计算机研究与发展
Journal of Computer Research and Development
ISSN 1000-1239/CN 11-1777/TP
48(8): 1363-1369, 2011

多主密钥功能加密:基于 LMSSS 的 M-KP-ABE 方案

杨晓元[1,2] 蔡伟艺[1] 陈海滨[2]
[1](武警工程学院电子技术系网络与信息安全武警部队重点实验室 西安 710086)
[2](武警工程学院网络与信息安全研究所 西安 710086)
(xyyangwj@126.com)

Multiple-Authority-Key Functional Encryption: A M-KP-ABE Scheme Based on LMSSS

Yang Xiaoyuan[1,2], Cai Weiyi[1], and Chen Haibin[2]
[1](*Key Laboratory of Network & Information Security under the Chinese Armed Police Force, Department of Electronic Technology, Engineering College of the Armed Police Force, Xi'an* 710086)
[2](*Institution of Network & Information Security, Engineering College of the Armed Police Force, Xi'an* 710086)

Abstract Functional encryption opens up a much larger world of possibilities for sharing encrypted data. It is sufficient for many emerging applications. Some recent work aimed at constructing different types of fine-grained encryption systems which could be cast in the framework of functional encryption, such as IBE, ABE, PE, but they only focused on the systems that supported single-authority-key functionality. We extend functional encryption to multiple-authority-key functional encryption, which can provide more sophisticated and flexible functionality. This system allows an encryptor to specify a policy and a capability by describing what users can learn from the ciphertext. The policies are similar to what were defined in the previous systems and the capabilities are expressed as different kinds of authority keys. This paper gives a security model for a class of multiple-authority-key functional encryption, multiple-authority-key KP-ABE. A new KP-ABE scheme, which supports functionalities taken in multiple authority keys, is proposed in the given security model. Our techniques allow for any attribute access the structure expressed by a linear multi-secret sharing scheme (LMSSS) matrix $\boldsymbol{M}$. Based on the assumption of DBDH, this scheme is proven to be selectively secure in the standard model under chosen plaintext attack. It is easy to derive the single-authority-key scheme from the multiple-authority-key scheme and construct fine-grained tree-access structure. The computational cost of our scheme is equal to the single-authority-key scheme, which makes it more appropriate in many practical applications.

Key words KP-ABE; LMSSS; functional encryption; functionality; bilinear pairings

摘 要 功能加密极大地拓宽了秘密信息的共享方式,但支持多主密钥功能性函数加密方案的构造问题仍未解决,多主密钥功能加密具有更强的表达能力和更广义的特性.在功能加密的一个子类密钥策略属性基加密上,首次提出了多主密钥形式的安全模型 M-KP-ABE.利用线性多秘密共享方案,设计了该安全模型下的一个支持多主密钥功能性函数的加密方案.基于 DBDH 假设,在标准模型下证明方案在适应性选择挑战和自适应选择明文攻击下是安全的.该方案加密数据的访问策略更为灵活,可退化为单主

收稿日期:2011-04-07;**修回日期**:2011-06-15
基金项目:国家自然科学基金重点项目(60633020);国家自然科学基金项目(60573036);武警工程学院基础基金项目(WJY201119)

密钥的加密方案,可构造具有精细访问树的方案,其计算量与单主密钥方案相等,具有较高的效率.

关键词 密钥策略属性基加密;线性多秘密共享方案;功能加密;功能性函数;双线性对

中图法分类号 TP3090

加密是在不安全网络或存储介质中共享敏感数据的有效方式.传统公钥密码体制的公私钥对应关系是单一的,只能支持简单的密文解密表达式.2010年欧密会上,Lewko等人[1]首次提出了功能加密(functional encryption,FE)的概念,突破了传统公钥的以上限制,能支持灵活的密文解密表达式,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(functionality)$F:K\times X\rightarrow\{0,1\}^*$,这个函数决定了拥有密钥$k$的用户能从加密数据$x$中获取的信息,当公钥与私钥满足特定关系式时,能得到正确的明文信息,这使得密文的访问能力是由关系式决定的.由于具有很强的实用性,随着云计算、社会网络等新型计算模式的兴起,功能加密正引起广泛关注.

关系式具有丰富的表达能力,部分关系类型能支持已有的密文解密表达式[2],这些研究工作,都可认为是功能加密的子类,例如支持相等关系的IBE(identity-based encryption),支持门限关系的ABE(attribute-based encryption),支持内积关系的PE(predicate encryption).1984年,Shamir[3]提出了基于身份密码学(IBE)的思想,Boneh,Franklin[4]和Cocks[5]分别独立地提出了第1个IBE方案.2005年,欧洲密码学年会上Sahai和Waters发表的文章[6]提出了基于身份的模糊加密,首次出现了属性这个概念,可以认为是ABE的雏形.2006年,CCS会议上Goyal等人首次将ABE分为密钥策略(key-policy ABE,KP-ABE)与密文策略(ciphertext-policy ABE,CP-ABE)2种[7].KP-ABE即密钥关联着访问结构,适合于数据静态的场景[6-9],CP-ABE则是密文关联着访问结构,适合于用户静态的场景[1,10].文献[11]提出了将KP-ABE转换为CP-ABE的有效方式.唐强等人[8]提出了多授权中心可验证的属性基加密方案.PE是由Katz,Sahai和Waters在2008年的欧密会上提出的[12].2010年,Waters等人在文献[2]中精确地定义了功能加密的概念及安全性,并指出了一些开放性的问题.同年的EuroCrypt[1],Crypto[13],PKC[14]会议上均有功能加密的研究成果发表.

但这些研究都是在单主密钥功能性函数的范畴下,文献[2]中提出了多主密钥功能函数$F:K_1\times K_2\times\cdots\times K_l\times X\rightarrow\{0,1\}^*$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.

本文在功能加密的子类KP-ABE上提出多主密钥安全模型(multiple-authority-key KP-ABE,M-KP-ABE),该安全模型能构造支持功能性函数$F:K_1\times K_2\times\cdots\times K_l\times X\rightarrow\{0,1\}^*$的方案,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线性多秘密共享方案(linear multi-secret sharing scheme,LMSSS)的访问结构.最后本文分析了方案的安全性和性能,得到了较优的结论:在标准模型下证明方案在适应性选择挑战和自适应选择明文攻击下是安全的;方案易于构造单主密钥的加密方案和具有精细访问树的方案,且其计算量与单主密钥方案相等.

1 预备知识

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

1.1 LMSSS

在定义LMSSS前,先介绍几个相关概念

定义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,即AS是由P的某些子集构成的非空集合,称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2. 单调张成方案(monotone span program)

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

由 $\mathcal{M}$构造的 $\boldsymbol{M}_G$ 为 $\boldsymbol{M}$ 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 $\boldsymbol{v}\in span(\boldsymbol{M}_G)$,其中 $span(\boldsymbol{M}_G)$为 $\boldsymbol{M}_G$ 生成的线性空间. 单调张成方案 $\mathcal{M}$相对非零向量 $\boldsymbol{v}$ 可计算单调布尔函数 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[15].

定义 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$\{AS_1,AS_2,\cdots,AS_l\}$上的单调特征函数,若:

1) 参与者的秘密分享值构成一个$\mathbb{Z}_p$上的向量;

2) 单调张成方案 $\mathcal{M}(\boldsymbol{M},\rho)$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,$r_{l+1},\cdots,r_n\in_R\mathbb{Z}_p$,计算 $\lambda=\boldsymbol{M}\boldsymbol{s}'$得到 m 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 $\lambda_i=(\boldsymbol{M}\boldsymbol{s}')_i$ 分配给参与者 $\rho(i)$.

不失一般性,设 P 中的某个子集 $G\subset AS_1\cap\cdots\cap AS_k$,若 $\boldsymbol{v}_j\in span(\boldsymbol{M}_G)$,$1\leqslant j\leqslant k$,则存在多项式时间算法计算出向量 $\boldsymbol{w}_j$,使得 $\boldsymbol{v}_j=\boldsymbol{w}_j\boldsymbol{M}_G$,$1\leqslant j\leqslant k$,于是 $y_j=\boldsymbol{v}_j\boldsymbol{s}'=(\boldsymbol{w}_j\boldsymbol{M}_G)\boldsymbol{s}'=\boldsymbol{w}_j(\boldsymbol{M}_G\boldsymbol{s}')$,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 双线性对

定义 4. 令 G_1,G_2 是具有大素数阶 p 的乘法循环群,且群中的离散对数问题都是困难问题,g 为 G_1 的生成元. 双线性对[4]是指满足下列性质的一个映射 $e:G_1\times G_1\to G_2$.

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

2) 非退化性:满足 $e(g,g)\neq 1$,其中 1 为循环乘法群 G_2 的幺元;

3) 可计算性:存在多项式算法计算 $e(g^a,g^b)$.

1.3 困难性假设

本文方案的安全性依赖于以下困难定义:

挑战者根据安全参数选取具有大素数阶 p 的群 G_1,令 $a,b,c\in_R\mathbb{Z}_p$,g 为 G_1 的生成元;给出多元组(g,g^a,g^b,g^c),有效区分 G_2 中的随机元 $Z\in G_2$ 与 $e(g,g)^{abc}\in G_2$ 的问题称为判定性 BDH 问题(DBDHP). 称输出为 $u\in\{0,1\}$的算法 $\mathcal{B}$ 解决 DBDH 问题的优势为 ε,若

$$|Pr[\mathcal{B}(g,g^a,g^b,g^c,T=e(g,g)^{abc})=0]-Pr[\mathcal{B}(g,g^a,g^b,g^c,T=Z)=0]|\geqslant\varepsilon.$$

定义 5. 称 DBDH 假设成立,若不存在多项式时间算法能以不可忽略的优势解决 DBDH 问题.

2 M-KP-ABE 安全模型

目前已有的文献,如文献[6-9]中提出的安全模型均只支持单主密钥功能性函数,其构造的 KP-ABE 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. 本节在其子类 KP-ABE 上定义具有更广义特性的多主密钥安全模型 M-KP-ABE,部分地解决多主密钥功能加密方案的构造问题. 该模型下用户能求解 $F:K_1\times K_2\times\cdots\times K_l\times X\to\{0,1\}^*$,能解密多种主密钥 K_j 加密的密文.

定义 6. 多主密钥策略属性基加密方案由以下 4 个算法组成:$\Sigma_{\text{M-KP-ABE}}=(\text{Setup},\text{Encrypt},\text{KeyGen},\text{Decrypt})$.

Setup:概率算法,输入安全参数,输出密钥生成中心(KGC)的 l 个主密钥对(PK_j,MK_j);

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

KeyGen:概率算法,输入多主密钥存取结构$\{AS_{j1},AS_{j2},\cdots,AS_{jk}\}$,多个主密钥$(MK_j)_{j\in\{j1,j2,\cdots,jk\}}$,输出解密密钥 D;

Decrypt: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挑战(selectively secure)和自适应选择明文攻击下(IND-CPA)的安全性,游戏分 6 个阶段.

1) Init:敌手出示所要挑战的属性集 γ^* 及主密钥 Y_j^*;

2) Setup:挑战者运行 Setup 算法,并将公开参数传送给敌手;

3) Phase1:敌手发起任意多主密钥存取结构,及相应的主密钥集合 H 的私钥询问,除了 $\gamma^* \in (\boldsymbol{M},\rho)$且 $Y_{j^*} \in H$;

4) Challenge:敌手提交 2 个等长的密文 M_0 和 M_1 给挑战者,挑战者抛掷公平硬币 b,用属性集 γ^* 和主密钥 Y_{j^*} 加密 M_b 得到目标密文 C^*,将 C^* 传给敌手;

5) Phase2:重复 Phase1 的询问;

6) Guess: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(IND-CCA).

定义 7. 称一个多主密钥 KP-ABE 方案 $\Sigma_{\text{M-KP-ABE}}$ 是安全的,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 基于 LMSSS 的 M-KP-ABE 方案

3.1 方案描述

单主密钥 KP-ABE 方案密钥中心 KGC 只拥有单个主密钥,根据用户属性为每个用户生成解密密钥,只要用户的存取结构满足密文的属性,就能解密.多主密钥 KP-ABE 方案的 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.根据已形式化定义的 M-KP-ABE 安全模型,结合以上定义的 LMSSS 方案,设计方案如下.

Setup(1^λ):定义全局属性 $U=\{1,2,\cdots,u\}$,对于任意 $i\in\mathcal{U}$,选取随机值 $t_i \in_R \mathbb{Z}_p$,计算 $T_i=g^{t_i}$;KGC 根据安全参数 λ 选取全局主私钥 $y_j \in_R \mathbb{Z}_p$,$j\in\{1,\cdots,l\}$,计算 $Y_j=e(g,g)^{y_j}$;

公开公钥 $PK=\{\{Y_j\}_{j\in(1,\cdots,l)},\{T_i\}_{i\in(1,\cdots,u)}\}$,保存私钥 $MK=\{\{t_i\}_{i\in(1,\cdots,u)},\{y_j\}_{j\in(1,\cdots,l)}\}$.

Encrypt(γ,m,Y_j):加密方选取属性集 $\gamma\subseteq\mathcal{U}$,$r\in_R\mathbb{Z}_p$,加密密文如下:

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

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

取分享向量为 $\boldsymbol{s}_u=\{r_1,\cdots,\overset{j1}{y_{j1}},\cdots,\overset{jk}{y_{jk}},r_{k+1},\cdots,r_n\}$,计算 $\boldsymbol{\lambda}=\boldsymbol{M}\boldsymbol{s}_u$ 得到分享值,计算 $D=\{\{d_i=g^{\frac{\lambda_i}{t_{\rho(i)}}}\}_{i\in(1,\cdots,m)}\}$,将其秘密传送给用户.

Decrypt(C,D):若 $Y_j\in H$,且 $\gamma\in(\boldsymbol{M},\rho)$,用户计算 $\boldsymbol{w}_j$,使得 $\boldsymbol{v}_j=\boldsymbol{w}_j\boldsymbol{M}_\gamma$,可恢复明文如下:

$$\prod_{i\in\gamma}e(c_i,d_{\rho^{-1}(i)})^{w_{j\rho^{-1}(i)}}=\prod_{i\in\gamma}e(g^{rt_i},g^{\frac{\lambda_{\rho^{-1}(i)}}{t_i}})^{w_{j\rho^{-1}(i)}}=\prod_{i\in\gamma}e(g,g)^{r\lambda_{\rho^{-1}(i)}w_{j\rho^{-1}(i)}}=e(g,g)^{r\sum_{i\in\gamma}\lambda_{\rho^{-1}(i)}w_{j\rho^{-1}(i)}}=e(g,g)^{ry_j}.$$

明显地,$m=c\Big/\prod_{i\in\gamma}e(c_i,d_{\rho^{-1}(i)})^{w_{j\rho^{-1}(i)}}$,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,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.当 $\boldsymbol{M}$ 为范德蒙德行列式时存取结构即为 Shamir 的(t,n)门限秘密共享体制,本文方案即为 FIBE 方案,本文的方案与文献[6]方案具有相同的效率.与文献[10]相比,本文的方案公开参数的长度随着属性的增加线性增加,但文献[10]的方案生成密钥时每个用户增加 3 个指数运算,加密时每个属性要多 1 个指数运算,解密时每个属性增加 1 个双线性对运算,因此本文的方案具有更高的计算效率.

与文献[7]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.构造方案与本文方案区别主要在:密钥生成时将按精细的访问树生成密钥,树中每个非叶节点都有一个存取结构$(\boldsymbol{M},\rho)$,$(\boldsymbol{M},\rho)$也可以是线性多秘密共享结构,标号函数 ρ 映射到子节点的标号;$\boldsymbol{M}$ 为 $n\times n$ 阶阵时为'与'结构,$\boldsymbol{M}$ 为 $n\times 1$ 阶阵时为'或'结构;叶子节点对应为属性,

生成秘密分享值的方法与本文定义的方法相同;解密算法需要回溯重构主密钥的过程.同上分析支持精细访问结构的方案效率与文献[7]相同.

3.3 安全性分析

根据第 2 节定义的安全性游戏,攻破本方案的优势可规约为解决 DBDH 问题的优势.

定理 1. 本文的方案是安全的,如果不存在多项式时间算法能以不可忽略的优势解决 DBDH 问题.

证明. 假设存在一个多项式有界的敌手 $\mathcal{A}$ 能以 ε 的优势攻破本文的方案,则能构造算法 $\mathcal{B}$ 以 $\varepsilon/2$ 的优势解决 DBDH 问题.游戏如下:

首先挑战者 $\mathcal{C}$ 选取具有大素数阶 p 的循环群 G_1,G_2,及相应的双线性映射 e,生成元 g. $\mathcal{C}$ 抛掷公平硬币 u,当 $u=0$ 时,设置 $(A,B,C,T)=(g^a,g^b,g^c,e(g,g)^{abc})$,否则设置 $(A,B,C,T)=(g^a,g^b,g^c,e(g,g)^z)$,其中 $a,b,c,z\in_R\mathbb{Z}_p$,将四元组传给 $\mathcal{B}$.

Init:敌手出示要挑战的属性集 γ^* 及主密钥 Y_{j^*}.

Setup:$\mathcal{B}$ 运行 Setup 算法,生成如下系统参数:敌手要挑战的主密钥设置为 $Y_{j^*}=e(A,B)=e(g,g)^{ab}$,对于其他主密钥设置为 $Y_j=e(g,B)^{y_j}$,$y_j\in_R\mathbb{Z}_p$,$j\in\{1,\cdots,j^*-1,j^*+1,\cdots,l\}$.为全局属性 $\mathcal{U}=\{1,2,\cdots,u\}$ 设置相应的公钥如下:对于任意 $i\in\gamma^*$,选取随机值 $t_i\in_R\mathbb{Z}_p$,计算 $T_i=g^{t_i}$;对于 $i\in\mathcal{U}-\gamma^*$,选取随机值 $\beta_i\in_R\mathbb{Z}_p$,计算 $T_i=B^{\beta_i}=g^{b\beta_i}$,公开参数给敌手.

Phase1:敌手发起任意存取结构 $\mathcal{M}(\boldsymbol{M},\rho)$ 及相应的主密钥集合 H 的私钥询问,有以下 3 种情况.

1) 当 $\gamma^*\in(\boldsymbol{M},\rho)$,$Y_{j^*}\in H$ 时,$\mathcal{B}$ 输出 $\perp$.

2) 当 $\gamma^*\notin(\boldsymbol{M},\rho)$,$Y_{j^*}\in H$ 时,设 $(\boldsymbol{M},\rho)$ 中满足 $\rho(i)\in\gamma^*$ 的个数为 $t<|\gamma^*|$,选取相应的分享值为随机值 $\lambda_i\in_R\mathbb{Z}_p$,则 $d_i=B^{\frac{\lambda_i}{t_{\rho(i)}}}$;在 $(\boldsymbol{M},\rho)$ 中任意选取其他 $n-t-|H|$ 行,选取相应的分享值为随机值 $\lambda_i\in_R\mathbb{Z}_p$,则 $d_i=g^{\frac{\lambda_i}{t_{\rho(i)}}}$.对于其他属性的密钥生成,根据已知的分享值 λ_i,计算秘密分享向量 $s=\{r_1,\cdots,y_{j1}^{j1},\cdots,a^{j^*},\cdots,y_{jk}^{jk},r_{jk+1},\cdots,r_n\}$ 中的 $n-|H|$ 个随机值 r_j 是可解的,详见附录 A,由于 y_j 已知,a 可由 A 代入求解,可计算其他属性的 λ_i,则 $d_i=g^{\frac{\lambda_i}{t_{\rho(i)}}}$.

3) 当 $Y_j^*\notin H$ 时,$\mathcal{B}$ 生成私钥如下:取分享向量为 $\boldsymbol{s}_u=\{r_1,\cdots,y_{j1}^{j1},\cdots,y_{jk}^{jk},r_{jk+1},\cdots,r_n\}$,计算 $\lambda=\boldsymbol{M}\boldsymbol{s}_u$ 得到分享值,对于 $\rho(i)\in\gamma^*$,$d_i=B^{\frac{\lambda_i}{t_{\rho(i)}}}$;对于 $\rho(i)\in\mathcal{U}-\gamma^*$,$d_i=g^{\frac{\lambda_i}{t_{\rho(i)}}}$.

敌手重复若干次询问.

Challenge:敌手提交 2 个等长的密文 M_0 和 M_1 给 $\mathcal{B}$,$\mathcal{B}$ 抛掷公平硬币 b,输出密文如下:

$$C^*=\{\gamma^*,Y_{j^*},c^*=M_bT,\{c_i=C^{t_i}\}_{i\in\gamma}\}.$$

当 $u=0$ 时,令 $r=c$,则 $Y_{j^*}^c=(e(g,g)^{ab})^c=e(g,g)^{abc}$,$c_i=g^{\alpha t_i}=(g^{t_i})^c$,即 C^* 是一个有效的密文;当 $u=1$ 时,c^* 为随机元,密文不包含 M_b 的任何信息.

Phase2:重复 Phase1 的询问.

Guess:敌手输出 b 的猜测值 b'.

若 $b'=b$,$\mathcal{B}$ 判断 $u'=0$;否则 $\mathcal{B}$ 判断 $u'=1$. $\mathcal{B}$ 成功解决 DBDH 问题的概率计算如下:

当 $u=0$ 时,则 C^* 为有效的密文,$\mathcal{A}$ 能以 ε 的优势攻破本文的方案,则 $Pr(b'=b|u=0)=\frac{1}{2}+\varepsilon$,由于 $b'=b$ 时 $\mathcal{B}$ 判断 $u'=u=0$,即 $Pr(u'=u|u=0)=\frac{1}{2}+\varepsilon$;当 $u=1$ 时,$\mathcal{A}$ 不能从密文中获得关于 b 的任何信息,即 $Pr(b'=b|u=1)=Pr(b'\neq b|u=1)=\frac{1}{2}$,由于 $b'\neq b$ 时 $\mathcal{B}$ 判断 $u'=u=1$ 则 $Pr(u'=u|u=1)=\frac{1}{2}$. 综上所述 $\mathcal{B}$ 解决 DBDH 问题的优势为:

$$Pr(u'=u)-\frac{1}{2}=\frac{1}{2}Pr(u'=u|u=0)+\frac{1}{2}Pr(u'=u|u=1)-\frac{1}{2}=\frac{1}{2}\left(\frac{1}{2}+\varepsilon\right)+\frac{1}{2}\cdot\frac{1}{2}-\frac{1}{2}=\frac{\varepsilon}{2}.$$

证毕.

4 结束语

本文首次解决了多主密钥形式功能性函数 $F:K_1\times K_2\times\cdots\times K_l\times X\to\{0,1\}^*$ 加密方案的构造问题,提出了 M-KP-ABE 安全模型;引入 LMSSS 设计了一个具有较强表达能力的方案;基于 DBDH 问题的困难性假设,在标准模型下证明方案在选择挑战和自适应选择明文攻击下是安全的;该方案具有更广义的特性和较高的效率.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,设计适应性安全的多主密钥功能加密方案也是一个重要方向.

参 考 文 献

[1] Lewko A, Okamoto T, Sahai A, et al. Fully secure functional encryption: Attribute-based encryption and (hierarchical) inner product encryption [G] //LNCS 6110: Proc of EUROCRYPT 2010. Berlin: Springer, 2010: 62-91

[2] Boneh D, Sahai A, Waters B. Functional encryption: Definitions and challenges [G] //LNCS 6597: Proc of TCC 2011. Berlin: Springer, 2011: 253-273

[3] Shamir A. Identity-based cryptosystems and signature schemes [G] //LNCS 196: Proc of CRYPTO 1984. Berlin: Springer, 1984: 47-53

[4] Boneh D, Franklin M. Identity based encryption from the Weil pairing [G] //LNCS 2139: Proc of CRYPTO 2001. Berlin: Springer, 2001: 213-229

[5] Cocks C. An identity based encryption scheme based on quadratic residues [C] //Proc of the 8th IMA Int Conf on Cryptography and Coding 2011. Berlin: Springer, 2001: 360-363

[6] Sahai A, Waters B. Fuzzy identity based encryption [C] // Proc of EUROCRYPT 2005. Berlin: Springer, 2005: 457-473

[7] Goyal V, Pandey O, Sahai A, et al. Attribute-based encryption for fine-grained access control of encrypted data [C] //Proc of ACM CCS 2006. New York: ACM, 2006: 89-98

[8] Ostrovsky R, Sahai A, Waters B. Attribute-based encryption with non-monotonic access structures [C] //Proc of ACM CCS 2007. New York: ACM, 2007: 195-203

[9] Tang Qiang, Ji Dongyao. Multi-authority verifiable attribute-based encryption [J]. Journal on Wuhan University: Nature Science Edition, 2008, 54(5): 607-610 (in Chinese)
(唐强, 姬东耀. 多授权中心可验证的基于属性的加密方案 [J]. 武汉大学学报: 理学版, 2008, 54(5): 607-610)

[10] Waters B. Ciphertext-policy attribute-based encryption: An expressive, efficient, and provably secure realization [G] // LNCS 6571: Proc of PKC 2011. Berlin: Springer, 2011: 53-70

[11] Goyal V, Jain A, Pandey O, et al. Bounded ciphertext policy attribute-based encryption [G] //LNCS 5126: Proc of ICALP 2008. Berlin: Springer, 2008: 579-591

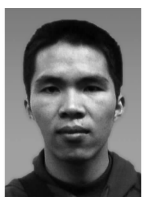
[12] Katz J, Sahai A, Waters B. Predicate encryption supporting disjunctions, polynomial equations, and inner products [G] // LNCS 4965: Proc of EUROCRYPT 2008. Berlin: Springer, 2008: 146-162

[13] Okamoto T, Takashima K. Fully secure functional encryption with general relations from the decisional linear assumption [G] //LNCS 6223: Proc of CRYPTO 2010. Berlin: Springer, 2010: 191-208

[14] Attrapadung N, Libert B. Functional encryption for inner product: Achieving constant-size ciphertexts with adaptive security or support for negation [G] //LNCS 6056: Proc of PKC 2010. Berlin: Springer, 2010: 384-402

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

Yang Xiaoyuan, born in 1959. Currently professor at the Engineering College of APF. His research interests include cryptography algorithm and protocol, and security of network (xyyangwj@126.com).



Cai Weiyi, born in 1986. Received his BSc degree in security of information and network from the Engineering College of APF. Since 2009 he has been a MSc candidate in cryptography. His current research interests include cryptography, provable security and cloud service(weiyi_i@yahoo.cn).

Chen Haibin, born in 1987. Received his BSc degree in security of information and network and MSc degree in cryptography from the Engineering College of APF. His research interests include information security and cryptography (hbchenwj@163.com).

附录 A

计算秘密分享向量 $\boldsymbol{s}=\{r_1,\cdots,\overset{j1}{y_{j1}},\cdots,\overset{j^*}{a},\cdots,\overset{jk}{y_{jk}},r_{jk+1},\cdots,r_n\}$ 中的 $n-|H|$ 个随机值 r_i，从 $(\boldsymbol{M},\rho)$ 中选取已确定 λ_i 的行构成子矩阵 $\boldsymbol{M}_t$，计算随机值 r_i 可由求解以下线性方程组得到：

$$\begin{bmatrix} m_{1,1} & m_{1,2} & \cdots & m_{1,n} \\ m_{2,1} & m_{2,2} & \cdots & m_{2,n} \\ \vdots & \vdots & & \vdots \\ m_{n-|H|,1} & m_{n-|H|,2} & \cdots & m_{n-|H|,n} \end{bmatrix} \boldsymbol{s}' = \begin{bmatrix} \lambda_1 \\ \lambda_n \\ \vdots \\ \lambda_{n-|H|} \end{bmatrix}.$$

在 $\boldsymbol{M}_t$ 中主密钥相对应的列移到右边得 $\boldsymbol{M}_r$：

$$\begin{bmatrix} m_{1,1} & m_{1,2} & \cdots & m_{1,n} \\ m_{2,1} & m_{2,2} & \cdots & m_{2,n} \\ \vdots & \vdots & & \vdots \\ m_{n-|H|,1} & m_{n-|H|,2} & \cdots & m_{n-|H|,n} \end{bmatrix} \begin{bmatrix} r_1 \\ r_2 \\ \vdots \\ r_n \end{bmatrix} =$$

$$\begin{bmatrix} \lambda_1 \\ \lambda_n \\ \vdots \\ \lambda_{n-|H|} \end{bmatrix} - y_{j1} \begin{bmatrix} m_{1,j1} \\ m_{2,j1} \\ \vdots \\ m_{n-|H|,j1} \end{bmatrix} - \cdots - a \begin{bmatrix} m_{1,j^*} \\ m_{2,j^*} \\ \vdots \\ m_{n-|H|,j^*} \end{bmatrix} - \cdots - y_{jk} \begin{bmatrix} m_{1,jk} \\ m_{2,jk} \\ \vdots \\ m_{n-|H|,jk} \end{bmatrix},$$

显然

$$\begin{bmatrix} r_1 \\ r_2 \\ \vdots \\ r_n \end{bmatrix} = (\boldsymbol{M}_r)^{-1} \left(\begin{bmatrix} \lambda_1 \\ \lambda_n \\ \vdots \\ \lambda_{n-|H|} \end{bmatrix} - y_{j1} \begin{bmatrix} m_{1,j1} \\ m_{2,j1} \\ \vdots \\ m_{n-|H|,j1} \end{bmatrix} - \cdots - a \begin{bmatrix} m_{1,j^*} \\ m_{2,j^*} \\ \vdots \\ m_{n-|H|,j^*} \end{bmatrix} - \cdots - y_{jk} \begin{bmatrix} m_{1,jk} \\ m_{2,jk} \\ \vdots \\ m_{n-|H|,jk} \end{bmatrix} \right),$$

将主密钥加入相应位置得到秘密分享向量 $\boldsymbol{s}$,对于$(\boldsymbol{M},\rho)$中的其他行,不失一般性取其中一行 $\boldsymbol{M}_h$,计算分享值 $\lambda_i=\boldsymbol{M}_h\boldsymbol{s}'$,则其相应的密钥

$$g^{\frac{\lambda_h}{\rho(h)}} = g^{\frac{m_{h,j1}y_{j1}+\cdots+m_{h,j^*}a+\cdots+m_{h,jk}y_{jk}+\begin{bmatrix} m_{h,1} & m_{h,2} & \cdots & m_{h,n} \end{bmatrix}(\boldsymbol{M}_r)^{-1}\left(\begin{bmatrix} \lambda_1 \\ \lambda_n \\ \vdots \\ \lambda_{n-|H|} \end{bmatrix} - y_{j1} \begin{bmatrix} m_{1,j1} \\ m_{2,j1} \\ \vdots \\ m_{n-|H|,j1} \end{bmatrix} - \cdots - a \begin{bmatrix} m_{1,j^*} \\ m_{2,j^*} \\ \vdots \\ m_{n-|H|,j^*} \end{bmatrix} - \cdots - y_{jk} \begin{bmatrix} m_{1,jk} \\ m_{2,jk} \\ \vdots \\ m_{n-|H|,jk} \end{bmatrix} \right)}{\rho(h)}} =$$

$$g^{\frac{m_{h,j1}y_{j1}+\cdots+m_{h,jk}y_{jk}+\begin{bmatrix} m_{h,1} & m_{h,2} & \cdots & m_{h,n} \end{bmatrix}(\boldsymbol{M}_r)^{-1}\left(\begin{bmatrix} \lambda_1 \\ \lambda_n \\ \vdots \\ \lambda_{n-|H|} \end{bmatrix} - y_{j1} \begin{bmatrix} m_{1,j1} \\ m_{2,j1} \\ \vdots \\ m_{n-|H|,j1} \end{bmatrix} - \cdots - y_{jk} \begin{bmatrix} m_{1,jk} \\ m_{2,jk} \\ \vdots \\ m_{n-|H|,jk} \end{bmatrix} \right)}{\rho(h)}} \cdot$$

$$g^{\frac{m_{h,j^*}a+a\begin{bmatrix} m_{h,1} & m_{h,2} & \cdots & m_{h,n} \end{bmatrix}(\boldsymbol{M}_r)^{-1}\begin{bmatrix} m_{1,j^*} \\ m_{2,j^*} \\ \vdots \\ m_{n-|H|,j^*} \end{bmatrix}}{\rho(h)}} =$$

$$g^{\frac{m_{h,j1}y_{j1}+\cdots+m_{h,jk}y_{jk}+\begin{bmatrix} m_{h,1} & m_{h,2} & \cdots & m_{h,n} \end{bmatrix}(M_r)^{-1}\left(\begin{bmatrix} \lambda_1 \\ \lambda_n \\ \vdots \\ \lambda_{n-|H|} \end{bmatrix} - y_{j1} \begin{bmatrix} m_{1,j1} \\ m_{2,j1} \\ \vdots \\ m_{n-|H|,j1} \end{bmatrix} - \cdots - y_{jk} \begin{bmatrix} m_{1,jk} \\ m_{2,jk} \\ \vdots \\ m_{n-|H|,jk} \end{bmatrix} \right)}{\rho(h)}} \cdot$$

$$A^{\frac{m_{h,j^*}+\begin{bmatrix} m_{h,1} & m_{h,2} & \cdots & m_{h,n} \end{bmatrix}(\boldsymbol{M}_r)^{-1}\begin{bmatrix} m_{1,j^*} \\ m_{2,j^*} \\ \vdots \\ m_{n-|H|,j^*} \end{bmatrix}}{\rho(h)}}.$$

综上所述能构造有效的密钥.