Blockchain-Based Mutual Authentication Protocol with Privacy Protection in Telemedicine

Duo Zhang\textsuperscript{1}, Shangping Wang\textsuperscript{2*}, Qian Zhang\textsuperscript{3}, Yinjuan Deng\textsuperscript{1} and Jifang Wang\textsuperscript{1}

\textsuperscript{1}School of Automation and Information Engineering, Xi’an University of Technology, Xi’an, China
\textsuperscript{2}School of Science, Xi’an University of Technology, Xi’an, China
\textsuperscript{3}School of Computer Science and Engineering, Xi’an University of Technology, Xi’an, China
Email: spwang@mail.xaut.edu.cn

Abstract. Telemedicine builds a patient-centered remote diagnosis and continuous monitoring service system, which can effectively alleviate the current situation of difficult and expensive medical treatment. This paper focuses on mutual authentication with privacy protection in telemedicine. First, we propose a decentralized multi-authority attribute-based signature scheme. The signature scheme can be used to verify the signer’s attributes without leaking the identity information, thereby achieving privacy protection while authenticating. Combined with the proposed signature scheme, a blockchain-based mutual authentication protocol with privacy protection in telemedicine is designed. By this protocol, patients and telemedicine terminal can encrypt and store the medical data off-chain, and store the data digest and decentralized attribute-based signature on the blockchain. As a result, the confidentiality of the data and the authenticity of the source can be guaranteed. In addition, the nature of the blockchain and signature ensure that accurate liability determination can be made when medical disputes occur. Theoretical analysis shows that our protocol is secure and practical.

Keywords. Telemedicine; blockchain; authentication; privacy protection.

1. Introduction
With the demand for long-term care brought about by the aging population structure, the telemedicine industry combined with wireless body area network has entered a brand-new application stage \cite{1}. Telemedicine mainly uses medical IoT devices (blood pressure meters, blood glucose meters, pulse oximeters etc.) to detect various health data of patients and upload it to telemedicine terminals. Doctors monitor patients’ health data in real time and provide management of chronic diseases, health guidance, follow-up and other services. Patients can enjoy rapid and professional medical diagnosis at home, thereby reducing the number of visits to hospitals and the cost of medical treatment.

Owing to the specificity of medical service, it is vital for both patients and telemedicine terminals to verify the authenticity of the source of the medical data \cite{2}. Only legitimate patients can request telemedicine terminals to diagnose their physiological data, so the authentication of the patients should be conducted; In turn, only the legitimate telemedicine terminals can diagnose the patient’s data and return the diagnosis result, so the authentication of the telemedicine terminals should be realized.

In addition, in telemedicine, patients’ physiological data with a large amount of private information need to be transmitted through the network, and hence the openness of the network makes patients face the risk of data and privacy leakage. Moreover, in many cases, patients only want telemedicine
terminals to provide diagnostic services and do not want to reveal their identity information. Therefore, in telemedicine, security requirements such as patient data confidentiality and identity privacy should be fully considered.

Attribute-Based Signature [3, 4] (ABS) provides a very good method to solve the contradiction between authentication and privacy. ABS schemes enable a signer to sign messages utilizing a set of attributes rather than the signer’s identity, and they have been widely used in anonymous authentication systems.

The emerging blockchain [5] technology greatly optimizes existing big data applications due to its distinctive characteristics of decentralization, immutability, openness, anonymity and so on. The combination of blockchain and telemedicine [6] will help ensure the authenticity of medical data and improve the quality of medical services, thus promoting the application of telemedicine and building mobile medical networks. Therefore, it is of great significance to design a mutual authentication protocol based on blockchain in telemedicine.

This paper is committed to addressing the issue of mutual authentication and privacy-protection in telemedicine with the help of ABS and blockchain technology. The contributions of paper are as follows.

• First, we propose a decentralized multi-authority attribute-based signature (DMA-ABS) scheme, in which multiple attribute authorities participate in signature key issue instead of a trusted central authority. Specifically, the DMA-ABS allows the verifier to authenticate the signer’s attributes without knowing the identity of the signer, thus protecting the signer’s identity privacy while authentication.

• Secondly, for telemedicine applications, we design a blockchain-based privacy protection authentication protocol, with which patients and telemedicine terminals can achieve medical data exchange aided by blockchain technology. The protocol can guarantee authentication, data confidentiality and privacy protection at the same time.

• Finally, the security analysis shows that the proposed DMA-ABS scheme and authentication protocol is secure and practical.

2. Related Work

2.1. Attribute-Based Signature

ABS is a cryptographic primitive extended from identity-based signature [3], where the identity of a signer is described to be a set of descriptive attributes instead of a single string. In the ABS scheme, the signer uses the private key associated with a set of attributes to sign the message under specific predicates or policies. Under this concept, what the signature proves is not the identity of the individual who signed the message, but a statement about the attributes owned by the signer. In addition to the unforgeability, non-repudiation and data integrity verification, ABS also provides a strong privacy guarantee for the signer, that is, the signature will not disclose the identity information of the signer.

Maji et al. [4, 7] first formally defined the concept of ABS and its security requirements, and described in detail an ABS construction that supports any predicate structure composed of AND gate, OR gate and threshold gate. Then, Shahandashti et al. [8] and Li et al. [9] proposed ABS schemes supporting \((t, n)\) threshold predicate structure. The dynamic threshold structure adopted by the latter is more flexible than the static threshold structure of the former. The predicate structure in the above scheme is called monotonic predicate structure. In order to expand the flexibility of the predicate structure, Okamoto et al. [10] proposed an ABS scheme with non-monotonic predicate structure, which supports the above predicate structure as well as NOT gate predicate structure. Rao et al. [11] proposed an ABS scheme based on a small attribute domain, in which LSSS access strategy was implemented. Compared with threshold access structure, more flexible fine-grained access control could be achieved. Later, Rao et al. [12] extended their previous work [11] and constructed an ABS scheme under large attribute domain that also supported LSSS access policy.
However, the above signature schemes may suffer from single point of failure and efficiency bottleneck for the setting of single attribute authority. Therefore, the concept of multi-authority ABS (MA-ABS) was introduced. Maji et al. [4, 7] and Li et al. [9] have extended the ABS scheme to multi-authority scenarios, but the security and supported policies are limited due to the original ABS scheme. Cao et al. [13] proposed an MA-ABS scheme based on multiple authorization centers and a trusted central authority (CA). Nevertheless, the CA is given so much power that if it is compromised or corrupted, the security of the system cannot be guaranteed. In addition, the formal security proof of the scheme is not given in this scheme.

In order to solve the security risks brought by CA, Okamoto et al. [14] proposed the first decentralized MA-ABS (DMA-ABS) scheme, in which the trusted central authority is removed, and a global user ID is used to bind the user’s key to prevent collusion attacks. Nevertheless, the scheme is constructed under the random oracle model. Li et al. [15] improved the ABS scheme [9] proposed in 2010, proposed a multi authorization center ABS scheme and proved the unforgeability of the scheme, but the scheme is based on threshold access strategy. Inspired by the decentralizing attribute-based encryption scheme [16] proposed by Lewko et al, Sun et al. [17] proposed a DMA-ABS scheme and showed its application to the privacy preserving verification of electronic health records in healthcare system.

3. System Overview

3.1. Entities
There are six types of entities in the system: administrator, the attribute authorities, IoT devices, patients, telemedicine terminals, and medical blockchain.

Administrator: The administrator is responsible for system initialization, i.e. global public parameters generation. And it also handles user registration, dispute resolution.

Attribute authorities: Multiple attribute authorities jointly participate in key distribution to prevent the single point of failure. An attribute authority manages a certain category or set of attributes and it issues the attribute signature key to the user based on the user’s attributes.

IoT devices: All wearable devices used to monitor patients’ physiological data are referred to IoT devices. Each IoT device corresponds to a unique owner (that is, a patient), and only its owner has access to the data on the IoT device. IoT devices are considered to be resource-constrained in terms of storage, memory and processing capacity.

Patients: Patients, as owners of IoT devices, collect or access personal physiological data from IoT devices, through personal smart phone. Patients achieve efficient personal physiological data management through decentralized storage with IPFS [18]. Patients can request telemedicine services from the telemedicine terminal by sharing their personal physiological data with the telemedicine terminal.

Telemedicine terminal: Telemedicine terminals provide patients with remote medical services. A telemedicine terminal makes diagnosis based on the personal physiological data provided by a patient and returns the diagnostic data to the patient.

Medical Blockchain: The digest of patient’s inquiry data and telemedicine’s diagnosis data as well as the signature on them will be recorded on the medical blockchain. The medical blockchain can be a public or consortium blockchain.

3.2. Workflow
The working flow of the system is shown in figure 1. To illustrate, consider the following scenario: A patient with chronic diseases needs to monitor a certain index of the body daily and follow up regularly. The patient can use telemedicine to reduce unnecessary referrals and improve the quality of health care.
First, the patient collects personal physiological data from IoT devices (as step ①). Then the patient symmetrically encrypts the physiological data and uploads the encrypted data to IPFS decentralized storage, which returns content hash for data addressing (as ②). Next, to request the telemedicine diagnostic service, the patient initiates an inquiry transaction, in which the content hash and its decentralized attribute-based signature are recorded (as ③).

After the transaction is written into the medical blockchain, the telemedicine terminal verifies the patient’s attributes by verifying the decentralized attribute-based signature data in the inquiry transaction. If the verification passes, the patient’s inquiry request will be accepted (as ④). The telemedicine terminal negotiates a session key with the patient for secret communication. The patient informs the telemedicine terminal of the decryption key of his physiological data (as ⑤). The telemedicine terminal downloads the patient’s physiological data from the IPFS system, and decrypts it (as ⑥). Then, the telemedicine terminal makes diagnosis according to physiological data and generates diagnostic data. The telemedicine terminal encrypts the diagnostic data with the key given by the patient and uploads ciphertexts to the IPFS system. IPFS returns the content hash for data addressing (as ⑦). The telemedicine terminal initiates a diagnostic transaction, which takes the content hash of the diagnostic data and its decentralized attribute-based signature as the transaction data (as ⑧).

Once the diagnostic transaction is recorded on the blockchain, the patient verifies the attributes of the telemedicine terminal by verifying the decentralized attribute-based signature data in the diagnostic transaction. If the verification passes, the patient accepts the diagnosis of the telemedicine terminal (as ⑨). The patient obtains the diagnostic results from IPFS according to the content hash in the transaction, and decrypts the diagnostic data using his symmetric key (as ⑩).

3.3. System Model of DMA-ABS
The DMA-ABS scheme proposed in this paper consists of five algorithms ($G\text{Setup}$, $AA\text{Setup}$, $\text{KeyGen}$, $\text{Sig}$, $\text{Ver}$).

- $G\text{Setup}(\lambda) \rightarrow GP$: On input a security parameter $\lambda$, the algorithm outputs global public parameter $GP$. 

Figure 1. System workflow.
• **AASetup**\((GP, i)\) →\((VK_i, MSK_i)\): On input the global public parameter \(GP\), and an attribute \(i\) managed by the authority that calls the algorithm, the algorithm outputs a verification key \(VK_i\) and a master signature key \(MSK_i\) on the attribute \(i\).

• **KeyGen**\((GP, MSK_i, GID, i)\) →\(SK_{i,GID}\): On input the global public parameter \(GP\), the master signature key \(MSK_i\) of attribute \(i\), the user’s unique identifier \(GID\), an attribute \(i\), the algorithm outputs signature key \(SK_{i,GID}\) on attribute \(i\) for user \(GID\).

• **Sig**\((GP, \{SK_{i,GID}\}, M, A)\) →\(\sigma\): On input the global public parameter \(GP\), user’s signature key set \(\{SK_{i,GID}\}\), a message \(M\), and an access control policy \(A\), the algorithm outputs a signature \(\sigma\) over \(M\).

• **Ver**\((GP, \{VK_i\}, M, A, \sigma)\) →\([0, 1]\): On input the global public parameter \(GP\), the verification key set \(\{VK_i\}\), the message \(M\), the access control policy \(A\), and the signature \(\sigma\) over \(M\), the algorithm verifies if \(\sigma\) is a valid signature over \(M\) and outputs 0 or 1.

### 4. System Design

In this section, we describe in detail the concrete construction of a novel DMA-ABS scheme and show how this signature scheme be applied to telemedicine by designing a blockchain-based privacy protection authentication protocol.

#### 4.1. Construction of the Proposed DMA-ABS

Our construction of DMA-ABS is inspired by the decentralizing attribute-based encryption scheme proposed by Lewko et al [16]. For the sake of description, we will term patients and telemedicine providers collectively as users in the DMA-ABS scheme. In our construction, users’ signature keys are assigned by multiple authorities who are independent each other. Each user entering the system will be assigned a global unique identifier \(GID\) to bind user’s signature keys issued by different authorities. The detailed construction of the proposed DMA-ABS scheme is shown as follows:

- **GSetup**\((\lambda)\) →\(GP\): Given a security parameter \(\lambda\), this algorithm chooses two multiplicative cyclic group \(G, G_t\) with order \(P\) and a bilinear map \(e: G × G \rightarrow G_t\). Let \(g\) be a generator of \(G\). It also chooses two hash functions \(H: \{0, 1\}^n \rightarrow G\) and \(H’: \{0, 1\}^n \rightarrow \mathbb{Z}_p\). It outputs the global public parameters as \(GP = \langle p, g, e(g, g), H, H’ \rangle\).

- **AASetup**\((GP, i)\) →\((VK_i, MSK_i)\): It takes as inputs the global public parameters \(GP\) and the attribute \(i\) managed by the caller authority. The algorithm chooses two random numbers \(\alpha_i, y_i \in \mathbb{Z}_p\), and outputs the verification key \(VK_i = \langle e(g, g)^{\alpha_i}, g^{y_i} \rangle \forall i\rangle\), the master signature key \(MSK_i = \langle \alpha_i, y_i \rangle \forall i\rangle\) on attribute \(i\). The validation key will be public, while the signature key will be kept secret.

- **KeyGen**\((GP, MSK_i, GID, i)\) →\(SK_{i,GID}\): It takes as inputs the global public parameters \(GP\), user’s global unique identifier \(GID\), the attribute \(i\) managed by the caller authority as well as the corresponding signature key \(MSK_i\). The signature key \(SK_{i,GID}\) on attribute \(i\) for user \(GID\) can be computed by: \(SK_{i,GID} = \langle g^{y_i}, H(GID)^{y_i} \rangle \forall i\rangle\).

- **Sig**\((GP, \{SK_{i,GID}\}_{i \in ATT}, M, (A, \rho))\) →\(\sigma\): It takes as inputs the global public parameters \(GP\), user’s signature key \(\{SK_{i,GID}\}_{i \in ATT}\), a message \(M\), and a LSSS [19] access control policy \(A, \rho\), where \(A\) is an \(n \times l\) matrix, \(\rho\) maps each row of \(A\) to an attribute \(i \in ATT\). The algorithm randomly chooses numbers \(s \in \mathbb{Z}_p\) and a vector \(v \in \mathbb{Z}_p^l\) with first component \(s\), and computes \(\lambda_s = A_i \cdot v\), where \(A_i\) is the vector corresponding to the \(x\)-th row of \(A\). Then it chooses a random vector \(\omega \in \mathbb{Z}_p^l\) with first
component 0, and computes $\omega_x = A_x \cdot \omega$. For each row of the matrix $A_x$, pick a number $r_x \in \mathbb{Z}_p$ at random, and computes

$$\begin{align*}
\text{Sig}_0 &= e(g, g)^f, \quad \forall x, \\
\text{Sig}_{1,x} &= H(GID)^{\alpha_x}, \\
\text{Sig}_{2,x} &= g^{s(r(H(M)) \cdot \omega_x)}, \\
\text{Sig}_{3,x} &= e(H(GID)^{\mu(r(H(M)))} \cdot g^{r(H(M))} \cdot e(H(GID), g^{\omega_x})),
\end{align*}$$

The algorithm outputs the signature as $\sigma = \{\text{Sig}_0, \text{Sig}_{1,x}, \text{Sig}_{2,x}, \text{Sig}_{3,x}, \forall x\}$.

* $\text{Ver}(GP, \{VK_i\}_{i \in ATT}, M, (A, \rho), \sigma) \rightarrow \{0, 1\}$: It takes as inputs the global public parameter $GP$, the verification key $\{VK_i\}_{i \in ATT}$, the message $M$, the access control policy $(A, \rho)$, and the signature $\sigma$ over $M$. For access control matrix $A$, the algorithm calculates $c_x$ so that $\sum_i c_i A_x = (1, 0, \cdots, 0)$, and determines whether the following equation is true:

$$\text{Sig}_0 = \prod_x \left( \frac{e(\text{Sig}_{2,x}, g) \cdot \text{Sig}_{3,x}}{(e(g, g)^{s(r(H(M)))} \cdot \text{Sig}_0^{r(H(M))} \cdot g^{\omega_x})} \right)^{c_x}$$

If the equation holds, it indicates that the signature came from a user who has attributes that satisfy the claimed access structure. Then the algorithm outputs 1, otherwise it outputs 0 to reject the signature.

Correctness:

$$\begin{align*}
\prod_x \left( \frac{e(\text{Sig}_{2,x}, g) \cdot \text{Sig}_{3,x}}{(e(g, g)^{s(r(H(M)))} \cdot \text{Sig}_0^{r(H(M))} \cdot g^{\omega_x})} \right)^{c_x} &= \prod_x \left( \frac{e(g^{s(r(H(M)))} \cdot g^{\omega_x} \cdot e(H(GID)^{\mu(r(H(M)))} \cdot g^{r(H(M))} \cdot e(H(GID), g^{\omega_x}))}{e(g, g)^{s(r(H(M)))} \cdot e(H(GID)^{\mu(r(H(M)))} \cdot g^{r(H(M))} \cdot e(H(GID), g^{\omega_x}))} \right)^{c_x} \\
&= e(g, g)^{\sum_x \omega_x} \cdot e(H(GID), g)^{\sum_x c_x \alpha_x} \\
&= e(g, g)^f \\
&= \text{Sig}_0
\end{align*}$$

4.2. Blockchain-Based Anonymous Authentication Protocol in Telemedicine

In this protocol, each user (including the patients and telemedicine terminal) is required to create a blockchain account to join the blockchain network. The physiological data of the patient and the diagnostic data of the telemedicine terminal are stored off-chain, and the digest of the data and its DMA-ABS signature will be recorded on the blockchain as the transaction data. The DMA-ABS signature can be used to verify the attributes of the signer without knowing its identity, so that privacy protection can be achieved during authentication.

This protocol consists of four phases: system setup, user registration, patient inquiry, telemedicine diagnosis.

4.2.1. System Setup. The system setup phase is mainly to initialize the system parameters. The establishment of the system can be divided into two parts: global setup and authority setup.

1) Global Setup: The administrator runs the algorithm $G\text{Setup}(\lambda)$ of the proposed DMA-ABS scheme, and publishes its output: public parameters $GP$.

2) Authority Setup: An attribute authority who manages attributes $i$ runs the algorithm $A\text{ASetup}(GP, i)$ which outputs a verification key $VK_i$ and a master signature key $MSK_i$ on the attributes $i$. The attribute authority publishes $VK_i$ and keeps the $MSK_i$ secret.
4.2.2. User Registration. All users need to register when they enter the system, and the registration process can be divided into identity registration and key distribution.

(1) Identity registration: Users submit their real identity certificate and blockchain account address to the administrator to request identity registration. After authenticating the user’s identity certificate, the administrator issues a global unique identifier GID to the user requesting registration, and binds it to the user’s blockchain account. It should be noted that the specific relevance between the real identity and blockchain accounts is kept secret, unless there is a medical dispute.

(2) Key distribution: A user GID requests signature key distribution from different attribute authority by submitting his identity and attribute certificate. Assume that the user’s attribute set is \( ATT = \{i\} \). For attribute \( i \in ATT \), the attribute authority managing this attribute runs the algorithm \( \text{KeyGen}(GP, MSK_i, GID, i) \) that outputs the signature key \( SK_{i, GID} \). The authority will transmit \( SK_{i, GID} \) to the user GID through the secure channel. The user can get the signature key \( SK_{GID} = \{SK_{i, GID}\}_{i \in ATT} \) by integrating the keys distributed by different authorities.

4.2.3. Patient Inquiry. (1) Data collection: A patient collects personal physiological data on IoT devices through personal smart devices.

(2) Data uploading: In order to ensure the confidentiality of the patient’s personal data, the patient will symmetrically encrypt the data with the symmetric key \( k \). The patient uploads ciphertexts to the decentralized storage platform IPFS, and then keeps the content hash \( h \) returned by IPFS, as well as the symmetric key \( k \).

(3) Inquiry: The patient signs hash \( h \) under an expressive LSSS access structure \( (A, \rho) \), and the signature \( \sigma \) can be generated by running the algorithm \( \text{Sig}(GP, \{SK_{i, GID}\}_{i \in ATT}, h(A, \rho)) \). Then the patient initiates an inquiry transaction:

\[
\text{Trans}_{\text{inq}} = (h, \sigma, (A, \rho), \{VK_i\}_{i \in ATT}, \sigma_{\text{Trans}_{\text{inq}}})
\]

4.2.4 Telemedicine Diagnosis. For the telemedicine terminal:

(1) Authentication: When telemedicine terminal monitors an inquiry transaction, it verifies signature \( \sigma \) on hash \( h \) with claim access structure \( (A, \rho) \), running the algorithm \( \text{Ver}(GP, \{VK_i\}_i, h(A, \rho), \sigma) \). The algorithm outputs 0 to reject the signature, or 1 to accept the signature that means the signature does come from the patient who owns attributes involved in the claim access structure \( (A, \rho) \). Thus, the patient’s attributes can be verified without knowing the patient’s identity.

(2) Key Agreement: After authentication is passed, the patient and the telemedicine terminal negotiate (such as Diffie-Hellman key agreement) a session key for secret communication. The patient sends the symmetric key \( k \) to the telemedicine terminal with session key. Then the telemedicine terminal downloads the patient’s physiological data from IPFS and decrypts it with the symmetric key \( k \).

(3) Diagnosis: After obtaining the physiological data of the patient, the telemedicine terminal carries out medical diagnosis and generates diagnostic data. The diagnostic data is encrypted with the symmetric key \( k \) received from the patient and then uploaded to IPFS that will return the content hash \( h' \). The telemedicine terminal generates the signature \( \sigma' \) on hash \( h' \) with claim access structure \( (A', \rho') \) by running the algorithm \( \text{Sig}(GP, \{SK_{i, GID}\}_{i \in ATT'}, h'(A', \rho')) \), where \( GID' \) is the global identity identifier of the telemedicine terminal, and \( ATT' \) is the attribute set of the telemedicine terminal. Then the telemedicine terminal initiates the diagnosis transaction to the patient:

\[
\text{Trans}_{\text{diag}} = (h', \sigma', (A', \rho'), \{VK_i\}_{i \in ATT'}, \text{txid}, \sigma_{\text{Trans}_{\text{diag}}})
\]
For patient:

When the diagnostic transaction of telemedicine terminal is monitored, the patient verifies signature \( \sigma' \) on hash \( h' \) with claim access structure \( (A', \rho') \), running the algorithm \( \text{Ver}(GP, \{VK\}, h', (A', \rho'), \sigma) \) that outputs 1 to accept the signature or 0 to reject. If the authentication is successful, the patient can verify that the signature \( \sigma' \) is indeed signed by the owner of the attributes corresponding to access structure \( (A', \rho') \). The patient then downloads the diagnostic data from IPFS according to the content hash \( h' \) and decrypts it with his symmetric key \( k \).

5. Security Analysis

5.1. Unforgeability

We illustrate the unforgeability of the DMA-ABS scheme in two cases.

Case 1: A malicious user has no attribute \( i \), but he wants to forge a signature about this attribute to pretend to the verifier that he has this attribute. Because the malicious user does not have attribute \( i \), he cannot calculate the value of \( g^{a_{\rho(x)}} r^{H(M)} \) and \( e(H(GID)^{\rho(x)}, g^r r^{H(M)}) \) when he forges the signature components \( \text{Sig}_{2,x} \) and \( \text{Sig}_{3,x} \) for \( x: \rho(x) = i \). Thus, it is impossible for the malicious user to forge the signature with attribute \( i \) he does not own.

Case 2: An adversary, who has tampered with the message \( m \), needs to tamper with the signature of \( m \). The adversary can directly misappropriate \( m \)'s partial signature \( \text{Sig}_0 \) and \( \text{Sig}_1 \), but he needs to forge \( \text{Sig}_{2,x} \) and \( \text{Sig}_{3,x} \). However, the adversary cannot obtain \( g^b \) and \( e(H(GID), g^{m_y}) \) in \( \text{Sig}_{2,x} \) and \( \text{Sig}_{3,x} \) respectively. Therefore, the adversary cannot successfully forge the signature of a new message.

5.2. Collusion Attack

We consider two types of collusion attacks: collusion between users and collusion between authorities.

For the collusion attack between users: The scheme uses the global identifier GID to bind the user signature keys from different authorities. Consider two users with global identifiers \( GID_1 \) and \( GID_2 \), and attributes sets \( S_1 \) and \( S_2 \) respectively, they would like to combine their signature key to forge the signature of the attribute set \( S \subseteq S_1 \cup S_2 \). For each \( i \in S \), they need to calculate \( e(H(GID)^{\rho(x)}, g^r r^{H(M)}) \) when forging \( \text{Sig}_{3,x} \), where \( x: \rho(x) = i \). However, the user \( GID_1 \) gets \( e(H(GID_1)^{\rho(x)}, g^r r^{H(M)}) \) for \( i \in S_1 \) and the user \( GID_2 \) gets \( e(H(GID_2)^{\rho(x)}, g^r r^{H(M)}) \) for \( i \in S_2 \). These two different items cannot be merged. Hence, they cannot forge signatures on the attribute set \( S \), that is, collusion attack between users will not succeed.

For the collusion attack between authorities: Assume that the attributes of the user come from \( t \) different authorities. Unless the number of authorities initiating the collusion attack is \( t \), the signature of that user cannot be forged.

5.3. Mutual Authentication

The digest of inquiry data of the patient is stored on the blockchain as well as its DMA-ABS signature. The telemedicine terminal can realize the attribute authentication of the signer by verifying the DMA-ABS signature. The telemedicine terminal also records diagnostic data and its DMA-ABS signature on the blockchain, and the patient can also authenticate the attribute of the signer without knowing his identity. In this way, we achieve anonymous two-way authentication.
5.4. Traceability
When medical disputes occur, it is often necessary to identify the responsibility. In this scheme, the patient’s inquiry data, as well as the telemedicine terminal’s diagnostic data are all recorded on the blockchain in the form of transactions, and each transaction is signed by the transaction initiator. By the nature of blockchain (openness, tamper-resistant and so on) and digital signature (unforgeability, non-repudiation and so on), the traceability of all behaviors can be guaranteed.

6. Conclusion
The authentication in telemedicine has high demand for privacy protection, including medical data privacy and identity privacy of both interacting parties. In this paper, we construct a DMA-ABS scheme to support mutual authentication with privacy protection. Then combined with the proposed signature scheme, we design a blockchain-based anonymous authentication protocol for telemedicine applications. The introduction of DMA-ABS can realize mutual anonymous authentication between patients and telemedicine terminals in telemedicine. In addition, the storage model that combines on-chain and off-chain enables data security sharing between the patients and telemedicine terminals. Off-chain storage can avoid the storage bottleneck of the blockchain, while on-chain storage anchors the data behavior on the blockchain to ensure that the data is tamper-proof, unforgeable, and verifiable. The security analysis shows that the protocol is secure and practical. In the future, we will consider giving formal security proof of the proposed DMA-ABS scheme. Furthermore, we plan to deploy the prototype of the protocol on blockchain platforms such as Ethereum or Hyperledger, to evaluate the performance of our protocol more systematically.

Acknowledgments
This work was supported by the National Natural Science Foundation of China [grant number 61572019] and the Shaanxi Province Key Research and Development Program [grant number 2020GY-006].

References
[1] Waller M and Stotler C 2018 Telemedicine: A primer Current Allergy and Asthma Reports 18 (10) 54.
[2] Garg V and Brewer J 2011 Telemedicine security: A systematic review Journal of Diabetes Science and Technology 5 (3) 768-77.
[3] Shamir A 1985 Identity-based cryptosystems and signature schemes Advances in Cryptology - CRYPTO’84 pp 47-53.
[4] Maji H K, Prabhakaran M and Rosulek M 2008 Attribute-based signatures: Achieving attribute-privacy and collusion-resistance IACR Cryptology ePrint Archive. Available from: https://eprint.iacr.org/2008/328.pdf.
[5] Nakamoto S 2008 Bitcoin: A peer-to-peer electronic cash system Available from: https://bitco.in/bitcoin.pdf.
[6] Hasselgren A, Králevska K, Gligoroski D, Pedersen S A and Faxvaag A 2020 Blockchain in healthcare and health sciences—A scoping review Int. J. Med. Inf. 134 104040.
[7] Maji H K, Prabhakaran M and Rosulek M 2011 Attribute-based signatures Topics in Cryptology–CT-RSA 2011 pp 376-92.
[8] Shahandashti S F and Safavi-Naini R 2009 Threshold attribute-based signatures and their application to anonymous credential systems Progress in Cryptology – AFRICACRYPT 2009 pp 198-216.
[9] Li J, Au M H, Susilo W, Xie D and Ren K 2010 Attribute-based signature and its applications Proceedings of the 5th ACM Symposium on Information, Computer and Communications Security pp 60-9.
[10] Okamoto T and Takashima K 2011 Efficient attribute-based signatures for non-monotone predicates in the standard model Public Key Cryptography–PKC 2011 pp 35-52.
[11] Rao Y S and Dutta R 2014 Expressive bandwidth-efficient attribute based signature and signcryption in standard model Information Security and Privacy 209-25.

[12] Rao Y S and Dutta R 2016 Efficient attribute-based signature and signcryption realizing expressive access structures Int. J. Inf. Secur. 15 (1) 81-109.

[13] Cao D, Zhao B, Wang X, Su J and Ji G 2011 Multi-authority attribute-based signature 2011 Third International Conference on Intelligent Networking and Collaborative Systems pp 668-72.

[14] Okamoto T and Takashima K 2013 Decentralized attribute-based signatures Public-Key Cryptography–PKC 2013 pp 125-42.

[15] Li J, Chen X and Huang X 2015 New attribute-based authentication and its application in anonymous cloud access service Int. J. Web. Grid. Serv 11 (1) 125-41.

[16] Lewko A and Waters B 2011 Decentralizing attribute-based encryption Advances in Cryptology–EUROCRYPT 2011 pp 568-88.

[17] Sun Y, Zhang R, Wang X, Gao K and Liu L 2018 A decentralizing attribute-based signature for healthcare blockchain 2018 27th International Conference on Computer Communication and Networks pp 1-9.

[18] Benet J 2014 IPFS—Content addressed, versioned, P2P file system arXiv:1407.3561p. https://ui.adsabs.harvard.edu/abs/2014arXiv1407.3561B.

[19] Waters B 2011 Ciphertext-policy attribute-based encryption: An expressive, efficient, and provably secure realization Public Key Cryptography–PKC 2011 pp 53-70.