doi:10.3969/j.issn.1000-436x.2014.z2.005

# 快速解密的自适应安全 KP-ABE 方案

李琦[1,2]，马建峰[1,2,3]，熊金波[4]，刘西蒙[2,5]

(1. 西安电子科技大学 计算机学院，陕西 西安 710071；
2. 西安电子科技大学 陕西省网络与系统安全重点实验室，陕西 西安 710071；
3. 通信信息控制和安全技术重点实验室，浙江 嘉兴，314033；4. 福建师范大学 软件学院，福建 福州 350108；
5. 西安电子科技大学 通信工程学院，陕西 西安 710071)

**摘 要**：已有的自适应安全 ABE(attribute-based encryption)方案的解密开销随着解密时用到的属性数量呈线性增长。针对该问题，提出了一种快速解密的自适应安全 key-policy ABE(FKP-ABE)方案，在合数阶群上构造，支持任意可以表达为线性秘密分享体制(LSSS, linear secret sharing schemes)的单调访问策略，将解密开销降为常数级，并在标准模型下证明该方案是自适应安全的。

**关键词**：基于属性的加密；密钥策略；自适应安全；快速解密；合数阶；标准模型
**中图分类号**：TP309 **文献标识码**：A **文章编号**：1000-436X(2014)Z2-0026-07

# Adaptively secure key-policy ABE scheme with fast decryption

LI Qi[1,2], MA Jian-feng[1,2,3], XIONG Jin-bo[4], LIU Xi-meng[2,5]

(1. School of Computer Science and Technology, Xidian University, Xi'an 710071, China;
2. Shaanxi Key Laboratory of Network and System Security, Xidian University, Xi'an 710071, China;
3. Science and Technology on Communication Information Security Control Laboratory, Jiaxing 314033, China;
4. Faculty of Software, Fujian Normal University, Fuzhou 350108, China;
5. School of Telecommunication Engineering, Xidian University, Xi'an 710071, China)

**Abstract:** In the existing adaptively secure ABE (attribute-based encryption) schemes, the decryption cost goes linearly with the number of attributes that are used in decryption. An adaptively secure key-policy ABE (FKP-ABE) scheme with fast decryption is proposed, where constant size of computation overhead is implemented in decryption. This scheme is constructed on composite order bilinear groups and supports any monotonic access structure that can be expressed by LSSS (linear secret sharing schemes). The proposed scheme is proved to be adaptively secure in the standard model.

**Key words:** attribute-based encryption; key-policy; adaptive security; fast decryption; composite order; standard model

## 1 引言

基于属性的加密[1]（ABE, attribute-based encryption）最早由 Sahai 和 Waters 在 2005 年欧密会上提出。在该 ABE 系统中，用户用一个属性集合来描述，密文与一个属性集合相关联，当这 2 个属性集的匹配超过一个预设的值即可完成解密。随后，Goyal 等提出了一个基于树访问结构的密钥策略 ABE(KP-ABE, key-policy ABE)方案，并且给出了密文策略 ABE (CP-ABE, ciphertext-policy ABE)的定义。KP-ABE 指的是密钥与访问控制策略相关联，而密文与属性集合相关联。与此相反，在 CP-ABE 方案中，密钥与属性集合相关联，而密文与访问策略相关联。之后，大量的 ABE 的方案[2~10]被提出。

然而，这些方案的安全性都是在选择性安全模

**收稿日期**：2014-07-01
**基金项目**：国家自然基金委员会—广东联合基金重点资助项目(U1135002)；国家自然科学基金资助项目(61370078，61402109)；中央高校基本科研业务费专项基金资助项目(JB142001-12)
**Foundation Items:** The Key Program of NSFC-Guangdong Union Foundation (U1135002); The National Natural Science Foundation of China (61370078,61402109); The Fundamental Research Funds for the Central Universities (JB142001-12)

型[11]下证明的，即在通过攻击者与挑战者进行一系列交互的游戏来证明方案安全性的时候，攻击者需事先声明要挑战的访问结构（针对 CP-ABE）或要挑战的属性集合（针对 KP-ABE）。而在自适应安全模型下，并无该限制。由此可见，选择性安全性相对于自适应安全是一个较弱的安全概念。针对该问题，OKAMOTO 等[12]与 LEWKO 等[13]分别给出了自适应安全 ABE 方案的构造方法。然而，文献[12,13]方案的解密开销较大，其解密时需计算的双线性配对次数随解密时用到的属性个数呈线性增长。因此，如何构造快速解密的自适应安全 ABE 方案仍然是一个具有挑战性的问题。

在 KP-ABE 文献[13]方案的基础上，利用文献[10]方案通过增加密钥数量来减少解密时双线性配对运算次数的技术，提出一个快速解密的自适应安全的 KP-ABE 方案，简称 FKP-ABE。该方案在合数阶群上构造，支持任意可以表达为 LSSS 的单调访问策略。解密时只需要进行 2 次双线性配对运算，同时在标准模型下证明该方案是自适应安全的。

## 2　背景知识

### 2.1　双线性配对

使用合数阶群上的双线性配对[14]，其定义如下。

选取 $G$ 和 $G_1$ 为 2 个阶为 $N=p_1p_2p_3$ 的群，其中 $p_1,p_2,p_3$ 是 3 个不同的素数，定义一个可有效计算的双线性映射 $e:G\times G\to G_1$。该映射满足下面条件。

1) 双线性：$e(u^a,v^b)=e(u,v)^{ab}$，对于所有的 $a,b\in \mathrm{Z}_N$ 和所有的 $u,v\in G$。

2) 非退化性：$\exists g\in G$，使 $e(g,g)$ 在 $G_1$ 中的阶为 $N$。

令 $G_{p_i}$ 表示 $G$ 的一个阶为 $p_i$ 的子群。注意：对于任意的 $h_i\in G_{p_i}$ 与 $h_j\in G_{p_j}$，如果 $i\neq j$，有 $e(h_i,h_j)=1$。对于 $G$ 中的元素 $T$，$T$ 可以写作是一个 $G_{p_1}$ 中的元素，一个 $G_{p_2}$ 中的元素和一个 $G_{p_3}$ 中元素的乘积形式。它们分别代表 $T$ 的 $G_{p_1}$，$G_{p_2}$ 和 $G_{p_3}$ 部分。

### 2.2　困难性假设

**假设 1**[13]　给定一个群生成器 $\mathcal{G}$，定义如下分布

$$G=(N=p_1p_2p_3,G,G_1,e)\xleftarrow{R}\mathcal{G}$$

$$g\xleftarrow{R}G_{p_1},X_3\xleftarrow{R}G_{p_3}$$

$$D=(G,g,X_3)$$

$$T_1\xleftarrow{R}G_{p_1p_2},T_2\xleftarrow{R}G_{p_1}$$

算法 $\mathcal{A}$ 攻破假设 1 的优势定义为：$Adv1_{\mathcal{G},\mathcal{A}}=|\Pr[\mathcal{A}(D,T_1)=1]-\Pr[\mathcal{A}(D,T_2)=1]|$。

**定义 1**　$\mathcal{G}$ 满足假设 1，如果对于任意的多项式时间算法 $\mathcal{A}$，优势 $Adv1_{\mathcal{G},\mathcal{A}}$ 是可忽略的。

**假设 2**[13]　给定一个群生成器 $\mathcal{G}$，定义如下分布

$$G=(N=p_1p_2p_3,G,G_1,e)\xleftarrow{R}\mathcal{G}$$

$$g,X_1\xleftarrow{R}G_{p_1},X_2,Y_2\xleftarrow{R}G_{p_2},X_3,Y_3\xleftarrow{R}G_{p_3}$$

$$D=(G,g,X_1X_2,X_3,Y_2Y_3)$$

$$T_1\xleftarrow{R}G,T_2\xleftarrow{R}G_{p_1p_3}$$

算法 $\mathcal{A}$ 攻破假设 2 的优势定义为：$Adv2_{\mathcal{G},\mathcal{A}}=|\Pr[\mathcal{A}(D,T_1)=1]-\Pr[\mathcal{A}(D,T_2)=1]|$。

**定义 2**　$\mathcal{G}$ 满足假设 2，如果对于任意的多项式时间算法 $\mathcal{A}$，优势 $Adv2_{\mathcal{G},\mathcal{A}}$ 是可忽略的。

**假设 3**[13]　给定一个群生成器 $\mathcal{G}$，定义如下分布

$$G=(N=p_1p_2p_3,G,G_1,e)\xleftarrow{R}\mathcal{G},\alpha,s\xleftarrow{R}\mathrm{Z}_N$$

$$g\xleftarrow{R}G_{p_1},X_2,Y_2,Z_2\xleftarrow{R}G_{p_2},X_3\xleftarrow{R}G_{p_3}$$

$$D=(G,g,g^{\alpha}X_2,X_3,g^{s}Y_2,Z_2)$$

$$T_1=e(g,g)^{\alpha s},T_2\xleftarrow{R}G_1$$

算法 $\mathcal{A}$ 攻破假设 3 的优势定义为：$Adv3_{\mathcal{G},\mathcal{A}}=|\Pr[\mathcal{A}(D,T_1)=1]-\Pr[\mathcal{A}(D,T_2)=1]|$。

**定义 3**　$\mathcal{G}$ 满足假设 3，如果对于任意的多项式时间算法 $\mathcal{A}$，优势 $Adv3_{\mathcal{G},\mathcal{A}}$ 是可忽略的。

### 2.3　访问结构

**定义 4**[15]　令 $P=\{P_1,P_2,\cdots,P_T\}$ 表示参与方的集合，若一个访问结构 $A\subseteq 2^{\{P_1,P_2,\cdots,P_T\}}$ 被称作是单调的，则有：$\forall A_1,A_2$，若 $A_1\in A$，且 $A_1\subseteq A_2$，故有 $A_2\in A$。访问结构 $A$ 中的集合称作授权集合，不在 $A$ 中的集合则称为非授权集合。

在 ABE 密码系统中，参与方的角色被属性取代。因此，访问结构将包含授权的属性。

### 2.4　线性秘密共享体制(LSSS)

**定义 5**[15]　令 $P=\{P_1,P_2,\cdots,P_T\}$ 表示参与方的集合，$P$ 上的一个秘密共享方案 $\Pi$ 被称作线性的，如果：

1) 每个参与方关于秘密 $s$ 的份额是 $\mathrm{Z}_N$ 上的一个向量；

2) 存在 $\Pi$ 的一个 $l$ 行 $n$ 列的共享生成矩阵 $\boldsymbol{A}$。

令 $\rho$ 为一个从 $\{1,2,\cdots,l\}$ 到 $P$ 的映射，即 $\rho$ 将矩阵 $\boldsymbol{A}$ 的每一行映射到一个参与方。选择一个随机向量 $\vec{\boldsymbol{v}}=(s,v_2,\cdots,v_n)^{\mathrm{T}}\in \mathrm{Z}_N^n$。则 $\boldsymbol{A}\vec{\boldsymbol{v}}$ 是 $s$ 关于 $\Pi$ 的 $l$ 个共享份额。而且第 $i$ 个份额 $\lambda_i$ 属于参与方 $\rho(i)$。

文献[15]表明，单调的访问结构与线性秘密共享方案是等价。且任何一个线性秘密共享方案都具有线性重构的性质。令 $(\boldsymbol{A},\rho)$ 表示一个访问结构 $A$，$S$ 为一个授权集合，令集合 $I=\{i:\rho(i)\in S\}$，存在常数 $\{\omega_i\in \mathrm{Z}_p\}_{i\in I}$ 使 $\sum_{i\in I}\omega_i\lambda_i=s$。对于非授权集合，这样的常数是不存在的。其中，只考虑每个属性在访问结构中出现一次的情况。

### 2.5 系统模型

一个 KP-ABE 方案由如下 4 种多项式时间算法组成。

**Setup**$(\lambda,U)\to(PK,MSK)$：输入安全参数 $\lambda$ 与系统的属性集合 $U=\{1,2,\cdots,u\}$，输出系统的公钥参数 $PK$ 与主密钥 $MSK$。

**Encrypt**$(M,S,PK)\to(CT)$：输入明文 $M$、一个属性集合 $S$ 与 $PK$，输出密文 $CT$。假设 $S$ 也包含在 $CT$ 中。

**KeyGen**$(\mathrm{A},PK,MSK)\to(SK)$：输入一个访问结构 A、$PK$ 与 $MSK$，输出用户私钥 $SK$。假设 $A$ 也包含在 $SK$ 中。

**Decrypt**$(CT,PK,SK)\to(M)$：输入 $CT$、$PK$ 与 $SK$，若密文中的属性集合 $S$ 满足访问结构 $A$，输出明文 $M$。否则，输出 $\perp$。

### 2.6 安全模型

通过攻击者 $\mathcal{A}$ 与挑战者 $\mathcal{B}$ 之间的攻击游戏来定义 KP-ABE 方案的安全模型。

**Setup** 挑战者 $\mathcal{B}$ 运行 KP-ABE 方案的 Setup 算法，并将系统公钥参数 $PK$ 发送至攻击者 $\mathcal{A}$。

**Phase 1** $\mathcal{A}$ 询问任意的访问结构 $A_1,\cdots,A_{q_1}$，挑战者 $\mathcal{B}$ 返回相对应的密钥。

**Challenge** $\mathcal{A}$ 提交 2 条长度相等的明文 $M_0$、$M_1$ 及一个挑战属性集合 $S^*$。$\mathcal{B}$ 从中随机选择一条明文 $M_b$ 用 $S^*$ 加密，并将挑战密文 $CT^*$ 返回给 $\mathcal{A}$。注意：$S^*$ 不能是满足 Phase 1 中访问结构的属性集合。

**Phase 2** 与 Phase 1 类似，$\mathcal{A}$ 可以询问密钥，但是 $\mathcal{A}$ 不能查询令 $S^*$ 满足的访问结构。

**Guess** $\mathcal{A}$ 输出对 $b$ 的猜测 $b'$。若 $b'=b$，则 $\mathcal{A}$ 获胜。$\mathcal{A}$ 的优势定义为 $\left|\Pr[b=b']-1/2\right|$。

**定义 6** 一个 KP-ABE 方案是安全的，当且仅当在上述的攻击游戏中，任何多项式时间攻击者 $\mathcal{A}$ 的优势是可以忽略的。

## 3 FKP-ABE 方案

**Setup**$(\lambda,U)\to(PK,MSK)$：输入一个安全参数 $\lambda$，输出 2 个阶为 $N=p_1p_2p_3$ 的群 $G$，$G_1$，其中 $p_1$、$p_2$、$p_3$ 为 3 个两两不同的素数。令 $e$ 是一个 $G\times G\to G_1$ 的双线性映射。从 $\mathrm{Z}_N$ 中选择一个随机数 $\alpha$。从 $G_{p_1}$ 中随机选择一个元素 $g$。对于每个属性 $i\in U$，从 $\mathrm{Z}_N$ 中选择一个随机数 $t_i$，并计算 $T_i=g^{t_i}$。最终发布公钥参数 $PK$ 为 $PK=(N,g,e(g,g)^{\alpha},T_1,\cdots,T_{|U|})$。系统主密钥 $MSK$ 为 $\alpha$ 及子群 $G_{p_3}$ 的一个生成元 $X_3$。

***Encrypt***$(M,S,PK)\to(CT)$：从 $\mathrm{Z}_N$ 中选择一个随机数 $s$，计算 $C=Me(g,g)^{\alpha s}$，$C_0=g^s$，对于每个属性 $i\in S$，计算 $C_i=T_i^s$。最终的密文 $CT$ 为 $CT=(C,C_0,C_i\forall i\in S)$。

***KeyGen***$(\mathrm{A},PK,MSK)\to(SK)$：令访问结构 $A$ 为 $(\boldsymbol{A},\rho)$，其中 $\boldsymbol{A}$ 为 $l$ 行 $n$ 列的矩阵。$\rho$ 将 $\boldsymbol{A}$ 的每一行 $x$ 映射到一个属性 $\rho(x)$。选择一个向量 $\vec{\boldsymbol{v}}=(\alpha,v_2,\cdots,v_n)^{\mathrm{T}}$，其中 $v_2,\cdots,v_n$ 是从 $\mathrm{Z}_N$ 中选择的随机数。对于 $\boldsymbol{A}$ 的每一行 $x$，从 $\mathrm{Z}_N$ 中选择一个随机数 $r_x$，从 $G_{p_3}$ 中随机选择 2 个元素 $W_x$，$V_x$，并计算

$$K_1^1=g^{\boldsymbol{A}_1\vec{\boldsymbol{v}}}T_{\rho(1)}^{r_1}W_1$$

$$K_1^2=g^{r_1}V_1,\quad \forall d\in\Theta/\rho(1),\quad O_{1,d}=T_d^{r_1}W_{1,d};\quad\cdots$$

$$K_l^1=g^{\boldsymbol{A}_l\vec{\boldsymbol{v}}}T_{\rho(l)}^{r_l}W_l$$

$$K_l^2=g^{r_l}V_l,\quad \forall d\in\Theta/\rho(l),\quad O_{l,d}=T_d^{r_l}W_{l,d}$$

其中，$\Theta=\{d:\exists x\in[1,l],\rho(x)=d\}$，而 $W_{1,2},\cdots,W_{1,l},\cdots,W_{l,1},\cdots,W_{l,l-1}$ 是从 $G_{p_3}$ 中随机选择的元素。

最终的私钥 $SK$ 为

$$SK=((K_1^1,K_1^2,\{O_{1,d}\}),\cdots,(K_l^1,K_l^2,\{O_{l,d}\}))$$

**Decrypt**$(CT,PK,SK)\to(M)$：如果 $CT$ 中的属性集 $S$ 不满足 $SK$ 中的访问结构 $A$，输出 $\perp$。否则，令集合 $I=\{x\,|\,\rho(x)\in S\}$，并计算常数 $\omega_x\in\mathrm{Z}_N$ 使 $\sum_{x\in I}\omega_xA_x=(1,0,\cdots,0)$。令 $\Delta=\{i:\exists x\in I,\rho(x)=i\}$。也就是说，$I$ 表示可能用来解密的矩阵 $\boldsymbol{A}$ 的行的集合，而 $\Delta$ 表示的是这些行对应的属性的集合。注意：$\Delta\subseteq S$，$\Delta\subseteq\Theta$。定义一个将一个属性集合映射为

$G$ 中元素的函数 $f$ 如下：$f(\Delta)=\prod_{j\in\Delta}T_j$。在解密密文之前，对密钥进行如下处理：对于矩阵 $\boldsymbol{A}$ 的每一行 $x$，计算：$\tilde{K}_x^1=K_x^1\prod_{j\in\Delta/\rho(x)}O_{x,j}=g^{A_x v}f(\Delta)^{r_x}\tilde{W}_x$，其中，$\tilde{W}_x=W_x\prod_{j\in\Delta/\rho(x)}W_{x,j}$。

对密文进行如下处理

$$Q=\prod_{i\in\Delta}C_i=\prod_{i\in\Delta}T_i^s=f(\Delta)^s$$

然后计算

$$\begin{aligned}B&=\frac{e\left(C_0,\prod_{x\in I}\left(\tilde{K}_x^1\right)^{\omega_x}\right)}{e\left(Q,\prod_{x\in I}\left(K_x^2\right)^{\omega_x}\right)}\\&=\frac{e\left(g^s,\prod_{x\in I}g^{A_x v\omega_x}f(\Delta)^{r_x\omega_x}\right)}{e\left(f(\Delta)^s,\prod_{x\in I}g^{r_x\omega_x}\right)}\\&=\frac{e(g,g)^{s\sum_{x\in I}\omega_x A_x v}\,e\left(f(\Delta),g\right)^{s\sum_{x\in I}\omega_x r_x}}{e\left(f(\Delta),g\right)^{s\sum_{x\in I}\omega_x r_x}}\\&=e(g,g)^{s\alpha}\end{aligned}$$

最后恢复消息 $M=C/e(g,g)^{\alpha s}$。

## 4　安全性证明

利用文献[13]的证明技术，证明本文方案在不可区分选择明文攻击下是自适应安全的。首先，给出只在攻击游戏中用到的半功能密文与半功能密钥的定义；然后，基于半功能密文和半功能密钥定义一系列攻击游戏；最后，基于困难假设 1、2、3，证明这些攻击游戏与真实的攻击游戏是不可区分的。进而证明攻击者在真实游戏中的优势也是可以忽略的。

半功能密文与半功能密钥定义如下。

半功能密文：令 $g_2$ 为 $\mathrm{G}_{p_2}$ 的一个生成元，随机选择 $c\in Z_N$，对于每一个属性 $i$，随机选择 $z_i\in Z_N$。设置半功能密文为：$C_0=g^s g_2^c$，$C_i=T_i^s g_2^{cz_i}\forall i\in S$。

半功能密钥有如下 2 种表现形式。

1) 随机选择一个向量 $\vec{\boldsymbol{v}}_1$，令 $\delta_x=A_x\vec{\boldsymbol{v}}_1$，另外，对于访问控制矩阵每一行 $x$，选择一个随机数 $\gamma_x\in Z_N$，计算

$K_1^1=g^{A_1\vec{\boldsymbol{v}}}T_{\rho(1)}^{r_1}W_1g_2^{\delta_1+\gamma_1 z_{\rho(1)}}$，$K_1^2=g^{r_1}V_1g_2^{\gamma_1}$，$\forall d\in\Theta/\rho(1)$，$O_{1,d}=T_d^{r_1}W_{1,d}g_2^{\gamma_1 z_{\rho(1)}}$；

…

$K_l^1=g^{A_l\vec{\boldsymbol{v}}}T_{\rho(l)}^{r_l}W_lg_2^{\delta_l+\gamma_l z_{\rho(l)}}$，$K_l^2=g^{r_l}V_lg_2^{\gamma_l}$，$\forall d\in\Theta/\rho(l)$，$O_{l,d}=T_d^{r_l}W_{l,d}g_2^{\gamma_l z_{\rho(l)}}$。

2) 形式 2)的半功能密钥没有 $g_2^{\gamma_x z_{\rho(x)}}$ 与 $g_2^{\gamma_x}$ 项，即

$K_1^1=g^{A_1\vec{\boldsymbol{v}}}T_{\rho(1)}^{r_1}W_1g_2^{\delta_1}$，$K_1^2=g^{r_1}V_1$，$\forall d\in\Theta/\rho(1)$，$O_{1,d}=T_d^{r_1}W_{1,d}$；

…

$K_l^1=g^{A_l\vec{\boldsymbol{v}}}T_{\rho(l)}^{r_l}W_lg_2^{\delta_l}$，$K_l^2=g^{r_l}V_l$，$\forall d\in\Theta/\rho(l)$，$O_{l,d}=T_d^{r_l}W_{l,d}$。

**注意**　半功能密钥可以解密正常的密文，正常的密钥可以解密半功能密文。但是，半功能密钥不能解密半功能密文。

令 $q$ 表示攻击者查询密钥的次数。令 $1\leqslant k\leqslant q$。攻击游戏定义如下。

$Game_{\mathrm{real}}$：该游戏为第 2 节中所定义的真实游戏，即密钥与挑战密文都是正常的。（为简便起见，在以下证明中挑战密文简称密文）

$Game_0$：在 $Game_0$ 中，密文是半功能密文，而密钥是正常密钥。

$Game_{k,1}$：在 $Game_{k,1}$ 中，密文是半功能的，前 $k-1$ 个密钥是形式 2)的半功能密钥，第 $k$ 个密钥是形式 1)的半功能密钥，其余的是正常密钥。

$Game_{k,2}$：在 $Game_{k,2}$ 中，密文是半功能的，前 $k$ 个密钥是形式 2)的半功能密钥，其余的是正常密钥。

$Game_{q,2}$：在 $Game_{q,2}$ 中，密文为半功能密文，所有的密钥都是形式 2)的半功能密钥。

$Game_{\mathrm{Final}}$：在 $Game_{\mathrm{Final}}$ 中，所有的密钥都是形式 2)半功能密钥。在挑战阶段，密文要么是加密 $M_b$ 后得到的半功能密文，要么是对一个随机消息加密后的密文，攻击者的优势为 0。

**定理 1**　若困难假设 1、2、3 成立，则 FKP-ABE 方案是安全的。

**证明**　通过下面 4 个引理来证明。

**引理 1**　若存在一个多项式时间攻击者 $\mathcal{A}$，其能够以不可忽略的优势 $\varepsilon$ 区分 $Game_{\mathrm{real}}$ 与 $Game_0$，那么就可以利用 $\mathcal{A}$ 构建一个多项式时间算法 $\mathcal{B}$ 以优势 $\varepsilon$ 攻破假设 1。

**证明** 给定$\{g,X_3,T\}$，挑战者$\mathcal{B}$将与攻击者$\mathcal{A}$模拟$Game_{\text{real}}$或者$Game_0$。$\mathcal{B}$如同实际方案一样设置公钥参数并且发送给$\mathcal{A}$。并且，对于$\mathcal{A}$的密钥查询，返回正常的密钥。

在挑战阶段，$\mathcal{B}$构造密文如下。

$C=M_b e(g,g)^{\alpha s}=M_b e(g,T)^{\alpha}$，$C_0=T^s$，对于每个属性$i\in S$，计算$C_i=T^{t_i}$。

**注意** 这里意味着设置$z_i=t_i$。

如果$T=g^s$，那么密文是一个正常密文。

如果$T=g^s X_2$，其中$X_2\in G_{p_2}$，则密文是一个半功能密文。

因此，若$\mathcal{A}$能够以不可忽略的优势$\varepsilon$区分$Game_{\text{real}}$与$Game_0$，那么$\mathcal{B}$就可以利用$\mathcal{A}$的输出来以优势$\varepsilon$区分$T_1$与$T_2$。

**引理2** 若存在一个多项式时间攻击者$\mathcal{A}$，其能以不可忽略的优势$\varepsilon$区分$Game_{k,1}$与$Game_{k-1,2}$，那么就可以利用$\mathcal{A}$构建一个多项式时间算法$\mathcal{B}$以优势$\varepsilon$攻破假设2。

**证明** 给定$\{g,X_3,g^s X_2,Y_2Y_3,T\}$，挑战者$\mathcal{B}$将与攻击者$\mathcal{A}$模拟$Game_{k-1,2}$或者$Game_{k,1}$。$\mathcal{B}$设置公钥参数并且发送给$\mathcal{A}$。令$z_i=t_i$。

在挑战阶段，$\mathcal{B}$构造密文如下。

$C=M_b e\left(g,g^s X_2\right)^{\alpha}$，$C_0=g^s X_2$，对于每个属性$i\in S$，计算$C_i=\left(g^s X_2\right)^{t_i}$。

对于$\mathcal{A}$前$k-1$次的密钥查询，$\mathcal{B}$将回应以形式2)半功能密钥。具体步骤如下。

$\mathcal{B}$如同实际方案里一样设置参数，另外，$\mathcal{B}$选择一个随机向量$\vec{\boldsymbol{v}}_1$，计算密钥：

$K_1^1=g^{A_1\vec{\boldsymbol{v}}}T_{\rho(1)}^{r_1}W_1\left(Y_2Y_3\right)^{A_1\vec{\boldsymbol{v}}_1}$，$K_1^2=g^{r_1}V_1$，$\forall d\in\Theta/\rho(1)$，$O_{1,d}=T_d^{r_1}W_{1,d}$；

…

$K_l^1=g^{A_l\vec{\boldsymbol{v}}}T_{\rho(l)}^{r_l}W_l\left(Y_2Y_3\right)^{A_l\vec{\boldsymbol{v}}_1}$，$K_l^2=g^{r_l}V_l$，$\forall d\in\Theta/\rho(l)$，$O_{l,d}=T_d^{r_l}W_{l,d}$。

对于$\mathcal{A}$第$k$次的密钥查询，$\mathcal{B}$将回应以形式1)半功能密钥。具体步骤如下。

$\mathcal{B}$如同实际方案里一样设置参数，另外，$\mathcal{B}$选择一个向量$\vec{\boldsymbol{v}}_1$，其第一个元素为0，其余的元素为随机选择的。另外，对于访问控制矩阵每一行$x$，选择一个随机数$\gamma_x\in Z_N$。计算密钥：

$K_1^1=g^{A_1\vec{\boldsymbol{v}}}T^{A_1\vec{\boldsymbol{v}}_1}T^{\gamma_1 z_{\rho(1)}}W_1$，$K_1^2=T^{\gamma_1}V_1$，$\forall d\in\Theta/\rho(1)$，$O_{1,d}=T^{\gamma_1 z_d}W_{1,d}$；

…

$K_l^1=g^{A_l\vec{\boldsymbol{v}}}T^{A_l\vec{\boldsymbol{v}}_1}T^{\gamma_l z_{\rho(l)}}W_l$，$K_l^2=T^{\gamma_l}V_l$，$\forall d\in\Theta/\rho(l)$，$O_{l,d}=T^{\gamma_d z_d}W_{l,d}$。

对于大于$k$次的密钥查询，$\mathcal{B}$将回应以正常密钥。

如果$\mathcal{A}$能以不可忽略的优势区分$Game_{k-1,2}$与$Game_{k,1}$。则$\mathcal{B}$就可以利用$\mathcal{A}$的输出区分$T_1$与$T_2$。

**引理3** 若存在一个多项式时间攻击者$\mathcal{A}$，能够以不可忽略的优势$\varepsilon$区分$Game_{k,1}$与$Game_{k,2}$，那么就可以利用$\mathcal{A}$构建一个多项式时间算法$\mathcal{B}$以优势$\varepsilon$攻破假设2。

**证明** 给定$\{g,X_3,g^s X_2,Y_2Y_3,T\}$，挑战者$\mathcal{B}$将与攻击者$\mathcal{A}$模拟$Game_{k,1}$或者$Game_{k,2}$。$\mathcal{B}$设置公钥参数并且发送给$\mathcal{A}$。令$z_i=t_i$。

在挑战阶段，$\mathcal{B}$构造挑战密文与在引理2的证明中一样。

针对$\mathcal{A}$的前$k-1$次与大于$k$次的密钥查询，$\mathcal{B}$表现与在引理2的证明中一样。

针对$\mathcal{A}$的第$k$次的密钥查询，$\mathcal{B}$如同实际方案里一样设置参数，另外，$\mathcal{B}$选择一个随机向量$\vec{\boldsymbol{v}}_1$，对于访问控制矩阵每一行$x$，选择一个随机数$\gamma_x\in Z_N$。计算密钥：

$K_1^1=g^{A_1\vec{\boldsymbol{v}}}\left(Y_2Y_3\right)^{A_1\vec{\boldsymbol{v}}_1}T^{\gamma_1 z_{\rho(1)}}W_1$，$K_1^2=T^{\gamma_1}V_1$，$\forall d\in\Theta/\rho(1)$，$O_{1,d}=T^{\gamma_1 z_d}W_{1,d}$；

…

$K_l^1=g^{A_l\vec{\boldsymbol{v}}}\left(Y_2Y_3\right)^{A_l\vec{\boldsymbol{v}}_1}T^{\gamma_l z_{\rho(l)}}W_l$，$K_l^2=T^{\gamma_l}V_l$，$\forall d\in\Theta/\rho(l)$，$O_{l,d}=T^{\gamma_d z_d}W_{l,d}$。

如果$T\in G$，那么这就是一个合理分布的形式1)半功能密钥。

如果$T\in G_{p_1p_3}$，那么这就是一个合理分布的形式2)半功能密钥。

如果$\mathcal{A}$能够以不可忽略的优势区分$Game_{k-1,2}$与$Game_{k,1}$，则$\mathcal{B}$就可以以不可忽略的优势区分$T_1$与$T_2$。

**引理4** 若存在一个多项式时间攻击者$\mathcal{A}$，其能够以不可忽略的优势$\varepsilon$区分$Game_{q,2}$与$Game_{\text{Final}}$，那么就可以利用$\mathcal{A}$构建一个多项式时间算法$\mathcal{B}$以优势$\varepsilon$攻破假设3。

**证明** 给定$\{g,g^{\alpha}X_2,X_3,g^s Y_2,Z_2,T\}$，挑战者$\mathcal{B}$

将与攻击者 $\mathcal{A}$ 模拟 $Game_{q,2}$ 或者 $Game_{Final}$。$\mathcal{B}$ 设置公钥参数并且发送给 $\mathcal{A}$，其中 $e(g,g)^{\alpha}=e(g,g^{\alpha}X_2)$。令 $z_i=t_i$。

在挑战阶段，$\mathcal{B}$ 构造密文如下：

$C=M_bT$，$C_0=g^sX_2$，计算 $C_i=(g^sX_2)^{t_i}$，$\forall i\in S$。

如果 $T=e(g,g)^{\alpha s}$，这就是一个对 $M_b$ 正常加密的半功能密文。否则，这将是一个对随机消息加密的半功能密文，攻击者将得不到 $b$ 的任何信息。

$\mathcal{B}$ 设置形式 2)半功能密钥如下。

选择随机向量 $\vec{\boldsymbol{v}}=(\alpha,v_2,\cdots,v_n)^{\mathrm{T}}$ 和 $\vec{\boldsymbol{v}}_1$。注意：$\alpha$ 对于 $\mathcal{B}$ 也是未知的，只是这样记，以便理解。

$K_1^1=g^{\sum_{j=2}^{n}A_{1,j}v_j}(g^{\alpha}X_2)^{A_{1,1}}g^{r_1t_{\rho(1)}}Z_2^{A_1\vec{\boldsymbol{v}}_1}W_1$，$K_1^2=g^{r_1}V_1$，$\forall d\in\Theta/\rho(1)$，$O_{1,d}=g^{r_1t_d}W_{1,d}$；

…

$K_l^1=g^{\sum_{j=2}^{n}A_{l,j}v_j}(g^{\alpha}X_2)^{A_{l,1}}g^{r_lt_{\rho(l)}}Z_2^{A_l\vec{\boldsymbol{v}}_1}W_l$，$K_l^2=g^{r_l}V_l$，$\forall d\in\Theta/\rho(l)$，$O_{l,d}=g^{r_dt_d}W_{l,d}$。

如果 $\mathcal{A}$ 能够以不可忽略的优势区分 $Game_{q,2}$ 与 $Game_{Final}$。那么 $\mathcal{B}$ 就可以以不可忽略的优势区分 $T_1$ 与 $T_2$。

如果假设 1、2、3 成立，通过前面的引理，可以得出真实的攻击游戏与 $Game_{Final}$ 是不可区分的。因此，攻击者不能以不可忽略的优势攻破的 FKP-ABE 方案。

至此，定理 1 证毕。

## 5　性能分析

表 1 将文献[10]方案，文献[13]方案与 FKP-ABE 方案在方案类型、安全性以及解密时用到的双线性配对次数进行了比较。令 $\Delta$ 表示解密时用到的属性的集合。令|$G$|表示群 $G$ 中元素的比特长度。由表 1 可知：本方案在达到自适应安全的同时将解密时双线性配对运算次数将为 2 次。其次数与解密时用到的属性数量无关。与文献[5]方案相比，并没有增加额外的公钥参数以及密文元素。

## 6　结束语

针对目前自适应安全 ABE 方案的解密效率较低的问题，提出了一种快速解密的自适应安全 KP-ABE 方案，在保持自适应安全性的同时，解密时只需要运行常数次（2 次）的双线性配对计算，与解密时用到的属性数量无关。该方案在合数阶群上构造，支持可以表达为 LSSS 的访问策略，在标准模型下被证明是自适应安全的。本方案中密钥的长度较长，复杂度为 $O(|\Theta|^2)$。

**表 1**　　**性能比较**

| 方案 | CP/KP | 安全性 | 公钥长度 | 密文长度 | 配对次数 |
|---|---|---|---|---|---|
| 文献[5]方案 | KP | 自适应 | (\|$U$\|+1)\|$G$\| | (\|$S$\|+1)\|$G$\| | 2\|$\Delta$\| |
| 文献[13]方案 | KP | 选择性 | (\|$U$\|+1)\|$G$\| | (\|$S$\|+1)\|$G$\| | 2 |
| FKP-ABE 方案 | KP | 自适应 | (\|$U$\|+1)\|$G$\| | (\|$S$\|+1)\|$G$\| | 2 |

**参考文献：**


[1] SAHAI A, WATERS B. Fuzzy identity-based encryption[A]. Cryptology-EUROCRYPT 2005[C]. Springer Berlin Heidelberg, 2005.457-473.

[2] 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 Security[C]. 2006.89-98.

[3] OSTROVSKY R, SAHAI A, WATERS B. Attribute-based encryption with non-monotonic access structures[A]. Proceedings of the 14th ACM Conference on Computer and Communications Security[C]. 2007.195-203.

[4] BETHENCOURT J, SAHAI A, WATERS B. Ciphertext-policy attribute-based encryption[A]. IEEE Symposium on Security and Privacy, 2007[C]. 2007.321-334.

[5] CHEUNG L, NEWPORT C. Provably secure ciphertext policy ABE[A]. Proceedings of the 14th ACM Conference on Computer and Communications Security[C]. 2007.456-465.

[6] GOYAL V, JAIN A, PANDEY O, *et al*. Bounded Ciphertext Policy Attribute Based Encryption[M]. Automata, Languages and Programming, Springer Berlin Heidelberg, 2008.579-591.

[7] WATERS B. Ciphertext-policy Attribute-based Encryption: an Expressive, Efficient, and Provably Secure Realization[M]. Public Key Cryptography-PKC 2011, Springer Berlin Heidelberg, 2011.53-70.

[8] ATTRAPADUNG N, LIBERT B, De PANAFIEU E. Expressive Key-Policy Attribute-based Encryption with Constant-size Ciphertexts[M]. Public Key Cryptography–PKC 2011, Springer Berlin Heidelberg, 2011.90-108.

[9] ATTRAPADUNG N, HERRANZ J, LAGUILLAUMIE F, *et al*. Attribute-based encryption schemes with constant-size ciphertexts[J]. Theoretical Computer Science, 2012, 422: 15-38.

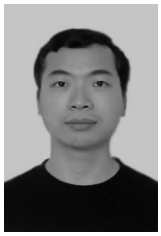
[10] HOHENBERGER S, WATERS B. Attribute-Based Encryption with Fast Decryption[M]. Public-Key Cryptography–PKC 2013, Springer Berlin Heidelberg, 2013.162-179.

[11] CANETTI R, HALEVI S, KATZ J. A forward-secure public-key encryption scheme[A]. Cryptology—Eurocrypt 2003[C]. Springer Berlin Heidelberg, 2003.255-271.
[12] OKAMOTO T, TAKASHIMA K. Fully secure functional encryption with general relations from the decisional linear assumption[A]. Cryptology–CRYPTO 2010[C]. Springer Berlin Heidelberg, 2010. 191-208.
[13] LEWKO A, OKAMOTO T, SAHAI A, *et al*. Fully secure functional encryption: attribute-based encryption and (hierarchical) inner product encryption[A]. Cryptology–EUROCRYPT 2010[C]. Springer Berlin Heidelberg, 2010.62-91.
[14] BONEH D, GOH E J, NISSIM K. Evaluating 2-DNF Formulas on Ciphertexts[M]. Theory of Cryptography. Springer Berlin Heidelberg, 2005.325-341.
[15] BEIMEL A. Secure Schemes for Secret Sharing and Key Distribution[D]. PhD Thesis, Israel Institute of Technology, Technion, Haifa, Israel, 1996.

**作者简介：**

**李琦**（1989-），男，江苏淮安人，西安电子科技大学博士生，主要研究方向为信息安全与基于属性的密码学。

**马建峰**（1963-），男，陕西西安人，博士，西安电子科技大学教授、博士生导师，主要研究方向为密码学、计算机网络与信息安全。



**熊金波**（1981-），男，湖南益阳人，福建师范大学讲师，主要研究方向为访问控制技术与结构化文档安全。

**刘西蒙**（1988-），男，陕西西安人，西安电子科技大学博士生，主要研究方向为公钥密码学与信息安全、安全网络编码及其应用。

（上接第 25 页）

[7] 席道瑛, 张涛. BP 网络的改进及模拟退火神经网络在地学中应用[J]. 物探化探计算技术, 1996, 18(3):219-224.
XI D Y, ZHANG T. Application of improved BP neural network and simulated annealing neural network in Earth Science[J]. Computing Techniques for Geophysical and Geochemical Exploration. 1996, 18(3): 219-224.
[8] 苏晨, 李成义. 基于遗传算法和 BP 神经网络的服装销售预测[J]. 经营与管理, 2012, 2: 145-158.
SU C, LI C Y. Garment sales prediction of based on genetic algorithm and BP neural network[J]. Operation and Management, 2012, 2: 145-158.
[9] TAN P N, MICHAEL S, VIPIN K. Introduction to Data Mining[M]. Beijing: Machine Industry Press, 2010:246-255.
[10] HAN J, KAMBER M, PEI J. Data Mining: Concepts and Techniques[M]. Morgan Kaufmann, 2006.
[11] 傅荟璇, 赵红等. MATLAB 神经网络应用设计[M]. 机械工业出版社, 2010.
FU H X, ZHAO H, *et al* .Neural network application design based on MATLAB[M].Beijing: Machine Industry Press, 2010.
[12] HECTOR C. Practical data analysis[M]. Beijing: Machine Industry Press, 2014.

**作者简介：**

**金鑫**（1973-），男，内蒙古乌海人，博士，中央财经大学教授，主要研究方向为商务智能。

**潘宜安**（1991-），女，福建福州人，中央财经大学硕士生，主要研究方向为数据挖掘。

**吴靖**（1957-），女，北京人，中央财经大学教授，主要研究方向为信息经济。