计算机系统应用 ISSN 1003-3254, CODEN CSAOBN
Computer Systems & Applications,2022,31(3):333−339 [doi: 10.15888/j.cnki.csa.008355]

E-mail: csa@iscas.ac.cn
http://www.c-s-a.org.cn
Tel: +86-10-62661041

高效可撤销的共享数据云存储审计①

仪张倩, 温琳雅, 张维鑫

(长安大学 信息工程学院, 西安 710064)
通信作者: 仪张倩, E-mail: 215214376@qq.com

摘　要: 共享数据的云存储审计是指对群用户共享的云数据的完整性进行审计. 由于在共享数据云存储审计中, 用户可能因各种原因加入和离开用户群, 因此这种方案通常支持群用户撤销. 在大多数现存的共享数据云审计方案中, 用户撤销的计算开销与用户群要上传的文件块总数成线性关系, 造成很大的计算和通信代价, 如何减少用户撤销产生的计算和通信开销成为实现共享云存储审计的关键问题. 然而, 本文在提出了一种高效可撤销的共享数据云存储审计方案, 利用椭圆曲线技术实现了无对认证, 利用中国剩余定理实现了高效的用户撤销, 在保证安全用户撤销的基础上, 极大地减少了共享数据云存储审计方案的通信和计算代价. 此外, 本方案采用基于身份密码学技术, 解决了传统公钥密码学复杂的证书管理问题. 安全性分析和实验结果表明了所提方案的可行性和高效性.

关键词: 数据共享; 用户撤销; 云存储; 完整性审计

引用格式: 仪张倩,温琳雅,张维鑫.高效可撤销的共享数据云存储审计.计算机系统应用,2022,31(3):333–339. http://www.c-s-a.org.cn/1003-3254/8355.html

Efficient and Revocable Cloud Storage Auditing for Shared Big Data

YI Zhang-Qian, WEN Lin-Ya, ZHANG Wei-Xin

(School of Information Engineering, Chang'an University, Xi'an 710064, China)

Abstract: Cloud storage auditing for shared data refers to the integrity auditing of cloud data shared by a group of users. Since users may join or leave user groups for various reasons, it usually supports user revocation. In most existing cloud storage auditing schemes for shared data, the computation cost of user revocation is linearly correlated to the number of file blocks to be uploaded by the user group, which results in high computation and communication costs. How to reduce the computation and communication overhead caused by user revocation has become a key issue for realizing shared cloud storage auditing. Therefore, this study proposes an efficient and revocable cloud storage auditing scheme for shared data, which uses the elliptic curve technology to achieve unpaired authentication and the Chinese remainder theorem to attain efficient user revocation. On the basis of ensuring safe user revocation, this scheme greatly reduces communication and computation costs. In addition, it uses identity-based cryptography technology to solve the complex certificate management problem of traditional public key cryptography. The safety analysis and experimental results show that the proposed scheme is both feasible and efficient.

Key words: data sharing; user revocation; cloud storage; integrity auditing

近年来, 云计算[1] 作为一种新的计算模型, 吸引了人们的广泛关注. 云存储作为云计算的重要组成部分, 已经被人们以极大优势频繁地用于存储数据. 比如, 数据所有者不再需要处理大量的数据, 无论数据使用者所处何地, 查阅资料都很方便. 由于云存储有很多优势, 越来越多的用户选择将他们的数据存储在知名的云服

① 收稿时间: 2021-05-07; 修改时间: 2021-06-08; 采用时间: 2021-06-21; csa 在线出版时间: 2022-01-24

务器 (CSP) 上. 例如, 大家所熟知的谷歌、微软等大型网络公司均有云存储的服务; 在国内, 百度云和微云则是市场占有量最大的存储云. 此外, 通过 CSP 提供的数据存储和共享服务, 使人们可以很轻松地进行团队合作. 更具体地说, 一旦用户在云端创建了共享数据, 用户群内的每个用户不仅可以访问和修改共享数据, 还可以与群内其他人共享最新版本的数据. 虽然数据存储和共享服务使数据所有者可以方便地访问、修改和共享用户群内的数据, 以致用户从这种数据管理方式中受益匪浅, 但是数据外包到云上进行存储的方式也引发了严重的安全问题. 首先, 一旦用户数据被外包到 CSP 上, 用户失去了对数据的直接控制权[2], 这使得用户担心 CSP 是否正确地存储了用户数据. 例如, CSP 可能由于软件或者硬件故障[3,4] 遭受内部敌手或者外部敌手的攻击. 其次, 恶意的 CSP 可能删除极少被访问的数据以节省存储空间或者掩盖数据被损坏的事实以维持自身的良好声誉. 因此, 如何保证用户外包数据的完整性[5–8] 是至关重要的问题之一.

为了解决数据完整性问题, 一些基于传统密码学的公开审计方案[5,9,10] 被提出. 其中, 用户的公、私钥是通过数字证书发放, 通信效率低, 计算量大, 证书的管理成本高. 为了解决复杂的证书管理问题, Shamir 等人[11] 引入基于身份的密码体制概念. 在基于身份的密码体制中, 用已知的身份信息作为公钥, 来避免使用公钥证书. 之后, 基于身份的可证明数据拥有方案[12–18] 被提出, 但是这些方案[12–18] 大多利用双线性对技术和映射到点的哈希函数来实现完整性认证, 需要昂贵的时间和通信成本, 造成很大的计算和存储负担.

为了在实现数据共享服务的同时, 高效实现用户可撤销, 本文提出了一种高效的隐私保护可证明数据拥有方案. 首先, 所提方案采用基于椭圆曲线密码学[19,20] 实现了无对认证, 并且不使用映射到点的哈希函数, 极大地减少了通信和计算代价[21,22]. 其次, 所提方案采用中国剩余定理[23] 实现了高效安全的用户撤销[24,25], 在实现隐私保护的同时, 保证方案的高效性. 最后, 在设定的实验模型下, 给出了所提方案的计算和通信成本分析, 证明所提方案的效率高于已知方案[15–17].

1 背景知识

1.1 椭圆曲线

椭圆曲线密码学的概念是由 Miller[19] 和 Koblitz[20] 基于椭圆曲线提出. 定义F_p是阶为素数p的有限域, 则F_p上的椭圆曲线E上所有的点(x,y)满足等式$y^2 = x^3 + a\cdot x + b \bmod p$, 其中$4a^3 + 27b^2 \neq 0$且$a,b \in F_p$. 椭圆曲线$E$上的无穷远点$O$与其他点构成一个循环加法群$\mathbb{G}$, 群$\mathbb{G}$的阶为$q$, $\mathbb{G}$生成元为P. 群$\mathbb{G}$上的标量乘法是$\theta P = P + P + \cdots + P(\theta\ times)$, 这里$\theta \in \mathbb{Z}_q^*$.

1.2 中国剩余定理

中国剩余定理[23] 是一种古老的求解相同余数的方法, 它是数论中的重要定理. 设定$k_1, k_2, \cdots, k_n$互为素数, 计算$M = \prod_{i=1}^{n} k_i$, $M_i = \frac{M}{k_i}(i = 1,2,\cdots,n)$, 以及$\beta_i$满足$M_i \times \beta_i \equiv 1 \bmod k_i$. 对于整数$var_1, var_2, \cdots, var_n$, 计算$\alpha = \sum_{i=1}^{n} var_i \cdot M_i \cdot \beta_i \bmod M$, 以下方程组成立:

$$\begin{cases} \alpha = var_1 \bmod k_1 \\ \alpha = var_2 \bmod k_2 \\ \quad\vdots \\ \alpha = var_n \bmod k_n \end{cases}$$

1.3 困难问题及假设

(1) 椭圆曲线离散对数问题 (ECDL 问题): 假定$\mathbb{G}$是一个加法群, P是$\mathbb{G}$的生成元, 给定元组$(P, a\cdot P \in \mathbb{G})$, 这里$a \in \mathbb{Z}_q^*$且未知, ECDL 问题是计算$a \in \mathbb{Z}_q^*$.

(2) 椭圆曲线离散对数 (ECDL 假设) : 任何概率多项式时间算法都不能以不可忽略的概率解决 ECDL 问题.

(3) 计算性 Diffie-Hellman 问题 (CDH 问题): 假定$\mathbb{G}_1$是一个循环加法群, P是$\mathbb{G}_1$的生成元. 给定元组$(P, a\cdot P, b\cdot P \in \mathbb{G}_1)$, 这里$a,b \in \mathbb{Z}_q^*$未知, CDH 问题就是计算$a\cdot b\cdot P$.

(4) 计算性 Diffie-Hellman 假设 (CDH 假设): 概率多项式时间算法都不能以不可忽略的概率解决 CDH 问题.

1.4 系统模型

所提方案的系统模型图, 如图 1 所示. 其中, 共有 5 个参与者, 包括密钥生成中心 (KGC), 车辆用户 (U_i $(i = 1,2,\cdots,n)$), 路边单元 (RSU), 第三方审计者 (TPA) 和云服务器 (CSP).

(1) RSU: 路边单元, 是具有足够计算能力的雾设备, 可以及时处理每个车辆用户的传感器产生的信息, 并将其上传到 CSP. 在本文中看作车辆用户群的群管理者 GM, 后续内容不再赘述.

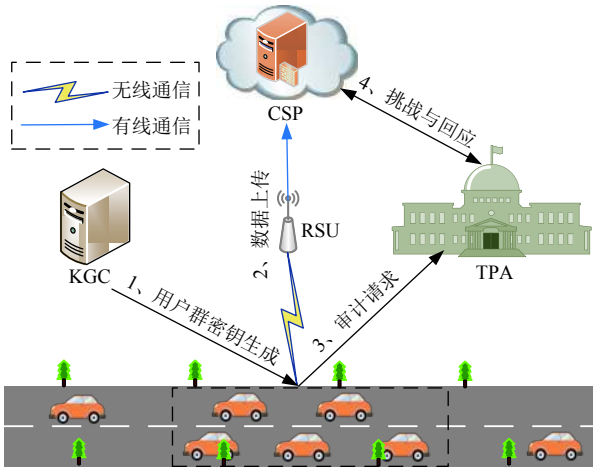

图 1 系统模型图

(2) U_i $(i=1,2,\cdots,n)$: 车辆用户. n个车辆用户U_i组成一个车辆用户群, 由群管理者 GM (即 RSU) 为其分发私钥和上传数据. 每个车辆用户U_i都可以通过云储存与其他用户共享数据. 离开的用户不能上传数据或者通过云存储访问共享数据.

(3) KGC: 密钥生成中心, 是一个完全可信的参与者, 具有强大的计算和存储能力, 负责初始化整个系统以生成主密钥和公共参数, 并且为用户群生成和分配群私钥.

(4) CSP: 云服务器, 是一个半可信实体, 具有强大存储空间和计算能力. 云服务器在接收到第三方审计者发来的审计请求时, 为第三方审计者生成相应的审计证据. 所有数据都存储在云服务器中, 所有的用户通过云服务器实现数据共享服务.

(5) TPA: 第三方审计者, 作为一个半可信的实体, 接受用户群的审计委托, 向云服务器发送审计询问, 并根据云服务器返回的证据确定共享数据是否完整存储在云服务器中.

1.5 安全需求

作为一个基于身份的共享数据云存储审计方案, 需要满足下面的安全需求:

公开审计: TPA 能够代表用户认证 CSP 中存储的数据的完整性.

存储正确性: 如果用户, TPA 和 CSP 都是诚实的, 并且正确地执行了指定的算法, 那么 CSP 生成的证据能够通过 TPA 的完整性认证.

安全用户撤销: 确保被撤销的用户无法像 CSP 上传数据和数据标签.

数据隐私保护: TPA 在审计阶段不能获得 CSP 中存储的任何数据.

2 本文方案

方案由 7 个算法组成, 包括系统建立算法, 密钥生成算法, 标签生成算法, 挑战生成算法, 证据生成算法, 证据认证算法, 和用户撤销算法.

2.1 系统建立算法

由 KGC 执行, 输入安全参数ξ, 输出系统参数$params$和主密钥msk.

(1) 给定一个安全参数ξ, 基于定义在有限域F_p上的椭圆曲线 E, 选择一个阶为q的群$\mathbb{G}$, 并且群$\mathbb{G}$的生成元为P.

(2) 随机选择$s\in\mathbb{Z}_q^*$, 计算$P_{pub}=s\cdot P$.

(3) 选择密码学安全的哈希函数: $h_1:\{0,1\}^*\to\mathbb{Z}_q^*$, $h_2:\{0,1\}^*\to\mathbb{Z}_q^*$.

KGC 保存主密钥$msk=s$, 公开系统参数$params=\{q,P,\mathbb{G},P_{pub},h_1,h_2,\psi,\pi\}$.

2.2 密钥生成算法

由 KGC, 群管理者 GM 和合法的车辆群用户 U_i $(i=1,2,\cdots,n)$执行:

(1) 在接收到 GM 的身份ID后, KGC 随机选择$r_{ID}\in\mathbb{Z}_q^*$, 计算$R_{ID}=r_{ID}\cdot P$, $sk_{ID}=r_{ID}+s\cdot h_1(R_{ID}\|ID)$. KGC 设置$(sk_{ID},R_{ID})$为身份密钥, 并将其发送给 GM.

(2) GM 接收到(sk_{ID},R_{ID})之后, 认证等式$sk_{ID}\cdot P=R_{ID}+P_{pub}\cdot h(R_{ID}\|ID)$是否成立. 如果成立, 接受身份私钥$(sk_{ID},R_{ID})$; 否则, 拒绝它.

(3) GM 随机选择$k_i\in\mathbb{Z}_q^*$ $(i=1,2,3,\cdots,n)$, 计算$S=k_1\cdot k_2\cdots k_n$, $x_i=\dfrac{S}{k_i}$ $(i=1,2,3,\cdots,n)$, 计算y_i以满足$x_i\times y_i\equiv 1 \bmod k_i$, 并计算$w=\sum_{i=1}^{n}w_i=\sum_{i=1}^{n}x_i\times y_i$.

(4) GM 随机选择$sk_{GM}\in\mathbb{Z}_q^*$作为n个用户的部分私钥, 计算$pk_{GM}=sk_{GM}\cdot P$. GM 计算车辆群用户私钥$sk=sk_{ID}+sk_{GM}$和$W=sk\cdot w=sk\cdot\sum_{i=1}^{n}x_i\cdot y_i$, 并将$k_i(i=1,2,\cdots,n)$以秘密信道发送给每个车辆群用户$U_i$, 将$W\|Sig_{msk}(W)$以公开信道发送给每个合法的车辆群用户$U_i$.

(5) 每个U_i接收到$W\|Sig_{msk}(W)$之后, 认证$Sig_{msk}(W)$的有效性. 如果认证失败, U_i回复“拒绝”, 算法终止; 否则, 合法的群用户U_i可以分解出W, 并计算$W \bmod k_i=sk$,

得到群私钥sk.

2.3 标签生成算法

给定原始文件F, U_i执行:

(1) 将原始文件F分为n个块, 得到$F=\{m_1,m_2,\cdots,m_n\}$, 且$m_i\in Z_p, i\in\{1,2,\cdots,n\}$.

(2) 对于每个$i\in\{1,2,\cdots,n\}$, 随机选择$r_i\in\mathbb{Z}_q^*$ ($i=1,2,3,\cdots,n$),计算$R_i=r_i\cdot P, \sigma_i=r_i\cdot m_i+sk\cdot h(ID_F\|pk_{GM}\|R_{ID}\|R_i)$, 这里$ID_F$表示文件标识符, i表示文件第i个数据块的索引标识符, pk_{GM}和R_{ID}为用户群公钥.

U_i生成文件标签$\sigma=\{(\sigma_i,R_i)\}_{i\in[1,n]}$, 上传至 CSP.

2.4 挑战生成算法

当收到来自U_i的审计请求之后, 由 TPA 执行:

随机选择$k_1,k_2\in\mathbb{Z}_q^*$, $c\in[1,n]$, 生成挑战消息$chal=\{c,k_1,k_2\}$, 将其发送给 CSP.

2.5 证据生成算法

在接收到来自 TPA 的挑战消息之后, 由 CSP 执行:

(1) 计算$v_j=\psi_{k_1}(j), w_j=\pi_{k_2}(j), 1\leqslant j\leqslant c$, 得到$Q=\{v_j,w_j\}_{1\leqslant j\leqslant c}$.

(2) 计算$a=\sum_{j=1}^{c}w_j\cdot\sigma_{v_j}\cdot P$, $b=\sum_{j=1}^{c}w_i\cdot m_{v_j}\cdot R_{v_j}$, 发送证据$proof=\{a,b\}$给 TPA.

2.6 证据认证算法

给定$proof=\{a,b\}$, 由 TPA 执行:

(1) 对于所有的$j\in Q$, 计算$H(ID_i\|pk\|R_i)$, 认证等式$a=b+\sum_{j\in Q}pk\cdot H(ID_i\|pk\|R_i)$是否成立.

(2) 如果等式成立, 说明 CSP 正确存储了用户的数据, 发送“成功”给U_i; 否则, 发送“失败”给U_i.

2.7 用户撤销算法

当用户群内有用户离开或者由于不合法的行为被撤销时, 由群管理者 GM 和合法群用户执行:

(1) 当用户U_i从用户群$\mathbb{U}$中撤销时, GM 计算$w'=w-w_i$.

(2) GM 选择一个新的部分私钥$sk'_{GM}\in\mathbb{Z}_q^*$, 并计算其对应的公钥$pk'_{GM}=sk'_{GM}\cdot P$, 车辆群用户私钥$sk'=sk_{ID}+sk'_{GM}$和$W=sk'\cdot w'$, 生成更新密钥的消息$W'=sk'\times w'$, 并将其以公开信道发送给每个合法的车辆群用户$U_i$.

(3) 车辆群用户U_i接受到更新密钥的消息$W=sk'\cdot w'$之后, 计算$W'\bmod k_i=sk'$, 即可以得到新的群私钥sk'.

3 方案分析

3.1 方案正确性分析

由所提方案可知, 如果 TPA 和 CSP 都是诚实的, 并且正确地执行了指定的算法, 且$proof=\{a,b\}$满足下列等式成立, 那么所提方案是正确的.

$$\begin{aligned}a&=\sum_{j=1}^{c}w_j\cdot\sigma_{v_j}\cdot P\\&=\sum_{j=1}^{c}w_j\cdot(r_{v_j}\cdot m_{v_j}+sk\cdot H(ID_F\|pk\|R_{v_j}))\cdot P\\&=\sum_{j=1}^{c}w_j\cdot r_{v_j}\cdot m_{v_j}\cdot P+\sum_{j=1}^{c}w_j\cdot sk\cdot H(ID_F\|pk\|R_{v_j})\cdot P\\&=b+pk\cdot\sum_{j=1}^{c}w_j\cdot H(ID_F\|pk\|R_{v_j})\end{aligned}$$

由于等式成立, 因此, 所提方案是正确的.

3.2 方案安全性分析

(1) 公开审计: 所提方案中, TPA 能够代表用户对 CSP 发起审计挑战, 并且可以通过系统公开参数, 用户群的公钥pk和挑战消息$chal=\{c,k_1,k_2\}$, 对来自 CSP 的审计证据的正确性进行认证.

(2) 存储正确性: 通过对方案的正确性分析, 我们得到, 如果用户, TPA 和 CSP 都是诚实的, 并且正确地执行了指定的算法, 那么 CSP 生成的证据能够通过 TPA 的完整性认证.

(3) 安全的用户撤销: 每当有群用户离开, 新的群用户加入和不合法的群用户被撤销时, 都生成新的用户群私钥sk'. 因此, 除了 KGC 和合法的群用户之外, 被撤销的群用户, 没有加入的群用户和不合法的用户不可能得到新生成的私钥的任何消息, 无法上传用户数据和相应的标签.

(4) 数据隐私保护: 在 TPA 对 CSP 进行审计的过程中, TPA 不能从$proof=\{a,b\}$中得到存储在 CSP 中消息的任何内容, 这里$a=\sum_{j=1}^{c}w_j\cdot\sigma_{v_j}\cdot P$, $b=\sum_{j=1}^{c}w_i\cdot m_{v_j}\cdot R_{v_j}$. 首先, TPA 尝试对$b$求解得到数据消息$m_{v_j}$, 但是由于$R_{v_j}=r_{v_j}\cdot P$, 这相当于解 ECDL 问题. 因此, TPA 不能从b中得到有关数据消息m_{v_j}的任何内容. 其次, TPA 尝试对a求解得到数据消息m_{v_j}, 但是由证明得到, 由于我们不能解 ECDL 问题, 因此, 无法得到有关数据消息m_{v_j}的任何内容. 综上所述, 所提方案满足数据隐私保护.

3.3 计算代价分析

为了满足 80 bit 的安全性, 对于现存方案[15–17], 选择双线性对$e:\mathbb{G}_1\times\mathbb{G}_1\to\mathbb{G}_2$, 群$\mathbb{G}_1$的阶为$p$, p是 512 bit 的素数. 对于所提方案, 选择椭圆曲线上的加法群$\mathbb{G}$, 群$\mathbb{G}$的阶为q, q是 160 bit 的素数. 基于 C++ MIRACL Crypto SDK 库[26], 仿真实验在 CPU 为英特尔 i5 (2.53 GHz), 内存为 4 GB 的 64 位 Windows 10 操作系统下进行. 表 1 给出了相关密码操作运行 10 000 次的平均时间. 表 2 给出了已知方案[15–17] 和所提方案计算代价的比较.

表 1 密码运算的运行时间

符号	描述	运行时间 (ms)
T_H	映射到点哈希运算	3.581 9
T_h	普通哈希运算	0.029 4
T_A	$\mathbb{G}_1$下的标量加法运算	0.017 2
T_M	$\mathbb{G}_1$下的标量乘法运算	1.420 2
T_{A-ECC}	ECC下的标量加法运算	0.002 9
T_{M-ECC}	ECC下的标量乘法运算	0.385 1
T_{pair}	双线性对运算	10.309 2
T_a	$\mathbb{Z}_q^*$下的标量加法运算	0.004 4
T_m	$\mathbb{Z}_q^*$下的标量乘法运算	0.004 4

表 2 计算代价对比

方案	标签生成阶段	证据生成阶段	证据认证阶段
文献[15]	$2nT_M+nT_A+nT_H=6.5955n$	$(c+1)T_M+(c-1)T_A=1.4374c+1.2482$	$2T_{\text{pair}}++cT_H+(c+2)T_M+(c+1)T_A=23.476+5.0205c$
文献[16]	$2nT_M+nT_A+nT_H=6.5955n$	$1T_{\text{pair}}+(c+1)T_M+cT_A=11.7294+1.4374c$	$cT_{\text{pair}}+T_M+(c-1)T_A+cT_H=13.9083+1.403c$
文献[17]	$2nT_M+nT_A+nT_H=6.5955n$	$cT_M+(c-1)T_A=1.4374c-0.0172$	$2T_{\text{pair}}+cT_H+(c+3)T_M+(c+3)T_A=24.9306+5.0205c$
本文方案	$2nT_m+nT_a+nT_h=0.0426n$	$(c-1)T_{M-ECC}+(c+1)T_{A-ECC}=0.388c-0.3822$	$T_{M-ECC}+T_{A-ECC}=0.388$

图 2–图 4 分别表示标签生成阶段, 证明生成阶段和证据认证阶段的计算代价比较. 正如图 2–图 4 显示, 所提方案的计算代价明显低于已知方案[15–17]. 并且, 随着文件块数量n的增加, 所提方案的优势更加明显, 具体原因如下. 首先, 由于已知方案[15–17] 的完整性认证是基于双线性对技术, 因此, 已知方案[15–17] 大多使用群$\mathbb{G}_1$下的标量加法运算, 群$\mathbb{G}_1$下的标量乘法运算, 映射到点的哈希函数运算和双线性对运算. 其次, 由于所提方案的完整性认证是基于椭圆曲线技术, 因此, 所提方案大多使用群$\mathbb{Z}_q^*$下的标量加法运算, 群$\mathbb{Z}_q^*$下的标量乘法运算, ECC 下的标量加法运算, ECC 下的标量乘法运算和普通哈希运算. 此外, 由表 1 可得, 群$\mathbb{G}_1$下的标量加法和乘法运算远远大于群$\mathbb{Z}_q^*$和 ECC 下的标量加法和乘法运算, 映射到点的哈希运算远远大于普通哈希运算, 并且双线性对运算花费很大的计算和通信成本. 因此, 所提方案的计算代价明显低于已知方案[15–17].

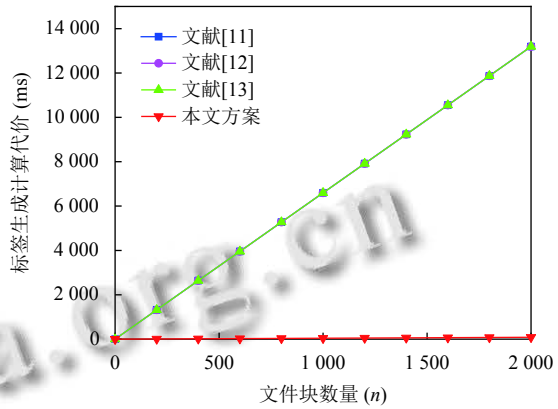

图 2 标签生成的计算代价比较

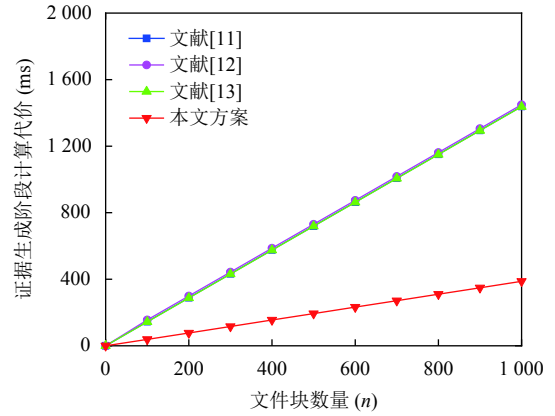

图 3 证据生成的计算代价比较

3.4 通信代价分析

为满足 80 bit 的安全性, $|\mathbb{G}_1|$, $|\mathbb{Z}_q^*|$, $|\mathbb{G}|$, $|n|$分别为 512 bit, 160 bit, 160 bit 和 32 bit. 通信代价主要讨论从 TPA 到 CSP 挑战信息和从 CSP 到 TPA 的响应信息. 表 3 展示了本方案与现存方案[15–17]在通信代价方面的比较.

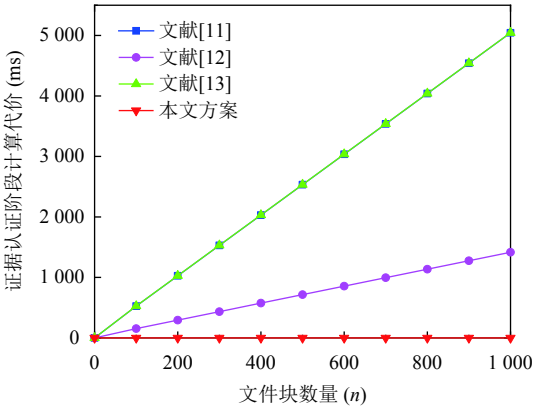

图 4 证据认证的计算代价比较

表 3 通讯数据对比 (bit)

方案	挑战生成	证据生成
文献[15]	$c\|n\|+c\|\mathbb{Z}_q^*\|=192\times c$	$1\|\mathbb{Z}_q^*\|+2\|\mathbb{G}_1\|=1\,184$
文献[16]	$c\|n\|+c\|\mathbb{Z}_q^*\|=192\times c$	$\|\mathbb{Z}_q^*\|+\|\mathbb{G}_1\|=672$
文献[17]	$c\|n\|+c\|\mathbb{Z}_q^*\|=192\times c$	$\|\mathbb{Z}_q^*\|+\|\mathbb{G}_1\|=672$
本文方案	$3\|\mathbb{Z}_q^*\|=480$	$2\|\mathbb{G}\|=320$

如表 3 所示, 首先, 从 TPA 到 CSP, 现存方案[15–17]有相同的192×c bit的通信代价. 显然, 从 TPA 到 CSP, 随着挑战块数量的增加, 现存方案的通信代价线性增加, 而所提方案的通信代价保持不变, 保持480 bit的通信代价. 因此, 在挑战生成阶段, 所提方案的通信代价明显低于已知方案[15–17].

其次, 从 CSP 到 TPA, 现存方案[15–17] 的通信代价都保持不变, 分别为 1 184 bit, 672 bit, 672 bit, 320 bit. 因此, 在证据生成阶段, 所提方案的通信代价明显低于已知方案[15–17].

4 结论与展望

为了解决复杂的证书管理问题, 一些基于身份的可证明数据拥有方案被提出. 但是, 这些方案大都采用昂贵的双线性对运算和映射到点的哈希函数, 具有很大的通信和计算代价. 本文采用椭圆曲线技术和中国剩余定理技术提出了一种高效的隐私保护可证明数据拥有方案, 在保证方案隐私和效率的同时, 实现了高效安全的用户撤销. 安全性分析表明, 所提方案能够满足基于身份的可证明数据拥有方案的安全需求. 计算代价和通信代价的分析表明, 与现存方案[15–17] 相比, 所提方案具有较低的通信和计算代价. 在本文的基础上, 可进一步研究用户如何以更低的代价将数据和标签上传到多个 CSP 上, 以及防止如何进一步防止 CSP 和 TPA 的合谋攻击.

参考文献

1 Armbrust M, Fox A, Griffith R, *et al*. A view of cloud computing. Communications of the ACM, 2010, 53(4): 50–58. [doi: 10.1145/1721654.1721672]

2 Li J, Ye H, Wang W, *et al*. Efficient and secure outsourcing of differentially private data publication. Proceedings of the 23rd European Symposium on Research in Computer Security. Barcelona: Springer, 2018. 187–206.

3 Li JG, Wang Y, Zhang YC, *et al*. Full verifiability for outsourced decryption in attribute based encryption. IEEE Transactions on Services Computing, 2020, 13(3): 478–487. [doi: 10.1109/TSC.2017.2710190]

4 Ali M, Khan SU, Vasilakos AV. Security in cloud computing: Opportunities and challenges. Information Sciences, 2015, 305: 357–383. [doi: 10.1016/j.ins.2015.01.025]

5 Ateniese G, Burns R, Curtmola R, *et al*. Provable data possession at untrusted stores. Proceedings of the 14th ACM Conference on Computer and Communications Security. Virginia: ACM, 2007. 598–609.

6 白国靖. 云计算环境下数据完整性验证方案的研究与设计 [硕士学位论文]. 重庆: 重庆邮电大学, 2012.

7 Shacham H, Waters B. Compact proofs of retrievability. Proceedings of the 14th International Conference on the Theory and Application of Cryptology and Information Security. Melbourne: Springer, 2008. 90–107.

8 王珺翔. 可证明数据持有模型与方案的研究 [硕士学位论文]. 上海: 上海交通大学, 2013.

9 Ateniese G, Di Pietro R, Mancini LV, *et al*. Scalable and efficient provable data possession. Proceedings of the 4th International Conference on Security and Privacy in Communication Netowrks. Istanbul: ACM, 2008. 9.

10 Sebé F, Domingo-Ferrer J, Martinez-Balleste A, *et al*. Efficient remote data possession checking in critical information infrastructures. IEEE Transactions on Knowledge and Data Engineering, 2008, 20(8): 1034 –1038. [doi: 10.1109/TKDE.2007.190647]

11 Shamir A. Identity-based cryptosystems and signature schemes. Workshop on the Theory and Application of Cryptographic Techniques. Aarhus: Springer, 1984. 47–53.

12 Wang HQ, He DB, Yu J, *et al*. Incentive and unconditionally anonymous identity-based public provable data possession. IEEE Transactions on Services Computing, 2019, 12(5): 824–835. [doi: 10.1109/TSC.2016.2633260]

13 Li YN, Yu Y, Min GY, *et al*. Fuzzy identity-based data integrity auditing for reliable cloud storage systems. IEEE Transactions on Dependable and Secure Computing, 2019, 16(1): 72–83. [doi: 10.1109/TDSC.2017.2662216]

14 Yang GY, Yu J, Shen WT, *et al*. Enabling public auditing for shared data in cloud storage supporting identity privacy and traceability. Journal of Systems and Software, 2016, 113: 130–139. [doi: 10.1016/j.jss.2015.11.044]

15 Wang C, Wang Q, Ren K, *et al*. Privacy-preserving public auditing for data storage security in cloud computing. 2010 Proceedings IEEE INFOCOM. San Diego: IEEE, 2010. 1–9.

16 Yu Y, Au MH, Ateniese G, *et al*. Identity-based remote data integrity checking with perfect data privacy preserving for cloud storage. IEEE Transactions on Information Forensics and Security, 2017, 12(4): 767–778. [doi: 10.1109/TIFS.2016.2615853]

17 Zhang Y, Yu J, Hao R, *et al*. Enabling efficient user revocation in identity-based cloud storage auditing for shared big data. IEEE Transactions on Dependable and Secure Computing, 2020, 17(3): 608–619. [doi: 10.1109/TDSC.2018.2829880]

18 王佳硕. 云存储中可证明数据持有性研究 [硕士学位论文]. 成都: 西南交通大学, 2018.

19 Miller VS. Use of elliptic curves in cryptography. Conference on the Theory and Application of Cryptographic Techniques. Bruges: Springer, 1985. 417–426.

20 Koblitz N. Elliptic curve cryptosystems. Mathematics of Computation, 1987, 48(177): 203–209. [doi: 10.1090/S0025-5718-1987-0866109-5]

21 Boneh D, Lynn B, Shacham H. Short signatures from the Weil pairing. International Conference on the Theory and Application of Cryptology and Information Security. Gold Coast: Springer, 2001. 514–532.

22 Schnorr CP. Efficient signature generation by smart cards. Journal of Cryptology, 1991, 4(3): 161–174. [doi: 10.1007/BF00196725]

23 Katz J, Lindell Y. Introduction to Modern Cryptography. Taylor and Francis, 2007.

24 Wang BY, Li BC, Li H. Panda: Public auditing for shared data with efficient user revocation in the cloud. IEEE Transactions on Services Computing, 2015, 8(1): 92–106. [doi: 10.1109/TSC.2013.2295611]

25 Jiang T, Chen XF, Ma JF. Public integrity auditing for shared dynamic cloud data with group user revocation. IEEE Transactions on Computers, 2016, 65(8): 2363–2373. [doi: 10.1109/TC.2015.2389955]

26 Shamus Software. Multiprecision Integer and Rational Arithmetic Cryptographic Library (MIRACL). https://github.com/miracl/MIRACL. (2019-06-10).