doi:10.3969/j.issn.1000-436x.2012.z1.036

新型自适应安全的密钥策略 ABE 方案

罗颂[1]，陈钟[2]
(1. 重庆理工大学 计算机科学与工程学院，重庆 400054；2. 北京大学 信息科学技术学院软件研究所，北京 100871)

摘 要：基于 3 维对偶正交基的技术，提出了一种新的密钥策略的基于属性的加密方案。该方案在素数阶群上构造，支持单调访问结构，具有自适应安全性。方案利用双重系统加密的证明方法将方案的自适应安全性归约到判定线性假设。与同样是自适应安全的密钥策略 ABE 方案相比，提出的方案在同等安全性上具有更高的效率。
关键词：基于属性的加密；密钥策略；素数阶群；自适应安全
中图分类号：TP309 **文献标识码**：A **文章编号**：1000-436X(2012)Z1-0270-06

New adaptively secure key-policy attribute-based encryption scheme

LUO Song[1], CHEN Zhong[2]
(1. College of Computer Science and Engineering, Chongqing University of Technology, Chongqing 400054, China;
2. Institute of Software, School of Electronics Engineering and Computer Science, Peking University, Beijing 100871, China)

Abstract: A new key-policy attribute-based encryption scheme based on 3 dimension dual orthonormal bases was proposed. This scheme was constructed in prime order groups with adaptive security and supporting access structures. It has been proved the security from decisional linear assumption by using dual system encryption technique. Compared with previous key-policy ABE scheme which is also adaptively secure, the scheme is more efficient at the same security level.
Key words: attribute-based encryption; key policy; prime order group; adaptive security

1 引言

基于属性的加密（ABE, attribute-based encryption）是基于身份的加密（IBE, identity-based encryption）[1~3]的泛化，即用户的公钥不再由某一个具体的身份（如 E-mail，IP 地址等）来代表，而是由一系列的属性（如单位、职称）来表示。在 ABE 中，密文或密钥可以结合访问控制策略，能够实现细粒度的访问控制，因而非常适合复杂开放式网络环境下对数据共享要求灵活可扩展的场合。ABE 继承了 IBE 的无证书特性，加密者仅需要使用接收者的属性信息结合公共参数即可完成加密，避免了管理公钥证书带来的开销。

基于属性的加密最早源于基于模糊身份的加密（FIBE，fuzzy identity-based encryption），由 Sahai 和 Waters[4]在 2005 年的欧密会上提出。模糊 IBE 又称为门限 ABE，密文可以对 n 个属性进行加密，并设置门限 t。当用户拥有的属性与密文加密的属性交集包含的属性个数大于等于 t 时即可成功解密。ABE 的正式定义由 Goyal 等人[5]给出，并分为 2 种类型：密钥策略 ABE 和密文策略 ABE。Goyal 等人还给出了一个密钥策略 ABE 方案。在密钥策略 ABE[4~6]中，用户的密钥与一个访问结构相联系，而密文则附带一些属性。而在密文策略 ABE[7, 8]中，情形正好相反。用户的密钥附带一些属性，而密文则与访问结构相联系。一般来说，密钥策略 ABE 比较适合数据静态的场景如付费电视、视频点播等，而密文策略 ABE 适合用户静态的场景如广播

收稿日期：2012-07-10
基金项目：国家自然科学基金资助项目（61073156, 61170263）
Foundation Item: The National Natural Science Foundation of China (61073156, 61170263)

加密等。

Goyal 等人[5]提出的密钥策略 ABE 方案支持单调访问结构，能够对加密数据进行细粒度的访问控制，但该方案仅具有选择安全性，且不支持属性的“非”操作。Ostrovsky 等人[6]利用广播撤销机制实现表示“非”的密钥策略 ABE 机制，使得策略表示更加灵活。但是该方案仍然是选择性安全的，而且密文和用户密钥大小、加解密开销都翻倍。Attrapadung 与 Imai[9]则提出了一个双重策略的 ABE 方案，该方案允许密钥策略和密文策略同时作用在加密数据上。杨晓元等人[10]研究了多授权机构的密文策略 ABE 方案，提出了一个选择性安全的多主密钥密文策略 ABE 方案。Katz、 Sahai 和 Waters[11]进一步增强了策略的表示，提出了“谓词加密”（predicate encryption），和“功能加密”（functional encryption）的概念，能够实现密钥策略或者密文策略。

在 Waters[12]提出双重系统加密的证明技术后，Lewko 等人[13]利用双重系统加密技术，在合数阶群上构造了一个自适应安全的密钥策略 ABE 方案，该方案同样支持单调访问结构，并且方案的安全性基于合数阶群上静态的困难性假设。

然而，由于基于合数阶群的困难性假设一般基于大数分解的困难性[11]，因此在同样的安全级别，合数阶群要求比素数阶群具有更大的尺寸，进而导致群上的一个关键运算且是最耗时的运算——双线性对运算在合数阶群和素数阶群上差距表现的相当惊人。文献[14]指出，在 80bit 的 AES 安全性上，前者的双线性对的单次运算时间是后者的 50 倍左右。因此，仍然有必要研究素数阶群上的密钥策略 ABE 方案的构造。

目前，关于素数阶群上的各类密码方案的构造（包括 IBE、ABE 等）通常有 2 种方法。一种是根据应用场景直接构造，这也是常用的构造方法；另外一种是将合数阶群上的方案翻译到素数阶群上来。Freeman[14]研究了这种翻译的可能性及困难性，之后由 Lewko[15]基于对偶正交基实现了对 Lewko-Waters IBE 方案[16]在素数阶群上的构造。

本文在 Lewko 工作[15]的基础上对密钥策略 ABE 的构造进行了深入研究，结合对偶正交基的技术，提出了一种新型的自适应安全的密钥策略 ABE 方案。该方案在素数阶上构造，支持单调访问结构，具有较高的计算效率。本文利用双重系统加密的证明技术，在标准模型上证明了提出的方案在判定线性假设下是自适应安全的。

2　背景知识

2.1　双线性对

定义 1　G，G_T 为 p 阶的乘法循环群，p 是素数。g 是 G 的一个生成元，$e:G\times G\to G_T$ 是一个双线性映射，具有如下性质。

1) 双线性性：对于任意的 $u,v\in G$ 和 $a,b\in\mathbb{Z}_p$，有 $e(u^a,v^b)=e(u,v)^{ab}$。

2) 非退化性：$e(g,g)\neq 1$。注意到 G_T 是素数阶群，这意味着 $e(g,g)$ 是 G_T 的生成元。

如果 G 中的运算及双线性映射 e 都是多项式时间可计算的，称 G 是一个双线性群，e 是一个双线性对。

本文假定有一个有效的算法 $\mathcal{G}$ 来生成双线性群。该算法以安全参数 λ 为输入，输出一个四元组（p，G，G_T，$g\in G$，e），其中 g 是 G 的一个生成元，$\log(p)=\Theta(\lambda)$。

2.2　对偶正交基

给定一个 $\mathbb{Z}_p$ 上的 n 维向量 $\vec{v}=(v_1,\cdots,v_n)\in\mathbb{Z}_p^n$，$g$ 是 G 中的一个元素，定义 $g^{\vec{v}}$ 为 G 上的一个 n 元组为

$$g^{\vec{v}}:=(g^{v_1},\cdots,g^{v_n})$$

任给 $a\in\mathbb{Z}_p$ 及 $\vec{v}$，$\vec{w}\in\mathbb{Z}_p^n$，有

$g^{a\vec{v}}=(g^{av_1},\cdots,g^{av_n})$ 及 $g^{\vec{v}+\vec{w}}=(g^{v_1+w_1},\cdots,g^{v_n+w_n})$。

利用双线性对 e 来定义向量的双线性对，记为 e_n：$e_n(g^{\vec{v}},g^{\vec{w}}):=\prod_{i=1}^{n}e(g^{v_i},g^{w_i})=e(g,g)^{\vec{v}\cdot\vec{w}}$。

定义 2　定维数 n，如果 $\mathbb{Z}_p^n$ 上的 2 组基 $\mathbb{B}:=(\vec{b}_1,\cdots,\vec{b}_n)$ 和 $\mathbb{B}^*:=(\vec{b}_1^*,\cdots,\vec{b}_n^*)$ 满足如下条件

$$\vec{b}_i\cdot\vec{b}_j^*=\begin{cases}0, & i\neq j\\ \psi, & i=j\end{cases}\pmod p$$

称 $(\mathbb{B},\mathbb{B}^*)$ 是 G 上一组 n 维对偶正交基。

在下文中，用 $Dual(\mathbb{Z}_p^n)$ 表示所有 n 维对偶正交基的集合，用 $a\xleftarrow{R}A$ 表示从集合 A 中随机选取一个元素 a。

2.3　困难性假设

定义 3　给定群生成算法 $\mathcal{G}$ 及 2 个正整数 $n,k>0$ 且 $k\leqslant\frac{n}{3}$，定义如下分布。

$(p, G, G_T, e) \xleftarrow{R} \mathcal{G}$， $(\mathbb{B}, \mathbb{B}^*) \xleftarrow{R} Dual(\mathbb{Z}_p^n)$，$g \xleftarrow{R} G$， $\eta, \beta, \tau_1, \tau_2, \tau_3, \mu_1, \mu_2, \mu_3 \xleftarrow{R} \mathbb{Z}_p$，$U_1 := g^{\mu_1 \vec{b}_1 + \mu_2 \vec{b}_{k+1} + \mu_3 \vec{b}_{2k+1}}$， $U_2 := g^{\mu_1 \vec{b}_2 + \mu_2 \vec{b}_{k+2} + \mu_3 \vec{b}_{2k+2}}$， …

$U_k := g^{\mu_1 \vec{b}_k + \mu_2 \vec{b}_{2k} + \mu_3 \vec{b}_{3k}}$， $V_1 := g^{\tau_1 \eta \vec{b}_1^* + \tau_2 \beta \vec{b}_{k+1}^*}$，

$V_2 := g^{\tau_1 \eta \vec{b}_2^* + \tau_2 \beta \vec{b}_{k+2}^*}$， …， $V_k := g^{\tau_1 \eta \vec{b}_k^* + \tau_2 \beta \vec{b}_{2k}^*}$，

$W_1 := g^{\tau_1 \eta \vec{b}_1^* + \tau_2 \beta \vec{b}_{k+1}^* + \tau_3 \vec{b}_{2k+1}^*}$，$W_2 := g^{\tau_1 \eta \vec{b}_2^* + \tau_2 \beta \vec{b}_{k+2}^* + \tau_3 \vec{b}_{2k+2}^*}$，…，

$W_k := g^{\tau_1 \eta \vec{b}_k^* + \tau_2 \beta \vec{b}_{2k}^* + + \tau_3 \vec{b}_{3k}^*}$，

$D := (g^{\vec{b}_1}, \cdots, g^{\vec{b}_{2k}}, g^{\vec{b}_{3k+1}}, \cdots, g^{\vec{b}_n}, g^{\eta \vec{b}_1^*}, \cdots, g^{\eta \vec{b}_k^*}, g^{\beta \vec{b}_{k+1}^*}, \cdots, g^{\beta \vec{b}_{2k}^*}, g^{\vec{b}_{2k+1}^*}, \cdots, g^{\vec{b}_n^*}, U_1, \cdots, U_k, \mu_3)$。

定义敌手 $\mathcal{A}$ 打破子空间假设的优势为

$$\left|\Pr[\mathcal{A}(D, V_1, \cdots, V_k) = 1] - \Pr[\mathcal{A}(D, W_1, \cdots, W_k) = 1]\right|$$

如果对于任何多项式时间的敌手 $\mathcal{A}$，该优势都是可忽略的，称群生成算法 $\mathcal{G}$ 满足子空间假设，或者子空间假设在 $\mathcal{G}$ 上成立。

根据文献[15]，子空间假设可以归约到判定线性假设。

引理 1 如果判定线性假设在 $\mathcal{G}$ 上成立，则子空间假设在 $\mathcal{G}$ 上也成立。

2.4 访问结构

定义 4 设 $\{P_1, \cdots, P_n\}$ 是 n 个参与者的集合。称集合 $\mathbb{A} \subseteq 2^{\{P_1, \cdots, P_n\}}$ 是单调的，如果 $\forall B, C$ 有 $B \in \mathbb{A}$ 且 $B \subseteq C$ 则 $C \in \mathbb{A}$。访问结构是 $\{P_1, \cdots, P_n\}$ 的非空子集，即 $\mathbb{A} \subseteq 2^{\{P_1, \cdots, P_n\}} \setminus \{\varnothing\}$。特别的，当 $\mathbb{A}$ 是单调时，称 $\mathbb{A}$ 是单调访问结构。$\mathbb{A}$ 中的元素称为授权集合，其余不在 $\mathbb{A}$ 中元素称为非授权集合。

定义 5 与者集合 $\mathcal{P}$ 上的秘密共享方案 $\prod$ 称为在 $\mathbb{Z}_p$ 上是线性的，如果

1) 每位参与者的份额是 $\mathbb{Z}_p$ 上的一个向量；

2) 存在 ℓ 行 n 列矩阵 A 称为 $\prod$ 的共享生成矩阵。令函数 ρ 为矩阵 A 的第 i 行到参与者的映射函数，即 $\rho(i) \in \mathcal{P}$。设要共享的秘密为 $s \in \mathbb{Z}_p$，考虑向量 $\vec{v} = (s, r_2, \cdots, r_n)^t$，这里 $r_2, \cdots, r_n$ 是随机选取的整数，则向量 $A\vec{v}$ 是秘密 s 关于 $\prod$ 的 ℓ 个份额，第 i 个份额 $(A\vec{v})_i$ 属于参与者 $\rho(i)$。

文献[17]表明，单调访问结构与线性秘密共享方案是等价的，且每个线性秘密共享方案具有线性重构的性质。设 $\prod$ 是访问结构 $\mathbb{A}$ 对应的线性秘密共享方案。令 $S \in \mathbb{A}$ 为一授权集，$I \subset \{1, \cdots, \ell\}$ 为 S 的指标集，即 $I = \{i : \rho(i) \in S\}$。则存在多项式时间可计算的常数 $\{\omega_i \in \mathbb{Z}_p\}_{i \in I}$，当 $\{\lambda_i\}$ 为秘密 s 关于 $\prod$ 的有效共享时，有 $\sum_{i \in I} \omega_i \lambda_i = s$。对于非授权集则不存在这样的 $\{\omega_i\}$。

2.5 密钥策略 ABE

定义 6 密钥策略 ABE 包含如下 4 个算法：系统建立（Setup），密钥生成（KeyGen），加密（Encrypt）及解密（Decrypt）。

Setup$(1^\lambda, \mathcal{U})$ 该算法以安全参数 λ 和属性集合 $\mathcal{U}$ 为输入，输出公钥 PK 及主密钥 MK。

KeyGen$(PK, MK, \mathbb{A})$ 该算法以公钥 PK、主密钥 MK 及一个访问结构 $\mathbb{A}$ 为输入，输出与 $\mathbb{A}$ 相联系的密钥 SK。

Encrypt(PK, M, S) 该算法以公钥 PK、明文消息 M 及接收者的属性集 S 为输入，输出密文 CT。

Decrypt(PK, CT, SK) 该算法以公钥 PK、以属性集 S 加密的密文 CT 及与访问结构 $\mathbb{A}$ 相联系的密钥 SK 为输入，如果 S 满足访问结构 $\mathbb{A}$，即 $S \models \mathbb{A}$，则输出明文 M；反之，则输出终止符 $\perp$。

给出密钥策略 ABE 的安全性定义。首先，定义一个挑战者与敌手之间的游戏如下。

Setup 挑战者运行 Setup 算法， 将公钥发送给敌手 $\mathcal{A}$。

Phase1 $\mathcal{A}$ 提交一个访问结构 $\mathbb{A}$ 进行 KeyGen 查询，挑战者返回相应的密钥 SK。$\mathcal{A}$ 提可以重复该过程多项式次数。

Challenge $\mathcal{A}$ 提交 2 个等长的消息 M_0，M_1 及属性集合 S。属性集 S 必须不满足之前提交的所有访问结构。挑战者随机选择一个比特 b，然后利用属性集 S 加密消息 M 得到 Encrypt(PK, M_b, S)，并将其返回给挑战者。

Phase2 重复 Phase 1，但要求 S 不能满足提交的访问结构。

Guess $\mathcal{A}$ 输出对 b 的猜测 b'。

在这个游戏中，敌手 $\mathcal{A}$ 的优势被定义为 $\left|\Pr[b' = b] - \frac{1}{2}\right|$。

定义 7 称一个密钥策略 ABE 方案是自适应安全的，如果任何多项式时间的敌手在上面游戏中的优势都是可忽略的。

3 方案构造

利用对偶正交基和线性秘密共享，给出一个密钥策略 ABE 方案的构造。将属性视为参与者，假设要加密的消息 M 是 G_T 上的元素，且在访问结构

的生成矩阵 A 中，每个属性只出现一次。

Setup$(1^\lambda, \mathcal{U})$ 给定安全参数 λ 及属性集合 $\mathcal{U}$，算法先运行群生成算法 $\mathcal{G}$ 得到（p，G，G_T，$g \in G$，e），并从 $Dual(\mathbb{Z}_p^3)$ 随机选取对偶正交基 $(\mathbb{D}, \mathbb{D}^*)$。设 $\mathbb{D}=(\vec{d}_1, \vec{d}_2, \vec{d}_3)$ 及 $\mathbb{D}^*=(\vec{d}_1^*, \vec{d}_2^*, \vec{d}_3^*)$。接着随机选取 $\alpha, \hat{\alpha}, \theta, \sigma \in \mathbb{Z}_p$。对于每个属性 $i \in \mathcal{U}$，随机选择 $s_i \in \mathbb{Z}_p$。最后算法发布公钥 $G, p, e(g,g)^{\alpha\theta\vec{d}_1\cdot\vec{d}_1^*}$，$e(g,g)^{\hat{\alpha}\sigma\vec{d}_2\cdot\vec{d}_2^*}$，$g^{\vec{d}_1}$，$g^{\vec{d}_2}$，$\{g^{s_i\vec{d}_1}$，$g^{s_i\vec{d}_2}\}\ \forall i$。主密钥为 α，$\hat{\alpha}$，$g^{\theta\vec{d}_1^*}, g^{\sigma\vec{d}_2^*}$ 及 $(g^{s_i\theta\vec{d}_1^*}, g^{s_i\sigma\vec{d}_2^*})\forall i$。

根据对偶正交基的定义，有 $\vec{d}_1\cdot\vec{d}_1^*=\vec{d}_2\cdot\vec{d}_2^*=\psi$。

KeyGen$(PK, MK, \mathcal{A}=(A,\rho))$ 算法随机选取 $\mathbb{Z}_p^n$ 上的两个随机向量 $\vec{v}$ 和 $\vec{w}$ 满足 $\vec{v}=(\alpha, v_2, \cdots, v_n)$ 及 $\vec{w}=(\hat{\alpha}, w_2, \cdots, w_n)$。对矩阵 A 的每一行 A_x，随机选取 $r_x, \hat{r}_x \in \mathbb{Z}_p$ 并计算 $D_x=g^{r_x\theta\vec{d}_1^*+\hat{r}_x\sigma\vec{d}_2^*}$ 及

$$K_x=g^{((A_x\cdot\vec{v})+r_x s_{\rho(x)})\theta\vec{d}_1^*+((A_x\cdot\vec{w})+\hat{r}_x s_{\rho(x)})\sigma\vec{d}_2^*}。$$

与 $\mathcal{A}$ 相应的密钥为 $(D_x, K_x)_{1\leqslant x\leqslant \ell}$。

Encrypt(PK, M, S) 算法随机选取 $t, \hat{t} \in \mathbb{Z}_p$ 并计算 $C=Me(g,g)^{s\alpha\theta\vec{d}_1\cdot\vec{d}_1^*+\hat{s}\hat{\alpha}\sigma\vec{d}_2\cdot\vec{d}_2^*}$，$C'=g^{s\vec{d}_1+\hat{s}\vec{d}_2}$ 及 $C_i=g^{ss_i\vec{d}_1+\hat{s}s_i\vec{d}_2}\ \forall i\in S$。

密文为 $C, C', C_i \forall i \in S$。这里默认包含集合 S。

Decrypt(PK, CT, SK) 如果 S 满足访问结构 $\mathcal{A}$，算法计算 $\omega_x \in \mathbb{Z}_p$ 使得 $\sum_{\rho(x)\in S}\omega_x A_x=(1,0,\cdots,0)$。接着计算

$$C_0=\prod_{\rho(x)\in S}(e_n(K_{\rho(x)}, C')/e_n(D_x, C_x))^{\omega_x}$$
$$=e(g,g)^{s\alpha\theta\vec{d}_1\cdot\vec{d}_1^*}e(g,g)^{\hat{s}\hat{\alpha}\sigma\vec{d}_2\cdot\vec{d}_2^*}$$

从而 $M=C/C_0$。

4　安全性证明

本节将给出上节构造的 ABE 方案的安全性。使用文献[12]介绍的双重系统加密证明技术，定义了 2 个额外的结构：半功能密文及半功能密钥。半功能密钥有 2 种形式，分别称为第 1 类和第 2 类。它们并不出现在实际的方案中，仅用于方案的安全性证明。

半功能密文　通过如下步骤得到一组半功能密文：首先调用加密算法得到一组正常密文 $S, \hat{C}, \hat{C}', \hat{C}_i \forall i\in S$。然后随机选取 $c\in\mathbb{Z}_p$，对 S 中的每个属性 i，同样随机选取 $z_i \in \mathbb{Z}_p$，这些 z_i 将被保存并用于生成第 1 类的半功能密钥。半功能密文为 $C=\hat{C}$，$C'=\hat{C}'\cdot g^{cd_3}$，$C_i=\hat{C}_i\cdot g^{cz_i\vec{d}_3}\forall i\in S$。

第 1 类的半功能密钥。通过如下步骤得到一组第 1 类的半功能密钥：首先调用密钥生成算法得到一组正常密钥 $(D_x', K_x')_{1\leqslant x\leqslant \ell}$，然后选取随机向量 $\vec{u}=(u_1, u_2, \cdots, u_n)\in\mathbb{Z}_p^n$。对访问结构中矩阵 A 的每一行 A_x，随机选取 $\gamma_x \in \mathbb{Z}_p$，并计算第 1 类的半功能密钥为 $D_x=D_x'\cdot g^{(A_x\cdot\vec{u}+\gamma_x z_{\rho(x)})\vec{d}_3^*}$，$K_x=K_x'\cdot g^{\gamma_x\vec{d}_3^*}$，$1\leqslant x\leqslant \ell$。

第 2 类的半功能密钥。第 2 类的半功能密钥计算与第 1 类的半功能密钥相似，但维持 K_x 不变：首先调用密钥生成算法得到一组正常密钥 $(D_x', K_x')_{1\leqslant x\leqslant \ell}$。然后选取随机向量 $\vec{u}\in\mathbb{Z}_p^n$，并计算第 2 类的半功能密钥为 $D_x=D_x' g^{(A_x\cdot\vec{u})\vec{d}_3^*}$，$K_x=K_x'$，$1\leqslant x\leqslant \ell$。

注意到第 1 类或第 2 类的半功能密钥均能解密正常密文，而正常密钥也能解密半功能密文。但当第 1 类或第 2 类的半功能密钥解密半功能密文时，解密过程将会出现一个扰动因子 $e(g,g)^{cu_1\vec{d}_3\cdot\vec{d}_3^*}$（注意第 1 类中的 z_i 与半功能密文选取的值相同），当 $u_1=0$ 时，仍然可以解密半功能密文。此时，本文称该半功能密钥是象征性的。

本文将方案的安全性归约于(3, 1)—子空间假设，最终归约于判定线性假设。证明过程使用双重系统加密证明技术，利用混合争论的方法，通过一系列游戏的两两不可区分性来证明系统的安全性。令 q 为攻击者能够进行密钥查询的最大次数。定义如下几种游戏。（$0\leqslant k\leqslant q$）。

$\text{Game}_{\text{Real}}$：该游戏为在第 2 节定义的真实游戏，即密文和密钥都是正常的。

$\text{Game}_{k,1}$：该游戏与 $\text{Game}_{\text{Real}}$ 相似，区别在于挑战密文为半功能密文，而前 $k-1$ 次密钥查询返回的是第 2 类的半功能密钥，第 k 次密钥查询返回的是第 1 类的半功能密钥，剩下的查询返回正常密钥。

$\text{Game}_{k,2}$：该游戏与 $\text{Game}_{\text{Real}}$ 相似，区别在于挑战密文为半功能密文，而前 k 次密钥查询返回的是第 2 类的半功能密钥，剩下的查询返回正常密钥。

$\text{Game}_{\text{Final}}$：此游戏与 $\text{Game}_{q,2}$ 相似，区别在于挑战密文则是对一个随机消息加密得到的一个半功能密文。

注意到 $\text{Game}_{0,1}=\text{Game}_{0,2}$，在该游戏中所有密

钥是正常的，而挑战密文是半功能密文。本文用 Game_0 来代表这 2 个游戏。在游戏 $\mathrm{Game}_{q,2}$ 中，所有返回的密钥都是第 2 类的，而在 $\mathrm{Game}_{\mathrm{Final}}$，攻击者的优势为 0，因为此时是对一个随机消息的加密。通过下列引理，证明这些游戏是两两不可区分的。

引理 2　假设存在多项式时间算法 $\mathcal{A}$ 满足

$$\mathrm{Game}_{\mathrm{Real}}Adv_{\mathcal{A}} - \mathrm{Game}_0 Adv_{\mathcal{A}} = \varepsilon$$

则我们可以构造算法 $\mathcal{B}$ 以 ε 的优势攻破(3, 1)—子空间假设。

引理 3　假设存在多项式时间算法 $\mathcal{A}$ 满足

$$\mathrm{Game}_{k-1,2}Adv_{\mathcal{A}} - \mathrm{Game}_{k,1}Adv_{\mathcal{A}} = \varepsilon$$

则我们可以构造算法 $\mathcal{B}$ 以 ε 的优势攻破(3, 1)—子空间假设。

引理 4　假设存在多项式时间算法 $\mathcal{A}$ 满足

$$\mathrm{Game}_{k,1}Adv_{\mathcal{A}} - \mathrm{Game}_{k,2}Adv_{\mathcal{A}} = \varepsilon$$

则我们可以构造算法 $\mathcal{B}$ 以 ε 的优势攻破(3, 1)—子空间假设。

引理 5　假设存在多项式时间算法 $\mathcal{A}$ 满足

$$\mathrm{Game}_{q,2}Adv_{\mathcal{A}} - \mathrm{Game}_{\mathrm{Final}}Adv_{\mathcal{A}} = \varepsilon$$

则可以构造算法 $\mathcal{B}$ 以 ε 的优势攻破(3, 1)—子空间假设。

囿于篇幅，略去以上引理的证明。对于上节构造的密钥策略 ABE 方案，有如下结论。

定理 1　如果判断线性假设成立，则密钥策略 ABE 方案是自适应安全的。

证明　由引理 2~引理 5 可知，如果(3, 1)—子空间假设成立，那么真实游戏 $\mathrm{Game}_{\mathrm{Real}}$ 与 $\mathrm{Game}_{\mathrm{Final}}$ 是不可区分的。又因为 $\mathrm{Game}_{\mathrm{Final}}$ 是对一随机消息的加密，因此在信息论意义上，b 的值对敌手是完全隐藏的，所以敌手在游戏 $\mathrm{Game}_{\mathrm{Real}}$ 中的优势是可忽略的。结合引理 1，子空间假设可以归约到判定线性假设，从而定理得证。

5　方案讨论

在本文给出的方案中，属性在密钥中的访问结构只能出现一次，这限制了方案的灵活性。如果需要属性是多用的，假设某属性 att 出现的最大次数是 k，可以将该属性进行如下编码：att:1，…，att:k，然后在加密和密钥生成时从低到高使用 att:1，…，att:k。这样方案的安全性不变，仍是自适应安全的，而属性的总数从 $|\mathcal{U}|$ 扩展到了 $k|\mathcal{U}|$。

目前支持单调访问结构的自适应安全的密钥策略 ABE 方案除了本文提出的方案，还有 Lewko 等人提出的方案（文献[13]）。表 1 对这 2 个方案在效率和安全性上做了简单对比。

表 1　　**方案对比**

方案	解密时对运算个数	群大小	假设
文献[13]	$2\|S\|$	$p_1p_2p_3$	合数阶群假设
本文方案	$6\|S\|$	p	判定线性假设

$|S|$：加密用的属性集包含的属性数目。

解密列出的是在同等条件下需要的双线性对数目，因为双线性对运算是解密中最为耗时的操作。尽管从数目上，本文方案需要进行 3 倍于 Lewko 等人方案的双线性对运算，但是由于 Lewko 等人的方案是在合数阶群上提出的，而合数阶群上的对运算效率远低于素数阶群上的对运算（例如在 80bit 的 AES 安全性上，前者的单次对运算时间是后者的 50 倍左右[14]），所以在同等安全级别上，本文的方案会更有效率。此外，本文的方案安全性基于标准的判定线性假设，这也是方案文献中[13]不能比拟的。

6　结束语

本文构造了一个密钥策略的 ABE 方案，该方案支持单调访问策略，并能够在标准模型上证明自适应安全性。本文的方案基于对偶正交基构造，利用双重系统加密技术将安全性归约于判定线性假设。与 Lewko 等人之前提出的同样是自适应安全的密钥策略 ABE 方案相比，在同样的安全性级别上，本文的方案更有效率。

参考文献：

[1] SHAMIR A. Identity-based cryptosystems and signatures schemes[J]. Lecture Notes in Computer Science, 1985,196: 47-53.

[2] BONEH D, FRANKLIN M. Identity-based encryption from the weil pairing[J]. Lecture Notes in Computer Science, 2001, 2139:213-229.

[3] COCKS C. An identity based encryption scheme based on quadratic residues[A]. The 8th IMA International Conference on Cryptography and Coding[C]. Cirencester, UK, 2001.360-363.

[4] SAHAI A, WATERS B. Fuzzy identity-based encryption[J]. Lecture Notes in Computer Science, 2005,3494:457-473.

[5] GOYAL V, PANDEY O, SAHAI A, *et al*. Attribute-based encryption for fine-grained access control of encrypted data[A]. The 13th ACM Conference on Computer and Communications Security ACM[C]. Alexandria, VA, USA, 2006. 89-98.

[6] OSTROVSKY R, SAHAI A, WATERS B. Attribute-based encryption with non-monotonic access structures[A]. The 14th ACM Conference on Computer and Communications Security ACM[C]. Alexandria, VA, USA, 2007. 195-203.

[7] BETHENCOURT J, SAHAI A, WATERS B. Ciphertext-policy attribute-based encryption[A]. IEEE Symposium on Security and Privacy[C]. Oakland, California, USA,2007. 321-334.

[8] WATERS B. Ciphertext-policy attribute-based encryption: An expressive, efficient, and provably secure realization[EB/OL]. http://eprint. iacr.org/,2008.

[9] ATTRAPADUNG N, IMAI H.Dual-policy attribute based encryption[A]. ACNS 2009[C]. France, 2009. 168-185.

[10] 杨晓元, 蔡伟艺, 陈海滨. 多主密钥功能加密: 基于 LMSSS 的 M-KP-ABE 方案[J]. 计算机研究与发展, 2011, 48(8): 1363-1369.
YANG X Y, CAI W Y, CHEN H B. Multiple-authority key functional encryption: a M-KP-ABE scheme based on LMSSS[J]. Journal of Computer Research and Development, 2011, 48(8): 1363-1369.

[11] KATZ J, SAHAI A, WATERS B. Predicate encryption supporting disjunctions, polynomial equations, and inner products[A]. Advances in Cryptology - EUROCRYPT 2008[C]. Istanbul, Turkey, 2008. 146-162.

[12] WATERS B. Dual system encryption: Realizing fully secure ibe and hibe under simple assumptions[A]. Advances in Cryptology - CRYPTO 2009[C]. Santa Barbara, California, USA, 2009. 619-636.

[13] LEWKO A, OKAMOTO T, SAHAI A, *et al*. Fully secure functional encryption: Attribute-based encryption and (hierarchical) inner product encryption[A]. Advances in Cryptology-EUROCRYPT 2010[C]. French, 2010. 62-91.

[14] FREEMAN D M. Converting pairing-based cryptosystems from composite-order groups to prime-order groups[A]. Advances in Cryptology - EUROCRYPT 2010[C]. French, 2010. 44-61.

[15] LEWKO A. Tools for simulating features of composite order bilinear groups in the prime order setting[EB/OL]. Cryptology ePrint Archive, Report 2011/490, http://eprint.iacr.org/. 2011.

[16] Lewko A, Waters B. New techniques for dual system encryption and fully secure hibe with short ciphertexts[A]. TCC 2010[C]. Zurich, Switzerland, 2010. 455-479.

[17] BEIMEL A. Secure Schemes for Secret Sharing and Key Distribution[D]. Haifa: Israel Institute of Technology, 1996.

作者简介：

罗颂（1979-），男，福建上杭人，博士，重庆理工大学讲师，主要研究方向为公钥密码学、信息安全。

陈钟（1963-），男，江苏徐州人，博士，北京大学教授、博士生导师，主要研究方向为网络与信息安全。