doi:10.11959/j.issn.1000-436x.2015135

基于访问树的策略隐藏属性加密方案

宋衍[1,2]，韩臻[1]，刘凤梅[2]，刘磊[2]
(1. 北京交通大学 计算机与信息技术学院，北京 100044；2. 信息保障技术重点实验室，北京 100072)

摘 要：已有的策略隐藏属性加密（ABE，attribute-based encryption）方案只支持受限的访问结构，策略表达能力弱，基于此提出一种新的访问树结构，使属性隐藏和秘密共享能够应用到“与”门、“或”门和“门限”门中。并且，利用合数阶双线性群构造了一种基于访问树的策略隐藏方案，并通过双系统加密的概念证明了方案的安全性。分析和实验验证表明，方案在实现复杂访问结构的策略隐藏的同时，并没有过多地增加计算开销，在实际应用过程中更加灵活和有效。

关键词：属性加密；密文策略；策略隐藏；访问结构；合数阶双线性群
中图分类号：TP309.7 **文献标识码**：A

Attribute-based encryption with hidden policies in the access tree

SONG Yan[1,2], HAN Zhen[1], LIU Feng-mei[2], LIU Lei[2]
(1. School of Computer and Information Technology, Beijing Jiaotong University, Beijing 100044, China;
2. Science and Technology on Information Assurance Laboratory, Beijing 100072, China)

Abstract: The existing policies-hidden attribute-based encryption (ABE) schemes could only support a limited access structure, which resulted in weak expressiveness. A new structure of access tree was thus proposed to integrate attribute hiding and secret sharing into “and” gate, “or” gate and “threshold” gate. Then, a tree-based policies-hidden scheme was constructed by using composite order bilinear groups. Under dual system encryption, the scheme was proved to be secure. Furthermore, the analysis and experiment demonstrate that the scheme realize policies-hidden in the complex access structure without increasing the overhead of computation. As a result, it is more feasible and flexible for applications.

Key words: attribute-based encryption; ciphertext policy; policies hidden; access structure; composite order bilinear groups

1 引言

云存储环境中，数据服务提供商（DSP，data service provider）不一定可信，解决不可信环境下数据机密性问题的最好方式就是加密；由数据拥有者（DO，data owner）加密数据，DSP 对密文进行存储和管理。公钥基础设施（PKI，public key infrastructure）作为公共第三方，提供了可信的用户公钥证书。DO 从 PKI 获取具有访问权限的数据请求者（DReq，data requirer）的公钥，生成不同的密文版本；DReq 发出请求后，DSP 将相应的密文版本返回给 DReq，实现基于密文的访问控制。这种做法虽然保证了数据机密性，但是还存在 2 个缺陷：一是 DO 并不是总能确定所有具有访问权限的用户身份；二是当消息发生变化时，需要更新所有的密文版本，多次加密导致处理开销大，因此当用户数量多或者消息变化频繁时，效率较低[1]。

收稿日期：2014-07-02；**修回日期**：2014-10-22
基金项目：国家自然科学基金资助项目（60973112）；北京市教育委员会学科建设与研究生培养基金资助项目（BMKY2011B06）；信息保障技术重点实验室开放基金资助项目（KJ-13-02）
Foundation Items: The National Natural Science Foundation of China(60973112); Discipline Construction and Graduate Education Foundation of Beijing Municipal Commission of Education(BMKY2011B06);Open Foundation of Science and Technology on Information Assurance Laboratory(KJ-13-02)

为解决上述问题，Sahai 和 Waters[2]基于身份加密提出了 ABE 的概念，通过双线性对将属性分别与密钥分量和秘密分量相关联，通过秘密共享确定具有访问权限的属性组合。最初的 ABE 机制虽然解决了用户确定和工作效率问题，但仅支持门限操作，策略表达不够丰富。因此，提出了基于密钥策略（KP，key-policy）[3]和基于密文策略（CP，ciphertext-policy）[4]的 ABE 机制，实现属性的与、或、非和门限操作，从而支持灵活的访问控制策略。

然而，除了信息敏感之外，策略也可能是敏感的。结果，一个“诚实但狡猾”的 DSP 能够根据策略得到感兴趣的信息。例如，一份病历通过 CP-ABE 机制加密，它的策略是只允许神经病科专家访问。这条策略已经暴露了这份病历的病人极有可能有神经方面的问题。在类似场景中，策略隐藏就显得十分必要。

Kapadia 等[5]提出了一种策略隐藏的 CP-ABE 方案，但是需要引入一个在线的半可信服务器，为每个用户重加密密文，使服务器成为安全和性能瓶颈。Nishide 等[6]提出了 2 种实现策略隐藏的 CP-ABE 构造，通过多值属性之间的与逻辑来表示访问控制策略。Lai 等[7]基于子群判定性假设，在合数阶双线性群上提出一种适应性选择密文攻击（adaptively-CCA，adaptively chosen ciphertext attack）安全的策略隐藏 CP-ABE 方案。Wang 等[8]基于文献[9]对 Lai 等[7]的方案进行了改进，提出一种素数阶双线性群上的策略隐藏 CP-ABE 方案，使私钥规模和解密运算量成为常量，在大规模属性应用环境中具有更高的效率。目前，策略隐藏的 CP-ABE 方案只支持受限的访问结构，策略由所有的属性通过一个“与”门组合而成，可表达性非常弱。

策略隐藏的实现与其所使用的访问结构紧密相关。CP-ABE 的访问结构可以分为：“与”门、访问树和 LSSS 矩阵 3 类[1]。“与”门结构较为简单，但仅能支持属性的“与”、“非”操作。访问树和 LSSS 矩阵 2 种结构较为复杂，但能够支持属性的任意“与”、“或”和“门限”操作，策略可表达性强。同时，访问树结构比 LSSS 矩阵更为直观。

本文在 Ibraimi[10]方案的基础上，对访问树进行相应的改进，通过秘密共享在“与”、“或”、“门限”中的结合应用，将具有权限的属性取值隐藏在系统所有的属性取值中，从而实现基于访问树的策略隐藏。通过构造与加密系统并行的验证系统，对是否满足权限进行验证，避免无权限的解密运算所带来的计算负担。通过运用合数阶双线性群，实现方案的 adaptively-CCA 安全。

相比于素数阶双线性群，合数阶双线性群具有算法组件较少，算法表示简单清晰的优点，这是本文没有采用素数阶双线性群的原因。但是，可以通过文献[9]中的方法将合数阶群构造方案转换为同等安全的素数阶群构造方案。

2 预备知识

2.1 合数阶双线性群

本文使用一个阶为 3 个素数乘积的双线性群[11]。假设群生成算法 $\mathcal{G}$ 的输入为安全参数 1^λ，输出元组 $(p,q,r,G,G_T,\hat{e})$，其中，p、q 和 r 为不同的素数，有 $p,q,r>2^\lambda$，G 和 G_T 为阶 $N=pqr$ 的循环群，G_p、G_q 和 G_r 分别表示群 G 的阶为 p、q 和 r 的子群，映射 $\hat{e}:G\times G\to G_T$ 满足：

1) $\forall g,h\in G$，$\forall a,b\in Z_N$，有 $\hat{e}(g^a,h^b)=\hat{e}(g,h)^{ab}$；

2) $\exists g\in G$，使 $\hat{e}(g,g)$ 在 G_T 中的阶为 N；

3) G 和 G_T 中的运算，以及双线性映射 $\hat{e}$ 的运算，都是在多项式时间内可完成的。

由子群的正交性[6]可知：

1) $\forall h_p\in G_p$，$\forall h_q\in G_q$，有 $\hat{e}(h_p,h_q)$ 为 G_T 的单位元；

2) $\forall h_p\in G_p$，$\forall h_q\in G_q$，$\forall a,b,c,d\in Z_N$，有 $\hat{e}(h_p^a h_q^b,h_p^c h_q^d)=\hat{e}(h_p,h_q)^{ab}\hat{e}(h_p,h_q)^{cd}$。

2.2 复杂性假设

本文使用的是 3 素数子群判定性假设。令 G_{pq} 表示 G 的阶为 pq 的子群，Pr 表示概率函数。

假设 1 定义分布：$G=(N=pqr,G,G_T,\hat{e})\leftarrow\mathcal{G}(1^\lambda)$，$g_p\leftarrow G_p$，$g_r\leftarrow G_r$，$D=(\underline{G},g_p,g_r)$，$T_1\leftarrow G_{pq}$，$T_2\leftarrow G_p$。

定义算法 $\mathcal{A}$ 攻破假设 1 的优势为 $\mathrm{Adv}^1_{g,\mathcal{A}(\lambda)}=|\Pr[\mathcal{A}(\underline{D},T_1)=1]-\Pr[\mathcal{A}(\underline{D},T_2)=1]|$。

假设 2 定义分布：$\underline{G}=(N=pqr,G,G_T,\hat{e})\leftarrow\mathcal{G}(1^\lambda)$，$g_p,X_1\leftarrow G_p$，$X_2\leftarrow G_q$，$g_r\leftarrow G_r$，$\underline{D}=(\underline{G},g_p,X_1X_2,g_r)$，$T_1\leftarrow G_{pq}$，$T_2\leftarrow G_p$。

定义算法 $\mathcal{A}$ 攻破假设 2 的优势为 $\mathrm{Adv}^2_{g,\mathcal{A}(\lambda)}=|\Pr[\mathcal{A}(\underline{D},T_1)=1]-\Pr[\mathcal{A}(\underline{D},T_2)=1]|$。

假设 3 定义分布：$\underline{G}=(N=pqr,G,G_T,\hat{e})\leftarrow\mathcal{G}(1^\lambda)$，$\omega,s\in Z_N/0$，$g_p\leftarrow G_p$，$X_2,Y,Z_2\leftarrow G_q$，$g_r\leftarrow G_r$，$\underline{D}=(\underline{G},g_p,g_p^\omega X_2,g_p^s Y_2,Z_1Z_2,g_r)$，$T_1\leftarrow\hat{e}(g_p,g_p)^{\omega s}$，$T_2\leftarrow G_p$。

定义算法 $\mathcal{A}$ 攻破假设 3 的优势为 $\mathrm{Adv}^3_{g,\mathcal{A}(\lambda)}$ =|Pr[$\mathcal{A}$ ($\underline{D}$,T_1)=1]-Pr[$\mathcal{A}$ ($\underline{D}$,T_2)=1]|。

定义 1　如果对于任意的多项式时间（PPT，polynomial time）算法 $\mathcal{A}$，$\mathrm{Adv}^1_{g,\mathcal{A}(\lambda)}$、$\mathrm{Adv}^2_{g,\mathcal{A}(\lambda)}$、$\mathrm{Adv}^3_{g,\mathcal{A}(\lambda)}$ 是可忽略的，称 $\mathcal{G}$ 满足假设 1~3。

2.3　安全模型

下面通过挑战者 $\mathcal{S}$ 和敌手 $\mathcal{A}$ 之间的交互性游戏给出策略隐藏的 CP-ABE 方案的一个 adaptively-CCA 安全性模型。

1) Setup：挑战者 $\mathcal{S}$ 运行初始化算法 $Setup(1^\lambda)$ 生成公钥 PK 和主密钥 MSK，保存 MSK 并将 PK 发送给敌手 $\mathcal{A}$。

2) Phase1：敌手 $\mathcal{A}$ 适应性地向挑战者 $\mathcal{S}$ 询问属性集 L 的私钥。$\mathcal{S}$ 运行算法 $KeyGen$ 生成私钥 SK_L 并发送给 $\mathcal{A}$，敌手 $\mathcal{A}$ 可以重复多次询问私钥。

3) Challenge：敌手 $\mathcal{A}$ 向挑战者 $\mathcal{A}$ 提交 2 个等长消息 m_0 和 m_1，以及访问结构 T_0 和 T_1（任何询问的属性集都不能满足 T_0 和 T_1）。$\mathcal{S}$ 抛掷一枚公平硬币 $b\in\{0,1\}$，计算 $c^*=Encrypt(PK,m_b,T_b)$，并将 c^* 发送给 $\mathcal{A}$ 作为挑战密文。

4) Phase2：重复执行询问阶段 1。

5) Guess：敌手 $\mathcal{A}$ 输出对密文 c^*的一个猜测值 $b'\in\{0,1\}$。

如果 $b'=b$，则称敌手 $\mathcal{A}$ 赢得这个游戏。$\mathcal{A}$ 在上述游戏中获胜的优势定义为 $\mathrm{Adv}_{\mathcal{A}}=|\Pr[b'=b]-\frac{1}{2}|$。

定义 2　如果在任意多项式时间内，敌手 $\mathcal{A}$ 赢得安全游戏的优势都是可以忽略的，那么这个策略隐藏的 CP-ABE 方案是 adaptively-CCA 安全的。

3　方案设计

3.1　访问控制结构

定义系统的属性集合为 $A=\{a_1,a_2,\cdots,a_n\}$，n 为 A 的阶。对于 $\forall\, i\in Z_N/0$，属性 a_i 的取值集合为 $F_i=\{v_{i,1},v_{i,2},\cdots,v_{i,n_i}\}$，$n_i$ 为 F_i 的阶。用户的属性集合 L 为 $\{l_1=v_{1,t_1},l_2=v_{2,t_2},\cdots,l_k=v_{k,t_k}\}$，$k$ 为 L 的阶。对于 $\forall\, i\in Z_k/0$，有 $l_1\in A$，$v_{i,t_i}\in F_i$。

使用树型结构来表示访问策略。树的内部节点代表关系，包括与（and）、或（or）和门限（threshold）；叶子节点代表属性条件表达式，形式为 $a_i=v_{i,t_i}(i\in Z_n/0,t_i\in Z_{n_i}/0)$。从根节点到叶子节点的每条路径中，最后一个内部节点是叶子节点的父节点，本文称之为末端内部节点。定义末端内部节点只能代表关系 and。根据语义一致性可知，每个末端内部节点下，一种属性只能出现一次。

3.2　秘密共享方案

随机选择 $s\in Z_N/0$ 为待共享的秘密，设置访问树的根节点 τ 的值为 s。假设 τ 的子节点个数为 u，为 τ 的子节点赋值如下。

Case 1：τ 代表关系 or，则设置 τ 的每个子节点的值为 s；

Case 2：τ 代表关系 and，则为前 $u-1$ 个子节点取随机值 $s_i\in Z_N/0$，设置最后一个子节点的值为 $s_u=s-\sum_{i=1}^{u-1}s_i$；

Case 3：τ 代表关系 threshold，节点的门限值为 h，则随机选择一个 $h-1$ 次多项式 f，满足 $f(0)=s$；对于索引次序为 $i\in Z_u/0$ 的子节点，设置其值为 $f(i)$。

从根节点开始，以上述方式自顶向下递归地为每个内部节点赋值。

3.3　算法设计

子群 G_p 用于正常加解密运算；G_r 用于参数的随机化，使方案达到 CCA 安全性；G_q 只用于安全性证明，不用于实际方案的运行。

1) $Setup(1^\lambda)$：运行算法 $\mathcal{G}$ (1^λ)获得$(N=pqr, G, G_T, \hat{e})$。在 G 中找出子群 G_p 和 G_r，以及各自的生成元 g_p 和 g_r。对于系统中的每个属性值 $v_{i,t_i}\left(i\in Z_n/0,t_i\in Z_{n_i}/0\right)$，随机选择 $a_{i,t_i}\in Z_N/0$ 和 $R_{i,t_i}\in G_r$，计算 $A_{i,t_i}=g_p^{a_{i,t_i}}R_{i,t_i}$。随机选择 $\omega,\varpi\in Z_N/0$ 和 $R_0\in G_r$，计算 $A_0=g_pR_0$，$Y=\hat{e}(g_p,g_p)^{\omega}$，$\overline{Y}=\hat{e}(g_p,g_p)^{\varpi}$。发布公钥

$$PK=\left\langle A_0,g_r,\left\{A_{i,t_i}\right\}_{1\le t_i\le n_i,1\le i\le n},Y,\overline{Y}\right\rangle \tag{1}$$

保存主密钥

$$MSK=\left\langle g_p,\left\{a_{i,t_i}\right\}_{1\le t_i\le n_i,1\le i\le n},\omega,\varpi\right\rangle \tag{2}$$

2) $KeyGen(L,MSK,PK)$：构造属性集 L 对应的私钥。对 $\forall\, i\in Z_k/0$，随机选择 $d_i\in Z_N/0$，计算 $D_i=g_p^{\frac{d_i}{a_{i,t_i}}}$。设置 $d=\sum_{i=1}^{k}d_i$，计算 $D_0=g_p^{\omega-d}$，$\overline{D_0}=g_p^{\varpi-d}$，构造私钥如下

$$SK_L=\left\langle D_0,\overline{D_0},\left\{D_i\right\}_{1\le i\le k}\right\rangle \tag{3}$$

3) $Encrypt(PK\ m,T)$：对于访问树中的末端内部节点 α，假设其共享秘密值为 s_α，为系统中每个属性

取值计算一个密文分量。如果该属性未出现在节点 α 下叶子节点所代表的表达式中，或者属性和属性值都出现，则计算 $C_{i,t_i}=A_{i,t_i}{}^{s_\alpha}R'_{i,t_i}$；否则随机选择 $s_{i,t_i}\in Z_N/0$ 且 $s_{i,t_i}\neq s_\alpha$，$R'_{i,t_i}\in G_r$，计算 $C_{i,t_i}=A_{i,t_i}{}^{s_{i,t_i}}R'_{i,t_i}$。假设 L_α 表示 α 下的叶子节点所代表的表达式中属性和属性值的集合，即有

$$C_{i,t_i}=\begin{cases}A_{i,t_i}{}^{s_{i,t_i}}R'_{i,t_i}, i\left(L_i\in L_\alpha \text{ and } v_{i,t_i}\notin L_\alpha\right)\\ A_{i,t_i}{}^{s_\alpha}R'_{i,t_i}, \text{其他}\end{cases} \tag{4}$$

随机选择 $R_\alpha\in G_r$，计算密文组件 $\overline{C_\alpha}=A_0{}^{s_\alpha}R_\alpha$，$H_\alpha=\overline{Y}^{s_\alpha}$。联合这些组件，得到 α 的密文为

$$C_\alpha=\left\langle H_\alpha,\overline{C_\alpha},\left\{C_{i,t_i}\right\}_{1\leqslant t_i\leqslant n_i,1\leqslant i\leqslant n}\right\rangle \tag{5}$$

随机选择 $R'_0\in G_r$，计算 $C_0=A_0{}^sR'_0$，$\widetilde{C}=mY^s$，则最终的密文为

$$C=\left\langle\widetilde{C},C_0,\left\{C_\alpha\right\}_{\forall\alpha}\right\rangle \tag{6}$$

4) *Decrypt*(*PK*,SK_L,*C*)：对于 *T* 中的每个末端内部节点 α，定义解密值函数

$$DecNode(\alpha)=\prod_{i=1}^{k}\hat{e}\left(C_{i,t_i},D_i\right) \tag{7}$$

对于 *T* 中的其他内部节点 β，定义解密值函数

$$DecNode(\beta)=\begin{cases}\prod_{i=1}^{u}DecNode\left(Child(\beta,i)\right), Op(\beta)=\text{and}\\ DecNode\left(Child(\beta,i)\right), Op(\beta)=\text{or}\\ \prod_{i=1}^{h}DecNode\left(Child(\beta,i)\right)^{\prod_{j=1,j\neq i}^{h}\frac{i}{j-i}}, Op(\beta)=\text{threshold}\end{cases} \tag{8}$$

其中，假设 *u* 为节点 β 的子节点个数，*h* 为门限值。

解密过程分为 3 步：1)计算并验证末端内部节点的解密值；2)是通过正确的末端内部节点解密值计算访问树根节点的解密值；3)是利用根节点的解密值计算明文。

对于末端内部节点 α，DReq 计算 $DecNode(\alpha)=\prod_{i=1}^{k}\hat{e}\left(C_{i,t_i},D_i\right)$，如果 DReq 满足 α 中每个叶子节点所代表的属性条件表达式，则可计算出正确的解密值 $DecNode(\alpha)=\hat{e}\left(g_p,g_p\right)^{ds_\alpha}$，通过验证系统 $\theta_\alpha=\dfrac{H_\alpha}{\hat{e}(\overline{C_\alpha},\overline{D_0})DecNode(\alpha)}$ 得出 θ_α=1（1 表示群 G_T 的单位元）；否则，得出 θ_α 为随机值。

如果 DReq 满足访问控制策略，可得根节点解密值 $DecNode(root(T))=\hat{e}(g_p,g_p)^{ds}$。则明文计算如下：

$$\begin{aligned}&\frac{\widetilde{C}}{\hat{e}\left(C_0,D_0\right)DecNode\left(root\left(T\right)\right)}\\ &=\frac{mY^s}{\hat{e}\left(A_0{}^sR'_0,g_p{}^{\omega-d}\right)\hat{e}\left(g_p,g_p\right)^{ds}}\\ &=\frac{m\hat{e}\left(g_p,g_p\right)^{\omega s}}{\hat{e}\left(g_p,g_p\right)^{\omega s-ds}\hat{e}\left(g_p,g_p\right)^{ds}}=m\end{aligned} \tag{9}$$

3.4 策略隐藏

1) DO 在加密消息之前，依据访问控制策略构造访问树。由于 DSP 并不可信，DO 不会将整个访问树发送给 DSP，而是去掉叶子节点所代表的属性条件表达式，只发送内部节点及其组织结构。因此，DSP 和 DReq 都无法得到访问控制策略对属性及其取值的要求。

2) DReq 计算末端内部节点的解密值时，将其所有属性的私钥分量都代入计算，并验证解密值是否正确。因此，DReq 只能确定自己的属性集合是否满足该末端内部节点，而无法得到末端内部节点下的具体属性条件表达式。

本文方案依据以上两点实现策略隐藏。

3.5 解密值验证

为了避免 DReq 使用错误的末端内部节点解密值参与进一步的解密，降低效率，需要为 DReq 提供一种手段，验证末端内部节点解密值的正确性。

为此，本文构造了 2 个并行的系统(加密系统和验证系统)。加密系统用于加解密真实的消息。验证系统用于 DReq 验证末端内部节点的解密值是否正确。2 个系统使用同样的群结构，只是在用户私钥组件 $D_0(\overline{D_0})$，以及密文组件 $\tilde{C}(H_\alpha)$和 $C_0(\overline{C_\alpha})$的参数取值上有所区别。加密系统的密文组件包括 $\left\langle\widetilde{C},C_0,\left\{\left\{C_{i,t_i}\right\}_{1\leqslant t_i\leqslant n_i,1\leqslant i\leqslant n}\right\}_{\forall\alpha}\right\rangle$，用户私钥组件包括 $\left\langle D_0,\left\{D_i\right\}_{1\leqslant i\leqslant k}\right\rangle$；验证系统的密文组件包括 $\left\langle H_\alpha,\overline{C_\alpha},\left\{\left\{C_{i,t_i}\right\}_{1\leqslant t_i\leqslant n_i,1\leqslant i\leqslant n}\right\}_{\forall\alpha}\right\rangle$，用户私钥组件包括 $\left\langle\overline{D_0},\left\{D_i\right\}_{1\leqslant i\leqslant k}\right\rangle$。

4　安全性证明

这里使用 Waters 等[12]提出的双系统加密的概念。首先定义半功能密文和半功能私钥，它们只应用在方案的安全性证明中，并不应用在真正系统的加解密中。假设 g_q 为子群 G_q 的生成元。

半功能密文：计算正规密文 $\left\langle \widetilde{C}', C_0', \{(C'_{i,t_i})_{1\leqslant t_i\leqslant n_i, 1\leqslant i\leqslant n}\}_{\forall\alpha} \right\rangle$；随机选择 $x_0\in Z_N/0$，在每个末端内部节点中，对于 $\forall t_i\left(i\in Z_n/0, t_i\in Z_{n_i}/0\right)$，随机选择 $x_{i,t_i}\in Z_N/0$；生成半功能密文如

$$\left\langle \widetilde{C}=\widetilde{C}', C_0=C_0' g_q^{x_0}, \left\{\left\{C_{i,t_i}=C'_{i,t_i} g_q^{x_{i,t_i}}\right\}_{1\leqslant t_i\leqslant n_i, 1\leqslant i\leqslant n}\right\}_{\forall\alpha} \right\rangle \tag{10}$$

半功能密钥：计算正规私钥 $\left\langle D_0', \left\{D_i'\right\}_{1\leqslant i\leqslant k} \right\rangle$；随机选择 $y_0\in Z_N/0$，对于 $\forall\ i(i\in Z_k/0)$，随机选择 $y_i\in Z_N/0$；生成半功能密钥如下

$$\left\langle D_0=D_0' g_q^{y_0}, \left\{D_i=D_i' g_q^{y_i}\right\}_{1\leqslant i\leqslant k} \right\rangle \tag{11}$$

当用户满足访问结构时，正规私钥可以解密正规密文和半功能密文，半功能私钥可以解密正规密文，但半功能私钥不能解密半功能密文。

方案的安全性依赖于 2.2 节中的 3 项假设；本文利用混合争论技术，借助一系列相邻游戏的不可区分性证明方案的安全性。设敌手在一次游戏中共进行了 u 次私钥询问。

$Game_{\text{real}}$：真实的安全性游戏，私钥和密文都是正规的。

$Game_0$：所有询问的私钥都是正规的，挑战密文是半功能的。

$Game_{1,k}$：挑战密文是半功能的，前 k 次询问的私钥是半功能的，剩余的私钥是正规的。

$Game_{\text{final}}$：所有询问的私钥都是半功能的，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 PPT 算法 $\mathcal{A}$ 在 $Game_{\text{real}}$ 和 $Game_0$ 上的优势满足 $\text{Adv}_{\mathcal{A}}^{Game_{\text{real}}}-\text{Adv}_{\mathcal{A}}^{Game_0}=\varepsilon$，那么可以构造一个 PPT 算法 $\mathcal{S}$ 以 ε 的优势攻破假设 1。

证明　给定假设 1 的条件$(\underline{G}, g_p, g_r)$。

Setup：同 2.4 节中的 *Setup* 算法。

Phase 1：敌手 $\mathcal{A}$ 可以询问任何属性集的私钥。

Challenge：敌手 $\text{Adv}^1_{g,\mathcal{A}(\lambda)}$ 选择 2 个等长的消息 m_0 和 m_1，以及访问结构 T_0 和 T_1（任何询问的属性集都不能满足访问结构 T_0 和 T_1），发送给挑战者 $\mathcal{S}$；$\mathcal{S}$ 随机选择 $b\in\{0,1\}$，用访问结构 T_b 加密 m_b，随机选择 $s\in Z_N/0$ 和 $R_0'\in G_r$，$\mathcal{S}$ 根据主密钥 *MSK* 及假设条件生成密文，$\widetilde{C}^*=m_b\ \hat{e}\ \left(g_p, X\right)^{\omega s}$，$C_0^*=X^s R_0'$，当 $\left(\left(L_i\in L_\alpha\right)\wedge\left(v_{i,t_i}\notin L_\alpha\right)\right)$ 时，取随机数 $s_{i,t_i}\in Z_N/0$ 且 $s_{i,t_i}\neq s_\alpha$，令 $C_{i,t_i}^*=X^{a_{i,t_i}\cdot s_{i,t_i}} R'_{i,t_i}$，否则令 $C_{i,t_i}^*=X^{a_{i,t_i}\cdot s_\alpha} R'_{i,t_i}$；最后 $\mathcal{S}$ 向 $\mathcal{A}$ 发送密文 $\left\langle C^*, C_0^*, \left\{\left\{C_{i,t_i}^*\right\}_{1\leqslant t_i\leqslant n_i, 1\leqslant i\leqslant n}\right\}_{\forall\alpha} \right\rangle$。

Phase 2：重复执行阶段 1。

Guess：敌手 $\mathcal{A}$ 输出一个关于 d 的猜测 d'。

如果 $X\in G_p$，那么询问密文 c^* 是正规密文；如果 $X\in G_{pq}$，那么 c^* 为半功能密文。因此，若敌手 $\mathcal{A}$ 使 $\text{Adv}_{\mathcal{A}}^{Game_{real}}-\text{Adv}_{\mathcal{A}}^{Game_0}=\varepsilon$ 不可忽视，那么挑战者同样能够以不可忽略的优势区分 G_{pq} 和 G_p 上的元素。

引理 2　如果存在一个 PPT 算法 $\mathcal{A}$ 使 $\text{Adv}_{\mathcal{A}}^{Game_{1,k-1}}-\text{Adv}_{\mathcal{A}}^{Game_{1,k}}=\varepsilon$，那么可以构造一个 PPT 算法 $\mathcal{S}$ 以 ε 的优势攻破假设 2。

证明　给定假设 2 的条件$(\underline{G}, g_p, X_1X_2, g_r)$。

Setup：同引理 1。

Challenge：敌手 $\mathcal{A}$ 选择 2 个等长的消息 m_0 和 m_1，以及访问结构 T_0 和 T_1（任何询问的属性集都不能满足访问结构 T_0 和 T_1），发送给挑战者 $\mathcal{S}$；$\mathcal{S}$ 随机选择 $b\in\{0,1\}$，用访问结构 T_b 加密 m_b，随机选择 $s\in Z_N/0$ 和 $R_0'\in G_r$，$\mathcal{S}$ 根据主密钥 *MSK* 及假设条件生成半功能密文，$\widetilde{C}^*=m_b\ \hat{e}\left(g_p, X_1X_2\right)^{\omega s}$，$C_0^*=\left(X_1X_2\right)^s R_0'$，当 $\left(\left(L_i\in L_\alpha\right)\wedge\left(v_{i,t_i}\notin L_\alpha\right)\right)$ 时，取随机数 $s_{i,t_i}\in Z_N/0$ 且 $s_{i,t_i}\neq s_\alpha$，令 $C_{i,t_i}^*=\left(X_1X_2\right)^{a_{i,t_i}s_{i,t_i}} R'_{i,t_i}$，否则，令 $C_{i,t_i}^*=\left(X_1X_2\right)^{a_{i,t_i}s_\alpha} R'_{i,t_i}$；并发送密文给敌手 $\mathcal{A}$。

Phase 1,2 将私钥询问分成 3 部分，考虑敌手的第 i 次询问。

Case 1：$i>k$ 时，挑战者 $\mathcal{S}$ 可以由主密钥和敌手 $\mathcal{A}$ 询问的属性集计算出正常私钥，并发送给敌手 $\mathcal{A}$。

Case 2：$i<k$ 时，由于 $Game_{1,k-1}$ 和 $Game_{1,k}$ 的前 $k-1$ 次私钥都是半功能的，因此挑战者 $\mathcal{S}$ 首先计算出半功能密钥并发送给敌手。

Case 3：$i=k$ 时，挑战者 $\mathcal{S}$ 根据敌手 $\mathcal{A}$ 询问的属性集 L，对 $\forall i\in Z_k/0$，随机选择 $d_i\in Z_N/0$，设置 $d=\sum_{i=1}^{k}d_i$，生成密钥 $D_0^{'}=X^{\omega-d}$，$D_i^{'}=X^{\frac{d_i}{a_{i,t_i}}}$。

Guess：敌手 $\mathcal{A}$ 输出一个关于 d 的猜测 d'。

如果 $X\in G_p$，设 $X=G_p$，则生成的是正规密钥，进行的游戏是 $Game_{1,k-1}$；如果 $X\in G_{pq}$，设 $X=g_pg_q^{\frac{y_0}{\omega-d}}$，则生成的是半功能密钥，进行的游戏是 $Game_{1,k}$。因此，若敌手 $\mathcal{A}$ 使 $\mathrm{Adv}_{\mathcal{A}}^{Game_{1,k-1}}-\mathrm{Adv}_{\mathcal{A}}^{Game_{1,k}}=\varepsilon$ 不可忽视，那么挑战者 $\mathcal{S}$ 同样能够以不可忽略的优势区分 G_{pq} 和 G_p 上的元素。

引理 3 如果存在一个 PPT 算法 $\mathcal{A}$ 使 $\mathrm{Adv}_{\mathcal{A}}^{Game_{1,u}}-\mathrm{Adv}_{\mathcal{A}}^{Game_{final}}=\varepsilon$，那么可以构造一个 PPT 算法 $\mathcal{S}$ 以 ε 的优势攻破假设 3。

证明 给定假设 3 的条件$(\underline{G}, g_p, g_p^{\omega}X_2, g_p^{s}Y_2, Z_1Z_2, g_r)$。

Setup：同引理 1。

Phase 1：在游戏 $Game_{1,u}$ 和 $Game_{final}$ 中，生成的密钥都是半功能的。挑战者 $\mathcal{S}$ 根据敌手 $\mathcal{A}$ 询问的属性集，对 $\forall i\in Z_k/0$，随机选择 $d_i\in Z_N/0$，设置 $d=\sum_{i=1}^{k}d_i$，生成半功能密钥 $D_0^{'}=g_p^{\omega}X_2(Z_1Z_2)^{-d}$，$D_i^{'}=(Z_1Z_2)^{\frac{d_i}{a_{i,t_i}}}$。

Challenge：敌手 $\mathcal{A}$ 选择 2 个等长的消息 m_0 和 m_1，以及访问结构 T_0 和 T_1（任何询问的属性集都不能满足访问结构 T_0 和 T_1），发送给挑战者 $\mathcal{S}$；$\mathcal{S}$ 随机选择 $b\in\{0,1\}$，用访问结构 T_b 加密 m_b 或者随机消息 r，$\mathcal{S}$ 随机选择 $s\in Z_N/0$ 和，根据主密钥 MSK 以及假设条件生成半功能密文，$\widetilde{C}^{*}=m_bT$，$C_0^{*}=g_p^{s}Y_2R_0^{'}$，当$\left((L_i\in L_\alpha)\wedge\left(v_{i,t_i}\notin L_\alpha\right)\right)$时，取随机数 $s_{i,t_i}\in Z_N/0$ 且 $s_{i,t_i}\neq s_\alpha$，令 $C_{i,t_i}^{*}=g_p^{a_{i,t_i}s_{i,t_i}}R_{i,t_i}^{'}$，否则令 $C_{i,t_i}^{*}=g_p^{a_{i,t_i}\cdot s_\alpha}R_{i,t_i}^{'}$；并发送密文给敌手 $\mathcal{A}$。

Phase 2：重复执行阶段 1。

Guess：敌手 $\mathcal{S}$ 输出一个关于 d 的猜测 d'。

当 $T=\hat{e}(g_p,g_p)^{\omega s}$ 时，生成的是 m_b 的半功能密文；否则，设 $T=\hat{e}\left(g_p,g_p\right)^{\omega s-x_0}$，生成的是随机消息 $m_b\hat{e}\left(g_p,g_p\right)^{\omega s-x_0}$ 的半功能密文。因此，若敌手 $\mathcal{A}$ 使得 $\mathrm{Adv}_{\mathcal{A}}^{Game_{1,u}}-\mathrm{Adv}_{\mathcal{A}}^{Game_{\mathrm{final}}}=\varepsilon$ 不可忽视，那么挑战者 $\mathcal{S}$ 同样能够以不可忽略的优势区分 $\hat{e}(g_p, g_p)^{\omega s}$ 与 G_T 上的一个随机元素。

定理 1 如果假设 1、假设 2 和假设 3 成立，则本文提出的 CP-ABE 方案是安全的。

证明 如果假设 1、假设 2 和假设 3 成立，则真实的安全游戏与 $Game_{\mathrm{final}}$ 之间是不可区分的，而在 $Game_{\mathrm{final}}$ 中，敌手的攻击优势 $\mathrm{Adv}_{\mathcal{A}}^{Game_{\mathrm{final}}}$ 是可忽略的，因此敌手在 $Game_{\mathrm{real}}$ 中的攻击优势 $\mathrm{Adv}_{\mathcal{A}}^{Game_{\mathrm{real}}}$ 也是可忽略的。所以本文方案是 adaptively-CCA 安全的。

5 方案分析和实验验证

5.1 方案分析

现将本文提出的方案与已有的几种策略隐藏方案在性能和安全性 2 个方面进行比较，主要考虑群阶的性质、用户私钥长度、密文长度、解密运算量，以及 CCA 安全性。具体比较结果如表 1 所示。其中，n 表示系统中的属性个数，n_i 表示第 i 个属性的取值个数，$k(k\leqslant n)$表示用户私钥的属性个数。$|G|$ 和$|G_T|$分别表示群 G 和 G_T 中元素的长度，G 和 G_T 分别表示群 G 和 G_T 中运算，$\hat{e}$ 表示双线性映射运算，$|\alpha|$表示访问结构中末端内部节点的个数。

表 1 不同策略隐藏方案的对比

方案	群阶	私钥长度		密文长度		解密运算		安全模型
		$\|G\|$	$\|G_T\|$	$\|G\|$	$\|G_T\|$	$\hat{e}$	G_T	
文献[6]	素数	$1+2n$	0	$1+n+\sum_{i=1}^{n}n_i$	1	$1+3n$	$1+3n$	selectly-CCA
文献[7]	合数	$1+n$	0	$1+\sum_{i=1}^{n}n_i$	1	$1+n$	$1+n$	adaptively-CCA
文献[8]	素数	8	0	$8+\sum_{i=1}^{n}n_i$	1	8	8	adaptively-CCA
本文	合数	$2+k$	0	$1+\lvert\alpha\rvert+\lvert\alpha\rvert\sum_{i=1}^{n}n_i$	$1+\lvert\alpha\rvert$	$1+\lvert\alpha\rvert+k\lvert\alpha\rvert$	$2+\lvert\alpha\rvert+k\lvert\alpha\rvert$	adaptively-CCA

表 1 中第 3 种方案是由第 2 种方案转换而来，本文方案同样可以使用这种方法转换为素数阶群构造，只是为了在达到 adaptively-CCA 安全性的同时，清晰的表示算法设计，所以才采用合数阶群。缺点在于，合数阶群方案的私钥长度和解密运算量与用户属性个数呈线性关系。

本文方案以末端内部节点为单位来实现加解密运算。加密时，在每个末端内部节点下为所有的属性取值计算一个密文分量；解密时，则基于这些密文分量和用户私钥分量通过双线性映射计算末端内部节点的解密值。因此，密文长度和加密运算量与访问结构中的末端内部节点数$|\alpha|$和系统的属性取值规模$\sum_{i=1}^{n} n_i$相关；而解密运算量则与访问树的末端内部节点数$|\alpha|$，以及用户的属性个数 k 相关。相比之下，当访问树结构复杂时，密文长度和加解密运算量较大；但是对于那些用户属性规模远小于系统属性规模的用户，则在私钥长度和解密运算量上具有一定优势。总之，本文方案以较小的性能损失为代价，实现了复杂结构的策略隐藏，同时达到了较高的安全性。

5.2　实验验证

实验设备为 Intel Core2 Quad 2.83 GHz，1.85 GB 内存，Microsoft Windows XP 专业版操作系统。实验环境搭建于 WMware Workstation 虚拟机上的 Read Hat Enterprise 6.2，分配 1GB 内存。实验代码基于 PBC-0.5.14[13]和 cpabe-0.11[14]进行修改和编写。

不失一般性，假设用户拥有的属性数目为 5，系统的属性数目在 5~50 之间波动，每个属性平均拥有 5 个不同的取值。对于访问树的末端内部节点数目，分别取 1 个、2 个、3 个这 3 种情形，以测试不同复杂程度的访问树结构对加解密的影响。

图 1 给出了本文方案在不同末端内部节点数目情形下与文献[7]方案的加密耗时对比。可见当访问树中末端内部节点为 1 时，加密耗时与文献[7]方案基本持平。但是随着访问树结构复杂程度的增加，加密耗时不断增加。

图 2 给出了本文方案在不同末端内部节点数目情形下与文献[7]方案的解密耗时对比。可见解密耗时与系统属性数目无关，但是同样随着访问树结构复杂程度的增加而增加。

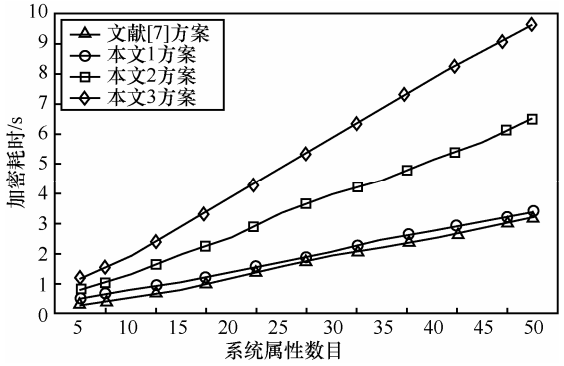


图 1　加密耗时与系统属性数目的关系

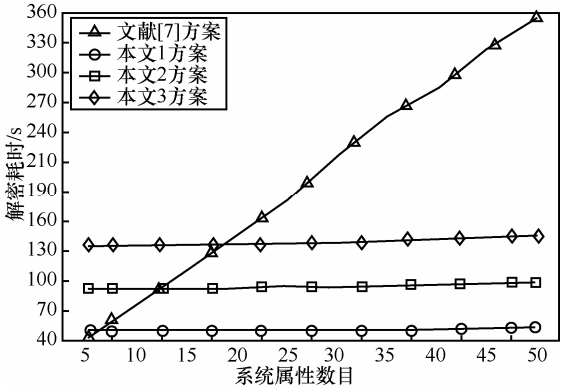


图 2　解密耗时与系统属性数目的关系

6　结束语

随着信息系统规模的日益扩大和系统用户的逐渐增加，使用复杂访问结构来表达细粒度的访问控制策略就越发显得重要。本文提出一种新的 CP-ABE 方案，解决了在访问树中实现策略隐藏的难题，使用户可以制定灵活的访问控制策略，而不用担心策略泄露的问题；通过双系统加密的概念证明了方案的 CCA 安全性；分析比较了方案的特点和性能。下一步，将重点研究减小密文规模和减少解密运算量。

参考文献：

[1] 苏金树, 曹丹, 王小峰, 等. 属性基加密机制[J]. 软件学报, 2011, 22(6):1299-1315.
SU J S, CAO D, WANG X F, *et al*. Attribute-based encryption schemes[J]. Journal of Software, 2011, 22(6):129-1315.

[2] SAHAI A, WATERS B. Fuzzy identity-based encryption[A]. Advances in the 24th Annual International Conference on the Theory and Applications of Cryptographic Techniques(EUROCRYPT 2005)[C]. Aarhus, Denmark, 2005.457-473.

[3] GOYAL V, PANDEY O, SAHAI A, *et al*. Attribute-based encryption for fine-grained access control of encrypted data[A]. Proceedings of the 13th ACM Conference on Computer and Communications Secu-

rity[C].Alexandria, VA, USA, 2006.89-98.

[4] BETHENCOUNT J, SAHAI A, WATERS B. Ciphertext-policy attribute-based encryption[A]. Proceedings of the 2007 IEEE Symposium on Security and Privacy(IEEE S&P 2007)[C]. Oakland,CA, USA, 2007.321-334.

[5] KAPADIA A, TSANG PP, SMITH S W. Attribute-based publishing with hidden credential and hidden policies[A]. Proceedings of the 14th Annual Network and Distributed System Security Symposim(NDSS 2007)[C]. San Diego, CA,USA,2007. 179-192.

[6] NISHIDE T, YONEYAMA K, OHTA K. Attribute-based encryption with partially hidden encryptor-specified access structures[A]. Proceedings of the Applied Cryptography and Network Security (ACNS 2008) [C].New York, NY, USA, 2008.111-129.

[7] LAI J Z, DENG R H, LI Y J. Fully secure cipertext-policy hiding CP-ABE[A]. Proceedings of the 7th Information Security Practice and Experience(ISPEC 2011)[C]. Guangzhou, China, 2011.24-39.

[8] 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):457-561.
WANG H B, CHEN S Z. Attribute-based encryption with hidden access structures[J]. Journal of Electronics and Information Technology, 2012,34(2)：457-561.

[9] FREEMAN M. Converting pairing-based cryptosystems from composite-order groups to prime-order groups[A]. Advances in Advances in the 29th Annual International Conference on the Theory and Applications of Cryptographic Techniques(EUROCRYPT 2010)[C]. Aarhus, Denmark, 2010. 44-61.

[10] IBRAIMI L, TANG Q, HARTEL P, *et al*. Efficient and provable secure ciphertext-policy attribute-based encryption schemes[A]. Proceedings of the Information Security Practice and Experience[C].Xi'an, China, 2009.1-12.

[11] BONEH D, GOH E, NISSIM K. Evaluating 2-dnf formulas on ciphertexts[A]. Proceedings of the 1st Theory of Cryptography Conference(TCC 2005)[C]. Cambridge, MA, USA, 2005. 325-341.

[12] WATERS B. Dual system encryption: realizing fully secure ibe and hibe under simple assumptions[A]. Advances in the 29th International CryptologyConference(CRYPTO 2009)[C]. Santa Barbara,CA, USA, 2009. 619-636.

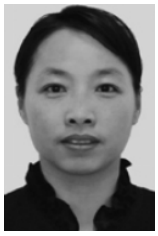
[13] LYNN B. The pairing-based cryptography(PBC) library[EB/OL]. http://crypto. Stanford. edu/pbc/.

[14] BETHENCOURT J, SAHAI A, WATERS B. Advanced crypto software collection：the cpabetoolkit[EB/OL]. http://acsc.cs.utexas.edu/cpabe/.2011.

作者简介：

宋衍（1982-），男，湖北老河口人，北京交通大学博士生，信息保障技术重点实验室工程师，主要研究方向为网络安全、数据库等。

韩臻（1962-），男，浙江宁波人，北京交通大学教授、博士生导师，主要研究方向为信息安全体系结构、可信计算等。



刘凤梅（1974-），女，河南郸城人，博士，信息保障技术重点实验室副研究员，主要研究方向为密码理论与应用。

刘磊（1979-），男，陕西户县人，信息保障技术重点实验室工程师，主要研究方向为信息安全、操作系统等。