doi:10.3969/j.issn.1000-436x.2014.03.022

群签名中成员撤销问题解决方案

张德栋[1]，马兆丰[2]，杨义先[2]，钮心忻[2]
（1.中国铁道科学研究院 电子计算技术研究所，北京 100081；2.北京邮电大学 信息安全中心，北京 100876）

摘 要：针对 Camenisch-Stadler 群签名方案中无法撤销成员的问题，提出了一种有效的群成员撤销方案，该方案可以灵活地增加和撤销群成员。当成员加入时，群主管向其颁发成员证书，其他成员无需更新成员密钥和证书；当成员撤销时，群主管只需将撤销成员的匿名身份更新到撤销列表中，无需更新群密钥和其他成员证书，且签名长度与验证工作量均独立于群成员和已撤销成员的个数。因此，新方案适用于群成员数较多和成员更新比较频繁的群签名。

关键词：群签名；成员撤销；离散对数；知识证明
中图分类号：TP309 **文献标识码**：A **文章编号**：1000-436X(2014)03-0193-08

New solution scheme for the member revocation in group signature

ZHANG De-dong[1], MA Zhao-feng[2], YANG Yi-xian[2], NIU Xin-xin[2]
(1.Institute of Computing Technology, China Academy of Railway Sciences, Beijing 100081, China;
2. Information Security Center, Beijing University of Posts and Telecommunications, Beijing 100876, China)

Abstract: In order to solve the problem that Camenisch-Stadler's group signature scheme could not revoke members, a new revocation scheme based on the Camenisch-Stadler's group scheme was proposed, allowing the group manager to add new members or revoke old members flexibly and freely. When a member joins the group, the group manager issues member certificate to him (her), and other members need not update the key and certificate; when a member is revoked, the group manager only adds the anonymous identity to revocation list, and other members need not update the key and certificate either. Furthermore, the length of the signature and the computational effort are independent of the number of the group members and the revoked members, so the new scheme is more suitable for large group and the group with members' heavy updates.

Key words: group signature; member revocation; discrete logarithm; knowledge proof

1 引言

在群签名中，群成员可以代表群进行签名，验证者只能验证签名是否由群内成员所签，不能确定具体签名成员的身份。在必要时，群主管可以打开签名揭示签名者的身份。在最初提出的群签名方案[1~3]中，签名长度或群公钥长度与群成员个数呈线性关系。群签名的一个重要进展是 Camenisch- Stadler 于 1997 年提出的群签名方案[4]，该方案摆脱了群公钥长度、签名长度与群成员个数之间的线性关系，群组建立后，方案可在不改变群公开钥和其他成员证书的前提下灵活地加入新成员。然而，该方案并没有给出群成员撤销方法。但在实际应用中，群成员是动态的，新成员加入的同时也会有一些群成员被撤销。

2001 年，E.Bresson 和 J.Stern 首次针对 Camenisch-Stadler 群签名方案提出了一种群成员撤销方案[5]。在该方案中，群主管将撤销成员的身份标识更新到撤销成员列表 L 中，群成员签名时，必须提供证据证明其不在群主管公布的撤销成员列表 L 中。假如被撤销的成员有 K 个，则群成员必须提供 K 个证据。当被撤销成员较多时，签名效率较低。2003 年，王

收稿日期：2012-12-03；**修回日期**：2013-10-23
基金项目：国家自然科学基金资助项目(61121061, 90812001, 61272519)
Foundation Item: The National Natural Science Foundation of China (61121061, 90812001, 61272519)

尚平、王育民等针对 Camenisch-Stadler 群签名方案，提出了群成员删除问题的更新算子解决方案[6]，在该方案中，当成员加入或撤销时，群主管计算并公布群特性公钥和成员秘密特性钥更新算子，群成员利用更新算子重新计算各自的秘密特性钥。2005 年，黄振杰和林宣治[7]从密码学的角度对王尚平、王育民等的方案进行了分析，并指出此方案是不安全的，不能实现删除成员的目的。2008 年，李新社和胡予濮[8]对王尚平、王育民等的方案进行改进，将秘密特性钥的更新工作由各成员计算交由群主管计算，实现了群成员的有效撤销。当群成员加入或撤销时，群主管都要重新计算新的公开特性钥、秘密特性钥更新算子及每个成员新的秘密特性钥，增加了群主管的计算负载，对成员数较多或成员更新比较频繁的群，该方案存在一定的不足。近几年，针对群成员撤销问题，研究者提出了一些其他解决方案。2008 年，魏凌波等在减少签名长度和计算代价基础上，提出了一种向后无关联性的本地验证者撤销短群签名方案[9]，然而该方案不能防止陷害攻击，并且验证计算量和撤销成员数呈线性增长。2009 年，Jin 等提出了一种前向安全的群成员撤销方案[10]，并声称群签名和验证工作量、群公钥以及群成员签名私钥均与群成员的个数无关。然而，2011 年，Fan 等指出 Jin 等的方案未能解决群成员撤销中签名计算量、验证计算量与群成员长度呈线性增长的问题，并提出了一种基于累加器的群成员撤销方案[11]。在 Fan 的方案中，群管理员负责更新公开撤销信息以减少群签名者和验证者的计算量，实现了恒定的群签名计算量和验证计算量。然而，群成员撤销时，群主管需要更新每个群成员的签名密钥，增加了群主管的计算量。2012 年，Libert 等提出了一种可扩展的群成员撤销方案[12]，解决了群成员撤销中签名计算量、验证计算量与群成员长度呈线性增长的问题。然而，群成员需要 $O(\log^3 N)$ 的空间存储群成员证书，该撤销方案不适用于成员数较多的群。

在文献[13~15]的启发下，本文针对 Camenisch-Stadler 群签名方案，提出了一种成员撤销问题解决方案。在该方案中，群主管将撤销成员的匿名身份按从小到大顺序排序，生成成员撤销列表；群成员签名时，利用零知识证明协议向验证者证明其不是撤销列表中元组的成员即可。相比 Bresson 等[5]和李新社等[8]的签名方案，本方案具有以下优点：1）成员加入时，群主管向其颁发成员证书，其他成员无需更新成员密钥和证书；2）成员撤销时，群主管只需将撤销成员的匿名身份更新到撤销列表中，无需更新群密钥和其他成员证书；3）群签名长度与验证工作量独立于群成员和已撤销成员的个数。因此，新方案比较适用于成员数较多的群签名和成员更新比较频繁的群签名。

2 预备知识

n 是一个 RSA 模数，其分解未知，Z_n 表示模 n 的剩余类，Z_n^* 表示 Z_n 中对乘法可逆的元素构成的乘法群，$|n|$ 表示整数 n 的二进制长度，$\log_g a$ 表示在模 n 乘法群 Z_n^* 中以 g 为底 a 的对数，l、t、s 是安全系数，$H(\ )$是输出为 $2t$ bit 的无碰撞杂凑函数。

2.1 强 RSA 假设

存在一个多项式时间算法，输入 $|n|$，输出一个 RSA 模数 n 和一个元素 $z' \in Z_n^*$，使找到整数 $e \notin \{-1,1\}$ 和 u 满足 $z' = u^e \bmod n$ 的概率是可以忽略的。

2.2 Fujisaki-Okamoto 承诺

设 Alice 和 Bob 不知 n 的分解。$g \in Z_n^*$，$h \in (g)$，g，h 的阶是大于 160 bit 的素数，这使得在它们生成循环群中计算离散对数是不可行的。Alice 不知 $\log_g h$ 和 $\log_h g$，随机选取 $r \in_R \{-2^s n+1, 2^s n-1\}$，计算 $E(x,r) = g^x h^r \bmod n$，发送 $E(x,r)$ 给 Bob 作为对 x 的承诺。Alice 在不知道 n 的分解和 $\log_g h$ 的情况下，不可能找到 $x_1 \neq x_2$ 满足 $E(x_1,r_1) = E(x_2,r_2)$；Bob 也不可能从 $E(x,r)$ 中获得关于 x 的任何信息，该协议是统计安全的，详细分析见文献[16]，称该承诺方案为 Fujisaki-Okamoto 承诺，简称 FO 承诺。

2.3 CFT 证明

Alice 用 FO 承诺方案承诺秘密随机数 $x \in [0,b]$，下面的零知识协议将证明 $x \in [-2^{t+l}b, 2^{t+l}b]$。1）Alice 随机选取 $\eta \in_R [-2^{l+t+s}n+1, 2^{l+t+s}n-1]$，$r \in_R \{-2^s n+1, 2^s n-1\}$ 和 $\omega \in_R [0, 2^{l+1}b-1]$，计算 $W = g^{\omega} h^{\eta}$，$C = H(W)$，$c = C \bmod 2^t$，$D_1 = cx + \omega$，$D_2 = cr + \eta$。如果 $D_1 \in [cb, 2^{l+t}b-1]$，则 Alice 发送 (c, D_1, D_2) 给 Bob，否则重复上述过程。2）Bob 首先计算 $c = C = H(g^{D_1} h^{D_2} E^{-c} \bmod n) \bmod 2^t$，验证 $D_1 \in [cb, 2^{l+t}b-1]$。零知识证明协议失败的概率小于 2^{-l}，Alice 成功欺骗的概率小于 2^{-t+1}，协议在随机预言模型下是统计安全的，Bob 不能从证明中获得关于

x 的信息，详细分析见文献[17]，称该证明为 CFT 证明，记为：$PK\{x,r:E=g^x h^r \wedge x\in[-2^{t+1}b,\ 2^{t+1}b]\}$。

2.4 两承诺值相等

Alice 有秘密数 $x\in[0,b]$，g_1、g_2、h_1、h_2 的阶是大于 160 bit 的素数，设 $E=E_1(x,r_1)=g_1^x h_1^{r_1}$，$F=E_2(x,r_2)=g_2^x h_2^{r_2}$ 为 2 个 FO 承诺，其中，$r_1\in\{-2^{s_1}n+1,\cdots,2^{s_1}n-1\}$，$r_2\in\{-2^{s_2}n+1,\cdots,2^{s_2}n-1\}$，$s_1$，$s_2$ 是安全参数。Alice 向 Bob 证明 E 和 F 都是对 x 的承诺：1) Alice 选取随机数 $\eta_1\in_R[1,2^{t+l+s_1}\cdot b-1]$，$\eta_2\in_R[1,2^{t+l+s_2}b-1]$，$\omega\in_R[1,2^{t+l}-1]$，计算 $c=H(W_1\|W_2)$，$W_1=g_1^{\omega}h_1^{\eta_1}\bmod n$，$D=cx+\omega$，$D_1=cr_1+\eta_1$，$W_2=g_2^{\omega}h_2^{\eta_2}\bmod n$，$D_2=cr_2+\eta_2$，发送 (c,D,D_1,D_2) 给 Bob；2) Bob 验证 $c=H(g_1^D h_1^{D_1}E^{-c}\bmod n\|g_2^D h_2^{D_2}E^{-c}\bmod n)$。该协议在随机预言模型下是统计安全的，诚实的证明者总能成功地执行该协议，欺骗者欺骗成功的概率小于 2^{-t+1}。对该协议的详细分析见文献[18]，该协议记为 $PK\{x,r:E_1=g_1^x h_1^{r_1}\wedge E_2=g_2^x h_2^{r_2}\}$。

3 Camenisch-Stadler 群签名方案

Camenisch-Stadler 群签名方案使用了知识签名(特别是 SKROOTLOG 签名及 SKLOGLOG 签名)的概念。本文中使用 Camenisch-Stadler 群签名方案的记号。

3.1 系统建立

群主管（Group manager）计算下列值。

1) 一个 RSA 模 n 及公开的指数 $e_1,e_2>1$，且 e_2 与 $\varphi(n)$ 互素。

2) 正整数 $f_1,f_2>1$，使得其 e_1 次根及 e_2 次根在不知 n 的因式分解的情况下计算是困难的。

3) 阶为 n 的循环群 $G=<g>$，使 G 中计算离散对数是困难的。

4) 一个元素 $h\in G$，h 关于以 g 为基的离散对数是计算困难。

5) 任选一个整数 $w\in Z_n^*$，令 $y_R=h^w$ 为群主管的公开钥。

则群的公开钥为 $Y=(n,e_1,e_2,f_1,f_2,G,g,h,y_R)$，而 $\frac{1}{w}$ 及 n 的素因子为群主管的秘密钥。

3.2 成员注册

用户 Alice 欲成为群的成员。首先计算其成员私钥，任选一个整数 $x\in Z_n^*$，令 $y=x^{e_1}\bmod n$，Alice 保存 y 与 x 作为她成员身份的密钥，计算 $z=g^y$，并以 z 代表 Alice 的身份，z 是 Aiice 成员身份的公开钥。

为加入群，Alice 必须向群主管注册以获得群主管颁发的成员证书。Alice 不能直接将 y 发送给群主管，否则群主管可以冒充 Alice 生成签名。因此，Alice 发送 z，y 的盲化值 $\tilde{y}$ 以及 z 和 $\tilde{y}$ 的知识证明。Alice 计算

$$\tilde{y}=r^{e_2}(f_1y+f_2)\bmod n,\quad r\in_R Z_n^*$$

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

$$V:=SKROOTLOG[\beta:g^{\tilde{y}}=(z^{f_1}g^{f_2})^{\beta^{e_2}}](")$$

Alice 发送 z、$\tilde{y}$、U、V 给群主管，群主管验证 U、V 是否正确。如果 U、V 均正确，则群主管确信 $\tilde{y}$ 是 z 所含成员密钥的盲化值，群主管计算 $\tilde{v}=\tilde{y}^{\frac{1}{e_2}}\bmod n$，发送 $\tilde{v}$ 给 Alice。接收 $\tilde{v}$ 后，Alice 计算其成员证书：$v=\frac{\tilde{v}}{r}=(f_1y+f_2)^{\frac{1}{e_2}}\bmod n$。

3.3 信息签名

Alice 作为群的成员可以代表群对信息 M 进行签名，Alice 首先计算对信息的知识签名，证明她是群成员；其次，利用群主管的公开钥对其成员公钥进行 $f_1,f_2>1$ 加密，以使群主管在必要的时候可以打开签名。具体过程描述如下。

Alice 任选一个随机数 $r\in Z_n^*$，计算

$$\tilde{z}=h^r g^y$$

$$d=y_R^r$$

$$V_1:=SKROOTREP[\alpha,\beta:\tilde{z}=h^{\alpha}g^{\beta^{e_1}}](M)$$

$$V_2:=SKROOTREP[\gamma,\delta:\tilde{z}^{f_1}g^{f_2}=h^{\gamma}g^{\delta^{e_2}}](M)$$

$$V_3:=SKREP[\varepsilon,\zeta:d=y_R^{\varepsilon}\wedge\tilde{z}=h^{\varepsilon}g^{\zeta}](M)$$

则 Alice 对 M 的签名为 $(\tilde{z},d,V_1,V_2,V_3)$。

3.4 签名验证

对信息 M 的签名 $(\tilde{z},d,V_1,V_2,V_3)$ 的正确性是通过对 (V_1,V_2,V_3) 的正确性来判断的。对 (V_1,V_2,V_3) 的正确性验证可使验证者确信

$$\delta^{e_2}=f_1\beta^{e_1}+f_2\bmod n,\quad \gamma=\alpha f_1\bmod n$$

第 1 个等式表示 Alice 的成员证书为 $v=\delta$，且其成员秘密钥为 $x=\beta$；通过对 V_3 的验证，验证者确信 $\tilde{z}$ 和 d 的计算使用了同一个随机数 $r=\varepsilon$，即 $(\tilde{z},d)$ 是 Alice 利用群主管公钥 (h,y_R) 对成员公开钥 z 的加密。V_3 的正确性确保了在必要时，群主管可以将签名打开。

3.5 签名打开

签名打开就是对签名的解密，群主管计算

$$z=\frac{\tilde{z}}{d^{\frac{1}{w}}}$$

得到签名者的公开钥 z，群主管生成 $\tilde{z}$ 及 h 关于 (z,d,y_R) 表示的知识签名，即

$$SKREP[\rho:\tilde{z}=zd^{\rho}\wedge h=y_R{}^{\rho}]('')$$

其中，ρ 表示 $\frac{1}{w}$，即群主管的秘密钥。

4 Camenisch-Stadler 群签名成员撤销方案

本节提出了针对 Camenisch-Stadler 群签名方案的成员撤销问题解决方案，本节采用第 3 节的符号。

4.1 系统建立

系统建立与 Camenisch-Stadler 群签名方案中基本一致，不同的是增加了群安全参数 l，t，s；限定 g，h 的阶是大于 160 bit 的素数。群主管生成群公开钥 $Y=(n,e_1,e_2,f_1,f_2,G,g,h,y_R,l,t,s)$，群主管的秘密钥 $\frac{1}{w}$ 及 n 的素因子。

4.2 成员注册

成员注册中，群成员 Alice 的公开钥生成、知识证明以及群主管的验证过程与 Camenisch-Stadler 的群签名方案中成员注册完全一致。群主管验证 U、V 正确后，确信 $\tilde{y}$ 是 z 所含的成员密钥的正确盲化值，则有如下结果。

1) 群主管生成随机数 N，计算 $UID_a=H(z\|N\|\tilde{y})$ 作为 Alice 的匿名身份；生成随机数 p，计算 $P=h^p \bmod n$，$Q=g^{UID_a} \bmod n$，$EID_a=wQ+Pp \bmod n$，$\tilde{v}=\tilde{y}^{\frac{1}{e_2}} \bmod n$，发送 $(UID_a,EID_a,\tilde{v},P,Q)$ 给 Alice。

2) Alice 计算 $v=\frac{\tilde{v}}{r}=(f_1y+f_2)^{\frac{1}{e_2}} \bmod n$，保存 (UID_a,EID_a,v,P,Q)。

4.3 成员撤销

成员撤销主要是群主管生成或更新群成员撤销列表的过程。为描述方便，记 RID_v 为群成员 UID_v 撤销后的标识（$RID_v=UID_v$），则群成员撤销列表生成及更新过程描述如下。

1) 群主管生成成员撤销序列的起始标识 RID_0 和结束标识 RID_n，使其对任意群成员 UID_j（包括群内成员和被撤销成员），满足 $RID_0<UID_j$ 和 $RID_n>UID_j$。

2) 设 t_i 时刻撤销成员包括 RID_1，RID_2，…，RID_u，且满足 $RID_i<RID_{i+1}(1\leqslant i\leqslant u)$；则生成的成员撤销序列为 RID_0，RID_1，RID_2，…，RID_u，RID_n。

3) 针对成员撤销序列内的成员 $RID_i(0\leqslant i\leqslant u)$，群主管产生随机整数 l_i，计算 $L_i=h^{l_i} \bmod n$，$\sigma_i=we_1+l_iH(RID_i\|RID_{i+1}) \bmod n$，生成成员撤销列表元组 $(RID_i,RID_{i+1},\sigma_i,L_i)$；则 t_i 时刻成员撤销列表为

$$RL_{t_i}=\{t_i,(RID_0,RID_1,\sigma_0,L_0),\cdots,(RID_i,RID_{i+1},\sigma_i,L_i),\cdots,(RID_u,RID_{u+1},\sigma_u,L_u)\}$$

其中，$RID_{u+1}=RID_n$。

4) 当新成员被撤销时，群主管更新成员撤销列表。设 t_j 时刻，群成员 UID_j 被撤销，则成员撤销列表的更新过程描述如下。

(a) 群主管在成员撤销列表中查找满足 $RID_i<UID_j<RID_{i+1}$ 成立的元组 $(RID_i,RID_{i+1},\ \sigma_i,L_i)$。

(b) 产生随机数 l_i'、l_j，计算 $L_i'=h^{l_i'} \bmod n$，$L_j=h^{l_j} \bmod n$，$\sigma_i'=we_1+l_i'H(RID_i\|RID_j) \bmod n$，$\sigma_j=we_1+l_jH(RID_j\|RID_{i+1}) \bmod n$，其中 $RID_j=UID_j$。

(c) 生成成员撤销列表元组 $(RID_i,RID_j,\sigma_i',L_i')$，$(RID_j,RID_{i+1},\sigma_j,L_j)$，则 t_j 时刻成员撤销列表为

$$RL_{t_j}=\{t_j,(RID_0,RID_1,\sigma_0,L_0),\cdots,(RID_i,RID_j,\sigma_i',L_i'),(RID_j,RID_{i+1},\sigma_j,L_j),\cdots,(RID_u,RID_{u+1},\sigma_u,L_u)\}$$

为了方便描述，记 t_j 时刻成员撤销列表为

$$RL_{t_j}=\{t_j,(RID_0,RID_1,\sigma_0,L_0),\cdots,(RID_i,RID_j,\sigma_i,L_i),(RID_j,RID_{j+1},\sigma_j,L_j),\cdots,(RID_u,RID_{u+1},\sigma_u,L_u)\}$$

其中，$\sigma_i=\sigma_i',L_i=L_i',RID_{j+1}=RID_{i+1}$。

显然，合法成员 UID_τ 可在撤销列表中找到使得 $RID_i<UID_\tau<RID_{i+1}$ 成立的元组 $(RID_i,RID_{i+1},\ \sigma_i,\ L_i)$；相反，若群成员 UID_υ 被撤销，$(RID_\upsilon,RID_{\upsilon+1},\sigma_\upsilon,\ L_\upsilon)$ 为成员撤销列表中的元组，则对于任意 $i<\upsilon$ 有 $RID_i<UID_\upsilon$，$i>\upsilon$ 有 $RID_i>UID_\upsilon$，所以撤销成员不能在撤销列表中找到使 $RID_i<UID_\upsilon<RID_{i+1}$ 成立的元组。因此，合法成员 UID 可以通过在撤销列表中找到满足 $RID_i<UID<RID_{i+1}$ 成立的元组 $(RID_i,\ RID_{i+1},\ \sigma_i,L_i)$ 以证明其成员身份没有被撤销。

4.4 群签名

为了代表群对信息 M 进行签名，群成员 Alice 需要完成两方面的工作：1）通过零知识证明方法向验证者证明其匿名身份 UID_a 没有被撤销；2）计算对 M 的知识签名，证明她是群的注册成员。具体实现如下。

1) Alice 从最新的撤销列表 RL_{t_i} 中查找满足 $RID_j < UID_a < RID_{j+1}$ 的元组 $(RID_j, RID_{j+1}, \sigma_j, L_j)$。

2) Alice 选取随机数 $\lambda_1, \lambda_2 \neq 0$，$\varpi \in (0, 2^{s+T}]$，$k, k_1, k_2, k_3, k_4, k_5, k_6 \in [-2^s n+1, 2^s n-1]$，使得 $-k\lambda_1^2 - k_1\lambda_1 - k_2 \in [-2^s n+1, 2^s n-1]$，$\mu_1 = \lambda_1^2\zeta_1 + \varpi > 2^{l+s+l+T}$，$k\lambda_2^2 - k_4\lambda_2 - k_5 \in [-2^s n+1, 2^s n-1]$，$\mu_2 = \lambda_2^2\zeta_2 + \varpi > 2^{l+s+l+T}$。其中，$T = RID_{j+1} - RID_j$，$\zeta_1 = UID_a - RID_j$，$\zeta_2 = RID_{j+1} - UID_a$。

3) Alice 计算 $E = g^{UID_a} h^k \bmod n$，$E_0 = g^{\zeta_1} h^k \bmod n$，$E_1 = E_0^{\lambda_1} h^{k_1} \bmod n$，$E_2 = E_1^{\lambda_1} h^{k_2} \bmod n$，$E_3 = g^{\varpi} h^{k_3} \bmod n$，$\theta_1 = g^{\mu_1} / E_2 = g^{\varpi} h^{-k\lambda_1^2 - k_1\lambda_1 - k_2} \bmod n$，$F_0 = g^{\zeta_2} h^{-k} \bmod n$，$F_1 = F_0^{\lambda_2} h^{k_4} \bmod n$，$F_2 = F_1^{\lambda_2} h^{k_5} \bmod n$，$F_3 = g^{\varpi} h^{k_6} \bmod n$，$\theta_2 = g^{\mu_2} / F_2 = g^{\varpi} h^{k\lambda_2^2 - k_4\lambda_2 - k_5} \bmod n$。

4) Alice 任选一个随机数 $r \in Z_n^*$，计算

$$\tilde{z} = h^r g^y$$

$$d = y_R^{\ r}$$

$$V_1 := SKROOTREP[\alpha, \beta : \tilde{z} = h^{\alpha} g^{\beta^{e_1}}](M)$$

$$V_2 := SKROOTREP[\gamma, \delta : \tilde{z}^{f_1} g^{f_2} = h^{\gamma} g^{\delta^{e_2}}](M)$$

$$V_3 := SKREP[\varepsilon, \zeta : d = y_R^{\varepsilon} \wedge \tilde{z} = h^{\varepsilon} g^{\zeta}](M)$$

$$S = EID_a H(RID_j \| RID_{j+1}) + k \bmod n。$$

5) 发送签名 $\{\mu_1, \mu_2, E, E_1, E_2, E_3, F_1, F_2, F_3, P, Q, S, (RID_j, RID_{j+1}, \sigma_j, L_j), \tilde{z}, d, V_1, V_2, V_3\}$ 给验证者，并执行下列零知识证明式

$$PK\{\lambda_1, k_1, k_2 : E_1 = E_0^{\lambda_1} h^{k_1} \bmod n \wedge E_2 = E_1^{\lambda_1} h^{k_2} \bmod n\} \quad (1)$$

$$PK\{\varpi, k_3, -k\lambda_1^2 - k_1\lambda_1 - k_2 : E_3 = g^{\varpi} h^{k_3} \bmod n \wedge \theta_1 = g^{\varpi} h^{-k\lambda_1^2 - k_1\lambda_1 - k_2} \bmod n\} \quad (2)$$

$$PK\{\lambda_2, k_4, k_5 : F_1 = F_0^{\lambda_2} h^{k_4} \bmod n \wedge F_2 = F_1^{\lambda_2} h^{k_5} \bmod n\} \quad (3)$$

$$PK\{\varpi, k_6, k\lambda_2^{\ 2} - k_4\lambda_2 - k_5 : F_3 = g^{\varpi} h^{k_6} \bmod n \wedge \theta_1 = g^{\varpi} h^{k\lambda_2^{\ 2} - k_4\lambda_2 - k_5} \bmod n\} \quad (4)$$

$$PK\{\omega, k_3 : E_3 = g^{\varpi} h^{k_3} \wedge -2^{l+s+t+T} \leqslant \varpi \leqslant 2^{l+s+t+T}\} \quad (5)$$

4.5 签名验证

收到签名后，验证者只需在 Camenisch-Stadler 群签名方案验证的基础上补充验证零知识证明式(1)~式(5)，$\mu_1 > 2^{l+t+s+T}$，$\mu_2 > 2^{l+t+s+T}$，$h^S Q = y_R^{\ c'Q} P^{c'P} E \bmod n$，$h^{\sigma_j} = y_R^{e_1} L_j^{\ c'} \bmod n$ 成立即可。其中，$c' = H(RID_j \| RID_{j+1})$。

4.6 签名打开

本方案中的群签名打开的过程与原群签名方案中群签名打开过程完全一致。

5 方案分析

下面对群成员撤销方案的正确性、撤销成员伪造签名攻击的安全性以及撤销方案的计算性能进行分析，设撤销成员的匿名身份为 UID_v，签名者 Alice。

5.1 正确性分析

1) 验证者通过验证零知识证明式(1)~式(5)，$\mu_1 > 2^{l+t+s+T}$ 和 $\mu_2 > 2^{l+t+s+T}$，确信 $RID_j < UID_a < RID_{j+1}$，则签名者 Alice 没有被撤销。

Alice 向验证者出示式(1)，验证者确信 $E_0 = g^{\zeta_1} h^k \bmod n$，$E_1 = E_0^{\lambda_1} h^{k_1} \bmod n$，$E_2 = E_1^{\lambda_1} h^{k_2} \bmod n$；向验证者出示式(2)，验证者确信 $E_3 = g^{\varpi} h^{k_3} \bmod n$，$\theta_1 = g^{\mu_1} / E_2 = g^{\varpi} h^{-k\lambda_1^2 - k_1\lambda_1 - k_2} \bmod n$。所以可得 $g^{\mu_1} = \theta_1 E_2 = g^{\varpi} h^{-k_2 - k_1\lambda_1 - k\lambda_1^2} g^{\lambda_1^2\zeta_1}\ h^{k_2 + k_1\lambda_1 + k\lambda_1^2} = g^{\varpi + \lambda_1^2\zeta_1} \bmod n$。即 $\mu_1 = \lambda_1^2\zeta_1 + \varpi \bmod \varphi(n)$，由于 Alice 不知 n 的分解，不可能求出 $\varphi(n)$ 的值，由强 RSA 假设知 $\mu_1 = \lambda_1^2\zeta_1 + \varpi$。同理，通过零知识证明式(3)和式(4)，验证者知 $\mu_2 = \lambda_2^2\zeta_2 + \varpi$。Alice 向验证者出示式(5)，验证者确信 $-2^{l+t+s+T} \leqslant \varpi \leqslant 2^{l+t+s+T}$。验证者验证 $\mu_1 > 2^{l+t+s+T}$ 和 $\mu_2 > 2^{l+t+s+T}$，则验证者确信 $\zeta_1 > 0$，$\zeta_2 > 0$，所以 $RID_j < UID_a < RID_{j+1}$。

2) 验证者可通过式 $h^S Q = y_R^{\ c'Q} P^{c'P} E \bmod n$ 和式 $h^{\sigma_j} = y_R^{e_1} L_j^{\ c'} \bmod n$ 分别验证匿名身份 UID_a 和元组 $(RID_j, RID_{j+1}, \sigma_j, L_j)$ 的有效性。因为

$$h^S Q = h^{cEID_a + k} g^{UID_a} = h^{c(wQ+pP)+k} g^{UID_a} = y_R^{\ c'Q} P^{c'P} E \bmod n,$$

$$h^{\sigma_j} = g^{we_1 + l_i H(RID_i \| RID_{i+1})} = y_R^{e_1} L_j^{\ c'} \bmod n$$

只有群主管能够产生使上述等式成立的 EID_a 值和 σ_j 值，所以验证者确信匿名身份 UID_a 和元组

$(RID_j, RID_{j+1}, \sigma_j, L_j)$ 是由群主管生成的。

5.2 安全性分析

1) 撤销成员不能通过欺骗方式向验证者证明 $UID_v \in (RID_j, RID_{j+1})$ 。

如果撤销成员向验证者发送的 $E = g^{UID_v} h^k \bmod n$ 中的 $UID_v \notin (RID_j, RID_{j+1})$，则只有在下述 2 种情况下可以欺骗验证者：a) 寻找 UID_v'， k' 使得 $UID_v' \notin (RID_j, RID_{j+1})$ 且 $g^{UID_v} h^k \bmod n = g^{UID_v'} h^{k'} \bmod n$，然后用 UID_v' 代替 UID_v 执行零知识证明，其难度相当于求解离散对数难题；b) 求解一个 UID_v' 使得 $UID_v' \notin (RID_j, RID_{j+1})$ 且满足 $g^{UID_v} \bmod n = g^{UID_v'} \bmod n$，有强 RSA 假设知，在不知 n 分解的情况下，这也是不可能的。

2) 撤销成员不能通过伪造匿名身份或撤销元组的方式生成通过验证者验证的签名。因为有如下原因。

(a) 设撤销成员 UID_v 能够伪造匿名身份 UID_v' 使其满足某个元组，即 $UID_v' \in (RID_j, RID_{j+1})$，$j \in [0,u]$ 。撤销成员零知识证明 $UID_v' \in (RID_j, RID_{j+1})$ 时，已经发送 E 的值。由于伪造的匿名身份为 UID_v'，所以 $E = g^{UID_v'} h^k \bmod n$，则 $h^S Q \neq y_R^{c'Q} \cdot P^{c'P} E' \bmod n$，因此不能通过验证。如果撤销成员 UID_v 重新构造 S、P、Q，使其满足 $h^S Q = y_R^{c'Q} \cdot P^{c'P} E' \bmod n$ 成立，则难度相当于求解离散对数难题。

(b)设撤销成员 UID_v 能够伪造撤销列表中的元组 $(RID_j', RID_{j+1}', \sigma_j', L_j')$ 满足 $UID_v \in (RID_j', RID_{j+1}')$ 。由于撤销元组中 $\sigma_i = we_1 + l_i H(RID_i \| RID_{i+1}) \bmod n$，其中 w 为群主管的私钥，其他成员无法获得 w 的值。若伪造 σ_i' 满足 $h^{\sigma_j'} = y_R^{e_1} L_j^c \bmod n$，难度相当于求解离散对数问题。

5.3 匿名性及不可关联性分析

方案在签名的过程中没有出现群成员的真实身份。群成员在注册时，群主管通过伪随机方式，利用公式 $UID = H(z \| N \| \tilde{y})$ 为每个群成员产生了匿名身份，只有知道秘密数 N，才能揭示群成员的真实身份。由于只有群主管掌握秘密数 N，因此，只有群主管能够揭示群成员的真实身份，满足群签名匿名性要求。

对于撤销列表中的元组 $(RID_i, RID_{i+1}, \sigma_i, L_i)$，由于 RID_i 和 RID_{i+1} 之间合法成员个数较多，群成员签名时只向验证者证明其匿名身份在 RID_i 和 RID_{i+1} 之间，没有出示其匿名身份。因此，群签名验证者很难判断 2 个群签名是否由同一个群成员所签，满足群签名的不可关联性。

5.4 抗联合攻击性分析

抗联合攻击性是指即使群内的部分成员联合在一起也不能产生有效的、不被群管理员跟踪的群签名。在群签名验证中，零知识证明式 V_1，V_2，V_3 的正确性使得验证者确信：a) $\delta^{e_2} = f_1 \beta^{e_1} + f_2 \bmod n$，$\gamma = \alpha f_1 \bmod n$，这表明群成员的成员证书为 $v = \delta$，且其成员秘密钥为 $x = \beta$；b) $\tilde{z}$ 和 d 的计算使用了同一个随机数 $r = \varepsilon$，即 $(\tilde{z}, d)$ 是 Alice 利用群主管公钥 (h, y_R) 对成员公开钥 z 的加密。如果群中部分成员能够产生有效的、不被群管理员跟踪的群签名，则表明群内部分成员能够伪造群主管的私钥，其难度相当于求解离散对数难题。因此，方案满足抗联合攻击性。

5.5 性能分析

性能分析主要包括计算性能分析和存储开销性能分析。本节将本方案和已有方案的性能进行比较，鉴于本文是对 Camenisch-Stadler 群签名方案增加了成员撤销功能，因此只与 Camenisch-Stadler 群签名成员撤销方案[5, 8]进行比较。其对比结果如表 1~表 3 所示。其中，“H”表示散列运算，“E”表示模幂运算，“I”表示求逆运算，“X”表示乘法运算，m_1 为群中现有成员数，m_2 为已撤销成员数。

由表 1 和表 2 中数据看出，本方案中群成员撤销计算量与群成员的个数和已撤销成员的个数无关；当撤销成员较多时，本文群成员撤销方案的计算性能优于 E.Bresson 的方案；当群成员较多或群

表 1 阶段计算量比较

方案名称	成员注册	成员撤销	签名	验证
E.Bresson[5]	0	0	$(3m_2+2)E + 2m_2 I + m_2 X$	$2m_2 E + m_2 I + 2m_2 X$
李新社[8]	$(m_1+3)E + 3I + (2m_1+2)X$	$(m_1+1)E + I + (2m_1+2)X$	$3E + 3X$	$E + 2X$
本方案	$2H + 2E + 3X$	$E + 2X$	$5H + 42E + 15M$	$6H + 35E + 6M$

表 2　　身份计算量比较

方案名称	群主管	签名成员	其他成员	验证者
E.Bresson[5]	$O(1)$	$(3m_2+2)E+2m_2I+m_2X$	0	$2m_2E+m_2I+2m_2X$
李新社[8]	$2E+2I+(2m_1+4)X$	$2E+4X$	$(2E+4X)m_1$	$E+2X$
本方案	$2H+3E+3X$	$5H+42E+15M$	0	$6H+35E+6M$

表 3　　存储开销比较

方案名称	群公钥长度	群公开特性钥长度	撤销列表长度	签名长度
E.Bresson[5]	$O(1)$	—	$O(m_2)$	$O(m_2)$
李新社[8]	$O(1)$	$O(m_1)$	—	$O(1)$
本方案	$O(1)$	—	$O(m_2)$	$O(1)$

成员更新较频繁时，本文群成员撤销方案的计算性能优于李新社的方案。从表 3 中数据可以看出，本文群成员撤销方案存储开销性能与李新社[8]的方案相似，略优于 E.Bresson 的方案。

6　结束语

本文针对 Camenisch-Stadler 群签名方案提出了群成员撤销方案，其实现思想：将已撤销成员按照其匿名身份大小进行排序，生成撤销列表。对于每一个合法的群成员 UID_a 都能从撤销列表中找到一个元组 $(RID_j, RID_{j+1}, \sigma_j, L_j)$ 使 $RID_j < UID_a < RID_{j+1}$ 成立，并用零知识证明协议向验证者证明，而已撤销的成员则不能。同时，在生成群成员匿名身份、撤销列表元组以及群签名验证的过程中增加了防止撤销成员伪造攻击的措施，实现了群成员的有效撤销。本文提出的群成员撤销方案也可以运用到其他群签名方案中。在该方案中，使用零知识证明协议证明 $RID_j < UID_a < RID_{j+1}$，增加了群签名的长度和计算量。本文在今后的设计中，将进一步研究优化零知识证明协议或探究其他方法证明 $RID_j < UID_a < RID_{j+1}$ 成立，以减少群成员签名的长度和计算量。

参考文献：

[1] CHAUM D, VAN H E. Group signatures[A]. Cryptology-EUROCRYPT'91: Workshop on the Theory and Application of Cryptographic Techniques[C]. Brighton, UK, 1991. 257-265.

[2] CHEN L, PEDERSEN T. On the efficiency of group signatures providing information-theoretic anonymity[A]. Cryptology-EUROCRYPT'95: International Conference on the Theory and Application of Cryptographic Techniques[C]. Saint-Malo, France, 1995. 39-49.

[3] CAMENISCH J. Efficient and generalized group signatures[A]. Cryptology-EUROCRYPT'97: International Conference on the Theory and Application of Cryptographic Techniques[C]. Konstanz, Germany, 1997. 465-479.

[4] CAMENISCH J, STADLER M. Efficient group signatures schemes for large groups[A]. Cryptology- CRYPTO'97: 17th Annual International Cryptology Conference[C]. California USA, 1997. 410-424.

[5] BRESSON E, STERN J. Efficient revocation in group signatures[A]. 4th International Workshop on Practice and Theory in Public Key Cryptography[C]. Cheju Island, Korea, 2001.190-206.

[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] 黄振杰, 林宣治. 一个群签名成员删除方案的密码学分析[J]. 软件学报, 2005, 16(3): 472-476.
HUANG Z J, LIN X Z. Cryptanalysis of a member deletion scheme for group signature[J]. Journal of Software, 2005, 16(3): 472-476.

[8] 李新社, 胡予濮. 一个群签名成员删除方案的分析与改进[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 Xidian University, 2008, 35(3): 478-482.

[9] 魏凌波, 武传坤, 周苏静. 具有向后无关性的本地验证撤销群签名方案[J]. 计算机研究与发展, 2008, 45(8): 1315- 1321.
WEI L B, WU C K, ZHOU S J. A new verifier-local revocation group signature with backward unlinkability[J]. Journal of Computer Research and Development, 2008, 45(8): 1315-1321.

[10] JIN H M, WONG S D, XU Y L. Efficient group signature with forward secure revocation[A]. Proceedings of International Conference on Security Technology[C]. Jeju Island, Korea, 2009. 124-131.

[11] FAN C I, HSU R H, MANULIS M. Group signature with constant revocation costs for signers and verifiers[A]. The 10th International Conference on Cryptology and Network Security (CANS 2011)[C]. Sanya, China, 2011. 214-233.

[12] LIBERT B, PETERS T, YUNG M. Scalable group signatures with revocation[A]. Eurocrypt'12[C]. Cambridge, UK, 2012. 609-627

[13] NAKANISHI T, FUJII H, HIRA Y, *et al*. Revocable group signature schemes with constant costs for signing and verifying[A]. Public Key Cryptography-PKC 2009: 12th International Conference on Practice and Theory in Public Key Cryptography[C]. Irvine, USA, 2009. 463-480.

[14] 伍前红, 张键红, 王育民. 简单证明一个承诺值在特定区间内[J]. 电子学报, 2004, 32(7): 1071-1073.
WU Q H, ZHANG J H, WANG Y M. Simple proof that a committed number is in a specific interval[J]. Acta Electronica Sinica, 2004, 32(7): 1071-1073.

[15] SUN Y, XU C, YU Y, *et al*. Strongly unforgeable proxy signature scheme secure in the stand and model[J]. The Journal of System and Software, 2011, 84 (9): 1471-1479.

[16] FUJISAKI E, OKAMOTO T. Statistical zero knowledge protocols to prove modular polynomial relations[A]. Cryptology-CRYPTO'97: 17th Annual International Cryptology Conference[C]. California USA, 1997. 16-30.

[17] BOUDOT F. Efficient proofs that a committed number lies in an interval[A]. Proceedings of EUROCRYPT'2000[C]. Berlin: Spring-Verlag, 2000.431-444.

[18] CHAUM D, EVERTSE J H, GRAAF J. An improved protocol for demonstrating possession of discrete logarithm and some generalizations[A]. Proceedings of EUROCRYPT'87[C]. Berlin: Spring-Verlag, 1988. 127-141.

作者简介：

张德栋（1982-），男，山东临沂人，博士，主要研究方向为网络安全、数字签名、无线匿名通信技术。

马兆丰（1974-），男，甘肃镇原人，博士，北京邮电大学教师，主要研究方向为网络安全、移动通信安全、数字内容安全。

杨义先（1961-），男，四川盐亭人，北京邮电大学教授、博士生导师，主要研究方向为密码学、计算机网络与信息安全。

钮心忻（1963-），女，浙江湖州人，北京邮电大学教授、博士生导师，主要研究方向为数字内容安全、计算机网络安全。