

支持云审计与设备安全检测的 IoMT 数据安全方案

谢鹏寿, 董欣瑶, 鲁晔, 孙宁, 景兰青

(兰州理工大学计算机与人工智能学院, 甘肃 兰州 730050)

摘要: 基于密文策略的属性基加密方案被广泛应用于医疗物联网数据安全传输与共享, 但传统方案在抵抗合谋攻击、数据完整性审计等方面存在不足。为此, 提出了一种支持云审计与设备安全检测的 IoMT 数据安全方案。该方案采用安全两方计算生成数据使用者密钥, 抵抗授权中心腐化下用户合谋攻击, 通过在密文聚合多项式中计算基于同态的隐私保护消息认证码来嵌入设备指纹, 实现云端数据的高效审计和医疗设备的安全检测。安全分析表明, 所提方案能够保证云端数据完整性审计、数据审计隐私和可靠性, 以及医疗设备安全状态检测, 并且具有授权中心腐化下抗用户合谋攻击的选择明文攻击不可区分性。仿真实验结果表明, 相较于同类方案, 所提方案在通信开销方面降低约 38.7%, 在计算开销方面降低约 68%, 明显提高了医疗数据共享的安全性和效率。

关键词: 云审计; 属性基加密; 物理不可克隆函数; 同态哈希函数; 安全两方计算

中图分类号: TP309

文献标志码: A

doi: 10.11959/j.issn.1000-436x.TXXB260083

IoMT data security scheme supporting cloud auditing and device security detection

Xie Pengshou, Dong Xinyao, Lu Ye, Sun Ning, Jing Lanqing

School of Computer Science and Artificial Intelligence, Lanzhou University of Technology, Lanzhou 730050, China

Abstract: Ciphertext-policy attribute-based encryption (CP-ABE) schemes are widely utilized for the secure transmission and sharing of data in the Internet of medical things (IoMT). However, conventional schemes exhibit deficiencies in resisting collusion attacks and providing data integrity auditing. To address these issues, an IoMT data security scheme supporting cloud auditing and device security detection was proposed. In this scheme, data user keys were generated using secure two-party computation to resist user collusion attacks under a corrupted authority. Furthermore, device fingerprints were embedded by computing a homomorphic privacy-preserving message authentication code within ciphertext-aggregated polynomials, thereby enabling efficient cloud data auditing and secure medical device detection. Security analysis indicates that the proposed scheme ensures cloud data integrity auditing, data auditing privacy and reliability, as well as the security status detection of medical devices. It also achieves indistinguishability under chosen-plaintext attacks (CPA) against user collusion even in the presence of a corrupted authority. Simulation results demonstrate that, compared with similar schemes, the proposed scheme reduces communication overhead by approximately 38.7% and computational overhead by approximately 68%. This scheme significantly improves the security and efficiency of medical data sharing.

Key words: cloud auditing, attribute-based encryption, physical unclonable function, homomorphic hash function, secure two-party computation

收稿日期: 2026-02-04; 修回日期: 2026-04-18

通信作者: 董欣瑶, 1824143940@qq.com

基金项目: 国家自然科学基金资助项目(No.62462044)

Foundation Item: The National Natural Science Foundation of China (No.62462044)

0 引言

云计算通过互联网集中共享计算与存储资源^[1]。随着医疗物联网(Internet of medical things, IoMT)的快速发展,可穿戴医疗设备在医疗保健中广泛使用,这种设备利用传感器通过贴近皮肤的方式实时采集数据,并将海量数据迁移到云端存储与计算。被授权的数据使用者(data user, DU)可对数据进行访问,用于医疗管理和患者护理等场景^[2]。然而,云存储的医疗数据因恶意的外部攻击、医疗设备的物理攻击以及未授权访问构成数据泄露等威胁,加剧了IoMT系统在隐私保护、细粒度访问控制、医疗设备物理安全以及医疗数据完整性审计方面的技术复杂性^[3]。

传统的数据保护方式无法适应医疗数字化快速发展的需求,如今云端的医疗数据采用密文方式存储,并且数据所有者(data owner, DO)采用访问控制策略对DU进行筛选。属性基加密(attribute-based encryption, ABE)是一种新兴加密技术^[4],其中DO设计数据访问策略,实现对云存储中加密数据的访问控制,仅当DU的属性集合与访问控制策略匹配时才能解密。ABE方案根据密文、密钥与访问策略的绑定关系分为密钥策略的属性加密(key-policy ABE, KP-ABE)和密文策略的属性加密(ciphertext-policy ABE, CP-ABE)两种类型^[5]。在CP-ABE方案中,访问策略包含在密文中,用户密钥与属性集合对应,当DU的属性与密文中的访问策略匹配时,该DU可以解密密文。在IoMT系统中,CP-ABE方案允许患者定义医疗数据的访问策略,并将访问策略与密文绑定并上传到云存储器上,指定能够获取此密文的DU,CP-ABE方案被认为是构建IoMT系统最具潜力的技术方案^[6]。

然而,传统CP-ABE方案存在一定局限性。在应对集中式授权管理风险方面,传统的单一授权中心容易面临单点故障和合谋攻击,导致系统故障或者敏感数据泄露。刘霞等^[7]在随机化密钥基础上,使用双层随机掩蔽技术抵御合谋攻击,即使攻击者获取多个用户的部分密钥,也无法通过属性交叉拼接破解密文。IoMT系统中访问策略复杂,方案的加/解密成本较高。为提高CP-ABE的运行效率,李集浩^[8]构建了支持在线/离线加密CP-ABE方案,降低用户在加密阶段的计算开销。徐航星^[9]提出了支持外包解密的CP-ABE方案,将绝大多数解密计算

委托给云端服务器,提高DU解密效率。当DO将数据上传到云端之后便失去对数据的访问控制,半可信的云存储商可能会在降低存储成本的情况下,对存储在云端的数据进行部分删除,故对云端数据进行完整性审计很重要。自Goodrich等^[10]提出对半可信的云服务器进行公开审计之后,现阶段的云存储数据完整性审计工作由第三方审计者(third-party auditor, TPA)执行。Yang等^[11]提出了一种基于关键词的数据完整性验证机制,在审计过程中,TPA只会看到哈希值,不会获知原始数据,保证审计的隐私性。Li等^[12]提出了一种安全的医疗数据共享系统,将区块链的防篡改审计能力与可信执行环境(trusted execution environment, TEE)的机密计算能力深度融合,实现数据的安全存储与完整性验证。Yang等^[13]提出了一种实时密文验证的方案并且支持外包解密,但是并未对医疗物理设备的安全状态检测提出解决方案。在IoMT系统中,医疗设备作为数据来源,必须具备可靠性。梁文丰^[14]提出了将物理不可克隆函数(physical unclonable function, PUF)集成于硬件设备的协同架构,构建针对医疗物理设备捕获与智能卡窃取的主动防御体系。王雄等^[15]提出了一种基于PUF的远程医疗身份认证协议与密钥交换方案,但是并未考虑PUF的噪声问题。综合现有研究发现,当前IoMT数据安全方案在实现细粒度访问控制的同时,仍面临以下问题:易遭受合谋攻击、计算开销较高、数据完整性审计与隐私保护难以兼顾,设备侧安全性与数据来源可信性保障不足,尚未形成兼顾多维安全需求的统一解决方案。

针对上述问题,本文提出了一种支持云审计与设备安全检测的IoMT数据安全方案。与同类方案的功能性对比如表1所示,其中√表示符合,×表示不符合。本文的主要贡献如下。

(1)在DU密钥生成阶段,本文采用Paillier同态加密^[16]实现安全两方计算(secure two-party computation, 2PC),由密钥生成中心与属性授权机构协同生成DU密钥,实现在授权中心腐化情况下抗用户合谋攻击,提高系统的安全性。

(2)在数据完整性审计方面,本文在CP-ABE框架之上设计了基于同态的隐私保护消息认证码(privacy-preserving message authentication code, PMAC),其中嵌入医疗设备的指纹信息,在不改变CP-ABE访问控制结构的前提下,可实现数据完

表 1

不同方案功能对比

方案	安全性	抗用户合谋	在线/离线加密	外包解密	数据完整性审计	挑战抗篡改	TPA-MCS 非交互式挑战-应答	设备安全状态检测
文献[3]	选择性	√	×	×	×	×	×	×
文献[6]	选择性	√	×	√	√	×	×	×
文献[7]	选择性	√	×	√	×	×	×	×
文献[8]	选择性	√	√	√	×	×	×	×
文献[9]	选择性	√	×	√	√	×	×	×
文献[11]	选择性	√	×	×	√	√	×	×
文献[12]	选择性	×	×	×	√	√	×	×
文献[15]	自适应	×	×	×	×	√	×	×
本文方案	选择性	√	√	√	√	√	√	√

完整性审计、审计隐私保护与设备物理安全状态检测的协同。

(3) 采用 DO 在线/离线加密与医疗云服务器 (medical cloud server, MCS) 外包解密, 提高数据的加解密效率。在 MCS 上部署 TEE, 采用非交互式挑战-应答机制进行数据完整性审计, 防止挑战被篡改以及云存储商的数据篡改行为。

1 预备知识

1.1 双线性映射

G_1 和 G_2 是两个阶为大素数 p 的乘法循环群, 如果一个映射 $e: G_1 \times G_1 \rightarrow G_2$ 满足以下 3 个属性, 则称为双线性映射^[17]。

(1) 双线性。对于 $a, b \in Z_p^*$ 和 $u, v \in G_1$, 有 $e(u^a, v^b) = e(u, v)^{ab}$ 。

(2) 非退化性。存在 $g \in G_1$, 使 $e(g, g) \neq 1_{G_2}$, 其中 1_{G_2} 是 G_2 的单位元。

(3) 可计算性。对于所有的 $u, v \in G_1$, 存在高效的算法计算 $e(u, v)$ 。

1.2 访问结构

令 $S = \{P_1, P_2, \dots, P_n\}$ 表示基于属性加密方案的包含 n 个属性的集合, 则访问结构 A 是由 S 的非空子集组成的集合。若存在访问结构 $B \in A$, $\forall B, C$, 若集合 $B \in A$ 且 $B \subseteq C$, 则有 $C \in A$, 称 A 是单调的访问结构。若集合 $D \in A$, 则称 D 为授权集合; 若集合 $D \notin A$, 则称 D 为非授权集合^[18]。

1.3 线性秘密共享方案

线性秘密共享方案 (linear secret sharing scheme, LSSS) 定义如下。设 p 是一个大素数, S 是一个属

性集合, M 是一个 $l \times n$ 的矩阵, ρ 是一个单射函数。如果 S 上的秘密共享方案在 Z_p^* 上是线性的, 则需要满足以下两个算法^[19]。

(1) 秘密值共享: M 共享秘密值 $s \in Z_p^*$, 设向量 $y = (s, \delta_2, \delta_3, \dots, \delta_n)^T \in Z_p^n$, 其中 $\delta_2, \delta_3, \dots, \delta_n \in Z_p^*$, 在该算法中, $\lambda'_i = M_i y$ 表示属性名 $\rho(i)$ 持有的共享子秘密值。

(2) 秘密值重构: $S \in A$ 是一个授权集合, 其中 $I \subseteq \{1, 2, \dots, l\}$ 定义为 $I = \{i | \rho(i) \in S\}$, 存在一组常数 $\{w_i \in Z_p\}_{i \in I}$, 使 $\sum_{i \in I} w_i M_i = (1, 0, \dots, 0)$, 因此

$$\sum_{i \in I} w_i \lambda_i = s。$$

1.4 物理不可克隆函数

PUF 利用芯片在制造过程中产生的细微物理差异^[20], 使每个芯片具备特有的设备指纹。PUF 特定的产生机制计算开销小, 具有不可预测和不可克隆性。PUF 的逻辑表达式为:

$$R_i = \text{PUF}(C_i) \quad (1)$$

其中, C_i 为挑战, R_i 为响应。为了使 PUF 在不同温度下仍能保持输出稳定, 采用模糊提取器 (fuzzy extractor, FE) 来确保输出结果的一致性。FE 包含两种算法: 生成算法 $\text{FE.Gen}(\cdot)$ 和重建算法 $\text{FE.Rec}(\cdot)$ 。

$$\text{FE.Gen}(R_i) \rightarrow (\beta_i, \text{RP}) \quad (2)$$

$$\text{FE.Rec}(R_i, \text{RP}) \rightarrow \beta_i \quad (3)$$

其中, 式(2)为 $\text{FE.Gen}(\cdot)$ 的逻辑表达式, 输入 R_i , 生成物理特征密钥 $\beta_i \in [0, 1]^{bkl}$ 和重建参数 RP ; 式(3)为 $\text{FE.Rec}(\cdot)$ 的逻辑表达式, 若满足

$HD(R_i^*, R_i) \leq \text{ert}$, 则可以重建 β_i , 其中 HD 为汉明距离, ert 为误差容忍。

1.5 安全两方计算

在安全两方计算协议中, 参与方 P_1 与 P_2 可借助各自的隐私输入 x_1 与 x_2 , 共同计算函数 $f = (f_1, f_2)$, 并分别输出 $f_1(x_1, x_2)$ 与 $f_2(x_1, x_2)$, 且无法获知除此之外的任何信息。其中, 安全性质可归纳为以下 5 个方面^[21]。

(1) 隐私性。除了从自己的输入和输出中推导出的信息外, 任何一方都不能获得关于另一方输入的任何额外信息。

(2) 正确性。诚实的参与方能够正确计算出协议预定的函数结果, 即其输出确实是基于双方输入的正确函数值。

(3) 输入独立性。被敌手腐化的参与方在选择输入时, 必须独立于诚实参与方的输入。

(4) 输出可达性。敌手不能通过偏离协议流程来阻止诚实方获得其应有的输出, 诚实方总能在协议执行后得到计算结果。

(5) 公平性。被腐化参与方可以获得输出, 当且仅当诚实的参与方获得输出。

1.6 同态哈希函数

HHF(x): 该算法为同态哈希函数 (homomorphic hash function, HHF), 输入消息 $x \in Z_p$, 输出 x 的哈希值, 即 $\text{HHF}: H \leftarrow g^x \in G_1$ 。

同态哈希函数满足以下两个性质^[22]。

(1) 同态性。对于任意两个数据 m_1 、 m_2 和实数 w_1 、 w_2 , 都有 $\text{HHF}(w_1 m_1 + w_2 m_2) = H(m_1)^{w_1} \cdot$

$H(m_2)^{w_2}$ 。

(2) 抗碰撞性。攻击者不存在概率多项式时间算法, 能伪造 $(m_1, m_2, m_3, w_1, w_2)$, 且 $m_3 \neq w_1 m_1 + w_2 m_2$, 使得 $\text{HHF}(m_3) \neq H(m_1)^{w_1} H(m_2)^{w_2}$ 。

1.7 q-Diffie-Hellman 指数假设(q-DHE)

设 G_1 是一个阶为素数 p 的乘法循环群, g 是 G_1 的生成元。随机选取指数 $\alpha \in Z_p^*$, 给定一个序列 U 包含 $2q$ 个群元素如式(4)所示, 以及一个挑战元素 $Z \in G_1$, 判断 Z 是否等于 $g^{\alpha^{q+1}}$ 。不存在概率多项式时间算法 A 以不可忽略的优势区分 $R = (U, g^{\alpha^{q+1}})$ 和 $D = (U, Z)$, 如式(5)所示, 则 q-DHE 假设在群 G_1 中成立^[23]。

$$U = (g, g^\alpha, g^{\alpha^2}, \dots, g^{\alpha^q}, g^{\alpha^{q+2}}, g^{\alpha^{q+3}}, \dots, g^{\alpha^{2q}}) \quad (4)$$

$$\text{Adv}_A^{\text{q-DHE}}(k) = |\Pr[A(R) = 1] - \Pr[A(D) = 1]| \quad (5)$$

2 形式化模型

2.1 方案模型

支持云审计与设备安全检测的 IoMT 数据安全方案包含 6 个实体: 密钥生成中心 (key generation center, KGC)、属性授权机构 (attribute authority, AA)、MCS、TPA、DO 和 DU, 其系统模型如图 1 所示。

(1) KGC。KGC 是一个半诚实的实体, 负责生成公共参数、系统主密钥以及与 AA 通过安全两方计算生成 DU 的辅助密钥。

(2) AA。AA 是一个半诚实的实体, 定义属性集合, 当 DU 加入系统时, 根据 DU 的属性集合生成 DU 的属性私钥。

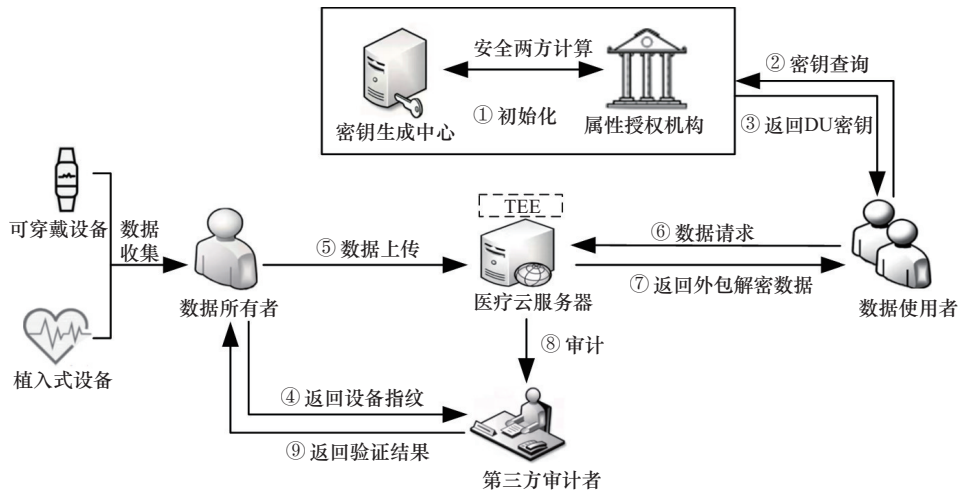


图1 系统模型

(3) MCS。MCS是一个半诚实的实体，拥有充足的存储容量，能为DO提供存储空间。在数据共享过程中，接收DU属性私钥，判断是否满足访问策略。在审计过程中，在TEE中生成挑战随机值，在非TEE中生成证明并发送给TPA用于验证。

(4) TPA。TPA是一个诚实且好奇的实体，负责检测DO的医疗设备安全状态以及审计存储在MCS上数据的完整性，与部署TEE的MCS采用非交互式挑战-应答机制进行数据审计，并且该审计过程具有安全性。

(5) DO。DO是拥有大量医疗数据且上传到MCS上的患者，通过可穿戴设备与植入式设备等医疗设备收集数据。DO负责制定访问策略，计算密文及PMAC并上传到MCS。

(6) DU。DU是向MCS请求加密数据的主体，只有DU的属性满足密文中预设的访问策略时，DU才可通过密钥解密获取数据。由于DU的完整密钥由KGC和AA生成，只有当DU密钥完全正确时，才能获得解密数据。

本文方案系统参数如表2所示。

表 2	系统参数
参数	含义
PP	公共参数
$SK_{DU} = (SK_{KGC}, SK_{AA})$	DU密钥=(辅助密钥, 属性私钥)
MSK_{KGC}, MSK_{AA}	KGC私钥, AA私钥
PK_{KGC}, PK_{AA}	KGC公钥, AA公钥
pk, sk	Paillier公钥, Paillier私钥
(M, ρ)	访问策略
PMAC	隐私保护消息认证码

2.2 安全模型

(1) 密文信息的不可区分性

游戏1：本文方案的密文信息具有选择明文攻击下的不可区分性(indistinguishability under chosen-plaintext attack, IND-CPA)，选择明文攻击游戏参与方包括挑战者C和敌手A。游戏流程如下。

初始阶段。敌手A选择欲挑战的访问策略 (M^*, ρ^*) 发送给挑战者C。

系统建立。挑战者C执行系统初始化算法，输入安全参数和属性空间，生成公共参数PP、公私钥，将PP、KGC公钥 PK_{KGC} 和AA公钥 PK_{AA} 发送

给敌手A。

查询1 敌手A向挑战者C请求属性集合S的密钥，如果S满足 (M^*, ρ^*) 则终止，否则挑战者C运行模拟安全两方计算生成S对应的密钥发送给敌手A，此过程可以重复多项式有界次。

挑战。敌手A发送两个等长的消息 m_0, m_1 给挑战者C，C随机选取 $c \leftarrow_R \{0, 1\}$ ，并且使用挑战访问策略 (M^*, ρ^*) 对 m_c 进行加密，然后将挑战密文 CT^* 发送给敌手A。

查询2 重复查询1，敌手A再度向挑战者C发送属性集合S申请密钥，但规定S不能满足 (M^*, ρ^*) 。

猜测。敌手A输出对c的猜想 c' ，若 $c' = c$ ，则敌手A成功。

定义1 若多项式时间敌手赢得以上安全模型游戏的优势 $\varepsilon = \left| \Pr[c' = c] - \frac{1}{2} \right|$ 为可忽略的，则本文方案是IND-CPA安全的。

(2) 授权中心腐化下抗用户合谋攻击的安全性

游戏2：安全模型由敌手A和挑战者C之间的挑战游戏定义，具体游戏如下。

系统建立。挑战者C运行系统初始化算法，获取公共参数和公私钥，并将PP、 PK_{KGC} 和 PK_{AA} 发送给敌手A，PP中包含Paillier公钥pk，挑战者C保存 MSK_{KGC}, MSK_{AA} 。

查询1 敌手A可以适应性地进行以下3种查询。

① 用户密钥查询 $Q_{KeyGen}(ID, S)$ ：输入DU的ID和属性集合S，调用KGC与AA之间的真实安全两方计算协议输出DU辅助密钥 SK_{KGC} ，并由AA生成属性私钥 SK_{AA} ，将 $SK_{DU} = (SK_{KGC}, SK_{AA})$ 发送给敌手A。

② 授权中心腐化查询 $Q_{corrupt}(auth)$ ：输入授权中心标识 $auth \in (KGC, AA)$ ，若腐化KGC，则敌手A获得 MSK_{KGC} 以及其持有的安全两方计算的私有信息；若腐化AA，则敌手A获得 MSK_{AA} 及安全两方计算的本地输入。该查询需要满足敌手A最多只能腐化一个授权中心。

③ 用户合谋查询 $Q_{collude}(ID_1, \dots, ID_k)$ ：输入多个DU的ID，输出这些DU密钥集合。

挑战。敌手A向挑战者C发送两个等长的消息 m_0, m_1 和欲挑战的访问策略 (M^*, ρ^*) 。C随机选取 $c \leftarrow_R \{0, 1\}$ ，并且使用 (M^*, ρ^*) 对 m_c 进行加密，然

后将挑战密文 CT^* 发送给敌手A。

挑战者C必须满足如下约束条件:若敌手A已腐化KGC或AA,则其在游戏中所有已查询过的属性集合 S 均不能满足 (M^*, ρ^*) ,即无法解密挑战密文;若敌手A未腐化任何授权中心,则对于敌手A通过合谋查询获得的任意用户群,这些用户的属性集合并不满足 (M^*, ρ^*) ,即无法通过合并多个用户的密钥来解密挑战密文。如果上述任何约束不满足,则C终止游戏并宣布敌手A失败。

查询2 敌手A可以适应性地进行与查询1相同的查询,并且需要满足挑战阶段的约束。

猜测。与游戏1的该阶段相同。

定义2 若多项式时间敌手赢得以上安全模型游戏的优势 $\varepsilon = \left| \Pr[c' = c] - \frac{1}{2} \right|$ 为可忽略的,则本文方案是授权中心腐化下抗用户合谋攻击的。

此外,本文在标准TEE信任假设下分析所提方案安全性。进一步,若放宽标准TEE信任假设,攻击者针对TEE发起侧信道等实现层攻击,本文方案不再假设TEE内部挑战生成状态绝对安全,因此对挑战不可预测性和抗操纵性相关的安全性作退化分析,相关讨论参考第3.3节。

2.3 算法描述

算法由系统初始化、密钥生成、数据加密、数据解密及数据审计5个部分组成,具体如下。方案时序图如图2所示。

(1) $\text{Setup}(\lambda) \rightarrow (\text{PP}, \text{PK}, \text{MSK})$ 。该算法由KGC和AA执行。系统初始化算法通过输入安全参数 λ ,输出系统公共参数PP、系统公钥 $\text{PK} = (\text{PK}_{\text{KGC}}, \text{PK}_{\text{AA}})$ 和系统主密钥 $\text{MSK} = (\text{MSK}_{\text{KGC}}, \text{MSK}_{\text{AA}})$ 。

给定安全参数 λ ,KGC生成双线性映射 $e: G_1 \times G_1 \rightarrow G_2$,其中 G_1 和 G_2 是具有相同素数阶 p ($|p| \geq \lambda$)的两个循环乘法群,设 g 为 G_1 的生成元。随机选择参数 $x \in Z_p^*$,KGC公钥 $\text{PK}_{\text{KGC}} = e(g, g)^x$,KGC私钥 $\text{MSK}_{\text{KGC}} = x$ 。选择抗碰撞哈希函数 $h_1: \{0,1\}^* \rightarrow Z_p^*$ 、 $H_1: \{0,1\}^* \rightarrow G_1$ 和同态哈希函数 $\text{HHF}(\cdot): \{0,1\}^* \rightarrow Z_p^*$ 。KGC为安全两方计算生成Paillier公私钥 $(\text{pk}, \text{sk}) = \text{KeyGen}_{\text{Paillier}}(1^\lambda)$,计算 $C_x = \text{Enc}_{\text{pk}}(x)$ 。其中,Paillier公钥模数为 N ,且满足 $p < N$ 。系统公共参数PP为:

$$\text{PP} = \{e, G_1, G_2, g, p, h_1, H_1, \text{HHF}(\cdot), e(g, g)^x, \text{pk}\} \quad (6)$$

AA随机选择参数 $\gamma, \mu \in Z_p^*$,计算AA公钥 $\text{PK}_{\text{AA}} = (g^\gamma, g^\mu)$ 和AA私钥 $\text{MSK}_{\text{AA}} = (\gamma, \mu)$,其中 MSK_{AA} 保密, PK_{AA} 公开。

(2) $\text{KeyGen}(\text{MSK}, S, c_i) \rightarrow (\text{SK}_{\text{DU}}, \psi_i)$ 。密钥生成算法包括DU密钥生成算法 $\text{KeyGen}_{\text{DU}}(\text{MSK}, S) \rightarrow \text{SK}_{\text{DU}}$ 和审计密钥生成算法 $\text{KeyGen}_{\text{TPA}}(c_i) \rightarrow (\psi_i)$ 。

算法1 $\text{KeyGen}_{\text{DU}}(\text{MSK}, S) \rightarrow \text{SK}_{\text{DU}}$ 。DU密钥采用Paillier同态加密的安全两方计算并由KGC和AA交互执行。该算法通过输入DU的属性集合 S 和系统主密钥 MSK 生成DU的辅助密钥 SK_{KGC} 和属性私钥 SK_{AA} 。

① DU向KGC发送身份ID进行注册,DU向AA发送ID和属性集合 S 申请属性私钥。

② AA为用户生成唯一随机数 $t \in Z_p^*$,计算 $\theta = \gamma t \pmod{p}$, $a = \mu^{-1} \pmod{p}$ 。AA选择随机盲化值 $b \in Z_p$,计算 $Q = g^{-b}$,利用Paillier的加法同态性质计算 $C_Y = (C_x)^a \text{Enc}_{\text{pk}}(a\theta + b)$,将 (Q, C_Y) 发送给KGC。

③ KGC使用Paillier私钥 sk 解密得到 $Y = \text{Dec}_{\text{sk}}(C_Y)$,随后计算辅助密钥 SK_{KGC} 如式(7)所示,并将 SK_{KGC} 发送给DU。

$$\text{SK}_{\text{KGC}} = g^Y Q = g^{\frac{x + \gamma t}{\mu}} \quad (7)$$

④ AA计算属性私钥 SK_{AA} 如式(8)所示,并将 SK_{AA} 发送给DU,即DU密钥 $\text{SK}_{\text{DU}} = (\text{SK}_{\text{KGC}}, \text{SK}_{\text{AA}})$ 。

$$\text{SK}_{\text{AA}} = \{L = g^t, \forall d \in S: k_d = H_1(d)^t (g^\mu)^t\} \quad (8)$$

算法2 $\text{KeyGen}_{\text{TPA}}(c_i) \rightarrow (\psi_i)$ 。审计密钥生成算法由TPA和DO交互执行。该算法通过输入TPA稳定的内存地址 c_i ,使用PUF计算DO的设备指纹 R_i ,TPA使用 R_i 计算审计密钥 ψ_i 。

① TPA使用模糊提取算法选择稳定的SRAM内存单元 c_i ,将 c_i 通过安全信道发送给DO。

② DO接收之后,使用PUF生成唯一的设备指纹 $R_i = \text{PUF}(c_i)$,并将 R_i 通过安全信道发送给TPA,之后销毁 R_i 。

③ TPA接收之后,使用模糊提取器的生成函数 $\text{FE.Gen}(\cdot)$ 生成临时密钥 β_i 和 β_i 的辅助信息 hd 。

④ TPA将辅助信息 hd 通过安全信道发送给DO,DO存储 $\{c_i, \text{hd}\}$ 。

⑤ TPA对 β_i 哈希得到 $\phi_i = h_1(\beta_i)$,再计算 $\psi_i = g^{\phi_i}$,之后TPA存储 ψ_i 。

(3) $\text{Enc}((\mathbf{M}, \rho), F) \rightarrow \text{CT}$ 。数据加密算法由 DO 执行, 其包含离线加密算法 $\text{OfflineEnc}((\mathbf{M}, \rho)) \rightarrow \text{IC}$ 和在线加密算法 $\text{OnlineEnc}(\text{IC}, F) \rightarrow \text{CT}$ 。离线加密算法在 DO 佩戴的医疗智能设备充电或未使用时执行, 设备使用时执行在线数据加密算法。

算法 3 $\text{OfflineEnc}((\mathbf{M}, \rho)) \rightarrow \text{IC}$ 。该算法通过输入访问策略 $(\mathbf{M}, \rho)$ 输出中间密文 IC。

① DO 定义一个 LSSS 类型的访问策略 $A = (\mathbf{M}, \rho)$, $\mathbf{M}$ 是一个 $l \times n$ 的访问矩阵, ρ 是一个映射函数, 将 $\mathbf{M}$ 的一行 $\mathbf{M}_i$ 映射到属性。

② DO 选取随机向量 $\mathbf{y} = (s, \delta_2, \delta_3, \dots, \delta_n) \in Z_p^n$, 其中 s 为秘密共享值, 其他的元素为隐藏 s 的随机值。计算秘密的分享份额 $\lambda_i = \mathbf{M}_i \mathbf{y} (i = 1, 2, \dots, l)$ 。

③ 对 $\mathbf{M}$ 的每行选取随机数 $r_i = (r_1, r_2, \dots, r_l)$ 。医疗智能设备计算 $D_i = g^{\lambda_i} g^{-\mu_i} H_1(\rho(i))^{-r_i}$, $D'_i = g^{r_i}$, 并返回中间密文 $\text{IC} = \{D_i, D'_i\}_{i=1}^l$ 。

算法 4 $\text{OnlineEnc}(\text{IC}, F) \rightarrow \text{CT}$ 。该算法通过输入中间密文 IC 与明文 F 生成密文 CT。DO 的在线加密算法包括生成密文和 PMAC。

① 生成加密密钥。DO 使用 PUF 对保存的稳定内存地址 c_i 生成设备指纹 $R_i^* = \text{PUF}(c_i)$, 使用模糊提取器重构密钥 $\beta = \text{FE.Rec}(R_i^*, \text{hd})$, β 的哈希值 $\varphi = h_1(\beta)$ 。

② DO 计算 $C' = g^{\mu s}$, 对明文 F 进行加密得到 C , 如式(10)所示。为支持 TPA 对数据随机抽样审计以及本文方案设计的 PMAC, 将 C 分为 m 个等长的文件块, 如式(11)所示。每个文件块 C_i 中包含 n 个数据块 $(C_{i,0}, C_{i,1}, \dots, C_{i,n-1})$, C_i 表示第 i 个文件块, 利用伪随机函数 $\text{PRF}(\cdot)$ 生成文件块中每个数据块的偏移系数 α_j , 如式(12)所示。

$$\text{IC} = \{D_i = g^{\lambda_i} g^{-\mu_i} H_1(\rho(i))^{-r_i}, D'_i = g^{r_i}\}_{i=1}^l \quad (9)$$

$$C = \text{Fe}(g, g)^{xs} \quad (10)$$

$$C = \{C_1, C_2, \dots, C_m\} \quad (11)$$

$$\alpha_j = \text{PRF}(\varphi, j) \quad (12)$$

③ 生成 C 的 PMAC。使用经 PUF 处理的加密密钥 φ 生成 C_i 多项式承诺 $P_{C_i}(\varphi)$, 如式(13)所示。选取当前时间 t_i , 将 X_i 与 t_i 作为同态哈希的输入, 如式(14)所示。输出 PMAC_i , 并且生成 PMAC_i 的哈希 hc_i , 如式(15)所示。

$$P_{C_i}(\varphi) = X_i = ((C_{i,0} + \alpha_0) + (C_{i,1} + \alpha_1)\varphi + (C_{i,2} + \alpha_2)\varphi^2 + \dots + (C_{i,n-1} + \alpha_{n-1})\varphi^{n-1}) \pmod{p} \quad (13)$$

$$\text{PMAC}_i = g^{t_i + X_i} \quad (14)$$

$$\text{hc}_i \leftarrow h_1(\text{PMAC}_i) \quad (15)$$

④ 对所有的 $\{\text{hc}_i\}$ 使用默克尔哈希树生成根哈希 hr , DO 将 hr 通过安全信道发送给 TPA。

⑤ DO 将 CT 发送给 MCS, 如式(16)所示。

$$\text{CT} = (C, C', \{D_i, D'_i\}_{i=1}^l, \{t_i, \text{PMAC}_i\}_{i=1}^m, (\mathbf{M}, \rho)) \quad (16)$$

(4) $\text{Decrypt}(\text{CT}) \rightarrow F$ 。数据解密算法包括外包解密算法 $\text{OutsourcedDec}(S, \text{SK}_{\text{AA}}) \rightarrow \text{TCT}$ 和 DU 解密算法 $\text{UserDec}(C, \text{TCT}, \text{SK}_{\text{KGC}}) \rightarrow F$ 。

算法 5 $\text{OutsourcedDec}(S, \text{SK}_{\text{AA}}) \rightarrow \text{TCT}$ 。外包解密算法由 MCS 执行。该算法输入 DU 属性集合和 DU 属性私钥 SK_{AA} , 若满足访问策略, 则输出 TCT。

① MCS 根据 DU 的 SK_{AA} 判断 DU 属性集合与请求密文的访问策略是否匹配。若不匹配, 则拒绝请求; 否则, 选择集合 $I = \{i; \rho(i) \in S\} \subseteq \{1, 2, \dots, l\}$ 。

② MCS 根据 LSSS 协议, 若能在多项式时间内找出一个常数集 $\{w_i \in Z_p^*\}_{i \in I}$, 使 $\sum_{i \in I} w_i \lambda_i = s$ 。

③ MCS 计算转换密文 TCT 如式(17)所示, 并将密文 C 和 TCT 发送给 DU。

$$\text{TCT} = \prod_{i \in I} (e(D_i, L) e(D'_i, k_{\rho(i)}))^{w_i} = e(g, g)^{\mu s} \quad (17)$$

算法 6 $\text{UserDec}(C, \text{TCT}, \text{SK}_{\text{KGC}}) \rightarrow F$ 。DU 解密算法由 DU 执行。该算法通过输入密文 C 、转换密文 TCT 和 DU 辅助密钥 SK_{KGC} , 输出明文 F' 为:

$$F' = \frac{C}{e(C', \text{SK}_{\text{KGC}})} \text{TCT} \quad (18)$$

(5) $\text{DataVerify}(\text{PMAC}_i, \text{cp}) \rightarrow \text{RST}$ 。数据审计包括证明生成算法 $\text{ProofGen}(\text{cp}) \rightarrow \text{Prf}$ 和证明验证算法 $\text{ProofVer}(\text{Prf}) \rightarrow \text{RST}$ 。数据审计采用非交互式挑战-应答机制进行数据完整性审计。当审计开始时, MCS 在受硬件保护的 TEE 中生成随机数集合 cp , 该集合作为挑战生成的随机性根, 通过安全信道同步至 TPA。随后 MCS 在非 TEE 中根据 cp 计算挑战和证明, 将证明发送给 TPA, TPA 首先对根哈希 hr' 进行判断, 之后对被挑战块进行完整性

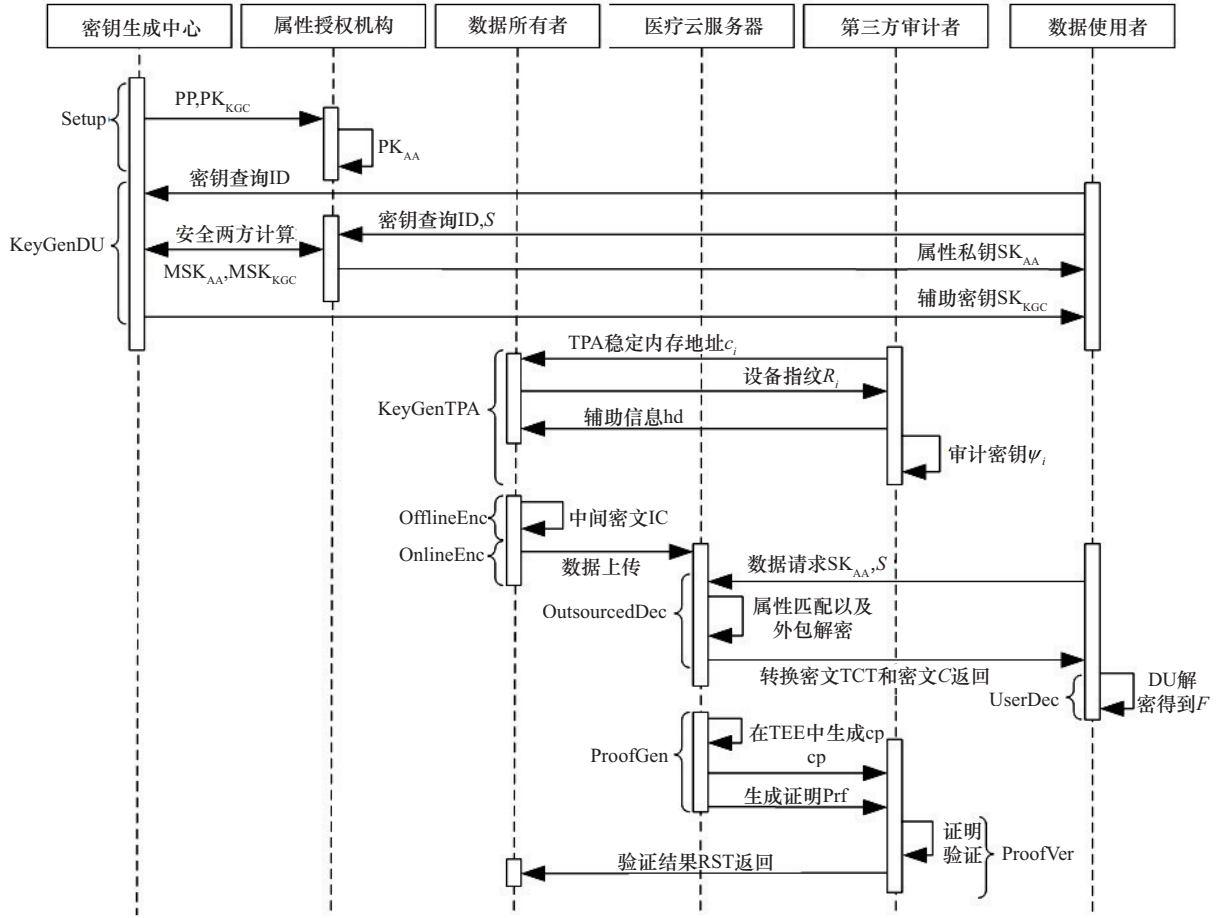


图2 方案时序

验证。TEE 仅生成审计挑战的随机性根，实现硬件可信根与业务逻辑的解耦，降低侧信道等攻击带来的安全风险。

算法7 $\text{ProofGen}(\text{cp}) \rightarrow \text{Prf}$ 。证明生成算法由MCS执行。该算法通过输入随机数集cp对抽样的密文数据块生成证明Prf。

① MCS在TEE中生成密钥 c_1, c_2 ，以及被挑战文件块的数目 c ，通过安全信道将 $\text{cp} = \{c_1, c_2, c\}$ 发送给TPA。

②将MCS的TEE生成的 $\text{cp} = \{c_1, c_2, c\}$ 发送给MCS的非TEE。使用伪随机置换函数 $\text{id} \leftarrow \pi_{c_1}(l)$ 生成被挑战块的位置标识符id，使用伪随机函数 $a_{\text{id}} \leftarrow f_{c_1}(l)$ 生成id对应被挑战块的证明系数，生成挑战 $G = \{(\text{id}, a_{\text{id}})\}$ 。使用 $z \leftarrow f_{c_2}(c+1)$ 生成多项式承诺的随机值，用于多项式评估。

③聚合证明 $P_{\text{Prf}}(q)$ 如式(19)所示，商多项式 $Z_{\text{Prf}}(q)$ 如式(20)所示。

$$P_{\text{Prf}}(q) = \sum_{i \in G} a_i C_{i,0} + \sum_{i \in G} a_i C_{i,1} q + \sum_{i \in G} a_i C_{i,2} q^2 + \dots + \sum_{i \in G} a_i C_{i,n-1} q^{n-1} \quad (19)$$

$$Z_{\text{Prf}}(q) = \frac{P_{\text{Prf}}(q) - P_{\text{Prf}}(z)}{q - z} \quad (20)$$

④对 $\{\text{PMAC}_i\}$ 中的每一项进行哈希 $\text{hc}_i^* \leftarrow h_1(\text{PMAC}_i)$ 得到 $\{\text{hc}_i^*\}$ 。

⑤MCS将Prf发送给TPA，如式(21)所示。

$$\text{Prf} = \{ \{ \text{PMAC}_i, \text{hc}_i^*, t_i \}_{i=1}^m, Z_{\text{Prf}}(q), P_{\text{Prf}}(z) \} \quad (21)$$

算法8 $\text{ProofVer}(\text{Prf}) \rightarrow \text{RST}$ 。证明验证算法由TPA执行。该算法通过输入证明Prf计算出审计结果RST。

①TPA收到cp后，与MCS执行相同方法生成挑战 $G = \{(\text{id}, a_{\text{id}})\}$ 和多项式承诺随机值 z 。

②在接收到Prf后，使用默克尔哈希树计算 $\{\text{hc}_i^*\}$ 得出根哈希 hr' ，若 $\text{hr} \neq \text{hr}'$ ，则向DU发送 $\text{RST} = \perp$ ，并且运算终止，否则执行后续步骤。

③重新构建偏移量 $\alpha_j = \text{PRF}(\phi, j)$ ，计算偏移补

偿项 $P_\alpha(\varphi)$, 如式(22)所示, 再计算式(23)~式(25)。

$$P_\alpha(\varphi) = \sum_{j=0}^{n-1} \alpha_j \varphi^j \quad (22)$$

$$H_z^{\varphi-z} = \text{HHF}(Z_{\text{Prf}}(\varphi))^{\varphi-z} \quad (23)$$

$$P'_{\text{Prf}}(\varphi) = \left(P_{\text{Prf}}(z) + \left(\sum_{i \in G} a_i \right) P_\alpha(\varphi) \right) \bmod p \quad (24)$$

$$H_t = \text{HHF} \left(\sum_{i \in G} t_i a_i \right) \quad (25)$$

④对计算结果进行验证, 判断式(26)是否成立, 若成立, 则返回 $\text{RST} = 1$; 否则, 返回 $\text{RST} = \perp$ 。

$$\text{RST} = \prod_{i \in G} (\text{PMAC}_i)^{a_i} = H_z^{\varphi-z} \text{HHF}(P'_{\text{Prf}}(\varphi)) H_t \quad (26)$$

3 安全分析

3.1 正确性证明

外包解密计算得到转换密文 TCT 如式(27)所示, 并发给 DU。

$$\begin{aligned} \text{TCT} &= \prod_{i \in I} \left(e(D_i, L) e(D'_i, k_{\rho(i)}) \right)^{w_i} = \\ &e \left(\prod_{i \in I} \left(g^{\gamma \lambda_i} g^{-\mu r_i} H_1(\rho(i))^{-r_i} g^t \right)^{w_i} \right) = \\ &e \left(\prod_{i \in I} \left(g^{r_i} H_1(\rho(i))^t (g^\mu)^t \right)^{w_i} \right) = \\ &\prod_{i \in I} \left(e(g^{\gamma \lambda_i w_i} g^{-\mu r_i w_i} H_1(\rho(i))^{-r_i w_i} g^t) \right. \\ &e(g^{r_i w_i} H_1(\rho(i))^t (g^\mu)^t) \Big) = \\ &\prod_{i \in I} \left(e(g^{\gamma \lambda_i w_i} g^t) e(g^{-\mu r_i w_i} g^t) e(H_1(\rho(i))^{-r_i w_i} g^t) \right. \\ &e(g^{r_i w_i} H_1(\rho(i))^t) e(g^{r_i w_i} (g^\mu)^t) \Big) = \\ &\prod_{i \in I} \left(e(g^{\gamma \lambda_i w_i} g^t) \right) = \\ &e(g, g)^{\gamma t \sum_{i \in I} w_i \lambda_i} = e(g, g)^{\gamma t s} \end{aligned} \quad (27)$$

之后, DU 使用 SK_{KGC} 解密得到数据, 如式(28)所示。

$$\begin{aligned} F' &= \frac{C}{e(C', \text{SK}_{\text{KGC}})} \text{TCT} = \\ &\frac{Fe(g, g)^{xs}}{e(g, g)^{\frac{x + \gamma t}{\mu}}} e(g, g)^{\gamma t s} = \\ &e(g^{\mu s}, g^{-\frac{x + \gamma t}{\mu}}) \\ &\frac{Fe(g, g)^{xs} e(g, g)^{\gamma t s}}{e(g, g)^{xs + \gamma t s}} = F \end{aligned} \quad (28)$$

因此, 本文方案的授权用户解密是正确的。

3.2 完整性证明

$R = L$, 即式(29)等于式(30)。因此, 本文方案具有数据完整性审计。

$$\begin{aligned} R &= H_z^{\varphi-z} \text{HHF}(P'_{\text{Prf}}(\varphi)) H_t = \\ &\text{HHF}(Z_{\text{Prf}}(\varphi))^{\varphi-z} \text{HHF}(P'_{\text{Prf}}(\varphi)) H_t = \\ &g^{P_{\text{Prf}}(\varphi) - P_{\text{Prf}}(z)} g^{P_{\text{Prf}}(z) + \left(\sum_{i \in G} a_i \right) P_\alpha(\varphi)} g^{\sum_{i \in G} a_i t_i} = \\ &g^{P_{\text{Prf}}(\varphi) + \left(\sum_{i \in G} a_i \right) P_\alpha(\varphi)} g^{\sum_{i \in G} a_i t_i} = \\ &g^{\sum_{i \in G} a_i P_{C_i}(\varphi) + \sum_{i \in G} a_i t_i} \end{aligned} \quad (29)$$

$$\begin{aligned} L &= \prod_{i \in G} (\text{PMAC}_i)^{a_i} = \prod_{i \in G} (g^{P_{C_i}(\varphi) + t_i})^{a_i} = \\ &g^{\sum_{i \in G} a_i P_{C_i}(\varphi) + \sum_{i \in G} a_i t_i} \end{aligned} \quad (30)$$

3.3 安全性证明

(1) 授权中心腐化下抗用户合谋攻击的 IND-CPA 安全性

定理 1 若用于 DU 密钥生成的基于 Paillier 同态加密的安全两方计算协议在半诚实模型下是安全的, q -DHE 假设在群 G_1 中成立, 则本文方案在单授权中心腐化下抗用户合谋攻击满足 IND-CPA。

抗合谋攻击下的安全性证明采用游戏序列, 构造一系列不可区分的游戏: $\text{Game}_0, \text{Game}_1, \text{Game}_2$, 通过混合论证证明完全安全性。其中, Game_0 与定义 2 的安全模型完全一致, 挑战者执行真实的基于 Paillier 同态加密的安全两方计算协议生成 SK_{KGC} , Game_1 用安全两方计算的理想功能替代真实协议, Game_2 是挑战密文与随机元素不可区分。 Game_1 和 Game_2 的定义如下。

Game₁: Game_1 与 Game_0 的区别在于用户密钥查询 $Q_{\text{KeyGen}}(\text{ID}, S)$, Game_1 不模拟 KGC 与 AA 之间真实的基于 Paillier 同态加密的安全两方计算, 而是调用理想功能 $F_{2\text{PC}}$ 直接生成 $\text{SK}_{\text{KGC}} = g^{\frac{x + \gamma t}{\mu}}$ 和 $\text{SK}_{\text{AA}} = \{L = g^t, \forall d \in S: k_d = H_1(d)^t (g^\mu)^t\}$, 之后挑战者 C 继续执行后续步骤, 其他步骤与 Game_0 相同。

Game₂: Game_2 与 Game_1 的区别在于挑战密文的生成, Game_2 挑战密文中的分量被替换为随机分量 $C = R$ 。

证明需要以下两个引理, 最终证明定理 1。以下是对引理的正式描述及证明。

引理 1 若用于 DU 密钥生成的基于 Paillier 同

态加密的安全两方计算协议在半诚实模型下是安全的, 则 Game_0 与 Game_1 在计算上不可区分, 即存在可忽略函数 $\text{negl}(\lambda)$, 使 $|\text{Adv}_0 - \text{Adv}_1| \leq \text{negl}(\lambda)$ 。

证明 假设敌手 A 以不可忽略的优势区分 Game_0 和 Game_1 , 通过构造模拟器 B 来攻破基于 Paillier 同态加密的安全两方计算协议。模拟器 B 接收一个安全两方计算协议的挑战, 该挑战来自真实协议 $\text{Real}_{2\text{PC}}$ 或理想功能 $\text{Ideal}_{2\text{PC}}$, 模拟器 B 需要判断接收的是哪种挑战。模拟器 B 模拟 Game_0 或 Game_1 给敌手 A。

初始化。模拟器 B 生成公共参数 $\text{PP} = \{e, G_1, G_2, g, p, h_1, H_1, \text{HHF}(\cdot), e(g, g)^x, \text{pk}\}$, AA 公钥 $\text{PK}_{\text{AA}} = (g^\gamma, g^\mu)$, 并将 $\text{PP}, \text{PK}_{\text{KGC}}, \text{PK}_{\text{AA}}$ 发送给敌手 A。

查询1 敌手 A 可以适应性地进行以下3种查询。

①用户密钥查询 $Q_{\text{KeyGen}}(\text{ID}, S)$: 当敌手 A 发起 $Q_{\text{KeyGen}}(\text{ID}, S)$, 模拟器 B 随机选取 $t \in Z_p^*$, 输入 (x, ID) 和 $(\gamma, \mu, t, \text{ID}, S)$, 提交给安全两方计算挑战接口。若挑战接口对应 $\text{Real}_{2\text{PC}}$, 则返回的密钥与 Game_0 中真实执行 Paillier 同态加密的安全两方计算协议所得结果一致; 若挑战接口对应 $\text{Ideal}_{2\text{PC}}$, 则返回 SK_{KGC} 和 SK_{AA} , 其分布与 Game_1 理想功能输出一致。随后模拟器 B 将 $\text{SK}_{\text{DU}} = (\text{SK}_{\text{KGC}}, \text{SK}_{\text{AA}})$ 返回给敌手 A。

②授权中心腐化查询 $Q_{\text{corrupt}}(\text{auth})$: 当敌手 A 发起 $Q_{\text{corrupt}}(\text{auth})$ 时, 模拟器 B 按照安全模型返回。

③用户合谋查询 $Q_{\text{collude}}(\text{ID}_1, \dots, \text{ID}_k)$: 当敌手 A 发起 $Q_{\text{collude}}(\text{ID}_1, \dots, \text{ID}_k)$ 时, 模拟器 B 返回对应 DU 密钥集合。

挑战。与游戏2该阶段相同, 生成挑战密文 CT^* , 并将 CT^* 返回给敌手 A。

猜测。敌手 A 输出对 c 的猜测, 若 $c' = c$, 则敌手 A 在该游戏中获胜。

若敌手 A 能以不可区分的优势区分 Game_0 和 Game_1 , 则模拟器 B 也能以不可区分的优势区分 $\text{Real}_{2\text{PC}}$ 和 $\text{Ideal}_{2\text{PC}}$, 从而破坏该安全两方计算协议在半诚实模型下的安全性, 这与协议的安全性假设矛盾, 故 $|\text{Adv}_0 - \text{Adv}_1| \leq \text{negl}(\lambda)$ 。证毕。

引理2 如果 q-DHE 假设成立, 则 Game_1 与 Game_2 在计算上不可区分, 即存在可忽略函数 $\text{negl}(\lambda)$, 使得 $|\text{Adv}_1 - \text{Adv}_2| \leq \text{negl}(\lambda)$ 。

证明 构造模拟器 B, 利用敌手 A 区分 Game_1 和 Game_2 的能力解决 q-DHE 问题。在定义的授权

中心腐化的安全模型中, 敌手最多腐化一个授权中心。为简化分析, 以下仅考虑敌手 A 腐化 AA 的情形。对于未腐化任何授权中心的情形, 其证明过程类似, 故在此省略。

初始化。模拟器 B 收到实例 (U, Z) , 设置 KGC 私钥 $x = \alpha^{q+1}$ 且模拟器 B 对 α 未知。B 生成公共参数 PP , $\text{PK}_{\text{AA}} = (g^\gamma, g^\mu)$, $\text{PK}_{\text{KGC}} = e(g, g)^x = e(g^{\alpha^q}, g^\alpha)$, 其中 g^{α^q} 和 g^α 从 U 中获取, 随机选择 $\gamma, \mu \in Z_p^*$, 将 PP 发送给敌手 A。

查询1 在授权中心腐化查询时, 限制敌手 A 只能腐化 AA, 若腐化 KGC 则终止。当发起 $Q_{\text{corrupt}}(\text{AA})$ 请求时, 返回 (γ, μ) 。当敌手 A 发起 $Q_{\text{KeyGen}}(\text{ID}, S)$ 请求时, 若 S 满足欲挑战的访问策略 (M^*, ρ^*) 则终止, 否则 B 随机选择 $t \in Z_p^*$, 生成 $\text{SK}_{\text{AA}} = \{L = g^t, \forall d \in S: k_d = H_1(d)^t (g^\mu)^t\}$ 。在生成 SK_{KGC} 时, 若 $Z = g^{\alpha^{q+1}}$ 则 $\text{SK}_{\text{KGC}} = g^{\frac{x+\gamma t}{\mu}}$, 若 Z 为随机数, 则 SK_{KGC} 为半功能密钥, 返回 $\text{SK}_{\text{DU}} = (\text{SK}_{\text{KGC}}, \text{SK}_{\text{AA}})$ 。

挑战。敌手 A 发送两个等长的消息 m_0, m_1 给挑战者 C, 挑战者 C 随机选取 $c \leftarrow_R \{0, 1\}$, 选取随机向量 $\mathbf{y} = (s, \delta_2, \delta_3, \dots, \delta_n) \in Z_p^n$, 计算 $\lambda_i = M_i \mathbf{y} (i = 1, 2, \dots, l)$, 计算 IC 如式(31)所示, $C' = g^{\mu s}$ 。若 $Z = g^{\alpha^{q+1}}$, 则 $C = Fe(g, g)^x$; 若 Z 随机, 则 C 随机 $C = R$, 并将 $\text{CT}^* = (C, C', \text{IC})$ 发送给敌手 A。

$$\text{IC} = \{D_i = g^{\lambda_i} g^{-\mu r_i} H_1(\rho(i))^{-r_i}, D'_i = g^{r_i}\}_{i=1}^l \quad (31)$$

查询2 敌手 A 可以适应性地进行与查询1相同的查询, 并且需要满足挑战阶段的约束。

猜测。敌手 A 输出对 c 的猜测。如果 $c' = c$, 则 B 输出 1 (猜测 $Z = g^{\alpha^{q+1}}$), 否则输出 0 (猜测 Z 随机)。

当 $Z = g^{\alpha^{q+1}}$ 时, 模拟器 B 模拟 Game_1 ; 当 Z 随机时, 模拟器 B 模拟 Game_2 。敌手 A 区分 Game_1 和 Game_2 的优势等于模拟器解决 q-DHE 问题的优势。由 q-DHE 假设, 该优势可忽略, 故 $|\text{Adv}_1 - \text{Adv}_2| \leq \text{negl}(\lambda)$ 。证毕。

在 Game_2 中, 挑战密文与消息无关, 故 $\text{Adv}_2 = 0$ 。

由引理1和引理2可得式(32), 故本文方案在授权中心腐化下抗用户合谋攻击是 IND-CPA 的。

$$\text{Adv}_0 = |\text{Adv}_0 - \text{Adv}_1 + \text{Adv}_1 - \text{Adv}_2 + \text{Adv}_2| \leq \text{negl}(\lambda) \quad (32)$$

定理1证毕。

(2) 数据审计隐私性

在数据完整性审计中, TPA 不需要知道所有数据, 便可对数据完整性进行审计。MCS 发送给 TPA 的审计证据包括 $\{ \{ \text{PMAC}_i, \text{hc}_i^*, t_i \}_{i=0}^m, Z_{\text{Prf}}(q), P_{\text{Prf}}(z) \}$, $\text{PMAC}_i = g^{P_{C_i}(\varphi) + t_i}$, 其中 $P_{C_i}(\varphi)$ 是包含隐藏偏移量 α_j 的多项式承诺在秘密值 φ 处的值, 由于 α_j 由 $\text{PRF}(\cdot)$ 生成, φ 由 PUF 生成, 从 PMAC_i 中恢复 $P_{C_i}(\varphi)$ 需解决离散对数问题, 在计算上不可行。在 TPA 收到的证明中, $Z_{\text{Prf}}(q)$ 是多项式商, TPA 只能评估它在 φ 处的值, 无法泄露具体多项式系数。 $P_{\text{Prf}}(z)$ 是被挑战文件块的随机线性组合在 z 处的值, TPA 无法再利用相同位置数据块信息构成线性方程组求解数据块信息, 从而实现云存储数据在 TPA 审计中的隐私保护。

(3) 概率审计可靠性

本文方案的审计算法基于概率模型, 可确保概率审计的可靠性。假设独立抽取 c 个文件块, 每个文件块包含 n 个数据块, 受损数据块为 b 个, 证明即使攻击者只损坏部分数据块 b 个, 验证者也能以高概率发现异常。使用超几何分布计算在单次抽查中至少发现一个受损块的概率 P , 如式(33)所示。

$$\begin{aligned} P &= 1 - \frac{\binom{mn-b}{n}}{\binom{mn}{n}} = \\ &= 1 - \frac{(mn-b)(mn-b-1)\cdots(mn-b-n+1)}{mn(mn-1)\cdots(mn-n+1)} = \\ &= 1 - \left(\frac{mn-b}{mn} \frac{mn-b-1}{mn-1} \cdots \frac{mn-b-n+1}{mn-n+1} \right) \geq \\ &= 1 - \left(\frac{mn-b}{mn} \right)^n = 1 - \left(1 - \frac{b}{mn} \right)^n = 1 - (1-\delta)^n \end{aligned} \quad (33)$$

其中, m 为文件块数, δ 为受损块的概率, 对 c 个文件块进行抽样至少一次发现受损的概率为 P_v , 代入单次下界, 得到 P_v 的下界, 如式(34)所示。

$$P_v \geq 1 - [(1-\delta)^n]^c = 1 - (1-\delta)^{nc} \quad (34)$$

因此, 当在 MCS 上存储的数据被减少或者被破坏时, TPA 不需要检测全部数据, 只需要检查部分数据块, 发现数据受损的概率也能无限高。

(4) 挑战抗篡改性

对于传统方案, TPA 向 MCS 发送挑战, 攻击者使用高级技术拦截甚至篡改传输的挑战, 使不诚

实的 MCS 在未被检测的情况下减少存储的数据量, 并可能通过验证过程欺骗 TPA。本文方案使用部署了 TEE 的 MCS 采用非交互式挑战-应答机制进行审计, 在标准 TEE 信任假设下, 由 TEE 生成随机数集 cp , 之后由 MCS 的非 TEE 与 TPA 根据 cp 生成挑战, cp 构成挑战生成的随机性, TPA 不需要向 MCS 发起挑战便可对存储在 MCS 上的数据进行完整性审计, 有效防范不诚实 MCS 对数据的损坏。若放宽标准 TEE 信任假设, 攻击者通过侧信道攻击、接口泄露攻击、状态回滚攻击等手段破坏 TEE, 则 cp 可能被泄露、预测或操纵, 进而使攻击者预知审计中的挑战。此时, 系统将发生局部安全性退化, 不诚实 MCS 可以通过定向保留部分数据块或针对性准备审计证明等方式, 降低本文方案对云端未完整保存数据行为的检测概率, 但其风险被严格限制在审计挑战的随机性范围内, 并不会直接导致本文方案全部安全属性同时失效。

本文方案采用安全机理相互解耦的防御架构, 确保了系统底层的鲁棒性。本文方案基于 CP-ABE 构造的细粒度访问控制与抗用户合谋安全性, 其数学基础建立在 q-DHE 假设及安全两方计算协议之上, 而非依赖 TEE 的机密保护。因此, TEE 状态的泄露无法赋予攻击者越权解密医疗密文的能力。本文方案的 PMAC 构造依赖于医疗设备 PUF 生成的唯一设备指纹。由于攻击者无法获取受硬件物理特性保护的加密密钥 φ , 即便其预知了审计挑战, 仍无法伪造出合法的 PMAC 和审计证据, 设备安全状态检测依然可靠。

(5) 医疗设备安全状态检测

在本文方案中, PUF 组件能够抵抗物理探测攻击和抗逆向工程攻击, 从而为医疗设备提供硬件级的设备指纹。当攻击者尝试物理探测或篡改设备时, PUF 独特的物理结构会被破坏, 导致其响应发生变化。系统通过监测 PUF 响应的异常, 能够识别设备是否处于非安全状态, 从而及时阻止对敏感医疗数据的非法访问或伪造, 实现对医疗设备物理安全状态的有效检测。

PUF 与满足 $(\omega, \lambda, \varepsilon)$ 的模糊提取器结合能抵抗环境干扰攻击。只要噪声版本 R^* 与原始 R 的汉明距离不超过 ω , 恢复算法就能以概率 1 正确输出原始密钥 β , 如式(35)所示。这确保了即使 PUF 响应因环境因素(如温度、湿度)出现轻微变化, 密钥也

能被可靠重建,从而实现了容错,确保密钥的稳定可用,进而保障基于该密钥的数据加密、完整性校验等安全机制持续有效。

$$\Pr [\beta = \text{FE.Rec}(R^*, \text{hd}) | (\beta, \text{hd}) \leftarrow \text{FE.Gen}(R), \text{HD}(R, R^*) \leq \omega] = 1 \quad (35)$$

在本文方案中,即使攻击者获得辅助数据hd,也无法恢复原始密钥 β 。若 R 的最小熵为 λ ,即 $H_\infty(R) \geq \lambda$,则 $\text{SD}((\beta, \text{hd}), (\beta^*, \text{hd})) \leq \varepsilon$,其中 SD 表示统计距离,即使攻击者获得hd,也无法区分真实 β 和均匀随机密钥 β^* 。

在方案初始化阶段,TPA需记录每个设备唯一审计密钥 $\psi_i = g^{\varphi_i}$, ψ_i 是每个医疗设备的审计密钥,用于数据审计时多项式对比。当医疗数据需上传到MCS时,DO使用PUF计算正确响应,通过模糊提取器恢复出正确的 β ,对 β 哈希得出 φ 参与计算PMAC,TPA使用 ψ_i 对MCS发送的审计证据进行审计,若审计通过则表明数据在生成和传输过程中未被篡改,且设备身份可信,从而间接保障了医疗数据的机密性、完整性和可用性。

3.4 安全性对比

各方案的功能对比结果如表1所示。在安全性方面,本文方案为选择性安全,除文献[15]之外,其他方案均为选择性安全。在抗用户合谋方面,除文献[12]和文献[15]外,其余文献均能抵抗用户之间的合谋攻击。为了降低计算开销,文献[8]使用在线/离线加密。进一步,文献[6-9]使用外包解密。本文通过在线/离线加密和外包解密大幅降低了计算开销。在数据完整性审计方面,文献[7-8,15]不支持数据完整性审计。本文与文献[6]和文献[11]采用概率审计模型实现具有隐私保护的数据完整性审计,而文献[3]对访问策略进行了审计。在挑战抗篡改方面,本文方案采用非交互式挑战-应答机制实现挑战抗篡改攻击,文献[3,6,11]采用交互式挑战-应答实现挑战抗篡改攻击。除此之外,本文方案还采用嵌入医疗设备指纹的PMAC检测医疗设备的物理安全状态。具体来说,文献[3]是基于区块链的可验证属性基加密方案,文献[6]是基于属性基加密的云审计方案,文献[11]是基于混合加密的支持审计的数据共享方案。本文与文献[3]和文献[6]采用CP-ABE进行加密,而文献[11]采用对称加密与CP-ABE混合加密,实现数据机密性与细粒度访问控制。

4 开销分析

本节将本文方案与文献[3]、文献[6]和文献[11]进行通信和计算开销对比。本文仿真实验环境为:AppleM4芯片(10核CPU+10核GPU)处理器,16GB内存,512GB SSD硬盘,macOS Sequoia操作系统,基于Python实现采用中国剩余定理优化的Paillier同态加密算法进行安全两方计算,利用gmpy2库对大整数运算并加速,并调用JPBC-2.0.0密码库中Type-A类椭圆曲线构造质数对称双线性群。在本文方案中,TEE的主要作用是在标准TEE信任假设下生成随机数集cp。本文实验的重点是评估密码运算与协议阶段的通信与计算开销,因此,实验将TEE抽象为可信执行模块进行功能仿真,而未在特定TEE平台上模拟Enclave初始化与安全世界切换等系统级开销。文献[12]使用与本文类似的TEE结构,在基于CP-ABE的医疗数据安全场景下,尽管TEE会引入指令级保护和安全世界切换的开销,但系统的主要性能瓶颈仍集中于密码学协议与大规模的数学运算,TEE带来的系统级时延通常为亚毫秒级。TEE产生的开销明显小于本文分析的双线性运算和同态加密运算的毫秒级开销,可以忽略。抽象处理能够更准确地反映协议在算法逻辑上的效率优化,同时避免特定硬件平台实现差异对实验结果造成干扰。对方案涉及的各阶段运算进行仿真,对比分析各方案开销,所用符号及含义如表3所示。

表3 符号含义

符号	含义
$ G_1 / G_2 / Z_p^* $	群 $G_1/G_2/Z_p^*$ 的阶数
l	属性数量
m, n	文件块的个数、文件块中的数据块
c	挑战过程中被挑战的块数
w	关键字的个数
z	访问控制树子节点数
H	群 G_1 上一次哈希运算
$E_{G_1}/E_{G_2}/E_{Z_p^*}$	群 $G_1/G_2/Z_p^*$ 上一次指数运算
h/HHF	群 Z_p^* 上一次哈希/同态哈希运算
$M_{G_1}/M_{G_2}/M_{Z_p^*}$	群 $G_1/G_2/Z_p^*$ 上一次乘法运算
P_{G_2}	群 G_2 上一次双线性运算
$\text{PL}_{\text{Enc}}/\text{PL}_{\text{Dec}}/\text{PL}_M/\text{PL}_E$	一次Paillier解密/加密/乘法/指数运算
—	不涉及

4.1 通信开销

在通信开销运算中, 利用 Type-A 类椭圆曲线 $y^2 = x^3 + x$ 构造质数对称双线性群, $|G_1| = |G_2| = 512$, $|Z_p^*| = 160$, $|h| = 256$ 。各方案的 DU 密钥、密文数据、审计密钥、审计阶段挑战数据和审计阶段响应数据的理论通信开销如表 4 所示。

如图 3(a)所示, 本文方案 DU 密钥由 KGC 与 AA 通过安全两方计算生成, 当属性数量从 0 增加到 20 个时, DU 密钥通信开销比文献[3]和文献[11]低 46%。如图 3(b)所示, 文件被分为 $m = 10$ 块, 关键字 $w = 20$ 个, 本文方案在属性数量从 0 增加到 20 个时, 密文数据的通信开销低于文献[6]和文献[11], 在属性数量大于 20 时, 本文方案的通信开销最低。如图 3(c)所示, 本文方案审计密钥的通信开销明显低于文献[3]和文献[11]。表 4 表明, 本文方案采用非交互式挑战-应答, 审计阶段的挑战数据没有通信开销, 审计阶段的响应数据中包含所有文件块的 PMAC, 需要对所有 PMAC 进行默克尔哈希运算, 判断所有文件块的数据完整性。因此, 审计阶段响应数据的通信开销高于文献[6]和文献[11]。

4.2 计算开销

对每种运算进行 2 000 次运算, 取平均值作为单次运算时间。计算结果表明, 在 G_1 上进行一次指数运算 E_{G_1} 、一次乘法运算 M_{G_1} 和一次哈希运算 H 的时间分别为 4.640 5 ms、0.026 ms 和 0.002 ms, 在 G_2 上进行一次指数运算 E_{G_2} 、一次乘法运算 M_{G_2} 和一次双线性运算 P_{G_2} 的时间分别为 4.617 1 ms、0.022 1 ms 和 4.320 5 ms。在 Z_p^* 上进行一次指数运算 $E_{Z_p^*}$ 、一次哈希运算 h 和一次同态哈希运算 HHF 的时间分别为 0.019 9 ms、0.001 8 ms 和 4.614 3 ms, 由于在 Z_p^* 上进行一次乘法运算的时间为 0.000 6 ms, 在计算开销时可忽略不计。当 Paillier 的公钥模数 N 的比特长度为 2 048 bit 时, 一次 Paillier 加密运算 PL_{Enc} 、一次 Paillier 解密运算 PL_{Dec} 和一次 Paillier 指数运算 PL_E 的平均时间分别为 2.056 5 ms、1.182 4 ms 和 2.074 6 ms, 由于一次 Paillier 乘法运算 PL_M 的平均时间为 0.000 1 ms, 在计算开销时可忽略不计。各方案的理论计算开销对比如表 5 所示, 其中加密数据开销包含数据签名的运算。

DU 密钥计算开销对比如图 4(a)所示, 本文

表 4

理论通信开销对比

对比项	文献[3]	文献[6]	文献[11]	本文方案
DU 密钥	$(1 + 2l) G_1 $	$(2 + l) G_1 + 2 Z_p^* $	$(1 + 2l) G_1 $	$(2 + l) G_1 $
密文数据	$(3 + 3l) G_1 + G_2 $	$(2l + 2) G_1 + G_2 + m G_1 $	$(1 + 2l) G_1 + G_2 + Z_p^* + w G_1 $	$(1 + 2l) G_1 + G_2 + m G_1 $
审计密钥	$ Z_p^* + 2 G_1 $	—	$m G_1 $	$ G_1 $
审计阶段挑战数据	$ Z_p^* $	$2c Z_p^* $	$(1 + 2c) Z_p^* $	—
审计阶段响应数据	$ Z_p^* + (3 + 2l) G_1 + G_2 $	$ G_1 + G_2 $	$2 G_1 $	$m G_1 + 2 Z_p^* (m + 2)$

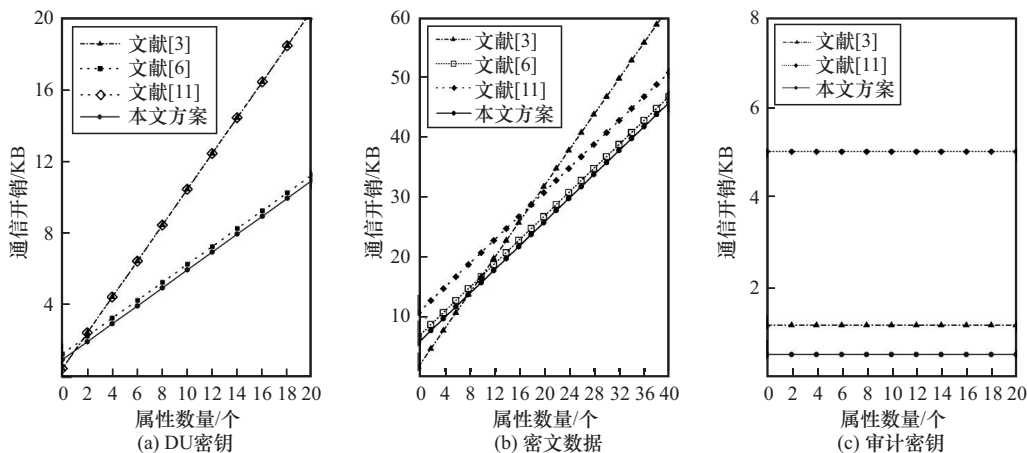


图 3 实际通信开销对比

表5

理论计算开销对比

对比项	文献[3]	文献[6]	文献[11]	本文方案
DU密钥	$(4l+2)E_{G_1} + Hl$	$(2l+3)E_{G_1} + H$	$(3l+2)E_{G_1} + Hl$	$(2l+3)E_{G_1} + Hl +$ $PL_{Ecc} + PL_{Ecc} + PL_E$
数据加密	$E_{G_2} + (3+2l)E_{Z_p^*} +$ $2lE_{G_1} + (1+l)H$	$E_{G_1} + E_{G_2} + (4E_{G_1} + H)l +$ $(M_{G_1} + 2H + 2E_{G_2})m$	$(2l+mn+m)E_{G_1} +$ $(l+m)H + E_{G_2} + M_{G_2}$	$lE_{G_1} + E_{G_2} + h \lg mn +$ $(mn+m)E_{z_p^*}$
审计密钥	$(E_{Z_p^*} + E_{G_1} + H)c + 2P_{G_2}$	$c(2E_{Z_p^*} + E_{G_2} + M_{G_2} + H) + P_{G_2}$	$2P_{G_2} + (c^2 + c + n)E_{G_1}$	$3HHF + (2+c)E_{z_p^*} + mh + 2ncM_{G_2}$
用户解密	$3P_{G_2} + (z+4)E_{G_2}$	$E_{G_2} + M_{G_2}$	$(2P_{G_2} + M_{G_2})l + P_{G_2} + 2M_{G_2}$	$P_{G_2} + 2M_{G_2}$

方案优于文献[3]和文献[11]。相较于文献[3], 本文方案减少了公共参数求逆运算, 计算开销降低约48%。同时, 本文方案KGC和AA通过安全两方计算, 利用盲化因子确保参与方私有数据机密性, 为每个DU引入唯一随机参数, 将属性分量与DU身份进行绑定, 有效防止授权中心腐化的多用户之间的合谋攻击。因此, 本文方案的计算开销略高于文献[6], 但其提供了更高的安全性。数据加密计算开销对比如图4(b)所示, 本文方案要优于文献[3,6,11]。假设数据中的文件块 $m=10$ 个、数据块 $n=5$ 个, 由于本文方案采用在线/离线加密, 在线阶段生成密文及PMAC, 而文献[3,6,11]对访问策略的计算设计在在线阶段, 本文方案的数据加密计算开销明显优于对比方案。审计密钥包含挑战、证明生成和证明验证三部分。审计密钥计算开销对比如图4(c)所示, 本文方案对其他方案具有显著的优势。假设挑战文件块个数 c 从0增加到40个, 因为本文方案证明生成时对抽取的被挑战块生成证明,

之后采用同态哈希运算进行验证, 降低了计算开销。文献[3,6,11]进行大量指数和双线性运算。以文献[11]为例, 计算开销降低了约79%。用户解密计算开销对比如图4(d)所示, 本文方案在进行外包解密之后, DU只需进行双线性运算即可解密, 计算开销显著低于文献[3,11]。利用外包解密充分使用MCS的计算能力, 假设属性数量 $l=10$, 降低了用户端超过90%的解密计算开销。以上分析表明, 本文方案相比于同类方案在性能方面具有优势。

5 结束语

确保医疗数据的隐私性和完整性以及医疗设备的物理安全性是医疗信息系统的核心, 本文提出的支持云审计与设备安全检测的IoMT数据安全方案可以很好地适配这些需求。在属性基加密过程中, 采用安全两方计算生成DU密钥, 以抵抗授权中心腐化下用户的合谋攻击。为提高效率, 本文利用在线/离线加密技术提高医疗设备的加密效率, 通过外包解密提高DU的解密效率。除此之外, 在密文

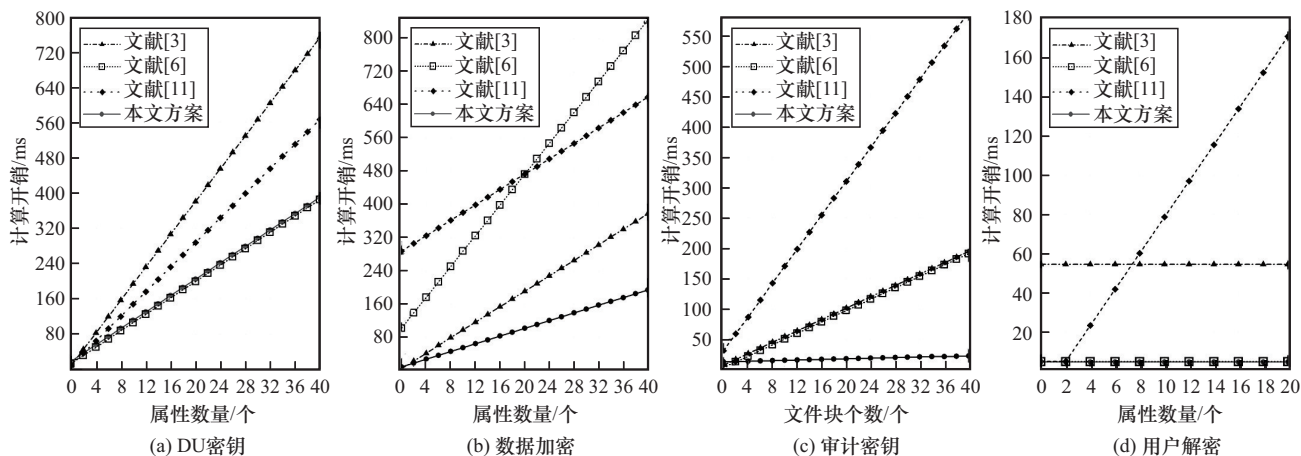


图4 实际计算开销对比

的PMAC中嵌入可穿戴设备的设备指纹来检测医疗设备的物理安全。在审计阶段，MCS和TPA之间采用了非交互式的挑战-应答机制。MCS在TEE下生成审计随机数集，在防止挑战篡改的同时提高审计的安全性，实现数据完整性以及医疗设备的物理安全检测，为医疗数据的安全共享提供了技术保障。为进一步提升医疗数据的安全共享能力，后续将在IoMT系统的跨域共享与溯源机制方面进行深入研究。

参考文献:

- [1] Katal A, Dahiya S, Choudhury T. Energy efficiency in cloud computing data centers: a survey on software technologies[J]. *Cluster Computing*, 2023, 26(3): 1845-1875.
- [2] Chen L, Chen Y X, Liang W, et al. MASS: a multiattribute sketch secure data sharing scheme for IoT wearable medical devices based on blockchain[J]. *IEEE Internet of Things Journal*, 2025, 12(2): 1990-2001.
- [3] Zhao L L, Dong G F, Yuan H. A blockchain-based verifiable CP-ABE scheme for medical data privacy protection[J]. *Scientific Reports*, 2025, 15: 27325.
- [4] Guo Y Y, Peng Z Y, Jiang M M, et al. A blockchain-based puncturable attribute-based encryption scheme with policy hiding for the Internet of things[J]. *IEEE Internet of Things Journal*, 2026, 13(1): 978-989.
- [5] Wazzeah M, Arafeh M, Sami H, et al. CRSFL: cluster-based resource-aware split federated learning for continuous authentication[J]. *Journal of Network and Computer Applications*, 2024, 231: 103987.
- [6] Wang H Y, Liang J L, Ding Y, et al. Ciphertext-policy attribute-based encryption supporting policy-hiding and cloud auditing in smart health[J]. *Computer Standards & Interfaces*, 2023, 84: 103696.
- [7] 刘霞, 王馨族, 张涛, 等. 支持访问策略部分隐藏的CP-ABE方案[J]. *通信学报*, 2024, 45(10): 180-190.
Liu X, Wang X Z, Zhang T, et al. CP-ABE scheme supporting partially hidden access policy[J]. *Journal on Communications*, 2024, 45(10): 180-190.
- [8] 李集浩. 面向边缘智能控制器的属性基加密访问控制机制研究[D]. 广州: 广州大学, 2025.
Li J H. Research on attribute-based encryption access control mechanism for edge intelligent controllers[D]. Guangzhou: Guangzhou University, 2025.
- [9] 徐航星. 支持分层访问控制的密文检索技术研究[D]. 西安: 西安电子科技大学, 2024.
Xu H X. Research on ciphertext retrieval technology supporting hierarchical access control[D]. Xi'an: Xidian University, 2024.
- [10] Goodrich M T, Kitagawa R, Sridhar V. Dynamic accountable storage: an efficient protocol for real-time cloud storage auditing[C]//*Algorithmic Aspects of Cloud Computing*. Berlin: Springer, 2025: 26-45.
- [11] Yang L Y, Chang J Y, Zhang Y H, et al. The hybrid-encryption-based data sharing scheme with keyword-based auditing function in cloud storage setting[J]. *Cluster Computing*, 2025, 28(13): 835.
- [12] Li J, Luo X M, Lei H. TrustHealth: enhancing eHealth security with blockchain and trusted execution environments[J]. *Electronics*, 2024, 13(12): 2425.
- [13] Yang X D, Wang C G, Li R T, et al. A verifiable CP-ABE scheme with policy hiding and dynamic attribute revocation for secure medical IoT system[C]//*Proceedings of the 2025 6th International Conference on Computing, Networks and Internet of Things (CNIOT)*. Piscataway: IEEE Press, 2025: 1-5.
- [14] 梁文丰. 四因素身份认证及多链访问控制的医疗物联网隐私保护研究[D]. 南京: 南京信息工程大学, 2025.
Liang W F. Research on privacy protection of medical IoT based on four-factor authentication and multi-chain access control[D]. Nanjing: Nanjing University of Information Science & Technology, 2025.
- [15] 王雄, 王文博, 刘昂, 等. 一种基于PUF的远程医疗身份认证与密钥协商协议[J]. *信息安全研究*, 2025, 11(7): 626-635.
Wang X, Wang W B, Liu A, et al. A PUF-based identity authentication and key negotiation protocol for telemedicine[J]. *Journal of Information Security Research*, 2025, 11(7): 626-635.
- [16] Liu J H, Long Q F, Liu R P, et al. Privacy-preserving peer-to-peer energy trading via hybrid secure computations[J]. *IEEE Transactions on Smart Grid*, 2024, 15(2): 1951-1964.
- [17] Xie P S, Yang H X, Feng T, et al. Implementing efficient attribute encryption in IoV under cloud environments[J]. *Computer Networks*, 2022, 218: 109363.
- [18] Guo R, Yang X, Jia C Y, et al. A searchable attribute-based encryption scheme supporting policy hiding in cloud-assisted Internet of medical things[J]. *Journal of Cryptologic Research*, 2025, 12(1): 49-68.
- [19] 郭丽峰, 徐卓恒, 刘华. 智慧医疗中具有策略完全隐藏的属性基加密方案[J]. *山西大学学报(自然科学版)*, 2025, 48(5): 933-945.
Guo L F, Xu Z H, Liu H. Attribute-based encryption scheme with policies fully hidden in smart health[J]. *Journal of Shanxi University (Natural Science Edition)*, 2025, 48(5): 933-945.
- [20] Tanveer M, Aldosary A, Khokhar S U D, et al. PAF-IoD: PUF-enabled authentication framework for the Internet of drones[J]. *IEEE Transactions on Vehicular Technology*, 2024, 73(7): 9560-9574.
- [21] 徐俊. 基于不经意传输的公开可验证隐蔽安全两方计算与应用协议研究[D]. 济南: 济南大学, 2023.
Xu J. Study of two-party computation with publicly verifiable covert security and application protocol based on oblivious transfer[D]. Jinan: University of Jinan, 2023.

- [22] Zheng G L, Cao L, Men H L, et al. Research on data security delivery algorithm for crowdsourcing scenario in Internet of vehicles[J]. Computer Networks, 2025, 270: 111505.
- [23] Kang Z Z, Li J G, Zuo Y T, et al. OABS: efficient outsourced attribute-based signature scheme with constant size[J]. IEEE Internet of Things Journal, 2024, 11(23): 38167-38177.

[作者简介]



谢鹏寿 (1972-), 男, 兰州理工大学教授、硕士生导师, 主要研究方向为隐私保护、车联网安全、工业互联网安全、物联网安全、人工智能安全。



董欣瑶 (2003-), 女, 兰州理工大学硕士生, 主要研究方向为网络与信息安全、隐私保护、物联网安全。



鲁晔 (1986-), 男, 博士, 兰州理工大学讲师、硕士生导师, 主要研究方向为网络空间安全、区块链等。



孙宁 (2002-), 女, 兰州理工大学硕士生, 主要研究方向为网络与信息安全、隐私保护、物联网安全。



景兰青 (2003-), 男, 兰州理工大学硕士生, 主要研究方向为网络与信息安全、隐私保护、工业互联网安全。