Journal of Systems Architecture 160 (2025) 103362

Contents lists available at ScienceDirect

Journal of Systems Architecture

journal homepage: www.elsevier.com/locate/sysarc

Quantum-safe identity-based designated verifier signature for BIoMT

Chaoyang Li [a,b,*], Yuling Chen [a], Mianxiong Dong [c], Jian Li [d], Min Huang [b], Xiangjun Xin [b], Kaoru Ota [c]

[a] State Key Laboratory of Public Big Data, Guizhou University, Guizhou Guiyang, 550025, China
[b] College of Software Engineering, Zhengzhou University of Light Industry, Zhengzhou 450001, China
[c] Department of Sciences and Informatics, Muroran Institution of Technology, Muroran 050-8585, Japan
[d] School of Cyberspace Security, Beijing University of Posts and Telecommunications, Beijing 100876, China

ARTICLE INFO

MSC:
00-01
99-00

Keywords:
Blockchain
Internet of medical things
Identity
DVS
Privacy-preserving

ABSTRACT

Blockchain technology changes the centralized management form in traditional healthcare systems and constructs the distributed and secure medical data-sharing mechanism to achieve data value maximization. However, the advanced capabilities of quantum algorithms bring a serious threat to current blockchain cryptographic algorithms which are based on classical mathematical difficulties. This paper proposes the first quantum-safe identity-based designated verifier signature (ID-DVS) scheme for blockchain-based Internet of medical things (BIoMT) systems. This scheme is constructed based on the lattice assumption of the short integer solution (SIS) problem, which is believed to resist the quantum attack. The identity mechanism helps to establish a transaction traceability mechanism when this data is shared among different medical institutions. The designated verifier mechanism also prevents unauthorized users from accessing data to improve the security of medical data-sharing processes. Next, this ID-DVS scheme is proved in random oracle model, which can achieve the security properties of anonymity and unforgeability. It also can capture the post-quantum security. Then, the performance analysis of the key size and time consumption are presented, and the results show that this ID-DVS is more efficient than other similar schemes. Therefore, this work supports secure medical data-sharing and protects the privacy of users and medical data.

1. Introduction

Blockchain-enabled Internet of Medical Things (BIoMT) profoundly affects people's lives and health with the gradual increase of wearable health devices [1]. Firstly, blockchain technology helps to establish a distributed medical data-sharing framework among different medical institutions, which replaces the traditional centralized management form and achieves cross-institutional medical data utilization. Then, the BIoMT solves the problems of collecting, storing, sharing, and using massive medical data. However, the security issues with medical data and user privacy in the cross-institutional data-sharing process have gained much attention as more sensitive information is inserted into these medical data. Especially for the sensitive information protection, the users do not want to give non-specified users access to the data. Hence, one-to-one data sharing can effectively prevent the leakage of sensitive information.

Blockchain cryptography has received more attention as it is increasingly essential in most blockchain-based applications [2]. It is relation to the cryptographic algorithms of the symmetric cryptographic, asymmetric cryptographic, hash function, public key infrastructure, Merkle tree, digital signature, and zero-knowledge proof, which are utilized to better adapt to the transaction privacy protection in the blockchain network. These blockchain cryptographic technologies jointly protect transaction security and user privacy. For example, the digital signature is responsible for transaction verification in the consensus process and for establishing links to different blocks [3]. The signature also provides the transaction traceability mechanism when some disputes occur. Especially the DVS is more suitable for one-to-one data-sharing among different BIoMT systems that it can guarantee the non-delegatability of signature. These technologies construct the trust foundation for the blockchain-based network as these NP-hard problem-based cryptographic algorithms cannot be broken through with the current most advanced classic computer. Most of these algorithms are based on RSA and ECC cryptographic theories, but the fundamental problems of large integer factorization and discrete logarithms are weak against the quantum attack [4].

Quantum threat is the main concern in current information systems with the rapid developments of quantum computers and quantum computing. The Grover quantum algorithm can speed up the efficiency

* Corresponding author at: College of Software Engineering, Zhengzhou University of Light Industry, Zhengzhou 450001, China.
E-mail address: lichaoyang@zzuli.edu.cn (C. Li).

https://doi.org/10.1016/j.sysarc.2025.103362
Received 9 December 2024; Received in revised form 13 January 2025; Accepted 6 February 2025
Available online 15 February 2025

of target search, which brings threats to the symmetric cryptographic algorithm, for example: Elliptic Curve Cryptography (ECC), by decreasing the search complexity from $O(N)$ to $O(\sqrt{N})$ [5]. The Shor quantum algorithm can achieve exponential acceleration for large integer factorization [6], which brings threats to the asymmetric cryptographic, for example: RSA. In recent years, post-quantum cryptographic algorithms have gained much attention in the areas of scientific research, finance, and industry [7]. Currently, code-based cryptography, Hash cryptography, lattice cryptography, and multivariate-quadratic-equations cryptography are some famous post-quantum cryptographic (PQC) algorithms. Code-based cryptography was first proposed by McEliece [8], which was constructed by the error correction codes. Although this cryptosystem has a significant anti-quantum attack advantage, its key size disadvantage makes it unsuitable for IoT systems. Hash cryptography was initially introduced by Lamport [9], which was known as the one-way function to provide quantum-proof security. The Merkle tree is another well-known hash-based cryptosystem [10]. These hash-based algorithms are not based on solving hard mathematical problems, but they can obtain the properties of one-wayness, collusion resistance, and preimage resistance. Lattice cryptography is one of the suggested PQC scheme in the NIST call, which was first proposed by Ajtai [11]. Multivariate-quadratic-equations cryptography is another kind of PQC that is based on the complexity of solving multivariate equations [12]. This kind of PQC algorithm suffers from efficiency hardship with the large key size and ciphertext overhead.

This paper focuses on the needs of security and integrity, and proposes a lattice-based ID-DVS scheme to cover the privacy-preserving issues, such as designated verifier, signer's anonymity, and signature non-delegatability in the BIoMT system. The contributions are summarized as follows.

- A lattice-based ID-DVS scheme has been proposed. This is the first ID-DVS scheme which is constructed with the reject sampling in Gaussian distribution and SIS lattice problem. The identity mechanism in this ID-DVS provides transaction traceability for medical data-sharing, and the designed verifier setting protects user privacy as unauthorized users cannot access the transaction.
- The security proof of the proposed ID-DVS scheme is given. In the random oracle model, this ID-DVS scheme can be proved to satisfy the security properties of anonymity and unforgeability. Meanwhile, this ID-DVS scheme can resist the quantum attack with the lattice assumption, which can prevent the quantum adversary in the future quantum computer age.
- The efficiency comparison and performance analysis are presented. The key size, time consumption, and energy consumption are calculated and compared with other similar schemes. The results show that this ID-DVS scheme is more efficient, which can well support secure medical data-sharing among different BIoMT systems.

Next, the related work is given in Section 2, some preliminaries are shown in Section 3, the ID-DVS scheme is proposed in Section 4, the security of the ID-DVS scheme is analyzed and proved in Section 5, the performance analysis is in Section 6, and the conclusion is in Section 7.

2. Related work

This paper mainly focuses on the research and applications of blockchain cryptography in BIoMT. Some reviews of blockchain cryptography for BIoMT, PQC, and lattice-based signature theory about this theme are given in the following subsections.

2.1. Blockchain cryptography for BIoMT

In the BIoMT system, identity authentication, data encryption/decryption, and transaction verification all need blockchain cryptography algorithms to protect privacy security in the medical data-sharing processes. For identity authentication, Jia et al. [13] constructed a privacy-aware authentication model with blockchain and proposed two authentication protocols based on ECC and physically unclonable function algorithm respectively to enhance privacy security in the IoMT ecosystem. Lin et al. [14] proposed a mutual user authentication protocol with the ECC algorithm, which could achieve a legal user authentication in blockchain-based IoMT networking. Chen et al. [15] designed a certificateless aggregate signcryption scheme based on ECC to protect the data privacy in IoT applications, but it could not provide anti-quantum attack security. Han et al. [16] introduced a blockchain based privacy-preserving framework and a public key searchable encryption scheme to strengthen the data traceability. Zou et al. [17] introduced a credential-embedded authentication protocol to protect users' privacy and designed an authenticated key agreement protocol to support bilateral authentication for medical data-sharing through IoMT systems. For data encryption/decryption, Guo et al. [18] presented an attributed-based encryption protocol with a ciphertext policy and set an outsourced online/offline revocable mechanism to guarantee fine-grained access control. Li and Dong et al. [19] gave a keyword-searchable encryption scheme to achieve cross-institution medical data utilization and established an on-chain ledger and off-chain storage model to reduce ledger redundancy. Liu et al. [20] designed a certificateless public key encryption protocol based on high-consumption bilinear pairing, combining the keyword search function to protect medical data in IoMT. Qu et al. [21] introduced an interesting work of quantum blockchain to improve privacy security in IoMT, which utilized the quantum signature and quantum identity authentication to achieve secure medical data-sharing with the quantum cloud. For transaction verification, Mao et al. [22] presented an identity-based aggregated signature scheme for IoMT, which could enable efficient local verification of medical data with a locally verifiable mechanism. Zhang et al. [23] proposed a certificateless signcryption protocol to guarantee privacy security in IoMT, which utilized bilinear pairings and zero-knowledge proof to resist super-level internal adversaries. Li et al. [24] proposed a designated verifier signature scheme and established a cross-chain medical data-sharing framework to support secure and efficient data-sharing among different BIoMT systems.

With the deepening application of blockchain in BIoMT, the research on blockchain cryptographic algorithms applicable to medical data-sharing transactions is also more urgent. Most of these BIoMT systems are also based on RSA and ECC cryptographic algorithms, which are vulnerable to quantum attacks. So it is urgent to seek more secure anti-quantum cryptographic algorithms to equip current BIoMT systems.

2.2. Post-quantum cryptography

PQC utilizes classical computationally hard problems to construct quantum-safe cryptosystems for current information systems. Especially for the sensitive information protection of medical data in BIoMT systems, the practical application of PQC is important and necessary. For code-based cryptography, Thiers et al. [25] presented a decoding algorithm based on the q-ary codes, which could achieve low complexity and anti-quantum security. Alahmadi et al. [26] introduced a signature scheme with error-correcting codes for blockchain-based networks and utilized bounded distance decoding for signature verification. For hash cryptography, Punithavathi et al. [27] established a double-layer encryption framework and proposed a crypto hash algorithm to resist the malware attack in medical data-sharing processes in the IoMT system. Kuznetsov et al. [28] gave the performance analysis of the hashing algorithm in blockchain-based systems and compared it with other related hashing algorithms to show its efficiency and practice. For lattice cryptography, Ye et al. [29] designed a traceable ring signature scheme based on lattice assumption for IoMT, which could obtain tag-linkability and exculpability in a random oracle model. Bagchi et al. [30] utilized the ring LWE problem to construct an

Table 1
Lattice-based schemes comparison.

Ref.	Lattice problem	Advantage	Limitation
Kim et al. [33]	NTRU	Key encapsulation; Randomness-recovery; Encoding	Centralized KGC; Key escrow; Chosen ciphertext attack weak
Yu et al. [35]	NTRU and SIS	Certificateless, Ring signature	Private key management
Li and Jiang et al. [34]	ring-LWE and SIS	Non-delegatability; Bimodal Gaussians	Centralized KGC; Key escrow
Yao et al. [36]	ring-LWE and ring-ISIS	Ring analog; Authenticate ciphertext	Centralized KGC; Key escrow
Zhang et al. [37]	ring-LWE and SIS	Non-delegatability; Chameleon hash	Centralized KGC; Key escrow
Zhang and Sun et al. [38]	ring-LWE	Re-signature; Semi-trusted proxy; Signature evolution	Centralized KGC; Key escrow; Double time consumption

aggregate signature scheme and applied this scheme to the Internet of drones for privacy preservation. For multivariate-quadratic-equations cryptography, Shim et al. [31] proposed a post-quantum signature with multivariate-quadratic-equations, which supported the dramatic online signing for cryptographic systems. These four PQC proposals are not only generally used for creating encryption/decryption and digital signature algorithms, but also for key exchange and authentication cryptosystems in the not-too-distant future.

This paper plans to utilize lattice theory to construct a PQC signature algorithm, as the digital signature plays an essential roles in transaction signature, blockchain system consistency, and data ownership confirmation in BIoMT systems.

2.3. Lattice-based signature theory

Lattice cryptography serves as one promising PQC theory that has gained much attention in recent years. Its security is also based on some NP-hard problems, such as shortest vector problem (SVP), shortest independent vectors problem (SIVP), closest vector problem (CVP), short integer solution (SIS), learning with errors (LWE), bounded distance decoding problem (BDD), and so on [32]. The Number Theory Research Unit (NTRU) algorithm is based on SVP or SIVP, which is designed with the polynomial ring. The scheme in the Refs. [19] is based on this mechanism. Kim et al. [33] introduced a key encapsulation mechanism with the NTRU lattice, which could resist significant cryptanalytic attacks in current information systems. The LWE is a CVP in which the hardness is solving linear equations with noise. The scheme in the Refs. [29] is based on this mechanism. Li and Jiang et al. [34] proposed a group signature scheme with the SIS lattice problem, which had been applied to the IoMT system with blockchain technology for secure medical data-sharing. Yu et al. [35] designed an NTRU-based certificateless ring signature for electronic voting, which could obtain the properties of quantum immunity, unconditional anonymity, and unforgeability. The ring-LWE is a variant of LWE that has more strengthened security properties. The schemes in the Refs. [30] are based on this mechanism. Yao et al. [36] designed a public-key authenticated encryption protocol with ring-LWE in the ideal lattice, which also could achieve keyword search ability in cloud computing. Zhang et al. [37] proposed a DVS scheme with the chameleon hash and without trapdoors, which could achieve non-delegatability. Zhang and Sun et al. [38] presented an ID-DVS scheme with a function of signature evolution, which also added the proxy and re-signature functions. The simple comparisons of these lattice-based schemes are shown in Table 1.

As in BIoMT, the protection of sensitive information in medical data is essential in the medical utilization processes among different medical institutions. Meanwhile, the threats to classical cryptographic algorithms from quantum computers should be taken more seriously. Therefore, This paper addresses security and privacy issues related to system users and medical data by proposing a quantum-safe ID-DVS scheme to strengthen the security of medical data-sharing in BIoMT systems.

3. Preliminaries

The lattice theories, ID-DVS scheme model, and security model have been presented in this section.

3.1. Lattice theories

Definition 1 (*Lattice [39]*)**.** Let $v_1, \ldots, v_n \in \mathbb{R}^m$ be a set of linearly independent vectors. The lattice Λ_L generated by $v_1, \ldots, v_n$ refers to the set formed by linear combinations of vectors $v_1, \ldots, v_n$.

$$\Lambda_L = \{a_1 v_1 + a_2 v_2 + \cdots + a_n v_n : a_1, a_2, \cdots, a_n \in \mathbb{Z}\} \tag{1}$$

Here, the matrices $A = (a_1, \ldots, a_m) \subset \mathbb{R}^{n \times m}$ is the coefficient matrix of lattice Λ, where the dimension n and rank m of this lattice satisfy $m = O(n \log q)$.

Definition 2 (*q-ary Lattice [39]*)**.** Eq. (1) is the "q-ary" lattice, which is constructed by a matrix $\mathcal{A} \in \mathbb{Z}_q^{n \times m}$, a prime number q, and a vector $\mu \in \mathbb{Z}_q^n$.

$$\begin{aligned} \Lambda^{\perp}(A) &= \{x \in \mathbb{Z}^m | \mathcal{A}x = 0 \mod q \ for \ x \in \mathbb{Z}^m\} \\ \Lambda_{\mu}^{\perp}(A) &= \{x \in \mathbb{Z}^m | \mathcal{A}x = \mu \ mod \ q \ for \ x \in \mathbb{Z}^m\} \end{aligned} \tag{2}$$

Definition 3 (*Gaussian Distribution [40]*)**.** The Gaussian distribution is $\rho_{c,\sigma}(x) = exp(\frac{-(x-c)^2}{2\sigma^2})$, where $\sigma \in \mathbb{R}$ is the standard deviation, $c \in \mathbb{R}$ is the center, and $x \in \mathbb{R}$ is vector. More generally, it can be defined as $\rho_{c,\sigma}(x) = exp(\frac{-\|x-c\|^2}{2\sigma^2})$ with $x, c \in \mathbb{R}^n$. When the center $c = 0$, it becomes $\rho_{\sigma}(x)$. Meanwhile, $D_{\sigma}(x) = \rho_{\sigma}(x)/\rho_{\sigma}(\mathbb{Z})$ is discrete Gaussian distribution over $\mathbb{Z}$ and $D_{\sigma}(x) = \rho_{\sigma}(x)/\rho_{\sigma}(\mathbb{Z}^m)$ is the general situation over $\mathbb{Z}^m$.

Definition 4 ($\mathfrak{R} - SIS_{q,n,m,\beta}^{\kappa}$ *Problem [40]*)**.** $\mathfrak{R} - SIS_{q,n,m,\beta}^{\kappa}$ is defined to find a non-zero $v \in \mathfrak{R}_q^m$ which satisfy $Av = 0$, where $\mathfrak{R}$ a ring, κ is a distribution over $\mathfrak{R}_q^{n \times m}$, $A \in \mathfrak{R}_q^{n \times m}$, and $\|v\|_2 \leq \beta$.

Definition 5 ($SamplePre(A, T, \sigma, y)$ *[40]*)**.** Given a matrix $A \in Z_q^{n \times m}$, a trapdoor basis T of lattice $\Lambda^{\perp}(A)$, $\sigma \geq L \cdot \omega(\sqrt{logn})$, and a random vector y, $SamplePre(A, T, \sigma, y)$ can derive a non-zero vector $e \in Z_q^m$, which satisfy $Ae = y \ mod \ q$. Here, $\|e\| \leq \sigma\sqrt{m}$.

3.2. Model descriptions

The scheme model and security model are given in this subsection, and they provide the formal definition of an ID-DVS scheme.

(1) Scheme model

For an ID-DVS scheme, it is mainly composed of five polynomial time algorithms.

- **Setup**(1^n): Input the security parameter n, key generation center (KGC) outputs the system parameters pp and system master secret key msk.
- **KeyGen.**(ID_a, ID_b, pp, msk): Input the identities ID_a and ID_b of the signer and designated verifier, pp, and msk, KGC generates the key pairs (pk_a, sk_a) and (pk_b, sk_b) respectively.
- **Sign**($pp, sk_a, pk_a, pk_b, \mu$): Input the message μ, pp, (pk_a, sk_a), the designated verifier's public key pk_b, the signer generates an ID-DVS signature (e, μ).
- **Verify**(sk_b, pk_b, pk_a, μ, e): Input (e, μ), pp, (pk_b, sk_b), and the signer's public key pk_a, the designated verifier checks the legality of the ID-DVS signature.
- **Simulation**($pp, sk_b, pk_b, pk_a, \mu$): Input the message μ, pp, (pk_b, sk_b), the singer's public key pk_a, the designed verifier generates another ID-DVS signature (e', μ).

(2) Security model

An ID-DVS scheme must satisfy the correctness, anonymity, and unforgeability. The correctness can be verified according to the verification process. The anonymity and unforgeability should be proved in the random oracle model as shown in the following Definitions 6 and 7, respectively. Note that only by passing this certification can it be shown that the designed ID-DVS scheme is safe. Next, the security proof model is constructed with a query-respond game, where an adversary Eve E performs the query and a challenger Charlie C performs the response.

Definition 6 (*Anonymity*)**.** If an adversary can make the right guess whether the signature is signed by the signer or the designated verifier with the adaptive selective identity attack in the random oracle model, he wins this round of the query-respond game. Detailed query-respond processes between A and C are shown as follows.

- *Initialize*: C performs the **Setup**(1^n) algorithm to obtain the system parameters pp and the master secret key msk. Then, he exposes pp and keeps msk in secret.
- *Query*: E can perform enough polynomial times of queries on the random oracle. Here, the hash function, secret key, and signature are all the query targets. E can perform queries on the non-target user's identity ID^* or the non-target message μ^*. C responds to the answers to the queries if the answers already exist. Otherwise, C executes the signature algorithms of **KeyGen.** or **Sign** to generate new answers to E's queries.
- *Challenge*: E selects two target system users' identities ID_{i_0} and ID_{i_1} and queries on the signature about these two identities. Next, C randomly chooses the identity ID_{i_b}, $b \in 0, 1$ as the signer and the other one as the designated verifier, derives the ID-DVS (e, μ^*) according to the processes of **KeyGen.** and **Sign** algorithms, and sends it back to E.
- *Guess*: E performs the guess of b^*. If $b^* = b$, E wins this game. Here the guess successful rate of E can be defined as shown in Eq. (3).

$$Adv_A^{Anon} = Pr[E\ successed.] \tag{3}$$

This anonymity increases the probability that the adversary will fail to attack the signature because he cannot determine whether the signer or the designated verifier is the real signer. Meanwhile, the designated verifier cannot prove to third parties that this signature is valid. This mechanism can protect user privacy in medical data-sharing transactions and prevent the designated verifier from authorizing other users to access the signature.

Definition 7 (*Unforgeability*)**.** If an adversary can forge a valid signature with the adaptive selective message attack in the random oracle model, a challenger can derive another valid signature and solve the lattice assumption with these two signatures. Here, the successful probability of this challenger is non-negligible. Detailed query-respond processes between E and C are shown below.

Table 2
System parameters.

Notation	Meaning
q	One large prime with $q = q(n) \geq 3$
n, m	The dimension of key matrix, and $m \geq 5nlogq$
κ	The system security parameter
$\mathbb{Z}$	The integer matrix/vector set for system keys
σ	A system parameter with $\sigma = L \cdot \omega(\sqrt{logn})$
mpk	The group public key
msk	The group muster secret key
ID_i	The user identity
H_1, H_2	The cryptographic Hash function
D_σ^m	The bimodal Gaussian distribution
σ	The standard deviation for D_σ^m
μ	The message to be signed
pk, sk	The public and private keys for system users

- *Initialize*: C performs the **Setup**(1^n) algorithm to obtain the system parameters pp and the master secret key msk. Then, he exposes pp and keeps msk in secret.
- *Query*: E can perform enough polynomial times of queries on the random oracle. Here, the hash function, secret key, and signature are all the query targets. E can perform queries on the non-target user's identity ID^* or the non-target message μ^*. C responds to the answers to the queries if the answers already exist. Otherwise, C executes the signature algorithms of **KeyGen.** or **Sign** to generate new answers to E's queries.
- *Forge*: E utilizes these enough queried answers to generate a valid signature (e, μ^*) for the target user's identity ID^* and message μ^*, and exposes this signature.
- *Challenge*: C also can execute the signature processes legally and derive another valid signature (e^*, μ^*) for the target user's identity ID^* and message μ^*. Then, C utilizes these two valid signatures about the same message μ^* to solve the $\mathbb{Z} - SIS^{\kappa}_{q,n,m,\beta}$ instance.
- *Analyze*: This step analyses two points. One is the probability that C can find a solution for the $\mathbb{Z} - SIS^{\kappa}_{q,n,m,\beta}$ instance, and the other one is the probability that E successfully generates a valid ID-DVS signature. Here the successful rate of E can be defined as shown in Eq. (4).

$$Adv_A^{Forge} = Pr[E\ successed.] \tag{4}$$

This unforgeability ensures that no one other than the signer can generate a legitimate signature, thus improving the security of the medical data-sharing process among different BIoMT systems.

4. The ID-DVS scheme

This ID-DVS scheme is constructed with the lattice assumption of $\mathfrak{R} - SIS^{\kappa}_{q,n,m,\beta}$. To improve the computational efficiency, the lattice assumption is reduced from $\mathfrak{R}$ to $\mathbb{Z}$, and the new lattice assumption $\mathbb{Z} - SIS^{\kappa}_{q,n,m,\beta}$ does not decrease the hardness. The parameter definitions are shown in Table 2. This scheme mainly contains five algorithms of $Setup$, $KeyGen.$, $Sign$, $Verify$, and $Simulation$. The simple framework of this ID-DVS scheme is shown in Fig. 1, and details of these algorithms are described as follows.

4.1. Setup

Some system parameters are preset according to the setting principle in Ref. [41], where n is the security parameter, q is a prime number which satisfies with $q = q(n) \geq 3$, m is a positive integer which satisfies $m \geq 5n\ log\ q$, $L = O(\sqrt{n\ log\ q})$, and $\sigma \geq L \cdot \omega(\sqrt{logn})$.

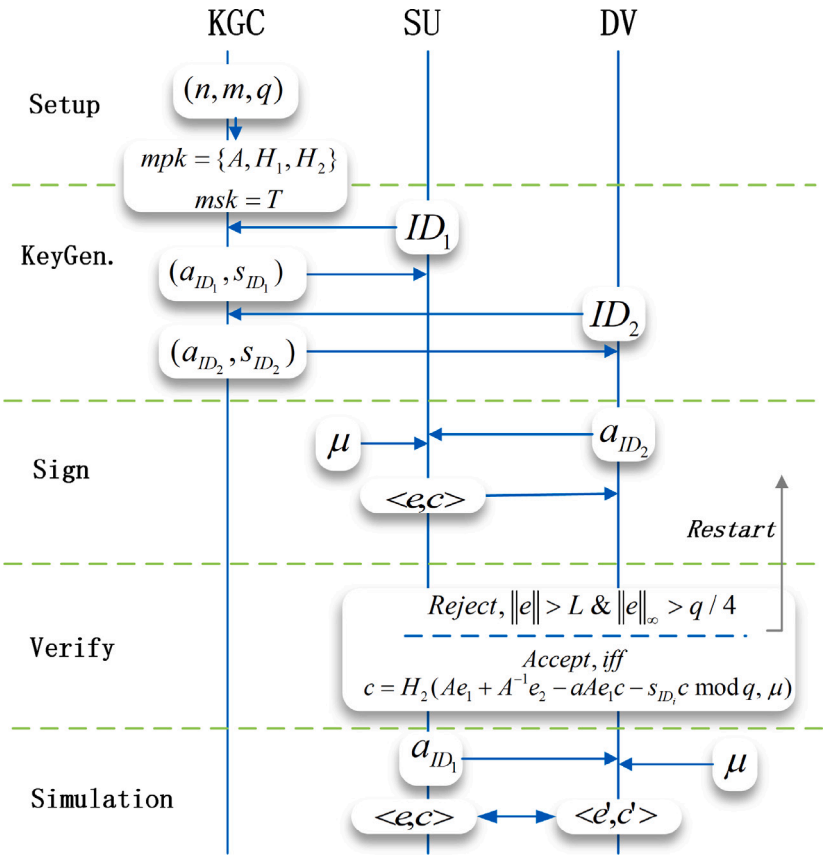


Fig. 1. The simple framework of ID-DVS scheme.

(1) KGC generates a matrix $mpk = A \in Z_q^{n\times m}$ with the former system parameters by the Trapdoor generation ($TrapGen.(1^n)$) algorithm, which is an approximate random distribution matrix. Then, a basis $T \in Z_q^{m\times m}$ is derived from $\Lambda^{\perp}(A)$ by $TrapGen.(1^n)$ as $\|\tilde{T}\| \le L$;
(2) Chooses $H_1, H_2 : \{0,1\}^* \to Z_q^n$;
(3) Outputs $pp = \{A, H_1, H_2\}$ as public system parameters;
(4) Serves $mpk = A$ as the master public key and $msk = T$ as the master secret key.

4.2. KeyGen

Given the system parameter pp and user's identity ID_i.

(1) KGC computes $a_{ID_i} = H_1(ID_i) \in Z_q^n$;
(2) Computes $s_{ID_i} \leftarrow SamplePre(A, T, a_{ID_i}, \sigma) \in Z_q^m$, where $\sigma \ge \|\tilde{T}\|\omega(\sqrt{log\ m})$, $a_{ID_i} mod q = A \cdot s_{ID_i}$, and $\|s_{ID_i}\| \le \sigma\sqrt{m}$;
(3) Outputs $pk = a_{ID_i}$ as the public key and $sk = s_{ID_i}$ as the secret key for system user with ID_i.

For the signer and designated verifier in this ID-DVS scheme, the signer's key pair is set as $(pk_1, sk_1) = (a_{ID_1}, s_{ID_1})$ and the designated verifier's key pair is set as $(pk_2, sk_2) = (a_{ID_2}, s_{ID_2})$. Then, they will work together to generate a legitimate ID-DVS with the following steps.

4.3. Sign

Given the system parameter pp and message μ.

(1) The signer ID_1 randomly chooses $x \in D_\sigma^m$;
(2) Computes $c = H_2(Ax + a_{ID_2} \ mod \ q, \mu)$;
(3) Utilizes his secret key sk to compute $e = x + s_{ID_1}$;
(4) Output the signature $< e, c >$ with probability $min(\frac{D_\sigma^m(e)}{M D_{s_{ID_1}c,\sigma}^m(e)}, 1)$; otherwise, restart.

This is a probabilistic algorithm, and M is some fixed positive real that is set large enough to ensure that the preceding probability is always at most 1. If there is no data output, the signer will repeat these sign processes until a legal ID-DVS is generated.

4.4. Verify

When receives the ID-DVS from the signer, the designated verifier utilizes pp, the signer's private key a_{ID_1}, and his private key $sk_2 = s_{ID_2}$ to verify the legality of (e, c) with message μ.

(1) The designated verifier checks $\|e\| > L$, and rejects it;
(2) Checks $\|e\|_\infty > q/4$, and rejects it;
(3) When the former conditions hold, he verifies whether $c = H_2(A(e + s_{ID_2}) - a_{ID_1} \ mod \ q, \mu)$ holds or not. Iff this condition holds, he accepts this signature; Otherwise, he rejects it.

4.5. Simulation

This subsection presents the generation simulation of a new ID-DVS performed by the designated verifier. According to the former generation processes, he can derive a legal ID-DVS with the same message μ.

(1) Selects a random vector $x' \leftarrow D_\sigma^m$
(2) Computes $c' = H(Ax' + a_{ID_1} \ mod \ q, \mu)$ with the system public key A and the same message μ;

(3) Computes $e' = x' + s_{ID_2}$;

(4) Outputs the ID-DVS (e, c') with probability $\min(\frac{D_\sigma^m(e')}{MD_{s_{ID_2}c',\sigma}(e')}, 1)$, otherwise he restarts this algorithm.

Here, the simulated signature (e', c') is indistinguishable from the former generated signature (e, c) with the same message μ. This is the inherent quality of the DVS scheme which can prevent attacks from unauthorized verifiers. It can improve the security of cross-institution medical data-sharing through the BIoMT system.

5. Security analysis

The security analyses of the correctness, anonymity, and unforgeability of the proposed ID-DVS scheme have been given in this section.

5.1. Correctness

According to the verification steps in *Verify* algorithm, a valid ID-DVS shall satisfy three conditions. From the signature generation process, (e, c) satisfy $\|e\| \leq L$ and $\|e\|_\infty \leq q/4$ which are easily verified. The third condition $c \leftarrow H_2(A(e + s_{ID_2}) - a_{ID_1} \ mod \ q, \mu) = H_2(Ax + a_{ID_2} \ mod \ q, \mu)$ holds which can be verified by the equation $A(e + s_{ID_2}) - a_{ID_1} = Ax + a_{ID_2} \ mod \ q$. Eq. (5) shows the detailed verification processes.

$$\begin{aligned} A(e + s_{ID_2}) - a_{ID_1} &= A(x + s_{ID_1} + s_{ID_2}) - a_{ID_1} \\ &= Ax + As_{ID_1} + As_{ID_2} - a_{ID_1} \\ &= Ax + a_{ID_1} + a_{ID_2} - a_{ID_1} \\ &= Ax + a_{ID_2} \end{aligned} \tag{5}$$

Meanwhile, the signature (e', c') simulated by the designated verifier also can be verified by the signer as the conditions of $\|e'\| \leq L$, $\|e'\|_\infty \leq q/4$, and the equation $c' \leftarrow H_2(A(e' + s_{ID_1}) - a_{ID_2} \ mod \ q, \mu) = H_2(Ax + a_{ID_1} \ mod \ q, \mu)$ holds, which is shown in Eq. (6) holds.

$$\begin{aligned} A(e' + s_{ID_1}) - a_{ID_2} &= A(x + s_{ID_2} + s_{ID_1}) - a_{ID_2} \\ &= Ax + As_{ID_2} + As_{ID_1} - a_{ID_2} \\ &= Ax + a_{ID_2} + a_{ID_1} - a_{ID_2} \\ &= Ax + a_{ID_1} \end{aligned} \tag{6}$$

5.2. Anonymity

Theorem 1. *The proposed ID-DVS can capture anonymity with lattice assumption $\mathbb{Z} - SIS^{\kappa}_{q,n,m,\beta}$ if no adversary can correctly distinguish the real signer with the non-negligible probability.*

Proof. According to Definition 6, E attempts to distinguish the real signer by performing the queries on Hash, secret key, and sign algorithms under the adaptively chosen identity attack. Here, E can execute enough times queries on three algorithms to obtain information about the non-target identity in polynomial time. Meanwhile, the probability that E wins one round query-respond game is defined as at least ζ. Then, C generates a signature with the target identity ID^* and lets E guess the real signer. Detailed query-respond processes are shown as follows.

- *Initialize*: C executes the *Setup* algorithm to generate the system parameters (n, m, q, k, σ) and sends them to E.
- *Query*: E adaptively chooses the non-target identity to query with C.
  - H_1 *query*: E adaptively chooses the non-target identity ID_i to query on H_1 function. C owns a list $List_{H_1}$ to store (ID_i, a_{ID_i}). When he obtains the query, he first searches the list $List_{H_1}$ whether the identity ID_i is queried or not. If exists, the result (ID_i, a_{ID_i}) is returned back to E. If not, C computes the corresponding $a_{ID_i} = H_1(ID_i)$, returns the result (ID_i, a_{ID_i}) back to E, and records this result into the list $List_{H_1}$.
  - H_2 *query*: E adaptively chooses a message μ_i to query on H_2 function. C owns a list $List_{H_2}$ to store (μ_i, c_i). When he obtains the query, he first searches the list $List_{H_2}$ whether the identity μ_i is queried or not. If exists, the result (μ_i, c_i) is returned back to E. If not, C randomly selects $x \in D_\sigma^m$, computes the corresponding $c_i = H_2(Ax \ mod \ q, \mu_i)$, returns the result (μ_i, c_i) back to E, and records this result into the list $List_{H_2}$.
  - *Secret key query*: E adaptively chooses the non-target identity ID_i to query on secret key. C owns a list L_K to store (s_{ID_i}, ID_i). When he obtains the query, he first searches the list L_K whether the identity ID_i is queried or not. If exists, the result (s_{ID_i}, ID_i) is returned back to E. If not, C obtains (ID_i, a_{ID_i}) from the list $List_{H_1}$ or regenerates it firstly. Next, C computes the corresponding $s_{ID_i} \leftarrow Samplepre(A, T, a_{ID_i}, \sigma)$, returns the result (s_{ID_i}, ID_i) back to E, and records this result into the list L_K.
  - *Signature query*: E adaptively chooses a message μ_i to query on signature. C owns a list L_S to store (e, c_i). When he obtains the query, he first searches the list L_S whether the message μ_i is queried or not. If exists, the result (e, c_i, μ) is returned back to E. If not, C obtains (μ_i, c_i) from the list $List_{H_2}$ or regenerates it firstly. Next, C computes the corresponding $e_1 = x + s_{ID_1}$, where ID_1 is set as the signer and ID_2 is set as the designated verifier. Then, he returns the result (e, c_i) back to E, and records this result into the list L_S.
- *Challenge*: E randomly selects two system users' identities ID_{i_0} and ID_{i_1} which are not queried before. Next, he sends these two target identities to C. C randomly selects the identity ID_{i_b}. $b \in 0, 1$ as the signer and the other one as the designated verifier, and derives the ID-DVS (e, c_{i_0}) and (e', c_{i_1}) according to the ID-DVS processes, and sends it back to E.
- *Guess*: E utilizes the formerly obtained messages and performs the guess of signer b^*. C confirms whether $ID_{i_{b^*}}$ is the real signer or not. If correct, E wins this game.
- *Analyze*: Because the parameter x is randomly selected with the same Gaussian distribution D_σ^m, the statistical distance of c_{i_0} and c_{i_1} is indistinguishable. Therefore, the statistical distance of these two signatures (e, c_{i_0}) and (e', c_{i_1}) generated by $e = x + s_{ID_{i_0}}$ and $e' = x + s_{ID_{i_1}}$ is also indistinguishable. This is to say that E cannot distinguish the correct signer of these two signatures and the proposed ID-DVS can guarantee the signer's anonymity.

5.3. Unforgeability

Theorem 2. *The proposed ID-DVS can capture unforgeability with lattice assumption $\mathbb{Z} - SIS^{\kappa}_{q,n,m,\beta}$ if no adversary can generate a valid signature with the non-negligible probability.*

Proof. According to Definition 7, E attempts to derive a valid signature by performing the queries on Hash, secret key, and sign algorithms under the adaptively chosen message attack. Here, E can execute enough time queries on three algorithms to obtain information about the non-target message in polynomial time. Meanwhile, the probability that E wins one round query-respond game is defined as at least ξ. Then, C attempts to utilize this forged signature to solve the lattice instance $\mathbb{Z} - SIS^{\kappa}_{q,n,m,\beta}$. Detailed query-respond processes are shown as follows.

- *Initialize*: C executes the *Setup* algorithm to generate the system parameters (n, m, q, k, σ) and sends them to E.
- *Query*: E adaptively chooses the non-target messages to query with C.
  - H_1 *query*: E adaptively chooses the identity ID_i to query on H_1 function. C owns a list $List_{H_1}$ to store (ID_i, a_{ID_i}). When he obtains the query, he first searches the list $List_{H_1}$ whether the identity ID_i is queried or not. If exists, the result (ID_i, a_{ID_i}) is returned back to E. If not, C computes the corresponding $a_{ID_i} = H_1(ID_i)$, returns the result (ID_i, a_{ID_i}) back to E, and records this result into the list $List_{H_1}$.
  - H_2 *query*: E adaptively chooses the non-target message μ_i to query on H_2 function. C owns a list $List_{H_2}$ to store (μ_i, c_i). When he obtains the query, he first searches the list $List_{H_2}$ whether the identity μ_i is queried or not. If exists, the result (μ_i, c_i) is returned back to E. If not, C randomly selects $x \in D_\sigma^m$, computes the corresponding $c_i = H_2(Ax \ mod \ q, \mu_i)$, returns the result (μ_i, c_i) back to E, and records this result into the list $List_{H_2}$.
  - *Secret key query*: E adaptively chooses the identity ID_i to query on secret key. C owns a list L_K to store (s_{ID_i}, ID_i). When he obtains the query, he first searches the list L_K whether the identity ID_i is queried or not. If exists, the result (s_{ID_i}, ID_i) is returned back to E. If not, C obtains (ID_i, a_{ID_i}) from the list $List_{H_1}$ or regenerates it firstly. Next, C computes the corresponding $s_{ID_i} \leftarrow Samplepre(A, T, a_{ID_i}, \sigma)$, returns the result (s_{ID_i}, ID_i) back to E, and records this result into the list L_K.
  - *Signature query*: E adaptively chooses the non-target message μ_i to query on signature. C owns a list L_S to store (e, c_i). When he obtains the query, he first searches the list L_S whether the message μ_i is queried or not. If exists, the result (e, c_i, μ) is returned back to E. If not, C obtains (μ_i, c_i) from the list $List_{H_2}$ or regenerates it firstly. Next, C computes the corresponding $e = x + s_{ID_1}$, where ID_1 is set as the signer and ID_2 is set as the designated verifier. Then, he returns the result (e, c_i) back to E, and records this result into the list L_S.
- *Forge*: E can respectively perform q_{H_1}, q_{H_2}, q_K, and q_S queries on the algorithms of H_1 Hash, H_2 Hash, secret key, and sign until obtaining enough information. With these query results, E can forge a valid signature (e^*, c_i^*) about the target message μ^*. Then, E returns it to C.
- *Challenge*: C first confirms that the signature secret key about identity ID_i^* is not queried, the signature about message μ^* is not queried, and the public keys of (a_{ID_1}, a_{ID_2}) is derived by C. Then, C utilizes this forged signature (e^*, c_i^*) to solve the $\mathbb{Z} - SIS_{q,n,m,\beta}^{\kappa}$ instance $Ae^* = 0 \ mod q$. He checks the list $List_{H_2}$ and quits this game if that (μ_i^*, c_i^*) does not exist. Otherwise, he utilizes the same random vector $x \in D_\sigma^m$ and derives a new valid signature (e^{**}, c_i^{**}) according to the sign algorithm with the following two equations.

$$\begin{cases} c_i^* \leftarrow H_2(A(e^* + s_{ID_2}) - a_{ID_1} \ mod \ q, \mu) \\ \qquad = H_2(Ax^* + a_{ID_2} \ mod \ q, \mu^*) \\ c_i^{**} \leftarrow H_2(A(e^{**} + s_{ID_2}) - a_{ID_1} \ mod \ q, \mu) \\ \qquad = H_2(Ax^{**} + a_{ID_2} \ mod \ q, \mu^*) \end{cases} \tag{7}$$

According to the verification algorithm, it has:

$$\begin{cases} A(e^* + s_{ID_2}) - a_{ID_1} = Ax^* + a_{ID_2} \ mod \ q \\ A(e^{**} + s_{ID_2}) - a_{ID_1} = Ax^{**} + a_{ID_2} \ mod \ q \end{cases} \tag{8}$$

Then, it has:

$$\begin{cases} Ae^* - a_{ID_1} = Ax^* \ mod \ q \\ Ae^{**} - a_{ID_1} = Ax^{**} \ mod \ q \end{cases} \tag{9}$$

It also has:

$$A(e^* - e^{**}) = A(x^* - x^{**}) \ mod \ q \tag{10}$$

Due to $e_1^* - e_1^{**} = x^* - x^{**} \neq 0 \ mod \ q$, it can derive

$$A(e^* - e^{**}) = 0 \ mod \ q \tag{11}$$

Here, C quits this game if $e_1^* - e_1^{**} = 0$. Otherwise, $e_1^* - e_1^{**}$ is a solution of SIS instance $Ae = 0 \ mod q$.

- *Analyze*: There are two situations in which C quits the query-respond game. Therefore, the success rate is $\frac{\xi}{q_{H_1} + q_{H_2} + q_K + q_S}$. This probability is negligible with the increase in query times. In addition, the lattice assumption is a non-deterministic polynomial problem that cannot be broken with current classical or quantum computational conditions.

From former theoretical security proof, the proposed ID-DVS scheme can obtain correctness, anonymity, and unforgeability. Meanwhile, this ID-DVS scheme can also satisfy the post-quantum security as it is constructed with lattice assumption. Compared with other classical cryptography algorithm-based BIoMT systems, this scheme can well guarantee anti-quantum security for medical data-sharing among different medical institutions.

6. Performance analysis

The performance analyses of this ID-DVS scheme from the theory and simulation aspects have been given in this section.

6.1. Theoretical analysis

In this phase, six items are selected for comparison, where the assumption is the lattice assumption, mpk is the system master key, msk is the system private key, pk is the system user's public key, sk is the system user's private key, and signature is the size of the proposed signature. The comparison results are shown in Table 3. Firstly, the schemes in Ref. [24,34] and this proposed scheme are based on the problem of $\mathbb{Z} - SIS$, the schemes in Ref. [29,30] are based on Ring-LWE, and the scheme in Ref. [35] is based on NTRU lattice. Secondly, the size of mpk, msk, pk, and sk is in relation to the parameters of m, n, and q. Then, the size of the signatures in these schemes is also with the effort scalar factor σ and ring number N. In Ref. [29] and Ref. [30], the signature size increases with the ring number increasing which will affect the efficiency of the signature algorithm. Here, there are no results about mpk and msk in Ref. [24] and Ref. [24,34] as the algorithms of *Setup* and *KeyGen.* in these two references are not divided. These theoretical comparisons and analyses show that the proposed ID-DVS has certain advantages over those in the other five related schemes.

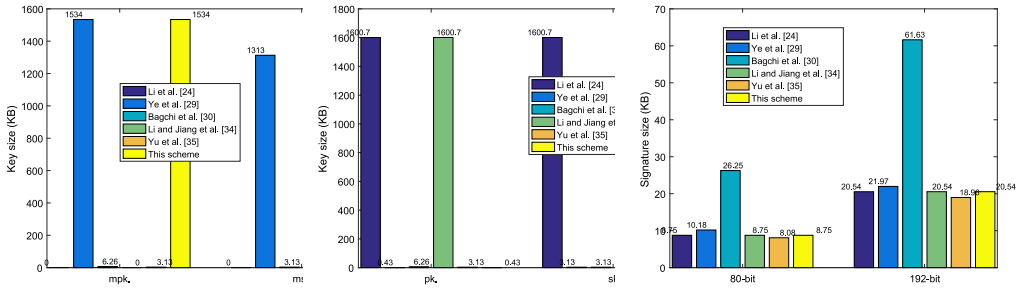
Meanwhile, the theoretical analyses of the times costs of *Setup*, *KeyGen*, *Sign*, and *Verify* algorithms are presented in Table 4, where T_{Trap} represents the time costs of trapdoor algorithm, T_{Sam} represents the Gaussian Samplepre algorithm, T_{Mul} represents the scalar multiplication algorithm, and T_H represents the hash algorithm. Here, some high-time-consuming algorithms and steps have been selected for comparison, and some other addition or modular operations that are low-time-consuming are not considered. The *Setup* and *KeyGen* algorithms can be prepared in advance, which can save time and costs. So the time-consuming in other algorithms will affect the efficiency more. In the proposed ID-DVS scheme, the time costs of *KeyGen* and *Sign* algorithms are lower than the other schemes. From these comparison results, it can derived that the proposed ID-DVS has certain advantages over those in the other five related schemes.

Table 3
Keys size comparison.

Ref.	Assumption	mpk	msk	pk	sk	signature
Li et al. [24]	$\mathbb{Z}-SIS$	–	–	*mnlog2q*	*mnlog2q*	*2mlog(12σ)*
Ye et al. [29]	Ring-LWE	*mnlogq*	*n(m-n)logq*	*nlogq*	*mlogq*	*2mlog(12σ)+Nlog3*
Bagchi et al. [30]	$\mathbb{Z}-SIS$	*2mlogq*	*mlogq*	*2mlogq*	*mlogq*	*2Nmlog(12σ)*
Li and Jiang et al. [34]	Ring-LWE	–	–	*mnlog2q*	*mnlog2q*	*2mlog(12σ)*
Yu et al. [35]	NTRU	*mlogq*	$4n^2logq$	*mlogq*	*2nlogq*	*2mlog(2σ)*
This scheme	$\mathbb{Z}-SIS$	*mnlogq*	*mmlogq*	*nlogq*	*mlogq*	*2mlog(12σ)*

Table 4
Time costs comparison.

Items	Setup	KeyGen.	Sign	Verify
Li et al. [24]	–	$2T_{Trap}$	$2T_{Mul}+T_H$	$3T_{Mul}+T_H$
Ye et al. [29]	T_{Trap}	$T_{Sam}+T_{Mul}$	$T_{Sam}+7T_{Mul}+3T_H$	$5T_{Mul}+2T_H$
Bagchi et al. [30]	$2T_{Trap}$	$3NT_{Mul}+NT_H$	$3NT_{Mul}+NT_H$	$2T_{Mul}+T_H$
Li and Jiang et al. [34]	–	$2NT_{Trap}$	$5T_{Mul}+2T_H$	$3T_{Mul}+T_H$
Yu et al. [35]	T_{Trap}	$NT_{Sam}+2NT_{Mul}+2NT_H$	$3T_{Mul}+T_H$	$6T_{Mul}+4T_H$
This scheme	T_{Trap}	$T_{Sam}+T_H$	$2T_{Mul}+T_H$	$4T_{Mul}+T_H$



(a) mpk and msk comparison (b) pk and sk comparison (c) Signature size comparison

Fig. 2. Keys size comparison (80-bit security level with parameter setting of $n = 512$ $m = 3549$, $q = 2^{23}$, and $\sigma = 2^{30}$; 192-bit security level with parameter setting of $n = 1024$ $m = 8323$, $q = 2^{27}$, and $\sigma = 2^{30}$).

6.2. Simulation evaluation

To more clearly compare the advantages and disadvantages of different schemes, the ID-DVS scheme has been executed with the Matlab 2016b on a Windows 11 desktop with Intel(R) Core(TM) i5-1240P 1.90 GHz and 16G RAM. Here, the system parameters are selected according to those in Ref. [39], which are presented in the tile of Fig. 2. Meanwhile, the signature size in Ref. [29] and Ref. [30] is in relation to the ring number N which is preset as $N = 3$. With the ring number increasing, the signature size in these two references will increase. From the comparison results, the key size of pk and sk in this ID-DVS has a certain advantage over other schemes. Although mpk and msk are equal to or bigger than that in other schemes, this ID-DVS is constructed with the lattice assumption $\mathbb{Z}-SIS$ which can provide a strong security guarantee. As the signing process is the main part of a signature scheme, the signature size is the smallest compared with these similar schemes, which can improve the algorithm execution efficiency.

Then, the simulation of the time-consuming and energy-consuming are shown in Fig. 3 and Fig. 4, respectively. Here, the time-consuming of T_{Trap}, T_{Sam}, T_{Mul}, T_H algorithms are set according to the principal in Ref. [40]. Then, the time-consuming results in Table 4 are calculated, and the results show that this ID-DVS scheme has obvious advantages that other similar schemes. Meanwhile, the simulated devices are with 3.2 V and 7.6 mA. With the former calculated time-consuming data, the energy-consuming results are calculated and shown in Fig. 4.

7. Conclusion

This paper contributes to privacy protection in the cross-chain health data-sharing process in the BIoMT systems and introduces an MCF model with a DVS scheme. The MCF model is constructed with blockchain and relay chain technologies, which can support cross-chain health data-sharing and guarantee that data is not tampered with. The DVS is designed with lattice cryptography which can resist anti-quantum attack. Meanwhile, the combination of the MCF model and DVS scheme can effectively improve the privacy security of system transactions and users. Then, it has proved that the DVS scheme can satisfy the security requirements of unforgeability, anonymity, and non-traceability. The key size comparison shows that the proposed DVS scheme is efficient and ledger space-saving, the consumption

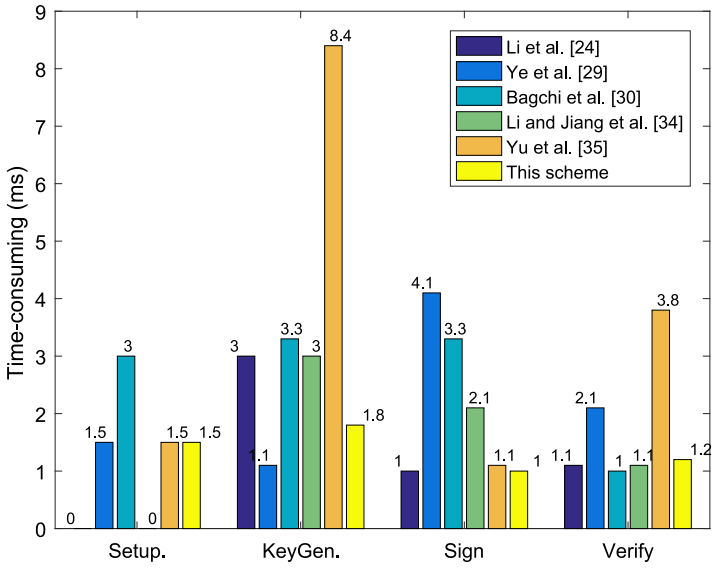


Fig. 3. Time-consuming comparison.

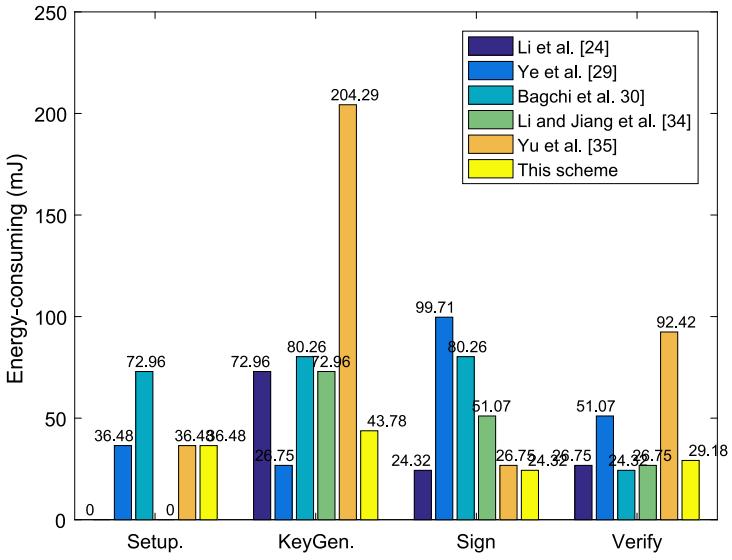


Fig. 4. Energy-consuming comparison.

comparison of time and energy shows that this DVS is more practical for cross-chain transactions and the performance evaluations of cross-chain transactions show that the proposed MCF model is efficient and practical for BIoMT systems. These works provide a new solution for the "data island" and privacy protection issues in current IoMT systems and promote the cross-chain technology application in BIoMT systems.

Moreover, there are still some worth exploring research directions, such as cross-chain identity authentication, secure secret sharing, data access control, and efficient data retrieval in cross-chain health data-sharing processes which will become the possible research orientations in future work.

CRediT authorship contribution statement

Chaoyang Li: Writing – review & editing, Writing – original draft, Formal analysis, Conceptualization. **Yuling Chen:** Writing – review & editing, Supervision. **Mianxiong Dong:** Project administration, Investigation. **Jian Li:** Validation, Supervision. **Min Huang:** Validation, Supervision. **Xiangjun Xin:** Supervision, Funding acquisition. **Kaoru Ota:** Supervision, Formal analysis.

Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Acknowledgments

This work was supported by the National Natural Science Foundation of China under Grant Numbers 62272090, 72293583, 72293580, the Foundation of State Key Laboratory of Public Big Data under Grant PBD2023-25, the Foundation and Cutting-Edge Technologies Research Program of Henan Province (CN) under Grant Numbers 242102211073, the Japan Society for the Promotion of Science (JSPS) KAKENHI Grant Numbers JP22K11989, JP24K14910, Leading Initiative for Excellent Young Researchers (LEADER), MEXT, Japan, and Japan Science and Technology Agency (JST), PRESTO Grant Number JPMJPR21P3, JST ASPIRE Grant Number JPMJAP2344, and the Soroptimist Japan Foundation. Mianxiong Dong is the corresponding author, and the Doctor Scientific Research Fund of Zhengzhou University of Light Industry under Grant 2021BSJJ033.

Data availability

No data was used for the research described in the article.

References

[1] X. Xiang, J. Cao, W. Fan, S. Xiang, G. Wang, Blockchain enabled dynamic trust management method for the internet of medical things, Decis. Support Syst. 180 (2024) 114184.

[2] A. Kosba, A. Miller, E. Shi, Z. Wen, C. Papamanthou, Hawk: The blockchain model of cryptography and privacy-preserving smart contracts, in: 2016 IEEE Symposium on Security and Privacy, SP, IEEE, 2016, pp. 839–858.

[3] W. Wang, H. Xu, M. Alazab, T.R. Gadekallu, Z. Han, C. Su, Blockchain-based reliable and efficient certificateless signature for iIoT devices, IEEE Trans. Ind. Inform. 18 (10) (2021) 7059–7067.

[4] Z. Wang, S. Wei, G.-L. Long, L. Hanzo, Variational quantum attacks threaten advanced encryption standard based symmetric cryptography, Sci. China Inf. Sci. 65 (10) (2022) 200503.

[5] L.K. Grover, Quantum mechanics helps in searching for a needle in a haystack, Phys. Rev. Lett. 79 (2) (1997) 325.

[6] P.W. Shor, Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer, SIAM Rev. 41 (2) (1999) 303–332.

[7] D.J. Bernstein, T. Lange, Post-quantum cryptography, Nature 549 (7671) (2017) 188–194.

[8] R.J. McEliece, A public-key cryptosystem based on algebraic, Coding Thv 4244 (1978) 114–116.

[9] L. Lamport, Constructing digital signatures from a one way function, 1979.

[10] R.C. Merkle, A certified digital signature, in: Conference on the Theory and Application of Cryptology, Springer, 1989, pp. 218–238.

[11] M. Ajtai, Generating hard instances of lattice problems, in: Proceedings of the Twenty-Eighth Annual ACM Symposium on Theory of Computing, 1996, pp. 99–108.

[12] J. Dey, R. Dutta, Progress in multivariate cryptography: Systematic review, challenges, and research directions, ACM Comput. Surv. 55 (12) (2023) 1–34.

[13] X. Jia, M. Luo, H. Wang, J. Shen, D. He, A blockchain-assisted privacy-aware authentication scheme for internet of medical things, IEEE Internet Things J. 9 (21) (2022) 21838–21850.

[14] Q. Lin, X. Li, K. Cai, M. Prakash, D. Paulraj, Secure Internet of medical Things (IoMT) based on ECMQV-MAC authentication protocol and EKMC-SCP blockchain networking, Inform. Sci. 654 (2024) 119783.

[15] D. Chen, F. Zhou, Y. Liu, L. Li, Y. Liang, Secure pairing-free certificateless aggregate signcryption scheme for IoT, J. Syst. Archit. 156 (2024) 103268.

[16] Y. Han, J. Han, W. Meng, J. Lai, G. Wu, Blockchain-based privacy-preserving public key searchable encryption with strong traceability, J. Syst. Archit. 155 (2024) 103264.

[17] S. Zou, Q. Cao, C. Huangqi, A. Huang, Y. Li, C. Wang, G. Xu, A physician's privacy-preserving authentication and key agreement protocol based on decentralized identity for medical data sharing in IoMT, IEEE Internet Things J. 11 (17) (2024) 29174–29189.

[18] R. Guo, G. Yang, H. Shi, Y. Zhang, D. Zheng, O 3-R-CP-ABE: An efficient and revocable attribute-based encryption scheme in the cloud-assisted IoMT system, IEEE Internet Things J. 8 (11) (2021) 8949–8963.

[19] C. Li, M. Dong, J. Li, G. Xu, X.-B. Chen, W. Liu, K. Ota, Efficient medical big data management with keyword-searchable encryption in healthchain, IEEE Syst. J. 16 (4) (2022) 5521–5532.

[20] X. Liu, Y. Sun, H. Dong, A pairing-free certificateless searchable public key encryption scheme for IoMT, J. Syst. Archit. 139 (2023) 102885.

[21] Z. Qu, Y. Meng, B. Liu, G. Muhammad, P. Tiwari, QB-IMD: A secure medical data processing system with privacy protection based on quantum blockchain for IoMT, IEEE Internet Things J. 11 (1) (2023) 40–49.

[22] W. Mao, P. Jiang, L. Zhu, Locally verifiable batch authentication in IoMT, IEEE Trans. Inf. Forensics Secur. 19 (2023) 1001–1014.

[23] J. Zhang, C. Dong, Y. Liu, Efficient pairing-free certificateless signcryption scheme for secure data transmission in IoMT, IEEE Internet Things J. (2023).

[24] C. Li, B. Jiang, M. Dong, Y. Chen, Z. Zhang, X. Xin, K. Ota, Efficient designated verifier signature for secure cross-chain health data sharing in BIoMT, IEEE Internet Things J. 11 (11) (2024) 19838–19851.

[25] J.-P. Thiers, J. Freudenberger, Code-based cryptography with generalized concatenated codes for restricted error values, IEEE Open J. Commun. Soc. 3 (2022) 1528–1539.

[26] A. Alahmadi, S. Çalkavur, P. Solé, A.N. Khan, M.A. Raza, V. Aggarwal, A new code based signature scheme for blockchain technology, Mathematics 11 (5) (2023) 1177.

[27] R. Punithavathi, K. Venkatachalam, M. Masud, M.A. AlZain, M. Abouhawwash, Crypto hash based malware detection in IoMT framework, Intell. Autom. Soft Comput. 34 (1) (2022).

[28] A. Kuznetsov, I. Oleshko, V. Tymchenko, K. Lisitsky, M. Rodinko, A. Kolhatin, Performance analysis of cryptographic hash functions suitable for use in blockchain, Int. J. Comput. Netw. Inf. Secur. 13 (2) (2021) 1–15.

[29] Q. Ye, Y. Lang, H. Guo, Y. Tang, Efficient lattice-based traceable ring signature scheme with its application in blockchain, Inform. Sci. 648 (2023) 119536.

[30] P. Bagchi, R. Maheshwari, B. Bera, A.K. Das, Y. Park, P. Lorenz, D.K. Yau, Public blockchain-envisioned security scheme using post quantum lattice-based aggregate signature for internet of drones applications, IEEE Trans. Veh. Technol. 72 (8) (2023) 10393–10408.

[31] K.-A. Shim, J. Kim, Y. An, Mq-sign: A new post-quantum signature scheme based on multivariate quadratic equations: Shorter and faster, KpqC Round 1 (2022).

[32] H. Nejatollahi, N. Dutt, S. Ray, F. Regazzoni, I. Banerjee, R. Cammarota, Post-quantum lattice-based cryptography implementations: A survey, ACM Comput. Surv. 51 (6) (2019) 1–41.

[33] J. Kim, J.H. Park, Ntru+: Compact construction of NTRU using simple encoding method, IEEE Trans. Inf. Forensics Secur. 18 (2023) 4760–4774.

[34] C. Li, B. Jiang, M. Dong, X. Xin, K. Ota, Privacy preserving for electronic medical record sharing in healthchain with group signature, IEEE Syst. J. 17 (4) (2023) 6114–6125.

[35] H. Yu, W. Hui, Certificateless ring signature from NTRU lattice for electronic voting, J. Inf. Secur. Appl. 75 (2023) 103496.

[36] L. Yao, J. Weng, A. Yang, X. Liang, Z. Wu, Z. Jiang, L. Hou, Scalable CCA-secure public-key authenticated encryption with keyword search from ideal lattices in cloud computing, Inform. Sci. 624 (2023) 777–795.

[37] Y. Zhang, W. Susilo, F. Guo, Lattice-based strong designated verifier signature with non-delegatability, Comput. Stand. Interfaces 92 (2025) 103904.

[38] Q. Zhang, Y. Sun, Y. Lu, W. Huang, Revocable identity-based designated verifier proxy re-signature with signature evolution, Comput. Stand. Interfaces 92 (2025) 103894.

[39] D. Micciancio, O. Regev, Lattice-based cryptography, in: Post-Quantum Cryptography, Springer, 2009, pp. 147–191.

[40] L. Ducas, A. Durmus, T. Lepoint, V. Lyubashevsky, Lattice signatures and bimodal Gaussians, in: Annual Cryptology Conference, Springer, 2013, pp. 40–56.

[41] M. Ajtai, Generating hard instances of the short basis problem, in: Automata, Languages and Programming: 26th International Colloquium, ICALP'99 Prague, Czech Republic, July 11–15, 1999 Proceedings 26, Springer, 1999, pp. 1–9.