_{\sigma_1}^m$ and a random bit $b \in \{0,1\}^n$;

b) Computes $c_{i_2} \leftarrow H(Ay_{i_3} \bmod 2q, m)$ and $w_{i_2} \leftarrow y_3 + (-1)^b S_A c_{i_2}$;

c) Derives the signature warrant $W_{A \to B}(W, w_{i_2}, c_{i_2})$ of message μ with probability $\min(\frac{D_{\sigma_1}^m(w_{i_2})}{M_1 D_{c_{i_2}, \sigma_1}^m(w_{i_2})}, 1)$, and sends it to proxy signer; otherwise, restart.

(2) Proxy signer performs following steps:

a) If $\|w_{i_1}\| > T_1$ or $\|w_{i_1}\|_\infty > q/4$, terminates and restarts delegation generation algorithm;

b) Continues iff $c_{i_1} \leftarrow H(Aw_{i_1} + qc_{i_1} \bmod 2q, A \cdot r_i)$;

c) If $\|w_{i_2}\| > T_1$ or $\|w_{i_2}\|_\infty > q/4$, terminates and restarts delegation generation algorithm;

d) Continues iff $c_{i_2} \leftarrow H(Aw_{i_2} + qc_{i_2} \bmod 2q, m)$;

e) Computes $M \leftarrow H_1(W_{A \to B})$;

f) Computes $A_P = U_i * M^T$ and $S_P = S_{U_i} * M$ as the public key and private key for proxy signer, respectively.

Here, denoting $T_1 = \eta\sqrt{m}\sigma_1$, one can set η so that $\|w_{i_1}\| > T_1$ is verified with probability $1 - 2^{-\kappa}$ for the security parameter κ (in practice $\eta \in [1.1, 1.4]$).

Sign algorithm $(m, A_P, B_P) \to (e_i)$: The proxy signer performs following five steps:

a) Conforms the signature expiration data $t_s < t_{r_i}$, otherwise restart;

b) Computes $c_{i_3} \leftarrow H(A_P y_{i_1} + A_P y_{i_2} \bmod 2q, m)$ with the former computed (y_{i_1}, y_{i_2});

c) Selects a random bit $b \in \{0,1\}^n$;

d) Computes $w_{i_3} \leftarrow w_{i_1} + y_{i_2} + (-1)^b S_P c_{i_3}$ with w_{i_1} and y_{i_2};

e) Derives the signature $e_i = (w_{i_3}, c_{i_3}, t_s)$ of message m with probability $\min\left(\frac{D^m_{\sigma_1}(w_{i_3})}{M_1 D^m_{c_{i3},\sigma_1}(w_{i_3})}, 1\right)$, otherwise, restart.

Verify algorithm $(m, e_i, A_P, mc_i) \to$ (*Reject* or *Accept*): Verifier makes *Accept* or *Reject* according to the following four steps:

a) SV first confirms current date and time $t_v < t_s$ and $t_s < t_{r_i}$, otherwise restart;

b) If $\|e_i\| > T_1$, then *Reject*;

c) If $\|e_i\|_\infty > q/4$, then *Reject*;

d) Accept iff $c_{i_3} \leftarrow H(A_P w_{i_3} + qc_{i_1} + qc_{i_2} \bmod 2q, m)$.

Open algorithm $(gpk, gmsk, e_i) \to$ (*Signature index* i): The following is the open algorithm which can approve that the signature e_i is signed by group guest (proxy signer) i.

a) Samples $r_i' \leftarrow SampleD(S_A, A, U_i y_{i_1} + S_B y_{i_2}, \sigma_2)$;

b) If $r_i' = r_i$, returns group guest's index i;

c) Otherwise, restart.

Revoke algorithm $(gpk, gmsk, reg[i]) \to (RL)$: Group manager performs following three steps to revoke the revoking member and inserts the revocation information to the revocation list RL.

a) Extracts revoking member i 's revocation token $Token_i = A \cdot r_i$ by querying $reg[i]$;

b) Changes the state to inactive (0) and updates $(A \cdot r_i)$ to revocation list RL;

c) Outputs the revocation list RL.

3 Security Analysis

Now, we analysis the proposed PGS scheme can capture the security properties of dynamical-almost-full anonymous and traceability.

3.1 Dynamical-Almost-Full Anonymous

Dynamical-almost-full anonymous: It cannot confirm the signer's identity from the signature without the group muster's secret key. That is to say the adversary cannot distinguish two signatures created by two different group members. Meanwhile, this scheme also supports group members' free joining and revoking.

Theorem 1: *The proposed PGS is dynamical-almost-full anonymous in the random oracle model based on the fact that* $\Re - SIS^{\kappa}_{q,n,m,\beta}$ *problem is hard.*

Proof: Theorem 1 will be proved by the following six games.

Game 0: Assume there exists an adversary A who can obtain the information about a group member's secret key usk. The challenger C establishes a query-answer game in random oracle model with A, and A cannot distinguish which user i_0 or i_1 generates the signature on the strength $\Re - SIS^{\kappa}_{q,n,m,\beta}$ problem's hardness. In this game model, A can query any opened signature, ask for any group member's revocation token, and add new users. When A asks to register a new group member, C checks the validity and updates its details to the registration list $List_{RU}$. Here, C only returns a successful registration message to A, and he does not return the revocation token and key-expiration time for this new user. Then, when A queries to reveal one group user i's revocation token, C traces this user's index, returns the member certificate mc_i in the former registration list, and adds this query into a new formed list $List_{RU}$. Furthermore, in the challenge phase, A sets two indices (i_0, i_1) for message M and sends them to A. After checking (i_0, i_1) are newly added in $List_{RU}$ and not in $List_{RU}$, C generates a signature $e_i = (w_{i_3}, c_{i_3}, t_s)$ with a random $\tau \leftarrow \{0,1\}$. In the end, A publics his guess $\tau' \leftarrow \{0,1\}$. If $\tau' \leftarrow \tau$, it outputs 1; otherwise outputs 0.

In addition, the adversary A must send two different expiration dates along with the two indices, respectively. If A provides one wrong key-expiration date, he cannot pass the validation step. Here, the data should satisfy $t_{r_i} > t_s \geq t_v$. Even though A provides two correct expiration dates, C will generate the challenging signature to verify it. Therefore, the adversary cannot utilize the time-bound keys to attack the anonymous of the proposed PGS.

Game 1: C serves as a challenger and generates key pair $(U_i^*, S_{U_i}^*)$ for the challenging signature in the initial **KeyGen. algorithm**. When the adversary A asks one opened signature $e_i = (w_{i_3}, c_{i_3}, t_s)$, C terminates this game and provides a random bit. In fact, this situation is impossible as A cannot know U_i^* and he does not be allowed to query the unopened signature. As a result, C keeps performing the following games, and this game is indistinguishable from **Game 0**.

Game 2: The challenger C sets the random oracle H in the **Join algorithm**. When the adversary A queries the opened signature (e_i, m), C executes $c_{i_3} \leftarrow H(A_P y_{i_1} + A_P y_{i_2} \bmod 2q, m)$ with message m. Before this, C performs the random oracle $H(Ay_{i_1} \bmod 2q, Token_i)$ in the **Join algorithm** first to obtain c_{i_1}. Then, C creates the signature e_i of queried message m and returns it back. As A does not have any information about the newly registered user, he obtains nothing with the results of a random

oracle. Moreover, this game is indistinguishable from the former two games as the random oracle is collision-resistant.

Game 3: As $e_i = (w_{i_3}, c_{i_3}, t_s)$ is related with w_{i_3} and c_{i_3}. Here, the challenger C not only acts the user of message owner, but also acts the signer. C randomly selects a random vector for y_{i_3}, and performs the **Delegation generation algorithm** to derive w_{i_2}. Meanwhile, C can compute w_{i_2} from the following **Game 4**. Then, C creates $e_i = (w_{i_3}, c_{i_3}, t_s)$ with probability $\min(\frac{D^m_{\sigma_1}(w_{i_3})}{M_1 D^m_{c_{i_3},\sigma_1}(w_{i_3})}, 1)$. In addition, the vector r_i^* is uniformly sampled from $\mathbb{Z}_q^n$, so this game and the former three games are indistinguishable.

Game 4: This game gives a trivial amendment w_{i_2} for **Game 3**. Because C does know the group manager's $gmsk$ to generate the revocation token $Token_i$, he will uniformly sample a vector r_i^* and compute $Token_i = Ar_i^*$ with the gpk. Next, C computes $w_{i_1} \leftarrow y_{i_1} + (-1)^a S_A c_{i_1}$ with y_{i_1} and c_{i_1}, here c_{i_1} is created with $Token_i^*$ by the random oracle query in **Game 2**. Here, C creates (w_{i_1}, c_{i_1}) with probability $\min(\frac{D^{Token_i}_{\sigma_1}(w_{i_1})}{M_1 D^{Token_i}_{c_{i_1},\sigma_1}(w_{i_1})}, 1)$.

Game 5: This game gives a trivial amendment e_i for **Game 3**. C creates the revocation token $Token_i$ is depending on the challenging bit τ, so e_i is generated uniformly. C randomly selects $\eta \in \mathbb{Z}_q^n$ and sets $e_i = \eta$. Here, $e_i = (w_{i_3}, c_{i_3}, t_s)$ is a proper $\Re - SIS^{\kappa}_{q,n,m,\beta}$ instance. The adversary A can solve SIS problem, if he can distinguish e_i and η. Therefore, this game is indistinguishable with **Game 3** as $\Re - SIS^{\kappa}_{q,n,m,\beta}$ problem is hard.

Game 6: The challenger C creates e_i^* independent of the bit τ. This game is statistically indistinguishable from former games. The probability A can win this game is negligible.

Hence, the proposed PGS scheme satisfies dynamical-almost-full anonymous with the time-bound keys.

3.2 Traceability

Traceability: If the occasion arises, the group manager can confirm the identity of one group member by opening his signature, and this group member cannot prevent the openness of the legitimate signature.

Theorem 3: *The proposed PGS is traceable in the random oracle model on the strength of the of SIS problem's hardness.*

Proof: Assume there exists an adversary A who has ability to forge a valid signature by grasping the keys gpk and $tmsk$. Meanwhile, he can add new users into the group and replace member's personal upk. He is also allowed to query for the group member's usk and revocation token. Then, we take a challenge pseudo polynomial time (PPT) algorithm C_1 to solve the SIS problem by performing the query-answer game with A. Next, A makes queries on the **KeyGen. algorithm**, **Join algorithm**, and **Delegation generation algorithm** for many times, and C_1 answers A's queries according the algorithm steps. Based on enough obtained information, A forges a signature $e_i = (w'_{i_3}, c'_{i_3}, t'_s)$ for the target

message M'. When receives the forgery signature (e_i', m'), C_1 opens it and identify its index. According to the Forking Lemma C_1 can derive the other one legitimate signature $(e_i'^*, m)$ with $e_i'^*=(w_{i_3}'^*, c_{i_3}'^*, t_s'^*)$. Here, C_1 can obtain two vectors z_i' and $z_i'^*$ ($z_i' \neq z_i'^*$) from the equations $U_i y_{i_1}' + S_B y_{i_2}' = q z_i' \bmod 2q$ and $U_i y_{i_1}'^* + S_B y_{i_2}'^* = q z_i'^* \bmod 2q$ respectively. Therefore, it can derive $A(r_i' - r_i'^*) = q(\mathrm{z}_i' - z_i'^*) \bmod 2\mathrm{q}$. Due to $(r_i' - r_i'^*)$, we can know $r_i' - r_i'^* \neq 0 \bmod 2q$. Because $q(\mathrm{z}_i' - z_i'^*) \bmod \mathrm{q} = 0$, C_1 can find out a solution $v = r_i' - r_i'^*$ for SIS instance as $Av = 0 \bmod 2q$.

However, the SIS problem cannot be solved with current computation power. Therefore, the assumption fails, and the proposed PGS scheme satisfies traceability.

4 Efficiency Comparison

Comparing with the similar PGS protocols, the proposed PGS protocol in this paper has many advantages, and the comparison results are shown in Table 1. We unify the parameter setting and set the parameters n, m, q, σ that are the same between these schemes. Then, compared with some similar related lattice-based PGS, the proposed new scheme has many advantages, as shown in Table 2. The size of gpk, $gmsk$, and $tmsk$ are with little difference, but the signature size has a big difference.

Table 2: Efficiency comparison of the similar schemes

Scheme	gpk	$gmsk$	$tmsk$	Signature
Perera et al. [19]	$mn\log\mathrm{q}$	$m \cdot n\log\mathrm{q}$	$mn\log\mathrm{q}$	$m\log\mathrm{q} + 3m\log(12\sigma)$
Xie et al. [20]	$mn\log\mathrm{q}$	$mn\log\mathrm{q}$	$2mn\log\mathrm{q}$	$(n+2m)\log\mathrm{q}$
Our protocol	$mn\log 2\mathrm{q}$	$mn\log 2\mathrm{q}$	$mn\log 2\mathrm{q}$	$2m\log(12\sigma)$

5 Conclusion

This paper introduces a data anonymous authentication model to improve the security of medical and user's privacy. Meanwhile, a proxy group signature has been proposed to realize the anonymous of user information and the secure authentication of medical data. It guarantees the signer's security as it does not know who signs the signature in the group, and the message's security as the original signer cannot deny this signature signed by the authorized proxy signer. Meanwhile, the PGS scheme can resist the quantum attack from the quantum computing in the future quantum computer age. Then, the security analysis and efficiency comparison show that the PGS scheme can well improve the security and efficiency of transaction's performance BIoMT system.

Funding Statement: This work was supported by the National Natural Science Foundation of China under Grants 92046001, 61962009, the Doctor Scientific Research Fund of Zhengzhou University of Light Industry under Grant 2021BSJJ033, Key Scientific Research Project of Colleges and Universities in Henan Province (CN) under Grant No. 22A413010.

Conflicts of Interest: The authors declare that they have no conflicts of interest to report regarding the present study.

References

[1] H. N. Dai, Z. Zheng and Y. Zhang, "Blockchain for Internet of Things: A survey," *IEEE Internet of Things Journal*, vol. 6, no. 5, pp. 8076–8094, 2019.

[2] M. Mettler, "Blockchain technology in healthcare: The revolution starts here," in *2016 IEEE 18th Int. Conf. on e-Health Networking, Applications and Services (Healthcom)*, IEEE, pp. 1–3, 2016.

[3] S. Shi, D. He, L. Li, N. Kumar, M. K. Khan *et al.,* "Applications of blockchain in ensuring the security and privacy of electronic health record systems: A survey," *Computers & Security*, 101966, 2020.

[4] S. Rouhani, L. Butterworth, A. D. Simmons, D. G. Humphery and R. Deters, "MediChain TM: A secure decentralized medical data asset management system," in *2018 IEEE Int. Conf. on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData)*, IEEE, pp. 1533–1538, 2018.

[5] J. Xu, K. Xue, S. Li, H. Tian, J. Hong *et al.,* "Healthchain: A blockchain-based privacy preserving scheme for large-scale health data," *IEEE Internet of Things Journal*, vol. 6, no. 5, pp. 8770–8781, 2019.

[6] R. H. Hylock and X. Zeng, "A blockchain framework for patient-centered health records and exchange (HealthChain): Evaluation and proof-of-concept study," *Journal of Medical Internet Research*, vol. 21, no. 8, e13592, 2019.

[7] S. Chenthara, K. Ahmed, H. Wang, F. Whittaker and Z. Chen, "Healthchain: A novel framework on privacy preservation of electronic health records using blockchain technology," *PLoS One*, vol. 15, no. 12, e0243043, 2020.

[8] T. P. A. Rahoof and V. R. Deepthi, "HealthChain: A secure scalable health care data management system using blockchain," in *Int. Conf. on Distributed Computing and Internet Technology*, Springer, Cham, pp. 380–391, 2020.

[9] C. Li, M. Dong, J. Li, G. Xu, X. B. Chen *et al.,* "Healthchain: Secure EMRs management and trading in distributed healthcare service system," *IEEE Internet of Things Journal*, vol. 8, no. 9, 71927202, 2021.

[10] A. I. Khan, A. A. L. Ghamdi, F. J. Alsolami, Y. B. Abushark, A. Almalawi *et al.,* "Integrating blockchain technology into healthcare through an intelligent computing technique," *Computers, Materials & Continua*, vol. 70, pp. 2835–2860, 2022.

[11] S. J. Hsiao and W. T. Sung, "Using mobile technology to construct a network medical health care system," *Intelligent Automation and Soft Computing*, vol. 31, no. 2, pp. 729–748, 2022.

[12] A. O. Almagrabi, R. Ali, D. Alghazzawi, A. AIBarakati and T. Khurshaid, "Blockchain-as-a-utility for next-generation healthcare Internet of Things," *Computers, Materials & Continua*, vol. 68, no. 1, pp. 359–376, 2021.

[13] C. Xu, M. Dong, K. Ota, J. Li, W. Yang *et al.,* "Sceh: smart customized e-health framework for countryside using edge AI and body sensor networks," in *2019 IEEE Global Communications Conf. (GLOBECOM)*, IEEE, pp. 1–6, 2019.

[14] G. Yang, Z. Pang, M. J. Deen, M. Dong, Y. T. Zhang *et al.,* "Homecare robotic systems for healthcare 4.0: Visions and enabling technologies," *IEEE Journal of Biomedical and Health Informatics*, vol. 24, no. 9, pp. 2535–2549, 2020.

[15] R. Kumar and R. Tripathi, "Towards design and implementation of security and privacy framework for Internet of Medical Things (IoMT) by leveraging blockchain and IPFS technology," *The Journal of Supercomputing*, pp. 1–40, 2021.

[16] L. Chen and T. P. Pedersen, "New group signature schemes," in *Workshop on the Theory and Application of Cryptographic Techniques. Springer*, Berlin, Heidelberg, pp. 171–181, 1994.

[17] A. S. Mbandu, C. X. Xu and K. D. Mutiria, "Secure opportunistic computing privacy preserving group signature authentication scheme for m-Healthcare emergency," *International Journal of Information and Electronics Engineering*, vol. 5, no. 5, pp. 335, 2015.

[18] S. Zhang and J. H. Lee, "A group signature and authentication scheme for blockchain-based mobile-edge computing," *IEEE Internet of Things Journal*, vol. 7, no. 5, pp. 4557–4565, 2019.

[19] M. N. S. Perera and T. Koshiba, "A guests managing system with lattice-based verifier-local revocation group signature scheme with time-bound keys," in *Proc. of the Fifth Int. Conf. on Mathematics and Computing*, Springer, Singapore, pp. 81–96, 2021.

[20] R. Xie, C. He, C. Xu and C. Gao, "Lattice-based dynamic group signature for anonymous authentication in IoT," *Annals of Telecommunications*, vol. 74, no. 7, pp. 531–542, 2019.

[21] Y. Zhang, X. Liu, Y. Hu, H. Jia and Q. Zhang, "An improved group signature scheme with VLR over lattices," *Security and Communication Networks*, vol. 2021, 2021.

[22] C. Li, X. B. Chen, Y. Chen, Y. Hou and J. Li, "A new lattice-based signature scheme in post-quantum blockchain network," *IEEE Access*, vol. 7, pp. 2026–2033, 2018.

[23] G. K. Verma, B. B. Singh and H. Singh, "Provably secure message recovery proxy signature scheme for wireless sensor networks in e-healthcare," *Wireless Personal Communications*, vol. 99, no. 1, pp. 539–554, 2018.

[24] C. Li, G. Xu, Y. Chen, H. Ahmad and J. Li, "A new anti-quantum proxy blind signature for blockchain-enabled Internet of Things," *Computers, Materials & Continua*, vol. 61, no. 2, pp. 711–726, 2019.

[25] H. Zhu, Y. Wang, C. Wang and X. Cheng, "An efficient identity-based proxy signcryption using lattice," *Future Generation Computer Systems*, vol. 117, pp. 321–327, 2021.

[26] S. Hussain, I. Ullah, H. Khattak, M. A. Khan, C. M. Chen *et al.,* "A lightweight and provable secure identity-based generalized proxy signcryption (IBGPS) scheme for Industrial Internet of Things (IIoT)," *Journal of Information Security and Applications*, vol. 58, 102625, 2021.

[27] C. Li, Y. Tian, X. B. Chen and J. Li, "An efficient anti-quantum lattice-based blind signature for blockchain-enabled systems," *Information Sciences*, vol. 546, pp. 253–264, 2021.