支持关键词搜索的属性代理重加密方案

刘振华 周佩琳* 段淑红
(西安电子科技大学数学与统计学院 西安 710071)

摘 要：属性代理重加密机制既能实现数据共享又能实现数据转发，但这种机制通常并不支持数据检索功能，阻碍了属性代理重加密的发展应用。为了解决这一问题，该文提出一个支持关键词搜索的密文策略的属性代理重加密方案。通过将密钥分为属性密钥和搜索密钥，不仅可以实现关键词可搜索，而且实现了代理重加密。在验证阶段，云服务器既执行关键词验证，又可以对原始密文和重加密密文进行部分解密，从而减轻用户的计算负担。通过安全性分析，该方案可以实现数据安全性、检索分离、关键词隐藏和抗共谋攻击。

关键词：云存储；属性重加密；代理重加密；可搜索加密；访问控制
中图分类号：TP309 **文献标识码**：A **文章编号**：1009-5896(2018)03-0683-07
DOI: 10.11999/JEIT170448

Attribute-based Proxy Re-encryption Scheme with Keyword Search

LIU Zhenhua ZHOU Peilin DUAN Shuhong
(*School of Mathematics and Statistics*, *Xidian University*, *Xi'an* 710071, *China*)

Abstract: Attribute-based proxy re-encryption mechanism can not only realize data sharing but also achieve data forwarding. However, this mechanism can not support the functionality of data retrieval, which hinders the applications of attribute-based proxy re-encryption. In order to solve the issue, this paper proposes a ciphertext-policy attribute-based proxy re-encryption scheme with keyword search. By dividing a secret key into an attribute key and a search key, the new scheme can not only achieve the keyword search, but also support proxy re-encryption. In the test phase, while conducting the keywords matching algorithm, the cloud server can do partial decryption of the original ciphertext and the re-encrypted ciphertext, which can reduce the computational burden for users. The security analysis indicates that the proposed scheme can achieve data security, hidden keywords, query isolation and collusion resistance.

Key words: Cloud storage; Attributed-based encryption; Proxy re-encryption; Searchable encryption; Access control

1 引言

物联网的快速发展带动了云计算[1]的兴起。云计算的基本数据服务包括海量数据的存储、检索以及各种服务的接入控制等。在众多的云服务器中，云存储[2]服务器凭借其低成本、按次付费和高扩展性等特点，赢得众多云用户的青睐。但是，云存储采用了与传统 IT 外包模式迥异的多租户规则，这些差异带来了一系列个人数据的安全问题。所以，云存储在为云用户提供数据服务的同时，也面临着诸多挑战和一些亟需解决的安全问题。

由于其自身的特点，属性基加密[3,4] (Attribute-Based Encryption, ABE)非常适合云存储这种大规模用户的访问控制，它能够在一定程度上限制用户的解密能力，同时也能够证数据的机密性。2005 年，Sahai 等人[5]在欧密会上提出模糊身份加密方案，后来 Goyal 等人[6]将其拓展为属性加密。按照密文或密钥关联属性的不同，基于属性的加密方案可以分为两种形式：密钥策略的属性基加密[6]和密文策略的属性基加密[7]。Guo 等人[8]在 ABE 方案中引入代理重加密技术，开创性地提出首个密钥策略属性代理重加密方案。后来，Liang 等人[9]提出密文策略属性代理重加密方案。但这两个方案只能达到选择明文攻击安全，因此 Liang 等人[10]提出首个在随机谕言机模型下选择密文安全的密文策略属性代理重加密方案。2016 年，Ge 等人[11]首次提出在标准模型下选择

收稿日期：2017-05-11；改回日期：2017-12-12；网络出版：2018-01-11
*通信作者：周佩琳 plzhou1224@163.com
基金项目：国家重点研发计划(2017YFB0802000)，国家自然科学基金(61472470)，陕西省教育厅专项科研计划(17JK0362)
Foundation Items: The National Key R&D Program of China (2017YFB0802000), The National Natural Science Foundation of China (61472470), The Scientific Research Plan Project of Education Department of Shaanxi Province (17JK0362)

密文安全的密钥策略属性代理重加密方案。为了解决用户的属性隐私和访问策略更新问题，Zhang 等人[12]提出匿名的密文策略属性代理重加密方案。实际上，属性代理重加密机制在云计算中有着广泛应用，例如个人健康管理系统和加密邮件的转发等。因为它既能实现数据共享，又能实现数据转发等机制。但是，上述方案均不支持安全的数据检索功能。为了使机密的数据能够被分享、检索并委派解密权力，Shi 等人[13]提出了支持关键词搜索的属性代理重加密(Attribute-Based Proxy Re- encryption with Keyword Search, ABPRKS)方案，并给出了两个方案：密钥策略 ABPRKS 和密文策略 ABPRKS，且证明了这两个方案在随机谕言机模型下是选择关键词攻击安全的。但是该方案中密文检索机制实质上是基于公钥的可搜索加密，尽管数据的访问控制是基于属性的密码体制，但它并不是纯粹的 ABPRKS，且不支持对原始密文和重加密密文的解密。后来，Liang 等人[14]提出可搜索的密钥策略的属性代理重加密系统，并证明了该方案在随机谕言机模型下是选择密文安全的，但该方案的计算代价太大。

本文针对上述问题，在 Liang 等人[10]方案的基础上提出一种支持可搜索的密文策略属性代理重加密方案，并进行了安全性分析。本文的主要贡献为：提出支持可搜索的密文策略的属性代理重加密方案。新方案不仅可以实现关键词可搜索，而且实现了代理重加密的性质，有效地将两种技术结合起来，具有更丰富的访问控制表达性。此外新方案可以实现数据安全性、检索分离、关键词隐藏和抗共谋攻击。

2 算法描述

本节给出支持可搜索的密文策略属性代理重加密方案(Ciphertext Policy Attribute-Based Proxy Re-encryption with Keyword Search, CP-ABPRKS)的系统模型和具体方案。

2.1 系统模型

为了更为直观地描述方案，我们用个人医疗记录来举例阐述，如图 1 所示。

考虑到以下场景：一个患有糖尿病的病人 A 想通过在线医疗服务机构(例如，在线医疗评定网)寻找一所医院进行常规的检查治疗。A 要求这家医院必须在郭杜镇 10 km 以内。为方便起见，将 A 的需求记为 I_1={郭杜镇 10 km 以内}。为了保护医疗记录的机密性，A 需要在上传到在线医疗服务机构(代理)之前将医疗记录在 I_1 的条件下加密。然后代理(知道 I_1 的内容)在自己的数据库中搜索满足 I_1 的候选医院，并将 A 的医疗记录发送给满足条件的医院 H_1，而 H_1 可以解密查看该记录。若在后续的治疗过程中，医院 H_1 的医疗条件和水平不能够继续为病人 A 治疗，H_1 需要与其它医院进行合作，并且 A 的医疗记录也要发送给满足以下条件的医院：必须是三级甲等医院，将该需求记为 I_2={三级甲等医院}并假设医院 H_2 和 H_3 都满足该需求。运用代理重加密机制，H_1 可作为委托者，在线医疗评定网(云服务器)可作为代理，H_2 和 H_3 可作为受托者。代理可用委托者产生的重加密密钥，将在 I_1 条件下加密的医疗记录密文转化为在 I_2 下加密的密文，使得 H_2 和 H_3 都能够解密该密文。

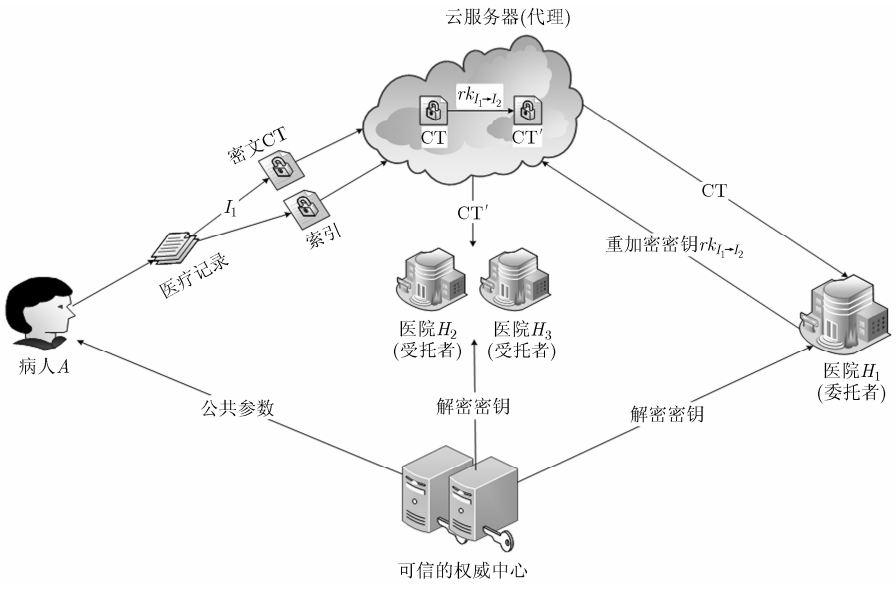

图 1 CP-ABPRKS 方案的系统模型图

需要注意的是，在整个过程中，代理无法获得关于病人医疗记录的任何内容。整个过程有两个搜索阶段：(1) A 发起搜索请求让云服务器进行搜索，并将匹配的结果发送给 H_1，该过程 A 充当数据拥有者；(2) H_1 发起搜索请求让云服务器进行搜索，并将匹配的结果发送给 H_2 和 H_3，该过程 H_1 充当数据拥有者。

2.2 具体方案

基于 Wang 等人[15]的属性可搜索加密方案与 Liang 等人[10]的属性代理重加密方案，本文提出一个新的支持可搜索的密文策略属性代理重加密方案。新方案既可以实现数据共享和关键词搜索，又能实现数据转发机制。记 $a \in_R \mathbb{Z}_p^*$ 表示从集合 $\mathbb{Z}_p^*$ 中均匀随机地选取元素 a。需要注意的是，方案中用 σ 表示用户的身份标签，拥有不同属性集 S 的标签 σ 也不相同，σ 只是用来区分用户身份。下面是具体方案描述：

系统建立 $(1^\kappa, \mathcal{U})$：可信权威中心(Trusted Authority, TA)执行该算法。输入安全参数 1^κ 和属性全集 $\mathcal{U}$。设 $\mathbb{G}$ 和 $\mathbb{G}_T$ 是两个阶为素数 p 的乘法循环群，g 是 $\mathbb{G}$ 的生成元，$e:\mathbb{G}\times\mathbb{G}\to\mathbb{G}_T$ 是一个双线性映射。随机选取 $\mathbb{G}$ 中的另一个生成元 g_1 并选择 $a,\alpha \in_R \mathbb{Z}_p^*$。定义 TCR 哈希函数 $H_1:\{0,1\}^{2k}\to\mathbb{Z}_p^*$，$H_2:\mathbb{G}_T\to\{0,1\}^{2k}$, $H_3:\{0,1\}^*\to\mathbb{G}$, $H_4:\{0,1\}^*\to\mathbb{G}$, $H_5:\{0,1\}^k\to\mathbb{Z}_p^*$, $H_6:\{0,1\}^*\to\mathbb{G}$，并定义消息认证函数为 F。输出公共参数 PP 和主密钥 MSK。

$$\mathrm{PP}=\langle e,p,g,g_1,g^a,e(g,g)^\alpha,H_1,H_2,H_3,H_4,H_5,H_6,F\rangle,$$
$$\mathrm{MSK}=\langle g^\alpha,a\rangle \tag{1}$$

私钥提取 (MSK,S)：输入主密钥 MSK 和具有身份标签 σ 的用户属性集 $S\subseteq\mathcal{U}$。选择 $t\in_R\mathbb{Z}_p^*$，输出私钥。

$$\mathrm{SK}_\sigma=\left\langle K=g^\alpha g^{at}, L=g^t, \{K_x=H_3(x)^t\}_{\forall x\in S}\right\rangle \tag{2}$$

最后，TA 将 (σ, g^{at}) 添加到用户列表 L_{DU} 中。

搜索密钥提取 $(\mathrm{MSK},\mathrm{PP})$：该算法由用户和 TA 交互进行。当用户对关键词 kw' 进行搜索时，随机选取 $u\in_R\mathbb{Z}_p^*$ 并令 $q_u=g^u$。然后将自己的身份标签 σ 和 q_u 发送给 TA。TA 查看用户的身份标签 σ 是否在用户列表 L_{DU} 里，如果存在，则为用户生成一个对应于关键词 kw' 的搜索密钥

$$\mathrm{SK}'=\left\langle g^{at}\cdot {q_u}^\alpha\right\rangle \tag{3}$$

数据加密 $(\mathrm{PP},(\boldsymbol{M},\rho),m)$：输入公共参数 PP、访问结构 $(\boldsymbol{M},\rho)$ ($\boldsymbol{M}$ 是一个 $l\times n$ 的矩阵，函数 ρ 将矩阵 $\boldsymbol{M}$ 的行映射成属性)和明文消息 $m\in\{0,1\}^k$。选择 $\beta\in_R\{0,1\}^k$，并计算 $s=H_1(m,\beta)$。然后选择一个随机向量 $\boldsymbol{v}=(s,y_2,\cdots,y_n)\in\mathbb{Z}_p^n$，该随机向量用来分享秘密指数 s。对于 $i=1,2,\cdots,l$，令 $\lambda_i=\boldsymbol{v}\cdot\boldsymbol{M}_i$，其中 $\boldsymbol{M}_i$ 是对应于 $\boldsymbol{M}$ 的第 i 行向量。最后选择 $r_1,r_2,\cdots,r_l\in_R\mathbb{Z}_p^*$，则密文为

$$\begin{aligned}\mathrm{CT}=\Big\langle & A_1=(m\,\|\,\beta)\oplus H_2(e(g,g)^{\alpha s}),\\ & A_2=g^s,\left\{B_i=g^{a\lambda_i}H_3(\rho(i))^{-r_i}\right\}_{i\in[l]},\\ & \{C_i=g^{r_i}\}_{i\in[l]},A_3=g_1^s,\\ & D=\left(H_4\left(A_1,A_3,(B_i,C_i)_{i=1}^l,(\boldsymbol{M},\rho)\right)\right)^s\Big\rangle\end{aligned} \tag{4}$$

数据拥有者将该密文上传到云服务器中。需要注意 $\{\rho(i)\,|\,1\le i\le l\}$ 是访问结构 $(\boldsymbol{M},\rho)$ 中用到的属性，且函数 ρ 是一个非单射函数，也就是说，允许一个属性与矩阵 $\boldsymbol{M}$ 的多行有关联。

重加密密钥提取 $(\mathrm{SK}_\sigma,(\boldsymbol{M}',\rho'),S)$：该算法输入用户私钥 SK_σ 和对应的属性集 S，以及访问结构 $(\boldsymbol{M}',\rho')$ ($\boldsymbol{M}'$ 是一个 $l'\times n'$ 的矩阵，函数 ρ' 将矩阵 $\boldsymbol{M}'$ 的行映射成属性)，重加密密钥按如下方式生成：

(1)委托者先进行如下的加密操作：

(a)选择 $\beta',\delta\in_R\{0,1\}^k$，并计算 $s'=H_1(\delta,\beta')$。

(b)选择一个随机向量 $\boldsymbol{v}'=\left(s',y_2',\cdots,y_n'\right)\in\mathbb{Z}_p^n$，该随机向量用来分享秘密指数 s'。对于 $i=1,2,\cdots,l'$，令 $\lambda_i'=\boldsymbol{v}'\cdot\boldsymbol{M}_i'$，其中 $\boldsymbol{M}_i'$ 是对应于 $\boldsymbol{M}'$ 的第 i 行向量。

(c)选择 $r_1',r_2',\cdots,r_{l'}'\in_R\mathbb{Z}_p^*$，并输出

$$\begin{aligned}\mathrm{rk}_4=\Big\langle & A_1'=(\delta\,\|\beta')\oplus H_2\left(e(g,g)^{\alpha s'}\right),\\ & A_2'=g^{s'},\left\{B_i'=g^{a\lambda_i'}H_3(\rho'(i))^{-r_i'}\right\}_{i\in[l']},\\ & \left\{C_i'=g^{r_i'}\right\}_{i\in[l']},\\ & D'=\left(H_6\left(A_1',A_2',\left(B_i',C_i'\right)_{i=1}^l,S,(\boldsymbol{M}',\rho')\right)\right)^{s'}\Big\rangle\end{aligned} \tag{5}$$

(2)然后选取 $\theta\in_R\mathbb{Z}_p^*$，则重加密密钥为

$$\begin{aligned}\mathrm{rk}=\Big\langle & \mathrm{rk}_1=K^{H_5(\delta)}\cdot g_1^\theta,\mathrm{rk}_2=g^\theta,\mathrm{rk}_3=L^{H_5(\delta)},\\ & \mathrm{rk}_4,\ \left\{R_x=K_x^{H_5(\delta)}\right\}_{\forall x\in S}\Big\rangle\end{aligned} \tag{6}$$

最后，委托者将 rk 发送给云服务器(代理)，该重加密密钥用来对原始密文进行重加密。

数据重加密 $(\mathrm{rk},\mathrm{CT})$：算法输入重加密密钥 rk 和原始密文 CT，令 $I=\{i:\rho(i)\in S\}\subseteq\{1,2,\cdots,l\}$，则存在系数 $\{\omega_i\,|\,i\in I\}$ 使得 $\sum_{i\in I}\omega_i\boldsymbol{M}_i=(1,0,\cdots,0)$，那么 $\sum_{i\in I}\omega_i\lambda_i=s$。代理者可以通过式(7)验证重加密密钥 rk 是否包含有效的属性集 S 和访问结构 $(\boldsymbol{M}',\rho')$。

$$e\left(A_2',H_6\left(A_1',A_2',\left(B_i',C_i'\right)_{i=1}^l,S,(\boldsymbol{M}',\rho')\right)\right)=e(g,D') \tag{7}$$

当属性集 S 满足访问结构 $(\boldsymbol{M},\rho)$，通过式(8)验证原始密文的有效性

$$\begin{aligned}&e(A_2,g_1)=e(g,A_3),\\&\quad e\left(A_3,H_4\left(A_1,A_3,(B_i,C_i)_{i=1}^{l},(\boldsymbol{M},\rho)\right)\right)\\&=e(g_1,D),e\left(\prod_{i\in I}B_i^{\omega_i},g^a\right)\\&=e(A_2,g)\cdot\prod_{i\in I}e\left(C_i^{-1},H_3(\rho(i))^{\omega_i}\right)\end{aligned}\tag{8}$$

如果式(8)不成立，停止。否则计算

$$A_4=\frac{e\left(A_2,\mathrm{rk}_1\right)/e\left(A_3,\mathrm{rk}_2\right)}{\prod\limits_{i\in I}\left(e\left(B_i,\mathrm{rk}_3\right)\cdot e\left(C_i,R_{\rho(i)}\right)^{\omega_i}\right)}$$

最后输出重加密密文为

$$\mathrm{CT}'=\left\langle A_1,A_2,A_3,A_4,\mathrm{rk}_4,(B_i,C_i)_{i=1}^{l},D,S,(\boldsymbol{M},\rho)\right\rangle$$

索引生成(PP,KW)：输入公共参数 PP 和对应于消息 m 的关键词集合 $\mathrm{KW}=\{\mathrm{kw}_i\}_{i=1}^{l}$。为每一个关键词 kw_i 选取一个随机比特串 t_i，分别计算原始密文 CT 中 kw_i 对应的消息认证码 $k_i=e(g,g)^{\alpha s}\cdot e\left(g,H_3\left(\mathrm{kw}_i\right)\right)^{s}$ 和重加密密文 CT′ 中 kw_i 对应的消息认证码 $k_i^{'}=e(g,g)^{\alpha s'}e\left(g,H_3(\mathrm{kw}_i)\right)^{s'}$。安全索引为

$$\mathrm{IX}=\left\langle t_i,F\left(k_i,t_i\right)\right\rangle,\ \mathrm{IX}'=\left\langle t_i,F\left(k_i^{'},t_i\right)\right\rangle\tag{9}$$

令牌生成$(\mathrm{SK}_\sigma,\mathrm{kw}',S,\mathrm{SK}')$：输入具有用户身份标签 σ 的私钥 SK_σ，属性集 S，关键词 kw' 以及 kw' 对应的搜索密钥 SK'。最后输出关键词 kw 的搜索令牌：

$$\begin{aligned}\mathrm{TK}=\Big\langle&T=H_3\left(\mathrm{kw}'\right)\left(g^{at}\cdot q_u^{\alpha}\right)^{1/u},\\&L'=L^{1/u},\ \left\{K_x^{'}=\left(K_x\right)^{1/u}\right\}_{x\in S}\Big\rangle\end{aligned}\tag{10}$$

通过将搜索令牌 TK 发送给云服务器，用户可以发起搜索询问。

验证(TK,CT)：通过发送给云服务器关键词 kw 的搜索令牌 TK 和对应于用户解密密钥的属性集 S，用户可以发起关键词搜索请求。用户既可以对原始密文进行搜索，又可以对重加密密文进行搜索。对于原始密文：

(1)收到用户发来的搜索令牌和属性集后，云服务器首先验证该属性集 S 是否满足嵌在密文 CT 中的访问结构 $(\boldsymbol{M},\rho)$。如果满足，云服务器计算

$$Q_{\mathrm{CT}}=\prod_{i\in I}\left(e\left(B_i,L'\right)\cdot e\left(C_i,K_{\rho(i)}^{'}\right)\right)^{\omega_i},\ K_{\mathrm{kw}}=\frac{e\left(A_2,T\right)}{Q_{\mathrm{CT}}}\tag{11}$$

(2)云服务器通过式(12)检验 TK 中的关键词 kw 是否与 IX 中的关键词相同：

$$F\left(t_i,K_{\mathrm{kw}}\right)=F\left(t_i,k_i\right)\tag{12}$$

(3)如果式(12)成立，云服务器将检索到的密文结果 CT 和部分解密数据 Q_{CT} 发送给用户，否则返回 $\perp$。

由于重加密密文与原始密文具有相同的形式，因此云服务器首先验证属性集 S' 是否满足嵌在重加密密文 CT′ 中的访问结构 $(\boldsymbol{M}',\rho')$。如果满足，云服务器计算 $Q_{\mathrm{CT}}^{'}=\prod_{i\in I}\left(e\left(B_i^{'},L'\right)\cdot e\left(C_i^{'},K_{\rho(i)}^{'}\right)\right)^{\omega_i'},K_{\mathrm{kw}}^{'}=\dfrac{e(A_2^{'},T)}{Q_{\mathrm{CT}}^{'}}$。

云服务器通过式(13)检验 TK 中的关键词 kw 是否与 IX′ 中的关键词相同：

$$F\left(t_i,K_{\mathrm{kw}}^{'}\right)=F\left(t_i,k_i^{'}\right)\tag{13}$$

如果式(13)成立，云服务器将检索到的密文结果 CT 和部分解密数据 Q_{CT} 发送给用户，否则返回 $\perp$。

数据解密$(\mathrm{CT},\mathrm{SK}_\sigma,S)$：给定对应于属性集 S 的解密密钥 SK_σ 和与访问结构 $(\boldsymbol{M},\rho)$ 相关的密文 CT，算法首先验证式(8)是否成立。如果不成立，输出 $\perp$，否则，计算 $Z=\dfrac{e(A_2,K)}{Q_{\mathrm{CT}}^{u_i}},m\,\|\,\beta=H_2(Z)\oplus A_1$。如果 $A_3=g_1^{H_1(m,\beta)}$，则可恢复出明文消息 m。否则输出 $\perp$。

重加密数据解密$\left(\mathrm{CT}',\mathrm{SK}_\sigma^{'},S'\right)$：输入重加密密文 CT′，对应于属性集 S' 的解密密钥 $\mathrm{SK}_\sigma^{'}$，其中 $\mathrm{SK}_\sigma^{'}$ 与对应于属性集 S 的解密密钥 SK_σ 具有形同的形式。算法按照如下执行：

首先恢复出 $\delta\,\|\,\beta'$。令 $I'=\{i:\rho'(i)\in S'\}\subseteq\{1,2,\cdots,l'\}$，当属性集 S' 满足访问结构 $(\boldsymbol{M}',\rho')$，则存在系数 $\left\{\omega_i^{'}\mid i\in I'\right\}$ 使得 $\sum_{i\in I'}\omega_i^{'}\boldsymbol{M}_i^{'}=(1,0,\cdots,0)$，那么 $\sum_{i\in I'}\omega_i^{'}\lambda_i^{'}=s'$。验证

$$e\left(A_2^{'},H_6\left(A_1^{'},A_2^{'},\left(B_i^{'},C_i^{'}\right)_{i=1}^{l'},S',(\boldsymbol{M}',\rho')\right)\right)=e(g,D')\tag{14}$$

如果式(14)不成立，输出 $\perp$，否则，计算 $Z'=\dfrac{e\left(A_2^{'},K\right)}{\left(Q_{\mathrm{CT}'}^{'}\right)^{u_i}},\ \delta\,\|\,\beta'=H_2(Z')\oplus A_1^{'}$。如果 $A_2^{'}=g^{H_1(\delta,\beta')}$ 不成立，则输出 $\perp$。否则计算 $m\,\|\,\beta=H_2\left(A_4^{\frac{1}{H_5(\delta)}}\right)\oplus A_1$。如果 $A_3=g_1^{H_1(m,\beta)}$，$D=H_4\left(A_1,A_3,(B_i,C_i)_{i=1}^{l},(\boldsymbol{M},\rho)\right)^{H_1(m,\beta)}$ 且属性集 S 满足访问结构 $(\boldsymbol{M},\rho)$ 则可恢复出 m。否则输出 $\perp$。

2.3 正确性分析

验证的正确性：

$$\begin{aligned}Q_{\mathrm{CT}} &= \prod_{i\in I}\left(e\left(B_i,L'\right)\cdot e\left(C_i,K'_{\rho(i)}\right)\right)^{\omega_i}\\ &= \prod_{i\in I}\left(e\left(g^{a\lambda_i}H_3(\rho(i))^{-r_i},g^t\right)\cdot e\left(g^{r_1},H_3(\rho(i))^t\right)\right)^{\omega_i\frac{1}{u_i}}\\ &= \prod_{i\in I}e(g,g)^{at\lambda_i\omega_i\frac{1}{u_i}} = e(g,g)^{ast/u_i}\end{aligned}$$

$$\begin{aligned}K_{\mathrm{kw}} &= \frac{e\left(A_2,T\right)}{Q_{\mathrm{CT}}} = \frac{e\left(g^s,H_3(\mathrm{kw})g^{at/u_i}\cdot g^{\alpha}\right)}{e(g,g)^{ast/u_i}}\\ &= e(g,g)^{\alpha s}e\left(g,H_3(\mathrm{kw})\right)^s\end{aligned}$$

由于对重加密密文的验证与对原始密文的验证具有相同的形式，因此可得 $Q'_{\mathrm{CT}'}=e(g,g)^{as't/u_i}$，$K'_{\mathrm{kw}}=e(g,g)^{\alpha s'}e\left(g,H_3(\mathrm{kw})\right)^{s'}$。

原始密文解密的正确性：

$$Z=\frac{e\left(A_2,K\right)}{Q_{\mathrm{CT}}^{u_i}}=\frac{e\left(g^s,g^{at}g^{\alpha}\right)}{e(g,g)^{ast}}=e(g,g)^{\alpha s}$$

因此，可以得到 $H_2(Z)\oplus A_1=H_2\left(e(g,g)^{\alpha s}\right)\oplus(m\,\|\,\beta)\oplus H_2\left(e(g,g)^{\alpha s}\right)=m\,\|\,\beta$。

重加密密文解密的正确性：

由原始密文解密的正确性可得 $Z'=e(g,g)^{\alpha s'}$，又 A_4

$$\begin{aligned}&=\frac{e\left(A_2,\mathrm{rk}_1\right)/e\left(A_3,\mathrm{rk}_2\right)}{\prod_{i\in I}\left(e\left(B_i,\mathrm{rk}_3\right)\cdot e\left(C_i,R_{\rho(i)}\right)\right)^{\omega_i}}g^s\\ &=\frac{e\left(g^s,\left(g^{\alpha}g^{at}\right)^{H_5(\delta)}\cdot g_1^{\theta}\right)/e\left(g_1^s,g^{\theta}\right)}{\prod_{i\in I}\left(e\left(g^{a\lambda_i}H_3\left(\rho(i)\right)^{-r_i},\left(g^t\right)^{H_5(\delta)}\right)\cdot e\left(g^{r_1},H_3\left(\rho(i)\right)^{tH_5(\delta)}\right)\right)^{\omega_i}}\\ &=\frac{e\left(g^s,g^{\alpha H_5(\delta)}\right)\cdot e\left(g^s,g^{atH_5(\delta)}\right)}{e\left(g,g^{atH_5(\delta)}\right)^{\sum_{i\in I}\lambda_i\omega_i}}=e(g,g)^{\alpha sH_5(\delta)}\end{aligned}$$

3 安全性分析

在云存储中，数据的安全性是众多安全问题中最为突出的，也是最基本的一条性质。众多用户选择将数据和文件存放在云中，目的就是更为便捷地存储以及最大程度地降低成本。本文方案最关心的就是数据的安全性，因此保护用户数据不被损坏是我们的主要目标，对于其它软硬件的安全性不作讨论。在云中，最具威胁的攻击就是云本身作为攻击者，在用户不知情的情况下去使用甚至篡改用户的数据。这些数据包括原始密文、重加密密文和索引等。为了确保上述信息的安全性，我们根据文献[10]和文献[15]进行如下安全分析：

3.1 数据安全性

在密文的构造中，我们采用 TCR 哈希函数来对密文组件“签名”，与此同时，构建一个“验证密钥”来检验该“签名”的有效性。下面我们对安全性进行分析：

(a)原始密文的安全性：　在数据加密算法中，可以将 D 看作是一个“签名”，将 A_3 看作是一个“验证密钥”，当属性集 S 满足访问结构 $(\boldsymbol{M},\rho)$ 时，原始密文的有效性可以通过式(15)验证

$$e\left(A_2,g_1\right)=e\left(g,A_3\right),$$
$$e\left(A_3,H_4\left(A_1,A_3,\left(B_i,C_i\right)_{i=1}^{l},(\boldsymbol{M},\rho)\right)\right)=e\left(g_1,D\right)\quad(15)$$

由于 $A_1,A_3,\left(B_i,C_i\right)_{i=1}^{l}$ 和 $(\boldsymbol{M},\rho)$ 由 D 进行签名，所以它们的有效性可以得到保证，而 A_2 的有效性由验证密钥 A_3 保证。如果密文被篡改，则上述式(15)不成立，这种篡改是显而易见的。

(b)重加密密文的安全性：　在数据重加密算法中，首先应该通过式(16)来检验原始密文是否有效。此外，为了验证重加密算法的输入组件 $\left(B_i,C_i\right)_{i=1}^{l}$ 具有良好的形式，还需要检验

$$e\left(\prod_{i\in I}B_i^{\omega_i},g^a\right)=e\left(A_2,g\right)\cdot\prod_{i\in I}e\left(C_i^{-1},H_3\left(\rho(i)\right)^{\omega_i}\right)\quad(16)$$

是否有效。

如果上述检验均成立，则可以满足重加密条件。合法的用户可以检验重加密密文是否有效，因为 $(\boldsymbol{M},\rho)$ 和 $A_1,A_3,\left(B_i,C_i\right)_{i=1}^{l}$ 由 D 进行签名，rk_4 由 S 进行签名。另外，A_4 与原始密文中的 A_1 和 A_3 紧密联系，因为由 $A_3=g_1^{H_1(m,\beta)}$ 可以辨别出 A_4 是否被改变。而对于不合法的用户，他不能检验出重加密密文是否有效。

(c)关键词安全性：　在索引生成算法中，$k_i=e(g,g)^{\alpha s}e\left(g,H_3\left(\mathrm{kw}_i\right)\right)^s$ 是对关键词进行加密后的结果。若要从 k_i 的值推导出关键词 kw_i 是不可能的。即使知道 $e(g,g)^{\alpha}$ 的值，但秘密值 s 无法恢复，因此得不到 $H_3\left(\mathrm{kw}_i\right)$，从而也就得不到 kw_i 的信息。同理，对重加密密文的分析也是如此。

综上所述，即使数据拥有者将 CT , CT′ 和 IX , IX′ 上传到云服务器中，云也不会从这些数据中得到一些想要的信息，如明文消息和关键词信息等。因此，该方案可以满足数据安全性的要求。

3.2 关键词隐藏

用户要进行搜索时，需将搜索令牌发送给云，而搜索令牌中的关键词组件是

$$\begin{aligned}T&=H_3(\mathrm{kw})q^{1/u}=H_3(\mathrm{kw})\left(g^t\cdot\left(g^{\alpha}\right)^u\right)^{1/u}\\ &=g^{t/u}\cdot g^{\alpha}H_3(\mathrm{kw})\end{aligned}\quad(17)$$

这种构造方式相对于 Wang 等人[15]提出的方案来说，由于对每个不同的关键词 kw，对应的 u 都不同，所以更安全。而 Li 等人[16]已经证明这种构造不会泄露关键词的信息。因此，该方案实现了关键词隐藏性质。

3.3 抗共谋攻击性

在重加密密钥的生成过程中，S 和 $(\boldsymbol{M}',\rho')$ 由 D' 进行签名，该签名可以通过 A_2' 来验证。rk_1，rk_3 和 R_x 通过 δ 与 rk_4 紧密联系，rk_1 通过 θ 与 rk_2 紧密联系，而 rk_4 是在访问策略 $(\boldsymbol{M}',\rho')$ 下对 δ 的加密，因此如果 $\mathrm{rk}_1,\mathrm{rk}_2,\mathrm{rk}_3$ 和 R_x 的值被敌手篡改，那么对应的重加密密文也就是无效的。如果 S，$(\boldsymbol{M}',\rho')$ 和 rk_4 被篡改，那么可以通过公式

$$e\left(A_2',H_6\left(A_1',A_2',\left(B_i',C_i'\right)_{i=1}^{l'},S,(\boldsymbol{M}',\rho')\right)\right)=e(g,D')$$

辨别出。

由于 rk_1 的特殊构造，在不知道 θ 的前提下，敌手无法窃取代理者的整个私钥，即使是与委托者合谋也不会。

4 功能分析

本节对CP-ABPRKS方案的功能特征与文献[10, 13, 14, 17, 18]作比较分析，见表1。表1表明，相比这5个方案，本文提出的方案具有一些优势。首先，文献[17]提出的方案既不支持代理重加密又不能解密密文，这在云计算的数据转发机制中并不适用；而文献[10]的方案不支持可搜索加密，这就阻碍了用户对数据的分享和检索功能；文献[18]的方案是基于公钥加密方案的可搜索的代理重加密方案，但是并不能对数据进行细粒度访问控制；尽管文献[13]的方案是基于属性的代理重加密可搜索，但是可搜索功能还是基于公钥加密机制完成的，并不是纯粹的属性方案。而本文方案可以同时实现表中的这几个功能，因此更适用于云计算和实际应用。

表 1 CP-ABPRKS 方案的功能特征比较

方案	关键词搜索	属性加密	代理重加密	可解密密文
文献[10]	×	√	√	√
文献[13]	√	√	√	×
文献[14]	√	√	√	√
文献[17]	√	√	×	×
文献[18]	√	×	√	√
本文方案	√	√	√	√

5 效率分析

本节将对本文方案与现有的既支持可搜索又支持代理重加密的属性基加密方案进行效率比较。为方便起见，用 E,P 分别代表指数运算和对运算，$|\mathcal{U}|$ 表示属性全集的大小，$|S|$ 表示用户属性集的大小，l 表示包含在访问策略 $(\boldsymbol{M},\rho)$ 中的属性的个数，$|I|$ 表示 $\{1,2,\cdots,l\}$ 的子集大小，$|\Delta|$ 表示集合 $\Delta=\{x:\exists i\in I,\rho(i)=x\}$ 中的元素个数。

从表 2 中可以看出，在原始密文解密和重加密密文解密阶段，本文方案的计算量明显少于文献[14]的方案。这是由于在验证阶段，云服务器在匹配关键词的同时可以对原始密文和重加密密文进行部分解密，从而大大减轻了用户端的计算量。在搜索验证阶段，本文方案的效率高于文献[13]的方案和文献[14]的方案。在数据加密阶段，本文方案的计算量略高于文献[14]。此外，本文方案在数据重加密阶段的计算量远高于文献[13]的方案，但比文献[14]的计算量低。这是因为本文方案采用属性基加密实现对明文消息和原始密文的加密，因此这两个阶段的计算量随属性呈线性增长；而文献[13]采用公钥加密体制与属性加密体制相结合的方式，尽管减少了计算量，但其实用性却有所降低。

表 2 CP-ABPRKS 方案的效率比较

算法	数据加密	令牌生成	数据重加密	验证数据	解密	重加密数据解密
文献[10]	$(2l+4)E$	–	$(10+4\|I\|)P$	–	$(2\|I\|+1)P$	$(2\|I\|+4)P$
文献[13]	$P+2E$	$(\|S\|+\|\mathcal{U}\|+1)\cdot P+E$	$(\|S\|+\|\mathcal{U}\|+3)E$	$(\|S\|^2+\|\mathcal{U}\|+4)P$	–	–
文献[14]	$(\|S\|+5)E$	l^2E	$(2\|\Delta\|\|I\|+\|I\|+2\|S\|+2)P$	$4\|\Delta\|\|I\|P$	$2\|\Delta\|\|I\|P+(2\|S\|+2)E$	$2\|\Delta\|\|I\|P+(2\|S\|+4)E$
文献[17]	$(2l+4)E$	$(2\|\mathrm{S}\|+4)E$	–	–	–	–
文献[18]	$P+5E$	E	$4P$	–	$2P$	–
本文方案	$(3l+4)E$	$(\|S\|+2)E$	$(4\|I\|+8)P$	$(2\|I\|+1)P$	$P+2E$	$3(P+E)$

6　结束语

本文提出了支持可搜索的密文策略的属性代理重加密方案。方案采用 LSSS 技术来实现数据的访问控制，因此支持任意单调的访问结构。通过将密钥分为属性密钥和搜索密钥从而实现关键词可搜索和属性代理重加密功能。搜索过程中云服务器在验证的同时可以对原始密文和重加密密文进行部分解密来减轻计算负担。功能分析和效率分析表明，本文方案更适用于实际。

参 考 文 献

[1] YANG Chaowei, HUANG Qunying, LI Zhenlong, *et al*. Big data and cloud computing: Innovation opportunities and challenges[J]. *International Journal of Digital Earth*, 2017, 10(1): 13–53. doi: 10.1080/17538947.2016.1239771.

[2] 黄海平, 杜建澎, 戴华, 等. 一种基于云存储的多服务器多关键词可搜索加密方案[J]. 电子与信息学报, 2017, 39(2): 389–396. doi: 10.11999/JEIT160338.
HUANG Haiping, DU Jianpeng, DAI Hua, *et al*. Multi-sever multi-keyword searchable encryption scheme based on cloud storage. *Journal of Electronics & Information Technology*, 2017, 39(2): 389–396. doi: 10.11999/JEIT160338.

[3] 王光波, 王建华. 基于属性加密的云存储方案研究[J]. 电子与信息学报, 2016, 38(11): 2931–2939. doi: 10.11999/JEIT160064.
WANG Guangbo and WANG Jianhua. Research on cloud storage scheme with attribute-based encryption[J]. *Journal of Electronics & Information Technology*, 2016, 38(11): 2931–2939. doi: 10.11999/JEIT160064.

[4] ATTRAPADUNG N, HANAOKA G, MATSUMOTO T, *et al*. Attribute based encryption with direct efficiency tradeoff[C]. Proceedings of the 14th International Conference on Applied Cryptography and Network Security, London, United Kindom, 2016: 249–266. doi: 10.1007/978-3-319-39555-5_14.

[5] SAHAI A and WATERS B. Fuzzy identity-based encryption[C]. Proceedings of the 24th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Aarhus, Denmark, 2005: 457–473. doi: 10.1007/11426639_27.

[6] GOYAL V, PANDEY O, SAHAI A, *et al*. Attribute-based encryption for fine-grained access control of encrypted data[C]. Proceedings of the 13th ACM Conference on Computer and Communications Security, Alexandria, Virginia, USA, 2006: 89–98. doi: 10.1145/1180405.1180418.

[7] WATERS B. Ciphertext-policy attribute-based encryption: An expressive, efficient, and provably secure realization[C]. Proceedings of 14th International Conference on Practice and Theory in Public Key Cryptography, Taormina, Italy, 2011: 53–70. doi: 10.1007/978-3-642-19379-8_4.

[8] GUO Shanqing, ZENG Yingpei, WEI Juan, *et al*. Attribute-based re-encryption scheme in the standard model[J]. *Wuhan University Journal of Natural Sciences*, 2008, 13(5): 621–625. doi: 10.1007/s11859-008-0522-5.

[9] LIANG Xiaohui, CAO Zhenfu, LIN Huang, *et al*. Attribute based proxy re-encryption with delegating capabilities[C]. Proceedings of the 4th International Symposium on Information, Computer, and Communications Security, Sydney, Australia, 2009: 276–286. doi: 10.1145/1533057.1533094.

[10] LIANG Kaitai, FANG Liming, SUSILO W, *et al*. A ciphertext-policy attribute-based proxy re-encryption with chosen-ciphertext security[C]. Proceedings of the 5th Intelligent Networking and Collaborative Systems (INCoS), Xi'an, China, 2013: 552–559. doi: 10.1109/INCoS.2013.103.

[11] GE Chunpeng, SUSILO W, WANG Jiandong, *et al*. A key-policy aattribute-based proxy re-encryption without random oracles[J]. *The Computer Journal*, 2016, 59(7): 970–982. doi: 10.1093/comjnl/bxv100.

[12] ZHANG Yinghui, LI Jin, CHEN Xiaofeng, *et al*. Anonymous attribute-based proxy re-encryption for access control in cloud computing[J]. *Security and Communication Networks*, 2016, 9(14): 2397–2411. doi: 10.1002/sec.1509.

[13] SHI Yanfeng, LIU Jiqiang, HAN Zhen, *et al*. Attribute-based proxy re-rncryption with keyword search[J]. *PloS One*, 2014, 9(12): e116325(1–24). doi: 10.1371/journal.pone.0116325.

[14] LIANG Kaitai and SUSILO W. Searchable attribute-based mechanism with efficient data sharing for secure cloud storage[J]. *IEEE Transactions on Information Forensics and Security*, 2015, 10(9): 1981–1992. doi: 10.1109/TIFS.2015.2442215.

[15] WANG Changji, LI Wentao, LI Yuan, *et al*. A ciphertext-policy attribute-based encryption scheme supporting keyword search function[C]. Proceedings of the 5th International Symposium on Cyberspace Safety and Security (CSS), Hunan, China, 2013: 377–386. doi: 10.1007/978-3-319-03584-0_28.

[16] LI Jiazhi and ZHANG Lei. Attribute-based keyword search and data access control in cloud[C]. Proceedings of the 10th International Conference on Computational Intelligence and Security, Kunming, China, 2014: 382–386. doi: 10.1109/CIS.2014.113.

[17] ZHENG Qingji, XU Shouhuai, and ATENIESE G. VABKS: Verifiable attribute-based keyword search over outsourced encrypted data[C]. Proceedings of the IEEE Conference on Computer Communications, Toronto, Canada, 2014: 522–530. doi: 10.1109/INFOCOM.2014.6847976.

[18] SHAO Jun, CAO Zhenfu, LIANG Xiaohui, *et al*. Proxy re-encryption with keyword search[J]. *Information Sciences*, 2010, 180(13): 2576–2587. doi: 10.1016/j.ins.2010.03.026.

刘振华：　男，1978 年生，教授，研究方向为云计算中的密码理论与安全协议、密文数据的再处理研究等.

周佩琳：　女，1991 年生，硕士，研究方向为云计算中的密码理论与安全协议、密文数据的再处理研究等.

段淑红：　女，1989 年生，硕士，研究方向为云计算中的密码理论与安全协议、密文数据的再处理研究等.