支持 LSSS 访问结构的属性基群签名方案的研究

许玉岚,陈燕俐,高诗尧
(南京邮电大学 计算机学院、软件学院、网络空间安全学院,江苏 南京 210003)

摘 要:群签名通过只能验证签名是由群中某一成员签署,但不能确定具体签名者身份来保证匿名性,同时在发生争议时,群管理员可以通过揭示签名者的身份来保证可追踪性。属性基群签名是对群签名的扩展,在保证只有具有特定属性集的群成员可对信息进行签名的同时实现了可追踪性,针对现有的属性基群签名方案仅支持访问树和门限访问结构,提出了一种可支持线性秘密分享(linear secret sharing schemes,LSSS)访问结构,并可实现属性匿名和追踪的属性基群签名方案。方案利用 Waters 签名技术和 Groth-Sahai 非交互证明构造群签名,保证只有满足 LSSS 访问结构属性集合的群用户才可对消息进行签名,并利用承诺系统保证了属性的匿名性和可追踪性,不仅可以追踪到签名用户的身份和属性集,还可以追踪到签名属性集合。方案的通信开销和计算开销较低,签名长度和验证计算开销都和属性的数量无关。最后的安全性证明和性能分析证明了方案的安全性和有效性。

关键词:群签名;属性基;访问结构;属性匿名;可追踪性
中图分类号:TP309 **文献标识码**:A **文章编号**:1673-629X(2021)09-0092-07
doi:10.3969/j.issn.1673-629X.2021.09.016

Research on Attribute-based Group Signature Scheme Supporting LSSS Access Structure

XU Yu-lan,CHEN Yan-li,GAO Shi-yao
(School of Computer Science,Nanjing University of Posts and Telecommunications,Nanjing 210003,China)

Abstract:A group signature can only verify that the signature is signed by a member of the group,but the identity of the specific signer cannot be determined to guarantee anonymity. Meanwhile,in case of dispute,the group administrator can guarantee traceability by revealing the identity of the signer. Attribute base group signature is an extension of group signature,which guarantees that only group members with specific attribute set can sign information and at the same time implements traceability. Because the existing property group signature scheme only supports access threshold access and tree structure,we propose a access structure of LSSS (linear secret sharing schemes) and can realize the attributes of anonymous and track the group signature scheme. In this scheme,the Waters signature technology and Groth-Sahai non-interactive proof are used to construct a group signature,which ensures that only group users who satisfy the attribute set of LSSS access structure can sign the message,and use the commitment system to ensure the properties of anonymity and traceability of attributes. The scheme can not only track the user's identity and attribute sets,but also track the signature attribute set. The communication and computation costs of the scheme are low,and the signature length and verification calculation cost are independent of the number of attributes. Finally,the security proof and performance analysis show the safety and effectiveness of the scheme.

Key words:group signature;attribute-based;access structure;attribute anonymity;traceability

0 引 言

属性基群签名(attribute-based group signature,ABGS)是对传统群签名(group signature,GS)的一种扩展,通过对群成员的身份特征进行划分,赋予用户不同的“属性”,这些“属性”可以用来标识群成员所拥有的权限,因此可以通过规定具有某些属性的群成员签署签名,来对签名者的权限进行限制,不符合要求的群成员生成的签名将被验证为无效签名。因为属性基群签名是将基于属性的签名[1](attribute based signature,ABS)与传统的群签名相结合,因此访问结构的选择与

收稿日期:2020-09-21 **修回日期**:2021-01-25
基金项目:国家自然科学基金资助项目(61572263,61272084)
作者简介:许玉岚(1995-),男,硕士研究生,研究方向为基于属性的签名;通信作者:陈燕俐(1971-),女,教授,硕导,博士,研究方向为信息安全。

方案的好坏有着直接的关系。而目前属性基的群签名都是基于访问树结构的情况,树结构能够表示灵活的访问控制策略,但其安全性证明仅基于一般的群假设,但因为访问结构表示为一棵树,因此需要使用递归来进行运算。而递归的深度达到一定的程度时,程序的运行时间空间将受到一定影响。而 LSSS 访问结构很好地解决了这个问题。LSSS 利用线性秘密分享方案的秘密可线性重组的性质重构秘密,不需要进行递归操作,提高了属性基签名方案的签名和效率,并且 LSSS 与访问控制树的表达性相当。因此,文中首次提出了一个支持 LSSS 访问结构的属性基群签名方案。

1　相关工作

1.1　群签名

自 Chaum 和 Heyst[2] 首次提出了群签名的概念,学者对群签名方案的研究包括增加各种功能,定义不同的安全概念以及提高方案的性能。

2000 年,Ateniese、Caneniseh、Joye 和 Tsudik[3] 使用交互的零知识证明(non-interactive zero-knowledge proof,NIZK)构造出第一个高效的、抗联合攻击的群签名方案,并且给出了随机预言模型下的安全性证明。Bellare,Micciancio 等人[4] 给出群签名的两个核心安全性质为强匿名性和强可追踪性。简化了群签名方案的安全性证明,即只需证明方案满足这两个安全性质。

2007 年,Boyen,Waters[5] 在标准模型下提出了群签名,该方案的基本思想是基于层次签名,即成员证书是第一层签名(即 GM 对用户身份的签名),利用第一层签名作为密钥,用户可生成第二层签名(即对某信息的签名),此签名还不可作为群签名,还需利用承诺方案对签名进行匿名化,最后利用标准模型下的 NIZK 证明承诺中的隐藏内容是合法的签名。

2019 年,李雪莲等人[6] 提出适合群成员数量较大的动态群签名,该方案利用群管理员或群成员本人与撤销图灵机通信,图灵机确定其身份后将撤销令牌添加到撤销列表即完成了撤销操作。2020 年,叶青,杨晓孟等人[7] 提出 NTRU 格上抗量子攻击的群签名方案,该方案利用 NTRU 格密码体制所需公私钥长度更短,运算速度更快的特点,构建了一个系统公钥长度小,计算效率高的群签名方案。张绪霞等人[8] 于 2020 年提出一个基于中国剩余定理的前向安全群签名方案,该方案可以动态地增加和删除群用户成员而无须频繁更改群公钥,并在验证签名和打开签名时只需要进行模运算即可实现,同时针对密钥泄露问题实现了前向安全性。欧海文等人[9] 于 2020 年提出一种具有前向和后向安全性的高效群签名方案,通过添加随机数的方式打破了公钥状态列表中公钥和私钥的直接联系,规避了被撤销成员联合得出其他成员私钥的风险,且群成员私钥随时间段跨越而自然更新(群管理员的私钥也因应改变),避免以往群成员发生私钥泄漏后需要重新选取密钥对才能保证后续签名安全性的繁琐过程。

1.2　属性基群签名

2007 年,Khader[10] 将传统的群签名方案进行了扩展,利用属性基的签名技术与群签名方案相结合,提出了属性基群签名。和属性基签名方案相同,用户是由属性集合表示,所以验证者并不知道群中用户的身份信息,只知道其相关属性,这样做到了对用户身份信息的隐私保护。与一般属性基方案不同的是,属性基群签名中的签名者在需要的时候可以由群管理员揭示。2008 年,Khader 在文献[11]中对上一方案进行了改进,实现了对群中用户的撤销和对属性的删除操作,使之更接近实际应用。

Emura 等人[12] 于 2009 年提出了动态的属性基群签名方案,其中允许访问结构树可变。2013 年,Syed,Amberker[13] 等人提出了一种具有属性匿名性和具有恒定签名大小的跟踪功能的 ABGS 方案,并证明了它在标准模型中的安全性。该方案的构造使用成员资格证书格式来实现标准模型中的不可陷害性,并使用 Groth-Sahai[14] 非交互式证明系统为标准模型下的群签名中的关系生成非交互式目击者不可区分性(NIWI)证明。

2017 年,基于 Merkle 类的访问树,Kuchta[15] 等人首次给出了基于格的属性基群签名方案,该方案同时具有加入和撤销机制,但该方案撤销成员时需要更新哈希树,计算复杂且耗时较长,并且该方案的签名长度与群成员数量相关。2019 年 Perera,Nakamura 等人[16] 提出了一种具有高效跟踪机制的新型 VLR-ABGS 方案。使用静态群签名方案中使用的跟踪算法来跟踪签名者及其在该方案中用于签名的属性。还使用群管理员的公钥来加密签名者的身份及其属性。因此,只有群管理员才能识别签名者和签名者的属性。2020 年张彦华等人[17] 针对本地验证者撤销的属性基群签名群公钥尺寸过长、空间效率不高的问题,采用身份编码技术对群成员身份信息进行编码,减少群公钥长度,通过单向和单射的带误差学习函数来完成撤销。

1.3　文中贡献

文中提出一种支持 LSSS 访问结构的属性基群签名方案,具体贡献如下:

(1)方案签名采用 LSSS 访问结构,效率更高。因为访问结构需要使用递归来进行运算,递归的深度达到一定的程度时,程序的运行时间空间将受到一定影响。本方案利用线性秘密分享方案的秘密可线性重组

的性质重构秘密,不需要进行递归操作,且 LSSS 与访问控制树的表达性相当。

(2)实现了签名属性匿名性且签名长度固定。一般属性基群签名中将签名属性与签名一起发送给验证者,方案利用 Groth-Sahai 非交互式证明系统实现了签名属性的匿名性。并且方案使签名长度和计算开销是固定值,与签名者的属性数量无关,减少了通信和计算开销。

(3)实现了属性可追踪性。在上述具有属性匿名性的 ABGS 方案的基础上,提出了属性追踪,在发生用户滥用签名权限时,不但可以追踪到用户的身份,还可以追踪到用户具有的属性和签名的属性。

2 预备知识

定义 1. 双线性映射(bilinear maps)[3]:设 G_1, G_2, G_T 是阶为素数 p 的乘法循环群, g_1, g_2 分别是 G_1, G_2 的生成元,存在一个具有如下性质的双线性映射 $e: G_1 \times G_2 \rightarrow G_T$:

(a)双线性:对于任意的 $u \in G_1, v \in G_2, a, b \in Z_p$,有 $e(u^a, v^b) = e(u, v)^{ab}$;

(b)非退化性: G_1, G_2 中存在 g_1, g_2,满足 $e(g_1, g_2) \neq 1$。

这里的双线性映射被认为是 type-3 映射:同构映射 $\psi: G_2 \rightarrow G_1$ 及其逆 $\psi^{-1}: G_1 \rightarrow G_2$ 都不能有效计算。

定义 2. 线性秘密分享方案(linear secret sharing schemes, LSSS)[17]:设 $\mathbb{P} = \{p_1, p_2, \cdots, p_n\}$ 为 n 个参与者集合。一个 $\mathbb{P}$ 上的秘密共享方案 $\prod$ 被称为 Z_p 上线性秘密共享方案,如果满足以下条件:

(1)每个参与者的秘密份额构成 Z_p 上的一个向量。

(2)存在一个 l 行 n 列的分享生成矩阵 $\boldsymbol{M}$,设 $\rho(i)$ 是从矩阵 M 的第 i 行到对应的参与者的一个映射,其中 $1 \leqslant i \leqslant l$。对于列向量 $\vec{v} = (s, r_2, \cdots, r_n)$,其中 $s \in Z_p$ 是被分享的秘密, $r_2, \cdots, r_n$ 随机选择。则 $M\vec{v}$ 是利用 $\prod$ 得到的关于 s 的 l 个秘密共享值形成的向量。其中 $(Mv)_i$ 为参与者 $\rho(i)$ 所获得的秘密份额。

根据上述定义的线性秘密共享方案具有线性重构性质,其定义如下:设 $\prod$ 为访问结构 $\mathbb{A}$ 上的线性秘密共享方案, $S \in \mathbb{A}$ 为授权集合,定义 $I = \{i, \rho(i) \in S\} \subseteq \{1, 2, \cdots, l\}$,如果 $\{\lambda_i\}$ 是参与者 $\rho(i)$ 根据 $\prod$ 关于 s 的有效秘密份额,则存在多项式时间算法计算得到常数向量 $\{w_i \in Z_p, i \in I\}$,使得 $\sum_{i \in I} w_i M_i = (1, 0, \cdots, 0)$,从而使得 $\sum_{i \in I} w_i \lambda_i = s$。

定义 3. DL[13](discrete logarithm)假设:已知 G_1 是一个阶为素数 p 的双线性群,随机选择 $g \in G_1, \xi \in Z_p$,对所有多项式算法 A,下面的优势是可忽略的:

$$\Pr[A(g, g^{\xi}) = \xi]$$

定义 4. SXDH 假设[18]:在群 G_1 和 G_2 上的 DDH 问题都是困难的,即不能有效计算同构映射 $\psi: G_2 \rightarrow G_1$ 及其逆 $\psi^{-1}: G_1 \rightarrow G_2$。

定义 5. q-HHSDH 假设[19]:设 h 是乘法群 G_1 的生成元,随机选择 $\gamma, x, y, x_i, y_i \in Z_p, i = 1, \cdots, q$,给定 $(g_1, h, g_2, g_2^{\gamma})$ 和部分隐藏元组 $(g_1^{x_i}, g_2^{x_i}, y_i, (hg_1^{y_i})^{1/(\gamma + x_i)})_{i \in [1,q]}$,对于一对新的数 (x, y),计算出 $(g_1^x, g_2^x, g_1^y, g_2^y, (hg_1^y)^{1/(\gamma + x)})$。对所有多项式算法 A,下面的优势是可忽略的:

$$\Pr[A(g_1, h, g_2, (g_1^{x_i}, g_2^{x_i}, y_i (hg_1^{y_i})^{1/(\gamma + x_i)})_{i \in [1-q]}) = (g_1^x, g_2^x, g_1^y, g_2^y, (hg_1^{\gamma})^{1/(\gamma + x)}) \wedge (x, y) \neq (x_i, y_i)_{i \in [1-q]}]$$

3 形式化定义与安全性定义

3.1 形式化定义

具有用户和属性匿名及追踪功能的 ABGS 方案由以下 6 个多项式算法组成:

(a) $\text{Setup}(1^k) \rightarrow (\text{params}, \text{ik}, \text{ok}_{\text{user}}, \text{tk}_{\text{att}})$:输入安全参数 1^k,输出公共参数 params,群密钥 ik,用户打开密钥 ok_{user} 和属性追踪密钥 tk_{att}。

(b) $\text{UserKey}(\text{params}, \text{ik}, \text{Att}_i) \rightarrow \text{sk}_i$:输入公共参数 params,群密钥 ik,用户属性集 $\text{Att}_i \subseteq \text{Att}$。输出用户成员私钥 sk_i,最新的成员注册表 reg。

(c) $\text{Sign}(\text{params}, \text{sk}_i, m, \Upsilon) \rightarrow \sigma$:输入公共参数 params,用户成员私钥 sk_i,消息 m,访问结构 Υ,输出群签名 σ。

(d) $\text{Verify}(\text{params}, m, \Upsilon, \sigma) \rightarrow 0/1$:输入公共参数 params,信息 m,访问策略 Υ,群签名 σ,返回是否接受该签名。

(e) $\text{OpenUser}(\text{params}, \text{ok}_{\text{user}}, m, \text{reg}, \sigma, \Upsilon) \rightarrow (i, \text{Att}_i)/\perp$:输入公共参数 params,用户打开密钥 ok_{user},消息 m,访问结构 Υ,群签名 σ,群成员列表 reg,返回身份 i 和用户的属性集 Att_i 或者 $\perp$。

(f) $\text{TraceAtt}(\text{params}, \text{tk}_{\text{att}}, m, \sigma, \Upsilon) \rightarrow \zeta/\perp$:输入公共参数 params,属性追踪密钥 tk_{att},信息 m,访问策略 Υ,群签名 σ,返回签名属性集合 $\zeta/\perp$。

3.2 安全性定义

定义 6. 正确性:当满足下列条件时,可认为该属性群签名方案是正确的:

对于所有的 $\text{Setup}(1^k) \rightarrow (\text{params}, \text{ik}, \text{ok}_{\text{user}}, \text{tk}_{\text{att}})$, $\text{UserKey}(\text{params}, \text{ik}, \text{Att}_i) \rightarrow \text{sk}_i, \Upsilon, m \in \{0,1\}^*$,如果 $\sigma = \text{Sign}(\text{params}, \text{sk}_i, m, \Upsilon)$,则:

Verify(params,m,Υ,σ) → 1 ∧

TraceAtt(params,$\mathrm{tk}_{\mathrm{att}}$,$m$,$\sigma$,Υ) → ζ ∧

OpenUser(params,$\mathrm{ok}_{\mathrm{user}}$,$\sigma$,$m$,reg,Υ) → ($i$,$\mathrm{Att}_i$)

成立。

在以下定义中,对手可以运行协议:

(1)通过 JoinP - oracle ,这意味着它创建了一个不知道其私钥的诚实用户:将索引 i 添加到 HU (诚实用户)列表中。

(2)通过 JoinA - oracle ,这表示它将与群管理员交互以创建它控制的用户:将索引 i 添加到 CU (不诚实用户)列表中。

当对手被赋予群密钥(群管理器已不诚实)时,对手不需要访问 JoinA - oracle ,因为它可以自己模拟来创建不诚实用户(不一定在 CU)。创建用户后,对手扮演不诚实用户的角色,并可以与诚实的用户交互,授予一些预言:

(1) corrupt(i) :如果 $i \in$ HU ,则提供此用户的特定私钥。对手可以在整个模拟过程中对其进行控制。将 i 从 HU 转移到 CU 中。

(2) sign(i,m,Υ) :如果 $i \in$ HU ,作为诚实的用户 i 将在签名过程中使用访问结构 Υ 在消息 m 上生成签名。

(3) openusr(m,σ,Υ) :如果 (m,σ,Υ) 是有效的,则返回签名者的身份 i 和属性集 Att_i 。

(4) tratt(m,σ,Υ) :如果 (m,σ,Υ) 是有效的,则返回用于生成签名的属性集 ζ 。

定义 7. 属性匿名性:对于所有多项式时间算法 A , A 赢得以下游戏的概率是可以忽略不计的,则称该方案具有属性匿名性。

初始化:挑战者 C 运行 Setup(1^k) → (params,ik,$\mathrm{ok}_{\mathrm{user}}$,$\mathrm{tk}_{\mathrm{att}}$) ,并将 (params,ik,$\mathrm{tk}_{\mathrm{att}}$) 发送给 A 。

第一步: A 被赋予询问 joinP,corrupt,sign,tratt 预言的权限。

挑战: A 输出信息 m^* ,访问结构 Υ^* ,诚实用户 U_i(即 $i \notin$ CU), 则 $\exists \zeta_{i0},\zeta_{i1} \subseteq \mathrm{Att}_i, \Upsilon(\zeta_{i0}) = 1, \Upsilon(\zeta_{i1}) = 1$ 成立。C 随机选择 $k \in_R \{0,1\}$,并响应一个群签名 $\sigma^* \leftarrow \mathrm{Sign}(\mathrm{params},\mathrm{sk}_i,\zeta_{i_k},m,\Upsilon)$ 。

第二步: A 可以进行类似于第一步的查询。但是 A 不能在任意时候对 i 进行 corrupt 查询。

输出:最后, A 输出 k' ,如果 $k = k'$ 则获胜。A 的优势定义 $\mathrm{Adv}^{\mathrm{user-anon}}(A) = |\Pr(k = k') - 1/2|$ 。

因此不存在任何多项式时间攻击者将群签名联系到用于生成它的一组属性。

4　支持 LSSS 访问结构的属性基群签名方案

4.1　角色分类

系统共有 5 个角色:群管理员(group manager, GM),用户,验证者,打开者(opener)以及属性追踪者(attribute tracer)

(a)群管理员:群管理员被认为是可以信任的,主要负责系统公共参数的生成,其次群管理通过群密钥与群成员交互为其发布密钥。

(b)用户:用户与 GM 进行交互,从而成为该群的成员,并且在满足访问策略的情况下代表该群进行签名,并将签名发送给验证者。

(c)验证者:在接收到群签名后,验证者可验证此签名的合法性,即是该群中的某一人签署了此签名,但不能确定具体的签名者。

(d)打开者:当发生用户滥用其签名权利时,打开者可以通过打开群签名找到签名者的身份和拥有属性。

(e)属性追踪者:可以追踪来自群签名的签名属性集,该属性集满足访问结构。

4.2　方案具体构造

(1) 初始化 Setup(1^k) → (params,ik,$\mathrm{ok}_{\mathrm{user}}$,$\mathrm{tk}_{\mathrm{att}}$) 。

由群管理员执行,具体步骤如下:

(a)生成阶为 q 的循环群 G_1,G_2 和 G_T ,双线性映射 $e: G_1 \times G_2 \rightarrow G_T$, g_1,g_2 分别是群 G_1,G_2 的生成元。

(b)随机选择 $\alpha \in Z_p^*$,并计算 $Z = g_2^{\alpha}$。

(c)定义系统属性集合 $\mathrm{Att} = \{\mathrm{att}_1, \mathrm{att}_2, \cdots, \mathrm{att}_n\}$ 。对于每个属性 $\mathrm{att}_j \in \mathrm{Att}$,选择一个秘密值 $s_j \in Z_p^*$,并计算 $Q_j = g_1^{s_j}, \forall\ \mathrm{att}_j \in \mathrm{Att}$ 。

(d)选择生成元 $h,u_0,\cdots,u_n \in G_1$,定义 Water 函数[16], $\mathbb{F}: \{0,1\}^m \rightarrow G_1$, 即对 $M = \{\mu_1,\cdots,\mu_m\} \in \{0,1\}^m$, $\mathbb{F}(M) = u_0 \prod_{j \in [1,m]} u_j^{\mu_j}$ 。

(e)由于本方案将采用基于 SXDH 为假设的 Groth-Sahai 证明,因此选择向量 $u = (u_1, u_2 = u_1^{t_1})$, $v = (v_1, v_2 = v_1^{t_2})$,其中 $u_1 = (g_1, g_1^{\alpha_1}) \in G_1^2$, $v_1 = (g_2, g_2^{\alpha_2}) \in G_2^2$, t_1, t_2, α_1, $\alpha_2 \in Z_p^*$ 。

最后生成公开参数 params ,群密钥 ik ,用户打开密钥 $\mathrm{ok}_{\mathrm{user}}$ 和属性跟踪密钥 $\mathrm{tk}_{\mathrm{att}}$ 如下:

$$\mathrm{params} = (q, G_1, G_2, e, g_1, g_2, \mathrm{Att}, \mathbb{F}, h, u_0, u_1, \cdots, u_m, Z, u, v)$$

$$\mathrm{ik} = (S = \{s_j\}_{\mathrm{att}_j \in \mathrm{Att}}, \alpha), \mathrm{ok}_{\mathrm{user}} = \alpha_1, \mathrm{tk}_{\mathrm{att}} = \{Q_j\}_{\mathrm{att}_j \in \mathrm{Att}}$$

(2)用户密钥生成 UserKey(params,ik,Att_i) →

sk_i。

用户与群管理员交互执行,用户可通过公私钥(upk_i,usk_i)和群管理员之间进行信息的交互。具体步骤如下:

(a)用户 U_i 首先随机选择 $y_i' \in Z_p^*$,计算生成 $Y_i' = g^{y_i'}$,并发送各群管理员。

(b)GM 接收到 Y_i' 后,随机选择 $x_i, y_i'', d \in Z_p^*$,计算 $Y_i'' = g_1^{y_i''}$,$B_i = h^{d/(x_i+\alpha)}$,$X_{i,2} = g_2^{x_i}$,并计算 $A_i = (hY_i'Y_i'')^{1/\alpha+x_i}$,对 $\forall\ att_j \in Att_i$,计算生成 $T_{i,j} = h^{s/(x_i+\alpha)}(\forall\ att_j \in Att_i)$。最后发送 $y_i'', A_i, B_i, X_{i,2}, \{T_{i,j}\}_{\forall att_j \in Att_i}, \{s_j\}_{\forall att_j \in Att_i}$ 给用户。

(c)用户 U_i 收到后验证 $e(A_i, Zg_2^{x_i}) = e(h, g_2)e(g_1, g_2)^{y_i+y_i''}$。然后计算 $y_i = y_i' + y_i''$,生成并发送一个签名 $\sigma_i = DSig_{usk_i}(A_i, X_{i,2}, Y_i = g_1^{y_i})$ 给 GM。

(d)GM 通过 upk_i 来验证 σ_i,并将 $(i, Att_i, upk_i, A_i, X_i = (X_{i,1} = g_1^{x_i}, X_{i,2}), Y_i, \sigma_i)$ 附加到群成员列表 reg 中,GM 发送 $X_{i,1}$ 给用户。

(e)用户检验 $e(X_{i,1}, g_2) = e(X_{i,2}, g_1)$,验证通过后,用户拥有有效的成员证书 (A_i, X_i, y_i) 和属性证书 $\{T_{i,j}\}_{\forall att_j \in Att_i}$。

最后,用户获得私钥 $sk_i = \{(A_i, X_i, y_i), \{T_{i,j}\}_{\forall att_j \in Att_i}, \{s_j\}_{\forall att_j \in Att_i}\}$,GM 获得最新的群成员列表 reg。

(3)签名 $Sign(params, sk_i, m, \Upsilon) \rightarrow \sigma$。

由用户执行,具体步骤如下:

(a)设签名结构 $\boldsymbol{\Upsilon}$ 是一个 $l \times n$ 的矩阵,函数 ρ 是 $\boldsymbol{M}$ 的行到属性的映射,M_i 是对应于矩阵第 i 行的向量,$\boldsymbol{M}_{ij}$ 为矩阵的第 i 行第 j 列元素。签名用户将该签名矩阵 $\boldsymbol{M}$ 和映射函数 ρ 发送给 GM,GM 构造所有可能满足签名结构的属性集合 $\psi \in Att: \Upsilon(\psi) = 1$,令 $I = \{j, \rho(j) \in \psi\} \subseteq \{1, \cdots, l\}$,即存在 $\{\omega_j \in Z_p : j \in I\}$ 满足 $\sum_{j \in I} \omega_j M_j = (1, 0, \cdots, 0)$,随机选择 $\alpha' \in Z_p^*$,计算并公开 $\{T_k\}_{k \in \{1,n'\}} = g_2^{\alpha' \sum_{j \in I} \omega_j M_{ji} s_{\rho(j)}}$,$n'$ 为满足签名结构 Υ 的属性集合数,将 $\{(T_{i,j})^{\alpha'}\}_{\forall att_j \in Att_i}$ 发给用户,并将 α' 发给属性跟踪者。

(b)设用户满足 LSSS 签名结构的用户属性集 $\zeta \in Att_i: \Upsilon(\zeta) = 1$,令 $I = \{i, \rho(i) \in \zeta\} \subseteq \{1, \cdots, l\}$,存在 $\{\omega_i \in Z_p : i \in I\}$ 满足 $\sum_{i \in I} \omega_i M_i = (1, 0, \cdots, 0)$。

(c)用户随机选择 $z \in Z_p^*$,生成一个临时身份 $ID(y_i, z) = g_1^{1/z+y_i}$。

(d)随机选择 $r \in Z_p^*$,计算 $\rho_1 = A_i, \rho_2 = y_i, \rho_3 = X_i = (g_1^{x_i}, g_2^{x_i}), \rho_4 = \prod_{j \in I}\left(T_{i,\rho(j)}^{\alpha' \omega_j M_{ji}} \cdot \prod_{l=2}^{n} (B_{\rho(i)})^{\omega_j M_{ji}}\right) = h^{\alpha' S_r/\alpha+x_i}$,令 $S_T = \sum_{j \in I} \omega_j M_{j1} s_{\rho(j)}$,$\rho_5 = ID(y_i, z)$,$\rho_6 = (g_1^z, g_2^z)$,$\rho_7 = h^z \mathbb{F}(m)^r$,$\rho_8 = g_2^r$。

(e)对群元素进行承诺得到 $\sigma_i = \mathbb{C}(\rho_i)$,$i = \{1, 3, 4\}$,$\sigma_2 = (\mathbb{C}^{(1)}(\rho_2), \mathbb{C}^{(2)}(\rho_2))$。

(f)计算 NIWI Groth-Sahai 证明[13]的承诺变量 $\rho_1, \rho_2, \rho_3, \rho_4$ 满足下列等式:

$$e(\rho_1, Z\rho_{3,2}) = e(h, g_2) \times e(g_1, g_2^{\rho_2}) \quad (1)$$

$$e(\rho_4, Z\rho_{3,2}) = e(h, \{T_k\}_{k \in \{1,n'\}}) \quad (2)$$

$$e(\rho_5, g_2^{\rho_2}\rho_{6,2}) = e(g_1, g_2) \quad (3)$$

$$e(\rho_7, g_2) = e(h, \rho_{6,2}) \times e(F(m), \rho_8) \quad (4)$$

$$e(g_1^{\rho_2}, g_2) = e(g_1, g_2^{\rho_2}) \quad (5)$$

$$e(\rho_{3,1}, g_2) = e(g_1, \rho_{3,2}) \quad (6)$$

$$e(\rho_{6,1}, g_2) = e(g_1, \rho_{6,2}) \quad (7)$$

最终输出群签名 $\sigma = (\{\sigma_i\}_{i=1}^4, \{\rho\}_{i=5}^8)$。

本方案通过签名上 Groth-Sahai 零知识证明,证明了上述映射等式的有效性。等式 1 是确定签名者具有通过用户密钥算法颁发的有效成员证书(即 A_i 格式正确);等式 2 确定签名者具有满足访问结构 Υ 的属性,并且证明了成员证书与属性证书相关联;等式 3 证明了 ρ_5 正确(即用户的身份 ID 正确);等式 4 不需要任何承诺,因此可以直接验证该签名 (ρ_7, ρ_8) 是在密钥 ρ_6 下对 M 的有效签名;等式 5、6 是确保可追踪对手模型中需要的 y_i, X_i 的正确性;等式 7 用于在不可陷害性对手模型中进行检测。

(4)签名验证 $Verify(params, m, \Upsilon, \sigma) \rightarrow 1/0$。

由验证者执行,根据 Groth-Sahai 证明验证所有的等式是否成立,若成立返回 1 则说明该签名有效。若不成立则返回 0 表示不接受该签名。

(5)打开 $OpenUser(params, ok_{user}, \sigma, m, reg, \Upsilon) \rightarrow (i/Att_i)/\perp$。

由打开者(Opener)执行,对于有效的群签名,打开者只需在签名 σ 中打开 A_i 的承诺,并在群成员列表 reg 中找到与 A_i 对应的身份 i 和属性 Att_i,否则输出 $\perp$。

(6)属性追踪 $TraceAtt(params, tk_{att}, m, \sigma, Att_i, \Upsilon) \rightarrow \zeta/\perp$。

由属性追踪者(attribute tracer)执行,对于有效的群签名,属性追踪者得到满足等式(2)中的 T_k。对于属性集 Att_i 判断是否存在满足签名结构 Υ 的属性子集 $\zeta_k: \Upsilon(\zeta_k) = 1$,令 $I = \{j, \rho(j) \in \zeta\} \subseteq \{1, \cdots, l\}$,即是否存在 $\{w_j \in Z_p : j \in I\}$,满足 $\sum_{j \in I} w_j M_j = (1, 0, \cdots, 0)$,计算 $Q^T = \prod_{j \in I} (Q_{\rho(j)})^{\alpha w_j M_{ji}}$,判断 $e(Q^T, g_2) = e(T_k, g_1)$,如果相等则输出 ζ,否则输出 $\perp$。

5　安全性分析与性能分析

5.1　安全性分析

文中方案具有属性匿名性、用户匿名性、可追踪性、不可伪造性、属性抗联合攻击性及属性不可伪造性,但因篇幅,仅给出了属性匿名性、可追踪性证明,其他证明见完整版。

定理 1:文中方案具有正确性。

证明:

$$e(\rho_1, Z\rho_{3,2}) = e((hy'_i y''_i)^{1/\alpha+x_i}, g_2^{\alpha} g_2^{x_i}) = e(h, g_2) \times e(g_1, g_2^{y_i}) = e(h, g_2) \times e(g_1, g_2^{\rho_2})$$

此等式成立表示签名者拥有通过密钥生成算法颁发的有效成员证书;

$$e(\rho_4, Z\rho_{3,2}) = e(\prod_{j\in\xi}(T_{i,j}^{\alpha\omega_j M_{j1}} \cdot \prod_{l=2}^{n}(B_i)^{\omega_j M_{jl}}), g_2^{\alpha} g_2^{x_i}) = e(h^{\alpha s/\alpha+x_i}, g_2^{\alpha+x_i}) = e(h, g_2^{s}) = e(h, \{T_k\}_{k\in\{1,n'\}})$$

此等式成立表示签名者拥有满足访问结构的属性证书;

$$e(\rho_5, g_2^{\rho_2}\rho_{6,2}) = e(\mathrm{ID}(y_i, z), g_2^{y_i} g_2^{z}) = e(g_1^{1/z+y_i}, g_2^{y_i+z}) = e(g_1, g_2)$$

此等式表示签名者的身份是正确的;

$$e(h^z F(m)^r, g_2) = e(h^z, g_2) \times e(F(m)^r, g_2) = e(h, g_2^{z}) \times e(F(m), g_2^{r}) = e(h, \rho_{6,2}) \times e(F(m), \rho_8)$$

此等式表示该签名是在密钥 ρ_6 下对 m 的有效签名;

$$e(g_1^{\rho_2}, g_2) = e(g_1^{y_i}, g_2) = e(g_1, g_2^{y_i}) = e(g_1, g_2^{\rho_2})$$

$$e(\rho_{3,1}, g_2) = e(g_1^{x_i}, g_2) = e(g_1, g_2^{x_i}) = e(g_1, \rho_{3,2})$$

$$e(\rho_{6,1}, g_2) = e(g_1^{z}, g_2) = e(g_1, g_2^{z}) = e(g_1, \rho_{6,2})$$

对于诚实的用户来说,根据零知识证明的完备性,拥有成员证书和属性证书的诚实用户始终可以生成一个有效的证明。通过以上分析,合法的签名总是可以通过验证,根据定义该方案满足正确性定义。

定理 2:文中方案在 SXDH 假设下具有属性匿名性。

证明:该证明来自 Groth-Sahai 证明系统。也就是说属性隐藏在 ρ_4 中,且用 Groth-Sahai 证明技术承诺到 σ_4 中。因此,在 SXDH 假设下,它是完全隐藏的。

定理 3:如果存在伪造属性签名通过验证的攻击者 A,那么就存在一个可以破坏 DL 和 KEA 假设的攻击者 B。

证明:模拟器 B 的输入是 DL 问题的一个实例,$(g, g') \in G_1^2$。令 $\xi = \log_g g'$。

初始化:该 ABGS 方案初始化阶段模拟器 B 生成系统参数 params。B 设置 $g_1 = g, h = g'$,生成其余参数 $(\mathrm{ik}, \mathrm{ok}_{\mathrm{user}}, \mathrm{tk}_{\mathrm{att}})$。并将 $(\mathrm{params}, \mathrm{ik}, \mathrm{tk}_{\mathrm{att}})$ 给攻击者 A。

查询:由于 B 知道所有的密钥,它可以根据属性不可伪造性的定义响应攻击者 A 产生的所有查询。

输出:A 输出用伪造的属性证书在消息 m^* 上签署的签名 σ^*,一个签名结构 Υ^*,满足 $\Upsilon(\mathrm{Att}_{i^*}) \neq 1$, $\Upsilon(\mathrm{Att}_{i^*} \cup \mathrm{att}_j) = 1$ 的签名者的密钥 sk_{i^*}。因为这是一个有效的签名,因此可通过验证算法。通过等式(2) $\rho_4^* = h^{\frac{\alpha' S_T}{\alpha+x_{i^*}}}$。这可以看作是 $\rho_4^* = h^{\frac{\alpha' s'}{\alpha+x_{i^*}}} h^{\frac{\alpha' s_j}{\alpha+x_{i^*}}}$,其中 A 不知道 $S_T = s' + s_j$ 和 $h^{\frac{\alpha' s_j}{\alpha+x_{i^*}}}$,但在签名中产生它。

B 向 A 提供输入 $(g_1 = g, g_1^{s_j} = g_{att_j} = g^{s_j})$,A 隐式返回 $h = g', h^{s_j} = g'^{s_j}$。然后根据 KEA 假设,可以利用提取器 $\bar{A}$ 来提取值 ξ。在 DL 假设下,可以以可忽略的概率完成此操作。因此,伪造的属性证书生成的签名可以以可忽略的概率通过验证。

5.2　性能分析

首先对本方案与现有属性基群签名方案进行功能上的比较,结果如表 1 所示。文献[11-13]方案都是采用访问树结构,访问树结构因为要采用递归运算,因此计算效率较低。本方案在提供了细粒度访问控制的同时支持 LSSS 访问结构,LSSS 利用线性秘密分享方案的秘密可线性重组的性质重构秘密,且 LSSS 与访问控制树的表达性相当。由于不需要递归运算,因此计算效率较高。文献[11-12]不具备属性匿名性和属性可追踪性,与文献[11]方案的属性可追踪性相比,本方案不仅可以追踪到签名用户的属性集,并且还可以追踪到用户签名属性集,即该用户签名时符合访问结构的子属性集合。

表 1　方案功能比较

性能	Khader[11]	Emura[12]	Ali[13]	文中
不可伪造	否	是	是	是
属性匿名	否	否	是	是
属性追踪	否	否	是	是
访问结构	访问树	访问树	访问树	LSSS
安全模型	ROM	ROM	标准模型	标准模型

本方案与现有属性基群签名方案效率比较如表 2 所示。设 n 表示与签名相关的属性数,l 表示用户的属性数。通过对比发现,文献[11-12]的签名大小和验证计算开销都与签名属性数相关,而文献[13]和文中方案的签名大小和计算开销均为固定值,与属性数无关。虽然文献[13]和文中方案的签名计算开销复

杂度相同,但文献[13]的方案在签名前需要构建一个冗余访问树,并且其为满足访问树可变,添加了冗余节点,增加了存储开销。而且在生成签名时,需要使用拉格朗日插值法,因此签名计算开销要大于文中方案,但文中方案在验证计算开销和满足签名策略的属性集合数相关,因此验证开销大于文献[13]方案。

表 2 方案效率分析

长度	Khader[11]	Emura[12]	Ali[13]	文中
签名	$(3+n)\|G_1\|+\|G_2\|+6\|Z_p\|=O(n)$	$(4+n)\|G_1\|+5\|Z_p\|=O(n)$	$29\|G_1\|+20\|G_2\|=O(1)$	$27\|G_1\|+22\|G_2\|=O(1)$
密钥	$(l+1)\|G_1\|+\|Z_p^*\|$	$(l+1)\|G_1\|+2\|Z_p^*\|$	$(2+l)\|G_1\|+\|G_2\|+\|Z_p^*\|$	$(1+l)\|Z_p^*\|+(2+l)\|G_1\|+\|G_2\|$

6 结束语

文中实现了一种支持 LSSS 访问结构的属性基的群签名方案。该方案不仅降低了计算开销,实现了属性匿名性,并且在发生用户滥用签名权利时,不但可以追踪到用户的身份和属性,还可以追踪到用户签名属性。方案的签名长度和验证计算开销均和属性数量无关,具有良好的通信和计算开销。文中的构造是基于双线性对的,随着量子计算机的到来,此类方案的安全性将受到威胁,而格密码系统不仅可抵抗量子计算攻击,安全性更高,因此在未来的工作中,将对格上基于 LSSS 访问结构的属性基群签名方案进行研究。

参考文献:

[1] MAJI H K, PRABHAKAEAN M. Attribute-based signatures: achieving attribute-privacy and collusion-resistance[J]. IACR Cryptology ePrint Archive, 2008, 15(7): 328-342.

[2] CHAUM D, VAN HEYST E. Group signatures[C]//Advances in cryptology: EUROCRYPT. Berlin: Springer-Verlag, 1991: 257-265.

[3] ATENIESE G, CAMENISCH J, JOYE M, et al. A practical and provably secure coalition-resistant group signature scheme [C]//Advances in cryptology — CRYPTO 2000. Kyoto, Japan: Springer-Verlag, 2000: 255-270.

[4] BELLARE M, MICCIANCIO D, WARINSCHI B. Foundations of group signatures: formal definitions, simplified requirements, and a construction based on general assumptions[C]// International conference on theory & applications of cryptographic techniques. Warsaw, Poland: Springer-Verlag, 2003: 614-629.

[5] BOYEN X, WATERS B. Full-domain subgroup hiding and constant-size group signatures[C]//International conference on practice and theory in public-key cryptography. Beijing, China: Springer-Verlag, 2007: 1-15.

[6] 李雪莲,吕晓琳,郭利娟,等. 适合大群组的格基动态群签名方案[J]. 电子科技大学学报,2019,48(1):80-87.

[7] 叶 青,杨晓孟,秦攀科,等. 新的 NTRU 格上抗量子攻击的群签名方案[J]. 计算机工程与应用,2020,56(2):89-96.

[8] 洪 璇,张绪霞. 基于中国剩余定理的前向安全群签名方案[J]. 计算机应用研究,2020,37(9):2806-2810.

[9] 欧海文,雷亚超,王湘南. 一种安全高效的群签名方案[J]. 计算机应用与软件,2020,37(7):309-312.

[10] KHADER D. Attribute based group signatures[J]. IACR Cryptology ePrint Archive, 2007(1): 159-173.

[11] KHADER D. Attribute based group signature with revocation [J]. IACR Cryptology ePrint Archive, 2007(9): 241-255.

[12] EMURA K, MIYAJI A, OMOTE K. A dynamic attribute-based group signature scheme and its application in an anonymous survey for the collection of attribute statistics[J]. Journal of Information Processing, 2009(17): 1968-1983.

[13] ALI S T, AMBERKER B B. Dynamic attribute based group signature with attribute anonymity and tracing in the standard model[C]//Security, privacy, and applied cryptography engineering. Kharagpur, India: Heidelberg, 2013: 147-171.

[14] GROTH J, SAHAI A. Efficient non-interactive proof systems for bilinear groups[C]//Advances in cryptology - EUROCRYPT 2008. Istanbul, Turkey: Springer, 2008: 415-432.

[15] KUCHTA V, SHARMA G, SAHU R A, et al. Generic framework for attribute-based group signature[C]//Information security practice and experience. Melbourne, VIC, Australia: Springer, 2017: 814-834.

[16] PERERA M N S, NAKAMURA T, HASHIMOTO M, et al. Traceable and fully anonymous attribute based group signature scheme with verifier local revocation from lattices[C]//Network and system security. Sapporo, Japan: Springer, 2019: 15-18.

[17] 张彦华,胡予濮,刘西蒙,等. 格上本地验证者撤销属性基群签名的零知识证明[J]. 电子与信息学报,2020,41(2): 315-321.

[18] BLAZY O, POINTCHEVAL D. Traceable signature with stepping capabilities[C]//Cryptography and security: from theory to applications - essays dedicated to jean-jacques quisquater on the occasion of his 65th birthday. Berlin Heidelerg: DBLP, 2015: 108-131.

[19] BELLARE M, PALACIO A. The knowledge-of-exponent assumptions and 3-round zero-knowledge protocols[C]//Advances in cryptology - CRYPTO 2004. Santa Barbara, California, USA: Springer, 2004: 273-289.