文章编号:1007-5321(2017)05-0043-07 DOI:10.13190/j.jbupt.2017-003

基于属性门限签名的动态群组共享数据公开审计方案

查雅行, 罗守山, 李 伟, 卞建超
(1. 北京邮电大学 信息安全中心, 北京 100876; 2. 北京邮电大学 灾备技术国家工程实验室, 北京 100876)

摘要: 提出了一种基于属性门限签名的动态群组隐私保护公开审计方案,将用户身份信息参数引入用户属性私钥中,有效地防止合谋攻击者通过组合属性密钥来伪造签名. 该方案利用基于属性的授权策略,支持用户权限撤销和数据动态操作. 分析结果表明,该方案在随机预言模型下具有不可伪造性和抵抗合谋攻击等特点,高效率且安全.

关 键 词: 属性门限签名; 隐私保护; 公开审计; 不可伪造性
中图分类号: TP391 **文献标志码**: A

Dynamic Group Public Auditing Scheme for Shared Data on Attribute-Based Threshold Signature

ZHA Ya-xing, LUO Shou-shan, LI Wei, BIAN Jian-chao
(1. Information Security Center, Beijing University of Posts and Telecommunications, Beijing 100876, China;
2. National Engineering Laboratory of Disaster Backup and Recovery, Beijing University of Posts and Telecommunications, Beijing 100876, China)

Abstract: A privacy-preserving public auditing scheme for dynamic group shared data based on attribute-based threshold signature was proposed, the identity information parameter was introduced into the attribute keys for preventing collusion attacker who wants to forge signature through the combination of these keys. The proposed scheme supports authority revocation of group user and data dynamic operation with attribute-based authorization strategy. Analysis shows that the proposed scheme with the characteristics of unforgeability and resistance collusion attack based on the random oracle model, and with better efficiency and security.

Key words: attribute-based threshold signature; privacy preserving; public auditing; unforgeability

云计算、物联网、社交网络等新兴服务促使人类社会的数据种类和规模快速增长,越来越多的企业和用户将数据存储在云服务提供商(CSP, cloud service provider)处,CSP 提供的资源相对集中,存在着数据信息在网络传输过程中的“失真”[1-2]、系统软硬件故障、不可信第 3 方导致数据丢失或损坏带来的数据不完整和用户隐私安全问题[3]亟待解决. 如何高效地进行数据持有性验证成为云存储安全的一大挑战[4]. Ateniese 等[5]首次提出了数据持有性证明的形式化模型,Curtmola 等[6]提出了多副本的数据持有性验证方案,基于此,查雅行等[7]提出了针对多用户多副本场景下的数据持有性证明方案. 上述方案考虑数据单一所有者情况下进行的完整性验证,云存储环境下存在群组用户对共享数据的完整性进行公开审计的新需求. 为此,Wang 等提出了保护群组用户隐私的完整性验证方案 Oruta[8] 和

收稿日期: 2017-01-13
基金项目: 国家高技术研究发展计划(863 计划)项目(2015AA016005, 2015AA017201);广东省应用型科技研发专项资金项目(2015B010131007)
作者简介: 查雅行(1985—), 男, 博士生, E-mail: zhayaxing@163.com; 罗守山(1962 —), 男, 教授, 博士生导师.

Knox[9],但不支持用户撤销操作. 针对用户权限撤销问题,Wang 等[10]在基于代理重签名机制上设计了一种公开审计方案 Panda,但存在替代攻击的风险[11]. 为此,Yuan 等[12]提出了一种支持抗合谋攻击、公共审计及用户撤销等特点的审计方案. Jiang 等[13]提出了一种支持群用户撤销机制的方案以解决合谋攻击的问题. 付安民等[14]设计了首个适用于多管理者群组共享数据的公开审计方案. 李晖等[15]提出了支持第3方审计者的审计方案. 针对密钥管理与安全分发的问题,黄龙霞等[16]首次使用基于逻辑层次密钥体系的密钥树进行密钥的建立和分发.

现有基于第3方审计者(TPA, third party auditor)的群组共享数据完整性审计方案,大多考虑数据更新操作或用户撤销等某一方面特性,存在泄露群组成员身份隐私和伪造攻击的风险. 因此,设计能阻止隐私信息泄露和抵抗伪造攻击的共享数据完整性验证方案是共享数据隐私保护的关键. 笔者采用基于属性门限签名机制[17-18],设计了一种支持动态群组隐私保护公开审计方案,利用用户私钥的产生与属性相关的特点,在计算密钥时引入用户身份信息参数,防止拥有互补属性的恶意群组用户利用组合用户私钥来伪造签名,最后给出方案的安全性和性能分析结果.

1 基于属性门限签名的群组共享数据公开审计方案

通过利用基于门限属性签名方案[18]良好的不可伪造性和抗合谋攻击等性质,设计群组共享数据公开审计方案. 具体算法描述如下:

1) 初始化 Setup(d)

在初始化阶段,输入系统参数 d,选择双线性映射 $e:G_1\times G_1\to G_2$,G_1、G_2表示阶为 p 的乘法循环群,群 G_1的生成元为 g,选取群 G_1中元素 g_1, $g_2\in G_1$,任意 $\alpha\in\mathbf{Z}_p^*$,计算 $g_1=g^\alpha$,$Z=e(g,g)^\alpha$. 选取抗碰撞的 Hash 函数 $H_1,H_2:\{0,1\}^*\to G_1$;选取伪随机函数 $\phi(i):\mathbf{Z}_p^*\to\{1,2,\cdots,n\}$,用于生成伪随机数.

假设属性域 U,集合元素个数为 $l=|U|$,U 中属性映射到 $\mathbf{Z}_p$中特定的整数(如 $1,2,3,\cdots,l\ (\mathrm{mod}\ p)$),给定 $d-1$ 个属性组成默认属性集 $\Omega=\{\Omega_1,\Omega_2,\cdots,\Omega_{d-1}\}$. 采用基于属性门限的签名断言 $Y_{k,\omega^*}()$,即对所有签名属性集 ω^*,门限值为 k,都有 $Y_{k,\omega^*}()\to 0/1$[18]. 定义属性域 U 对应的公钥集 $T=\{T_1,T_2,\cdots,T_l\}$,$t_1,t_2,\cdots,t_l\in\mathbf{Z}_p^*$,计算 $T_i=g^{t_i}$. 计算得到公开参数 $\Psi=\{G_1,G_2,g,g_1,g_2,d,p,H_1,H_2,Z,T_1,T_2,\cdots,T_l\}$,主密钥 $\kappa=\{\alpha,t_1,t_2,\cdots,t_l\}$.

2) 密钥生成 KeyGen(χ_i,κ,ω)

授权机构选取 $d-1$ 次多项式 $q(x)$,令 $q(0)=\alpha$,授权机构秘密保存 $q(x)$,并随机选取其余 $d-1$ 个系数. 假设用户域 $u=\{u_1,u_2,\cdots,u_{|u|}\}$,给定用户身份信息参数$\chi_i$及其对应属性集 $\omega\subset U$,生成新属性集 $\omega_0=\omega\cup\Omega$,对任意 $i\in\omega_0$,授权机构选取用户身份信息参数$\chi_i\in\mathbf{Z}_p$,将 χ_i嵌入到属性私钥中,同时,生成属性私钥:

$$\left.\begin{aligned} d_{i,1}&=g^{q(i)/t_i}H_1(\chi_i)^\alpha\\ d_{i,2}&=H_1(\chi_i)^{t_i}\end{aligned}\right\}\tag{1}$$

授权机构输出用户属性私钥 $\xi_i=\{d_{i,1},d_{i,2}\}$,$\xi=\{\xi_i,1\leqslant i\leqslant|u|\}$,$\chi=\{\chi_i,1\leqslant i\leqslant|u|\}$,将属性私钥发送给对应的用户,并存储用户属性私钥与身份信息映射表 $T_{st}=(\chi,\xi)$.

3) 签名 Sign(m,κ,ξ)

假设共享的数据 $m=\{m_j\}_{1\leqslant j\leqslant n}$,数据拥有者制定授权策略$\rho=(u_i,m_j,\omega)$,拥有属性集 ω 的用户 u_i 才能访问数据 m_j. 声明基于门限的签名断言 $Y_{k,\omega^*}()$,当属性集 ω 满足 $Y_{k,\omega^*}()$时,即 $Y_{k,\omega^*}(\omega)$,则属性集 ω 和 ω^* 至少有 k 个相同元素. 数据拥有者随机选取 k 元属性子集 ω',使得 $\omega'\subseteq\omega\cap\omega^*$. 在 Ω 中选择 $d-k$ 个默认属性组成属性子集 Ω',满足 $\Omega'\subseteq\Omega$,$|\Omega'|=d-k$.

数据拥有者对数据 m_j进行签名,对每个属性$i\in\omega^*\cap\Omega'$,选取随机数 $\tau\in\mathbf{Z}_p^*$,计算:

$$\sigma_{i,0}=g_1^{t_i}H_2(m_j)^\tau\tag{2}$$

$$\sigma_{i,1}=\begin{cases}\prod\limits_{i\in\omega'\cup\Omega'}(d_{i,1})^{m_jt_i}T_i^\alpha H_2(m_j)^\tau\\ \prod\limits_{i\in\omega^*/\omega'}T_i^\alpha H_2(m_j)^\tau\end{cases}\tag{3}$$

$$\sigma_{i,2}=(d_{i,2})^{\alpha m_j\sum\limits_{i\in\omega'\cup\Omega'}\Delta_{i,S(0)}}\tag{4}$$

得到签名值 $\sigma=\{\sigma_{i,0},\sigma_{i,1},\sigma_{i,2}\}_{1\leqslant j\leqslant n}$,数据拥有者将 $\{m,\sigma\}$发送给 CSP,将 σ 和 $Y_{k,\omega^*}()$发送给 TPA.

4) 证据生成 GenProof(m, σ)

数据拥有者向 TPA 发起数据验证请求,TPA 从集合$\{1,2,\cdots,n\}$中选取 c 个元素 $I=\{s_1,s_2,\cdots,s_c\}$,$1\leqslant s_1\leqslant\cdots\leqslant s_c\leqslant n$,对于每个 $j\in I$,TPA 选取随机数 $k\in\mathbf{Z}_p$,生成挑战消息 $\pi=\{(j,v_j)\}_{s_1\leqslant j\leqslant s_c}$,其中$v_j=$

$\phi_k(j)$. TPA 将挑战消息 π 发送给 CSP，CSP 收到后计算完整性证据 P：

$$\hat{m}=\sum_{s_1\leqslant j\leqslant s_c} v_j m_j,\ \sigma_0=\prod_{s_1\leqslant j\leqslant s_c}(\sigma_{i,0})^{v_j},$$

$$\sigma_2=\prod_{s_1\leqslant j\leqslant s_c}(\sigma_{i,2})^{v_j}$$

$$\left\{\sigma_1=\prod_{s_1\leqslant j\leqslant s_c}(\sigma_{i,1})^{v_j}\right\}_{i\in\omega^*\cup\Omega'}$$

CSP 将证据 $P=(\hat{m},\sigma_0,\sigma_1,\sigma_2)$ 发给 TPA.

5）验证 Verify(P)

TPA 收到证据 P 后，判断数据块的签名是否满足断言 $Y_{k,\omega^*}()$，并验证等式：

$$\frac{\prod_{i\in\omega^*\cup\Omega'} e(g,\sigma_1)^{\Delta_{i,S(0)}}}{e(g,\sigma_0)e(g,\sigma_2)}=Z^{\hat{m}} \tag{5}$$

如果等式成立，输出 True，证明数据块被正确持有；否则，输出 False，说明数据块损坏或丢失.

6）数据更新 Update(m_j')

假设数据拥有者将数据块 m_j 更新为 m_j'，得到新数据 m'. 调用签名算法得到新的签名 $\sigma'=\{\sigma'_{i,0},\sigma'_{i,1},\sigma'_{i,2}\}$，将$\{m',\sigma'\}$发送给 CSP，CSP 判断更新数据的签名是否满足断言 $Y_{k,\omega^*}()$，并验证等式：

$$\frac{\prod_{i\in\omega^*\cup\Omega'} e(g,\sigma_{i,1})^{\Delta_{i,S(0)}}}{e(g,\sigma_{i,0})e(g,\sigma_{i,2})}=Z^{m'} \tag{6}$$

若等式成立，则 CSP 保存 m'和签名 σ'.

7）用户撤销 Revoke(σ,T_{st})

当数据访问者离开群组时，需要进行用户撤销操作. 首先，授权机构需要更新映射表 T_{st}，得到 T'_{st}. 数据拥有者及时更新授权策略 $\rho=(u_i,m_j,\omega)$，删除已撤销用户的访问权限，计算新签名值 $\sigma'=\{\sigma'_{i,0},\sigma'_{i,1},\sigma'_{i,2}\}$，并发送给 CSP 和 TPA. CSP 判断用户撤销操作后数据的签名是否满足断言 $Y_{k,\omega^*}()$，并验证等式：

$$\frac{\prod_{i\in\omega^*\cup\Omega'} e(g,\sigma'_{i,1})^{\Delta_{i,S(0)}}}{e(g,\sigma'_{i,0})e(g,\sigma'_{i,2})}=Z^{m} \tag{7}$$

如果验证成功，CSP 保存新签名 σ'.

2　正确性与安全性分析

2.1　正确性分析

定理 1　如果 TPA 和 CSP 能够回复并通过数据持有性验证，则证明所提方案的正确性.

证明　在进行持有性验证时，如果数据拥有者的属性集 ω 存在足够的 k 元属性子集 ω'，与默认属性子集 Ω'组成 d 元属性集合，并且 TPA 与 CSP 交互过程中回复的消息都是正确的，则在验证阶段，TPA 收到 CSP 发送的证据 $P=(\hat{m},\sigma_0,\sigma_1,\sigma_2)$ 是正确的. TPA 利用拉格朗日定理及收到的证据，进行如下计算：

$$\frac{\prod_{i\in\omega^*\cup\Omega'} e(g,\sigma_1)^{\Delta_{i,S(0)}}}{e(g,\sigma_0)e(g,\sigma_2)}=$$

$$\frac{\prod_{i\in\omega^*\cup\Omega'} e\left(g,\prod_{s_1\leqslant j\leqslant s_c}(\sigma_{i,1})^{v_j}\right)^{\Delta_{i,S(0)}}}{e\left(g,\prod_{s_1\leqslant j\leqslant s_c}(\sigma_{i,0})^{v_j}\right)e\left(g,\prod_{s_1\leqslant j\leqslant s_c}(\sigma_{i,2})^{v_j}\right)}=$$

$$e(g,g)^{\alpha\sum_{s_1\leqslant j\leqslant s_c} m_j x_j}=Z^{\hat{m}}$$

证毕.

2.2　安全性分析

定理 2　如果 e 是(t,ε)安全的，在计算迪菲-赫尔曼(CDH, computational Differ-Hellman)困难问题和随机预言模型假设下，提出的方案在适应性选择消息攻击模型下具有不可伪造性.

证明　假设存在$(t,q_H,q_C,q_S,\varepsilon)$－敌手 A 对方案进行适应性选择消息攻击，敌手 A 通过伪造签名证据在多项式时间 t 内以 ε 的优势破解该方案，存在一个(t',ε')－算法 F 以 $\varepsilon'=\dfrac{c\varepsilon}{nq_{H_1}q_{H_2}\binom{d-k}{d}}$的优势能解决 CDH 困难问题，A 询问 Hash 预言机的次数分别为 q_{H_1}和 q_{H_2}. 假设给定 g, g^x, $g^y\in G_1$，利用算法 F 通过(t,q_H,q_S,ε)－敌手 A 使用适应性选择消息攻击方法计算 g^{xy}，即解决 CDH 困难问题. 利用 Game 游戏[17-18]来证明定理 2.

Game0　考虑敌手 A 与挑战环境之间初始化挑战游戏. 首先，运行初始化算法，挑战者 C 计算 $g_1=g^x$，$g_2=g^y$. C 生成主密钥 κ 和公开参数 Ψ，C 生成 $Y_{k,\omega^*}()$，属性集 ω'和 ω^* 至少有 k 个相同元素，$|\omega'|=k$. C 随机选取 $d\in\mathbf{Z}_p^*$，$1\leqslant k\leqslant d$，从 d 个属性中选择 $d-k$ 个默认属性组成属性子集 Ω'，满足$\Omega'\subseteq\Omega$，$|\Omega'|=d-k$，C 将 Ψ 发送给 A.

Game1　主要考虑在 A 与交互环境之间初始化挑战游戏. A 与 C 进行交互，C 在多项式时间内进行 Hash 询问(H_1询问和 H_2询问)、KeyGen 询问、Sign 询问和 GenProof 询问.

1）H_1 询问：C 维护一个 Hash 查询列表 $H_{list1}=\{\chi_i,\omega_i,Q_i\}$. 选择随机数 $c\in[1,q_H]$，A 对 χ_i进行 Hash 询问，如果 χ_i已在列表 H_{list1} 中，C 返回对应的

Hash 询问结果 Q_i. 否则进行如下操作:若 $\omega_i \subseteq \Omega' \cup \omega'$,C 选择随机数 a_i,计算 $Q_i = H_1(\chi_i) = g_1^{a_i}$ 并发给 A,且更新列表 H_{list1};否则,C 选择 a_i, $b_i \in \mathbf{Z}_p^*$,计算 $Q_i = H_1(\chi_i) = g_1^{a_i} g_1^{-b_i}$ 并发送给 A,同时更新列表 H_{list1}.

2) H_2 询问:C 维护一个 Hash 查询列表 $H_{\text{list2}} = \{m_i, h_i\}$. A 对 m_i 进行 Hash 询问,如果 m_i 已在列表 H_{list2} 中,C 返回对应的 Hash 询问结果 h_i. 否则进行如下操作:C 选择随机数 $a_i \in \mathbf{Z}_p^*$,计算 $h_i = H_2(m_i) = g_2^{a_i}$ 发送给 A,并更新列表 H_{list2};否则,C 选择 $a_i', b_i \in \mathbf{Z}_p^*$,计算 $h_i = H_2(m_i) = g_2^{a_i'} g_2^{b_i}$ 并发送给 A,同时更新列表 H_{list2}.

3) KeyGen 询问:C 维护密钥生成询问列表 $K_{\text{list}} = \{\chi_i, \omega_i, Q_i, \{\xi_i, T_i\}\}$,A 选择属性集 ω_i 向 C 询问对应用户公私钥,C 检查 K_{list} 中是否有对应的询问结果,如果存在,则返回对应的 $\{\xi_i, T_i\}_{i \in \omega_i}$. 否则,对属性 $i \in \omega_i$,C 进行如下操作:假设 $i \in (\omega_i \cap \omega') \cup \Omega_i'$,C 选择 $a, \chi_i, t_i \in \mathbf{Z}_p^*$,选择 d 次多项式 $q(x)$ 使得 $\alpha_i = q(i)$,计算 $d_{i,1} = g_2^{q(i)/t_i} H_1(\chi_i)^{\alpha}$, $d_{i,2} = H_1(\chi_i)^{t_i}$, $\xi_i = \{d_{i,1}, d_{i,2}\}$,C 返回结果给 A,并记录到询问列表 $K_{\text{list}} = \{\chi_i, \omega_i, Q_i, \{\xi_i, T_i\}\}$ 中;否则,终止询问.

4) Sign 询问:C 维护签名询问列表 $S_{\text{list}} = \{\chi_i, \omega_i, m_i\}$. 如果 $|\omega_i \cap \omega'| \geqslant k$,A 向 C 询问在属性集 ω_i 和断言 $Y_{k,\omega^*}()$ 条件下 m^* 的签名 σ^*,C 运行 $\text{Sign}(m_i, \omega_i, Y_{k,\omega^*}())$ 生成数据签名 $\sigma^* = \{\sigma_{i,0}^*, \sigma_{i,1}^*, \sigma_{i,2}^*\}$,并返回给 A;否则,终止询问.

5) GenProof 询问:A 选择数据签名值为 σ^*,生成挑战消息 $\pi^* = \{(j, v_j)\}_{s_1 \leqslant j \leqslant s_c}$,向 C 进行询问,C 运行证据生成算法 $\text{GenProof}(m, \sigma)$,生成挑战证据 $P^* = \{\hat{m}, \sigma_0^*, \sigma_1^*, \sigma_2^*\}$,且返回给 A.

Game2 C 保存 A 询问后产生的应答列表,A 通过伪造签名信息进行挑战. 首先,A 选择挑战属性 $\hat{\omega}$ 和默认属性集 $\hat{\Omega}$,输出 $\hat{m}$ 的签名信息 σ_0^*、σ_1^* 和 σ_2^*. 如果 $\hat{\Omega} \neq \Omega^*$ 或 $H_2(m_i) \neq g^{a_c}$,A 挑战失败;否则,若满足 $\dfrac{\prod_{i \in \omega^* \cup \Omega'} e(g, \sigma_1)^{\Delta_{i,S}(0)}}{e(g, \sigma_0) e(g, \sigma_2)} = Z^{\hat{m}}$ 成立,A 挑战成功.

当 C 通过数据挑战证据 P^* 时,$\hat{\Omega} = \Omega^*$,A 通过 $\dfrac{\prod_{i \in \tilde{\omega}} e(g, \sigma_1^*)^{\Delta_{i,s}(0)}}{e(g, \sigma_0^*) e(g, \sigma_2^*)} = Z^{m^*}$ 来验证 P^*,其中,$\hat{m} \neq m^*$、$\sigma_0^* \neq \sigma_0$、$\sigma_1^* \neq \sigma_1$ 和 $\sigma_2^* \neq \sigma_2$. A 利用 P^* 破解 CDH 困难问题. 给定 $g_1 = g^x, g_2 = g^y$,其中 $x, y \in \mathbf{Z}_p^*, g \in G_1$,C 输出目标为 g^{xy},C 通过计算得到 $g^{xy} = \dfrac{\prod_{i \in \tilde{\omega}} (\sigma_1^*)^x}{\alpha \hat{m} \sigma_0^* \sigma_2^*}$,即破解 CDH 困难问题.

Game3 假设 C 观察整个数据完整性证明过程,密钥生成预言机和签名预言机的应答是无效的,导致 C 终止挑战过程. A 回复证据为 $P^* = \{\hat{m}, \sigma_0^*, \sigma_1^*, \sigma_2^*\}$. 诚实证明者回复证据 P,验证者收到 P 后验证等式 $\dfrac{\prod_{i \in \omega^* \cup \Omega'} e(g, \sigma_1)^{\Delta_{i,S}(0)}}{e(g, \sigma_0) e(g, \sigma_2)} = Z^{\hat{m}}$ 是否成立.

假设当 $\hat{m} \neq m^*$ 时,$\sigma_0^* = \sigma_0$、$\sigma_1^* = \sigma_1$ 和 $\sigma_2^* = \sigma_2$,定义 $\Delta m = \hat{m} - m^*$,C 回复 A 的质询,最终敌手 A 回复伪造的证据 $P^* = \{\hat{m}, \sigma_0^*, \sigma_1^*, \sigma_2^*\}$,并验证:

$$\frac{\prod_{i \in \tilde{\omega}} e(g, \sigma_1^*)^{\Delta_{i,s}(0)}}{e(g, \sigma_0^*) e(g, \sigma_2^*)} = Z^{m^*} = \frac{\prod_{i \in \omega^* \cup \Omega'} e(g, \sigma_1)^{\Delta_{i,S}(0)}}{e(g, \sigma_0) e(g, \sigma_2)} = Z^{\hat{m}}$$

则可得到 $Z^{\Delta m} = 1$,即 $\hat{m} = m^* \bmod p$. 经过以上分析,这些游戏之间的差异存在可以忽略的概率.

如果挑战者 C 在多项式时间 t 内进行询问的应答都是有效的,分析 A 解决 CDH 困难问题时的优势. A 进行 H_1 询问和 H_2 询问获取正确结果的概率分别为 $P_{H1} = 1/q_{H_1}$ 和 $P_{H2} = 1/q_{H_2}$,则 A 成功获取 Hash 询问(H_1 询问和 H_2 询问)结果的概率为 $P_1 = P_{H1} \times P_{H2} = 1/(q_{H_1} q_{H_2})$;A 成功从 d 个属性中选取 $d-k$ 个默认属性组成属性子集 Ω' 的概率为 $P_2 = 1/\binom{d-k}{d}$;A 进行 GenProof 询问成功选取挑战消息 π^* 的概率为 $P_3 = \dfrac{c}{n}$;A 通过伪造签名证据在多项式时间 t 内破解该方案的概率 $P_0 = \varepsilon$. 即存在一个 (t', ε') - 算法以 ε' 的优势能解决 CDH 困难问题,其中:

$$\varepsilon' = P_0 P_1 P_2 P_3 = \frac{c\varepsilon}{n q_{H_1} q_{H_2} \binom{d-k}{d}}$$

定理 3 在 CDH 问题和随机预言模型假设下,提出的方案在适应性选择消息攻击模型下具有抗合谋攻击性.

证明 同定理 2 中基本假设所述.

Game0　同定理 2 中的 Game0，主要是游戏的初始化阶段.

Game1　同定理 2 中的 Game1.

Game2　挑战者 C 保存敌手 A 询问后产生的应答列表，A 伪造实施合谋攻击时的信息，并进行相应的查询. 首先，A 选择参与合谋攻击的用户 u_i、u_j，对应属性集为 $\widetilde{\omega}_i$ 和 $\widetilde{\omega}_j$，进行 KeyGen 询问，得到对应的用户私钥集 ξ_i 和 ξ_j，计算 $T_i = g_2^{t_i}$，$\xi_i = \{g_2^{q(i)/t_i} H_1(\chi_i)^{\alpha}, H_1(\chi_i)^{t_i}\}$，$T_j = g_2^{t_j}$，$\xi_j = \{g_2^{q(j)/t_j} H_1(\chi_j)^{\alpha}, H_1(\chi_j)^{t_j}\}$，C 将 ξ_i 和 ξ_j 发送给 A. A 选取密钥 $\xi' = \xi_i' \cup \xi_j'$，其中 $\xi_i' \subseteq \xi_i$，$\xi_j' \subseteq \xi_j$，ξ' 对应属性 $\omega'' = \widetilde{\omega}_i \cup \widetilde{\omega}_j$，满足 $Y_{k',\tilde{\omega}}(\omega'') = 1$. A 选取 m^* 和属性集 ω'' 下的签名 $\hat{\sigma}$，生成完整性证据 $\hat{P} = (\hat{m}, \hat{\sigma}_0, \hat{\sigma}_1, \hat{\sigma}_2)$.

Game3　敌手 A 通过收集伪造实施合谋攻击时的属性及签名信息，挑战方案的抗合谋攻击性. 首先，A 选择挑战属性 ω'' 和默认属性集 $\hat{\Omega}$，输出完整性证据 $\hat{P}$. 敌手 A 利用 $\hat{P}$ 破解 CDH 困难问题，即给定 $g_1 = g^x$，$g_2 = g^y$，其中 x，$y \in \mathbf{Z}_p^*$，$g \in G_1$，输出目标为 g^{xy}，同定理 2，C 计算出 g^{xy}. 即敌手 A 以 $\varepsilon' = c\varepsilon / \left(nq_{H_1}q_{H_2}\binom{d-k}{d}\right)$ 的优势解决 CDH 困难问题.

3　性能分析

下面主要通过与同类方案[12-13,16]对比分析计算开销和通信开销情况. 首先，定义如下符号含义：$T_{\exp}$ 表示指数运算所需的时间，T_{mul} 表示乘法运算所需的时间，T_{pair} 表示双线性对运算所需的时间，T_{Hash} 表示 Hash 运算所需的时间，T_{m} 表示模运算所需的时间，u 表示签名的用户数，c 表示挑战的数据块数目，d 表示默认属性域中属性个数，z 表示被撤销的用户数，n 表示数据分块数，s 表示每个数据块中包含的子数据块数.

3.1　计算开销

在计算开销方面，与同类方案[12-13,16]进行对比. 方案 1[12] 和方案 2[13] 主要是支持群组用户撤销及共享数据更新的公共审计方案. 其中，方案 1[12] 计算开销随着数据块的增多而增大，开销远大于本方案及其他方案[13,16]；方案 2[13] 计算开销随着撤销用户数量的增加而增大. 通过采用基于随机数的挑战方法，方案 3[16] 在挑战与响应阶段的计算开销与本方案相当，在验证阶段的计算开销比本方案大. 具体对比情况如表 1 所示.

表 1　方案计算开销对比

方案	方案 1[12]	方案 2[13]	方案 3[16]	本方案
初始化	$(s+2)nT_{\exp} + nsT_{\exp}$	$2nT_{\exp} + nT_{\text{mul}}$	T_{mul}	$T_{\text{pair}} + (d+1)T_{\exp}$
密钥生成	$u(s+4)T_{\exp}$	$u(n+1)T_{\exp}$	$u(T_{\text{mul}} + T_{\text{m}})$	$u(T_{\text{mul}} + T_{\text{hash}} + 2T_{\exp})$
签名	$u((s+1)T_{\text{mul}} + 2(s+1)T_{\exp})$	$u((n+9)T_{\exp} + 3T_{\text{pair}} + (2n+4)T_{\text{mul}} + 2T_{\text{hash}})$	$u(T_{\text{hash}} + T_{\text{mul}} + 2T_{\exp})$	$u(6T_{\text{mul}} + 3T_{\text{hash}} + 8T_{\exp})$
挑战/询问		$(n-1)(T_{\text{mul}} + T_{\exp})$	$(2c-1)T_{\text{mul}} + cT_{\exp} + T_{\text{m}}$	$c(T_{\text{mul}} + 3T_{\exp})$
验证	$3T_{\text{pair}} + 3T_{\text{mul}} + 6T_{\exp}$	$7T_{\text{pair}} + T_{\text{mul}} + 9T_{\exp} + 5T_{\text{hash}}$	$cT_{\text{hash}} + cT_{\text{mul}} + T_{\text{m}} + (c+1)\ T_{\exp}$	$3T_{\text{pair}} + T_{\text{mul}} + 2T_{\exp}$
更新及证明	$2(s+1)T_{\exp} + uT_{\text{pair}} + (2s+u+1)T_{\text{mul}}$	$3u(T_{\text{mul}} + T_{\exp})$ 或 $2u(T_{\text{mul}} + T_{\exp})^*$		$3T_{\text{pair}} + 6T_{\text{mul}} + 3T_{\text{hash}} + 5T_{\exp}$
用户撤销	$u(T_{\text{pair}} + T_{\exp})$	$z(2T_{\text{pair}} + T_{\text{mul}})$	$T_{\text{mul}} + cT_{\exp} + T_{\text{m}}$	$3T_{\text{pair}} + T_{\text{mul}} + 2T_{\exp}$

3.2　通信开销

在数据完整性验证过程中，主要分析审计阶段的通信开销，其中 $|\lambda|$ 为随机数大小，$|G_1|$ 为群 G_1 中元素的大小，$|I|$ 表示数据块索引大小. 具体对比结果如表 2 所示.

表 2　审计阶段通信开销对比

方案	通信开销
方案 1[12]	$c*|I| + (u+3)|G_1| + 2|\lambda|$
方案 2[13]	$2(c+1)|\lambda| + n|G_1|$
方案 3[16]	$(c+3)|G_1|$
本方案	$6|G_1| + c|\lambda|$

3.3　结果对比

本方案采用的实验环境：Intel Core i3-2350 CPU 2.30 GHz，4 GB 内存，Windows7 x64 位操作系统，采用密码学函数库 PBC 版本为 PBC-0.4.7，VC + + 6.0 环境下进行实验. 本方案使用椭圆曲线域表示 G_1 和 G_2，密钥大小为 160 bit，随机数大小为 80 bit. 假设存储在 CSP 中的用户数据文件有 1% 的内容被损坏，如果要保证用户检查出此事件发生的概率不

低于99%,则只需随机验证其中 $c=460$ 个数据块的持有性证据[5]. 假设数据块数 $n=10\,000$ 个,每个分块子块数 $s=50$ 个,群用户数 $u=10$ 个时,具体审计阶段开销对比情况如表3所示.

表3 审计阶段开销结果对比情况

方案	计算开销/s	通信开销/KB
方案1[12]	18.33	4.97
方案2[13]	3 855.00	209.00
方案3[16]	17.08	9.00
本方案	23.61	4.60

通过以上的对比分析可知,本方案在计算开销和通信开销方面都具有较好的效率,设计了基于属性的授权策略,在进行数据访问、用户撤销和数据更新时,相对较为灵活. 在用户撤销方面,同类方案[12-13,16]的计算开销随数据分块数、所撤销的用户数或挑战数据块数的增加而增大,本方案的计算开销较小. 在数据更新方面,方案3[16]不支持数据更新操作;方案1[12]需要对进行数据分块的再处理,更新操作开销大;方案2[12]更新操作的计算开销随着群组用户数量的增加而增大,但更新操作较为灵活;本方案更新操作主要是由数据拥有者更新数据并产生新的签名值,每次更新计算开销较小. 由于本方案采用基于属性的门限机制以抵抗恶意用户利用互补属性构造私钥来伪造签名而实施合谋攻击,签名过程设计相对复杂,而且随着群组用户增多、共享数据量增大时,签名效率会降低.

4 结束语

针对现有大多数动态群组共享数据公开审计方案主要考虑数据更新操作或用户撤销等某一方面特性,及无法有效防止合谋攻击者利用互补属性来伪造签名的问题,提出了一种基于属性门限签名的动态群组隐私保护公开审计方案,将用户身份信息参数引入用户属性私钥中,防止攻击者通过利用互补属性构造属性私钥来伪造签名,支持群组用户撤销和数据动态操作. 分析结果表明,方案具有不可伪造性和抵抗合谋攻击性. 下一步计划研究基于属性门限签名的且适用于多数据提供者及大数据环境下的群组共享数据批量审计方案.

参考文献:

[1] Qiao Jianyong. Julia sets and complex singularities of free energies[J]. Memoirs of American Mathematical Society, 2015(234): 1-89.

[2] Qiao Jianyong. On the preimages of parabolic points[J]. Nonlinearity, 2000(13): 813-818.

[3] 高志鹏, 牛琨, 刘杰. 面向大数据的分析技术[J]. 北京邮电大学学报, 2015, 38(3): 1-12.
Gao Zhipeng, Niu Kun, Liu Jie. Analytics towards big data[J]. Journal of Beijing University of Posts and Telecommunications, 2015, 38(3): 1-12.

[4] Chen Hefeng, Lin Bogang, Yang Yang, et al. Public batch auditing for 2M-PDP based on BLS in cloud storage [J]. Journal of Cryptologic Research, 2014, 1(4): 368-378.

[5] Ateniese G, Burns R, Curtmola R. Provable data possession at untrusted stores[C]// Proc of CCS'07. New York: ACM, 2007: 598-609.

[6] Curtmola R, Khan O, Burns R, et al. MR-PDP: multiple-replica provable data possession[C]//The 28th International Conference on Distributed Computing Systems. IEEE Computer Society, 2008: 411-420.

[7] 查雅行, 罗守山, 卞建超, 等. 基于多分支认证树的多用户多副本数据持有性证明方案[J]. 通信学报, 2015, 36(11): 80-91.
Zha Yaxing, Luo Shoushan, Bian Jianchao, et al. Multi-user and multiple-replica provable data possession scheme based on multi-branch authentication tree[J]. Journal on Communications, 2015, 36(11): 80-91.

[8] Wang Boyang, Li Baochun, Li Hui. Oruta: privacy-preserving public auditing for shared data in the cloud[C]// Proceedings of the 2012 IEEE Fifth International Conference on Cloud Computing. [S. l.]: IEEE Computer Society, 2012: 295-302.

[9] Wang Boyang, Li Baochun, Li Hui. Knox: privacy-preserving auditing for shared data with large groups in the cloud[C]//International Conference on Applied Cryptography and Network Security. [S. l.]: Springer-Verlag, 2012: 507-525.

[10] Wang Boyang, Li Baochun, Li Hui. Panda: public auditing for shared data with efficient user revocation in the cloud[J]. IEEE Transactions on Services Computing, 2015, 8(1): 92-106.

[11] Yu Yong, Ni Jianbing, Au Manho, et al. On the security of a public auditing mechanism for shared cloud data service[J]. IEEE Transactions on Services Computing, 2014, 8(6): 1-2.

[12] Yuan Jiawei, Yu Shucheng. Efficient public integrity checking for cloud data sharing with multi-user modifica-

tion[C]//2014 Proceedings IEEE INFOCOM. [S.l.]: IEEE, 2014: 2121-2129.

[13] Jiang Tao, Chen Xiaofeng, Ma Jianfeng. Public integrity auditing for shared dynamic cloud data with group user revocation[J]. IEEE Transactions on Computers, 2016, 65(8): 2363-2373.

[14] 付安民, 秦宁元, 宋建业, 等. 云端多管理者群组共享数据中具有隐私保护的公开审计方案[J]. 计算机研究与发展, 2015, 52(10): 2353-2362.
Fu Anmin, Qin Ningyuan, Song Jianye, et al. Privacy-preserving public auditing for multiple managers shared data in the cloud[J]. Journal of Computer Research and Development, 2015, 52(10): 2353-2362.

[15] 李晖, 孙文海, 李凤华, 等. 公共云存储服务数据安全及隐私保护技术综述[J]. 计算机研究与发展, 2014, 51(7): 1397-1409.
Li Hui, Sun Wenhai, Li Fenghua, et al. Secure and privacy-preserving data storage service in public cloud [J]. Journal of Computer Research and Development, 2014, 51(7): 1397-1409.

[16] 黄龙霞, 张功萱, 付安民. 基于层次树的动态群组隐私保护公开审计方案[J]. 计算机研究与发展, 2016, 53(10): 2334-2342.
Huang Longxia, Zhang Gongxuan, Fu Anmin. Privacy-preserving public auditing for dynamic group based on hierarchical tree[J]. Journal of Computer Research and Development, 2016, 53(10): 2334-2342.

[17] Li Jin, Kim Kwangjo. Hidden attribute-based signatures without anonymity revocation[J]. Information Sciences, 2010, 180(9): 1681-1689.

[18] 陈桢, 张文芳, 王小敏. 基于属性的抗合谋攻击可变门限环签名方案[J]. 通信学报, 2015, 36(12): 212-222.
Chen Zhen, Zhang Wenfang, Wang Xiaomin. Attribute-based alterable threshold ring signature scheme with conspiracy attack immunity[J]. Journal on Communications, 2015, 36(12): 212-222.