**Computer Science and Application** 计算机科学与应用, 2019, 9(2), 275-281
Published Online February 2019 in Hans. http://www.hanspub.org/journal/csa
https://doi.org/10.12677/csa.2019.92032

Hans汉斯

# Research of CP-ABE Supported Hidden Access Policy

**Xinglan Zhang, Mingming Wang**

Beijing University of Technology, Beijing
Email: 1547049327@qq.com

Received: Jan. 16th, 2019; accepted: Jan. 28th, 2019; published: Feb. 12th, 2019

## Abstract

**Attribute-based encryption that supports policy hiding not only protects plaintext, but also protects user's sensitive information. The existing schemes have limitations on the access structure and weak strategy expression. This paper proposes an attribute-based encryption scheme for hidden access policies. It implements policy hiding by transforming the access structure into a property list and then encrypting the property list. The scheme has no restrictions on the access structure. In addition, outsourcing partial decryption calculations reduce the computational burden on users. Analysis shows that the new scheme enhances the flexibility of policy expression and decryption efficiency while implementing policy hiding, and proves to be secure under the DBDH assumption.**

## Keywords

**CP-ABE, Hidden Policy, DBDH Assumption**

# 支持访问策略隐藏的属性基加密方案研究

**张兴兰，王明明**

北京工业大学，北京
Email: 1547049327@qq.com

收稿日期：2019年1月16日；录用日期：2019年1月28日；发布日期：2019年2月12日

## 摘　要

**支持策略隐藏的属性基加密不仅可以保护明文，还可以保护用户的敏感信息。现有方案对访问结构有所限制，策略表达能力比较弱。本文提出一种隐藏访问策略的属性基加密方案，通过将访问结构转换成属性列表，然后对属性列表加密处理实现了策略隐藏，并且该方案对访问结构没有任何的限制。此外，将部分解密计算外包，减轻了用户的计算负担。分析表明，新方案在实现策略隐藏的同时增强了策略表达**

文章引用: 张兴兰, 王明明. 支持访问策略隐藏的属性基加密方案研究[J]. 计算机科学与应用, 2019, 9(2): 275-281.
DOI: 10.12677/csa.2019.92032

**的灵活性，提高了解密效率，并且在DBDH假设下证明是选择明文攻击安全的。**

## 关键词

**属性基加密，隐藏策略，DBDH假设**



## 1. 引言

随着云存储的发展，越来越多的企业选择在云上存储数据，而不是花费昂贵的费用来购买存储设备。然而云存储目前最大难题之一就是安全隐患[1]，为了保证数据的机密性，Shamir 和 Bonehe [2]首次了提出身份加密机制的概念，在加密明文前，数据拥有者需要知道用户的身份信息，用户解密密钥和用户的身份信息相关联，该机制为公钥密码体系的一对一加密。在实际应用中常常需要一对多的加密模型，例如数据拥有者共享的数据多个用户都可以解密查看。Sahai 和 Waters [3]首次提出了模糊身份基加密，增加了访问控制策略[4]，用属性来标记用户身份信息，实现了公钥密码体系的一对多加密。随后 Goyal 等人[5]将基于属性加密体制分为密文策略 ABE (CP-ABE)和密钥策略 ABE (KP-ABE)两种。在 CP-ABE 中，数据拥有者具备制定策略的权利，密文和加密者定义的访问策略相关联，密钥则是和属性相关联；在 KP-ABE 中密文则是和属性相关，而密钥与访问策略相关联。属性基加密要求将访问策略在明文中公开，攻击者可以根据访问策略推测出用户的敏感信息，从而泄露用户隐私。

随着近年来对属性加密方案的研究[6] [7]，为了进一步保护用户信息的安全性，Nishide 等人[8]提出了一个隐藏访问策略的加密方案，将访问策略隐藏在密文中，实现了在保护消息机密性的同时保护了访问策略，但该方案只支持“与”操作，访问策略的可表达性受到较大影响。Lai 等人[9]在合数阶双线性群上提出一种在标准模型下证明是完全安全的隐藏访问结构的 CP-ABE 方案。文献[10] [11]提出了可支持任意门限或者布尔表达式的属性基加密方案，增加了访问结构的灵活性。宋衍等人[12]提出了一种基于访问树的策略隐藏属性加密方案，该方案是通过定义末端节点实现访问策略的隐藏，并证明是自适应安全的。基于属性基加密的方案中，往往用户需要大量的计算才能够获得明文，为了提高计算效率，Green 等[13]提出了带外包解密的属性基加密概念，将部分计算交给云服务器计算。Lai 等人[14]提出了改进的带可验证的外包解密的属性基加密概念，从用户可以验证云服务器计算的是否正确。文献[15] [16] [17]相继提出了一些基于外包解密的 ABE 方案。

本文在文献[12]的基础上，通过将树型访问结构转换成属性列表，取消了文献[12]中定义的末端节点只能表示与的限制。采用分割加密的思想，将访问策略加密和明文加密分别加密，实现访问策略的隐藏。用户只能判断自己是否符合访问策略，但无法知道具体的访问策略是什么，在解密步骤通过引入了外包计算简化用户的计算开销，提高了解密效率。

## 2. 预备知识

### 2.1. 双线性映射

设 $G_1$，$G_2$ 是阶为素数 $p$ 的循环群，$Z_p^*$ 表示模 $p$ 循环群，$g$ 是 $G_1$ 的生成元。$e: G_1 X G_1 \to G_2$ 是从$(G_1, G_1)$

到 $G_2$ 的一个映射。如果满足一下条件，则称 $e:G_1XG_1\to G_2$ 是一个双线性映射：

1) 双线性性质：$e\left(g^a,h^b\right)=e\left(g,h\right)^{ab}$。$g$，$h$ 是 $G_1$ 中的元素，$a$，$b$ 是 $Z_p^*$ 中的元素。

2) 非退化性：$e\left(g,g\right)\neq 1$。

3) 可计算性：对 $G_1$ 中的所有元素 $g,h$，存在一个有效的算法计算出 $e\left(g,h\right)$ 的值。

## 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 $\left[g,g^a,g^b,g^c,e\left(g,g\right)^{abc}\right]$ 和元组 $\left[g,g^a,g^b,g^c,e\left(g,g\right)^z\right]$。

## 2.3. 本文方案

### 2.3.1. 系统模型

本方案共包含四个实体：可信机构，数据拥有者，用户和云服务器。各个实体的功能如下：

1) 可信机构：可信机构是完全受信任的中央授权机构，它生成系统的公共参数并为用户计算私钥。

2) 数据拥有者：数据拥有者的工作是制定访问结构、对数据加密并将密文上传到云服务器。

3) 用户：用户从云端服务器下载密文，然后向可信机构提交自己的属性列表，并从可信机构获得相应的私钥，当且仅当属性列表满足访问结构的时候可以成功解密密文。

4) 云服务器：云服务器负责存储密文和解密外包计算。云服务器是不完全受信任的，它有可能会泄露存储的数据或给用户故意返回错误的计算结果。

### 2.3.2. 访问结构转换规则

将访问结构转换成属性列表的规则，假设节点 $\alpha$ 的叶子节点个数为 $\alpha_k$。

1) 如果节点是 and，则 $W_\alpha=\left\{W_1=\left[a_1,a_2\cdots a_{\alpha k}\right]\right\}$

2) 如果节点为 or，则 $W_\alpha=\left\{W_1=\left[a_1\right],W_2=\left[a_2\right]\cdots W_{\alpha k}=\left[a_{\alpha k}\right]\right\}$

3) 如果节点为 of，门限值为 $h$，则 $W_\alpha=\left\{W_i=\left[a_i\cdots a_m\right]\cdots W_n=\left[a_i\cdots a_m\right]\right\}\left(n=C_{\alpha_k}^h\right)$

由下到上，计算出根节点对应的所有属性列表 $W=\left\{W_1,W_2,\cdots,W_n\right\}$

### 2.3.3. 访问结构

在本文中，用户的身份由特定是属性集合表示，本方案的访问结构为树型，可以灵活的支持 and、or 和 threshold。

系统中是所有属性集合为 $A=\left\{a_1,a_2,\cdots,a_m\right\}$，对于任何 $a_i\left(1\le i\le m\right)$ 的取值集合为 $S_i=\left\{v_{i,1},v_{i,2},\cdots,v_{i,t}\right\}$，访问树为 $T$，转换后的属性组合为 $W=\left\{w_1,w_2,\cdots,w_n\right\}$，其中 $w_i=\left[v_{1,t},v_{2,t},\cdots,v_{m,t}\right]$，用户的属性列表为 $U=\left[U_1,U_2,\cdots,U_m\right]$，其中 $U_i\in S_i$。

本文利用加密分割思想将对访问结构的加密和密文加密分割开，数据拥有着将定义好的访问结构转换成符合访问结构的所有可能组合的列表，然后加密。例如图 1 访问树 $T$，将转换成 $W=\left\{W_1=\left[A,B\right],W_2=\left[A,C\right],W_3=\left[B,C\right],W_4=\left[D,E\right]\right\}$，然后 $W_i$ 中的属性值用 $g^{sa_{i,t}}$ 代替，不以明文的形式出现在属性列表中，攻击者虽然可以根据加密后的属性列表恢复出访问结构的内部节点，但具体的属性值无法确认，因此实现了策略的隐藏。用户通过判断自己的属性列表是否与其中的某一条一致来确定是否满足访问策略。

## 2.4. 方案安全模型

本方案可在标准模式下达到完全安全。其所基于的安全模型通过以下挑战者 $S$ 和敌手 $A$ 之间的交互游戏进行描述，若最终敌手 $A$ 给出正确的猜测，则敌手胜利，反之挑战者胜利。游戏过程入下：

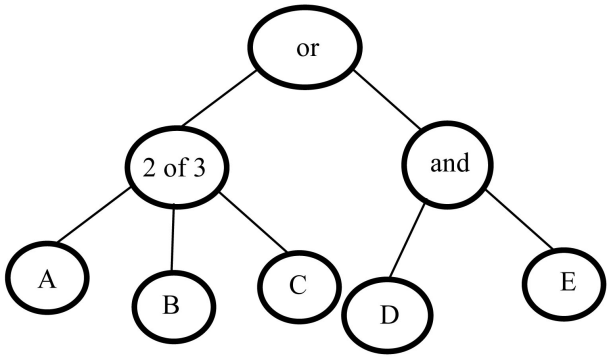


**Figure 1.** Access tree T
**图 1.** 访问树 T

初始化阶段：敌手 $A$ 向挑战者 $S$ 提交访问结构 $T_0$ 和 $T_1$。挑战者 $S$ 选择安全参数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 $MSK$，并且把系统公钥 $PK$ 发送给敌手 $A$。

第一阶段：敌手向挑战者询问属性集 $U$ 的私钥(可多次)，同时要求私钥既不能满足 $T_0$ 也不也能满足 $T_1$，挑战者 $S$ 运行生成私钥算法，生成 $SK$ 并发送给 $A$。

挑战：敌手 $A$ 输出两个长度相同的消息 $M_0$ 和 $M_1$。挑战者随机选择 $j \in \{0,1\}$，对 $M_j$ 进行加密，并且将密文发送给敌手 $A$。

第二阶段：重复第一阶段，继续询问私钥。

猜测：敌手 $A$ 输出对 $j$ 的猜测 $j'$，如果 $j' = j$，则称敌手 $A$ 赢得游戏；否则，敌手 $A$ 失败。我们定义敌手 $A$ 获得胜利的优势为 $Adv = \Pr[j = j'] - \frac{1}{2}$。

**定义 1：**

基于属性基的加密方案在选择性明文攻击下是完全安全的，并且只有在没有多项式有界攻击者的情况下才能以不可忽略的优势赢得上述游戏。

## 3. 算法设计

1) 初始化过程($1^\lambda$)

输入公共参数$1^\lambda$，生成两个阶为素数 $p$ 的乘法循环群 $G_1$、$G_2$，$G_1$ 的生成元是 $g$。$e$ 为双线性映射 $e: G_1 X\ G_1 \to G_2$。系统随机选择 $y \in Z_p^*$，计算 $Y = e(g,g)^y$ 对于每个属性 $a_i\ (1 \le i \le m)$ 系统随机选择 $a_{i,t} \in Z_p^*$ $(1 \le t \le m_i)$，计算 $A_{i,t} = g^{ai,t}\ (1 \le i \le m, 1 \le t \le m_i)$。输出：系统公钥 $PK = \left\langle g, Y, \{A_{i,t}\}_{1 \le i \le n,\ 1 \le t \le k} \right\rangle$，主密钥 $MSK = \left\langle y, \{a_{i,t}\}_{1 \le i \le n,\ 1 \le t \le k} \right\rangle$。

2) 加密过程($PK$, $T$, $M$)

输入：明文 $M$，访问结构 $T$，和系统公钥 $PK$。

第一步：加密访问结构。将访问结构根据转换规则转换成属性列表 $W = \{w_1, w_2, \cdots, w_n\}$。$w_i = [v_{1,t}, v_{2,t}, \cdots, v_{m,t}]_{1 \le t \le mi}$，将 $w_i$ 进行加密，随机选择 $s \in Z_p^*$，对于 $v_{i,t}$，计算如下 $C_{i,t} = A_{i,t}^s$。$C_t' = \prod_{t=1}^{m_i} A_{i,t}$，$C_i = \{C_{i,t}\}_{1 \le t \le mi}$。如果数据拥有者的计算能力有限，该步骤也可以交给云端服务器计算，因为只是将访问结构暴露了出去，即使攻击者获得到了所有的信息，攻击者也不知道该访问结构能够解密的是那一个密文，所以云端服务器来进行访问结构的加密也是安全的。

第二步：加密明文 $M$。计算 $C_0 = g^s, C = MY^s = Me(g,g)^{ys}$。

生成密文为：$CT = \left\langle C, C_0, CR = \left\langle \{C_i\}_{1\le i\le m}, \{C_i'\}_{1\le i\le m} \right\rangle \right\rangle$。

3) 提取私钥

输入：用户的属性列表 $U$，主私钥 $MSK$，和系统公钥 $PK$。

随机选择 $\theta \in Z_p^*$，对于任意 $v_{i,t} \in U$，随机选取 $d_i \in Z_p^*$，计算 $D_i = g^{di/ai,t}, D_i' = D_i^{1/\theta}$。设置 $d = \sum_{i=1}^{m} d_i$，计算 $D_0 = g^{y-d}$，$F = \prod_{i=1}^{m} g^{a_{i,t}}$。最后输出 $SK = \langle \theta, D_0 \rangle, TK = \left\langle \{D_i'\}_{0\le i\le m}, F \right\rangle$。

假设 $\forall U, U'(U \ne U')$，$\sum_{v_{i,t}\in U} a_{i,t} \ne \sum_{v_{i,t}\in U'} a_{i,t}$，以免不同的属性列表 $U$、$U'$ 实现相同的解密功能。以上假设成立的概率 $P_{\text{assump}} > \left(1 - p_0^2/p\right)$，其中 $p_0 = \prod_{i=1}^{m} m_i$ [18]。

4) 外包解密

输入：转换密钥 $TK$，密文 $CT$。

服务器根据 $TK$ 和 $CT$，首先判断用户的属性列表是否符合解密条件，如果符合则进行密文转换计算，否则终止服务。

服务器根据 $TK$ 和 $CT$ 计算，验证是否存在 $C_i'$ 使得 $F$ 等于 $C_i'$，如果存在，则用户属性列表 $U$ 满足访问条件则相等，否则终止服务。若满足访问条件则计算

$$CT' = \prod_{i=1}^{m} e\left(C_{i,t}, D_i\right) = e(g,g)^{\sum_{i=1}^{m} sa_{i,t}\cdot d_i/\theta a_{i,t}} = e(g,g)^{s/\theta\cdot\sum_{i=1}^{m} d_i} = e(g,g)^{sd/\theta}。$$

5) 用户解密

如果用户收到云端服务器返回的 $CT'$，明文计算如下：

$$\frac{C}{e(C_0, D_0)^{?} CT'^{\theta}} = \frac{MY^s}{e\left(g^s, g^{y-d}\right)^{?} e(g,g)^{(sd/\theta)\theta}} = \frac{Me(g,g)^{ys}}{e(g,g)^{sy-sd\,?} e(g,g)^{sd}} = M$$；否则，用户无权解密。

## 4. 安全性证明

以下证明该方案在 DBDH 假设下满足选择明文攻击的完全安全。假设敌手 A 能以不可忽略的优势 ε 来攻破本文方案，那么就能够构造出一个模拟器 $S$，它可以以 $\varepsilon$ 的优势打破 DBDH。

在 DBDH 游戏中，挑战者 $S$ 会选择群 $G_1$ 和 $G_2$，群 $G_1$ 的生成元为 $g$，映射为 $e(g,g)$，随机选择数 $a,b,c,z \in Z_p$。挑战者 $S$ 投掷硬币 $\mu \in \{0,1\}$，如果 $\mu = 0$，则设置 $Z = e(g,g)^{abc}$，否则 $\mu = 1$，设置 $Z = e(g,g)^{z}$。

初始化阶段：敌手 $A$ 提供给挑战者 $S$ 两个要挑战的访问结构 $T_0$ 和 $T_1$。挑战者 $S$ 随机选择 $j \in \{0,1\}$，对于 $0 \le i \le m, 1 \le t \le m_i$ 随机选取 $a_{i,t} \in Z_p^*$，当属性值存在于访问树 $T_j$ 的叶子节点中，令 $A_{i,t} = g^{ai,t}$，否则令 $A_{i,t} = g^{bai,t}$，$Y = e\left(g^a, g^b\right) = e(g,g)^{ab}$，$S$ 把系统公钥 $PK = \left\langle g, Y, \left\{A_{i,t}\right\}_{0\le i\le m,\ 0\le t\le k} \right\rangle$ 发送给敌手 $A$。

第一阶段：敌手 $A$ 提供一个属性集合 $U = \{U_1, U_2, \cdots, U_m\}$ 作为私钥询问的输入，要求属性集合 $U$ 不满足访问结构 $T_0$ 和访问结构 $T_1$。挑战者 $S$ 计算出私钥发送给 $A$，对于 $U$ 内的属性 $U_i\left(1 \le i \le m\right)$，只是存在一个 Ψ 使得 $U_\Psi$ 不满足 $T_j$。对于 $\forall 1 \le i \le m$，随机选择 $d_i' \in Z_p$，如果 $i = \Psi$，计算 $d_i = ab + d_i'$，否则 $d_i = d_i'$，计算 $D_i = g^{d_i/a_{i,t}}$，$D_i' = D_i^{1/\theta}$，设置 $d = \sum_{i=1}^{n} d_i = ab + \sum_{i=1}^{n} d_\psi$，$F = \prod_{i=1}^{m} g^{a_{i,t}}$，令 $D_0 = g^{ab-d}$，$TK = \left\langle F, \{D_i'\}_{0\le i\le m} \right\rangle, SK = \langle \theta, D_0 \rangle$，将私钥发送给敌手 $A$。

挑战阶段：敌手 $A$ 提交 $M_0$ 和 $M_1$ 给挑战者 $S$。将 $T_j$ 转化成属性列表 $W_j$。令 $s=c$，设 $C_0=g^s$，$C=M_jZ=M_je(g,g)^z$，当 $j=0$ 时，$e(g,g)^z=e(g,g)^{abc}$；当 $j=1$ 时，$e(g,g)^z$ 为随机值。对于 $v_{i,t}\in w_i$，计算如下 $C_{i,t}=A_{i,t}^s$，$C_i^{'}=\prod_{t=1}^{m_i}C_{i,t}$，$C_i=\{C_{i,t}\}_{1\le t\le mi}$。$CR=\langle\{C_i\}_{1\le i\le m},\{C_i'\}_{1\le i\le m}\rangle$，把密文 $CT=\langle C,C_0,CR\rangle$ 发送给外包服务器，外包服务器通过转换密钥 $TK$ 将密文 $CT$ 转换成 $CT'$，首次判断用户属性列表是否符合访问结构，如果符合则计算 $CT'=\prod_{i=1}^{m}e(C_{i,t},D_i')=e(g,g)^{\sum_{i=1}^{m}sa_{i,t}\cdot d_i/\theta a_{i,t}}=e(g,g)^{s/\theta\cdot\left(ab+\sum_{i=1}^{m}d_\psi\right)}$，然后将密文 $CT'$ 发送给敌手 $A$。

第二阶段：重复第一阶段，继续询问私钥。

猜测阶段：敌手输出对 $j$ 的猜测 $j'$，如果 $j'=j$，模拟器会猜测 $\mu=0$；$j'\neq j$，模拟器会猜测 $\mu=1$。

当 $\mu=0$ 时，敌手 $A$ 获得有效密文 $CT'$。敌手的优势为：$\Pr\left[j'=j\middle|Z=e(g,g)^{abc}\right]=\frac{1}{2}+\varepsilon$。当 $\mu=1$ 时，敌手获得的密文 $CT'$ 是随机的，无法得知它明文的任何信息，$\Pr\left[j'\neq j\middle|Z=e(g,g)^{z}\right]=\frac{1}{2}$。因此，模拟器在解决 DBDH 假设上总的优势为：$\frac{1}{2}\Pr\left[j'=j\middle|Z=e(g,g)^{abc}\right]+\frac{1}{2}\Pr\left[j'\neq j\middle|Z=e(g,g)^{z}\right]-\frac{1}{2}=\frac{\varepsilon}{2}$。

由以上证明可知，在 DBDH 假设中，若多项式时间敌手 $A$ 的优势为 $\varepsilon$，则模拟器 $S$ 的优势为 $\frac{\varepsilon}{2}$。因此，如果敌手 $A$ 可以在安全模型下能够以不可忽略的优势破坏本方案，则模拟器 $S$ 的优势也不容忽视，由此可证明在安全模型下没有敌手可以破坏本方案。

## 5. 效率分析

本文通过将访问结构转换成属性列表，实现了方案中策略隐藏的要求。为了彰显本方案的优点，本节将本方案分别从用户的私钥长度，解密长度以及系统的采用的双线性群阶和复杂性假设四个方面与其它方案做对比。$e$ 表示双线性配对运算所需的时间，$G_2$ 表示群 $G_2$ 中的运算，$|G_1|$ 和 $|G_2|$ 分别表示群 $G_1$ 和 $G_2$ 中元素的长度，$m$ 表示系统中的属性个数，$\alpha$ 表示访问结构中末端内部节点的个数，$\alpha_k$ 表示 $\alpha$ 的子结点个数。具体结果如表 1 所示。

**Table 1.** Comparison of this scheme and other schemes
**表 1.** 本方案与其它方案比较

| 方案 | 双线性群阶 | 私钥长度 | | 解密时间 | | 复杂性假设 |
|---|---|---|---|---|---|---|
| | | $\|G_1\|$ | $\|G_2\|$ | $e$ | $G_2$ | |
| 文献[8] | 素数 | $1+2m$ | 0 | $1+3m$ | $1+3m$ | DBDH |
| 文献[9] | 合数 | $1+m$ | 0 | $1+m$ | $1+m$ | Non-standard |
| 文献[11] | 合数 | $2+m$ | $2+m$ | $1+\alpha+\alpha\alpha_k$ | $1+\alpha+\alpha\alpha_k$ | Non-standard |
| 本文 | 素数 | $2+m$ | 0 | 1 | 1 | DBDH |

## 6. 结束语

随着云存储的发展，系统用户和信息量将会不断增长，方案的计算复杂度也越来越大。如何在安全的前提下，支持灵活的访问结构，用户通过少量的计算可以得到明文是一个值得研究的问题。本文提出了一种基于属性基加密的策略隐藏方案，对访问结构没有任何限制，通过将部分运算交由云服务器来计算，大大减少了用户的计算量。考虑到在实际应用中，系统中用户的属性会经常性变化，后续工作将在

此解决方案的基础上进一步研究属性撤销操作的方法。

## 参考文献


[1] 曹珍富, 董晓蕾, 周俊, 等. 大数据安全与隐私保护研究进展[J]. 计算机研究与发展, 2016, 53(10): 2137-2151.

[2] Shamir, A. (1985) Identity-Based Cryptosystems and Signature Schemes. In: *Advances in Cryptology*, Springer, Berlin Heidelberg, 47-53. https://doi.org/10.1007/3-540-39568-7_5

[3] Sahai, A. and Waters, B. (2005) Fuzzy Identity-Based Encryption. *Advances in Cryptology—EUROCRYPT* 2005. Springer, Berlin Heidelberg, 457-473. https://doi.org/10.1007/11426639_27

[4] Chander, V.P., Babu, G.C., Babu, S.S., *et al*. (2013) Procure Data Storage in Clode Using CPABE. *International Journal of Computer Trends & Technology*, **4**, 77-84.

[5] Goyal, V., Pandey, O., Sahai, A., *et al*. (2006) Attribute-Based Encryption for Fine-Grained Access Control of Encrypted Data. *Proceedings of ACMCCS*'06, ACM Press, New York, 89-98.

[6] 冯登国, 陈成. 属性密码学研究[J]. 密码学报, 2014, 1(1): 1-12.

[7] 苏金树, 曹丹, 王小峰. 属性基加密机制[J]. 软件学报, 2011, 22(6): 1299-1315.

[8] Nishide, T., Yoneyama, K. and Ohta, K. (2008) Attribute-Based Encryption with Partially Hidden Encryptor-Specified Access Structures. *ACNS* 2008: *Applied Cryptography and Network Security*, New York, 3-6 June 2008, 111-129. https://doi.org/10.1007/978-3-540-68914-0_7

[9] Lai, J., Deng, R.H. and Li, Y. (2011) Fully Secure Cipertext-Policy Hiding CP-ABE. *ISPEC* 2011: *Information Security Practice and Experience*, Guangzhou, May 30-June 1 2011, 24-39. https://doi.org/10.1007/978-3-642-21031-0_3

[10] Hur, J. (2013) Attribute-Based Secure Data Sharing with Hidden Policies in Smart Grid. *IEEE Transactions on Parallel and Distributed Systems*, **24**, 2171-2180. https://doi.org/10.1109/TPDS.2012.61

[11] 杜瑞颖, 沈剑, 陈晶, 周顺淦. 基于策略隐藏属性加密的云访问控制方案[J]. 武汉大学学报(理学版), 2016, 62(3): 242-248.

[12] 宋衍, 韩臻, 刘凤梅, 等. 基于访问树的策略隐藏属性加密方案[J]. 通信学报, 2015, 36(9): 119-126.

[13] Green, M., Hohenberger, S. and Waters, B. (2011) Outsourcing the Decryption of ABE Ciphertexts. *Proceedings of the* 20*th USENIX Conference on Security*, San Francisco, 8-12 August 2011, 34-34.

[14] Lai, J., Deng, R.H., Guan, C., *et al*. (2015) Attribute-Based Encryption with Verifiable Outsourced Decryption. *IEEE Transactions on Information Forensics & Security*, **10**, 1384-1393. https://doi.org/10.1109/TIFS.2015.2410137

[15] Liu, H., Wang, X. and Zhang, P. (2015) Verifying Outsourced Decryption of CP-ABE with Signature. 2015 4*th International Conference on Mechatronics*, *Materials*, *Chemistry and Computer Engineering*.

[16] 马华, 白翠翠, 李宾, 刘振华. 支持属性撤销和解密外包的属性基加密方案[J]. 西安电子科技大学学报, 2015, 42(6): 6-10+55.

[17] 丁晓红, 秦敬源, 王新. 一种属性基加密方案的外包解密方法[J]. 计算机科学, 2016, 43(S1): 357-360.

[18] Emura, K., Miyaji, A., Nomura, A., *et al.* (2009) A Ciphertext-Policy Attribute-Based Encryption Scheme with Constant Ciphertext Length. *Proceedings of ISPEC* 2009, Springer, Berlin, 12-23. https://doi.org/10.1007/978-3-642-00843-6_2