改进的群签名策略隐藏方案

朱　林,张　伟,谢宝文

(哈尔滨师范大学 计算机科学与信息工程学院,黑龙江 哈尔滨 150025)

摘　要:针对 CP-ABE 方案在解密阶段中存在访问策略可能泄露隐私的问题,提出了一种改进的群签名策略隐藏方案。首先,通过权重门限访问结构构建属性集合,在安全模型中对属性集合分割确定挑战者和敌对手的属性集合。然后,应用群签名方法实现访问策略的隐藏。最后,构建改进的策略隐藏方案的算法,对方案的安全性进行证明。通过对比分析,证明了提出的改进群签名策略隐藏方案在保护用户隐私的同时,适用范围更广泛。

关键词:策略隐藏;属性加密;属性权重;群签名

中图分类号:TP309.7　　**文献标识码**:A　　DOI:10.19358/j.issn.2096-5133.2020.01.008

引用格式:朱林,张伟,谢宝文.改进的群签名策略隐藏方案[J].信息技术与网络安全,2020,39(1):42-49.

An improved scheme of policy hiding based on group signature

Zhu Lin,Zhang Wei,Xie Baowen

(School of Computer Science and Information Engineering,Harbin Normal University,Harbin 150025,China)

Abstract:Aiming at the problem that the access strategy reveal privacy in the decryption phase of Ciphertext policy attribute based encryption(CP-ABE) scheme,an improved scheme of group signature strategy hiding is proposed. Firstly,the attribute set is constructed by the weight threshold access structure,and the attribute set of the challenger and the enemy is determined in the security model. Secondly,the group signature method is applied to realize the hiding of the access policy. Finally,an algorithm for the improved strategy hiding scheme is constructed to prove the security of the scheme. We prove that the improved group signature scheme can protect the privacy of users,also can be used in a wider range by comparative analysis.

Key words: hidden policy;attribute-based encryption;attribute weight;group signature

0　引言

云计算、边缘计算等新型的计算模式兴起,使得对数据的处理效率显著提高,但也存在一些安全问题,比如存储在云端的隐私被泄露、云端的数据被滥用、云端被黑客入侵等[1]。为了解决这些安全问题,SAHAI A 等人[2]提出了基于属性的加密机制(Attribute-Based Encryption,ABE),以实现细粒度的访问控制。GOYAL V 等人[3]根据制定访问策略角色的不同情况,进一步将 ABE 细分为基于密钥策略的属性加密(Key Policy Attribute Based Encryption,KP-ABE)[3]以及基于密文策略的属性加密(Ciphertext Policy Attribute Based Encryption,CP-ABE)[4]两种方案。首先在 KP-ABE 方案中,密钥对应一个访问策略,密文对应一个数据拥有者的属性集合,如要实现成功解密,用户属性集合中的子属性就必须满足访问策略的结构。在 CP-ABE 方案中,与 KP-ABE 方案相反,密钥对应一个数据拥有者的属性集合,密文对应一个访问策略,如要实现成功解密,用户属性集合中的子属性也必须要满足访问策略的结构。但是在这种方案下,会出现一个隐患,由于访问策略自身就包含了隐私信息,解密时,又会将密文以及访问策略一同发给用户,极大增加了用户的安全风险。

针对上述安全策略问题,国内外学者相继提出了隐藏访问策略的属性加密方案。KAPADIA A 等人加入一个半信任服务器,提出了一个基于隐私的属性数据发布(Privacy-Enhanced Attribute-based Publishing Of Data,PEAPOD)的 CP-ABE 方案[5],但该方案太过依赖于第三方服务器,同样有安全风险。NISHIDE T 等人使用通配符在多值属性上表示“与”门逻辑[6],并以此来表示访问策略,同时将访问策略隐藏在加密信息中,提出了隐藏部分访问策

略功能的 CP-ABE 方案,但该方案仅在弱模型上被证明,不具有广泛推广的价值。LAI J 等人[7]从隐藏属性的内积角度提出一种策略隐藏的 CP-ABE 方案,使用和 Nishide 等人提出的“与”门逻辑相同的访问结构,该方案使用了合数阶双线性群,并在双系统加密下被证明是完全安全的。文献[8]、[9]提出了多值线性秘密共享方案作为访问结构,实现了部分策略隐藏。文献[10]、[11]提出了使用多值与门作为访问结构来实现访问策略的完全隐藏。文献[12]使用正负属性上的与门表示访问结构,并首次在判定行双线性(Decision Bilinear Diffie-Hellman,DBDH)假设下证明方案的安全性。文献[13]使用线性秘密共享(Linear Secret Sharing Scheme,LSSS)表示访问结构,并在平行双线性 Diffie-Hellman 指数(Parallel Bilinear Diffie-Hellman Expone,PBDHE)假设下证明了安全性。上述策略隐藏加密方案忽略了属性集合中的每个属性有不同的权重比例,在一个系统中,每个属性并不是同等重要的,例如在一个医疗系统中,患者的属性包括病种、姓名、年龄、性别等,很明显,医生会优先根据病种的不同来制定对患者进行治疗的不同方案,在此方案下的特定病种的权重大于其他病种,根据这类思想的特点,在策略隐藏方案中属性就显得尤为重要。

基于以上分析,本文方案基于文献[14]的研究,使用群签名方法,将用户属性以及属性权重加入群组,并对整个群进行签名,不仅丰富了访问策略的表示,而且可以更好地隐藏访问策略中的属性信息[15]。如图 1 所示,在权重门限访问结构中,以属性和属性的权重为叶子节点,门限节点(“与”、“或”、“非”)为非叶子节点。本文方案引入群签名方法,将权重门限访问结构最后一层的叶子节点分别加入不同的群。如图 2 所示,将属性 A、B、C 和属性 D、E,及其对应的权重分别作为群 $G1$ 和 $G2$。若用户拥有的属性符合访问结构,在对访问信息验证时,仅知道访问者满足访问条件,不能明确群成员的来源。

1 基础知识题

1.1 双线性映射

设 G 和 G_T 是以素数 p 为阶的乘法循环群,g 是 G 的生成元,如果映射 $e:G\times G_T\rightarrow G_T$ 具有下列 3 个性质,就将该映射称为双线性映射。

(1)双线性 $\forall u,v\in G,\forall a,b\in \mathbf{Z}_p$,都满足等式:$e(u^a,v^b)=e(u,v)^{ab}$。

(2)非退化性:$\exists f\in G$,使得 $e(f,f)\neq 1$。

(3)可计算性:对于 $\forall f,h\in G$,存在一个有效的算法计算 $e(f,h)$。

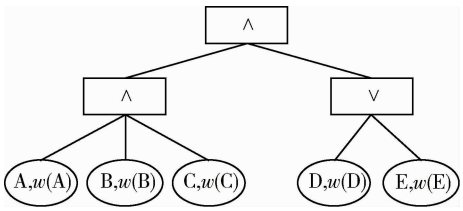

图 1 权重门限访问结构

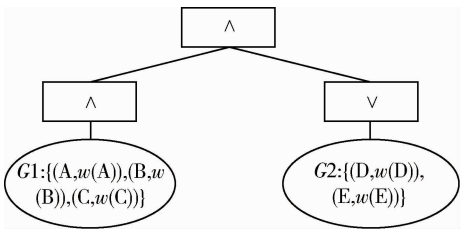

图 2 群签名的门限访问结构

1.2 访问结构

设 T 是一棵权重访问树,用门限值以及该节点所有孩子节点表示 T 中的任意某个非叶子节点,用属性以及属性的权值共同表示 T 中的叶子节点。

假定节点 x 的孩子节点数量是 N_x,节点 x 的门限值是 K_x,孩子数和门限值满足:$0<K_x\leqslant N_x$,若 $K_x=N_x$,则该门限是“与”门,若 $K_x=1$,则表示“或”门。另外,若叶子节点的权重小于属性集中的权重,令 $K_x=1$。

定义 1(权重门限访问结构) 设 T 是一棵根节点为 r 的权重访问树,记为 T_r。而 T_x 表示 T 中一个根节点为 x 的子树,若带有权重的属性集 S 满足权重访问树 T_x,用 $T_x(S)=1$ 表示。用以下递归方式计算 $T_x(S)$ 的值:

(1)若 x 是叶子节点,λ_x 是属性集 S 中的一个属性,当 $w(\lambda_x)\geqslant w(\mathrm{att}(x))$ 时(代表与叶子节点相关联的有权重的属性值),$T_x(S)=1$。

(2)若 x 是非叶子节点,先计算节点 x 的所有孩子节点 z 的 $T_z(S)$ 值,当至少有 K_x 个子节点的值等于 1 时,$T_x(S)=1$。

1.3 群签名

群签名[16]这一概念首次被 CHAUM D 和 HEYST V 提出。在一个群体签名方案中,群体中的成员都可以生成群签名,外界可验证其合法性,但无法确定到底是哪一个成员,即匿名性。若外界对

群签名存在争议,此时群管理员只需“打开”争议的签名,揭示真正的签名者,即追踪性。

1.4 DBDH 假设

对于一个双线性映射: $e:G \times G \rightarrow G_T$,随机数 $a,b,c \in \mathbf{Z}_p$,给定元组 (g,g^a,g^b,g^c,r) ,其中, $r \in G_T$,判定是否等于 r 。

2 方案构造

2.1 系统模型

本文方案系统模型如图 3 所示,由 6 个部分组成:数据所有者、用户、可信中心、云服务器、属性群、群组管理员。

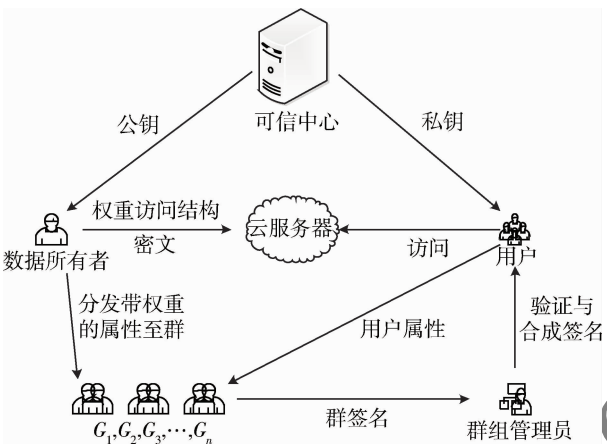

图 3 系统模型

数据所有者:制定访问策略,对属性加权分割并分发至属性群,对数据加密并发送至云服务器。

用户:将访问请求发送给服务器,如果用户拥有的属性能与访问结构相对应,解密成功,取得明文。

可信中心:发布系统公钥和私钥。

云服务器:将数据所有者的密文存储起来,并处理来自用户的访问请求。

属性群 $(G_1,G_2,\cdots,G_n)$:对用户拥有的属性生成签名,之后群组管理员接收该签名。

群组管理员:首先验证群签名有效性,然后将被验证的签名合成最后的签名。

2.2 安全模型

本文方案的安全性将由一个挑战者和敌手的游戏证明,过程如下:

(1)初始化,确定敌手需要挑战的属性集合。

(2)分割属性集合,挑战者按照属性的权重比例对接收到的属性集合分割,得到分割后的集合 S^* 。

(3)系统建立,挑战者执行系统初始化算法,把生成的系统公钥 PK 发给敌手。

(4)阶段一,挑战者对敌手分割后的集合 S^* 执行查询,之后挑战者执行密钥生成算法,得到敌手的私钥 SK,并对其查询回答。

(5)挑战,敌手将两个等长的明文 $m_0,m_1(m_0 \neq m_1)$ 交给挑战者,挑战者投掷一个随机的硬币 b ,然后利用访问结构 Π(阶段一分割后的集合 S^* 不满足此访问结构)对明文 m_b 加密,并将密文 CT 发送给敌手。

(6)阶段二,重复阶段一的操作。

(7)猜测,敌手输出 b 的猜测值 b' 。

在上述游戏中,定义敌手的优势为 $\mathrm{Adv} = \Pr[b' = b]^{-1/2}$,若这个优势能够被忽略,则证明此方案的安全性。

2.3 算法定义

本文的方案包含 5 个算法。

算法 1:属性集转换,将系统属性集合输入算法,数据所有者按照具体情况给所有属性分配权值。定义属性集 $S = \{\lambda_1,\lambda_2,\cdots,\lambda_n\}$ 的任意属性 λ_i ,其权值最大为 $\omega_i = \mathrm{weight}(\lambda_i)$ 。根据权值对属性集 S 中的每个属性 λ_i 进行分割,假设分割以后,权值最小为 1,则 λ_i 与集合 $(\lambda_i,1),\cdots,(\lambda_i,\omega_i)$ 相对应,这个集合就是经过转换后的权重属性分割集合 S^* 。

算法 1 属性集转换
输入:属性集合 S
输出:权重属性分割集合 S^*
1: for 属性集合 S 中每个属性 λ_i do
2: 计算 ω_i
3: 定义 $\min\omega_i = 1$
4: return $(\lambda_i,1),\cdots,(\lambda_i,\omega_i)$
5: end for
6: returnS^*

算法 2:系统初始化,G 和 G_T 是以素数 p 为阶的乘法循环群,双线性映射 $e:G \times G \rightarrow G_T$,g 是 G 的生成元。

(1)输入安全参数 k,并定义权重属性分割集合 S^* 里的全部元素,选取 $\mathbf{Z}_p^*$ 上前面 $|S^*|$ 个元素,即

选取 $1,\cdots,|S_p^*|(\text{bmodp})$。然后可信中心选取可抗碰撞的哈希函数 $H()$,随机地选取元素 $y,t_1,t_2,\cdots,t_{|S^*|}\in \mathbf{Z}_p$。

(2)输出系统公钥 $PK=\{e,g,Y=e(g,g)^y,T_j=g^{t_j}(1<j\leqslant|S^*|),H()\}$,主密钥 $MK=\{y,t_j(1\leqslant j\leqslant|S^*|)\}$。

算法 2　系统初始化

输入:安全参数 k

输出:公钥 PK,主密钥 MK

1:生成两个以 p 为阶的乘法循环群 G 和 G_T 存在映射 $e:G\times G\rightarrow G_T$ 其中 g 是 G 的生成元

2:定义转换后的权重属性分割集合是 S^*

3:　for $\mathbf{Z}_p^*$ 上的每一个元素 do

4:　　选择 $1,\cdots,|S_p^*|(\text{bmodp})\leftarrow\mathbf{Z}_p^*$

5:end for

6:选择一个抗碰撞的哈希函数 $H()$

7:随机选取 $y,t_1,t_2,\cdots,t_{|S^*|}\leftarrow\mathbf{Z}_p$

8:计算 Y 和 T_j

9:return PK,MK

算法 3:密钥生成,输入主密钥 MK 以及权重属性的分割集合 S^*,输出私钥 SK。

(1)输入主密钥 MK 以及权重属性的分割集合 S^*,可信中心随机选择一个阶为 d-1 的多项式 q,让 $q(0)=y$。

(2)输出私钥 $SK=\{\forall i\in S^*,D_i=g^{\frac{q(i)}{t_i}}\}$。

算法 3　密钥生成

输入:主密钥 MK,权重属性分割集合 S^*

输出:私钥 SK

1:随机选取一个阶为 q 的多项式 d-1

2:计算 $q(0)$ 和 D_i

3:return SK

算法 4:加密算法,输入公钥 PK,消息 m,以及包含权重的访问结构 Π,输出密文 CT。

(1)设定叶子节点的集合为 w^*,则权重属性的分割集合为 w。数据所有者从 $\mathbf{Z}_p^*$ 选择随机数 $m\in\mathbf{Z}_p^*$,根据访问策略将属性集 w^* 分为不同的群,记为 $G_1,G_2,\cdots,G_m$,从 $\mathbf{Z}_p^*$ 选择随机数 $g_1,g_2,\cdots,g_m$ 作为每个群的私钥,计算 $PK_{G_j}=g_jE(1\leqslant j\leqslant m)$,设定群 $G_j(1\leqslant j\leqslant m)$ 的公钥为 PK_{G_j},同时将每个群 ID 发送给群组管理员 GM,GM 就拥有了私钥 GM_{SK},公钥 GM_{PK}。

(2)利用 Shamir 秘密共享机制进行秘密分发,对于树形访问结构 Π,其根节点为 r。若当前节点是“或”门,则当前节点的子树相对应的节点或群的秘密值均为 s,若当前节点是“与”门或其他情况,则对当前节点的子树按照从左至右分发秘密值。随机选择秘密值 $s_i(b\leqslant i<e)$ 到节点最后一个子树,(b,e) 为节点或群的范围。最后的子树秘密值为 $s_e=\dfrac{s'-\sum s_i}{p(b\leqslant i<e)}$,式中 s' 为此节点的秘密值。

(3)群 $G_j(1\leqslant j\leqslant m)$ 的秘密值为 s_j,对于 (t,n) 门限函数,选择素数 $q>\max(s_j,n)$,然后随机地选择 $a_1,a_2,\cdots,a_{t-1},0\leqslant a_j\leqslant q$-1,定义 $a_0=s_j$,$t-1$ 次的多项式 $f(x)=a_{t-1}x^{t-1}+a_{t-2}x^{t-2}+\cdots+a_1x+a_0$。对于每一个加入该群的属性 w_i^*,从 $\mathbf{Z}_p^*$ 选择一个随机数 $u\in\mathbf{Z}_p^*$,计算 $uE=(x_u,y_u)=U$,$ID'_i=(u)H(ID_T)+(u)H(G_j)$,并把 U 和 ID'_i 发送到属性群 G_j。当群收到属性,并判断 $ID'_iE=UH(ID_i)+UH(G_j)$ 是否满足,如果满足就让属性入群,每个属性将获得该群其中一块秘密 $s_i=f(i)$,计算 $E_i=T_{is_i}$。

(4)输入消息 m,返回密文 $CT=\{\Pi,E'=mY^s,\forall i\in w^*:E_i=T_{is_i}\}$。

算法 4　加密

输入:公钥 PK,消息 m 和访问结构 Π

输出:密文 CT

1:定义叶子节点的集合为 w^*,权重属性分割集合为 w

2:　for w^* 中的每一个属性 do

3:　　随机选取 $m\leftarrow\mathbf{Z}_p^*$

4:　　将 w^* 按照访问策略分成不同的群 $G_1,G_2,\cdots,G_m$

5:　　随机选取 $g_1,g_2,\cdots,g_m\leftarrow\mathbf{Z}_p^*$ 作为每个群的私钥

6:　　计算 PK_{G_j}

7:　　定义群 G_j 的公钥为 PK_{G_j}

8:　　将群组 ID 发送给 GM

9:　end for

10:　for 每个秘密值 s_i do

11: 随机选取 $i \leftarrow (b,e)$
12: 计算 s_e
13: end for
14: 选取素数 $q > \max(s_j, n)$
15: 随机选取 $a_1, a_2, \cdots, a_{t-1}$, $0 \leqslant a_j \leqslant q\text{-}1$
16: 定义 $a_0 = s_j$
17: 计算 $t-1$ 次的多项式 $f(x)$
18: for 每个 w_i^* do
19: 随机选取 $u \leftarrow \mathbf{Z}_p^*$
20: 计算 uE, ID'_i
21: 将 U 和 ID'_i 发送给 G_j
22: if $\mathrm{ID}'_i E = \mathrm{UH}(\mathrm{ID}_i) + \mathrm{UH}(G_j)$ do
23: $s_i = f(i)$
24: 计算 E_i
25: end if
26: end for
27: returnCT

算法 5：解密算法，输入属性集 w，公钥 PK，私钥 SK，密文 CT，输出消息 m。

(1) w^* 为群 $G_j(1 \leqslant j \leqslant m)$ 的属性集合，依据用户拥有的属性，计算群签名：

$$\prod_{a_i \in w^*} e(D_i, E_i)^{l_i(0)} = \prod_{a_i \in w^*} e(g^{\frac{q(i)}{t_i}}, T_i^{S_i})^{l_i(0)} = \prod_{a_i \in w^*} e(g^{\frac{q(i)}{t_i}}, g^{t_i s_i})^{l_i(0)} = \prod_{a_i \in w^*} e(g,g)^{q(i)s_i l_i(0)} = e(g,g)^{q(i)s_i}$$

即 $\mathrm{Sign}_{G_i} = e(g,g)^{q(i)s_i}$，式中 $l_i(0)$ 是拉格朗日系数，并与属性 a_i 对应。

(2) 计算 $H = (v)H(G_l) + g_l, V = vE, e = \mathrm{Encrept}(H \,//\, \mathrm{Sign}_{G_i} \,//\, V \,//\, G_l)_{\mathrm{GM}_{\mathrm{pk}}}$，其中随机数 $v \in \mathbf{Z}_p^*$。把 (H,e,V) 发送给群组管理员，对消息 e 解密，并确定群 G_l 是否存在，如果存在，则检验 $HE = VH(G_l) + \mathrm{PK}_{G_i}$ 是否满足，如果满足，接受签名 $\mathrm{Sign}_{G_i} = e(g,g)^{q(i)s_i}$。把 $\mathrm{Sign} = \prod_{l \in (l \to m)} \mathrm{Sign}_{G_i} = e(g,g)^{ys}$ 的结果返回给用户，否则返回 $\perp$，当用户收到签名之后，计算 $e(g^s, g^{y-\gamma})Sign = e(g^s, g^{y-\gamma})e(g,g)^{\gamma s} = e(g,g)^{ys}$，继而求出消息 $m = \dfrac{E'}{e(g,g)^{ys}} = \dfrac{me(g,g)^{ys}}{e(g,g)^{ys}}$。

算法 5 解密

输入：属性集合 w，公钥 PK，私钥 SK，密文 CT
输出：消息 m
1: 定义群 G_j 的属性集合为 $w^{*\prime}$
2: for 每个 G_j do
3: 计算 $\prod_{a_i \in w^{*\prime}} e(D_i, E_i)^{l_i(0)}$
4: return 群签名 Sign_{G_l}
5: end for
6: 随机选取 $v \leftarrow \mathbf{Z}_p^*$
7: 计算 $\boldsymbol{H}, V, e$
8: 将 $(\boldsymbol{H}, e, V)$ 发送给 GM
9: 解密消息 e
10: if G_l 存在 then
11: if $HE = VH(G_l) + \mathrm{PK}_{G_l}$ then
12: 接收 Sign_{G_l}
13: return Sign
14: else
15: return
16: end if
17: end if
18: 计算 $e(g^s, g^{y-\gamma})\mathrm{Sign}$
19: return m

3 安全性证明

定理 1 若在本文方案模型下，敌手可以攻破本方案，那么 DBDH 假设就会被模拟器以不可忽略的概率攻破。

证明：在一个多项式时间内，若敌手 A 能够以不可忽略的优势 ε 取得游戏胜利，则建立模拟器 B' 以 $\dfrac{\varepsilon}{2}$ 的优势模拟 DBDH 假设游戏，步骤如下：

挑战者指定 DBDH 要挑战的元组 (g, g^a, g^b, g^c, r)，其中 $r \in G_T$，它的取值概率等于 $e(g,g)^{abc}$。

(1) 初始化：A 提供给模拟器 B' 要挑战的访问结构 Π 以及其拥有的属性集合 w。

(2) 属性集分割：模拟器按照权重对所有属性集 S 中的每一个属性分割，得到的分割属性集合为 S^*。然后按照上述方式对属性集合 w 分割，得到分割后的权重属性集合 w^*。

(3) 系统建立：模拟器执行系统初始

化算法，生成系统公钥 $PK = \begin{cases} e, g, Y = e(g,g)^{a} \\ T_i = g^{(c\beta_i)} (\beta_i \in \mathbf{Z}_p, i \in w^*) \\ T_i = g^{(w_i)} (w_i \in \mathbf{Z}_p, i \in S^* - w^*) \end{cases}$，并且公钥中的所有参数都是随机的，随后模拟器把公钥 PK 发送给 A。

(4)阶段一：假定敌手 A 请求的私钥 γ 包含了属性分割集 S^*，且 S^* 满足 $|S^* \cap w^*| < d$。定义三个集合：Ω、Ω'、K，令 $\Omega = S^* \cap w^*$，$|\Omega'| = d-1$，$K = \Omega' \cap \{0\}$。

定义 D_i，若 $i \in \Omega' \cap \Omega$，则 $D_i = g^{s_i}$，随机元素 $s_i \in \mathbf{Z}_P$，若 $i \in \Omega' - \Omega$，则 $D_i = g^{\frac{\eta}{w_i}}$，随机即元素 $w_i \in \mathbf{Z}_p$。然后随机选择一个次数为 d-1 的多项式 $q(x)$，满足 $q(0) = a$，并随机选择其中的 d-1 个点。有 $q(i) = c\beta_i s_i, i \in \Omega' \cap \Omega$ 和 $q(i) = \eta_i, i \in \Omega' - \Omega$。当 $i \notin \Omega'$，模拟器计算 $D_i = (\Pi_{j \in \Omega \cap \Omega'} c^{\frac{\beta_i \lambda_{i,K}(0)}{w_i}})(\Pi_{j \in \Omega' - \Omega} g^{\frac{\eta_i \lambda_{i,K}(i)}{w_i}}) A^{\frac{\lambda_{i,K}(i)}{w_i}}$。模拟器通过插值法计算当 $i \notin \Omega'$ 时，$D_i = g^{\frac{q(i)}{w_i}}$。由上述可知，属性集 S 的私钥能够被模拟器构造得和原来方案相同。

(5)挑战：敌手 A 提交两个挑战消息 m_0、m_1 给模拟器，模拟器投掷一枚公平的硬币 $b = \{0,1\}$，计算 m_b 的加密值，最后输出密文 $CT = \{\Pi, E' = m_b e(g,g)^{ys}, \forall i \in S^* : E_i = B^{\beta_i}\}$。

(6)阶段二：与阶段一相同。

(7)猜测：敌手 A 输出对 b 的猜测值 b'，当 $b' = b$，说明敌手 A 能够以不可忽略的优势攻破本文方案，此时 $r = e(g,g)^{abc}$，不然 r 等于随机的值。

在上述游戏中，当 $b' \neq b$ 时，r 为一个随机的值，此时敌手 A 没有获得消息 m_b 的信息，$\Pr[b' \neq b] = \frac{1}{2}$，当 $b' = b$ 时，敌手有 ε 的优势攻破本文方案，$\Pr[b' = b] = \frac{1}{2} + \varepsilon$。

所以综合一下敌手的优势为 $\mathrm{Adv} = \Pr[b' = b] - \frac{1}{2} = \frac{1}{2} \times \frac{1}{2} + \frac{1}{2} \times \left(\frac{1}{2} + \varepsilon\right) - \frac{1}{2} = \frac{\varepsilon}{2}$。

由上述证明可知，若敌手 A 在安全模型下能以不可忽略的优势 ε 攻破本文方案，则模拟器 B' 也能以同样的优势打破 DBDH 假设。通过上面证明，即证得该方案在标准模型下是选择明文安全的。

4 方案分析

4.1 理论分析

将本文方案与文献[2,9,10,11]进行比较，从模型和功能方面选定 3 个参数，结果如表 1 所示。

表 1 方案比较

方案	安全模型	属性是否带权重	访问策略是否隐藏
文献[2]	标准模型	否	否
文献[9]	标准模型	否	是
文献[10]	标准模型	否	是
文献[11]	标准模型	否	是
文献[14]	标准模型	是	否
本文方案	标准模型	是	是

文献[2]提出方案是以门限结构作为访问结构，用户属性集为 ω，与密文相对应的属性集为 ω'，当 $|\omega \cap \omega'| \geqslant d$，式中 d 为门限值，才可以解密出密文。但是该方案没有考虑到访问策略隐藏的问题。文献[9]提出方案是以 LSSS 矩阵作为访问结构，访问结构表达灵活，但是在合数阶群下，线性对的计算效率会增加，同时对访问策略的隐藏只做到了部分隐藏，方案中，把属性分成属性值以及属性名，却忽略权重对于属性的价值，并且部分隐藏还是会有隐私泄露风险。文献[10]中给出的方案是以多值与门作为访问结构，并对属性加了一个标记，用以描述属性的需求状态，虽然实现了策略的完全隐藏，但是却增加了存储的开销以及计算的效率，也忽略了权重对于属性的重要性。文献[11]提出方案以多值与门来表达访问结构，访问结构中的每个属性 ω_i 可以取多个值，并将访问结构转变成一棵访问树，隐式地嵌入到密文中，但是该方案同样没有考虑到实际情况下不同属性拥有不同权重比例。本文是在文献[14]的基础上进行改进的，与文献[14]相比，在都考虑到权重对属性的价值之外，本文又将属性以及属性权重的集合加入到一个群组中，群中的任何成员都可以对当前群组签名，以此来实现对访问策略的隐藏。并且本文方案还可以隐式地达到追踪效果。

本文的方案与其他几个方案相比，以群签名的方式实现访问策略的完全隐藏，不仅可以隐藏访问策略，而且在外界对群签名产生质疑时，群组管理员可以确定真实签名者，达到了签名可追踪的效

果,使得方案功能性更强,另外在现实生活中,每个属性所占的比例也有不同,本文方案充分考虑此类现实问题,使得能保护用户隐私的同时,适用范围也更广泛。

4.2 实验分析

为了更加直观地比较不同方案的性能,实验选取文献[4]与文献[17]方案的加密与解密时间与本文方案进行比较。实验设备为 Intel(R) Core(TM) i5-4210U 2.40 GHz,16 GB 内存,Centos6.5 操作系统,实验代码基于 JPBC 2.0.0 和 cpabe-0.11 进行修改和编写。本次实验迭代选取 5 ~ 100 个系统属性,以测试不同的属性个数对加密解密时间的影响。

实验结果如图 4 和图 5 所示。从结果可以看出,属性个数为 5 时,3 种方案加解密时间基本持平,但随着属性个数增加时,3 种方案的加解密时间均随着属性个数线性增长,且本文方案在同等条件下,明显优于文献[4]方案,原因在于,文献[4]是最初编写的 CP-ABE 方案,方案仅实现最基本的加解密,并没有进行改进优化。本文方案在访问结构中对属性合并入群改进之后,减少了加解密的运算量,所以方案的效率稍优于文献[17]。

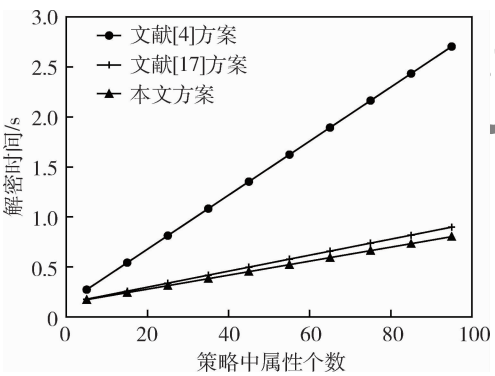

图 4 各个方案加密时间对比

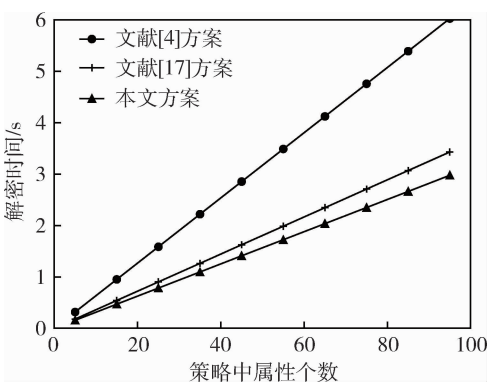

图 5 各个方案解密时间对比

5 结论

本文将群签名以及属性权重引入到属性加密领域,可以有效解决由访问策略导致的隐私泄露问题。通过研究,本文完成了基于群签名的 CP-ABE 方案模型构建,通过属性集转换、系统初始化、密钥生成、加密和解密这 5 个算法充分验证方案的可行性,并在标准模型下证明了所提方案的安全性。

本文的方案证明了在权重门限访问结构下的安全性,下一步将在格理论下结合本文提出的方案展开研究。

参考文献

[1] 房梁,殷丽华,郭云川,等. 基于属性的访问控制关键技术研究综述[J]. 计算机学报,2017,40(7):1680-1698.

[2] SAHAI A,WATERS B. Fuzzy identity-based encryption [C]. Annual International Conference on the Theory and Applications of Cryptographic Techniques. Springer, Berlin, Heidelberg,2005:457-473.

[3] GOYAL V, PANDEY O, SAHAI A, et al. Attribute-based encryption for fine-grained access control of encrypted data[C]. Proceedings of the 13th ACM conference on Computer and communications security. ACM, 2006: 89-98.

[4] BETHENCOURT J,SAHAI A,WATERS B. Ciphertext-policy attribute-based encryption[C]. 2007 IEEE Symposium on Security and Privacy (SP07). IEEE,2007:321-334.

[5] KAPADIA A, TSANG P P, SMITH S W. Attribute-based publishing with hidden credentials and hidden policies [C]. Network and Distributed System Security Symposium, NDSS 2007, San Diego, CA, USA, 2007: 179 – 192.

[6] NISHIDE T, YONEYAMA K, OHTA K. Attribute-based encryption with partially hidden encryptor-specified access structures[C]. In ACNS 2008, 2008, LNCS 5037: 111 – 129.

[7] LAI J,DENG R H,LI Y. Fully secure cipertext-policy hiding CP-ABE[C]. International Conference on Information Security Practice and Experience. Springer, Berlin, Heidelberg,2011:24-39.

[8] ZHANG L,HU G,MU Y,et al. Hidden ciphertext policy attribute-based encryption with fast decryption for personal health record system [J]. IEEE Access, 2019, 7: 33202-33213.

[9] 应作斌,马建峰,崔江涛. 支持动态策略更新的半策略隐藏属性加密方案[J]. 通信学报,2015,36(12):178-189.

[10] 刘雪艳,郑等凤. 基于素数群完全隐藏访问结构的 CP-ABE 方案[J]. 计算机工程,2016,42(10):140-145.

[11] 汪海萍,赵晶晶. 隐藏访问结构的密文策略的属性基加密方案[J]. 计算机科学,2016,43(2):175-178.
[12] CHEUNG L, NEWPORT C. Provably secure ciphertext policy ABE[C]. Proceedings of the 14th ACM Conference on Computer and Communications Security. ACM, 2007: 456-465.
[13] WATERS B. Ciphertext-policy attribute-based encryption: an expressive, efficient, and provably secure realization [C]. International Workshop on Public Key Cryptography. Springer, Berlin, Heidelberg, 2011:53-70.
[14] 刘西蒙,马建峰,熊金波,等. 云计算环境下基于密文策略的权重属性加密方案[J]. 四川大学学报(工程科学版),2013 (6):21-26.
[15] TSAI C Y, HO P F, HWANG M S. A secure group signature scheme [J]. IJ Network Security, 2018, 20 (2): 201-205.
[16] 张兴兰,崔遥. 基于群签名的属性加密方案[J]. 网络与信息安全学报,2019,5(1):15-21.
[17] 范运东,吴晓平. 基于策略隐藏属性加密的云存储访问控制方案[J]. 计算机工程,2018 (7):24.

(收稿日期:2019-10-30)

作者简介:

朱林(1995 -),男,硕士,主要研究方向:网络安全、密码学。

张伟(1964 -),通信作者,女,硕士,副教授,主要研究方向:网络安全、密码学。E-mail:283186823@ qq. com。

谢宝文(1993 -),男,硕士,主要研究方向:网络空间安全、可信计算。

(上接第 41 页)

[6] ALBERTINI D A, CARMINATI B, FERRARI E. An extended access control mechanism exploiting data dependencies[J]. International Journal of Information Security, 2017 (2):107-115.
[7] SOMAVARAPU A K, KEPP K P. The dynamic mechanism of presenilin-1 function: sensitive gate dynamics and loop unplugging control protein access[J]. Neurobiology of Disease, 2016(5):78-82.
[8] 陆佳炜,吴斐斐,徐俊. 基于动态授权机制的自适应云访问控制方法研究[J]. 计算机应用与软件,2017(11):203-211.
[9] 廖大强. 基于云计算的密集型数据库资源快速检索方法研究[J]. 内蒙古民族大学学报(自然科学版),2019(5):215-220.
[10] 邹德清,杨凯,张晓旭. 虚拟域内访问控制系统的保护机制研究[J]. 山东大学学报(理学版),2014(8):96-104.
[11] 赵坤,方鹏. 数据库的安全机制及访问控制策略分析[J]. 通讯世界,2016(12):81-90.

(收稿日期:2019-07-20)

作者简介:

文星(1987 -),男,硕士研究生,工程师,主要研究方向:电力信息化技术。

版权声明