隐藏访问结构的密文策略的属性基加密方案

汪海萍 赵晶晶
(河海大学计算机与信息学院 南京 211100)

摘 要 在密文策略的属性基加密方案中,用户的私钥与属性集合关联,密文与访问策略关联,当且仅当用户私钥中所包含的属性满足嵌入在密文中的访问策略时,用户方能成功解密该密文。在现有方案的解密过程中,访问策略连同密文被发送给解密者,这意味着加密者的隐私被泄露。为解决该问题,提出了具有隐藏访问策略的密文策略属性基加密方案,以保护加密者的隐私;并基于DBDH假设,证明了该方案在标准模型中是选择明文安全的。

关键词 属性基加密,隐藏访问策略,DBDH假设,选择明文安全
中图法分类号 TP309 **文献标识码** A **DOI** 10.11896/j.issn.1002-137X.2016.2.038

Ciphertext-policy Attribute-based Encryption with Anonymous Access Structure

WANG Hai-ping ZHAO Jing-jing
(School of Computer and Information, Hohai University, Nanjing 211100, China)

Abstract In ciphertext-policy attribute-based encryption(CP-ABE) scheme, a user's secret key is associated with a set of attributes, and the ciphertext is associated with an access policy. The user can decrypt the ciphertext if and only if the attribute set embedded in his secret key satisfies the access policy specified in the ciphertext. In the present schemes, the access policy is sent to the decryptor along with the ciphertext, which means that the privacy of the encryptor is revealed. In order to solve such problem, we proposed a CP-ABE scheme with anonymous access policy, which is able to preserve the privacy of the encryptor. Our new scheme is proved to be selectively secure against chosen-plaintext attack under DBDH assumption in the standard model.

Keywords Attribute-based encryption, Anonymous access policy, DBDH assumption, Chosen-plaintext secure

1 引言

为了实现加密数据的细粒度访问控制,Sahai等人[1]首次提出了一种新的公钥密码学概念——属性基加密,该机制实现了公钥密码体系的一对多加密。之后,Goyal等人[2]进一步明确了属性基加密的概念,将属性基加密分为两大类:密钥策略的属性基加密和密文策略的属性基加密。对于密钥策略的属性基加密,密钥与访问结构相关,而密文与属性集相关;相反,密文策略的属性基加密将密文和访问结构关联,将密钥和属性基关联[3-5]。其中,对于密文策略的属性加密方案,加密者使用访问结构加密消息,解密者根据自身所拥有的属性预先从一个可信的授权方(Trusted Authority, TA)获取解密密钥,如果解密者本身的属性不满足嵌入在密文中的访问结构,解密者将不能解密该密文。形象地说,假设一个情景,Alice想要在某征婚网站上找男朋友,她希望只有能够满足她所提条件的男士可以访问她的详细信息,从而可以避免不必要的打扰,则Alice可使用访问结构 $W=$[男 $\wedge$ (年龄 25—35) $\wedge$ 博士]来加密她的私人详细信息;同时,假设用户Bob在该征婚网站根据个人信息注册,被标识属性集合 $S=$(男 $\wedge$ 年龄 28 $\wedge$ 硕士),经授权方认证后获取与其属性集合相对应的私钥。很明显,Bob私钥对应的属性集不满足嵌入在Alice私人信息密文中的访问结构,因此,Bob不能访问Alice的个人详细信息。

为了进一步保护用户的隐私,Kapadia等人[6]提出了隐藏访问结构的密文策略基于属性加密方案,同时在访问结构的表达能力上,该方案能做到与文献[7]中给出的方案一样丰富,但存在安全性的不足。因此,Nishide等人[8]在此基础上提出了选择安全的两个方案,这两个方案均只能实现部分隐藏访问结构。Müller等人[9]在其中一个方案上使用了一个新颖的基于树的访问结构技术,将原与门访问结构变成与之对应的布尔表达式,从而实现了完全隐藏访问结构。考虑到基于树的访问结构的表达能力的丰富性,Xu等人[10]提出了基于树的隐藏访问结构的密文策略属性基加密方案,并将该方案应用于云计算中。在隐藏访问结构的密文策略基于属性加密方案中,加密者使用一个隐藏访问结构来加密消息,解密者根据自身所拥有的属性预先从一个TA获取解密密钥,如果解密者本身的属性不满足嵌入在密文中的访问结构,解密者将不能解密该密文,也不能获得任何有关嵌入在密文中访问结构的信息。隐藏访问结构的基于属性密码体制是一个非常值得关注的研究课题,因为访问结构中可能包含敏感信息,在

到稿日期:2015-05-11 返修日期:2015-08-11
汪海萍(1989—),女,硕士,主要研究方向为基于属性加密,E-mail:761248339@qq.com;赵晶晶(1990—),女,硕士,主要研究方向为在线/离线签密,E-mail:565474418@qq.com。

某种特殊的使用背景下，若不能实现访问结构的隐藏，可能会造成严重的安全隐患。隐藏访问结构的基于属性加密方案使嵌入在密文中的访问结构对于解密者而言是隐藏的，从而可以更好地保护加密者的隐私。但是，前面提到的方案只能实现选择性安全，并不是完全意义上的安全。为了实现方案的完全安全，Waters 等人[11]第一次提出了使用双系统加密机制来做到隐藏访问结构的功能，然而，该方案是在基于身份的环境下实现的，也就不能拥有基于属性加密机制的一对多加密优势。因而，Lai 等人[12]鉴于 Waters 等人[11]的工作，结合双系统加密技术，提出了一个隐藏访问结构的密文策略基于属性加密方案。然而，在以上的方案[6-12]中，密文长度和双线性对运算数量与属性数量成正比，这就增加了系统的通信代价，降低了系统运行的效率。为降低方案的通信代价，文献[13，14]提出了固定密文长度的密文策略基于属性加密方案。文献[15]利用文献[9]的安全模型，以文献[13]的方案为基础提出了一个改进的固定密文长度的隐藏访问结构的密文策略属性基加密方案。为了进一步扩充隐藏访问结构的密文策略属性基加密方案的实用性，在 Zhang 等人[16]提出的谓词加密方案的基础上，Mukti 等人[17]将关键字搜索的功能加入到属性基加密方案中。

在隐藏访问结构的密文策略基于属性加密方案中，密文长度和双线性对运算数量都比较多，因此，此类方案的效率通常不是很高。另一方面，一些密文策略的基于属性加密方案尽管比较高效，但是它们不能实现访问结构的隐藏性。为此，本文方案在效率和访问结构隐藏性之间做了一个折中。

本文构造了一个能实现访问结构隐藏的密文策略基于属性加密方案，并在现有的方案基础上对方案的运行效率做了一定的改进。在本方案中，加密者在访问树的帮助下预先将访问结构嵌入到密文中，并使用多值与门来表达访问结构，访问结构中的每个属性 w_i 可以取多个值，从而增加了系统的灵活性；而且，使用了一种简单的方法来将加密者需要嵌入到密文中的访问结构转换成一个 n 元的访问树，访问树的叶子节点代表属性，而中间节点代表与或门运算符。在系统中，解密者获得的信息仅为他自己是否有解密该密文的能力，而关于其他任何能够解密该密文的解密者信息一概不知，因为访问结构被隐藏在了密文当中。同时，基于 DBDH 安全性假设(Decisional Bilinear Diffie-Hellman Assumption，判定双线性 Diffie-Hellman 假设)，给出了方案的安全性分析，证明其是选择明文安全的；并将本文提出的方案与现有相关工作作了对比分析，指出本方案的优势与不足。

本文第 2 节主要介绍使用到的一些基础知识；第 3 节给出一个具有隐藏访问结构的密文策略基于属性加密方案的具体构造；第 4 节给出该方案的安全性证明；第 5 节从系统参数长度、效率和安全性等方面，将本文方案同其它现有方案作了比较分析；最后总结全文。

2 预备知识

2.1 双线性对

令 p 为素数，G，G_T 是阶为 p 的乘法循环群，g 是 G 的生成元，若存在映射 $e:G\times G\rightarrow G_T$ 满足以下性质，则此映射为双线性映射。

1)可计算性(Computability)：存在有效的算法对任意的 $u,v\in G$ 计算 $e(u,v)$ 的值。

2)双线性(Bilinearity)：对于任意的 $u,v\in G$ 和 $a,b\in Z_p^*$，都满足 $e(u^a,v^b)=e(u,v)^{ab}$。

3)非退化性(Non-degeneracy)：存在 $u,v\in G$，使得 $e(u,v)\neq 1$。

2.2 DBDH 假设

随机选择 $a,b,c,z\in Z_p^*$，p 是 G 的阶，g 是 G 的生成元。DBDH 假设即为不存在一个多项式时间的概率算法能够以不可忽略的优势区分元组$[g,g^a,g^b,g^c,e(g,g)^{abc}]$和元组$[g,g^a,g^b,g^c,e(g,g)^z]$。

2.3 访问结构

在本文中，用户的身份由特定的属性集合来表示，访问结构使用多值与门来表达。

令 $U=\{att_1,\cdots,att_n\}$ 为一个属性集合，对于所有的 att_i $(att_i\in U)$，$S_i=\{v_{i,1},v_{i,2},\cdots,v_{i,n_i}\}$是一个可能的取值集合，其中 n_i 为属性 i 可能取值的个数。用户的属性列表为 $L=[L_1,L_2,\cdots,L_n]$，其中 $L_i=v_{i,t_i}\in S_i$，且 $t_i\in\{1,2,\cdots,n_i\}$。访问结构为 $W=[W_1,W_2,\cdots,W_n]$，其中 $W_i\subset S_i$。对于 $\forall i=1,2,\cdots,n$，若 $L_i\in W_i$，则称用户属性列表 L 满足访问结构 W。

在本文隐藏访问结构的密文策略基于属性加密方案中，用多值与门来表达访问结构，以增加系统的灵活性；在加密消息之前，加密者首先将访问结构转换成一棵访问树 τ，访问树的中间节点表示 $\wedge$、$\vee$ 运算符，叶子节点表示属性。密文中不能显示地包含访问树，访问时由加密者隐式地嵌入到密文中，因此，解密者仅仅知道他自己是否有能力解密该密文，而不能获得任何有关其他能够解密该密文的解密者信息。图 1 给出了由访问结构 $W=[\{v_{1,2}\},\{v_{2,1},v_{2,4}\},\{v_{3,1}\},\{v_{4,2},v_{4,3},v_{4,4}\}]$转换而成的访问树 τ，有很多属性集合可以满足图 1 中的访问树，比如 $L_1=\{v_{1,2},v_{2,4},v_{3,1},v_{4,2}\}$或者$L_2=\{v_{1,2},v_{2,1},v_{3,1},v_{4,4}\}$。

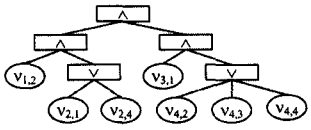

图 1 访问结构树

2.4 方案的定义

一个密文策略的基于属性加密方案包括 3 个实体：可信的授权中心 TA、加密者和解密者。TA 负责分发与解密者属性相对应的私钥，加密者指定用来控制解密者解密密文所需要满足的访问结构。为了描述的简洁性，本文使用拥有两个输入的函数 F 来表示属性列表 L 是否满足访问结构 W：$F(L,W)=1$ 表示属性列表满足访问结构，而 $F(L,W)=0$ 表示属性列表不满足访问结构。一个完整的密文策略属性基加密方案[4]包括 4 个算法：初始化算法、加密算法、密钥提取算法和解密算法，详细描述如下。

1)初始化算法：由 TA 运行。输入公共参数 1^λ，算法产生公钥 PK 和系统主私钥 MSK。

2)密钥产生算法：由可信授权方 TA 运行。输入系统公钥 PK、系统主私钥 MSK 以及用户的属性列表 L，算法产生该用户的私钥 sk_L。

3)加密算法：由加密者运行。输入需要加密的消息 M、系统公钥 PK 和用户属性集合表示的访问结构 W，算法产生密文 CT。

4)解密算法：由解密者运行。输入系统公钥 PK、隐式嵌入访问结构 W 的密文 CT 和包含属性列表 L 的用户私钥 sk_L。如果判定函数 $F(L,W)=1$，则表示能成功解密密文 CT，输出消息 M；否则，算法输出错误标识符 $\perp$。

2.5 方案的安全模型

本文方案可在选择属性模式下达到选择明文攻击的密文不可区分性（Indistinguishability of Ciphertext under Chosen-Message，IND-CMA），其所基于的安全模型[8]通过以下敌手 $\mathcal{A}$ 和挑战者 $\mathcal{B}$ 之间的交互游戏进行描述。

初始化阶段：敌手 $\mathcal{A}$ 向挑战者 $\mathcal{B}$ 提交要挑战的访问结构 W_0^*，W_1^*。挑战者选定安全参数 1^λ 并运行初始化算法得到系统公钥 PK 和系统主私钥 MSK，挑战者保留系统主私钥 MSK 并把系统公钥 PK 发送给敌手。

第一阶段：敌手向挑战者 $\mathcal{B}$ 进行属性列表 L 的密钥询问。但是有一个限制性的要求，$F(L,W_0^*)=0\wedge F(L,W_1^*)=0$，即属性列表 L 必须同时不满足敌手提供的两个访问结构，挑战者才运行密钥产生算法，并将私钥 sk_L 发送给敌手。敌手可以进行多项式次数的询问。

挑战阶段：敌手提交两个消息 M_0^*，M_1^*。挑战者随机选取一个 M_b^*，用 W_b^* 进行加密，其中 $b\in\{0,1\}$ 的值由挑战者随机抛币决定。挑战者运行加密算法并将密文返回给敌手。

第二阶段：重复第一阶段，同时敌手发起的询问必须满足 $F(L,W_0^*)=0\wedge F(L,W_1^*)=0$ 的要求。

猜测阶段：敌手输出对 b 的猜测 $b'\in\{0,1\}$，若 $b=b'$，敌手 $\mathcal{A}$ 赢得游戏，否则敌手失败。

敌手获得攻击游戏胜利的优势定义为 $Adv_{CP\text{-}ABE}^{IND\text{-}CMA}(\mathcal{A})=\left|\Pr[b'=b]-\frac{1}{2}\right|$。

定义 1 在多项式时间内，若不存在以不可忽略的优势赢得上述游戏的多项式时间敌手，则称该隐藏访问结构的密文策略基于属性加密方案是 IND-CMA 安全的。

3 方案描述

本节将给出隐藏访问结构的密文策略属性基加密方案的具体构造。

令 $U=\{att_1,\cdots,att_n\}$ 代表一个属性集合，对于所有的 $att_i(att_i\in U)$，$S_i=\{v_{i,1},v_{i,2},\cdots,v_{i,n_i}\}$ 是一个可能的取值集合，其中 n_i 为属性 i 可能取值的个数。用户的属性列表为 $L=[L_1,L_2,\cdots,L_n]$，其中 $L_i=v_{i,t_i}\in S_i$，且 $t_i\in\{1,2,\cdots,n_i\}$。访问结构为 $W=[W_1,W_2,\cdots,W_n]$，其中 $W_i\subset S_i$。

(1)初始化算法

1)输入：公共参数 1^λ。

2)过程：TA 产生一个线性群组 (p,G,G_T,e)，其中 G,G_T 是阶为 p 的乘法循环群，e 为双线性映射 $e:G\times G\to G_T$。系统选取 $y\in_R Z_p^*$ 和 $a_{i,t}\in_R Z_p^*$，并计算 $Y=e(g,g)^y$ 和 $T_{i,t}=g^{a_{i,t}}$，其中 $i\in[1,n],t\in[1,n_i]$。

3)输出：$PK=(e,G,G_T,g,Y,\{T_{i,t}\}_{i\in[1,n],t\in[1,n_i]})$ 为系统公钥，$MSK=(y,\{a_{i,t}\}_{i\in[1,n],t\in[1,n_i]})$ 为主私钥。

(2)密钥产生算法

1)输入：系统公钥 PK、系统主私钥 MSK 以及用户的属性列表 $L=[L_1,L_2,\cdots,L_n]$。

2)过程：对于 $1\leqslant i\leqslant n$，TA 选择 $r_i,\lambda_i\in_R Z_p^*$，并计算 $r=\sum_{i=1}^{n}r_i$，$D_0=g^{y-r}$，$D_{i,1}=g^{\lambda_i}$，$D_{i,2}=g^{r_i}T_{i,t}^{\lambda_i}$，其中 $L_i=v_{i,t}$。

3)输出：与用户属性列表 $L=[L_1,L_2,\cdots,L_n]$ 对应的用户私钥 $sk_L=\langle D_0,\{D_{i,1},D_{i,2}\}_{1\leqslant i\leqslant n}\rangle$。

(3)加密算法

1)输入：加密的消息 M、系统公钥 PK 和用户属性集合表示的访问结构 $W=[W_1,W_2,\cdots,W_n]$。

2)过程：加密者首先将使用多值与门表达的访问结构按前面提到的转换规则转换成对应的访问树 τ。加密者选择 $s\in_R Z_p^*$，并计算 $C_0=g^s$，$\tilde{C}=M\cdot Y^s=M\cdot e(g,g)^{ys}$。令访问树 τ 的根节点为 s，加密者标记根节点为已读状态，标记所有其他节点为未读状态。

如果当前节点的值为 $\wedge$ 且它所有的孩子节点均为未读状态，加密者为每一个孩子节点 i 选择 $s_i\in_R Z_p^*$，对于最后一个孩子节点，计算 $s_t=s-\sum_{i=1}^{t-1}s_i \bmod p$，把这些节点都标记为已读状态。

如果当前节点的值为 $\vee$ 且它所有的孩子节点均为未读状态，加密者设置它的所有孩子节点为 s_i，把这些节点标记为已读状态。

对于每一个 $W_i=v_{i,t}$，计算 $C_{i,1}=T_{i,t}^{s_i}$，$C_{i,2}=g^{s_i}$。

3)输出：密文 $CT=\langle C_0,\tilde{C},\{C_{i,1},C_{i,2}\}_{1\leqslant i\leqslant n}\rangle$。

(4)解密算法

1)输入：系统公钥 PK、隐式地嵌入访问结构 W 的密文 CT 和包含属性列表 L 的用户私钥 sk_L。

2)过程：计算出 $F(L,W)$ 的值，根据结果决定下一步的操作。

3)输出：如果 $F(L,W)=1$，则解密者计算 $\frac{e(C_0,D_0)\prod_{i=1}^{n}e(C_{i,2},D_{i,2})}{\prod_{i=1}^{n}e(C_{i,1},D_{i,1})}=e(g,g)^{ys}$，得出 $M=\frac{\tilde{C}}{e(g,g)^{ys}}$；如果 $F(L,W)=0$，则输出错误标识 $\perp$。

4 安全证明

本节在基于 DBDH 的假设下，证明本文隐藏访问结构的密文策略基于属性加密方案在标准模型中是 IND-CMA 安全的。

定义 2 该隐藏访问结构的密文策略基于属性加密方案在 DBDH 假设下满足密文的不可区分性。

证明：假设有敌手 $\mathcal{A}$ 能够以不可忽略的优势 ε 来攻破本文方案，那么就可以构造一个算法 $\mathcal{B}$ 能够以相同的优势 ε 来打破 DBDH 假设，模拟过程具体描述如下。

挑战者给定 DBDH 挑战元组 $[g,g^a,g^b,g^c,Z]$，其中 Z 的取值与 $e(g,g)^{abc}$ 在 G_T 中具有相同的概率分布。

初始化阶段：$\mathcal{A}$ 提供给 $\mathcal{B}$ 两个挑战访问结构 $W_0^*=[W_{0,1},\cdots,W_{0,n}]$，$W_1^*=[W_{1,1},\cdots,W_{1,n}]$，$\mathcal{B}$ 抛币得到随机值 $b\in\{0,1\}$。$\mathcal{B}$ 令 $Y=e(g,g)^{ab}=e(g^a,g^b)$，即有 $y=ab$。对于 $\forall 1\leqslant i\leqslant n$，当 $v_{i,t}\in W_{b,i}$ 时，算法 $\mathcal{B}$ 令 $T_{i,t}=g^{a_{i,t}}$；当 $v_{i,t}\notin W_{b,i}$ 时，$\mathcal{B}$ 令 $T_{i,t}=g^{ba_{i,t}}$，其中 $\{a_{i,t}\in_R Z_p\}_{1\leqslant i\leqslant n_i}$。$\mathcal{B}$ 把 $PK=(e,G,G_T,g,Y,\{T_{i,t}\}_{i\in[1,n],t\in[1,n_i]})$ 发送给敌手 $\mathcal{A}$。

第一阶段：敌手 $\mathcal{A}$ 提供一个属性列表 $L=[L_1,L_2,\cdots,L_n]$ 作为私钥询问的输入，因为 $F(L,W_0^*)=0\wedge F(L,W_1^*)=0$ 是挑战访问结构的要求，所以一定存在一个 $j\in\{1,\cdots,n\}$ 使得 $L_j(v_{j,t_j})\neq W_{b,j}$。

对于 $\forall 1\leqslant i\leqslant n$，挑战者 $\mathcal{B}$ 择 $r_i'\in_R Z_p^*$，$\lambda_i'\in_R Z_p^*$。如果 $i=j$，$\mathcal{B}$ 设 $r_j=ab+r_j'$，$\lambda_j=\frac{-a}{a_{j,t}}+\lambda_i'$；否则，设 $r_i=r_i'$。最后 $\mathcal{B}$ 设 $r=\sum_{i=1}^{n}r_i=ab+\sum_{i=1}^{n}r_j'$。

私钥 sk_L 中的 D_0 部分即可通过计算 $D_0=g^{y-r}=g^{ab-r}=g^{-\sum_{i=1}^{n}r_i'}$ 得到。

对于 $i=j$，$\mathcal{B}$ 计算 sk_L 私钥中$[D_{j,1},D_{j,2}]$部分的过程如下：

$$D_{j,1}=g^{\lambda_j}=g^{\frac{-a}{a_{j,t}}+\lambda_i'}=(\frac{1}{g^a})^{\frac{1}{a_{j,t}}}\cdot g^{\lambda_i'}$$

$$D_{j,2}=g^{r_j}T_{j,t}^{\lambda_j}=g^{ab+r_j'}g^{ba_{j,t}(\frac{-a}{a_{j,t}}+\lambda_i')}=g^{r_j'+ba_{j,t}\lambda_i'}=g^{r_j'}\cdot(g^b)^{a_{j,t}\lambda_i'}$$

对于 $i\neq j$，$\mathcal{B}$ 计算 sk_L 私钥中$[D_{i,1},D_{i,2}]$部分的过程为：$D_{i,1}=g^{\lambda_i}=g^{\lambda_i'}$，$D_{i,2}=g^{r_i}T_{i,t}^{\lambda_i}=g^{r_i'}g^{a_{i,t}\lambda_i}$。

敌手 $\mathcal{A}$ 提交挑战消息 M_0^*，M_1^* 给 $\mathcal{B}$。$\mathcal{B}$ 令 $s=c$，设 $C_0=g^c$ 且 $\tilde{C}=M_b^*\cdot Y^z=M_b^*\cdot e(g,g)^z$。对于 $\forall 1\leqslant i\leqslant n-1$，$\mathcal{B}$ 选择 $c_i\in_R Z_p^*$ 且对于 $i=n$，$\mathcal{B}$ 计算 $c_n=c-\sum_{i=1}^{n-1}c_i$。

对于 $i=n$，密文中的$[C_{n,1},C_{n,2}]$可通过计算$C_{n,1}=g^{c_n}=g^{c-\sum_{i=1}^{n-1}c_i}=\frac{g^c}{g^{\sum_{i=1}^{n-1}c_i}}$，$C_{n,2}=T_{i,t}^{c_n}=g^{a_{i,t}(c-\sum_{i=1}^{n-1}c_i)}=\frac{(g^c)^{a_{i,t}}}{g^{a_{i,t}\sum_{i=1}^{n-1}c_i}}$得到。

对于 $\forall 1\leqslant i\leqslant n-1$，密文中的$[C_{i,1},C_{i,2}]$可通过计算 $C_{i,1}=g^{c_i}$，$C_{i,2}=T_{i,t}^{c_i}=g^{a_{i,t}c_i}$ 得到。

第二阶段：重复第一阶段的过程，继续私钥询问。

猜测阶段：如果 $T=e(g,g)^{abc}$，敌手 $\mathcal{A}$ 就能准确输出对 b 的猜测 b'；否则，$T=e(g,g)^z$，敌手 $\mathcal{A}$ 只能做一个随机的猜测。如果 $b'=b$，$\mathcal{B}$ 输出 $\beta=1$；否则，输出 $\beta=0$。因此，$\mathcal{B}$ 能够以 ε 的优势解决 DBDH 问题。

5 效率分析

为了突出本方案的优势，本节将本方案从加解密所需要的时间和参数长度等方面与文献[8,9]作对比。为了描述的方便，本节使用 *PK*、*MSK*、*SK*、*CT* 分别代表系统公钥、系统主私钥、用户私钥和密文的长度；*Enc.* 和 *Dec.* 分别代表加密和解密的时间；*D-Linear* 代表决策线性假设；$|G|$，$|G_T|$，$|Z_p^*|$分别代表 G,G_T,Z_p^* 中元素的位数；令 $U=\{att_1,\cdots,att_n\}$为系统的属性集合；n 为系统属性的总数；n_i 表示属性 i 的取值的个数，那么 $N=\sum_{i=1}^{n}n_i$ 就表示所有可能的属性的取值总数；G 和 G_T 分别表示群 G 和 G_T 上计算所用的时间；C_e 代表双线性对计算需要的时间。

参数长度比较的结果如表 1 所列，文献[11,17]与本方案相同，而文献[8]系统公钥 *PK* 长度为 $N|G|$ 比特，方案[9]系统公钥 *PK* 长度为 $|G|$ 比特；用户私钥 *SK* 的长度比文献[8,9]短，而相对于文献[11,17]要长；密文 *CT* 长度相对来说是最短的。总体上来说，本文方案的参数长度具有优势，特别是密文的长度，因为密文的长度关系到系统的通信代价。

加解密的时间对比如表 2 所列，本方案的加密时间比其他方案都短，具有很高的效率；而解密效率相较于文献[17]还有待改进，特别是双线性对这样代价高的运算需尽量减少，以实现方案的高效性。

表 1 参数长度的比较

方案	PK	MK	SK	CT
NYO[8]	$(2N+1)\|G\|+\|G_T\|$	$(2N+1)\|Z_p^*\|$	$3(n+1)\|G\|$	$(2N+1)\|G\|+\|G_T\|$
MK[9]	$(N+2)\|G\|+\|G_T\|$	$(N+4)\|Z_p^*\|$	$(2n+2)\|G\|$	$(2N+3)\|G\|+\|G_T\|$
LDL[11]	$(N+1)\|G\|+\|G_T\|$	$(N+1)\|Z_p^*\|+\|G\|$	$(n+1)\|G\|$	$(N+1)\|G\|+\|G_T\|$
PJ[17]	$(N+1)\|G\|+\|G_T\|$	$(N+1)\|Z_p^*\|$	$4\|G\|$	$(N+2)\|G\|+\|G_T\|$
Our scheme	$(N+1)\|G\|+\|G_T\|$	$N\|Z_p^*\|+\|G_T\|$	$(2n+1)\|G\|$	$(2n+1)\|G\|+\|G_T\|$

表 2 算法时间比较

方案	Enc.	Dec.
NYO[8]	$(2N+1)G+2G_T$	$(3n+1)C_e+(3n+1)G_T$
MK[9]	$(2N+3)G+G_T$	$(2n+1)C_e+3G_T$
LDL[11]	$(N+1)G+G_T$	$(n+1)C_e+2G_T$
PJ[17]	$(N+2)G+G_T$	$4C_e+4G_T$
Our scheme	$(2n+1)G+G_T$	$(2n+1)C_e+3G_T$

方案所具有的相关特点如表 3 所列。本方案与文献[8,9]采取的是选择性的安全模型，而文献[11,17]实现了完全安全；然而，本方案与文献[8,17]采用类似的标准安全假设，文献[9,11]基于的安全假设是非标的；同时，文献[8]只能实现部分隐藏，本方案与余下几个方案都能实现隐藏访问结构的功能，能实现完全隐藏、完全保密加密者的隐私。对于基于的困难性问题，本文的 DBDH 困难性问题是比较经典的困难性问题，优于其他方案基于其他一个或多个困难性问题的证明。

表 3 方案特点比较

方案	Security Model	Access policy hidden	Assumption
NYO[8]	Selective	Partial	DBDH, D-Linear
MK[9]	Selective	Full	Non-standard
LDL[11]	Fully	Full	Non-standard
PJ[17]	Fully	Full	Discrete Logarithm Problem, DBDH
Our scheme	Selective	Full	DBDH

总之，本方案在参数的长度、加解密的效率及相关特点上都具有一定的优势，特别是在密文的长度与加密的效率上，而且拥有能完全隐藏用户隐私的访问结构，所以同时保证了系统的高效性与安全性。同时，我们的方案也存在一些不足之处，例如用户私钥的长度与解密的效率，这都是我们以后致力解决的问题，甚至做到系统参数长度及加解密的时间都不随属性数量线性增长，实现真正意义上的高效。

结束语 本文提出了一个全新、高效的隐藏访问结构的密文策略基于属性加密方案，其满足解密者无法从密文中提取任何信息的要求，保证了密文加密者的隐私；同时，方案的加密效率很高。另外，基于 DBDH 安全假设，证明了方案能抵抗选择明文攻击，实现了密文的不可区分安全性，做到了安全性与高效性的统一。

参 考 文 献

[1] Sahai A, Waters B. Fuzzy identity-based encryption[C]// Advances in Cryptology-EUROCRYPT 2005. Berlin: Springer Berlin Heidelberg, 2005: 457-473

(下转第 198 页)

org/ATL/Tutorials

[10] The Eclipse Foundation. The Eclipse Modeling Framework Overview [EB/OL]. (2011-12-03) [2014-07-11]. http://www.eclipse.org/emf.

[11] ATLAS group LINA & INRIA Nantes. ATLAS Transformation Language (ATL) Home Page [EB/OL]. (2011-12-03) [2014-07-11]. http://www.eclipse.org/atl/documentation/old/ATL_User_Manual[v0.7].pdf

[12] Jounult F, Bezivin J. KM3: A DSL for metamodel specification [M]// Gorrieri R, Wehrheim H, eds. Proc. of the 8th IFIP Int'l conf. on Formal Methods for Open Object-Based Distributed System. Berlin: Springer-Verlag, 2006: 171-185

[13] Jouault F, Allilaire F, Bezivina J, et al. ATL: A model transformation tool [J]. Science of Computer Programming, 2008, 72 (2): 21-29

[14] Object Management Group (OMG). UML2.0 Infrastruture-Specification[EB/OL]. (2009-04-01) [2014-07-11]. New York: Object Management Group. http: www.omg.org.does/ptc/03-09-15.pdf

[15] Zhang Tian, Jouault F, Attiogbe C, et al. MDE-Based Mode Transformation: From MARTE Model to FIACRE Model[J]. Journal of Software, 2009, 20(2): 214-233(in Chinese)
张天, Jouault F, Attiogbe C, 等. 基于 MDE 的异构模型转换: 从 MARTE 模型到 FIACRE 模型[J]. 软件学报, 2009, 20(2): 214-233

[16] Han Zhen, Zhao Quan-xiang. Logic Modeling and Application of Under Water Control System [J]. Automation Application, 2011, 11(3): 23-27(in Chinese)
韩振, 赵全香. 水下控制系统逻辑建模与应用[J]. 自动化应用, 2011, 11(3): 23-27

[17] Gao Jin-yuan, Jiao Zong-xia, Zhang Ping. The Plane Telex Control System Active Control Technology[M]. Beijing: Beihang University Press, 2005: 34-65(in Chinese)
高金源, 焦宗夏, 张平. 飞机电传操纵系统主动控制技术[M]. 北京: 北京航空航天大学出版社, 2005: 34-65

[18] Wang Yong, Liang De-fang. Civilian Aircraft Fly-By-Wire Flight Control System [J]. Aeronautic Standardization & Quality, 2008, 227(5): 24-28(in Chinese)
王永, 梁德芳. 民用飞机电传飞行控制系统初探[J]. 航空标准化与质量, 2008, 227(5): 24-28

(上接第 178 页)

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

[3] Bethencourt J, Sahai A, Waters B. Ciphertext-policy attribute-based encryption[C]// IEEE Symposium on Security and Privacy 2007 (SP 2007). Piscataway: IEEE, 2006: 321-334

[4] Cheung L, Newport C. Provably secure ciphertext policy ABE [C]// 14th ACM Conference on Computer and Communications Security (ACM CSS 2007). New York: ACM, 2007: 456-465

[5] Lbraimi L, Tang Q, Hartel P, et al. Efficient and provably secure ciphertext-policy attribute-based encryption schemes [C]// Information Security Practice and Experience. Berlin: Springer Berlin Heidelberg, 2009: 1-12

[6] Kapadia A, Tsang P P, Smith S W. Attribute-based publishing with hidden credentials and hidden policies [C]// Proceedings USA of 14th Annual Network & Distributed System Security Symposium (NDSS 2007). San Diego, California, USA: NDSS, 2007: 179-192

[7] Boneh D, Waters B. Conjunctive, subset, and range queries on encrypted data[C]// 4th Theory of Cryptography Conference. Berlin: Springer Berlin Heidelberg, 2007: 535-554

[8] Nishide T, Yoneyama K, Ohta K. Attribute-based encryption with partially hidden encryptor-specified access structures[C]// 6th International Conference on Applied Cryptography and Network Security. Berlin: Springer Berlin Heidelberg, 2008: 111-129

[9] Müller S, Katzenbeisser S. Hiding the policy in cryptographic access control [M]// Security and Trust Management. Berlin: Springer Berlin Heidelberg, 2012: 90-105

[10] Xu R, Wang Y, Lang B. A Tree-Based CP-ABE Scheme with Hidden Policy Supporting Secure Data Sharing in Cloud Computing[C]// 2013 International Conference on Advanced Cloud and Big Data (CBD). Piscataway: IEEE, 2013: 51-57

[11] Lai J Z, Deng R H, Li Y J. Fully secure ciphertext-policy hiding CP-ABE[C]// 7th International Conference on Information Security Practice and Experience. Berlin: Springer Berlin Heidelberg, 2011: 24-39

[12] Waters B. Dual system encryption: realizing fully secure IBE and HIBE under simple assumptions[C]// Advances in Cryptology-CRYPTO 2009(009). Berlin: Springer Berlin Heidelberg, 2011: 619-636

[13] Emura K, Miyaji A, Nomura A, et al. A ciphertext-policy attribute-based encryption scheme with constant ciphertext length[C]// 5th International Conference on Information Security Practice and Experience. Berlin: Springer Berlin Heidelberg, 2009: 13-23

[14] Zhou Z B, Huang D J. On efficient ciphertext-policy attribute-based encryption and broadcast encryption extended abstract [C]// Proceedings of the 17th ACM Conference on Computer and Communications Security. New York: ACM, 2010: 753-755

[15] Rao Y S, Dutta R. Recipient anonymous ciphertext-policy attribute based encryption[C]// 9th Internatonal Conference on Information Systems Security. Berlin: Springer Berlin Heidelberg, 2013: 329-344

[16] Zhang M, Wang X A, Yang X, et al. Efficient Predicate Encryption Supporting Construction of Fine-Grained Searchable Encryption[C]// 2013 5th International Conference on Intelligent Networking and Collaborative Systems (INCoS). Piscataway: IEEE, 2013: 438-442

[17] Padhya M, Jinwala D. A Novel Approach for Searchable CP-ABE with Hidden Ciphertext-Policy [C]// 10th International Conference on Information Systems Security. Berlin: Springer Berlin Heidelberg, 2014: 167-184