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加密方案被广泛应用于医疗物联网数据安全传输与共享，而传统的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，本文提出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，以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隐私标签来嵌入设备指纹，实现云端数据的高效审计和医疗设备安全检测。安全分析表明，本文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，本文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：数据完整性审计；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

An 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, Gansu 730050, China

Abstract: Ciphertext-Policy Attribute-Based Encryption (CP-ABE) schemes are widely utilized for the secure transmission and sharing of data in the Medical Internet of Things (IoMT); however, conventional schemes exhibit deficiencies in resisting collusion attacks and providing data integrity auditing. To address these issues, a secure IoMT data 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 calculating privacy labels within ciphertext-aggregated polynomials, enabling efficient cloud data auditing and security detection of medical devices. Security analysis indicates that the proposed scheme ensures cloud data integrity auditing, 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.

Keywords: cloud auditing, Attribute-Based encryption, Physical unclonable funcation, Homomorphic hash function, Secure two-party computation

收稿日期：2025–08–16；**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 Items：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访问控制，仅当DU的属性集合与访问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的属性与匹配密文中的访问策略时，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系统的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保证抗合谋，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，李集浩等[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。徐航星等[9]提出支持外包解密的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，对存储在云上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Ateniese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未提出解决方案。在IoMT系统中，医疗设备作为数据来源，必须具备可靠性。梁文丰等[14]提出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。本文方案的主要贡献如下：

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框架之上设计了隐私标签（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，实现数据完整性审计、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 环境，采用非交互挑战-应答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 $e:G_1 \times G_1 \to G_2$ 满足以下三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 $u,v \in G_1$，存在高效的算法来计算 $e(u,v)$。

1.2　访问结构

令 $S = \{P_1,P_2,\cdots,P_n\}$ 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 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 $B \in A$ 且 $B \subseteq C$，则有 $C \in A$,则称 A 是单调的访问结构。若集合 $D \in A$，则称 D 为授权集合；若 $D \notin A$，则称 D 为非授权集合[18]。

1.3　线性秘密共享(LSSS)

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上 Z_p^* 是线性的，则需要满足以下两个算法[19]。

1) 秘密值分享：M 共享秘密值 $s \in Z_p^*$，设向量 $\vec{y} = (s,\delta_2,\delta_3,...,\delta_n)^T \in Z_p^n$，其中 $\delta_2,\delta_3,...,\delta_n \in Z_p^*$，在该算法中，$\lambda_i' = M_i\vec{y}$ 表示属性名 $\rho(i)$ 所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 $I \subseteq \{1,2,...,l\}$ 定义为 $I = \{i|\rho(i) \in S\}$，存在一组常数 $\{w_i \in Z_p\}_{i \in I}$，使 $\sum_{i \in I} w_i \cdot M_i = (1,0,\cdots,0)$，因此 $\sum_{i \in I} w_i \cdot \lambda_i = s$。

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的物理差异[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、不可克隆性。PUF 的逻辑表达式为

$$R_i = \mathrm{PUF}(C_i) \tag{1}$$

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（FE, Fuzzy Extractor）来确保输出结果的一致性。FE 包含两种算法：生成算法 $\mathrm{FE.Gen}(\cdot)$ 和重建算法 $\mathrm{FE.Rec}(\cdot)$。

$$\mathrm{FE.Gen}(R_i) \to (\beta_i,\mathrm{RP}) \tag{2}$$

$$\mathrm{FE.Rec}(R_i,\mathrm{RP}) \to \beta_i \tag{3}$$

式(2)为 $\mathrm{FE.Gen}(\cdot)$ 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 $\mathrm{FE.Rec}(\cdot)$ 的逻辑表达式，若满足 $\mathrm{HD}(R_i^*,R_i) \leqslant$ ert，则可以重建 β_i，HD 为汉明距离，ert 为误差容限。

表1　　**功能对比表**

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
[3]	选择性	√	×	×	×	×	×	×
[6]	选择性	√	×	√	√	×	×	×
[7]	选择性	√	×	√	×	×	×	×
[8]	选择性	√	√	√	×	×	×	×
[9]	选择性	√	×	√	√	×	×	×
[11]	选择性	√	×	×	√	√	×	×
[12]	选择性	×	×	×	√	√	×	×
[15]	自适应	×	×	×	×	√	×	×
本文方案	选择性	√	√	√	√	√	√	√

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$f=(f_1,f_2)$，并分别得到输出$f_1(x_1,x_2)$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方面[21]：

1) 隐私性：除了从自己的输入和输出中能够推导出的信息外，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，输入消息$x\in Z_p$，输出x的哈希值，即HHF:$H\leftarrow g^x\in G_1$。

同态哈希函数满足以下2个性质[22]。

1) 同态性。对于任意2个数据m_1、m_2和实数w_1、w_2，都有$\mathrm{HHF}(w_1m_1+w_2m_2)=H(m_1)^{w_1}H(m_2)^{w_2}$。

2) 抗碰撞性。攻击者不存在概率多项式算法，能伪造(m_1,m_2,m_3,w_1,w_2)，且$m_3\neq w_1m_1+w_2m_2$，使得$\mathrm{HHF}(m_3)\neq H(m_1)^{w_1}H(m_2)^{w_2}$。

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是的生成元。随机选取指数$\alpha\in Z_p^*$，给定一个序列$\vec{V}$包含$2q$个群元素如式(4)，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以不可忽略的优势如式(5)区分$R=(\vec{V},g^{\alpha^{q+1}})$和$D=(\vec{V},Z)$，则称q-DHE假设在群$G_1$中成立[23]。

$$\vec{V}=(g,g^{\alpha},g^{\alpha^2},\cdots,g^{\alpha^q},g^{\alpha^{q+2}}g^{\alpha^{q+3}},\cdots,g^{\alpha^{2q}}) \tag{4}$$

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

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）、医疗云服务器（MCS）、第三方审计者（TPA）、数据所有者（DO）和数据使用者（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属性私钥。

3) MCS：MCS是一个半诚实的实体。拥有充

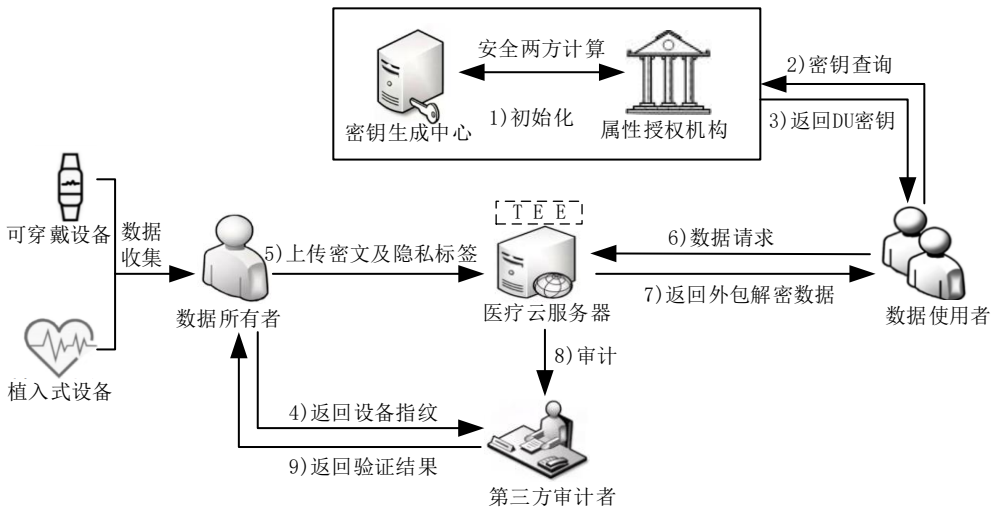

图1　系统模型

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环境中生成挑战随机值，在非TEE环境中生成证明发送给TPA用于证明验证。

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环境的MCS进行非交互式挑战-应答进行数据审计，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进行数据收集。DO负责制定访问策略，计算密文及隐私标签并上传到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，DU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	隐私标签

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（IND-CPA，Indistinguishability under Chosen-Plaintext Attack），选择明文攻击游戏参与方包括挑战者$\mathbb{C}$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$\mathbb{C}$。

系统建立 挑战者$\mathbb{C}$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}、AA公钥PK_{AA}发送给A。

查询1 敌手A向挑战者$\mathbb{C}$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$\mathbb{C}$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$\mathbb{C}$，$\mathbb{C}$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$\mathbb{C}$发送属性集合S申请密钥，但规定S不能满足(M^*,ρ^*)。

猜测 A输出对c的猜想c'，若$c'=c$，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$\varepsilon=|\Pr[c'=c]-\frac{1}{2}|$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$\mathbb{C}$之间的挑战游戏定义，具体游戏如下：

系统建立 挑战者$\mathbb{C}$运行系统初始化算法，获取公共系统参数、公私钥，$\mathbb{C}$将PP、PK_{KGC}、PK_{AA}发送给A，PP中包含Paillier公钥pk，挑战者$\mathbb{C}$保存MSK_{KGC},MSK_{AA}。

查询1 敌手A可以适应性地进行以下三种查询：

□ 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A。

□ 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。

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

挑战 敌手A向$\mathbb{C}$发送两个等长的消息m_0,m_1和欲挑战访问策略(M^*,ρ^*)。$\mathbb{C}$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。

$\mathbb{C}$必须满足如下约束条件：在若敌手A已腐化KGC或AA，则敌手A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，这些用户的属性并集并不满足(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，$\mathbb{C}$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$\varepsilon = |\Pr[c' = c] - \frac{1}{2}|$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，本文方案在标准TEE信任假设下分析方案安全性。进一步地，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质作退化分析，相关讨论见第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) $\text{Setup}(\lambda) \to (\text{PP},\text{PK},\text{MSK})$。该算法由KGC和AA参与执行。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$e:G_1 \times G_1 \to G_2$，其中G_1和G_2是具有相同素数阶$p(|p| \geqslant \lambda)$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$h_1:\{0,1\}^* \to Z_p^*$，$H_1:\{0,1\}^* \to G_1$和同态哈希函数$\text{HHF}(\cdot):\{0,1\}^* \to Z_p^*$。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$N$，满足$p < N$。系统公共参数PP如式

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

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

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

算法1 $\text{KeyGenDU}(\text{MSK},S) \to \text{SK}_{\text{DU}}$。DU密钥采用Paillier同态加密的安全两方计算由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}。

□ 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。

□ 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$C_y = C_x^a \cdot \text{Enc}_{\text{pk}}(a\theta + b)$，将$(Q,C_y)$发送给KGC。

□ 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$\text{SK}_{\text{KGC}}$如式(7)，并将$\text{SK}_{\text{KGC}}$发送给DU。

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

□ AA计算属性私钥SK_{AA}如式(8)，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 $\text{KeyGenTPA}(c_i) \to (\psi_i)$。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。

□ 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。

□ 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。

□ 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，以及β_i的辅助信息hd。

□ TPA将hd通过安全信道发送给DO，DO存储$\{c_i,\text{hd}\}$。

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

4) $\text{Enc}((M,\rho),F) \to \text{CT}$。数据加密算法由DO

执行。数据加密算法包含离线加密算法 $\mathrm{OfflineEnc}((M,\rho)) \to \mathrm{IC}$ 和在线加密算法 $\mathrm{OnlineEnc}(\mathrm{IC},F) \to \mathrm{CT}$。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离线数据加密，设备使用时执行在线数据加密。

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

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

□ DO选取随机向量$\vec{y}=(s,\delta_2,\delta_3,...,\delta_n) \in Z_p^n$，其中$s$是秘密共享数值，其他的元素为了隐藏$s$的随机值。计算秘密的分享份额$\lambda_i = M_i\vec{y}(i=1,2,...l)$。

□ 对M的每行，选取随机数$r_i=(r_1,r_2,...r_l)$。医疗智能设备计算$D_i = g^{\gamma\lambda_i}g^{-\mu r_i}H_1(\rho(i))^{-r_i}$，$D_i' = g^{r_i}$。并返回中间密文$\mathrm{IC}=\{D_i,D_i'\}_{i=1}^{l}$。

算法 4　$\mathrm{OnlineEnc}(\mathrm{IC},F) \to \mathrm{CT}$。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及隐私标签PMAC。

□ 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$R_i^* = \mathrm{PUF}(c_i)$，使用模糊提取器重构密钥$\beta = \mathrm{FE.Rec}(R_i^*,\mathrm{hd})$，$\beta$的哈希值$\varphi = h_1(\beta)$。

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

$$\mathrm{IC}=\{D_i = g^{\gamma\lambda_i}g^{-\mu r_i}H_1(\rho(i))^{-r_i}, D_i' = g^{r_i}\}_{i=1}^{l} \tag{9}$$

$$C = F\cdot e(g,g)^{xs} \tag{10}$$

$$C=\{C_1,C_2,...,C_m\} \tag{11}$$

$$\alpha_j = \mathrm{PRF}(\varphi,j) \tag{12}$$

□ 生成C的隐私标签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)，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)，输出PMAC_i，并且生成PMAC_i的哈希hc_i如式(15)。

$$P_{C_i}(\varphi) = X_i = \begin{pmatrix}(C_{i,0}+\alpha_0)+(C_{i,1}+\alpha_1)\varphi \\ +(C_{i,2}+\alpha_2)\varphi^2+...+ \\ (C_{i,n-1}+\alpha_{n-1})\varphi^{n-1}\end{pmatrix}(\mathrm{mod}\,p) \tag{13}$$

$$\mathrm{PMAC}_i = g^{t_i+X_i} \tag{14}$$

$$\mathrm{hc}_i \leftarrow h_1(\mathrm{PMAC}_i) \tag{15}$$

□ 对所有的$\{\mathrm{hc}_i\}$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。

□ DO将CT如式(16)发送给MCS。

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

5) $\mathrm{Decrypt}(\mathrm{CT}) \to F$。数据解密算法包括外包解密算法$\mathrm{OutsourcedDec}(S,\mathrm{SK_{AA}}) \to \mathrm{TCT}$和DU解密算法$\mathrm{UserDec}(C,\mathrm{TCT},\mathrm{SK_{KGC}}) \to F$。

算法 5　$\mathrm{OutsourcedDec}(S,\mathrm{SK_{AA}}) \to \mathrm{TCT}$。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$\mathrm{SK_{AA}}$，若满足访问策略，则输出TCT。

□ MCS根据DU的$\mathrm{SK_{AA}}$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$I=\{i:\rho(i) \in P\} \subseteq \{1,2,...,l\}$，$P$为授权属性集合。

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

□ MCS计算转换密文TCT如式(17)，并将密文C和TCT发送给DU。

$$\mathrm{TCT} = \prod_{i\in I}\left(e(D_i,L)\cdot e(D_i',k_{\rho(i)})\right)^{w_i} = e(g,g)^{\gamma s} \tag{17}$$

算法 6　$\mathrm{UserDec}(C,\mathrm{TCT},\mathrm{SK_{KGC}}) \to F$。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$\mathrm{SK_{KGC}}$，输出明文$F'$如式

$$F' = \frac{C}{e(C',\mathrm{SK_{KGC}})/\mathrm{TCT}} \tag{18}$$

6) $\mathrm{DataVerify}(\mathrm{PMAC}_i,\mathrm{cp}) \to \mathrm{RST}$。数据审计包括证明生成算法$\mathrm{ProofGen}(\mathrm{cp}) \to \mathrm{Prf}$和证明验证算法$\mathrm{ProofVer}(\mathrm{Prf}) \to \mathrm{RST}$。数据审计采用非交互式挑战-应答进行数据完整性审计。审计开始时，MCS在受硬件保护的TEE环境中生成随机数集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

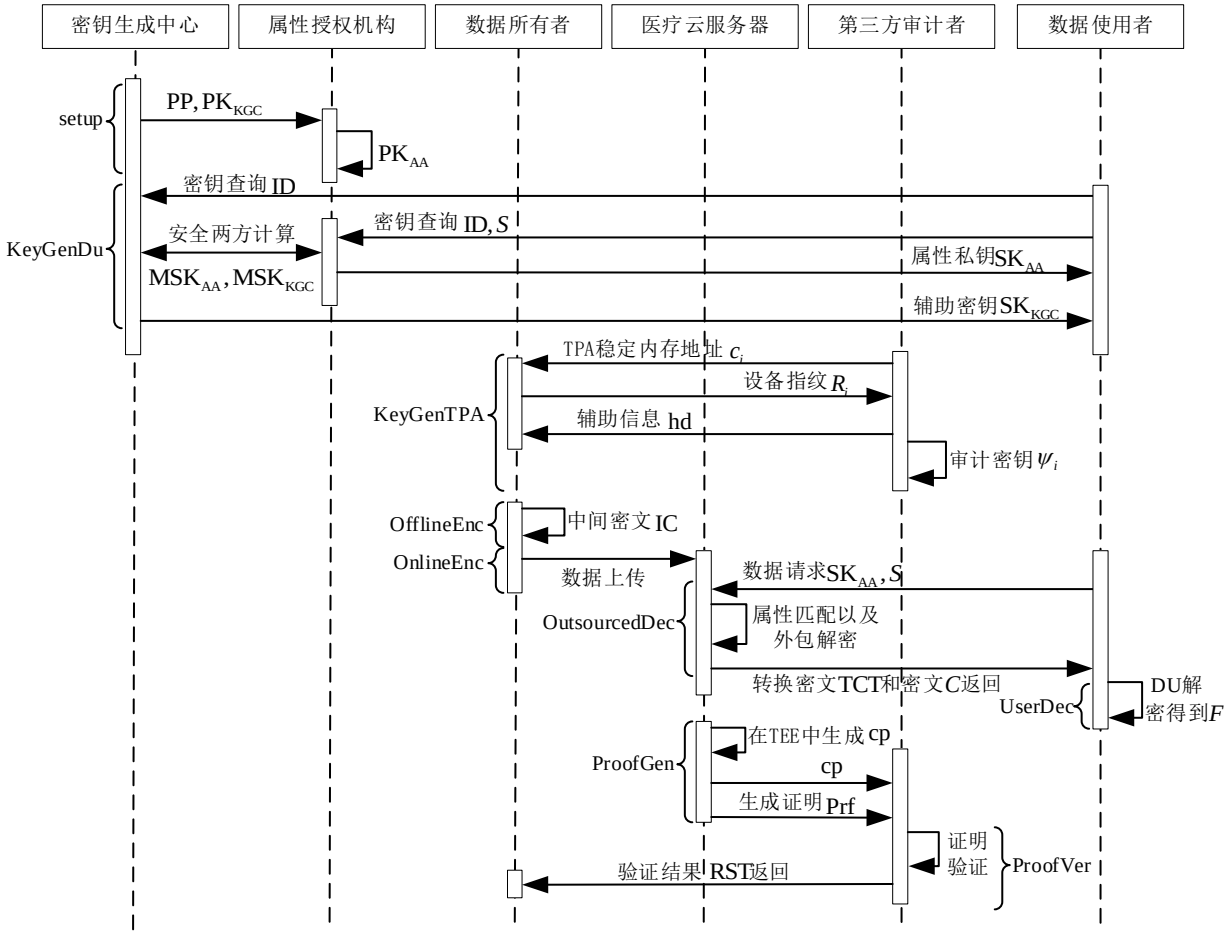

图2　方案时序图

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　ProofGen(cp) → 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。

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

□ 将 MCS 的 TEE 生成的 cp = $\{c_1,c_2,c\}$ 发送给 MCS 的非 TEE 环境。使用伪随机置换函数 $\mathrm{id} \leftarrow \pi_{c_1}(l)$ 生成被挑战块的位置标识符 id，使用伪随机函数 $a_{\mathrm{id}} \leftarrow f_{c_1}(l)$ 生成 id 对应被挑战块的证明系数，生成挑战 $G = \{(\mathrm{id}, a_{\mathrm{id}})\}$。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。

□ 计算聚合证明 $P_{\mathrm{Prf}}(q)$ 如式(19)和商多项式如式(20)。

$$P_{\mathrm{Prf}}(q) = \sum_{i \in G} a_i C_{i,0} + \sum_{i \in G} a_i C_{i,1} \cdot q + \sum_{i \in G} a_i C_{i,2} \cdot q^2 + \ldots + \sum_{i \in G} a_i C_{i,n-1} \cdot q^{n-1} \tag{19}$$

$$Z_{\mathrm{Prf}}(q) = \frac{P_{\mathrm{Prf}}(q) - P_{\mathrm{Prf}}(z)}{q - z} \tag{20}$$

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

□ MCS 将 Prf 如式(21)发送给 TPA。

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

算法 8　ProofVer(Prf) → 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。

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

□ 在接收到 Prf 之后，使用默克尔哈希树计算

$\{hc_i^*\}$得出根哈希hr'，若hr ≠ hr'则向DU发送RST =⊥，并且运算终止，否则执行后续。

□ 重新构建偏移量$\alpha_j = \mathrm{PRF}(\varphi,j)$，计算偏移补偿项$P_\alpha(\varphi)$如式(22),再计算式(23-25)。

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

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

$$P'_{\mathrm{Prf}}(\varphi) = \left(P_{\mathrm{Prf}}(\varphi) + (\sum a_{id}) P_\alpha(\varphi)\right) \bmod p \tag{24}$$

$$H_t = \mathrm{HHF}(\sum_{i \in G} t_i * a_i) \tag{25}$$

□ 对计算结果进行验证，判断以下等式是否成立，若成立，返回RST = 1，否则，返回RST =⊥。

$$\begin{aligned} \mathrm{RST} &= \prod_{i \in G} \left(\mathrm{PMAC}_i\right)^{a_i} \\ &= H_z^{\varphi - z} \cdot \mathrm{HHF}(P'_{\mathrm{Prf}}(\varphi)) \cdot H_t \end{aligned} \tag{26}$$

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)并发给DU。

$$\begin{aligned} \mathrm{TCT} &= \prod\nolimits_{i \in l} \left(e(D_i,L) \cdot e(D'_i,k_{\rho(i)})\right)^{w_i} \\ &= e\left(\prod\nolimits_{i \in l} \left(g^{\gamma\lambda_i} g^{-\mu r_i} H_1(\rho(i))^{-r_i}, g^t\right)\right)^{w_i} \cdot \\ &\quad e\left(\prod\nolimits_{i \in l} (g^{r_i}, H_1(\rho(i))^t (g^\mu)^t)\right)^{w_i} \\ &= \prod\nolimits_{i \in l} \begin{pmatrix} e(g^{\gamma\lambda_i w_i} g^{-\mu r_i w_i} H_1(\rho(i))^{-r_i w_i}, g^t) \cdot \\ e(g^{r_i w_i}, H_1(\rho(i))^t (g^\mu)^t) \end{pmatrix} \\ &= \prod\nolimits_{i \in l} \begin{pmatrix} e(g^{\gamma\lambda_i w_i}, g^t) \cdot e(g^{-\mu r_i w_i}, g^t) \cdot \\ e(H_1(\rho(i))^{-r_i w_i}, g^t) \cdot \\ e(g^{r_i w_i}, H_1(\rho(i))^t) \cdot e(g^{r_i w_i}, (g^\mu)^t) \end{pmatrix} \\ &= \prod\nolimits_{i \in l} \left(e(g^{\gamma\lambda_i w_i}, g^t)\right) \\ &= e(g,g)^{\gamma t \sum_{i \in l} w_i \lambda_i} \\ &= e(g,g)^{\gamma t s} \end{aligned} \tag{27}$$

之后，DU使用$\mathrm{SK}_{\mathrm{KGC}}$解密得到的数据如式

$$\begin{aligned} F' &= \frac{C}{e(C', \mathrm{SK}_{\mathrm{KGC}})/\mathrm{TCT}} \\ &= \frac{F \cdot e(g,g)^{xs}}{e(g^{\mu s}, g^{(x+\gamma t)/\mu})/e(g,g)^{\gamma t s}} \\ &= \frac{F \cdot e(g,g)^{xs} \cdot e(g,g)^{\gamma t s}}{e(g,g)^{xs+\gamma t s}} \\ &= F \end{aligned} \tag{28}$$

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。

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

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

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：Game_0,Game_1,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$\mathrm{SK}_{\mathrm{KGC}}$，$\mathrm{Game}_1$用安全两方计算的理想功能替代真实协议，$\mathrm{Game}_2$是挑战密文与随机元素不可区分。如下对$\mathrm{Game}_1$和$\mathrm{Game}_2$定义。

Game_1：Game_1与Game_0的区别在于用户密钥查询$Q_{\mathrm{KeyGen}}(\mathrm{ID},S)$，$\mathrm{Game}_1$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$F_{2\mathrm{pc}}$直接生成$\mathrm{SK}_{\mathrm{KGC}} = g^{(x+\gamma t)/\mu}$和$\mathrm{SK}_{\mathrm{AA}} = \{L = g^t, \forall d \in S: k_d = H_1(d)^t (g^\mu)^t\}$，之后挑战者$\mathbb{C}$继续执行后续步骤，其他步骤与$\mathrm{Game}_0$

相同。

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

证明需要以下2个引理，最终证明出定理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$\mathrm{negl}(\lambda)$，使得$|\mathrm{Adv}_0 - \mathrm{Adv}_1| \leqslant \mathrm{negl}(\lambda)$。

证明 假设存在敌手A以不可忽略的优势区分$Game_0$和$Game_1$，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$Real_{2pc}$或理想功能$Ideal_{2pc}$，模拟器B需要判断接收的哪种挑战。模拟器B模拟$Game_0$或$Game_1$给敌手A：

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

查询1 敌手A可以适应性地进行以下三种查询：

□ 用户密钥查询$Q_{\mathrm{KeyGen}}(\mathrm{ID},S)$：当敌手A发起$Q_{\mathrm{KeyGen}}(\mathrm{ID},S)$，B随机选取$t \in Z_p^*$，输入$(x,\mathrm{ID})$和$(\gamma,\mu,t,\mathrm{ID},S)$，提交给安全两方计算挑战接口。若挑战接口对应$Real_{2pc}$，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$Ideal_{2pc}$，则返回SK_{KGC}以及SK_{AA}，其分布与$Game_1$理想功能输出一致。随后模拟器B将$SK_{DU} = (SK_{KGC},SK_{AA})$返回给敌手A。

□ 授权中心腐化查询$Q_{\mathrm{corrupt}}(\mathrm{auth})$：当敌手A发起$Q_{\mathrm{corrupt}}(\mathrm{auth})$，B按照安全模型进行返回。

□ 用户合谋查询$Q_{\mathrm{collude}}(\mathrm{ID}_1,...,\mathrm{ID}_k)$：当敌手A发起$Q_{\mathrm{collude}}(\mathrm{ID}_1,...,\mathrm{ID}_k)$，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^*，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B也能以不可区分的优势区分$Real_{2pc}$和$Ideal_{2pc}$，从而破坏该安全两方计算协议在半诚实模型下的安全性，与协议的安全性假设矛盾，故$|\mathrm{Adv}_0 - \mathrm{Adv}_1| \leqslant \mathrm{negl}(\lambda)$。

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$\mathrm{negl}(\lambda)$，使得$|\mathrm{Adv}_1 - \mathrm{Adv}_2| \leqslant \mathrm{negl}(\lambda)$。

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$(\vec{V},Z)$，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，$PK_{AA} = (g^{\gamma},g^{\mu})$，$PK_{KGC} = e(g,g)^x = e(g^{\alpha^q},g^{\alpha})$其中$g^{\alpha^q}$和$g^{\alpha}$从$\vec{V}$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$Q_{\mathrm{corrupt}}(\mathrm{AA})$时，返回$(\gamma,\mu)$。用户密钥查询时，当敌手A发起$Q_{\mathrm{KeyGen}}(\mathrm{ID},S)$请求时，若$S$满足欲挑战的访问策略$(M^*,\rho^*)$，则终止，否则B随机选择$t \in Z_p^*$，生成$SK_{AA} = \{L = g^t,\forall d \in S: k_d = H_1(d)^t(g^{\mu})^t\}$。在生成$SK_{KGC}$时，若$Z = g^{\alpha^{q+1}}$则$SK_{KGC} = g^{(x+\gamma t)/\mu}$，若$Z$为随机数，则$SK_{KGC}$为半功能密钥。返回$SK_{DU} = (SK_{KGC},SK_{AA})$。

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

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

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$c' = c$，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$|\mathrm{Adv}_1 - \mathrm{Adv}_2| \leqslant \mathrm{negl}(\lambda)$。

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

由引理1和引理2可知式(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。

$$\begin{aligned}\mathrm{Adv}_0 &= |\mathrm{Adv}_0 - \mathrm{Adv}_1 + \mathrm{Adv}_1 - \mathrm{Adv}_2 + \mathrm{Adv}_2| \\ &\leqslant \mathrm{negl}(\lambda)\end{aligned} \tag{32}$$

证毕。

2) 数据审计隐私性

数据完整性审计中，TPA无需知道所有数据，便可对数据完整性进行审计。MCS发送给TPA的审计证据包括$\{\{\mathrm{PMAC}_i, \mathrm{hc}_i^*, t_i\}_{i=0}^m, Z_{\mathrm{Prf}}(q), P_{\mathrm{Prf}}(z)\}$，$\mathrm{PMAC}_i = g^{P_{C_i}(\varphi)+t_i}$，其中$P_{C_i}(\varphi)$是包含隐藏偏移量$\alpha_j$的多项式承诺在秘密值$\varphi$处的值，由于$\alpha_j$由$\mathrm{PRF}(\cdot)$生成，$\varphi$由PUF生成，从$\mathrm{PMAC}_i$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，$Z_{\mathrm{Prf}}(q)$是多项式商，TPA只能评估它在φ的值，无法泄露具体多项式系数；$P_{\mathrm{Prf}}(z)$是被挑战文件块的随机线性组合在z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，实现云存储数据在TPA审计中隐私保护。

3) 概率审计可靠性

本文方案的审计算法基于概率模型，方案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，受损数据块数为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

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

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

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

因此，当在MCS上存储的数据被减少或者被破坏，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在不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可信执行环境TEE的MCS采用非交互式挑战-应答策略进行审计，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环境与TPA根据cp生成挑战，cp构成挑战生成的随机性，TPA无需向MCS发起挑战便可对存储在MCS上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。本文方案的隐私标签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隐私标签及审计证据，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式，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$(\omega,\lambda,\varepsilon)$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$\omega$，恢复算法就能以概率1正确输出原始密钥$\beta$如式(35)。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，从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。

$$\Pr\left[\begin{array}{l}\beta=\mathrm{FE.Rec}(R^*,\mathrm{hd})|(\beta,\mathrm{hd})\\ \leftarrow \mathrm{FE.Gen}(R),\mathrm{HD}(R,R^*)\leqslant\omega\end{array}\right]=1 \quad (35)$$

本文方案中即使攻击者获得辅助数据hd，也无法恢复密钥β。若R的最小熵至少为λ即$H_\infty(R)\geqslant\lambda$，则$\mathrm{SD}((\beta,\mathrm{hd}),(\beta^*,\mathrm{hd}))\leqslant\varepsilon$，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^*。

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，若审计通过即表明数据在生成、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

方案的安全性对比的结果如表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，其他方案为选择性安全。在抗用户合谋方面，除文献[12][15]外，其余文献均能抵抗用户之间的合谋。为了降低计算开销，文献[8]使用了在线/离线加密。进一步的，文献[6][7][8][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-应答实现挑战抗篡改，文献[3][6][11]采用交互式挑战-应答存在挑战篡改攻击。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

本文方案与文献[3]、文献[6]、文献[11]的方案进行通信开销和计算开销对比。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(Java Pairing-Based Cryptography Library)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的主要作用是标准TEE信任假设下生成随机数集cp。本文实验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]使用了与本文类似的TEE结构，在基于CP-ABE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带来的系统级延迟通常为亚毫秒级。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。

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

表3　　**符号含义表**

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

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，当属性从0个增加到20个时，DU密钥计算开销比文献[3]、文献[11]低46%。如图3(b)所示，设文件被分为$m = 10$块，关键字$w = 20$个，本文方案在属性从0个到20个时，密文数据的通信开销低于文献[6]、文献[11]，在属性个数大于20时，本文方案的通信开销最低。如图3(c)所示，审计密钥的通信开销明显低于文献[3]、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]、文献[11]。

4.2　计算开销

对每种运算进行2000次运算，求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

表4　　**理论通信开销对比**

对比项	方案			
	[3]	[6]	[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	$\|Z_p^*\|+(3+2l)\|G_1\|+\|G_2\|$	$\|G_1\|+\|G_2\|$	$2\|G_1\|$	$m\|G_1\|+2\|Z_p^*\|(m+2)$

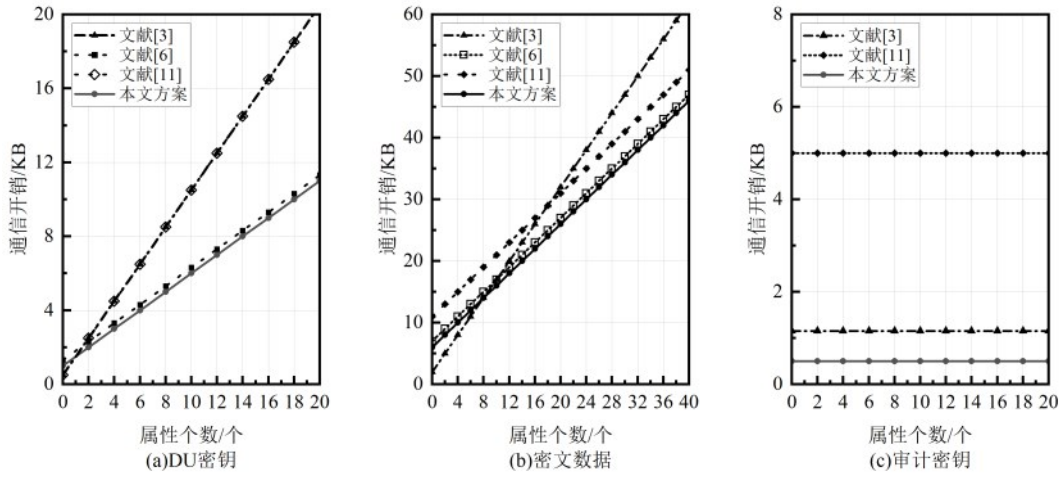

图3　实际通信开销对比

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4.6405ms、0.0260ms和0.0020ms，在G_2上进行一次指数运算E_{G_2}和一次乘法运算M_{G_2}的时间分别为4.6171ms和0.0221ms，一次双线性运算P_{G_2}的时间为4.3205ms。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0.0199ms、0.0018ms和4.6143ms，由于在Z_P^*上进行一次乘法运算的时间为0.0006ms，在计算开销时可忽略不计。取Paillier的公钥模数N的比特长度为2048bit时，一次Paillier加密运算$\mathrm{PL_{ENC}}$、一次Paillier解密运算$\mathrm{PL_{DEC}}$和一次Paillier指数运算PL_E的平均时间分别为2.0565ms、1.1824ms和2.0746ms，由于一次Paillier乘法运算PL_M的平均时间为0.0001ms，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，其中加密数据开销中包含数据签名的运算。

DU密钥计算开销对比如图4(a)所示，本文方案优于文献[3]、[11]。相较于[3]来说，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。因此本文方案计算开销略高于文献[6]，但本文方案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密文隐私标签，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。审计包含挑战、证明生成和证明验证三部分。审计计算开销对比如图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，之后采用同态哈希进行验证，降低了计算开销。而文献[3][6][11]进行大量指数运算和双线性运算。以方案[11]为例，计算开销降低了约79%。用户解密计算开销分析如图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，提出的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及完整性和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的适配这些需求。在属性基加密过程中：采用安全两方计算生成DU密钥，来抵抗授权中心腐化下的用户的合谋攻击。为提高方案效率，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，在密文的隐私标签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环境下生成审计随机数集，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。

表5　理论计算开销对比

对比项	方案			
	[3]	[6]	[11]	本文方案
DU密钥生成	$(4l+2)E_{G_1}+Hl$	$(2l+3)E_{G_1}+H$	$(3l+2)E_{G_1}+Hl$	$(2l+3)E_{G_1}+Hl+\mathrm{PL_{ENC}}+\mathrm{PL_{DEC}}+\mathrm{PL_E}$
数据加密	$E_{G_2}+(3+2l)E_{Z_p^*}+2lE_{G_1}+(1+l)H$	$E_{G_1}+E_{G_2}+(4E_{G_1}+H)l+(M_{G_1}+2H+2E_{G_2})m$	$(2l+mn+m)E_{G_1}+(l+m)H+E_{G_2}+M_{G_2}$	$lE_{G_1}+E_{G_2}+h\log_2 mn+(mn+m)E_{z_p^*}$
审计	$(E_{Z_p^*}+E_{G_1}+H)c+2P_{G_2}$	$c(2E_{Z_p^*}+E_{G_2}+M_{G_2}+H)+P_{G_2}$	$2P_{G_2}+(\mathrm{c}^2+c+n)E_{G_1}$	$3\mathrm{HHF}+(2+\mathrm{c})E_{z_p^*}+mh+2ncM_{G_2}$
用户解密	$3P_{G_2}+(z+4)E_{G_2}$	$E_{G_2}+M_{G_2}$	$(2P_{G_2}+M_{G_2})l+P_{G_2}+2M_{G_2}$	$P_{G_2}+2M_{G_2}$

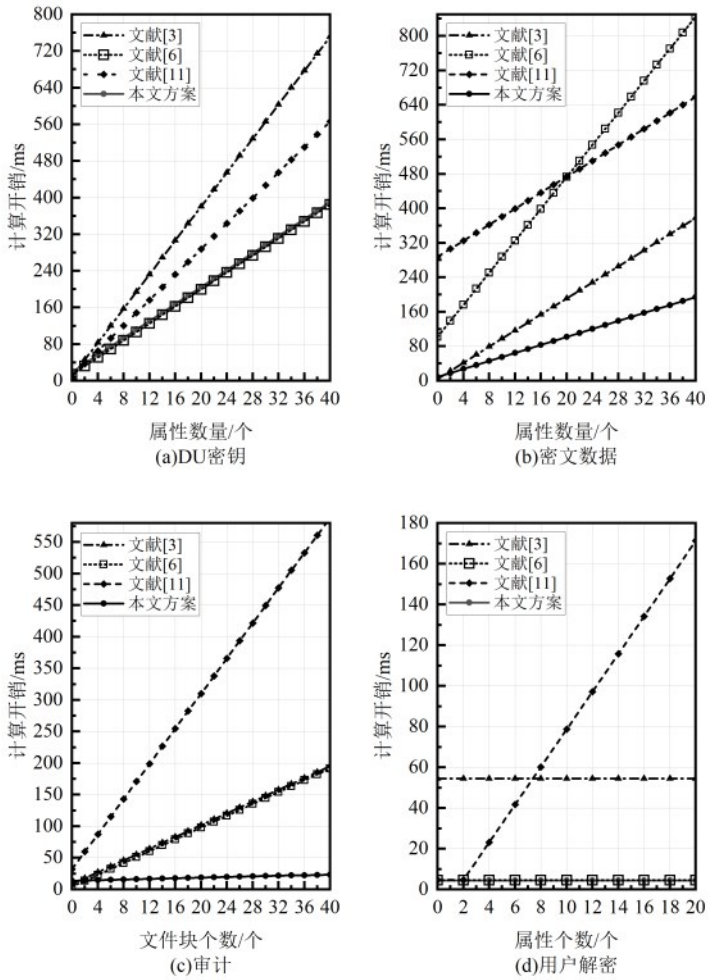

图4　实际计算开销对比

董欣瑶（2003-），女，陕西宝鸡人，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，陕西宝鸡人，博士，兰州理工大学讲师，硕士生导师，主要研究方向为网络与信息安全、隐私保护、物联网安全。

孙宁（2002-），女，山东临沂人，兰州理工大学硕士生，主要研究方向为网络空间安全、区块链等。

景兰青（2003-），男，甘肃泾川人，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。

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(1): 1-24.

[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] WAZZEH 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]. 广州大学, 2025. 10. 27040.
LI J. Research on attribute-based encryption access control mechanism for edge intelligent controllers[D]. Guangzhou University, 2025. 10. 27040.

[9] 徐航星.支持分层访问控制的密文检索技术研究[D]. 西安电子科技大学, 2024.
XU H X. Research on ciphertext retrieval technology supporting hierarchical access control[D]. Xidian University, 2024.

[10] GOODRICH M T, KITAGAWA R, SRIDHAR V. Dynamic accountable storage: an efficient protocol for real-time cloud storage auditing [C]. //9th International Symposium on Algorithmic Aspects of Cloud Computing-ALGOCLOUD-Annual, 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): 1-17.

[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 6th International Conference on Computing, Networks and Internet of Things, 2025: 136-140.

[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 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]. 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 medical IoT[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, et al. Attribute-based encryption scheme with policies fully hidden in smart health[J]. Nat. Sci. Univ. Shanxi, 2025, 48(5): 933-945.

[20] TANVEER M, ALDOSARY A, KHOKHAR S, 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]. 济南大学, 2023.
XU J. Study of two-party computation with publicly verifiable covert security and application protocol based on oblivious transfer[D]. 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.

谢鹏寿（1972-），男，甘肃清水人，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。