不可克隆的动态 *k* 次匿名认证方案

柳欣 [1,2,3]，徐秋亮 [1]

（1. 山东大学 计算机科学与技术学院，山东 济南 250101；2. 山东青年政治学院 信息工程学院，山东 济南 250014；
3. 山东青年政治学院 山东省高校信息安全与智能控制重点实验室，山东 济南 250103）

摘 要：在已有的 *k* 次匿名认证方案中，尚存在 2 个未解决问题：1）如何实现允许服务供应商为每个用户设置不同的访问次数上界，同时不能以损失用户的匿名性作为代价；2）如何防止恶意用户发动大规模的克隆攻击。为此提出一个改进方案。新方案的构造过程使用了多项关键技术，包括关于“一个被承诺元素小于另一个被承诺元素”的知识证明，动态累加器和基于 *n* 次可展示令牌的克隆攻击检测方法等。对 Teranishi 等人的安全性模型做出修改，并且证明新方案在该模型下满足可证安全。此外，新方案的成员注册协议是并发安全的，因而适合于在实际的异步网络环境（如互联网）下进行部署。

关键词：*k* 次匿名认证；零知识证明；克隆攻击；Ω协议；并发零知识

中图分类号：TN918.2 **文献标识码**：A **文章编号**：1000-436X(2012)07-0075-15

Unclonable dynamic *k*-times anonymous authentication

LIU Xin [1,2,3], XU Qiu-liang [1]

(1. School of Computer Science and Technology, Shandong University, Ji’nan 250101, China;
2. School of Information Engineering, Shandong Youth University of Political Science, Ji’nan 250014, China; 3. Key Laboratory of Information Security and Intelligent Control in Universities of Shandong, Shandong Youth University of Political Science, Ji’nan 250103, China)

Abstract: In previous works of *k*-times anonymous authentication, two problems have not been properly solved: 1) how to allow application providers to assign different maximal numbers of access for each user without weakened anonymity, and 2) how to protect against massive clone attacks mounted by malicious users. To overcome these obstacles, a revised scheme was proposed. It incorporated several crucial tools including the proof that a committed value is less than another committed value, dynamic accumulator, the method of cloning detection based on n-times show e-tokens, etc. The new scheme is proven secure in a new security model which was obtained by modifying the security model of Teranishi et al. Moreover, the registration protocol of the new scheme is concurrently-secure, so it is fit for the deployment in realistic asynchronous network setting (e.g., Internet).

Key words: *k*-times anonymous authentication; zero-knowledge proof; the cloning attack; Omega-protocol; concurrent zero-knowledge

---

收稿日期：2011-09-28；**修回日期**：2011-12-30

基金项目：国家自然科学基金资助项目（61173139）；山东省自然科学重点基金资助项目（ZR2010FM045）；教育部博士点基金资助项目（20110131110027）

Foundation Items: The National Natural Science Foundation of China (61173139)； The Natural Science Foundation of Shandong Province (ZR2010FM045); Doctoral Fund of Ministry of Education of China (20110131110027)

1 引言

当前，许多基于互联网的服务（如试用浏览、电子投票、电子息票、匿名问卷调查等）都要求允许经过认证的用户以匿名方式进行访问，同时服务供应商（简称 AP）可以决定用户访问其应用的次数。为此，Teranishi 等人[1]在 ASIA CRYPT 2004 会议上提出了 *k*-TAA（*k*-times anonymous authentication）（即 *k* 次匿名认证）的概念。与传统的群签名[2]方案相比，*k*-TAA 方案不仅增加了次数限制机制，而且实现了更强的匿名性（即只要用户保持诚实，即使权威也无法获得有关用户身份的任何信息）和可追踪性（即任何的验证者都能根据认证日志对认证次数超过 *k* 次的恶意用户进行追踪）。此后，Nguyen 与 Safavi-Naini[3]提出第一个支持 AP 独立地授予或撤销用户访问权利的动态 *k*-TAA 方案。然而，文献[1,3]方案的认证协议效率不高，这表现在运算耗费与 AP 公开设置的访问次数上界 *k* 呈线性关系，即 $O(k)$。为此，文献[4~7]提出了认证协议更为高效的改进方案。需要指出的是，尽管 Teranishi 等人[4,5]与 Nguyen[6]提出了认证耗费为 $O(1)$的方案，但是使得 AP 的公钥长度与 *k* 呈线性关系，而且要求 AP 保持诚实。否则，与 AP 合谋的用户就能成功躲避方案的追踪过程。最近，Emura 等人[8]指出，已有的方案都要求 AP 为所有用户设置相同的访问次数上界 *k*，而在实际应用中，如 SaaS（software as a service）服务[8]，应当允许愿意支付更多费用的用户获得更大的访问次数。为此，Emura 等人提出一个可选择的 *k* 次放宽匿名认证方案，使得 AP 可以灵活地为每个用户 *i* 设置不同的访问次数上界 k_i。然而，该方案的最大弱点是用户与同一个 AP 间的认证过程是可关联的，即需要以损失用户的部分匿名性作为代价。

综上所述，已有的 *k*-TAA 方案尚未能有效地解决允许 AP 为每个用户灵活设置访问次数上界的问题。此外，已有的方案均未考虑恶意用户发动克隆攻击的问题，即恶意用户对自己的证书进行大规模的共享，从而严重损害了 AP 的利益。需要指出的是，抵抗此类攻击的性质已经在匿名证书系统的设计中得到关注，并称之为证书的不可转移性。根据所采用的技术手段，通常可以将不可转移的证书系统分为 3 种类型[9]。第 1 种是基于硬件（即嵌入的抗篡改设备或外部安全设备）的系统（如文献[10,11]），此类系统的主要缺点是，当使用嵌入的抗篡改设备（如 TPM[10]）时，被攻破的主机有可能会破坏用户的匿名性；当使用外部安全设备（如智能卡[11]）时，系统的不可转移性质严重地依赖于智能卡的长期抗篡改性质[12]。第 2 种是基于生物特征数据的系统（如文献[12, 13]），此类系统的主要缺点是当前将密码技术与以经验为依据的生物特征数据相结合的技术并不成熟[13]，这主要表现在所得方案效率太低，为用户对生物特征读取设备的使用设置了过多的条件[12]等。第 3 种是纯软件的系统（如文献[14~17]）。此类系统的主要缺点是仅能实现较弱的“完全或无”的共享（即要求共享证书的用户事先建立信任关系）[14,15]，或者要求为用户颁发一次性证书，并且要求在线权威在每次认证过程后为用户颁发新证书[16]，即不支持证书重用。最近，Camenisch 等人[17]提出一种较为理想的基于 *n* 次可展示令牌的克隆攻击检测技术，该技术的优势在于：①可有效防止用户大规模地共享证书的行为；②并不要求使用任何的硬件设备；③支持证书重用；④易于与 *k*-TAA 方案相结合。因此，将该项技术作为实现本文设计目标的主要技术手段。

本文对 Au 等人的方案[7]做出扩展，提出第一个不可克隆的动态 *k*-TAA 方案。新方案具备如下的特点：①允许 AP 根据需要为用户设置不同的访问次数上界且不会有损于用户的匿名性；②AP 能独立地授予或撤销用户的访问权利；③成员注册协议实现了理想的并发安全性，因此特别适合于现实的异步网络环境（如 Internet ）；④可以有效防止恶意用户发动大规模的克隆攻击；⑤通过对文献[4,5]的安全模型做出扩展，可以证明新方案满足 *k*-TAA 方案所要求的全部性质。

2 预备知识

2.1 ∑协议

关系 R 的∑协议[18](P, V)是符合 (com, c, res) 形式的 3 轮零知识的知识证明协议。此类协议的公共输入为字符串 x，且证明者 P 拥有秘密的证据 w，使得 $(x,w)\in R$。在 P 与 V 的交互过程中，P 首先发送对 w 的承诺 com，然后 V 返回随机选取的挑战 c，最后 P 向 V 提供应答 res。∑协议要求满足 2 个特殊性质，即诚实验证者的零知识性和特殊可靠性。前者表明给定 x 和 c，可以有效地产生符合正

确分布的会话 (com,c,res)。后者表明根据 x 以及任何可接受的会话 (com,c,res), $(com,\ c',res')$，其中 $c\neq c'$，可以有效地提取出证据 w。

2.2 Ω协议

Ω协议[19,20]与∑协议类似，但此类协议假设存在公共参考字符串[18]，而且允许在无需对证明者执行重绕的条件下从协议的单次执行过程中提取出证据。

2.3 并发零知识

令 (P,V) 为语言 L 的交互式的证明（或论证）系统。所谓并发攻击者 V^* 是指，给定输入 $x\in L$，V^* 能以任意交叉方式与证明者 P 执行任意次数的交互过程。(P,V) 满足并发零知识[21]，条件是对于每个概率多项式时间的并发攻击者 V^*，存在概率多项式时间的模拟器 Sim_{V^*}，使得由 Sim_{V^*} 模拟产生的证明过程副本与由 V^* 在与真实证明者 P 的交互过程中获得的副本满足不可分辨性。

2.4 利用签名方案对∑协议进行增强的技术

在文献[19]中，Garay 等人提出了利用签名方案对底层∑协议进行增强的技术，从而实现模拟可靠性、非可展性以及通用可组合框架下的零知识性，且并发零知识性为这些更强的性质所蕴含。假设 $\Pi=\Sigma^R(x)$ 为关系 R 的标准∑协议。可以采用如下方式对协议 Π 进行增强，从而实现并发零知识性。首先，分别产生签名方案 $\mathrm{SIG}_{\mathrm{adap}}$ 和 $\mathrm{SIG}_{\text{one-time}}$ 的实例，它们分别表示能安全抵抗适应性选择消息攻击的签名方案和一次性签名方案。同时，将 $\mathrm{SIG}_{\mathrm{adap}}$ 方案的公钥 vk 设置为公共参考字符串。然后，利用 OR 关系合成技术[22]将∑协议 Π 增强为 $\Phi=\Sigma^R(x)\vee\Sigma^{R_{vk}}(vk')$ 的形式。其中，子协议 $\Sigma^{R_{vk}}(vk')$ 的作用是证明掌握在 $\mathrm{SIG}_{\mathrm{adap}}$ 方案的公钥 vk 下，$\mathrm{SIG}_{\text{one-time}}$ 方案的公钥 vk' 产生的 $\mathrm{SIG}_{\mathrm{adap}}$ 方案签名。

2.5 Cramer-Shoup 签名方案

在文献[23]中，Cramer 与 Shoup 提出一个基于强 RSA 假设的可证明在适应性选择消息攻击下满足不可伪造性的签名方案。Garay 等人[19]指出，可以利用 Cramer-Shoup 方案实现 $\mathrm{SIG}_{\mathrm{adap}}$ 方案。Cramer-Shoup 方案的具体过程如下。

参数产生：选取 $k'/2$ bit 的安全素数 p,q，设置 RSA 模数 $N=pq$。选取 $x,h\in_R QR_N$，选取 $(k+1)$bit 素数 e'，选取抗碰撞的散列函数 $Hash$: $\{0,1\}^*\to\{0,1\}^k$。设置公钥为 $(N,h,x,e',Hash)$，私钥为 (p,q)。

签名：给定消息 m，选取 $y'\in_R QR_N$，选取 $(k+1)$ bit 素数 $e\neq e'$，计算 $x'=(y')^{e'}h^{-HASH(m)} \bmod N$，$y=(xh^{-HASH(x')})^{e^{-1}\bmod\varphi(N)} \bmod N$。

验证：给定 $(vk,m,(e,y,y'))$，检查 e 是否为 $(k+1)$ bit 奇数且 $e\neq e'$。若是，则计算 $x'=(y')^{e'}h^{-HASH(m)}$，$\bmod N$ 验证是否满足 $x=y^eh^{HASH(x')} \bmod N$。

3 提出的方案

3.1 本文方案的设计思想

本文方案涉及 3 类参与方，即群管理员 GM、服务供应商 AP 与用户 U。本文方案要求用户 U 首先通过与 GM 执行注册协议而获得有效的成员证书 cert。此后，当访问 AP 的服务时，U 需要证明自己掌握该证书。利用动态累加器技术[24]，使得每个 AP 都可以自行维护一个有权访问其应用的用户群体 AG，并根据需要授予或撤销用户访问其应用的能力。为此，U 需要在访问应用之前与 AP 执行一个授予访问权利的协议。在该协议中，AP 灵活地为每个用户设置不同的访问次数上界 k，并向后者提供为这个上界发布的证书 $\mathrm{cert}_{\mathrm{AP}}$。此外，AP 还需要向 U 提供今后能证明自己尚未被从 AG 中废除的证据 W_{AP}。在认证协议中，U 需要向 AP 证明自己拥有合法证书 cert 与 $\mathrm{cert}_{\mathrm{AP}}$。同时，要求 U 在不泄露认证次数上界 k 的条件下证明自己与 AP 执行的认证次数 J_{AP} 尚未超过这个上界。为此，需要使用文献[25]中的关于“一个被承诺元素小于另一个被承诺元素”的证明技术。受文献[17]的启发，为了防止 U 对自己证书 cert 与 $\mathrm{cert}_{\mathrm{AP}}$ 进行大规模的共享，要求 U 在认证协议中证明：在当前的系统周期 t_0 内，自己与所有的 AP 执行的认证次数总数 J 不超过由系统预先设定的次数 n。一旦恶意用户发动了克隆攻击，系统就能检测到这一点，并通过追踪算法揭示该用户的身份。最后，注册协议满足并发零知识性，该性质是借鉴 Garay 等人[19]的技术实现的。需要指出的是，利用相同的技术，可以实现授予访问权利协议的并发零知识性。

3.2 方案的具体描述

假设系统的生命周期可划分为 $2^{l_{\text{time}}}$ 个连续的时间区间，同时假设 GM 与所有的 AP 采用文献[26]中的方法对唯一的时间周期标识符进行协商。

公共参考字符串（CRS, common reference string）。可信算法 F_{CRS}^{D} 产生公共参考字符串，具体如下。

1) 选取 $k'/2$ bit 素数 $\tilde{p},\tilde{q}$，设置 $\tilde{N}_1=\tilde{p}\tilde{q}$。选取 $\tilde{h},\tilde{x},\tilde{h}_1,\tilde{h}_2\in_R QR_{\tilde{N}_1}$，选取$(k+1)$bit 素数 $\tilde{e}'$，选取抗碰撞的散列函数 $Hash:\{0,1\}^*\to\{0,1\}^k$，设置 $\tilde{H}=1+\tilde{N}$。于是，$CRS_1=(\tilde{N}_1,\tilde{h},\tilde{x},\tilde{e}',Hash,\tilde{h}_1,\ \tilde{h}_2,\tilde{H})$，其中，$(\tilde{N}_1,\tilde{h},\tilde{x},\tilde{e}',Hash)$ 构成 Cramer-Shoup 方案的公钥，$(\tilde{N}_1,\tilde{h}_1,\tilde{h}_2)$ 构成模数为 $\tilde{N}_1$ 的整数承诺方案的实例，$(\tilde{N}_1,\tilde{H})$ 构成 Paillier 加密方案[27]的公钥。

2) 选取 $k'/2$ bit 素数 $\tilde{p}',\tilde{q}'$，设置 $\tilde{N}_2=\tilde{p}'\tilde{q}'$，选取 $\tilde{h}_3,\tilde{h}_4\in_R QR_{\tilde{N}_2}$。于是，$CRS_2=(\tilde{N}_2,\tilde{h}_3,\tilde{h}_4)$ 构成模数为 $\tilde{N}_2$ 的整数承诺方案的实例。

3) 丢弃陷门 $Trapdoor_1=(\tilde{p},\tilde{q}),Trapdoor_2=(\tilde{p}',\tilde{q}')$。

对于系统参数，具体定义方法如下。

1) 定义参数 n，表示系统允许用户在每个时间周期内执行认证的最大次数。定义参数 l_p, l_x, l_{time}, l，满足 $l_p\geqslant l_x\geqslant l_{time}+l+1,\ 2^l-1>n$。定义函数 $c(u,v,z)=(u\cdot 2^{l_{time}}+v)2^l+z$，其中，$u\in\{0,1\}^{l_x-l_{time}-l}$，$v\in\{0,1\}^{l_{time}}$，$z\in\{0,1\}^{l_x}$。

2) 令 (G_1,G_2) 为类型 2 的双线性对[28]，满足 $\hat{e}:G_1\times G_2\to G_T$，使得 $ord(G_1)=ord(G_2)=ord(G_T)=p$，$\psi:G_2\to G_1$，其中，$p$ 为 l_p bit 素数。令 G 为椭圆曲线群，使得 DDH（decisional Diffie-Hellman）问题在该群上是困难的[29]，且 $ord(G)=p$。

3) 定义抗碰撞的散列函数 $H:\{0,1\}^*\to Z_p$, $H_{evt}:\{0,1\}^*\to G$。

GM 的系统建立，GM 执行以下过程。

1) 选取 g_0,g_1,g_2,g_3 为群 G_1 的生成元，选取 h_0 为群 G_2 的生成元，满足 $g_0=\psi(h_0)$。假设元素 $g_0,g_1,\ g_2,g_3$ 相互间的离散对数是未知的。选取 $\gamma\in_R Z_p^*$，计算 $w=h_0^{\gamma}$。选取 $u_0\in_R G$。

2) 建立用户识别列表 List，且 List 最初为空。

AP 的系统建立，AP 执行以下过程。

1) 选取 $h_0'\in_R G_2$，选取 g_0',g_1',g_2',g_3' 为群 G_1 的生成元，且满足 $g_0'=\psi(h_0')$。选取 $\gamma'\in_R Z_p^*$，计算 $w'=h_0'^{\gamma'}$。选取 $h_{AP}\in_R G_2,q_{AP}\in_R Z_p^*$，设置 $p_{AP}=h_{AP}^{q_{AP}}$，选取 G_2 上的任意元素作为公开累加值 v_{AP} 的初值。

2) 采用文献[6,7]中的方式建立档案文件 ARC，其中，每个元组都符合 $(arc1,arc2,arc3)$ 的形式，且 $arc1$ 表示用户成员身份公钥中的某个元素，$arc2$ 为单一的比特 1/0，用以指示该用户被授予/撤销访问权利。最后，$arc3$ 是执行完授予/撤销访问操作后得到的累加值。

3) 建立认证日志 Log，设置并公开列表 $VList=(g_0',g_1',g_2',g_3',h_0',w',h_{AP},p_{AP},v_{AP},ARC,v,Log)$，其中，$v$ 表示 AP 的身份。

最终，系统公钥为 $PK=(CRS,H,H_{evt},g_0,g_1,g_2,g_3,h_0,w,u_0,List;VList)$。

用户的系统建立。假设 PKI（public key infrastructure）是存在的。用户 U 选取公/私钥对 $(pk_U,sk_U)=(u_0^{sk_U},sk_U)$，其中，$sk_U\in_R Z_p$。

注册。U 与 GM 执行以下过程。

1) U 选取 $s',t\in_R Z_p$，计算 $C=g_1^{sk_U}g_2^tg_3^{s'}$。然后，U 与 GM 执行协议 $\Phi=\Omega^R(C,pk_U)\vee\Sigma^{R_{vk}}(vk')$。同时，在 List 中添加 (U,pk_U)。协议 Φ 的作用是证明 U 掌握 C 的以 g_1,g_2,g_3 为底的离散对数表达式，同时掌握 pk_U 的以 u_0 为底的离散对数，具体构造过程将在第 4 节中给出。

2) 若 List 中存在表目 (U,pk_U) 且 GM 在协议 Φ 中接受，则 GM 选取 $s'',e\in_R Z_p^*$，计算 $A=(g_0Cg_3^{s''})^{1/(e+\gamma)}$，并向 U 发送 (A,e,s'')。

3) U 设置 $s=s'+s''\bmod p$，并且验证是否满足 $\hat{e}(A,wh_0^e)=\hat{e}(g_0g_1^{sk_U}g_2^tg_3^s,h_0)$，若是，则保存 $J=0,T=1,cert=((sk_U,t,s),A,e)$。其中，$J$ 表示在当前时间周期内展示证书 $cert$ 的次数，T 表示当前的时间周期。

授予访问权利。假设 AP 希望向拥有成员公钥元素 e 的用户 U 授予“可访问自己服务 k 次”的权利，同时假设 AP 的访问群体的当前累加值为 v_j。AP 与 U 执行以下过程。

1) U 选取 $r_1,r_2\in_R Z_p^*$，计算 $A_1=Ag_2^{r_1}$，$A_2=g_1^{r_1}g_2^{r_2}$。选取 $\tilde{s}'\in_R Z_p^*$，计算 $C'=g_1'^{sk_U}g_2'^kg_3'^{\tilde{s}'}$。U 向 AP 提供 NIZK（non-interactive zero knowledge）（即非交互零知识）证明

$$\Pi_2=NIZK\{(sk_U,\tilde{s}',r_1,r_2,r_1e,r_2e,t,s):C'g_2'^{-k}=g_1'^{sk_U}g_3'^{\tilde{s}'}\wedge A_2=g_1^{r_1}g_2^{r_2}\wedge A_2^e=g_1^{r_1e}g_2^{r_2e}\wedge\frac{\hat{e}(A_1,w)}{\hat{e}(g_0,h_0)}\hat{e}(A_1,h_0)^e=\hat{e}(g_1,h_0)^{sk_U}\ \hat{e}(g_2,w)^{r_1}\ \hat{e}(g_2,h_0)^{r_1e}\ \hat{e}(g_2,h_0)^t\ \hat{e}(g_3,h_0)^s\}$$

需要指出的是，Π_2 证明了以下事实：①U 掌握承诺串 C' 的离散对数表达式（但向 AP 揭示了元素 k 的取值）；②U 掌握合法的成员证书 cert，同时将

证书中的元素 A 随机化为 A_1 的形式。

2) 若 Π_2 有效，则 AP 选取 $\tilde{s}'', \tilde{e} \in_R Z_p^*$，计算 $\tilde{A} = (g_0' C' g_3'^{\tilde{s}''})^{1/(\tilde{e}+\gamma')}$ 并向 U 返回 $(\tilde{A}, \tilde{e}, \tilde{s}'')$ 以及证据 $W=v_j$。同时，AP 在 ARC 中增加记录$(e,1,v_{j+1})$，其中，$v_{j+1} = v_j^{e+q_{AP}}$。

3)U 设置 $\tilde{s} = \tilde{s}' + \tilde{s}'' \bmod p$ 并验证是否满足 $\hat{e}(\tilde{A}, w' h_0'^{\tilde{e}}) = \hat{e}(g_0' g_1'^{sk_U} g_2'^{k} g_3'^{\tilde{s}}, h_0')$，$\hat{e}(W, h_{AP}^e p_{AP}) = \hat{e}(v_{j+1}, h_{AP})$，若是，则保存 $cert_{AP} = ((sk_U, k, \tilde{s}), \tilde{A}, \tilde{e}), W, J_{AP} = 0$，其中，$J_{AP}$ 表示 U 与 AP 执行认证过程的次数。

撤销访问权利。假设 AP 希望撤销拥有成员公钥元素 e 的用户 U 的访问权利。假设 ARC 中当前存在 j 条记录，且当前的累加值为 v_j。为此，AP 向 ARC 中添加记录$(e,0,v_{j+1})$，其中，$v_{j+1} = v_j^{1/(e+q_{AP})}$。

认证。假设当前 U 与 AP 正在执行第 J_{AP}（$0 \leqslant J_{AP} < k$）次认证过程，假设 AP 为设置 U 的认证次数上界为 k。假设系统当前的时间周期为 t_0，满足 $0 < t_0 < 2^{l_{time}}$，且 U 在当前周期内展示成员证书的次数为 J ($0 \leqslant J < n$)。假设 AP 的访问群体的当前累加值为 v_{AP}。

1) U 检查是否满足 $T = t_0$，若否，则设置 $T = t_0, J = 0$。若 $T = t_0$ 且 $J \geqslant n$，则终止执行。此外，U 检查是否满足 $J_{AP} \geqslant k$，若是，则终止执行，否则就执行文献[6]中的更新算法 Update，从而计算出证据 W_{AP}，使得 $W_{AP} = v_{AP}^{1/(e+q_{AP})}$。

2) AP 向 U 发送随机种子 $seed_1, seed_2 \in_R \{0,1\}^*$，双方各自在本地计算 $R_i = H_i(seed_i), i = 1,2$。此外，U 计算 $u_{AP} = H_{evt}(v)$。最后，U 向 AP 提供以下证明：

$$\Pi_3 = NIZK\{(\cdots) : (i) A^{e+\gamma} = g_0 g_1^{sk_U} g_2^t g_3^s \wedge (ii) W_{AP}^{e+q_{AP}} = v_{AP} \wedge (iii) S_1 = u_0^{\frac{1}{s+c(0,t_0,J)+1}} \wedge T_1 = pk_U u_0^{\frac{R_1}{s+c(1,t_0,J)+1}} \wedge (iv) 0 \leqslant J < n \wedge (v) S_2 = u_{AP}^{\frac{1}{s+J_{AP}+1}} \wedge T_2 = pk_U u_{AP}^{\frac{R_2}{t+J_{AP}+1}} \wedge (vi) 0 \leqslant J_{AP} < k \wedge (vii) \tilde{A}^{\tilde{e}+\gamma'} = g_0' g_1'^{sk_U} g_2'^{k} g_3'^{\tilde{s}}\}$$

需要指出的是，Π_3 证明了以下事实：①U 拥有合法的群成员身份；②U 尚未被 AP 撤销访问其应用的能力；③追踪标签(S_1,T_1)是采用正确方式产生的；④U 在当前时间周期内展示其成员证书的次数尚未超过 n 次；⑤追踪标签(S_2,T_2)是采用正确方式产生的；⑥U 与 AP 执行的认证次数尚未超过 k 次；⑦AP 已经为 U 授予了访问其应用 k 次的权利。假设上界 n 与 k 的二进制表达式长度分别为 l 和 l'。

Π_3 的构造过程如下。

1)U 选取 $r_1, r_2, r_3, r_4, r_s, r_{sk_U}, r_J, r_0', r_1', \cdots, r_{l-1}', r_5, r_{J_{AP}}, r_k, r_0'', \cdots r_{l'-1}'', r_0''', \cdots, r_{l'-1}''' \in_R Z_p^*$，计算

$A_1 = A g_2^{r_1}, A_2 = g_1^{r_1} g_2^{r_2}, A_3 = W_{AP} g_2^{r_3}, A_4 = g_1^{r_3} g_2^{r_4}$，

$C_s = g_1^s g_2^{r_s}, C_{sk_U} = g_1^{sk_U} g_2^{r_{sk_U}}, C_J = g_1^J g_2^{r_J}$，

$C_{J,0} = g_1^{J_0} g_2^{r_0'}, C_{J,1} = g_1^{J_1} g_2^{r_1'}, \cdots, C_{J,l-1} = g_1^{J_{l-1}} g_2^{r_{l-1}'}$，

$\tilde{C} = \prod_{i=0}^{l-1} C_{J,i}^{2^i} = g_1^{\sum_{i=0}^{l-1} J_i 2^i} g_2^{\sum_{i=0}^{l-1} r_i' 2^i} = g_1^{\tilde{J}} g_2^{\tilde{r}_J}$，

$A_5 = g_1^t g_2^{J_{AP}} g_3^{r_5}, C_{J_{AP}} = g_1^{J_{AP}} g_2^{r_{J_{AP}}}, C_k = g_1^k g_2^{r_k}$，

$C_{J_{AP},0} = g_1^{J_{AP,0}} g_2^{r_0''}, C_{J_{AP},1} = g_1^{J_{AP,1}} g_2^{r_1''}, \cdots,$

$C_{J_{AP},l'-1} = g_1^{J_{AP,l'-1}} g_2^{r_{l'-1}''}, \tilde{C}_{J_{AP}} = \prod_{i=0}^{l'-1} C_{J_{AP},i}^{2^i} =$

$g_1^{\sum_{i=0}^{l'-1} J_{AP,i} 2^i} g_2^{\sum_{i=0}^{l'-1} r_i'' 2^i}, C_{k,0} = g_1^{k_0} g_2^{r_0'''}, C_{k,1} = g_1^{k_1} g_2^{r_1'''}, \cdots,$

$C_{k,l'-1} = g_1^{k_{l'-1}} g_2^{r_{l'-1}'''}, \tilde{C}_k = \prod_{i=0}^{l'-1} C_{k,i}^{2^i} =$

$g_1^{\sum_{i=0}^{l'-1} k_i 2^i} g_2^{\sum_{i=0}^{l'-1} r_i''' 2^i}, A_6 = \tilde{A} g_2^{r_6}, A_7 = g_1^{r_6} g_2^{r_7}$

2) U 产生以下的证明：

$$\Pi_3 = NIZK\{(r_1, r_2, -e, r_1 e, r_2 e, sk_U, t, s, r_3, r_4, r_3 e, r_4 e, \frac{1}{s+c(0,t_0,J)+1}, -\frac{r_s + r_J}{s+c(0,t_0,J)+1}, \frac{1}{s+c(1,t_0,J)+1}, -\frac{r_s + r_J}{s+c(1,t_0,J)+1}, r_{sk_U}, r_0', \cdots, r_{l-1}', J, r_J, r_J - \tilde{r}_J, J_{AP}, r_5, sk_U t, J_{AP} sk_U, r_5 sk_U, r_0'', \cdots, r_{l'-1}'', r_0''', \cdots, r_{l'-1}''', r_{J_{AP}}, r_{J_{AP}} - \sum_{i=0}^{l'-1} r_i'' 2^i, k, r_k, r_k - \sum_{i=0}^{l'-1} r_i''' 2^i, r_{l'-1}'' - r_{l'-1}''', \cdots, r_1'' - r_1''', r_6, r_7, -\tilde{e}, r_6 \tilde{e}, r_7 \tilde{e}, \tilde{s}) :$$

$$(i) A_2 = g_1^{r_1} g_2^{r_2} \wedge 1 = A_2^{-e} g_1^{r_1 e} g_2^{r_2 e} \wedge \frac{\hat{e}(A_1, w)}{\hat{e}(g_0, h_0)} = \hat{e}(A_1, h_0)^{-e}\ \hat{e}(g_1, h_0)^{sk_U}\ \hat{e}(g_2, w)^{r_1}\ \hat{e}(g_2, h_0)^{r_1 e} \hat{e}(g_2, h_0)^t\ \hat{e}(g_3, h_0)^s \wedge (ii) A_4 = g_1^{r_3} g_2^{r_4} \wedge 1 = A_4^{-e} g_1^{r_3 e} g_2^{r_4 e} \wedge \frac{\hat{e}(A_3, p_{AP})}{\hat{e}(v_{AP}, h_{AP})} = \hat{e}(A_3, h_{AP})^{-e}\ \hat{e}(g_2, p_{AP})^{r_3}\ \hat{e}(g_2, h_{AP})^{r_3 e} \wedge$$

$$(iii) g_1 = (C_s g_1^{c(0,t_0,0)+1} C_J)^{\frac{1}{s+c(0,t_0,J)+1}} g_2^{-\frac{r_s+r_J}{s+c(0,t_0,J)+1}} \wedge S_1 = u_0^{\frac{1}{s+c(0,t_0,J)+1}} \wedge g_1 = (C_s g_1^{c(1,t_0,0)+1} C_J)^{\frac{1}{s+c(1,t_0,J)+1}} g_2^{-\frac{r_s+r_J}{s+c(1,t_0,J)+1}} \wedge C_{sk_U} = g_1^{sk_U} g_2^{r_{sk_U}} \wedge T_1 = u_0^{sk_U} (u_0^{R_1})^{\frac{1}{s+c(1,t_0,J)+1}} \wedge$$

$$(iv)(C_{J,0} = g_2^{r_0'} \vee C_{J,0} / g_1 = g_2^{r_0'}) \wedge \cdots \wedge (C_{J,l-1} = g_2^{r_{l-1}'} \vee C_{J,l-1} / g_1 = g_2^{r_{l-1}'}) \wedge C_J = g_1^J g_2^{r_J} \wedge C_J / \tilde{C}_J = g_2^{r_J - \tilde{r}_J} \wedge (v) u_{AP} / S_2 = S_2^s S_2^{J_{AP}} \wedge A_5 = g_1^t g_2^{J_{AP}} g_3^{r_5} \wedge 1 = g_1^{sk_U t} g_2^{J_{AP} sk_U} g_3^{r_5 sk_U} A_5^{-sk_U} \wedge T_2 / u_{AP}^{R_2} = u_0^{sk_U t} u_0^{sk_U J_{AP}} u_0^{sk_U} T_2^{-t} T_2^{-J_{AP}} \wedge$$

$(vi)(C_{J_{\mathrm{AP},0}} = g_2^{r_0''} \vee C_{J_{\mathrm{AP},0}} / g_1 = g_2^{r_0''})$

$\wedge \cdots \wedge (C_{J_{\mathrm{AP},l'-1}} = g_2^{r_{l'-1}''} \vee C_{J_{\mathrm{AP},l'-1}} / g_1 = g_2^{r_{l'-1}''})$

$\wedge (C_{k,0} = g_2^{r_0'''} \vee C_{k,0} / g_1 = g_2^{r_0'''}) \wedge \cdots \wedge$

$(C_{k,l'-1} = g_2^{r_{l'-1}'''} \vee C_{k,l'-1} / g_1 = g_2^{r_{l'-1}'''}) \wedge$

$C_{J_{\mathrm{AP}}} = g_1^{J_{\mathrm{AP}}} g_2^{r_{J_{\mathrm{AP}}}} \wedge C_{J_{\mathrm{AP}}} / \tilde{C}_{J_{\mathrm{AP}}} = g_2^{r_{J_{\mathrm{AP}}} - \sum_{i=0}^{l'-1} r_i''' 2^i} \wedge$

$C_k = g_1^k g_2^{r_k} \wedge C_k / \tilde{C}_k = g_2^{r_k - \sum_{i=0}^{l'-1} r_i''' 2^i} \wedge$

$$\left(\begin{array}{l} (C_{J_{\mathrm{AP},l'-1}} / C_{k,l'-1} = g_2^{r_{l'-1}'' - r_{l'-1}'''} \wedge C_{J_{\mathrm{AP},l'-2}} = g_2^{r_{l'-2}''} \wedge \\ C_{k,l'-2} / g_1 = g_2^{r_{l'-2}'''}) \vee (C_{J_{\mathrm{AP},l'-1}} / C_{k,l'-1} = \\ g_2^{r_{l'-1}'' - r_{l'-1}'''} \wedge C_{J_{\mathrm{AP},l'-2}} / C_{k,l'-2} = g_2^{r_{l'-2}'' - r_{l'-2}'''} \wedge \\ C_{J_{\mathrm{AP},l'-3}} = g_2^{r_{l'-3}''} \wedge C_{k,l'-3} / g_1 = g_2^{r_{l'-3}'''}) \vee \cdots \vee \\ (C_{J_{\mathrm{AP},l'-1}} / C_{k,l'-1} = g_2^{r_{l'-1}'' - r_{l'-1}'''} \wedge \cdots \wedge C_{J_{\mathrm{AP},1}} / C_{k,1} \\ = g_2^{r_1'' - r_1'''} \wedge C_{J_{\mathrm{AP},0}} = g_2^{r_0''} \wedge C_{k,0} / g_1 = g_2^{r_0'''}) \end{array} \right) \wedge$$

$(vii) A_7 = g_1^{r_6} g_2^{r_7} \wedge 1 = A_7^{-\bar{e}} g_1^{r_6 \bar{e}} g_2^{r_7 \bar{e}} \wedge$

$$\frac{\hat{e}(A_6, w')}{\hat{e}(g_0', h_0')} = \hat{e}(g_1', h_0')^{sk_{\mathrm{U}}} \ \hat{e}(g_2', h_0')^{k} \ \hat{e}(g_3', h_0')^{\bar{s}} \cdot$$

$$\hat{e}(A_6, h_0')^{-\bar{e}} \ \hat{e}(g_2, w')^{r_6} \ \hat{e}(g_2, h_0')^{r_6 \bar{e}} \}$$

其中，$c(0, t_0, 0) = t_0 2^l$，$c(1, t_0, 0) = (2^{l_{time}} + t_0) 2^l$，$c(0, t_0, J) = t_0 2^l + J$，$c(1, t_0, J) = (2^{l_{time}} + t_0) 2^l + J$。

3) *AP* 执行以下过程：若 Π_3 有效且 $S_1, S_2 \notin Log$，则 AP 在 *Log* 中保存 $(t_0, R_1, R_2, S_1, T_1, S_2, T_2, \Pi_3)$ 并输出 accept。若 Π_3 有效且 $(S_1 \in Log) \vee (S_2 \in Log)$，则 AP 在 *Log* 中保存 $(t_0, R_1, R_2, S_1, T_1, S_2, T_2, \Pi_3)$ 并输出 refuse，否则，直接输出 refuse。

4) 若 AP 在上述过程中输出 accept，则 U 执行 $J = J + 1, J_{\mathrm{AP}} = J_{\mathrm{AP}} + 1$。

公开的追踪。检查 *Log* 中是否存在表目 $(t_0, R_1, R_2, S_1, T_1, S_2, T_2, \Pi_3), (t_0', R_1', R_2', S_1', T_1', S_2', T_2', \Pi_3')$，且满足 $(S_1 = S_1') \vee (S_2 = S_2')$：若是，则执行如下操作。

① 检查 Π_3, Π_3' 是否都为有效，若是，则转②；否则，输出 Π_3 并停止运行。

② 检查是否满足 $(R_1 \neq R_1') \wedge (R_2 \neq R_2')$，若否，则输出 Π_3 并停止运行。若是，则在 $S_1 = S_1'$ 且 $t_0 = t_0'$ 的情况下计算 $pk_{\mathrm{U}} = \dfrac{T_1}{(T_1 / T_1')^{R_1 / (R_1 - R_1')}}$，而在 $S_2 = S_2'$ 的情况下，计算 $pk_{\mathrm{U}} = \dfrac{T_2}{(T_2 / T_2')^{R_2 / (R_2 - R_2')}}$。

然后，在 List 中搜索是否存在表目 $(\mathrm{U}, pk_{\mathrm{U}})$，若是，则输出 U，否则，输出 GM。

4 协议 Φ 的构造过程及其安全性

在注册协议中，为了实现并发零知识性，采用 Garay 等人的技术将底层∑协议 $\Pi_1 = PK\{(sk_{\mathrm{U}}, t, s') : C = g_1^{sk_{\mathrm{U}}} g_2^t g_3^{s'} \wedge pk_{\mathrm{U}} = u_0^{sk_{\mathrm{U}}}\}$ 增强为协议 Φ。具体地，协议 $\Phi = \Omega^R(C, pk_{\mathrm{U}}) \vee \Sigma^{R_{vk}}(vk')$ 是采用 OR 合成技术对子协议 A 与 B 进行合成而得到的。子协议 $A = \Omega^R(C, pk_{\mathrm{U}})$ 表明 U 掌握秘密元组 (sk_{U}, t, s')，且满足关系 $R = \{C, pk_{\mathrm{U}}, (sk_{\mathrm{U}}, t, s') : C = g_1^{sk_{\mathrm{U}}} g_2^t g_3^{s'} \wedge pk_{\mathrm{U}} = u_0^{sk_{\mathrm{U}}}\}$。子协议 $B = \Sigma^{R_{vk}}(vk')$ 表明 U 掌握在 Cramer-Shoup 方案公钥 $vk = \{\tilde{N}_1, \tilde{h}, \tilde{x}, \tilde{e}', Hash\}$ 下为一次性签名方案 $\mathrm{SIG}_{\text{one-time}}$ 的公钥 vk' 产生的有效签名 $(\bar{e}, \bar{y}, \bar{y}')$，即满足关系 $R_{vk} = \{\tilde{x}\tilde{h}^{-Hash(\bar{x}')}, (\bar{y}, \bar{e}) : \tilde{x}\tilde{h}^{-Hash(\bar{x}')} = \bar{y}^{\bar{e}} \bmod \tilde{N}_1\}$。子协议 A 是利用文献[19]的技术实现。为了实现子协议 B，要求 U 首先向 GM 提供 $\bar{y}'$（该元素与 $QR_{\tilde{N}_1}$ 上的随机元素满足不可分辨性），然后采用文献[30]的技术证明自己掌握秘密数对 $(\bar{y}, \bar{e})$，使得 $\tilde{x}\tilde{h}^{-Hash(\bar{x}')} = \bar{y}^{\bar{e}} \bmod \tilde{N}_1$。在具体合成过程中，子协议 A 是采用诚实方式产生的，而子协议 B 是采用标准的模拟方式产生的。此外，尽管利用标准的∑协议实现子协议 A 就足以实现并发零知识性，但本文采用了更强的 Ω 协议，其目的是使得协议 Φ 具有直线提取器。Garay 等人[19]指出，可以利用著名的 DSA（digital signature algorithm）方案具体实现一次性签名方案 $\mathrm{SIG}_{\text{one-time}}$。为了描述过程的简单，同样使用了 $\mathrm{SIG}_{\text{one-time}}$ 这个抽象形式。协议 Φ 的具体执行过程如下。

1) U 自行产生 $\mathrm{SIG}_{\text{one-time}}$ 方案的公/私钥对 (vk', sk')，选取 $\bar{y}' \in_R QR_{\tilde{N}_1}$，计算 $\bar{x}' = (\bar{y}')^{\tilde{e}'} \tilde{h}^{-Hash(vk')} \bmod \tilde{N}_1$，选取 $C_{\bar{y}}, C_w \in_R Z_{\tilde{N}_1}$。选取 $\alpha, \beta, \gamma \in_R Z_{\tilde{N}_1}^*$，计算 $E_1 = \tilde{H}^{sk_{\mathrm{U}}} \alpha^{\tilde{N}_1} \bmod \tilde{N}_1^2$，$E_2 = \tilde{H}^{t} \beta^{\tilde{N}_1} \bmod \tilde{N}_1^2$，$E_3 = \tilde{H}^{s'} \gamma^{\tilde{N}_1} \bmod \tilde{N}_1^2$。选取 $r_{sk_U}, r_t, r_{s'} \in \in_R Z_{\tilde{N}_1}^*$，计算 $S_1 = \tilde{h}_3^{sk_{\mathrm{U}}} \ \tilde{h}_4^{r_{sk_{\mathrm{U}}}} \bmod \tilde{N}_2$，$S_2 = \tilde{h}_3^{t} \tilde{h}_4^{r_t} \bmod \tilde{N}_2$，$S_3 = \tilde{h}_3^{s'} \tilde{h}_4^{r_{s'}} \bmod \tilde{N}_2$。然后，向 GM 发送 $(C, pk_{\mathrm{U}}, vk', \bar{y}', \bar{x}', C_{\bar{y}}, C_w, E_1, E_2, E_3, S_1, S_2, S_3)$。

2) GM 验证等式 $\bar{x}' = (\bar{y}')^{\tilde{e}'} \tilde{h}^{-HASH(vk')} \bmod \tilde{N}_1$ 是否成立，若是，则 U 与 GM 执行如下的证明：

$\Pi_1 = PK\{(sk_{\mathrm{U}}, t, s', \alpha, \beta, \gamma, r_{sk_{\mathrm{U}}}, r_t, r_{s'}, \bar{e}, w\bar{e}, w, r_w, r_w\bar{e}) :$

$(C = g_1^{sk_{\mathrm{U}}} g_2^t g_3^{s'} \wedge pk_{\mathrm{U}} = u_0^{sk_{\mathrm{U}}} \wedge E_1 = \tilde{H}^{sk_{\mathrm{U}}} \alpha^{\tilde{N}_1} \bmod \tilde{N}_1^2 \wedge$

$E_2 = \tilde{H}^t \beta^{\tilde{N}_1} \bmod \tilde{N}_1^2 \wedge E_3 = \tilde{H}^{s'} \gamma^{\tilde{N}_1} \bmod \tilde{N}_1^2 \wedge$
$S_1 = \tilde{h}_3^{sk_U} \tilde{h}_4^{r_{sk_U}} \bmod \tilde{N}_2 \wedge S_2 = \tilde{h}_3^t \tilde{h}_4^{r_t} \bmod \tilde{N}_2 \wedge$
$S_3 = \tilde{h}_3^{s'} \tilde{h}_4^{r_{s'}} \bmod \tilde{N}_2) \vee (\tilde{x}\tilde{h}^{-Hash(\vec{x}')} = C_{\vec{y}}^{\vec{e}} \tilde{h}_1^{-w\vec{e}} \bmod \tilde{N}_1 \wedge$
$C_w = \tilde{h}_1^w \tilde{h}_2^{r_w} \bmod \tilde{N}_1 \wedge 1 = C_w^{\vec{e}} \tilde{h}_1^{-w\vec{e}} \tilde{h}_2^{-r_w\vec{e}} \bmod \tilde{N}_1)\}$。

3) 若 GM 在上述证明中接受，则 U 向 GM 提供使用 sk' 为上述证明过程的副本 *transcript* 产生的 $\mathrm{SIG}_{\text{one-time}}$ 方案签名 s。

4) GM 利用 vk' 验证 s 的有效性，若有效，则接受。

定理 1　在公共参考字符串模型下，协议Φ是具有直线提取器的并发零知识的知识证明协议。

证明　在以下证明过程中，用 (com_1, c_1, res_1) 表示子协议 A 的副本，用 (com_2, c_2, res_2) 表示子协议 B 的副本。

证据不可分辨性。协议Φ是采用标准的 OR 关系合成技术构造的，而根据文献[19]结论可知，采用这种方式构造的协议满足证据不可分辨性。

并发零知识性。协议Φ的模拟器 Sim_Φ 以 C, pk_U 作为输入，并在不掌握秘密元组 (sk_U, t, s') 的情况下与验证者 V 执行以下的模拟过程。

1) Sim_Φ 采用本文方案中描述的方式自行产生 CRS。

2) Sim_Φ 以并发方式与验证者 V 执行以下的交互过程：

① Sim_Φ 自行产生方案 $\mathrm{SIG}_{\text{one-time}}$ 的公/私钥对 (vk', sk')，利用陷门 $Trapdoor_1 = (\tilde{p}, \tilde{q})$ 产生对消息 vk' 的 Cramer-Shoup 方案签名 $(\vec{e}, \vec{y}, \vec{y}')$。$Sim_\Phi$ 选取 $E_1, E_2, E_3 \in_R Z_{\tilde{N}_1^2}, S_1, S_2, S_3 \in_R Z_{\tilde{N}_2}$。

② Sim_Φ 选取 $c_1 \in_R Z_{p^2}$，以 C, pk_U, c_1 为输入调用子协议 A 的模拟器 Sim_A，从而获得可接受的副本 (com_1, c_1, res_1)。Sim_Φ 选取 $w, r_w \in_R Z_{\tilde{N}_1}$，计算 $C_{\vec{y}} = \vec{y}\tilde{h}_1^w \bmod \tilde{N}_1, C_w = \tilde{h}_1^w \tilde{h}_2^{r_w} \bmod \tilde{N}_1$。$Sim_\Phi$ 向 V 发送元组 $(C, pk_U, vk', \vec{y}', \vec{x}', C_{\vec{y}}, C_w, E_1, E_2, E_3, S_1, S_2, S_3)$。

③V 验证等式 $\vec{x}' = (\vec{y}')^{\vec{e}'} \tilde{h}^{-Hash(vk')} \bmod \tilde{N}_1$ 是否成立，若否，则终止协议。

④ Sim_Φ 向 V 发送 (com_1, com_2)，其中，com_2 是以诚实方式产生的。

⑤V 返回挑战 $c \in Z_p$。

⑥ Sim_Φ 设置 $c_2 = c_1 - c$。根据 com_2 与 c_2 以诚实方式产生 res_2，向 V 发送 $(c_1, res_1), (c_2, res_2)$。

⑦V 验证以下条件是否同时得到满足，即 (com_1, c_1, res_1) 为可接受的子协议 A 的副本；(com_2, c_2, res_2) 为可接受的子协议 B 的副本；$c = c_1 - c_2$。

显然，不掌握 (sk_U, t, s') 的 Sim_Φ 可以在无需对 V 执行重绕的条件下实现对协议Φ的完全模拟。而根据协议Φ的证据不可分辨性质可知，V 无法分辨在上述的交互过程中，子协议 A 是由掌握秘密元组 (sk_U, t, s') 的真实用户 U 产生的，还是由模拟器 Sim_Φ 产生的。因此，协议Φ满足并发的零知识。

知识证明性质由于子协议 A 是关于“掌握秘密元组 (sk_U, t, s')”的Ω协议，因此协议Φ的知识提取器可以直接调用子协议 A 的直线提取器，后者将利用陷门对 Paillier 密文 E_1, E_2, E_3 执行解密，从而获得证据 (sk_U, t, s')。

5　方案的安全性分析

本文方案的安全性证明基于了文献[4,5]的安全模型，但需要对其中的可检测性的实验做出如下的修改：1）修改攻击者 **A** 的获胜条件，即若发生以下 2 种情况之一，则判定 **A** 获胜。①认证日志 Log_v 中包含超过 $\sum_{i=1}^{\#List} k_i$ 个元组，且追踪算法（此后记为 *Trace*）在 (v, API_v, Log_v) 上的输出为 *None*，其中，v 表示 *AP* v 的身份，Log_v 表示 *AP* v 的认证日志，$\#List$ 表示列表 *List* 中的元组数量，k_i 表示 *AP* v 为每个用户 U_i 设置的认证次数上界，API_v 表示 *AP* v 的公开信息。②在当前的时间周期 t_0 中，*AP* v 在 Log_v 中写入了超过 $n \cdot \#List$ 条记录，且 *Trace* 算法在 (v, API_v, Log_v) 上的输出为 *None*。2) 采用文献[6]中的方式在实验中增加 3 个预言机，即 $O_{Gran\text{-}AP}, O_{Revo\text{-}AP}, O_{Coll\text{-}AP}$。

在安全性证明中，采用了如下的证明思想。算法 **A** 代表了系统中已经被攻击者控制的参与方，算法 **B** 负责对系统中尚未被攻破的部分进行模拟，并且向 **A** 提供预言机服务 O_{List}, O_{VList}, O_{Issue}, O_{Join}, $O_{AP\text{-}Setup}$, $O_{Verify}, O_{Gran\text{-}AP}, O_{Reve\text{-}AP}, O_{Corr\text{-}AP}$, O_{Proof}, O_{Query}。其中，O_{List}、O_{VList} 的作用是以诚实方式对公开列表 *List*, *VList* 进行管理。O_{Issue} 的作用是代表 GM 以诚实方式执行注册协议。O_{Join} 的作用是代表用户以诚实方式执行注册协议。$O_{AP\text{-}Setup}$ 的作用是代表 AP 以诚实方式执行 AP 的系统建立算法。O_{Verify} 的作用是代表 AP 以诚实方式执行认证协议中的验证过程。

$O_{Gran\text{-}AP}$, $O_{Reve\text{-}AP}$ 的作用是代表 AP 以诚实方式执行授予/撤销用户访问权利的操作。$O_{Corr\text{-}AP}$ 的作用是攻破诚实的 AP。O_{Proof} 的作用是代表用户以诚实方式执行认证协议。O_{Query} 的作用是向攻击者提供作为挑战的认证协议副本。

定理 2 在群 (G_1,G_2) 上的 q-SDH（q-strong diffie-hellman）的假设[31]，群 G 上的 y-DDHI（y-decisional Diffie-Hellman inversion）假设[7]和离散对数假设下，本文方案可证满足正确性、可检测性、匿名性、用户的可开脱性、GM 的可开脱性以及 AP 的可开脱性。

正确性。限于篇幅，省略了具体过程。

可检测性。假设攻击者 **A** 能以不可忽略概率攻破本文方案的可检测性，则能借助 **A** 构造归约算法 **B**，且 **B** 能以不可忽略的概率攻破文献[24]动态累加器方案的抗碰撞性或文献[7]签名方案（作者称之为 BBS+方案）的不可伪造性。假设 **A** 在实验中的执行步骤总数为 T。**B** 获得 2 个 BBS+方案实例的公钥 $(g_0,g_1,g_2,g_3,h_0,w),(g_0',g_1',g_2',g_3',h_0',w')$ 以及给定的 q-SDH 问题实例 $(g_0'',h_0'',h_0''^{z},\cdots,h_0''^{z^q})\in_R G_1\times G_2^q$。**B** 在这些输入的基础上创建本文方案的一个实例，事先选取 $v_0\in_R\{1,\cdots,T\}$，并在可检测性实验过程中对预言机 O_{List},O_{VList},O_{Issue},$O_{AP\text{-}Setup}$, O_{Verify}, $O_{Gran\text{-}AP}$, $O_{Reve\text{-}AP}$, $O_{Corr\text{-}AP}$ 进行模拟。具体执行过程如下。

O_{List},O_{VList} **B** 采用诚实方式分别对列表 *List* 与 *VList* 进行管理，具体可以参考文献[5]。

O_{Issue} 在模拟过程中，当 **A** 提供 C,pk_{U} 并且与 **B** 执行协议Φ，**B** 利用协议Φ的直线提取器从密文 E_1,E_2,E_3 中提取出秘密证据 (sk_U,t,s')，**B** 将 C 提供给第一个 BBS+方案的签名预言机，并获得后者返回的 (A,e,s'')。此时，**B** 向 **A** 提供 (A,e,s'')，然后自行保存 $cert=((sk_{\mathrm{U}},t,s=s'+s''\bmod p),A,e)$。

$O_{AP\text{-}Setup}$ 在模拟过程中，**B** 根据 **A** 的请求创建身份为 v 的诚实 *AP* v。若 $v\neq v_0$，则 **B** 选取 $h_0'\in_R G_2$，选取 g_0',g_1',g_2',g_3' 为群 G_1 的生成元，且满足 $g_0'=\psi(h_0')$。选取 $\gamma'\in_R Z_p^*$，计算 $w'=h_0'^{\gamma'}$。选取 $h_{AP}\in_R G_2,q_{\mathrm{AP}}\in_R Z_p^*$，设置 $p_{\mathrm{AP}}=h_{\mathrm{AP}}^{q_{\mathrm{AP}}}$，选取 $v_{AP}\in_R G_2$。若 $v=v_0$，则 **B** 在第 2 个 BBS+方案公钥 $(g_0',g_1',g_2',g_3',h_0',w')$ 的基础上模拟产生 $(h_{\mathrm{AP}},p_{\mathrm{AP}},v_{\mathrm{AP}})$，即选取 $f\in_R Z_p^*$，设置 $h_{\mathrm{AP}}=h_0'',p_{\mathrm{AP}}=h_0''^{z},v_{\mathrm{AP}}=h_0''^{f}$，其中，$v_{\mathrm{AP}}$ 表示 *AP* v 维护的公开累加值的初值。

O_{Verify}**B** 采用诚实方式执行认证协议中的步骤 2）与 3）。

$O_{Gran-AP}$ **B** 以诚实方式执行 *AP* v 授予用户访问权利的操作，并借助 q-SDH 问题实例 $(g_0'',h_0'',h_0''^{z},\cdots,h_0''^{z^q})$ 计算更新后的累加值。

$O_{Reve\text{-}AP}$**B** 以诚实方式执行 *AP* v 撤销用户访问权利的操作，并且借助 q-SDH 问题的实例 $(g_0'',h_0'',h_0''^{z},\cdots,h_0''^{z^q})$ 计算更新后的累加值。

$O_{Corr-AP}$ **B** 根据 **A** 的请求 v 向其提供被攻破的 *AP* v 的私钥。若 $v=v_0$，则 **B** 运行失败。

假设 **A** 最终在当前实验中获胜，采用文献[5]中的做法，假设 $v=v_0$ 成立（原因是 **A** 至多能访问预言机 $O_{\text{AP-Setup}}$ 多项式，因此关系 $v=v_0$ 在不可忽略的概率下得到满足）。

根据可检测性定义中的获胜条件，此时必然属于以下 4 种情况之一。

情况 1 **A** 为某个拥有合法成员证书的用户伪造了有效的证据 W_{AP}^*，从而与 *AP* v 执行了超过 $\sum_{i=1}^{\#List}k_i$ 次认证过程。假设 *AP* v 的公开档案文件为 $ARC_v=\{(e_i,\cdot,\cdot)\}_{i=1}^{\#List}$，且 *AP* v 的当前累加值为 $v_{AP}=(h_0''^{f})^{\prod_{i=1}^{\#List}(e_i+z)}$。此时，**B** 通过对 **A** 执行重绕而从证明 Π_3 中提取出秘密证据 $(e^*,W_{\mathrm{AP}}^*,\cdots)$，使得 $e^*\notin\{e_1,\cdots,e_{\#List}\}$。由动态累加器的性质[24]可知，此时必然满足

$$W_{AP}^*=(h_0''^{f})^{\prod_{i=1}^{\#List}\frac{e_i+z}{e^*+z}}=(h_0''^{f})^{\frac{\sum_{i=0}^{\#List}A_i'z^i}{e^*+z}}=(h_0''^{f})^{Q(z)+\frac{r}{e^*+z}},$$

$$Q(z)=\sum_{i=0}^{\#List-1}A_i'z^i$$

于是，可以得出 $h_0''^{\frac{1}{e^*+z}}=\left(W_{\mathrm{AP}}^*/(h_0''^{f})^{Q(z)}\right)^{1/fr}$，从而攻破了文献[24]动态累加器的抗碰撞性，即违背了 q-SDH 假设。

情况 2 **A** 为某个用户伪造了新的成员证书 *cert*，从而与 *AP* v 在当前的时间周期 t_0 内执行了超过 $n\cdot\#List$ 次的认证过程，使得 *AP* v 在时间周期 t_0 内在 Log_v 中写入了超过 $n\cdot\#List$ 个元组。对于 $u=1,\cdots,\#List$ 以及 $J=0,\cdots,n-1$，**B** 计算元素 $S_{1,u,J}=u_0^{\frac{1}{s_u+c(0,J_0,J)+1}}$。由于 Log_v 中含有超过 $n\cdot\#List$ 个形式为 $(t_0,R_1,R_2,S_1,T_1,S_2,T_2,\Pi_3)$ 的元组，因此其中必然存在某个元组 $(t_0,R_1^*,R_2^*,S_1^*,T_1^*,S_2^*,T_2^*,\Pi_3^*)$，使得 $S_1^*\neq S_{1,u,J},u=1,\cdots,\#List,J=0,\cdots,n-1$。通过对 **A** 执行重绕，**B** 可以从 Π_3^* 中提取出秘密证据

$(\cdots, sk_U^*, t^*, s^*, J^*, \cdots)$，使得事实 $(i)\sim(vii)$ 成立，其中，事实 (iii) 表明 $S_1^* = u_0^{\frac{1}{s^*+c(0,t_0,J^*)+1}}$。由于 $J^* \in \{0,\cdots,n-1\}$，因此 $s^* \notin \{s_1,\cdots,s_{\#List}\}$。这表明 **A** 为一个新的成员秘密元组 (sk_U^*, t^*, s^*) 伪造了有效的 BBS+方案签名，从而得出与第一个 BBS+方案的不可伪造性间的矛盾，即违背了 q-SDH 假设。

情况 3　**A** 为某个用户 U_i 伪造了新的成员证书 $cert$，从而与 AP v 执行了超过 k_i 次的认证过程。

对于 $u = 1,\cdots,\#List$ 以及 J_{AP} 的所有可能取值，**B** 计算元素 $S_{2,u,J_{\mathrm{AP}}} = u_{\mathrm{AP}}^{\frac{1}{s_u+J_{\mathrm{AP}}+1}}$。由于 Log_v 中含有超过 $\sum_{i=1}^{\#List} k_i$ 个元组，因此必然存在元组 $(t_0^*, R_1^*, R_2^*, S_1^*, T_1^*, S_2^*, T_2^*, \Pi_3^*)$，使得 $S_2^* \neq S_{2,u,J_{\mathrm{AP}}}$。通过对 **A** 执行重绕，**B** 可以从 Π_3^* 中提取出秘密证据 $(\cdots, sk_U^*, t^*, s^*, J_{AP}^*, \cdots)$，使得事实 $(i)\sim(vii)$ 成立。根据事实 (v) 可知，$S_2^* = u_{\mathrm{AP}}^{\frac{1}{s^*+J_{\mathrm{AP}}^*+1}}$。由于 $S_2^* \neq S_{2,u,J_{\mathrm{AP}}}$ 且 J_{AP} 已经取遍所有可能的取值，因此 $s^* \notin \{s_1,\cdots,s_{\#List}\}$。这表明 **A** 为新的成员秘密元组 $(sk_{\mathrm{U}}^*, t^*, s^*)$ 伪造了有效的 BBS+方案签名，从而得出与第一个 BBS+方案的不可伪造性间的矛盾，即违背了 q-SDH 假设。

情况 4　**A** 为某个用户 U_i 伪造了关于认证次数上界 $k^* > k_i$ 的新证书 $cert_{\mathrm{AP}}$，从而与 AP v 执行了超过 k_i 次的认证过程。由于 Log_v 中含有超过 $\sum_{i=1}^{\#List} k_i$ 个元组，与情况 3 类似，必然存在元组 $(t_0^*, R_1^*, R_2^*, S_1^*, T_1^*, S_2^*, T_2^*, \Pi_3^*)$，使得 $S_2^* \neq S_{2,u,J_{AP}}$。

通过对 **A** 执行重绕，**B** 可以从 Π_3^* 中提取出秘密证据 $(\cdots, sk_U^*, k^*, \tilde{s}^*, \tilde{A}^*, \tilde{e}^*, J_{AP}^*, \cdots)$，使得事实 $(i)\sim(vii)$ 成立。根据事实 (vi, vii) 可知，$0 \leqslant J_{AP}^* < k^*$，$(\tilde{A}^*)^{\tilde{e}^*+\gamma'} = g_0' g_1'^{sk_U^*} g_2'^{k^*} g_3'^{\tilde{s}^*}$。由于 $S_2^* = u_{\mathrm{AP}}^{\frac{1}{s^*+J_{\mathrm{AP}}^*+1}}$ 且满足 $s^* \in \{s_1,\cdots,s_{\#List}\}$（因为 **A** 并未伪造新的证书 $cert$），这表明 **A** 必然为某个新的上界 $k^* > k_i$ 伪造了 BBS+方案签名，使得 $k_i < J_{\mathrm{AP}}^* < k^*$，从而得出与第 2 个 BBS+方案的不可伪造性间的矛盾，即违背了 q-SDH 假设。

匿名性。对于 $c = 0,1$，定义函数 $f_{G,(\cdot)}^{(c)}(\cdot)$。$c = 0$ 时，该函数是群 G 上的真正的随机函数，$c = 1$ 时，该函数是群 G 上的 Dodis-Yampolskiy 伪随机函数[32]。假设攻击者 **A** 能以不可忽略概率攻破本文方案的匿名性，则能得出与 Dodis-Yampolskiy 伪随机函数安全性间的矛盾。在实验开始之前，归约算法 **B** 预先确定目标用户 u_1, u_2，选取 $\beta \in_R \{0,1\}$。在实验过程中，**B** 需要对预言机 O_{List}, O_{VList}, O_{Join}, O_{Proof}, O_{Query} 进行模拟。具体过程如下。

O_{List}, O_{VList}. 模拟方法同上。

O_{Join} 在模拟过程中，**B** 以诚实用户 $u_i (i = 1,2)$ 的身份与 **A** 共同执行本文方案的注册协议并采用如下方式与 **A** 进行交互。首先，**B** 选取 $C_i \in_R G_1$, $pk_i \in_R G$，**B** 将 (C_i, pk_i) 写入 $List$ 并且向 **A** 提供 C_i, pk_i，同时 **B** 借助协议Φ的模拟器 Sim_Φ与 **A** 进行交互。在获得 **A** 返回的元组 (A_i, e_i, s_i'') 之后，**B** 保存 $cert_i = ((-,-,-), A_i, e_i)$，其中“−”表示未知元素。

O_{Proof} 在模拟过程中，**B** 以诚实用户 u_i 的身份与 **A** 执行认证协议，具体方法是：**B** 选取 $S_1, T_1, S_2, T_2 \in_R G$，然后在不掌握 (sk_i^*, t_i^*, s_i^*) 的条件下采用标准技术模拟产生证明 Π_3。需要指出的是，$c = 1$ 时，S_1, T_1, S_2, T_2 是利用函数 $f_{G,(\cdot)}^{(1)}(\cdot)$ 产生的，而 $c = 0$ 时，这些元素是在群 G 上随机选取的（即可视为利用函数 $f_{G,(\cdot)}^{(0)}(\cdot)$ 产生的）。在群 G 上的 y-DDHI 假设下，**A** 无法对此进行分辨。

O_{Query} 在模拟过程中，**B** 以诚实用户 $U_{1+(\beta\oplus d)}$ 的身份（其中，$d \in \{0,1\}$ 是由 **A** 选取的）与 **A** 执行认证协议，并且需要在不掌握成员证书元素 $(sk_{1+(\beta\oplus d)}^*, t_{1+(\beta\oplus d)}^*, s_{1+(\beta\oplus d)}^*)$ 的条件下采用与 O_{Proof} 询问中相同的方式模拟产生证明 Π_3。

在当前实验的末尾，**A** 输出对 β 取值的猜测结果 β'。若满足 $\beta' = \beta$，则判定 **A** 在当前实验中获胜。然而，采用与文献[5]类似的论证方法，可以证明 **A** 获胜的概率是可忽略的。具体地，若满足 $c = 0$（即 **B** 在对 Π_3 的模拟过程中使用了函数 $f_{G,(\cdot)}^{(0)}(\cdot)$），由于 $f_{G,(\cdot)}^{(0)}(\cdot)$ 是真正的随机函数，因此 β 的分布独立于 **A** 在实验中的观察结果。于是，**A** 在实验中获得的优势为 0。若满足 $c = 1$（即 **B** 在对 Π_3 的模拟过程中使用了函数 $f_{G,(\cdot)}^{(1)}(\cdot)$），则根据 Dodis- Yampolskiy 伪随机函数的安全性可知，**A** 在实验中获得的优势是可忽略的。最终，由于 $c = 1$ 时 **A** 在当前实验中获得的优势与它在真实实验中获得的优势相同，因此 **A** 在真实实验中获得的优势是可忽略的。

用户的可开脱性。假设攻击者 **A** 能以不可忽略概率攻破用户的可开脱性，则能借助 **A** 构造归约算法 **B**，且 **B** 能以不可忽略的概率攻破群 G 上的离散

对数假设。在实验开始之前，**B** 选取目标用户 U，并且在实验中对预言机 O_{List},O_{VList},O_{Join},O_{Proof} 进行模拟。具体过程如下：

O_{List},O_{VList} 模拟方法同上。

O_{Join},O_{Proof} 采用匿名性实验中的方式对 O_{Join}, O_{Proof} 进行模拟。

假设 **A** 最终在当前的实验中获胜。此时可分为以下 2 种情况。

情况 1 *Trace* 算法在 *Log* 中找到 2 个元组 $(t_0,R_1,R_2,S_1,T_1,S_2,T_2,\Pi_3),(t_0,R_1',R_2',S_1',T_1',S_2',T_2',\Pi_3')$，$\Pi_3,\Pi_3'$ 均为有效且 $R_1\neq R_1',R_2\neq R_2'$。

情况 2 *Trace* 算法在 *Log* 中找到 2 个元组 $(t_0,R_1,R_2,S_1,T_1,S_2,T_2,\Pi_3),(t_0',R_1',R_2',S_1',T_1',S_2',T_2',\Pi_3')$，$\Pi_3,\Pi_3'$ 均为有效且 $R_1\neq R_1',R_2\neq R_2'$。

可以证明，无论发生哪种情况，**B** 都能借助 **A** 攻破群 G 上的离散对数假设。现在以情况 1 为例进行分析，且对情况 2 的分析方法是类似的。具体地，此时 **B** 对 **A** 执行重绕，从而在证明 Π_3,Π_3' 中分别提取出秘密证据 $(\cdots,sk_{\text{U}}^*,t^*,s^*,A^*,e^*,J^*,\cdots)$, $(\cdots,sk_{\text{U}}^{**},t^{**},s^{**},A^{**},e^{**},J^{**},\cdots)$。根据 Π_3 的可靠性，可以得出

$$A^{*e^*+\gamma}=g_0g_1^{sk_{\text{U}}^*}g_2^{t^*}g_3^{s^*},S_1=u_0^{\frac{1}{s^*+c(0,t_0,J^*)+1}},$$

$$T_1=pk_{\text{U}}^*u_0^{\frac{R_1}{s^*+c(1,t_0,J^*)+1}},0\leqslant J^*<n$$

类似地，根据 Π_3' 的可靠性，可以得出

$$A^{**e^{**}+\gamma}=g_0g_1^{sk_{\text{U}}^{**}}g_2^{t^{**}}g_3^{s^{**}},S_1'=u_0^{\frac{1}{s^{**}+c(0,t_0,J^{**})+1}},$$

$$T_1'=pk_{\text{U}}^{**}u_0^{\frac{R_1'}{s^{**}+c(1,t_0,J^{**})+1}},0\leqslant J^{**}<n$$

由于 $S_1=S_1'$，根据 Dodis-Yampolskiy 伪随机函数的唯一性（即抗碰撞性）可知，$s^*=s^{**}$, $J^*=J^{**}$。此时，**B** 可以计算出

$$pk_U^*=pk_U^{**}=\frac{T_1}{(T_1/T_1')^{R_1/(R_1-R_1')}}$$

根据 Π_3,Π_3' 的可靠性可知，**B** 在重绕过程中从 Π_3,Π_3' 中提取出的证据 sk_{U}^* 的确是以 u_0 为底 pk_{U}^* 的离散对数，而根据对预言机 O_{Join} 的模拟过程可知，pk_{U}^* 是由 **B** 在群 G 上随机选取的，因此 **B** 借助 **A** 求解了群 G 上的离散对数问题实例 $(pk_{\text{U}}^*,u_0)\in G^2$。

GM 的可开脱性。假设攻击者 **A** 能以不可忽略概率攻破 GM 的可开脱性，则能借助 **A** 构造归约算法 **B**，且 **B** 能以不可忽略的概率攻破 BBS+签名方案的不可伪造性。**B** 以某个 BBS+签名方案实例的公钥 (g_0,g_1,g_2,g_3,h_0,w) 作为输入，并在以下的实验中对预言机 O_{List},O_{VList}, O_{Issue} 进行模拟。具体过程如下。

O_{List},O_{VList} 模拟方法同上。

O_{Issue} 借助底层 BBS+方案的签名预言机对 O_{Issue} 进行模拟，且具体过程与可检测性证明中对 O_{Issue} 的模拟方法相同。

假设 **A** 最终在当前的实验中获胜。此时可分为以下 2 种情况。

情况 1 *Trace* 算法在 *Log* 中找到 2 个元组 $(t_0,R_1,R_2,S_1,T_1,S_2,T_2,\Pi_3),(t_0,R_1',R_2',S_1',T_1',S_2',T_2',\Pi_3')$，$\Pi_3,\Pi_3'$ 均为有效，$R_1\neq R_1',R_2\neq R_2'$，而且 $pk_{\text{U}}^*=\frac{T_1}{(T_1/T_1')^{R_1/(R_1-R_1')}}\notin List$。

情况 2 *Trace* 算法在 *LOG* 中找到 2 个元组 $(t_0,R_1,R_2,S_1,T_1,S_2,T_2,\Pi_3),(t_0',R_1',R_2',S_1',T_1',S_2',T_2',\Pi_3')$，$\Pi_3,\Pi_3'$ 均为有效，$R_1\neq R_1',R_2\neq R_2'$，而且 $pk_{\text{U}}^*=\frac{T_2}{(T_2/T_2')^{R_2/(R_2-R_2')}}\notin List$。

可以证明，无论发生哪种情况，**B** 都能借助 **A** 攻破底层 BBS+方案的不可伪造性。现在以情况 1 为例进行分析，且对情况 2 的分析方法是类似的。具体地，此时 **B** 对 **A** 执行重绕，从而在证明 Π_3,Π_3' 中分别提取出秘密证据 $(\cdots,sk_{\text{U}}^*,t^*,s^*,A^*,e^*,J^*,\cdots)$, $(\cdots,sk_{\text{U}}^{**},t^{**},s^{**},A^{**},e^{**},J^{**},\cdots)$。根据 Π_3 的可靠性，可以得出

$$A^{*e^*+\gamma}=g_0g_1^{sk_{\text{U}}^*}g_2^{t^*}g_3^{s^*},S_1=u_0^{\frac{1}{s^*+c(0,t_0,J^*)+1}},$$

$$T_1=pk_{\text{U}}^*u_0^{\frac{R_1}{s^*+c(1,t_0,J^*)+1}},0\leqslant J^*<n$$

类似地，根据 Π_3' 的可靠性，可以得出

$$A^{**e^{**}+\gamma}=g_0g_1^{sk_{\text{U}}^{**}}g_2^{t^{**}}g_3^{s^{**}},S_1'=u_0^{\frac{1}{s^{**}+c(0,t_0,J^{**})+1}},$$

$$T_1'=pk_{\text{U}}^{**}u_0^{\frac{R_1'}{s^{**}+c(1,t_0,J^{**})+1}},0\leqslant J^{**}<n$$

由于 $S_1=S_1'$，根据 Dodis-Yampolskiy 伪随机函数的唯一性（即抗碰撞性）可知，$s^*=s^{**}$, $J^*=J^{**}$。此时，**B** 可以计算出

$$pk_{\text{U}}^*=pk_{\text{U}}^{**}=\frac{T_1}{(T_1/T_1')^{R_1/(R_1-R_1')}}$$

由于 $pk_{\text{U}}^*=u_0^{sk_{\text{U}}^*}\notin List$，因此，$sk_{\text{U}}^*\neq sk_u$ $(u=1,\cdots,\#List)$。这表明 **B** 提取出来的秘密元组

$((sk_{\mathrm{U}}^{*},t^{*},s^{*}),A^{*},e^{*})$ 与所有的 $((sk_{\mathrm{u}},t_{\mathrm{u}},s_{\mathrm{u}}),A_{\mathrm{u}},e_{\mathrm{u}})$, $(u=1,\cdots,\#List)$ 都不相同，而后者是通过与 **B** 执行注册协议产生的。因此，**A** 必然为秘密元组 $(sk_{\mathrm{U}}^{*},t^{*},s^{*})$ 伪造了 BBS+方案签名，因此 **B** 借助 **A** 攻破了底层 BBS+方案的不可伪造性。

AP 的可开脱性。在当前的实验中，**B** 充当目标 *APv*，而 **A** 的目标是对 *APv* 进行陷害。在实验过程中，**B** 需要采用如下方式对预言机 O_{List}, O_{VList}, O_{Verify} 进行模拟。具体过程如下：

O_{List}, O_{VList} 模拟方法同上。

O_{Verify}**B** 在认证协议中以诚实方式执行对证明 Π_3 的验证过程。

根据本文 *Trace* 算法的定义可知，**A** 最终在实验中获胜的条件是：*Trace* 算法在认证日志 Log_v 中找到元组 $(t_0,R_1,R_2,S_1,T_1,S_2,T_2,\Pi_3),(t_0',R_1',R_2',S_1',T_1',S_2',T_2',\Pi_3')$，满足条件 $(S_1=S_1')\vee(S_2=S_2')$，同时 Π_3,Π_3' 并非都为有效或 Π_3,Π_3' 都为有效但不满足条件 $(R_1\neq R_1')\wedge(R_2\neq R_2')$。由于 **B** 在实验中诚实地执行了认证协议中的步骤 2）和步骤 3），因此上述的任何一种情况必然不会发生。这表明 *Trace* 算法在当前实验中的输出必不会为 *APv*，即 **A** 不会在当前实验中获胜。

6　方案的性能分析

本节对本文方案的性能做出简要分析。与已有的 k-TAA 方案相比，本文方案的优势并不体现在参与方的通信耗费和运算耗费方面，而是体现在所实现的安全性质方面。为此，在表 1 中对本文方案与已有方案进行了比较。需要指出的是，文献[1,4,5,8]并未考虑 AP 撤销用户访问权利的情况，因此 AP 的用户群体是静态的。而本文方案与文献[3,6,7]方案都是基于双线性群上的累加器机制实现了动态的用户群体。文献[8]以牺牲用户的匿名性作为代价实现了允许 AP 灵活设置用户的访问次数的性质，因此该方案仅满足弱的用户匿名性，而在其他的方案中，只要用户保持诚实，都能满足完全的匿名性。尽管文献[4~6]中提出了认证耗费为 $O(1)$的方案，但正如引言部分所述，这是以 AP 保持诚实为条件的。文献[8]方案的认证耗费同样为 $O(1)$，但是该性质同样是以牺牲用户的匿名性作为代价的。此外，本文方案无需要求 AP 保持诚实，因为在考虑克隆攻击的应用背景下，AP 必须保持诚实，否则将面对因用户发动克隆攻击所造成的巨大损失。与已有方案相比，本文方案不但满足已有方案的全部性质，而且增加了并发注册，允许 AP 灵活设置用户的访问次数和抗克隆攻击的理想性质。

本文方案是通过对文献[7]方案做出扩展而得到的。在表 2 中总结了本文方案在通信耗费和运算耗费方面所付出的额外代价。2 个方案的主要区别和参数选取方法如下。

1) 2 个方案的 *GM* 系统建立，AP 系统建立，用户系统建立和撤销访问权利协议是大致相当的。但本文方案要求执行额外的公共参考字符串的建立过程。

2) 在注册协议方面，2 个方案最大的区别是文献[7]方案仅能支持串行注册，而本文方案支持并发注册。在授予访问权利的协议方面，本文方案对文献[7]方案做出了扩展，即为了能为每个用户灵活地设置访问次数上界 k，AP 需要额外地向用户颁发证书 $cert_{AP}$。与文献[7]方案相比，用户需要在认证协议中额外地证明以下事实，即

$$S_1=u_0^{\frac{1}{s+c(0,t_0,J)+1}},T_1=pk_{\mathrm{U}}u_0^{\frac{R_1}{s+c(1,t_0,J)+1}},$$
$$0\leqslant J<n,\tilde{A}^{\tilde{e}+\gamma'}=g_0'g_1'^{sk_{\mathrm{U}}}g_2'^{k}g_3'^{\tilde{s}}$$

此外，尽管 2 个方案都要求用户证明“$0\leqslant J_{\mathrm{AP}}<k$”，

表 1　　**本文方案与已有方案的重要安全性质比较**

方案	用户群体的性质	用户的匿名性	认证协议的运算耗费	要求 AP 保持诚实	并发注册	允许 AP 灵活设置用户的访问次数	抗克隆攻击
文献[1]	静态	强	$O(k)$	否	否	否	否
文献[3]	动态	强	$O(k)$	否	否	否	否
文献[4,5]	静态	强	$O(\log k)/O(1)$	否/是	否	否	否
文献[6]	动态	强	$O(1)$	是	否	否	否
文献[7]	动态	强	$O(\log k)$	否	否	否	否
文献[8]	静态	弱	$O(1)$	否	是	是	否
本文	动态	强	$O(\log k)$	否	是	是	是

表 2 本文方案在文献[7]方案基础上增加的通信和运算耗费

额外耗费	注册协议	授予访问权利协议	认证协议
通信耗费（U）	39 602bit	686bit	36 622bit
运算耗费（U）	$7Exp_{Z_{\tilde{N}_1}}+6Exp_{Z_{\tilde{N}_2^2}}+6Exp_{Z_{\tilde{N}_2}}$	$3Exp_{G_1}$	$90Exp_{G_1}+2Exp_G+Exp_{G_T}$
运算耗费（GM）	$4Exp_{Z_{\tilde{N}_1}}+3Exp_{Z_{\tilde{N}_2}}+3Exp_{Z_{\tilde{N}_2^2}}$	–	–
运算耗费（AP）	-	$Pair+2Exp_{G_1}+Exp_{G_2}+Exp_{G_T}$	$Pair+65Exp_{G_1}+Exp_{G_2}+2Exp_G+Exp_{G_T}$

但所采用的实现方式并不相同。在文献[7]方案中，k 是公开的系统参数，而在本文方案中，用户同样需要对 k 值进行隐藏。

3) 为了对通信与运算耗费进行估算，假设 $n=250,k=30$，于是 $l=8,l'=5$ bit。此外，选取模数 $\tilde{N}_1$、$\tilde{N}_2$ 的长度为 1 024bit。选取 l_p=171bit，群 G、G_1、G_2、G_T 上的元素长度分别为 172bit、172bit、1 020bit、1 020bit[29]。此外，用 *Pair* 表示执行 1 次对运算的耗费，用 Exp_G 表示执行 1 次群 G 上的指数（多指数）运算的耗费。对于其他群上的指数（多指数）运算的耗费，则采用类似的符号进行表示。

7 结束语

迄今为止，尚未提出充分考虑实际应用需要的 k-TAA 方案。这主要体现在已有方案均未能较好地解决服务供应商根据用户支付的费用为其设置认证次数上界的问题，以及防止恶意用户发动大规模克隆攻击的问题。为了克服这些困难，提出一个支持并发注册的改进方案。形式化的安全性分析表明，新方案在扩展的 Teranishi-Furukawa-Sako 模型下满足可证安全。此外，新方案采用了纯软件的克隆攻击检测技术，显著地降低了广泛部署的成本，因此具有较好的应用推广价值。

附录 证明 Π_1 的执行过程和证明 Π_3 的构造过程

1 证明 Π_1 的具体执行过程

1) U 选取 $c_2\in_R Z_{p^2}$，选取 $\xi_{\bar{e}}\in_R Z_{p^3}$，$\xi_{w\bar{e}}\in_R Z_{p^3\tilde{N}_1}$，$\xi_w,\xi_{r_w}\in_R Z_{\tilde{N}_1},\xi_{r_w\bar{e}}\in_R Z_{p^3\tilde{N}_1}$，计算

$$R_{2,1}=C_{\bar{y}}^{\xi_{\bar{e}}}\tilde{h}_1^{-\xi_{w\bar{e}}}(\tilde{x}\tilde{h}^{-Hash(\bar{x}')})^{-c_2}\bmod\tilde{N}_1,$$
$$R_{2,2}=\tilde{h}_1^{\xi_w}\tilde{h}_2^{\xi_{r_w}}C_w^{-c_2}\bmod\tilde{N}_1,$$
$$R_{2,3}=C_w^{\xi_{\bar{e}}}\tilde{h}_1^{-\xi_{w\bar{e}}}\tilde{h}_2^{-\xi_{r_w\bar{e}}}\bmod\tilde{N}_1$$

选取 $\theta_{sk_U},\theta_t,\theta_{s'}\in_R Z_{p^3},\theta_\alpha,\theta_\beta,\theta_\gamma\in_R Z_{\tilde{N}_1}^*$，$\theta_{r_{sk_U}},\theta_{r_t},\theta_{r_{s'}}\in_R Z_{p^3\tilde{N}_2}$，计算

$$R_{1,1}=g_1^{\theta_{sk_U}}g_2^{\theta_t}g_3^{\theta_{s'}},$$
$$R_{1,2}=u_0^{\theta_{sk_U}},R_{1,3}=\tilde{H}^{\theta_{sk_U}}\theta_\alpha^{\tilde{N}_1}\bmod\tilde{N}_1^2,$$
$$R_{1,4}=\tilde{H}^{\theta_t}\theta_\beta^{\tilde{N}_1}\bmod\tilde{N}_1^2,R_{1,5}=\tilde{H}^{\theta_{s'}}\theta_\gamma^{\tilde{N}_1}\bmod\tilde{N}_1^2,$$
$$R_{1,6}=\tilde{h}_3^{\theta_{sk_U}}\tilde{h}_4^{\theta_{r_{sk_U}}}\bmod\tilde{N}_2,R_{1,7}=\tilde{h}_3^{\theta_t}\tilde{h}_4^{\theta_{r_t}}\bmod\tilde{N}_2,$$
$$R_{1,8}=\tilde{h}_3^{\theta_{s'}}\tilde{h}_4^{\theta_{r_{s'}}}\bmod\tilde{N}_2$$

最后，U 向 *GM* 发送 $((R_{1,1},\cdots,R_{1,8}),(R_{2,1},R_{2,2},R_{2,3}))$。

2) GM 返回挑战 $c\in_R Z_p$。

3) U 设置 $c_1=c+c_2$，计算

$$\xi_{sk_U}=\theta_{sk_U}+c_1sk_U,\xi_t=\theta_t+c_1t,\xi_{s'}=\theta_{s'}+c_1s',$$
$$\xi_\alpha=\theta_\alpha\alpha^{c_1}\bmod\tilde{N}_1,\xi_\beta=\theta_\beta\beta^{c_1}\bmod\tilde{N}_1,$$
$$\xi_\gamma=\theta_\gamma\gamma^{c_1}\bmod\tilde{N}_1,\xi_{r_{sk_U}}=\theta_{r_{sk_U}}+c_1r_{sk_U},$$
$$\xi_{r_t}=\theta_{r_t}+c_1r_t,\xi_{r_{s'}}=\theta_{r_{s'}}+c_1r_{s'},$$

并向 GM 发送 $(c_1,\xi_{sk_U},\xi_t,\xi_{s'},\xi_\alpha,\xi_\beta,\xi_\gamma,\xi_{r_{sk_U}},\xi_{r_t},\xi_{r_{s'}})$，$(c_2,\xi_{\bar{e}},\xi_{w\bar{e}},\xi_w,\xi_{r_w},\xi_{r_w\bar{e}})$。

4) GM 验证是否满足

$$c=c_1-c_2,\xi_{sk_U},\xi_t,\xi_{s'}\in Z_{p^3},R_{1,1}=g_1^{\xi_{sk_U}}g_2^{\xi_t}g_3^{\xi_{s'}}C^{-c_1},$$
$$R_{1,2}=u_0^{\xi_{sk_U}}pk_U^{-c_1},R_{1,3}=\tilde{H}^{\xi_{sk_U}}\xi_\alpha^{\tilde{N}_1}E_1^{-c_1}\bmod\tilde{N}_1^2,$$
$$R_{1,4}=\tilde{H}^{\xi_t}\xi_\beta^{\tilde{N}_1}E_2^{-c_1}\bmod\tilde{N}_1^2,$$
$$R_{1,5}=\tilde{H}^{\xi_{s'}}\xi_\gamma^{\tilde{N}_1}E_3^{-c_1}\bmod\tilde{N}_1^2,$$
$$R_{1,6}=\tilde{h}_3^{\xi_{sk_U}}\tilde{h}_4^{\xi_{r_{sk_U}}}S_1^{-c_1}\bmod\tilde{N}_2,$$
$$R_{1,7}=\tilde{h}_3^{\xi_t}\tilde{h}_4^{\xi_{r_t}}S_2^{-c_1}\bmod\tilde{N}_2,$$
$$R_{1,8}=\tilde{h}_3^{\xi_{s'}}\tilde{h}_4^{\xi_{r_{s'}}}S_3^{-c_1}\bmod\tilde{N}_2,$$
$$R_{2,1}=C_{\bar{y}}^{\xi_{\bar{e}}}\tilde{h}_1^{-\xi_{w\bar{e}}}(\tilde{x}\tilde{h}^{-Hash(\bar{x}')})^{-c_2}\bmod\tilde{N}_1,$$
$$R_{2,2}=\tilde{h}_1^{\xi_w}\tilde{h}_2^{\xi_{r_w}}C_w^{-c_2}\bmod\tilde{N}_1,$$
$$R_{2,3}=C_w^{\xi_{\bar{e}}}\tilde{h}_1^{-\xi_{w\bar{e}}}\tilde{h}_2^{-\xi_{r_w\bar{e}}}\bmod\tilde{N}_1.$$

2 证明 Π_3 的构造过程

假设上界 n 与 k 的二进制表达式长度分别为 l 和 l'。

1) U 设置

$$\alpha_1=\frac{1}{s+c(0,t_0,J)+1},\alpha_2=\frac{r_s+r_J}{s+c(0,t_0,J)+1},$$
$$\alpha_3=\frac{1}{s+c(1,t_0,J)+1},\alpha_4=\frac{r_s+r_J}{s+c(1,t_0,J)+1},\alpha_5=r_J-\tilde{r}_J,$$
$$\alpha_6=r_{J_{AP}}-\sum_{i=0}^{l'-1}r_i''2^i,\alpha_7=r_k-\sum_{i=0}^{l'-1}r_i'''2^i$$

并且选取

$\theta_{r_1},\theta_{r_2},\theta_e,\theta_{r_1e},\theta_{r_2e},\theta_{sk_U},\theta_t,\theta_s,\theta_{r_3},\theta_{r_4},\theta_{r_3e},\theta_{r_4e},$
$\theta_{\alpha_1},\theta_{\alpha_2},\theta_{\alpha_3},\theta_{\alpha_4},\theta_{r_{sk_U}},\xi_{r'_0,0},\theta_{r'_0,1},\ldots,\xi_{r'_{l-1},0},\theta_{r'_{l-1},1},$
$\theta_J,\theta_{r_J},\theta_{\alpha_5},\theta_{J_{AP}},\theta_{r_5},\theta_{sk_Ut},\theta_{J_{AP}sk_U},\theta_{r_5sk_U},\xi_{r''_0,0},$
$\theta_{r''_0,1},\ldots,\xi_{r''_{l-1},0},\theta_{r''_{l-1},1},\xi_{r'''_0,0},\theta_{r'''_0,1},\ldots,\xi_{r'''_{l-1},0},\theta_{r'''_{l-1},1},$
$\theta_{r_{J_{AP}}},\theta_{\alpha_6},\theta_k,\theta_{r_k},\theta_{\alpha_7},\xi_{l+2l'+22,r''_{l-1}},\xi_{l+2l'+22,r'''_{l-1}},$
$\xi_{l+2l'+22,r''_{l-2}},\xi_{l+2l'+22,r'''_{l-2}},\xi_{l+2l'+23,r''_{l-1}},\xi_{l+2l'+23,r'''_{l-1}},$
$\xi_{l+2l'+23,r''_{l-2}},\xi_{l+2l'+23,r'''_{l-2}},\xi_{l+2l'+23,r''_{l-3}},\xi_{l+2l'+23,r'''_{l-3}},$
$\theta_{l+3l'+21,r''_{l-1}},\theta_{l+3l'+21,r'''_{l-1}},\ldots,\theta_{l+3l'+21,r''_1},\theta_{l+3l'+21,r'''_1},$
$\theta_{l+3l'+21,r''_0},\theta_{l+3l'+21,r'''_0},\theta_{r_6},\theta_{r_7},\theta_{\tilde{e}},\theta_{r_6\tilde{e}},\theta_{r_7\tilde{e}},\theta_{\tilde{s}}$
$\in_R Z_p,c_{12,0},\ldots,c_{l+11,0},c_{l+18,0},\ldots,c_{l+l'+17,0},c_{l+l'+18,0}$
$,\ldots,c_{l+2l'+17,0},c_{l+2l'+22},c_{l+2l'+23},\ldots,c_{l+3l'+20}\in_R Z_{p^2}$

2）U 计算

$R_1=g_1^{\theta_{r_1}}g_2^{\theta_{r_2}},R_2=A_2^{-\theta_e}g_1^{\theta_{r_1e}}g_2^{\theta_{r_2e}},R_3=\hat{e}(A_1,h_0)^{-\theta_e}$
$\hat{e}(g_1,h_0)^{\theta_{sk_U}}\ \hat{e}(g_2,w)^{\theta_{r_1}}\ \hat{e}(g_2,h_0)^{\theta_{r_1e}}\ \hat{e}(g_2,h_0)^{\theta_t}$
$\hat{e}(g_3,h_0)^{\theta_s},R_4=g_1^{\theta_{r_3}}g_2^{\theta_{r_4}},R_5=A_4^{-\theta_e}g_1^{\theta_{r_3e}}g_2^{\theta_{r_4e}},$
$R_6=\hat{e}(A_3,h_{AP})^{-\theta_e}\ \hat{e}(g_2,p_{AP})^{\theta_{r_3}}\ \hat{e}(g_2,h_{AP})^{\theta_{r_3e}},$
$R_7=(C_sg_1^{c(0,t_0,0)+1}C_J)^{\theta_{\alpha_1}}g_2^{-\theta_{\alpha_2}},R_8=u_0^{\theta_{\alpha_1}},$
$R_9=(C_sg_1^{c(1,t_0,0)+1}C_J)^{\theta_{\alpha_3}}g_2^{-\theta_{\alpha_4}},R_{10}=g_1^{\theta_{sk_U}}g_2^{\theta_{r_{sk_U}}},$
$R_{11}=u_0^{\theta_{sk_U}}(u_0^{R_1})^{\theta_{\alpha_3}},R_{12,0}=g_2^{\xi_{r'_0,0}}C_{J,0}^{-c_{12,0}},$
$R_{12,1}=g_2^{\theta_{r'_0,1}},\ldots,R_{l+11,0}=g_2^{\xi_{r'_{l-1},0}}C_{J,l-1}^{-c_{l+11,0}},$
$R_{l+11,1}=g_2^{\theta_{r'_{l-1},1}},R_{l+12}=g_1^{\theta_J}g_2^{\theta_{r_J}},R_{l+13}=g_2^{\theta_{\alpha_5}},$
$R_{l+14}=S_2^{\theta_s}S_2^{\theta_{J_{AP}}},R_{l+15}=g_1^{\theta_t}g_2^{\theta_{J_{AP}}}g_3^{\theta_{r_5}},$
$R_{l+16}=g_1^{\theta_{sk_Ut}}g_2^{\theta_{J_{AP}sk_U}}g_3^{\theta_{r_5sk_U}}A_5^{-\theta_{sk_U}},$
$R_{l+17}=u_0^{\theta_{sk_Ut}}u_0^{\theta_{sk_UJ_{AP}}}u_0^{\theta_{sk_U}}T_2^{-\theta_t}T_2^{-\theta_{J_{AP}}},$
$R_{l+18,0}=g_2^{\xi_{r''_0,0}}C_{J_{AP},0}^{-c_{l+18,0}},R_{l+18,1}=g_2^{\theta_{r''_0,1}},\ldots,$
$R_{l+l'+17,0}=g_2^{\xi_{r''_{l-1},0}}C_{J_{AP},l'-1}^{-c_{l+l'+17,0}},R_{l+l'+17,1}=g_2^{\theta_{r''_{l-1},1}},$
$R_{l+l'+18,0}=g_2^{\xi_{r'''_0,0}}C_{k,0}^{-c_{l+l'+18,0}},R_{l+l'+18,1}=g_2^{\xi_{r'''_0,1}}$
$,\ldots,R_{l+2l'+17,0}=g_2^{\xi_{r'''_{l-1},0}}C_{k,l'-1}^{-c_{l+2l'+17,0}},R_{l+2l'+17,1}=g_2^{\theta_{r'''_{l-1},1}},$
$R_{l+2l'+18}=g_1^{\theta_{J_{AP}}}g_2^{\theta_{r_{J_{AP}}}},R_{l+2l'+19}=g_2^{\theta_{\alpha_6}},$
$R_{l+2l'+20}=g_1^{\theta_k}g_2^{\theta_{r_k}},R_{l+2l'+21}=g_2^{\theta_{\alpha_7}},$
$R_{l+2l'+22,0}=g_2^{\xi_{l+2l'+22,r''_{l-1}}-\xi_{l+2l'+22,r'''_{l-1}}}\left(\frac{C_{J_{AP},l'-1}}{C_{k,l'-1}}\right)^{-c_{l+2l'+22}},$
$R_{l+2l'+22,1}=g_2^{\xi_{l+2l'+22,r''_{l-2}}}C_{J_{AP},l'-2}^{-c_{l+2l'+22}},\ldots,$
$R_{l+2l'+22,2}=g_2^{\xi_{l+2l'+22,r'''_{l-2}}}\left(\frac{C_{k,l'-2}}{g_1}\right)^{-c_{l+2l'+22}},$
$R_{l+2l'+23,0}=g_2^{\xi_{l+2l'+23,r''_{l-1}}-\xi_{l+2l'+23,r'''_{l-1}}}\left(\frac{C_{J_{AP},l'-1}}{C_{k,l'-1}}\right)^{-c_{l+2l'+23}},$
$R_{l+2l'+23,1}=g_2^{\xi_{l+2l'+23,r''_{l-2}}-\xi_{l+2l'+23,r'''_{l-2}}}\left(\frac{C_{J_{AP},l'-2}}{C_{k,l'-2}}\right)^{-c_{l+2l'+23}},$
$R_{l+2l'+23,2}=g_2^{\xi_{l+2l'+23,r''_{l-3}}}C_{J_{AP},l'-3}^{-c_{l+2l'+23}},$
$R_{l+2l'+23,3}=g_2^{\xi_{l+2l'+23,r'''_{l-3}}}\left(\frac{C_{k,l'-3}}{g_1}\right)^{-c_{l+2l'+23}},\ldots,$
$R_{l+3l'+21,0}=g_2^{\theta_{l+3l'+21,r''_{l-1}}-\theta_{l+3l'+21,r'''_{l-1}}},\ldots,$
$R_{l+3l'+21,l'-2}=g_2^{\theta_{l+3l'+21,r''_1}-\theta_{l+3l'+21,r'''_1}},$
$R_{l+3l'+21,l'-1}=g_2^{\theta_{l+3l'+21,r''_0}},R_{l+3l'+21,l'}=g_2^{\theta_{l+3l'+21,r'''_0}},$
$R_{l+3l'+22}=g_1^{\theta_{r_6}}g_2^{\theta_{r_7}},R_{l+3l'+23}=A_7^{-\theta_{\tilde{e}}}g_1^{\theta_{r_6\tilde{e}}}g_2^{\theta_{r_7\tilde{e}}},$
$R_{l+3l'+24}=\hat{e}(g'_1,h'_0)^{\theta_{sk_U}}\ \hat{e}(g'_2,h'_0)^{\theta_k}$
$\hat{e}(g'_3,h'_0)^{\theta_{\tilde{s}}}\ \hat{e}(A_6,h'_0)^{-\theta_{\tilde{e}}}\ \hat{e}(g_2,w')^{\theta_{r_6}}\ \hat{e}(g_2,h'_0)^{\theta_{r_6\tilde{e}}}$
然后，U 计算挑战 $\bar{c}=H(R_1,\cdots,R_{l+3l'+24})$。

3) U 设置

$c_{12,1}=c_{12,0}-\bar{c},\ldots,c_{l+11,1}=c_{l+11,0}-\bar{c},$
$c_{l+18,1}=c_{l+18,0}-\bar{c},\ldots,c_{l+l'+17,1}=c_{l+l'+17,0}-\bar{c},$
$c_{l+l'+18,1}=c_{l+l'+18,0}-\bar{c},\ldots,c_{l+2l'+17,1}=c_{l+2l'+17,0}-\bar{c},$
$c_{l+3l'+21}=c_{l+2l'+22}+\cdots+c_{l+3l'+20}-\bar{c}$
并在 Z_p 上计算
$\xi_{r_1}=\theta_{r_1}+\bar{c}r_1,\xi_{r_2}=\theta_{r_2}+\bar{c}r_2,\xi_e=\theta_e+\bar{c}e,$
$\xi_{r_1e}=\theta_{r_1e}+\bar{c}r_1e,\xi_{r_2e}=\theta_{r_2e}+\bar{c}r_2e,$
$\xi_{sk_U}=\theta_{sk_U}+\bar{c}sk_U,\xi_t=\theta_t+\bar{c}t,\xi_s=\theta_s+\bar{c}s,$
$\xi_{r_3}=\theta_{r_3}+\bar{c}r_3,\xi_{r_4}=\theta_{r_4}+\bar{c}r_4,\xi_{r_3e}=\theta_{r_3e}+\bar{c}r_3e,$
$\xi_{r_4e}=\theta_{r_4e}+\bar{c}r_4e,\xi_{\alpha_1}=\theta_{\alpha_1}+\bar{c}\alpha_1,$
$\xi_{\alpha_2}=\theta_{\alpha_2}+\bar{c}\alpha_2,\xi_{\alpha_3}=\theta_{\alpha_3}+\bar{c}\alpha_3,$
$\xi_{\alpha_4}=\theta_{\alpha_4}+\bar{c}\alpha_4,\xi_{r_{sk_U}}=\theta_{r_{sk_U}}+\bar{c}r_{sk_U},$
$\xi_{r'_0,1}=\theta_{r'_0,1}+c_{12,1}r'_0,\ldots,\xi_{r'_{l-1},1}=\theta_{r'_{l-1},1}+c_{l+11,1}r'_{l-1},$
$\xi_J=\theta_J+\bar{c}J,\xi_{r_J}=\theta_{r_J}+\bar{c}r_J,\xi_{\alpha_5}=\theta_{\alpha_5}+\bar{c}\alpha_5,$
$\xi_{J_{AP}}=\theta_{J_{AP}}+\bar{c}J_{AP},\xi_{r_5}=\theta_{r_5}+\bar{c}r_5,$
$\xi_{sk_Ut}=\theta_{sk_Ut}+\bar{c}sk_Ut,\xi_{J_{AP}sk_U}=\theta_{J_{AP}sk_U}+\bar{c}J_{AP}sk_U,$
$\xi_{r_5sk_U}=\theta_{r_5sk_U}+\bar{c}r_5sk_U,\xi_{r''_0,1}=\theta_{r''_0,1}+c_{l+18,1}r''_0,$
$\ldots,\xi_{r''_{l-1},1}=\theta_{r''_{l-1},1}+c_{l+l'+17,1}r''_{l-1},$
$\xi_{r'''_0,1}=\theta_{r'''_0,1}+c_{l+l'+18,1}r'''_0,\ldots,$
$\xi_{r'''_{l-1},1}=\theta_{r'''_{l-1},1}+c_{l+2l'+17,1}r'''_{l-1},\xi_{r_{J_{AP}}}=\theta_{r_{J_{AP}}}+\bar{c}r_{J_{AP}},$
$\xi_{\alpha_6}=\theta_{\alpha_6}+\bar{c}\alpha_6,\xi_k=\theta_k+\bar{c}k,$
$\xi_{r_k}=\theta_{r_k}+\bar{c}r_k,\xi_{\alpha_7}=\theta_{\alpha_7}+\bar{c}\alpha_7,$
$\xi_{l+3l'+21,r''_{l-1}}=\theta_{l+3l'+21,r''_{l-1}}+c_{l+3l'+21}r''_{l-1},$
$\xi_{l+3l'+21,r'''_{l-1}}=\theta_{l+3l'+21,r'''_{l-1}}+c_{4l+21}r'''_{l-1},\ldots,$
$\xi_{l+3l'+21,r''_1}=\theta_{l+3l'+21,r''_1}+c_{l+3l'+21}r''_1,$
$\xi_{l+3l'+21,r'''_1}=\theta_{l+3l'+21,r'''_1}+c_{l+3l'+21}r'''_1,$
$\xi_{l+3l'+21,r''_0}=\theta_{l+3l'+21,r''_0}+c_{l+3l'+21}r''_0,$
$\xi_{l+3l'+21,r'''_0}=\theta_{l+3l'+21,r'''_0}+c_{l+3l'+21}r'''_0,$
$\xi_{r_6}=\theta_{r_6}+\bar{c}r_6,\xi_{r_7}=\theta_{r_7}+\bar{c}r_7,\xi_{\tilde{e}}=\theta_{\tilde{e}}+\bar{c}\tilde{e},$
$\xi_{r_6\tilde{e}}=\theta_{r_6\tilde{e}}+\bar{c}r_6\tilde{e},\xi_{r_7\tilde{e}}=\theta_{r_7\tilde{e}}+\bar{c}r_7\tilde{e},\xi_{\tilde{s}}=\theta_{\tilde{s}}+\bar{c}\tilde{s}$

4) 给定证明

$\Pi_3=(C_s,C_{sk_U},\ldots,A_6,A_7,\bar{c},\xi_{r_1},\xi_{r_2},\ldots,\xi_{\tilde{s}},$
$c_{12,0},c_{12,1},\ldots,c_{l+11,0},c_{l+11,1},c_{l+18,0},c_{l+18,1},\ldots,$
$c_{l+l'+17,0},c_{l+l'+17,1},c_{l+l'+18,0},c_{l+l'+18,1},\ldots,c_{l+2l'+17,0},$

$c_{l+2l'+17,1}, c_{l+2l'+22}, \ldots, c_{l+3l'+20}, c_{l+3l'+21})$,

AP 计算

$R'_1 = g_1^{\xi_{\eta}} g_2^{\xi_{\eta_2}} A_2^{-\overline{c}}, R'_2 = A_2^{-\xi_e} g_1^{\xi_{\eta e}} g_2^{\xi_{\eta_2 e}}$,

$R'_3 = \hat{e}(A_1, h_0)^{-\xi_e}\ \hat{e}(g_1, h_0)^{\xi_{sk_U}}\ \hat{e}(g_2, w)^{\xi_{\eta}} \cdot$

$\hat{e}(g_2, h_0)^{\xi_{\eta e}}\ \hat{e}(g_2, h_0)^{\xi_t}\ \hat{e}(g_3, h_0)^{\xi_s} \left(\frac{\hat{e}(A_1, w)}{\hat{e}(g_0, h_0)}\right)^{-\overline{c}}$,

$R'_4 = g_1^{\xi_{\eta_3}} g_2^{\xi_{\eta_4}} A_4^{-\overline{c}}, R'_5 = A_4^{-\xi_e} g_1^{\xi_{\eta_3 e}} g_2^{\xi_{\eta_4 e}}$,

$R'_6 = \hat{e}(A_3, h_{\mathrm{AP}})^{-\xi_e}\ \hat{e}(g_2, p_{\mathrm{AP}})^{\xi_{\eta_3}}$

$\hat{e}(g_2, h_{\mathrm{AP}})^{\xi_{\eta e}} \left(\frac{\hat{e}(A_3, p_{\mathrm{AP}})}{\hat{e}(v_{\mathrm{AP}}, h_{\mathrm{AP}})}\right)^{-\overline{c}}$,

$R'_7 = (C_s g_1^{c(0,t_0,0)+1} C_J)^{\xi_{\alpha_1}} g_2^{-\xi_{\alpha_2}} g_1^{-\overline{c}}, R'_8 = u_0^{\xi_{\alpha_1}} S_1^{-\overline{c}}$,

$R'_9 = (C_s g_1^{c(1,t_0,0)+1} C_J)^{\xi_{\alpha_3}} g_2^{-\xi_{\alpha_4}} g_1^{-\overline{c}}$,

$R_{10} = g_1^{\xi_{sk_U}} g_2^{\xi_{r_{sk_U}}} C_{sk_U}^{-\overline{c}}, R_{11} = u_0^{\xi_{sk_U}} (u_0^{R_1})^{\xi_{\alpha_3}} T_1^{-\overline{c}}$,

$R'_{12,0} = g_2^{\xi_{\eta_0,0}} C_{J,0}^{-c_{12,0}}, R'_{12,1} = g_2^{\xi_{\eta_0,1}} \left(\frac{C_{J,0}}{g_1}\right)^{-c_{12,1}}, \ldots,$

$R'_{l+11,0} = g_2^{\xi_{\eta_{l-1,0}}} C_{J,l-1}^{-c_{l+11,0}}, R'_{l+11,1} = g_2^{\xi_{\eta_{l-1,1}}} \left(\frac{C_{J,l-1}}{g_1}\right)^{-c_{l+11,1}}$,

$R'_{l+12} = g_1^{\xi_J} g_2^{\xi_{r_J}} C_J^{-\overline{c}}, R'_{l+13} = g_2^{\xi_{\alpha_5}} \left(\frac{C_J}{\tilde{C}_J}\right)^{-\overline{c}}$,

$R'_{l+14} = S_2^{\xi_s} S_2^{\xi_{J_{\mathrm{AP}}}} \left(\frac{u_{\mathrm{AP}}}{S_2}\right)^{-\overline{c}}, R'_{l+15} = g_1^{\xi_t} g_2^{\xi_{J_{\mathrm{AP}}}} g_3^{\xi_{r_5}} A_5^{-\overline{c}}$,

$R'_{l+16} = g_1^{\xi_{sk_U t}} g_2^{\xi_{J_{\mathrm{AP}} sk_U}} g_3^{\xi_{r_5 sk_U}} A_5^{-\xi_{sk_U}}$,

$R'_{l+17} = u_0^{\xi_{sk_U t}} u_0^{\xi_{sk_U J_{\mathrm{AP}}}} u_0^{\xi_{sk_U}} T_2^{-\xi_t} T_2^{-\xi_{J_{\mathrm{AP}}}} \left(\frac{T_2}{u_{\mathrm{AP}}^{R_2}}\right)^{-\overline{c}}$,

$R'_{l+18,0} = g_2^{\xi_{\eta_0,0}} C_{J_{\mathrm{AP},0}}^{-c_{l+18,0}}, R'_{l+18,1} = g_2^{\xi_{\eta_0,1}} \left(\frac{C_{J_{\mathrm{AP},0}}}{g_1}\right)^{-c_{l+18,1}}$

$, \ldots, R'_{l+l'+17,0} = g_2^{\xi_{\eta^{l'}-1,0}} C_{J_{\mathrm{AP},l'-1}}^{-c_{l+l'+17,0}}$,

$R'_{l+l'+17,1} = g_2^{\xi_{\eta^{l'}-1,1}} \left(\frac{C_{J_{\mathrm{AP},l'-1}}}{g_1}\right)^{-c_{l+l'+17,1}}$,

$R'_{l+l'+18,0} = g_2^{\xi_{\eta_0^{l'},0}} C_{k,0}^{-c_{l+l'+18,0}}$,

$R'_{l+l'+18,1} = g_2^{\xi_{\eta_0^{l'},1}} \left(\frac{C_{k,0}}{g_1}\right)^{-c_{l+l'+18,1}}, \ldots,$

$R'_{l+2l'+17,0} = g_2^{\xi_{\eta^{l'}-1,0}} C_{k,l'-1}^{-c_{l+2l'+17}}$,

$R'_{l+2l'+17,1} = g_2^{\xi_{\eta^{l'}-1,1}} \left(\frac{C_{k,l'-1}}{g_1}\right)^{-c_{l+2l'+17}}$,

$R'_{l+2l'+18} = g_1^{\xi_{J_{\mathrm{AP}}}} g_2^{\xi_{r_{J_{\mathrm{AP}}}}} C_{J_{\mathrm{AP}}}^{-\overline{c}}, R'_{l+2l'+19} = g_2^{\xi_{\alpha_6}} \left(\frac{C_{J_{\mathrm{AP}}}}{\tilde{C}_{J_{\mathrm{AP}}}}\right)^{-\overline{c}}$,

$R'_{l+2l'+20} = g_1^{\xi_k} g_2^{\xi_{r_k}} C_k^{-\overline{c}}, R'_{l+2l'+21} = g_2^{\xi_{\alpha_7}} \left(\frac{C_k}{\tilde{C}_k}\right)^{-\overline{c}}$,

$R'_{l+2l'+22,0} = g_2^{\xi_{l+2l'+22,\eta^{l'}-1} - \xi_{l+2l'+22,\eta^{l'}-1}} \left(\frac{C_{J_{\mathrm{AP}},l'-1}}{C_{k,l'-1}}\right)^{-c_{l+2l'+22}}$,

$R'_{l+2l'+22,1} = g_2^{\xi_{l+2l'+22,\eta^{l'}-2}} C_{J_{\mathrm{AP}},l'-2}^{-c_{l+2l'+22}}, \ldots,$

$R'_{l+2l'+22,2} = g_2^{\xi_{l+2l'+22,\eta^{l'}-2}} \left(\frac{C_{k,l'-2}}{g_1}\right)^{-c_{l+2l'+22}}$,

$R'_{l+2l'+23,0} = g_2^{\xi_{l+2l'+23,\eta^{l'}-1} - \xi_{l+2l'+23,\eta^{l'}-1}} \left(\frac{C_{J_{\mathrm{AP}},l'-1}}{C_{k,l'-1}}\right)^{-c_{l+2l'+23}}$,

$R'_{l+2l'+23,1} = g_2^{\xi_{l+2l'+23,\eta^{l'}-2} - \xi_{l+2l'+23,\eta^{l'}-2}} \left(\frac{C_{J_{\mathrm{AP}},l'-2}}{C_{k,l'-2}}\right)^{-c_{l+2l'+23}}$,

$R'_{l+2l'+23,2} = g_2^{\xi_{l+2l'+23,\eta^{l'}-3}} C_{J_{\mathrm{AP},l'-3}}^{-c_{l+2l'+23}}$,

$R'_{l+2l'+23,3} = g_2^{\xi_{l+2l'+23,\eta^{l'}-3}} \left(\frac{C_{k,l'-3}}{g_1}\right)^{-c_{l+2l'+23}}, \ldots,$

$R'_{l+3l'+21,0} = g_2^{\xi_{l+3l'+21,\eta^{l'}-1} - \xi_{l+3l'+21,\eta^{l'}-1}} \left(\frac{C_{J_{\mathrm{AP}},l'-1}}{C_{k,l'-1}}\right)^{-c_{l+3l'+21}}$,

$\ldots, R'_{l+3l'+21,l'-2} = g_2^{\xi_{l+3l'+21,\eta^{l'}} - \xi_{l+3l'+21,\eta^{l'}}} \left(\frac{C_{J_{\mathrm{AP}},1}}{C_{k,1}}\right)^{-c_{l+3l'+21}}$,

$R'_{l+3l'+21,l'-1} = g_2^{\xi_{l+3l'+21,\eta_0^{l'}}} C_{J_{\mathrm{AP}},0}^{-c_{l+3l'+21}}$,

$R'_{l+3l'+21,l'} = g_2^{\xi_{l+3l'+21,\eta_0^{l'}}} \left(\frac{C_{k,0}}{g_1}\right)^{-c_{l+3l'+21}}$,

$R'_{l+3l'+22} = g_1^{\xi_{r_6}} g_2^{\xi_{r_7}} A_7^{-\overline{c}}, R'_{l+3l'+23} = A_7^{-\xi_e} g_1^{\xi_{r_6 e}} g_2^{\xi_{r_7 e}}$,

$R'_{l+3l'+24} = \hat{e}(g'_1, h'_0)^{\xi_{sk_U}}\ \hat{e}(g'_2, h'_0)^{\xi_k}\ \hat{e}(g'_3, h'_0)^{\xi_{\tilde{s}}} \cdot$

$\hat{e}(A_6, h'_0)^{-\xi_{\tilde{e}}}\ \hat{e}(g_2, w')^{\xi_{r_6}}\ \hat{e}(g_2, h'_0)^{\xi_{r_6 \tilde{e}}} \left(\frac{\hat{e}(A_6, w')}{\hat{e}(g'_0, h'_0)}\right)^{-\overline{c}}$

然后检查是否满足

$\overline{c} = H(R'_1, \ldots, R'_{l+3l'+24}), c_{12,0} + c_{12,1} = \overline{c}, \ldots,$

$c_{l+11,0} + c_{l+11,1} = \overline{c}, c_{l+18,0} + c_{l+18,1} = \overline{c}, \ldots,$

$c_{l+l'+17,0} + c_{l+l'+17,1} = \overline{c}, c_{l+l'+18,0} + c_{l+l'+18,1} = \overline{c}$

$, \ldots, c_{l+2l'+17,0} + c_{l+2l'+17,1} = \overline{c}, c_{l+2l'+22} + \cdots +$

$c_{l+3l'+20} + c_{l+3l'+21} = \overline{c}$

参考文献：

[1] TERANISHI I, FURUKAWA J, SAKO K. K-times anonymous authentication[A]. Proceedings of ASIACRYPT 2004[C]. Berlin: Springer-Verlag, 2004. 308-322.

[2] 鲁荣波，宣恒农，何大可. 对一种高效群签名方案的安全性分析[J]. 通信学报, 2007, 28(4): 9-12.
LV R B, XUAN H N, HE D K. Cryptanalysis of an efficient group signature scheme[J]. Journal on Communications, 2007, 28(4): 9-12.

[3] NGUYEN L, SAFAVI-NAINI R. Dynamic *k*-times anonymous authentication[A]. Proceedings of ACNS 2005[C]. Berlin: Springer-Verlag, 2005. 318-333.

[4] TERANISHI I, SAKO K. *K*-times anonymous authentication with a constant proving cost[A]. Proceedings of PKC 2006[C]. Berlin: Springer-Verlag, 2006. 525-542.

[5] TERANISHI I, FURUKAWA J, SAKO K. K-times anonymous authentication[J]. IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, 2009, 92(1): 147-165.

[6] NGUYEN L. Efficient dynamic k-times anonymous authentication[EB/OL]. http://eprint.iacr.org/2007/006, 2007-01-07/2011-03-01.

[7] AU M H, SUSILO W, MU Y. Constant-size dynamic k-TAA[EB/OL]. http://eprint.iacr.org/2008/136, 2008-03-31/2010-02-01.

[8] EMURA K, MIYAJI A, OMETE K. A selectable k-times relaxed anonymous authentication scheme[A]. Proceedings of WISA 2009[C]. Berlin: Springer-Verlag, 2009. 281-295.

[9] BICHSEL P. Theft and Misuse Protection for Anonymous Credentials[D]. Zürich: Swiss Federal Institute of Technology, Switzerland, 2007.

[10] CAMENISCH J. Protecting (anonymous) credentials with the trusted computing group's TPM v1.2[A]. Proceedings of SEC 2006[C]. Berlin: Springer-Verlag, 2006. 135-147.

[11] IMPAGLIAZZO R, MORE S M. Anonymous credentials with biometrically-enforced non-transferability[A]. Proceedings of WPES 2003[C]. New York: ACM Press, 2003. 60-71.

[12] ADAMS C. Achieving non-transferability in credential systems using hidden biometrics[J]. Security and Communication Networks, 2011, 4(2): 195-206.

[13] BLANTON M, HUDELSON W M P. Biometric-based non-transferable anonymous credentials[A]. Proceedings of ICICS 2009[C]. Berlin: Springer-Verlag, 2009. 165-180.

[14] CAMENISCH J, LYSYANSKAYA A. An efficient system for non-transferable anonymous credentials with optional anonymity revocation[A]. Proceedings of EUROCRYPT 2001[C]. Berlin: Springer-Verlag, 2001. 93-118.

[15] CHEN L, ESCALANTE A, LÖHR H, *et al*. A privacy-protecting multi-coupon scheme with stronger protection against splitting[A]. Proceedings of Financial Cryptography 2007[C]. Berlin: Springer-Verlag, 2008. 29-44.

[16] BLANTON M. Online subscriptions with anonymous access[A]. Proceedings of ASIA-CCS 2008[C]. New York: ACM Press, 2008, 217-227.

[17] CAMENISCH J, HOHENBERGER S, KOHLWEISS S M, *et al*. How to win the clonewars: efficient periodic n-times anonymous authentication[A]. Proceedings of ACM-CCS 2006[C]. New York: ACM Press, 2006. 201-210.

[18] DAMGÅRD I. Efficient concurrent zero-knowledge in the auxiliary string model[A]. Proceedings of EUROCRYPT 2000[C]. Berlin: Springer-Verlag, 2000. 418-430.

[19] GARAY J A, MACKENZIN P, YANG K. Strengthening zero knowledge protocols using signatures[J]. Journal of Cryptology, 2006, 19(2): 169-209.

[20] DODIS Y, SHOUP V, WALFISH S. Efficient constructions of composable commitments and zero-knowledge proofs[A]. Proceedings of CRYPTO 2008[C]. Berlin: Springer-Verlag, 2008. 515-535.

[21] ROSEN A, SHELAT A. Optimistic concurrent zero knowledge[A]. Proceedings of ASIACRYPT 2010[C]. Berlin: Springer-Verlag, 2010. 359-376.

[22] DAMGÅRD I, FAZIO N, NICOLOSI A. Non-interactive zero-knowledge from homomorphic encryption[A]. Proceedings of TCC 2006[C]. Berlin: Springer-Verlag, 2006. 41-59.

[23] CRAMER R, SHOUP V. Signature scheme based on the strong RSA assumption[J]. ACM Transactions on Information and System Security, 2000, 3(3): 161-185.

[24] NGUYEN L. Accumulators from bilinear pairings and applications[A]. Proceedings of CT-RSA 2005[C]. Berlin: Springer-Verlag, 2005. 275-292.

[25] CANARD S, GOUGET A, HUFSCHMITT E. A handy multi-coupon system[A]. Proceedings of ACNS 2006[C]. Berlin: Springer-Verlag, 2006. 66-81.

[26] DAMGÅRD I, DUPONT K, PEDERSEN M Ø. Unclonable group identification[A]. Proceedings of EUROCRYPT 2006[C]. Berlin: Springer-Verlag, 2006. 555-572.

[27] PAILLIER P. Public-key cryptosystems based on composite degree residuosity classes[A]. Proceedings of EUROCRYPT 1999[C]. Berlin: Springer-Verlag, 1999. 223-238.

[28] GALBRAITH S D, PATERSON K G, SMART N P. Pairings for cryptographers[J]. Discrete Applied Mathematics, 2008, 156: 3113-3121.

[29] FURUKAWA J, IMAI H. An efficient group signature scheme from bilinear maps[J]. IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, 2006, 89(5): 1328-1338.

[30] CAMENISCH J, LYSYANSKAYA A. A signature scheme with efficient protocols[A]. Proceedings of SCN 2002[C]. Berlin: Springer-Verlag, 2002. 268-289.

[31] BONEH D, BOYEN X. Short signatures without random oracles and the SDH assumption in bilinear groups[J]. Journal of Cryptology, 2008, 21(2): 149-177.

[32] DODIS Y, YAMPOLSKIY A. A verifiable random function with short proofs and keys[A]. Proceedings of PKC 2005[C]. Berlin: Springer-Verlag, 2005. 416-431.

作者简介：

柳欣（1978-），男，山东广饶人，山东大学博士生，山东青年政治学院讲师，主要研究方向为面向群体的安全协议设计与分析。

徐秋亮（1960-），男，山东淄博人，博士，山东大学计算机科学与技术学院副院长，主要研究方向为密码协议、可证明安全性、椭圆曲线密码学等。