基于组合阶双线性群的组签名方案的分析与改进

余家福[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 周福才等利用组合阶双线性群理论和非交互式零知识证明理论构建了一个基于BMW模型的高效组签名方案,解决了传统组签名方案通信效率低、不能抵抗选择密文攻击等问题。然而研究发现该方案在正确性方面存在不足:验证者不能正确地验证签名者的身份,进而无法完成后续的签名验证操作。据此提出了一个改进方案,并给出了严格的安全性证明,通过增加身份信息的承诺值及对应的非交互式零知识证明,修正了原方案中的缺陷。最后将该改进方案与同类其他方案在安全性和效率方面进行了分析与比较,结果表明该改进方案在保证高效性和安全性的前提下解决了原方案中存在的问题。

关键词 组签名,组合阶双线性群,非交互式零知识证明,正确性分析
中图法分类号 TP309 **文献标识码** A **DOI** 10.11896/j.issn.1002-137X.2016.2.039

Correctness Analysis and Improvement of Group Signature in Composite Order Bilinear Groups

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

Abstract Zhou Fu-cai et al proposed an efficient group signature scheme based on BMW model by utilizing the composite order bilinear groups theory and non-interactive zero knowledge proof system. However, this study demonstrates that there are some deficiencies in Zhou's scheme that signature verifier cannot verify signer's ID correctly and cannot finish the signature verification. Then, the authors provided an improved scheme and proved its security strictly. The proposed scheme corrects the errors by adding the commitment to signer's ID and corresponding non-interactive zero knowledge proof. At last, this paper compared the security and efficiency respectively with the similar group signatures. And the result of analysis shows that the improved scheme resolves the problem of Zhou's scheme in the premise of assuring the security and efficiency.

Keywords Group signature, Composite order bilinear groups, Non-interactive zero knowledge proof, Correctness analysis

1 概述

组签名(Group Signature)也称群签名,是一种具有特殊性质的数字签名,它允许任一成员代表整个组进行签名,外界可以验证签名的合法性,同时签名者在签名过程中隐藏了自己的身份,其保护了签名者的隐私。在发生纠纷时,组管理者能够打开签名,恢复签名者的身份信息,其提供了签名者身份的可追踪性。1991年,Chaum等[1]提出了第一个组签名方案。随后许多组签名方案陆续被提出,这些方案的安全性大多是在随机预言机模型(Random Oracle Model, ROM)[2]下证明的,但是在实际执行时Hash函数的输出并不随机,使得在ROM下可证明安全的方案在现实中根本不安全[3]。标准模型是相对ROM而言的,在此基础上构建的方案具有更高的安全性。2003年,Bellare等[4]首次提出在标准模型下可证明安全的组签名模型,即BMW模型,该模型定义了组签名的通用结构及其应该满足的安全性要求。Boyen等[5]基于分层签名机制提出了新的组签名方案,其基本思想是:首先将组管理者对成员身份信息的签名作为第一层签名,然后利用第一层签名作为密钥对消息进行签名,接着对消息签名进行随机化,使其满足匿名性和不可链接性,最后再用标准模型下的非交互式零知识证明[6](Non-interactive Zero Knowledge, NIZK)来证明这些随机化的签名是合法的。文献[7]基于标准模型和Certified Signature的概念,提出了一个组签名方案,Certified Signature同时考虑了签名和公钥证书的合法性,即不要求公钥证书是不可伪造的,但是要求证书及签名在一起是不可伪造的。Emura等[8]提出的方案允许成员动态加入,但同时也增加了交互次数和通信代价。Wei等[9]提出的群签名方案缩短了签名长度,降低了签名和验证过程的时间复杂度,但增加了验证阶段的交互次数,而且撤销列表的大小也与已撤销成员的数量呈正比。Libert等[10]使用Groth-Sahai证明系统[11]构建了一个组签名方案,该方案满足不可连接性,支持成员撤销,但其计算代价较大,并且没有提供追踪

到稿日期:2015-01-26 返修日期:2015-05-26 本文受国家自然科学基金资助项目(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。
余家福(1990-),男,硕士生,主要研究方向为云中数据访问控制技术,E-mail:yujiafu7@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。

机制，不能解决不可伪造性和不可否认性的问题。文献[12]的安全性基于多项式同构问题，该方案的签名和验证均需要常数阶的时间，但组管理员需要线性的密钥存储空间。

周福才等[13]利用 Lewko[14] 提出的组合阶双线性群理论和 Groth 等[15]设计的非交互式零知识证明系统，构建了一个基于 BMW 模型的组签名方案——GSCOBG 方案，解决了传统组签名方案中存在的效率问题，并证明了方案在 BMW 模型下可以抵抗选择密文攻击，保证了签名的安全性和高效性。然而本文研究发现在 GSCOBG 方案的签名验证阶段，验证者不能验证签名者的身份，进而无法完成对签名的验证操作。本文首先对 GSCOBG 方案进行介绍，分析其正确性，证明 GSCOBG 方案中的验证者不能正确地验证签名者的身份，然后在此基础上提出一个安全高效的改进方案，并给出严格的安全性证明。

2 预备知识

2.1 组合阶双线性群

Lewko 和 Waters 使用群生成器 $\mathcal{G}$ 和一个参数生成算法重新定义组合阶双线性群 $(N=p_1p_2p_3, G, G_T, e)$，其中 G 和 G_T 是两个 N 阶循环群，p_1, p_2, p_3 是 3 个互不相同的素数。双线性映射 $e: G^2 \to G_T$ 满足以下性质：

(1)双线性：$\forall g, h \in G, a, b \in \mathbb{Z}_N, e(g^a, h^b) = e(g,h)^{ab}$。

(2)非退化性：$\exists g \in G$，若 g 是群 G 的生成元，则 $e(g,g)$ 是群 G_T 的生成元。

(3)可计算性：$\forall g, h \in G$，存在有效算法计算 $e(g,h)$。

假设 $G_{p_1}, G_{p_2}, G_{p_3}$ 分别是群 G 中阶为 p_1, p_2, p_3 的子群，若 $h_i \in G_{p_i}, h_j \in G_{p_j}$ 且 $i \neq j$，则 $e(h_i, h_j)$ 是群 G_T 的单位元，该性质被称为正交性，是组合阶双线性群特有的性质，是改进方案构造过程中使用的重要工具。为证明这个性质，令 g 是群 G 的一个生成元，则 $g^{p_1p_2}$ 是群 G_{p_3} 的生成元，类似地，$g^{p_1p_3}$ 是群 G_{p_2} 的生成元，$g^{p_2p_3}$ 是群 G_{p_1} 的生成元。对于 $h_1 \in G_{p_1}$，$h_2 \in G_{p_2}$，$\exists \alpha_1, \alpha_2$，使得 $h_1 = (g^{p_2p_3})^{\alpha_1}$，$h_2 = (g^{p_1p_3})^{\alpha_2}$，于是，$e(h_1, h_2) = e(g^{p_2p_3\alpha_1}, g^{p_1p_3\alpha_2}) = e(g^{\alpha_1}, g^{p_3\alpha_2})^{p_1p_2p_3} = 1$。因此可以很容易地得出下面的结论：若配对函数中的两个元素来自群 G 的任意两个不同的子群，则配对函数值为群 G_T 的单位元 1。

2.2 改进方案的结构

GSCOBG 方案的主要参与者有组管理者、签名者和验证者。方案由以下 6 个多项式时间内的算法组成。

(1)*Setup* 算法：输入安全参数 λ，输出系统公开参数 PP 和系统主密钥 MK 和追踪密钥 TK。

(2)*KeyGen* 算法：系统为用户分配一个唯一标识 ID，输入公开参数 PP 和系统主密钥 MK，输出身份信息为 ID 的用户签名密钥 K_{ID}。

(3)*Sign* 算法：输入系统公开参数 PP、用户签名密钥 K_{ID} 和消息 M，输出原始签名 S。

(4)*Commit* 算法：输入公开参数 PP 和原始签名 S，输出组签名 σ。

(5)*Verify* 算法：输入公开参数 PP 和组签名 σ，对组签名进行验证，输出签名有效或无效。

(6) *Trace* 算法：当发生纠纷时，输入公开参数 PP、消息 M、组签名 σ 和追踪密钥 TK，输出签名者身份标识 ID。

3 GSCOBG 方案

3.1 GSCOBG 方案设计

令 λ 是安全参数，用户身份信息 ID 和消息 M 分别是 k 位和 n 位的二进制串，组内最多可以支持 2^k 个成员加入。G 是一个可交换的乘法群，阶为 $N=p_1p_2p_3$，其中 p_1, p_2, p_3 为互不相同的素数，映射 $e: G^2 \to G_T$ 为双线性映射。方案具体构造如下。

(1)$Setup(1^\lambda)$。令 $G_{p_1}, G_{p_2}, G_{p_3}$ 是群 G 中阶为 p_1, p_2, p_3 的子群。在 G_{p_1} 中随机选择生成元 $g, v \leftarrow G_{p_1}^2$，向量 $(u_1, \cdots, u_k) \leftarrow G_{p_1}^k$ 用于承诺用户 ID，其中 $ID=(x_1, \cdots, x_k) \leftarrow \{0,1\}^k$，向量 $(v_1, \cdots, v_n) \leftarrow G_{p_1}^n$ 用于承诺消息 M，其中，$M=(m_1, \cdots, m_n) \leftarrow \{0,1\}^n$。在 G_{p_2} 中随机选择生成元 $u \leftarrow G_{p_2}$。选择随机数 $\alpha \leftarrow \mathbb{Z}_N$，计算 $A=e(g,g)^\alpha$。系统的公共参数为 $PP=\{G, G_T, e, N, k, n, g, u, u_1, \cdots, u_k, v, v_1, \cdots, v_n, A\}$，系统主密钥 $MK=g^\alpha$，追踪密钥为 $TK=p_2$，组管理者保密 MK 和 TK。

(2)$KeyGen(PP, MK, ID)$。系统为每个用户分配一个全局唯一身份标识 ID，在群 G_{p_3} 中随机选择两个元素 $R_3, R_3' \leftarrow G_{p_3}^2$，随机数 $r_1 \leftarrow \mathbb{Z}_N$，计算用户 ID 的签名密钥：

$$K_{ID}=(K_1=g^\alpha(u^{r_1}\prod_{i=1}^{k}u_i^{x_i})^{r_1}R_3, K_2=g^{r_1}R_3')$$

并生成非交互式零知识证明 $\pi_1=(u^{r_1}\prod_{i=1}^{k}u_i^{2x_i-1})^{r_1}$，用于证实签名者的身份。

(3)$Sign(PP, K_{ID}, M)$。签名者使用签名密钥 $K_{ID}=\{K_1, K_2\}$ 对消息 M 进行签名。选择随机数 $r_2, s \leftarrow \mathbb{Z}_N$，计算签名如下：

$$S=(S_1, S_2, S_3)=(K_1(v^{r_2}\prod_{j=1}^{n}v_j^{m_j})^s, K_2^{-1}, g^{-s})$$

而 S_1, S_2, S_3 满足如下等式：

$$e(S_1, g)e(S_2, u^{r_1}\prod_{i=1}^{k}u_i^{x_i})e(S_3, v^{r_2}\prod_{j=1}^{n}v_j^{m_j})=A$$

(4)$Commit(PP, S)$。签名者选择随机数 $t, t_1, t_2, t_3 \in \mathbb{Z}_N$，对上述签名过程中产生的 3 个签名消息 S_1、S_2、S_3 以及 $u^{r_1}\prod_{i=1}^{k}u_i^{x_i}$ 和 $v^{r_2}\prod_{j=1}^{n}v_j^{m_j}$ 进行如下承诺：

$$com_1=S_1h^{t_1}, com_2=S_2h^{t_2}, com_3=S_3h^{t_3}, com_4=u^{r_1}\prod_{i=1}^{k}u_i^{x_i}h^t, com_5=v^{r_2}\prod_{j=1}^{n}v_j^{m_j}h^t$$

并计算

$$\pi_2=g^{t_1-r_1t-st}\cdot(u^{r_1}\prod_{i=1}^{k}u_i^{x_i})^{t_2}\cdot(v^{r_2}\prod_{j=1}^{n}v_j^{m_j})^{t_3}\cdot h^{t(t_2+t_3)}$$

组签名为：

$$\sigma=(com_1, com_2, com_3, com_4, com_5, \pi_2)$$

(5)$Verify(PP, \sigma)$。验证者对签名者的身份和签名 (m, σ) 进行验证。

1)对身份进行验证时，令 $C=u^{r_1}\prod_{i=1}^{k}u_i^{x_i}$，验证下面等式是否成立：

$$e(C, C\prod_{i=1}^{k}u_i^{-1})=e(u, \pi_1)$$

如果等式成立，则继续对签名进行验证；否则返回错误消息。

2)对签名进行验证时，验证下面等式是否成立：

$$e(com_1, g)\cdot e(com_2, com_4)\cdot e(com_3, com_5)=A\cdot e(h, \pi_2)$$

如果等式成立，则验证通过；否则返回错误消息。

(6)$Trace(PP,C_i,TK)$。签名者在承诺 ID 时，选择 k 个随机数 $r_{1_1},\cdots,r_{1_k}\leftarrow(Z_N)^k$，令 $C_i=u^{r_{1_i}}\cdot u_i^{x_i}$，计算 $C=C_1\cdot C_2\cdot\cdots\cdot C_k=u^{r_1}\cdot u_i^{x_i}$，其中，$r_1=r_{1_1}+r_{1_2}+\cdots+r_{1_k}$。当发生纠纷时，组管理者使用秘密的追踪密钥 $TK=p_2$，通过计算 $(C_i)^{p_2}$ 的值恢复出 ID。若 $(C_i)^{p_2}=1$，则 $x_i=0$；否则 $x_i=1$。从而恢复出用户的 ID，找出签名者。

3.2 正确性分析

在方案的验证阶段，当验证者对签名者的身份进行验证时，只需验证等式 $e(C,C\prod_{i=1}^{k}u_i^{-1})=e(u,\pi_1)$ 是否成立，但是该等式对于任意的 $ID=(x_1,\cdots,x_k)\leftarrow\{0,1\}^k$ 不成立，亦即方案不满足正确性。下面给出上述论述的证明。

证明：通过计算等式的左边可得

$$\begin{aligned}&e(C,C\prod_{i=1}^{k}u_i^{-1})\\&=e(u^{r_1}\prod_{i=1}^{k}u_i^{x_i},u^{r_1}\prod_{i=1}^{k}u_i^{x_i-1})\\&=e(u^{r_1},u^{r_1})\cdot e(u^{r_1},\prod_{i=1}^{k}u_i^{x_i-1})\cdot e(u^{r_1},\prod_{i=1}^{k}u_i^{x_i})\cdot\\&\quad e(\prod_{i=1}^{k}u_i^{x_i},\prod_{i=1}^{k}u_i^{x_i-1})\\&=e(u,(u^{r_1}\prod_{i=1}^{k}u_i^{2x_i-1})^{r_1})\cdot\prod_{i=1}^{k}\prod_{j=1}^{k}e(u_i,u_j)^{x_i(x_j-1)}\end{aligned}$$

假设 $e(C,C\prod_{i=1}^{k}u_i^{-1})=e(u,\pi_1)$ 成立，那么等式

$$\prod_{i=1}^{k}\prod_{j=1}^{k}e(u_i,u_j)^{x_i(x_j-1)}=1$$

成立。将等式的左边展开得

$$\begin{aligned}&\prod_{i=1}^{k}\prod_{j=1}^{k}e(u_i,u_j)^{x_i(x_j-1)}\\&=e(u_1,u_1)^{x_1(x_1-1)}\cdot\cdots\cdot e(u_1,u_k)^{x_1(x_k-1)}\cdot e(u_2,\\&\quad u_1)^{x_2(x_1-1)}\cdot\cdots\cdot e(u_2,u_k)^{x_2(x_k-1)}\cdot\cdots\cdot e(u_k,\\&\quad u_1)^{x_k(x_1-1)}\cdot\cdots\cdot e(u_k,u_k)^{x_k(x_k-1)}\end{aligned}$$

容易看出，当且仅当 $ID=(\underbrace{00\cdots0}_{k})$ 或 $ID=(\underbrace{11\cdots1}_{k})$ 时，等式 $\prod_{i=1}^{k}\prod_{j=1}^{k}e(u_i,u_j)^{x_i(x_j-1)}=1$ 成立，使 ID 失去了其应有的一般性，故从某种意义上讲，身份验证等式 $e(C,C\prod_{i=1}^{k}u_i^{-1})=e(u,\pi_1)$ 不成立，即在 GSCOBG 方案的验证阶段，验证者不能验证签名者的身份，从而无法完成后续的签名验证操作。

4 改进方案

4.1 改进方案的设计

(1)$Setup(1^\lambda)$。同 3.1 节中的系统建立算法 $Setup(1^\lambda)$。

(2)$KeyGen(PP,MK,ID)$。系统为用户分配一个全局唯一身份标识 ID 后，用户选择随机数 $r_{1_1},r_{1_2},\cdots,r_{1_k}\leftarrow(Z_N)^k$，使得 $r_1=r_{1_1}+r_{1_2}+\cdots+r_{1_k}$。计算 $C_{1_i}=u^{r_{1_i}}\cdot u_i^{2x_i^2-1}$ 和 $C_{2_i}=u^{r_{1_i}}\cdot u_i^{1-x_i}$，使得 $C_1=\prod_{i=1}^{k}C_{1_i}=C_{1_1}\cdot C_{1_2}\cdot\cdots\cdot C_{1_k}=u^{r_1}\prod_{i=1}^{k}u_i^{2x_i^2-1}$，$C_2=\prod_{i=1}^{k}C_{2_i}=C_{2_1}\cdot C_{2_2}\cdot\cdots\cdot C_{2_k}=u^{r_1}\prod_{i=1}^{k}u_i^{1-x_i}$。随机选择两个元素 $R_3,R_3'\leftarrow G_{p_3}^2$，计算签名密钥如下：

$$K_{ID}=\{K_1=g^{\alpha}(u^{r_1}\prod_{i=1}^{k}u_i^{2x_i^2-1}\cdot u^{r_1}\prod_{i=1}^{k}u_i^{1-x_i})^{r_1}R_3,K_2=g^{r_1}R_3'\}$$

并生成非交互式零知识证明 $\pi_1=(u^{r_1}\cdot\prod_{i=1}^{k}u_i^{4x_i^2-2})^{r_1}$ 和 $\pi_2=(u^{r_1}\cdot\prod_{i=1}^{k}u_i^{1-2x_i})^{r_1}$，用于证实签名者的身份。

(3)$Sign(PP,K_{ID},M)$。用户使用秘密的签名密钥 K_{ID} 对消息 M 进行签名。选择随机数 $r_2,s\leftarrow Z_N$ 得到如下结果：

$$S=(S_1,S_2,S_3)=(K_1(v^{r_2}\prod_{j=1}^{n}v_j^{m_j})^s,K_2^{-1},g^{-s})$$

而 S_1,S_2,S_3 满足下面的等式：

$$e(S_1,g)e(S_2,u^{2r_1}\prod_{i=1}^{k}u_i^{2x_i^2-x_i})e(S_3,v^{r_2}\prod_{j=1}^{n}v_j^{m_j})=A$$

(4)$Commit(PP,S)$。签名者选择随机数 $t,t_1,t_2,t_3\in Z_N$，在群 G_{p_1} 中随机选择生成元 $h\leftarrow G_{p_1}$，并对上述签名过程中产生的 3 个签名消息 S_1、S_2、S_3 以及 $u^{r_1}\prod_{i=1}^{k}u_i^{2x_i^2-1}$、$u^{r_1}\prod_{i=1}^{k}u_i^{1-x_i}$、$v^{r_2}\prod_{j=1}^{n}v_j^{m_j}$ 进行如下承诺：

$$com_1=S_1h^{t_1},com_2=S_2h^{t_2},com_3=S_3h^{t_3},com_4=u^{r_1}\prod_{i=1}^{k}u_i^{2x_i^2-1}h^t,com_5=u^{r_1}\prod_{i=1}^{k}u_i^{1-x_i}h^t,com_6=v^{r_2}\prod_{j=1}^{n}v_j^{m_j}h^t$$

并计算

$$\pi_3=g^{t_1-2r_1t-st}\cdot(u^{2r_1}\prod_{i=1}^{k}u_i^{2x_i^2-x_i})^{t_2}\cdot(v^{r_2}\prod_{j=1}^{n}v_j^{m_j})^{t_3}\cdot h^{t(2t_2+t_3)}$$

组签名为：

$$\sigma=(com_1,com_2,com_3,com_4,com_5,com_6,\pi_3)$$

(5)$Verify(PP,\sigma)$。验证者收到签名后，对签名者的身份和签名 (m,σ) 进行验证。

1)对身份进行验证时，验证下面等式是否成立：

$$e(C_1,\frac{C_1\cdot C_2^2\cdot\prod_{i=1}^{k}u_i^{-1}}{u^{2r_1}})=e(u,\frac{\pi_1\cdot\pi_2}{u^{r_1^2}})$$

如果成立，则继续对签名进行验证；否则返回错误消息。

2)对签名进行验证时，验证下面等式是否成立：

$$e(com_1,g)\cdot e(com_2,com_4\cdot com_5)\cdot e(com_3,com_6)=A\cdot e(h,\pi_3)$$

如果等式成立，则验证通过；否则返回错误消息。

(6)$Trace(PP,C_{1_i},TK)$。当产生纠纷时，组管理者使用追踪密钥 $TK=p_2$，通过计算 $(C_{1_i}\cdot C_{2_i})^{p_2}$ 的值恢复出 ID。若 $(C_{1_i}\cdot C_{2_i})^{p_2}=1$，则 $x_i=0$；否则 $x_i=1$。从而恢复出用户的 ID，找出签名者。

4.2 安全性证明

定理 1 改进方案是一个具有正确性、完全匿名性、不可伪造性、完全可追踪性的组签名方案。

证明：正确性的证明包含 3 个部分：身份验证的正确性、原始签名验证的正确性、组签名验证的正确性。下面分别对以上 3 个部分进行验证。

(1)身份验证

对签名者身份的验证如下：

$$\begin{aligned}&e(C_1,\frac{C_1\cdot C_2^2\cdot\prod_{i=1}^{k}u_i^{-1}}{u^{2r_1}})\\&=e(u^{r_1}\prod_{i=1}^{k}u_i^{2x_i^2-1},\frac{u^{r_1}\prod_{i=1}^{k}u_i^{2x_i^2-1}\cdot(u^{r_1}\prod_{i=1}^{k}u_i^{1-x_i})^2\cdot\prod_{i=1}^{k}u_i^{-1}}{u^{2r_1}})\\&=e(u^{r_1}\prod_{i=1}^{k}u_i^{2x_i^2-1},u^{r_1}\prod_{i=1}^{k}u_i^{2x_i^2-2x_i})\\&=e(u^{r_1},u^{r_1})\cdot e(u^{r_1},\prod_{i=1}^{k}u_i^{2x_i^2-2x_i})\cdot e(\prod_{i=1}^{k}u_i^{2x_i^2-1},u^{r_1})\cdot\\&\quad e(\prod_{i=1}^{k}u_i^{2x_i^2-1},\prod_{i=1}^{k}u_i^{2x_i^2-2x_i})\end{aligned}$$

$$=e(u,(u^{r_1}\prod_{i=1}^{k}u_i^{4x_i^2-2x_i-1})^{r_1})\cdot\prod_{i=1}^{k}\prod_{j=1}^{k}e(u_i,u_j)^{2\cdot(2x_i^2-1)\cdot(x_j^2-x_j)}$$

$$=e(u,\frac{\pi_1\cdot\pi_2}{u^{r_1^2}})$$

(2)原始签名验证

签名者产生原始签名 $S=(S_1,S_2,S_3)$，该三元组满足等式：

$$e(S_1,g)\cdot e(S_2,u^{2r_1}\prod_{i=1}^{k}u_i^{2x_i^2-x_i})\cdot e(S_3,v^{r_2}\prod_{j=1}^{n}v_j^{m_j})=A$$

验证如下：

$$e(S_1,g)\cdot e(S_2,u^{2r_1}\prod_{i=1}^{k}u_i^{2x_i^2-x_i})\cdot e(S_3,v^{r_2}\prod_{j=1}^{n}v_j^{m_j})$$

$$=e(g^{\alpha}(u^{2r_1}\prod_{i=1}^{k}u_i^{2x_i^2-x_i})^{r_1}R_3(v^{r_2}\prod_{j=1}^{n}v_j^{m_j})^{s},g)\cdot e((g^{r_1}R_3')^{-1},u^{2r_1}\prod_{i=1}^{k}u_i^{2x_i^2-x_i})\cdot e(g^{-s},v^{r_2}\prod_{j=1}^{n}v_j^{m_j})$$

$$=e(g^{\alpha},g)\cdot e(R_3,g)\cdot e((R_3')^{-1},u^{2r_1}\prod_{i=1}^{k}u_i^{2x_i^2-x_i})$$

$$=e(g^{\alpha},g)=A$$

(3)组签名验证

签名者承诺后的签名值 $\sigma=(com_1,com_2,com_3,com_4,com_5,\pi_3)$ 满足验证等式：

$$e(com_1,g)\cdot e(com_2,com_4\cdot com_5)\cdot e(com_3,com_6)=A\cdot e(h,\pi_3)$$

验证如下：

$$e(com_1,g)\cdot e(com_2,com_4\cdot com_5)\cdot e(com_3,com_6)$$

$$=e(S_1h^{t_1},g)\cdot e(S_2h^{t_2},u^{2r_1}\prod_{i=1}^{k}u_i^{2x_i^2-x_i}h^{2t})\cdot e(S_3h^{t_3},v^{r_2}\prod_{j=1}^{n}v_j^{m_j}h^{t})$$

$$=e(g^{\alpha},g)\cdot e(h,g^{t_1-r_1t-st}h^{t(2t_2+t_3)})\cdot e(h,(u^{2r_1}\cdot\prod_{i=1}^{k}u_i^{2x_i^2-x_i})^{t_2}\cdot(v^{r_2}\prod_{j=1}^{n}v_j^{m_j})^{t_3})$$

$$=A\cdot e(h,\pi_3)$$

身份验证、原始签名验证和组签名验证这 3 部分都满足正确性，从而改进方案满足正确性。

改进方案对完全匿名性、不可伪造性、完全可追踪性等性质的证明与 GSCOBG 类似，故在这里省略。

定理 2 改进后的系统是一个具有正确性、合理性、证据不可区分性、可追踪性的非交互式零知识证明系统。

证明：该非交互式零知识证明系统的正确性证明见定理 1，下面主要证明其合理性、证据不可区分性、可追踪性。

(1)合理性

已知身份验证等式 $e(C_1,\frac{C_1\cdot C_2^2\cdot\prod_{i=1}^{k}u_i^{-1}}{u^{2r_1}})=e(u,\frac{\pi_1\cdot\pi_2}{u^{r_1^2}})$ 是成立的。

$$e(C_1,\frac{C_1\cdot C_2^2\cdot\prod_{i=1}^{k}u_i^{-1}}{u^{2r_1}})$$

$$=e(u^{r_1}\prod_{i=1}^{k}u_i^{2x_i^2-1},u^{r_1}\prod_{i=1}^{k}u_i^{2x_i^2-2x_i})$$

$$=e(u,(u^{r_1}\prod_{i=1}^{k}u_i^{4x_i^2-2x_i-1})^{r_1})\cdot\prod_{i=1}^{k}\prod_{j=1}^{k}e(u_i,u_j)^{2\cdot(2x_i^2-1)\cdot(x_j^2-x_j)}$$

u 是 G_{p_2} 的生成元，$e(u,(u^{r_1}\prod_{i=1}^{k}u_i^{4x_i^2-2x_i-1})^{r_1})$ 的阶为 1 或 p_2，由身份验证等式成立可以得出 $e(C_1,\frac{C_1\cdot C_2^2\cdot\prod_{i=1}^{k}u_i^{-1}}{u^{2r_1}})$ 的阶为 1 或 p_2，因此，$\prod_{i=1}^{k}\prod_{j=1}^{k}e(u_i,u_j)^{2\cdot(2x_i^2-1)\cdot(x_j^2-x_j)}$ 的阶为 1 或 p_2，而 u_i 是 G_{p_1} 的生成元，其阶为 p_1，故 $x_i=0$ 或 $x_i=1$。

(2)证据不可区分性

签名者选择随机数 $r_{1_1},r_{1_2},\cdots,r_{1_k}\leftarrow(\mathbb{Z}_N)^k$，且 $r_1=r_{1_1}+r_{1_2}+\cdots+r_{1_k}$，计算 $C_{1_i}=u^{r_{1_i}}\cdot u_i^{2x_i^2-1}$ 和 $C_{2_i}=u^{r_{1_i}}\cdot u_i^{1-x_i}$，使得 $C_1=\prod_{i=1}^{k}C_{1_i}=C_{1_1}\cdot C_{1_2}\cdot\cdots\cdot C_{1_k}=u^{r_1}\prod_{i=1}^{k}u_i^{2x_i^2-1}$，$C_2=\prod_{i=1}^{k}C_{2_i}=C_{2_1}\cdot C_{2_2}\cdot\cdots\cdot C_{2_k}=u^{r_1}\prod_{i=1}^{k}u_i^{1-x_i}$，对 $ID=(x_1,\cdots,x_k)\leftarrow\{0,1\}$ 的每一位进行承诺。令 $C_{1_i}=u^{r_{1_i}}\cdot u_i^{-1}=u^{r'_{1_i}}\cdot u_i^{1}$，产生唯一的证明 π_1；令 $C_{2_i}=u^{r_{1_i}}\cdot u_i^{1}=u^{r'_{1_i}}\cdot u_i^{0}$，产生唯一的证明 π_2，满足身份验证等式。因此，对于具有相同承诺值的不同承诺对象，生成的证明 $\pi_1=(u^{r_{1_i}}\cdot u_i^{-2})^{r_{1_i}}=u^{r'_{1_i}r_{1_i}}=(u^{r'_{1_i}}\cdot u_i^{2})^{r'_{1_i}}$ 的值相等，$\pi_2=(u^{r_{1_i}}\cdot u_i^{1})^{r_{1_i}}=u^{r'_{1_i}r_{1_i}}=(u^{r'_{1_i}}\cdot u_i^{-1})^{r'_{1_i}}$ 值也相等。

(3)可追踪性

已知承诺值为 $C_{1_i}=u^{r_{1_i}}\cdot u_i^{2x_i^2-1}$ 和 $C_{2_i}=u^{r_{1_i}}\cdot u_i^{1-x_i}$ 时，验证者并不能从中获得签名者的签名密钥以及身份信息。同时，承诺对象 x_i 与承诺值 $C_i=C_{1_i}\cdot C_{2_i}$ 一一对应，即对两个不同的 x_i 承诺后得到的承诺值不相同。当产生纠纷时，组管理者可以使用追踪密钥 $TK=p_2$，通过计算 $(C_i)^{p_2}=(u^{2r_{1_i}}\cdot u_i^{2x_i^2-x_i})^{p_2}=(u_i^{p_2})^{2x_i^2-x_i}$ 提取出承诺对象 x_i，从而恢复签名者的 ID。

5 分析与比较

本节从安全性和效率两个方面对本文提出的方案与同类其他方案进行了比较。表 1 是安全性对比。

表 1 安全性对比

方案	正确性	非交互式	匿名性	抗 CCA	不可否认性	可追踪性	不可连接性	不可区分性	成员撤销
WL[9]	√	×	√	×	×	×	√	√	√
LV[10]	√	√	√	√	×	×	√	√	√
GSCOBG[13]	×	√	√	√	√	√	×	√	×
本文	√	√	√	√	√	√	×	√	×

表 2 效率对比

方案	通信次数	通信代价	计算代价
WL[9]	5	$(3n+4)\|G\|+7\|Z_N\|$	12BP+7SM+27P
LV[10]	3	$(2n+38)\|G\|+(n+12)\|Z_N\|$	22BP+(n+23)SM+(n+21)P
本文	3	$(4n+15)\|G\|+12\|Z_N\|$	9BP+(6n+15)SM+(n+30)P

表 2 是效率对比，分别从通信次数、通信代价、计算代价 3 个方面进行分析。为了便于比较，将 G 中元素的长度记为 $|G|$，Z_N 中元素的长度记为 $|Z_N|$，双线性对运算记为 BP，椭圆曲线 G 上的标量点乘运算记为 SM，G 上的幂运算记为 P。其中，双线性对所花费的运算时间远多于其他运算，因此，在效率分析上应该作为主要的考虑因素。通过计算，本文提出的组签名方案的交互次数为 3，通信代价为 $(4n+15)|G|+12|Z_N|$（其中，n 为消息的长度），计算代价为 $9BP+(6n+15)SM+(n+30)P$。

(下转第 209 页)

[18] Li X, Wang K, Liu L, et al. Application of the entropy weight and TOPSIS method in safety evaluation of coal mines[J]. Procedia Engineering, 2011, 26: 2085-2091

[19] Liu W B. Research and realization of fuzzy synthetical evaluation system[D]. Tianjin: Hebei University of Technology, 2003 (in Chinese)
刘文彬. 模糊综合评价系统研究与实现[D]. 天津: 河北工业大学, 2003

[20] Huang J H, Peng K H. Fuzzy Rasch model in TOPSIS: A new approach for generating fuzzy numbers to assess the competitiveness of the tourism industries in Asian countries [J]. Tourism Management, 2012, 33(2): 456-465

[21] Li C Y, Sun J F, Hu D, et al. Application of IAHP and TOPSIS in the evaluation of heavy metal pollution[J]. Chinese Journal of Health Statistics, 2010, 27(2): 166-168 (in Chinese)
李朝赟, 孙金芳, 胡丹, 等. 改进层次分析法和逼近理想解排序法结合在重金属污染评价中的应用[J]. 中国卫生统计, 2010, 27(2): 166-168

[22] Deng H, Yeh C H, Willis R J. Inter-company comparison using modified TOPSIS with objective weights[J]. Computers & Operations Research, 2000, 27(10): 963-973

[23] Du Y. Research on the component quality model and evaluation method[D]. Kunming: Kunming University of Science and Technology, 2011 (in Chinese)
杜云. 构件质量模型的建立与评估方法研究[D]. 昆明: 昆明理工大学, 2011

[24] Jia J, Fan Y, Guo X. The low carbon development (LCD) levels' evaluation of the world's 47 countries (areas) by combining the FAHP with the TOPSIS method[J]. Expert Systems with Applications, 2012, 39(7): 6628-6640

[25] Bulgurcu B K. Application of TOPSIS Technique for Financial Performance Evaluation of Technology Firms in Istanbul Stock Exchange Market[J]. Procedia-Social and Behavioral Sciences, 2012, 62: 1033-1040

[26] Zhang H, Gu C, Gu L, et al. The evaluation of tourism destination competitiveness by TOPSIS & information entropy — A case in the Yangtze River Delta of China[J]. Tourism Management, 2011, 32(2): 443-451

(上接第 182 页)

通过表 1 和表 2 可以得出以下结论：本文提出的组签名方案可以正确地对签名者的身份和签名进行验证，在通信次数方面优于方案 WL[9]，在配对运算量方面优于方案 WL[9] 和方案 LV[10]。

结束语 在解决传统组签名方案通信效率低、不能抵抗选择密文攻击等问题时，周福才等提出了一个基于 BMW 模型的组签名方案 GSCOBG，并提供了严格的安全性证明。然而对 GSCOBG 方案进行正确性分析后，发现验证者并不能对签名者的合法身份和签名进行身份验证和签名验证。针对 GSCOBG 方案这一缺陷，本文提出了一个改进方案，通过增加对身份信息的承诺值和相应非交互式零知识证明，解决了 GSCOBG 中的问题，使得验证者能够验证签名者的身份，从而使整个改进方案具有正确性，并且满足安全性和高效性。但是改进方案也存在不足之处，比如不满足不可连接性、不支持成员撤销等，这需要在今后的工作中继续完善。

参 考 文 献

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

[2] Bellare M, Rogaway P. Random oracles are practical: A paradigm for designing efficient protocols[C]// Proceedings of the 1st ACM Conference on Computer and Communications Security. ACM, 1993: 62-73

[3] Canetti R, Goldreich O, Halevi S. The random oracle methodology, revisited[J]. Journal of the ACM (JACM), 2004, 51(4): 557-594

[4] Bellare M, Micciancio D, Warinschi B. Foundations of group signatures: Formal definitions, simplified requirements, and a construction based on general assumptions [M]// Advances in Cryptology-Eurocrypt 2003. Springer Berlin Heidelberg, 2003: 614-629

[5] Boyen X, Waters B. Full-domain subgroup hiding and constant-size group signatures [M]// Public Key Cryptography-PKC 2007. Springer Berlin Heidelberg, 2007: 1-15

[6] Groth J, Ostrovsky R, Sahai A. Non-interactive zaps and new techniques for NIZK[M]// Advances in Cryptology-CRYPTO 2006. Springer Berlin Heidelberg, 2006: 97-111

[7] Groth J. Fully anonymous group signatures without random oracles[M]// Advances in Cryptology-ASIACRYPT 2007. Springer Berlin Heidelberg, 2007: 164-180

[8] Emura K, Hanaoka G, Sakai Y. Group signature implies PKE with non-interactive opening and threshold PKE[M]// Advances in Information and Computer Security. Springer Berlin Heidelberg, 2010: 181-198

[9] Wei L, Liu J. Shorter verifier-local revocation group signature with backward unlinkability[M]// Pairing-Based Cryptography-Pairing 2010. Springer Berlin Heidelberg, 2010: 136-146

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

[11] Groth J, Ostrovsky R, Sahai A. Perfect non-interactive zero knowledge for NP[M]// Advances in Cryptology-EUROCRYPT 2006. Springer Berlin Heidelberg, 2006: 339-358

[12] Yang G, Tang S, Yang L. A novel group signature scheme based on mpkc[M]// Information Security Practice and Experience. Springer Berlin Heidelberg, 2011: 181-195

[13] Zhou F C, Xu J, Wang L L, et al. A group signature in the composite order bilinear groups[J]. Chinese Journal of Computers, 2012, 35(4): 654-663 (in Chinese)
周福才, 徐剑, 王兰兰, 等. 基于组合阶双线性群的组签名方案[J]. 计算机学报, 2012, 35(4): 654-663

[14] Lewko A, Waters B. New techniques for dual system encryption and fully secure HIBE with short ciphertexts [M]// Theory of Cryptography. Springer Berlin Heidelberg, 2010: 455-479

[15] Groth J, Sahai A. Efficient non-interactive proof systems for bilinear groups [M]// Advances in Cryptology-EUROCRYPT 2008. Springer Berlin Heidelberg, 2008: 415-432