基于组合阶双线性群的组签名方案

周福才[1)] 徐 剑[1),2)] 王兰兰[2)] 陈 晨[2)] 李福祥[2)]

[1)](东北大学软件学院 沈阳 110819)

[2)](东北大学信息科学与工程学院 沈阳 110819)

摘 要 利用Lewko等人于2010年提出的三素数组合阶双线性群理论,构建了一个基于BMW模型的高效组签名方案,并通过引进Groth-Sahai等人提出的非交互式零知识证明理论,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.方案中签名的大小是一个常量而非依赖于其它系统参数.作者同时给出了严格的安全性证明,并将文中方案分别与已有的典型方案在效率和安全性方面进行了比较,结果表明该方案在这两方面均具有一定优势.

关键词 组签名;组合阶双线性群;非交互式零知识证明;BMW模型

中图法分类号 TP309 **DOI号**: 10.3724/SP.J.1016.2012.00654

A Group Signature in the Composite Order Bilinear Groups

ZHOU Fu-Cai[1)] XU Jian[1),2)] WANG Lan-Lan[2)] CHEN Chen[2)] LI Fu-Xiang[2)]

[1)](*Software College*, *Northeastern University*, *Shenyang* 110819)

[2)](*College of Information Science and Engineering*, *Northeastern University*, *Shenyang* 110819)

Abstract We present an efficient group signature scheme based on BMW model utilizing composite order (of 3 primes) bilinear groups theory proposed by Lewko et al. in 2010. Besides, we apply the Groth-Sahai non-interactive proof system in this scheme to solve the problem of traditional group signatures such as inefficient communication and chosen ciphertext attack. In addition, the size of the signature is a constant rather than relying on other parameters and the security of the scheme is proved under standard model. We compare the security and the efficiency respectively with the similar group signatures, and achieve the advantage.

Keywords group signature; composite order bilinear groups; non-interactive zero-knowledge proofs; BMW model

1 引 言

1.1 相关工作

Chaum和Van Heyst[1]于1991年首次提出组签名方案,该方案允许组内成员代表整个组进行签名而不暴露签名者身份.由于组签名的特殊性质,很快引起各国学者的广泛关注.按照组签名安全性的证明方法,可以分为基于随机预言模型(ROM)和基于标准模型的组签名.基于ROM的安全性证明已经取得了很多成果,组签名方案[2-5]的安全性证明依赖于ROM,研究者通过利用ROM证明签名的不可

收稿日期:2011-05-11;最终修改稿收到日期:2012-02-28.本课题得到国家"八六三"高技术研究发展计划项目基金(2009AA01Z122)、辽宁省百千万人才工程项目(2011921071)、沈阳市自然科学基金(F10-205-1-12)资助.**周福才**,男,1964年生,教授,博士生导师,中国计算机学会(CCF)高级会员,主要研究领域为密码学与网络安全、可信计算、电子商务基础理论与关键技术.E-mail:fczhou@mail.neu.edu.cn.**徐 剑**(通信作者),男,1978年生,博士研究生,讲师,主要研究方向为密码学与网络安全、数据与身份认证技术.E-mail:xuj@mail.neu.edu.cn.**王兰兰**,女,1986年生,硕士研究生,主要研究方向为组签名与非交互式零知识证明.**陈 晨**,女,1987年生,硕士研究生,主要研究方向为密码学与网络安全、非交互式零知识证明.**李福祥**,男,1984年生,博士研究生,主要研究方向为格理论与密码学.

否认性、抗联合攻击等重要性质，从而证明组签名方案的安全性. Canetti 等人[6]指出在 ROM 中理论上存在安全的签名和加密方案，但在实际使用 ROM 时需假设签名的明文是均匀随机的，实际上并不存在这样的明文，因此在实际应用中并不安全. 也有其它研究者指出了 ROM 存在的缺陷[7-9]. 在后续的研究中，研究人员开始避免使用 ROM，而逐渐向标准模型过渡.

Bellare 等人提出了第一个在标准模型下证明安全的组签名模型，称之为 BMW 模型[10]，该模型给出了组签名的通用结构及其应该满足的安全性要求，并在组签名过程中引入非交互式零知识证明(NIZK)理论. 该结构满足完全匿名性和完全可追踪性，组签名的其它性质可以从这两个基本性质中得到证明，而且签名密钥的长度是组内成员数量的对数，签名的大小是常量. 文献[11-15]方案都是基于 BMW 模型构建的组签名方案，其中文献[11]方案由 Boyen 和 Waters 于 2005 年提出，其安全性证明依赖于标准模型，他们将分层签名机制和 NIZK[16]相结合，其中安全的分层签名来源于组合阶双线性群中高效的基于身份的加密方案[17]. 但该组签名方案仅在选择明文攻击下是安全的，并不能抵抗选择密文攻击，而且所使用的群中元素个数依赖于签名者的数量. 2007 年 Boyen 等人改进了文献[11]方案的缺陷，并提出了新的组签名方案[12]. 该方案中，引进了 Groth 的 NIZK 理论[18]，其效率和文献[11]方案相比有所提高. Libert 等人于 2009 年使用 Groth-Sahai 证明系统的第 3 个实例——DLIN[19]构建了组签名方案[14]，并给出不可连接性的证明，同时解决了组内成员的证书撤销机制，但由于非交互式证明系统的计算代价较大，所以不适合实际应用，也没有提供合理的追踪机制，导致其不能解决不可伪造性和不可否认性等问题.

BMW 模型的缺点之一是组成员不能动态加入，成员最大数量在初始化阶段就已经确定，而且真实的成员数量也是难以确定的，这一点影响了组签名在很多方面的应用(比如可信计算平台的匿名认证环境中). 为了解决上述问题，Bellare 等人于 2005 年将 BMW 模型扩展为 BSZ 模型[20]，BSZ 模型中增加了成员的“加入”阶段，并增强了安全性. 但每增加一个阶段，就意味着增加交互次数，增加通信代价. 方案[21-22]是基于 BSZ 模型构建的组签名方案，其中 Ateniese 和 Camenisch 等人提出的方案[21]是早期比较高效的方案之一，其中应用了 BB+签名和 CL+签名的重要性质. 但他们所使用的安全性证明依赖于交互式假设，所以不能抵抗选择密文攻击.

1.2　本文工作

2010 年，Lewko 等人在文献[23]中提出了三素数组合阶双线性群理论，并构建了一个 HIBE 加密方案，此方案被证明是完全安全的，而且能够解决在 HIBE 系统中不使用标签和密文压缩等问题. 本文利用上述三素数组合阶双线性群及 HIBE 加密方案构建了一个基于 BMW 模型的高效组签名方案，满足 BMW 模型中定义的完全匿名性和完全可追踪性等安全性要求，除此之外，本文运用假设 2、3 证明了该组签名方案的不可伪造性.

NIZK 的重要特点之一是能够抵抗选择密文攻击，此外，非交互式证明中交互的单向性也是密码学协议的一个重要应用. Groth 和 Sahai 在文献[24]中提出了强有力的非交互式证明系统，用于证明被承诺的变量所满足的特定关系. 本文将 NIZK 的理论应用于组签名方案中，一方面解决选择密文攻击的问题，另一方面利用非交互式证明的交互单向性保证签名的安全性和通信的高效性. 在文章的第 5 节，将通信代价和计算代价分别与同类文章进行对比分析.

2　预备知识

2.1　组合阶双线性群

2010 年 Lewko 和 Waters 使用群生成器$\mathcal{G}$和一个参数生成算法重新定义了组合阶双线性群，其中参数生成算法以安全参数 λ 作为输入，以双线性群 G 的描述作为输出. 群生成器$\mathcal{G}$输出参数 $(N=p_1p_2p_3, G, G_T, e)$，其中 p_1, p_2, p_3 是互不相同的素数，G 和 G_T 是阶为 $N=p_1p_2p_3$ 的循环群，映射 $e: G^2 \to G_T$ 的性质描述如下：

(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. $\exists g \in G$, g 是群 G 的生成元，则 $e(g, g)$ 是 G_T 的生成元.

假设 1.　三素数组合阶双线性群中的子群判定假设，给定一个群的生成器$\mathcal{G}$，定义下列关系：

$$\mathbb{G}=(N=p_1p_2p_3, G, G_T, e) \xleftarrow{R} \mathcal{G},$$
$$g \xleftarrow{R} G_{p_1},\ X_3 \xleftarrow{R} G_{p_3},$$
$$D=(\mathbb{G}, g, X_3),\ T_1 \xleftarrow{R} G_{p_1p_2},\ T_2 \xleftarrow{R} G_{p_1}.$$

定义敌手$\mathcal{A}$攻破假设1的优势为$Adv1_{\mathcal{G},\mathcal{A}}(\lambda):=|Pr[\mathcal{A}(D,T_1)=1]-Pr[\mathcal{A}(D,T_2)=1]|$. 对于任一个多项式时间算法$\mathcal{A}$,$Adv1_{\mathcal{G},\mathcal{A}}(\lambda)$是一个关于$\lambda$可忽略函数.

假设2. 给定一个群生成器$\mathcal{G}$,定义下列关系:

$$\mathbb{G}=(N=p_1p_2p_3,G,G_T,e)\xleftarrow{R}\mathcal{G},g,X_1\xleftarrow{R}G_{p_1},$$
$$X_2,Y_2\xleftarrow{R}G_{p_2},X_3,Y_3\xleftarrow{R}G_{p_3},$$
$$D=(\mathbb{G},g,X_1X_2,X_3,Y_2Y_3),T_1\xleftarrow{R}G,T_2\xleftarrow{R}G_{p_1p_3}.$$

定义敌手$\mathcal{A}$攻破假设2的优势为$Adv2_{\mathcal{G},\mathcal{A}}(\lambda):=|Pr[\mathcal{A}(D,T_1)=1]-Pr[\mathcal{A}(D,T_2)=1]|$. 对于任一个多项式时间算法$\mathcal{A}$,$Adv1_{\mathcal{G},\mathcal{A}}(\lambda)$是一个关于$\lambda$可忽略函数.

假设3. 给定一个群生成器$\mathcal{G}$,定义下列关系:

$$\mathbb{G}=(N=p_1p_2p_3,G,G_T,e)\xleftarrow{R}\mathcal{G},\alpha,s\xleftarrow{R}\mathbb{Z}_N,$$
$$g\xleftarrow{R}G_{p_1},X_2,Y_2,Z_2\xleftarrow{R}G_{p_2},X_3\xleftarrow{R}G_{p_3},$$
$$D=(\mathbb{G},g,g^{\alpha}X_2,X_3,g^{s}Y_2,Z_2),$$
$$T_1=e(g,g)^{\alpha s},T_2\xleftarrow{R}G_T.$$

定义敌手$\mathcal{A}$攻破假设2的优势为$Adv3_{\mathcal{G},\mathcal{A}}(\lambda):=|Pr[\mathcal{A}(D,T_1)=1]-Pr[\mathcal{A}(D,T_2)=1]|$. 对于任一个多项式时间算法$\mathcal{A}$,$Adv1_{\mathcal{G},\mathcal{A}}(\lambda)$是一个关于$\lambda$可忽略函数.

2.2 Groth-Sahai 证明系统

Groth 和 Sahai 给出了如何使用非交互式零知识理论构建证明系统的方法. 其中常用的基本概念如下:承诺是指将$\{x_m\}_{m=1\cdots M}\in G_1$进行隐藏,计算得出其唯一绑定的承诺值$\{C_m\}_{m=1\cdots M}$. 随机选择$\{a_q\}_{q=1\cdots Q}\in G_1$,$\{b_q\}_{q=1\cdots Q}\in G_2$,$\{\alpha_{q,m}\}_{q=1\cdots Q,m=1\cdots M}\in Z_p$,$\{\beta_{q,n}\}_{q=1\cdots Q,n=1\cdots N}\in Z_p$,则$\{x_m\}_{m=1\cdots M}\in G_1$在群$G_1$上的承诺为$\left\{C_m=a_q\prod_{m=1}^{M}x_m^{\alpha_{q,m}}\right\}_{m=1\cdots M}$,$\{y_n\}_{n=1\cdots N}\in G_2$在群$G_2$上的承诺为$\left\{D_n=b_q\prod_{n=1}^{N}y_n^{\beta_{q,n}}\right\}_{n=1\cdots N}$. 包含承诺值的双线性配对等式$\prod_{q=1}^{Q}e\left(a_q\prod_{m=1}^{M}x_m^{\alpha_{q,m}},b_q\prod_{n=1}^{N}y_n^{\beta_{q,n}}\right)=t$称为陈述$s$. 证明$\pi$是要证明陈述$s$是正确的,即配对等式有解存在,系统能够从承诺中提取相应的x_m和y_n,使得陈述s中的等式成立. 形式化的表示如下:

$$\pi=NIZK\{((c_1:x_1),\cdots,(c_M:x_M),(d_1:y_1),\cdots,(d_N:y_N)):\prod_{q=1}^{Q}e\left(a_q\prod_{m=1}^{M}x_m^{\alpha_{q,m}},b_q\prod_{n=1}^{N}y_n^{\beta_{q,n}}\right)=t\}.$$

上述证明系统满足如下安全性要求:

(1) 正确性. 即诚实的示证者持有证据w,则其陈述s一定会被诚实的验证者接受.

(2) 合理性. 若$x\notin L$,一个多项式时间内的敌手PPT不能伪造一个可以被诚实验证者接受的证明.

(3) 可追踪性. 若诚实验证者接受了证明,则可以从承诺中提取出满足配对等式的值.

(4) 证据不可区分性. 若关于陈述$x\in L$存在着两个证据w_1,w_2,多项式时间内敌手PPT不能分辨出证明过程使用的是哪一个证据.

3 GSCOBG 方案

本节在 BMW 模型的基础上给出了 GSCOBG 方案的算法构成与安全性定义,以及该方案的详细设计过程.

3.1 GSCOBG 方案结构及其安全性定义

本文所给出的组签名方案包含6个多项式时间内算法:组签名初始化算法$Setup$,组签名密钥产生算法$KeyGen$,组内成员签名算法$Sign$,承诺算法$Commit$,签名验证算法$Verify$,签名追踪算法$Trace$.

$Setup$算法. 输入安全参数,系统产生所用到的所有公共参数和随机数.

$KeyGen$算法. 系统将公共参数作为输入,产生三元组(TK,MK,K_{ID}),其中TK为追踪密钥,MK为组管理者私钥,K_{ID}是身份信息为ID的组内成员的签名密钥.

$Sign$算法. 该算法将组内成员ID的签名密钥和要签署的消息M作为输入,算法输出一个在消息M上的签名,签名要满足特定的验证等式.

$Commit$算法. 该算法将上述的签名值及其满足的特定关系作为输入,产生和签名值所对应的承诺值,并将特定关系转化为配对乘积等式.

$Verify$算法. 该算法将公共参数、消息M,签名值σ作为输入,如验证通过则输出1,否则输出0.

$Trace$算法. 该算法将组管理追踪密钥TK、消息M和在M上的签名值σ作为输入,算法输出签名者标识ID.

对于一个安全的组签名方案须满足下列安全性:

正确性. 对于诚实的组成员生成的签名,验证者必须接受,且通过追踪算法能够从正确的签名中提取出正确的成员身份. 形式化表述为

$$Pr[params \leftarrow Setup(1^{\lambda}); (MK, TK, K_{ID}) \leftarrow Keygen(params); \sigma \leftarrow Sign(params, K_{ID}, M): Verify(params, m, \sigma) = 1 \wedge Trace(TK, M, \sigma) = ID] = 1.$$

完全匿名性. 匿名性要求敌手不能计算出组管理者的私钥，也不能恢复出组成员的身份信息. 敌手 $\mathcal{A}$ 执行两个阶段：选择阶段和猜测阶段. 在选择阶段 $\mathcal{A}$ 输入组成员的私钥 K_{ID} 和公共参数 $params$，在该阶段结束时，$\mathcal{A}$ 输出两个合法的成员标识 ID_1，ID_2 和消息 M. 在第二阶段敌手得到随机签名者在 M 上的一个签名值. 敌手的最终目标是猜出签名值是使用哪个密钥所签署的，但猜中的概率是 1/2. 形式化表述为

$$Pr[params \leftarrow Setup(1^{\lambda}); (ID_1, ID_2, M, State) \leftarrow \mathcal{A}_1(params, K_{ID}); b \leftarrow \{0,1\}; \sigma \leftarrow Sign(params, K_{ID_b}, M); b' \leftarrow \mathcal{A}_2(params, K_{ID}): Verify(params, m, \sigma) = 1 \wedge b = b'] = \frac{1}{2}.$$

完全可追踪性. 完全可追踪性要求组内若干个成员不能密谋伪造签名，伪造的签名不能提取出合法的成员身份. 敌手 $\mathcal{A}$ 执行两个阶段操作：选择阶段和猜测阶段. 集合 G 中包含合法的用户 ID 与数量，选择阶段敌手通过不可靠的集合展开攻击，集合 G' 包含不可靠成员的身份标识和成员数量. 猜测阶段敌手尝试伪造一个在消息 M 上的签名 σ，如果是合法签名，追踪算法若能够输出身份标识 $ID' \in G$，则敌手攻击成功，否则失败. 形式化表述为

$$Pr[params \leftarrow Setup(1^{\lambda}); G' \leftarrow \mathcal{A}_1(params); \sigma' \leftarrow Sign(params, K_{ID^*}, M); ID' \leftarrow Trace(params, TK, \sigma'): Verify(params, m, \sigma') = 1 \wedge ID' \in G] = 0.$$

不可伪造性. 数字签名的基本要求是签名不能被伪造，即伪造的签名不能被验证算法所接受. 实际上不可伪造性包含在完全可追踪性中. 敌手可以通过签名预言机获得选择阶段的数字签名. 若敌手产生一个合法的签名 (m, σ)，并使用追踪算法追踪成员身份，算法输出均属于集合 G'，而实际上集合 G' 是一个空集合.

3.2　GSCOBG 方案设计

本节利用组合阶双线性群构建了一个高效组签名方案，方案中引入了 Groth 和 Sahai 提出的非交互式证明理论，并结合承诺方案加以构建. 图 1 描述了整个组签名方案的执行过程.

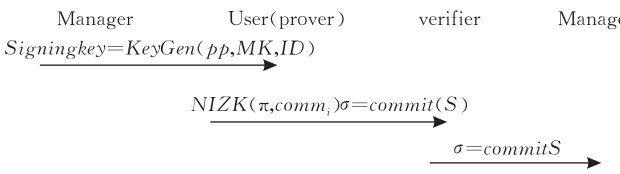

图 1　GSCOBG 组签名方案执行过程

初始化过程中，λ 是安全参数，身份信息 ID 和消息 M 可以分别表示成 k 位和 n 位的二进制串，要求 $k <= n \ll \lambda$，组内可以支持 2^k 个成员加入. G 是一个可交换的乘法群，阶为 $N = p_1 p_2 p_3$，其中 p_1，p_2，p_3 为素数，$e: G \times G \rightarrow G_T$ 为双线性映射.

$Setup(1^{\lambda})$. 令 G_{p_i} 是群 G 的一个子群，阶为 p_i，在群 G_{p_i} 中随机选择生成元 g，$v \leftarrow G_{p_1}^2$，$u \leftarrow G_{p_2}$，向量 $(u_1, \cdots, u_k) \leftarrow G_{p_1}^k$ 用于承诺用户 ID，$ID = (x_1, \cdots, x_k) \leftarrow \{0,1\}^k$；向量 $(v_1, \cdots, v_n) \leftarrow G_{p_1}^n$ 用于承诺签名消息 M，$M = (m_1, \cdots, m_n) \leftarrow \{0,1\}^n$，选择数 $\alpha \leftarrow \mathbb{Z}_N$. 因此公共参数为 $PP = \{N, g, u, u_1, \cdots, u_k, v, v_1, \cdots, v_n, A = e(g,g)^{\alpha}\}$，$MK = g^{\alpha} \leftarrow G$，$TK = p_2$ 公共参数不仅包括 pp 而且包括了 k，n 以及 (N, G, G_T, e) 的相关描述.

$KeyGen(PP, MK, ID)$. 系统为用户分配一个唯一标识 $ID = (x_1, \cdots, x_k) \leftarrow \{0,1\}^k$，并为其产生签名密钥，选择随机数 $r_1 \leftarrow \mathbb{Z}_N$，在群 G_{p_3} 中选择两个元素，R_3，$R_3' \leftarrow G_{p_3}^2$，可以通过 G_{p_3} 中的生成元和随机数计算产生. 由所选的元素计算用户 ID 的签名密钥如下：

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

并生成非交互式零知识证明 $\pi_1 = \left(u^{r_1} \prod_{i=1}^{k} u_i^{2x_i - 1} \right)^{r_1}$，用于向验证者证实自己的身份.

$Sign(PP, K_{ID}, M)$. 用户使用秘密的签名密钥 $K_{ID} = (K_1, K_2) \leftarrow G^2$ 对消息 M 进行签名. 选择随机数 $s \leftarrow \mathbb{Z}_N$，得到如下签名：

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

而 S_1，S_2，S_3 首先满足配对乘积等式：

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

因为以上签名中包含秘密签名密钥，所以根据 Groth-Sahai 的非交互式零知识证明理论，应对私密信息进行承诺，进而使得验证者确信承诺中包含私密信息. 按照 $NIZK$ 中的承诺方法，如果对群中元素 $x \leftarrow G$ 承诺，则将 x 的一一映射为 x'，选择随机数 $r_1, \cdots, r_I \leftarrow \mathbb{Z}_N^I$ 计算承诺值 $comm = x' \prod_{i=1}^{I} u_i^{r_i}$. 为了

方便最后的追踪,本方案中将 x 作为 x 的一一映射即 $x\rightarrow x$,从而简化承诺的复杂程度.

$Commit(pp,S)$. 本方案中需要对上述签名过程中产生的 3 个签名元素 S_1,S_2,S_3 以及 $u^{r_1}\prod_{i=1}^{k}u_i^{x_i}$, $v^{r_2}\prod_{j=1}^{n}v_j^{m_j}$ 进行承诺. 选择 $t,t_1,t_2,t_3\in\mathbb{Z}_N$ 对元组 S_1, $S_2,S_3,u^{ID}h_1,v^mh_2$ 承诺如下:

$$comm_1=S_1h^{t_1},\ comm_2=S_2h^{t_2},\ comm_3=S_3h^{t_3},$$

$$comm_4=u^{r_1}\prod_{i=1}^{k}u_i^{x_i}h^t,\ comm_5=v^{r_2}\prod_{j=1}^{n}v_j^{m_j}h^t,$$

并计算

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

最终签名由以下元组组成:

$$\sigma=(comm_1,comm_2,comm_3,comm_4,comm_5,\pi_2).$$

$Verify(PP,\sigma)$. 验证者收到签名后,利用公开参数对身份的证明和签名进行验证,如果身份和签名都满足验证等式,则验证通过,否则返回错误消息. 对身份进行验证时,令 $C=u^{r_1}\prod_{i=1}^{k}u_i^{x_i}$,只需验证等式 $e(C,C\prod_{i=1}^{k}u_i^{-1})=e(u,\pi_1)$ 是否成立,如果成立则继续对签名进行验证,否则返回错误消息. 对消息进行验证时只需验证下面等式是否成立:

$$e(comm_1,g)e(comm_2,comm_4)e(comm_3,comm_5)=A\cdot e(h,\pi_2),$$

如果等式成立则签名将被验证者所接受,否则返回错误消息.

$Trace(pp,C_i,TK)$. 当签名者对 $ID=x_1,\cdots,x_k\leftarrow\{0,1\}^k$ 的每一位进行承诺时,选择随机数 $r_{1_1},\cdots,r_{1_k}\leftarrow(\mathbb{Z}_N)^k$,而 $r=r_{1_1}+r_{1_2}+\cdots+r_{1_k}$,计算 $C_i=u^{r_{1_i}}\cdot u_i^{x_i}$ 使得 $C=C_1\cdot C_2\cdot\cdots\cdot C_n=u^{r_1}\prod_{i=1}^{k}u_i^{x_i}$. 当产生纠纷时,需要组管理者追踪签名者身份,组管理者使用追踪密钥 $TK=p_2$,通过计算 $(C_i)^{p_2}$ 的值恢复出 ID. 若 $(C_i)^{p_2}=1$(其中 1 为群 G 中的单位元),则 $x_i=0$;若 $(C_i)^{p_2}\neq1$,则 $x_i=1$. 进而依次恢复出用户身份信息 ID 所对应的二进制串.

4 安全性证明

定义 1. 如果 $(Setup,KeyGen,Sign,Verify)$ 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,且对于组成员身份的证明过程 $(Setup,KeyGen,Verify,Trace)$ 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证明系统,则该组签名方案是安全的.

定理 1. $Setup(1^k),KeyGen(PP,MK,ID)$, $Verify\ (PP,\sigma)$ 是一个具有正确性、不可伪造性、完全匿名性、完全可追踪性的组签名方案.

下面给出定理 1 的证明.

(1) 正确性.

正确性的证明包含 3 个部分:身份验证等式的正确性、最初签名验证等式的正确性、承诺以后最终签名验证等式的正确性,下面分别对以上 3 个等式进行验证.

若要证明对于身份的验证等式 $e\left(C,C\prod_{i=1}^{k}u_i^{-1}\right)=e(u,\pi_1)$ 成立,通过等式的左边可得

$$\begin{aligned}e\left(C,C\prod_{i=1}^{k}u_i^{-1}\right)&=e\left(u^{r_1}\prod_{i=1}^{k}u_i^{x_i},u^{r_1}\prod_{i=1}^{k}u_i^{x_i-1}\right)\\&=e(u^{r_1},u^{r_1})e\left(\prod_{i=1}^{k}u_i^{x_i},\prod_{i=1}^{k}u_i^{x_i-1}\right)\cdot\\&\quad e\left(u^{r_1},\prod_{i=1}^{k}u_i^{x_i-1}\right)e\left(u^{r_1},\prod_{i=1}^{k}u_i^{x_i}\right)\\&=e\left(u,\left(u^{r_1}\prod_{i=1}^{k}u_i^{2x_i-1}\right)^{r_1}\right)\prod_{i=1}^{k}\prod_{j=1}^{k}e(u_i,u_j)^{x_i(x_j-1)}\\&=e(u,\pi_1).\end{aligned}$$

签名算法中,组成员产生最初的签名包含 3 个签名值 (S_1,S_2,S_3),该三元组满足等式

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

若要证明该签名的验证等式成立,通过计算等式的左边可得

$$\begin{aligned}&e(S_1,g)e\left(S_2,u^{r_1}\prod_{i=1}^{k}u_i^{x_i}\right)e\left(S_3,v^{r_2}\prod_{j=1}^{n}v_j^{m_j}\right)\\&=e\left(g^{\alpha}\left(u^{r_1}\prod_{i=1}^{k}u_i^{x_i}\right)^{r_1}R_3\left(v^{r_2}\prod_{j=1}^{n}v_j^{m_j}\right)^{s},g\right)\cdot\\&\quad e\left((g^{r_1}R_3')^{-1},u^{r_1}\prod_{i=1}^{k}u_i^{x_i}\right)e\left(g^{-s},v^{r_2}\prod_{j=1}^{n}v_j^{m_j}\right)\\&=e(g^{\alpha},g)e(R_3,g)e\left((R_3')^{-1},u^{r_1}\prod_{i=1}^{k}u_i^{x_i}\right)\\&=e(g^{\alpha},g)=A.\end{aligned}$$

若元素 g' 是群 G 的一个生成元,根据组合阶双线性群的正交性,元素 $g'^{p_1p_2}$ 是群 G_{p_3} 的生成元,元素 $g'^{p_1p_3}$ 是群 G_{p_2} 的生成元,元素 $g'^{p_2p_3}$ 是群 G_{p_1} 的生成元. 假设 $h_1\in G_{p_1}$, $h_2\in G_{p_2}$,因此,对于 α_1,α_2, $h_1=(g'^{p_2p_3})^{\alpha_1}$ 和 $h_2=(g'^{p_1p_3})^{\alpha_2}$,可以推导出 $e(h_1,h_2)=e(g'^{p_2p_3\alpha_1},g'^{p_1p_3\alpha_2})=e(g'^{\alpha_1},g'^{p_3\alpha_2})^{p_1p_2p_3}=1$. 因此

很容易得出如下结论：在配对函数中的两个元素若来自群 G 的任意两个不同子群 G_{p_i}，则其配对函数值为单位元 1，从而配对函数 $e(R_3, g)$ 和 $e\left((R_3')^{-1}, u^{r_1}\prod_{i=1}^{k}u_i^{x_i}\right)$ 的值均为 1. 因此签名验证等式 $e(S_1, g)e\left(S_2, u^{r_1}\prod_{i=1}^{k}u_i^{x_i}\right)e\left(S_3, v^{r_2}\prod_{j=1}^{n}v_j^{m_j}\right)=A$ 满足正确性要求.

承诺后的签名值 $\sigma=(comm_1, comm_2, comm_3, comm_4, comm_5, \pi_2)$ 满足验证等式 $e(comm_1, g)\cdot e(comm_2, comm_4)e(comm_3, comm_5)=A\cdot e(h, \pi_2)$，为证明上述等式成立，计算等式的左边可以得出

$$e(comm_1, g)e(comm_2, comm_4)e(comm_3, comm_5)$$
$$=e(S_1h^{t_1}, g)e\left(S_2h^{t_2}, u^{r_1}\prod_{i=1}^{k}u_i^{x_i}h^{t}\right)e\left(S_3h^{t_3}, v^{r_2}\prod_{j=1}^{n}v_j^{m_j}h^{t}\right)$$
$$=e(g^{\alpha}, g)e\left(h, g^{t_1-r_1t-st}h^{t(t_2+t_3)}\left(u^{r_1}\prod_{i=1}^{k}u_i^{x_i}\right)^{t_2}\left(v^{r_2}\prod_{j=1}^{n}v_j^{m_j}\right)^{t_3}\right)$$
$$=A\cdot e(h, \pi_2).$$

因此可以得出三部分验证等式都是满足正确性的，从而整个签名方案满足正确性要求.

(2) 完全匿名性.

引理 1.　如果敌手 $\mathcal{A}$ 在多项式时间 t 内，可以以 ε 的概率攻破假设 1 或假设 2，则在多项式时间 t' 内，敌手 $\mathcal{A}$ 就可以以 $\geq\frac{\varepsilon}{2}$ 的概率攻破完全匿名性，其中 $t\approx t'$.

引理 1 的证明.　Waters 等人[25]提出了半适用性的概念，半适用性签名密钥 $K_1'=K_1\cdot g_2^{\gamma z_k}$，$K_2'=K_2\cdot g_2^{\gamma}$，$E_{k+1}=E_{k+1}'g^{\gamma z_{k+1}}$，…，$E_l=E_l'g^{\gamma z_l}$，半适用性签名：$comm_4'=comm_4\cdot g_2^{xz_s}$，$comm'=g'=g\cdot g_2^{x}$. 使用半适用性的签名和密钥可以得出 $e(g, g)^{\alpha}\cdot e(g_2, g_2)^{x\gamma(z_k-z_s)}$，如果 $z_k=z_s$ 则验证等式是成立的.

本节将使用 $Game$ 序列进行证明，其中 $Game_{\text{Real}}$ 是真实且安全的 $Game$ 序列，而 $Game_{\text{Restricted}}$ 序列相对于 $Game_{\text{Real}}$ 而言，对敌手询问做了一些限制，要求所有身份信息 ID 模 N 后的值是不相同的. q 表示敌手询问密钥的次数. k 从 0～q 中取值，定义 $Game_k$ 如下：

给定 $g, X_3, \mathcal{B}$ 可以使用算法 $\mathcal{A}$ 模拟 $Game_{\text{Real}}$，算法 $\mathcal{A}$ 产生身份标识 ID, ID^*，其满足 $ID\neq ID^* \bmod N$，并且 p_2 整除 $ID-ID^*$. 算法 $\mathcal{B}$ 使用上述 ID 计算有效解 $a=gcd(ID-ID^*, N)$. 令 $b=\frac{N}{a}$，有 p_2 整除 a，且 $N=ab=p_1p_2p_3$. 存在两种情况：p_1 整除 b，或 p_1 整除 a，从而有 $a=p_1p_2$，$b=p_3$. 其中之一会以 $\geq\frac{\varepsilon}{2}$ 的概率出现. 在情况 1 中算法 $\mathcal{B}$ 会攻破假设 1. 给定的 g, X_3，$\mathcal{B}$ 能够通过验证 g^b 是否是身份标识来判定 p_1 整除 b，然后验证 T^b 是否是身份标识，如果是身份标识，则 $T\in G_{p_1}$，反之，$T\in G_{p_1p_2}$. 情况 2 中，算法 $\mathcal{B}$ 攻破假设 2，给定 g, X_1X_2, X_3, Y_2Y，算法 $\mathcal{B}$ 能够通过验证 $(X_1X_2)^a$ 是身份标识来判定 $a=p_1p_2$，然后验证双线性函数 $e((Y_2Y_3)^b, T)$ 是否是身份标识，如果是，则 $T\in G_{p_1p_3}$，否则 $T\in G$.

然而敌手攻破假设 1 的概率是可忽略的，说明 $Game_{\text{Real}}$ 序列与 $Game_{\text{Restricted}}$ 序列是不可区分的，即 $Game_{\text{Real}}Adv_{\mathcal{A}}-Game_{\text{Restricted}}Adv_{\mathcal{A}}=0$，根据逆否命题的性质可以得出敌手攻破完全匿名性的概率为 $Adv_A<\frac{\varepsilon}{2}$.

(3) 不可伪造性.

不可伪造性的证明依赖于假设 1～3，以下引理说明 $Game_{\text{Restricted}}$ 序列与 $Game_0$ 序列是不可区分的，$Game_0$ 序列与 $Game_{k-1}$ 序列是不可区分的，以此类推，最终得出每个序列都是不可区分的.

引理 2.　假设如果存在算法 $\mathcal{A}$ 使得

$$Game_{\text{Restricted}}Adv_{\mathcal{A}}-Game_0Adv_{\mathcal{A}}=\varepsilon,$$

那么可以构造一个算法 $\mathcal{B}$ 以 $\geq\frac{\varepsilon}{2}$ 的概率攻破假设 1.

引理 2 的证明.　$\mathcal{B}$ 首先得到值 g, X_3, T 之后可以使用算法 $\mathcal{A}$ 模拟 $Game_{\text{Restricted}}$ 或 $Game_0$. $\mathcal{B}$ 算法选择随机数 $\alpha, a_1, \cdots, a_l, b\in Z_N$，计算 $g=g, u_i=g^{a_i}$，$h=g^b, i\in\{1, \cdots, l\}$，并将公共参数 $\{N, u_1, \cdots, u_l, g, h, e(g, g)^{\alpha}\}$ 发给 $\mathcal{A}$. 当攻击者询问算法 $\mathcal{B}$ 用户 $ID=(x_1, \cdots, x_k)$ 的密钥时，选择随机数 $r, t, w, v_j, \cdots, v_l\in Z_N$，计算 $K_1=g^{\alpha}\left(u^r\prod_{i=1}^{k}u_i^{x_i}\right)^rX_3^w$，$K_2=g^rX_3^tE_{k+1}=u_{k+1}^rX^{v_{k+1}}$，…，$E_l=u_l^rX_3^{v_l}$. 算法 $\mathcal{A}$ 发送给 $\mathcal{B}$ 两个消息，M_0, M_1 和一个挑战身份信息 $ID^*=(x_1^*, \cdots, x_k^*)$，算法 $\mathcal{B}$ 随机选择 $\beta\in\{0, 1\}$，产生签名 $comm_1=comm_{1\beta}$，$comm_4=T^{a_1x_1^*+\cdots+a_kx_k^*+b}$，$g'=T$. 若 $T\in G_{p_1p_2}$，那么签名是一个 $z_c=a_1x_1^*+\cdots+a_kx_k^*+b$ 的半适用性签名. 如果 $T\in G_{p_1}$ 这将是一个正常的签名，因此算法 $\mathcal{B}$ 可以使用算法 $\mathcal{A}$ 的输出区分 T.

引理 3.　如果存在一个算法 $\mathcal{A}$ 满足

$$Game_{k-1}Adv_{\mathcal{A}}-Game_kAdv_{\mathcal{A}}=\varepsilon,$$

那么可以构造一个算法 $\mathcal{B}$ 以 ε 的概率攻破假设 2.

引理 3 的证明.　算法 $\mathcal{B}$ 得到 g, X_1X_2, X_3, Y_2Y_3，

T,选择随机数 $a_1,\cdots,a_l,b\in Z_N$,并设置公共参数为 $g=g,u_i=g^{a_i},h=g^b,e(g,g)^\alpha$,并发给算法 $\mathcal{A}$,当攻击者询问身份为 ID 的第 i 位信息,$i<j$,算法 $\mathcal{B}$ 创建一个半适用性密钥,同时选择随机数 $r,t,z_{k+1},\cdots,z_l\in Z_N$,计算:$K_1=g^\alpha\left(u^r\prod_{i=1}^{k}u_i^{x_i}\right)^r(Y_2Y_3)^z$,$K_2=g^r(Y_2Y_3)^t$,$E_{k+1}=u_{k+1}^r(Y_2Y_3)^{z_{k+1}},\cdots,E_l=u_l^r(Y_2Y_3)^{z_l}$,通过 $g_2^\gamma=Y_2^t$ 产生半适用性密钥.对于 $i>j$,算法 $\mathcal{B}$ 产生正常的密钥.为了建立身份信息 $ID=(x_1,\cdots,x_k)$ 第 j 次密钥询问,使用随机数 $w_k,w_{j+1},\cdots,w_l\in\mathbb{Z}_N$ 产生密钥 $K_1=g^\alpha T^{z_k}X^{w_{k3}}$,$K_2=T$,$E_{k+1}=T^{a_{j+1}}X^{w_j+1},\cdots,E_l=T^{a_l}X_3^{w_l}$.如果 $T\in G_{p_1p_3}$ 则上述密钥为正常密钥,如果 $T\in G$ 则为半适用性密钥.在某一时刻,算法 $\mathcal{A}$ 发送给 $\mathcal{B}$ 两个消息 M_0,M_1 和一个挑战身份 $ID^*=(x_1^*,\cdots,x_k^*)$.算法 $\mathcal{B}$ 随机选择 $\beta\in\{0,1\}$,构成的签名表示为如下形式:$comm_1=comm_{1\beta}$,$comm_4=(X_1X_2)^{a_1x_1^*+\cdots+a_kx_k^*+b}$,$g'=X_1X_2$.如果 $T\in G_{p_1p_3}$,算法 $\mathcal{B}$ 能够模拟出 $Game_{k-1}$,如果 $T\in G$,$\mathcal{B}$ 能够模拟出 $Game_k$,因此 $\mathcal{B}$ 能够使用算法 $\mathcal{A}$ 的输出区分出 T.

引理 4. 如果存在一个算法 $\mathcal{A}$ 满足

$$Game_qAdv_{\mathcal{A}}-Game_{\text{Final}}Adv_{\mathcal{A}}=\varepsilon,$$

那么可以构造一个算法 $\mathcal{B}$ 以 ε 的概率攻破假设 3.

引理 4 的证明. 算法 $\mathcal{B}$ 得到 $g,g^\alpha X_2,X_3,g^sY_2,Z_2,T$,算法 $\mathcal{B}$ 选择随机数 $a_1,\cdots,a_l,b\in Z_N$,设置公共参数 $g=g,u_i=g^{a_i},h=g^b$,$e(g,g)^\alpha=e(g^\alpha X_2,g)$,并发给 $\mathcal{A}$,当 $\mathcal{A}$ 询问用户 $ID=(x_1,\cdots,x_k)$ 的密钥时,算法 $\mathcal{B}$ 产生一个半适用性密钥,选择随机数 $c,r,t,w,z,z_{k+1},\cdots,z_l,w_{j+1},\cdots,w_l\in\mathbb{Z}_N$,计算:

$$K_1=g^\alpha\left(u^{r_i}\prod_{i=1}^{k}u_i^{x_i}\right)^{r_i}X_2Z_2^cX_3^w,\ K_2=g^rZ_2^zX_3^t,$$

$$E_{k+1}=u_{k+1}^r(Z_2)^{z_{k+1}}X_3^{w_{j+1}},\cdots,E_l=u_l^rZ_2^{z_l}X_3^{w_l},$$

算法 $\mathcal{A}$ 发送给 $\mathcal{B}$ 两个消息,M_0,M_1 和一个挑战身份信息 $ID^*=(x_1^*,\cdots,x_k^*)$,算法 $\mathcal{B}$ 随机选择 $\beta\in\{0,1\}$,产生签名 $comm_1=comm_{1\beta}$,$comm_4=(g^sY_2)^{a_1x_1^*+\cdots+a_kx_k^*+b}$,$g'=g^sY_2$.如果 $T=e(g,g)^\alpha$,那么该签名就是对于消息 M_β 的半适用性签名.如果 T 是 G_T 中的一个元素,那么该签名是对随机消息产生的签名.因此算法 $\mathcal{B}$ 使用算法 $\mathcal{A}$ 的输出可以区分 T.

如果假设 1,2 和假设 3 成立,那么通过上述引理可以得出真实的安全 $Game$ 序列与 $Game_{\text{Final}}$ 序列是不可区分的,这表明 β 值对于攻击者而言是隐藏的,因此,攻击者攻伪造一个组签名方案的概率是一个可忽略的函数.

(4) 完全可追踪性.

完全可追踪性的证明,基于上述签名的不可伪造性,构造一个模拟器 $\mathcal{B}$ 与敌手 $\mathcal{A}$ 进行组签名 $Game$ 序列的交互.

引理 5. 如果存在一个敌手在多项式时间 t 内可以以概率 ε 攻破组签名的完全可追踪性,则存在一个敌手在 t' 时间内可以以概率 ε 攻破签名的不可伪造性,其中 $t\approx t'$.

引理 5 的证明. 在初始化算法中,$\mathcal{B}$ 产生公共参数,将追踪密钥 TK 发送给敌手 $\mathcal{A}$,敌手得到提取的权限.在模拟器与敌手的交互过程中,如果敌手 $\mathcal{A}$ 询问某一用户 ID 的签名密钥,则模拟器 $\mathcal{B}$ 通过询问签名预言机获得用户 $ID=(x_1,\cdots,x_k)$ 的签名密钥 (K_1,K_2),然后将其发送给敌手 $\mathcal{A}$.敌手询问在身份信息为 $ID=(x_1,\cdots,x_k)$ 的用户在消息 $M=(m_1,\cdots,m_n)$ 上的签名,$\mathcal{B}$ 得到签名 $S=(S_1^*,S_2^*,S_3^*)$,$\mathcal{B}$ 选择随机数 $t,t_1,t_2,t_3\in\mathbb{Z}_N$ 生成最终的签名 $\sigma=(S_1^*h^{t_1},S_2^*h^{t_2},S_3^*h^{t_3},u^{r_1}\prod_{i=1}^{k}u_i^{x_i}h^t,v^{r_2}\prod_{j=1}^{n}v_j^{m_j}h^t)$,该签名的合法性可以通过追踪密钥 TK 最终能否提取出组内一个合法的身份来验证.

某时刻,敌手 $\mathcal{A}$ 可以通过自己掌握的知识伪造用户 $ID^*=(x_1^*,\cdots,x_k^*)$ 在消息 $M^*=(m_1^*,\cdots,m_n^*)$ 的签名 $\sigma^*=(comm_1^*,comm_2^*,comm_3^*,comm_4^*,comm_5^*,\pi^*)$,模拟器产生 λ,其中 λ 满足 $\lambda\equiv1(\bmod p_1)$ 且 $\lambda\equiv0(\bmod p_2p_3)$.

而 $comm_1^{*\lambda},comm_2^{*\lambda},comm_3^{*\lambda},comm_4^{*\lambda},comm_5^{*\lambda},\pi^{*\lambda}$ 满足如下验证等式:

$$e(comm_1^{*\lambda},g)e(comm_2^{*\lambda},comm_4^{*\lambda})e(comm_3^{*\lambda},comm_5^{*\lambda})=A\cdot e(h,\pi_2^{*\lambda}).$$

因此证明敌手可以伪造出用户签名,而在引理 2～4 中已经证明出签名的不可伪造性,所以该结论与假设相矛盾,从而得出引理 5 的正确性.至此,定理 1 得证. 证毕.

定理 2. $Setup(1^k)$,$KeyGen(PP,MK,ID)$,$Verify(PP,\sigma)$,$Trace(pp,\sigma)$ 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. 正确性已经在定理 1 中得到证明,下面主要证明该非交互式证明系统的其它特性.

(1) 合理性.

已知验证等式 $e\left(C,C\prod_{i=1}^{k}u_i^{-1}\right)=e(u,\pi_1)$ 成立,

通过计算可得

$$e\left(C,C\prod_{i=1}^{k}u_i^{-1}\right)=e\left(u^{r_1}\prod_{i=1}^{k}u_i^{x_i},u^{r_1}\prod_{i=1}^{k}u_i^{x_i-1}\right)$$
$$=e\left(u,\left(u^{r_1}\prod_{i=1}^{k}u_i^{2x_i-1}\right)^{r_1}\right)\prod_{i=1}^{k}\prod_{j=1}^{k}e(u_i,u_j)^{x_i(x_j-1)}.$$

u 的阶为 p_2，所对应的配对 $e\left(u,\left(u^{r_1}\prod_{i=1}^{k}u_i^{2x_i-1}\right)^{r_1}\right)$ 的阶为 1 或 p_2，从验证等式 $e\left(C,C\prod_{i=1}^{k}u_i^{-1}\right)=e(u,\pi_1)$ 中可以得出 $e\left(C,C\prod_{i=1}^{k}u_i^{-1}\right)$ 的阶为 1 或 p_2，因此 $\prod_{i=1}^{k}\prod_{j=1}^{k}e(u_i,u_j)^{x_i(x_j-1)}$ 的阶为 1 或 p_2，而 u_i 是 G_{p_1} 的生成元，其阶为 p_1，所以 $x_i=0$ 或 $x_i=1$.

(2) 证据不可区分性.

当签名者对 $ID=x_1,\cdots,x_k\leftarrow\{0,1\}^k$ 的每一位进行承诺时，选择随机数 $r_{1_1},\cdots,r_{1_k}\leftarrow(\mathbb{Z}_N)^k$，而 $r=r_{1_1}+r_{1_2}+\cdots+r_{1_k}$，计算 $C_i=u^{r_{1_i}}\cdot u_i^{x_i}$，使得 $C=C_1\cdot C_2\cdot\cdots\cdot C_n=u^{r_1}\prod_{i=1}^{k}u_i^{x_i}$. 对于每一位的承诺值而言，令 $C_i=u^{r_{1_i}}\cdot u_i^0=u^{r'_{1_i}}\cdot u_i^1$，产生唯一的证明 π，满足验证等式 $e(C_i,C_iu_i^{-1})=e(u_i,(u_i^{2x_i-1}u^{r_i})^{r_i})=e(u_i,\pi)$. 因此对于承诺值相同的不同承诺对象而言，生成的证明 $\pi=(u^{r'_{1_i}}\cdot u_i^1)^{r'_{1_i}}=u^{r_{1_i}r'_{1_i}}=(u_i^{-1}u^{r_{1_i}})^{r_{1_i}}$ 的值是相等的，具有证据不可区分性.

(3) 可追踪性.

可追踪性证明包含隐藏性和绑定性两部分.

隐藏性. 若验证者已知承诺值为 $C_i=u^{r_{1_i}}\cdot u_i^{x_i}$，并不能从中得到签名者的签名密钥以及身份信息 x. 在组签名方案中生成参数时，根据假设 1 可知 u 与 $u'\notin G_{p_2}$ 在计算上是不可区分的. 通过计算 $C_i=u^{r_{1_i}}\cdot u_i^{x_i}$ 所得的承诺值，根据假设 1，不存在多项式时间内的敌手分辨出究竟使用的是 $u^{r_{1_i}}$ 还是 $u'^{r_{1_i}}$. 若使用 $u'^{r_{1_i}}$ 时使用追踪密钥 $TK=p_2$，C 可变形为 $C_i=u'^{r_{1_i}}\cdot u_i^{x_i}=u_i^{x'_i}\cdot u'^{r_{1_i}-(x'_i-x_i)/\alpha_2}$，其中 $g'^{p_1p_3\alpha_2}\in G_{p_2}$，$g'\in G$，$u'=u_i^{\alpha_2}$ 通过追踪方式打开 C_i 得到的可为任意值，计算过程如下：

$$C_i^{p_2}=(u'^{r_{1_i}}\cdot u_i^{x_i})^{p_2}=(u_i^{x'_i}\cdot u'^{r_{1_i}-(x'_i-x_i)/\alpha_2})^{\alpha_2}$$
$$=u_i^{x'_i\alpha_2}u'^{r_{1_i}\alpha_2-x'_i+x_i}=u_i^{x'_i\alpha_2}u_i'^{r_{1_i}\alpha_2^2-x'_i\alpha_2+x_i\alpha_2}$$
$$=u_i^{r_{1_i}\alpha_2^2+x_i\alpha_2}=(u_i^{\alpha_2})^{r_{1_i}\alpha_2}u_i^{\alpha_2x_i}=u'^{r_{1_i}\alpha_2}u'^{x_i}.$$

绑定性. 承诺值 C_i 与承诺对象身份 x_i 是一一对应的，即不存在两个 x_i 承诺后生成相同的承诺值. 使用 $C_i=u^{r_{1_i}}\cdot u_i^{x_i}$ 构建承诺值，根据假设 1，C_i 与 x_i 值一一对应. 若给出 $u\in G_{p_2}$ 时使用追踪密钥 $TK=p_2$ 可以从 C_i 中提取出承诺对象 x_i，即 $(C_i)^{p_2}=(u^{r_{1_i}}\cdot u_i^{x_i})^{p_2}=(u_i^{p_2})^{x_i}$，如果 $(C_i)^{p_2}=1$，则 $x_i=0$；如果 $(C_i)^{p_2}\neq1$，则 $x_i=1$，从而依次恢复出唯一的用户身份信息 ID 对应的二进制串.　　证毕.

5　分析与比较

本节将 GSCOBG 方案与同类其它方案在安全性和效率两方面分别作了比较，表 1 是本文方案与上文提到的基于 BMW 模型和 BSZ 模型的系列组签名方案的安全性对比.

表 1　安全性对比

方案	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
ACHdM[21]	×	√	×	×	√	×	×	×
BW06[11]	√	√	×	×	√	×	√	×
BW07[12]	√	√	√	√	√	×	×	×
LV09[14]	√	√	√	×	×	√	√	√
WL10[15]	×	√	×	×	×	√	√	√
本文方案	√	√	√	√	√	×	√	×

表 2 是对提出的 GSCOBG 方案的效率分别从通信次数、通信代价、计算代价三个方面进行分析. 通过计算，本文提出的组签名方案的 6 个算法中共使用群中元素 $2k+14$ 个(其中 k 为消息串的长度)，随机数 12 个，幂运算 $k+26$ 个，配对运算 9 个. 由于配对的计算较复杂，所以在效率分析上应该作为主要的考虑因素.

表 2　效率对比

方案	通信次数	通信代价		计算代价		
		G 中元素	Z_N 中元素	求幂	点乘	配对
ACHdM[21]	5	20	$6+l$	40	5	19
BW06[11]	3	$4k+12$	$4k+6$	$k+10$	$2k+6$	$k+4$
BW07[12]	3	$k+22$	11	$2k+3$	$2k+12$	14
VLRGS[14]	3	$2k+38$	$k+12$	$k+21$	$k+23$	22
WL[15]	5	$3k+4$	7	27	7	12
本文方案	3	$2k+14$	12	$k+26$	$4k+12$	9

本文将提出的 GSCOBG 方案与同类的其它组签名方案进行了对比，通过表 1 和表 2 可以得出以下结论：GSCOBG 方案在交互次数方面优于交互式的方案 ACHdM[21] 和文献[15]中的方案，在通信代价方面整体优于文献[11,14]中的方案，在计算代价方面优于非交互式组签名方案 BW07[12]，在配对的计算量方面优于文献[11-12,14-15,21]中的方案.

6 总 结

本文使用组合阶双线性群构建了一个基于 BMW 模型的高效组签名方案，在方案中引进了 Groth-Sahai 证明系统的思想，并提供了严格的安全性证明，最后分别从安全性和效率两方面将该方案与同类其它组签名方案做出对比，从而得出该方案在效率和安全性上的优势. GSCOBG 方案，解决了传统组签名的通信效率低、不能抵抗选择密文攻击等问题. 此外，签名的大小是一个常量，不依赖于其它系统参数. 同时 GSCOBG 方案也存在不足之处，比如没有提供完整的成员撤销机制等问题，这需要在今后的工作中得以继续完善.

参 考 文 献

[1] Chaum D, Van Heyst E. Group signatures//Proceedings of the CRYPTO. Santa Babara, California, USA, 1991: 257-265

[2] Boneh D, Shacham H. Group signature with verifier-local revocation//Proceedings of the ACM CCS. Washington, DC, USA, 2004: 168-177

[3] Ateniese Giuseppe, Song Dawn, Tsudik Gene. Quasi-efficient revocation of group signatures//Proceedings of the Financial Cryptography. Southampton, Bermuda, 2002: 183-197

[4] Camenisch Jan, Lysyanskaya Anna. Dynamic accumulators and application to efficient revocation of anonymous credentials//Proceedings of the CRYPTO. Santa Barbara, California, USA, 2002: 61-76

[5] Boneh Dan, Boyen Xavier, Shacham Hovav. Short group signatures//Proceedings of the CRYPTO. Santa Barbara, California, USA, 2004: 41-55

[6] Canetti Ran, Goldreich Oded, Halevi Shai. The random oracle methodology, revisited//Proceedings of the Annual ACM Symposium on Theory of Computing. New York, USA, 1998: 209-218

[7] Goldwasser Shafi, Kalai Yael Tauman. On the (in) security of the Fiat-Shamir paradigm//Proceedings of the Annual IEEE Symposium on Foundations of Computer Science. Cambridge, MA, USA, 2003: 102-113

[8] Bellare Mihir, Boldyreva Alexandra, Palacio Adriana. An uninstantiable random-oracle-model scheme for a hybrid encryption problem//Proceedings of the EUROCRYPT. Interlaken, Switzerland, 2004: 171-188

[9] Canetti Ran, Goldreich Oded, Halevi Shai. On the random-oracle methodology as applied to length-restricted signature schemes//Proceedings of the IACR Theory of Cryptography Conference. Cambridge, MA, USA, 2004: 40-57

[10] Bellare Mihir, Micciancio Daniele, Warinschi Bogdan. Foundations of group signatures: Formal definitions, simplified requirements, and a construction based on general assumptions//Proceedings of the EUROCRYPT. Warsaw, Poland, 2003: 614-629

[11] Boyen Xavier, Waters Brent. Compact group signatures without random oracles//Proceedings of the EUROCRYPT. Saint Petersburg, Russia, 2006: 427-444

[12] Boyen Xavier, Waters Brent. Full-domain subgroup hiding and constant-size group signatures//Proceedings of the Public Key Cryptography. Beijing, China, 2007: 1-15

[13] Wang S H, Wang M Q. An efficient group signature scheme without random oracles//Proceedings of the CIS. Harbin, China, 2007: 807-810

[14] Libert Benoît, Vergnaud Damien. Group signatures with verifier-local revocation and backward unlinkability in the standard model//Proceedings of the 8th International Conference on Cryptology and Network Security. Springer, 2009: 498-517

[15] Wei Lingbo, Liu Jianwei. Shorter verifier-local revocation group signature with backward unlinkability//Proceedings of the International Conference on Pairing-Based Cryptography. Yamanaka Hot Spring, Japan, 2010: 136-146

[16] Groth Jens, Ostrovsky Rafail, Sahai Amit. Perfect non-interactive zero-knowledge for NP//Proceedings of the EUROCRYPT. Saint Petersburg, Russia, 2006: 339-358

[17] Waters Brent. Efficient identity-based encryption without random oracles//Proceedings of the EUROCRYPT. Aarhus, Denmark, 2005: 114-127

[18] Groth Jens, Ostrovsky Rafail, Sahai Amit. Non-interactive zaps and new techniques for nizk//Proceedings of the CRYPTO. Santa Barbara, California, USA, 2006: 97-111

[19] Groth Jens, Ostrovsky Rafail, Sahai Amit. Perfect non-interactive zero-knowledge for NP//Proceedings of the EUROCRYPT. Saint Petersburg, Russia, 2006: 339-358

[20] Bellare M, Shi H, Zhang C. Foundations of group signatures: The case of dynamic groups//Proceedings of the Topics in Cryptology—CT-RSA. Springer, 2005: 136-153

[21] Ateniese G, Camenisch J, Hohenberger S, De Medeiros B. Practical group signature without random oracles. Cryptology ePrint Archive, http://eprint. iacr. org/2005/385. pdf, 2011-12-13

[22] Echizen I, Kunihiro N, Sasaki R. Group signature implies PKE with non-interactive opening and threshold//Proceedings of the International Workshop on Security. Kobe, Japan, 2010: 181-198

[23] Lewko A, Waters B. New techniques for dual system encryption and fully secure HIBE with short ciphertexts//Proceedings of the IACR Theory of Cryptography Conference. ETH Zurich Zurich, Switzerland, 2010: 455-479

[24] Groth Jens, Sahai Amit. Efficient non-interactive proof systems for bilinear groups//Proceedings of the EUROCRYPT. Istanbul, Turkey, 2008: 415-432

[25] Lewko A, Waters B. New techniques for dual system encryption and fully secure HIBE with short ciphertexts//Proceedings of the TCC 2010. ETH Zurich Zurich, Switzerland, 2010: 455-479

ZHOU Fu-Cai, born in 1964, Ph.D., professor, Ph. D. supervisor. His main research interests include cryptography and network security, trusted computing, basic theory and critical technology in electronic commerce.

XU Jian, born in 1978, Ph. D. candidate, lecturer. His main research interests include cryptography and network security, data and identity authentication technology.

WANG Lan-Lan, born in 1986, M. S. candidate. Her main research interests include group signature and non-interactive zero knowledge proof.

CHEN Chen, born in 1987, M. S. candidate. Her main research interests include cryptography and network security, non-interactive zero knowledge proof.

LI Fu-Xiang, born in 1984, Ph. D. candidate. His main research interests include cryptography and data authentication.

Background

Group signature schemes as a way to provide anonymity for signers within a group, introduced by Chaum and van Heyst in 1991, allows members to make signatures on behalf of the group. The first group signature model in the Standard Model(SM), which is called BMW model, was proposed by Bellare who presented a universal structure and security requirements of group signature, and introduced Non-Interactive Zero Knowledge (NIZK) proof theory in the process of signature.

There were many group signature schemes based on the BMW model, among which Boyen and Waters proposed a scheme in 2005, whose security proof relied on the SM. They combined secure hierarchical signatures from an efficient identity-based encryption system in composite order bilinear groups with a mechanism of the NIZK proofs of Groth, Ostrovsky, and Sahai. However, their group signature was only secure against chosen-plaintext attacks but not for chosen-ciphertext attacks, and the number of group elements depended on the number of signers. Later, in 2007 Boyen et al. gave a new construction of the group signature scheme that addressed the drawbacks of the Boyen-Waters solution. They introduced NIZK proof theory of Jens Groth, and enhanced the efficiency as well. L. V. et al. proposed a scheme by utilizing the 3rd example-DLIN of Groth-Sahai proof system, presented the unlinkability proof, and solved the certificate revoking mechanism of the group member. However, it was not suitable for practice due to high computational cost of the non-interactive proof system. Furthermore, without being provided with reasonable tractable mechanism, it was impossible for them to solve unforgeability and non-repudiation problem.

Lewko Allison et al. proposed composite order (of 3 primes) bilinear groups theory in 2010, introduced proved secure assumptions, which were independent from the hierarchy and times of the adversary queries. They constructed a HIBE encryption scheme applying the proposed theory, which was proved to be full secure, and can solve the incapability of using label and ciphertext compression in the HIBE system. In this paper, we introduced an efficient group signature scheme based on BMW model, using the composite order (of 3 primes) bilinear groups theory and HIBE encryption scheme, which met the security requirements of full anonymity and full extractionality defined in the BMW model. In addition, we applied the NIZK proof idea in group signature scheme, both solving the CCA problem and ensuring the signature security and communication efficiency using the one-way interaction.

This research work was supported by the National High Technology Research and Development Plan (863) under Grant No. 2009AA01Z122, the Liaoning BaiQianWan Talents Program No. 2011921071 and the Natural Science Foundation of Shenyang City of China under Grant No. F10-205-1-12.