A Threshold Signature Scheme Without Trusted Center for Blockchain-Based Medical Cyber-Physical Systems

Xianfei Zhou, Jing Huang, Fulong Chen, Yuqing Tang, Canlin Wang, Taochun Wang, Dong Xie, and Chuanxin Zhao

Abstract—With the rapid development of medical information technology, the medical cyber-physical system is undergoing a rapid transformation, and the safe storage and sharing of medical data are facing great challenges. It makes the work of safe medical data storage, privacy protection and data sharing get more difficult. In this paper, we propose the combination of private blockchain and consortium blockchain that can protect information security and realize data sharing. In the system, the medical records of each node are stored in the private blockchain, and the shared data is on the consortium blockchain so as to improve the data storage and reduce data redundancy. And the threshold signature scheme without trusted center is applied in the system. In order to initiate threshold signature, a set of nodes is constructed by the sponsoring doctor, in which the threshold signature process is initiated. When there are no less than t nodes sending part-signatures, the signature can be synthesized to group signature. This scheme can be well applied to the scene of multidisciplinary joint consultation in the medical blockchain. The scheme proposed in this paper has high security and computing efficiency.

Index Terms—Medical Cyber-Physical Systems, Threshold signature, Blockchain, Without trust center

1 Introduction

With the rapid development of medical information, medical information sharing is facing new challenges. First of all, lacking of unified planning of medical cyber-physical system [1]platform to manage various sources and rapid updating massive medical data, causing disordered data standards, difficult data sharing, and serious information isolation; second, patients have not participated in the access control strategy of medical information, and division of authority in the medical information system is not clear, which can not realize the personalized privacy protection of patients [2].

In the medical cyber-physical system, patients medical data security and privacy can not be ignored. Data security means the integrity, validity and authenticity of medical data [3]. The safe storage, transmission and access of the medical cyber-physical system are the most important guarantee for medical data sharing and informatization, which ensure the data that can complete the medical diagnosis and treatment without leakage, loss or tampering.

Blockchain has the characteristics of distributed, decentralized, time-series data, data encryption and so on [4]. The decentralization of blockchain can solve the trust problem for the medical cyber physical system. The distributed architecture is also fit for the development direction of intelligent medical in the future. MCPS based on blockchain can promote the sharing of resources and can be well applied in the medical field. Krotofil [5] proposed a blockchain based on electronic medical record architecture, which can authorize different levels of granularity. Now, most of the research and application of "MCPS + blockchain" is on the top application or architecture design [6–8], ignoring the storage, transmission and access security of the bottom data. Only when the bottom data is guaranteed, can the security of top application and architecture cab be more improved.

Cryptographic algorithm is very important in the blockchain system, and it is the skeleton of the blockchain system. Including hash computation, public keys and private keys generation,signatures generation and etc. Are all using cryptographic algorithms. The security of digital signature depends on the key used in the signature. Threshold signature technology can distribute the signature key to other users in a threshold way, which can partly solve key leakage and key loss in key management [9]. In the (t, n) threshold signature system, the original signer gives n secrets, in the signature process, only when no less than t participants agree to cooperate, a valid group signature can be generated. No less than t participants can recover the signature representing the group member.

- *Corresponding author: Fulong Chen.*
- *Xianfei Zhou is with Department of Information Engineering, Wuhu Institute of Technology, Wuhu, Anhui 241002, China. Fulong Chen, Yuqing Tang, Canlin Wang, Jing Huang, Taochun Wang, Dong Xie and Chuanxin Zhao are with the Anhui Normal University and with the Anhui Provincial Key Laboratory of Network and Information Security, Wuhu, Anhui 241002, China.(e-mail:zhouxf1982@whit.edu.cn, huangjing@ahnu.edu.cn,long005@ahnu.edu.cn, tangyuqing@ahnu.edu.cn, wangcanling@ahnu.edu.cn, wangtc@ahnu.edu.cn, xiedong@ahnu.edu.cn, zhaocx@ahnu.edu.cn).*

Manuscript received xx xx, 2021; revised xx xx, 2021.

2 Related Works

2.1 BlockChain

Blockchain is distributed data storage network, it is a new application mode of computer technology, such as point-to-point transmission, consensus mechanism, encryption algorithm,and etc. It is essentially a decentralized database with the characteristics of decentralization, anonymity, untrustworthy, tamper proof and

traceability. Blockchain is originated from bitcoin. On November 1,2008, Satoshi Nakamoto published bitcoin: a peer-to-peer e-cash system [10], which described the architecture of e-cash system based on P2P network technology, encryption technology, blockchain technology,and etc. On January 3, 2009, the first Genesis block with serial number 0 was born. A few days later, on January 9, 2009, a block with a sequence number 1 appeared, connected with the Genesis block with the serial number 0 to form a chain, marked the birth of the blockchain [11].

According to the difference of open objects, blockchain can be divided into: public blockchain, consortium blockchain and private blockchain [12]. The comparison of different blockchain is listed in Table I.

TABLE I. The Comparison of Different Blockchains

Blcokchain Type	Public Blockchain	Consortium Blockchain	Private Blockchain
Characteristic	Openness No Tampering	Between Private Chain And Public Chain	Read And Write Fast
Openness	Fully Open	Authorize To Open	Private
Decentralization	Fully Decentralization	Partial Decentralization	Centralization
Consensus	PoW, PoS,DPOS	PBFT,RAFT	PBFT
Typical application	Bitcoin Ethereum	Ant Financial	Hyperledger, r3cev

Xue [13] proposed a medical blockchain system MDSM ,which combined medical institution federated servers (MIFS) and audit federated servers (AFS) by using the improved DPOS consensus mechanism. Azaria [14] used Ethereum blockchain to realize a medical information sharing platform combining medical blockchain and big data. Zhang [15] proposed a medical blockchain system based on consortium blockchain,which is a multi-node maintenance and sharing system. It prevented medical data from being tampered with or leaked and was used to solve these medical problems.

In the special field of MCPS, medical data contains both a large amount of private information and needs to be shared between medical institutions; therefore the a mixed blockchain is more suitable for the secure storage and sharing of medical data.

2.2 Threshold signature

In recent years, there are a lot of research achievements around blockchain-based aggregate signature [16], multi-signature [17], and ring signature [18]. Threshold signature is a kind of multi-signature. The threshold signature scheme can improve security and privacy in many scenarios.

According to manager's identity, the threshold signature scheme can be divided into two types: with trusted center [19]and without trusted center [20]. In the threshold signature scheme with trusted center, the trusted center plays the role of manager and undertakes most of the management tasks,which can not avoid the authority deception of the trusted center. In contrast,the threshold signature scheme without trusted center does not need to consider the problems of centralization. In order to propose a threshold signature scheme based on blockchain, we need to consider the decentralization of blockchain.

Secret sharing was first proposed by Shamir [21] in 1979, and a (t, n) threshold secret sharing scheme based on Lagrange interpolation polynomial was proposed. However, his scheme can not prevent the fraud of the secret distributor and the participants, and the secret share obtained by the participants can only be used once. If there are multiple keys to be shared at the same time, the secret share needs distribute multiple times.

In 1983, Asmuth and Bloom [22] applied the Chinese Remainder Theorem and proposed a threshold secret sharing scheme based on the Chinese remainder theorem. Compared with shamirs secret sharing scheme, this scheme has less computation, but it can not guarantee data security when transmitting data in an insecure communication channel.

In 2003, Wang [20] proposed (t, n) threshold signature scheme without a trusted center by using Shamir(t, n) threshold scheme, modular operation over finite field $GF(p)$ and Lagrange interpolation polynomial, designed a verifiable multi-secret sharing threshold scheme, which solved the problem of member's private key revealed caused by traditional secret sharing scheme, but the scheme didnt consider the actual signature member's identity information.

In 2011, Cheng [23] proposed a verifiable (t, n) threshold secret sharing scheme by combining ElGamal scheme with Asmuth-Bloom threshold secret sharing scheme. The scheme designed effective measured to prevent the secret share from being tampered in the process of distribution. Also, it provided a method to verify whether the participants given the correct secret share. The security of this scheme is based on the difficulty of solving discrete logarithm problem in finite fields.

In 2018, Wang [24] proposed a threshold group signature scheme without a trusted center. In this scheme, the power of selecting signature members is given to the signature organizer. When the threshold signature is synthesized, the private key is added to verify the threshold signature corresponding to the public key. The organizer completely controlled authority of giving out signature, and the scheme is vulnerable to attackers.

In 2020, Wang [25] applied on blockchain voting scene based on Chinese remainder theorem. Through cooperation,the share signatures synthesized the final signature. The scheme supported the nodes join/leave behaviors.It also excluded the distributor from participation to improve the availability.The scheme can effectively fit into the blockchain scenario.

In the medical blockchain, the application of threshold signature scheme is very convenient, especially in the multi-disciplinary joint outpatient scenarios, which can save network resources, and improves system throughput.

3 PRELIMINARIES

3.1 Digital signature

Digital signature is a cryptographic protection technology which uses cryptography technology to confirm the source of data and data integrity. It uses public key cryptography algorithm, thats digital signatures employ asymmetric cryptography. The signer first encrypts the message with the receiver's public key, and then encrypts the message again with his own private key. The encrypted ciphertext is called digital signature. After it is sent to the receiver,the receiver uses the signer's public key to decrypt. In this algorithm, only the signer has his own private key, so the receiver can believe that the message is from the signer.In many instances digital signature provides a layer of validation and security to messages sending through a non-secure channel.Properly implemented, a digital signature gives the receiver

reason to believe the claimed sender sending the message. The steps of the signature process are as follows[25]:

- $G(p)$ $\underline{generate \quad key}$ (sk, pk). sk is the private key,and pk is public key.
- $Sig(sk, m)$ $\underline{generate \quad signature}$ (sig). m is plaintext message,sig is the generated signature.
- $Ver(pk, m, sig)$ $\underline{verify \quad signature}$ $(True, Flase)$. Verifies whether the data is modified according to the public key pk and plaintext m. If it is $True$, the verification is successful, and if it is $False$, the verification is failed.

At present, the commonly used signature algorithms are elliptic curve digital signature and threshold signature. Elliptic curve digital signature algorithm is mainly based on the elliptic curve discrete logarithm problem, so its security mainly depends on the difficulty of solving elliptic curve problems.Threshold signature was proposed by Desmedt Y in 1987[26]. The threshold signature mechanism allows any t of n signers to generate signatures for messages, but less than t signers can not generate valid signatures. Threshold signature mechanism can build a robust signature system and prevent some signers from illegal behavior.

Threshold signature is a combination of threshold secret sharing technology and digital signature. Shamir first proposed the concept of secret sharing in the threshold signature. The idea is to divide the secret into n parts by appropriate method, and send each secret to different participants for management. When recovering the secret, the number of participants must be at least equal to a certain threshold value to recover the message. Classical secret sharing algorithms include Shamir algorithm based on polynomial interpolation and Asmuth-Bloom algorithm based on Chinese remainder theorem.

3.2 Shamir secret sharing based on polynomial interpolation

Shamir's (t, n) secret sharing algorithm divides secret s into n sub secrets. Any t sub secrets can recover s, while any $t-1$ sub secrets cannot recover s.

(1)Initialization. Suppose n participants compose a set $Q = \{Q_1, Q_2, \ldots, Q_n\}$,the threshold value is t, p is prime, its Galois Field is $GF(p)$, and each participant number is $x_i \in GF(p)(i = 1, 2, \ldots, n)$.

(2)Encryption. The trust center chooses $t-1$ polynomial

$$f(x) = A_0 + A_1 x + A_2 x^2 + \ldots + A_{k-1} x^k - 1$$

Where $A_i \in GF(p)(i = 1, 2, \ldots, n)$., Let $x_i \in GF(p)(i = 1, 2, \ldots, n)$ substitute into the above equation to obtain$((x_1, f(x_1), \ldots, (x_n, f(x_n))$, and send these information pairs to the participants.

(3)Decryption. n participants select t information pairs,reconstructed polynomial $f(x)$ by Lagrange interpolation formula and solve the polynomial $f(x)$ is reconstructed by Lagrange interpolation formula, and solve the solution $f(0) = A0 = s$.

3.3 Asmuth-Bloom algorithm based on Chinese remainder theorem

(1)Initialization. Suppose n participants compose a set $Q = \{Q_1, Q_2, \ldots, Q_n\}$,the threshold value is t, the secret is s,select a large prime $p(p > s)$, and n integer sequences $m = \{m_1, m_2, \ldots, m_n\}$, and satisfy the following conditions

- $m_1 < m_2 < \ldots < m_n$,that $m_1, m_2, \ldots, m_n$ strictly monotonic increasing
- $\{(m_i, m_j) = 1 \mid i \neq j\}, m_i, m_j$ mutual prime
- $\{(m_i, p) = 1 \mid i = 1, 2, \ldots, n\}, m_i, p$ mutual prime
- $M = \prod_{i=1}^{t} m_i > p \prod_{i=1}^{t-1} m_{n-i+1}$

(2)Secret Share.$M = \prod_{i=1}^{t} m_i$,obvious thatM/P is greater than the product of any other $t-1sm_i$,randomly selects an integer B,and the number B satisfies the formula $B \in [0, [\frac{M}{p}] - 1]$,calculate $s' = s + Bp$,evidently know that $s' \in [0, M - 1]$,generate secret shares,that is $s_i = s' \bmod m_i (i = 1, 2, \ldots, n)$.

(3)Secret Recovery.Any t members can exchange their secret shares to recover the secret s,It is assumed that the secret shares submitted by the participant is $s_1, s_2, \ldots, s_n$, the congruence equations are constructed as follow:

$$y = \begin{cases} s' = s_1 \bmod m_1 \\ s' = s_2 \bmod m_2 \\ \quad \vdots \\ s' = s_t \bmod m_t \end{cases}$$

According to the Chinese remainder theorem,The equations are in$[m_1, m_2, \ldots, m_n]$ have a unique solution. The solution is $s' = \sum_{i=1}^{t} M \times r_i \times s_i \bmod M$,among them $r_i = M_i^{-1}$ is $M_i \bmod m_i$ modular inversion,that is $r_i M_i \equiv 1 \bmod m_i, \forall i \in (1, 2, \ldots, n)$,and can get the secret$s = s' - Bp$.

4 Blockchain-based on medical cyber-Physical systems

4.1 System model

A Medical Cyber-Physical Systems based on blockchain based on the blockchain is proposed to achieve more secure medical data storage, privacy protection and data sharing. Based on high-speed network technology, consortium blockchain and private blockchain are combined into a mixed blockchain to alleviate data verification delay[27]. The system architecture is shown in Figure 1. In the mixed medical blockchain, the private blockchain is used as the traditional database of hospitals to store medical data, while the consortium blockchain is used to store the medical data submitted by the hospitals. The medical data in the mixed medical blockchain is authorized by the medical supervision organization and public to the all participating nodes. A Byzantine fault-tolerant mechanism [28] is used to attach new blocks to the consortium blockchain. In order to protect the privacy of patients, each medical data is asymmetrically encrypted before it is attached to the mixed blockchain.

The relationship among patients medical records, blockchain and cluster storage is shown in Figure 2. The hash tree composed of a large number of patients medical records is stored on the blockchain, and the content of patients medical records is stored on the cloud storage platform composed of multiple computing centers, that is patients medical records are stored by cluster storage. Users can transparently access and utilize the patients medical records in all storage devices through the unified access interface.

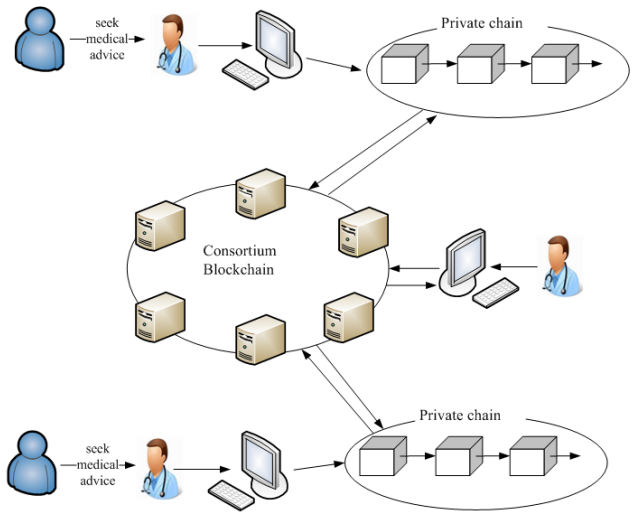

Fig. 1. The architecture of mixed Medical blockchain.

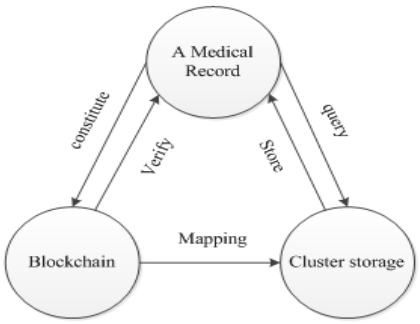

Fig. 2. The relationship diagram of MCPS based on consortium blockchain.

The structure of a medical record is shown in Figure 3. The medical record contains the specific information of each medical data, including patient account (address), patient health data digest,patient signature, doctor signature, patient public key, doctor public key, priority level, etc.

Patient ID	Patient Name	Consultation hours	Consultation hospital	Medical Record	Doctor Signature	Prority Level

Fig. 3. Component of Medical Records.

Patients can obtain the private key after registration and identity authentication in the hospital's computing center, Randomly generate a 256 bits data. The private key represents the user's ownership of the data. If the private key is lost, the data ownership will also be lost.

The public key is the user's account. The public key and the private key are generated in pairs, and the public key can generate the corresponding unique address, which can confirm the location of the patient 's medical data .

The address is calculated by the public key. The public key is used as the input, and use hash function to generate the address.

patient signature: the patient uses the private key to encrypt the medical data digest and the public key of user and doctor. One is to prove that the message is actually send with the patient signature, and the other is to confirm the integrity of the message.

Doctor signature: doctors use private key to encrypt medical data digest, in order to confirm the authenticity of medical data.

Priority level: After doctor diagnoses patient, doctors write medical records in the system. Doctors have the right to set the priority of patients' medical records, if the priority level is high,the patients' medical records attach to the consortium blcokchain for sharing. In comparison, the low priority level just write into private blockchain. In this way, the data in the alliance chain can be controlled to prevent the data from growing too fast.

4.2 The working procedure of the mixed medical blockchain

The reason to replace the traditional database with the private blockchain is that if the node wants to add it to the consortium blockchain, the node can directly use the block in the current private blockchain as the block of the new block in the consortium chain. All nodes are allowed to add their medical data to the consortium blockchain.But, if the blockchain is too long, it takes a long time to track the consortium blockchain blocks.

Besides, the size of many medical records, such as laboratory examination results, pathological examination, prescriptions and medical images, have a large amount of data. With the continuous generation of new blocks, the scale of medical data in the consortium blockchain will be very large, each node needs to use a very large storage to save medical data in the consortium blcokchain. This is a waste of storage space for nodes, because they both store their own medical data in the private blcokchain, and store many shared medical data in the consortium blockchain. In order to reduce the storage burden of the consortium blcokchain, doctors will decide whether they need to attach the current patient's medical block to the consortium blockchain. It reduces the increasing number of medical blocks in the main blockchain, and reduces the storage burden of nodes in the network to a certain extent.

Therefore, each node selects the number of candidate blocks to be added to the consortium blockchain by using the queue collection.

The working procedure of medical records is described as algorithm I.

Step 1. if the patients is unwilling to public his/her medical records, the medical record is encrypted by the patient's public key.

Step 2. The node generates a new block based on the previous block and adds it to the private blockchain.

Step 3. Medical institutions present medical records of patients with higher priority label.

The node of the new block checks the priority label. If the priority label is equal to true, the number of blocks is appended to the candidate queue.

Consortium blockchain is used to realize medical information sharing among nodes. In consortium blockchain, data is only public to authorized users of MCPS, and each node keeps a copy of the data. All nodes use the practical Byzantine algorithm to generate consensus and attach them to the consortium blockchain.

The parameters of the block head in the consortium blockchain are set as that in the normal blockchain, and the block body is composed of the candidate blocks in the private blockchain and

the digital signature of the node. The node should use the private key to sign the private candidate block.

The working procedures of constructing consortium blockchain is described as algorithm II.

Step 1. Every node writes a candidate block from its private chain and its digital signature into a new block.

Step 2. Inform other nodes that they have received the voting request and can vote ,accept and refuse.

Step 3. A node received accept number is greater than number of byzantine nodes tolerated.

Step 4. Other nodes receive this block and validate its signature. The block is acceptable only if its signature passes validations.

The private blockchain of the mixed medical blockchain is private to each node, and only the user authorized by the node can query the medical information. The medical information in the consortium blockchain of mixed medical blockchain is public and ordered by time sequence. Consortium blockchain applies practical Byzantine consensus algorithm to build trust in nodes without centralized institutions. After a block reach a consensus and attach to the block chain, it is recorded by all nodes and connected to the previous block using cryptography, which makes tampering very difficult and costly. The digital digest of digital signature technology is the hash value of the original data. Any change of the original data will change the hash value, ensuring that no one can tamper with the original data. Therefore, through consortium blockchains application to realize the medical data sharing of some medical institutions, the fraud risk will be reduced.

5 THRESHOLD SIGNATURE SCHEME IN BLOCKCHAIN BASED ON MCPS

5.1 Application scenario description of threshold signature

In some cases, it is difficult to get the final treatment plan in one department because of the complexity of patients' actual disease. In order to effectively save the cost and time of refer to a different hospitals,the mode of multidisciplinary consultation can be adopted. Only when the number of doctors' signatures on the treatment plan meets the threshold value,can the hospital make the final treatment plan for patients. The threshold signature scheme is applied to the medical cyber physical system based on mixed medical blockchain, which ensures the systems security and tamper resistance [29].

A patient P goes to the hospital to receive the outpatient treatment of doctor D. for the actual disease of patient P,doctor D can start the multidisciplinary consultation mode when it is difficult for one person to get the final treatment plan. Only when the number of doctors' signatures on the treatment plan meets the threshold value, can the hospital make the final treatment plan for the patient. Doctor D uses threshold signature to guarantee multidisciplinary consultation, showing the basic workflow of the blockchain. The private key and public key of the patient are stored in the patient's electronic device.the application scenario process of threshold signature is described as below:

Step 1.The information of patient P is stored in a transaction list in the blockchain. The information of the patient contains:ID number, name, gender, age, and public key PUB_KEY_P. The ID number and the name are encrypted by asymmetric encryption, while gender and age are not encrypted. The information of doctor D is similar to that of patients.

Step 2. Patient P has complicated disease and finds doctor D through the registration system;

Step 3. Patient P arrives at doctor D's consulting room, and patient P receives the public key PUB_KEY_P to generate a query transaction list and uses its own private key for digital signature SIG_P.To obtain the transaction list with its own information from the system. The system uses the public key PUB_KEY_P and digital signature SIG_P to verify P's identity in the key and authentication architecture,and returns the transaction sheet containing the patient's information after pass verification. The query transaction will be saved in each verification nodes local database, waiting for the packer to pack into the new block. After the patient decrypts with the private key, the decrypted information(excluding the patient's private key) will be sent to the doctor client and displayed on the doctor's computer.

Step 4.First,Doctor D signs the treatment plan (corresponding share signature), package the public key in the form of private blockchain data structure and upload it to the private blcokchain of the hospital for other $n-1$ doctor nodes verification. Second, other doctors in the group download the transaction from the private chain through the server for correctness verification (share verification), and if it is correct, the verification transaction will be broadcast, that is, other doctors sign on the treatment scheme and broadcast it to the private chain of the hospital in the form of transaction; then, doctor D collects the transaction on the chain for verification, and if the number of effective transactions verified meets or exceeds number t, A signature SIG_H is generated. After the treatment plan, and package the transaction data (composite signature) into the block and broadcast to the whole network on behalf of the hospitals final treatment plan.

Step 5. If the lower limit of threshold signature is not reached, the signature can not be generated. At this time, doctor D can transfer the patient to another hospital.

5.2 Architecture of blockchain threshold signature system

Through the previous discussion, compared with the scheme based on Lagrange interpolation, the scheme based on Chinese Remainder Theorem had less computation [30]. In this paper, a threshold signature scheme based on Chinese remainder theorem is used to realize the threshold signature based on mixed medical blockchain. The framework of the system is shown in the Figure 4:

Its working process consisted of the following steps:

Step 1. The Sponsor node invites external nodes to join the process to form a group. In this blockchain, each node can act as a signature synthesizer and a signature verifier.

Step 2. Threshold signature initialization. Generates the parameters needed by the signature algorithm, generates its own private key and public key for each node, and broadcasts public key to other nodes in the group.

Step 3. The system divides the secret of the node, and broadcasts the secret share to other nodes to provide other nodes to generate part-signature.

Step 4. Each node in the system solves the secret information according to the Chinese Remainder Theorem for the received secret share, generates a part-signature, and broadcasts it to the signature synthesizer.

Step 5. The signature synthesizer synthesizes the received part-signatures, and only needs no less than t part-signatures

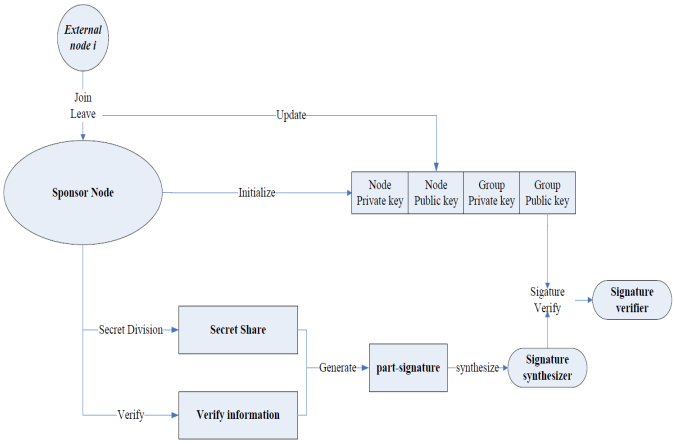

Fig. 4. Architecture of blockchain threshold signature system.

to synthesize the final signature and sends the signature to the signature verifier.

Step 6. The signature verifier verifies the synthesized signature information, and then feeds back the signature result to the sponsor.

5.2.1 Detailed design of blockchain threshold signature system

The following described the detailed design process of (t, n) threshold signature in the medical blockchain based on Chinese remainder theorem. Firstly, the symbols used in the detailed design are listed, and their contents are shown in Table II

TABLE II. Symbols used in threshold signature

Symbol	Description	Symbol	Description
Q	Member set	E_i	Private key of node i
r_i	Sub secret of node i	K_i	Public key of node i
B_i	Arbitrary integer of node i	G	Group private key
Y_{ij}	Secret share shadow	C	Group public key
m	Message to be signed	g	Generator of GF(p)
p	Large prime	Z_i	Part-signature of node i
q	prime of group public key	Z	complete signature

Setp 1.Initialization of the sponsor node

The sponsoring node invites the external nodes to form a set $Q = \{Q_1, Q_2, \ldots, Q_n\}$,contains n nodes participating in the joint consultation signature in the medical blockchain, and t is the threshold value. Two big prime numbers p and q are selected. A set of positive integer sequences $d = \{d_1, d_2, \ldots, d_n\}$,and generating element g on a prime field $GF(p)$ are also selected.q and d satisfies the Asmulth-Bloom scheme, and the message to be signed is m,let $D = \prod_{i=1}^{t} d_i$.public information$\{n, t, g, p, q, d, D\}$ to all the other nodes.

Setp 2.Generate secret sharing

The blockchain nodes cooperates with each other. Blockchain node Q_i randomly selects the sub secret r_i and the integer B_i. The sub secret r_i and the integer B_i are selected secretly by the current blockchain node, and they do not need to be broadcast them to other nodes. As long as the node does not actively disclose these two parameters, others can not obtain them.

The selection of r_i and B_i meet the following conditions:

$$0 < r_i < [q/n] \tag{1}$$

$$0 < B_i < [D/q - 1]/n \tag{2}$$

Node Q_i calculates the secret share Y_{ij}
let $x_i = r_i + B_i q$

$$Y_{ij} = x_i \bmod d_j \tag{3}$$

Q_i preserves the value of Y_{ij} and public g^{r_i} ,g^{B_i} , and broadcast $Y_{ij}(i \neq j)$ to node Q_j .

Step 3.Verify node information

The blockchain node Q_i calculates the verification information u_i ,w_{ij} and v_{ij}, and verifies the correctness of the information .

$$u_i = g^{x_i} \bmod p \tag{4}$$

$$w_{ij} = (x_i - Y_{ij})/d_j \tag{5}$$

$$v_{ij} = g^{w_{ij}} \bmod p \tag{6}$$

And broadcast u_i and v_{ij} in the blockchain network. In addition, after receiving the information u_i and Y_{ij}, the node Q_j verifies the correctness of the secret share through the following formula:

$$g^{r_i} \cdot g^{B_i q} \bmod p = u \tag{7}$$

$$((g^{r_i} \bmod p)((v_{ij})^{d_j} \bmod p)) \bmod p = u \tag{8}$$

If the u_i satisfies the above equation (7) and (8), then the secret share shadow Y_{ij} send by the member Q_i is true, and the message is trusted; otherwise, the blockchain node Q_j will ask the node Q_i to re-transmit the message again.

Step 4.Generate blockchain node key and group key.

According to the verification above, if the verification result is correct, the node Q_j calculates its own private key.

$$E_j = \sum_{i=1}^{n} Y_{ij} \bmod d_j \tag{9}$$

So the node pubic key is $K_j = g^{E_j}$.

According to the number of secrets selected by each blockchain node, the group public key and group private key can be generated. The group public key is:

$$C = \prod_{i=1}^{n} g^{r_i} \bmod p = g^{\sum_{i=1}^{n} r^i} \bmod p \tag{10}$$

And group private key is $G = \sum_{i=1}^{n} r_i$.

Step 5.Generate signature

According to the Chinese remainder theorem,any t blockchain nodes use their private key to generate their own part-signature , and t part-signature can compose the signature of message m .

First, generate part-signature.the node Q_i chooses a integer $\varphi_i \in GF(p)$,and calculate δ_i.

$$\delta_i = g^{\varphi_i} \bmod p \tag{11}$$

Q_i received δ_i and calculated

$$\delta = g^{\sum_{i=1}^{t} \varphi_i} \bmod p = \prod_{i=1}^{t} g^{\varphi_i} \bmod p = \prod_{i=1}^{t} \delta_i \bmod p \tag{12}$$

the δ is a coefficient of the formula to compose a part-signature.

Than Q_i continues to calculate the other coefficient L_i

$$L_i = \frac{D}{d_i} \times h_i \times E_i \bmod D \tag{13}$$

in the formula (13) $h_i \equiv (\frac{D}{d_i})^{-1} \bmod d_i$,$(i = 1, 2, \ldots, n)$.node Q_i calculated the part-signature Z_i by equation (14)

$$Z_i = E_i \cdot m + \delta \cdot L_i \tag{14}$$

After receiving the part-signature$\{m, \delta, Z_i\}$ send by t blockchain nodes, the signature synthesizer synthesizes the signature Z. It should be noted that every node can assume the role of signature synthesizer in the blockchain scenario. The calculation formula of completed signature is as follows:

$$Z = \sum_{i=1}^{t} (Z_i \bmod D) \bmod q \tag{15}$$

Then the completed signature of message m is $\{m, \delta, Z\}$.

Step 6.Verify signature

After receiving the signature information m is $\{m, \delta, Z\}$, the versifier uses the group public key C to verify the validity of the signature according to the following equation (16):

$$g^z = \delta^{s \times \delta} \times C \bmod p \tag{16}$$

If the equation (16) is true, the signature is valid and accepted.

6 SCHEME ANALYSIS

6.1 Security analysis

(1) This scheme does not need trusted center, and the secret shares are generated by all participants. No single node can know the group private key, which effectively avoids the authority deception of the trusted center.

(2)The scheme can distinguish the fraud between member nodes, and each member must public the real u_i and v_{ij}. If Q_i provides the fault secret share shadow Y_{ij}, it can be detected by $u_i v_{ij}$ through verification equations (3) to (8).

(3)In the verification process, each member's sub secret r_i is secure. Although the member Q_i public g^{r_i}, but through $g^{r_i} \bmod p$ to solve r_i is still a discrete logarithm problem , so the member sub secret r_i will not be disclosed. In the process of verifying Y_{ij} ,each member Q_i is required to public the verification information through the equation equations (4) to (6).

Through u_i to slove x_i is a discrete logarithm,so u_i is safe,on other hand ,if attackers want to through v_{ij} to get x_i, they must know w_{ij}, and get v_{ij} from w_{ij} is still a discrete logarithm problem. So x_i is safe ,and r_i is safe too.

(4)The group private key G is secure and reusable. Through the group public key C to calculate group private key G belongs to the problem of discrete logarithm. Therefore, unless all members cooperate, no one can obtain the group private key G.

In the part-signature generation process, each member calculates the par- signature use the formula (14),do not directly use or expose any information of the group private key G.so the group private key G can still be reused after one signature.

6.2 Unforgeability analysis

(1)If a malicious node Q_i' wants to replace the blockchain node Q_i to generate secret share, the malicious node Q_i' randomly selects the secret numbers r_i' and B_i' . Because $r_i' \neq r_i$,$B_i' \neq B_i$, then $r_i' + B_i'q \neq r_i + B_iq$, so $Y_{ij}' \neq Y_{ij}$, and other nodes receive the broadcast information $g^{r_i'}$,$g^{B_i'}$ from malicious node Q_i'.Through verification, it is easy to verify $g^{r_i'} \cdot g^{B_i'q} \neq g^{r_i} \cdot g^{B_iq}$.Therefore,node Q_i' can not replace any other blockchain nodes to forge r_i and B_i.

(2)If a the malicious node Q_i' wants to replace the blockchain node Q_i to generate the private key of node, the malicious node may intercept the Y_{ij} send by the other $n-1$ nodes to construct the private key of the blockchain node. However, the other nodes keep their own Y_{ii} which can not be obtained by the attacker. From $Y_{ii} = (r_i + B_iq) \bmod d_i$,the attacker may attempt to obtain r_i and B_i by intercepting g^{r_i} and g^{B_i} , so as to calculate Y_{ii} .However, solving r_i and B_i through g^{r_i} and g^{B_i} is a discrete logarithm problem, and the attacker cannot obtain them through calculation, so the attacker cannot forge the private key of the blockchain node.

(3)If a malicious node wantes to forge the completed signature, the attacker randomly selects φ_i', calculates δ_i', δ' and part-signature Z_i', and synthesized the signature Z'. In the signature verification process, because $Z' \neq Z$,so $g^{Z'} \neq \delta^{m\delta} \cdot C \bmod p$,the attacker can not pass the verification and the signature is invalid, so the attacker cannot forge the signature.

6.3 Efficiency analysis

The proposed threshold signature scheme based on Chinese remainder theorem, that has less computationally difficult than the interpolation algorithm based on Lagrange.The signature algorithm proposed in this paper is compared with the literature based on Lagrange interpolation[31].

In the following, we compare the proposed scheme with the scheme in [31] in terms of computation to show the advantages of this scheme in this respect. Since the key generation process of threshold signature is not frequent, the amount of computation required by the process have little impact on the practicability of the scheme. Therefore, we mainly compare the two schemes in the signature generation stage and signature verification stage.the symbols are defined in Table III.

TABLE III. modulus symbols description

Symbol	Description
M_m	Modular Multiplication
M_e	Modular exponentiation

Compared with modular exponentiation and modular multiplication, modular addition and modular subtraction are more efficient. Therefore, this paper only compares modular exponents and modular multiplication.

TABLE IV. Computational complexity of two schemes

scheme	Signature generation	Signature verification
Alg.in[31	(8t+1)M_m+(2t+2)M_e	$2M_m$
Proposed	(2t)M_m+tM_e	M_m

It can be seen from Table IV that for signature generation and signature verification, our algorithm is better than[31].As a

decentralized distributed network,due to the limited computing resources, the algorithm is required to be more efficient.

6.4 Blockchain evaluation

To evaluate the proposed architecture of mixed medical blockchain , we compared it with the existing system based on blockchain technology. At present, the main medical blockchain systems are MDSM [13], MedRec [14] and MedicalChain [15], and the comparison results with the existing solutions are as follows.

TABLE V. The comparison of different systems

system	Consensus	computing power	payment	Alleviating data size
Alg.in[13]	DPOS	Small	No	NO
Alg.in[14]	PoW	Big	YES	NO
Alg.in[15]	PoI	Big	YES	YES
Proposed	PBFT	Small	No	YES

From Table V, compared with PoW algorithm and PoI algorithm, PBFT consensus algorithm has less computing power, and does not need to pay, requires less running nodes, and does not need "mining" operation. Moreover, this scheme combines private blockchain and consortium blockchain, effectively controls the rapid growth of data in the consortium blockchain, which is consistent with the needs and characteristics of the medical system.

7 Conclusions and future Works

In this paper, we proposed the combination of private blockchain and consortium blockchain to secure storage and share medical data in the medical cyber physical system. In the system, each node's the medical records are stored in the private blockchain. To improve the data storage and reduce data redundancy, the shared data is on the consortium blockchain. A verifiable threshold signature scheme without centrality based on chinese remainder theorem is proposed. Members exchanged secret share shadows to generate their own secret shares ,to avoid the authority deception of the trusted center, and identify the deception between members. The group private key is not directly used or exposed in the process of signature, which ensures the reusability and security of the group private key.

As a part of future work, we are cooperating with medical institutions to develop the system based on blockchain, and applying our scheme to test, in order to reconstruct and optimize the smart medical collaborative service technology for the hospital.

Conflict of interest

The authors declare that this work has no conflict of interest.

Acknowledgments

Funding: This research was funded by National Natural Science Foundation of China under Grant No. 61972438 ; Key Research and Development Projects in Anhui Province under Grant No. 202004a05020002; Outstanding youth talent support project in Anhui Province under Grant No.gxyq2019200;Quality engineering project in Anhui Province under Grant No.2020xsxxkc481.

References

[1] I. Lee, O. Sokolsky, "Medical cyber physical systems", in Proceedings of IEEE International Conference and Workshops on Engineering of Computer Based Systems, pp.743-748, 2010.

[2] R. Wang, S. Yu, Y. Li, et al. "Medical Blockchain of Privacy Data Sharing Model Based on Ring Signature". Journal of UEST of China. vol.48, no.6, pp.886-892,2019.

[3] H. Shu, P. Qi, Y. Huang, et al. "An Efficient Certificateless Aggregate Signature Scheme for Blockchain-Based Medical Cyber Physical Systems", Sensors, vol.20, no.5, pp.1521-1545,2020.

[4] A. Liu, X. Du, N. Wang, et al, "Research Progress of Blockchain Technology and Its Application in Information Security", Journal of Software, vol.29, no.7, pp.2092-2115,July 2018.

[5] M. Krotofil, J. Larsen, D. Gollmann, "The process matters: Ensuring data veracity in cyber-physical systems", in Proceedings of the 10th ACM Symposium on Information, Computer and Communications Security, pp.133-144, 2015.

[6] A. Dubovitskaya, Z. Xu, S. Ryu, et al, "Secure and Trustable Electronic Medical Records Sharing using Blockchain".Amia Annual Symposium Proceedings, pp.650-659, 2017.

[7] X. Cheng, F. Chen, D. Xie, et al, "Design of a Secure Medical Data Sharing Scheme Based on Blockchain", J. Medical Syst., vol.44, no.2, 52, Jan. 2020.

[8] C. Chen. "Toward Security and Confidentiality in Personal Health Records via Blockchain Technology", Basic Clinical Pharmacology Toxicology,vol.126,no.s5,10,2020

[9] B. Tu, Y. Chen. "A survey of threshold cryptosystems", Journal of Cryptologic Research", vol.7,no.1, pp.1C14,2020.

[10] S.Nakamoto."Bitcoin: A peer-to-peer electronic cash system".http://bitcoin.org/bitcoin.pdf,2008

[11] X. Fan."Winners, losers and watchers of financial technology", financial view, no.021, pp.42-43, 2017

[12] D. Guegan. "Public Blockchain versus Private blockhain", Universit Paris1 Panthon-Sorbonne ,2017.

[13] T.Xue, Q. Fu, C. Wang, et al, "A Medical Data Sharing Model via Blockchain", Acta Automatica Sinica, vol.43,no.9, pp.1555-1562.2017

[14] A. Azaria, A. Ekblaw, T. Vieira, et al, "Medrec: Using blockchain for medical data access and permission management", in Proceedings of 2nd International Conference on Open and Big Data (OBD) , pp.25-30, 2016.

[15] C.Zhang, Q.Li, Z.Chen, et al, "Medical chain: alliance medical blockchain system", Acta Automatica Sinica,vol.45,no.8, pp.1495-1510,2019

[16] Y.Gao, J.WU, "Efficient Multi-party Fair Contract Signing Protocol based on Blockchains", Cryptologic Res, no.5, pp.556-567,2018.

[17] N.Aitzhan, D.Svetinovic, "Security and Privacy in Decentralized Energy Trading through Multi-signatures, Blockchain and Anonymous Messaging Streams", IEEE Transactions on Dependable and Secure Computing, vol.15, no.5,pp.840-852,2016.

[18] Y. Liu, R. Li, X. Liu, et al, "Enhancing Anonymity of Bitcoin Based on Ring Signature Algorithm",in Proceedings of the 13th International Conference on Computational Intelligence and Security (CIS 2017),pp.317-321,2017

[19] Y. Liang,X.Zhang, Z.Zheng, ”Electronic cash system based on certificateless group signature”, Journal of Communications, vol.37,no.5,pp.184-190,2016.
[20] B. Wang, J. Li, ”A (t,n) threshold signature scheme without a trusted party”, Chinese Journal of Computers,,vol.26,no.11, pp.1581 -1584,2003.
[21] A. Shamir, ”How to share a secret”, Communication of the ACM, vol.22, no.11, pp.612-613, 1979
[22] C.Asmuth, J.Bloom, ”A Modular Approach to Key Safeguarding”, IEEE Transactions on Information Theory ,vol.29,no.2,pp.208-210,1983.
[23] Y. Cheng, H.Liu, ”The Asmuth-Bloom verifiable threshold sharing scheme”, Natural Science Journal of Harbin Normal University,vol.27,no.3, pp.35-38,2011.
[24] T. Wang, S. Hou, ”Research on threshold signature scheme and its security analysis”, Computer Engineering and Applications, vol.54, no.13, pp.123-130,2018.
[25] L. Wang, M. Hu, Z. Jia, et al, ”A Signature Scheme Applying on Blockchain Voting Scene Based on the Asmuth-Bloom Algorithm”, in Proceedings of IEEE 4th International Conference on Computer and Communications, pp.2372-2378, 2018.
[26] Y. Desmedt, ”Society and Group Oriented Cryptography: a New Concept. Advances in Cryptology”, CRYPTO 1987,Lecture Notes in Computer Science, vol 293. Springer, Berlin, Heidelberg,1987
[27] H.Han, M.Huang, Y. Zhang et al, ”An Architecture of Secure Health Information Storage System Based on Blockchain Technology”, in Proceedings of Cloud Computing and Security,ICCCS 2018, Lecture Notes in Computer Science, vol. 11064, Springer, Cham,2018
[28] M. Castro, B. Liskov. ”Practical Byzantine fault tolerance”, in Proceedings of the 3rd Symposium on Operating Systems Design and Implementation, pp.173-186, 1999.
[29] J. Chen, ”Research on Threshold Group Signature Scheme in Blockchain Mode”.Northwestern Normal University,2020
[30] Y. Cheng, Z.Jia, M. Hu, ”Threshold signature scheme suitable for blockchain electronic voting scenes”, Journal of Computer Applications, vol.39,no.9, pp.2629-2635,2019.
[31] X. Fu, ”Proactive Threshold RSA Signature Scheme Based on Polynomial Secret Sharing”, Journal of Electronics and Information Technology, vol. 38, pp. 2280-2286, 2016.