基于 LSSS 的隐藏策略属性基加密方案

陈丹伟,汤 波
(南京邮电大学 信息安全系,江苏 南京 210003)

摘 要: 传统的密文策略属性基加密方案(CP-ABE)在解密阶段会将密文连同访问策略一起发送给用户,但有时访问策略本身就是敏感信息,同样会泄露用户的隐私信息。因此,针对 CP-ABE 方案的访问策略隐藏这一问题,在现有 CP-ABE 方案的基础上,提出了一种新的隐藏策略属性基加密方案。该方案采用线性秘密分享矩阵(LSSS)作为访问结构,策略表达能力强,可以表达任意的访问策略,使用 3 素数合数阶双线性群来构造方案以及实现策略的隐藏,并且借助双系统加密技术证明方案在选择明文攻击下的安全性。与同类的基于 LSSS 隐藏策略的方案相比,该方案不仅降低了合数阶双线性群的阶数,减少了系统开销,而且减少了加密阶段的运算次数,提高了加密效率,增加了方案在实际应用中的可行性。

关键词: 密文策略; 属性基加密; 线性秘密分享矩阵; 策略隐藏; 合数阶双线性群
中图分类号: TP301 **文献标识码:** A **文章编号:** 1673-629X(2018)02-0119-06
doi: 10.3969/j.issn.1673-629X.2018.02.026

An Attribute-based Encryption Scheme with Hidden Policy Based on LSSS

CHEN Dan-wei, TANG Bo
(School of Information Security, Nanjing University of Posts and Telecommunications, Nanjing 210003, China)

Abstract: In traditional ciphertext policy attribute-based encryption schemes, it will send ciphertext to the decryptor along with access policy during decryption phase, but sometimes the access policy itself contains sensitive information, which will also leak the user's privacy information. Therefore, for the problem of policy without hidden in CP-ABE schemes, we propose a new ciphertext policy attribute-based encryption with policy hidden based on existing CP-ABE schemes. It employs linear secret sharing schemes (LSSS) as access structure which has strong expression and can express any access policy. We adopt three primes composite order bilinear groups to construct the scheme and realize the policy hidden. Under dual system encryption technology, it could be proved chosen-plaintext attack (CPA) secure. Compared with the other schemes based LSSS with policy hidden, the proposed scheme not only reduces system overhead by decreasing the order of composite order bilinear groups, but also improves encryption efficiency by reducing the number of operations in the encryption phase and increases the feasibility in practical application.

Key words: ciphertext policy; attribute-based encryption; linear secret sharing schemes; hidden policy; composite order bilinear groups

0 引 言

近年来,访问控制成为云计算研究的热点问题,传统的加密方法虽然能够保护数据的隐私,但增加了系统对用户细粒度访问控制的难度。为了实现云环境下的细粒度访问控制,2005 年 Sahai 等[1]提出了基于属性的加密体制的概念,在这种加密体制中加密者无需知道解密者的具体身份信息,而只需要掌握解密者一系列描述的属性,然后在加密过程中用属性定义访问结构对消息进行加密,当用户的密钥满足这个访问结构时就可以解密该密文。

2006 年,Goyal 等将基于属性的加密体制分为密文策略属性基加密[2]和密钥策略属性基加密[3-7]两种,但这些方案都未对访问策略进行隐藏,当访问策略本身就是敏感信息,同样会泄露用户的隐私信息。例如,在个人健康记录系统中,某位患者的电子病历只允许脑科专家访问,那么从这条策略就能间接推断出该

收稿日期: 2016-12-29 修回日期: 2017-04-20 网络出版时间: 2017-11-15
基金项目: 国家 242 信息安全计划(2015A051,2012A138);国家十一五科技支撑计划课题(2007BAK34B06);十五科技攻关计划课题(2004BA811B04)
作者简介: 陈丹伟(1970-),男,教授,博士,研究方向为信息安全、计算机应用;汤 波(1989-),男,硕士,研究方向为信息安全。
网络出版地址: http://kns.cnki.net/kcms/detail/61.1450.TP.20171115.1128.004.html

患者很有可能脑部患有疾病，由此看出访问策略同样需要加以保护。因此，2008 年 Nishide 等[8] 提出了一种可以隐藏部分访问策略的加密方案，用多值属性之间的与逻辑表示访问策略，实现了同时保护消息和访问结构私密性的功能。2011 年，Lai[9] 等在合数阶双线性群的基础上提出了一种隐藏访问策略的 CP-ABE 方案，并证明其是完全安全的。2012 年，王海斌等[10] 提出一种素数阶双线性群的策略隐藏 CP-ABE 方案，使私钥长度和解密算法中的双线性配对运算为固定值，方案中采用多值属性与门的访问结构。2013 年，Sreenivasa[11] 等提出了一种匿名接收的 CP-ABE 方案，其采用与门的访问结构，并证明是完全安全的。2015 年，宋衍等[12] 提出一种基于访问树的策略隐藏属性加密方案，并证明其是自适应安全的。

以上的隐藏策略的属性基加密方案大多采用与门或访问树的访问结构，在策略表达上有诸多限制，而 LSSS 矩阵在访问策略表达上更强，可表达任意访问策略，包括与门或门和门限，访问结构灵活。2011 年，Waters[13] 提出了一种基于 LSSS 访问矩阵的 CP-ABE 方案，但方案中并没有对访问策略进行隐藏。2012 年，Lai 等[14] 提出了一种基于 LSSS 访问矩阵隐藏部分访问策略的 CP-ABE 方案。在借鉴上述方案的基础上，文中提出一种基于 LSSS 隐藏访问策略的 CP-ABE 方案，应用合数阶双线性群来隐藏访问策略，使用双系统加密机制证明其安全性。

1 预备知识

本节介绍相关的基础知识，包括合数阶双线性群、子群假设问题、访问结构以及线性秘密共享方案。

1.1 合数阶双线性群

应用阶为 $Q = p_1p_2p_3$ 的双线性群，其中 p_1、p_2、p_3 为三个不同的素数，G_0 和 G_1 是两个阶为 $Q = p_1p_2p_3$ 的乘法循环群，G_{p_i} 是群 G_0 的阶为 p_i 的子群，$G_{p_ip_j}(i \neq j)$ 是群 G_0 的阶为 p_ip_j 的子群。双线性映射 $e: G_0 \times G_0 \rightarrow G_1$ 满足如下性质：

(1) 双线性：对于任意的 $u, v \in G_0$ 和 $a, b \in Z_p$，都有 $e(u^a, v^b) = e(u, v)^{ab}$。

(2) 非退化性：存在 $g \in G_0$，使得 $e(g, g)$ 在 G_1 中的阶为 Q。

(3) 可计算性：对于任意的 $u, v \in G_0$，存在一个有效的算法以计算 $e(u, v)$。

(4) 子群正交性：对 $\forall g_i \in G_{p_i}, \forall g_j \in G_{p_j}(i \neq j)$，有 $e(g_i, g_j) = 1$。

1.2 合数阶子群判定假设

应用 Lewko 中的子群判定假设[15]，后面会依赖这些假设证明方案的安全性。

假设 1：给定一个双线性群生成器 Φ，定义如下分布：$G = (Q = p_1p_2p_3, G_0, G_1, e) \leftarrow \Phi, g_1 \leftarrow G_{p_1}, Z_2 \leftarrow G_{p_2}, D = (G, g_1, Z_2), T_1 \leftarrow G_{p_1p_3}, T_2 \leftarrow G_{p_1}$。

定义算法 Ψ 攻破假设 1 的优势为：

$$\mathrm{Adv1}_{\Phi,\Psi(\lambda)} = |\Pr[\Psi(D, T_1) = 1] - \Pr[\Psi(D, T_2) = 1]|$$

假设 2：给定一个双线性群生成器 Φ，定义如下分布：$G = (Q = p_1p_2p_3, G_0, G_1, e) \leftarrow \Phi, g_1, Z_1 \leftarrow G_{p_1}, g_2 \leftarrow G_{p_2}, Z_3 \leftarrow G_{p_3}, D = (G, g_1, g_2, Z_1Z_3), T_1 \leftarrow G_{p_1p_3}, T_2 \leftarrow G_{p_1}$。

定义算法 Ψ 攻破假设 2 的优势为：

$$\mathrm{Adv2}_{\Phi,\Psi(\lambda)} = |\Pr[\Psi(D, T_1) = 1] - \Pr[\Psi(D, T_2) = 1]|$$

假设 3：给定一个双线性群生成器 Φ，定义如下分布：$G = (Q = p_1p_2p_3, G_0, G_1, e) \leftarrow \Phi, \alpha, s \leftarrow Z_N, g_1 \leftarrow G_{p_1}, X_2 \leftarrow G_{p_2}, X_3, Y_3, Z_3 \leftarrow G_{p_3}, D = (G, g_1, g_1^{\alpha}X_3, X_2, g_1^{s}Y_3, Z_3), T_1 = e(g_1, g_1)^{\alpha s}, T_2 \leftarrow G_1$。

定义算法 Ψ 攻破假设 3 的优势为：

$$\mathrm{Adv3}_{\Phi,\Psi(\lambda)} = |\Pr[\Psi(D, T_1) = 1] - \Pr[\Psi(D, T_2) = 1]|。$$

定理 1：如果对于假设 1、2 和 3，算法 Ψ 攻破它们的优势是可忽略的，那么就认为该方案是安全的。

1.3 访问结构

设 $\{P_1, P_2, \cdots, P_n\}$ 是由 n 个参与者组成的实体集，集合 $A \subseteq 2^{\{p_1, p_2, \cdots, p_n\}}$，如果对于 $\forall B, C, B \in A, B \subseteq C$，有 $C \in A$，那么 A 就是单调的。如果集合 A 是 $\{P_1, P_2, \cdots, P_n\}$ 的非空子集，即 $A \subseteq 2^{\{p_1, p_2, \cdots, p_n\}} \setminus \{\varnothing\}$，那么 A 就是一个访问结构，包含在 A 中的集合称为授权集，不包含在 A 中的集合就称为非授权集。

1.4 线性秘密共享方案

一个定义在实体集 P 上的线性秘密共享方案 $\prod$ (LSSS) 满足以下两点：

(1) 所有实体的共享组成 Z_p 上的一个向量；

(2) 存在一个 $l \times n$ 的 $\prod$ 的共享矩阵 M 和一个从 $\{1, 2, \cdots, l\}$ 到 P 的映射，随机选取 $v = (s, r_2, \cdots, r_n) \in Z_p$，$s \in Z_p$ 是需要共享的秘密，那么 M_v 是根据 $\prod$ 得到的关于 s 的 l 个共享组成的向量，其中 $(M_v)_i$ 属于实体 $\rho(i)$，记作 λ_i。

由以上定义得到的每一个线性秘密共享方案都具有线性重构的性质。假设 $\prod$ 是一个对应于访问结构 A 的线性秘密共享方案，对于任何授权集 $S \in A$，定义 $I = \{i: \rho(i) \in S\} \subset \{1, 2, \cdots, l\}$，如果 $\{\lambda_i\}$ 是秘密 s 根据 $\prod$ 的有效分享，则存在一个常数集 $\{\omega_i \in Z_p\}_{i \in I}$，使得 $\sum_{i \in I} \omega_i \lambda_i = s$；对于任何非授权集，存在向量 $w \in Z_p$，使得 $w \cdot (1, 0, \cdots, 0)^{\mathrm{T}} = -1, w \cdot M_i = 0, i \in I$。

2　基于 LSSS 隐藏策略的 CP-ABE 方案

2.1　CP-ABE 方案的安全模型

该系统的安全模型基于选择明文攻击,称为选择明文攻击游戏(IND-CPA),定义模型的交互步骤如下:

(1) 系统建立: 挑战者运行系统初始化算法,生成系统公钥 PK 和主私钥 MSK,并将 PK 发送给敌手。

(2) 阶段 1: 敌手向挑战者进行属性集 $\{S_1,\cdots,S_{q_1}\}$ 的私钥询问,挑战者使用密钥生成算法生成私钥 $\{SK_1,\cdots,SK_{q_1}\}$,然后返回给敌手。

(3) 挑战阶段: 敌手提交两个相同长度的明文消息 M_0 和 M_1 以及两个访问结构 (M_0,ρ_0) 和 (M_1,ρ_1) 发送给挑战者。挑战者抛掷一枚公平硬币 $\beta\in\{0,1\}$,使用访问结构 (M_β,ρ_β) 对消息 M_β 进行加密,并将密文 CT 发送给敌手。

(4) 阶段 2: 重复执行阶段 1。

(5) 猜测: 敌手根据密文 CT 对 β 进行猜测,得到预测 β'。如果 $\beta'=\beta$,则认为敌手赢得了游戏。

攻击者赢得上述游戏的概率为:

$$\left|\Pr[\beta'=\beta]-\frac{1}{2}\right|$$

对于一个加密方案,如果在任意概率多项式时间内,敌手在游戏中的优势是可忽略的,即其赢得游戏的概率都趋近于 0,则称该加密方案 IND-CPA 安全。

2.2　隐藏策略的 CP-ABE 方案描述

该方案主要包括四个算法: 系统建立算法、加密算法、密钥生成算法以及解密算法。详细过程如下:

(1) 系统建立算法(Setup)。

输入: 安全参数 λ 以及系统属性个数 N。

过程: 利用算法中的双线性参数生成器生成 $\Phi=(Q=p_1p_2p_3,G_0,G_1,e)$,其中 p_1,p_2,p_3 是三个不同的素数,g_1 为 G_{p_1} 的生成元,g_2 为 G_{p_2} 的生成元,g_3 为 G_{p_3} 的生成元,随机选择 $h_1,h_2,\cdots,h_N\in G_{p_1}$,取 $a,\alpha,t_1,t_2,\cdots,t_N\in Z_N$,属性集 $A_1=h_1g_2^{t_1},\cdots,A_N=h_Ng_2^{t_N}$。

输出: 系统公钥 PK 和主私钥 MSK。

$$PK=\{\Phi,g_1,g_2,g_1^a,e(g_1,g_1)^\alpha,A_1,\cdots,A_N\}$$

$$MSK=\{g_1^a\}$$

(2) 加密算法(Encryption)。

输入: 系统公钥 PK,待加密消息 M 以及 LSSS 对应的 (M,ρ)。

过程: M 是一个 $l\times n$ 的秘密分享矩阵,通过函数 ρ 将矩阵 M 中的每一行与属性对应,算法选择一个随机向量 $v=(s,y_2,y_3,\cdots,y_n)\in Z_p^n$,其中 s 是待分享的秘密指数。对于 $i=1,2,\cdots,l$,计算 $\lambda_i=v\cdot M_i$,随机选择 $r_1,r_2,\cdots,r_l\in Z_N$,$\{X_i,X_i'\in G_{p_2}\}_{i\in\{1,2,\cdots,l\}}$ 生成密文 CT。

输出: 密文 CT。

$$C=Me(g_1,g_1)^{\alpha s}$$

$$C'=g_1^s$$

$$(C_1=g_1^{a\lambda_1}A_{\rho(1)}^{-r_1}X_1',D_1=g_1^{r_1}X_1),\cdots,(C_l=g_1^{a\lambda_l}A_{\rho(l)}^{-r_l}X_l',D_l=g_1^{r_l}X_l)$$

(3) 密钥生成算法(KeyGen)。

输入: 主私钥 MSK 和用户属性集 S。

过程: 算法选择一个随机数 $t\in Z_p$,计算用户的私钥 SK。

输出: 密钥 $SK=\{K=g_1^\alpha g_1^{at},L=g_1^t,SK_x=h_x^t,\forall x\in S\}$。

(4) 解密算法(Decryption)。

输入: 密文 CT 以及用户私钥 SK。

过程: 若 S 是一个授权集,则满足 (M,ρ) 且 $I=\{i:\rho(i)\in S\}$,那么在多项式时间内能找到一组常数集 $\{\omega_i\in Z_N\}_{i\in I}$,使得 $\sum_{i\in I}\omega_i\lambda_i=s$,其中 λ_i 是秘密 s 的有效分享,可以解密成功,解密算法首先计算:

$$e(C',K)/\left(\prod_{i\in I}(e(C_i,L)e(D_i,SK_{\rho(i)}))^{\omega_i}\right)=e(g_1,g_1)^{\alpha s}$$

然后通过密文 C 将明文 M 恢复; 若 S 是一个非授权集,那么解密失败。

输出: 明文 M。

2.3　正确性推导

若用户的属性集 S 是一个授权集,那么用户获得对应的私钥 SK,且 $\sum_{i\in I}\omega_i\lambda_i=s$,进行如下解密运算:

$$\frac{e(C',K)}{\prod_{i\in I}(e(C_i,L)e(D_i,SK_{\rho(i)}))^{\omega_i}}=$$

$$\frac{e(g_1^s,g_1^\alpha g_1^{at})}{\prod_{i\in I}(e(g_1^{a\lambda_i}A_{\rho(i)}^{-r_i}X_i',g_1^t)e(g_1^{r_i}X_i,h_{\rho(i)}^t))^{\omega_i}}=$$

$$\frac{e(g_1,g_1)^{\alpha s}e(g_1,g_1)^{ast}}{\prod_{i\in I}(e(g_1^{a\lambda_i}(h_{\rho(i)}g_2^{t_{\rho(i)}})^{-r_i}X_i',g_1^t)e(g_1^{r_i}X_i,h_{\rho(i)}^t))^{\omega_i}}=$$

$$\frac{e(g_1,g_1)^{\alpha s}e(g_1,g_1)^{ast}}{\prod_{i\in I}(e(g_1^{a\lambda_i}h_{\rho(i)}^{-r_i},g_1^t)e(g_1^{r_i}X_i,h_{\rho(i)}^t))^{\omega_i}}=$$

$$\frac{e(g_1,g_1)^{\alpha s}e(g_1,g_1)^{ast}}{\prod_{i\in I}(e(g_1^{a\lambda_i},g_1^t)e(h_{\rho(i)}^{-r_i},g_1^t)e(g_1^{r_i},h_{\rho(i)}^t))^{\omega_i}}=$$

$$\frac{e(g_1,g_1)^{\alpha s}e(g_1,g_1)^{ast}}{\prod_{i\in I}(e(g_1^{a\lambda_i},g_1^t))^{\omega_i}}=$$

$$\frac{e(g_1,g_1)^{\alpha s}e(g_1,g_1)^{ast}}{e(g_1,g_1)^{at\sum_{i\in I}\lambda_i\omega_i}}=$$

$$e(g_1,g_1)^{\alpha s}$$

最后通过 $C/e(g_1,g_1)^{\alpha s}$ 即可恢复明文 M。

2.4 策略隐藏

假设敌手得到一个访问策略 (M',ρ') 以及一个密文 $CT=(C,C',(C_i,D_i)_{i=1,2,\cdots,l})$，其中密文 CT 是在策略 (M,ρ) 下加密得到的，敌手会根据策略 (M',ρ') 选择 $I'\subset\{1,2,\cdots,l\}$，$\{\lambda_i'\}$ 是秘密 s 根据 M' 的有效分享，那么在多项式时间内能够找到这样一组常数 $\{\omega_i'\in Z_N\}_{i\in I'}$，使得 $\sum_{i\in I'}\omega_i'\lambda_i'=s$。为了确定密文 CT 是否由 (M',ρ') 加密得到，敌手会进行下面的一系列运算:

$$\frac{e(C',g_1^a)}{\prod_{i\in I'}(e(C_i,g_1)e(D_i,A_{\rho(i)}))^{\omega_i'}}=$$

$$\frac{e(g_1^s,g_1^a)}{\prod_{i\in I'}(e(g_1^{a\lambda_i'}(h_{\rho(i)}g_2^{t_{\rho(i)}})^{-r_i'}X_i',g_1)e(g_1^{r_i'}X_i',h_{\rho(i)}g_2^{t_{\rho(i)}}))^{\omega_i'}}=$$

$$\frac{e(g_1^s,g_1^a)}{\prod_{i\in I'}(e(g_1^{a\lambda_i'}h_{\rho(i)}^{-r_i'},g_1)e(g_1^{r_i'}X_i',h_{\rho(i)}g_2^{t_{\rho(i)}}))^{\omega_i'}}=$$

$$\frac{e(g_1,g_1)^{as}}{\prod_{i\in I'}(e(g_1^{a\lambda_i'}h_{\rho(i)}^{-r_i'},g_1)e(g_1^{r_i'},h_{\rho(i)})e(X_i',g_2^{t_{\rho(i)}}))^{\omega_i'}}=$$

$$\frac{e(g_1,g_1)^{as}}{\prod_{i\in I'}(e(g_1^{a\lambda_i'},g_1)e(X_i',g_2^{t_{\rho(i)}}))^{\omega_i'}}=$$

$$\frac{e(g_1,g_1)^{as}}{e(g_1,g_1)^{a\sum_{i\in I'}\lambda_i'\omega_i'}\prod_{i\in I'}(e(X_i',g_2^{t_{\rho(i)}}))^{\omega_i'}}$$

不难看出，上式中存在 G_{p_2} 中的随机元素，所以敌手并不能确定密文 CT 由哪个访问策略加密得到，因此通过 G_{p_2} 能够实现访问策略的隐藏。

2.5 安全性证明

使用 Waters 等[16]提出的双系统加密技术来证明本方案的安全性。由于需要借助两个新的概念: 半功能密文和半功能私钥，所以首先给出它们的定义。

半功能密文: 运用加密算法得到正常密文 $(C',C'',(C_i',D_i')_{i=1,2,\cdots,l})$，随机选择 $b_0\in Z_N,b_i\in Z_N(1\leqslant i\leqslant l)$，生成半功能密文: $(C=C',C'=C''g_3^{b_0},(C_i=C_i'g_3^{b_i},D_i=D_i'g_3^{b_i})_{i=1,2,\cdots,l})$。

半功能私钥: 运用密钥生成算法得到正常私钥 $(K',L',\mathrm{SK}_x',\forall x\in S)$，随机选择 $d,d',d_i\in Z_N(1\leqslant i\leqslant n)$，其中 n 为用户属性的个数，生成半功能私钥如下: $(K=K'g_3^d,L=L'g_3^{d'},\mathrm{SK}_x=\mathrm{SK}_x'g_3^{d_i},(i=1,2,\cdots,n))$。

当用户拥有的属性集满足访问结构时，正常私钥可以解密半功能密文，半功能私钥可以解密正常密文，但半功能私钥不能解密半功能密文。

文中借助一系列相邻游戏的不可区分性来证明方案的安全性。假设敌手在一次游戏中共做了 q 次私钥询问，定义如下一些游戏:

$\mathrm{Game}_{\mathrm{real}}$: 这个游戏是真实的安全游戏，也就是密文和所有的私钥都是正常的。

Game_0: 在这个游戏中，挑战密文是半功能的，所有的私钥是正常的。

$\mathrm{Game}_{k,l}$: 在这个游戏中，挑战密文是半功能的，前 k 次的私钥是半功能私钥，剩下的私钥都是正常的。

$\mathrm{Game}_{\mathrm{final}}$: 在这个游戏中，所有的私钥都是半功能私钥，挑战密文是对一个随机消息加密生成的半功能密文。

引理 1: 如果存在一个多项式时间内的算法 Ψ 在 $\mathrm{Game}_{\mathrm{real}}$ 和 Game_0 上的优势满足 $\mathrm{Game}_{\mathrm{real}}\ \mathrm{Adv}_{\Phi}-\mathrm{Game}_0\ \mathrm{Adv}_{\Phi}=\varepsilon$，那么可以构造一个多项式时间算法 Ψ 以 ε 的优势攻破假设 1。

证明: 给定假设条件 $D=(G,g_1,Z_2)$。

系统建立: 和 2.2 节中的系统建立算法一样。

阶段 1: 敌手 A 通过密钥生成算法询问私钥。

挑战阶段: 敌手 A 选择两个等长的明文 M_0 和 M_1 以及访问结构 (M_0,ρ_0) 和 (M_1,ρ_1) 发送给挑战者 B，挑战者随机选择 $\beta\in(0,1)$，用访问结构 (M_β,ρ_β) 来加密 M_β，挑战者 B 根据主密钥以及假设条件生成密文，$C^*=M_\beta e(g_1^\alpha,T)$，$C''=T,C_i^*=T^{a\lambda_i}A_{\rho(i)}^{-r_i}X_i',D_i=T^{r_i}X_i,i=1,2,\cdots,l$，然后挑战者 B 向敌手 A 发送密文 $(C^*,C'',(C_i^*,D_i^*)_{i=1,2,\cdots,l})$。

阶段 2: 重复执行阶段 1。

猜测: 敌手 A 输出一个关于 β 的猜测 β'。

如果 $T=T_1\in G_{p_1p_3}$，那么密文为半功能密文; 如果 $T=T_2\in G_{p_3}$，那么密文是正常密文。因此，若敌手 A 使 $\mathrm{Game}_{\mathrm{real}}\ \mathrm{Adv}_{\Phi}-\mathrm{Game}_0\ \mathrm{Adv}_{\Phi}=\varepsilon$ 不可忽视，那么挑战者 B 同样能够以不可忽略的优势区分 G_{p_1} 和 $G_{p_1p_3}$ 上的元素。

引理 2: 如果存在一个多项式时间内的算法 Ψ 在 $\mathrm{Game}_{k-1,1}$ 和 $\mathrm{Game}_{k,1}$ 上的优势满足 $\mathrm{Game}_{k-1,1}\ \mathrm{Adv}_{\Phi}-\mathrm{Game}_{k,1}\ \mathrm{Adv}_{\Phi}=\varepsilon$，那么可以构造一个多项式时间算法 Ψ 以 ε 的优势攻破假设 2。

证明: 给定假设条件 $D=(G,g_1,g_2,Z_1Z_3)$。

系统建立: 和 2.2 节中的系统建立算法一样。

阶段 1: 敌手 A 通过密钥生成算法进行第 x 次询问私钥，如果 $x\leqslant k$，那么根据主密钥和假设条件生成半功能私钥 $K=g_1^\alpha T^a,L=T$; 如果 $x>k$，那么生成的是正常私钥。

挑战阶段: 敌手 A 选择两个等长的明文 M_0 和 M_1 及访问结构 (M_0,ρ_0) 和 (M_1,ρ_1) 发送给挑战者 B，挑战者随机选择 $\beta\in(0,1)$，用访问结构 (M_β,ρ_β) 加密 M_β，挑战者 B 根据主密钥及假设条件生成密文，$C^*=M_\beta e(g_1,Z_1Z_3)^{\alpha s},C''=(Z_1Z_3)^s,C_i^*=(Z_1Z_3)^{a\lambda_i}A_{\rho(i)}^{-r_i}X_i',D_i=(Z_1Z_3)^{r_i}X_i,i=1,2,\cdots,l$，然后挑战者 B 向敌手 A

发送密文 $(C^*, C', (C_i^*, D_i^*)_{i=1,2,\cdots,l})$。

阶段 2: 重复执行阶段 1。

猜测: 敌手 A 输出一个关于 β 的猜测 β'。

如果 $T \in G_{p_1}$，那么密钥为正常密钥，进行的游戏是 $\mathrm{Game}_{k-1,1}$；如果 $T \in G_{p_1p_3}$，那么密钥为半功能密钥，进行的游戏是 $\mathrm{Game}_{k,1}$。因此，若敌手 A 使 $\mathrm{Game}_{k-1,1}\ \mathrm{Adv}_{\Phi} - \mathrm{Game}_{k,1}\ \mathrm{Adv}_{\Phi} = \varepsilon$ 不可忽视，那么挑战者 B 同样能够以不可忽略的优势区分 G_{p_1} 和 $G_{p_1p_3}$ 上的元素。

引理 3: 如果存在一个多项式时间内的算法 Ψ 在 $\mathrm{Game}_{q,1}$ 和 $\mathrm{Game}_{\mathrm{final}}$ 上的优势满足 $\mathrm{Game}_{q,1}\ \mathrm{Adv}_{\Phi} - \mathrm{Game}_{\mathrm{final}}\ \mathrm{Adv}_{\Phi} = \varepsilon$，那么可以构造一个多项式时间算法 Ψ 以 ε 的优势攻破假设 3。

证明: 给定假设条件 $D = (G, g_1, g_1^{\alpha}X_3, X_2, g_1^{s}Y_3, Z_3)$。

系统建立: 和 2.2 节中的系统建立算法一样。

阶段 1: 敌手 A 通过密钥生成算法进行私钥询问，挑战者 B 根据敌手 A 的属性集生成密钥: $K = g_1^{\alpha}X_3 (g_1^{t}Z_3)^{a}$，$L = g_1^{t}Z_3^{w}$，其中随机元素 $w \in Z_N$。

挑战阶段: 敌手 A 选择两个等长的明文 M_0 和 M_1 以及访问结构 (M_0, ρ_0) 和 (M_1, ρ_1) 发送给挑战者 B，挑战者随机选择 $\beta \in (0,1)$，用访问结构 (M_β, ρ_β) 来加密 M_β，挑战者 B 根据主密钥以及假设条件生成密文，$C^* = M_\beta T$，$C' = g_1^{\alpha}X_3$，$C_i^* = (g_1^{s}Y_3)^{a\lambda_i}A_{\rho(i)}^{-r_i}X_i'$，$D_i = (g_1^{s}Y_3)^{r_i}X_i$，$i = 1,2,\cdots,l$，然后挑战者 B 向敌手 A 发送密文 $(C^*, C', (C_i^*, D_i^*)_{i=1,2,\cdots,l})$。

阶段 2: 重复执行阶段 1。

猜测: 敌手 A 输出一个关于 β 的猜测 β'。

如果 $T = T_1 = e(g_1, g_1)^{\alpha s}$，那么生成的是 M_β 的半功能密文; 如果 $T = T_2 \in G_{p_1}$，那么生成的是随机消息的半功能密文。因此，若敌手 A 使 $\mathrm{Game}_{q,1}\ \mathrm{Adv}_{\Phi} - \mathrm{Game}_{\mathrm{final}}\ \mathrm{Adv}_{\Phi} = \varepsilon$ 不可忽视，那么挑战者 B 同样能够以不可忽略的优势区分 $T_1 = e(g_1, g_1)^{\alpha s}$ 和 G_1 上的元素。

至此，定理 1 证明完毕。

2.6　效率分析

主要从算法的运算量以及密文、密钥、公钥长度两个方面来分析上述方案的效率。

算法执行的时间主要分布在指数(Exp)和双线性配对(Pairing)运算上，所以主要分析这两种运算。加密算法主要涉及指数 Exp 运算，而解密算法主要涉及 Pairing 运算。

在上述方案中，N 为系统属性个数，n 为用户属性个数，系统建立阶段的运算主要包括: 双线性配对运算 $e(g_1, g_1)$，G_{p_1} 上的指数运算 $e(g_1, g_1)^{\alpha}$ 以及 G_{p_2} 上的指数运算 $A_1 = h_1 g_2^{t_1}, \cdots, A_N = h_N g_2^{t_N}$; 加密阶段的运算量主要由访问策略 (M, ρ) 来决定，主要的运算包括: G_{p_1} 上的指数运算 $C = Me(g_1, g_1)^{\alpha s}$，$C' = g_1^{s}$ 以及 G_{p_2} 上的指数运算: $(C_1 = g_1^{a\lambda_1}A_{\rho(1)}^{-r_1}X_1', D_1 = g_1^{r_1}X_1), \cdots, (C_l = g_1^{a\lambda_l}A_{\rho(l)}^{-r_l}X_l', D_l = g_1^{r_l}X_l)$。

密钥生成阶段主要的运算为 G_{p_1} 上的指数运算 $K = g_1^{\alpha}g_1^{\alpha t}$，$L = g_1^{t}$，$\mathrm{SK}_x = h_x^{t}, \forall x \in S$; 解密阶段主要进行的是双线性配对运算:

$$\prod_{i \in I} \left(e(C_i, \mathrm{SK}_2)\, e(D_i, \mathrm{SK}_{\rho(i)})\right)^{\omega_i}$$

从计算次数以及消息长度两个方面对比上述方案与基于 LSSS 隐藏策略的 CP-ABE 方案(简称 Lai 方案)[14]，结果见表 1 和表 2。

表 1　计算次数比较

阶段	运算类型	文中方案	Lai 方案
初始化	Exp	$N+3$	2
	Pairing	1	1
加密	Exp	$3l+2$	$6l+4$
	Pairing	1	2
密钥生成	Exp	$n+3$	$2n+3$
	Pairing	0	0
解密	Exp	$\lvert I\rvert$	$\lvert I\rvert$
	Pairing	$2\lvert I\rvert+1$	$2\lvert I\rvert+1$

表 2　消息长度比较

消息	文中方案	Lai 方案
公钥	$(2+N)\lvert G_{p_1}\rvert + (1+N)\lvert G_{p_2}\rvert$	$(3+n)\lvert G_{p_1}\rvert + 2\lvert G_{p_4}\rvert$
主密钥	$\lvert G_{p_1}\rvert$	$\lvert G_{p_1}\rvert + \lvert G_{p_3}\rvert$
私钥	$2\lvert G_{p_1}\rvert$	$\lvert G_{p_1}\rvert + \lvert G_{p_3}\rvert$
密文	$(3l+1)\lvert G_{p_1}\rvert + 3l\lvert G_{p_2}\rvert$	$(6l+2)\lvert G_{p_1}\rvert + 4l\lvert G_{p_4}\rvert$

从表 1 可以看出，对于系统建立阶段，首先对 N 个属性进行处理，因此会多出 N 个指数运算，在加密和密钥生成阶段，文中方案的指数运算次数都为对比方案的一半，双线性配对运算次数则差不多，而解密阶段两个方案的运算次数则相同。

从表 2 可以看出，文中方案会使得公钥长度有所增加，但密文长度减少一半，总体来说，文中方案会增加一些系统存储空间。

最后，通过仿真实验，将文中方案与 Lai 方案在加密时间上作一个比较，结果如图 1 所示。

从图 1 可以看出，加密时间随着访问结构中属性个数的增加基本呈线性增长的趋势，在相同的属性个数下，文中方案所用加密时间要少于 Lai 方案，且属性个数越多，相应减少的时间也越多。

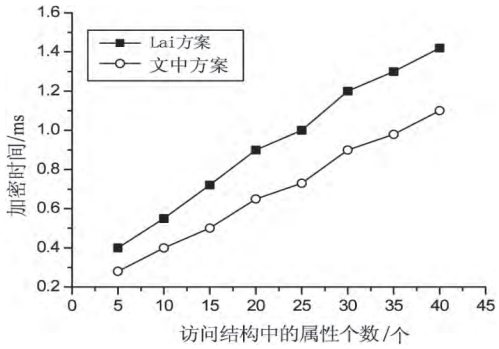

图 1 加密时间对比曲线

3 结束语

在现有 CP-ABE 方案的基础上，提出了一种基于 LSSS 隐藏策略的 CP-ABE 方案。该方案使用 LSSS 来表示访问结构，使得策略表达更为灵活，通过 3 素数合数阶双线性群来构造方案，实现了访问策略的隐藏，保护了访问策略中的敏感信息；同时，从指数和双线性配对运算次数和密文、密钥长度等方面对该方案进行了效率分析。结果表明，该方案提高了加密效率，但也增加了密文、密钥等消息的长度，因此如何减小消息长度从而减少系统存储空间是今后进一步研究的工作。

参考文献：

[1] SAHAI A, WATERS B. Fuzzy identity-based encryption [C] //Annual international conference on the theory and applications of cryptographic techniques. Berlin: Springer-Verlag, 2005: 457-473.

[2] 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. New York, NY, USA: ACM, 2006: 89-98.

[3] BETHENCOURT J, SAHAI A, WATERS B. Ciphertext-policy attribute-based encryption [C] //IEEE symposium on security and privacy. [s.l.]: IEEE, 2007: 321-334.

[4] CHEUNG L, NEWPORT C. Provably secure ciphertext policy ABE [C] //Proceeding of the ACM conference on computer and communications security. New York, NY, USA: ACM, 2007: 456-465.

[5] GOYAL V, JAIN A, PANDEY O, et al. Bounded ciphertext policy attribute based encryption [C] //Proceedings of the 35th international colloquium on automata, languages and programming, part II. Berlin: Springer-Verlag, 2008: 579-591.

[6] IBRAIMI L, TANG Q, HARTEL P. Efficient and provable Secure ciphertext-policy attribute-based encryption schemes [C] //Proceedings of the 5th international conference on information security practice and experience. Berlin: Springer-Verlag, 2009: 1-12.

[7] EMURA K, MIYAJI A, NOMURA A, et al. A ciphertext-policy attribute-based encryption scheme with constant ciphertext length [C] //IS-PEC 2009. Berlin: Springer-Verlag, 2009: 13-23.

[8] NISHIDE T, YONEYAMA K, OHTA K. Attribute-based encryption with partially hidden encryptor-specified access structure [C] //Proceedings of the 6th international conference on applied cryptography and network security. Berlin: Springer-Verlag, 2008: 111-129.

[9] LAI J Z, DENG R H, LI Y J. Fully secure cipertext-policy hiding CP-ABE [C] //Proceedings of the 7th information conference on security practice and experience. Berlin: Springer-Verlag, 2011: 24-39.

[10] 王海斌，陈少真. 隐藏访问结构的基于属性加密方案 [J]. 电子与信息学报，2012，34(2)：457-461.

[11] RAO Y S, DUTTA R. Recipient anonymous ciphertext-policy attribute based encryption [C] //Proceedings of the 9th international conference on information systems security. New York, NY, USA: Springer-Verlag New York, Inc., 2013.

[12] 宋 衍，韩 臻，刘凤梅，等. 基于访问树的策略隐藏属性加密方案 [J]. 通信学报，2015，36(9)：119-126.

[13] WATERS B. Ciphertext-policy attribute-based encryption: an expressive, efficient, and provably secure realization [C] //Proceedings of the 14th international conference on practice and theory in public key cryptography. Berlin: Springer-Verlag, 2011: 53-70.

[14] LAI J, DENG R H, LI Y. Expressive CP-ABE with partially hidden access structures [C] //Proceedings of the 7th ACM symposium on information, computer and communications and security. New York, NY, USA: ACM, 2012.

[15] LEWKO A, OKAMOTO T, SAHAI A, et al. Fully secure functional encryption: attribute-based encryption and (hierarchical) inner product encryption [C] //Proceedings of the 29th annual international conference on theory and applications of cryptographic techniques. Berlin: Springer-Verlag, 2010: 62-91.

[16] LEWKO A, WATERS B. New techniques for dual system encryption and fully secure hibe with short ciphertexts [C] //7th theory of cryptography conference. Berlin: Springer-Verlag, 2010.