doi:10.11959/j.issn.1000-436x.2016191

高效的可撤销群签名方案

仲红，黄丛林，许艳，崔杰
（安徽大学计算机科学与技术学院，安徽 合肥 230601）

摘 要：将子集覆盖框架与 Camenisch-Stadler 方案相结合，实现群成员的加入和撤销，且无需改变其他成员私钥，实现高效的签名验证效率。同时，在成员注册时增加一个知识签名，实现防联合攻击。分析表明，方案满足匿名性和抗联合攻击、伪造攻击和权威陷害攻击，并具有非关联性。效率方面，仅略增加群成员证书长度，达到常数级的签名和验证开销。

关键词：群签名；子集覆盖框架；联合攻击；非关联性
中图分类号：TP309.7 **文献标识码**：A

Efficient group signature scheme with revocation

ZHONG Hong, HUANG Cong-lin, XU Yan, CUI Jie
(School of Computer Science and Technology, Anhui University, Hefei 230601, China)

Abstract: A group signature scheme which combines the subset cover framework with Camenisch-Stadler scheme was proposed. This scheme allowed any group members' entrance and revocation without changing other members' secret key. Meanwhile, the scheme added a knowledge signature while registering, that realized coalition resistance. It is shown that the scheme not only has the characteristics of anonymity and no-relation, but also can resist conspiracy attacks, forgery attack and authority trap attack. As for efficiency, the scheme just slightly increases the length of group members' certificates, with the signature and verification complexity remaining at constant level.

Key words: group signature, subset cover framework, conspiracy attack, no-relation

1 引言

群签名（group signature）概念是 1991 年由 Chaum 和 Heyst 首次提出[1]的，在群签名中，群成员可以匿名代表群进行签名，验证者只能验证签名是否由群成员签署，却不能确定签名者的身份。必要时，如签名被举报，群管理员可以打开签名追踪签名者真实身份。由于这些特征，群签名能广泛运用于政务、商务等场景[2~4]。早期提出的群签名方案中，群公钥或签名长度与群成员数线性相关，签名效率低，不适合大群。1997 年，Camenisch 等[5]首次提出适用于大群的群签名方案，该方案中的群签名长度和群公钥是固定的，独立于群成员个数，且加入新成员时无需改变其他成员私钥，但该方案不能撤销群成员。

然而，在实际应用中，群中成员是动态加入和退出的，其中，成员撤销是群管理员主动撤销非法群成员或群成员主动离开群。例如，某恶意群成员发送的非法信息遭举报，群管理员核实后将该恶意成员踢出群，保障群中其他合法成员安全。2003 年，王尚平等[6]在 Camenisch-Stadler 群签名方案基础上，提出利用更新算子进行成员撤销的解决方案，当群成员加入或撤销时，群管理员公布群特性公钥和成员特性私钥更新算子，群成员根据更新算子计算签名密钥，但不能完全撤销群成员。Libert 等在 2005 年[7]和 Nakanishi[8]在

收稿日期：2016-02-02；**修回日期**：2016-06-07
通信作者：黄丛林，hcllin313@163.com
基金项目：国家自然科学基金资助项目（No.61572001）；安徽省自然科学基金资助项目（No.201508085QF132）
Foundation Items: The National Natural Science Foundation of China (No.61572001), The Natural Science Foundation of Anhui Province (No.201508085QF132)

2009 年都提出离线验证的群成员撤销方案，群成员维护一个撤销列表，撤销信息仅发送给验证者进行验证，签名开销独立于撤销群成员数量，但每次撤销群成员都要更新撤销列表，验证开销与撤销成员数呈线性增加。2008 年，李新社等[9]对文献[6]方案进行改进，群成员计算自己的特性密钥，然后交给群管理员计算特性密钥更新算子，实现群成员有效撤销。群成员每次加入或撤销时，群管理员都要重新计算自己的特性公钥和群成员的特性密钥更新算子，大大增加群管理员计算开销。2011 年，Fan 等[10]提出基于累加器的群签名撤销方案，群管理员负责更新撤销信息，然而，群成员撤销时，群管理员需要更新每个群成员的签名密钥，大大增加了群管理员的计算量。2012 年，Libert 等[11]提出个可扩展撤销方案，实现群成员加入或撤销时，签名和验证复杂度独立于群成员数量，但群成员需要存储 $O(\log^3 N)$ 的成员证书，大大增加系统的存储代价。2014 年，张德栋等[12]针对 Camenisch-Stadler 方案提出一个有效成员撤销解决方案，利用群成员证明其身份不在排序的撤销列表中，达到撤销目的，但该方案在签名证明和验证签名时使用较多的模幂运算，效率较低。近年，一些新型群签名也被提出，如基于格群签名[13]、基于量子群签名[14]等。

本文将子集覆盖框架中的完备子树方法和子集差分方法分别与 Camenisch-Stadler 方案相结合，提出 2 种可撤销的群签名方案。子集覆盖框架原本是针对广播加密的密钥分发提出的，群管理员将群成员对应一个完备树的叶节点，同时为树中每个节点分配一个密钥值，将群成员对应叶节点到根节点的值发送给对应群成员，作为签名密钥；然后，群管理员选取包含群中所有合法节点的子集，公布子集节点对应密钥值，这样，合法群成员就利用自己存储的与群管理员公布相同的密钥值进行签名，被撤销成员无法找到对应值进行签名，达到撤销成员目的。同时，通过在成员向群管理员注册时增加一个知识签名，弥补 Camenisch-Stadler 方案不能抗联合攻击问题，防止成员联合进行内联注册，进而伪造签名。最后，对本方案安全性和效率进行分析，得出方案具有如下优点：1) 当有群成员加入和撤销时，无需改变其他群成员的签名私钥和证书；2) 群签名长度和验证开销独立于群成员数和撤销成员数。

2　预备知识

2.1　子集覆盖框架

子集覆盖框架是由 Naor 等[15]提出，用于广播加密密钥分发。根据选取子集的方法不同，分为完备子树方法和子集差分方法。

2.1.1　完备子树方法

完备子树方法中，首先构建一个 $l=\log N-1$ 层的完全二叉树 T，树中节点标记为 $x_{i,j}$，$i\in l, j\in N$，把用户分配到叶节点 $x_{l,j}$，用户存储其对应叶节点到根节点路径上所有节点值。N 是叶节点总数，R 是被撤销叶节点。完备子树方法选取包含所有未被撤销合法叶节点 $\frac{N}{R}$ 的 m 个子树集合 $S_1,S_2,\cdots,S_m$，$m\leqslant R\log\left(\frac{N}{R}\right)$。

如图 1 所示，高为 3 的完全二叉树有 8 个叶节点，对应 8 个用户，其中，$x_{3,1}$、$x_{3,7}$、$x_{3,8}$ 是要撤销的节点。利用完备子树方法选取包含未撤销叶节点的子集为 $S_i=\{x_{3,2},x_{2,2},x_{2,3}\}$，其中，$i=3$。

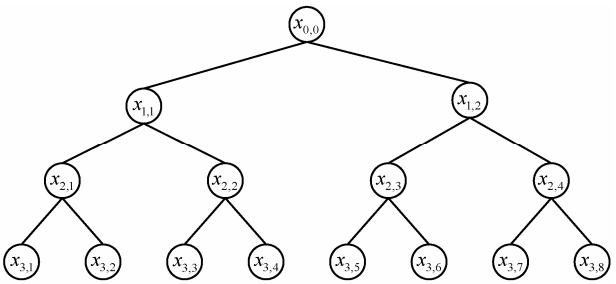


图 1　完备子树方法示例

2.1.2　子集差分方法

同完备子树方法，首先构建一个 $l=\log N-1$ 层的完全二叉树 T，树中节点标记为 $x_{i,j}$，$i\in l, j\in N$，把用户分配到叶节点 $x_{l,j}$。集合 S 表示在以 $x_{i,j}$ 为根节点的子集中且不在以 $x_{p,q}$ 为根节点的子集中的节点集合，其中，$x_{i,j}$ 是 $x_{p,q}$ 根节点。子集差表示为 $S=x_{i,j}-x_{p,q}$，为每个 S 选取不同的值，令 w_j 为从叶节点 $x_{l,j}$ 到根节点 $x_{0,0}$ 路径上所有节点的兄弟节点（根节点无兄弟节点）。用户存储从其对应叶节点 $x_{l,j}$ 到根节点路径上的所有节点 $x_{i,j}$ 减去以其为根的 $x_{l,j}$ 所有兄弟节点 w_j 的集合 S_j 值，其中，$j=l^2$。子集差分方法利用差集选取包含所有未撤销叶节

点成员 $\frac{N}{R}$ 的子集 S_m， $m \leqslant 2R-1$。

如图 2 所示，高为 3 的完全二叉树有 8 个叶节点，对应 8 个用户，其中，$x_{3,1}$、$x_{3,7}$、$x_{3,8}$ 是要撤销的节点。利用子集差分方法选取包含未撤销叶节点的子集为 $S_i=\{(x_{2,1}-x_{3,1}),(x_{1,1}-x_{2,1}),(x_{1,2}-x_{2,4})\}$，其中，$i=3$。

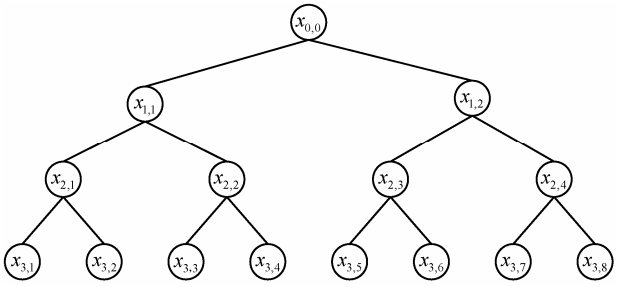


图 2 子集差分方法示例

2.2 基于离散对数的知识签名

知识签名是一种数学构造，签名者可以利用这种数学构造在不泄露某秘密的前提下，证明自己拥有这个秘密。本方案使用基于离散对数的知识签名，具体如下。

称使等式 $c=H(g\|y\|g^s y^c\|m)$ 成立的二元组 $(c,s)\in\{0,1\}^k\times Z_n^*$ 为对消息 m 关于 $y\in G$ 的离散对数知识签名，表示为 $SKLOG\{\alpha: y=g^a\}$。其中，$H:\{0,1\}^*\to\{0,1\}^k$ 是具有抗碰撞性的散列函数。假设成员拥有使等式 $y=g^x$ 成立的私钥 x，对消息 m 的知识签名 (c,s) 获得步骤如下。

1) 随机选择 $r\in Z_n^*$，计算 $t=g^r \bmod p$。

2) 计算 $c=H(g\|y\|t\|m)$。

3) 计算 $s=(r-xc)\bmod n$。

3 本文方案

3.1 系统初始化

1) 群管理员身份为 ID_C，选取一个 RSA 模数 n_C 和一个散列函数 $h(\cdot)$。选择公开指数 $e_1,e_2>1$ 和正整数 $f_1,f_2>1$，且 e_2 与 $\phi(n_C)$ 互素，n_C 因式分解未知，f_1,f_2 的 e_1 次根和 e_2 次根是计算困难的。

2) 选择在其中计算是离散对数困难的循环群 $G=<g>$，阶为 n_C，元素 $h\in G$ 是以 g 为基的离散对数，是计算困难的。

3) 选择私钥 $x_C\in Z_n^*$，令 $y_C=h^{x_C}(\bmod n_C)$。随机选择 $e_C\in Z^*{}_n$，计算 d_C 满足 $e_C d_C\equiv 1(\bmod \phi(n_C))$。其中，$y_C$、$e_C$ 为群管理员公钥，x_C、d_C 为群管理员私钥。公开 $(n_C,y_C,e_1,e_2,f_1,f_2,G,g,h)$。

4) 群管理员建立一个层数为 $l=\log N-1$ 的完全二叉树 T，N 为树中叶节点数。树中节点被标识为 $x_{i,j}$，$i=0,\cdots,l$ 和 $j=0,\cdots,2^i$ 分别表示每层和对应层的节点。群管理员为每个群成员 U_j 分配树中叶节点 $x_{l,j}$。利用以下完备子树方法或子集差分方法初始化。

①完备子树方法。对每个节点 $x_{i,j}$，群管理员选择一个对应整数 b_k，b_k 也相当于以对应节点为根的子集 S_j 值，其中，$k=0,\cdots,2^l-1$。使 a_k 满足 $a_k b_k\equiv 1(\bmod \phi(n_C))$，最终群管理员存储每个树节点元组 $(x_{i,j},g^{a_k},b_k,(b_k)^{d_C})$。此过程在群管理员后台离线运行，并不占用签名时间。将从树根节点到用户对应叶节点路径上所有节点元组 $\{g^{a_k},b_k,(b_k)^{d_C}\}_{k=0}^{l}$ 发送给 U_j。群管理员存储每个用户信息元组表 $(ID_j,x_{l,j},\{g^{a_k},b_k,(b_k)^{d_C}\}_{k=0}^{l})$。

②子集差分方法。对每个叶节点 $x_{l,j}$，群管理员选取 $x_{l,j}$ 到根节点路径上的所有节点 $x_{i,j}$ 减去以 $x_{i,j}$ 为根到 $x_{l,j}$ 路径上所有兄弟节点 w_j 的集合 S_j，为每个集合 S_j 选取一个对应整数 b_k，其中，$k=0,\cdots,2^{l^2}-1$。使 a_k 满足 $a_k b_k\equiv 1(\bmod \phi(n_C))$。发送对应元组 $\{g^{a_k},b_k,(b_k)^{d_C}\}_{k=0}^{l^2}$ 给 U_j。群管理员存储每个用户信息元组表 $(ID_j,x_{l,j},\{g^{a_k},b_k,(b_k)^{d_C}\}_{k=0}^{l^2})$。

5) 假设系统中有 n 个成员 $(n\geqslant 2)$。群管理员利用完备子树方法或子集差分方法，选取包含所有未撤销用户对应叶节点的子树集合 S_m，用每个子树的根节点表示对应子集，m 为子集数目。如图 1 和图 2 所示，群管理员公布子集 S_m 对应的 b_k 集合 $C=(t,\{b_k\}_{k=1}^{m})$，其中，t 为时间戳。

3.2 成员加入

1) 用户 U_i 要加入群，首先随机选择 $x_i\in Z_n^*$，令 $y_i=x_i^{e_1}(\bmod n_C)$，计算身份 $ID_i=g^{y_i}(\bmod n_C)$，其中，x_i、y_i 是其身份私钥，并产生一个 ID_i 对 g 的知识签名[16] $W=SPK[\lambda: ID_i=g^{\lambda}](\prime\prime)$。

2) 为防止申请成员证书时群管理员伪造签名，U_i 计算 y_i 的盲化值 y_i^* 以及 ID_i 和 y_i^* 的知识证明为

$$y_i^*=r^{e_2}(f_1 y+f_2)(\bmod n_C),\quad r\in_R Z_n^*$$

$$U:=SKROOTLOG[\alpha: ID_i=g^{\alpha^{e_1}}](\prime\prime)$$

$V \coloneqq SKROOTLOG[\beta : g^{y_i^*} = (ID_i^{f_1} g^{f_2})^{\beta^{e_1}}](r')$

U_i 将 ID_i、y_i^*、W、U、V 发送给群管理员。

3) 群管理员验证 W、U、V 是否正确，若正确，则确信 y_i^* 是 ID_i 所含成员密钥的盲化值，并计算 $v^* = (y^*)^{\frac{1}{e_2}} (\mathrm{mod}\, n_C)$。然后群管理员根据子集覆盖给 U_i 分配一个 T 中叶节点 $x_{l,i}$，群管理员用完备子树方法选择从叶节点 $x_{l,i}$ 到根节点路径上所有节点元组或利用子集差分方法选取从其对应叶节点 $x_{l,j}$ 到根节点路径上的所有节点 $x_{i,j}$ 减去以其为根的 $x_{l,j}$ 所有兄弟节点 w_j 的集合 S_j 值，并存储用户元组表 $Y = (ID_i, x_{l,i}, v_i^*, (v_i^*)^{d_C}, \{g^{a_k}, b_k, (b_k)^{d_C}\}_{k=0}^{l})$。将 U_i 部分证书 $H = (v_i^*, (v_i^*)^{d_C}, \{g^{a_k}, b_k, (b_k)^{d_C}\}_{k=1}^{l})$ 发送给 U_i。

4) U_i 收到 H 后，验证 $v_i^* = ((v_i^*)^{d_C})^{e_C}$，若等式成立，则确认是群管理员发送并保存，计算 $v_i = \dfrac{v_i^*}{r} = (f_1 y + f_2)^{\frac{1}{e_2}} (\mathrm{mod}\, n_C)$。$U_i$ 最终成员证书为 $(v_i, \{g^{a_k}, b_k, (b_k)^{d_C}\}_{k=0}^{l})$。

5) 群管理员利用子集覆盖框架方法，重新选取包含新加入成员和其他所有合法用户对应叶节点的子树集合 S_m，并公布其对应 b_k 集合 $C = (t, \{b_k\}_{k=1}^{m})$。

3.3 成员撤销

群管理员若要撤销成员 U_j，利用完备子树方法，首先定位到 U_j 对应叶节点 $x_{l,j}$，重新选择不包含 U_j 对应叶节点的子集。根据树形结构可知，完备子树方法中只需避免选择从 $x_{i,j}$ 到根节点路径上节点即可，其他子集节点不变，最后，发布新的子集列表 $S_m^{'} = \{x_{i,j}\}_{i \in l, j \in 2^i}$ 所对应 b_k 集合 $C = (t, \{b_k\}_{k=1}^{m})$；子集差分方法只需选取新的不包含 U_j 对应叶节点的差集 $S = x_{i,j} - x_{p,q}$ 的 b_k 值即可，最后也发布新的子集列表对应集合 C。由于新子集列表不包含 U_j 存储的 b_k，U_j 无法利用其产生合法签名。

3.4 签名

1) U_i 要对消息 m 进行签名，首先根据群管理员最新发布的 C 和自己的成员证书 $\{g^{a_k}, b_k, (b_k)^{d_C}\}_{k=0}^{l}$ 找到相同 b_t，然后利用 (g^{a_t}, b_t) 元组进行签名。其中定能找到唯一相同 b_t，因为群管理员根据子集覆盖框架中方法选取包含 U_i 对应叶节点的子集时，必会选取 U_i 存储的从 $x_{l,i}$ 到根节点路径上一节点或子集差中包含其叶节点（此步骤可在签名前离线处理，只要收到新的 C 即可）。然后计算 $q = (g^{a_t})^{h(m)} (\mathrm{mod}\, n_C)$。

2) 与原方案相同，U_i 首先计算对信息的知识签名，证明是其群成员；其次，利用群管理员的公钥对其成员公钥进行加密，让群管理员在必要时可以打开签名。具体描述如下。

U_i 随机选择 $r \in Z_n^*$，计算

$ID_i^* = h^r g^{y_i}$，　$d = y_C^r$

$V_1 \coloneqq SKROOTREP[\alpha, \beta : ID_i^* = h^{\alpha} g^{\beta^{e_1}}](m)$

$V_2 \coloneqq SKROOTREP[\gamma, \delta : ID_i^{*f_1} g^{f_2} = h^{\gamma} g^{\beta^{e_2}}](m)$

$V_3 \coloneqq SKREP[\varepsilon, \varsigma : d = y_C^{\varepsilon} \wedge ID_i^* = h^{\varepsilon} g^{\varsigma}](m)$

U_i 消息签名 $\sigma_i = (q, b_t, (b_t)^{d_C}, ID_i^*, d, V_1, V_2, V_3)$

3.5 验证

U_j 收到 U_i 的签名，首先确认 b_t 在最新群公布列表中，验证等式 $b_t = ((b_t)^{d_C})^{e_C} (\mathrm{mod}\, n_C)$ 和 $g^{h(m)} = q^{b_t} (\mathrm{mod}\, n_C)$ 是否成立，若都成立，验证消息的完整性和 U_i 是未被撤销成员群成员，否则拒绝签名。然后验证 (V_1, V_2, V_3) 的正确性，若正确，验证者确信 $\delta^{e_2} = f_1 \beta^{e_1} + f_2 (\mathrm{mod}\, n_C)$，$\gamma = \alpha f_1 (\mathrm{mod}\, n_C)$，从而使验证者相信 ID_i^* 和 d 的计算使用了同一个随机数 $r = \varepsilon$，接受签名。同时确保在必要时，群管理员可以打开签名。

3.6 追踪

本方案的追踪过程与原群签名方案的追踪过程完全一致，通过计算 $ID_i = \dfrac{ID_i^*}{d^{\frac{1}{x_C}}}$ 来追踪 U_i 身份。

4 安全性和效率分析

本节对方案的安全性和效率进行分析。安全性主要包括正确性、匿名性、防联合攻击、防伪造攻击、防权威陷害攻击、非关联性 6 个方面内容。此外，将方案安全性和效率与已有方案进行对比，体现本方案的优势。

4.1 安全性分析

4.1.1 正确性

若签名 $\sigma_i = (q, b_t, (b_t)^{d_C}, ID_i^*, d, V_1, V_2, V_3)$ 由合法群成员 U_i 产生，一定能通过验证，且能被群管理员追踪签名者身份。

1) 验证者首先通过检查 b_t 是否在最新群公布的列表 C 中来判断签名者是否被撤销；通过验证等式 $e_C d_C \equiv 1 (\mathrm{mod}\, \phi(n_C))$ 和 $g^{h(m)} = q^{b_t} (\mathrm{mod}\, n_C)$ 来确认签名的合法性和消息完整性。因为 $e_C d_C \equiv 1 (\mathrm{mod}\, \phi(n_C))$

中 d_C 是群管理员私钥，表明 b_t 是群管理员私钥签署；因为 $q^{b_t}=((g^{a_t})^{h(m)})^{b_t}(\mathrm{mod}\,n_C)=g^{h(m)}$，其中，$h(m)$ 表明消息的完整性，g^{a_t} 是成员注册时群管理员秘密发送给群成员的，等式成立表明该成员是合法群成员。

2) 验证 (V_1,V_2,V_3) 的正确性描述与原文相同，目的是使验证者确信 $\delta^{e_2}=f_1\beta^{e_1}+f_2(\mathrm{mod}\,n_C)$，$\gamma=\alpha f_1(\mathrm{mod}\,n_C)$，表示 U_i 成员私钥为 $x_i=\beta$，同时拥有成员证书 $v_i=\delta$；通过 V_3 的验证，验证者确信 ID^* 和 d 的计算使用同一个随机数 $r=\varepsilon$，即 (d,ID_i^*) 是 U_i 利用群管理员公钥 (h,y_C) 对成员公钥 ID_i 的一个 ElGamal 加密，确保在必要时，群管理员可以打开签名，追踪签名者的真实身份。

3) 若群管理员追踪签名者 U_i 身份，发现其有非法行为，就要把 U_i 撤销。根据子集覆盖中完备子树方法或子集差分方法，群管理员选取新的子集时不包含 U_i 存储的 $\{(g^{a_k},b_k,(b_k)^{d_C})\}_{k=0}^{k=l}$ 元组对应节点，然后发布新子集节点对应的 b_k 集合 $C=\{t,b_k\}_{k=1}^{m}$。这样，U_i 在签名时无法在新 C 中找到相同 b_k，无法通过 $q=(g^{a_t})^{h(m)}(\mathrm{mod}\,n_C)$ 等式验证，因为解 g^{a_t} 为离散对数困难性问题。因此，U_i 被撤销。

4.1.2 匿名性

U_i 签名为 $\sigma_i=(q,b_t,(b_t)^{d_C},ID_i^*,d,V_1,V_2,V_3)$，其中，$ID_i^*$ 是 U_i 身份 ID_i 的盲化值，每次签名都取不同随机数进行盲化，攻击者若想从 ID_i^* 中计算得出 ID_i，就要解决离散对数困难性问题。因此，本方案满足匿名性。

4.1.3 防联合攻击

1) 若 $n>1$ 个群成员想联合进行共模攻击[16]，则需得到 n_C 分解因子，从而攻破群系统，伪造其他任何成员签名。但通过 $a_kb_k\equiv 1(\mathrm{mod}\,\phi(n_C))$ 进行共模攻击分解 n_C，就要知道 a_k 和 b_k。由于群成员只知道 g^{a_k} 和 b_k，求解 a_k 等价于求解离散对数困难问题。因此，群成员无法进行联合攻击分解 n_C。

2) 根据周玉等[17]对 Camenisch-Stadler 方案安全分析可知，在不知 n_C 因式分解前提下，群成员可以联合攻击，以此伪造密钥身份证书进行签名，并被跟踪。此类攻击策略是几个用户利用关联的私钥注册，获得内在关联的身份证书，然后算出群管理员签名的关键因子。本方案在用户注册时产生一个 ID_i 对 g 的知识签名 $W=SPK[\lambda:ID_i=g^{\lambda}]('')$，防止用户关联私钥进行注册。同时，在签名验证时验证 (V_1,V_2,V_3) 的正确性，使验证者确信 $\delta^{e_2}=f_1\beta^{e_1}+f_2(\mathrm{mod}\,n_C)$，$\gamma=\alpha f_1(\mathrm{mod}\,n_C)$，从而验证者相信 ID_i^* 和 d 的计算使用同一个随机数 $r=\varepsilon$，即 (d,ID_i^*) 是 U_i 利用群管理员公钥 (h,y_C) 对成员公钥 ID_i 的一个 ElGamal 加密。若群中能够产生有效、不被追踪的签名，则表明群成员能伪造群私钥，其难度相当于求解离散对数困难性难题。

4.1.4 防伪造攻击

若成员 U_j 想要伪造一个可通过验证的签名，且真实身份不被追踪。U_j 可从以下 3 个方面进行伪造攻击。

1) U_j 联合其他成员利用关联注册或共模攻击分解 n_C，从而攻破整个系统，进行伪造攻击。由 4.1.1 节可知，本方案在注册时利用知识签名实现防联合攻击，U_j 无论被撤销与否，都不能联合攻击，也无法利用共模攻击分解 n_C，从而不能伪造签名。

2) U_j 从收到的签名中获取签名信息伪造签名。假设 U_j 收到成员 U_i 的签名 σ_i，利用其 $(q,b_t,(b_t)^{d_C},ID_i^*,d)$ 签名信息伪造签名。若 U_j 被撤销，群管理员利用子集覆盖中方法选择的子集对应值 $\{b_k\}_{k=1}^{m}$ 并不在 U_j 存储的元组列表 $\{(g^{a_k},b_k,(b_k)^{d_C})\}_{k=0}^{k=l}$ 中，解 g^{a_t} 为离散对数困难性问题，因此，U_j 签名无法通过 U_i 等式验证；若 $\sigma_i=(q,b_t,(b_t)^{d_C},ID_i^*,d,V_1,V_2,V_3)$ 未被撤销，在群管理员公布的 ID_i^* 中找到自己存储 U_i 对应元组 ID_i，签名能够通过 ID_i^* 等式验证，但由于不知 ID_i 私钥和 (ID_i^*,d) 分解，无法通过 (V_1,V_2,V_3) 正确性验证。因此，U_j 无法成功利用其他成员签名信息伪造签名。

3) U_j 被撤销后，修改自己的签名和验证，信息通过验证来伪造签名。由于 U_j 被撤销，C 被更新，其存储的 b_k 不属于当前群发布 C 中的值，已不能通过验证。U_j 想伪造 b_t' 和 q' 值进行签名，并通过 $((q')^{h(m)})^{b_k}(\mathrm{mod}\,n_C)=g^{h(m)}$ 验证，但 U_j 无法获知群私钥 d_C，无法通过 $b_t'=((b_t')^{d_C})^{e_C}(\mathrm{mod}\,n_C)$ 验证。所以，无法通过修改信息伪造签名。

4.1.5 防权威陷害攻击

本文方案中成员 U_i 向群管理员注册时，U_i 只将 y_i 的盲化值 y_i^* 和 ID_i 发送给群管理员，其私钥信息 x_i,y_i 并未告知群管理员，群管理员若要伪造 U_i 签名，计算 $ID_i=g^{y_i}(\mathrm{mod}\,n_C)$ 中 y_i 为离散对数难题。所以，群管理员无法冒充群成员进行签名。

4.1.6 非关联性

根据树结构特性，本方案中 b_k 并不是唯一对应一个成员身份，即使群成员收到签名中的 b_k，也无法确定 b_k 对应多少成员身份，更无法定位到哪个成员，满足非关联性。

群成员在签名时选择随机数 r 生成 ID_i^*、d，且 q、b_t 与群成员身份无直接关联，因此，验证者无法通过签名判断 2 个不同群签名是否来自一个签名者，满足非关联性。

4.2 效率分析

针对效率分析，本方案对基于完备子树方法方案和基于子集差分方法方案效率都进行了分析和对比。对比方案都满足成员撤销，如表 1 所示，既有基于双线性对的 Libert 方案[7]和 Nakanish 方案[8]，又有对 Camenisch-Stadler 方案修改的李新社方案[9]和张德栋方案[12]。同时给出了本文方案与李新社方案[9]和张德栋方案[12]的详细开销对比，体现了本文方案具有一定优势。表 1 中，“T”表示撤销成员次数，“R”和“N”分别表示撤销成员数和成员总数；表 2 中，“E”表示模幂运算次数，“H”表示散列运算次数。

从表 1 可知，本文完备子树方案和子集差分方案在群公钥长度、签名长度以及签名开销和验证开销都是最低的 $O(1)$，完备子树方案增加了少量撤销开销，但达到比子集差分方案更小的成员证书长度；子集差分在撤销开销和存储方面更低，但增加了成员证书存储。相比其他方案，本文 2 种方案在群公钥长度、签名长度、签名开销和验证开销复杂度都是最低，其中，完备子树的撤销列表长度也较低；虽然张德栋方案撤销开销更低，但其签名、验证具体开销大大高于本文 2 种方案，且本文撤销开销都是查询逻辑树结构代价，并非计算代价。综合对比，本文方案具有更平衡的整体开销。

表 2 开销详细对比中的方案都是基于对 Camenisch-Stadler 方案的修改方案，从对比中可知，本文 2 种方案的签名开销最低，验证开销略高于李新社方案，但李新社方案撤销计算开销太大，撤销开销只比张德栋方案略高，但张方案在签名和验证开销使用了大量的散列函数和指数运算，开销明显高于本文方案；同时，本文撤销开销为群管理员选取子集时查询代价，无需大量计算开销。故在整体开销方面，本方案是对比方案中最好的。

表 2　开销详细对比

方案名称	签名开销	验证开销	撤销开销
李新社方案[9]	$3E$	E	$(N+1)E$
张德栋方案[12]	$5H+42E$	$6H+35E$	E
完备子树方案	$H+E$	$H+3E$	$O\left(R\log\left(\frac{N}{R}\right)\right)$
子集差分方案	$H+E$	$H+3E$	$O(R\log N)$

5 结束语

本文方案通过将子集覆盖框架的完备子树方法或子集差分方法与 Camenisch-Stadler 方案相结合，实现了成员撤销和加入，并在成员注册时增加一次知识签名，实现了防联合攻击，同时，还实现了匿名性、防伪造性和防权威陷害攻击以及非关联性。效率方面，通过对本文 2 种方法方案对比可见，完备子树方案适合群管理员计算能力和开销较强，用户只需存储很少成员证书的情况；而子集差分方法适合群管理员计算和存储能力适中，用户存储能力较强的情况。在与其他方案对比中可看出，本方案具有更平衡的整体开销，体现了本方案的一定优势。但本文 2 种方案在撤销时的查询代价与撤销成员数相关，如何减少撤销代价有待今后进一步研究。

表 1　各协议开销复杂度对比

方案名称	群公钥长度	签名长度	成员证书长度	撤销列表长度	签名开销	验证开销	撤销开销
Libert 方案[7]	$O(T)$	$O(1)$	$O(1)$	$O(R)$	$O(1)$	$O(R)$	$O(R)$
Nakanish 方案[8]	$O(T)$	$O(1)$	$O(1)$	$O(R)$	$O(1)$	$O(R)$	$O(R)$
李新社方案[9]	$O(1)$	$O(1)$	$O(1)$	—	$O(1)$	$O(1)$	$O(N)$
张德栋方案[12]	$O(1)$	$O(1)$	$O(1)$	$O(R)$	$O(1)$	$O(1)$	$O(1)$
完备子树方案	$O(1)$	$O(1)$	$O(\log N)$	$O\left(R\log\left(\frac{N}{R}\right)\right)$	$O(1)$	$O(1)$	$O\left(R\log\left(\frac{N}{R}\right)\right)$
子集差分方案	$O(1)$	$O(1)$	$O(\log^2 N)$	$O(R)$	$O(1)$	$O(1)$	$O(R\log N)$

参考文献：

[1] CHAUM D, VAN H E. Group signatures[M]//Advances in Cryptology. Berlin Heidelberg: Springer, 1991: 257-265

[2] MALINA L, VIVES-GUASCH A, CASTELLÀ-ROCA J, et al. Efficient group signatures for privacy-preserving vehicular networks[J]. Telecommunication Systems, 2015, 58(4): 293-311.

[3] KUZHALVAIMOZHI S, RAO G R. Privacy protection in cloud using identity based group signature[C]//2014 Fifth Applications of Digital Information and Web Technologies (ICADIWT), IEEE. 2014: 75-80.

[4] MALINA L, SMRZ J, HAJNY J, et al. Secure electronic voting based on group signatures[C]// 2015 38th International Conference on Telecommunications and Signal Processing. 2015: 6-10.

[5] CAMENISCH J, STADLER M. Efficient group signature schemes for large groups[M]//Advances in Cryptology. Berlin Heidelberg: Springer, 1997: 410-424.

[6] 王尚平, 王育民, 王晓峰, 等. 群签名中成员删除问题的更新算子解决方案[J]. 软件学报, 2003, 14(11): 1911-1917.
WANG S P, WANG Y M, WANG X F, et al. A new solution scheme for the member deletion problem in group signature by use of renew operator[J]. Journal of Software, 2003, 14(11): 1911-1917.

[7] LIBERT B, VERGNAUD D. Group signatures with verifier-local revocation and backward unlinkability in the standard model[M]// Cryptology and Network Security. Berlin Heidelberg: Springer, 2009: 498-517.

[8] NAKANISHI T, FUNABIKI N. Verifier-local revocation group signature schemes with backward unlinkability from bilinear maps[M]// Advances in Cryptology. Berlin Heidelberg: Springer, 2005: 533-548.

[9] 李新社, 胡予濮. 一个群签名成员删除方案的分析和改进[J]. 西安电子科技大学学报, 2008, 35(3): 478-482.
LI X S, HU Y P. Analysis and improvement of the group signature member deletion scheme[J]. Journal of Xindian University, 2008, 35(3): 478-482.

[10] FAN C I, HSU R H, MANULIS M. Group signature with constant revocation costs for signers and verifiers[M]//Cryptology and Network Security. Berlin Heidelberg: Springer, 2011: 214-233.

[11] LIBERT B, PETERS T, YUNG M. Scalable group signatures with revocation[M]//Advances in Cryptology. Berlin Heidelberg: Springer, 2012: 609-627.

[12] 张德栋, 马兆丰, 杨义先, 等. 群签名中成员撤销问题解决方案[J]. 通信学报, 2014, 35(3): 193-200.
ZHANG D D, MA Z F, YANG Y X, et al. New solution scheme for the member revocation in group signature[J]. Journal on Communications, 2014, 35(3): 193-200.

[13] LING S, NGUYEN K, WANG H. Group signatures from lattices: simpler, tighter, shorter, ring-based[M]//Public-Key Cryptography. Berlin Heidelberg: Springer, 2015: 427-449.

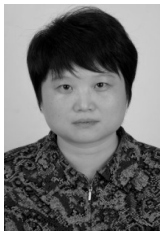
[14] SU Q, LI W M. Improved group signature scheme based on quantum teleportation[J]. International Journal of Theoretical Physics, 2014, 53(4): 1208-1216.

[15] NAOR D, NAOR M, LOTSPIECH J. Revocation and tracing schemes for stateless receivers[M]//Advances in Cryptology. Berlin Heidelberg: Springer, 2001: 41-62.

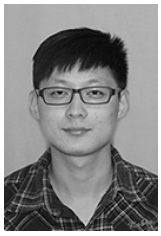
[16] STINSON D R. Cryptography: theory and practice[M]. CRC Press, 2005.

[17] 周玉, 施荣华, 胥磊. Camenisch—Stadler 群签名方案安全性的进一步分析与改进[J]. 计算机工程与应用, 2007, 42(35): 130-132.
ZHOU Y, SHI R H, XU L. Further analysis and improvement for Camenisch-Stadler group signature schemes[J]. Computer Engineering and Applications, 2007, 42(35): 130-132.

作者简介：

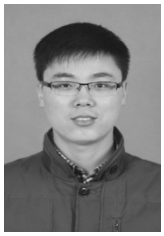


仲红（1965-），女，安徽固镇人，博士，安徽大学教授、博士生导师，主要研究方向为网络与信息安全。



黄丛林（1990-），男，安徽广德人，安徽大学硕士生，主要研究方向为车联网匿名认证协议和群签名方案。

许艳（1982-），女，江苏泗洪人，博士，安徽大学讲师，主要研究方向为信息安全和无线传感网络。



崔杰（1980-），男，河南淮阳人，博士，安徽大学副教授、硕士生导师，主要研究方向为网络与信息安全。