DOI：10.7652/xjtuxb201308008

密文策略的权重属性基加密方案

刘西蒙[1]，马建峰[2]，熊金波[2]，李琦[2]，张涛[2]
（1.西安电子科技大学通信工程学院，710071，西安；2.西安电子科技大学计算机学院，710071，西安）

摘要：在综合分析现有密文策略属性基加密方案的基础上，针对现有密文策略属性基加密方案较少考虑属性重要性的现状，将权重的概念引入到密文策略属性基加密方案中。授权机构依据属性在系统中的重要程度为其分配不同的权值，并依据属性的权值，通过属性转化算法将属性集合转化为属性权重分割集，利用线性秘密共享方法来实现密文策略权重属性基加密方案。提出了密文策略权重属性基加密方案的安全模型，在判定性双线性 Diffie-Hellman 指数假设下证明了该方案在标准模型下抵抗选择明文攻击的能力。密文策略权重属性基加密方案尽管在密文和密钥长度方面有所增加，但方案既可以支持细粒度的访问控制，又可以体现出属性的重要性，更加贴近于实际环境。

关键词：加密；访问控制；属性基加密；权重属性
中图分类号：TP309 **文献标志码**：A **文章编号**：0253-987X(2013)08-0044-05

Ciphertext-Policy Weighted Attribute Based Encryption Scheme

LIU Ximeng[1], MA Jianfeng[2], XIONG Jinbo[2], LI Qi[2], ZHANG Tao[2]
(1. School of Telecommunication Engineering, Xidian University, Xi'an 710071, China;
2. School of Computer Science and Technology, Xidian University, Xi'an 710071, China)

Abstract: The previous ciphertext-policy attribute based encryption scheme scarcely considers the significance of attributes. The concept of weight is thus introduced into the ciphertext-policy attribute based encryption scheme. The authority assigns different weights to attributes according to their importance in the system. The authority transfers the attribute set into weight attribute separation set according to the weight of attributes. Ciphertext-policy weighted attribute based encryption scheme is realized with linear secret sharing methods. And the security model of ciphertext-policy weighted attribute based encryption scheme is proposed. This scheme verifies the security against chosen-plaintext attack under the decisional bilinear Diffie-Hellman exponent (DBDHE) assumption in the standard model. Although the size of ciphertext and private key increases, the new scheme achieves fine-grained access control, and reflects the significance of attributes, which is more suitable for the practical applications.

Keywords: encryption; access control; attribute-based encryption; weighted attribute

随着互联网与云计算的发展，在开放的环境下进行数据共享与数据处理的需求越来越多。信息技术给人们带来方便的同时，也带来了安全方面的挑战[1]。数据的提供方在共享数据时不仅需要灵活的定制访问控制策略，而且要保证数据提供方与用户之间通信过程中保证数据的机密性。在云计算环境

收稿日期：2012-12-12。 作者简介：刘西蒙(1988—)，男，博士生；马建峰(通信作者)，男，教授，博士生导师。 基金项目：长江学者和创新团队发展计划资助项目(IRT1078)；国家自然科学基金重点资助项目(U1135002)；国家科技部重大专项资助项目(2011ZX03005-002)。
网络出版时间：2013-06-17 网络出版地址：http://www.cnki.net/kcms/detail/61.1069.T.20130617.1818.010.html

下迫切需要支持一对多的通信模式,从而降低每个用户加密数据所带来的巨大开销。虽然现有的广播加密技术可以解决部分效率问题,但是在现有的云计算环境下难以一次性获取接收群体的规模与成员的身份。

为了满足灵活的访问控制策略的同时保证数据的机密性,文献[2]首次引入属性基加密的概念。属性基加密的根源可以追溯到基于身份的密码学[3-7],基于身份的加密可以看成是属性基加密的一种特殊情况。文献[8]根据属性与策略是依附于密文还是用户的私钥上,提出了对基于属性加密方案的一种划分,即密钥策略基于属性的加密(KP-ABE)算法和密文策略的属性基加密(CP-ABE)算法。在 KP-ABE 算法中,密文与一个属性集相关联而密钥相对应于访问结构,只有当密文中的属性集满足私钥中的访问结构时,解密者才能获得相对应的明文。与 KP-ABE 算法对应,CP-ABE 中的密文与一个访问结构相关联而密钥对应与一个属性集合,只有私钥中的属性满足了密文中的访问结构时才能获得明文。文献[9]采用了与门表示访问策略,首次在判定双线性 Diffie-Hellman(DBDH)假设下证明了 CP-ABE 机制的安全性。文献[10]采用树形结构来表示灵活的访问控制策略,其安全性的证明基于一般的群假设。文献[11]采用线性秘密共享方案(LSSS)访问结构与判定并行性双线性 Diffie-Hellman 假设(q-BDHE),直接实现了支持与门、或门和门限操作的 CP-ABE 机制。文献[14]提到用链状权重秘密共享方案来构造属性基加密,但是用链状 Mignotte 序列来构造访问控制树局限性比较大,并且文中没有安全性证明。虽然现在有很多的属性基加密方案,但是这些方案都有一个共同的特点,很少考虑到属性的重要性,也就是说,属性之间的地位是平等的。由于每一个属性在系统中所担任的角色不同,相应的他们在系统中所具有的发言权也不同。因此,在现实的生活中,属性带有权值是具有实际意义的。与之前的属性基加密方案相比,我们将属性的权重引入到系统中,这样使方案更加贴近于实际情况,并且对现实系统是具有实际意义的。所构造的方案可以支持属性权重的同时在标准模型下可抵御不可区分选择的明文攻击。

1　预备知识

1.1　访问结构

定义 1　(访问结构[12])　令$\{P_1,P_2,\cdots,P_n\}$为参与者的集合,对于聚集 $A\subseteq 2^{\{P_1,P_2,\cdots,P_n\}}$,如果 $\forall B,C$:若 $B\in A$ 且 $B\subseteq C$,有 $C\in A$,那么称 A 是单调的。访问结构 A 是非空参与者的子集构成的集合。设 D 表示参与者的任一子集,如果 $D\in A$,叫做授权集合,如果 $D\notin A$,那么叫做非授权集合。

1.2　线性秘密共享方案

定义 2　(线性秘密共享方案(LSSS)[12])　秘密分享方案 Π 是相对于参与者的集合来说如果是线性的,且有:

(1)每个参与者的共享为 Z_p 上的一个向量;

(2)存在一个 l 行 n 列的矩阵 $\boldsymbol{M}$ 叫做方案 Π 的共享生成矩阵。对于所有的 $i=1,\cdots,l$,函数 f 定义参与者的行标签为 $f(i)$。当考虑到列向量 $\boldsymbol{v}=(s,r_2,r_3,\cdots,r_n)$,其中 $s\in Z_p$ 为需要共享的秘密信息,$r_2,r_3,\cdots,r_n$ 在 Z_p 上随机选择,那么向量 $\boldsymbol{Mv}$ 就为方案 Π 的 l 个共享,共享$(\boldsymbol{Mv})_i$ 属于第 $f(i)$个参与者。

那么我们说秘密分享方案在 Z_p 上是线性的。

文献[12]说明了对于每一个线性秘密共享方案,上述的定义具有线性重构的性质。线性重构的性质描述如下:方案 Π 对于访问结构 A 来说是 LSSS,令 $S\in A$ 为授权集合,并且对于 $I\subset\{1,2,\cdots,l\}$,令 $I=\{i:f(i)\in S\}$,那么存在常数$\{k_i\in Z_p\}_{i\in I}$如果$\{\gamma_i\}$为方案 Π 秘密 s 的合法共享,那么有 $\sum_{i\in I}k_i\gamma_i=s$。对于任何未授权的行向量的集合 I,目标向量并不在行向量集合 I 所张成的空间中。此外,对于所有的 $i\in I$,存在向量 $\boldsymbol{\omega}$ 使得 $\boldsymbol{\omega}\cdot(1,0,\cdots,0)=-1$ 并且 $\boldsymbol{\omega}\cdot\boldsymbol{M}_i=0$。

1.3　双线性对

令 G 和 G_T 是以素数阶为 p 的循环群,设 g 是 G 的生成元,并且 e 为双线性映射 $e:G\times G\rightarrow G_T$。双线性映射有以下的性质。

(1)双线性性:对于所有的 $x,y\in G$ 和 $c,d\in Z_p$,有 $e(x^c,y^d)=e(x,y)^{cd}$。

(2)非退化性:$e(g,g)\neq 1$。

如果对于群 G 中的运算和双线性运算 $e:G\times G\rightarrow G_T$ 都可以有效计算,那么称 G 是双线性群。注意到 $e(*,*)$是对称操作,也就是说,$e(x^c,y^d)=e(x,y)^{cd}=e(x^d,y^c)$。

1.4　判定双线性 Diffie-Hellman 指数假设

定义判定双线性 Diffie-Hellman 指数问题(DBDHE)如下,系统根据安全参数选择素数阶为 p 的循环群 G。令 a、s 为 Z_p 上随机选择的参数,g 为

群 G 的生成元。当将 $\boldsymbol{y}=(g,g^{a},\cdots,g^{a^{q}},g^{a^{q+2}},\cdots,g^{a^{2q}},g^{s})$ 给敌手，敌手必须可以将 $e(g,g)^{a^{q+1}s}\in G$ 与 G 中的任意一个元素区分。

模拟器 $\mathcal{B}$ 以优势在 G 中解决 DBDHE 问题并输出，若

$$\left|\Pr[\mathcal{B}(\boldsymbol{y},T=e(g,g)^{a^{q+1}s})=0]-\Pr[\mathcal{B}(\boldsymbol{y},T=R)=0]\right|\geqslant\varepsilon$$

定义 3 若没有多项式时间的算法以不可忽略的优势来解决 DBDHE 问题，我们称 DBDHE 假设成立。

2 密文-策略权重属性基加密算法框架与安全模型

2.1 算法框架

基于权重密文-策略属性基加密包含 5 个算法：属性集转化，系统建立，加密算法，密钥生成，解密算法。

属性集转化(Γ)：属性集转化算法输入为全体属性集 Γ，由于系统中的每一个属性都具有不同的权值，可信中心对系统中的每一个属性都分配一个系统允许的最大权值，然后依据权值将全体属性集 Γ 转变为全体属性权重分割集 Γ^{*}。

系统建立($1^{\lambda},\Gamma^{*}$)：可信中心根据安全参数 1^{λ} 与全体属性权重分割集 Γ^{*} 运行系统建立算法，生成并且输出公钥 P_{K} 和主密钥 M_{K}。

加密算法(P_{K},m,A)：发送者将公钥参数 P_{K}，消息 m 和访问结构 A 输进加密算法。加密算法用公钥参数 P_{K} 加密消息 m，生成密文 C_{T}，其中密文中包含了访问结构 A。只有当用户所具有的属性的分割集满足了访问结构，才能正确解密消息。

密钥生成算法(M_{K},S^{*})：可信中心将主密钥 M_{K} 与用户对应的属性分割集 S^{*} 输入到密钥生成算法中，输出为属性分割集 S^{*} 所对应的私钥 S_{K}。

解密算法($P_{\mathrm{K}},C_{\mathrm{T}},S_{\mathrm{K}}$)：当接收者收到密文后，将公钥参数 P_{K}、密文 C_{T}、以及私钥 S_{K} 输入到解密算法中，当私钥中包含的属性分割集 S^{*} 满足了密文中的访问结构 A，那么算法就可以正确解密恢复出消息 m。

2.2 安全模型

本小节给出基于权重密文-策略属性基加密的标准模型来抵御不可区分的选择访问结构和选择明文攻击(IND-sAcc-CPA)。本文给出的安全模型需要敌手在模拟器运行系统建立算法之前将提交需要挑战的访问结构。

初始化：敌手 $\mathcal{A}$ 产生需要挑战的访问结构 A^{*}，并将 A^{*} 输入到算法中。

属性集转化：模拟器 $\mathcal{B}$ 运行属性集转化算法，将全体属性集 Γ 转变成全体属性权重分割集 Γ^{*}。

系统建立：模拟器 $\mathcal{B}$ 运行系统建立算法，输入为全体属性的分割集，将运行算法后输出的公钥参数 P_{K} 交给 $\mathcal{A}$。

阶段 1：$\mathcal{A}$ 选择属性分割集 $S_{1}^{*}\cdots S_{q_1}^{*}$ 交给模拟器 $\mathcal{B}$，其中 $S_{1}^{*}\cdots S_{q_1}^{*}$ 不满足访问结构 A^{*}。$\mathcal{B}$ 根据 $S_{1}^{*}\cdots S_{q_1}^{*}$ 生成对应私钥，并将生成的私钥传给敌手。

挑战：$\mathcal{A}$ 提交给两个相同长度的密文 m_0 和 m_1，并且 $\mathcal{A}$ 提交挑战访问结构 A^{*}，使得阶段 1 所对应的属性分割集 $S_{1}^{*}\cdots S_{q_1}^{*}$ 都不满足这个访问结构 A^{*}。$\mathcal{B}$ 随机掷硬币 $b\leftarrow\{0,1\}$，在访问结构 A^{*} 下加密消息 m_{b}，将密文 C_{T}^{*} 提交给敌手。

阶段 2：与阶段 1 相同，$\mathcal{A}$ 选择的属性分割集 $S_{q_1+1}^{*}\cdots S_{q}^{*}$ 不满足访问结构 A^{*}，并将其传给 $\mathcal{B}$。$\mathcal{B}$ 根据 $S_{q_1+1}^{*}\cdots S_{q}^{*}$ 生成对应私钥，并将生成的私钥传给敌手。

猜测：敌手猜测 $b'\leftarrow\{0,1\}$。

敌手 $\mathcal{A}$ 在 IND-sAcc-CPA 游戏中的优势定义为 $\mathcal{A}_{\mathrm{Adv}}=\Pr[b'=b]-\frac{1}{2}$

定义 4 如果对于所有的多项式时间的敌手赢得上述游戏的优势至多可忽略的，那么称基于权重密文-策略属性基加密是 IND-sAcc-CPA 安全的。

3 密文策略的权重属性基加密

考虑实际的应用环境中，每个属性值的地位可能并不相同，本文将权重的概念引入到属性基加密中。系统中用户的每一个属性都被分配了一个权值，只有当密钥中所含有的属性满足密文中的访问结构时，才可以正确解密。文献[13]证明了任何的权重门限访问结构都可以定义权重为自然数的门限访问结构，因此本文仅考虑属性的权重值为自然数，算法实现如下。

属性集转化(Γ)：属性集转化算法输入为系统中的全体属性，可信中心依据属性在系统中重要程度的不同，分配不同的权值。对于全体属性集 $\Gamma=\{\lambda_1,\lambda_2,\cdots,\lambda_r\}$ 中的每一个属性 λ_i，分配属性 λ_i 允许在系统中的最大权值为 $\theta_i=w(\lambda_i)$，注意到这里的权值仅是整数。将属性集 Γ 中的每一个属性 λ_i，依据权重进行分割，分割后属性 λ_i 对应于 $(\lambda_i,1)\cdots(\lambda_i,\theta_i)$，设定分割后的最小的份额为 1，其构成的集合称为全体属性权重的分割集 Γ^{*}。

系统建立$(1^\lambda,\Gamma^*)$:将全体属性权重的分割集Γ^*输入到系统建立算法中。选择素数阶p的群G,记$u=\sum_i\theta_i$。系统随机选择$h_1,\cdots,h_u\in G$,此外随机地选定指数$a,\alpha\in Z_p$,那么公钥就为

$$P_{\mathrm{K}}=\{g,e(g,g)^{\alpha},g^{a},h_1,\cdots,h_u\}$$

主密钥为

$$M_{\mathrm{K}}=g^{\alpha}$$

加密算法$(P_{\mathrm{K}},m,(\boldsymbol{M},f))$:加密算法输入参数为公钥参数$P_{\mathrm{K}}$、消息$m$和LSSS矩阵访问结构$(\boldsymbol{M},f)$,函数$f$将属性权重的最小份额与$\boldsymbol{M}$中行对应起来。将矩阵的第$i$个位置对应于属性$\lambda_c$的第$\theta_t$个权重分割位置,即$f(i)\rightarrow(\lambda_c,\theta_t)$。

令$\boldsymbol{M}$为$l\times n$的矩阵,算法首先在Z_p^n上选择一随机的行向量$\boldsymbol{v}=(s,y_2,y_3,\cdots,y_n)$,这些值用于分享加密元素$s$。对于$i=1,\cdots,l$,计算$\gamma_i=\boldsymbol{v}\cdot\boldsymbol{M}_i$,其中$\boldsymbol{M}_i$对应于$\boldsymbol{M}$的第$i$行。

密文公布为

$$C_{\mathrm{T}}=\{C=me(g,g)^{\alpha s},C^*=g^s,$$
$$C_1=g^{a\gamma_1}h_{f(1)}^{-s},\cdots,C_l=g^{a\gamma_l}h_{f(l)}^{-s}\}$$

密钥生成(M_{K},S^*):密钥生成算法输入为主密钥和属性权重的分割集S^*,算法首先随机地选择$t\in Z_p$,生成的私钥为

$$S_{\mathrm{K}}=\{K=g^{\alpha}g^{at},L=g^t,\forall x\in S^*:K_x=h_x^t\}$$

解密算法$(P_{\mathrm{K}},C_{\mathrm{T}},S_{\mathrm{K}})$:解密算法输入为密文$C_{\mathrm{T}}$与私钥$S_{\mathrm{K}}$。$I\subset\{1,2,\cdots,l\}$定义$I=\{i:f(i)\in S^*\}$,假定属性权重的分割集$S^*$满足了LSSS访问结构,那么存在$\{k_i\in Z_p\}$,使得$\sum_{i\in I}k_i\gamma_i=s$。注意到可能有多种不同的选择$k_i$来满足上述等式。

解密算法首先计算

$$S_{\mathrm{S}}=e(C^*,K)/\Big(\prod_{i\in I}(e(C_i,L)e(C^*,K_{f(i)}))^{k_i}\Big)=$$
$$e(g,g)^{\alpha s}e(g,g)^{ast}/\Big(\prod_{i\in I}e(g,g)^{a\alpha\gamma_ik_i}\Big)=e(g,g)^{\alpha s}$$

通过S_{S}可以解密消息:$m^*=C/S_{\mathrm{S}}$

4　安全性证明

定理　假定DBDHE假设成立,那么没有多项式时间的敌手以大小$l^*\times n^*$的挑战矩阵来选择性的攻破我们的系统,其中$n^*\leqslant q$。

证明　假定敌手选定一个维数至多为q的挑战矩阵$\boldsymbol{M}^*$,我们来构造模拟器$\mathcal{B}$。

初始化:模拟器输入为DBDHE挑战$\boldsymbol{y}=(g,g^{a},\cdots,g^{a^{q}},g^{a^{q+2}},\cdots,g^{a^{2q}})$和$T$。敌手将挑战结构$(\boldsymbol{M}^*,f^*)$输入算法,其中$\boldsymbol{M}^*$列数为$n^*$($n^*\leqslant q$)。

属性集分割:模拟器将属性集Γ中的每一个属性λ_i,依据权重θ_i进行分割,其构成的集合称为属性权重的分割集Γ^*,记$u=\sum_i\theta_i$。

系统建立:模拟器在Z_p上随机的选择元素α',并且令$\alpha=\alpha'+a^{q+1}$,那么$e(g,g)^{\alpha}=e(g^{\alpha},g^{a^q})e(g,g)^{\alpha'}$。

下面,使用模拟器来模拟参数$h_1,\cdots,h_u$。对于从1到u的每一个x,选择一个随机的$z_x\in Z_p$,若存在i,使得$f^*(i)=x$,那么令$h_x=g^{z_x}g^{aM_{i,1}^*}g^{a^2M_{i,2}^*}\cdots g^{a^{n^*}M_{i,n^*}^*}$。若不存在$i$使得$f^*(i)=x$,那么令$h_x=g^{z_x}$。注意到$f^*$是单射函数,对于任意的$x$,至多有一个$i$使得$f^*(i)=x$。

阶段1:在这一阶段,模拟器模拟私钥。假定模拟器被给予一个对于集合S的私钥的询问,其中S不满足$\boldsymbol{M}^*$。

模拟器选定一个随机数$r\in Z_p$,当S不满足集合$\boldsymbol{M}^*$时,找到一个向量$\boldsymbol{\omega}=(\omega_1,\cdots,\omega_{n^*})\in Z_p^{n^*}$使得$\omega_1=-1$,并且对于所有的$i$,$f^*(i)\in S$有$\boldsymbol{\omega}\cdot\boldsymbol{M}_i^*=0$。由LSSS的定义可知,这样的向量是存在的。

模拟器定义

$$t=r+\omega_1a^q+\omega_2a^{q-1}+\cdots+\omega_{n^*}a^{q-n^*+1}$$

那么

$$L=g^t=g^r\prod_{i=1\cdots n^*}(g^{a^{q+1-i}})^{\omega_i}$$

由t的定义可知,g^{at}中包含项$g^{a^{q+1}}$,用g^{α}将$g^{a^{q+1}}$项消去。模拟器计算出

$$K=g^{\alpha}g^{at}=g^{\alpha'}g^{ar}\prod_{t=2,\cdots,n^*}(g^{a^{q+1-i}})^{\omega_i}$$

对于$\forall x\in S$,若不存在i使得$f^*(i)=x$,则令$K_x=L^{z_x}$。对于$\forall x\in S$,若存在i使得$f^*(i)=x$,使用模拟器来计算$K_x=h_x^t$。由于$h_x=g^{z_x}g^{aM_{i,1}^*}g^{a^2M_{i,2}^*}\cdots g^{a^{n^*}M_{i,n^*}^*}$且$t=r+\omega_1a^q+\omega_2a^{q-1}+\cdots+\omega_{n^*}a^{q-n^*+1}$。那么$K_x$的指数中应当包含$a^jM_{i,j}^*\cdot\omega_ja^{q+1-j}$。当$f^*(i)\in S$时,有$\boldsymbol{M}_i^*\cdot\boldsymbol{\varepsilon}=0$,那么指数上带有$a^{q+1}$在结合的时候都会被消去。

使用模拟器计算出

$$K_x=L^{z_x}\prod_{j=1,\cdots,n^*}\Big(g^{a^j\cdot r}\prod_{k=1,\cdots,n^*;k\neq j}(g^{a^{q+1+j-k}})^{\omega_i}\Big)^{M_{i,j}^*}$$

挑战:建立挑战密文,敌手将两个消息m_0和m_1给模拟器。模拟器随机掷硬币$b\leftarrow\{0,1\}$,产生$C=m_be(g,g)^{\alpha s}=m_bTe(g,g)^{\alpha' s}$与$C'=g^s$。

使用模拟器来模拟$C_i=h_{f^*(i)}^s$,由于其中含有g^{a^js},模拟器不知道如何模拟。模拟器随机地选择$y_2',\cdots,y_{n^*}'\in Z_p$,用$\boldsymbol{v}=(s,sa+y_2',\cdots,sa^{n^*}+y_{n^*}')$

$\in Z_{p^{n^*}}$ 来分享秘密值。那么

$$C_i = g^{a\lambda_i} h_{f^{*(i)}}^{-s} = g^{asM_{i,1}^*} g^{(sa^2+y_2'a)M_{i,2}^*} \cdots$$

$$g^{(sa^{n^*}+y_{n^*}'a)M_{i,n^*}^*} g^{-sZ_{f^*(i)}} g^{-saM_{i,1}^*} \cdots g^{-sa^{n^*}M_{i,n^*}^*}$$

故 $C_i = g^{-sZ_{f^*(i)}} \left(\prod_{j=2,\cdots,n^*} (g^a)^{M_{i,j}^* y_j'} \right)$

阶段 2：与阶段 1 相同。

猜测：敌手最终输出他的猜测 b'。若 $b=b'$，模拟器输出 0 并且回答 $T=e(g,g)^{a^{q+1}s}$，否则模拟器输出 1 并且回答 G 中的一个随机值。

当 T 是 DBDHE 元组时，$\Pr[\mathcal{B}(\boldsymbol{y}, T=e(g,g)^{a^{q+1}s})=0]=\frac{1}{2}+\mathcal{A}_{\mathrm{Adv}}$，当 T 是随机的时候，$\Pr[\mathcal{B}(\boldsymbol{y}, T=R)=0]=\frac{1}{2}$。由于 A 以不可忽略的优势攻破方案，那么 $\mathcal{B}$ 也以不可忽略的优势来模拟 DBDHE 游戏。

5 方案分析

文献[2]方案给出的访问结构为门限结构，当用户私钥的属性集与密文相关的属性集相交的属性集超过门限值时，该用户可以解密密文。由于文献[2]方案不能达到细粒度的访问控制，文献[8]方案使用访问控制树来达到细粒度的访问控制。当私钥中的访问控制树与密文相关联的属性相匹配时，用户就可以解密密文。文献[11]方案用线性秘密共享方案矩阵作为访问控制策略，LSSS 方案在保证安全性的同时又能提高效率。以上的方案都没有考虑到属性权重的问题，本文提出的方案不仅可以达到细粒度的访问控制，并且可以体现出属性的重要性。将本文方案与文献[2,8,11]方案相比较，其中 n 为访问公式的大小，A 为用户密钥中属性的数量，$k_{\max}$ 为所有属性中权重的最大值，比较结果如表 1 所示。虽然本文方案在密文与密钥长度方面有所增加，但是其仅支持细粒度的访问控制，并且支持权重属性。

表 1 几种方案使用特性的比较

方案	密文长度	密钥长度	使用的假设	可否达到细粒度访问控制	属性是否带权重
文献[2]方案	$O(n)$	$O(A)$	一般群	×	×
文献[8]方案	$O(n)$	$O(A)$	BDH	√	×
文献[11]方案	$O(n)$	$O(A)$	q-BDHE	√	×
本文方案	$O(n^2)$	$O(A^{k_{\max}})$	DBDHE	√	√

由于本文方案更贴近于实际环境，我们认为这些开销是值得的。

6 结 论

在实际的环境中权重是一个值得考虑的方面，将权重引入到方案中可以更加贴近于实际情况。本文根据当前密文策略属性基加密方法，将权重的概念引入到属性中，提出了一种更符合实际情况的基于权重的密文策略的属性加密方案及安全模型，并证明在标准模型下的安全性。本文提出的基于权重的密文策略的属性加密方案仅仅考虑 LSSS 访问结构，下一步的研究工作的重点是将其他的访问结构引入到我们的方案中，如树形访问结构。

参考文献：

[1] ARMBRUST M, FOX A, GRIFFITH R, et al. A view of cloud computing [J]. Communications of the ACM, 2010, 53(4): 50-58.

[2] SAHAI A, WATERS B. Fuzzy identity-based encryption [M]// LNCS: Volume 3494 Advances in Cryptology-EUROCRYPT 2005. Berlin, Germany: Springer-Verlag, 2005: 557-557.

[3] BONEH D, FRANKLIN M. Identity-based encryption from the Weil pairing [M]// LNCS: Volume 2139 Advances in Cryptology-CRYPTO 2001. Berlin, Germany: Springer-Verlag, 2001: 213-229.

[4] BONEH D, BOYEN X. Efficient selective-ID secure identity-based encryption without random oracles [M]// LNCS: Volume 3027 Advances in Cryptology-EUROCRYPT 2004. Berlin, Germany: Springer-Verlag, 2004: 223-238.

[5] BONEH D, BOYEN X. Secure identity based encryption without random oracles [M]// LNCS: Volume 3152 Advances in Cryptology-CRYPTO 2004. Berlin, Germany: Springer-Verlag, 2004: 443-459.

[6] WATERS B. Efficient identity-based encryption without random oracles [M]// LNCS: Volume 3494 Advances in Cryptology-EUROCRYPT 2005. Berlin, Germany: Springer-Verlag, 2005: 557-557.

[7] 杨旸，胡予濮，张乐友，等. 标准模型下可证明安全的分级身份签名方案 [J]. 西安交通大学学报，2011，45(2)：27-33.
YANG Yang, HU Yupu, ZHANG Leyou, et al. Provable secure hierarchical identity based signature scheme in the standard model [J]. Journal of Xi'an Jiaotong University, 2011, 45(2): 27-33.

(下转第 86 页)