基于中国剩余定理的群签名改进方案

黄丛林[1] 仲 红[1] 汪益民[1,2]
(安徽大学计算机科学与技术学院 合肥 230601)[1] (安徽农业大学现代教育信息中心 合肥 230636)[2]

摘 要 自陈泽文首次提出基于中国剩余定理的群签名后,已出现不少对其改进的方案,但仍未有方案在不使用第三方辅助签名或验证的情况下实现非关联性。针对这一问题,提出了一个基于中国剩余定理的群签名改进方案,通过结合子集覆盖框架中完备子树的方法来实现上述非关联性,以满足群成员安全、快速的加入和撤销,而无需改变其他成员私钥。该方案还实现了防权威陷害攻击。最后对其安全性和效率进行分析,并与现有方案进行对比,结果表明,所提方案具有一定的优势。

关键词 群签名,中国剩余定理,非关联性,完备子树方法,权威陷害攻击
中图法分类号 TP393 **文献标识码** A **DOI** 10.11896/j.issn.1002-137X.2016.3.033

Improved Group Signature Scheme Based on Chinese Remainder Theorem

HUANG Cong-lin[1] ZHONG Hong[1] WANG Yi-min[1,2]
(School of Computer Science and Technology, Anhui University, Hefei 230601, China)[1]
(Modern Education and Information Center, Anhui Agricultural University, Hefei 230636, China)[2]

Abstract The group signature scheme based on Chinese remainder theorem was first proposed by Chen Ze-wen. Since then, several improved schemes have been proposed, but no scheme achieves the non-relation without using the third party to sign or verify. In order to solve this problem, we proposed an improved group signature scheme based on Chinese remainder theorem, which combines with the notion of complete subtree method in the subset cover framework. In addition, our scheme can provide non-relation, joining or revoking safely and quickly for each member without changing other members' private key, and also resist against authority trap attacks. Finally, we analyzed the security and efficiency of our scheme, and comparison results suggest that our scheme has some advantages over the existing schemes.

Keywords Group signature, Chinese remainder theorem, Non-relation, Complete subtree method, Authority trap attack

1 引言

群签名是 Chaum 和 Heyst[1] 在 1991 年首次提出的数字签名方案。群签名允许群中合法成员匿名地代表群进行签名,验证者只能验证签名者属于群,却不能获知签名者的身份,出现争议时,还可以通过群管理员揭露签名者身份信息。因此群签名有条件匿名性,此外群签名还有防伪造性、防陷害攻击和联合攻击能力等。由于群签名这些特征,使得群签名在政治、军事、经济等方面都有广泛的应用前景,如应用于电子选举、电子现金系统等,因此群签名受到重点关注。

1997 年 Camenish 等人[2] 提出第一个相对高效且适用于大群体的群签名方案,但此方案不能防联合攻击。随后在 2000 年,Ateniese 等人[3] 提出了抗自适应攻击者发动的联合攻击的 ACJT 群签名方案,效率比文献[2]方案优越,但 ACJT 方案并未实现成员撤销问题。而群签名实际运用中,高效安全地撤销和加入群成员是很重要的问题[3-5]。2004 年陈泽文[6] 提出了基于中国剩余定理的群签名方案,该方案可以实现加入和撤销成员时无需改变其他成员的签名密钥,且只需要乘法运算,开销代价较小,群公钥大小也固定。但陈方案存在严重安全缺陷,不能抵御联合攻击。后来也有不少方案对陈方案进行改进。2007 年李俊等人[7] 对陈方案进行安全分析和改进,解决了联合攻击。同年王凤和[8] 以及 2013 年张凯等人[9] 也改进了陈方案,实现了防联合攻击。但他们都未实现签名的非关联性,即验证者不能分辨两个签名是否来自同一个签名者。最近,2015 年党佳莉等人[10] 也提出一个防联合攻击和防重放攻击的中国剩余定理群签名方案,依旧未实现非关联性。虽然崔国华[11] 在 2009 年提出了一个解决非关联性的方案,但此方案需要群成员和群中心合作签名实现,签名时需要签名者与群交互,不仅增加了通讯代价,还大量增加了群计算代价。

针对以上问题,本文将中国剩余定理与 Naor[12] 提出的完备子树方法相结合,实现了无需第三方辅助签名或验证的非关联性,且降低了群计算同余式代价。

本文第 2 节介绍本方案的相关背景知识,包括中国剩余

到稿日期:2015-03-25 返修日期:2015-06-14 本文受国家自然科学基金项目(61173188),安徽省科技攻关项目(1401b042015),安徽省高校自然科学研究重点项目(KJ2013A017)资助。

黄丛林(1990—),男,硕士生,主要研究方向为车载自组织网络隐私保护技术,E-mail:hcllin313@163.com;仲 红(1965—),女,博士,教授,主要研究方向为网络与信息安全;汪益民(1980—),男,博士生,主要研究方向为物联网安全与隐私保护技术。

定理和完备子树方法以及陈方案；第3节详细介绍本方案；第4节对本方案的安全性和效率进行分析，并与已有方案进行对比，体现本方案的优越性；最后总结全文。

2 预备知识

2.1 中国剩余定理

假设 k 个两两互素的正整数，$k\geqslant 2$，其中 $P=p_1p_2\cdots p_k$，$P_i=P/p_i$，$i=1,2,\cdots,k$，$p_i>y_i$。满足如下同余方程组：

$$\begin{cases} C\equiv y_1 (\bmod\ p_1) \\ C\equiv y_2 (\bmod\ p_2) \\ \cdots \\ C\equiv y_k (\bmod\ p_k) \end{cases}$$

其正整数解为：$C\equiv y_1P_1P_1'+y_2P_2P_2'+\cdots+y_kP_kP_k' (\bmod P)$。其中 $P_i'P_i\equiv 1(\bmod p_i)$，$i=1,2,\cdots,k$。

2.2 完备子树方法

子集覆盖框架是由 Naor 等人提出，用于广播加密密钥分发。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 $x_{i,j}$，把用户分配到一个叶节点 $x_{l,j}$，用户存储其对应叶节点到根节点路径上所有节点值，$j\in N$。N 是叶节点总数，R 是被撤销叶节点。完备子树方法就是选取包含所有未被撤销合法叶节点 N/R 的 m 个子树集合 $S_1,S_2,\cdots,S_m$，$m\leqslant R\log(N/R)$。

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 $x_{3,3}$，$x_{3,5}$，$x_{3,6}$ 是要撤销节点。利用完备子树方法选取包含未撤销叶节点的子集为 $S_i=\{x_{2,1},x_{3,4},x_{2,4}\}$，其中 $i=0,\cdots,3$。

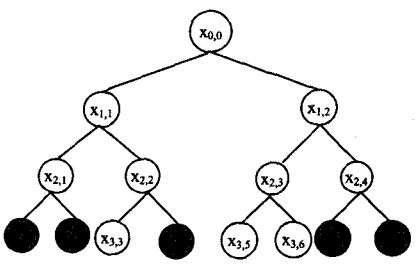

图1 二叉树结构示例图

2.3 陈的方案

陈泽文首次提出基于中国剩余定理的群签名方案，包括群中心、群管理员、群成员3种参与方，其安全性是建立在RSA大素数分解难题上。

2.3.1 系统建立

①群中心秘密选择两个大素数 p,q 和一个 Hash 函数，并计算 $n=pq$。

②选择 $e\in Z_n$，通过 $ed\equiv 1(\bmod \phi(n))$ 求 d，其中 e,d 分别为群中心公钥和私钥，$\phi(\cdot)$ 为欧拉函数。

③对身份为 ID_i 的用户 U_i，群中心随机选择 $x_i,y_i\in Z_n$，满足 $x_i\cdot y_i\equiv 1(\bmod \phi(n))$，再随机选择素数 $p_i>y_i$，当 $i\neq j$ 时 $p_i\neq p_j$。将 (x_i,p_i,p_i^d) 发送给 U_i，U_i 验证等式 $p_i=(p_i^d)^e (\bmod n)$ 是否成立，成立就将 (x_i,p_i,p_i^d) 作为签名密钥保存。

④群中心将 (ID_i,y_i) 发送给群管理员保存。群中心利用中国剩余定理计算群中 k 个成员的同余方程组 $C\equiv y_i(\bmod p_i)$ 的唯一解，其中 $i=0,1,\cdots,k$，$C\equiv y_1P_1P_1'+y_2P_2P_2'+\cdots+y_kP_kP_k' (\bmod P)$，如2.1节所介绍，公开群公钥 (n,e,C)。

2.3.2 成员加入

①U_j 向群中心申请加入群。群中心先随机选择 $x_{k+1}\in Z_n$，由 $x_{k+1}\cdot y_{k+1}\equiv 1(\bmod \phi(n))$ 求得 y_{k+1}，然后选择素数 $p_{k+1}>y_{k+1}$，满足 $gcd(p_{k+1},p_i)=1$，其中 $i=1,\cdots,k$。

②重新计算 $C\equiv y_1P_1P_1'+y_2P_2P_2'+\cdots+y_kP_kP_k' (\bmod P)$，其中 $P=Pp_{k+1}$，$P_i=P_ip_{k+1}$，$i\in k$，$p_{k+1}'\ p_{k+1}\equiv 1(\bmod p_{k+1})$，发布新的 C。

③群中心将 $(x_{k+1},p_{k+1},p_{k+1}^d)$ 发送给 U_j，U_j 验证接受后成为群新成员。群中心将 (ID_{k+1},y_{k+1}) 发送给群管理员保存。

2.3.3 成员撤销

与加入类似，设现有 k 个成员，撤销群中的成员 U_j，只需将 y_j 改为一个随机素数 y_j'，计算新的 C 发布。其中 $C\equiv y_1P_1P_1'+\cdots+y_jP_jP_j'+\cdots y_kP_kP_k' (\bmod P)$。

2.3.4 签名

U_i 利用密钥 (x_i,p_i,p_i^d) 对消息 m 进行签名，计算 $s_i=m^{x_i} (\bmod n)$，则签名 $\sigma_i=(m,s_i,p_i^d)$。

2.3.5 验证

U_j 收到 U_i 的签名 σ_i，首先利用群公钥计算等式 $p_i=(p_i^d)^e (\bmod n)$ 和 $y_i\equiv C(\bmod p_i)$，接着验证式子 $h(m)=s_i^{y_i} (\bmod n)$ 是否成立，若成立则接受签名，否则丢弃。

2.3.6 揭露

群管理员在揭露签名 σ_i 时，通过签名 (m,s_i,p_i^d) 计算 $p_i=(p_i^d)^e (\bmod n)$ 和 $y_i=C(\bmod p_i)$，通过查询 y_i 对应的 ID_i 即可给出签名者的身份。

2.3.7 安全性分析

①不满足非关联性，验证者能根据计算签名的 y_i 值是否相等来判断两个签名是否来自同一个签名者。

②不满足防联合攻击，所有成员私钥生成共模 n，成员联合起来由概率计算出 $\phi(n)$[13]，然后利用 $x_iy_i\equiv 1(\bmod \phi(n))$ 得到签名者私钥 x_i 来伪造签名。

③满足防伪造攻击，由②可知。

④不满足防权威陷害攻击，群中心知道所有成员私钥，能够伪造任意成员的签名。

3 本文方案

针对陈方案的以上安全问题，本文都进行了弥补。将完备子树方法和中国剩余定理相结合，实现了无需第三方辅助签名的非关联性。并通过修改密钥分发形式，实现了防权威陷害攻击。本文同样包含群中心、群管理员、群成员3个实体。群中心初始化系统参数并颁发群成员证书，群管理员也参与群成员证书颁发过程，同时执行揭露群成员身份职责。方案具体描述如下。

3.1 系统初始化

3.1.1 群中心初始化

①群中心身份为 ID_C，选择大素数 q_1,q_2 和一个 Hash 函数 $h(\cdot)$，$g\in Z_n$。计算 $n_C=q_1q_2$。

②选择私钥 x_C，计算 $y_C=g^{x_C} (\bmod n_C)$。随机选择 $e_C\in Z_n$，计算 d_C 满足 $e_Cd_C\equiv 1(\bmod \phi(n_C))$。其中 y_C,e_C 为群中心公钥，x_C,d_C 为群中心私钥。公开 $(n_C,y_C,e_C,g,h(\cdot),ID_C)$。

③群中心构建一个层数为 $l=\log N-1$ 的完全二叉树 T，N 为树中叶节点数目。树中节点被标示为 $x_{i,j}$，$i=0,\cdots,$

$l,j=0,\cdots,2^i$ 分别表示每层和对应层的节点。对每个节点 $x_{i,j}$，选择一个对应整数 y_k，其中 $k=0,\cdots,2^l-1$。使 x_k 满足 $x_k y_k \equiv 1 (\mathrm{mod}\ \phi(n_C))$，计算 g^{x_C}，并选择素数 $p_k > y_k$，当 $k \neq k'$ 时 $p_k \neq p_{k'}$，计算 $(p_k)^{d_C}$。最终群中心存储每个树节点记录表 $(x_{i,j}, g^{x_k}, y_k, p_k, (p_k)^{d_C})$。此过程是群中心后台离线运行，并不占用签名时间。

④群中心为每个向其注册成功的用户 U_j 分配树中一个叶节点 $x_{l,j}$，并将从树根节点到用户对应叶节点路径上所有节点列表的 $\{g^{x_k}, y_k, p_k, (p_k)^{d_C}\}_{k\in l}$ 秘密发送给 U_j。群中心存储每个用户信息记录表 $(ID_j, x_{l,j}, \{g^{x_k}, y_k, p_k, (p_k)^{d_C}\}_{k\in l})$。

⑤假设系统中有 n 个成员($n \geqslant 2$)。群中心利用子集覆盖中完备子树方法，选取包含所有合法用户对应叶节点的子树集合 $S_m = \{x_{i,j}\}_{i\in l, j\in 2^i}$（用每个子树的根节点表示对应子集，$m$ 为子集数目）。如图 1 所示，$S_m = \{x_{2,1}, x_{3,4}, x_{2,4}\}$，$m=3$。计算每个子集根节点记录对应的 $\{y_i, p_i\}$ 同余式方程组 $C \equiv y_i (\mathrm{mod}\ p_i)$，$i=0,\cdots,m$。利用中国剩余定理求解为 $C \equiv y_0 P_0 P_0' + y_1 P_1 P_1' + \cdots + y_m P_m P_m' (\mathrm{mod}\ P)$，$P_i' P_i \equiv 1 (\mathrm{mod}\ p_i)$，$i=1,2,3\cdots,k$ 并发布 C。

3.1.2 *群管理员初始化*

①群管理员身份为 ID_G，选取大素数 q_3, q_4，计算 $n_G = q_3 q_4$。

②选取 $e_G \in Z_n$，计算 d_G 满足等式 $e_G d_G \equiv 1 (\mathrm{mod}\ \phi(n))$。公开 (n_G, e_G, ID_G)。

3.2 成员加入

①用户 U_i 要加入群，首先随机选择 $k \in Z_n$，计算 $ID_i = g^k$。产生一个 ID_i 对 g 的知识签名[14] $\delta = SPK[\gamma: ID_i = g^\gamma](")$，发送 (ID_i, δ) 给群中心。

②群中心验证其身份和其知识签名 δ 是否正确，正确就分配给 U_i 一个 T 中叶节点 $x_{l,i}$，群中心选择从叶节点 $x_{l,i}$ 到 T 根节点路径上所有节点记录，存储用户记录表 $(ID_i, x_{l,i}, \{g^{x_k}, y_k, p_k, (p_k)^{d_C}\}_{k\in l})$。

③群中心随机选择 $\alpha \in Z_{n_G}$，计算 $r_C = g^\alpha (\mathrm{mod}\ n_G)$，$s_C = \alpha + r_C x_C h(ID_i) (\mathrm{mod}\ n_G)$。群中心将 $(r_C, (r_C)^{d_C}, s_C, \{g^{x_k}, y_k, p_k, (p_k)^{d_C}\}_{k\in l})$ 发送给 U_i，然后验证 $g^{s_C} = r_C g_C^{r_C h(ID_i)} (\mathrm{mod}\ n_G)$ 和 $r_C = ((r_C)^{d_C})^{e_C} (\mathrm{mod}\ n_C)$ 是否成立，成立则接受。群中心同时将 (ID_i, r_C, g^{s_C}) 发送给群管理员，群管理员验证 $g^{s_C} = r_C g_C^{r_C h(ID_i)} (\mathrm{mod}\ n_G)$ 是否成立，成立则接受。

④群管理员接受 (ID_i, r_C, g^{s_C}) 后，计算 $w_G = (ID_G r_C y_C^{r_C h(ID_i)} ID_i)^{-d_G} (\mathrm{mod}\ n_G)$，并发送 w_G 给用户 U_i，U_i 验证 $w_G^{e_G} = ID_G r_C y_C^{r_C h(ID_i)} ID_i (\mathrm{mod}\ n_G)$ 是否成立，成立则接受。此时 U_i 已加入群，其群成员证书为 $(r_C, (r_C)^{d_C}, s_C, w_G, \{g^{x_k}, y_k, p_k\}_{k\in l})$。

⑤群中心利用完备子树方法选取包含 U_i 在内的所有合法成员子集 $S_m = \{x_{i,j}\}_{i\in l, j\in 2^i}$，重新计算 $C \equiv y_0 P_0 P_0' + y_1 P_1 P_1' + \cdots + y_m P_m P_m' (\mathrm{mod}\ P)$，并公布新的 C。

3.3 签名

①U_i 要对消息 m 进行签名，首先根据群中心最新发布的 C 和自己的成员证书 $\{g^{x_k}, y_k, p_k\}_{k\in l}$ 计算 $y_k' = C (\mathrm{mod}\ p_k)$。其中必有一个 $y_k' = y_k$，记为 $(g^{x_t}, y_t, p_t, (p_t)^{d_C})$。因为群中心根据完备子树方法选取包含 U_i 对应叶节点的子集时，必会选取 U_i 存储的从 $x_{l,j}$ 到根节点路径上的一个节点（此步骤可在签名前离线处理，只要收到新的 C 即可）。

②U_i 随机选择 $\beta_1, \beta_2 \in Z_n$，计算等式：$z_1 = g^{h(m)} (\mathrm{mod}\ n_C)$，$z_2 = \beta_2^{e_G} g^{\beta_1} (\mathrm{mod}\ n_G)$，$u = h(z_1, z_2, m)$，$r_1 = \beta_1 + u(k + s_C) (\mathrm{mod}\ n_G)$，$r_2 = \beta_2 w_G^u (\mathrm{mod}\ n_G)$，$r_3 = (g^{r_t})^{h(m)} (\mathrm{mod}\ n_C)$。$\sigma_i = (m, u, r_1, r_2, r_3, p_t, (p_t)^{d_C})$ 即为最后的签名。

3.4 验证

U_j 收到 U_i 的签名 σ_i，首先验证等式 $p_t = ((p_t)^{d_C})^{e_C} (\mathrm{mod}\ n_C)$ 是否成立，成立则依次计算如下等式：$y_t = C (\mathrm{mod}\ p_t)$，$z_1' = r_3^{y_t} (\mathrm{mod}\ n_C)$，$z_2' = ID_C^u g^{r_1} r_2^{e_G} (\mathrm{mod}\ n_G)$，$u' = h(z_1', z_2', m)$。验证 $u = u'$ 是否成立，成立则接受签名，否则丢弃。

3.5 成员撤销

群中心要撤销成员 U_j，利用完备子树方法，重新选择不包含 U_j 对应叶节点的子集，重新计算 C，并发布。

3.6 揭露

群管理员要对签名 σ_i 进行揭露，首先计算等式 $\theta = 1/u (\mathrm{mod}\ \phi(n_G))$，$\lambda = ID_C^u g^{r_1} (\mathrm{mod}\ n_G)$，然后利用存储的成员信息列表 (ID_i, w_G, g^{s_C})，代入等式验证 $ID_i = (g^{r_1}/\lambda g^{us_C})^\theta / w_G^{e_G} (\mathrm{mod}\ n_G)$ 是否成立，等式成立的 ID_i 即为所要揭露的签名者身份。

4 安全性和效率分析

本节对本方案的安全性和效率进行分析，安全性主要包括正确性、抗共模攻击、不可伪造性、防权威陷害攻击、非关联性几个方面内容，并与现有方案进行对比。同时，对效率进行分析和对比。

4.1 安全性分析

4.1.1 *正确性*

若签名 $\sigma_i = (m, u, r_1, r_2, r_3, p_t, (p_t)^{d_C})$ 由合法群成员产生，一定能通过验证。证明如下：

$$
\begin{aligned}
①\ z_1' &= r_3^{y_t} (\mathrm{mod}\ n_C) \\
&= ((g^{r_t})^{h(m)})^{y_t} (\mathrm{mod}\ n_C) \\
&= g^{h(m)} (\mathrm{mod}\ n_C) \\
&= z_1 \\
②\ z_2' &= ID_C^u g^{r_1} r_2^{e_G} (\mathrm{mod}\ n_G) \\
&= ID_C^u g^{\beta_1 + u(k+s_C)} (\beta_2 w_G^u)^{e_G} (\mathrm{mod}\ n_G) \\
&= ID_C^u g^{\beta_1} (r_C y_C^{r_C h(ID_i)})^u ID_i^u ((ID_G r_C y_C^{r_C h(ID_i)} ID_i)^{-d_G})^{ue_G} \\
&\quad \beta_2^{e_G} (\mathrm{mod}\ n_G) \\
&= \beta_2^{e_G} g^{\beta_1} (\mathrm{mod}\ n_G) \\
&= z_2
\end{aligned}
$$

因此 $u = u' = h(z_1', z_2', m)$ 一定成立，能通过验证。

4.1.2 *防联合攻击*

若群成员联合起来，想通过 $x_k y_k \equiv 1 (\mathrm{mod}\ \phi(n_C))$ 进行共模攻击分解 n_C，就要知道 x_k 和 y_k。由于群成员只知道 g^{x_k} 和 y_k，求解 x_k 等价于求解离散对数问题。因此群成员无法进行联合攻击。

4.1.3 *防伪造攻击*

若被撤销成员 U_j 想要伪造一个可通过验证的签名，可以从以下 3 方面入手：

①联合其他成员利用共模攻击分解 n_C，从而攻破整个系统。由 4.1.2 节可知，本方案满足防联合攻击，U_j 无法利用

共模攻击分解 n_C，从而也不能伪造签名。

②从收到的合法签名中获取合法成员签名私钥。假设 U_j 收到合法群成员 U_i 的签名 $\sigma_i=(m,u,r_1,r_2,r_3,p_t,(p_t)^{d_C})$，想利用其 $p_t,(p_t)^{d_C}$ 通过签名验证 $z_1=z_1'$。由于 U_j 被撤销，群中心利用完备子树方法选择子集时并不包含 U_j 存储的 g^{x_k}，因此 U_j 无法获取 $r_3=(g^{x_t})^{h(m)}(\bmod n_C)$，签名不能使 $z_1=z_1'$ 成立。

③修改自己的签名和验证信息，让用自己私钥生成的签名通过验证。由于 U_j 被撤销，C 被更新，其存储的签名密钥 g^{x_k} 和 y_k 已经不能通过验证。因为 $y_j\neq y_j'=C(\bmod p_j)$，所以 U_j 伪造 p_t' 满足 $y_t=C(\bmod p_t')$，然后利用 $(g^{x_t},y_t,p_t',(p_t')^{d_C})$ 进行签名并通过验证。但这是不可能的，因为并不知道群私钥 d_C，无法通过 $p_t'=((p_t')^{d_C})^{e_C}(\bmod n_C)$ 验证。

4.1.4 防权威陷害攻击

文献[6-9]中群中心知道所有群成员的私钥，因此群中心能够伪造任意群成员签名，实行陷害攻击。本文方案中群中心只拥有成员证书的一部分：$(r_C,(r_C)^{d_C},s_C,\{g^{x_k},y_k,p_k\}_{k\in I})$，但不知道 w_C，因此无法伪造 r_2，无法通过签名验证。同样，对于群管理员也不知道群中心私钥 d_C 和 s_C，也无法伪造 r_1,r_3，也无法通过签名验证。

4.1.5 非关联性

①本方案中 y_k 并不是唯一对应一个成员身份，即使群成员对签名进行验证求得 $y_k=C(\bmod p_k)$，也无法确定 y_k 对应多少成员身份，更无法确定对应哪个成员。

②群成员在每次签名时选择随机数 β_1,β_2 生成 r_1,r_2,z_2,u，且 z_1,r_3,p_t 与成员身份无直接关联，所以验证者也无法通过签名判断两个不同群签名是否来自一个签名者。

4.1.6 安全性分析

通过上述分析，下面给出本方案与现有基于中国剩余定理的群签名方案安全性的对比，结果如表1所列，其中"√"代表满足此项性能，"×"表示不满足此项性能。

表1 各协议安全性能对比

安全性能	文献[7]	文献[9]	文献[10]	文献[11]	本文方案
匿名性	√	√	√	√	√
防联合攻击	×	√	√	√	√
抗伪造攻击	×	×	√	√	√
防权威陷害攻击	×	×	×	√	√
非关联性	×	×	×	√	√
无需第三方辅助签名	√	√	√	×	√

从表1可知，除了本方案满足无需第三方辅助签名实现了非关联性外，其他4个方案都未实现。同时，只有本方案和方案[11]实现了防权威陷害攻击，但方案[11]需要第三方辅助签名。

4.2 效率分析

本文在效率对比中，既选择了同本方案一样基于RSA的李新社方案[15]和张德栋方案[16]，也选择了基于双线相对的Libert B方案[17]和Nakanishi T方案[18]。同时给出了本方案和李方案、张方案运算开销的详细对比。这些方案都满足非关联性。表1中"T"表示撤销成员次数，"N"和"R"分别表示成员总数和撤销成员数；表2中"E"表示模幂运算，"H"表示Hash运算。

①初始化中群中心虽利用了树型存储结构，需要产生和存储大量树节点信息，但此过程是后台离线产生，并不占用签名时间。群成员增加了很少的 $O(\log N)$ 固定存储量。

②群中心利用子集覆盖的完备子树方法选取包含合法节点的子集 $m\leqslant R\log N/R$，利用中国剩余定理求得子集的同余方乘组解，并发布。同余式复杂度为 $O(R\log N/R)$，相比文献[6-10]，此过程的计算复杂度 $O(N)$ 更低。

③如表2所列，本方案在群公钥长度、签名长度、签名开销和验证开销复杂度上都是最低的 $O(1)$；在增加了少量 $O(\log N)$ 的成员证书长度前提下，除了方案[18]的撤销开销复杂度为 $O(1)$，本方案的撤销列表长度和撤销开销也是对比方案中较低的 $O(R\log(N/R))$。

表2 各协议效率对比

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
LV[15]	O(T)	O(1)	O(1)	O(R)	O(1)	O(R)	O(R)
NF[16]	O(T)	O(1)	O(1)	O(R)	O(1)	O(R)	O(R)
李新社[17]	O(1)	O(1)	O(1)	—	O(1)	O(1)	O(N)
张德栋[18]	O(1)	O(1)	O(1)	O(R)	O(1)	O(1)	O(1)
本文方案	O(1)	O(1)	O(logN)	O(Rlog(N/R))	O(1)	O(1)	O(Rlog(N/R))

④如表3所列，在基于RSA离散对数困难问题的3个群签名方案运算开销对比中，本方案在签名开销和验证开销上比李方案稍高，比张方案开销低很多；但本方案撤销开销比李方案的成员数线性相关低很多，张方案在撤销开销中是最低的，但其他开销较大。总体而言，本方案具有更平衡的整体开销。

表3 基于RSA方案的运算开销对比

方案名称	签名开销	验证开销	撤销开销
李新社[17]	3E	E	(N+1)E
张德栋[18]	5H+42E	6H+35E	E
本文方案	H+5E	H+5E	Rlog(N/R)

结束语 本文方案保留了陈方案中利用中国剩余定理快速加入和撤销群成员的优点，同时实现了匿名性、防共模攻击、防伪造性和防权威陷害攻击，并将中国剩余定理和完备子树方法相结合，实现无需利用第三方辅助签名或验证实现非关联性。通过增加一轮群管理员参与成员加入的通信代价，实现了防权威陷害攻击，效率方面减少了群中心计算同余方程组计算量，并对比其他已实现的非关联性群签名方案，体现了本方案的一定优势。但本方案在揭露方面计算代价仍然与加入成员数量线性相关，如何减少揭露代价有待今后进一步研究。

参考文献

[1] Chaum D, Van Heyst E. Group signatures [C]// Advances in Cryptolog — EUROCRYPT'91. Springer Berlin Heidelberg, 1991:257-265

[2] Camenisch J, Stadler M. Efficient group signature schemes for large groups [M] // Advances in Cryptology—RYPTO'97. Springer Berlin Heidelberg, 1997:410-424

[3] Bresson E, Stern J. Efficient revocation in group signatures [M]// Public Key Cryptography. Springer Berlin Heidelberg, 2001: 190-206

[4] Nakanishi T, Fujii H, Yuta H, et al. Revocable group signature schemes with constant costs for signing and verifying[J]. IEICE Transactions on Fundamentals of Electronics, Communications

and Computer Sciences,2010,93(1):50-62

[5] Libert B, Peters T, Yung M. Scalable group signatures with revocation[M]// Advances in Cryptology-EUROCRYPT 2012. Springer Berlin Heidelberg,2012:609-627

[6] Chen Ze-wen, Zhang Long-jun, Wang Yu-min, et al. A Group Signature Scheme Based on Chinese Remainder Theorem[J]. Chinese Journal of Electronics,2004,32(7):1062-1065(in Chinese)
陈泽文,张龙军,王育民,等. 一种基于中国剩余定理的群签名方案[J]. 电子学报,2004,32(7):1062-1065

[7] Li Jun,Cui Guo-hua,Liu Zhi-yuan. Cryptanalysis and Improvement of a Group Signature Scheme[J]. Chinese Journal of Electronics,2007,35(4):778-781(in Chinese)
李俊,崔国华,刘志远. 一个群签名方案的密码学分析与改进[J]. 电子学报,2007,35(4):778-781

[8] Wang Feng-he,Hu Yu-pu,Wang Chun-xiao. An Attack and Improve of a Group Signature Scheme Based on Chinese Remainder Theorem[J]. Journal of Electronic & Information technology,2007,29(1):182-184(in Chinese)
王凤和,胡予濮,王春晓. 一个基于中国剩余定理的群签名方案的攻击及其改进方案[J]. 电子与信息学报,2007,29(1):182-184

[9] Zhang Kai, Zhang Jian-zhong. Analysis and improvement of a group signature scheme[J]. Computer Engineering and Applications,2013,49(19):75-78(in Chinese)
张凯,张建中. 对一个群签名方案的分析与改进[J]. 计算机工程与应用,2013,49(19):75-78

[10] Dang Jia-li, Yu Hui-fang. Group Signature Scheme Using Chinese Remainder Theorem[J]. Computer Engineering,2015,41(2):113-116(in Chinese)
党佳莉,俞惠芳. 使用中国剩余定理的群签名方案[J]. 计算机工程,2015,41(2):113-116

[11] Cui Guo-hua, Geng Yong-jun, Lu She-jie, et al. Improved group signature scheme based on Chinese remainder theorem[J]. Journal of Huazhong University of Science and Technology(Natural Science Edition),2009 (6):1-3(in Chinese)
崔国华,耿永军,卢社阶,等. 改进的基于中国剩余定理群签名方案[J]. 华中科技大学学报(自然科学版),2009 (6):1-3

[12] Naor D, Naor M, Lotspiech J. Revocation and tracing schemes for stateless receivers[C]// Advances in Cryptology CRYPTO 2001. Springer Berlin Heidelberg,2001:41-62

[13] Stinson D R. Cryptography: theory and practice [M]. CRC Press,2005

[14] Ateniese G, Tsudik G. Some open issues and new directions in group signatures[M]// Financial Cryptography. Springer Berlin Heidelberg,1999:196-211

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

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

[17] Li Xin-she, Hu Yu-pu. Analysis and improvement of the group signature member deletion scheme[J]. Journal of Xindian Univercity,2008,35(3):478-482(in Chinese)
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

[18] Zheng De-dong, Ma Zhao-feng, Yang Yi-xian, et al. New solution scheme for the member revocation in group signature[J]. Journal on Communications,2014,35(3):193-200(in Chinese)
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

(上接第 157 页)

[14] Wang X F, Li X, Chen G R. Network Science: An Introduction [M]. Beijing: Higher education press,2012:205-208(in Chinese)
汪小帆,李翔,陈关荣. 网络科学导论[M]. 北京:高等教育出版社,2012:205-208

[15] Nexus. The network repository [DB/OL]. http://nexus.igraph.org

[16] Tan L. The theory and application of the dimension reduction on the high dimensional dataset[D]. Changsha: National University of Defense Technology,2005(in Chinese)
谭璐. 高维数据的降维理论及应用[D]. 长沙:国防科技大学,2005

[17] Liu B. Infrared face recognition methods based on the random projection and sparse representation[D]. Xi'an: Xidian University,2009(in Chinese)
刘彬. 基于随机投影和稀疏表征的红外人脸识别方法[D]. 西安:西安电子科技大学,2009

[18] Vempala S S. The Random Projection Method [M]. American Mathematical Society,2004:1-6

[19] Matoušek J. On variants of the Johnson-Lindenstrauss lemma [J]. Random Structures & Algorithms,2008,33(2):142-156

[20] Frankl P, Maehara H. The Johnson-Lindenstrauss lemma and the sphericity of some graphs[J]. Journal of Combinatorial Theory, Series B,1988,44(3):355-362

[21] Arriaga R I, Vempala S. An Algorithmic Theory of Learning: Robust Concepts and Random Projection[C]// Proc of the 40th Annual Symposium Foundations of Computer Science. IEEE, 1999:616-623

[22] Lü L, Zhou T. Link prediction in complex networks: A survey [J]. Physica A: Statistical Mechanics and its Applications,2011, 390(6):1150-1170

[23] Sang Y, Shen H, Tian H. Reconstructing Data Perturbed by Random Projections When the Mixing Matrix Is Known[M]// Machine Learning and Knowledge Discovery in Databases. Springer Berlin: Heidelberg,2009:334-349

[24] Zou L, Chen L, Özsu M T. K-Automorphism: General Framework for Privacy reserving Network Publication [C]// Proc of VLDB'09. Lyon, France,2009:946-957

[25] Newman M E J. The structure and function of complex networks[J]. Society for Industrial and Applied Mathematics, 2003,45(2):167-256