doi:10.11959/j.issn.1000-436x.2017201

支持策略动态更新的多机构属性基加密方案

闫玺玺[1]，刘媛[1]，李子臣[2]，汤永利[1]
(1. 河南理工大学计算机科学与技术学院，河南 焦作 454003；2. 北京印刷学院信息工程学院，北京 102600)

摘 要：属性基加密方案被认为是云存储环境下数据资源访问控制的最佳选择，但是策略更新很大程度上限制了其在实际中的应用。针对此问题，提出一种支持策略动态更新的多机构属性基加密方案。该方案引入匿名密钥分发协议为用户生成私钥，有效地保护用户的隐私，并抵抗属性机构的共谋攻击。另外，方案采用动态策略更新算法，支持任何类型的策略更新，大大减少传统策略更新中的计算和通信开销。经安全性分析证明，方案在标准模型下满足自适应选择明文攻击安全。通过对比，用户私钥和密文长度都有所减少，密文更新交给云服务器完成，降低了数据拥有者的工作量，更加贴近实际应用。

关键词：属性基加密；多机构；动态策略更新；隐私保护
中图分类号：TP309 **文献标识码**：A

Multi-authority attribute-based encryption scheme with policy dynamic updating

YAN Xi-xi[1], LIU Yuan[1], LI Zi-chen[2], TANG Yong-li[1]
(1. College of Computer Science and Technology, Henan Polytechnic University, Jiaozuo 454003, China;
2. College of Information Engineering, Beijing Institute of Graphic Communication, Beijing 102600, China)

Abstract: Attribute-based encryption (ABE) is a new cryptographic technique which guarantees fine-grained access control of outsourced encrypted data in the cloud environment. However, a key limitation remains, namely policy updating. Thus, a multi-authority attribute-based encryption scheme with policy dynamic updating was proposed. In the scheme, an anonymous key issuing protocol was introduced to protect users' privacy and resist collusion attack of attribute authority. The scheme with dynamic policy updating technique was secure against chosen plaintext attack under the standard model and can support any types of policy updating. Compared to the existing related schemes, the size of ciphertext and users' secret key is reduced and can significantly reduce the computation and communication costs of updating ciphertext. It is more effective in the practical application.

Key words: attribute based encryption, multi-authority, dynamic policy updating, privacy protection

1 引言

随着互联网的发展以及云计算的应用，越来越多的数据存储在云端，然而这些数据经常包含一些敏感信息，因此为了保护用户隐私，需要对敏感的隐私信息进行加密处理。属性基加密（ABE, attribute based encryption）作为一种新兴的公钥加密技术，将用户的身份与一系列的属性绑定，通过对用户的私钥或密文设置属性集或访问结构，只有属性集和访问结构相匹配时才能解密，从而实现了一对多的通信以及对文件的细粒度访问控制，因此更适用于云端数据的加密处理。然而，用户将加密数据存储

收稿日期：2016-12-09；**修回日期**：2017-07-25
基金项目：国家自然科学基金资助项目（No.61300216）；河南省科技厅基金资助项目（No.132102210123）；河南省教育厅科研基金资助项目（No.16A520013）；河南理工大学 2015 年青年骨干教师基金资助项目
Foundation Items: The National Natural Science Foundation of China (No.61300216), The Science Project of Henan Province (No.132102210123), The Scientific Research Project of Henan Province (No.16A520013), The Research Fund for Young Backbone Teachers of Henan Polytechnic University in 2015

在云端，设置的访问策略并不是一成不变的。例如，在个人健康病例系统中，病人将病历放在云服务器中，设置的访问策略为{人民医院,医生,心脏科}，只有满足这 3 个属性的用户才可以访问其病历，但当病人转院时，只有满足{红十字医院，医生，心脏科}的用户可以访问其病历，这就需要云服务器具有支持改变访问策略的功能。

传统的 ABE 只有一个可信的机构来管理所有的属性，但在实际应用中，属性是由多个机构管理运行的，如个人健康病例系统；在此基础上提出多机构 ABE，多个机构分别管理不同的属性集，并为其权限内的属性用户分发密钥。文献[1]提出分权的多机构 ABE，该方案中任何一方都可以通过为不同的用户生成公钥和发放私钥成为机构，且提出一种将用户的密钥与 GID 相连的技术以抵抗共谋攻击。文献[2]提出云计算中具有隐私意识的基于属性的个人健康记录共享系统，该方案是一种密钥策略的多机构的 ABE，通过隐藏访问策略保护访问用户的隐私。文献[3]提出提高隐私和安全的分权的密文策略的多机构 ABE，该方案采用承诺方案和零知识证明技术来保护用户的 GID 和属性，这是第一个保护用户属性的方案。文献[4]提出基于密文策略多机构属性基加密方案，该方案去除中央机构，采用访问树策略及 Shamir 秘密共享技术，并支持属性撤销。但上述文献并没有考虑用户的访问策略更新问题，当用户需要更新密文的访问策略时，用户需重新用新的访问策略加密数据并传至云服务器，极易造成较大的系统通信和计算开销。

文献[5]提出支持动态证书和密文授权的 ABE 方案，该方案首次提出策略更新的思想，采用代理的方法更新密文，但其新的策略比原策略更严格。文献[6]提出新的动态策略更新方案，该方案可以支持任何形式的策略更新，但只在一般群模型下是安全的。文献[7]提出支持动态策略更新的半策略隐藏属性加密方案，该方案可以支持任何形式的策略更新并通过半策略隐藏的方式保护用户的隐私，并在标准模型下证明其是选择明文攻击（CPA）安全的。文献[8]提出智能电网中具有细粒度访问控制的属性撤销和动态策略更新的属性基加密方案，该方案给出智能电网中的系统模型，通过引入第三方审计实现属性撤销，并设计策略更新算法实现动态更新，有效地将 ABE 应用于智能电网中。文献[9]提出个人健康病例系统中具有隐私保护的多机构属性基加密方案，该方案采用匿名密钥分发协议保护用户的隐私，但该方案的策略更新采用的是传统的策略更新方式，计算和通信开销较大。文献[10]提出适合云存储的访问策略可更新多中心 CP-ABE 方案，该方案设置的多授权机构可以防止密钥泄露，并且可以支持访问策略更新。文献[11]提出具有动态策略更新的自适应安全的密文策略 ABE 方案，该方案是第一个多机构的动态策略更新 ABE 方案，该方案通过引入签名认证防止共谋攻击，但系统有多个中央机构、多个属性机构，用户密钥由中央机构生成的密钥、属性密钥构成，密钥生成的通信开销较大。文献[12]提出支持位置验证和策略变更的属性加密方案，该方案使用同态加密技术保护移动办公环境中用户的位置隐私，并可支持访问策略的更新。

从以上分析可以看出，属性基加密方案中密文的策略更新技术并不成熟，涉及策略更新的单机构 ABE 方案只由一个可信的机构管理所有属性，安全性并不高，不能满足实际应用需求。多机构 ABE 方案提高了属性管理的安全性，但效率往往不高。因此，本文提出一种高效的支持策略动态更新的多机构属性基加密方案，主要包括以下 2 个创新点：1)采用 LSSS 访问策略，引入动态策略更新算法，支持任何类型的策略更新，并减少了传统策略更新中的通信和计算开销问题，提高系统效率；2)利用匿名密钥分发协议[12]为用户分发密钥，从而保护用户的隐私，同时抵抗属性机构的共谋攻击。

2　相关知识

2.1　双线性对

令 G_0、G_T 为 2 个阶为素数 p 的乘法循环群，g_0 为 G_0 的生成元，存在双线性映射 $e: G_0 \times G_0 \to G_T$，且有以下特征。

1) 双线性：$\forall x, y \in Z_p$，$\forall m, n \in G_0$，有 $e(m^x, n^y) = e(m,n)^{xy}$。

2) 可计算性：$\forall m, n \in G_0$，存在有效算法计算 $e(m,n)$。

3) 非退化性：$e(g_0, g_0) \neq 1$。

2.2　访问结构

假定 $\{p_1, p_2, \cdots, p_n\}$ 为参与方的集合，集合 $P \subseteq 2^{\{p_1, p_2, \cdots, p_n\}}$，若对于 $\forall X, Y$：若 $X \in P$ 且 $X \subseteq Y$，有 $Y \in P$，则称 P 是单调的；访问结构是

$\{p_1,p_2,\cdots,p_n\}$ 的非空子集 P，即 $P\subseteq 2^{\{p_1,p_2,\cdots,p_n\}}\setminus\{\varnothing\}$，包含在 P 内的集合是授权集合，不包含在 P 内的集合是非授权集合。

2.3 线性秘密共享(LSSS, linear secret-sharing schemes)

对于一个集合 P 上密钥分享方案是线性的，如果满足以下条件：1) 集合中的每一个元素所获得的分享部分可以形成一个 Z_p 上的向量；2) 存在一个 $l\times n$ 的矩阵 $\boldsymbol{M}$，对于所有的 $i=1,\cdots,l$，矩阵中的第 i 行表示集合中的一个元素，并且可以通过映射 $\rho(i)$ 找到对应的元素，随机选择 $s\in Z_p$ 和一随机向量 $\boldsymbol{v}=(s,v_2,\cdots,v_n)\in Z_p^n$，$s$ 为要分享的秘密，则 $\lambda_i=\boldsymbol{M}_i\boldsymbol{v}$ 即为其分享的信息，$\boldsymbol{M}_i$ 为矩阵 $\boldsymbol{M}$ 的第 i 行。

线性重构功能：假设方案的访问结构 A 采用 LSSS，令 S 作为一授权集合，$I=\{i|\rho(i)\in S\}$，则存在 $\{\omega_i\in Z_p\}_{i\in I}$，使 $\sum_{i\in I}\omega_i\lambda_i=s$，从而获得分享的秘密 s。

2.4 q-PBDHE 假设(decisional q-parallel bilinear Diffie-Hellman exponent assumption)

令 G、G_T 为 2 个阶为素数 p 的乘法循环群，g 为 G 的生成元，存在双线性映射 $e:G\times G\to G_T$，随机选择 $a,s,b_1,\cdots,b_q\in Z_p$，$T\in G_T$，若敌手给定元组 $\boldsymbol{y}=g,g^s,g^a,\cdots,g^{(a^q)},g^{(a^{q+2})},\cdots,g^{(a^{2q})}$；$\forall 1\leqslant j\leqslant q,\ g^{s\cdot b_j},g^{\frac{a}{b_j}},\cdots,g^{\frac{a^q}{b_j}},g^{\frac{a^{q+2}}{b_j}},\cdots,g^{\frac{a^{2q}}{b_j}}$；$\forall 1\leqslant j,k\leqslant q,\ k\neq j,\ g^{\frac{a\cdot s\cdot b_k}{b_j}},\cdots,g^{\frac{a^q\cdot s\cdot b_k}{b_j}}$，判断 $T=e(g,g)^{a^{q+1}s}$ 是否成立。如果对于任一多项式时间的敌手 $\mathcal{A}$ 区分 $\left(\boldsymbol{y},e(g,g)^{a^{q+1}s}\right)$ 和 $(\boldsymbol{y},T)$ 的优势 $Adv_{\mathcal{A}}=\left|\Pr\left[\mathcal{A}\left(\boldsymbol{y},e(g,g)^{a^{q+1}s}\right)=1\right]-\Pr\left[\mathcal{A}(\boldsymbol{y},T)=1\right]\right|\geqslant\varepsilon$ 是可忽略的，则在群 (e,p,G,G_T) 上的 q-PBDHE 问题是困难的。

2.5 匿名密钥分发协议

本文的匿名密钥分发协议参考文献[9]，并在密钥中增加一个额外的元素，令 $u\in Z_p$ 为用户的隐私值，α、β、γ 为机构私钥，g、g_1、h 是群 G 的生成元，通过运行匿名密钥分发协议，用户可获得私钥 $D=\left(g^{\alpha}h^{r}g_1^{\frac{1}{(u+\beta)}}\right)^{\gamma}$，其具体运行如图 1 所示，其中，$2PC$ 表示双方安全计算协议，PoK 表示包含隐私值的知识证明。

用户	属性机构
$\rho_1\in Z_p$	$\xleftarrow{2PC}\ x=(\beta+u)\rho_1,\tau\ ,r\in Z_p$
$\rho_2\in Z_p$	$\xleftarrow{X_1,X_2,X_3,PoK(\alpha,\tau,x,r)}\ (X_1=g_1^{\frac{\tau}{x}},X_2=g^{\alpha\tau}\ ,X_3=h^{r\tau})$
$Y=\left(X_1^{\rho_1}X_2X_3\right)^{\rho_2}$	$\xrightarrow{Y,PoK(\rho_2)}$
$D=Z^{\frac{1}{\rho_2}}$	$\xleftarrow{Z,PoK(\tau,\gamma)}\ Z=Y^{\frac{\gamma}{\tau}}$

图 1 匿名密钥分发协议

3 算法定义与安全模型

3.1 算法定义

本文方案包括系统初始化 $Global\ Setup(1^{\lambda})$、属性机构初始化 $Authority\ Setup(PP)$、密钥生成 $KeyGen(PP,SK_i,A_u)$、加密 $Encrypt(PP,m,(\boldsymbol{M},\rho))$、解密 $Decrypt\ (PP,C,SK_u)$、动态更新密钥生成 $DK_mGen\ (En(m),(\boldsymbol{M}',\rho'),(\boldsymbol{M},\rho))$、动态更新密文 $CUpdate(DK_m)$ 这 7 个算法，具体如下。

1) 系统初始化 $Global\ Setup(1^{\lambda})$：系统初始化算法由系统执行，输入安全参数 1^{λ}，输出系统公共参数 PP。

2) 属性机构初始化 $Authority\ Setup(PP)\to(PK_i,SK_i)$：算法由属性机构执行，输入公共参数 PP，输出属性机构的公私钥对。

3) 密钥生成 $KeyGen(PP,SK_i,A_u)\to SK_u$：算法由机构与用户交互完成，输入公共参数 PP、属性机构私钥 SK_i、用户属性集 A_u，输出用户私钥 SK_u。

4) 加密 $Encrypt(PP,m,(\boldsymbol{M},\rho))\to C$：算法由用户执行，输入公共参数 PP、明文 m、访问结构 (M,ρ)，输出密文 C，且用户保留加密信息 $En(m)=(\boldsymbol{v},q_1,\cdots,q_l)$。

5) 解密 $Decrypt(PP,C,SK_u)\to m$：算法由用户执行，输入公共参数 PP、用户私钥 SK_u、密文 C，输出明文 m。

6) 动态更新密钥生成 $DK_mGen(En(m),(\boldsymbol{M}',\rho'),(\boldsymbol{M},\rho))\to DK_m$：算法由用户执行，输入用户保留的加密信息、新策略 $(\boldsymbol{M}',\rho')$、旧策略 $(\boldsymbol{M},\rho)$，输出动态更新密钥 DK_m。

7) 动态更新密文 $CUpdate(DK_m)\to C'$：算法由云服务器执行，输入动态更新密钥 DK_m，输出更新的密文 C'。

3.2 安全模型

本方案的安全模型是选择属性和选择明文攻击下的不可区分性（IND-SAS-CPA, indistinguish ability against selective access structure and chosen plaintext attack）游戏，游戏中包含一个挑战者和一个敌手，挑战者模拟系统运行并回答敌手的询问；具体游戏如下。

Init：敌手 $\mathcal{A}$ 提交要挑战的旧的访问结构 $(\boldsymbol{M}^*,\rho^*)$ 和新的访问结构 $(\boldsymbol{M}^{\#},\rho^{\#})$ 给挑战者。

Global Setup：挑战者运行 *Global Setup* 算法，生成公共参数 *PP*，并发送给敌手。

Authorities Setup：挑战者运行 *Authorities Setup* 算法，生成属性机构的公私钥对，并将公钥发送给敌手。

Phase 1　敌手选择不属于 $(\boldsymbol{M}^*,\rho^*)$ 和 $(\boldsymbol{M}^{\#},\rho^{\#})$ 的属性，并发出私钥请求，挑战者返回其私钥。

Challenge　1) 敌手发送 2 个等长的消息 m_0 和 m_1 给挑战者，挑战者随机选取 $c\in\{0,1\}$，使用旧的访问结构 $(\boldsymbol{M}^*,\rho^*)$ 对 m_c 进行加密；2) 挑战者进行访问策略的动态更新，对敌手提交的新旧策略 $(\boldsymbol{M}^*,\rho^*)$ 和 $(\boldsymbol{M}^{\#},\rho^{\#})$ 进行对比，并将对比结果分为 3 种类型，根据对比结果生成相应的更新密文；3)挑战者将更新密文 C 发送给敌手。

Phase 2　重复 Phase 1。

Guess　敌手输出对 c 的猜想 $c'\in\{0,1\}$。

定义本文方案适应性选择明文攻击(CPA)是安全的，如果存在任意多项式时间的攻击者攻击游戏的优势 $\varepsilon=\left|\Pr[c=c']-\frac{1}{2}\right|$ 是可忽略的。

4 方案构造

本文方案采用 LSSS 访问策略，最大化根据旧的访问策略将新旧访问策略进行关联。引入动态策略更新算法，支持与、或、非等任何类型的策略更新。属性机构与用户之间通过运行匿名密钥分发协议为用户分发密钥，保护用户的 GID 隐私。假设本文方案共有 N 个属性机构 $AA_1,AA_2,\cdots,AA_N$，每个属性机构 AA_i 控制一组属性集 $A_i=(a_{i,1},a_{i,2},\cdots,a_{i,n_i})$，且每个用户拥有唯一身份标识 GID。具体方案构造如下。

1) 系统初始化 *Global Setup* (1^λ)

输入安全参数 λ，输出 $PP=(e,p,g,h,h_1,G,G_T)$，其中，G 和 G_T 是 2 个阶为素数 p 的乘法循环群，g、h、h_1 是群 G 的生成元，$e:G\times G\to G_T$；该算法选择散列函数：$H:\{0,1\}^*\to Z_p$，计算 $u=H(GID)$。

2) 属性机构初始化 *Authority Setup*(*PP*)

属性机构 AA_i 随机选择 $\alpha_i\in Z_p$，计算 $A_i=e(g,g)^{\alpha_i}$；对其管理的每个属性 $a_{i,j}\in A_i$，随机选择 $t_{i,j}\in Z_p$，计算 $T_{i,j}=g^{t_{i,j}}$；属性机构 AA_i 随机选择 $\beta_i\in Z_p$，计算 $B_i=h_1^{\beta_i}$，且定义一个仅可由 AA_i 与 AA_j 计算的伪随机函数 $PRF_{i,j}(\cdot)$，且 $PRF_{i,j}(u)=h_1^{\frac{\beta_i\beta_j}{(s_{i,j}+u)}}$，其中，$s_{i,j}$ 为 PRF 种子，是由机构 AA_i 与 AA_j 通过双方密钥交换共享一个只有双方知道的种子 $s_{i,j}$，显然 $s_{i,j}=s_{j,i}$，则机构 AA_i 私钥 $SK_i=\left\{\alpha_i,\beta_i,\left(s_{i,j}\right)_{j\in\{1,\cdots,N\}\setminus\{i\}},\left(t_{i,j}\right)_{j\in\{1,\cdots,n_i\}}\right\}$，机构公钥 $PK_i=\left\{A_i,B_i,\left(T_{i,j}\right)_{j\in\{1,\cdots,n_i\}}\right\}$。

3) 密钥生成 *KeyGen*(*PP*,SK_i,A_u)

定义 A_u 为用户属性集，用户与属性机构 AA_i 交互，对 $a_{i,j}\in A_u\cap A_i$，机构 AA_i 随机选择 $r_i\in Z_p$，计算 $R_i=g^{r_i}$，$R_{i,j}=T_{i,j}^{r_i}$；用户与属性机构之间运行匿名密钥分发协议（见第 2.5 节），令 $\gamma=\eta_{i,j}$，$\alpha=\eta_{i,j}\alpha_i$，$r=\eta_{i,j}r_i$，$g_1=B_j^{\beta_i}=h_i^{\beta_j\beta_i}$，$\beta=s_{i,j}$，当 $i>j$ 时，$\eta_{i,j}=1$，可得 $D_{i,j}=g^{\alpha_i}h^{r_i}PRF_{i,j}(u)$；当 $i<j$，$\eta_{i,j}=-1$，可得 $D_{i,j}=\frac{g^{\alpha_i}h^{r_i}}{PRF_{i,j}(u)}$；最后计算 $D_u=\prod_{(i,j)\in\{1,\cdots,N\}\times(\{1,\cdots,N\}\setminus(i))}D_{i,j}=g^{\sum_{i\in\{1,\cdots,N\}}(N-1)\alpha_i}\cdot h^{\sum_{i\in\{1,\cdots,N\}}(N-1)r_i}$。用户私钥 $SK_u=\left\{D_u,\left(R_i,R_{i,j}\right)_{a_{i,j}\in A_u\cap A_i}\right\}$。

4) 加密 *Encrypt*(*PP*,*m*,(M,ρ))

为加密明文 m，设定访问策略 A 为 $(\boldsymbol{M},\rho)$，$\boldsymbol{M}$ 是 $l\times n$ 的矩阵，映射 ρ 将 $\boldsymbol{M}$ 的每一行 $\boldsymbol{M}_i$ 与加密的每个属性映射，随机选择 $s\in Z_p$ 和随机向量 $\boldsymbol{v}=(s,v_2,\cdots,v_n)\in Z_p^n$，令 $\lambda_i=\boldsymbol{M}_i\boldsymbol{v}$，随机选择 $q_1,\cdots,q_l\in Z_p$，计算 $C_0=m\prod_{i\in\{1,\cdots,N\}}e(g,g)^{\alpha_i s}$，

$C_1 = g^s$，对于所有的 $a_{i,j} \in A$，计算 $C_{2,i} = h^{\lambda_i} T_{\rho(i)}^{-q_i}$，$C_{3,i} = g^{q_i}$，其中，$i \in (1,\cdots,l)$。则密文 $C = \{C_0, C_1, (C_{2,i}, C_{3,i})_{i\in(1,\cdots,l)}\}$。用户保留加密信息 $En(m) = (\boldsymbol{v}, q_1, \cdots, q_l)$。

5) 解密 $Decrypt(PP, C, SK_u)$

该算法输入密文 C、用户密钥 SK_u 及属性，如果解密者属性满足 A，则首先计算 $e(D_u, C_1) = e(g,g)^{s\sum_{i\in\{1,\cdots,N\}}(N-1)\alpha_i} e(g,h)^{s\sum_{i\in\{1,\cdots,N\}}(N-1)r_i}$，所以 $m = \dfrac{C_0 \prod_{i\in\{1,\cdots,N\}} \prod_{i=1}^{l} \left(e(C_{2,i}, R_i) e(C_{3,i}, R_{i,j})\right)^{\omega_i}}{e(D_u, C_1)^{\frac{1}{(N-1)}}}$，其中 $\sum_{i=1}^{l} \omega_i \lambda_i = s$。

6) 动态更新密钥生成 $DK_m Gen(En(m), (\boldsymbol{M}', \rho'), (\boldsymbol{M}, \rho))$

当用户发送到云服务器文件的访问策略需要变更时，用户只需根据其保留的加密信息 $En(m)$ 生成动态更新密钥 DK_m，并将其发送给云服务器，由云端更新对应密文。

在运行动态更新密钥 DK_m 生成前，系统首先运行 *PolicyCompare* 算法，进行新旧策略对比，输出行索引信息并将其存入 A_1'、A_2' 和 A_3' 中，定义 $n_{\rho(i),\boldsymbol{M}}$、$n_{\rho(i),\boldsymbol{M}'}$ 分别表示属性 $\rho(i)$ 在矩阵 $\boldsymbol{M}$、$\boldsymbol{M}'$ 中的数目，A_1', A_2' 表示 $\rho'(j)$ 存在 $\boldsymbol{M}$ 中的 j 的索引信息集，且 $\rho(i) = \rho'(j)$，如果 $n_{\rho'(j),\boldsymbol{M}'} \leqslant n_{\rho'(j),\boldsymbol{M}}$，则将 j 的索引信息存入 A_1'，如果 $n_{\rho'(j),\boldsymbol{M}'} > n_{\rho'(j),\boldsymbol{M}}$，则将 $n_{\rho'(j),\boldsymbol{M}'} - n_{\rho'(j),\boldsymbol{M}}$ 的行索引信息 j 存入 A_2'；A_3' 表示的是 $\rho'(j)$ 从未在 $\boldsymbol{M}$ 中出现的 j 的索引信息。

动态更新密钥 DK_m 生成算法选择一个新的随机向量 $\boldsymbol{v}' \in Z_p^{n'}$ 并将 s 作为其第一个输入值，令 $\lambda_j' = \boldsymbol{M}_j' \boldsymbol{v}'$，$\boldsymbol{M}_j'$ 表示矩阵 $\boldsymbol{M}'$ 的第 j 行；对于 $j \in [1, l']$，用户根据不同的类型。计算更新密钥

$$DK_m = \begin{cases} \left(DK = h^{\lambda_j' - \lambda_i}\right), (j,i) \in A_1' \\ \left(x_j, DK = h^{\lambda_j' - x_j\lambda_i}\right), (j,i) \in A_2' \\ \left(DK^{(1)} = h^{\lambda_j'} T_{\rho'(j)}^{-q_j'}, DK^{(2)} = g^{q_j'}\right), (j,i) \in A_3' \end{cases}$$

其中，$x_j, q_j' \in Z_p$。然后，用户将动态更新密钥 DK_m 发送至云服务器。

7) 动态更新密文 $DK_m Gen(En(m))$

$CUpdate(DK_m)$：云服务器接收到用户的动态更新密钥 DK_m 后，对于 $j \in [1, l']$，云服务器运行该算法，更新对应的密文元素，则

$$C_{2,j}' = \begin{cases} C_{2,i} DK = h^{\lambda_j'} T_{\rho'(j)}^{-q_j'}, & q_j' = q_i, \quad (j,i) \in A_1' \\ \left(C_{2,i}\right)^{x_j} DK = h^{\lambda_j'} T_{\rho'(j)}^{-q_j'}, & q_j' = x_j q_i, \quad (j,i) \in A_2' \\ DK^{(1)} = h^{\lambda_j'} T_{\rho'(j)}^{-q_j'}, & q_j' \in Z_p, \quad (j,i) \in A_3' \end{cases}$$

$$C_{3,j}' = \begin{cases} C_{3,i} = g^{q_j'}, & q_j' = q_i, \quad (j,i) \in A_1' \\ g^{q_j'}, & q_j' = x_j q_i, \quad (j,i) \in A_2' \\ DK^{(2)} = g^{q_j'}, & q_j' \in Z_p, \quad (j,i) \in A_3' \end{cases}$$

所以，新的密文为 $C' = \left\{C_0, C_1, \left(C_{2,j}', C_{3,j}'\right)_{j\in(1,\cdots,l')}\right\}$。

5 方案分析

5.1 安全性证明

定义 1 假设 q-PBDHE 假设成立，如果不存在任意多项式时间的敌手选择访问结构 $(\boldsymbol{M}^*, \rho^*)$ 下攻击支持策略动态更新的多机构 ABE 方案成功，那么该方案是 IND-SAS-CPA 安全的。

游戏开始前挑战者生成 q-PBDHE 挑战 $(\boldsymbol{y}, T)$：

Init: 敌手 $\mathcal{A}$ 提交要挑战的旧的访问结构 $(\boldsymbol{M}^*, \rho^*)$ 和新的访问结构 $(\boldsymbol{M}^{\#}, \rho^{\#})$，其中，$\boldsymbol{M}^*$ 是 $l^* \times n^*$ 的矩阵，$\boldsymbol{M}^{\#}$ 是 $l^{\#} \times n^{\#}$ 的矩阵，且 $l^*, n^*, l^{\#}, n^{\#} \leqslant q$。

Global Setup: 挑战者随机选择 $m \in Z_p$，计算 $h = g^m$，然后将公共参数 $PP = (e, p, g, h, h_1, G, G_T)$ 发送给 $\mathcal{A}$。

Authorities Setup: 属性机构 AA_i 随机选择 $\alpha_i' \in Z_p$，令 $\alpha_i = \alpha_i' + a^{q+1}$，计算 $A_i = e(g,g)^{\alpha_i} = e(g,g)^{\alpha_i'} e\left(g^a, g^{a^q}\right)$，随机选择 $\beta_i \in Z_p$，计算 $B_i = h_1^{\beta_i}$，并保存其 PRF 种子 $s_{i,j}$，定义伪随机函数 $PRF_{i,j}(u) = h_1^{\beta_i \beta_j / (s_{i,j} + u)}$；令 X 为指数 i 的集，$\rho^*(i) = x\left(i \in \left[1, \cdots, l^*\right]\right)$，对每个属性 $a_{i,j} \in A_i$ 且 $\rho^*(i) = x$，随机选择 $t_{i,j} \in Z_p$，计算 $T_{i,j} = g^{t_{i,j}} \prod_{i\in X} g^{\frac{aM_{i,1}^*}{b_i}} g^{\frac{a^2 M_{i,2}^*}{b_i}} \cdots g^{\frac{a^{n^*} M_{i,n^*}^*}{b_i}}$；对每个属性 $a_{i,j} \in A_i$ 且 $\rho^*(i) \neq x$，随机选择 $t_{i,j} \in Z_p$，计算 $T_{i,j} = g^{t_{i,j}}$。机构 AA_i 私钥 $SK_i = \{\alpha_i', \beta_i, (s_{i,j})_{j\in\{1,\cdots,N\}\setminus\{i\}}, (t_{i,j})_{j\in\{1,\cdots,n_i\}}\}$，机构公钥 $PK_i =$

$\left\{A_i, B_i, \left(T_{i,j}\right)_{j\in\{1,\ldots,n_i\}}\right\}$，挑战者将属性机构公钥 PK_i 发送给敌手。

Phase 1　敌手为其不属于$\left(\boldsymbol{M}^*, \rho^*\right)$和$\left(\boldsymbol{M}^{\#}, \rho^{\#}\right)$的属性集 S 询问私钥，挑战者随机选择$n\in Z_p$，$\boldsymbol{\omega}=\left(\omega_1,\omega_2,\cdots,\omega_{n^*}\right)\in Z_p^{n^*}$，且 $\omega_1=-1$，对所有的$\rho^*(i)\in S$，有$\boldsymbol{\omega}\boldsymbol{M}_i^*=0$；对于所有的$a_{i,j}\in A_u\cap A_i$，随机选择 $r_i'\in Z_p$，令 $r_i=r_i'+\omega_1 a^q+\omega_2 a^{q-1}+\cdots+\omega_{n^*}a^{q-n^*+1}$，则 $R_i=g^{r_i'}\prod_{i=1,\cdots,n^*}\left(g^{a^{q+1-i}}\right)^{\omega_i}=g^{r_i}$，对每个属性 $a_{i,j}\in A_u\cap A_i$ 且 $\rho^*(i)\neq x$，计算 $R_{i,j}=R_i^{t_{i,j}}=T_{i,j}^{r_i}$，对每个属性$a_{i,j}\in A_u\cap A_i$且$\rho^*(i)=x$，计算 $R_{i,j}=R_i^{t_{i,j}}\prod_{i\in X}\prod_{j=1,\cdots,n^*}\left(g^{\left(\frac{a^j}{b_i}\right)r_i'}\prod_{k=1,\cdots,n^*,k\neq j}\left(g^{\frac{a^{q+1+j-k}}{b_i}}\right)^{\omega_k}\right)^{\boldsymbol{M}_{i,j}^*}=T_{i,j}^{r_i}$；敌手根据匿名密钥分发协议计算 $D_u=\prod_{(i,j)\in\{1,\cdots,N\}\times(\{1,\cdots,N\}\setminus(i))}D_{i,j}=g^{\sum_{i\in\{1,\cdots,N\}}(N-1)\alpha_i'}\cdot h^{\sum_{i\in\{1,\cdots,N\}}(N-1)r_i}$，挑战者将敌手的私钥 $SK_u=\left\{D_u,\left(R_i,R_{i,j}\right)_{a_{i,j}\in A_u\cap A_i}\right\}$发送给敌手。

Challenge　1) 攻击者随机选择 2 个等长的消息 m_0、m_1 给挑战者，挑战者随机选取$c\in\{0,1\}$，对m_c进行加密，计算$C_0=m_cT\prod_i e(g,g)^{\alpha_i' s}$，$C_1=g^s$，随机选择 $\boldsymbol{v}^*=(s, sa+v_2^*, sa^2+v_3^*,\cdots, sa^{n-1}+v_{n^*}^*)\in Z_p^{n^*}$，$q_1^*,\cdots,q_{l^*}^*\in Z_p$，对$i=1,\cdots,n^*$，定义 H_i 为 $i\neq j$ 时 $\rho^*(i)=\rho^*(j)$ 的集合，则密文元素 $C_{2,i}=T_{\rho^*(i)}^{q_i^*}\left(\prod_{j=1,\cdots,n^*}(h)^{\boldsymbol{M}_{i,j}^*v_j^*}\right)\left(g^{b_i s}\right)^{-t_{\rho^*(i)}}\cdot\left(\prod_{k\in H_i}\prod_{j=1,\cdots,n^*}\left(g^{a^j s\left(\frac{b_i}{b_k}\right)}\right)^{\boldsymbol{M}_{k,j}^*}\right)C_{3,i}=g^{-q_i^*}g^{-sb_i}$。2) 挑战者根据敌手提供的新的访问策略$\left(\boldsymbol{M}^{\#},\rho^{\#}\right)$进行新旧策略对比，并将新策略中的属性分为 3 种类型分别将其行索引信息存入I_1'、I_2'、I_3'中，定义$n_{\rho^*(i),\boldsymbol{M}^*}$、$n_{\rho^*(i),\boldsymbol{M}^{\#}}$分别表示属性$\rho^*(i)$在矩阵 $\boldsymbol{M}^*$、$\boldsymbol{M}^{\#}$中的数目，I_1'和I_2'表示$\rho^{\#}(j)$存在$\boldsymbol{M}^*$中的j的索引信息集，且$\rho^*(i)=\rho^{\#}(j)$，如果$n_{\rho^{\#}(j),\boldsymbol{M}^{\#}}\leqslant n_{\rho^{\#}(j),\boldsymbol{M}^*}$，则将 j 的索引信息存入I_1'，如果$n_{\rho^{\#}(j),\boldsymbol{M}^{\#}}>n_{\rho^{\#}(j),\boldsymbol{M}^*}$，则将 $n_{\rho^{\#}(j),\boldsymbol{M}^{\#}}-n_{\rho^{\#}(j),\boldsymbol{M}^*}$ 的行索引信息 j 存入I_2'；I_3'表示$\rho^{\#}(j)$从未在$\boldsymbol{M}^*$中出现的j的索引信息。随机向量$\boldsymbol{v}^{\#}=\left(s, sa+v_2^{\#}, sa^2+v_3^{\#},\cdots, sa^{n-1}+v_{n^{\#}}^{\#}\right)\in Z_p^{n^{\#}}$，计算更新密钥；若$(j,i)\in I_1'$，更新密钥 $DK=\left(DK=h^{\boldsymbol{M}_{i,j}^{\#}v_j^{\#}-\boldsymbol{M}_{i,j}^*v_j^*}\right)$。若$(j,i)\in I_2'$，算法随机选择$x_j, q_j{}^{\#}\in Z_p$，更新密钥$DK=\left(x_j, DK=h^{\boldsymbol{M}_{i,j}^{\#}v_j^{\#}-x_j\boldsymbol{M}_{i,j}^*v_j^*}\right)$。若$(j,i)\in I_3'$，算法随机选择$q_j{}^{\#}\in Z_p$，更新密钥 $DK=(DK^{(1)}=T_{\rho^{\#}(i)}^{q_i^{\#}}\left(\prod_{j=1,\cdots,n^{\#}}(h)^{\boldsymbol{M}_{i,j}^{\#}v_j^{\#}}\right)\left(g^{b_i s}\right)^{-t_{\rho^{\#}(i)}}\cdot\left(\prod_{k\in H_i}\prod_{j=1,\ldots,n^{\#}}\left(g^{a^j s\cdot\left(\frac{b_i}{b_k}\right)}\right)^{\boldsymbol{M}_{k,j}^{\#}}\right)$，$DK^{(2)}=g^{-q_i^{\#}}g^{-sb_i}$)，最后，挑战者计算新访问策略对应的密文元素 $C_{2,j}^{\#}=T_{\rho^{\#}(i)}^{q_i^{\#}}\left(\prod_{j=1,\ldots,n^{\#}}(h)^{\boldsymbol{M}_{i,j}^{\#}v_j^{\#}}\right)\left(g^{b_i s}\right)^{-t_{\rho^{\#}(i)}}\cdot\left(\prod_{k\in H_i}\prod_{j=1,\ldots,n^{\#}}\left(g^{a^j s\left(b_i/b_k\right)}\right)^{\boldsymbol{M}_{k,j}^{\#}}\right)$，$C_{3,j}^{\#}=g^{-q_i^{\#}}g^{-sb_i}$。3) 挑战者将密文 $C=\{C_0,C_1,(C_{2,j}^{\#},C_{3,j}^{\#})_{i\in(1,\cdots,l^{\#})}\}$ 发送给敌手。

Phase 2　重复 Phase 1。

Guess　敌手输出对 c 的猜想$c'\in\{0,1\}$。如果$c'=c$，则挑战者输出$\theta=0$，表示$T=e(g,g)^{a^{q+1}s}$，此时敌手的优势 $\Pr[c'=c\,|\,\theta=0]=\frac{1}{2}+\varepsilon$。如果$c'\neq c$，则输出$\theta=1$，表示 T 是群 G_T 中的一个随机元素，此时敌手的优势$\Pr[c'=c\,|\,\theta=1]=\frac{1}{2}$。

因此，敌手攻击 q-PBDHE 假设的优势为 $Adv_{\mathcal{A}}=\left|\frac{1}{2}\Pr[c'=c\,|\,\theta=0]+\frac{1}{2}\Pr[c'=c\,|\,\theta=1]-\frac{1}{2}\right|=\frac{1}{2}\times\frac{1}{2}+\frac{1}{2}\times\left(\frac{1}{2}+\varepsilon\right)-\frac{1}{2}=\frac{1}{2}\varepsilon$。任何多项式时间内敌手赢得 IND-SAS-CPA 游戏的优势是可忽略的。

5.2　性能分析

本文从功能、安全和通信代价 3 个方面对相关方案进行比较，具体结果如表 1 所示。功能方面主要从是否支持多机构以及动态策略更新方面进行分析，安全性从群阶、安全模型和安全性方面进行分析，通信代价从用户私钥大小、密文大小和动态更新密钥大小方面进行分析。其中，S 表示用户的属性

表 1 **相关 ABE 方案对比**

方案	功能		安全性		通信代价				
	多机构	动态策略更新	群阶	安全模型	用户私钥大小	密文大小	动态更新密钥大小		
							类型 1	类型 2	类型 3
文献[3]方案	√	×	素数	Standard	$S+6$	$(2l+3)I_c+1$	—	—	—
文献[6]方案	√	√	合数	Generic Group	S	$3l+1$	$2l_1'$	$3l_2'$	$3l_3'$
文献[7]方案	×	√	合数	Standard	$S+2$	$2(2l+2)$	$5l_1'$	$6l_2'$	$4l_3'$
文献[11]方案	√	√	合数	Standard	$S+D(N+2)$	$2l+2$	l_1'	$2l_2'$	$2l_3'$
本文方案	√	√	素数	Standard	$2S+1$	$2l+2$	l_1'	$2l_2'$	$2l_3'$

个数，D 表示中央机构 CA 的个数，N 表示属性机构 AA 的个数，l 表示加密所用的属性个数，I_c 表示加密时使用的属性所属的机构数，l_1'、l_2'、l_3' 分别表示更新策略时类型 1、类型 2、类型 3 的属性个数。

从表 1 可以看出文献[3]并不支持策略更新，文献[7]虽支持策略更新，但其方案是单机构的，单机构的属性基加密方案安全性和实用性较低，而本文方案和文献[6,11]支持多个机构管理不同的属性集，并为其权限下的用户分发密钥，具有更好的实用性。从安全方面来看，文献[7]仅仅满足一般群模型下安全，而本文方案和其他文献是在标准模型下安全的，另外本文采用的匿名密钥分发协议可以很好地保护用户的 GID，安全性更高。

从通信代价对比结果来看，其中用户私钥方面文献[3]、文献[6]和文献[7]的方案相对较小，仅和用户的属性个数相关。文献[11]中用户私钥由多个中央机构、多个属性机构共同生成，用户需要与多个中央机构和多个属性机构进行交互并进行签名认证，通信代价较大，且用户私钥大小与中央机构、属性机构以及用户属性个数线性相关，私钥长度较长。而本文方案采用匿名密钥分发协议，减轻了用户密钥生成中用户与各机构之间的通信开销，用户密钥长度仅和用户属性个数相关，远远小于文献[11]。密文长度方面，本文方案和文献[11]中方案相同，长度与加密时访问策略中的属性个数呈线性增长。相比较于文献[3]、文献[6]和文献[7]，本文方案的密文长度大大缩短，比文献[7]缩短了 $\frac{1}{2}$。动态策略更新密钥方面，本文方案 3 种类型密钥大小同样和文献[11]相同，远远小于文献[6]和文献[7]。

综合分析，本文在用户私钥、密文以及动态更新密钥大小等性能方面是较优的，并可支持动态策略更新，可以很好地应用于个人健康病例等系统中。

6 结束语

针对云环境应用中数据拥有者经常需要动态地更新加密策略，提出支持策略动态更新的多机构 ABE 方案，本文方案中用户在更新访问策略时，仅需做少量的计算，其他更新计算由云服务器操作，较大地节省了计算与通信开销；另外，本文还提供对用户的隐私保护，并可抵抗 N−1 个属性机构的共谋攻击。现有的动态策略更新都是基于 LSSS 的，研究访问树的较少，下一步工作将对基于访问树的动态策略更新进行深入的研究。

参考文献：

[1] LEWKO A, WATERS B. Decentralizing attribute-based encryption[C]//International Conference Theory and Applications of Cryptographic Techniques. 2011: 568-588.

[2] XHAFA F, FENG J, ZHANG Y, et al. Privacy-aware attribute-based PHR sharing with user accountability in cloud computing[J]. Journal of Supercomputing, 2015,71:1607-1619.

[3] HAN J, SUSILO W, MU Y, et al. Improving privacy and security in decentralized ciphertext-policy attribute-based encryption[J]. IEEE Transactions on Information Forensics and Security, 2015, 10 (3): 665-678.

[4] 陶启, 黄晓芳. 基于密文策略多机构属性基加密方案[J]. 武汉大学学报(理学版), 2015, 61(6): 545-548 .

TAO Q, HUANG X F. Multi-authority ciphertext-policy attribute-based encryption scheme[J]. Journal of Wuhan University (Nature Science Edition), 2015, 61(6): 545-548 .

[5] SAHAI A, SEYALIOGLU H, WATERS B. Dynamic credentials and ciphertext delegation for attribute-based encryption[M]. Advances in Cryptology-EUROCRYPT 2012, Springer Berlin Heidelberg, 2012: 199-217.

[6] YANG K, JIA X H, REN K. Secure and veritiable policy update outsourcing for big data access control in the cloud[J]. IEEE Transactions on Parallel and Distributed Systems, 2015, 26(12)：3461-3470.

[7] 应作斌, 马建峰, 崔江涛. 支持动态策略更新的半策略隐藏属性加密方案[J]. 通信学报, 2015, 36(12):178-189.
YING Z B, MA J F, CUI J T. Partially policy hidden CP-ABE supporting dynamic policy updating[J]. Journal on Communications, 2015, 36(12):178-189.

[8] LI H, LIU D X, ALHARBI K, et al. Enabling fine-grained access control with efficient attribute revocation and policy updating in smart grid[J]. KSII Transactions on Internet and Information Systems, 2015, 9(4):1404-1423.

[9] QIAN H L, LI J G, ZHANG Y C, et al. Privacy-preserving personal health record using multi-authority attribute-based encryption with revocation[J]. International Journal of Information Security, 2015, 14(6):487-497.

[10] 吴光强. 适合云存储的访问策略可更新多中心 CP-ABE 方案[J]. 计算机研究与发展. 2016, 53(10):2393-2399.
WU G Q. Multi-authority CP-ABE with policy update in cloud storage[J]. Journal of Computer Research and Development, 2016, 53(10): 2393-2399.

[11] YING Z B, LI H, MA J F, et al. Adaptively secure ciphertext-policy attribute-based encryption with dynamic policy updating[J]. Science China-Information Sciences, 2016, 59(4):1-16.

[12] 应作斌, 马建峰, 崔江涛, 等. 支持位置验证和策略变更的属性加密方案[J]. 西安电子科技大学学报(自然科学版), 2017, 44(2): 57-62.
YING Z B, MA J F, CUI J T, et al. Attribute-based encryption with location verification and policy adjusting supporting the cloud mobile office[J]. Journal of Xidian University (Nature Science Edition), 2017, 44(2):57-62.

作者简介：

闫玺玺（1985-），女，河南灵宝人，博士，河南理工大学讲师、硕士生导师，主要研究方向为网络与信息安全、数字版权管理、数字内容安全和密码学。

刘媛（1989-），女，河南濮阳人，河南理工大学硕士生，主要研究方向为密码学、网络与信息安全。

李子臣（1965-），男，河南温县人，北京印刷学院教授、博士生导师，主要研究方向为信息安全、电子商务和密码学。

汤永利（1972-），男，河南焦作人，河南理工大学教授、硕士生导师，主要研究方向为密码学算法检测、网络与信息安全。