IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

SPECIAL SECTION ON RESEARCH CHALLENGES AND OPPORTUNITIES IN SECURITY AND PRIVACY OF BLOCKCHAIN TECHNOLOGIES

Received December 21, 2017, accepted January 29, 2018, date of publication February 2, 2018, date of current version March 16, 2018.

Digital Object Identifier 10.1109/ACCESS.2018.2801266

Secure Attribute-Based Signature Scheme With Multiple Authorities for Blockchain in Electronic Health Records Systems

RUI GUO[1,2,5], HUIXIAN SHI[3], QINGLAN ZHAO[1,4], AND DONG ZHENG[1,5]

[1]National Engineering Laboratory for Wireless Security, Xi'an University of Posts and Telecommunications, Xi'an 710121, China
[2]State Key Laboratory of Networking and Switching Technology, Beijing University of Posts and Telecommunications, Beijing 100876, China
[3]Department of Mathematics and Information Science, Shaanxi Normal University, Xi'an 710062, China
[4]School of Information Security Engineering, Shanghai Jiao Tong University, Shanghai 200240, China
[5]Westone Cryptologic Research Center, Beijing 100070, China

Corresponding author: Rui Guo (guorui@xupt.edu.cn)

This work was supported in part by the National Key Research and Development Program of China under Grant 2017YFB0802000, in part by the Natural Science Foundation of China under Grant 61472472 and Grant 11501343, in part by the Innovation Ability Support Program in Shaanxi Province of China under Grant 2017KJXX-47, in part by the Natural Science Basic Research Plan in Shaanxi Province of China under Grant 2016JM6033, and in part by the Open Foundation of State Key Laboratory of Networking and Switching Technology, Beijing University of Posts and Telecommunications, under Grant SKLNST-2016-2-11.

ABSTRACT Electronic Health Records (EHRs) are entirely controlled by hospitals instead of patients, which complicates seeking medical advices from different hospitals. Patients face a critical need to focus on the details of their own healthcare and restore management of their own medical data. The rapid development of blockchain technology promotes population healthcare, including medical records as well as patient-related data. This technology provides patients with comprehensive, immutable records, and access to EHRs free from service providers and treatment websites. In this paper, to guarantee the validity of EHRs encapsulated in blockchain, we present an attribute-based signature scheme with multiple authorities, in which a patient endorses a message according to the attribute while disclosing no information other than the evidence that he has attested to it. Furthermore, there are multiple authorities without a trusted single or central one to generate and distribute public/private keys of the patient, which avoids the escrow problem and conforms to the mode of distributed data storage in the blockchain. By sharing the secret pseudorandom function seeds among authorities, this protocol resists collusion attack out of N from $N-1$ corrupted authorities. Under the assumption of the computational bilinear Diffie-Hellman, we also formally demonstrate that, in terms of the unforgeability and perfect privacy of the attribute-signer, this attribute-based signature scheme is secure in the random oracle model. The comparison shows the efficiency and properties between the proposed method and methods proposed in other studies.

INDEX TERMS Attribute-based signature (ABS), blockchain, electronic health records (EHRs), multiple authorities, preserve privacy.

I. INTRODUCTION

Electronic Health Records (EHRs) provide a convenient health record storage service, which promotes traditional patient medical records on paper to be electronically accessible on the web. This system was designed to allow patients to possess the control of generating, managing and sharing EHRs with family, friends, healthcare providers and other authorized data consumers. Moreover, provided that the healthcare researcher and providers of such service access these EHRs across-the aboard, the transition program of healthcare solution is expected to be achieved. However, in the current situation, patients scatter their EHRs across the different areas during life events, causing the EHRs to move from one service provider database to another. Therefore, the patient may lose control of the existing healthcare data, while the service provider usually maintains the primary stewardship [1]. Patient access permissions to EHRs are very limited, and patients are typically unable to easily share these data with researchers or providers. Interoperability challenges between different providers, hospitals, research

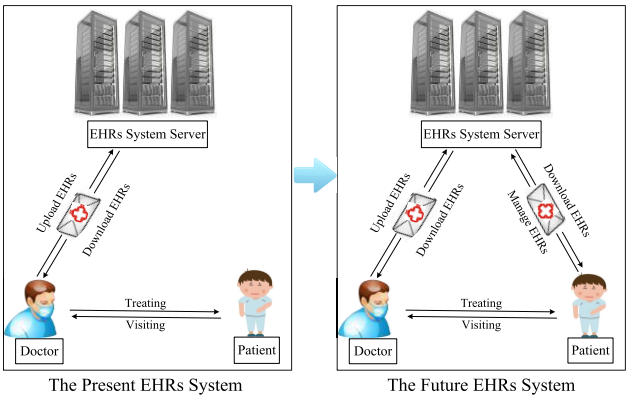


FIGURE 1. EHRs system in the present and future. The patient should have right to access his EHRs for managing and sharing them independently.

institutions, etc. add extra barriers to high-performance data sharing. Without coordinated data management and exchange, the health records are fragmented instead of cohesive [2]. If the patient has the capability of managing and sharing his EHRs securely and completely, as shown in Fig. 1, regardless of the research purpose or the data sharing among healthcare providers, the healthcare industry will benefit greatly. Drawing support from blockchain technology, the proposed method accomplishes this goal to promote cooperation in the way of deep mutual trust between each organization.

Blockchain technology was formerly developed for the cryptocurrency Bitcoin and was first presented in the Bitcoin whitepaper by Nakamoto [3] in 2008. Since blockchain technology appeared, it has been celebrated as a new technological revolution just like the invention of the steam engine or the Internet because of its huge impaction on society. In a 2015 World Economic Forum report, 58% of survey respondents expected that 10% of global Gross Domestic Product (GDP) will be relevant to the blockchain technology through 2025 [4].

Previously, many restrictions have been placed on sharing massive EHRs because of the risks to data security or leakage of private patient information during data exchange. Furthermore, current EHRs are managed by hospitals and providers, whereas patients are deprived of the right to freely control their own EHRs. Through utilizing blockchain technology, standards for recording data and managing identity are established, and the blockchain of EHRs is constructed. In addition, this technology records the auditing traces of all transactions in an immutable distributed ledger, which guarantees responsibility and transparency in the procession of data exchange. Therefore, the patient has the ability to record healthcare and diagnostic information from doctors in their own EHRs, thus reducing the number of medical accidents and preserving patient privacy.

The Institute for Business Value at IBM issued a whitepaper titled, ''Healthcare rallies for blockchains: Keeping patients at the center'' [5]. This investigation shows that, for the healthcare industry, more than 70% of industry leader predict that the greatest advantage of blockchain technology is contributing to manage clinical trial records, supervised compliance and EHRs. Blockchain in the healthcare industry provides a secure, decentralized framework for the controlled sharing of patient EHRs, and blockchain is the perfect solution to EHRs and data exchange.

Blockchain is a decentralized database whose data block is connected chronologically. In the healthcare industry, there are many different parties who need to collaboratively manage personal EHRs blockchain (in a model of consortium blockchain), such as medical specialists, hospitals, insurance departments, etc. A variety of parties can lead to resource-intensive authentication and the costly information processes for all the stakeholders involved [6]. Based on the Ethereum blockchain technology, the Gem Health Network [7] was constructed to facilitate the access of different healthcare specialists and departments to patient data, reduce health resource waste and treat important illnesses rapidly. In this scenario, the EMRs (in the form of blockchain) of patients should be authenticated based on ownership to avoid misdiagnoses before making accurate diagnoses into block. Furthermore, EMRs stored in block includes name, ID, allergy history and other sensitive data. According to the guidelines of the Health Insurance Portability and Accountability Act (HIPPA) [8], the privacy of patients should be preserved in the process of sharing EHRs [9]–[13].

In authentication, for conforming to the characteristics of multiple departments, an attribute-based signature with multiple authorities [14] provides an effective solution to protect the privacy in EHRs systems while attesting that the endorsement derived from the correct patient.

A. RELATED WORKS

Sahai and Waters [15] first examined the attribute based framework as a powerful tool to construct a variety of cryptographic primitives. Attribute-based signature (ABS) enables user identifying information to be hidden and the signer to have fine-grained control over his identifying information in the course of endorsing a message. The signature only reveals that the verified message must be endorsed from a signer whose attributes satisfy the predicate. ABS provides a strong guarantee for the signer on privacy while a strong guarantee for the verifier on unforgeability. In 2007, Khader [16] introduced the prototype of ABS in the form of a group signature. However, the formal definition of ABS was first presented in another study [14], [17], which covered threshold predicates as special cases. Though these protocols were high-performance and practical, the security was analyzed only in the generic group model. Li *et al.* [18] and Herranz *et al.* [19] put forward ABS schemes and proved that these two schemes were secure in the standard model respectively. However, they did not assess adaptive-predicate unforgeability and privacy (i.e., fully security). Under the standard model and based on another study [14], Okamoto and Takashima [20] introduced a fully secure

ABS scheme that supported the non-monotone predicate. However, their general form is not efficient enough in practice. To make progress on the efficiency, based on threshold access structure, Chen *et al.* [21] published an attribute-based short signature protocol with fully security. Unfortunately, this scheme has a single authority that is insufficient to fit the distributed system. Rao and Dutta [22] addressed the puzzle of designing ABS scheme with constant number of the bilinear pairing operation for verification and the short signature for more general policy. For achieving a stronger form and supporting a wide class of predicates, Sakai *et al.* [23] presented an ABS scheme that can be used arbitrary circuit as the predicate with practical efficiency. To reduce the computational cost, Gu *et al.* [24] proposed a more efficient ABS scheme with the monotone predicates than that in the standard model by Maji. Aimed at guaranteeing the integrity of e-health records, Liu *et al.* [25] designed a general ABS scheme that was highly efficient and secure online/offline. Cui *et al.* [26] introduced the notion of escrow free ABS scheme with revealability to weaken the dependence on the attribute authority. Moreover, this proposal allowed the user to demonstrate evidence to the verifier whether he is the right signer. Nevertheless, all these schemes have a single authority that is insufficient to meet the characteristics of the distributed system except of [14] and [18]. Although these two schemes could be extended to the scenarios of multi-authority, the security and the policy supported in design is limited on account of the original ABS scheme [27].

B. OUR CONTRIBUTIONS

In this paper, to meet the requirement of blockchain in distributed EHRs systems, we construct an attribute-based signature (MA-ABS) scheme with multiple authorities. Taking advantage of ABS with the blockchain technology, this proposal could preserve the privacy of patients and maintain the immutability of EHRs. The contributions of this work are as follows:

- First, combing the blockchain technology and the construction of Maji et al., this work proposed an ABS scheme with multiple authorities in an EHRs system for monotone predicates, and the number of the bilinear pairing involving in **Signing** is linearly increased with the number of authorities.
- Second, the primary challenge for multiple authorities is collusion attack. To address this risk, a pseudorandom function seed is shared in every two authorities and preserved secretly. Moreover, in **KeyGen**, the private key of each authority is embedded into the private key of the patient. According to this structure, the protocol resists $N-1$ corrupted authorities collusion attacks.
- Finally, under the computation bilinear Diffie-Hellman assumption, we prove that, in the random oracle model, the proposal is unforgeable in suffering a selective predicate attack, and it enjoys the perfect privacy for the signer, which prevents the privacy for patient data leakage. Furthermore, we make a comparison between the proposed method and other typical works on cost and property. It demonstrates that this proposal generally offers better performance.

C. ORGANIZATION

The remainder of this work is as follows. Section II demonstrates a concise overview of the bilinear map, related computational assumptions and definitions, and blockchain in an EHRs system. In Section III, a detailed ABS with multiple authorities for an EHRs system is discussed. Section IV proves the security of the proposal as well as evaluates the theoretical performance. Finally, Section V concludes the paper.

II. PRELIMINARIES

Definitions and notations employed in this work are defined below.

A. BILINEAR MAP

Suppose that $(G, +)$ and $(G_T, \times)$ are the prime q-order cyclic groups. A bilinear pairing map $\hat{e} : G \times G \to G_T$ possesses the follow properties:

- *Bilinearity*: For any $P, Q \in G$ and $a, b \in Z_q^*$, it has $\hat{e}(aP, bQ) = \hat{e}(P, Q)^{ab}$.
- *Non-degeneracy*: There exists $P, Q \in G$ such that $\hat{e}(P, Q) \neq 1_{G_T}$.
- *Computability*: For any $P, Q \in G$, there is an efficient algorithm to compute $\hat{e}(P, Q)$.

B. COMPUTATIONAL ASSUMPTIONS

There is a finite cyclic group G with prime order q, and $a, b, c, n \in Z_q^*$ are picked out randomly. The difficult problems bellows underlying the security of this scheme.

Definition 1 (Discrete Logarithm (DL) Problem): Given two elements $P, Q \in G$, find an integer n to satisfy the equation $Q = nP$.

Definition 2 (Computational Bilinear Diffie-Hellman (CBDH) Problem): Given random elements $\{A = aP, B = bP, C = cP\} \in G^3$ and the bilinear pairing map $\hat{e} : G \times G \to G_T$, it is computing the value $\hat{e}(P, P)^{abc}$.

The CBDH assumption asserts that there exists no probabilistic polynomial-time algorithm $\mathcal{B}$ to successfully solve the CBDH problem, i.e., for any positive number $\varepsilon > 0$, the equation $\Pr[\mathcal{B}(A, B, C) = \hat{e}(g, g)^{abc}] < \varepsilon$ holds.

C. PREDICATES

Definition 3: Suppose that $P_a = \{P_{a_1}, P_{a_2}, \cdots, P_{a_n}\}$ is a parties set and there is a monotone collection $\mathbb{A} \in 2^{\{P_{a_1}, P_{a_2}, \cdots, P_{a_n}\}}$. For all D, E, if $D \in \mathbb{A}$ and $D \subseteq E$, it has $E \in \mathbb{A}$. Moreover, the access structure $\mathbb{A}$ (monotone access structure) is called a collection (monotone collection) of non-empty subsets of $\{P_{a_1}, P_{a_2}, \cdots, P_{a_n}\}$, i.e., $\mathbb{A} \subseteq 2^{\{P_{a_1}, P_{a_2}, \cdots, P_{a_n}\}} \setminus \{\emptyset\}$. Thus, this set belonging to $\mathbb{A}$ is an authorized set. Otherwise, this is an unauthorized set.

Definition 4: Suppose that S is the universe of the attributes. There is a predicate over S that is a monotone

Boolean function, whose inputs are associated with the attributes of S. There exists another attribute set $W \in S$ that is considered to satisfy the predicate Υ if $\Upsilon(W) = 1$. The value is set to 1 (i.e., true), its corresponding attribute is a member of W. Otherwise, it is set to 0 (i.e., false).

Note that, because Υ is the monotone predicate, the equation $\Upsilon(W) = 1$ implies $\Upsilon(V) = 1$ for every attribute set $W \subset V$.

D. NOTATIONS

In this work, a user is described by the attribute, and the authorized set is included in an access tree structure $\mathbb{T}$, which is a monotone access tree. A data verifier could receive the signature only if his attribute satisfies the access tree embedded in signature. To facilitate the description, access tree $\mathbb{T}$ contains $\langle x, num_x, k_x, parent(x), att(x), index(x)\rangle$, which are defined as follows.

- *x:* This represents a node of the access tree $\mathbb{T}$. Each interior node is threshold gate, e.g., "AND" or "OR" gates, while leaves are associated with attributes. For example, in Fig. 2, the node A denotes a threshold gate.

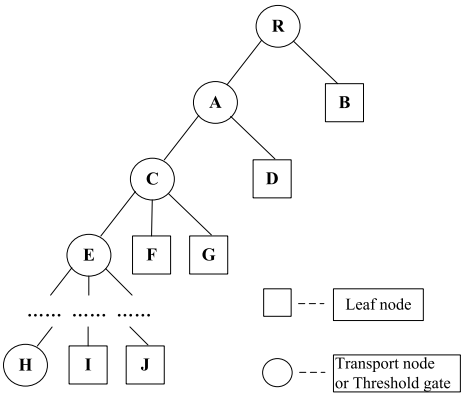


FIGURE 2. A monotone access tree structure. Only if the attribute of the bearer satisfies the predicate embedded in signature will he be allowed to access the record.

- num_x: This represents the number of children in node x in $\mathbb{T}$. For instance, in Fig. 2, num_C is equal to 3.
- k_x: This represents the threshold value of x, and $0 < k_x \leq num_x$. For $k_x = 1$, the threshold gate is considered an OR gate while $k_x = num_x$ indicating that it is an AND gate. Specially, if x is a leaf node, k_x is equal to 1. For instance, in Fig. 2, $k_A = 2$ means that it is an AND gate.
- $parent(x)$: This is the parent of x. Fox example, $parent$ (A) denotes the root node R.
- $att(x)$: This is an attribute value on the leaf node x in $\mathbb{T}$.
- $index(x)$: This denotes the number associated with x; the value is from 1 to num_x, which is assigned to x for a designated key.

E. SYNTAX OF MA-ABS

Definition 5: The MA-ABS scheme in EHRs system has five algorithms as follows.

- **Setup** $(1^\lambda) \rightarrow params$: It inputs the security parameter 1^λ and then outputs the public parameters of this system *params*.
- **Authority Setup** $(1^\lambda) \rightarrow (PK_k, SK_k)$: This algorithm is executed by the authority. Every authority A_k generates his public and private key (PK_k, SK_k), where $k \in \{1, 2, \ldots, N\}$, and N denotes the number of authority in this system.
- **KeyGen** $(SK_k, GID, S) \rightarrow (PK_U, SK_U)$: This algorithm is controlled by each authority A_k and patient U. It inputs the private key SK_k of A_k, the global identifier GID of the patient and an attribute set S; then the algorithm returns the public and private keys (PK_U, SK_U) of the patient.
- **Sign** $(PK_k, SK_U, M, \Upsilon) \rightarrow \sigma$: To sign a message M under the predicate Υ, it inputs the public key PK_k of A_k, the private key SK_U and the predicate Υ; then the algorithm outputs the signature σ of M.
- **Verify** $(PK_U, S, \sigma, M, \Upsilon) \rightarrow Accept/Reject$: To verify a signature σ on a message M with predicate Υ, it inputs the public key PK_U of the patient with attribute set S and the signature with predicate Υ. First, if the attributes of the data verifier do not satisfy Υ, it returns *null*. Otherwise, only if the attribute set S satisfies the predicate, will this algorithm verify the correctness of signature σ and return *Accept* or *Reject*.

F. SECURITY DEFINITIONS

The foremost character of the ABS scheme in security is the property of unforgeability, even though it may suffer from a group of colluding users or authorities attack. For more details, the unforgeability is defined on executing the following game between a challenger $\mathcal{C}$ and a forger $\mathcal{F}$.

- *Setup*: The challenger $\mathcal{C}$ selects a security parameter 1^λ and performs **Setup;** then, it transmits the public parameters *params* to the forger $\mathcal{F}$. $\mathcal{F}$ submits a challenging predicate Υ^* as well as a list of corrupted authorities L_A to the challenger $\mathcal{C}$.
- *Authority Setup*: For the corrupted authority, the challenger $\mathcal{C}$ delivers the public and private keys (PK_k, SK_k) to the forger $\mathcal{F}$. Otherwise, for the honest authority, $\mathcal{C}$ delivers the public key PK_k to $\mathcal{F}$.
- *Queries*: $\mathcal{C}$ initializes an integer $i = 0$ in the empty list $L = \{i, S, SK_U\}$, and $\mathcal{F}$ is allowed to execute the oracles as follows.
  - *Private Key Extraction Oracle*: Upon receiving an integer i and an attribute set S, $\mathcal{C}$ returns SK_U to the forger $\mathcal{F}$ if such an entry exists in the list L. Otherwise, if no such entry, the challenger runs **KeyGen** and outputs SK_U after adding the new entry $\{i, S, SK_U\}$ into the list L.
  - *Signing Oracle*: Upon receiving a message M and a predicate Υ, $\mathcal{C}$ returns a signature σ by running **Sign**.
- *Forgery*: Finally, the forger $\mathcal{F}$ outputs a tuple of (M^*, σ^*) with the predicate Υ^*.

The forger $\mathcal{F}$ wins the game above provided that (1) σ^* is a valid signature on M^* with Υ^*, (2) for any queried attribute set S, $\Upsilon^*(S) \neq 1$, and (3) the forger $\mathcal{F}$ has not queried the *Signing Oracle* on the tuple (M^*, Υ^*). Accordingly, the advantage of winning this game by $\mathcal{F}$ is defined as the probability in $Adv^{EUF}_{MA-ABS,\mathcal{F}}(\lambda)$.

Definition 6 (Unforgeability): A forger $\mathcal{F}$ could $(t, q_H, q_P, q_S, \varepsilon)$-break a MA-ABS scheme if $\mathcal{F}$ executes the game at most t in time, and makes at most q_H hash function queries, q_P *Private Key Extraction Oracle* queries and q_S *Signing Oracle* queries while the advantage $Adv^{EUF}_{MA-ABS,\mathcal{F}}(\lambda)$ is at least ε. A MA-ABS scheme is $(t, q_H, q_P, q_S, \varepsilon)$-unforgeable, if no probabilistic polynomial-time forger exists that could $(t, q_H, q_P, q_S, \varepsilon)$-break it.

Definition 7 (Perfect Privacy): An MA-ABS scheme is perfectly private, provided that, for all the parameters $params \leftarrow \mathbf{Setup}(1^\lambda)$, all the messages M, all the attribute sets S_1 and S_2, all the private keys $SK_{S_1} \leftarrow \mathbf{KeyGen}(SK_k, GID, S_1)$ and $SK_{S_2} \leftarrow \mathbf{KeyGen}(SK_k, GID, S_2)$, all the predicates Υ, such that $\Upsilon(S_1) = \Upsilon(S_2) = 1$, the distributions $\mathbf{Sign}(PK_k, SK_{S_1}, M, \Upsilon)$ and $\mathbf{Sign}(PK_k, SK_{S_2}, M, \Upsilon)$ are equal.

Since the correct signature distribution can be perfectly simulated without depending on any specific private information, the signature must not leak any private signer information.

G. MA-ABS FOR HEALTHCARE IN THE BLOCKCHAIN APPLICATION

Blockchain is considered as a new technological revolution that was introduced as the backbone of the Bitcoin cryptocurrency. It is a peer-to-peer distributed ledger technology to record transactions, agreements, and sales. The benefits of the blockchain technology are decentralized maintenance, data saving in the block-then-chain structure, secure transporting and accessing of data as well as anti-tamper and undeniable data security [28]. Taking advantage of these distinguishing features above in an EHRs system, blockchain enables the management of authentication, confidentiality, accountability and data sharing while handing information related to privacy, medical resource saving and facilitating for the patient, and making population healthcare smarter.

Assuming that there is an EHRs system in a cloud storage platform, which consists of some departments, such as hospitals, pharmaceutical departments, insurance departments, disease research departments and so on, EHRs systems can be jointly managed. All departments can offer services for patients together and restrict the rights of each department to prevent EHRs abuse. Thus, an EHRs system with a blockchain structure is designed as shown in Fig. 3. Suppose that every patient owns one blockchain of healthcare alone. After being treated in a hospital, all the information including EHRs, consumption records, insurance records, etc. is encapsulated in one block. Patient treatments at different times will be generated in different blocks. Then, a series of blocks are

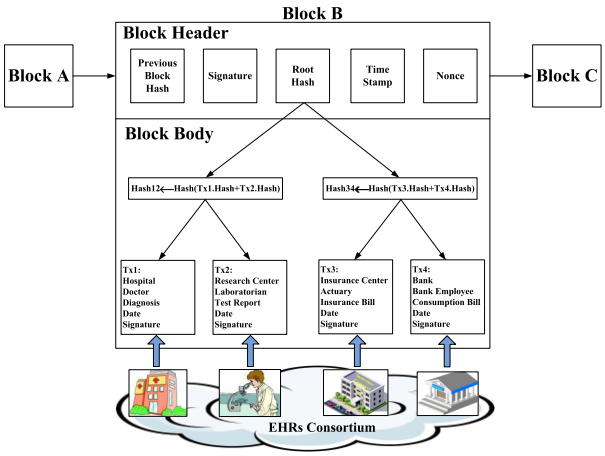


FIGURE 3. EHRs system in blockchain. Every patient owns this chain by himself, after being treated in one hospital, all the information related to patient is encapsulated in one block.

generated according to the time sequence and a healthcare blockchain of this patient is constructed.

Authorized entity might look over the health records of this patient by means of his blockchain, and has powerless to tamper the data in established block (such as drug allergy and dosage). When the patient goes to be treated in other clinical departments or hospitals next time, the new entity needs to identify this patient and authenticate his available blockchain, which could save the medical resources and avoid the repeated detection.

To meet the requirement of distributed structure in EHRs system, we employ attributes based signature with multiple authorities to address the above application. A MA-ABS scheme is a protocol that a signature attests not to the identity of the patient who endorsed a message, but instead to a claim (like access policy) regarding the attributes delegated from some authorities he possesses. Suppose that a patient Alice wishes to anonymously publish a block with sensitive data on EHRs system. To give credibility to her block she decides to take the following claim to endorse message:

((cardiopath) AND (disease period more than 10 years)) OR (((Harvard professor) OR (Yale professor)) AND (Expert on cardiopathy))).

Alice would acquire these attributes from the different attribute authorities, who may not trust or even be aware of each other. In the special cases, a party of the attribute authorities may be corrupted. Under this case, it should not impede the acquirement of attributes from the other hornist authorities. Alice is allowed to endorse her message under the claim above, without having to reveal how she meets the claim. Authorities jointly guarantees her signature for Alice, while guaranteeing it for herself in the identity-based signature scheme.

Taking advantage of this technique, it achieves a perfect privacy-preserving for patient. The explicit claim of the signature reveals nothing about the identity or attributes of the patient. From another point of view, it guarantees the verifier

in unforgeability as well. The signature of patient whose attributes satisfy the claim cannot be generated by a collusion of parties who integrate their attributes together. Hence, it constructs a secure and controllable mechanism in EHRs system to confirm the validity of the healthcare block.

III. MULTI-AUTHORITY ABS SCHEME IN EHRs SYSTEM

We now describe the EHRs system model and detailed ABS construction in this section. The proposal is an ABS scheme with multiple authorities which can be applied in the healthcare with blockchain technology.

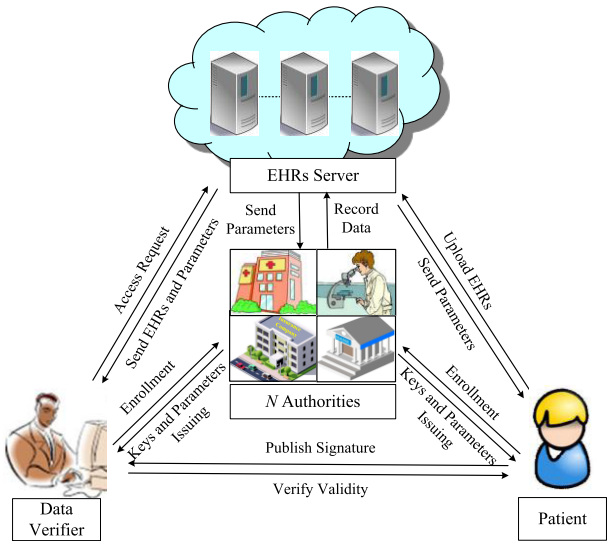


FIGURE 4. The EHRs system model. This model consisted of the four parties: EHRs Server, Authorities, Patient and Data Verifier.

A. EHRs SYSTEM MODEL

This EHRs system model consisted of the following four parties: an EHRs server, N authorities, patients and data verifiers. As shown in Fig. 4, the EHRs server is just like a cloud storage server, which is responsible for storing and transmitting the EHRs. N authorities are various different organizations, such as hospitals, medical insurance organizations, medical research institutes, etc., which are responsible for accepting the enrollment and exchange of patient information. Patients may create, manage, control and sign their own EHRs and define the predicate while the data verifier is allowed to access this signature and verify the correctness.

B. THE PROPOSED MA-ABS SCHEME

For any $i \in Z_q$, an attribute set S whose element also belongs to Z_q, and the Lagrage coefficient is defined as $\Delta_{i,S}(x) = \prod_{j \in S, j \neq i} \frac{x-j}{i-j}$. For each attribute, the scheme associates a single element in Z_q^* corresponding with this attribute. The detailed scheme is presented as follows.

- **Setup**: The EHRs server chooses two suitable additional cyclic groups G and G_T with the prime order q, equipped with a bilinear map $\hat{e} : G \times G \to G_T$. Let P be a random generator of G, $H : \{0,1\}^* \to Z_q^*$ be a strong collision-resistant hash function such as SHA-256. Computing $u = H(\mathrm{GID})$ for Patient's global identities GID. Suppose that there are N authorities all together in this system, named $A_1, A_2, \ldots, A_N$. Each authority A_k monitors an attribute set $\widetilde{A}_k = \{a_{k,1}, a_{k,2}, \ldots, a_{k,n_k}\}$. Choosing $\omega \in Z_q^*$ at random and setting $Q = \omega P$. The public parameters of this system are $params = \langle \hat{e}, q, P, Q, G, G_T, H \rangle$.
- **Authority Setup**: Each authority A_k chooses $\alpha_k \in Z_q^*$ at random and computes $y_k = \alpha_k P$. For each attribute $a_{k,i} \in \widetilde{A}_k$, it chooses $t_{k,i} \in Z_q^*$ and computes $T_{k,i} = t_{k,i} P$. Two authorities A_k and A_j select $s_{kj} \in Z_q^*$ randomly and share the selected value between them as a secret pseudorandom function (PRF) seed through a 2-party key exchange channel, which then sets $s_{kj} = s_{jk}$. A_k and A_j choose $x_i, x_j \in Z_q^*$, respectively, and define a common PRF as $PRF_{kj}(u) = \left(\frac{x_k x_j}{s_{kj}+u}\right) Q$. The authority A_k outputs the public keys as $PK_k = \left\langle y_k, \{T_{k,i}\}_{i \in \{1,2,\ldots,n_k\}} \right\rangle$ and the private keys as $SK_k = \left\langle \alpha_k, x_k, \{s_{kj}\}_{j \in \{1,2,\ldots,N\} \setminus \{k\}}, \{t_{k,i}\}_{i \in \{1,2,\ldots,n_k\}} \right\rangle$.
- **KeyGen**: Suppose that the patient possesses an attribute set $\widetilde{A}_U$. Authority A_k picks $r_k \in Z_q^*$ and computes $S_{k,i} = \frac{r_k}{t_{k,i}}$ for $a_{k,i} \in \widetilde{A}_U^k$, where $\widetilde{A}_U^k = \widetilde{A}_U \cap \widetilde{A}_k$. Patient U interacts with each authority A_k $N-1$ times to finish the anonymous key issuing and computes

$$D_{kj} = \alpha_k P + r_k Q + PRF_{kj}(u) \quad \text{for } k > j,$$

and

$$D_{kj} = \alpha_k P + r_k Q - PRF_{kj}(u) \quad \text{for } k \leq j.$$

Finally, patient U can compute

$$D_U = \sum_{(k,j) \in \{1,2,\ldots,N\} \times (\{1,2,\ldots,N\} \setminus \{k\})} D_{kj} = \sum_{k \in \{1,2,\ldots,N\}} (N-1)\alpha_k P + \sum_{k \in \{1,2,\ldots,N\}} (N-1) r_k Q,$$

and output his public keys as

$$PK_U = \left\langle \{S_{k,i} Q\}_{k \in \{1,2,\ldots,N\}, i \in \{1,2,\ldots,n_k\}, a_{k,i} \in \widetilde{A}_U^k} \right\rangle,$$

and his private keys as

$$SK_U = \left\langle D_U, \{S_{k,i}\}_{k \in \{1,2,\ldots,N\}, i \in \{1,2,\ldots,n_k\}, a_{k,i} \in \widetilde{A}_U^k} \right\rangle.$$

- **Sign**: To sign the message M under the predicate Υ, a polynomial q_x is chosen for every node x, and the degree of q_x is defined as $k_x - 1$, where k_x is the threshold value of x. Beginning from the root node R, sets $q_R(0) = s$. After that, it selects some other points and finishes the polynomial q_R. Otherwise, $q_x(0) = q_{parent(x)}(index(x))$ and other points are

randomly selected to complete the polynomial q_x. The patient picks a random value $\upsilon \in Z_q^*$ and computes

$$\begin{aligned}
&\sigma_1 = sD_U, \quad \sigma_2 = \left(\frac{H(M)+\upsilon}{N-1}\right)P, \\
&\sigma_3 = \prod_{k\in\{1,2,\ldots,N\}} \hat{e}(sP, y_k), \\
&\sigma_4 = \upsilon sP, \quad \sigma_5 = sPK_U, \ \sigma_6 = \upsilon\sigma_5, \\
&\sigma_7 = \left\{q_x(0)\, T_{k,i}\right\}_{a_{k,i}\in\tilde{A}_\Upsilon},
\end{aligned}$$

where $a_{k,i}$ is a value of attribute in predicate Υ. Then, the final signature is output as

$$\sigma = \{\sigma_1, \sigma_2, \sigma_3, \sigma_4, \sigma_5, \sigma_6, \sigma_7\}.$$

- **Verify**: Suppose that the data verifier possesses a set of attributes $\widetilde{A}_{DV} = \{b_1, b_2, \ldots, b_t\}$. If $\Upsilon\left(\widetilde{A}_{DV}\right) \neq 1$, the output is *null*. Otherwise, the data verifier obtains the signature σ and defines a recursive operation *VerifyNode* (σ, PK_U, x) that takes the signature σ, The public key of the patient PK_U and a node x from the predicate Υ are used as inputs. If $a_{k,i} \in \widetilde{A}_U^k$,

$$\begin{aligned}
&\textit{VerifyNode}(\sigma, PK_U, x) \\
&= \prod_{k\in\{1,2,\ldots,N\}} \hat{e}(\sigma_7, PK_U) \\
&= \prod_{k\in\{1,2,\ldots,N\}} \hat{e}\left(q_x(0)\, T_{k,i}, \frac{r_k}{t_{k,i}}Q\right) \\
&= \prod_{k\in\{1,2,\ldots,N\}} \hat{e}\left(q_x(0)\, t_{k,i}P, \frac{r_k}{t_{k,i}}Q\right) \\
&= \prod_{k\in\{1,2,\ldots,N\}} \hat{e}(P,Q)^{q_x(0)t_{k,i}\frac{r_k}{t_{k,i}}} \\
&= \hat{e}(P,Q)^{q_x(0)\left(\sum_{k\in\{1,2,\ldots,N\}} r_k\right)}.
\end{aligned}$$

If $a_{k,i} \notin \widetilde{A}_U^k$, *VerifyNode* $(\sigma, PK_U, x) = null$. Provided that the node x is not a leaf node, this algorithm *VerifyNode* (σ, PK_U, x) executes recursively as below. If the node z is a child node of x, it computes $F_z = \textit{VerifyNode}(\sigma, PK_U, z)$ and keeps the result. Let S_x be an arbitrary k_x-sized set of child node z, sets $F_z \neq null$. If such a set does not exist, set $F_z = null$. Otherwise, computes F_x as below, where $S_x' = \{index(z) : z \in S_x\}$ and $d = index(z)$,

$$\begin{aligned}
F_x &= \prod_{z\in S_x} F_z^{\Delta_{d,S_x'}(0)} \\
&= \prod_{z\in S_x}\left(\hat{e}(P,Q)^{q_z(0)\left(\sum_{k\in\{1,2,\ldots,N\}} r_k\right)}\right)^{\Delta_{d,S_x'}(0)} \\
&= \prod_{z\in S_x}\left(\hat{e}(P,Q)^{q_{parent(z)}(index(z))\left(\sum_{k\in\{1,2,\ldots,N\}} r_k\right)}\right)^{\Delta_{d,S_x'}(0)} \\
&= \prod_{z\in S_x}\left(\hat{e}(P,Q)^{q_x(d)\left(\sum_{k\in\{1,2,\ldots,N\}} r_k\right)\Delta_{d,S_x'}(0)}\right) \\
&= \hat{e}(P,Q)^{q_x(0)\left(\sum_{k\in\{1,2,\ldots,N\}} r_k\right)}.
\end{aligned}$$

If the predicate $\Upsilon\left(\widetilde{A}_U^k\right) = 1$, it is verified that the equation $\textit{VerifyNode}(\sigma, PK_U, x) = \hat{e}(P,Q)^{s\left(\sum_{k\in\{1,2,\ldots,N\}} r_k\right)}$ is holding.
Then, the data verifier checks the following constraints:

$$\hat{e}(\sigma_1, \sigma_2) \stackrel{?}{=} \sigma_3^{H(M)} \prod_{k\in\{1,2,\ldots,N\}} \times \left(\hat{e}(\sigma_4, y_k)\, \hat{e}\left(H(M)\sigma_5 + \sigma_6, T_{k,i}\right)\right).$$

The verifier returns *Accept* if and only if all the above checks are successful, and the signature is valid. Otherwise, *Reject* is returned.

- **Correctness**: The correctness is derived from the equation as below:

$$\begin{aligned}
&\hat{e}(\sigma_1, \sigma_2) \\
&= \hat{e}\left(s\sum_{k\in\{1,2,\ldots,N\}} (N-1)\,\alpha_k P \right. \\
&\qquad \left. + s\sum_{k\in\{1,2,\ldots,N\}} (N-1)\, r_k Q, \frac{H(M)+\upsilon}{N-1}P\right) \\
&= \hat{e}\left(s\sum_{k\in\{1,2,\ldots,N\}} (N-1)\,\alpha_k P, \frac{H(M)+\upsilon}{N-1}P\right) \\
&\quad \cdot \hat{e}\left(s\sum_{k\in\{1,2,\ldots,N\}} (N-1)\, r_k P, \frac{H(M)+\upsilon}{N-1}P\right) \\
&= \hat{e}(P,P)^{s\sum_{k\in\{1,2,\ldots,N\}} \alpha_k(H(M)+\upsilon)} \\
&\quad \times \hat{e}(Q,P)^{s\sum_{k\in\{1,2,\ldots,N\}} r_k(H(M)+\upsilon)} \\
&= \hat{e}(P,P)^{s\sum_{k\in\{1,2,\ldots,N\}} \alpha_k H(M)}\, \hat{e}(P,P)^{s\sum_{k\in\{1,2,\ldots,N\}} \alpha_k \upsilon} \\
&\quad \cdot \hat{e}(Q,P)^{s\sum_{k\in\{1,2,\ldots,N\}} r_k H(M)}\, \hat{e}(Q,P)^{s\sum_{k\in\{1,2,\ldots,N\}} r_k \upsilon} \\
&= \sigma_3^{H(M)} \prod_{k\in\{1,2,\ldots,N\}} \left(\hat{e}(\sigma_4, y_k)\, \hat{e}\left(H(M)\sigma_5 + \sigma_6, T_{k,i}\right)\right).
\end{aligned}$$

IV. SECURITY AND PERFORMANCE ANALYSIS

The security of this protocol is analyzed in the random oracle model in this section, and it demonstrates the performance.

A. SECURITY ANALYSIS

Collusion Resistance: In this system, there are two authorities A_k and A_j to share a PRF seed s_{kj} and keep it secretly between them. Therefore, even if $N-2$ authorities are corrupted,

it has only one PRF seed that it still not captured by malicious authority at least. Moreover, in the process of **KeyGen**, the private key α_k of each authority is combined into the private key D_U of the patient. If only one authority is honest, the other malicious authorities still obtain nothing about D_U, which means that this protocol resists $N-1$ corrupted authorities collusion attacks. To preserve the privacy of the patient, his GID is not exposed to directly to the authority. Therefore, the corrupted authority fails to trace the GID and steal the private information of the patient.

Theorem 1: The proposed MA-ABS scheme for the EHRs system, in the random oracle model, is unforgeable under the selective predicate attack with the CBDH assumption holding.

Proof: Suppose that a forger $\mathcal{F}$ has a non-negligible advantage ε in attacking MA-ABS in the sense of selective predicate. The challenger $\mathcal{C}$ chooses a security parameter $1^\lambda$and runs **Setup**, sending the public parameters *params* to the forger $\mathcal{F}$. There also exists a simulator $\mathcal{S}$ that utilizes $\mathcal{F}$ as a sub-algorithm to solve the CBDH problem with a non-negligible probability ε'.

Assuming that the forger $\mathcal{F}$ makes at most q_H queries to the hash function, q_P queries to the private key extraction oracle and q_S queries to the signing oracle. The simulator $\mathcal{S}$ is given an instance of the CBDH problem $\langle P, A=aP, B=bP, C=cP\rangle$ where $a, b, c \in Z_q^*$ and is used to compute $\hat{e}(P,P)^{abc}$. The detailed simulation is proceeded as follows.

- *Setup*: A challenge predicate Υ^* with attribute set S^* is selected by the forger $\mathcal{F}$. It sends a list of corrupted authorities L_A, Υ^* and S^* to the simulator $\mathcal{S}$, sets $Q=(a+\omega)P$, where $|L_A|<N$. Then, $\mathcal{S}$ gives A, B and C to $\mathcal{F}$.
- *Authority Setup*: $\mathcal{S}$ selects $A_k^* \in \{A_1, A_2, \ldots, A_N\} \setminus L_A$ at random.
  (1) For $A_k \in L_A$, $\mathcal{S}$ chooses $v_k, w_{k,i} \in Z_q^*$ at random, and computes $T_{k,i}=w_{k,i}P$ for $a_{k,i} \in A_k$. Then, $\mathcal{S}$ selects $x_k \in Z_q^*$, a PRF seed $s_{kj} \in Z_q^*$ for corrupted authorities A_k and A_j, $\mathcal{S}$ gives $\langle v_k, w_{k,i}, x_k, s_{kj}\rangle$ and $\langle y_k, T_{k,i}\rangle$ to the forger $\mathcal{F}$, where $y_k=v_kP$.
  (2) For $A_k \notin L_A$, $\mathcal{S}$ chooses $v_k, w_{k,i} \in Z_q^*$ at random, and computes $T_{k,i}=w_{k,i}P$ for $a_{k,i} \in \Upsilon^*$, and $T_{k,i}=w_{k,i}A=w_{k,i}aP$ for $a_{k,i} \notin \Upsilon^*$. If $A_k \neq A_k^*$, $\mathcal{S}$ sets $y_k=bv_kP$. Otherwise, sets $y_k=\hat{e}(P,P)^{ab}\prod_{A_k\in L_A}\hat{e}(P,P)^{-v_k}\prod_{A_k\in L_A, A_k\neq A_k^*}\hat{e}(P,P)^{-bv_k}$. Finally, the simulator $\mathcal{S}$ randomly chooses a PRF seed $s_{kj} \in Z_q^*$ for two honest authorities A_k and A_j, and gives $\langle y_k, T_{k,i}\rangle$ to $\mathcal{F}$.
- *Query*: The simulator $\mathcal{S}$ initializes an integer $i=0$ and an empty list L, $\mathcal{F}$ is allowed to issue queries as follows.
  - *H-Query*: $\mathcal{S}$ maintains a list of L_H to gather the answers to the hash function oracle H. Then, after receiving the i-th time query M_i for $1 \le i \le q_H$, the simulator $\mathcal{S}$ performs a check on the list L_H. If such an entry for the query is existed, returns it as an answer. Otherwise, $\mathcal{S}$ computes $H(M_i)$, and return $H(M_i)$ after adding the tuple $\langle M_i, H(M_i)\rangle$ into L_H.
  - *Private Key Extraction Oracle Query*: Upon receiving an attribute set S with $\Upsilon(S) \neq 1$. $\mathcal{S}$ first checks whether the entry $\langle i, S, SK_U\rangle$ exist in L, if holds, return SK_U. Otherwise, $\mathcal{S}$ does the following.
    (1) For $A_k \in L_A$, $\mathcal{S}$ computes the secret key by using $\langle v_k, w_{k,i}, x_k, s_{kj}\rangle$ for the corresponding attribute sets.
    (2) For $A_k \notin L_A$, $\mathcal{S}$ picks $r_k \in Z_q^*$ at random, computes

$$\left\{s_{k,i}=\frac{r_k}{w_{k,i}}\right\}_{a_{k,i}\in\Upsilon^*} \text{ and } \left\{s_{k,i}=\frac{r_k}{w_{k,i}a}\right\}_{a_{k,i}\notin\Upsilon^*}.$$

    $\mathcal{S}$ computes D_{kj} in two different conditions as below.
    1) $A_k \neq A_k^*$: For $k>j$, sets

$$D_{kj}=v_kbP+r_kQ+PRF_{kj}(u).$$

    Otherwise, sets

$$D_{kj}=v_kbP+r_kQ-PRF_{kj}(u).$$

    2) $A_k = A_k^*$: For $k>j$, sets

$$D_{kj}=-\frac{b\omega}{s}P+\sum_{A_k\in L_A}((-v_k)P)+\sum_{A_k\notin L_A, A_k\neq A_k^*}((-v_k)bP)+r_kQ+PRF_{kj}(u).$$

    Otherwise, sets

$$D_{kj}=-\frac{b\omega}{s}P+\sum_{A_k\in L_A}((-v_k)P)+\sum_{A_k\notin L_A, A_k\neq A_k^*}((-v_k)bP)+r_kQ-PRF_{kj}(u).$$

    D_{kj} is distributed correctly. Because that the simulation $k<j$ is similar to the simulation $k>j$, we only describe the latter simulation as below.

$$\begin{aligned}D_{kj}&=-\frac{b\omega}{s}P+\sum_{A_k\in L_A}((-v_k)P)+\sum_{A_k\notin L_A, A_k\neq A_k^*}((-v_k)bP)+r_kQ-PRF_{kj}(u)\\&=-\frac{b\omega}{s}P+r_k(a+\omega)P-\sum_{A_k\in L_A}(v_kP)-\sum_{A_k\notin L_A, A_k\neq A_k^*}(bv_kP)-PRF_{kj}(u)\end{aligned}$$

$$
\begin{aligned}
&= -\frac{b\,(a+\omega)}{s}P + \frac{ab}{s}P + r_k\,(a+\omega)\,P \\
&\quad - \sum_{A_k \in L_A} (v_k P) - \sum_{A_k \notin L_A, A_k \neq A_k^*} (bv_k P) \\
&\quad - PRF_{kj}\,(u) \\
&= \frac{ab}{s}P + \left(r_k - \frac{b}{s}\right) \\
&\quad \times (a+\omega)\,P - \sum_{A_k \in L_A} (v_k P) \\
&\quad - \sum_{A_k \notin L_A, A_k \neq A_k^*} (bv_k P) - PRF_{kj}\,(u) \\
&= \frac{ab}{s}P + \sum_{A_k \in L_A} ((-v_k)\,P) \\
&\quad + \sum_{A_k \notin L_A, A_k \neq A_k^*} ((-bv_k)\,P) \\
&\quad + (r_k - b)\,Q - PRF_{kj}\,(u)\,.
\end{aligned}
$$

Let $r'_k = r_k - \frac{b}{s}$, we have

$$
\begin{aligned}
D_{kj} = \frac{ab}{s}P &+ \sum_{A_k \in L_A} ((-v_k)\,P) \\
&+ \sum_{A_k \notin L_A, A_k \neq A_k^*} ((-v_k)\,bP) \\
&+ r'_k Q - PRF_{kj}\,(u)\,.
\end{aligned}
$$

At last, simulator $\mathcal{S}$ adding the entry $\langle i, S, SK_U\rangle$ in L, where $SK_U = \langle D_U, \{S_{k,i}\}\rangle$, and returns it to $\mathcal{F}$.

- *Signing Oracle Query*: The signing request is received on $(M^*, \Upsilon^*(S^*))$. If $|S \cap S^*| < k$, the simulator $\mathcal{S}$ is able to generate the simulated private key as in *Private Key Extraction Oracle Query*. Then, the signature can be simulated normally. Otherwise, (i.e., $|S \cap S^*| \geq k$), $\mathcal{S}$ simulates the signature on M with $\Upsilon'(S)$ by computing $Q^* = \omega(cP) = cQ$ and the simulated signature is output as follows.

$$
\begin{aligned}
&\sigma_1^* = sD_U, \quad \sigma_2^* = \left(\frac{H(M) + \upsilon}{N-1}\right) cP, \\
&\sigma_3^* = \prod_{k \in \{1,2,\ldots,N\}} \hat{e}\,(s\,(cP), y_k), \\
&\sigma_4^* = \upsilon s\,(cP), \quad \sigma_5^* = sPK_U^*, \\
&\sigma_6^* = \upsilon\sigma_5^*, \quad \sigma_7^* = \left\{q_x\,(0)\,T_{k,i}\right\}_{a_{k,i} \in \tilde{A}_{\Upsilon^*}},
\end{aligned}
$$

where $PK_U^* = s_{k,i}Q^*$.
Finally, the simulator $\mathcal{S}$ returns the signature $\sigma^* = \{\sigma_1^*, \sigma_2^*, \sigma_3^*, \sigma_4^*, \sigma_5^*, \sigma_6^*, \sigma_7^*\}$ back to the forger $\mathcal{F}$.

- Forgery: The forger $\mathcal{F}$ outputs a forged signature σ^* on message M^* with $\Upsilon^*(S^*)$. The submitted signature satisfies the verification which means that

$$
\begin{aligned}
&\left(\frac{\hat{e}\left(\sigma_1^*, \sigma_2^*\right)}{\sigma_3^{*H(M^*)} \prod_{k \in \{1,2,\ldots,N\}} \left(\hat{e}\left(\sigma_4^*, y_k\right) \hat{e}\left(H(M^*)\sigma_5^* + \sigma_6^*, T_{k,i}\right)\right)}\right)^{\frac{1}{H(M^*)+\upsilon}} \\
&= \hat{e}\,(abP, cP)\,\hat{e}\left(s \sum_{k \in \{1,2,\ldots,N\}} \alpha_k P, cP\right) \\
&\times \left(\frac{\hat{e}\left(s \sum_{k \in \{1,2,\ldots,N\}} r_k Q, (H(M^*) + \upsilon)\,cP\right)}{\hat{e}(P,P)^{scH(M^*) \sum_{k \in \{1,2,\ldots,N\}} \alpha_k}\ \hat{e}(P,P)^{sc\upsilon \sum_{k \in \{1,2,\ldots,N\}} \alpha_k}}\right)^{\frac{1}{H(M^*)+\upsilon}} \\
&\times \left(\frac{1}{\hat{e}(Q^*,P)^{sH(M^*) \sum_{k \in \{1,2,\ldots,N\}} r_k}\ \hat{e}(Q^*,P)^{s\upsilon \sum_{k \in \{1,2,\ldots,N\}} r_k}}\right)^{\frac{1}{H(M^*)+\upsilon}} \\
&= \hat{e}\,(P,P)^{abc}\,\hat{e}\,(P,P)^{sc \sum_{k \in \{1,2,\ldots,N\}} \alpha_k} \\
&\times \frac{\hat{e}\,(Q,P)^{sc \sum_{k \in \{1,2,\ldots,N\}} r_k}}{\hat{e}\,(P,P)^{sc \sum_{k \in \{1,2,\ldots,N\}} \alpha_k}} \times \frac{1}{\hat{e}\,(Q^*,P)^{s \sum_{k \in \{1,2,\ldots,N\}} r_k}} \\
&= \hat{e}\,(P,P)^{abc}\,.
\end{aligned}
$$

In a successful simulation game, t_S is used to denote the time cost for scalar multiplication operation in the elliptic curve group G, and t_B is used to denote the time cost for the bilinear pairing operation. Suppose that the forger $\mathcal{F}$ successfully attacks this MA-ABS scheme with time t, it another algorithm can be easily constructed to solve the CBDH problem with time t', where

$$
\begin{aligned}
t' \approx t + q_H\,(t_S + t_B) + q_P\,(3+2N)\,N\,(N-1)\,t_S \\
+ q_S\,(6t_S + Nt_B)\,.
\end{aligned}
$$

Suppose also that N_i is the number of situations in which a valid private key could be generated from i private keys chosen by the forger. Hence, the worst case when the forger possesses $n_k - 1$ private keys out of total n_k private key that the authority A_k controlling. Thus, we can determine the probability of success is

$$
\begin{aligned}
&\frac{1}{q-1}\left(\frac{N_2}{C_{q-1}^2} + \frac{N_3}{C_{q-1}^3} + \cdots + \frac{N_{n_k-1}}{C_{q-1}^{n_k-1}}\right) \\
&< \frac{1}{q-1} \cdot \frac{N_2\,(n_k-2)}{C_{q-1}^2} < \frac{n_k-2}{(q-1)^2}.
\end{aligned}
$$

Therefore, the probability of solving CBDH problem is calculated as

$$
\varepsilon' \geq \frac{\varepsilon}{2} \prod_{k \in \{1,2,\ldots,N\}} \left(1 - \frac{n_k - 2}{(q-1)^2}\right).
$$

□

Theorem 2: This MA-ABS scheme achieves the perfectly attribute-signer privacy.

TABLE 1. Comparison between ABS schemes.

Properties	[14]	[20]	[24]	[26]	Ours
Cost of Signing	$(lt+t+3)T_e$	$(7l+15)T_e$	$(6+2l+lt)T_e$	$(l+t+16)T_e+3T_p$	$(6+t)T_s+NT_p$
Cost of Verifying	$(2lt+1)T_e+(l+2+(t-1)(l+1))T_p$	$(l+1)T_e+(l+2)T_p$	$(l+2)T_e+(l+4)T_p$	$(2lt+12)T_e+(l+7+(t-1)(l+1))T_p$	$T_s+T_e+(2tN+1)T_p$
Size of Signature	$(l+t+2)\|G\|$	$(7l+11)\|G\|$	$(l+t+2)\|G\|$	$(l+t+11)\|G\|$	$(6+t)\|G\|$
Predicates	Monotone	Non-Monotone	Monotone	Monotone	Monotone
Multi-Authority	Extensible	Extensible	No	No	Yes
Security Model	Generic Group	Standard	Standard	Generic Group	Random
Security Assumption	CR Hash	DLIN/ CR Hash	CDH	CR Hash	CBDH
Privacy	Perfect Privacy	Perfect Privacy	Perfect Privacy	Imperfect Privacy	Perfect Privacy
Resisting Collusion Attack	No	No	No	No	Yes

l denotes the number of attributes involved in the predicate.
t denotes the number of user attributes that meets the predicate.
CR Hash represents the Collision Resistant (CR) Hash Function.
DLIN represents the Decisional Linear problem.

Proof: To verify the signer privacy, for any predicate Υ and any attribute set S that satisfies it, a valid signature will be created by any other set satisfying such predicate Υ. Furthermore, the signature will not reveal which attribute subset is really employed to sign the message, for the reason that any attribute subset with k elements among the given attribute will be utilized to produce a signature. Therefore, we need to show the proof of the signer privacy in case of $k = n$, where n is the number of the attribute set S.

First, the challenger operates the **Setup** and **Authority Setup** algorithms to publish parameters, the public key PK_k and the private key SK_k of the authority to the forger. The forger $\mathcal{F}$ is allowed to query*Private Key Extraction Oracle* and *Signing Oracle*. Then, $\mathcal{F}$ outputs a tuple $\langle \Upsilon, S_0, S_1, M^* \rangle$ with the restriction $S_0 \supseteq S$ and $S_1 \supseteq S$ and requests the challenger $\mathcal{C}$ to endorse a message M^* with respect to Υ from either S_0 or S_1.

The challenger $\mathcal{C}$ will generate the challenge signature by himself. For detailed, since $S_0 \cap S = S$ and $S_1 \cap S = S$, $\mathcal{C}$ chooses a bit $b \in \{0, 1\}$ at random and outputs the challenge signature σ^* with the private key SK_{S_b} on the attribute set S_B. Based on the Lagrange interpolation function, it concludes that σ^* could be obviously generated from either SK_{S_b} or $SK_{S_{1-b}}$. Therefore, the forger is incapable of colluding with the authority to steal the signer attribute, and the information privacy in MA-ABS scheme is preserved. □

B. PERFORMANCE ANALYSIS

This subsection compares the efficiency and other important properties of the proposed and previous ABS schemes. Without considering the hash function, we denote T_P as the cost of the bilinear pairing operation, T_s as the scalar multiplication operation, and T_e as the exponentiation operation.

As illustrated in Table 1, the proposed protocol is more suitable for application to a distributed system (such as the distributed ledger) with multiple authorities. With respect to the computation in**Sign-Verify**, the cost of the proposed protocol increases with number to the authority and attribute of the user linearly. In the process of **Sign**, this protocol needs the cost of $(6 + t)\, T_s + NT_p$. In the process of **Verify**, the cost of $T_s + T_e + (2tN + 1)\, T_p$ is consumed. For the communication overhead, the signature size in the proposed construction is only related to the entity attribute number, i.e., the size of signature is $(6 + t)\, |G|$. Considering the other properties, this protocol with multiple authorities supporting monotone predicate, and its security is proven in the random oracle model under the intractability of CBDH problem. Furthermore, the proposed protocol achieves perfect privacy and resists collusion attacks.

In addition, the protocol developed by Okamoto and Takashima [20] has a unique feature of supporting the non-monotone predicate, which can be described by the NOT gates as well as the AND, OR and threshold gates.

V. CONCLUSION AND FUTURE WORK

Aiming at preserving patient privacy in an EHRs system on blockchain, multiple authorities are introduced into ABS and put forward a MA-ABS scheme, which meets the requirement of the structure of blockchain, as well as guaranteeing the anonymity and immutability of the information. PRF seeds are needed among authorities and the patient private keys need to be constructed, $N - 1$ corrupted authorities cannot succeed in collusion attacks. Finally, the security of the protocol is proven under the CBDH assumption in terms of unforgeability and perfect privacy. The comparison analysis demonstrates the performance and the cost of this protocol increases linearly with the number of authorities and patient attributes as well.

A non-monotone predicate could be used in many distributed system applications, which enriches the representation of the predicate. Supporting general non-monotone predicates in blockchain technology is the direction of future work.

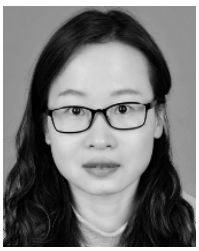
REFERENCES

[1] Health Information and the Law. George Washington University Hirsh Health Law and Policy Program. (Aug. 20, 2015). *Who Owns Medical Records: 50 State Comparison*. [Online]. Available: http://www.healthinfolaw.org/comparative-analysis/who-owns-medical-records-50-state-comparison

[2] K. D. Mandl, P. Szolovits, and I. S. Kohane, "Public standards and patients' control: How to keep electronic medical records accessible but private," *BMJ*, vol. 322, no. 7281, pp. 283–287, Feb. 2001.
[3] S. Nakamoto. *Bitcoin: A Peer-to-Peer Electronic Cash System*. Accessed: 2008. [Online]. Available: https://bitcoin.org/bitcoin.pdf
[4] World Economic Forum. (Sep. 9, 2015). *Deep Shift: Technology Tipping Points and Societal Impact*. [Online]. Available: http://www3.weforum.org/docs/WEF_GAC15_Technological_Tipping_Points_report_2015.pdf
[5] (Dec. 12, 2016). *Healthcare Rallies for Blockchains: Keeping Patients at the Center*. [Online]. Available: http://www.ibm.biz/blockchainhealth
[6] M. Swan, *Blockchain: Blueprint for a New Economy*. Sebastopol, CA, USA: O'Reilly Media, 2015, pp. 53–68.
[7] G. Prisco. (Apr. 26, 2016). *The Blockchain for Healthcare: Gem Launches Gem Health Network With Philips Blockchain Lab*. [Online]. Available: https://bitcoinmagazine.com/articles/the-blockchain-for-heathcare-gem-launches-gem-health-network-with-philips-blockchain-lab-1461674938
[8] U.S. White House. 104th Congress. (Aug. 21, 1996). *Public Health Insurance Portability and Accountability Act*. [Online]. Available: https://en.wikipedia.org/wiki/Health_Insurance_Portability_and_Accountability_Act
[9] P. Taylor. (Apr. 27, 2016). *Applying Blockchain Technology to Medicine Traceability*. [Online]. Available: https://www.securingindustry.com/pharmaceuticals/applying-blockchain-technology-to-medicine-traceability/s40/a2766/#.V5mxL_mLTIV
[10] P. B. Nichol. (Mar. 17, 2016). *Blockchain Applications for Healthcare: Blockchain Opportunities are Changing Healthcare Globally-Innovative Leaders See the Change*. [Online]. Available: http://www.cio.com/article/3042603/innovation/blockchain-applications-for-healthcare.html
[11] G. Irving and J. Holden, "How blockchain-timestamped protocols could improve the trustworthiness of medical science," *F1000Research*, vol. 5, p. 222, May 2016.
[12] P. Jiang, F. Guo, K. Liang, J. Lai, and Q. Wen, "Searchain: Blockchain-based private keyword search in decentralized storage," *Future Generat. Comput. Syst.*, 2017, doi: 10.1016/j.future.2017.08.036.
[13] X. Liao, J. Yin, S. Guo, X. Li, and A. K. Sangaiah, "Medical JPEG image steganography based on preserving inter-block dependencies," *Comput. Electr. Eng.*, 2017, doi: 10.1016/j.compeleceng.2017.08.020.
[14] H. K. Maji, M. Prabhakaran, and M. Rosulek, "Attribute-based signatures: Achieving attribute-privacy and collusion-resistance," in *Proc. IACR Cryptol. ePrint Arch.*, Apr. 2008, pp. 1–23. [Online]. Available: https://eprint.iacr.org/2008/328.pdf
[15] A. Sahai and B. Waters, "Fuzzy identity-based encryption," in *Proc. EUROCRYPT*, Aarhus, Denmark, 2005, pp. 457–473.
[16] D. Khader, "Attribute based group signature with revocation," in *Proc. IACR Cryptol. ePrint Arch.*, Jun. 2007, pp. 1–19. [Online]. Available: https://eprint.iacr.org/2007/241.pdf
[17] H. K. Maji, M. Prabhakaran, and M. Rosulek, "Attribute-based signatures," in *Proc. CT-RSA*, San Francisco, CA, USA, 2011, pp. 376–392.
[18] J. Li, M. H. Au, W. Susilo, D. Xie, and K. Ren, "Attribute-based signature and its applications," in *Proc. ASIACCS*, Beijing, China, 2010, pp. 60–69.
[19] J. Herranz, F. Laguillaumie, B. Libert, and C. Ràfols, "Short attribute-based signatures for threshold predicates," in *Proc. CT-RSA*, San Francisco, CA, USA, 2012, pp. 51–67.
[20] T. Okamoto and K. Takashima, "Efficient attribute-based signatures for non-monotone predicates in the standard model," in *Proc. PKC*, Taormina, Italy, 2011, pp. 35–52.
[21] C. Chen *et al.*, "Fully secure attribute-based systems with short ciphertexts/signatures and threshold access structures," in *Proc. CT-RSA*, San Francisco, CA, USA, 2013, pp. 50–67.
[22] Y. S. Rao and R. Dutta, "Efficient attribute-based signature and signcryption realizing expressive access structures," *Int. J. Inf. Secur.*, vol. 15, no. 1, pp. 81–109, Feb. 2016.
[23] Y. Sakai, N. Attrapadung, and G. Hanaoka, "Attribute-based signatures for circuits from bilinear map," in *Proc. PKC*, Taipei, Taiwan, 2016, pp. 283–300.
[24] K. Gu, W. Jia, G. Wang, and S. Wen, "Efficient and secure attribute-based signature for monotone predicates," *Acta Inf.*, vol. 54, no. 5, pp. 521–541, Aug. 2017.
[25] J. Liu *et al.*, "Protecting mobile health records in cloud computing: A secure, efficient, and anonymous design," *ACM Trans. Embed. Comput. Syst.*, vol. 16, no. 2, Apr. 2017, Art. no. 57.
[26] H. Cui, G. Wang, R. H. Deng, and B. Qin, "Escrow free attribute-based signature with self-revealability," *Inf. Sci.*, vols. 367–368, pp. 660–672, Nov. 2016.
[27] D. Cao, B. Zhao, X. Wang, J. Su, and G. Ji, "Multi-authority attribute-based signature," in *Proc. 3rd IEEE INCoS*, Fukuoka, Japan, Nov. 2011, pp. 668–672.
[28] S.-F. Sun, M. H. Au, J. K. Liu, and T. H. Yuen, "RingCT 2.0: A compact accumulator-based (linkable ring signature) protocol for blockchain cryptocurrency monero," in *Proc. ESORICS*, Oslo, Norway, 2017, pp. 456–474.

RUI GUO received the Ph.D. degree from the State Key Laboratory of Networking and Switch Technology, Beijing University of Posts and Telecommunications, China, in 2014. He is currently a Lecturer with the National Engineering Laboratory for Wireless Security, Xi'an University of Posts and Telecommunications. His present research interests include attribute-based cryptograph, cloud computing, and blockchain technology.

HUIXIAN SHI received the B.S. and Ph.D. degrees from the Department of Mathematics and Information Science, Shaanxi Normal University, Xi'an, China, in 2007 and 2013, respectively. She is currently an Associate Professor with the Department of Mathematics and Information Science, Shaanxi Normal University. Her present research interests include information security and blockchain technology.



QINGLAN ZHAO received the B.S. degree from Shaanxi Normal University in 1999 and the M.S. degree from Northwestern Polytechnical University in 2006. She is currently pursuing the Ph.D. degree with Shanghai Jiao Tong University, China. Since 2014, she has been an Associate Professor with the Xi'an University of Posts and Telecommunications, Xian, China. Her research interests focus on cryptographic functions and information security.

DONG ZHENG received the Ph.D. degree from Xidian University in 1999. He joined the School of Information Security Engineering, Shanghai Jiao-Tong University. He is currently a Professor with the Xi'an University of Posts and Telecommunications, China. His research interests include information theory, cryptography, and information security. He is a Senior Member of the Chinese Association for Cryptologic Research and a member of the Chinese Communication Society.