

基于区块链的多权限属性隐藏电子病历共享方案

金琳¹, 田有亮^{1,2}

(贵州大学计算机科学与技术学院 贵州 贵阳 550025; 2. 贵州省公共大数据重点实验室 贵州 贵阳 550025)

摘要: 现阶段, 不同医院之间没有数据交换共享, 容易形成数据孤岛。同时, 区域医疗数据含有大量患者的敏感信息, 这些数据的公开获取、共享及流通会导致恶意篡改、窃取、滥用与所有权丢失, 从而泄露患者隐私。由于庞大的医疗数据量以及医疗数据的非结构化, 一些具有较强针对性的恶意攻击更加难以防范与追责, 如对医疗数据的窃取、篡改、勒索等恶意攻击。针对以上问题, 提出一种基于区块链的多权限属性隐藏电子病历共享方案, 以实现共享电子病历的细粒度访问的同时, 保证患者隐私安全。引入多授权属性加密(MA-ABE)算法, 利用多权限机构管理分散属性, 同时通过哈希函数来识别不同用户, 可以有效抵抗不同权限用户之间的共谋攻击; 利用线性秘密共享方案(LSSS)实现属性的部分隐藏, 将属性分为属性名与属性值两部分, 以保护属性隐私; 结合区块链公开透明、不易篡改等特性, 设计访问策略可更新算法, 基于访问策略更新算法追加策略区块, 将新的访问策略上传至区块链中形成策略可更新溯源链, 在隐藏策略条件下实现分布式和可信赖的访问控制管理, 同时实现数据隐私保护和用户行为的可追溯。通过安全性证明和实验分析, 所提方案能在有效保护属性隐私的同时, 降低计算开销。

关键词: 属性隐藏; 区块链; 属性加密; 隐私保护; 数据共享

中图分类号: TP393

文献标志码: A

DOI: 10.11959/j.issn.2096-109x.2022044

Multi-authority attribute hidden for electronic medical record sharing scheme based on blockchain

JIN Lin¹, TIAN Youliang^{1,2}

收稿日期: 2022-03-08; 修回日期: 2022-06-27

通信作者: 田有亮, youliangtian@163.com

基金项目: 国家自然科学基金(61662009, 61772008); 贵州省教育厅科技拔尖人才支持项目(黔教合KY字[2016]060); 贵州省科技重大专项计划(20183001); 贵州省科技计划项目(黔科合平台人才[2017]5788号); 教育部—中国移动科研基金研发项目(MCM20170401); 贵州大学培育项目(黔科合平台人才[2017]5788); 数据共享应用的块数据融合分析理论与安全管控模型研究(U1836205); 面向大数据应用的区块链关键技术研究(黔科合基础[2019]1098)

Foundation Items: The National Natural Science Foundation of China (61662009, 61772008), Guizhou Provincial Department of Education Science and Technology Top-notch Talent Support Project ([2016]060), Science and Technology Major Support Program of Guizhou Province (20183001), Guizhou Provincial Science and Technology Plan Project ([2017]5788), Ministry of Education-China Mobile Research Fund Project (MCM20170401), Guizhou University Cultivation Project ([2017]5788), Research on Block Data Fusion Analysis Theory and Security Management Model of Data Sharing Application(U1836205), Research on Key Technologies of Blockchain for Big Data Applications([2019]1098)

引用格式: 金琳, 田有亮. 基于区块链的多权限属性隐藏电子病历共享方案[J]. 网络与信息安全学报, 2022, 8(4): 66-76.

Citation Format: JIN L, TIAN Y L. Multi-authority attribute hidden for electronic medical record sharing scheme based on blockchain[J]. Chinese Journal of Network and Information Security, 2022, 8(4): 66-76.

1. College of Computer Science and Technology, Guizhou University, Guiyang 550025, China
2. State Key Laboratory of Public Big Data, Guizhou University, Guiyang 550025, China

Abstract: Currently, there is no data exchanging and sharing between different hospitals, and it is easy to form data islands. At the same time, regional medical data contains a large amount of sensitive information of patients. The public acquisition, sharing and circulation of these data will lead to malicious tampering, theft, abuse and loss of ownership, thereby revealing patient privacy. In addition, the size of medical data is enormous and the data is unstructured, then it is more difficult to prevent and hold accountable some highly targeted malicious attacks, such as malicious attacks on medical data theft, tampering, and extortion. In view of the above problems, a blockchain-based on multi-authority attribute hidden electronic medical record sharing scheme was proposed to achieve fine-grained access to shared electronic medical records while ensuring patient privacy. The Multi-Authorization Attribute Encryption (MA-ABE) algorithm was introduced, which used multi-authority organizations to manage decentralized attributes. It also used hash functions to identify different users, in order to effectively resist collusion attacks between users with different authorizations. Besides, the linear secrets sharing scheme (LSSS) was used to realize partial hiding of attributes, and the attributes were divided into two parts: attribute name and attribute value. In addition, combined with the characteristics of blockchain openness, transparency and tamper-proof, the design of access policy can update the algorithm. Based on the access policy update algorithm, the policy block was added. The new access policy was uploaded to the blockchain to form a policy update traceability chain, which can realize distributed and reliable access control management under the condition of hidden policy. It can also support data privacy protection at the same time, and traceability of user behavior. The theoretical proof and experimental analysis have proved that this scheme protect attribute privacy effectively, while reduces computational overhead.

Keywords: hidden attribute, blockchain, attribute encryption, privacy protection, data sharing

0 引言

随着“互联网+医疗健康”的普及,电子病历(HER, electronic health record)因易存储、易操作和易共享等特性逐渐常态化。电子病历存储着病人的诊断信息和治疗信息,有助于提供便利的健康记录存储服务。但是随着电子医疗数据的广泛共享,患者的隐私安全问题受到越来越多的关注,特别是对敏感数据的安全防护正面临着严峻的挑战。首先,医疗数据资源的外包存储服务使患者的数据不受自己掌控,分布式存储的医疗数据的流通共享变得愈加复杂,这带来了潜在的安全风险。其次,利用数据挖掘技术,原有的“低价值”数据经过聚类分类能够推导出固定的用户模式,导致用户隐私信息泄露。最后,由于庞大的医疗数据量以及医疗数据的非结构化,一些具有较强针对性的恶意攻击更加难以防范,如对医疗数据的窃取、篡改、勒索等恶意攻击。访问控制作为一种重要的信息安全技术,其通过某种途

径显式地准许或限制主体对客体的访问能力及范围,保证数据用户在其合法权限内访问数据,并禁止非授权用户的违规和越界操作,从而保证数据的安全可控共享。

近年来,基于属性的加密(ABE, attribute-based encryption)^[1]被认为是一种对加密数据提供细粒度访问控制的高级加密工具,已被广泛应用于云数据上的可搜索加密和医疗数据的可控共享等领域^[2-4]。ABE的现有方案可分为两种,即基于密钥属性的加密(KP-ABE, key-policy attribute-based encryption)^[5]方案和基于密文属性的加密(CP-ABE, ciphertext-policy attribute-based encryption)^[6]方案。在KP-ABE方案中,密钥是基于访问策略生成的,访问策略决定哪些密文可以解密,密文与属性集相关联。相反,在CP-ABE方案中,密钥是通过属性集生成的,密文与访问策略相关联。CP-ABE方案允许数据所有者定义自己的访问策略,因此比KP-ABE方案更适合在分散的系统中进行访问控制。在大多数现有的

CP-ABE 方案^[2-3,7]中,需要中央权威机构来颁发和验证私钥,数据用户可以使用一组属性从权威机构获得密钥,以解密来自云服务器的加密数据^[8-9]。显然,数据访问控制的信任性强烈依赖于中间实体,但这是不切实际的,且中间实体可能存在高信任建立成本、单点故障等问题,因此传统的 ABE 方案不适用于跨不同管理域共享数据的分布式环境。

为解决现有 ABE 方案中的单授权问题,本文提出了一种基于多权限属性加密(MA-ABE, multi-authority attribute-based encryption)方案,通过多授权机构分散管理属性以提高系统安全性,其中不需要中央机构授权,并且可以防止串通。对多授权机构环境下的密文访问控制研究主要有 Chase^[10]提出的多授权机构 ABE 方案,该方案通过中央授权机构(CA, central authority),将用户身份标识(GID, global identity)和各属性授权机构(AA, attribute authority),生成的私钥结合在一起。然而,CA 拥有系统的主密钥和用户私钥,其一旦被攻破,将造成数据的泄露。为解决 CA 造成的安全隐患,Lin 等^[11]采用无 CA 的密钥分发和联合的零秘密共享技术,但此技术最多只能防止 m 个用户的联合攻击。Lewko 等^[12]提出了一种新的基于多授权机构的属性加密方案,此方案仅在初始化阶段采用 CA,由 CA 为授权机构分发公共参数并根据用户的请求验证 AA,此后 CA 将不再参与任何运算。Qian 等^[13]提出了支持隐私保护和高效用户撤销的 MA-ABE 解决方案,实现了动态策略更新以及健康记录访问控制的高扩展性。Zhong 等^[14]提出了一种去中心化的多权限 CP-ABE 访问控制方案,能够高效实现用户撤销。Yan 等^[15]引入了一种匿名发布密钥的协议,以保护参与者的隐私并抵抗属性权限的合谋攻击。文献[15]提出的方案不仅支持任何类型的策略更新,而且与现有相关方案相比,缩短了密文和密钥长度,在实际应用中更有效。Zhang 等^[16]提出了第一个支持雾计算外包和属性更新的 CP-ABE 访问控制方案,将加密和解密的繁重计算操作外包给雾节点,因此数据所有者加密和用户解密的计算操作分别与访问结构和密钥中的属性数量无关。

区块链具有分布式、交易透明、不易篡改的特点以及无须第三方背书的可信机制,这符合大数据环境下访问控制待解决的分布式部署、审计机制、信任机制等需求。为了实现可信的访问控制,大部分研究^[17-21]集中于区块链上部署访问控制策略,使用区块链来存储加密的密钥或一组属性。然而,区块链具有透明性,直接将访问策略或用户属性集发送到区块链^[22]将对隐私的披露构成巨大威胁。特别是在 CP-ABE 方案中,人们可以从嵌入密文的访问策略中推断出一些私有属性^[23-25]。例如,在医疗系统中,电子病历访问控制策略为(“心内科”“心脏病”“患者”“三甲医院”),则可能会泄露用户的健康状况等。文献[23]提出了第一个基于分散内积谓词加密的属性隐藏多权限 ABE 方案,但它只能隐藏整个属性集,同时仍然显示某个机构正在控制的属性。为了防止从访问策略暴露用户隐私信息,Nishide 等^[26]提出了隐藏策略的 CP-ABE。树形访问结构的 CP-ABE^[27]通过属性匿名技术隐藏访问策略中全部属性,而线性秘密共享方案(LSSS, linear secret sharing scheme)的 CP-ABE^[28-29]通过隐藏属性映射关系隐藏访问策略。文献[28]中访问矩阵的属性映射关系被隐藏,并将策略中的所有属性用属性布隆过滤器(ABF, attribute bloom filter)隐藏。用户执行解密算法之前先通过 ABF 查询,验证用户是否满足访问策略。验证通过的用户可以进行解密算法;验证没有通过的用户无法获取访问与策略相关的任何信息,巧妙地实现了策略隐藏功能。Wang 等^[29]利用 LSSS 结构,同样将属性分为属性名和属性值两部分,在执行策略隐藏时,只隐藏属性值,而属性名是公开的。Liu 等^[30]利用 LSSS 结构,同样将属性分为属性名和属性值两部分,实现物联网中高效的多权限部分属性隐藏访问控制。然而,访问策略中不是所有的属性泄露用户隐私信息,完全隐藏属性计算开销较大且可扩展性较弱。为提高计算效率,文献[30]提出的方案利用灵活的 LSSS 结构实现属性的部分隐藏。

为进一步扩展访问控制的灵活性,研究者提出了策略更新机制。Yang 等^[31]通过策略动态更新对云环境中的数据进行访问控制。Liu 等^[32]提出

一种智能电网多权限访问控制的高效属性撤销方案。Huang 等^[33]提出一种多权限属性加密方案，其允许属性撤销。田有亮等^[34]提出基于属性加密的区块溯源算法，实现了区块交易数据的动态更新。但上述方案都没有兼顾数据隐私保护和恶意行为追责问题。

鉴于上述分析，本文提出一种基于区块链的多权限属性隐藏电子病历共享方案。利用设计的访问策略可更新的多权限部分属性隐藏加密算法完成电子病历共享的隐私安全保护，结合区块链设计策略更新溯源链，实现分布式和可信赖的访问控制管理，同时实现数据隐私保护和用户行为的可追溯。本文的主要贡献如下。

1) 设计基于多权限的属性隐藏加密算法。利用多权限属性加密，结合线性秘密共享方案，设计访问策略可更新的多权限部分属性隐藏加密算法，将属性分为属性名与属性值两部分，实现属性的部分隐藏，以保护属性隐私。

2) 实现隐藏策略下的可追溯。结合区块链的公开透明、不易篡改特性，基于访问策略更新算法追加策略区块，实现访问策略的可信动态更新及隐藏策略下的追溯和追责。

3) 安全性分析和实验表明，本文所提方案在保护数据隐私安全的同时，降低了计算开销。

1 准备知识

1.1 参数定义

基于区块链的多权限属性隐藏电子病历共享方案涉及的主要参数如表 1 所示。

1.2 双线性映射

设 p 是一大素数， G 和 G_T 是 p 阶乘法群， G 到 G_T 的双线性映射 $e: G \times G \rightarrow G_T$ ，满足下面的性质。

1) 双线性：任意 $u, v \in G$ ， $a, b \in \mathbb{Z}_p^*$ ，则有 $e(u^a, v^b) = e(u, v)^{ab}$ 。

2) 非退化性：存在 $u, v \in G$ ， $e(u, v) \neq 1$ 。

3) 可计算性：对任意的 $u, v \in G$ ，存在一个有效算法计算 $e(u, v)$ 。

1.3 访问结构

用 $U = \{P_1, P_2, \dots, P_n\}$ 表示参与者集合， $A \subseteq 2^U$ ，对于任意的集合 B 和 C ，如果满足 $B \in A$ 且 $B \subseteq C$ ，则 $C \in A$ ，那么称集合 A 是单调的，

且 $A \subseteq 2^{\{P_1, P_2, \dots, P_n\} \setminus \{\emptyset\}}$ ， A 是一个单调的非空子集。称在 A 中的集合为授权集，不在 A 中的集合被称为未授权的集合。

表 1 方案参数
Table 1 Scheme parameters

参数	含义
θ	属性加密算法的系统安全参数
PK_{aid}	机构 aid 的系统主公钥
SK_{aid}	机构 aid 的系统主私钥
GP	全局参数
$S_{aid,uid}$	对应机构 aid 的用户 uid 的属性集
GID	参与者的身份唯一标识
$K_{aid,uid}$	对应机构 aid 的用户 uid 的属性密钥
UK_{uid}	用户 uid 的身份认证密钥
$TK_{i,uid}$	用户 uid 的转换密钥
M_i	$l \times n$ 型访问矩阵 M 的第 i 行
$\rho(i)$	函数 ρ 将矩阵 M 的第 i 行映射到属性
s	秘密共享密钥
λ	秘密共享份额
v	加密算法所选择的随机向量
m	待加密的明文
σ	用户签名
CT	密文
IT	中间密文
$En(s)$	保留加密信息

1.4 线性秘密共享方案

实体集 P 上的一个秘密共享方案 Π 如果满足下列两个条件，则称之为线性秘密共享方案。

1) 每个实体的共享份额能够组成有限域 $\mathbb{Z}_p$ 上的一个向量，其中 p 是有限域的阶。

2) 存在一个 l 行 n 列的共享矩阵 $M_{l \times n}$ ，对于矩阵的每一行 $i \in \{1, 2, \dots, l\}$ ，有单射函数 ρ 映射到每个实体 $\rho(i)$ 。随机选取一个向量 $v = (s, t_2, t_3, \dots, t_n) \in \mathbb{Z}_p^n$ ，其中， s 是共享的秘密， $t_2, t_3, \dots, t_n$ 用来隐藏秘密 s ， $\lambda_i = (Mv)_i$ 表示实体 $\rho(i)$ 拥有的秘密份额。如果属性集 $S \in \mathbf{M}$ 是访问授权集合，定义 $I = \{i; \rho(i) \in S\} \subset \{1, 2, \dots, l\}$ 。如果 $\{\lambda_i\}$ 是秘密 s 在 Π 上的有效共享，那么存在一组

常数 $\{\omega_i \in \mathbb{Z}_p^n\}_{i \in I}$, 使得等式 $\sum_{i \in I} \omega_i \lambda_i = s$ 。

2 系统设计

本文所提方案中每个医院都是独立的管理域, 与 MA-ABE 方案中的权限相对应, 每个机构负责在其域中发布和验证属性密钥。本文方案的总体流程如图 1 所示。

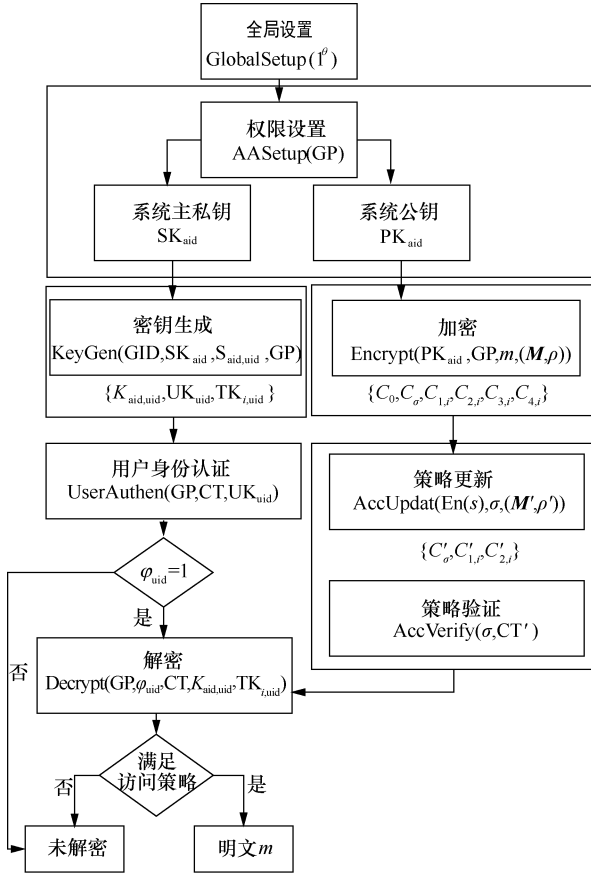


图 1 方案流程
Figure 1 Scheme process

2.1 系统模型

系统模型包括以下实体: 属性权威机构 (AA)、患者 (Patient)、医疗联盟机构 (MIS)、区块链网络 (BC)、云服务提供商 (CSP) 和数据用户 (DU), 如图 2 所示。

(1) 属性权威机构

AA 是相互独立的 (AA 中的属性集不重复)。一个 AA 对应管理一个独立的医疗机构, 每个属性机构负责在其域中发布和验证属性密钥。

(2) 患者

患者负责制定访问策略 (M, ρ) , 并使用多授权部分隐藏属性加密算法对其生成的电子医疗数据进行加密, 将生成的密文 CT 存储至医院本地云服务器, 云服务器返回其密文存储地址 address, 最后, 患者将密文存储地址 address 上传至区块链。

(3) 医疗联盟机构

多个医疗机构组成医疗联盟, 每个医院都是独立的管理域, 与 MA-ABE 方案中的权限相对应, 负责存储和管理患者数据。

(4) 区块链网络

BC 由各验证节点组成, 区块链网络节点负责对数据用户身份进行认证, 并存储访问控制策略区块 $T_{(M, \rho)}$ 。

(5) 数据用户

DU 可以是医疗机构、保险公司、医保管理部门等。当 DU 想要访问数据时, 需经过区块链节点运行用户身份认证算法, 对其身份进行认证, 若认证通过, 则可以得到密文地址; 否则, 拒绝访问。当 DU 得到密文地址后, DU 可根据其密文地址从云服务器获取密文, 只有 DU 的属性集 $S_{aid, uid}$ 满足密文策略中的属性集时, 才能成功解密密文, 获取明文信息。

(6) 云服务提供商

CSP 负责代理加密或解密。

2.2 算法描述

每个 AA 管理一个医疗机构, 为其管理域中的用户生成和分发属性密钥。当患者到医院就诊时, 医生为其生成电子病历, 患者利用自定义的访问策略对生成的电子病历加密和签名, 并将生成的密文 CT 存储至医院本地云服务器, 云服务器返回其密文存储地址 address, 患者通过存储事务将密文存储地址 address 上传至区块链存储。当数据用户想要访问数据时, 区块链节点首先对其身份进行认证, 认证通过后得到数据密文存储地址 address, 数据用户根据其密文存储地址从云服务器获取相关密文, 仅当数据用户满足密文中的访问策略, 才能解密从云服务器获取的密文。当患者更新访问策略时, 将更新后的访问策略生成访问控制策略区块 $T_{(M, \rho)}$ 并上传至区块链中, 实现

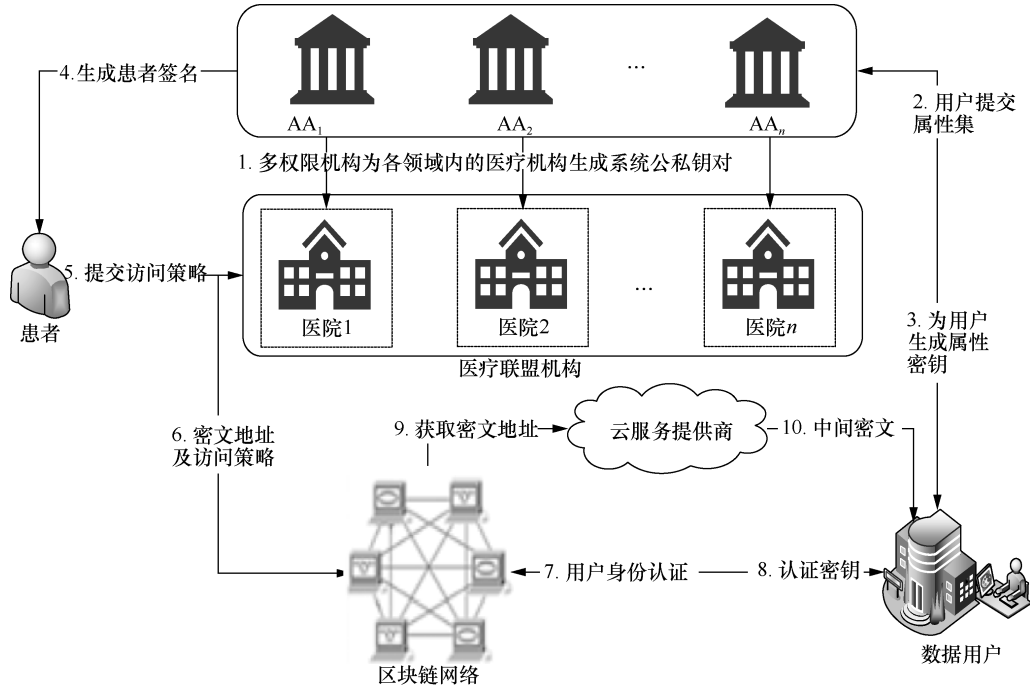


图2 系统模型
Figure 2 System model

隐藏策略条件下的数据追责，保证电子病历的安全共享。

本文方案主要由全局设置算法、权限设置算法、属性密钥生成算法、加密算法、用户身份认证算法、解密算法、策略更新算法和策略验证算法组成。各算法描述如下。

1) 全局设置算法 $\text{GlobalSetup}(1^\theta) \rightarrow \{\text{GP}\}$ 。输入安全参数 θ ，输出全局参数 GP。

全局设置算法首先选择 p 阶循环群 G 和 G_T ， G 到 G_T 的双线性映射 $e: G \times G \rightarrow G_T$ 。选择哈希函数 $H: \{0,1\}^* \rightarrow G_T$ ，将全局标识 GID 映射到 G_T 。

2) 权限设置算法 $\text{AASetup}(\text{GP}) \rightarrow (\text{PK}_{\text{aid}}, \text{SK}_{\text{aid}})$ 。权限设置算法由各医疗机构系统管理员运行，通过输入全局参数 GP，输出对应其身份 aid 机构的系统公私钥对 $(\text{PK}_{\text{aid}}, \text{SK}_{\text{aid}})$ ，系统公钥 PK_{aid} 对外公开，主私钥 SK_{aid} 秘密保留。

对于机构 AA_{aid} 的一组属性集 S_{aid} 中的每个属性 i ， AA_{aid} 随机选择 $\alpha_i, y_i \in Z_p$ ，则输出密钥对 $(\text{PK}_{\text{aid}}, \text{SK}_{\text{aid}})$ 为 $\text{PK}_{\text{aid}} = \{e(g_1, g_1)^{\alpha_i}, g_1^{y_i} \forall i\}$ ， $\text{SK}_{\text{aid}} = \{\alpha_i, y_i \forall i\}$ 。

3) 属性密钥生成算法 $\text{KeyGen}(\text{GID}, \text{SK}_{\text{aid}}, S_{\text{aid,uid}})$ ，

$\text{GP}) \rightarrow \{K_{\text{aid,uid}}, \text{UK}_{\text{uid}}, \text{TK}_{i,\text{uid}}\}$ 。密钥生成算法由属性授权机构 AA 运行，通过输入全局参数 GP，主私钥 SK_{aid} 和属于某权威机构 aid 的用户身份 uid 属性集 $S_{\text{aid,uid}}$ ，对于属性集 $S_{\text{aid,uid}}$ 中的每个属性 i ，算法生成属性私钥 $K_{\text{aid,uid}}$ 、用户身份验证密钥 UK_{uid} 和转换密钥 $\text{TK}_{i,\text{uid}}$ 。

一旦用户 uid 希望访问数据，他需要从相关的 AAs 请求密钥，为每个属性 i 生成对应其 GID 的属性密钥 $K_{\text{aid,uid}}$ 。 AA_{aid} 随机选择 $\varphi_{\text{uid}} \in Z_p$ ，则计算身份验证密钥 UK_{uid} 、转换密钥 $\text{TK}_{i,\text{uid}}$ 和用户密钥 $K_{\text{aid,uid}}$ 为 $K_{\text{aid,uid}} = \varphi_{\text{uid}}$ ， $\text{KS}_{\text{uid}} = g^{1/\varphi_{\text{uid}}}$ ， $\text{UK}_{\text{uid}} = g^{\alpha_i} H(\text{GID})^{y_i}$ ， $\text{TK}_{i,\text{uid}} = (g^{\alpha_i})^{1/\varphi_{\text{uid}}}$ 。

4) 加密算法 $\text{Encrypt}(\text{PK}_{\text{aid}}, \text{GP}, m, (\text{M}, \rho)) \rightarrow \text{CT}$ 。加密算法由患者运行。算法输入系统公钥 PK_{aid} ，全局参数 GP，待加密电子病历 m 和数据拥有者自定义的访问策略 (M, ρ) 。患者首先将其全局身份标识 GID 发送给权威机构，生成其签名 σ ；当患者去医院就诊时，主治医生生成患者电子病历；然后患者利用多权限部分属性隐藏加密算法对电子病历进行加密并签名，生成密文 CT。

患者首先根据其身份标识 GID 生成签名 σ 。加密过程中， M 是一个 $l \times n$ 阶矩阵， M_i 表示矩

阵中的第 i 行, $i \in [1, 2, \dots, l]$ 。函数 ρ 把 M 的每一行 M_i 映射到不同的属性上。选择随机数 $s \in Z_p$ 为秘密共享密钥, 选择随机向量 $\mathbf{v} = (s, t_2, t_3, \dots, t_n)^T \in Z_p^n$, 其中 $t_2, t_3, \dots, t_n$ 为随机值, $\lambda_i = M_i \mathbf{v}$ 表示秘密共享密钥份额, 随机向量 $\omega = (0, h_1, h_2, \dots, h_n)^T \in Z_p^n$, 且 $\omega_i = M_i \omega$, 患者随机选择 $\delta_i \in Z_p$ ($i \in \{1, 2, \dots, l\}$), 则生成密文 CT 为 $C_0 = me(g, g)^{\alpha s}$, $C_\sigma = g^{\sigma s}$, $C_{1,i} = g^{\lambda_i} g^{-\alpha_{\rho(i)} \delta_i}$, $C_{2,i} = g^{\delta_i}$, $C_{3,i} = g^{y_{\rho(i)} \delta_i} g^{\omega_i}$, $C_{4,i} = e(g, g)^{\alpha_{\rho(i)} \delta_i}$, 则 $CT = \{C_0, C_\sigma, C_{1,i}, C_{2,i}, C_{3,i}, C_{4,i}\}_{i \in [1, l]}$ 。

为实现访问控制策略动态更新, 加密完成后, 属性加密算法根据安全加密算法 (如 SM9) 对 s 进行加密, 作为保留加密信息 $En(s)$ 。

5) 用户身份认证算法 $UserAuthen(GP, CT, UK_{uid}) \rightarrow \varphi_{uid}$ 。用户认证算法由区块链节点运行。输入密文 CT 和用户身份验证密钥 UK_{uid} , 输出验证结果 φ_{uid} , 计算如下:

$$\varphi_{uid} = \prod_i \left(\frac{C_{4,i} e(H(uid), C_{3,i})}{e(UK_{\rho(i), uid}, C_{2,i})} \right)^{c_i} = \prod_i e(H(uid), g)^{\omega_i c_i} \quad (1)$$

当用户向区块链提交数据访问请求时, 用户身份认证算法由区块链节点运行。节点选择常数 $c_i \in Z_p^*$, 满足 $\sum_i c_i \lambda_i = s$ 。若计算结果 $\varphi_{uid} = 1$,

则用户认证通过, CSP 可以执行下一步解密操作。

6) 解密算法 $Decrypt(GP, \varphi_{uid}, CT, K_{aid, uid}, TK_{i, uid}) \rightarrow m \text{ or } \perp$ 。解密算法由数据用户运行。如果数据用户的身份认证通过, 且用户属性集 $S_{aid, uid}$ 满足 CT 中的访问策略 (M, ρ) , 则可以解密密文 CT 获得消息明文 m 。否则, 输出 $\perp$ 。

若用户满足步骤 5), 有 $\sum_i c_i \lambda_i = s$, 则先由云服务提供商执行解密算法, 得到中间密文 IT, 之后用户执行简单的解密算法, 获得其明文 m , 计算如下:

$$IT = \prod_i e(C_{1,i}, KS_{uid}) e(C_{2,i}, TK_{\rho(i), uid})^{c_i} = e(g, g)^{\alpha s / \varphi_{uid}} \quad (2)$$

$$m = C_0 / IT^{\varphi_{uid}}$$

7) 策略更新算法 $AccUpdat(En(s), \sigma, (M', \rho')) \rightarrow CT'$ 。策略更新算法输入保留的加密信息

$En(s)$, 更新者签名 σ 和新的访问策略 (M', ρ') , 输出新的策略密文 CT' 。

通过更新者签名 σ 对 $En(s)$ 解密获取 s' 作为第一个输入值, 根据新访问策略 (M', ρ') 选择随机向量 $\mathbf{v}' = (s', t'_2, t'_3, \dots, t'_n)^T \in Z_p^n$ 计算 $\lambda'_i = M'_i \mathbf{v}'$, 随机选取 $\delta'_i \in Z_p$ ($i \in \{1, 2, \dots, l'\}$), 则更新后的密文策略 CT' 为 $C'_\sigma = g^{\sigma s'}$, $C'_{1,i} = g^{\lambda'_i} g^{-\alpha_{\rho'(i)} \delta'_i}$, $C'_{2,i} = g^{\delta'_i}$, 则 $CT' = \{C'_\sigma, C'_{1,i}, C'_{2,i}\}$ 。

8) 策略验证算法 $AccVerify(\sigma, CT') \rightarrow CT''$ 。策略验证算法由区块链节点运行。输入更新者身份验证密钥 σ 和新的策略密文 CT' , 如果验证成功, 则输出更新后的密文 CT'' 。

共识节点首先验证签名消息 σ , 判断等式 $C_\sigma = C'_\sigma$ 是否成立。若验证通过, 以 $\{C'_{1,i}, C'_{2,i}\}_{i \in [1, l']}$ 生成新策略区块 $T'_{(M, \rho)}$, 并上传至区块链中, 同时输出更新后的密文 $CT'' = \{C_0, C_\sigma, C'_{1,i}, C'_{2,i}\}_{i \in [1, l']}$ 。

本方案设计了双重访问控制。当数据用户需要访问相关医疗数据时, 区块链共识节点先要对其身份进行验证, 只有验证通过才能获得密文存储地址; 当数据用户验证通过获得密文时, 数据用户还需满足密文中的访问策略才能最终解密获取明文。将密文存储地址及更新的访问策略上传至区块链中, 通过访问策略块 $T'_{(M, \rho)}$ 实现隐藏策略下的可追溯, 以保证各医疗机构间电子病历的安全共享。

3 方案分析

3.1 正确性分析

1) 当用户想要访问数据时, 区块链节点需运行用户身份认证算法对用户进行认证。若属性集满足 uid 的属性集, 且 $\omega_i = M_i \omega$, 其中 $\omega \cdot (1, 0, \dots, 0) = 0$, 则进行以下计算:

$$\varphi_{uid} = \prod_i \left(\frac{C_{4,i} e(H(uid), C_{3,i})}{e(UK_{\rho(i), uid}, C_{2,i})} \right)^{c_i} =$$

$$\prod_i \left(\frac{e(g, g)^{\alpha_{\rho(i)} \delta_i} e(H(uid), g^{y_{\rho(i)} \delta_i} g^{\omega_i})}{e(g^{\alpha_{\rho(i)}} H(uid)^{y_{\rho(i)}}, g^{\delta_i})} \right)^{c_i} =$$

$$\prod_i \left(\frac{e(g, g)^{\alpha_{\rho(i)} \delta_i} e(H(uid), g)^{y_{\rho(i)} \delta_i} e(H(uid), g)^{\omega_i}}{e(g, g)^{\alpha_{\rho(i)} \delta_i} e(H(uid), g)^{y_{\rho(i)} \delta_i}} \right)^{c_i} =$$

$$\prod_i e(H(uid), g)^{\omega_i c_i} \quad (3)$$

若式(3)成立,则用户身份认证算法满足正确性。

2) 若用户的属性集 $S_{\text{aid},\text{uid}}$ 是一个授权集,那么用户获得对应的私钥 $K_{\text{aid},\text{uid}}$, 且 $\sum_i c_i \lambda_i = s$, 进行以下解密运算:

$$m = \frac{C_0}{\prod_i (e(C_{1,i}, \text{KS}_{\text{uid}}) e(C_{2,i}, \text{TK}_{\rho(i),\text{uid}}))^{\varphi_{\text{uid}} c_i}} = \frac{me(g, g)^{\sigma \alpha s}}{\prod_i (e(g^{\lambda_i} g^{-\alpha_{\rho(i)} \delta_i}, g^{1/\varphi_{\text{uid}}}) e(g^{\delta_i}, (g^{\alpha_i})^{1/\varphi_{\text{uid}}}))^{\varphi_{\text{uid}} c_i}} = \frac{me(g, g)^{\sigma \alpha s}}{\prod_i e(g^{\lambda_i} g^{-\alpha_{\rho(i)} \delta_i}, g^{1/\varphi_{\text{uid}}}) e(g^{\delta_i}, (g^{\alpha_i})^{1/\varphi_{\text{uid}}})^{\varphi_{\text{uid}} c_i}} = \frac{me(g, g)^{\sigma \alpha s}}{e(g, g)^{\sigma \alpha s}} = m \quad (4)$$

若式(4)成立,则解密算法满足正确性。

3.2 安全性分析

定理 1 在选择明文攻击下的不可区分性 (IND-CPA), 本文方案是安全的。

证明 定理 1 的证明采用 IND 游戏的方法, 假设游戏中存在多项式时间敌手 A , 用 ε 表示敌手 A 在游戏中的优势。

初始化阶段: 挑战者 C 产生系统 Π , 调用 $\text{AASetup}(\text{GP})$ 算法得到公私钥对 $(\text{PK}_{\text{aid}}, \text{SK}_{\text{aid}})$, 并将公钥 PK_{aid} 发给敌手。

查询阶段 1: 敌手 A 提交他的 $(\text{uid}, S_{\text{aid},\text{uid}})$ 并自适应查询挑战者的密钥, 挑战者运行密钥生成算法, 生成密钥 $K_{\text{aid},\text{uid}} = \varphi_{\text{uid}}$ 和 $\text{KS}_{\text{uid}} = g^{1/\varphi_{\text{uid}}}$ 发送给敌手。

挑战阶段: 敌手 A 随机选择两个长度相同的明文消息 m_0 和 m_1 及两个访问结构 $(\mathbf{M}, \rho, M_{\rho(\beta)}) \beta \in (0,1)$ 提交给系统。前提条件是, 对查询阶段 1 中的任何查询, 属性集都不能满足访问结构。挑战者随机选择访问结构 $(\mathbf{M}, \rho, M_{\rho(\beta)}) \beta \in (0,1)$ 加密消息 m_β , 随机选择用于将 CT 输出到对手的秘密 s 作为其挑战密文, 敌手可以得到 CT' 。

查询阶段 2: 敌手 A 自适应地对不满足访问结构 $(\mathbf{M}, \rho, M_{\rho(\beta)}), \beta \in (0,1)$ 的挑战者询问相关属性密钥。

猜测阶段: 敌手 A 输出对 β 的猜想 $\beta' \in (0,1)$ 。

如果 $\beta = \beta'$, 则挑战者输出 1, 否则输出 0。

在上述安全游戏中, 在查询阶段敌手 A 获得 $\text{CT}' = e(g, g)^{s \varphi_{\text{uid}}}$ 和 $\text{KS}_{\text{uid}} = g^{1/\varphi_{\text{uid}}}$, 令 $B = \text{KS}_{\text{uid}}$, $Z = \text{CT}'$, 假设敌手可以在 CPA 游戏中获胜的优势为:

$$\Pr[S(B, Z) = 1 | Z] = \frac{1}{2} \quad (5)$$

敌手无法猜测消息 m_β 的优势为

$$\Pr[S(B, Z) = 1 | Z'] = \frac{1}{2} \quad (6)$$

挑战者赢得游戏的优势为

$$\begin{aligned} \Pr[S(B, Z) = 1] &= \frac{1}{2} \Pr[S(B, Z) = 1 | Z] + \frac{1}{2} \Pr[S(B, Z) = 1 | Z'] = \\ &= \frac{1}{2} \left(\frac{1}{2} + \varepsilon \right) + \frac{1}{2} \cdot \frac{1}{2} = \frac{1}{2} + \frac{\varepsilon}{2} \end{aligned} \quad (7)$$

因此多项式时间中, 任何敌手赢得 IND-CPA 游戏的优势是可忽略的。

证毕。

定理 2 若数字签名算法满足不可伪造性, 则该算法可以抵抗策略更新攻击。

证明 根据访问策略更新算法 $\text{AccUpdat}(\text{En}(s), \sigma, (\mathbf{M}', \rho'))$ 可知, 若恶意管理者欲发起访问策略攻击, 即不解密 $\text{En}(s)$ 而直接计算 $C'_\sigma = g^{\sigma s'}$, 则 $C'_\sigma = g^{\sigma s'} \neq g^{\sigma s}$ 将无法通过验证, 因此恶意管理者无法成功更新访问策略; 若恶意用户欲发起攻击, 则需提供管理者的身份签名消息 σ 和策略密文 C'_σ , 由于签名算法具有不可伪造性且恶意用户无法提供有效的 C'_σ , 因此恶意用户无法通过验证, 即恶意用户无法成功更新访问策略, 则该算法可以抵抗策略更新攻击。

证毕。

定理 3 若通过 $\text{En}(s)$ 解密得到的 s' 与加密时使用的 s 一致, 则更新算法具有正确性。

证明 根据加密算法 $\text{Encrypt}(\text{PK}_{\text{aid}}, \text{GP}, m, (\mathbf{M}, \rho))$ 及其生成的密文结构 $\text{CT} = \{C_0, C_\sigma, C_{1,i}, C_{2,i}, C_{3,i}, C_{4,i}\}, i \in [1, l]$ 知, 若要对 CT 的访问控制策略进行更新, 则对 CT 解密获取 m 后重新加密即可。通过旧的属性私钥 $K_{\text{aid},\text{uid}}$ 解密密文 CT 获取

m 后, 更新者输入 σ 和新访问策略 (M', ρ') , 算法选取新秘密共享值 s' 和随机参数 $t'_2, t'_3, \dots, t'_n$, 对 m 再次加密生成全新密文 $CT'' = \{C_0, C_\sigma, C'_{1,i}, C'_{2,i}\}_{i \in [1, l']}$ 即可。根据解密算法 $\text{Decrypt}(GP, \phi_{\text{uid}}, CT, K_{\text{aid,uid}}, TK_{i,\text{uid}})$ 可知, 满足新策略的用户可以借助属性密钥 $K'_{\text{aid,uid}}$ 通过解密 C'_σ 和 $(C'_{1,i}, C'_{2,i})_{i \in [1, l']}$ 最后得到 m 。即 $K'_{\text{aid,uid}}$ 可以正确解密更新后的密文 $CT'' = \{C_0, C_\sigma, C'_{1,i}, C'_{2,i}\}_{i \in [1, l']}$ 。

证毕。

4 性能分析

4.1 功能性分析

通过将本文方案与文献[23-25]提出的方案在授权类型、访问结构、隐藏策略、外包解密和访问策略更新方面的功能对比, 可以看出本文方案具有综合功能优势, 如表 2 所示。

表 2 功能比较
Table 2 Function comparison

方案	授权类型	访问结构	隐藏策略	外包解密	访问策略更新
文献[23]	多授权	LSSS	是	否	否
文献[24]	单授权	AND	否	是	否
文献[25]	多授权	LSSS	是	否	否
本文方案	多授权	LSSS	是	是	是

4.2 实验分析

本文仿真实验采用一台主机 (CPU 为 Intel Core i32120, 内存为 4 GB, 操作系统为 Windows 7), 并选用 Python 编程语言来构建实验框架, 以比较本文方案的解密计算成本与文献[23]、文献[25]所提方案的不同。当机构数分别设置为 4, 6, 8, 10, 12, 14, 16, 18, 20 时, 权限机构数量越多, 方案的用户解密时间越长, 而本文方案的解密时间比其他两种方案解密所需时间较少, 如图 3 所示。可见, 本文方案能够降低一定的时间开销。

若要实现用户访问权限的更改, 可以通过重加密方式和策略更新方式完成。通过仿真实验得到二者的时间代价如图 4 所示, 当更新算法的属性个数依次递增时, 策略更新总时间消耗比重加密总时间消耗少, 因此本文方案的访

问策略更新算法有一定优势。

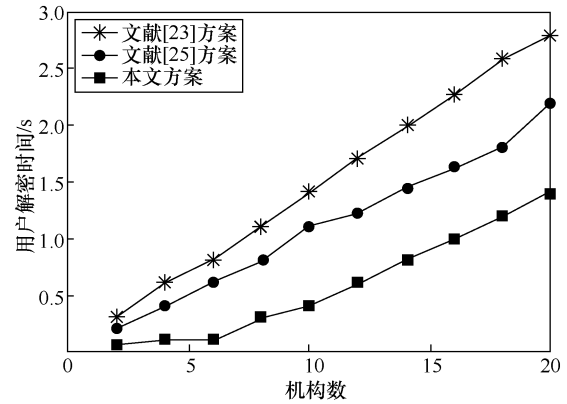


图 3 用户解密时间对比
Figure 3 Comparison of user decryption time

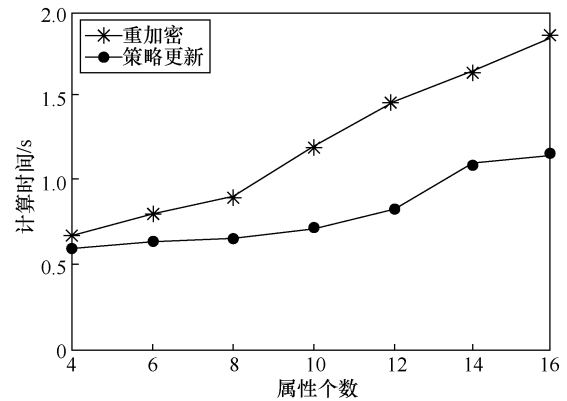


图 4 重加密与策略更新时间对比
Figure 4 Comparison of re-encryption and policy update time

5 结束语

针对不同医院之间共享电子病历信任建立成本高、患者隐私易泄露及难以追责等问题, 本文提出一种基于区块链的多权限属性隐藏电子病历共享方案, 可以实现分布式和可信的电子病历安全共享。首先, 引入多权限属性加密以解决信任成本高及单点故障问题; 由于访问策略中包含与用户相关的某些敏感数据, 本文采用线性秘密共享方案, 这样不仅可以支持灵活的访问结构, 同时可以实现属性的部分隐藏, 保护用户隐私。其次, 结合区块链设计可信的访问策略动态更新算法, 用户可以动态更新访问策略, 将生成的新访问策略区块上传至区块链中, 能够实现隐藏策略下的可追溯。最后, 通过安全性及实验分析表明, 所提方案可以在保护用户隐私安全的同时, 降低

计算开销, 实现动态隐私保护。

但现有的电子病历共享方案还存在一些不足之处, 仍需要持续更新和完善, 如访问控制细粒度不够, 数据共享效率低等问题。在未来工作中, 将继续探究基于区块链的医疗数据共享方案的实现途径和方法, 如基于区块链设计高效灵活、更细粒度的分级诊疗方案, 利用智能合约自动实现分级访问控制算法等以提高系统的高效性和可扩展性。

参考文献:

- [1] SAHAI A, WATERS B R. Fuzzy identity-based encryption[C]//24th Annual International Conference on Theory and Applications of Cryptographic Techniques. 2004: 457-473.
- [2] LI H, YANG Y, DAI Y, et al. Achieving secure and efficient dynamic searchable symmetric encryption over medical cloud data[J]. IEEE Transactions on Cloud Computing, 2020, 8(2): 484-494.
- [3] LI H, LIU D, DAI Y, et al. Personalized search over encrypted data with efficient and secure updates in mobile clouds[J]. IEEE Transactions on Emerging Topics in Computing, 2018, 6(1): 97-109.
- [4] WANG S, ZHANG Y, ZHANG Y. A blockchain-based framework for data sharing with fine-grained access control in decentralized storage systems[J]. IEEE Access, 2018, 6: 38437-38450.
- [5] GOYAL V, PANDEY O, SAHAI A, et al. Attribute-based encryption for fine-grained access control of encrypted data[C]//13th ACM conference on Computer and Communications Security. 2006: 89-98.
- [6] BETHENCOURT J, SAHAI A, WATERS B. Ciphertext-policy attribute-based encryption[C]//2007 IEEE Symposium on Security and Privacy (SP'07). 2007: 321-334.
- [7] ZHANG Y, ZHENG D, DENG R H. Security and privacy in smart health: Efficient policy-hiding attribute-based access control[J]. IEEE Internet Things, 2018, 5(3): 2130-2145.
- [8] WU A, ZHANG Y, ZHENG X, et al. Efficient and privacy-preserving traceable attribute-based encryption in blockchain[J]. Ann. Telecommun., 2019, 74(7-8): 401-411.
- [9] MIAO Y, MA J, LIU X, et al. Lightweight fine-grained search over encrypted data in fog computing[J]. IEEE Transactions on Services Computing, 2019, 12(5): 772-785.
- [10] CHASE M. Multi-authority attribute-based encryption[C]//Proceedings of Cryptography Conference on Theory of Cryptography (TCC'07). 2007: 515-534.
- [11] LIN H, CAO Z F, LIANG X. Secure threshold multi-authority attribute-based encryption without a central authority[C]//Proceedings of International Conference on Cryptology. 2008: 426-436.
- [12] LEWKO A, WATERS B. Decentralizing attribute-based encryption[C]//Proceedings of International Conference on the Theory and Applications of Cryptographic Techniques. 2011: 568-588.
- [13] QIAN H L, LI J G, ZHANG Y C, et al. Privacy-preserving personal health record using multi-authority attribute-based encryption with revocation[J]. International Journal of Information Security, 2015(14): 487-497.
- [14] ZHONG H, ZHU W, XU Y, et al. Multi-authority attribute-based encryption access control scheme with policy hidden for cloud storage[J]. Soft Computing A Fusion of Foundations Methodologies & Applications, 2018, 22(1): 243-251.
- [15] YAN X, LIU Y, LI Z, et al. Multi-authority attribute-based encryption scheme with policy dynamic updating[J]. Journal on Communications, 2017, 38(10): 94-101.
- [16] ZHANG P, CHEN Z, LIU J K, et al. An efficient access control scheme with outsourcing capability and attribute update for fog computing[J]. Future Generation Computer Systems, 2018, 78: 753-762.
- [17] DI FRANCESCO MAESA D, MORI P, RICCI L. A blockchain based approach for the definition of auditable access control systems[J]. Computers & Security, 2019, 84: 93-119.
- [18] LI R, SONG T, MEI B, et al. Blockchain for large-scale internet of things data storage and protection[J]. IEEE Transactions on Services Computing, 2019, 12(5): 762-771.
- [19] DORRI A, KANHERE S S, JURDAK R, et al. Blockchain for IoT security and privacy: The case study of a smart home[C]//2017 IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom Workshops). 2017: 618-623.
- [20] DING S, CAO J, LI C, et al. A novel attribute-based access control scheme using blockchain for IoT[J]. IEEE Access, 2019, 7: 38431-38441.
- [21] MAESA D D F, MORI P, RICCI L. Blockchain based access control[C]//2017 IFIP International Conference on Distributed Applications and Interoperable Systems. 2017: 206-220.
- [22] LAI J, DENG R H, LI Y. Fully secure ciphertext-policy hiding CP-ABE[C]//2011 International Conference on Information Security Practice and Experience. 2011: 24-39.
- [23] WANG H, NING J, HUANG X, et al. Secure fine-grained encrypted keyword search for e-healthcare cloud[C]//IEEE Transactions on Dependable and Secure Computing. 2021: 1307-13019.
- [24] CUI H, DENG R H, WU G, et al. An efficient and expressive ciphertext-policy attribute-based encryption scheme with partially hidden access structures[C]//2016 International Conference on Provable Security. 2016: 19-38.
- [25] YANG K, HAN Q, LI H, et al. An efficient and fine-grained big data access control scheme with privacy-preserving policy[J]. IEEE Internet Things, 2017, 4(2): 563-571.
- [26] NISHIDE T, YONEYAMA K, OHTA K. Attribute-based encryption with partially hidden encryptor-specified access structures[C]//2008 International Conference on Applied Cryptography and Network Security. 2008: 111-129.
- [27] HUR J. Attribute-based secure data sharing with hidden policies in smart grid[J]. IEEE Transactions on Parallel & Distributed Systems, 2013, 24(11): 2171-2180.
- [28] QI H, YING H Z, HUI L. Efficient and robust attribute-based encryption supporting access policy hiding in Internet of Things[J]. Future Generation Computer Systems, 2018, 83: 269-277.

- [29] WANG Y, FAN K. Effective CP-ABE with hidden access policy[J]. Journal of Computer Research and Development, 2019, 56(10): 2151-2159.
- [30] LIU Y, DU R. Efficient partially policy-hidden with multi-authority for access control scheme in Internet of Things[C]//2020 International Conference on Networking and Network Applications (NaNA). 2020: 375-380.
- [31] YANG K, JIA X, REN K. Secure and verifiable policy update out-sourcing for big data access control in the cloud[J]. IEEE Transactions on Parallel and Distributed Systems, 2015, 26(12): 3461-3470.
- [32] LIU D, LI H, YANG Y, et al. Achieving multi-authority access control with efficient attribute revocation in smart grid[C]//2014 IEEE International Conference on Communications. 2014: 634-639.
- [33] HUANG X F, TAO Q, QIN B D, et al. Multi-authority attribute based encryption scheme with revocation[C]//2015 IEEE International Conference on Computer Communication & Networks. 2015: 1-5.
- [34] 田有亮, 杨科迪, 王纘, 等. 基于属性加密的区块链数据溯源算法[J]. 通信学报, 2019, 40 (11): 101-111.
TIAN Y L, YANG K D, WANG Z, et al. Algorithm of blockchain data provenance based on ABE[J]. Journal on Communications, 2019, 40 (11): 101-111.

[作者简介]



金琳 (1997-), 女, 云南曲靖人, 贵州大学硕士生, 主要研究方向为属性加密、区块链。



田有亮 (1982-), 男, 贵州盘县人, 博士, 贵州大学教授、博士生导师, 主要研究方向为算法博弈论、密码学与安全协议、大数据隐私保护与区块链技术。