具有隐私保护的完整性可验证的关键字搜索方案

刘雪艳* 芦婷婷 杨晓涛

(西北师范大学数学与统计学院 兰州 730070)

摘 要：针对传统基于属性关键字搜索(ABKS)方案存在访问结构泄密、用户侧计算量高及缺乏完整性验证问题，该文提出具有隐私保护和完整性可验证的基于属性的关键字搜索方案。该方案提出了有序多值属性访问结构和有序多值属性集，固定每个属性的位置，减少参数及相关计算，提高了方案的效率，而在密钥生成时计算具体属性取值的哈希值，从而达到区别多值属性取值的不同。同时，采用Hash和对运算实现对访问结构的隐藏，防止访问结构泄密；采用倒序索引结构和Merkle树建立数据认证树，可验证云服务器返回文档和外包解密结果的正确性。此外，支持外包解密以降低用户侧的计算量。安全分析和实验表明所提方案实现云中共享数据的可验证性、关键字不可区分性和关键字不可链接性，且是高效的。

关键词：基于属性关键字搜索；有序多值属性集；隐藏访问结构；数据完整性认证；外包解密

中图分类号：TN918 **文献标识码**：A **文章编号**：1009-5896(2021)01-0218-08

DOI: 10.11999/JEIT190817

Verifiable Attribute-based Keyword Search Scheme with Privacy Preservation

LIU Xueyan LU Tingting YANG Xiaotao

(*School of Mathematics and Statistics, Northwest Normal University, Lanzhou* 730070, *China*)

Abstract: To address the problems of the leakage of access structure, high computation of user side and lack of integrity verification in current Attribute-Based Keyword Search (ABKS) scheme, a verifiable attribute-based keyword search scheme with privacy preservation is proposed. The scheme adopts the ordered multi-valued attribute access structure and ordered multi-valued attribute set, and fixes the position of each attribute to reduce the parameters and related computation cost and to improve the efficiency of the scheme, while in key generation, the Hash values of specific attributes are calculated to distinguish the different values of multi-valued attributes. At the same time, Hash and pair operation are used to hide the access structure and prevent the disclosure of the access structure. The inverted index structure and Merkle tree are used to establish the data authentication tree, which can verify the correctness of the document returned by the cloud server provider and the result of outsourced decryption. In addition, outsourced decryption is used to reduce the computation cost on the user side. Finally, formal proofs and experimental results show that the scheme achieve verifiability of shared data in the cloud, keyword undistinguishable and keyword unlinkable, and is efficient.

Key words: Attribute-Based Keyword Search (ABKS); Ordered multi-valued attribute set; Hidden access policy; Data integrity verification; Outsourced decryption

1 引言

随着大数据和云计算时代的到来，越来越多的个人和企业将大量私有数据上传到云中，从而节省本地存储和管理成本。为了保证数据的机密性和隐私性，数据属主需要将数据加密后再上传到云中，传统的明文搜索不适用于当前需求。2000年，Song等人[1]提出了可搜索加密(Searchable Encryption, SE)的概念，实现了不解密密文情况下对密文的快速检索。2004 年，Boneh等人[2]首次提出了公钥可搜索加密的概念，随后，具有连接关键词[3,4]、模糊关键词[5]、动态关键字[6,7]、子集关键字[8]等功能的公钥可搜索加密方案也相继被提出。但是在实际应用中，数据拥有者往往无法预先确定所有访问者的信息，但是又希望能控制共享数据的访问权限，并且实现

收稿日期：2019-10-22；改回日期：2020-06-12；网络出版：2020-07-20
*通信作者： 刘雪艳 liuxy@nwnu.edu.cn
基金项目：国家自然科学基金(61662071, 61562077)
Foundation Items: The National Natural Science Foundation of China (61662071, 61562077)

一对多的通信模式，显然传统的公钥可搜索加密和基于身份的可搜索加密技术已经不能解决这一难题，而基于属性关键字搜索(Attribute-Based Keyword Search, ABKS)的加密机制引起众多学者的关注。

基于属性关键词搜索加密机制是一对多的公钥加密搜索方式：数据属主可以使用自己定义的访问结构加密关键字和共享信息，属性集满足访问结构的用户才能获得搜索授权和解密操作。文献[9]在属性加密方案[10]的基础上提出基于属性的密文检索方案，该方案实现了快速关键字搜索，但没有对搜索结果进行验证。Ameri等人[11]在密钥策略属性加密方案[12]的基础上提出一个密钥策略的可搜索加密方案，该方案在搜索令牌中加入时间戳，只能提取在指定时间间隔内生成的密文。Miao 等人[13,14]提出了一种可验证的关键字搜索方案，通过对每个密文文档设置签名，由第三方审计检验返回密文的正确性，但是该方案密文大小与属性的个数成正比，导致搜索时间随属性的增加而增加。Ballard等人[15]提出动态的关键字搜索方案，采用Merkle 树实现数据的完整性认证，但是，该认证方法不支持多关键字搜索。为解决上述问题，文献[7]提出完整性验证的多关键字搜索方案，减少了计算量。文献[16]提出支持属性撤销的关键字搜索方案，该方案将繁重的代理重加密工作交给授权中心，造成授权中心的瓶颈。随后一些支持代理重加密等特点的关键字搜索方案相继被提出[17,18]，但是由于将访问结构和索引一起发送给云服务器，导致访问结构信息泄露问题。文献[19]提出了隐藏访问结构的ABKS方案，并支持属性撤销，但该方案只适合单个关键字的搜索。还出现了一些具有其它特色的搜索方案[20,21]，但这些方案都没有考虑关键字搜索。

本文将关键字搜索技术与ABE技术结合，提出具有隐私保护的完整性可验证的关键字搜索方案，实现了细粒度的搜索授权，主要工作有：(1)方案采用了一个有序多值属性访问结构和有序多值属性集，固定每个属性的位置，减少参数及相关计算，提高了方案的效率；(2)方案采用倒序索引结构和Merkle哈希树生成数据认证树，实现对云服务器返回密文的完整性认证，防止云服务器对数据的恶意篡改和返回不正确的结果；(3)为了防止访问结构泄露和保护用户身份隐私性，采用hash及对运算实现对访问结构的隐藏；(4)外包解密技术减少了用户侧的计算开销。

2　准备工作

2.1　判定性DL(Decisional Linear)假设

给定阶为素数p的循环群G_1，挑战者从群G_1上选择g,h,f，随机选择$a,b\in Z_p^*$，敌手在获得$Y=\{g,f,h,h^a,f^b\}$以及随机值$Z\in G_1$后，必须将$g^{a+b}\in G_1$和Z区分出来，定义输出$b\in\{0,1\}$的算法解决判定性DL假设的优势为ε。若$\Pr\left|\mathrm{adv}(g,f,h,h^a,f^b)=g^{a+b}\right|\geq\varepsilon$，则说明敌手只能以$\varepsilon$的优势解决DL假设。

2.2　有序多值属性访问结构

令$U=\{\mathrm{attr}_1,\mathrm{attr}_2,\cdots,\mathrm{attr}_n\}$表示一个有序属性集，$U$中每个属性的位置是唯一确定的，有序位置：$J=\{1,2,\cdots,n\}$，$n$为属性的个数，$V_i=\{v_{i,1},v_{i,2},\cdots,v_{i,ni}\}$表示属性$\mathrm{attr}_i$所有可能值的集合，其中$n_i$是属性$\mathrm{attr}_i$所有可能值的个数，且$V_i$中每个可能值$v_{i,j}\bmod n$等于$\mathrm{attr}_i$的位置，属性$\mathrm{attr}_i$的取值如表1所示。

用户属性集S的属性列表为$L=\{x_{1j_u},x_{2j_u},\cdots,x_{nj_u}\}$，$x_{ij_u}\in V_i$。访问结构$\mathbb{A}=\{v_{1j_o},v_{2j_o},\cdots,v_{nj_o}\}$，$v_{ij_o}\in V_i$，当且仅当$x_{ij_u}=v_{ij_o}$，$i=1,2,\cdots,n$，称用户的属性集$S$满足访问策略$\mathbb{A}$，即$H_1(x_{ij_u})=H_1(v_{ij_o})$成立。

2.3　Merkle 哈希树

Merkle哈希树(见图1)是一类基于哈希值的二叉树或多叉树，其叶子节点上的值通常为数据或文档等的哈希值，从节结点开始，进行递归运算，父节点的值等于所有孩子节点组合的哈希值。Merkle树可以验证数据的完整性。图1为一个Merkle哈希树，数据存储在叶子节点。对非叶子节点：节点A的值等于节点B, C组合的哈希值，即：$A=\mathrm{Hash}(C\|D)$，节点B的值等于节点E, F组合的哈希值，即：$B=\mathrm{Hash}(E\|F)$。同理：$C=\mathrm{Hash}(d_0\|d_1)$, $D=\mathrm{Hash}(d_2)$, $E=\mathrm{Hash}(d_3\|d_4)$, $F=\mathrm{Hash}(d_5\|d_6)$, $\mathrm{Root}=\mathrm{Hash}(A\|B)$。叶子节点$d_i(i\in[1,6])$分别存储数据块，而非叶子节点$A$存储其子节点$C$, D组合的哈希值。

2.4　倒序索引结构与数据认证树

倒序索引结构(见图2)由关键字w_j和包含w_j的所有相关文档$f_{j1},f_{j2},\cdots,f_{jm_j}$组成，其中$m_j$是包含关键字$w_j$的文档个数。

数据认证树的建立采用倒序索引结构和二叉Merkle哈希树(见图3)，Hash加密算法采用SHA-256。用对称钥加密包含关键字w的所有相关文档

表 1　属性值

attr_1	attr_2	…	attr_n
V_1	V_2	…	V_n
1	2	…	n
$n+1$	$n+2$	…	$2n$
$2n+1$	$2n+2$	…	$3n$
…	…	…	…

集$\{f_1, f_2, \cdots, f_m\}$，生成包含关键字$w$的密文文档集$L_w$，对密文文档集$L_w$生成认证哈希树$\mathrm{MT}_w$，其中每个叶子节点存储一个密文文档，$\delta_w$是树$\mathrm{MT}_w$的根节点。

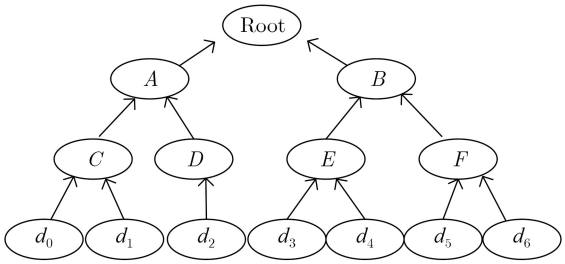

图 1 Merkel树

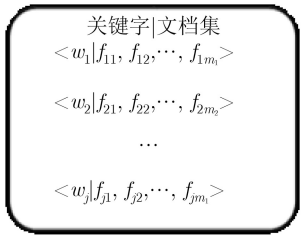

图 2 倒序索引列表

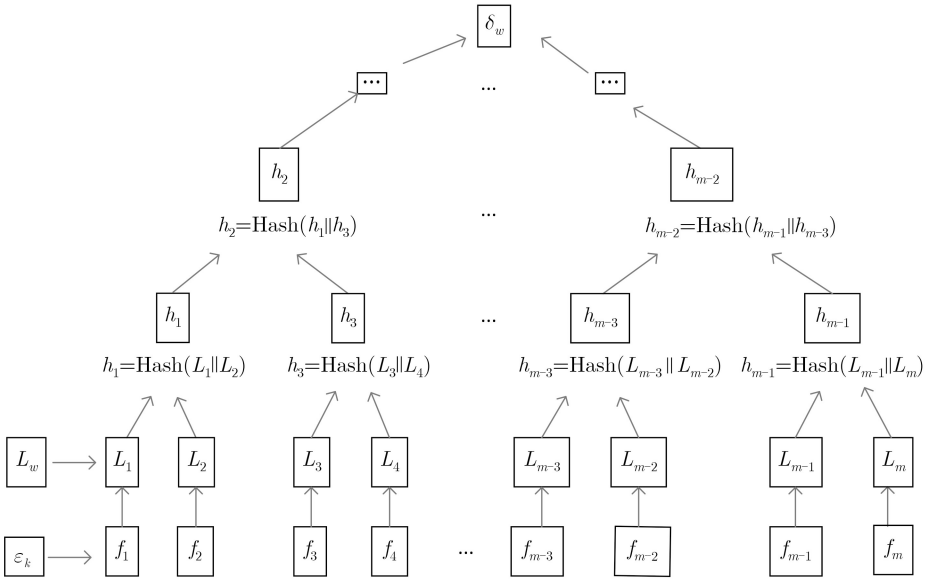

图 3 数据认证

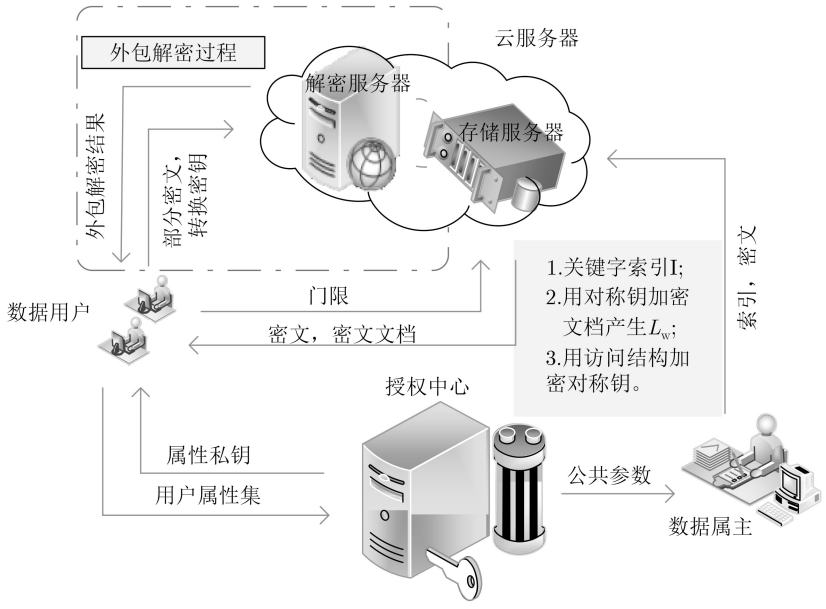

图 4 系统模型

3 可实现隐私保护的关键字搜索方案

3.1 系统模型

本文方案主要有4个实体(如图4)：数据属主(DO)，数据用户(DU)，授权中心(TA)，云服务器(CSP)。TA是可信的，为系统产生公钥和主密

钥，并为用户产生私钥，用户的私钥与自身属性相关。DO决定访问策略并加密对称钥，建立关键字索引，为每个关键字建立密文认证树，将索引、认证树、密文文档发送给云服务器。CSP是诚实又好奇的，它会诚实地遵守协议但又试图解密文档，CSP分为存储服务器和解密服务器。存储服务器存储和管理数据属主上传的关键字索引、加密文档，并通过判断用户上传的门限值提供相应的检索服务。DU收到密文，将其外包给解密服务器进行部分解密，并检验返回密文与外包解密的正确性。

3.2 方案描述

方案由以下8个算法组成：

Setup：给定系统有序属性集$U=\{\text{attr}_1,\text{attr}_2,\cdots,\text{attr}_n\}$及位置$J=\{1,2,\cdots,n\}$，$V_i=\{v_{i,1},v_{i,2},\cdots,v_{i,ni}\}$是属性$\text{attr}_i$可能值的集合。两个阶为素数$p$的循环群$G_1$和$G_2$，$g,g_1\in G_1$，随机选择$a\in F_q$，对每个位置的属性$\text{attr}_i(i\in[1,n])$，设置$\beta_i=a^{-i}$，$\alpha_i=g^{a^i}$，双线性映射:$e:G_1\times G_1\to G_2$，抗碰撞的Hash函数$H_1:\{0,1\}^*\to G_1$，$H_2:\{0,1\}^*\to Z_P^*$，$H_3:\{0,1\}^*\to\{0,1\}^{256}$，主密钥$\text{Msk}=\{a,\{\beta_i\}(i\in[1,n])\}$，系统公共参数为$\text{Pk}=\{G_1,G_2,g,g_1,e,H_1,H_2,H_3,\{g^{\beta_i},\alpha_i\},(i\in[1,n])\}$。

KeyGen：对于用户的有序属性集S，授权中心随机选择$s_1\in Z_p^*$，计算用户属性私钥：$\text{sk}'_1=g^{s_1}$，$\text{sk}'_2=g_1{}^{s_1}$，$\text{sk}'_3=\left(\prod_{i=1}^{n}H_1(x_{ij_u})\right)^{s_1}$，$\text{sk}'_i=\{H_1(x_{ij_u})^{\beta_i}\}_{i\in[1,n]}$，$\text{sk}=\{\text{sk}'_1,\text{sk}'_2,\text{sk}'_3,\{\text{sk}_i\}_{i\in[1,n]}\}$。

Encryption：给定关键字w及包含关键字w的文档集合$F=\{f_1,f_2,\cdots,f_m\}$，对称钥$\varepsilon\text{k}\in G_2$，访问结构$\mathbb{A}=\{v_{1j_o},v_{2j_o},\cdots,v_{nj_o}\}$。DO随机选择$r\in Z_p^*$，计算：$I_0=g_1{}^r$，$I_w=\left(g^{H_2(w)}\cdot\prod_{=1}^{n}H_1(v_{ij_o})\right)^r$，关键字索引$I=\{I_0,I_w\}$。使用对称钥$\varepsilon\text{k}$加密文档$F$，生成密文文档集$L_w$，即$\text{Enc}_{\varepsilon\text{k}}(F)\to L_w$。然后生成$L_w$的认证树$\text{MT}_w$，其中$L_w$是认证树$\text{MT}_w$的叶子节点的集合，$\delta_w$是树$\text{MT}_w$的根节点。用$\varepsilon\text{k}$加密根节点$\delta_w$与对应的关键字$w$，即：$\text{Enc}_{\varepsilon\text{k}}(\delta_w,w)\to\tilde{\delta}_w$。对每个属性值$v_{ij_o}\in\mathbb{A}$，随机选择$r_i\in Z_p^*$，计算：$\tilde{C}_0=\varepsilon\text{k}\cdot e\left(\prod_{i=1}^{n}H_1(v_{ij_o})^{r_i},g\right)$，$\tilde{C}=g_1{}^{H_2(\varepsilon\text{k})}$，$\{\tilde{C}_i=\alpha_i{}^{r_i}\}_{i\in[1,n]}$，则密文$\text{CT}=\{\tilde{C}_0,\tilde{C},\{\tilde{C}_i\}_{i\in[1,n]}\}$。接下来，DO通过计算$\{h_i=e(g^{\beta_i},H_1(v_{ij_o}))\}$来替代访问结构中每个属性值$v_{ij_o}\in\mathbb{A}(i=\{1,2,\cdots,n\})$，实现访问结构的隐藏(见图5)，则访问结构转化为$\bar{\mathbb{A}}$。最终，DO将密文$\text{CF}=\{\text{CT},\text{MT}_w,\tilde{\delta}_w\}$、索引$I$和访问结构$\bar{\mathbb{A}}$发送给云服务器。

TrapGen：若待查关键字为w'，属性集S，DU计算：$\{h_i{}'=e(g,H_1(x_{ij_u})^{\beta_i})\}_{i\in[1,n]}$，则$h_i{}'$替代属性集$S$中属性的取值$x_{ij_u}$，属性集转换为$\bar{S}$(如图6)，算法产生一个随机值$s_2\in Z_p^*$，计算：$\text{tok}_1=\text{sk}'_1{}^{s_2H_2(w')}$，$\text{tok}_2=\text{sk}'_2{}^{s_2}$，$\text{tok}_3=\text{sk}'_3{}^{s_2}$，将$\text{Trap}=\{\text{tok}_1,\text{tok}_2,\text{tok}_3,\bar{S}\}$发送给云服务器进行关键字检索。

Search：CSP收到Trap后，首先判断$\bar{S}$是否满足访问结构$\bar{\mathbb{A}}$，若满足访问结构，则用户达到授权搜索，并进行下一步。计算公式CF是否成立。若成立，则说明门限中的关键字等于索引中的关键字，即：$w=w'$，则CSP将包含关键字w'的密文文档CF发送给用户。

Transform：用户随机选择$z\in Z_p^*$，计算转换钥$\text{tfk}=\{H_1(x_{ij_u})^{\beta_i})^{\frac{1}{z}}\}_{i\in[1,n]}$，将$\{\text{tfk},\{\tilde{C}_i\}_{i\in[1,n]}\}$发送给解密服务器。

$\text{Decryption}_{\text{out}}$：解密服务器收到$\{\text{tfk},(\tilde{C}_i)_{i\in[1,n]}\}$，计算$V=\prod_{i=1}^{n}e((H_1(x_{ij_u})^{\beta_i})^{\frac{1}{z}},\tilde{C}_i)$，将$V$发送给用户。

Decryption：用户收到V后，进行以下3步：

(1) 计算$\varepsilon\text{k}=\tilde{C}_0/V^z$，$\sigma=H_2(\varepsilon\text{k})$，若$g_1{}^{\sigma}=g_1{}^{H_2(\varepsilon\text{k})}=\tilde{C}$，则对称钥$\varepsilon\text{k}$正确，进行第(2)步，否则终止。

(2) 首先用εk解密$\tilde{\delta}_w$得到δ_w，即$\text{Dec}_{\varepsilon\text{k}}(\bar{\delta}_w,w')=\delta_w$，接着，从密文CF中的$\text{MT}_w$，获得$L_w$，计算出认证树的根节点$\delta_w{}'$，若$\delta_w=\delta'_w$，则对密文完整性和搜索结果正确，进行第(3)步，否则终止。

(3) 用εk解密密文文档L_w获得明文文档F，即：$\text{Dec}_{\varepsilon\text{k}}(L_w)=F$。

多关键字搜索的完整性验证：在实际应用中，用户可能会进行多个关键字$W=\{w_1,w_2,\cdots,w_t\}$查询，为此，在单关键字的基础上，计算$\text{tok}_1=g^{s_2\sum_{w_j\in W}H_2(w_j)}$，用户可满足多关键字授权搜索，但是上述的Merkle哈希树认证方法用于多关键字搜

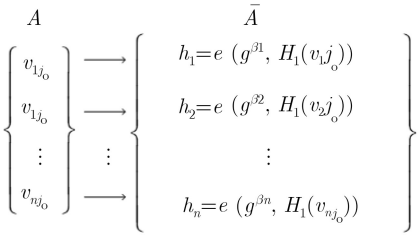

图 5 访问结构的隐藏

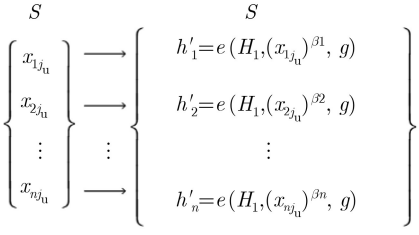

图 6 用户属性集的转化

索时通信与计算开销较大，为解决这个问题，对每个关键字w_j建立查找表，查找表的每个位置存放关键字w_j有关的文档标记符id_k，再采用文献[7]用到的技术：Merkle哈希树中引入双线性映射累加器和集合操作认证技术，将方案复杂的认证过程转化为证明包含关键字w_j的文档集合L_{w_j}的交集D的完整性，从而实现多关键字查询的完整性验证。

4 正确性分析与安全性证明

4.1 正确性分析

若用户属性集满足访问结构当且仅当$x_{ij_u}=v_{ij_o}$，$i=1,2,\cdots,n$时，有$H_1(x_{ij_u})=H_1(v_{ij_o})$，$i=1,2,\cdots,n$，则：

(1) 授权用户的搜索过程是正确的，具体为

$$e(I_w,\mathrm{tok}_2)=e\left(\left(g^{H_2(w)}\cdot\prod_{i=1}^{n}H_1(v_{ij_o})\right)^{r},{g_1}^{s_1s_2}\right)=e(g,g_1)^{rs_1s_2H_2(w)}\cdot e\left(\prod_{i=1}^{n}H_1(v_{ij_o}),g_1\right)^{rs_1s_2} \tag{1}$$

$$e(I_0,\mathrm{tok}_1\cdot\mathrm{tok}_3)=e\left({g_1}^{r},g^{s_1s_2H_2(w')}\cdot\prod_{i=1}^{n}H_1(x_{ij_u})^{s_1s_2}\right)=e(g,g_1)^{rs_1s_2H_2(w')}\cdot e\left(\prod_{i=1}^{n}H_1(x_{ij_u}),g_1\right)^{rs_1s_2} \tag{2}$$

(2) 解密过程是正确的，具体为

$$V=\prod_{i=1}^{n}e((H_1(x_{ij_u})^{\beta_i})^{\frac{1}{z}},\tilde{C}_i)=\prod_{i=1}^{n}e(H_1(x_{ij_u})^{\beta_i},{\alpha_i}^{r_i})^{\frac{1}{z}}=\prod_{i=1}^{n}e(H_1(x_{ij_u})^{a^{-i}},g^{a^ir_i})^{\frac{1}{z}}=e\left(\prod_{i=1}^{n}H_1(x_{ij_u})^{r_i},g\right)^{\frac{1}{z}} \tag{3}$$

$$C_0\cdot(V^z)^{-1}=\varepsilon\mathrm{k}\cdot e\left(\prod_{i=1}^{n}H_1(v_{ij_o})^{r_i},g\right)\cdot\left(e\left(\prod_{i=1}^{n}H_1(v_{ij_o})^{r_i},g\right)^{\frac{z}{z}}\right)^{-1}=\varepsilon\mathrm{k} \tag{4}$$

4.2 安全性证明

定理1 如果DL问题在群G_1上是难解的，则本方案是可认证的。

证明 假设存在敌手$\mathcal{A}$以不可忽略的优势攻击方案的有效性，那么存在敌手$\mathcal{B}$以不可忽略的优势解决DL问题.

系统建立：$\mathcal{B}$随机选择$a\in F_q$，对每个位置的属性$x_i(i\in[1,n])$，设置$\beta_i=a^{-i}$，$\alpha_i=g^{a^i}$，抗碰撞的Hash函数$H_1:\{0,1\}^*\to G_1$，$H_2:\{0,1\}^*\to Z_p^*$，$H_3:\{0,1\}^*\to\{0,1\}^{256}$，主密钥$\mathrm{Msk}=\{a,\beta_i\}$，系统公共参数为$\mathrm{PK}=\{G_1,G_2,g,g_1,e,H_1,H_2,H_3,\{g^{\beta_i},\alpha_i\}_{i\in[1,n]}\}$, TA将PK发送给$\mathcal{A}$。

第1阶段询问：$\mathcal{A}$适应性地发起转换钥、私钥和外包解密询问，$\mathcal{B}$能正确的回复询问。

挑战阶段：$\mathcal{A}$选择两个长度相同的消息$\varepsilon\mathrm{k}_0$, $\varepsilon\mathrm{k}_1$发送给$\mathcal{B}$, $\mathcal{B}$选择一个比特$\gamma\in\{0,1\}$，用公钥PK和访问策略$\mathbb{A}^*$加密$\varepsilon\mathrm{k}_\gamma$, $\mathcal{B}$随机选择$r_i\in Z_p^*$，计算$\tilde{C}_0=\varepsilon\mathrm{k}_\gamma\cdot e\left(\prod_{i=1}^{n}H_1(v_{ij_o})^{r_i},g\right)$，$\tilde{C}={g_1}^{H_2(\varepsilon\mathrm{k}_\gamma)}$，$\{\tilde{C}_i={\alpha_i}^{r_i}\}_{i\in[1,n]}$，并将密文$\mathrm{CT}^*=\{\mathbb{A}^*,\tilde{C}_0,\tilde{C},\{\tilde{C}_i\}_{i\in[1,n]}\}$发给$\mathcal{A}$。

第2阶段：重复第1阶段密钥询问。

输出：$\mathcal{A}$选择一个比特$\beta'\in\{0,1\}$，返回转换密文$\{V'=V_\gamma,\tilde{C}_0\}$, $\mathcal{A}$输出β'作为γ的猜测，$\mathcal{B}$计算$\varepsilon\mathrm{k}_\gamma=\tilde{C}_0/{V'}^z$，其中$z$是转换钥。

假定$\mathcal{A}$可以攻破上述游戏，则敌手$\mathcal{B}$可计算${g_1}^{H_2(\varepsilon\mathrm{k}_\gamma)}={g_1}^{\theta}\Rightarrow{g_1}^{H_2(\varepsilon\mathrm{k}_\gamma)-\theta}=1\Rightarrow{g_1}^{\Delta\varepsilon\mathrm{k}}=1$。任意$h_1,h_2\in G_1$，有$h_2={h_1}^{t}$，不失一般性，存在$t_1,t_2\in Z_p^*$，使得$g_1={h_1}^{t_1}\cdot h_2^{t_2}$，则$1=({h_1}^{t_1}\cdot h_2^{t_2})^{\Delta\varepsilon\mathrm{k}}$，$h_2={h_1}^{-t_1\Delta\varepsilon\mathrm{k}/-t_2\Delta\varepsilon\mathrm{k}}$，$t=-t_1\Delta\varepsilon\mathrm{k}/-t_2\Delta\varepsilon\mathrm{k}$ $(-t_2\Delta\varepsilon\mathrm{k}\neq0)$。从而敌手$\mathcal{B}$以$1-1/p$优势攻破DL问题。证毕

定理2 如果DL假设在群G_1上是难解的，则本方案是选择关键字攻击安全的。

证明 若存在敌手$\mathcal{A}$以不可忽略的优势攻破本文方案，那么，存在多项式时间敌手$\mathcal{B}$以不可忽略的优势攻破DL问题。$\mathcal{A}$与$\mathcal{B}$的交互如下：

初始化：首先$\mathcal{A}$选择要进行挑战的访问策略$\mathbb{A}^*$，并将$\mathbb{A}^*$发送$\mathcal{B}$。

系统建立: $\mathcal{B}$随机选择$a\in F_q$，对每个位置的属性$\mathrm{attr}_i(i\in[1,n])$，设置$\beta_i=a^{-i}$，$\alpha_i=g^{a^i}$，抗碰撞的Hash函数$H_1:\{0,1\}^*\to G_1$，$H_2:\{0,1\}^*\to Z_p^*$，$H_3:\{0,1\}^*\to\{0,1\}^{256}$，系统公共参数为$\mathrm{PK}=\{G_1,G_2,g,g_1,e,H_1,H_2,\{g^{\beta_i},\alpha_i\}_{i\in[1,n]}\}$，主密钥$\mathrm{Msk}=\{a,\beta_i\}$,TA将PK发送给$\mathcal{A}$。

第1阶段: $\mathcal{A}$询问属性集S的私钥和关键字的门限值。$\mathcal{B}$选择$s_1,s_2\in_R Z_p^*$，计算：${\mathrm{sk}'}_1=g^{s_1}$，${\mathrm{sk}'}_2={g_1}^{s_1}$，${\mathrm{sk}'}_3=\left(\prod_{i=1}^{n}H_1(x_{ij_u})\right)^{s_1}$，$\mathrm{sk}_i=\{H_1(x_{ij_u})^{\beta_i}\}_{i\in[1,n]}$，$\mathrm{tok}_1={\mathrm{sk}'}_1^{s_2H_2(w')}$，$\mathrm{tok}_2={{\mathrm{sk}'}_2}^{s_2}$，$\mathrm{tok}_3={{\mathrm{sk}'}_3}^{s_2}$，并返回私钥和Trap。

挑战阶段: $\mathcal{A}$选择两个长度相同的关键字w_0,w_1发送给$\mathcal{B}$, $\mathcal{B}$随机选择一个比特$b\in\{0,1\}$，设置w_b的门限值：$\mathrm{tok}_1={\mathrm{sk}'}_1^{s_2H_2(w_b)}$，$\mathrm{tok}_2={{\mathrm{sk}'}_2}^{s_2}$，$\mathrm{tok}_3={{\mathrm{sk}'}_3}^{s_2}$。

此时是w_b的密文，否则为G_1中的任意元素的密文。

第2阶段: 重复第1阶段询问，但不能发出任何关于w_0, w_1的门限询问。

猜测：$\mathcal{A}$选择一个比特b'，若输出$b'=b$，输出1，否则为0。

若存在敌手$\mathcal{A}$以不可忽略的优势攻破本文方案，那么，存在多项式时间敌手$\mathcal{B}$以不可忽略的优势攻破DL问题。　　证毕

除了上述安全性，本文方案还具有下述特点：

(1)有序多值属性集：本文中，采用有序属性集，将每个属性的位置唯一固定，不论具体的属性取值，只有唯一的β_i, α_i与第i个属性对应，从而减少了参数和相应的计算，提高了方案的效率；此外，在密钥生成时计算具体属性取值的哈希值，从而达到区别多值属性取值的不同。

(2) 门限不可链接性：在搜索阶段，用户需要将关键字加密后上传到云中，如果门限生成函数是固定的，那么包含相同关键字的门限也是相同的，这样会泄露搜索信息给云服务器，因此，在本方案中，用户在生成门限时，搜索者选择一个随机值s_2,设置门限值：$\mathrm{tok}_1 = g^{s_1 s_2 H_2(w')}$，因此，相同的关键字每次加密生成的门限是不一样的。从而，云服务器从门限中不能得到任何关键字之间的联系。

(3) 完整性验证：本方案中包含了对称钥、搜索结果和密文的完整性验证，具体为：(a)通过计算：$\varepsilon\mathrm{k} = \tilde{C}_0 / V^z$, $\sigma = H_2(\varepsilon\mathrm{k})$, ${g_1}^{\sigma} = {g_1}^{H_2(\varepsilon\mathrm{k})} = \tilde{C}$，实现对对称钥$\varepsilon$k的正确性验证；(b)通过加入关键字，计算$\mathrm{Dec}_{\varepsilon\mathrm{k}}(\bar{\delta}_w, w') = \delta_w$与从$\mathrm{MT}_w$中得到的$\delta_w{}'$比较，同时对密文完整性和搜索结果正确性的验证。

5　性能分析

5.1　理论分析

本节主要在功能性、通信开销和计算开销方面与文献[13,19]进行了比较。$|G_1|$表示群G_1中一个元素的长度，$|G_2|$表示群G_2中一个元素的长度，$|Z_p|$表示Z_p中一个元素的长度，n表示属性个数，l_1表示询问的关键字个数，l_2表示提取的关键字个数。

表2给出了本文方案与文献[13,19]在功能上的比较。表3和表4分别给出了本文方案及文献[13,19]在存储开销与计算开销的比较。e_1是G_1中指数运算的时间, e_2是G_2中指数运算的时间，τ是双线性映射运算所需的时间, H是Hash函数运算所需的时间。从表中可以看出本文在实现功能性方面比较好，并且通信开销和计算开销明显较少。

5.2　实验分析

本小节对本方案和文献[13,19]的密钥生成算法、门限生成算法、搜索和解密算法进行了实验仿真。仿真平台Windows 10，AMD A8-6410 APU with AMD Randeon R5 Graphics 2.00 GHz，内存为8 GB，代码库PBC(Paring-Based Cryptography[22])，使用大素数为512位。从图7—图10可以看出，本文方案与文献[13]方案在密钥生成、门限生成、搜索阶段效率几乎持平，但是在解密阶段效率高很多，而相比文献[19]的各个阶段，本文方案是高效的。图11和图12分别给出本文方案在属性个数变化时多关键字情形下，门限生成时间与搜索时间，从图中可以得出，门限生成与属性个数和各关键字个数无关，而搜索阶段仅与关键字个数有关，其余两个方案不支持多关键字搜索。

6　结束语

本文就不可信云环境下，提出具有隐私保护的

表 2　功能比较

方案	隐藏访问结构	外包解密	匿名性	完整性认证	多关键字搜索
文献[13]	×	×	×	√	×
文献[19]	√	×	×	√	×
本文方案	√	√	√	√	√

表 3　通信开销比较

	文献[13]	文献[19]	本文方案
密钥生成	$(2n+3)\lvert G_2\rvert + \lvert Z_p\rvert$	$(n+5)\lvert G_2\rvert + n\lvert Z_p\rvert$	$(n+3)\lvert G_1\rvert + \lvert Z_p\rvert$
门限生成	$(2n+3)\lvert G_2\rvert$	$\lvert G_2\rvert + \lvert G_1\rvert$	$3\lvert G_1\rvert + \lvert Z_p\rvert$
搜索	$(3n+1)\lvert G_1\rvert$	$3\lvert G_2\rvert + n\lvert G_1\rvert$	$\lvert G_2\rvert + \lvert G_1\rvert$
解密	$(2n+2)\lvert G_2\rvert + 2\lvert G_1\rvert$	$(n+3)\lvert G_2\rvert$	$\lvert G_2\rvert$

表 4　计算开销比较

	文献[13]	文献[19]	本文方案
密钥生成	$(2n+4)e_1 + nH$	$(n+5)e_1 + nH$	$(n+3)e_1 + nH$
门限生成	$(2n+4)e_1$	$2e_2$	$3e_1$
搜索	$(2n+1)\tau + ne_1$	$ne_1 + 2\tau$	$e_1 + \tau$
解密	$(2n+2)\tau + 2e_2$	$ne_1 + 3\tau$	e_2

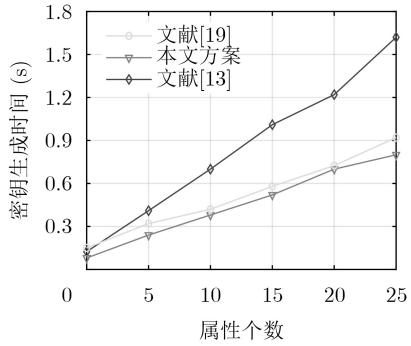

图 7 密钥生成阶段

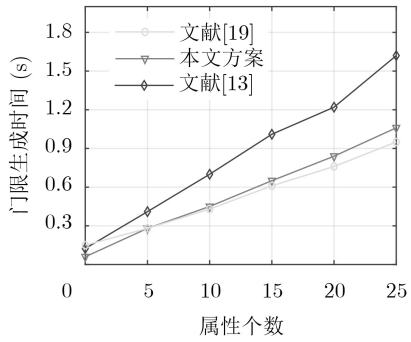

图 8 门限生成阶段

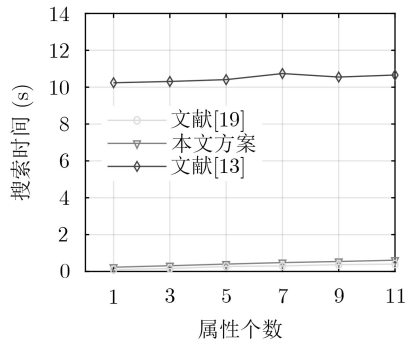

图 9 搜索阶段

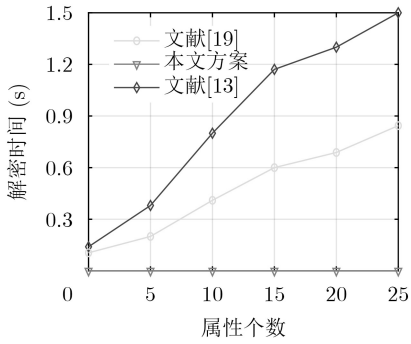

图 10 解密阶段

完整性可验证的ABKS方案。方案提出有序多值属性访问结构和有序多值属性集，固定每个属性的位置，减少参数及相关计算，提高了方案的效率；采用Hash和对运算实现访问结构的隐藏，保护了访问结构的安全性与用户身份的隐私性；在密钥生成时计算具体属性取值的哈希值，从而达到区别多值属性取值的不同；同时，采用倒序索引结构和Merkle树建立数据认证树，实现对云服务器返回密文的完整性认证并确保外包解密的正确性，防止云服务器对数据的恶意篡改和返回不正确的结果。此外，充分利用云的计算能力，支持外包解密以降低用户侧的计算量。安全性分析和实验表明，本文方案可实现云中共享数据的可验证性、关键字不可区分性和关键字不可链接性，且是高效的。在未来工作中，将探索云存储中的关键字的更新和文件的删除和添加。

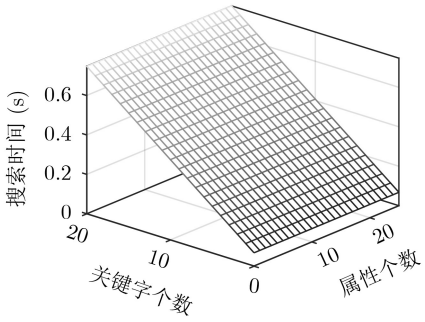

图 11 多关键字搜索阶段

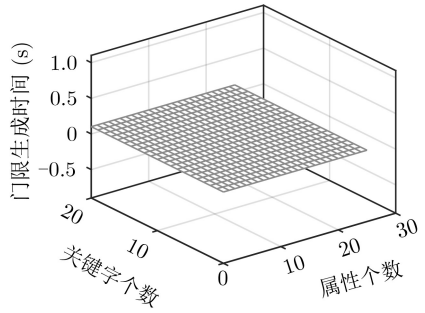

图 12 多关键字门限生成阶段

参 考 文 献

[1] SONG Xiaodong, WAGNER D, and PERRIG A. Practical techniques for searches on encrypted data[C]. 2000 IEEE Symposium on Security and Privacy, Berkeley, USA, 2000: 44–55.

[2] BONEH D, DI CRESCENZO G, OSTROVSKY R, *et al*. Public key encryption with keyword search[C]. International Conference on the Theory and Applications of Cryptographic Techniques, Interlaken, Switzerland, 2004: 506–522.

[3] LU Yang, WANG Gang, LI Jiguo, *et al*. Efficient designated server identity-based encryption with conjunctive keyword search[J]. *Annals of Telecommunications*, 2017, 72(5/6): 359–370. doi: 10.1007/s12243-017-0574-7.

[4] MIAO Yinbing, MA Jianfeng, LIU Ximeng, *et al*. VMKDO: Verifiable multi-keyword search over encrypted cloud data for dynamic data-owner[J]. *Peer-to-Peer Networking and Applications*, 2018, 11(2): 287–297. doi: 10.1007/s12083-016-0487-7.

[5] GE Xinrui, YU Jia, HU Chengyu, *et al*. Enabling efficient verifiable fuzzy keyword search over encrypted data in cloud computing[J]. *IEEE Access*, 2018, 6: 45725–45739. doi: 10.1109/ACCESS.2018.2866031.

[6] TURKY A, ABDULLAH S, and DAWOD A. A dual-population multi operators harmony search algorithm for dynamic optimization problems[J]. *Computers & Industrial Engineering*, 2018, 117: 19–28. doi: 10.1016/j.cie.2018.01.003.

[7] LI Yuxi, ZHOU Fucai, QIN Yuhai, *et al*. Integrity-verifiable conjunctive keyword searchable encryption in cloud storage[J]. *International Journal of Information Security*, 2018, 17(5): 549–568. doi: 10.1007/s10207-017-0394-9.

[8] FARRÀS O and RIBES-GONZÁLEZ J. Provably secure public-key encryption with conjunctive and subset keyword search[J]. *International Journal of Information Security*, 2019, 18(5): 533–548. doi: 10.1007/s10207-018-00426-7.

[9] WANG Haijiang, DONG Xiaolei, and CAO Zhenfu. Multi-value-independent ciphertext-policy attribute based encryption with fast keyword search[J]. *IEEE Transactions on Services Computing*, 2017(99): 1–11. doi: 10.1109/TSC.2017.2753231.

[10] SHIRAISHI Y, NOMURA K, MOHRI M, *et al*. Attribute revocable attribute-based encryption with forward secrecy for fine-grained access control of shared data[J]. *IEICE Transactions on Information and Systems*, 2017, E100.D(10): 2432–2439. doi: 10.1587/transinf.2016OFP0008.

[11] AMERI M H, DELAVAR M, MOHAJERI J, *et al*. A key-policy attribute-based temporary keyword search scheme for secure cloud storage[J]. *IEEE Transactions on Cloud Computing*, 2018(99): 1–12. doi: 10.1109/TCC.2018.2825983.

[12] 张玉磊, 刘文静, 刘祥震, 等. 基于授权的多服务器可搜索密文策略属性基加密方案[J]. 电子与信息学报, 2019, 41(8): 1808–1814. doi: 10.11999/JEIT180944.

ZHANG Yulei, LIU Wenjing, LIU Xiangzhen, *et al*. Searchable Multi-server CP-ABE scheme based on authorization[J]. *Journal of Electronics & Information Technology*, 2019, 41(8): 1808–1814. doi: 10.11999/JEIT180944.

[13] MIAO Yinbin, MA Jianfeng, JIANG Qi, *et al*. Verifiable keyword search over encrypted cloud data in smart city[J]. *Computers & Electrical Engineering*, 2018, 65: 90–101. doi: 10.1016/j.compeleceng.2017.06.021.

[14] MIAO Yinbin, MA Jianfeng, WEI Fushan, *et al*. VCSE: Verifiable conjunctive keywords search over encrypted data without secure-channel[J]. *Peer-to-Peer Networking and Applications*, 2017, 10(4): 995–1007. doi: 10.1007/s12083-016-0458-z.

[15] BALLARD L, KAMARA S, and MONROSE F. Achieving efficient conjunctive keyword searches over encrypted data[C]. The 7th International Conference on Information and Communications Security, Beijing, China, 2005: 414–426.

[16] TIWARI D and GANGADHARAN G R. SecCloudSharing: Secure data sharing in public cloud using ciphertext-policy attribute-based proxy re-encryption with revocation[J]. *International Journal of Communication Systems*, 2018, 31(5): e3494. doi: 10.1002/dac.3494.

[17] BHATEJA R, ACHARJYA D P, and SAXENA N. Enhanced timing enabled proxy re-encryption model for E-health data in the public cloud[C]. 2017 International Conference on Advances in Computing, Communications and Informatics (ICACCI), Udupi, India, 2017: 2040–2044.

[18] YANG Yang and MA Maode. Conjunctive keyword search with designated tester and timing enabled proxy Re-encryption function for E-health clouds[J]. *IEEE Transactions on Information Forensics and Security*, 2016, 11(4): 746–759. doi: 10.1109/TIFS.2015.2509912.

[19] WU Axin, ZHENG Dong, ZHANG Yinhui, *et al*. Hidden policy attribute-based data sharing with direct revocation and keyword search in cloud computing[J]. *Sensors*, 2018, 18(7): 2158. doi: 10.3390/s18072158.

[20] LI Jiguo, SHA Fengjie, ZHANG Yichen, *et al*. Verifiable outsourced decryption of attribute-based encryption with constant ciphertext length[J]. *Security and Communication Networks*, 2017, 2017: 3596205. doi: 10.1155/2017/3596205.

[21] 赵志远, 孙磊, 户家富, 等. 可验证外包解密的离线/在线属性基加密方案[J]. 电子与信息学报, 2018, 40(12): 2998–3006. doi: 10.11999/JEIT180122.

ZHAO Zhiyuan, SUN Lei, HU Jiafu, *et al*. Efficient offline/online attribute based encryption with verifiable outsourced decryption[J]. *Journal of Electronics & Information Technology*, 2018, 40(12): 2998–3006. doi: 10.11999/JEIT180122.

[22] LYNN B. PBC library[EB/OL]. http://cryptostanford.edu/pbc, 2006.

刘雪艳：女，1978年生，副教授，硕士生导师，研究方向为密码学与云存储中数据隐私保护.

芦婷婷：女，1994年生，硕士生，研究方向为密码学与可搜索加密.

杨晓涛：女，1993年生，硕士生，研究方向为密码学与属性密码学.

责任编辑：马秀强