支持条件身份匿名的云存储医疗数据轻量级完整性验证方案

张晓均*① 王 鑫① 廖文才① 赵 芥① 付兴兵②③

①(西南石油大学计算机科学学院网络空间安全研究中心 成都 610500)

②(宜宾学院理学部 宜宾 644000)

③(杭州电子科技大学网络空间安全学院 杭州 310018)

摘 要：医疗云存储服务是云计算技术的一个重要应用，同时外包医疗数据的完整性和用户的身份隐私保护已变得越来越重要。该文提出适用于无线医疗传感器网络的支持条件身份匿名的外包云存储医疗数据轻量级完整性验证方案。方案结合同态哈希函数设计了聚合签名，通过第三方审计者(TPA)对外包云存储医疗数据进行完整性验证，在TPA端存放审计辅助信息，利用同态哈希函数的同态性质将TPA端的计算优化为常量运算，大大降低了第三方审计者的计算开销，同时支持TPA对多个数据文件执行批量验证，其验证开销几乎是恒定的，与医疗数据文件的数量无关。方案有效防止了第三方审计者通过求解线性方程恢复原始医疗数据，并且设计了条件身份匿名算法，密钥生成中心(PKG)根据用户唯一标识的身份信息为用户生成匿名身份及对应的签名私钥。即使攻击者截获到用户传输的医疗数据，也无法获知拥有此数据的真实身份，有效避免了对公钥证书的复杂管理，同时使得密钥生成中心可以有效追踪医疗信息系统中具有恶意行为的用户。安全性分析与性能评估结果表明该方案能够安全高效地部署在云辅助无线医疗传感器网络。

关键词：无线医疗传感器网络；云存储；聚合签名；完整性验证；条件身份匿名

中图分类号：TN918; TP309.2 **文献标识码**：A **文章编号**：1009-5896(2022)12-4348-09

DOI: 10.11999/JEIT210971

Lightweight Integrity Verification Scheme for Outsourced Medical Data in Cloud Storage Supporting Conditional Identity Anonymity

ZHANG Xiaojun① WANG Xin① LIAO Wencai① ZHAO Jie① FU Xingbing②③

①(*School of Computer Science, Research Center for Cyber Security, Southwest Petroleum University, Chengdu* 610500, *China*)

②(*Faculty of Science, Yibin University, Yibin* 644000, *China*)

③(*School of Cyberspace, Hangzhou Dianzi University, Hangzhou* 310018, *China*)

Abstract: Medical cloud storage service is one of the most significant applications in cloud computing. Simultaneously, the integrity of outsourced medical data and users' identity privacy-preservation have been more and more important. To this end, an outsourced cloud storage medical data lightweight integrity verification scheme is proposed for wireless medical sensor networks, supporting conditional identity anonymity. The scheme combines the homomorphic hash function to design an aggregated signature to enable a Third Party Auditor (TPA) to check the integrity of outsourced medical data effectively. The scheme stores auditing auxiliary information on TPA side and uses the homomorphic property of the homomorphic hash function to optimize the calculations on TPA side to a constant, which reduces greatly the computational costs of TPA. The scheme enables TPA to perform batch verification on multiple data files, and the verification costs are nearly constant, independent of the number of data files. In addition, this scheme prevents effectively TPA

收稿日期：2021-09-13；改回日期：2022-08-25；网络出版：2022-09-08

*通信作者： 张晓均 zhangxjdzkd2012@163.com

基金项目：国家自然科学基金(61902327)，中国博士后科学基金(2020M681316)，浙江省自然科学基金(LY19F020045)，成都市科技局项目(2021-YF05-00965-SN)，西南石油大学研究生教研教改项目(JY20ZD06)

Foundation Items: The National Natural Science Foundation of China (61902327), China Postdoctoral Science Foundation (2020M681316), Zhejiang Provincial Natural Science Foundation of China (LY19F020045), Chengdu Key R & D Project (2021-YF05-00965-SN), Southwest Petroleum University Graduate Teaching Research and Reform Project (JY20ZD06)

from recovering the original medical data by solving the linear equations, and a conditional identity anonymous algorithm is designed, thus the Private Key Generator (PKG) could generate the anonymous identity of a user and corresponding singing key. Even if the attacker intercepts the medical data transmitted by the user, it can not know the real identity of the data. In addition, the complex certificates management is efficiently avoided, and PKG could also trace and revoke the real identities of misbehaved users efficiently. The security analysis and performance evaluation demonstrate that this scheme could be securely and efficiently deployed in wireless medical sensor networks.

Key words: Wireless medical sensor network; Cloud storage; Aggregate signature; Integrity verification; Conditional identity anonymity

1　引言

医疗大数据由于其在现代医疗系统中的潜在价值，受到了人们的广泛关注。医疗大数据的蓬勃发展不可避免地产生新的数据安全和隐私保护问题。如果医疗大数据不完整和不真实，新挖掘的知识将无法令人信服。随着信息技术的高速发展，远程医疗信息系统将与云计算技术相结合，提供一种便捷的新型服务模式[1]。云计算技术拥有强大的计算能力和存储能力，它为用户提供高效灵活的存储服务来维护数据[2,3]。在基于云辅助的无线医疗传感器网络中，医疗用户通过无线医疗传感器设备收集重要的生理特征参数(如血压、血糖等)，实时地将这些医疗数据上传到云服务器进行存储、分析与处理[4]。

虽然云计算提供的服务有着非常多的优势，但数据存储于云服务器，用户对数据失去绝对控制权，容易遭受外部敌手恶意删除或篡改等方面的攻击。除此之外，某些硬件和软件故障因素的存在将不可避免地导致数据损坏，而云服务提供商可能会只考虑自身利益不受损坏，从而隐瞒数据不完整的事实[5]。近年来频繁发生云安全和云犯罪事件，严重影响了用户和云服务提供商的信任关系。医疗用户关注的焦点在于存储在云端的医疗健康数据的完整性，它是所有临床诊断的基础，任何数据篡改或者丢失都会导致错误诊断，甚至会导致死亡等严重后果[6]，因此对云服务器上的医疗数据进行完整性验证变得尤为关键。

为了检查云存储外包数据的完整性，Ateniese等人[7]首次提出数据可持有性验证(Provable Data Possession, PDP)审计机制。 Juels 等人[8]提出了数据可恢复证明(Proofs of Retrievability, PoR)审计模型。Wang等人[9]提出了一种具有隐私保护的公共云审计方案，引入第三方审计者为用户完成外包数据的完整性审计任务。最近，许多具有新型安全功能的公共云存储审计方案已陆续被提出[10–13]。特别地，文献[10]利用高效去重技术来支持去重搜索，同时实现了过期用户撤销和云存储数据审计。文献[11]设计出了既能支持数据的动态操作(对云端数据文件进行更新、删除和插入等操作)，又能实现用户任意次数撤销的审计机制。Hahn等人[12]基于同态哈希函数技术实现数据快速动态更新的完整性审计方案。文献[13]将Shamir秘密共享方法和代数签名应用到外包云存储审计之中，并提出了高效撤销群组成员的共享数据审计方案。

然而，以上提出的云存储审计方案主要依赖公钥基础设施(Public Key Infrastructure, PKI)设计的，这将造成对公钥证书复杂的管理，包括公钥证书的创建、分发、存储和撤销，并不适用于移动终端的实际部署环境。而在基于身份密码(Identity-Based Cryptography, IBC)体制之中[14]，用户私钥是由一个可信的权威机构-密钥生成中心(Private Key Generator, PKG)生成，它利用自己的主私钥与用户唯一可识别的身份信息(如身份证号、护照证号、邮件地址、电话号码)来为用户生成私钥，避免了基于证书的公钥密码机制中复杂证书管理问题。在近几年内，许多基于身份的公共云存储审计方案已经提出[15–18]。特别地，Ni等人[15]基于RSA假设，提出了一个基于身份的远程数据完整性验证方案，该方案实现了不同云用户拥有的外包数据完整性的聚合验证，其将身份作为哈希函数的输入生成一长串参数，导致用户的身份隐私不能得到很好的保护，另外其方案在完整性验证阶段的通信开销也很大，随着扇区数的增长而增长。Zhang等人[16]引入了区块链技术，第三方审计者将审计结果记录到以太坊中，从而用户可以检测第三方审计者的恶意行为，但是存储的医疗数据的隐私容易泄露给云服务器。有些用户可能只关注他感兴趣的部分加密云文件的完整性，Gao等人[17]应用了一种关系认证标签技术，它可以用来查询哪些文件包含感兴趣的关键字和生成审计证明信息，但是在交互过程中，TPA容易通过对响应信息进行线性运算获取外包文件的内容，导致隐私泄露。Xue等人[18]基于比特币的公共区块链随机数来生成挑战信息，可以有效抵御恶意审计者，但是用户的身份隐私依然没有得到有效的保护。且以上这些方案在TPA端的

计算开销比较大，且用于验证数据文件完整性的时间与挑战数据块的数量线性相关。5G时代到来，个人数据量爆炸，实际上TPA需要快速地完成用户的审计任务，由于审计请求可能集中在特定的时间段内，因此过长的延迟是不可接受的，这对于TPA的计算能力要求很高。

在保证基于身份的公共云存储审计机制安全性的前提下，扩展系统功能是一项非常有意义的工作。溯源技术就被应用到云存储环境中来实现数字取证和实体追踪功能。一旦系统发生数据不一致导致的纠纷或用户在系统中恶意操作的情况都将是后续追踪调查、划分责任和解决诉讼的第一手证明材料。文献[19]最先将实体溯源的想法应用到基于无线体域网的环境中，利用人体指纹的不可伪造性来安全快速地溯源并识别原始用户。Zhang等人[20]的方案中，单个用户(包括组管理者)无法知道签名者的身份，同时基于秘密共享技术实现了用户的可追溯性。然而，这些方案的计算成本相对较高，而且没有解决复杂的证书管理问题。

针对上述问题，本文设计了一种支持条件身份匿名的外包云存储医疗数据完整性验证方案。该方案基于同态哈希函数技术设计了数字聚合签名算法，进一步构造轻量级完整性验证方案。方案是基于身份的密码系统设计的，有效避免了PKI关于公钥证书的复杂管理。方案使得第三方审计者定期代替医疗用户验证存储在云辅助医疗系统的外包数据的完整性，且能检测出云医疗数据是否被篡改，从而防止医生的临床误诊。性能分析与比较表明方案在计算开销与通信开销方面具有较大优势。特别是在第三方审计者方面，其完整性验证计算开销是轻量级的，非常有利于部署在移动终端计算资源受限的设备环境。

2 预备知识

2.1 双线性对映射

设G_1和G_2分别是两个阶为素数p的乘法循环群，g是G_1的一个生成元，$e:G_1\times G_1\to G_2$是满足以下条件的双线性对映射。

(1) 双线性。对于任意的$a,b\in Z_p^*$，有$e\left(g^a,g^b\right)=e(g,g)^{ab}$。

(2) 非退化性。$e(g,g)\neq 1$，其中1是G_2的单位元。

(3) 可计算性。对于群G_1的任意两个元素h_1,h_2，存在一个高效的算法计算$e(h_1,h_2)$。

2.2 同态哈希函数

H是一个同态哈希函数，它满足如下性质。

(1) 同态性。对于两个消息m_1,m_2和标量k_1,k_2，有$H(k_1m_1+k_2m_2)=H(m_1)^{k_1}\cdot H(m_2)^{k_2}$。

(2) 抗碰撞性。不存在多项式时间敌手能够伪造元组(m_1,m_2,m_3,k_1,k_2)，使之能同时满足$m_3=k_1m_1+k_2m_2$和$H(m_3)=H(m_1)^{k_1}\cdot H(m_2)^{k_2}$。

2.3 密码学困难问题

定义1 DL(Discrete Logarithm)问题：给定$g,g^a\in G_1$，其中$a\in Z_p^*$是未知的，DL问题求解目标是计算a。

定义2 CDH(Computational Diffie-Hellman)问题：给定$g,g^a,g^b\in G_1$，其中$a,b\in Z_p^*$是未知的，CDH问题求解目标是计算g^{ab}。

事实上，敌手在多项式时间内能够求解DL困难问题和CDH困难问题的概率是可以忽略的。

2.4 系统模型

支持条件身份匿名的云存储医疗数据完整性验证模型如图1所示，包含密钥生成中心(Private Key Generator, PKG)、用户、医院、云服务器和第三方审计者(Third Party Auditor, TPA)。各通信实体的功能介绍如下：

(1) PKG。PKG是一个权威且完全可信的实体，主要负责系统初始化阶段公开参数设置，以及根据用户真实身份生成相应的匿名身份和公私钥对。

(2) 医院。为用户提供医疗服务，利用无线医疗传感器网络收集用户的健康数据，生成用户的医疗数据文件。

(3) 用户。根据医疗数据文件生成相应的数字签名和审计辅助信息(Auditing Auxiliary Information, AAI)，将医疗数据文件和数字签名上传给云服务器，将AAI上传给TPA。最后，用户删除本地存储。

(4) 云服务器。拥有巨大存储容量和计算能力，根据用户需求存储用户的医疗数据以及相应的数字签名，接受来自TPA的完整性验证挑战，并返回完整性验证证明响应信息给TPA。

(5) TPA。TPA得到用户的授权并且能够代表医疗用户周期性验证存储在云服务器的健康医疗数

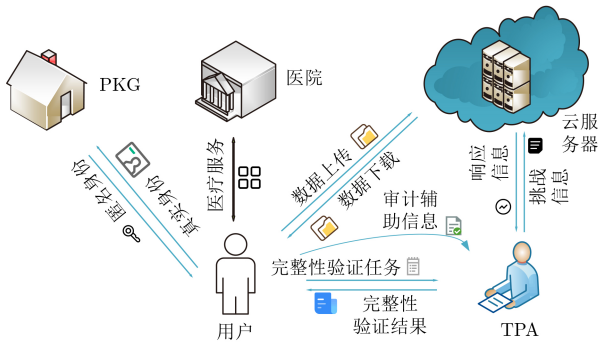

图 1 条件身份匿名的云存储医疗数据完整性验证模型

据的完整性，定期与云服务器交互以执行完整性审计任务，并将完整性验证结果返回给用户。

支持条件身份匿名的云存储医疗数据完整性验证模型包含以下多项式算法：

(1)系统初始化。由PKG执行。系统初始化，输入安全参数，生成系统公共参数并公开。

(2)用户匿名身份和签名私钥生成。由PKG执行。输入用户真实身份，PKG生成用户的匿名身份以及签名私钥，并将其通过安全信道发送给用户。

(3)数字签名生成。由用户执行。用户对数据分块后使用签名算法对数据进行签名，将数据和签名发送给云服务器，将审计辅助信息发送给TPA，最后删除本地存储。

(4)挑战信息生成。由TPA执行。TPA生成挑战信息并发送给云服务器，在等待云服务器响应证明信的时间内，执行预计算操作。

(5)完整性验证证明响应信息生成。由云服务器执行。云服务器根据挑战信息定位相关的数据块和签名，生成完整性验证证明响应信息，并将其发送给TPA。

(6)完整性验证。由TPA执行。输入挑战信息、系统参数、预计算值、用户匿名身份和完整验证证明信息，生成计算结果并通知用户。

3　支持条件身份匿名的外包云存储医疗数据完整性验证方案

3.1　具体方案

本文提出一个支持条件身份匿名的外包云存储医疗数据完整性验证方案，方案包括系统初始化、用户匿名身份和签名私钥生成、数字签名生成、挑战信息生成、完整性验证证明响应信息生成、完整性验证6个阶段。具体工作流程如图2所示。

(1)系统初始化。输入安全参数ζ，PKG执行如下步骤：

(a)PKG设置一个双线性对映射$e: G_1 \times G_1 \to G_2$，其中$G_1$和$G_2$是具有相同阶为素数$p$的乘法循环群，$g$是$G_1$的生成元。

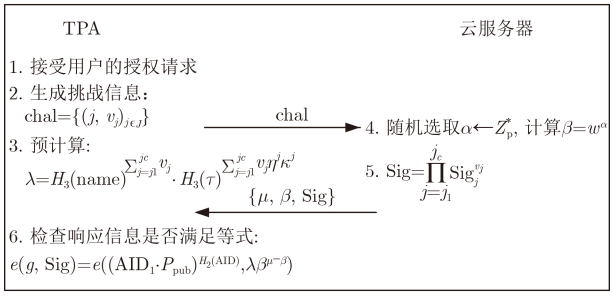

图 2 条件身份匿名的云存储医疗数据完整性验证工作流程

(b)PKG随机选取$s \leftarrow Z_p^*$作为主私钥，计算$p_{\text{pub}} = g^s$作为PKG的主公钥。PKG随机均匀地选取元素$w \leftarrow G_1$。

(c)PKG设置两个安全且抗碰撞的通用哈希函数 $H_1: G_1 \times G_1 \times \{0,1\}^* \to \{0,1\}^\rho$，$H_2: G_1 \times \{0,1\}^\rho \to Z_p{}^*$。同时，PKG设置一个同态哈希函数$H_3: Z_p \to G_1$。

最后，PKG公布系统公开参数$\text{Para} = (e, G_1, G_2, g, p, p_{\text{pub}}, w, H_1, H_2, H_3)$，PKG秘密安全地保存主私钥$s$。

(2)用户匿名身份和签名私钥生成。根据医疗用户真实身份$\text{RID} \in \{0,1\}^\rho$和登录口令PWD，PKG为用户产生匿名身份，以及相对应的签名私钥：

(a)PKG随机均匀地选取$r \leftarrow Z_p^*$，并使用主私钥s为用户产生匿名身份信息$\text{AID} = (\text{AID}_1, \text{AID}_2)$，其中$\text{AID}_1 = g^r$，$\text{AID}_2 = \text{RID} \oplus H_1(\text{AID}_1{}^s || p_{\text{pub}} || T)$，$T$为一个用户匿名的有效使用周期。

(b)PKG使用主私钥s计算匿名身份AID对应的签名私钥$\text{SK}_{\text{AID}} = (r+s)H_2(\text{AID})$。

最后，PKG 通过安全信道返回$\{\text{AID}, \text{SK}_{\text{AID}}, T\}$给相应的医疗用户。

(3)数字签名生成。医疗用户根据医疗健康数据文件生成如下数字签名，并产生完整性验证辅助信息：

(a)将医疗健康数据文件F(文件名为$\text{name} \in Z_p^*$)分块预处理成$F = \{m_1, m_2, \cdots, m_n\}$，$m_i \in Z_p^* (i = 1, 2, \cdots, n)$。

(b)随机均匀地选取$\eta, \kappa, \tau \leftarrow Z_p$，计算种子信息$\psi_1 = \eta.\kappa.\tau$，$\psi_2 = \eta^2.\kappa^2.\tau$，$\cdots$，$\psi_n = \eta^n.\kappa^n.\tau$，以及完整性验证辅助信息$\text{AAI} = \{\eta, \kappa, \tau, H_3(\psi_1), \cdots, H_3(\psi_n)\}$。

(c)利用签名私钥SK_{AID}计算每个医疗数据块$m_i (i = 1, 2, \cdots, n)$的数字签名信息$\text{Sig}_i = (w^{m_i} H_3(\text{name} + \psi_i))^{\text{SK}_{\text{AID}}}$。

最后，医疗用户通过无线医疗传感器网络将$(\{m_i\}_{1 \le i \le n}, \{\text{Sig}_i\}_{1 \le i \le n})$上传到云服务器，通过安全信道将AAI发送给TPA保存，并在本地端删除副本。

(4)挑战信息生成。当收到医疗用户授权TPA验证存储在云服务器的外包医疗数据完整性的请求时，TPA生成挑战信息并发送给云服务器：

(a)TPA首先从集合$\{1, 2, \cdots, n\}$中随机性地选取一个包含c个元素的子集$J = \{j_1, j_2, \cdots, j_c\}$，并为每一个$j \in J$匹配随机系数$v_j \leftarrow Z_p$，发送挑战信息$\text{chal} = \{(j, v_j)_{j \in J}\}$给云服务器。

(b)在等待云服务器响应期间，TPA基于完整性验证辅助信息$\text{AAI} = \{\eta, \kappa, \tau, H_3(\psi_1), \cdots, H_3(\psi_n)\}$执行预计算：

$\lambda = H_3(\text{name})^{\sum_{j=j_1}^{j_c} v_j} \cdot H_3(\tau)^{\sum_{j=j_1}^{j_c} v_j \eta^j \kappa^j}$

(5)完整性验证证明响应信息生成。云服务器基于挑战信息$\text{chal} = \{(j, v_j)_{j\in J}\}$生成完整性验证证明响应信息。

(a)随机选取$\alpha \leftarrow Z_p^*$，计算$\beta = w^\alpha$，以及组合医疗数据块：$\mu = \alpha^{-1} \sum_{j=j_1}^{j_c} v_j m_j + \beta$。

(b)计算聚合签名$\text{Sig} = \prod_{j=j_1}^{j_c} \text{Sig}_j{}^{v_j}$。

最后，TPA发送完整性验证证明响应信息$\{\mu, \beta, \text{Sig}\}$给云服务器。

(6)完整性验证。当收到来自云服务器返回的完整性验证证明响应信息$\{\mu, \beta, \text{Sig}\}$，TPA利用预计算值$\lambda$判断完整性验证方程$e(g, \text{Sig}) = e((\text{AID}_1 \cdot p_{\text{pub}})^{H_2(\text{AID})}, \lambda\beta^{\mu-\beta})$是否成立。若成立，则说明医疗用户存储在云服务器上的医疗数据是完整的。反之，则医疗数据是不完整的。

3.2 方案正确性证明

现在对医疗健康数据完整性验证方程的正确性进行详细推导为

$$
\begin{aligned}
e(g,\text{Sig}) =& e\left(g, \prod_{j=j_1}^{j_c} \text{Sig}_j{}^{v_j}\right)\\
=& e\left(g, \prod_{j=j_1}^{j_c} ((w^{m_j} \cdot H_3(\text{name}+\psi_j))^{\text{SK}_{\text{AID}}})^{v_j}\right)\\
=& e\left(g^{\text{SK}_{\text{AID}}}, \prod_{j=j_1}^{j_c} (w^{m_j v_j} \cdot H_3(\text{name})^{v_j} H_3(\psi_j)^{v_j})\right)\\
=& e\left(\text{AID}_1{}^{H_2(\text{AID})}.p_{\text{pub}}{}^{H_2(\text{AID})}, w^{\sum_{j\in J} v_j m_j} \cdot \prod_{j=j_1}^{j_c} H_3(\text{name})^{v_j} \cdot \prod_{j=j_1}^{j_c} H_3(\psi_j)^{v_j}\right)\\
=& e\left(\text{AID}_1{}^{H_2(\text{AID})}.p_{\text{pub}}{}^{H_2(\text{AID})}, w^{\alpha(\mu-\beta)} \cdot H_3(\text{name})^{\sum_{j\in J} v_j} \cdot \prod_{j=j_1}^{j_c} H_3(\psi_j)^{v_j}\right)\\
=& e\left((\text{AID}_1 \cdot p_{\text{pub}})^{H_2(\text{AID})}, w^{\alpha(\mu-\beta)} \cdot H_3(\text{name})^{\sum_{j\in J} v_j} \cdot H_3(\eta^{j_1}\kappa^{j_1}\tau)^{v_{j_1}} \cdot \cdots \cdot H_3(\eta^{j_c}\kappa^{j_c}\tau)^{v_{j_c}}\right)\\
=& e\left((\text{AID}_1 \cdot p_{\text{pub}})^{H_2(\text{AID})}, \beta^{\mu-\beta} \cdot H_3(\text{name})^{\sum_{j\in J} v_j} \cdot H_3(\tau)^{\sum_{j=j_1}^{j_c} v_j \eta^j \kappa^j}\right)\\
=& e\left((\text{AID}_1 \cdot p_{\text{pub}})^{H_2(\text{AID})}, \lambda\beta^{\mu-\beta}\right)
\end{aligned}
$$

证毕

3.3 多文件批量完整性验证

支持条件身份匿名的外包云存储医疗数据完整性验证方案可以使得TPA对医疗用户的多个医疗数据文件同时进行批量验证，具体拓展细节描述如下：

医疗用户另外选定3个随机系数$\gamma, \upsilon, \theta \leftarrow Z_p$，这里假设用户有$d$份医疗文件需要外包存储在云服务器，它们的文件名分别是$\{\text{name}_1, \text{name}_2, \cdots, \text{name}_d\}$。对于每一个$\ell \in \{1,2,\cdots,d\}$，$\text{name}_\ell = \gamma^\ell \upsilon^\ell \theta$，每一份文件由$n$个数据块组成，如：$F_\ell = \{m_{\ell_1}, m_{\ell_2}, \cdots, m_{\ell_n}\}$。数据文件$F_\ell$对应的种子信息集合为$\{\psi_{\ell_i}\}_{1\le i\le n}$，对于$i = 1, 2, \cdots, n$，$\psi_{\ell_i} = \eta^{\ell\cdot i}\kappa^{\ell\cdot i}\tau^{\ell\cdot i}$。$F_\ell$对应的签名集合是$\{\text{Sig}_{\ell_1}, \text{Sig}_{\ell_2}, \cdots, \text{Sig}_{\ell_n}\}$，对于$i = 1, 2, \cdots, n$，$\text{Sig}_{\ell_i} = (w^{m_{\ell_i}} H_3(\text{name}_\ell + \psi_{\ell_i}))^{\text{SK}_{\text{AID}}}$。

在挑战信息生成阶段，TPA在生成挑战信息$\text{chal} = \{(j, v_j)_{j\in J}\}$并发送给云服务器之后，计算预计算值

$$\lambda\prime = H_3(\theta)^{\sum_{\ell=1}^{d}\sum_{j=j_1}^{j_c} \gamma^{\ell\cdot j}\cdot\upsilon^{\ell\cdot j}\cdot v_j} \cdot H_3(\tau)^{\sum_{\ell=1}^{d}\sum_{j=j_1}^{j_c} \eta^{\ell\cdot j}\cdot\kappa^{\ell\cdot j}\cdot v_j}$$

在完整性验证证明响应信息产生阶段，在收到挑战信息后，云服务器随机选取$\alpha\prime \leftarrow Z_p^*$，计算$\beta\prime = w^{\alpha\prime}$，组合数据块$\mu\prime = (\alpha\prime)^{-1} \sum_{\ell=1}^{d} \sum_{j=j_1}^{j_c} v_j m_{\ell_j} + \beta\prime$以及聚合签名$\text{Sig}\prime = \prod_{\ell=1}^{d} \prod_{j=j_1}^{j_c} \text{Sig}_{\ell_j}^{v_j}$。最后云服务器发送完整性验证证明响应信息$\{\mu\prime, \beta\prime, \text{Sig}\prime\}$给TPA。

在完整性验证阶段，TPA使用预计算值$\lambda\prime$来验证方程$e(g, \text{Sig}\prime) = e((\text{AID}_1 \cdot p_{\text{pub}})^{H_2(\text{AID})}, \lambda\prime(\beta\prime)^{\mu\prime-\beta\prime})$是否成立。如果等式成立，则表明医疗用户存储在远端云服务器上的d份医疗数据文件是完整的。反之，则不完整。

多文件批量完整性验证过程的正确性证明为

$$
\begin{aligned}
e(g,\mathrm{Sig}\prime) =& e\left(g,\prod_{\ell=1}^{d}\prod_{j=j_1}^{j_c}\mathrm{Sig}_{\ell_j}^{v_j}\right)\\
=& e\left(g,\prod_{\ell=1}^{d}\prod_{j=j_1}^{j_c}\left(\left(w^{m_{\ell_j}}H_3(\mathrm{name}_\ell+\psi_{\ell_j})\right)^{\mathrm{SK_{AID}}}\right)^{v_j}\right)\\
=& e\left(g^{\mathrm{SK_{AID}}},\prod_{\ell=1}^{d}\prod_{j=j_1}^{j_c}\left(w^{m_{\ell_j}}H_3(\mathrm{name}_\ell+\psi_{\ell_j})\right)^{v_j}\right)\\
=& e\left(g^{\mathrm{SK_{AID}}},\prod_{\ell=1}^{d}\prod_{j=j_1}^{j_c}w^{m_{\ell_j}\cdot v_j}\cdot\prod_{\ell=1}^{d}\prod_{j=j_1}^{j_c}H_3(\mathrm{name}_\ell+\psi_{\ell_j})^{v_j}\right)\\
=& e\left(g^{\mathrm{SK_{AID}}},w^{\sum_{\ell=1}^{d}\sum_{j=j_1}^{j_c}v_jm_{\ell_j}}\cdot\prod_{\ell=1}^{d}\prod_{j=j_1}^{j_c}H_3(\mathrm{name}_\ell)^{v_j}\cdot\prod_{\ell=1}^{d}\prod_{j=j_1}^{j_c}H_3(\psi_{\ell_j})^{v_j}\right)\\
=& e\left((\mathrm{AID}_1\cdot p_{\mathrm{pub}})^{H_2(\mathrm{AID})},w^{\alpha\prime(\mu\prime-\beta\prime)}\cdot H_3(\theta)^{\sum_{\ell=1}^{d}\sum_{j=j_1}^{j_c}\gamma^{\ell}\cdot\upsilon^{\ell}\cdot v_j}\cdot H_3(\tau)^{\sum_{\ell=1}^{d}\sum_{j=j_1}^{j_c}\eta^{\ell\cdot j}\cdot\kappa^{\ell\cdot j}\cdot v_j}\right)\\
=& e\left((\mathrm{AID}_1\cdot p_{\mathrm{pub}})^{H_2(\mathrm{AID})},\lambda\prime(\beta\prime)^{\mu\prime-\beta\prime}\right)
\end{aligned}
$$

证毕

通过以上多文件批量完整性验证过程得知，TPA所需的验证计算开销与单个数据文件的计算开销几乎相同，与数据文件的个数没有关系，这是源于方案设计中用到同态哈希函数技术，使得TPA在生成挑战信息时，做了相关的预计算。因此本方案在TPA端的开销是轻量级的。

4　安全性分析

现在，本文给出支持条件身份匿名的外包云存储医疗数据完整性验证方案的安全性分析，包括存储正确性，用户的条件身份隐私保护，以及防止TPA的数据恢复攻击。

定理1　在概率多项式时间内，方案中的云服务器试图产生伪造的完整性验证证明响应信息，通过TPA的验证在计算上是不可行的。

证明　TPA随机地生成一个完整性验证挑战信息$\{(j,v_j)_{j\in J}\}$，并通过无线医疗传感器网络发送给云服务器。云服务器返回给TPA一个有效的完整性验证证明响应信息$\{\mu,\beta,\mathrm{Sig}\}$，其应该通过验证方程：$e(g,\mathrm{Sig})=e((\mathrm{AID}_1\cdot p_{\mathrm{pub}})^{H_2(\mathrm{AID})},\lambda\beta^{\mu-\beta})$。

在真实情况下，云服务器可能通过篡改或者替换部分数据，伪造数字签名等方式产生伪造的完整性验证证明响应信息通过TPA的验证。首先，如果云服务器伪造某一个数字签名Sig_i为$\mathrm{Sig}_i\prime$，导致聚合签名$\mathrm{Sig}\neq\mathrm{Sig}\prime$，这样$e(g,\mathrm{Sig}\prime)=e((\mathrm{AID}_1\cdot p_{\mathrm{pub}})^{H_2(\mathrm{AID})},\lambda\beta^{\mu-\beta})$是不满足的。

现在假设恶意云服务器至少通过篡改或者替换某个数据块m_i为$m_i\prime$，这样恶意云服务器产生伪造的完整性验证证明响应信息$\{\mu\prime,\beta,\mathrm{Sig}\}$，其中$\mu\prime\neq\mu$，令$\Delta=\mu\prime-\mu$。如果恶意云服务器能够成功伪造完整性验证响应证明信息，则其一定能够通过验证方程：$e(g,\mathrm{Sig})=e((\mathrm{AID}_1\cdot p_{\mathrm{pub}})^{H_2(\mathrm{AID})},\lambda\beta^{\mu\prime-\beta})$。根据以上两个验证方程，可以得到$\beta^{\mu}=\beta^{\mu\prime}$，进而得到$\beta^{\Delta}=1$。因为$G_1$是一个乘法循环群，对于任意两个元素$A,B\in G_1$，存在$\Theta\in Z_p$，使得$A=B^{\Theta}\in G_1$成立。不失一般性，随机生成$A,B\in G_1$，满足$\beta=A^{k_1}\cdot B^{k_2}$，其中$k_1,k_2\in Z_p$。显然，我们可以以$1-1/p$的概率找到DL问题的一个解。具体而言，除了$k_2\cdot\Delta=0$的情况，我们可以得到$A=B^{-k_2\cdot\Delta/k_1\cdot\Delta}$，故$\Theta=-k_2\cdot\Delta/k_1\cdot\Delta$。由于$\Delta\neq0$，$k_1$是$Z_p$中的一个元素，所以$k_1\cdot\Delta\neq0$的概率为$1-1/p$，这样我们就找到DL问题的一个解，这与DL困难问题求解相矛盾。

因此，本方案中的云服务器试图产生伪造的完整性验证证明响应信息，通过TPA的验证在计算上是不可行的。　　证毕

定理2　支持条件身份匿名的外包云存储医疗数据完整性验证方案可确保用户的条件身份隐私性。

证明　首先说明用户身份对外的隐私性。在本方案中，每个医疗用户用以唯一标识真实身份信息的是$\mathrm{RID}\in\{0,1\}^{\rho}$，PKG生成对应的匿名身份：$\mathrm{AID}=(\mathrm{AID}_1,\mathrm{AID}_2)$，其中$\mathrm{AID}_1=g^{r}$，$\mathrm{AID}_1$与$g$是乘法循环群中的元素，在多项式时间内，由于离散对数困难问题，敌手获得了AID_1与g而设法计算出r是可以忽略的。此外，PKG利用主私钥s计算

$\mathrm{AID}_2=\mathrm{RID}\oplus H_1({\mathrm{AID}_1}^s||p_{\mathrm{pub}}||T)$，由于PKG是基于身份密码体制中的权威可信实体，主私钥s是PKG秘密保存的，不能被敌手获取。因此，即使敌手获取到了$\mathrm{AID}_1=g^r$和$p_{\mathrm{pub}}=g^s$，基于CDH困难问题假设，敌手也无法计算出${\mathrm{AID}_1}^s=g^{rs}$，进而不能完全恢复用户的真实身份RID。

其次说明用户身份的条件匿名性。假设系统中存在一个注册成功的恶意用户RID^*，其认为在系统中自己是以匿名身份$\mathrm{AID}=(\mathrm{AID}_1,\mathrm{AID}_2)$存在的。为了获取利益，他可能会在系统中做有关违反数据隐私安全的事情。因此，在医疗环境中需要有一个安全技术来溯源某些恶意用户的真实身份，从而追踪、揭示和撤销系统中恶意用户。本方案设计出了在云辅助无线传感器网络中用户的匿名身份的溯源算法。具体地，根据恶意用户的匿名身份$\mathrm{AID}=(\mathrm{AID}_1,\mathrm{AID}_2)$，PKG利用主私钥$s$来计算出$H_1({\mathrm{AID}_1}^s||p_{\mathrm{pub}}||T)$。PKG可计算出用户的真实身份：$\mathrm{RID}^*=\mathrm{AID}_2\oplus H_1({\mathrm{AID}_1}^s||p_{\mathrm{pub}}||T)$。 证毕

定理3 支持条件身份匿名的外包云存储医疗数据完整性验证方案可防止TPA的数据恢复攻击。

证明 当TPA发送挑战信息给云服务器时，得到云服务器返回的完整性验证证明响应信息$\{\mu,\beta,\mathrm{Sig}\}$。因为$\mu=\alpha^{-1}\sum_{j=j_1}^{j_c}v_jm_j+\beta$，$\alpha^{-1}$是$\alpha$在$Z_p^*$中的逆元，其中$\alpha$是由云服务器随机选择的，又由于$\beta=w^{\alpha}$，基于DL困难问题假设，TPA不能获取$\alpha$，进而不能获取$\sum_{j=j_1}^{j_c}v_jm_j=\alpha(\mu-\beta)$。因此在完整性验证过程中，即便TPA可以求解线性方程组，TPA也无法从完整性验证证明响应信息$\{\mu,\beta,\mathrm{Sig}\}$推导出医疗用户的原始医疗数据块。 证毕

5 性能分析

将本设计方案与相关方案在完整性验证方面进行性能分析与比较，这些方案分别是：RDIC方案[21]，IBPA方案[18]，以及CIPPPA方案[16]。为便于表述：用符号Pair表示双线性对算法运算时间，Exp表示普通模指数运算时间，Mult表示椭圆曲线中的倍点运算运行时间，Add表示椭圆曲线上的加法运算时间，ha表示普通哈希函数运算时间，mult表示普通模乘运行时间，Ha表示哈希函数映射到基于椭圆曲线加法群上的点的运行时间。关于通信开销，本文用$|n|$表示集合$\{1,2,\cdots,n\}$中元素的大小，定义Z_p中元素比特长度为$|p|$；此外，$|G|$是循环群G元素的比特长度，定义零知识证明通信开销的比特长度为$|\mathrm{pf}|$。

本文将4个方案进行实验仿真分析与比较，实验仿真以操作系统为Windows 10，处理器为Intel(R)Core(TM)I5-4210 2.40 GHz，内存为4 GB的主机以及jpbc-2.0.0密码库为实验环境，所有算法的计算开销时间都使用C语言及其版本号为5.6.2密码算法基础函数库MIRACL得出。

在本方案中，由于用户存储了审计辅助信息在TPA端，TPA在发送挑战信息给云服务器之后，在等待云服务器响应的时间内，TPA可以预计算λ，在方案设计中，我们采用了同态哈希函数设计签名，进而将λ的计算复杂性优化为常量，故而λ的计算可以忽略。在进行完整性验证时TPA仅需要2次模指数运算、2次双线性对运算、2次普通模乘运算和1次普通哈希运算，其计算开销为$2\mathrm{Exp}+2\mathrm{Pair}+2\cdot\mathrm{mult}+\mathrm{ha}$，同理经过理论分析可以得到RDIC方案，IBPA方案，以及CIPPPA方案相应的TPA端的计算开销分别为$(2c+6)\cdot\mathrm{Exp}+(c+1)\cdot\mathrm{Pair}+c\cdot\mathrm{mult}$，$(2c+4)\cdot\mathrm{Mult}+3\mathrm{Pair}+(2c-1)\cdot\mathrm{Add}+(c+2)\cdot\mathrm{Ha}+(c+1)\cdot\mathrm{ha}$，以及$(c+2)\cdot\mathrm{Mult}+3\mathrm{Pair}+(c-1)\cdot\mathrm{Add}+c\cdot\mathrm{Ha}+\mathrm{ha}$。这4个方案在完整性验证阶段，TPA端的计算开销的理论比较结果如表1所示。另外，在云服务器响应完整性证明信息给TPA时，完整性证明响应信息通信开销为$2|G|+|p|$，我们也可以分析得到RDIC方案，IBPA方案，以及CIPPPA方案相应的完整性验证证明的通信开销分别为$3|G|$，$3|G|+|p|$，以及$3|G|+|p|$。这4个方案在TPA端产生的挑战信息通信开销、完整性证明响应信息通信开销的理论比较结果如表2所示。在这里图3的实验仿真结果表明了本设计方案比现有的数据完整性验证方案更加轻量级，例如，当挑战数据块的数量为500时，TPA实际上大约只需要0.013 s就可以完成验证任务，而在

表 1 完整性验证计算开销比较

方案	完整性验证计算开销
RDIC	$(2c+6)\cdot\mathrm{Exp}+(c+1)\cdot\mathrm{Pair}+c\cdot\mathrm{mult}$
IBPA	$(2c+4)\cdot\mathrm{Mult}+3\mathrm{Pair}+(2c-1)\cdot\mathrm{Add}+(c+2)\cdot\mathrm{Ha}+(c+1)\cdot\mathrm{ha}$
CIPPPA	$(c+2)\cdot\mathrm{Mult}+3\mathrm{Pair}+(c-1)\cdot\mathrm{Add}+c\cdot\mathrm{Ha}+\mathrm{ha}$
本文	$2\mathrm{Exp}+2\mathrm{Pair}+2\cdot\mathrm{mult}+\mathrm{ha}$

表 2 完整性验证通信开销比较

方案	挑战信息	完整性验证证明信息
RDIC	$c\cdot(\lvert n\rvert+\lvert p\rvert)+\lvert\mathrm{pf}\rvert+2\lvert G\rvert$	$3\lvert G\rvert$
IBPA	$c\cdot(\lvert n\rvert+\lvert p\rvert)$	$3\lvert G\rvert+\lvert p\rvert$
CIPPPA	$c\cdot(\lvert n\rvert+\lvert p\rvert)$	$3\lvert G\rvert+\lvert p\rvert$
本文	$c\cdot(\lvert n\rvert+\lvert p\rvert)$	$2\lvert G\rvert+\lvert p\rvert$

RDIC方案，IBPA方案，以及CIPPPA方案中，TPA分别大约需要3.8963 s, 4.9647 s和1.1098 s。在完整性验证阶段，TPA的验证计算开销几乎常量，不会随着挑战数据块数量的增加而增加。而在其他方案中，TPA的用于验证完整性的时间都随着挑战数据块的数量增加而增加，在挑战数据块的数量很大时，这将非常消耗TPA的计算资源。图4的实验仿真结果表明本设计方案在完整性验证证明信息通信开销方面低于IBPA方案和CIPPPA方案。本设计方案在完整性验证证明信息通信开销方面与RDIC方案一致，但在挑战信息阶段RDIC方案的通信开销显然远远高于其他方案，而且RDIC方案不具备本设计方案的条件匿名安全特性。因此，本设计方案在TPA端具有合理的通信开销，而且根据前面可知，本方案计算开销在随着数据块数量增加时，不会随着数据块数量呈线性增长趋势，拥有更为明显的计算效率优势。因此，从以上性能分析与实验仿真结果可知，本设计方案在TPA的完整性验证过程中，整体上在计算开销与通信开销方面也有较大优势。而且本设计方案同时确保了存储正确性，用户的条件身份隐私保护，以及防止TPA的数据恢复攻击的安全特性，非常有利于本方案在云辅助无线医疗传感器网络环境的安全高效部署。

6　结束语

针对用户身份隐私保护，云存储医疗数据完整性，以及现有完整性验证方案在TPA端计算开销较大等问题，该文提出一种条件身份匿名的外包云存储医疗轻量级数据完整性验证方案。该方案结合同态哈希函数设计了一种基于身份的聚合签名算法，来进行高效安全的完整性验证。方案是基于身份密码系统设计的，有效避免了对公钥证书的复杂管理，同时保证了用户的身份隐私，也结合实体身份溯源技术来对系统中存在的恶意用户进行跟踪、揭示和问责。安全性分析与性能评估结果表明本方案可以安全高效地部署在云辅助无线医疗传感器网络。

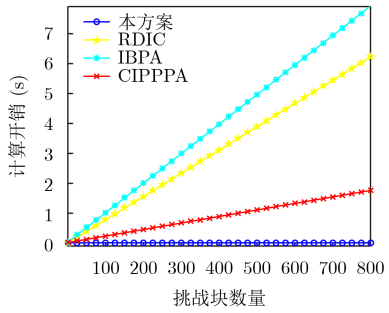

图 3 完整性验证计算开销实验仿真

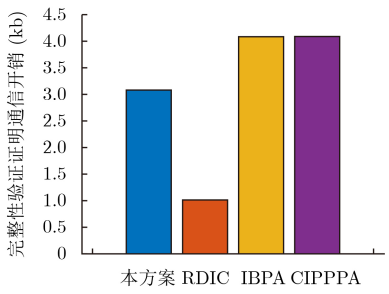

图 4 完整性验证证明通信开销实验仿真

参 考 文 献

[1] BARATI M, AUJLA G S, LLANOS J T, *et al*. Privacy-aware cloud auditing for GDPR compliance verification in online healthcare[J]. *IEEE Transactions on Industrial Informatics*, 2022, 18(7): 4808–4819. doi: 10.1109/TII.2021.3100152.

[2] NAYAK S K and TRIPATHY S. SEPDP: Secure and efficient privacy preserving provable data possession in cloud storage[J]. *IEEE Transactions on Services Computing*, 2021, 14(3): 876–888. doi: 10.1109/TSC.2018.2820713.

[3] LI Hongzhi, HAN Dezhi, and TANG Mingdong. A privacy-preserving storage scheme for logistics data with assistance of blockchain[J]. *IEEE Internet of Things Journal*, 2022, 9(6): 4704–4720. doi: 10.1109/JIOT.2021.3107846.

[4] SUBRAMANI J, MARIA A, RAJASEKARAN A S, *et al*. Lightweight privacy and confidentiality preserving anonymous authentication scheme for WBANs[J]. *IEEE Transactions on Industrial Informatics*, 2022, 18(5): 3484–3491. doi: 10.1109/TII.2021.3097759.

[5] REN Kui, WANG Cong, and WANG Qian. Security challenges for the public cloud[J]. *IEEE Internet Computing*, 2012, 16(1): 69–73. doi: 10.1109/MIC.2012.14.

[6] SUN Jinyuan, FANG Yuguang, and ZHU Xiaoyan. Privacy and emergency response in e-healthcare leveraging wireless body sensor networks[J]. *IEEE Wireless Communications*, 2010, 17(1): 66–73. doi: 10.1109/MWC.2010.5416352.

[7] ATENIESE G, BURNS R, CURTMOLA R, *et al*. Provable data possession at untrusted stores[C]. The 14th ACM Conference on Computer and Communications Security, Alexandria, USA, 2007: 598–609. doi: 10.1145/1315245.1315318.

[8] JUELS A and KALISKI B S. PORs: Proofs of retrievability for large files[C]. The 14th ACM Conference on Computer and Communications Security, Alexandria, USA, 2007: 584–597. doi: 10.1145/1315245.1315317.

[9] WANG Cong, CHOW S S M, WANG Qian, *et al*. Privacy-preserving public auditing for secure cloud storage[J]. *IEEE Transactions on Computers*, 2013, 62(2): 362–375. doi: 10.1109/TC.2011.245.

[10] 马华, 党乾龙, 王剑锋, 等. 基于属性加密的高效密文去重和审计方案[J]. 电子与信息学报, 2019, 41(2): 355–361. doi: 10.

11999/JEIT170935.

MA Hua, DANG Qianlong, WANG Jianfeng, *et al*. Efficient ciphertext deduplication and auditing scheme with attribute-based encryption[J]. *Journal of Electronics & Information Technology*, 2019, 41(2): 355–361. doi: 10.11999/JEIT170935.

[11] YEH L Y, CHIANG P Y, TSAI Y L, *et al*. Cloud-based fine-grained health information access control framework for LightweightIoT devices with dynamic auditing and attribute revocation[J]. *IEEE Transactions on Cloud Computing*, 2018, 6(2): 532–544. doi: 10.1109/TCC.2015.2485199.

[12] HAHN C, KWON H, KIM D, *et al*. Enabling fast public auditing and data dynamics in cloud services[J]. *IEEE Transactions on Services Computing*, 2022, 15(4): 2047–2059. doi: 10.1109/TSC.2020.3030947.

[13] 田俊峰, 井宣. 多方参与高效撤销组成员的共享数据审计方案[J]. 电子与信息学报, 2020, 42(6): 1534–1541. doi: 10.11999/JEIT190468.

TIAN Junfeng and JING Xuan. Shared data auditing scheme for efficient revocation of group members via multi-participation[J]. *Journal of Electronics & Information Technology*, 2020, 42(6): 1534–1541. doi: 10.11999/JEIT190468.

[14] SHAMIR A. Identity-based cryptosystems and signature schemes[C]. Workshop on the Theory and Application of Cryptographic Techniques, Santa Barbara, USA, 1984: 47–53. doi: 10.1007/3-540-39568-7_5.

[15] NI Jianbing, ZHANG Kuan, YU Yong, *et al*. Identity-based provable data possession from RSA assumption for secure cloud storage[J]. *IEEE Transactions on Dependable and Secure Computing*, 2022, 19(3): 1753–1769. doi: 10.1109/TDSC.2020.3036641.

[16] ZHANG Xiaojun, ZHAO Jie, XU Chunxiang, *et al*. CIPPPA: Conditional identity privacy-preserving public auditing for cloud-based WBANs against malicious auditors[J]. *IEEE Transactions on Cloud Computing*, 2021, 9(4): 1362–1375. doi: 10.1109/TCC.2019.2927219.

[17] GAO Xiang, YU Jia, CHANG Yan, *et al*. Checking only when it is necessary: Enabling integrity auditing based on the keyword with sensitive information privacy for encrypted cloud data[J]. *IEEE Transactions on Dependable and Secure Computing*, 2021, 19(6): 3774–3789. doi: 10.1109/TDSC.2021.3106780..

[18] XUE Jingting, XU Chunxiang, ZHAO Jining, *et al*. Identity-based public auditing for cloud storage systems against malicious auditors via blockchain[J]. *Science China Information Sciences*, 2019, 62(3): 32104. doi: 10.1007/s11432-018-9462-0.

[19] ALI S T, SIVARAMAN V, OSTRY D, *et al*. Securing first-hop data provenance for bodyworn devices using wireless link fingerprints[J]. *IEEE Transactions on Information Forensics and Security*, 2014, 9(12): 2193–2204. doi: 10.1109/TIFS.2014.2357998.

[20] ZHANG Yinghui, ZHANG Tiantian, GUO Rui, *et al*. Traceable dynamic public auditing with identity privacy preserving for cloud storage[J]. *KSII Transactions on Internet and Information Systems*, 2019, 13(11): 5653–5672. doi: 10.3837/tiis.2019.11.021.

[21] YU Yong, AU M H, ATENIESE G, *et al*. Identity-based remote data integrity checking with perfect data privacy preserving for cloud storage[J]. *IEEE Transactions on Information Forensics and Security*, 2017, 12(4): 767–778. doi: 10.1109/TIFS.2016.2615853.

张晓均：男，博士，副教授，研究方向为密码学和信息安全、云计算安全.

王 鑫：男，硕士生，研究方向为密码学与信息安全、云计算安全.

廖文才：男，硕士生，研究方向为密码学与信息安全、云计算安全.

赵 芥：男，硕士生，研究方向为密码学与信息安全、云计算安全.

付兴兵：男，博士，讲师，研究方向为密码学与信息安全、物联网安全.

责任编辑：马秀强