doi:10.11959/j.issn.1000-436x.2015327

支持动态策略更新的半策略隐藏属性加密方案

应作斌，马建峰，崔江涛
（西安电子科技大学 计算机学院，陕西 西安 710071）

摘 要：基于密文策略的属性加密被认为适用于云存储的环境，但当数据拥有者需要更新访问策略时，现有的更新方式因受数据的规模和属性集的大小的限制，会使数据拥有者增加相应的计算开销和通信开销。同时，以明文形式存放在云端的访问策略也会造成用户数据的隐私泄露。针对以上 2 个问题，提出了一种支持动态策略更新的半策略隐藏属性加密方案，使用所提方案进行策略更新时，用户的计算开销减少，大量的计算由云服务器承担。由于使用了半策略隐藏，用户的具体属性值不会泄露给其他任何第三方，有效保护了用户的隐私。此外，所提方案可以支持任何形式的策略更新，在标准模型下证明了方案是自适应选择明文攻击（CPA）安全的。
关键词：密文策略属性加密；动态策略更新；半策略隐藏；标准模型；自适应选择明文攻击安全
中图分类号：TP309 **文献标识码**：A

Partially policy hidden CP-ABE supporting dynamic policy updating

YING Zuo-bin, MA Jian-feng, CUI Jiang-tao
(School of Computer Science and Technology, Xidian University, Xi'an 710071, China)

Abstract: Ciphertext-policy attribute-based encryption (CP-ABE) was considered to be appropriate for cloud storage. However, under traditional CP-ABE scheme which was limited in terms of the scale of the data and the quantities of the attributes, computation and communication costs would be introduced correspondingly whenever the data owner wants to update the policy. Moreover, the policy which was stored in the form of plaintext would also result in privacy leakage. Aiming at tackling the above two problems, a novel scheme called partially policy hidden CP-ABE supporting dynamic policy updating (DPUPH-CP-ABE) was proposed. Through utilizing proposed scheme, the computation cost will be reduced, especially on user side, leaving the most computational work to the cloud server. Meanwhile, the value of the user's attributes will never be revealed to any third parties, and the users' privacy will be effectively preserved. Besides, the scheme is proved to be adaptively chosen plaintext attack (CPA) secure in the standard model and can support any types of policy updating.
Key words: ciphertext-policy ABE; dynamic policy updating; partially policy hidden; standard model; adaptive chosen plaintext attack secure

1 引言

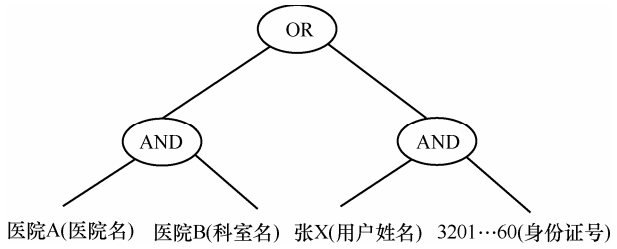
随着云计算的日益普及，越来越多的企业和个体开始接触并使用云平台。考虑到云平台存储成本的低廉以及访问的便捷性，用户习惯于将海量数据上传至云端保存，但在这些数据中，有一些包含了非常敏感的隐私信息。而绝大部分云平台被认定为是半可信的[1]，即云会遵循用户发出指令，但同时也会对存储在其上的用户数据产生好奇并尽力挖掘用户的隐私信息。因此，用户在上传数据至云端之前，需要对某些敏感的隐私数据进行加密处理。

属性加密(attribute based encryption)[2]自 2005

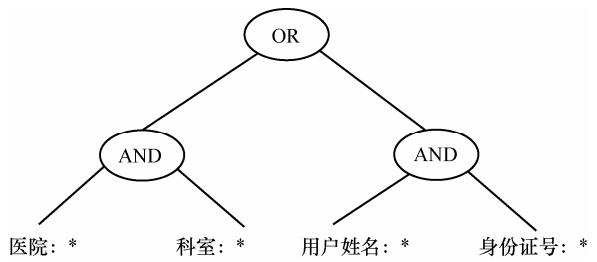
收稿日期：2015-05-25；**修回日期**：2015-08-23
基金项目：国家自然科学基金资助项目(61202179, 61173089, 61472298, U1135002)；国家高技术研究发展计划(“863”计划)基金资助项目(2015AA016007)；教育部留学回国人员科研启动计划基金资助项目
Foundation Items: The National Natural Science Foundation of China (61202179, 61173089, 61472298, U1135002); The National High Technology Research and Development Program (863 Program)(2015AA016007); SRF for ROCS, SEM and the Fundamental Research Funds for the Central Universities

年被提出至今，一直受到国内外相关研究团队的广泛关注。而结合了访问控制机制的属性加密，可以实现更加细粒度的文件访问控制操作，因此属性加密被认为是适合云存储环境的加密方式之一。

现实生活当中，个体往往包含多个属性，但属性并不都是一成不变的。有些属性会随着个体的变化而产生变更。如图 1 所示，某医疗机构将所有注册用户的医疗档案信息托管至云服务器。为了保障用户的个人隐私，机构使用用户姓名、身份证号、就诊医院、科室加密每个用户的医疗档案信息，访问策略如图 1(a)所示。这样做可以在一定程度上防止用户的隐私不被非授权用户访问，但是其存在的问题也是显而易见的。一方面，在这些属性当中，身份证号、医院、科室这些属性相较于其他属性来说是比较敏感的，其中的内容涉及到病人的个人隐私。另一方面，当病人需要转院或是转科室的时候，属性会随之变更。例如，病人甲原先所在的医院是综合型医院，后转至某心脏专科医院，则可以通过此属性判定病人甲极有可能患有心脏方面的疾病，这样就造成了病人的隐私泄露。此外，由于属性发生变更，医疗机构需要重新下载该用户的医疗档案，解密后使用新的属性重新加密再上传。这种常规的更新方式会带来巨大的通信和计算开销，效率极低。针对上述问题，本文提出了一种支持动态策略更新的半策略隐藏属性加密方案（DPUPH-CP-ABE，partially policy hidden CP-ABE supporting dynamic policy updating）。本文方案的主要思想可以概括为如下 2 方面。



(a) 常规访问策略



(b) 半策略隐藏的访问策略

图 1　常规访问策略和半策略隐藏的访问策略

1) 最大化利用当前的访问策略，通过策略比对找出需要更新的模块，生成更新密钥发送给云服务器，将大量运算外包给云服务器完成。

2) 将属性分割为属性名称和属性值 2 部分，使用半策略隐藏的方法将属性值进行隐藏，以保护用户的隐私，如图 1(b)所示。

本文方案主要有以下 3 个特点。

1) 针对动态策略更新时产生的隐私泄露，使用半策略隐藏的方案加密隐私数据。

2) 方案支持任何形式的动态策略更新，同时在引入半策略隐藏的时候不会增加密钥的长度。

3) 在标准模型下证明了该方案是自适应安全的。

ABE 的概念最早在 2005 年由 Sahai 和 Waters 提出[2]，但最基本的 ABE 只能支持 (t,n) 门限的单层结构，为了让 ABE 支持更加灵活的访问策略，学者引入树形访问控制结构，于 2006 年和 2007 年相继提出了密钥策略 ABE (KP-ABE)[3]及密文策略 ABE (CP-ABE)[4]。随后，在 2011 年，Waters[5]在维持方案效率不变的前提下，首次在标准模型下证明了 CP-ABE 的安全性。

2007 年，Chase 在文献[6]中首次考虑了多授权机构下的 ABE。在 2011 年，Lewko 等在文献[7]中提出了分权型的属性加密方案，在此方案中授权机构 CA 的职能被分散到多个 AA 中。随后，Liu 等[8]首次在标准模型下构造了的多授权机构 ABE 模型。

Goyal 在文献[3]中最早考虑了 KP-ABE 的策略更新问题。直到 2012 年，Sahai 等才在文献[9]中讨论了 CP-ABE 的策略更新问题。但这里所提到的策略更新都使用了代理(delegation)的思想，即更新后的策略需要比更新前的策略更严格。因此，当出现上文中提及的病人需要更换医院的场景时，上述方案均无法满足需求。Yang 等[10]提出了一种高效的支持所有策略更新的 CP-ABE 方案，但是只证明了其在一般群模型下是自适应安全的。

Nishide 等[11]于 2008 年首次将半策略隐藏的概念引入 CP-ABE，但该方案只支持与门的结构。Li 等[12]延续了这方面的研究，并提出了用户追责问题。上述 2 个方案都被证明是选择性安全而非自适应安全的。Lai 等[13]使用 LSSS 结构描述了半策略隐藏的 CP-ABE，并在标准模型下证明了其是自适应安全的。

2 背景知识

本节给出 DPUPH-CP-ABE 方案的系统模型、安全模型以及所需的背景知识和相关定义。

2.1 DPUPH-CP-ABE 系统模型

DPUPH-CP-ABE 方案由如下 6 个算法组成。

$Setup(1^{\lambda},U)\to PK,MSK$。*Setup* 算法输入一个安全参数 λ、属性总集合 U，输出公开参数 *PK* 和主密钥 *MSK*。

$KeyGen(PK,MSK,S=(s_1,\cdots,s_n))\to SK_S$。*KeyGen* 算法输入公开参数 *PK*，主密钥 *MSK* 以及用户的属性集合 S，输出用户私钥 SK_S。

$Encrypt(PK,M\in\mathbb{G}_T,(A,\rho,\Gamma))\to CT$。*Encrypt* 算法输入公钥 *PK*、消息 *M* 以及访问策略 (A,ρ,Γ)，输出密文 *CT*。

$Decrypt(PK,SK_S,CT)\to M$。*Decrypt* 算法输入公钥 *PK*、用户私钥 SK_S 以及密文 *CT*。当用户的属性集合 S 满足访问策略 (A,ρ,Γ) 时，正确解密，输出 *M*。否则随机输出 $\perp$，表示解密失败。

$DPUKeyGen(PK,E_{info}(M),(A,\rho,\Gamma),(A',\rho',\Gamma'))\to DPUK_M$。*DPUKeyGen* 算法输入公钥 *PK*、关于 *M* 的加密信息 $E_{info}(M)$、旧的访问策略 (A,ρ,Γ) 以及新的访问策略 (A',ρ',Γ')，生成密钥 $DPUK_M$，将被发给云服务器对原始密文 *CT* 的访问策略部分进行更新。

$CTUpdate(CT,DPUK_M)\to CT'$。*CTUpdate* 算法由云服务器执行，输入原始密文 *CT* 以及更新密钥 $DPUK_M$，通过比对将原始密文 *CT* 更新为新密文 CT'。

2.2 安全模型

下面给出 DPUPH-CP-ABE 的安全模型，敌手和挑战者之间的游戏模拟如下。

初始化 挑战者运行 $Setup(1^{\lambda},U)$，获取公钥 *PK* 及主密钥 *MSK*。挑战者将 *PK* 发给敌手 $\mathcal{A}$，自己保存 *MSK*。

询问阶段 1 敌手根据已掌握的属性 $S_1,\cdots,S_k$ 自适应的向挑战者发出密钥查询请求。挑战者运行 *KeyGen* 算法获取 $SK_{S_i},i\in[1,k]$，并将 SK_{S_i} 发给敌手。

挑战 敌手 $\mathcal{A}$ 提交 2 个等长的信息 M_0、M_1，此外，敌手还需要提供一组需要挑战的访问策略 $\{(A_i,\rho_i,\Gamma_{i0}),(A_i,\rho_i,\Gamma_{i1})\}_{i\in\{1,\cdots,q\}}$。限定条件是，敌手询问的属性集合不能满足这些访问结构。挑战者随机选择 $\beta\in\{0,1\}$，使用上述访问策略加密并得到密文 $\{C_{i0},C_{i1}\}_{i\in\{1,\cdots,q\}}$，将 $\{C_{i0},C_{i1}\}_{i\in\{1,\cdots,q\}}$ 发送给敌手作为其挑战密文集。

询问阶段 2 敌手 $\mathcal{A}$ 继续自适应的向挑战者发送询问请求，和询问阶段 1 类似，限定条件挑战阶段。$\mathcal{A}$ 也可以通过选取任意的策略更新对 $(A_x,\rho_x,\Gamma_{x,k1}),(A_y,\rho_y,\Gamma_{y,k2})$ 询问更新密钥。挑战者使用更新密钥 $DPUK_{M_\beta}$ 进行回应。

竞猜：敌手 $\mathcal{A}$ 输出关于 β 的竞猜结果 $\beta'\in\{0,1\}$，若 $\beta=\beta'$，则敌手获胜。

敌手在上述安全游戏里的优势定义为 $\left|\Pr[\beta=\beta']-\frac{1}{2}\right|$。

若任何多项式时间敌手在上述安全游戏里的优势是可以忽略的，则支持动态策略更新的方案在选择明文攻击下是半策略隐藏的。

2.3 访问结构

定义 1（访问结构[14]）。令 $\{P_1,\cdots,P_n\}$ 为所有参与者的集合。对于集合 $\mathbb{A}\subseteq 2^{\{P_1,\cdots,P_n\}}$，若存在 $\forall B,C$：若 $B\in\mathbb{A}$ 且 $B\subseteq C$，有 $C\in\mathbb{A}$。则称 $\mathbb{A}$ 是单调的。访问结构 $\mathbb{A}$ 是参与者的非空子集构成的集合，即 $\mathbb{A}\subseteq 2^{\{P_1,\cdots,P_n\}}\setminus\{\varnothing\}$。在 $\mathbb{A}$ 内的集合是授权集合，不在 $\mathbb{A}$ 内的集合为非授权集合。

在本文讨论的方案中，属性代表参与者，文中涉及的方案也只考虑单调访问结构。

2.4 线性秘密共享

定义 2（线性秘密共享）。一个定义在一组参与者 $\mathcal{P}$ 上的秘密共享方案 Π 是线性的，若

1) 每个参与者关于秘密 *s* 的分享值构成一个在 $\mathbb{Z}_p$ 上的向量；

2) 存在 Π 的一个 *l* 行 *n* 列的生成矩阵 $\boldsymbol{A}$，设存在一个映射 ρ，将生成矩阵 $\boldsymbol{A}$ 的每一行与每一个参与者相映射，选择一随机向量 $\vec{\boldsymbol{v}}=(s,r_2,\cdots,r_n)$，则 $\boldsymbol{A}\vec{\boldsymbol{v}}$ 是 *s* 关于 Π 的 *l* 个份额，$(\boldsymbol{A}\vec{\boldsymbol{v}})_i$ 隶属于参与者 $\rho(i)$。

文献[14]表明，任何一个 LSSS 方案都具有线性重构的性质。设存在一访问策略 $\mathbb{A}$，授权集合为 S，令 $I=\{i|\rho(i)\in S\}$，则存在常数 $\{\omega_i\in\mathbb{Z}_p\}_{i\in I}$，使 $\sum_{i\in I}\omega_i\lambda_i=s$。而对于非授权集合，则不存在这样的常数。

2.5 合数阶群下的困难问题假设

本文在合数阶群下构造方案，该合数群的阶为

4 个不同的素数的乘积。Boneh 最早在文献[15]中讨论了合数阶群的性质。

设 $\mathcal{G}$ 为一个群生成元，输入为安全参数 1^λ，输出为 $(e,\mathbb{G},\mathbb{G}_T,p_1,p_2,p_3,p_4)$，$p_1,p_2,p_3,p_4$ 为不同的素数，$\mathbb{G}$ 和 $\mathbb{G}_{\mathrm{T}}$ 是阶为 N 的循环群，$N=p_1p_2p_3p_4$，$e:\mathbb{G}\times\mathbb{G}\to\mathbb{G}_{\mathrm{T}}$，且具有如下性质。

1) 双线性：$\forall g,h\in\mathbb{G},x,y\in\mathbb{Z}_N,e(g^x,h^y)=e(g,h)^{xy}$。

2) 非退化性：$\exists g\in\mathbb{G}$，使 $e(g,g)$ 在 $\mathbb{G}_{\mathrm{T}}$ 中的阶为 N。

用 $\mathbb{G}_{p1},\mathbb{G}_{p2},\mathbb{G}_{p3},\mathbb{G}_{p4}$ 表示 $\mathbb{G}$ 的子群，且各自的阶分别为 p_1,p_2,p_3,p_4。若 $g_1\in\mathbb{G}_{p1}$，$g_2\in\mathbb{G}_{p2}$，则有 $e(g_1,g_2)=1$。该性质同样适用于 2 个元素分别取值于不同子群内的情况。

下面给出本文所引用的复杂性假设，假设 1~假设 3 和文献[16]中的一样，但这里用到群的阶为 4 个不同素数的乘积。文献[17]中使用了假设 4。

假设 1　设 $\mathcal{G}$ 为一个群生成元，有如下定义

$$(e,\mathbb{G},\mathbb{G}_T,p_1,p_2,p_3,p_4)\leftarrow\mathcal{G}(1^\lambda),N=p_1p_2p_3p_4,$$
$$g\overset{R}{\leftarrow}\mathbb{G}_{p1},I_3\overset{R}{\leftarrow}\mathbb{G}_{p3},I_4\overset{R}{\leftarrow}\mathbb{G}_{p4},$$
$$D=(N,e,g,I_3,I_4,\mathbb{G},\mathbb{G}_T),T_1\overset{R}{\leftarrow}\mathbb{G}_{p1}\mathbb{G}_{p2},T_2\overset{R}{\leftarrow}\mathbb{G}_{p1}$$

敌手 $\mathcal{A}$ 攻破假设 1 的优势定义为：$Adv_{\mathcal{A}}^1=|\Pr[\mathcal{A}(D,T_1)=1]-\Pr[\mathcal{A}(D,T_2)=1]|$。

定义 3　若对于任何多项式时间敌手 $\mathcal{A}$，$Adv_{\mathcal{A}}^1$ 是可忽略的，则称 $\mathcal{G}$ 满足假设 1。

假设 2　设 $\mathcal{G}$ 为一个群生成元，有如下定义

$$(e,\mathbb{G},\mathbb{G}_T,p_1,p_2,p_3,p_4)\leftarrow\mathcal{G}(1^\lambda),N=p_1p_2p_3p_4,$$
$$g,I_1\overset{R}{\leftarrow}\mathbb{G}_{p1},I_2,J_2\overset{R}{\leftarrow}\mathbb{G}_{p2},I_3,J_3\overset{R}{\leftarrow}\mathbb{G}_{p3},I_4\overset{R}{\leftarrow}\mathbb{G}_{p4},$$
$$D=(N,e,g,I_1I_2,J_2J_3,I_3,I_4,\mathbb{G},\mathbb{G}_T),$$
$$T_1\overset{R}{\leftarrow}\mathbb{G}_{p1}\times\mathbb{G}_{p2}\times\mathbb{G}_{p3},T_2\overset{R}{\leftarrow}\mathbb{G}_{p1}\times\mathbb{G}_{p3}$$

敌手 $\mathcal{A}$ 攻破假设 2 的优势定义为 $Adv_{\mathcal{A}}^2=|\Pr[\mathcal{A}(D,T_1)=1]-\Pr[\mathcal{A}(D,T_2)=1]|$。

定义 4　若对于任何多项式时间敌手 $\mathcal{A}$，$Adv_{\mathcal{A}}^2$ 是可忽略的，则称 $\mathcal{G}$ 满足假设 2。

假设 3　设 $\mathcal{G}$ 为一个群生成元，有如下定义

$$(e,\mathbb{G},\mathbb{G}_T,p_1,p_2,p_3,p_4)\leftarrow\mathcal{G}(1^\lambda),$$
$$N=p_1p_2p_3p_4,g\overset{R}{\leftarrow}\mathbb{G}_{p1},\alpha,s\in\mathbb{Z}_N,$$
$$g_2,I_2,J_2\overset{R}{\leftarrow}\mathbb{G}_{p2},I_3\overset{R}{\leftarrow}\mathbb{G}_{p3},I_4\overset{R}{\leftarrow}\mathbb{G}_{p4},$$
$$D=(N,e,g,g_2,g^\alpha I_2,g^sJ_2,J_2J_3,I_3,I_4,\mathbb{G},\mathbb{G}_T),$$
$$T_1=e(g,g)^{\alpha s},T_2\overset{R}{\leftarrow}\mathbb{G}_T$$

敌手 $\mathcal{A}$ 攻破假设 3 的优势定义为：$Adv_{\mathcal{A}}^3=|\Pr[\mathcal{A}(D,T_1)=1]-\Pr[\mathcal{A}(D,T_2)=1]|$。

定义 5　若对于任何多项式时间敌手 $\mathcal{A}$，$Adv_{\mathcal{A}}^3$ 是可忽略的，则称 $\mathcal{G}$ 满足假设 3。

假设 4　设 $\mathcal{G}$ 为一个群生成元，有如下定义

$$(e,\mathbb{G},\mathbb{G}_T,p_1,p_2,p_3,p_4)\leftarrow\mathcal{G}(1^\lambda),$$
$$N=p_1p_2p_3p_4,g,h\overset{R}{\leftarrow}\mathbb{G}_{p1},$$
$$g_2,I_2,U_2,V_2,W_2\overset{R}{\leftarrow}\mathbb{G}_{p2},t',r'\in\mathbb{Z}_N,$$
$$I_3\overset{R}{\leftarrow}\mathbb{G}_{p3},I_4,F,U_4,W_4\overset{R}{\leftarrow}\mathbb{G}_{p4},$$
$$D=(N,e,g,g_2,g^{t'}V_2,h^{t'}J_2,I_3,I_4,hF,g^{r'}W_2W_4,\mathbb{G},\mathbb{G}_T),$$
$$T_1=h^{r'}U_2U_4,T_2\overset{R}{\leftarrow}\mathbb{G}_{p1}\times\mathbb{G}_{p2}\times\mathbb{G}_{p4}$$

敌手 $\mathcal{A}$ 攻破假设 4 的优势定义为：$Adv_{\mathcal{A}}^4=|\Pr[\mathcal{A}(D,T_1)=1]-\Pr[\mathcal{A}(D,T_2)=1]|$。

定义 6　若对于任何多项式时间敌手 $\mathcal{A}$，$Adv_{\mathcal{A}}^4$ 是可忽略的，则称 $\mathcal{G}$ 满足假设 4。

3　具体方案

为了方便阅读，首先在表 1 中给出了在 DPUPH-CP-ABE 方案中用到的主要符号的描述。

本文方案使用的基本 CP-ABE 模型和文献[16]中的类似，区别在于，本文方案里的属性名称在一个访问结构里只能使用一次。

本文方案支持任何单调的访问结构，使用 LSSS 结构进行描述，方案中的每个属性都由 2 部分构成：属性名称和属性值。为方便描述，假设属性有 n 个不同的范畴，且每个属性分属不同的范畴，则每个用户有 n 个属性。用 i 指代第 i 个范畴的属性名。这样一个用户的属性集合 S 就可以划分为 $(s_1,\cdots,s_n)$。$s_i\in\mathbb{Z}_N$ 表示属性 i 的值。本文用 $(\boldsymbol{A},\rho,\Gamma)$ 表示访问结构，其中，$\boldsymbol{A}$ 是被分享的生成矩阵，ρ 把每一行和每个属性名称相映射，Γ 可以被分为 $(v_{\rho(1)},\cdots,v_{\rho(l)})$，$v_{\rho(i)}$ 是由访问策略指定的 $\rho(i)$ 的值。

按照这样的定义，一个用户的属性集合 S 满足访问结构 $(\boldsymbol{A},\rho,\Gamma)$，当且仅当存在 $\mathcal{L}\subseteq\{1,\cdots,l\}$ 及常数 $\{\omega_i\}_{i\in\mathcal{L}}$，使 $\sum_{i\in\mathcal{L}}\omega_iA_i=(1,0,\cdots,0)$ 且 $s_{\rho(i)}=v_{\rho(i)}\ \forall i\in\mathcal{L}$，这里 A_i 表示 $\boldsymbol{A}$ 的第 i 行。

请注意，在接下来的方案介绍中，属性值（即 Γ ）是始终被隐藏起来的，因此属性值的更新不会造成隐私信息的泄露，但是访问结构的其他部分（即 $(\boldsymbol{A},\rho)$ ）是可见的，并和密文一起发送给云进行保存。

表 1 DPUPH-CP-ABE 符号说明

符号	描述
U	属性总集合
PK, MSK, SK_S	系统公开参数，主密钥及用户私钥
CT, CT'	原始密文及新密文
$(\boldsymbol{A},\rho,\Gamma),(\boldsymbol{A}',\rho',\Gamma')$	旧访问策略及新访问策略。其中 $\boldsymbol{A}$ 是被分享的矩阵，ρ 将属性和每一行映射，Γ 为属性值，$(\boldsymbol{A}',\rho',\Gamma')$ 的定义与其类似
$E_{info}(M)$	关于 M 的加密信息，用于策略更新
$DPUK_M$	关于 M 的升级秘钥，发给云端对原始密文 CT 进行更新
$R_{1,A'}, R_{2,A'}, R_{3,A'}$	新旧策略对比后产生的属性名称对应的行索引信息

3.1 DPUPH-CP-ABE

在文献[13]的基础上构造了本文的方案，不同之处在于，本方案中增加的 *DPUKeyGen* 和 *CTUpdate* 算法可支持任何形式的访问策略更新，同时支持半策略隐藏，方案具体构造如下。

Setup$(1^\lambda, U)$。*Setup* 算法首先运行 $\mathcal{G}(1^\lambda)$，获取 $(e,\mathbb{G},\mathbb{G}_T,p_1,p_2,p_3,p_4)$。$\mathbb{G}=\mathbb{G}_{p1}\times\mathbb{G}_{p2}\times\mathbb{G}_{p3}\times\mathbb{G}_{p4}$。$\mathbb{G}$ 和 $\mathbb{G}_T$ 是阶为 N 的循环群，$N=p_1p_2p_3p_4$。属性总集合为 $U\in\mathbb{Z}_N$。接下来，系统将随机选择 $\alpha,s\in\mathbb{Z}_N,g,h,u_1,\cdots,u_n\in\mathbb{G}_{p1},I_3\in\mathbb{G}_{p3},I_4,F\in\mathbb{G}_{p4}$。最终得到公钥 $PK=(g,g^a,e(g,g)^\alpha,u_1,\cdots,u_n,H=hF,I_4)$。主密钥为 $MSK=(\alpha,h,I_3)$。

KeyGen$(PK,MSK,S=(s_1,\cdots,s_n))$。*KeyGen* 算法随机选择 $t\in\mathbb{Z}_N,R,R',R_1,\cdots,R_n\in\mathbb{G}_{p3}$。生成的用户私钥 $SK_S=\left(S,K,K',\{K_i\}_{1\leqslant i\leqslant n}\right)$ 为 $K=g^\alpha g^{at}R$，$K'=g^tR'$，$K_i=\left(u_i^{s_i}h\right)^t R_i$。

Encrypt$(PK,M\in\mathbb{G}_T,(A,\rho,\Gamma))$。*Encrypt* 算法设定 $\boldsymbol{A}$ 为 l 行 n 列的生成矩阵，映射 ρ 将生成矩阵 $\boldsymbol{A}$ 的每一行 A_x 与每一个属性名称相映射，$\Gamma=\left(v_{\rho(1)},\cdots,v_{\rho(l)}\right)\in\mathbb{Z}_N^l$。任意选择 2 个向量 $\vec{\boldsymbol{v}},\vec{\boldsymbol{v}'}\in\mathbb{Z}_N^n$，令 $\vec{\boldsymbol{v}}=(s,v_2,\cdots,v_n)$，$\vec{\boldsymbol{v}'}=(s',v_2',\cdots,v_n')$。对于 $1\leqslant x\leqslant l$，随机选择 $r_x,r_x'\in\mathbb{Z}_N,F_{1,x},F_{1,x}',F_{2,x},F_{2,x}'\in\mathbb{G}_{p4}$。生成密文 $C=((\boldsymbol{A},\rho),\tilde{C}_1,C_1',\{C_{1,x},D_{1,x}\}_{1\leqslant x\leqslant l},\tilde{C}_2,C_2',\{C_{2,x},D_{2,x}\}_{1\leqslant x\leqslant l})$，其中

$$\tilde{C}_1=Me(g,g)^{\alpha s},C_1'=g^s,$$

$$C_{1,x}=g^{aA_x\vec{v}}\left(u_{\rho(x)}^{v_{\rho(x)}}H\right)^{-r_x}F_{1,x},$$

$$D_{1,x}=g^{r_x}F_{1,x}',$$

$$\tilde{C}_2=Me(g,g)^{\alpha s'},C_2'=g^{s'},$$

$$C_{2,x}=g^{aA_x\vec{v}'}\left(u_{\rho(x)}^{v_{\rho(x)}}H\right)^{-r_x'}F_{2,x},$$

$$D_{2,x}=g^{r_x'}F_{2,x}'$$

同时，算法还会输出关于 M 的加密信息 $E_{info}(M)=\{s,r_1,\cdots,r_x,r_1',\cdots,r_x',F_{1,x},F_{1,x}',F_{2,x},F_{2,x}'\}$。这部分信息将由数据拥有者妥善保存，并用于下面的 *DPUKeyGen* 算法中生成更新密钥。

Decrypt(PK,SK_S,CT)。*Decrypt* 算法输入密文 CT，用户私钥 SK_S，$S=(s_1,\cdots,s_n)$。解密算法首先计算可以满足 $(\boldsymbol{A},\rho)$ 的最小子集访问结构 $\min_{(\boldsymbol{A},\rho)}$，然后确定是否存在 $\mathcal{L}\in\min_{(\boldsymbol{A},\rho)}$，使 $\tilde{C}_2=\dfrac{e(C_2',K)}{\prod_{i\in\mathcal{L}}\left(e(C_{2,i},K')e\left(D_{2,i},K_{\rho(i)}\right)\right)^{\omega_i}}$，其中，$\sum_{i\in\mathcal{L}}\omega_iA_i=(1,0,\cdots,0)$。

若在 $\min_{(\boldsymbol{A},\rho)}$ 找不到任何值可以满足上述等式，则判定解密失败，输出 $\perp$。否则将计算：$\dfrac{e(C_1',K)}{\prod_{i\in\mathcal{L}}\left(e(C_{1,i},K')e\left(D_{1,i},K_{\rho(i)}\right)\right)^{\omega_i}}=\dfrac{e(g,g)^{\alpha s}e(g,g)^{ats}}{\prod_{i\in\mathcal{L}}e(g,g)^{atA_i\omega_i\vec{v}}}=e(g,g)^{\alpha s}$。再通过 $\dfrac{\tilde{C}_1}{e(g,g)^{\alpha s}}$，可以恢复出 M。

在本文提出的方案中，密文可以分为 2 部分：$(\tilde{C}_1,C_1',\{C_{1,x},D_{1,x}\}_{1\leqslant x\leqslant l})$ 和 $(\tilde{C}_2,C_2',\{C_{2,x},D_{2,x}\}_{1\leqslant x\leqslant l})$。第一部分为原始 CP-ABE 加密方案，第二部分是冗余部分，可以看作是第一部分的加密。如果一个用户私钥对应的属性满足访问策略，密文的冗余部分可以帮助用户确定哪个属性集合满足访问策略。这样用户就可以使用相关信息和私钥解密密文的第一部分，获取 M。

当数据提供者上传的文件所对应的访问策略发生变更时，最简单的操作是将该文件下载，解密后使用新的策略重新加密，然后重新上传至云端，但此方法会带来极大的通信开销，同时也会让数据提供者承担巨大的加解密运算开销。为了确保用户的数据安全

性，同时也为了最大程度降低各种开销，本文方案选择使用原始密文中的加密信息 $E_{info}(M)=\{s,r_1,\cdots,r_x,r_1',\cdots,r_x',F_{1,x},F_{1,x}',F_{2,x},F_{2,x}'\}$，其中随机数 s、群随机元素 $\{F_{1,x},F_{1,x}',F_{2,x},F_{2,x}'\}$ 和原始密文中保持一致，$\{r_1,\cdots,r_x,r_1',\cdots,r_x'\}$ 作为新随机数的参照。

在运行 *DPUKeyGen* 之前，系统首先要执行 PolicyComp 算法，对新旧策略进行比对。该算法输出参与属性名称的行索引信息，这些信息可以被归为 3 类：$R_{1,A'},R_{2,A'},R_{3,A'}$。$R_{1,A'},R_{2,A'}$ 共同表示新的属性名称 $\rho'(y)$ 在当前的策略中存在。若 $num_{\rho'(y),A'}\leqslant num_{\rho'(y),A}$，则令 $\rho(x)=\rho'(y)$，并将索引信息放入 $R_{1,A'}$。若 $num_{\rho'(y),A'}>num_{\rho'(y),A}$，则表示出现了多次新属性名称，将多出的新属性名称索引信息放入 $R_{2,A'}$ 中。$R_{3,A'}$ 中记录的是没有出现在当前策略中的属性名称，即新属性名称。

$DPUKeyGen(PK,E_{info}(M),(A,\rho,\Gamma),(A',\rho',\Gamma'))$。数据拥有者运行该算法获取更新密钥，*PK* 为公钥，$E_{info}(M)$ 是关于 *M* 的加密信息，$(\boldsymbol{A},\rho,\Gamma)$ 为旧的访问策略，$(\boldsymbol{A}',\rho',\Gamma')$ 为新的访问策略。生成的密钥 $DPUK_M$ 将被用于原始密文 *CT* 的访问策略部分的更新。请注意，在策略变更过程中，属性的值 $\Gamma=(v_{\rho(1)},\cdots,v_{\rho(l)})$ 中 $v_{\rho(i)}$ 是由访问策略指定的 $\rho(i)$ 的值，只会根据访问策略的变化而变化，数据拥有者将所有的属性值 Γ 更新为新属性值 Γ'。

算法将随机选择一个新的向量 $\vec{\boldsymbol{w}}\in\mathbb{Z}_p^{n'}$，将 s 选作其第一个值，$\overrightarrow{\boldsymbol{w}'}\in\mathbb{Z}_p^{n'}$，将 s' 选作其第一个值，然后计算如下。

1) $\delta_x=A_x\vec{\boldsymbol{v}}$。$A_x$ 是 $\boldsymbol{A}$ 中的第 x 行对应的有效分享值。

2) $\delta_y'=A_y'\vec{\boldsymbol{w}}$。$A_y'$ 是 $\boldsymbol{A}$ 中的第 y 行对应的有效分享值。

3) $\delta_x'=A_x\overrightarrow{\boldsymbol{v}'}$。$A_x$ 是 $\boldsymbol{A}$ 中的第 x 行对应的有效分享值（该项为冗余部分）。

4) $\delta_y''=A_y'\overrightarrow{\boldsymbol{w}'}$。$A_y'$ 是 $\boldsymbol{A}$ 中的第 y 行对应的有效分享值（该项为冗余部分）。

5) $R_A=\{1,\cdots,l\}$ 为 $\boldsymbol{A}$ 中的行索引。

6) $v_{\rho'(y)}$ 为更新新策略后对应的属性值。

对于每个 $y\in[1,\cdots,l']$，随机选择 $F_{1,y},F_{1,y}',F_{2,y},F_{2,y}'\in\mathbb{G}_{p4}$。

TYPE1: $(y,x)\in R_{1,A'}$，更新密钥的元素为

$$DPUK_{y,x,M}=\left(C_{1,x}^{\uparrow}=g^{a\delta_y'-\delta_x}\frac{F_{1,y}}{F_{1,x}},u_{\rho'(y)}^{v_{\rho'(y)}},D_{1,x}^{\uparrow}=\frac{F_{1,y}'}{F_{1,x}'},\right.$$

$$\left.C_{2,x}^{\uparrow}=g^{a\delta_y''-\delta_x'}\frac{F_{2,y}}{F_{2,x}},D_{2,x}^{\uparrow}=\frac{F_{2,y}'}{F_{2,x}'}\right)$$

设 $r_y'=r_x,r_y''=r_x'$。

TYPE2: $(y,x)\in R_{2,A'}$，算法随机选择 r_y',r_y''，$d_y\in\mathbb{Z}_p$，生成更新密钥元素

$$DPUK_{y,x,M}=\left(d_y,C_{1,x}^{\uparrow}=g^{a\delta_y'-d_y\delta_x}\frac{F_{1,y}}{F_{1,x}},u_{\rho'(y)}^{v_{\rho'(y)}},\right.$$

$$\left.D_{1,x}^{\uparrow}=\frac{F_{1,y}'}{F_{1,x}'},C_{2,x}^{\uparrow}=g^{a\delta_y''-d_y\delta_x'}\frac{F_{2,y}}{F_{2,x}},D_{2,x}^{\uparrow}=\frac{F_{2,y}'}{F_{2,x}'}\right)$$

TYPE 3: $(y,x)\in R_{3,A'}$，算法随机选择 $r_y',r_y''\in\mathbb{Z}_p$，生成更新密钥元素

$$DPUK_{y,x,M}=(C_{1,x}^{\uparrow}=g^{a\delta_y'}\left(u_{\rho'(y)}^{v_{\rho'(y)}}H\right)^{-r_y'}F_{1,y},$$

$$C_{2,x}^{\uparrow}=g^{a\delta_y''}\left(u_{\rho'(y)}^{v_{\rho'(y)}}H\right)^{-r_y''}F_{2,y},D_{1,x}^{\uparrow}=g^{-r_y'}F_{1,y}',$$

$$D_{2,x}^{\uparrow}=g^{-r_y''}F_{2,y}')$$

因此，更新密钥构成如下

$$DPUK_M=\left(\left(\text{TYPE1},\left\{DPUK_{y,x,M}\right\}_{(y,x)\in R_{1,A'}}\right)\right.$$

$$\left(\text{TYPE2},\left\{DPUK_{y,x,M}\right\}_{(y,x)\in R_{2,A'}}\right)$$

$$\left.\left(\text{TYPE3},\left\{DPUK_{y,x,M}\right\}_{(y,x)\in R_{3,A'}}\right)\right)$$

接下来，数据拥有者将更新密钥 $DPUK_M$ 发送至云服务器。

$CTUpdate(CT,DPUK_M)$。用户将上一步生成的 $DPUK_M$ 发送至云服务器，云收到更新密钥后，对于每一个 $y=[1,\cdots,l']$，将原始密文 *CT* 根据更新密钥 $DPUK_M$ 里的新策略更新为 CT'。具体更新方法如下。

类型 1　$y\in R_{1,A'}$，新密文组件 E' 为

$$E'=(C_1'=g^s,C_{1,y}=C_{1,x}C_{1,x}^{\uparrow}=g^{aA_y'\vec{\boldsymbol{w}}}\left(u_{\rho'(y)}^{v_{\rho'(y)}}H\right)^{-r_y'}F_{1,y},$$

$$D_{1,y}=g^{r_y'}F_{1,y}',C_2'=g^{s'},$$

$$C_{2,y}=C_{2,x}C_{2,x}^{\uparrow}=g^{aA_y'\overrightarrow{\boldsymbol{w}'}}\left(u_{\rho'(y)}^{v_{\rho'(y)}}H\right)^{-r_y''}F_{2,y},D_{2,y}=g^{r_y''}F_{2,y}')$$

这里 $r_y'=r_x,r_y''=r_x'$。

类型 2　$y\in R_{2,A'}$，新密文组件 E' 为

$$E'=(C_1'=g^s,C_{1,y}=\left(C_{1,x}\right)^{d_y}C_{1,x}^{\uparrow}=g^{aA_y'\vec{\boldsymbol{w}}}\left(u_{\rho'(y)}^{v_{\rho'(y)}}H\right)^{-r_y'}F_{1,y},$$

$$D_{1,y}=g^{r_y'}F_{1,y}',C_2'=g^{s'},C_{2,y}=\left(C_{2,x}\right)^{d_y}C_{2,x}^{\uparrow}$$

$$= g^{\alpha A_y^{'}\vec{\boldsymbol{w}}}\left(u_{\rho'(y)}^{v_{\rho'(y)}}H\right)^{-r_y^{''}}F_{2,y}, D_{2,y} = g^{r_y^{''}}F_{2,y}^{'})$$

这里 $r_y^{'} = d_y r_x, r_y^{''} = d_y r_x^{'}$。

类型 3 $y \in R_{3,A'}$，新密文组件 E' 为

$$E' = (C_1^{'} = g^s, C_{1,y} = C_{1,x}^{\uparrow} = g^{\alpha A_y^{'}\vec{\boldsymbol{w}}}\left(u_{\rho'(y)}^{v_{\rho'(y)}}H\right)^{-r_y^{'}}F_{1,y},$$

$$D_{1,y} = g^{r_y^{'}}F_{1,y}^{'}, C_2^{'} = g^{s'}, C_{2,y} = C_{2,x}^{\uparrow} = g^{\alpha A_y^{'}\vec{\boldsymbol{w}}}\left(u_{\rho'(y)}^{v_{\rho'(y)}}H\right)^{-r_y^{''}}F_{2,y},$$

$$D_{2,y} = g^{r_y^{''}}F_{2,y}^{'})$$

这样，新密文 CT' 就被重构为：$CT' = \left(\tilde{C}_1 = Me(g,g)^{\alpha s}, E' \mid \forall y \in [1,\cdots,l']\right)$。

在整个更新过程中，数据拥有者只需要做很少的一部分运算，大量的更新操作被交给云服务器执行，大大节省了通信和计算开销。

3.2 安全性证明

首先给出关于 DPUPH-CP-ABE 的安全定理。

定理 1 若假设 1~假设 4 成立，则本文方案在选择明文攻击下是半策略隐藏的。

证明 参照 Lewko 和 Waters 在文献[18]中的可证明安全，同样定义 2 个额外的结构：半功能密文（semi-functional ciphertext）和半功能密钥（semi-functional key）。在真实系统中不会用到这 2 个结构，它们仅出现在安全性证明里。

半功能密文令 g_2 表示 $\mathbb{G}_{p2}$ 的生成元。构造半功能密文如下：首先使用加密算法生成常规密文 $C' = \left((\boldsymbol{A},\boldsymbol{\rho}), \tilde{C}_1^{'}, C_1^{'}, \left\{C_{1,x}^{'}, D_{1,x}^{'}\right\}_{1\leqslant x\leqslant l}, \tilde{C}_2^{'}, C_2^{'}, \left\{C_{2,x}^{'}, D_{2,x}^{'}\right\}_{1\leqslant x\leqslant l}\right)$。然后随机选择指数 $c, c' \in \mathbb{Z}_N$，2 个随机的向量 $\vec{\boldsymbol{\omega}}, \overrightarrow{\boldsymbol{\omega}'} \in \mathbb{Z}_N^n$。再选择和属性相关的 $z_i \in \mathbb{Z}_N$，以及和生成矩阵 $\boldsymbol{A}$ 的每一行相关的 $\gamma_x, \gamma_x^{'} \in \mathbb{Z}_N$，半功能密文构成如下

$$\left((\boldsymbol{A},\boldsymbol{\rho}), \tilde{C}_1 = \tilde{C}_1^{'}, C_1^{'} = C_1^{''}g_2^{c}, \{C_{1,x} = C_{1,x}^{'}g_2^{A_x\vec{\boldsymbol{\omega}}+\gamma_x z_{\rho(x)}},\right.$$
$$D_{1,x} = D_{1,x}^{'}g_2^{-\gamma_x}\}_{1\leqslant x\leqslant l}, C_2^{'} = C_2^{''}g_2^{c'},$$
$$\left.\left\{C_{2,x} = C_{2,x}^{'}g_2^{A_x\overrightarrow{\boldsymbol{\omega}'}+\gamma_x' z_{\rho(x)}}, D_{2,x} = D_{2,x}^{'}g_2^{-\gamma_x'}\right\}_{1\leqslant x\leqslant l}\right)$$

半功能密钥可能呈现如下 3 种形式，为了生成半功能密钥，首先需要用到密钥生成算法生成常规的密钥 $SK_S^{'} = \left(S, K', K'', \left\{K_i^{'}\right\}_{1\leqslant i\leqslant n}\right), SK_S = \left(S, K, K', \left\{K_i\right\}_{1\leqslant i\leqslant n}\right)$。接下来随机选择 $d, d', d_i \in \mathbb{Z}_N$。

类型 1 的半功能密钥设定为：$(S, K = K'g_2^{d}, K' = K''g_2^{d'}, \{K_i = K_i^{'}g_2^{d'z_i}\}_{1\leqslant i\leqslant n})$。

类型 2 的半功能密钥设定为：$(S, K = K'g_2^{d}, K' = K'', \{K_i = K_i^{'}\}_{1\leqslant i\leqslant n})$。

类型 3 的半功能密钥设定为：$(S, K = K'g_2^{d}, K' = K''g_2^{d'}, \{K_i = K_i^{'}g_2^{d'}\}_{1\leqslant i\leqslant n})$。

将通过假设 1~假设 4 来证明方案的安全性，这些假设使用的是建立在一个系列游戏上的混合论证方式。第一个游戏 $Game_{\text{real}}$ 是真实的安全性游戏（其中的密文和密钥均是常规的）。在 $Game_0$ 中，所有的密钥是常规的，但挑战密文是半功能的，令 q 表示敌手的密钥查询次数，则对于 $k = [1,\cdots,q]$，有如下定义。

$Game_{k,1}$ 中的挑战密文为半功能的，前 $k-1$ 个密钥为类型 3 的半功能密钥，第 k 密钥为类型 1 的半功能密钥，剩余的密钥为常规密钥。

$Game_{k,2}$ 中的挑战密文为半功能的，前 $k-1$ 个密钥为类型 3 的半功能密钥，第 k 密钥为类型 2 的半功能密钥，剩余的密钥为常规密钥。

$Game_{k,3}$ 中的挑战密文为半功能的，前 k 个密钥为类型 3 的半功能密钥，剩余密钥为常规密钥。

为了方便描述，用 $Game_{0,3}$ 表示 $Game_0$。值得注意的是，在 $Game_{q,3}$ 里，所有的密钥均为类型 3 的半功能密钥。在倒数第二个游戏 $Game_{final_0}$ 中，所有密钥均为半功能密钥，密文也是关于一个敌手提供的随机信息（非 M_0, M_1）的半功能加密的密文。最终游戏 $Game_{final_1}$ 和 $Game_{final_0}$ 类似，区别在于生成的挑战密文中，$C_{1,x}$ 和 $C_{2,x}$ 是从 $\mathbb{G}_{p1}\times\mathbb{G}_{p2}\times\mathbb{G}_{p4}$ 中随机选择的，因此密文可以独立于敌手提供的 Γ_0 和 Γ_1。很明显，在最终的游戏中，任何敌手的优势都不会大于 0。

下面通过 6 个引理来证明这些游戏是不可区分的[13]。由此可以得出，在 $Game_{\text{real}}$ 中，敌手的优势是可以忽略的。定理 1 由此得证。

引理 1 假设 $\mathcal{G}$ 可以满足假设 1，则 $Game_{\text{real}}$ 和 $Game_0$ 是计算性不可区分的。

证明 假设存在一多项式时间敌手 $\mathcal{A}$ 可以区分 $Game_{\text{real}}$ 和 $Game_0$，则可以构造一个算法 $\mathcal{B}$ 以不可忽略的优势攻破假设 1。$\mathcal{B}$ 获取 g, I_3, I_4, T，并可以和 $\mathcal{A}$ 模拟游戏 $Game_{\text{real}}$ 或 $Game_0$。$\mathcal{B}$ 随机选择 $\alpha, a, a_0, a_1, \cdots, a_n \in \mathbb{Z}_N, F \in \mathbb{G}_{p4}$。然后令 $h = g^{a_0}$，$u_1 = g^{a_1}, \cdots, u_n = g^{a_n}$，再将公开参数发给敌手 $\mathcal{A}$，公开参数为：$PK = (N, g, g^a, e(g,g)^{\alpha}, u_1, \cdots, u_n, H = hF, I_4)$。

因为 $\mathcal{B}$ 持有主密钥 $MSK=(\alpha,h,I_3)$。它可以根据 $\mathcal{A}$ 发出的密钥询问请求生成常规密钥。

在某一时刻，$\mathcal{A}$ 向 $\mathcal{B}$ 发送 2 个等长的消息 M_0,M_1 以及一组需要挑战的访问策略 $\{(\boldsymbol{A}_i,\rho_i,\Gamma_{i0}),(\boldsymbol{A}_i,\rho_i,\Gamma_{i1})\}_{i\in\{1,\cdots,q\}}$，$\mathcal{B}$ 随机选择 $\beta\in\{0,1\}$，执行下面的操作。

1) $\mathcal{B}$ 随机选择 $\tilde{v}_2,\cdots,\tilde{v}_n,\tilde{v}_2',\cdots,\tilde{v}_n'\in\mathbb{Z}_N$，生成向量 $\tilde{\boldsymbol{v}}=(1,\tilde{v}_2,\cdots,\tilde{v}_n),\tilde{\boldsymbol{v}}'=(1,\tilde{v}_2',\cdots,\tilde{v}_n')$。

2) 对于 $1\leqslant x\leqslant l$，$\mathcal{B}$ 随机选择 $\tilde{r}_x,\tilde{r}_x'\in\mathbb{Z}_N$，$\tilde{F}_{1,x},\tilde{F}_{1,x}',\tilde{F}_{2,x},\tilde{F}_{2,x}'\in\mathbb{G}_{p4}$。

3) 令 $\Gamma_\beta=\left(v_{\rho(1)},\ldots,v_{\rho(l)}\right)$。$\mathcal{B}$ 随机选择指数 $\tilde{s}\in\mathbb{Z}_N$ 并计算

$$\tilde{C}_1=M_\beta e\left(g^\alpha,T\right),C_1'=T,C_{1,x}=T^{aA_x\vec{v}}T^{-\left(a_0+a_{\rho(x)}v_{\rho(x)}\right)\tilde{r}_x}\tilde{F}_{1,x},$$
$$D_{1,x}=T^{\tilde{r}_x}\tilde{F}_{1,x}'$$

$$\tilde{C}_2=e\left(g^\alpha,T^{\tilde{s}}\right),C_2'=T^{\tilde{s}},C_{2,x}=T^{\tilde{s}aA_x\cdot\vec{v}'}T^{-\left(a_0+a_{\rho(x)}v_{\rho(x)}\right)\tilde{r}_x'}\tilde{F}_{2,x},$$
$$D_{2,x}=T^{\tilde{r}_x'}\tilde{F}_{2,x}'$$

4) $\mathcal{B}$ 设定挑战密文为 $C=((\boldsymbol{A},\rho),\tilde{C}_1,C_1',\{C_{1,x},D_{1,x}\}_{1\leqslant x\leqslant l},\tilde{C}_2,C_2',\{C_{2,x},D_{2,x}\}_{1\leqslant x\leqslant l})$ 并将其发送给 $\mathcal{A}$。

若 $T\overset{R}{\leftarrow}\mathbb{G}_{p1}\times\mathbb{G}_{p2}$，令 $T=g^sg_2^c$，则

$$\tilde{C}_1=M_\beta e(g,g)^{\alpha s},C_1'=g^sg_2^c,$$
$$C_{1,x}=g^{aA_x\vec{v}}\left(u_{\rho(x)}^{v_{\rho(x)}}H\right)^{-r_x}F_{1,x}g_2^{A_x\vec{\omega}+\gamma_xz_{\rho(x)}},$$
$$D_{1,x}=g^{r_x}F_{1,x}'g_2^{-\gamma_x};$$
$$\tilde{C}_2=Me(g,g)^{\alpha s'},C_2'=g^{s'}g_2^{c'},$$
$$C_{2,x}=g^{aA_x\vec{v}'}\left(u_{\rho(x)}^{v_{\rho(x)}}H\right)^{-r_x'}F_{2,x}g_2^{A_x\vec{\omega}'+\gamma_x'z_{\rho(x)}},$$
$$D_{2,x}=g^{r_x'}F_{2,x}'g_2^{-\gamma_x'}$$

其中，$s'=s\tilde{s},c'=c\tilde{s},\vec{\boldsymbol{v}}=(s,s\tilde{v}_2,\cdots,s\tilde{v}_n),\vec{\boldsymbol{v}'}=(s',s'\tilde{v}_2',\cdots,s'\tilde{v}_n')$，$r_x=s\tilde{r}_x,r_x'=s\tilde{r}_x',F_{1,x}=\tilde{F}_{1,x}F^{r_x},F_{2,x}=\tilde{F}_{2,x}F^{r_x}$，$\vec{\boldsymbol{\omega}}=ca\tilde{\boldsymbol{v}},\vec{\boldsymbol{\omega}'}=c\tilde{s}a\tilde{\boldsymbol{v}}',\gamma_x=-c\tilde{r}_x,\gamma_x'=-c\tilde{r}_x',v_{\rho(x)}=a_0+a_{\rho(x)}v_{\rho(x)}$。这是一个半功能密文，$\mathcal{B}$ 模拟的是 $Game_0$。这里的 $a,a_0,a_{\rho(x)},v_{\rho(x)},\tilde{s},\tilde{v}_2,\cdots,\tilde{v}_n,\tilde{v}_2',\cdots,\tilde{v}_n',\tilde{r}_x,\tilde{r}_x'$ 模 p_1 的值和其模 p_2 的值无任何联系，因此这些参数是均匀分布的。如果 $T\overset{R}{\leftarrow}\mathbb{G}_{p1}$，很容易发现这是一个常规密文，$\mathcal{B}$ 模拟的是 $Game_{\text{real}}$。敌手 $\mathcal{A}$ 还可以对 *DPUKeyGen* 算法生成的更新密钥进行查询以获取更多信息，考虑如下的 2 个更新密钥查询 $DPUK\left(m_0,\left(\boldsymbol{A}_x,\rho_x,\Gamma_{x,k1}\right),\left(\boldsymbol{A}_y,\rho_y,\Gamma_{y,k2}\right)\right)$ 和 $DPUK\left(m_1,\left(\boldsymbol{A}_x,\rho_x,\Gamma_{x,k1}\right),\left(\boldsymbol{A}_y,\rho_y,\Gamma_{y,k2}\right)\right)$。由于 $\mathcal{B}$ 在每一次的安全游戏中只选一次 $\beta\in\{0,1\}$。*DPUKeyGen* 算法回复给敌手 $\mathcal{A}$ 的更新密钥没有泄露需要挑战的信息，换句话说，敌手 $\mathcal{A}$ 通过对更新密钥的查询并未获取更多可以优势。因此，$\mathcal{B}$ 可以使用 $\mathcal{A}$ 的输出来获取区分 T 的可能性。证毕。

引理 2　假设 $\mathcal{G}$ 可以满足假设 2，则 $Game_{k-1,3}$ 和 $Game_{k,1}$ 是计算性不可区分的。

证明　假设存在一多项式时间敌手 $\mathcal{A}$ 可以区分 $Game_{k-1,3}$ 和 $Game_{k,1}$。则可以构造一个算法 $\mathcal{B}$ 以不可忽略的优势攻破假设 2。$\mathcal{B}$ 获取 $g,I_1I_2,J_2J_3,I_3,I_4,T$，并可以和 $\mathcal{A}$ 模拟游戏 $Game_{k-1,3}$ 或 $Game_{k,1}$。$\mathcal{B}$ 随机选择 $\alpha,a,a_0,a_1,\cdots,a_n\in\mathbb{Z}_N,F\in\mathbb{G}_{p4}$。然后令 $h=g^{a_0},u_1=g^{a_1},\cdots,u_n=g^{a_n}$，再将公开参数发给敌手 $\mathcal{A}$，公开参数为：$PK=(N,g,g^a,e(g,g)^\alpha,\ u_1,\cdots,u_n,H=hF,I_4)$。

因为 $\mathcal{B}$ 持有主密钥 $MSK=(\alpha,h,I_3)$。下面解释 $\mathcal{B}$ 如何应对属性集为 $S=(s_1,\cdots,s_n)$ 时第 j 密钥查询。

当 $j<k$，$\mathcal{B}$ 随机选择 $t,\tilde{d},\tilde{d}',\tilde{d}_1',\cdots,\tilde{d}_n'\in\mathbb{Z}_N$，创建一个类型 3 的半功能密钥，设定

$$K=g^\alpha g^{at}\left(J_2J_3\right)^{\tilde{d}},K'=g^t\left(J_2J_3\right)^{\tilde{d}'},$$
$$\left\{K_i=(u_i^{s_i}h)^t\left(J_2J_3\right)^{\tilde{d}_i'}\right\}_{1\leqslant i\leqslant n}$$

请注意，因 $\tilde{d},\tilde{d}',\tilde{d}_i'$ 模 p_2 的值与其模 p_3 的值无任何联系，故这是一个均匀分布的类型 3 半功能性密钥。

当 $j>k$，$\mathcal{B}$ 运行密钥生成算法生成常规密钥。

对属性集为 $S=(s_1,\cdots,s_n)$ 时第 k 密钥查询。$\mathcal{B}$ 随机选择 $\tilde{R},\tilde{R}',\tilde{R}_1,\cdots,\tilde{R}_n\in\mathbb{G}_{p3}$ 并设定

$$K=g^\alpha T^a\tilde{R},K'=T\tilde{R}',\left\{K_i=T^{a_0+a_is_i}\tilde{R}_i\right\}_{1\leqslant i\leqslant n}$$

容易得出，若 $T\overset{R}{\leftarrow}\mathbb{G}_{p1}\times\mathbb{G}_{p2}\times\mathbb{G}_{p3}$，则 T 可以记为 $g^tg_2^{d'}\tilde{R}$，同时

$$K=g^\alpha g^{at}Rg_2^d,K'=g^tR'g_2^{d'}\ \left\{K_i=(u_i^{s_i}h)^tR_ig_2^{d'z_i}\right\}_{1\leqslant i\leqslant n}$$

其中，$R=\bar{R}^a\tilde{R},d=ad',R'=\bar{R}\tilde{R}',R_i=\bar{R}^{a_0+a_is_i}\tilde{R}_i,z_i=a_0+a_is_i$。这是一个类型 1 的半功能密钥。注意 a,a_0,a_i,s_i 模 p_1 的值和其模 p_2 的值无任何联系。若 $T\overset{R}{\leftarrow}\mathbb{G}_{p1}\times\mathbb{G}_{p3}$，这是一个均匀分布的常规密钥。

在某一时刻，$\mathcal{A}$ 向 $\mathcal{B}$ 发送 2 个等长的消息 M_0、M_1 以及一组需要挑战的访问策略

$\{(\boldsymbol{A}_i,\rho_i,\Gamma_{i0}),(\boldsymbol{A}_i,\rho_i,\Gamma_{i1})\}_{i\in\{1,\cdots,q\}}$，$\mathcal{B}$ 随机选择 $\beta\in\{0,1\}$，执行下面的操作。

1) $\mathcal{B}$ 随机选择 $\tilde{v}_2,\cdots,\tilde{v}_n,\tilde{v}_2^{'},\cdots,\tilde{v}_n^{'}\in\mathbb{Z}_N$，生成向量 $\tilde{\boldsymbol{v}}=(1,\tilde{v}_2,\cdots,\tilde{v}_n),\tilde{\boldsymbol{v}}'=(1,\tilde{v}_2^{'},\cdots,\tilde{v}_n^{'})$。

2) 对于 $1\leqslant x\leqslant l$，$\mathcal{B}$ 随机选择 $\tilde{r}_x,\tilde{r}_x^{'}\in\mathbb{Z}_N$，$\tilde{F}_{1,x},\tilde{F}_{1,x}^{'},\tilde{F}_{2,x},\tilde{F}_{2,x}^{'}\in\mathbb{G}_{p4}$。

3) 令 $\Gamma_\beta=(v_{\rho(1)},\cdots,v_{\rho(l)})$。$\mathcal{B}$ 随机选择指数 $\tilde{s}\in\mathbb{Z}_N$ 并计算

$$\tilde{C}_1=M_\beta e(g^\alpha,I_1I_2),C_1^{'}=I_1I_2$$

$$C_{1,x}=(I_1I_2)^{\alpha A_x\tilde{\boldsymbol{v}}}(I_1I_2)^{-(a_0+a_{\rho(x)}v_{\rho(x)})\tilde{r}_x}\tilde{F}_{1,x}$$

$$D_{1,x}=(I_1I_2)^{\tilde{r}_x}\tilde{F}_{1,x}^{'}$$

$$\tilde{C}_2=e(g^\alpha,(I_1I_2)^{\tilde{s}}),C_2^{'}=(I_1I_2)^{\tilde{s}}$$

$$C_{2,x}=(I_1I_2)^{\tilde{s}\alpha A_x\tilde{\boldsymbol{v}}'}(I_1I_2)^{-(a_0+a_{\rho(x)}v_{\rho(x)})\tilde{r}_x^{'}}\tilde{F}_{2,x}$$

$$D_{2,x}=(I_1I_2)^{\tilde{r}_x^{'}}\tilde{F}_{2,x}^{'}$$

4) $\mathcal{B}$ 设定挑战密文为 $C=((\boldsymbol{A},\rho),\tilde{C}_1,C_1^{'},\{C_{1,x},D_{1,x}\}_{1\leqslant x\leqslant l},\tilde{C}_2,C_2^{'},\{C_{2,x},D_{2,x}\}_{1\leqslant x\leqslant l})$ 并将其发送给 $\mathcal{A}$。

若令 $I_1I_2=g^sg_2^c$，则

$$\tilde{C}_1=M_\beta e(g,g)^{\alpha s},C_1^{'}=g^sg_2^c$$

$$C_{1,x}=g^{\alpha A_x\vec{\boldsymbol{v}}}\left(u_{\rho(x)}^{v_{\rho(x)}}H\right)^{-r_x}F_{1,x}g_2^{A_x\vec{\boldsymbol{\omega}}+\gamma_xz_{\rho(x)}}$$

$$D_{1,x}=g^{r_x}F_{1,x}^{'}g_2^{-\gamma_x}$$

$$\tilde{C}_2=Me(g,g)^{\alpha s'},C_2^{'}=g^{s'}g_2^{c'}$$

$$C_{2,x}=g^{\alpha A_x\vec{\boldsymbol{v}}'}\left(u_{\rho(x)}^{v_{\rho(x)}}H\right)^{-r_x^{'}}F_{2,x}g_2^{A_x\vec{\boldsymbol{\omega}}'+\gamma_x'z_{\rho(x)}}$$

$$D_{2,x}=g^{r_x^{'}}F_{2,x}^{'}g_2^{-\gamma_x^{'}}$$

其中，$s'=s\tilde{s},c'=c\tilde{s},\vec{\boldsymbol{v}}=(s,s\tilde{v}_2,\cdots,s\tilde{v}_n),\vec{\boldsymbol{v}}'=(s',s'\tilde{v}_2^{'},\cdots,s'\tilde{v}_n^{'})$，$r_x=s\tilde{r}_x,r_x^{'}=s\tilde{r}_x^{'},F_{1,x}=\tilde{F}_{1,x}F^{r_x},F_{2,x}=\tilde{F}_{2,x}F^{r_x}$，$\vec{\boldsymbol{\omega}}=c\alpha\tilde{\boldsymbol{v}},\vec{\boldsymbol{\omega}}'=c\tilde{s}\alpha\tilde{\boldsymbol{v}}',\gamma_x=-c\tilde{r}_x,\gamma_x^{'}=-c\tilde{r}_x^{'},v_{\rho(x)}=a_0+a_{\rho(x)}v_{\rho(x)}$。这是一个半功能密文。这里的 $a,a_0,a_{\rho(x)},v_{\rho(x)},\tilde{s},\tilde{v}_2,\cdots,\tilde{v}_n,\tilde{v}_2^{'},\cdots,\tilde{v}_n^{'},\tilde{r}_x,\tilde{r}_x^{'}$ 模 p_1 的值和其模 p_2 的值无任何联系，因此这些参数是均匀分布的。因此第 k 个密钥和密文是均匀分布的。由此可以得出，若 $T\overset{R}{\leftarrow}\mathbb{G}_{p1}\times\mathbb{G}_{p2}\times\mathbb{G}_{p3}$，则 $\mathcal{B}$ 模拟的是 $Game_{k,1}$，$T\overset{R}{\leftarrow}\mathbb{G}_{p1}\times\mathbb{G}_{p3}$，则 $\mathcal{B}$ 模拟的是 $Game_{k-1,3}$。因此，$\mathcal{B}$ 可以使用 $\mathcal{A}$ 的输出来获取区分 T 的可能性。证毕。

引理 3 假设 $\mathcal{G}$ 可以满足假设 2，则 $Game_{k,1}$ 和 $Game_{k,2}$ 是计算性不可区分的。

证明 假设存在一多项式时间敌手 $\mathcal{A}$ 可以区分 $Game_{k,1}$ 和 $Game_{k,2}$。则可以构造一个算法 $\mathcal{B}$ 以不可忽略的优势攻破假设 2。$\mathcal{B}$ 获取 $g,I_1I_2,J_2J_3,I_3,I_4,T$，并可以和 $\mathcal{A}$ 模拟游戏 $Game_{k,1}$ 或 $Game_{k,2}$。$\mathcal{B}$ 随机选择 $\alpha,a,a_0,a_1,\cdots,a_n\in\mathbb{Z}_N,F\in\mathbb{G}_{p4}$。然后令 $h=g^{a_0},u_1=g^{a_1},\cdots,u_n=g^{a_n}$，再将公开参数发给敌手 $\mathcal{A}$，公开参数为：$PK=\left(N,g,g^a,e(g,g)^\alpha,u_1,\cdots,u_n,H=hF,I_4\right)$。

前 $k-1$ 个半功能密钥为类型 3，大于 k 的密钥为常规密钥，挑战密文的构造方式同引理 2。

对属性集为 $S=(s_1,\cdots,s_n)$ 时第 k 密钥查询。$\mathcal{B}$ 的操作同引理 2，但 $\mathcal{B}$ 额外选择一个随机指数 $\mu\in\mathbb{Z}_N$ 并设定：$K=g^\alpha T^a\tilde{R}(J_2J_3)^\mu,K'=T\tilde{R}^{'},\{K_i=T^{a_0+a_is_i}\tilde{R}_i\}_{1\leqslant i\leqslant n}$。

这里做的唯一改动就是增加了 $(J_2J_3)^\mu$，随机化了 K 的 $\mathbb{G}_{p2}$ 部分，若 $T\overset{R}{\leftarrow}\mathbb{G}_{p1}\times\mathbb{G}_{p2}\times\mathbb{G}_{p3}$，这是一个均匀分布的类型 1 半功能密钥。若 $T\overset{R}{\leftarrow}\mathbb{G}_{p1}\times\mathbb{G}_{p3}$，这是一个均匀分布的类型 2 半功能密钥。

由此可以得出，若 $T\overset{R}{\leftarrow}\mathbb{G}_{p1}\times\mathbb{G}_{p2}\times\mathbb{G}_{p3}$，则 $\mathcal{B}$ 模拟的是 $Game_{k,1}$，$T\overset{R}{\leftarrow}\mathbb{G}_{p1}\times\mathbb{G}_{p3}$，则 $\mathcal{B}$ 模拟的是 $Game_{k,2}$。因此，$\mathcal{B}$ 可以使用 $\mathcal{A}$ 的输出来获取区分 T 的可能性。证毕。

引理 4 假设 $\mathcal{G}$ 可以满足假设 2，则 $Game_{k,2}$ 和 $Game_{k,3}$ 是计算性不可区分的。

证明 假设存在一多项式时间敌手 $\mathcal{A}$ 可以区分 $Game_{k,2}$ 和 $Game_{k,3}$。则可以构造一个算法 $\mathcal{B}$ 以不可忽略的优势攻破假设 2。$\mathcal{B}$ 获取 $g,I_1I_2,J_2J_3,I_3,I_4,T$，并可以和 $\mathcal{A}$ 模拟游戏 $Game_{k,2}$ 或 $Game_{k,3}$。$\mathcal{B}$ 随机选择 $\alpha,a,a_0,a_1,\cdots,a_n\in\mathbb{Z}_N,F\in\mathbb{G}_{p4}$。然后令 $h=g^{a_0},u_1=g^{a_1},\cdots,u_n=g^{a_n}$，再将公开参数发给敌手 $\mathcal{A}$，公开参数为：$PK=(N,g,g^a,e(g,g)^\alpha,u_1,\cdots,u_n,H=hF,I_4)$。

前 $k-1$ 个半功能密钥为类型 3，大于 k 的密钥为常规密钥，挑战密文的构造方式同引理 2。

对属性集为 $S=(s_1,\cdots,s_n)$ 时第 k 密钥查询。$\mathcal{B}$ 选择一个随机指数 $\mu\in\mathbb{Z}_N$，$\tilde{R},\tilde{R}^{'},\tilde{R}_1,\cdots,\tilde{R}_n\in\mathbb{G}_{p3}$ 并设定 $K=g^\alpha T^a\tilde{R}(J_2J_3)^\mu,K'=T\tilde{R}^{'},\{K_i=T^{a_0+a_is_i}\tilde{R}_i\}_{1\leqslant i\leqslant n}$。

容易得出，若 $T\overset{R}{\leftarrow}\mathbb{G}_{p1}\times\mathbb{G}_{p2}\times\mathbb{G}_{p3}$，则 T 可以记做 $g^tg_2^{d'}\tilde{R}$，同时

$K=g^{\alpha}g^{at}Rg_2^{d},K'=g^{t}R'g_2^{d'},\left\{K_i=(u_i^{s_i}h)^{t}R_ig_2^{d'z_i}\right\}_{1\leqslant i\leqslant n}$

其中，$R=\bar{R}^{a}\tilde{R},d=ad',R'=\bar{R}\tilde{R}',R_i=\bar{R}^{a_0+a_is_i}\tilde{R}_i,z_i=a_0+a_is_i$。这是一个类型 3 的半功能密钥。注意 μ 模 p_2 的值和其模 p_3 的值无任何联系。若 $T\overset{R}{\leftarrow}\mathbb{G}_{p1}\times\mathbb{G}_{p3}$，这是一个类型 2 的半功能密钥。因而第 k 个密钥和密文是均匀分布的。由此可以得出，若 $T\overset{R}{\leftarrow}\mathbb{G}_{p1}\times\mathbb{G}_{p2}\times\mathbb{G}_{p3}$，则 $\mathcal{B}$ 模拟的是 $Game_{k,3}$，$T\overset{R}{\leftarrow}\mathbb{G}_{p1}\times\mathbb{G}_{p3}$，则 $\mathcal{B}$ 模拟的是 $Game_{k,2}$。因此，$\mathcal{B}$ 可以使用 $\mathcal{A}$ 的输出来获取区分 T 的可能性。证毕。

引理 5　假设 $\mathcal{G}$ 可以满足假设 3，则 $Game_{q,3}$ 和 $Game_{final_0}$ 是计算性不可区分的。

证明　假设存在一多项式时间敌手 $\mathcal{A}$ 可以区分 $Game_{q,3}$ 和 $Game_{final_0}$。则可以构造一个算法 $\mathcal{B}$ 以不可忽略的优势攻破假设 3。$\mathcal{B}$ 获取 $g,g_2,g^{\alpha}I_2,g^{s}J_2,I_3,I_4,T$，并可以和 $\mathcal{A}$ 模拟游戏 $Game_{q,3}$ 或 $Game_{final_0}$。$\mathcal{B}$ 随机选择 $\alpha,a,a_0,a_1,\cdots,a_n\in\mathbb{Z}_N,F\in\mathbb{G}_{p4}$。然后令 $h=g^{a_0},u_1=g^{a_1},\cdots,u_n=g^{a_n}$，再将公开参数发给敌手 $\mathcal{A}$，公开参数为：$PK=\left(N,g,g^{a},e(g,g)^{\alpha},u_1,\cdots,u_n,H=hF,I_4\right)$。

每次当 $\mathcal{B}$ 需要对属性集为 $S=(s_1,\cdots,s_n)$ 时生成密钥，$\mathcal{B}$ 随机选择指数 $t,\tilde{d},d',d_1,\cdots,d_n\in\mathbb{Z}_N$，$R,R',R_1,\cdots,R_n\in\mathbb{G}_{p3}$ 创建一个类型 3 的半功能密钥：$K=(g^{\alpha}I_2)g^{at}Rg_2^{\tilde{d}},K'=g^{t}R'g_2^{d'},\left\{K_i=(u_i^{s_i}h)^{t}R_ig_2^{d'z_i}\right\}_{1\leqslant i\leqslant n}$。

注意到 K 可以被写成 $g^{\alpha}g^{at}Rg_2^{d}$ 的形式，$g_2^{d}=I_2g_2^{\tilde{d}}$，因此，这是一个均匀分布的类型 3 半功能密钥。

在某一时刻，$\mathcal{A}$ 向 $\mathcal{B}$ 发送 2 个等长的消息 M_0、M_1 以及一组需要挑战的访问策略 $\{(\boldsymbol{A}_i,\rho_i,\Gamma_{i0}),(\boldsymbol{A}_i,\rho_i,\Gamma_{i1})\}_{i\in\{1,\cdots,q\}}$，$\mathcal{B}$ 随机选择 $\beta\in\{0,1\}$，执行下面的操作。

1) $\mathcal{B}$ 随机选择 $\tilde{v}_2,\cdots,\tilde{v}_n\in\mathbb{Z}_N$，生成向量 $\tilde{\boldsymbol{v}}=(1,\tilde{v}_2,\cdots,\tilde{v}_n)$。$\mathcal{B}$ 还会选择两个随机向量 $\vec{\boldsymbol{v}'}=(s',v_2',\cdots,v_n'),\vec{\boldsymbol{\omega}'}=(\omega_1',\cdots,\omega_n')\in\mathbb{Z}_N^n$。

2) 对于 $1\leqslant x\leqslant l$，$\mathcal{B}$ 随机选择 $\tilde{r}_x,r_x',\gamma_x'\in\mathbb{Z}_N$，$\tilde{F}_{1,x},F_{1,x}',F_{2,x},F_{2,x}'\in\mathbb{G}_{p4}$。

3) 令 $\Gamma_{\beta}=(v_{\rho(1)},\cdots,v_{\rho(l)})$。$\mathcal{B}$ 随机选择指数 $c'\in\mathbb{Z}_N$ 并计算

$\tilde{C}_1=M_{\beta}T,C_1'=g^{s}J_2$

$C_{1,x}=\left(g^{s}J_2\right)^{aA_x\vec{v}}\left(g^{s}J_2\right)^{-\left(a_0+a_{\rho(x)}v_{\rho(x)}\right)\tilde{r}_x}\tilde{F}_{1,x}$

$D_{1,x}=\left(g^{s}J_2\right)^{\tilde{r}_x}F_{1,x}'$

$\tilde{C}_2=e(g,g)^{\alpha s'},C_2'=g^{s'}g_2^{c'}$

$C_{2,x}=g^{aA_x\vec{v}'}\left(u_{\rho(x)}^{v_{\rho(x)}}H\right)^{-r_x'}F_{2,x}'g_2^{A_x\vec{\omega}'+\gamma_x'\left(a_0+a_{\rho(x)}v_{\rho(x)}\right)}$

$D_{2,x}=g^{r_x'}F_{2,x}'g_2^{-\gamma_x'}$

4) $\mathcal{B}$ 设定挑战密文为 $C=((\boldsymbol{A},\rho),\tilde{C}_1,C_1',\{C_{1,x},D_{1,x}\}_{1\leqslant x\leqslant l},\tilde{C}_2,C_2',\{C_{2,x},D_{2,x}\}_{1\leqslant x\leqslant l})$ 并将其发送给 $\mathcal{A}$。

令 $g^{s}J_2=g^{s}g_2^{c}$，则

$\tilde{C}_1=M_{\beta}T,C_1'=g^{s}g_2^{c}$

$C_{1,x}=g^{aA_x\vec{v}}\left(u_{\rho(x)}^{v_{\rho(x)}}H\right)^{-r_x}F_{1,x}g_2^{A_x\vec{\omega}+\gamma_xz_{\rho(x)}}$

$D_{1,x}=g^{r_x}F_{1,x}'g_2^{-\gamma_x}$

$\tilde{C}_2=Me(g,g)^{\alpha s'},C_2'=g^{s'}g_2^{c'}$

$C_{2,x}=g^{aA_x\vec{v}'}\left(u_{\rho(x)}^{v_{\rho(x)}}H\right)^{-r_x'}F_{2,x}'g_2^{A_x\vec{\omega}'+\gamma_x'z_{\rho(x)}}$

$D_{2,x}=g^{r_x'}F_{2,x}'g_2^{-\gamma_x'}$

其中，$\vec{\boldsymbol{v}}=\left(s,s\tilde{v}_2,\cdots,s\tilde{v}_n\right),r_x=s\tilde{r}_x,F_{1,x}=\tilde{F}_{1,x}F^{r_x}$，$\vec{\boldsymbol{\omega}}=ca\tilde{\boldsymbol{v}},\gamma_x=-c\tilde{r}_x,v_{\rho(x)}=a_0+a_{\rho(x)}v_{\rho(x)}$。需要注意的是，$a,a_0,a_{\rho(x)},v_{\rho(x)},\tilde{v}_2,\cdots,\tilde{v}_n,\tilde{r}_x$ 模 p_1 的值和其模 p_2 的值无任何联系。

若 $T=e(g,g)^{\alpha s}$，这是一个均匀分布的关于 M_{β} 的半功能加密，$\mathcal{B}$ 模拟了 $Game_{q,3}$。否则，这是一个均匀分布的在 $\mathbb{G}_T$ 上的一个随机信息的半功能加密，$\mathcal{B}$ 模拟了 $Game_{final_0}$。因此，$\mathcal{B}$ 可以使用 $\mathcal{A}$ 的输出来获取区分 T 的可能性。证毕。

引理 6　假设 $\mathcal{G}$ 可以满足假设 4，则 $Game_{final_0}$ 和 $Game_{final_1}$ 是计算性不可区分的。

证明　假设存在一多项式时间敌手 $\mathcal{A}$ 可以区分 $Game_{final_0}$ 和 $Game_{final_1}$。则可以构造一个算法 $\mathcal{B}$ 以不可忽略的优势攻破假设 4。$\mathcal{B}$ 获取 $g,g_2,g^{t'}V_2,h^{t'}J_2,I_3,I_4,hF,g^{r'}W_2W_4,T$，并可以和 $\mathcal{A}$ 模拟游戏 $Game_{final_0}$ 或 $Game_{final_1}$。$\mathcal{B}$ 随机选择 $\alpha,a,a_0,a_1,\cdots,a_n\in\mathbb{Z}_N,F\in\mathbb{G}_{p4}$。然后令 $h=g^{a_0}$，$u_1=g^{a_1},\cdots,u_n=g^{a_n}$，再将公开参数发给敌手 $\mathcal{A}$，公开参数为：$PK=(N,g,g^{a},e(g,g)^{\alpha},u_1,\cdots,u_n,H=hF,I_4)$。

当 $\mathcal{B}$ 需要对属性集为 $S=(s_1,\cdots,s_n)$ 时生成密钥，$\mathcal{B}$ 随机选择指数 $\tilde{t}\in\mathbb{Z}_N,R,R',R_1,\cdots,R_n\in\mathbb{G}_{p3}$，并设置

$$K=g^{\alpha}\left(g^{t'}V_2\right)^{a\tilde{t}}R, K'=\left(g^{t'}V_2\right)^{\tilde{t}}R',$$
$$\left\{K_i=\left(g^{t'}V_2\right)^{a_i s_i\tilde{t}}\left(h^{t'}J_2\right)^{\tilde{t}}R_i\right\}_{1\leqslant i\leqslant n}$$

容易看出，$K=g^{\alpha}g^{at}Rg_2^{d}, K'=g^{t}R'g_2^{d'}$，$\{K_i=(u_i^{s_i}h)^{t}R_ig_2^{d_i}\}_{1\leqslant i\leqslant n}$。

其中，$t=t'\tilde{t}, g_2^{d}=V_2^{a\tilde{t}}, g_2^{d'}=V_2^{\tilde{t}}, g_2^{d_i}=V_2^{a_is_i\tilde{t}}J_2^{\tilde{t}}$。由于$\tilde{t},a,a_i,s_i$模$p_2$的值与其模$p_1$的值无任何联系，因此，这是一个均匀分布的类型 3 半功能密钥。

在某一时刻，$\mathcal{A}$ 向 $\mathcal{B}$ 发送 2 个等长的消息 M_0、M_1 以及一组需要挑战的访问策略 $\{(\boldsymbol{A}_i,\rho_i,\Gamma_{i0}),(\boldsymbol{A}_i,\rho_i,\Gamma_{i1})\}_{i\in\{1,\cdots,q\}}$，$\mathcal{B}$ 随机选择 $\beta\in\{0,1\}$，执行下面的操作。

1) $\mathcal{B}$ 随机选择向量 $\vec{\boldsymbol{v}}=(s,v_2,\cdots,v_n)$，$\overrightarrow{\boldsymbol{v}'}=(s',v_2',\cdots,v_n')$，$\vec{\boldsymbol{\omega}},\overrightarrow{\boldsymbol{\omega}'}\in\mathbb{Z}_N^n$。

2) 对于 $1\leqslant x\leqslant l$，$\mathcal{B}$ 随机选择 $\tilde{r}_x,\tilde{r}_x'\in\mathbb{Z}_N$，$\tilde{F}_{1,x},\tilde{F}_{2,x}\in\mathbb{G}_{p4}$。

3) 令 $\Gamma_{\beta}=(v_{\rho(1)},\cdots,v_{\rho(l)})$。$\mathcal{B}$ 随机选择指数 $c,c'\in\mathbb{Z}_N$ 并计算

$$\tilde{C}_1\overset{R}{\leftarrow}\mathbb{G}_T, C_1'=g^{s}g_2^{c}$$
$$C_{1,x}=g^{\alpha A_x\vec{v}}\left(g^{r'}W_2W_4\right)^{-\tilde{r}_x a_{\rho(x)}v_{\rho(x)}}T^{-\tilde{r}_x}\tilde{F}_{1,x}g_2^{A_x\vec{\omega}}$$
$$D_{1,x}=\left(g^{r'}W_2W_4\right)^{\tilde{r}_x}$$
$$\tilde{C}_2=Me(g,g)^{\alpha s'}, C_2'=g^{s'}g_2^{c'}$$
$$C_{2,x}=g^{\alpha A_x\overrightarrow{v'}}\left(g^{r'}W_2W_4\right)^{-\tilde{r}_x'a_{\rho(x)}v_{\rho(x)}}T^{-\tilde{r}_x'}\tilde{F}_{2,x}g_2^{A_x\overrightarrow{\omega'}}$$
$$D_{2,x}=\left(g^{r'}W_2W_4\right)^{\tilde{r}_x'}$$

4) $\mathcal{B}$ 设定挑战密文为 $C=((\boldsymbol{A},\rho),\tilde{C}_1,C_1',\{C_{1,x},D_{1,x}\}_{1\leqslant x\leqslant l},\tilde{C}_2,C_2',\{C_{2,x},D_{2,x}\}_{1\leqslant x\leqslant l})$ 并将其发送给 $\mathcal{A}$。

若 $T=h^{r'}U_2U_4$，令 $W_2=g_2^{\gamma},U_2=g_2^{\mu\gamma}$，可得

$$\tilde{C}_1\overset{R}{\leftarrow}\mathbb{G}_T, C_1'=g^{s}g_2^{c}$$
$$C_{1,x}=g^{\alpha A_x\vec{v}}\left(u_{\rho(x)}^{v_{\rho(x)}}H\right)^{-r_x}F_{1,x}g_2^{A_x\vec{\omega}+\gamma_x z_{\rho(x)}}$$
$$D_{1,x}=g^{r_x}F_{1,x}'g_2^{-\gamma_x}$$
$$\tilde{C}_2=Me(g,g)^{\alpha s'}, C_2'=g^{s'}g_2^{c'}$$
$$C_{2,x}=g^{\alpha A_x\overrightarrow{v'}}\left(u_{\rho(x)}^{v_{\rho(x)}}H\right)^{-r_x'}F_{2,x}g_2^{A_x\overrightarrow{\omega'}+\gamma_x'z_{\rho(x)}}$$
$$D_{2,x}=g^{r_x'}F_{2,x}'g_2^{-\gamma_x'}$$

其中，

$$r_x=r'^{\tilde{r}_x}, F_{1,x}=F'^{r_x}\tilde{F}_{1,x}U_4^{-\tilde{r}_x}W_4^{-\tilde{r}_x a_{\rho(x)}v_{\rho(x)}}$$
$$\gamma_x=-\gamma\tilde{r}_x, z_{\rho(x)}=\mu+a_{\rho(x)}v_{\rho(x)}$$
$$F_{1,x}'=W_4^{\tilde{r}_x}, F_{2,x}=F'^{r_x'}\tilde{F}_{2,x}U_4^{-\tilde{r}_x'}W_4^{-\tilde{r}_x'a_{\rho(x)}v_{\rho(x)}}$$
$$\gamma_x'=-\gamma\tilde{r}_x', F_{2,x}'=W_4^{\tilde{r}_x'}$$

由于 $\tilde{r}_x,\tilde{r}_x',a_{\rho(x)},v_{\rho(x)}$ 模 p_1 和 p_2 的值和其模 p_4 的值无任何联系，这是一个均匀分布在 $\mathbb{G}_T$ 上的随机信息的半功能加密。若 $T\overset{R}{\leftarrow}\mathbb{G}_{p1}\times\mathbb{G}_{p2}\times\mathbb{G}_{p4}$，$\tilde{C}_1$ 是一个均匀分布在 $\mathbb{G}_T$ 上随机的半功能密文，且 $C_{1,x},C_{2,x}\overset{R}{\leftarrow}\mathbb{G}_{p1}\times\mathbb{G}_{p2}\times\mathbb{G}_{p4}$。

因此，可以得出结论，若 $T=h^{r'}U_2U_4$，则 $\mathcal{B}$ 模拟了 $Game_{final_0}$。若 $T\overset{R}{\leftarrow}\mathbb{G}_{p1}\times\mathbb{G}_{p2}\times\mathbb{G}_{p4}$，则 $\mathcal{B}$ 模拟了 $Game_{final_1}$。因此，$\mathcal{B}$ 可以使用 $\mathcal{A}$ 的输出来获取区分 T 的可能性。证毕。

4 结束语

本文提出了一种支持任意策略更新的半策略隐藏 CP-ABE 方案，有效解决了策略更新时会造成的用户隐私数据泄露的问题。此外，在引入半策略隐藏的方法时，不会增加用户的密钥长度。数据拥有者在更新策略时，只需要做少量的运算，大量的更新操作被交给云服务器执行，大大节省了通信和计算开销。通过使用文献[19]中的双重体系加密方法(dual system encryption methodology)，在标准模型下证明了本文的方案是自适应安全的。

参考文献：

[1] YU S, WANG C, REN K, et al. Achieving secure, scalable, and fine-grained data access control in cloud computing[A]. INFOCOM, 2010 Proceedings IEEE[C]. 2010. 1-9.

[2] SAHAI A, WATERS B. Fuzzy Identity-Based Encryption[M]. Springer Berlin Heidelberg, 2005.

[3] GOYAL V, PANDEY O, SAHAI A, et al. Attribute-based encryption for fine-grained access control of encrypted data[A]. Proceedings of the 13th ACM Conference on Computer and Communications Security[C]. ACM, 2006. 89-98.

[4] BETHENCOURT J, SAHAI A, WATERS B. Ciphertext-policy attribute-based encryption[A]. Security and Privacy[C]. 2007. 321-334.

[5] WATERS B. Ciphertext-Policy Attribute-Based Encryption: An Expressive, Efficient, and Provably Secure Realization[M]. Springer Berlin Heidelberg, 2011.

[6] CHASE M. Multi-Authority Attribute based Encryption[M]. Theory of Cryptography. Springer Berlin Heidelberg, 2007.

[7] LEWKO A, WATERS B. Decentralizing Attribute-based Encryption[M]. Springer Berlin Heidelberg, 2011.

[8] LIU Z, CAO Z, HUANG Q, et al. Fully secure multi-authority ciphertext-policy attribute-based encryption without random oracles[A]. Computer Security–ESORICS 2011[C]. Springer Berlin Heidelberg, 2011. 278-297.

[9] SAHAI A, SEYALIOGLU H, WATERS B. Dynamic credentials and ciphertext delegation for attribute-based encryption[A]. Advances in Cryptology–CRYPTO 2012[C]. Springer Berlin Heidelberg, 2012. 199-217.

[10] YANG K, JIA X, REN K, et al. Enabling efficient access control with dynamic policy updating for big data in the cloud[A]. INFOCOM, 2014 Proceedings IEEE[C]. 2014. 2013-2021.

[11] NISHIDE T, YONEYAMA K, OHTA K. Attribute-based encryption with partially hidden encryptor-specified access structures[A]. Applied cryptography and network security[C]. Springer Berlin Heidelberg, 2008. 111-129.

[12] LI J, REN K, ZHU B, et al. Privacy-aware attribute-based encryption with user accountability[A]. Information Security[C]. Springer Berlin Heidelberg, 2009.347-362.

[13] LAI J, DENG R H, LI Y. Expressive CP-ABE with partially hidden access structures[A]. Proceedings of the 7th ACM Symposium on Information, Computer and Communications Security[C]. ACM, 2012. 18-19.

[14] BEIMEL A. Secure Schemes for Secret Sharing and Key Distribution[D]. Technion-Israel Institute of Technology, Faculty of Computer Science, 1996.

[15] BONEH D, GOH E J, NISSIM K. Evaluating 2-DNF formulas on ciphertexts[A]. Theory of Cryptography[C]. Springer Berlin Heidelberg, 2005.325-341.

[16] LEWKO A, OKAMOTO T, SAHAI A, et al. Fully secure functional encryption: attribute-based encryption and (hierarchical) inner product encryption[A]. Advances in Cryptology–EUROCRYPT 2010[C]. Springer Berlin Heidelberg, 2010. 62-91.

[17] DE CARO A, IOVINO V, PERSIANO G. Fully secure anonymous hibe and secret-key anonymousibe with short ciphertexts[A]. Pairing-Based Cryptography-Pairing 2010[C]. Springer Berlin Heidelberg, 2010.347-366.

[18] LEWKO A, WATERS B. New techniques for dual system encryption and fully secure HIBE with short ciphertexts[A]. Theory of Cryptography[C]. Springer Berlin Heidelberg, 2010.455-479.

[19] WATERS B. Dual system encryption: realizing fully secure IBE and HIBE under simple assumptions[A]. Advances in Cryptology-CRYPTO 2009[C]. Springer Berlin Heidelberg, 2009.619-636.

作者简介：

应作斌（1982-），男，安徽芜湖人，西安电子科技大学博士生，主要研究方向为密码学与网络安全、基于位置的隐私保护等。

马建峰（1963-），男，陕西西安人，博士，西安电子科技大学教授、博士生导师，主要研究方向为网络与信息安全等。

崔江涛（1975-），男，山东平度人，博士，西安电子科技大学副教授、博士生导师，主要研究方向为高维索引技术、数据与知识工程等。