第41卷第7期 中国科学技术大学学报 Vol. 41, No. 7
2011年7月 JOURNAL OF UNIVERSITY OF SCIENCE AND TECHNOLOGY OF CHINA Jul. 2011

文章编号:0253-2778(2011)07-0619-07

适应性安全的多主密钥 KP-ABE 方案

杨晓元[1],王志强[2],蔡伟艺[1]

(1.武警工程学院电子技术系,陕西西安 710086;2.武警总医院通信站,北京 100039)

摘要:功能加密能很好地满足多对多的网络环境下的机密性需求,功能性函数提供了比传统公钥更灵活的密文存取能力.已有的功能加密系统均只支持单主密钥功能性函数,本文提出了功能加密子类 KP-ABE(key-policy attribute-based encryption)上的多主密钥适应性安全模型,该模型具有更强的表达能力及更广义的特性.利用线性多秘密共享方案,设计了该安全模型下的一个加密方案,并采用对偶法在标准模型下证明方案是 IND-CPA(indistinguishability against chosen-ciphertext attacks)安全的.该方案加密数据的存取策略更为灵活,用户可根据权限存取多种类型的密文;提出的构造方法可应用于功能加密的其他子类,且计算量与单主密钥方案相比不存在线性扩张,具有较高的效率.

关键词:密钥策略属性基加密;适应性安全;线性多秘密共享方案;对偶法

中图分类号:TP309 **文献标识码**:A doi:10.3969/j.issn.0253-2778.2011.07.009

Multiple-authority-key KP-ABE scheme with adaptive security

YANG Xiaoyuan[1], WANG Zhiqiang[2], CAI Weiyi[1]

(1. *Department of Electronic Technology, Engineering College of the A. P. F., Xi'an* 710086, *China*;
2. *Station of Communication, General Hospital of A. P. F., Beijing* 100039, *China*)

Abstract: Functional encryption provides a good way for sharing encrypted data in the network environment, which is sufficient for new emerging applications. Several recent works only focused on the systems that supported single-authority-key functionality. In order to solve the open problem of the construction of multiple authority keys functional encryption, an adaptive security model of multiple-authority-key key-policy attribute-based encryption (M-KP-ABE) was presented, which allows for functionalities that take in multiple authority keys. In this system, an encryptor can specify a policy and a capability describing what the decryptor can learn from the ciphertext. A new M-KP-ABE scheme was proposed for any attribute access structure that could be expressed by a linear multi-secret sharing scheme (LMSSS). This scheme is proven to be adaptively secure in the standard model by using the dual system encryption methodology recently introduced. The key generation centre (KGC) with multiple authority keys can combine user's capabilities in a specified manner and users can decrypt many kinds of ciphertexts. It is easy to apply this methodology to other subclasses of functional encryption with equal security and efficiency, which makes it more appropriate for applications.

Key words: KP-ABE; adaptive security; LMSSS; dual system encryption

收稿日期:2011-04-28;**修回日期**:2011-07-13

基金项目:国家自然科学基金(60573036),陕西省自然科学基金(2010JM8034),武警工程学院基础基金(wjy201119)资助.

作者简介:杨晓元(通讯作者),男,1959年生,教授. 研究方向:密码算法与协议和网络安全. E-mail: xyyangwj@126.com

0 引言

2010年欧密会上,Lewko等[1]首次提出了功能加密(functional encryption,FE)的概念,突破了传统公钥大多只适用于点对点环境的限制,FE提供了灵活的密文共享方式,具有很强的实用性.在功能加密系统中,用户拥有的私钥能够求解加密数据的一个函数,即功能性函数 $F:K\times X\to\{0,1\}^*$,这个函数决定了拥有密钥 k 的用户能从加密数据 x 中获取的知识.由于FE能定制灵活的公私钥关系,使得其在云计算和现代复杂网络环境下有很强的实用价值,因而正引起广泛关注.

功能加密是基于身份加密(identity-based encryption,IBE)的推广,也是非交互型密码的一种.先前的许多研究工作,如IBE[2-4],ABE(attribute-based encryption)[5-10],PE(predicate encryption)[11-13]都是功能加密的范畴,但已有研究都是在单主密钥功能性函数的形式下.2010年,Boneh等在文献[14]中精确地定义了功能加密的概念及安全性,并指出多主密钥功能性函数 $F:K_1\times K_2\times\cdots\times K_l\times X\to\{0,1\}^*$ 方案构造的开放性问题.这种类型的方案具有更广义的特性,且具有更丰富的应用场景,例如可以应用在以下场合:在一个机构中,不同级别的文件用不同的密钥加密,成员拥有相应的属性,同时具有不同的解密权限,KGC(key generation centre)按成员的权限和属性生成相应的解密私钥,即成员能解密多种类型的密文,而单主密钥的情形则难以实现.

功能加密的安全性分析主要有两种形式:选择挑战(selective security)模型和适应性安全(adaptive security)模型.选择挑战模型在挑战者-敌手游戏开始前,敌手要先出示要挑战的密钥信息,这不能客观自然地刻画攻击者,而适应性安全模型则不需要这个限制.已有的功能加密方案,部分[5-11]只能达到选择挑战安全,这是由于这些方案采用了分类法(partitioning strategy)证明,分类法的内在特性使方案不可避免地只能是选择挑战安全.文献[15-16]提出了对偶法(dual system encryption),对偶法通过一系列不可区分的游戏,使证明规约到一个简单的游戏上.文献[1]也是通过这种方法设计了适应性安全方案.

本文在功能加密的子类密钥策略属性基加密(key-policy ABE,KP-ABE)上提出多主密钥适应性安全模型,该安全模型能支持功能性函数 $F:K_1\times K_2\times\cdots\times K_l\times X\to\{0,1\}^*$,部分地解决了多主密钥方案构造的问题;在该模型下设计了一个表达能力较强的方案,能接受任意可表达为LMSSS(linear multi-secret sharing scheme)的存取结构;最后利用对偶法分析了方案的安全性并讨论了方案的效率,得到了较优的结论.

1 预备知识

本节定义下节方案构造中的线性多秘密共享方案(LMSSS)、合数阶双线性对及困难性假设.

1.1 LMSSS

定义 1.1 存取结构(access structure)

设 $P=\{P_1,\cdots,P_n\}$ 是 n 个参与者集合,$AS\subseteq 2^P$ 是 2^P 的一个子集,其中 2^P 表示 P 的全部子集构成的集合.称非空集合AS是 P 上的存储结构,如果集合AS满足单调性:

如果 $A\in AS$,则对任何的 $A'\in 2^P$ 和 $A\subseteq A'$,有 $A'\in AS$.

若AS是 P 上的存储结构,则AS中任何集合称为 P 上的授权集;对于 $2^P\backslash AS$ 中任意集合称为非授权集.

定义 1.2 单调张成方案(monotone span program)

$\mathbf{M}$ 是 Z_p 上 $m\times n$ 阶阵,$\{x_1,\cdots,x_u\}$ 是标号集,映射 ρ:{矩阵的行标号}$\to\{x_1,\cdots,x_u\}$,给出矩阵 $\mathbf{M}$ 的行用 $x_1,\cdots,x_u$ 作为标记方式.标记后的矩阵用 $\mathcal{M}=\mathcal{M}(\mathbf{M},\rho)$ 表示,称为相对映射 ρ 的单调张成方案.

由 $\mathcal{M}$ 构造的 $\mathbf{M}_G$ 为 $\mathbf{M}$ 上 $\rho(i)\in G$ 的行构成的子矩阵.称 $\mathcal{M}$ 相对非零向量 $\boldsymbol{v}$ 接受 G,当且仅当 $\boldsymbol{v}\in$ span($\mathbf{M}_G$),其中 span($\mathbf{M}_G$)为 $\mathbf{M}_G$ 生成的线性空间.单调张成方案 $\mathcal{M}$ 相对非零向量 $\boldsymbol{v}$ 可计算布尔函数 f,是指所有 $\boldsymbol{v}$ 可接受的 G 都有 $f_M(G)=1$.

单调张成方案与存取结构具有一一对应的关系,存在多存取结构$\{AS_1,AS_2,\cdots,AS_l\}$的线性多秘密共享体制则存在可计算单调布尔函数$\{f_{AS_1},f_{AS_2},\cdots,f_{AS_l}\}$的单调张成方案[17].

定义 1.3 线性多秘密共享方案(LMSSS)

称参与者集合 P 上的一个多秘密共享方案是线性的,其中$\{AS_1,AS_2,\cdots,AS_l\}$是 P 上的 l 个存取结构,f_{AS_1},$f_{AS_2}\cdots$,f_{AS_l} 分别是$\{AS_1,AS_2,\cdots,AS_l\}$的单调特征函数,若:

①参与者的秘密分享值构成一个 Z_p 上的向量；

②单调张成方案 $\mathcal{M}(\mathbf{M},\rho)$可计算 l 个单调布尔函数 f_{AS_1}，$f_{AS_2}\cdots$，f_{AS_l}，不失一般性取相应的 l 个 n 维目标向量为 $\boldsymbol{v}_1=(1,0,\cdots,0)$，$\cdots$，$\boldsymbol{v}_l=(0,\cdots,\overset{l}{1},\cdots,0)$. 对于向量 $\boldsymbol{s}=(y_1,\cdots,y_l,r_{l+1},\cdots,r_n)$，其中 $(y_1,\cdots,y_l)$是待共享的秘密，$r_{l+1},\cdots,r_n\in_R Z_p$，计算 $\boldsymbol{\lambda}=\mathbf{M}\boldsymbol{s}'$得到 l 个秘密份额(其中 $\boldsymbol{s}'$为 $\boldsymbol{s}$ 的转置)，根据标号函数将秘密份额 $\lambda_i=(\mathbf{M}\boldsymbol{s}')_i$ 分配给参与者 $\rho(i)$.

不失一般性，设 P 中的某个子集 $G\in AS_1\cap\cdots\cap AS_k$，若 $\boldsymbol{v}_j\in\mathrm{span}(\mathbf{M}_G)$，$1\leqslant j\leqslant k$，存在多项式时间算法计算出向量 $\boldsymbol{w}_j$，使得 $\boldsymbol{v}_j=\boldsymbol{w}_j\mathbf{M}_G$，$1\leqslant j\leqslant k$，于是 $\boldsymbol{y}_j=\boldsymbol{v}_j\boldsymbol{s}'=(\boldsymbol{w}_j\mathbf{M}_G)\boldsymbol{s}'=\boldsymbol{w}_j(\mathbf{M}_G\boldsymbol{s}')$，由于 G 对 k 个存取结构都是授权集，G 中成员掌握的信息可以恢复出这 k 个密钥.

将 LMSSS 引入本文的方案，参与者即为属性，存取结构 AS 即为授权属性集. 由于用户拥有自身具有的属性，所以不用考虑重构过程中产生的信息泄露问题.

1.2　合数阶双线性对

定义 1.4　令 G 为群生成器，输入安全参数，输出$(N=p_1p_2p_3,G,G_T,e)$，其中 p_1,p_2,p_3 为 3 个不同的素数，G,G_T 是具有大数阶 N 的乘法循环群. 合数阶双线性对[18]是指满足下列性质的一个映射 e：$G\times G\to G_T$：

①双线性：$e(g^a,g^b)=e(g,g)^{ab}$，$a,b\in_R Z_q^*$；

②非退化性：满足 $e(g,g)\neq 1$，其中 1 为循环乘法群 G_T 的幺元；

③可计算性：存在多项式算法计算 $e(g^a,g^b)$.

令 G_{p1},G_{p2},G_{p3}为 G 的 3 个子群，这些子群具有正交性，即对于 $h_i\in G_{pi}$，$h_j\in G_{pj}$，$i\neq j$ 有 $e(h_i,h_j)$为 G_T 中的一个常量.

1.3　困难性假设

假设 1.1　给定生成器 G，定义以下分布：

$$\mathbb{G}=(N=p_1p_2p_3,G,G_T,e)\xleftarrow{R}\mathcal{G},$$
$$g\xleftarrow{R}G_{p_1},X_3\xleftarrow{R}G_{p_3},$$
$$D=(\mathbb{G},g,X_3),$$
$$T_0\xleftarrow{R}G_{p_1},T_1\xleftarrow{R}G_{p_1p_2}.$$

定义算法 $\mathcal{A}$ 攻破假设 1.1 的优势为

$$Adv1_{\mathcal{G},\mathcal{A}}(\lambda):=$$
$$|\Pr[\mathcal{A}(D,T_0)=0]-\Pr[\mathcal{A}(D,T_1)=0]|$$

定义 1.5　称假设 1.1 成立，若对于任意多项式时间算法 $\mathcal{A}$，$Adv1_{\mathcal{G},\mathcal{A}}(\lambda)$是一个可忽略的量.

假设 1.2　给定生成器 $\mathcal{G}$，定义以下分布：

$$\mathbb{G}=(N=p_1p_2p_3,G,G_T,e)\xleftarrow{R}\mathcal{G},$$
$$g,X_1\xleftarrow{R}G_{p_1},X_2,Y_2\xleftarrow{R}G_{p_2},X_3,Y_3\xleftarrow{R}G_{p_3},$$
$$D=(\mathbb{G},g,X_1X_2,X_3,Y_2Y_3),$$
$$T_0\xleftarrow{R}G_{p_1p_3},T_1\xleftarrow{R}G.$$

定义算法 $\mathcal{A}$ 攻破假设 1.2 的优势为

$$Adv2_{\mathcal{G},\mathcal{A}}(\lambda):=$$
$$|\Pr[\mathcal{A}(D,T_0)=0]-\Pr[\mathcal{A}(D,T_1)=0]|$$

定义 1.6　称假设 1.2 成立，若对于任意多项式时间算法 $\mathcal{A}$，$Adv2_{\mathcal{G},\mathcal{A}}(\lambda)$是一个可忽略的量.

假设 1.3　给定生成器 $\mathcal{G}$，定义以下分布：

$$\mathbb{G}=(N=p_1p_2p_3,G,G_T,e)\xleftarrow{R}\mathcal{G},$$
$$y_1,\cdots,y_l,r\in\mathbf{Z}_N,$$
$$g\xleftarrow{R}G_{p_1},X_2,Y_2,Z_2\xleftarrow{R}G_{p2},X_3\xleftarrow{R}G_{p_3},$$
$$D=(\mathbb{G},g,g^{y_1}X_2,\cdots,g^{y_l}X_2,X_3,g^rY_2,Z_2),$$
$$\{T_{0,j}=e(g,g)^{y_jr},T_{1,j}\xleftarrow{R}G_T\}_{j=1,\cdots,l}.$$

定义对于任意的 $j\in\{1,\cdots,l\}$算法 $\mathcal{A}$ 攻破假设 1.3 的优势为

$$Adv3_{\mathcal{G},\mathcal{A}_j}(\lambda):=$$
$$|\Pr[\mathcal{A}(D,T_{0,j})=0]-\Pr[\mathcal{A}(D,T_{1,j})=0]|$$

定义 1.7　称假设 1.3 成立，若对于任意多项式时间算法 $\mathcal{A}$，$Adv3_{\mathcal{G},\mathcal{A}}(\lambda)$是一个可忽略的量.

前两个假设在文献[16]中已作了证明，假设 1.3 证明如下.

证明　应用文献[11]中定义的表示方式，可将假设 1.3 表示为

$$A_1=(1,0,0),A_{2,1}=(B_1,1,0),\cdots,$$
$$A_{2,l}=(B_l,1,0),A_3=(0,0,1),$$
$$A_4=(R,X_2,0),A_5=(0,Y_2,0),$$
$$\{T_0=[B_jR,0,0],T_1=[Z_1,Z_2,Z_3]\}_{j=1,\cdots,l}.$$

$T_{0,j}$独立于任意$\{e(A_n,A_m)\}$，因为要获得第一个坐标中 B_jR，必须要计算 $e(A_{2,j},A_4)$，但是 A_4 的第二个坐标 X_2 不能消除. 根据文献[11]中定理 A.1，求解假设 1.3 的复杂度可规约为分解大整数 N. 证毕.

2　M-KP-ABE 适应性安全模型

目前已提出的功能加密安全模型均为单主密钥

形式,其构造的方案中用户拥有的密钥 D 能从密文 C 中求解的函数为 $F:K\times X\to\{0,1\}^*$,只能求解单一类型的密文.本节提出功能加密子类 KP-ABE 的多主密钥适应性安全模型 M-KP-ABE,该模型支持功能性函数 $F:K_1\times K_2\times\cdots\times K_l\times X\to\{0,1\}^*$,具有更强表达能力和更广义特性.KGC 含有多个主密钥,根据用户的权限和属性生成解密密钥,只有满足相应属性,并被授权相应的主密钥才能恢复明文.用户可被授权多个主密钥,能解密多种类型的密文,使得加密系统更加灵活.

定义 2.1 密钥策略多主密钥属性基加密方案(multiple-authority-key KP-ABE, M-KP-ABE)由以下 4 个算法组成:

$\Sigma_{\text{M-KP-ABE}}=(\text{Setup},\text{Encrypt},\text{KeyGen},\text{Decrypt})$

①Setup:概率算法,输入安全参数,输出授权中心(KGC)的 l 个主密钥对(PK_i,MK_i);

②Encrypt:概率算法,输入明文 m,属性集 γ,及选取的公钥 PK_i,输出密文 C;

③KeyGen:概率算法,输入存取结构$\mathcal{M}(\mathbf{M},\rho)$,一个或多个主密钥$(MK_j)_{j\in\{j1,j2,\cdots,jk\}}$,输出解密密钥 D;

④Decrypt:确定性算法,输入密文 C 及解密密钥 D,若密文属性满足密钥存取结构则输出明文 m,否则输出$\perp$.

下面讨论 M-KP-ABE 的安全性,通过挑战者与敌手的游戏定义选择明文攻击下(indistinguishability against chosen-ciphertext attacks, IND-CPA)的安全性,游戏分 5 个阶段:

①Setup:挑战者运行 Setup 算法,并将公开参数传送给敌手;

②Phase1:敌手发起任意存取结构$(\mathcal{M},\rho)$及主密钥集合 H 的私钥询问;

③Challenge:敌手提交两个等长的密文 M_0 和 M_1 及要挑战的主密钥 Y_j^* 和属性集 γ^* 给挑战者,其中 Y_j^* 和 γ^* 不能同时满足 Phase1 中的同一个询问;挑战者抛掷公平硬币 b,用 γ^* 和 Y_j^* 加密 M_b 得到目标密文 C^*,将 C^* 传给敌手;

④Phase2:重复 Phase1 的询问,其中$(\mathbf{M},\rho)$和 H 不能同时满足挑战的密钥;

⑤Guess:敌手输出 b 的猜测值 b'.

游戏中敌手 $\mathcal{A}$ 的优势定义为

$$\Pr[b'=b]-\frac{1}{2}$$

只要在游戏的 Phase1 与 Phase2 中添加解密询问,则可以拓展到选择密文安全性.此外,适应性安全模型不需要敌手事先出示所要挑战的属性集 γ^* 及主密钥 Y_j^*.

定义 2.2 称一个多主密钥 KP-ABE 方案 $\Sigma_{\text{M-KP-ABE}}$是适应性安全的,如果任意多项式有界敌手赢得以上游戏的概率是可忽略的.

3 适应性安全的 M-KP-ABE 方案

3.1 方案描述

根据节 2 定义的 M-KP-ABE 安全模型,结合 LMSSS,设计方案如下:

①Setup(1^λ):KGC 选取阶为 $N=p_1p_2p_3$ 的双线性群 G,定义全局属性 $\mathcal{U}=\{1,2,\cdots,u\}$,对于任意 $i\in\mathcal{U}$,选取随机值 $t_i\in_R Z_N$,计算 $T_i=g^{t_i}$;密钥中心根据安全参数 λ 选取全局主私钥 $y_j\in_R Z_N$,$j\in\{1,\cdots,l\}$,计算 $Y_j=e(g,g)^{y_j}$,其中 $g\in G_{p_1}$;公开公钥 $PK=\{\{Y_j\}_{j\in(1,\cdots,l)},\{T_i\}_{i\in(1,\cdots,u)}\}$,保存私钥 $MK=\{\{y_j\}_{j\in(1,\cdots,l)},\{t_i\}_{i\in(1,\cdots,u)}\}$.

②Encrypt(γ,m,Y_j):加密方选取 $r\in_R Z_N$,加密密文如下:

$$C=\{Y_j,\gamma,c=mY_j^r,c_0=g^r,\{c_i=T_i^r\}_{i\in\gamma}\}$$

③KeyGen$(H,\mathcal{M}(\mathbf{M},\rho),MK)$:用户被授权的主密钥表示为 $H=\{Y_{j1},\cdots,Y_{jk}\}$,秘密共享矩阵 $\mathbf{M}$ 为 $m\times n$ 阶阵,$n>k$,标号函数 ρ 映射到的属性集为 $U\subset\mathcal{U}$,本文只考虑 ρ 为单射的情况,即 $|U|=m$.KGC 验证用户所能拥有的主密钥 H 和具有的存取结构 $\mathcal{M}(\mathbf{M},\rho)$后,分发相应的密钥计算如下:

取分享向量为

$$\boldsymbol{\kappa}=\{r_1,\cdots,\overset{j1}{y_{j1}},\cdots,\overset{jk}{y_{jk}},r_{k+1},\cdots,r_n\},$$

计算 $\boldsymbol{\lambda}=\mathbf{M}\boldsymbol{\kappa}$ 得到分享值;对每个属性 $i\in U$,KGC 选取 $s_i\in\mathbf{Z}_N$,$W_i,V_i\in G_{p_3}$,密钥生成为

$$D=\{d_i^1=g^{\lambda_i}T_{\rho(i)}^{s_i}W_i,d_i^2=g^{s_i}V_i\}_{i\in U}.$$

④Decrypt(C,D):若 $Y_j\in H$,且 $\gamma\in\mathcal{M}$,从 $\gamma\cap U$ 中任意选取 n 个属性构成 U_n,用户计算 $\boldsymbol{w}$,使得 $\boldsymbol{v}_j=\boldsymbol{w}\mathbf{M}_{U_n}$,可恢复明文如下:

$$\prod_{i\in U_n}\left(\frac{e(c_0,d_{\rho^{-1}(i)}^1)}{e(c_i,d_{\rho^{-1}(i)}^2)}\right)^{w_{\rho^{-1}(i)}}=$$

$$\prod_{i\in U_n}\left(\frac{e(g,g)^{r\cdot\lambda_{\rho^{-1}(i)}}e(g,T_{\rho(i)})^{r\cdot s_{\rho^{-1}(i)}}}{e(T_i,g)^{r\cdot s_{\rho^{-1}(i)}}}\right)^{w_{\rho^{-1}(i)}}=$$

$$e(g,g)^{r\sum_{i\in U_n}\lambda_{\rho^{-1}(i)}\cdot w_{\rho^{-1}(i)}}=e(g,g)^{ry_j}.$$

明显的 $m=c/e(g,g)^{ry_j}$,否则输出$\perp$.

3.2 性能分析

令 $l=1$ 即 $j\in\{1\}$，则多主密钥方案退化为单主密钥方案[1]，显然，多主密钥与单主密钥方案的公开参数长度、密文长度、公钥长度相同，加密与解密的计算时间复杂度相同，不存在时间复杂度与空间复杂度的线性扩张. 与文献[6]提出的精细访问树一样，本文的方案也可从只支持门限的存取结构，扩展为支持“与”、“或”和门限的精细访问树.

对于其他类型的功能加密系统，构造支持多主密钥功能性函数的加密方案也可采用本文的方法. 构造的方案的安全性与单主密钥方案相同，效率与单主密钥方案相比都不存在复杂度的线性扩张. 例如构造多主密钥 CP-ABE 方案，加密者在加密过程中设计访问结构，选取某个主密钥 K_j 加密，KGC 授权用户多个主密钥，主密钥信息分发形式与单主密钥形式相同.

3.3 安全性分析

本节采用对偶法来证明方案的安全性.

首先，定义半功能密钥(semi-functional key)和半功能密文(semi-functional ciphertext).

半功能密文即为

$$c_0 = g^r g_2^c, \{c_i = T_i^r g_2^{c\cdot z_i}\}_{i\in\gamma},$$

其中 g_2 为 G_{p_2} 的一个生成元，c 和 $\{z_i\}_{i\in U}$ 为随机值.

半功能密钥有两种形式.

type1：

$$d_i^1 = g^{\lambda_i} T_{\rho(i)}^{s_i} W_i g_2^{\delta_i + r_i\cdot z_{\rho(i)}}, d_i^2 = g^{s_i} V_i g_2^{r_i}$$

type2：

$$d_i^1 = g^{\lambda_i} T_{\rho(i)}^{s_i} W_i g_2^{\delta_i}, d_i^2 = g^{s_i} V_i$$

其中 $\boldsymbol{u}$ 为非零随机向量，$\boldsymbol{\delta}=\boldsymbol{M}\cdot\boldsymbol{u}$，$\{r_i\}_{i\in U}$ 为随机值.

由于合数阶双线性对的正交性，以半功能密钥解密正常密文或者以正常密钥解密半功能密文，都能正确地执行. 但以半功能密钥解密以 Y_j 加密半功能密文，将得到附加项

$$e(g_2, g_2)^{c\cdot \boldsymbol{v}_j \boldsymbol{u}} = e(g_2, g_2)^{c\cdot u_j}.$$

令随机向量 $\boldsymbol{u}$ 中的 $u_{j1},\cdots,u_{jk}$ 为 0，这种情况下半功能密钥能解密半功能密文，否则不能. 称这种类型的半功能密钥为伪半功能密钥(nominally semi-functional key).

再者，对偶法包含以下一系列不可区分的游戏. $\mathrm{Game}_{\mathrm{real}}$，真实情况下的游戏，即密文和密钥都是正常的；$\mathrm{Game}_0$，游戏中所有密钥都是正常的，而挑战密文是半功能的；$\mathrm{Game}_{k,1}$，游戏中前 $k-1$ 个密钥为半功能 type2，第 k 个为半功能 type1，其余密钥为正常型；$\mathrm{Game}_{k,2}$，游戏中前 k 个密钥为半功能 type2，其余密钥为正常型；$\mathrm{Game}_{q,2}$，全部密钥均为半功能 type2；$\mathrm{Game}_{\mathrm{final}}$，密钥均为 type2 半功能型，密文为半功能随机密文. 其中 q 为敌手密钥询问的次数，$k\in(1,\cdots,q)$.

下面，通过 4 个引理对这些游戏的不可区分性进行证明，其困难性可规约到节 1 中的假设.

引理 3.1　如果存在多项式算法 $\mathcal{A}$ 使得 $Adv_{\mathcal{A}}^{\mathrm{Game}_{\mathrm{real}}} - Adv_{\mathcal{A}}^{\mathrm{Game}_0} = \varepsilon$，则能构造算法 $\mathcal{B}$ 能以 ε 的优势解决假设 1.1.

证明　$\mathcal{B}$ 获取假设 1.1 的一个挑战实例 $\{g, X_3, T\}$. $\mathcal{B}$ 运行 Setup，选择 MK 生成 PK，将公开参数传给敌手. $\mathcal{B}$ 同时要模拟 $\mathrm{Game}_{\mathrm{real}}$，$\mathrm{Game}_0$ 两个游戏. 对于存取结构 $(\boldsymbol{M},\rho)$ 和相关的主密钥 H 的密钥询问，由于 $\mathcal{B}$ 知道 MK，故只需运行 KeyGen 来作出应答；对于要挑战的 m_0，m_1 和目标属性集 γ^* 和主密钥 Y_{j^*} 的密文询问，$\mathcal{B}$ 则要通过 T 来模拟. 计算密文如下：

$$C^* = \{Y_{j^*}, \gamma^*, c = m_b e(g, T)^{y_{j^*}}, c_0 = T, \{c_i = T^{t_i}\}_{i\in\gamma^*}\}.$$

当 $T\in G_{p_1}$，将 T 表示为 g^r，显然这是正常的密文；当 $T\in G_{p_1 p_2}$，将 T 表示为 $g^r X_2$，则有 $z_i = t_i$，根据中国剩余定理，$z_i \bmod p_2$ 与 $t_i \bmod p_1$ 不相关，这是合理的，即密文为半功能型.

综上所述，若 $\mathcal{A}$ 区分以上游戏的概率为 ε，则 $\mathcal{B}$ 能根据 $\mathcal{A}$ 的输出以 ε 的概率解决假设 1.1. 证毕.

引理 3.2　如果存在多项式算法 $\mathcal{A}$ 使得 $Adv_{\mathcal{A}}^{\mathrm{Game}_{k-1,2}} - Adv_{\mathcal{A}}^{\mathrm{Game}_{k,1}} = \varepsilon$，则能构造算法 $\mathcal{B}$ 能以 ε 的优势解决假设 1.2.

证明　$\mathcal{B}$ 获取假设 1.2 的一个挑战实例 $(g, X_1X_2, X_3, Y_2Y_3, T)$，$\mathcal{B}$ 运行 Setup，选择 MK 生成 PK，将公开参数传给敌手. 对于要挑战的 m_0，m_1 和目标属性集 γ^* 和主密钥 Y_{j^*} 的密文询问，$\mathcal{B}$ 计算半功能密文：

$$C^* = \{Y_{j^*}, \gamma^*, c = m_b e(g, X_1X_2)^{y_{j^*}}, c_0 = X_1X_2, \{c_i = (X_1X_2)^{t_i}\}_{i\in\gamma^*}\}$$

不妨令 $X_1X_2 = g^r g_2^c$，同引理 3.1 证明，密文的设置蕴含了令 $z_i = t_i$，故这是一个有效的半功能密文.

对于存取结构 $(\boldsymbol{M},\rho)$ 和相关的主密钥 H 的密钥询问，有以下 3 种情况.

①对于前 $k-1$ 次询问，$\mathcal{B}$ 根据 KeyGen 算法设

置随机向量 $\boldsymbol{\kappa}$，选取随机向量 $\boldsymbol{u}'$，选取随机值 $\{s_i \in \mathbf{Z}_N, V_i, W_i \in G_{p_3}\}_{i \in U}$，令 $\boldsymbol{\lambda} = \boldsymbol{M\kappa}$，$\boldsymbol{\delta}' = \boldsymbol{Mu}'$，生成 type2 半功能密钥：

$$d_i^1 = g^{\lambda_i} T_{\rho(i)}^{s_i} W_i (Y_2 Y_3)^{\delta_i'}, d_i^2 = g^{s_i} V_i.$$

②对于第 k 次密钥询问，$\mathcal{B}$ 将根据 T 来生成一个正常的密钥或者伪 type1 半功能密钥. $\mathcal{B}$ 根据 KeyGen 算法设置随机向量 $\boldsymbol{\kappa}'$，根据伪半功能密钥中的设置方法选取随机向量 $\boldsymbol{u}$，选取随机值 $\{r_i \in Z_N, V_i, W_i \in G_{p_3}\}_{i \in U}$，令 $\boldsymbol{\lambda}' = \boldsymbol{M\kappa}'$，$\boldsymbol{\delta} = \boldsymbol{Mu}$，计算密钥为

$$d_i^1 = g^{\lambda_i'} T^{\delta_i + r_i z_{\rho(i)}} W_i, d_i^2 = T^{r_i} V_i.$$

令 g^{ξ} 为 T 中的 G_{p_1} 部分，则有 $s_i = \xi r_i$，$\boldsymbol{\kappa} = \xi \boldsymbol{u} + \boldsymbol{\kappa}'$，这是合理的，因为 $r_i \bmod p_2$ 与 $s_i \bmod p_1$ 不相关. 当 $T \in G_{p_1} G_{p_3}$ 时，所生成的密钥是正常的密钥；当 $T \in G$ 时，所生成的密钥是伪 type1 半功能密钥. 并且这个伪 type1 半功能密钥对于敌手来说与 type1 有着相同的分布. 分析如下：

令 $g_2^{\xi_2}$ 为 T 中的 G_{p_2} 部分，则生成密钥中包含 G_{p_2} 的指数为 $\mathbf{M}_i \boldsymbol{u} + r_i z_{\rho(i)}$，其中 $z_{\rho(i)} = t_{\rho(i)}$，$z_{\rho(i)} \bmod p_2$ 与 $t_{\rho(i)} \bmod p_1$ 不相关. 只要 $r_i \bmod p_2$ 不为 0 则敌手得不到关于 $\mathbf{M}_i \boldsymbol{u}$ 的任何信息. 由于 $r_i \bmod p_2$ 均为 0 的概率是可忽略的，故敌手获得的信息是可忽略的. 因而，对于敌手来说伪 type1 和 type1 以接近于 1 的概率具有相同的分布.

③对于其余的密钥询问，要求 $\mathcal{B}$ 生成正常的密钥，由于 $\mathcal{B}$ 知道 MK，所以只需运行 KeyGen 来作出应答.

综上所述，$\mathcal{B}$ 利用 T 来正确模拟 $\mathrm{Game}_{k-1,2}$ 或者以接近于 1 的概率模拟 $\mathrm{Game}_{k,1}$，若 $\mathcal{A}$ 区分以上游戏的概率为 ε，则 $\mathcal{B}$ 能根据 $\mathcal{A}$ 的输出以接近于 ε 的概率解决假设 1.2. 证毕.

引理 3.3 如果存在多项式算法 $\mathcal{A}$ 使得 $Adv_{\mathcal{A}}^{\mathrm{Game}_{k,2}} - Adv_{\mathcal{A}}^{\mathrm{Game}_{k,1}} = \varepsilon$，则能构造算法 $\mathcal{B}$ 能以 ε 的优势解决假设 1.2.

证明 $\mathcal{B}$ 获取假设 1.2 的一个挑战实例 $(g, X_1 X_2, X_3, Y_2 Y_3, T)$，挑战密文、前 $k-1$ 个密钥和其他正常密钥生成与引理 3.2 相同. 下面描述 $\mathcal{B}$ 通过 T 来设置第 k 个密钥. $\mathcal{B}$ 根据 KeyGen 算法设置随机向量 $\boldsymbol{\kappa}$，选取随机向量 $\boldsymbol{u}'$，选取随机值 $\{r_i \in \mathbf{Z}_{p_2}, V_i, W_i \in G_{p_3}\}_{i \in U}$，令 $\boldsymbol{\lambda} = \boldsymbol{M\kappa}$，$\boldsymbol{\delta}' = \boldsymbol{Mu}'$，构造密钥如下：

$$d_i^1 = g^{\lambda_i} (Y_2 Y_3)^{\delta_i'} T^{r_i t_{\rho(i)}} W_i, d_i^2 = T^{r_i} V_i.$$

当 $T \in G_{p_1} G_{p_3}$ 时，所生成的密钥是 type2 半功能密钥；当 $T \in G$ 时，所生成的密钥是 type1 半功能密钥.

综上所述，$\mathcal{B}$ 利用 T 来正确模拟 $\mathrm{Game}_{k,2}$ 或者 $\mathrm{Game}_{k,1}$，若 $\mathcal{A}$ 区分以上游戏的概率为 ε，则 $\mathcal{B}$ 能根据 $\mathcal{A}$ 的输出以 ε 的概率解决假设 1.2. 证毕.

引理 3.4 如果存在多项式算法 $\mathcal{A}$ 使得 $Adv_{\mathcal{A}}^{\mathrm{Game}_{q,2}} - Adv_{\mathcal{A}}^{\mathrm{Game}_{\mathrm{final}}} = \varepsilon$，则能构造算法 $\mathcal{B}$ 能以 ε 的优势解决假设 1.3.

证明 $\mathcal{B}$ 获取假设 1.3 的一个挑战实例 $(g, g^{y_1} X_2, \cdots, g^{y_l} X_2, X_3, g^r Y_2, Z_2, T)$，选取随机值 $t_i \in {}_R Z_N$，计算 $T_i = g^{t_i}$，令 $Y_j = e(g, g^{\alpha_j} X_2)$，发布公开参数. 对于要挑战的 m_0, m_1 和目标属性集 γ^* 和主密钥 Y_{j^*} 的密文询问，$\mathcal{B}$ 选取 T 中的第 j 个挑战 T_j，计算：

$$C^* = \{Y_{j^*}, \gamma^*, c = m_b T_j, c_0 = g^r Y_2, \{c_i = (g^r Y_2)^{t_i}\}_{i \in \gamma^*}\}.$$

若 $T_0 = e(g, g)^{\alpha_j r}$，则生成 m_b 有效半功能密文；若 $T \in {}_R G_T$，则生成的半功能密文为随机元，密文不包含关于 b 的任何信息.

对于存取结构 $(\mathbf{M}, \rho)$ 和相关的主密钥 H 的密钥询问，$\mathcal{B}$ 根据 KeyGen 算法设置随机向量

$$\boldsymbol{\kappa} = \{r_1, \cdots, \overset{j1}{y_{j1}}, \cdots, \overset{jk}{y_{jk}}, r_{k+1}, \cdots, r_n\},$$

选取随机向量 $\boldsymbol{u}'$，选取随机值 $\{s_i \in \mathbf{Z}_N, V_i, W_i \in G_{p_3}\}_{i \in U}$，计算：

$$d_i^1 = g^{M_{i,1} \cdot r_1} \cdots (g^{y_{j1}} X_2)^{M_{i,j1}} \cdots (g^{y_{jk}} X_2)^{M_{i,jk}} g^{M_{i,jk+1} \cdot r_{jk+1}} \cdots g^{M_{i,n} \cdot r_n} T_{\rho(i)}^{s_i} W_i Z_2^{\delta_i'},$$

$$d_i^2 = g^{s_i} V_i.$$

令 $X_2 = g_2^{\xi_1}$，$Z_2 = g_2^{\xi_2}$，则有对于 $\boldsymbol{u}$ 的 $j1, \cdots jk$ 坐标有 $u_j = \xi_1 + \xi_2 u_j'$，其他 $u_j = \xi_2 u_j'$，故这是对 type2 半功能密钥的有效模拟. 若 $\mathcal{A}$ 区分游戏 $\mathrm{Game}_{q,2}$ 与 $\mathrm{Game}_{\mathrm{final}}$ 的概率为 ε，则 $\mathcal{B}$ 能根据 $\mathcal{A}$ 的输出以 ε 的概率解决假设 1.3. 证毕.

通过以上引理可以证明以下定理：

定理 3.1 如果假设 1.1、假设 1.2、假设 1.3 成立，则 M-KP-ABE 方案是安全的.

证明 如果假设 1.1、假设 1.2、假设 1.3 成立，根据引理 3.1、引理 3.2、引理 3.3、引理 3.4，$\mathrm{Game}_{\mathrm{real}}$ 与 $\mathrm{Game}_{\mathrm{final}}$ 是不可区分的，而 $\mathrm{Game}_{\mathrm{final}}$ 中密文在密文空间中均匀分布. 因而本文的方案是安全的.

4 结论

本文提出了适应性安全的多主密钥 KP-ABE

安全模型，结合 LMSSS 设计了一个具有较强表达能力的方案，部分地解决了多主密钥形式功能性函数 $F: K_1 \times K_2 \times \cdots \times K_l \times X \rightarrow \{0,1\}^*$ 方案的构造问题；采用对偶法在标准模型下证明方案在选择明文攻击下是适应性安全的，游戏中对敌手的模拟能精确描述敌手的能力；该方案与单主密钥方案相比不存在计算量的增加，具有较高的效率. 多主密钥功能加密系统中用户能操作不同类型的密文，使得用户具有不同的权限，更接近于现实中的应用场景. 目前多主密钥功能加密安全模型的定义及其他子类的多主密钥方案有待进一步研究；设计具有更强表达能力的功能性函数也是一个重要方向.

参考文献(References)

[1] Lewko A, Okamoto T, Sahai A, et al. Fully secure functional encryption: Attribute-based encryption and (hierarchical) inner product encryption[J]. Lecture Notes in Computer Science, 2010, 6 110: 62-91.

[2] Shamir A. Identity-based cryptosystems and signature schemes[J]. Lecture Notes in Computer Science, 1985, 196: 47-53.

[3] Boneh D, Franklin M. Identity based encryption from the Weil pairing[J]. Lecture Notes in Computer Science, 2001, 2 139: 213-229.

[4] Cocks C. An identity based encryption scheme based on quadratic residues[J]. Lecture Notes in Computer Science, 2001, 2 260: 360-363.

[5] Sahai A, Waters B. Fuzzy Identity Based Encryption [J]. Lecture Notes in Computer Science, 2005, 3 494: 457-473.

[6] Goyal V, Pandey O, Sahai A, et al. Attribute-based encryption for finegrained access control of encrypted data[C]//Proceedings of the 13th ACM Conference on Computer and Communications Security. New York: ACM, 2006: 89-98.

[7] Ostrovsky R, Sahai A, Waters B. Attribute-based encryption with nonmonotonic access structures[C]// Proceedings of the 14th ACM Conference on Computer and Communication Security. New York: ACM, 2007: 195-203.

[8] Chase M. Multi-authority attribute based encryption [J]. Lecture Notes in Computer Science, 2007, 4 392: 515-534.

[9] Waters B. Ciphertext-policy attribute-based encryption: An expressive, efficient, and provably secure realization[J]. Lecture Notes in Computer Science, 2011, 6 571: 53-70.

[10] Goyal V, Jain A, Pandey O, et al. Bounded ciphertext policy attribute-based encryption[J]. Lecture Notes in Computer Science, 2008, 5 126: 579-591.

[11] Katz J, Sahai A, Waters B. Predicate encryption supporting disjunctions, polynomial equations, and inner products[J]. Lecture Notes in Computer Science, 2008, 4 965: 146-162.

[12] Okamoto T, Takashima K. Fully secure functional encryption with general relations from the decisional linear assumption[J]. Lecture Notes in Computer Science, 2010, 6 223: 191-208.

[13] Attrapadung N, Libert B. Functional encryption for inner product: Achieving constant-size ciphertexts with adaptive security or support for negation[J]. Lecture Notes in Computer Science, 2010, 6 056: 384-402.

[14] Boneh D, Sahai A, Waters B. Functional encryption: Definitions and challenges[J]. Lecture Notes in Computer Science, 2011, 6 597: 253-273.

[15] Waters B. Dual system encryption: realizing fully secure ibe and hibe under simple assumptions[J]. Lecture Notes in Computer Science, 2009, 5 677: 619-636.

[16] Lewko A, Waters B. New techniques for dual system encryption and fully secure hibe with short ciphertexts [J]. Lecture Notes in Computer Science, 2010, 5 978: 455-479.

[17] Xiao Liangliang, Liu Mulan. Linear multi-secret sharing schemes[J]. Science in China Series F: Information Sciences, 2005,48(1): 125-136.

[18] Boneh D, Goh E, Nissim K. Evaluating 2-dnf formulas on ciphertexts[J]. Lecture Notes in Computer Science, 2005, 3378: 325-341.