隐藏访问结构的基于属性加密方案

王海斌* 陈少真
(信息工程大学信息工程学院 郑州 450002)

摘 要：该文利用双系统密码技术在素数群中提出了一个具有隐藏访问结构功能的基于属性加密方案。该方案的安全性依赖于 D-Linear 假设和 DBDH(Decision Bilinear Diffie-Hellman)假设，并且在标准模型下证明是完全安全的。同时，方案中用户私钥长度和解密过程中双线性对的运算量都为固定值，适用于存储量和计算量小的系统。

关键词：基于属性的加密；隐藏访问结构；完全安全；双线性对
中图分类号：TP309 **文献标识码**：A **文章编号**：1009-5896(2012)02-0457-05
DOI: 10.3724/SP.J.1146.2011.00682

Attribute-based Encryption with Hidden Access Structures

Wang Hai-bin Chen Shao-zhen
(*Institute of Information Engineering*, *Information Engineering University*, *Zhengzhou* 450002, *China*)

Abstract: Using dual system encryption, a attribute-based encryption scheme with hidden access structures is proposed in prime order bilinear group in this paper. The scheme relies on the D-Linear and Decision Bilinear Diffie-Hellman (DBDH) assumptions, and is proven fully secure under standard model. Moreover, it is suitable for the system with lower storage devices and higher efficiency computations because it achieves constant size private key and constant length of pairing computations.

Key words: Attribute-based encryption; Hidden access structures; Fully secure; Bilinear pairing

1 引言

2005 年 Sahai 等人[1]在欧密会上提出了基于属性的加密体制(Attribute-Based Encryption, ABE)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 等人[2]将基于属性加密体制分为密文策略(CP-ABE)和密钥策略(KP-ABE)两种。所谓密文策略，是指密文和一个访问结构结合而密钥对应于一个属性集合，当且仅当密钥中的属性能够满足访问结构时才能解密。所谓的密钥策略，是指密钥和一个访问结构相对应，而密文和一个属性集合相结合，当且仅当密文的属性集合满足密钥的访问结构时才能解密。本文重点研究密文策略的加密体制。以往提出的大多数基于属性加密方案[3−5]都只有保护消息私密性的功能，2008 年 Nishide 等人[6]提出了一个可以隐藏访问结构的加密方案，实现了同时保护消息和访问结构私密性的功能，但是该方案的安全模型较弱。2011 年 Lai 等人[7]利用子群判定假设在合数阶群中提出了一个新的可以隐藏访问结构的加密方案，并证明是完全安全的。但是为了达到一定的安全级别，合数群的阶会取得比较大。例如，在椭圆曲线上，相同的安全级别，合数群的阶至少为 1024 bit，而素数群的阶只需要 160 bit 就可以了，因此双线性对的计算效率在合数群中会比素数群中低很多，差别大约为 50 倍，并且当安全级别提高时，这个差距会更大[8]。

本文利用双系统密码技术[9]首次在素数群中提出了一个可以隐藏访问结构的基于属性加密方案，并且依赖于 D-Linear 假设和 DBDH(Decision Bilinear Diffie-Hellman)假设[10]，在标准模型下证明是完全安全的。同时，方案中用户私钥长度和解密过程中双线性对的运算量都为固定值，因此，该方案适用于存储量和计算量较小的系统。

2 预备知识

2.1 双线性映射

设 G_1, G_2 是阶为素数 p 的乘法循环群，g 是 G_1 的生成元。双线性映射 $e: G_1 \times G_1 \to G_2$ 满足下面性质：

双线性：$e(g^a, h^b) = e(g,h)^{ab}$，$g$, h 是 G_1 中的元素，a, b 是 Z_p^* 中的元素。

非退化性：$e(g,g) \neq 1$。

可计算性：对 G_1 中的所有元素 g, h，存在一个有效的算法计算 $e(g,h)$。

2011-07-06 收到，2011-10-25 改回
国家自然科学基金(60833008)，信息安全国家重点实验室开放课题基金(01-02-8)和全军军事学研究生课题资助项目
*通信作者：王海斌 wanghaibin4882@126.com

2.2 访问结构

设 $U=\{A_1,A_2,\cdots,A_n\}$ 是所有的属性集合，每个属性 A_i 有 l_i 个值 $\{A_i^1,A_i^2,\cdots,A_i^{l_i}\}$，该方案中的访问结构为操作符“与门”连接不同的属性，“或门”连接同一个属性的不同取值。

例如 A_1 表示性别，则 A_1 有两个值{ A_1^1 =“男”，A_1^2 =“女””}，A_2 表示年龄，则我们可以定义以下 3 个值{ A_2^1 =“40 岁以下”，A_2^2 =“40–60 岁”，A_2^3 =“60 岁以上”}。假设我们定义的访问结构 $\mathbb{A}$ 为“40 岁以上的男士”，则 $\mathbb{A}=\{\{A_1^1\}\wedge\{A_2^2\vee A_2^3\}\}$。

用户 u 的属性集合定义为 $L=\{L_1,L_2,\cdots,L_n\}$，其中 $L_i\in A_i$。

定义 1 设 $\mathbb{A}=\{W_1,\cdots,W_n\}$ 是一个访问结构，其中 $W_i\subseteq A_i$，则用户 u 的属性集合 $L=\{L_1,L_2,\cdots,L_n\}$ 满足访问结构 $\mathbb{A}$ 当且仅当 $L_i\in W_i, i=1,\cdots,n$。

2.3 复杂性假设

假设 1 D-Linear 假设 给定阶为素数 p 的乘法群 G_1，然后随机选择生成元 $g,f,\pi\in G_1$ 和随机数 $c_1,c_2\in Z_p$，并将元素 $g,f,\pi,g^{c_1},f^{c_2},T\in G_1$ 发送给 $\mathcal{A}$，由 $\mathcal{A}$ 判定 T 是否等于 $\pi^{c_1+c_2}$，当 $T=\pi^{c_1+c_2}$ 时，$\mathcal{A}$ 输出 1；否则输出 0。

定义算法 $\mathcal{A}$ 解决上述问题的优势是：

$$\begin{aligned}\mathrm{Adv}_{\text{D-Linear}}=&\Pr[\mathcal{A}(g,f,\pi,g^{c_1},f^{c_2},\pi^{c_1+c_2})=1]\\&-\Pr[\mathcal{A}(g,f,\pi,g^{c_1},f^{c_2},T)=1]\end{aligned}$$

如果没有多项式时间算法以不可忽略的优势解决 D-Linear 假设，则我们就称 D-Linear 假设在群 G_1 中是成立的。

假设 2 DBDH 假设 给定阶为素数 p 的乘法群 G_1 和 G_2，然后随机选择生成元 $g\in G_1$ 和随机数 $c_1,c_2,c_3\in Z_p$，并将元素 $g,g^{c_1},g^{c_2},g^{c_3}\in G_1$ 和 $T\in G_2$ 发送给 $\mathcal{A}$，由 $\mathcal{A}$ 判定 T 是否等于 $e(g,g)^{c_1c_2c_3}$，当 $T=e(g,g)^{c_1c_2c_3}$ 时，$\mathcal{A}$ 输出 1；否则输出 0。

定义算法 $\mathcal{A}$ 解决上述问题的优势是：

$$\begin{aligned}\mathrm{Adv}_{\text{DBDH}}=&\Pr[\mathcal{A}(g,g^{c_1},g^{c_2},g^{c_3},e(g,g)^{c_1c_2c_3})=1]\\&-\Pr[\mathcal{A}(g,g^{c_1},g^{c_2},g^{c_3},T)=1]\end{aligned}$$

如果没有多项式时间算法以不可忽略的优势解决 DBDH 假设，则我们就称 DBDH 假设在群 G_1,G_2 中是成立的。

2.4 基于属性加密方案的结构

基于属性的加密方案包含 4 个算法：系统建立算法，加密算法，密钥生成算法和解密算法。

建立算法(λ) 输入安全参数 λ，输出公共参数 PK 和主密钥 MSK。

加密算法(PK,$m,\mathbb{A}$) 输入公共参数 PK，消息 m 和一个访问结构 $\mathbb{A}$，输出一个密文 CT。

密钥生成算法(MSK, L) 输入主密钥 MSK 和一个属性列表 L，返回关于属性列表 L 的私钥 SK。

解密算法(PK, CT, SK) 输入公共参数 PK，密文 CT 和私钥 SK。如果关于私钥的属性列表能满足密文的访问结构，就输出解密消息 m，否则解密失败。

2.5 隐藏访问结构的基于属性加密方案的安全模型[7]

我们通过攻击者 $\mathcal{A}$ 和挑战者 $\mathcal{B}$ 之间的交互式游戏来定义基于属性加密方案的安全模型。

初始化 挑战者 $\mathcal{B}$ 运行系统建立算法生成公共参数 PK，并发送给攻击者 $\mathcal{A}$。

阶段 1 攻击者 $\mathcal{A}$ 适应性地选择属性列表 L 进行私钥提取询问，挑战者返回 L 的私钥，这些私钥询问可以重复多次。

挑战 攻击者 $\mathcal{A}$ 选择两个等长的消息 m_0 和 m_1 以及访问结构 $\mathbb{A}_0^*,\mathbb{A}_1^*$ 提交给挑战者 $\mathcal{B}$，$\mathcal{B}$ 随机地选择 $d\in\{0,1\}$，在访问结构 $\mathbb{A}_d^*$ 条件下加密 m_d，并把密文发送给攻击者 $\mathcal{A}$。

阶段 2 重复阶段 1 的私钥提取询问，此时要求 L 不能满足结构 $\mathbb{A}_0^*$ 和 $\mathbb{A}_1^*$。

猜测 攻击者 $\mathcal{A}$ 输出对 d 的猜测值 d'，$\mathcal{A}$ 赢得游戏当且仅当 $d=d'$。

我们定义攻击者 $\mathcal{A}$ 赢得游戏的优势为 $\Pr[d'=d]-(1/2)$。

定义 2 一个基于属性加密方案是完全安全的，当且仅当不存在多项式有界的攻击者能以不可忽略的优势赢得以上游戏。

3 方案介绍

本节提出一个新的可以隐藏访问结构的基于属性加密方案，并对其安全性以及性能进行分析。

3.1 所提方案

系统建立(1^λ) 输入安全参数 1^λ，系统可信中心 TA 选择一个阶为素数 p 的群 G。设该系统的属性空间为 $U=\{A_1,A_2,\cdots,A_n\}$，共有 n 个不同的属性，并且每个属性 A_i 有 l_i 个值 $\{A_i^1,A_i^2,\cdots,A_i^{l_i}\}$。随机选择生成元 $g,g_0,v,v_1,v_2,u_{1,1},\cdots,u_{1,l_1},\cdots,u_{n,1},\cdots,u_{n,l_n}\in G$，其中 $\{u_{i,j}\,|\,j=1,\cdots,l_i\}$ 对应属性 A_i 的 l_i 个不同的取值。选择随机整数 $a_1,a_2,b,\alpha\in Z_p$，计算 $\tau_1=vv_1^{a_1},\tau_2=vv_2^{a_2}$，$Y=e(g,g)^{\alpha\cdot a_1\cdot b}$。则公共参数

$$\begin{aligned}\mathrm{PK}=\{&Y,g^b,g^{a_1},g^{a_2},g^{b\cdot a_1},g^{b\cdot a_2},g_0,\tau_1,\tau_2,\tau_1^b,\tau_2^b,v,v_1,\\&v_2,u_{1,1},\cdots,u_{1,l_1},\cdots,u_{n,1},\cdots,u_{n,l_n}\}\end{aligned}$$

主密钥 $\mathrm{MSK}=\{g^\alpha,g^{\alpha\cdot a_1}\}$。

私钥生成(PK,MK,L) 输入用户 u 的属性 $L=\{L_1,L_2,\cdots,L_n\}=\{A_1^{j_1},A_2^{j_2},\cdots,A_n^{j_n}\}$。然后随机选取 $r_1,r_2,z_1,z_2\in Z_p$，计算 $D_1=g^{\alpha a_1}v^{r_1+r_2}$，$D_2=g^{-\alpha}v_1^{r_1+r_2}g^{z_1}$，

$D_3=(g^b)^{-z_1}$，$D_4=v_2^{r_1+r_2}g^{z_2}$，$D_5=(g^b)^{-z_2}$，$D_6=(g^b)^{r_2}$，$D_7=g^{r_1}$，$K=\left(g_0\prod_{i=1}^{n}u_{i,j_i}\right)^{r_1}$，其中 $A_i^{j_i}\in L$。最后输出私钥 $\mathrm{SK}_u=\{D_1,D_2,\cdots,D_7,K\}$。

加密算法(PK, $\mathcal{A}$, m)　访问结构 $\mathcal{A}=\{W_1,\cdots,W_n\}$，其中 $W_i\subseteq A_i$，消息 $m\in G_2$，然后随机选择 $s_1,s_2,t\in Z_p$，计算 $C_0=mY^{s_2}$, $C_1=(g^b)^{s_1+s_2}$，$C_2=(g^{ba_1})^{s_1}$，$C_3=(g^{a_1})^{s_1}$，$C_4=(g^{ba_2})^{s_2}$，$C_5=(g^{a_2})^{s_2}$, $C_6=\tau_1^{s_1}\tau_2^{s_2}$, $C_7=(\tau_1^b)^{s_1}(\tau_2^b)^{s_2}\cdot g_0^t$, $C_8=g^t$。接下对 $i=1,\cdots,n$，$j=1,\cdots,l_i$ 计算，当 $A_i^j\in W_i$ 时，$E_i^j=u_{i,j}^t$，当 $A_i^j\notin W_i$ 时，取随机数 $t_{i,j}\in Z_p$，且 $t_{i,j}\neq t$，令 $E_i^j=u_{i,j}^{t_{i,j}}$。最后输出密文为 $\mathrm{CT}=\{C_0,C_1,\cdots,C_8,\{E_i^j\,|i=1,\cdots,n,j=1,\cdots,l_i\}\}$。

解密算法(SK_u,CT)　接收者收到密文后，将密文中对应接收者属性 $L_u=\{L_1,\cdots,L_n\}$ 的部分取出来，即当 $L_i=A_i^{j_i}$ 时 $E_i'=E_i^j$，并计算 $E=C_7\cdot\prod_{i=1}^{n}E_i'$。如果接收者属性 L_u 不满足加密访问结构 $\mathcal{A}$，则无法输出正确明文，否则

$$Y'=\{e(C_1,D_1)\cdot e(C_2,D_2)\cdot e(C_3,D_3)\cdot e(C_4,D_4)\cdot e(C_5,D_5)\cdot e(C_8,K)\}/\{e(C_6,D_6)\cdot e(E,D_7)\}$$

$$m=C_0/Y'$$

3.2 正确性验证

(1)如果接收者属性 L_u 不满足加密访问结构 $\mathcal{A}$，则无法算出正确明文，否则

$$E=C_7\cdot\prod_{i=1}^{n}E_i'=(\tau_1^b)^{s_1}(\tau_2^b)^{s_2}\cdot g_0^t\cdot\prod_{i=1}^{n}u_{i,j}^t$$

(2)

$$e(C_1,D_1)\cdot e(C_2,D_2)\cdot e(C_3,D_3)\cdot e(C_4,D_4)\cdot e(C_5,D_5)\cdot e(C_8,K)=e((g^b)^{s_1+s_2},g^{\alpha a_1}v^{r_1+r_2})\cdot e((g^{ba_1})^{s_1},g^{-\alpha}v_1^{r_1+r_2}g^{z_1})\cdot e((g^{a_1})^{s_1},(g^b)^{-z_1})\cdot e((g^{ba_2})^{s_2},v_2^{r_1+r_2}\cdot g^{z_2})\cdot e((g^{a_2})^{s_2},(g^b)^{-z_2})\cdot e\left(g^t,\left(g_0\prod_{i=1}^{n}u_{i,j_i}\right)^{r_1}\right)$$

$$=e(g,g)^{\alpha a_1bs_2}\cdot e(v,g)^{b(s_1+s_2)(r_1+r_2)}\cdot e(v_1,g)^{a_1bs_1(r_1+r_2)}\cdot e(v_2,g)^{a_2bs_2(r_1+r_2)}\cdot e(g,g_0)^{t\,r_1}\cdot e\left(g,\prod_{i=1}^{n}u_{i,j_i}\right)^{t\,r_1}$$

(3)

$$e(C_6,D_6)\cdot e(E,D_7)=e(\tau_1^{s_1}\tau_2^{s_2},(g^b)^{r_2})\cdot e\left((\tau_1^b)^{s_1}\cdot(\tau_2^b)^{s_2}\cdot g_0^t\cdot\prod_{i=1}^{n}u_{i,j}^t,g^{r_1}\right)=e(v,g)^{b(s_1+s_2)(r_1+r_2)}\cdot e(v_1,g)^{a_1bs_1(r_1+r_2)}\cdot e(v_2,g)^{a_2bs_2(r_1+r_2)}\cdot e(g,g_0)^{t\,r_1}\cdot e\left(g,\prod_{i=1}^{n}u_{i,j_i}\right)^{t\,r_1}$$

所以

$$Y'=\{e(C_1,D_1)\cdot e(C_2,D_2)\cdot e(C_3,D_3)\cdot e(C_4,D_4)\cdot e(C_5,D_5)\cdot e(C_8,K)\}/\{[e(C_6,D_6)\cdot e(E,D_7)]\}=e(g,g)^{\alpha a_1bs_2}$$

最后，$C_0/Y'=C_0/e(g,g)^{\alpha a_1bs_2}=m$。

3.3 安全性证明

在证明方案的安全性之前，我们需要先给出两个附加的定义，半功能密文(semi-functional ciphertext)和半功能密钥(semi-functional key)。

半功能密文　首先由加密算法生成消息 m 的正常密文 $\mathrm{CT}=\{C_0',C_1',\cdots,C_8',\{E_i'^j|i=1,\cdots,n,j=1,\cdots,l_i\}\}$，然后选择随机数 $x\in Z_p$，并且令 $C_0=C_0'$, $C_1=C_1'$, $C_2=C_2'$, $C_3=C_3'$, $C_8=C_8'$, $C_4=C_4'g^{ba_2x}$, $C_5=C_5'g^{a_2x}$, $C_6=C_6'v_2^{a_2x}$, $C_7=C_7'v_2^{ba_2x}$, $E_i^j=E_i'^j$。则半功能密文为 $\mathrm{CT}_S=\{C_0,C_1,\cdots,C_8,\{E_i^j|i=1,\cdots,n,j=1,\cdots,l_i\}\}$。

半功能密钥　设用户 u 拥有属性 $L=\{L_1,L_2,\cdots,L_n\}=\{A_1^{j_1},A_2^{j_2},\cdots,A_n^{j_n}\}$，然后随机选择 $r_1,r_2,z_1,z_2,\gamma\in Z_p$，计算 $D_1=g^{\alpha a_1}v^{r_1+r_2}g^{-a_1a_2\gamma}$，$D_2=g^{-\alpha}v_1^{r_1+r_2}g^{z_1}\cdot g^{a_2\gamma}$, $D_3=(g^b)^{-z_1}$, $D_4=v_2^{r_1+r_2}g^{z_2}g^{a_1\gamma}$, $D_5=(g^b)^{-z_2}$, $D_6=(g^b)^{r_2}$, $D_7=g^{r_1}$, $K=\left(g_0\prod_{i=1}^{n}u_{i,j_i}\right)^{r_1}$，其中 $A_i^{j_i}\in L$。则半功能密钥为 $\{D_1,D_2,\cdots,D_7,K\}$。

注意：半功能密钥可以解密正常密文，正常密钥也可以解密半功能密文，但是半功能密钥无法解密半功能密文。

接下来，我们考虑如下 3 个游戏：

$\mathrm{Game}_{\mathrm{Real}}$ 一个真实的安全游戏，生成的密文和私钥都是正常的。

Game_i 这个游戏与游戏 $\mathrm{Game}_{\mathrm{Real}}$ 相似，只有挑战密文和前 i 次询问的私钥是半功能的，其余的私钥是正常的。

$\mathrm{Game}_{\mathrm{Final}}$ 这个游戏中，挑战密文和私钥都是半功能的，并且密文加密的是一个随机消息。

下面我们用 3 个引理来证明以上所述的各个游戏彼此不可区分。

引理 1　假设存在一个攻击者 $\mathcal{A}$ 使得 $\mathrm{Game}_{\mathrm{Real}'}\cdot\mathrm{Adv}_{\mathcal{A}}-\mathrm{Game}_0\mathrm{Adv}_{\mathcal{A}}=\varepsilon$。我们就能找到一个算法 $\mathcal{B}$ 以 ε 优势解决假设 1。

证明　给定假设 1 的条件 $(g,f,\pi,g^{c_1},f^{c_2},T)$，挑战者 $\mathcal{B}$ 随机选择 $b,\alpha,y_v,y_{v_1},y_{v_2}\in Z_p$, $g_0,u_{1,1},\cdots,u_{1,l_1},\cdots,u_{n,1},\cdots,u_{n,l_n}\in G$，然后计算出公共参数 g^b, $g^{a_1}=f$, $g^{a_2}=\pi$, $g^{ba_1}=f^b$, $g^{ba_2}=\pi^b$, $v=g^{y_v}$, $v_1=g^{y_{v_1}}$, $v_2=g^{y_{v_2}}$, $\tau_1=vv_1^{a_1}=g^{y_v}f^{y_{v_1}}$, $\tau_2=vv_2^{a_2}=g^{y_v}\pi^{y_{v_2}}$, $\tau_1^b=(g^{y_v}\cdot f^{y_{v_1}})^b$, $\tau_2^b=(g^{y_v}\pi^{y_{v_2}})$, $Y=e(g,f)^{\alpha\cdot b}$，并把这些公共参数发送给攻击者 $\mathcal{A}$，$\mathcal{B}$ 保存主密钥 $\mathrm{MSK}=\{g^{\alpha},g^{\alpha a_1}$

$=f^{\alpha}\}$。

私钥询问阶段 1　因为 $\mathcal{B}$ 保存有主密钥，所以 $\mathcal{B}$ 可以生成任何属性集的私钥。

挑战　攻击者 $\mathcal{A}$ 决定结束私钥询问，则他选择等长的两个消息 m_0, m_1 和挑战的访问结构 $\mathbb{A}_0^*=\{W_{0,1},\cdots,W_{0,n}\}$, $\mathbb{A}_1^*=\{W_{1,1},\cdots,W_{1,n}\}$，并把它们发送给挑战者 $\mathcal{B}$，然后 $\mathcal{B}$ 随机选择 $d\in\{0,1\}$，在访问结构 $\mathbb{A}_d^*$ 条件下加密 m_d，选择随机数 $s_1^{'},s_2^{'},t'\in Z_p$，生成正常密文 $\mathrm{CT}=\{C_0^{'},C_1^{'},\cdots,C_8^{'},\{E_i^{'j}\,|i=1,\cdots,n,j=1,\cdots,l_i\}\}$，然后 $\mathcal{B}$ 令 $C_0=C_0^{'}\cdot(e(g^{c_1},f)\cdot e(g,f^{c_2}))^{b\cdot\alpha}$, $C_1=C_1^{'}\cdot(g^{c_1})^{b}$, $C_2=C_2^{'}\cdot(f^{c_2})^{-b}$, $C_3=C_3^{'}\cdot(f^{c_2})$, $C_4=C_4^{'}\cdot T^{b}$, $C_5=C_5^{'}\cdot T$, $C_6=C_6^{'}\cdot(g^{c_1})^{y_v}\cdot(f^{c_2})^{-y_{v_1}}\cdot T^{y_{v_2}}$, $C_7=C_7^{'}\cdot((g^{c_1})^{y_v}\cdot(f^{c_2})^{-y_{v_1}}\cdot T^{y_{v_2}})^{b}$, $C_8=C_8^{'}$, $E_i^{j}=E_i^{'j}$，最后挑战者 $\mathcal{B}$ 向攻击者 $\mathcal{A}$ 发送密文 $\mathrm{CT}=\{C_0,C_1,\cdots,C_8,\{E_i^{j}\,|i=1,\cdots,n\,,j=1,\cdots,l_i\}\}$。

私钥询问阶段 2　与阶段 1 相同，但是不可以询问满足挑战访问结构 $\mathbb{A}_0^*$ 和 $\mathbb{A}_1^*$ 的属性集合。

猜测　攻击者 $\mathcal{A}$ 输出一个关于 d 的猜测 d'，如果 $T=\pi^{c_1+c_2}$，则密文 CT 为正常密文，其中 $s_1=s_1^{'}-c_2\,,s_2=s_2^{'}+c_1+c_2$，否则，CT 为半功能密文。因此，挑战者 $\mathcal{B}$ 可以根据 $\mathcal{A}$ 的输出以 ε 优势解决假设 1。　证毕

引理 2　假设存在一个攻击者 $\mathcal{A}$ 使得 $\mathrm{Game}_{k-1}\cdot\mathrm{Adv}_{\mathcal{A}}-\mathrm{Game}_{k}\mathrm{Adv}_{\mathcal{A}}=\varepsilon$。我们就能找到一个算法 $\mathcal{B}$ 以 ε 优势解决假设 1。

证明　给定假设 1 的条件 $(g,f,\pi,g^{c_1},f^{c_2},T)$，挑战者 $\mathcal{B}$ 随机选择 $\alpha,a_1,a_2,y_{v_1},y_{v_2}\in Z_p$，令 $g^{b}=f$, $g^{ba_1}=f^{a_1}$, $g^{ba_2}=f^{a_2}$, $v=\pi^{-a_1a_2}$, $v_1=\pi^{a_2}\cdot g^{y_{v_1}}$, $v_2=\pi^{a_1}\cdot g^{y_{v_2}}$, $Y=e(g,f)^{\alpha\cdot a_1}$，然后可以根据以上条件求出 τ_1, τ_2, τ_1^{b}, τ_2^{b}。$\mathcal{B}$ 随机选择 $y_0,y_{u_{1,1}},\cdots,y_{u_{1,l_1}},\cdots,y_{u_{n,1}},\cdots,y_{u_{1,l_n}}\in Z_p$，则 $g_0=g^{y_0}$, $u_{i,j}=g^{y_{u_{i,j}}}$，其中 $i=1,\cdots,n$, $j=1,\cdots,l_i$，最后 $\mathcal{B}$ 把公共参数 PK 发送给攻击者 $\mathcal{A}$。

私钥询问　这个阶段，我们将私钥询问分为 3 部分，下面 i 表示攻击者 $\mathcal{A}$ 的第 i 次询问。

(1)当 $i<k$ 时，因为 Game_k 和 Game_{k-1} 的前 $k-1$ 次私钥都是半功能的，所以挑战者 $\mathcal{B}$ 可以由主密钥和攻击者 $\mathcal{A}$ 询问的属性集计算出正常私钥，然后再将其转换为半功能密钥并发送给攻击者 $\mathcal{A}$。

(2)当 $i>k$ 时，Game_k 和 Game_{k-1} 生成的密钥都是正常的，此时，挑战者 $\mathcal{B}$ 可以由主密钥和攻击者 $\mathcal{A}$ 询问的属性集计算出正常私钥，然后发送给攻击者 $\mathcal{A}$。

(3)当 $i=k$ 时，挑战者 $\mathcal{B}$ 首先根据攻击者 $\mathcal{A}$ 询问的属性集 $L=\{L_1,L_2,\cdots,L_n\}$，随机选取 $r_1,r_2,z_1,z_2\in Z_p$，生成正常密钥 $D_1^{'},D_2^{'},\cdots,D_7^{'},K'=\left(g_0\prod_{i=1}^{n}u_{i,j_i}\right)^{r_1}$，其中 $A_i^{j_i}\in L$。然后令 $D_1=D_1^{'}\cdot T^{-a_1a_2}$, $D_2=D_2^{'}\cdot T^{a_2}(g^{c_1})^{y_{v_1}}$, $D_3=D_3^{'}\cdot(f^{c_2})^{y_{v_1}}$, $D_4=D_4^{'}\cdot T^{a_1}(g^{c_1})^{y_{v_2}}$, $D_5=D_5^{'}\cdot(f^{c_2})^{y_{v_2}}$, $D_6=D_6^{'}\cdot f^{c_2}$, $D_7=D_7^{'}\cdot(g^{c_1})$, $K=K'\cdot(g^{c_1})^{y_0+\sum_{i=1}^{j}y_{u_{i,j_i}}}$，其中 $A_i^{j_i}\in L$。当 $T=\pi^{c_1+c_2}$ 时，第 k 次询问生成的私钥是正常的，其中 $r_1=r_1^{'}+c_1$, $r_2=r_2^{'}+c_2$, $z_1=z_1^{'}-c_2y_{v_1}$, $z_2=z_2^{'}-c_2y_{v_2}$。当 T 是随机元素，则我们可以令 $T=\pi^{c_1+c_2}\cdot g^{\gamma}$，其中 $\gamma\in Z_p$，此时生成的密钥是半功能的。

如果 $T=\pi^{c_1+c_2}$，则我们进行的是游戏 Game_{k-1}，否则我们进行的是游戏 Game_k。因此，挑战者 $\mathcal{B}$ 可以根据 $\mathcal{A}$ 对 Game_k 或者 Game_{k-1} 判断的输出以 ε 优势解决假设 1。　证毕

引理 3　假设存在一个攻击者 $\mathcal{A}$ 使得 $\mathrm{Game}_q\cdot\mathrm{Adv}_{\mathcal{A}}-\mathrm{Game}_{\mathrm{Final}}\mathrm{Adv}_{\mathcal{A}}=\varepsilon$。我们就能找到一个算法 $\mathcal{B}$ 以 ε 优势解决假设 2。

证明　给定假设 2 的条件 $(g,g^{c_1},g^{c_2},g^{c_3},T)$，挑战者 $\mathcal{B}$ 选择随机数 $a_1,b,y_v,y_{v_1},y_{v_2},y_0,\ y_{u_{1,1}},\cdots,y_{u_{1,l_1}},\cdots,y_{u_{n,1}},\cdots,y_{u_{1,l_n}}\in Z_p$。令 $g^{a_2}=g^{c_2}$, $g^{ba_2}=g^{c_2b}$, $v=g^{y_v}$, $v_1=g^{y_{v_1}}$, $v_2=g^{y_{v_2}}$, $Y=e(g^{c_1},g^{c_2})^{a_1b}$, $g_0=g^{y_0}$, $u_{i,j}=g^{y_{u_{i,j}}}$，其中 $i=1,\cdots,n$, $j=1,\cdots,l_i$，然后可以根据以上条件求出 τ_1, τ_2, τ_1^{b}, τ_2^{b}。最后 $\mathcal{B}$ 把公共参数 PK 发送给 $\mathcal{A}$。

私钥询问阶段 1　在游戏 Game_q 和 $\mathrm{Game}_{\mathrm{Final}}$ 中，生成的密钥都是半功能的。挑战者 $\mathcal{B}$ 首先根据攻击者 $\mathcal{A}$ 询问的属性集 $L=\{L_1,L_2,\cdots,L_n\}=\{A_1^{j_1},A_2^{j_2},\cdots,A_n^{j_n}\}$，随机选取 $r_1,r_2,z_1,z_2,\gamma'\in Z_p$，生成半功能密钥 $D_1=(g^{c_2})^{-\gamma'a_1}v^{r_1+r_2}$, $D_2=(g^{c_2})^{-\gamma'}v_1^{r_1+r_2}g^{z_1}$, $D_3=(g^{b})^{-z_1}$, $D_4=(g^{c_1})^{a_1}g^{a_1\gamma'}v_2^{r_1+r_2}g^{z_2}$, $D_5=(g^{b})^{-z_2}$, $D_6=(g^{b})^{r_2}$, $D_7=g^{r_1}$, $K=\left(g_0\prod_{i=1}^{n}u_{i,j_i}\right)^{r_1}$，其中 $A_i^{j_i}\in L$。则半功能密钥为 $\{D_1,D_2,\cdots,D_7,K\}$。

挑战　当攻击者 $\mathcal{A}$ 决定结束私钥询问，则他选择等长的两个消息 m_0, m_1 和挑战的访问结构 $\mathbb{A}_0^*=\{W_{0,1},\cdots,W_{0,n}\}$, $\mathbb{A}_1^*=\{W_{1,1},\cdots,W_{1,n}\}$，并把它们发送给 $\mathcal{B}$，然后 $\mathcal{B}$ 随机选择 $d\in\{0,1\}$，在访问结构 $\mathbb{A}_d^*$ 条件下生成 m_d 或者一个随机数 R 的半功能密文。$\mathcal{B}$ 随机选择 $s_1,t,x'\in Z_p$，令 $C_0=m_d\cdot T^{a_1b}$, $C_1=g^{s_1b}(g^{c_3})^{b}$, $C_2=g^{ba_1s_1}$, $C_3=g^{a_1s_1}$, $C_4=(g^{c_2})^{x'b}$, $C_5=(g^{c_2})^{x'}$, $C_6=\tau_1^{s_1}(g^{c_3})^{y_v}(g^{c_2})^{y_{v_2}x'}$, $C_7=(\tau_1^{s_1}(g^{c_3})^{y_v}\cdot(g^{c_2})^{y_{v_2}x'})^{b}\cdot g_0^{t}$, $C_8=g^{t}$。接下对 $i=1,\cdots,n\,,j=1,\cdots,l_i$ 计算，当 $A_i^{j}\in W_i$ 时，$E_i^{j}=u_{i,j}^{t}$，当 $A_i^{j}\notin W_i$ 时，取随机数 $t_{i,j}\in Z_p$，且 $t_{i,j}\neq t$，令 $E_i^{j}=u_{i,j}^{t_{i,j}}$。最后 $\mathcal{B}$ 向攻击者 $\mathcal{A}$ 发送半功能密文为 $\mathrm{CT}=\{C_0,C_1,\cdots,C_8,\{E_i^{j}\,|i=1,\cdots,n,j=1,\cdots,l_i\}\}$。

私钥询问阶段 2　与阶段 1 相同，但是不可以

询问满足挑战访问结构 $\mathbb{A}_0^*$ 和 $\mathbb{A}_1^*$ 的属性集合。

猜测　攻击者 $\mathcal{A}$ 输出一个关于 d 的猜测 d'，如果 $T=e(g,g)^{c_1c_2c_3}$，则生成的是 m_d 的半功能密文，即我们进行的是 Game_q，否则我们进行的是游戏 $\mathrm{Game}_{\mathrm{Final}}$。因此，挑战者 $\mathcal{B}$ 可以根据 $\mathcal{A}$ 的输出以 ε 优势解决假设 2。　　证毕

综上所述，我们可以得出下面的定理：

定理 1　如果假设 1 和假设 2 成立，则本文提出的可以隐藏访问结构的基于属性加密方案是安全的。

证明　如果假设 1，假设 2 成立，则上述 3 个引理已经证明真实的安全游戏和 $\mathrm{Game}_{\mathrm{Final}}$ 之间是不可区分的，因此攻击者攻击该方案将一无所得，故本文提出的加密方案是安全的。　　证毕

3.4 效率分析

现将本文提出的方案与 Nishide 等人[6]提出的方案和 Lai 等人[7]提出的方案进行比较。其中 n 表示系统中的属性个数，l_i 表示第 i 个属性的取值个数，pair 表示解密过程中双线性对的运算，具体比较结果见表 1。

表 1 本文方案与文献[6]，文献[7]方案比较

方案	双线性群的阶	公钥长度		私钥长度		密文长度		解密运算	安全模型
		$\lvert G_1\rvert$	$\lvert G_2\rvert$	$\lvert G_1\rvert$	$\lvert G_2\rvert$	$\lvert G_1\rvert$	$\lvert G_2\rvert$	pair	
文献[6]方案	素数阶	$3+\sum_{i=1}^{n} l_i$	1	$1+2n$	0	$1+n+\sum_{i=1}^{n} l_i$	1	$1+2n$	选择安全
文献[7]方案	合数阶	$2+\sum_{i=1}^{n} l_i$	1	$1+n$	0	$1+\sum_{i=1}^{n} l_i$	1	$1+n$	完全安全
本文方案	素数阶	$13+\sum_{i=1}^{n} l_i$	1	8	0	$8+\sum_{i=1}^{n} l_i$	1	8	完全安全

4　结束语

本文利用双系统密码技术在素数群中提出了一个可以隐藏访问结构的基于属性加密方案。该方案将访问结构隐藏，使得非法接收者不但无法解密，而且也无法得知哪些用户可以解密，合法用户只能判断自己是否可以解密，但无法判断还有哪些用户可以解密，达到了较强的匿名性。另外，方案中用户私钥长度和解密过程中双线性对的运算量都为固定值，对系统的存储和计算能力要求较低。

参 考 文 献

[1] Sahai A and Waters B. Fuzzy identity-based encryption[C]. In EUROCRYPT 2005, 2005, LNCS 3494: 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, 2006, New York, USA, 2006: 89–98.

[3] Herranz J, Laguillaumie F, and Rafols C. Constant size ciphertexts in threshold attribute-based encryption[C]. In PKC 2010, 2010, LNCS 6065: 19–34.

[4] Waters B. Ciphertext-policy attribute-based encryption: an expressive, efficient, and provably secure realization[C]. In PKC 2011, 2011, LNCS 6571: 53–70.

[5] Attrapadung N, Libert B, and Panafieu E. Expressive key-policy attribute-based encryption with constant-size ciphertexts[C]. In PKC 2011, 2011, LNCS 6571: 90–108.

[6] Nishide T, Yoneyama K, and 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, and Li Y. Fully secure cipertext-policy hiding CP-ABE[C]. In ISPEC 2011, 2011, LNCS 6672: 24–39.

[8] Freeman D M. Converting pairing-based cryptosystems from composite-order groups to prime-order groups[C]. In EUROCRYPT 2010, 2010, LNCS 6110: 44–61.

[9] Lewko A and Waters B. New techniques for dual system encryption and fully secure HIBE with short ciphertexts [EB/OL]. http://eprint.iracr.org/2009/482, 2009.

[10] Waters B. Dual system encryption: realizing fully secure IBE and HIBE under simple assumptions[C]. In CRYPTO 2009, 2009, LNCS 5677: 619–636.

王海斌：　男，1986 年生，硕士生，研究方向为信息安全.

陈少真：　女，1967 年生，教授，博士生导师，研究方向为信息安全.