

云存储中基于属性的关键词搜索加密方案研究

朱智强, 苏航, 孙磊, 李作辉

(信息工程大学三院, 河南 郑州 450000)

摘要: 为保证云端敏感数据安全性的同时提高数据共享效率, 提出了一种安全、灵活、高效的基于属性的关键词搜索加密方案。方案中设计了一种需要数据拥有者私钥参与的索引生成机制抵抗关键词猜测攻击, 基于线性秘密共享访问结构描述用户的搜索权限, 支持一对多应用场景, 借鉴连接子集关键词搜索技术和在线/离线思想提高搜索的灵活性和效率。理论分析与实验评估结果表明, 该方案具有较高的效率。

关键词: 可搜索加密; 关键词猜测攻击; 连接关键词; 在线/离线

中图分类号: TP311

文献标识码: A

doi: 10.11959/j.issn.2096-109x.2017.00214

Research on attribute-based encryption with keyword search for cloud storage

ZHU Zhi-qiang, SU Hang, SUN Lei, LI Zuo-hui

(The Third Party, Information Engineering University, Zhengzhou 450000, China)

Abstract: To safeguard the sensitive data stored on the cloud and promote the efficiency of data sharing simultaneously, a secure flexible and efficient attribute-based encryption scheme with keyword search is proposed, which designs an index generation mechanism that requires the private key of data owner to resist the keyword guessing attack, supports one-to-many application scenarios based on the linear secret shared access structure, introduces the conjunctive subset keyword search technique and online/offline technique to improve search flexibility and efficiency. Theoretical analysis and experimental evaluation show that the proposed scheme enjoys high efficiency.

Key words: searchable encryption, keyword guessing attack, conjunctive keyword, online/offline

1 引言

随着云存储技术迅猛发展, 越来越多的企业和个人选择在云端存储和共享数据, 但由于云端数据使用权和管理权的分离, 数据拥有者通常会加密敏感数据以确保其在云端的安全性, 这造成了数据可供检索的语义和统计特性丢失, 导致云服务提供商无法为用户提供数据搜索服务, 极大地降低了云端数据的共享效率。公钥可搜索加密

技术(PKES, public key encryption with keyword search)的出现为解决上述问题提供了解决方案, 该技术确保只有合法用户具备执行关键词搜索的能力, 搜索过程不会影响数据安全性。

近年来, 公钥可搜索加密技术得到广泛研究和快速发展^[1], 为适用于云存储环境, 公钥可搜索加密方案需要满足下述特性。一是抵抗内部、外部关键词猜测攻击。由于可搜索加密方案具有一致性, 并且关键词空间具有低熵性, 关键词猜

收稿日期: 2017-08-25; 修回日期: 2017-10-19。通信作者: 苏航, suhang_039@163.com

基金项目: 国家重点研发计划基金资助项目 (No.2016YFB0501900)

Foundation Item: The National Key R&D Program of China (No.2016YFB0501900)

测攻击 (KGA, keyword guessing attack) (攻击者通过收集陷门信息, 利用系统中的公开信息生成多个包含不同关键词的索引, 进而推导出陷门中包含的关键词信息) 往往十分有效。二是支持多用户共享检索。云端数据共享的参与者往往是多个数据拥有者与数据使用者, 为适用于云存储, 要求可搜索加密方案支持一对多的应用场景。三是支持连接关键词搜索。数据使用者通常需要查找多个关键词以实现文件的精确定位, 为支持灵活的搜索操作, 要求可搜索加密方案支持连接关键词搜索。四是用户计算开销较低。当前大量移动终端参与云端数据共享, 为支持运算能力、电池容量受限的移动终端, 要求方案减少搜索过程中用户的计算复杂度。

1.1 相关工作

为有效地支持云存储中的一对多应用场景, Zheng 等^[2]和 Sun 等^[3]结合属性基加密 (ABE, attribute-based encryption) 技术与可搜索加密 (SE, searchable encryption) 技术, 提出基于属性的关键词搜索方案 (ABKS, attribute-based keyword search), 既支持密文数据的细粒度访问控制, 又能提供对密文数据的快速检索, 有效提高了云端密文数据的共享效率。

KGA 最早由 Byun 等^[4]提出, 根据攻击者所处位置的不同, 可分为内部 KGA 和外部 KGA^[5], 前者主要由 PEKS 系统中的恶意搜索服务器发起; 后者由除搜索服务器外的其他敌手发起。Wang 等^[6]提出了一种可抵抗内部和外部 KGA 的搜索方法, 即指定多个搜索服务器共同参与搜索过程, 但仍无法抵抗多搜索服务器的共谋攻击。Li 等^[7]提出了一种基于混沌映射的抵抗内外 KGA 的搜索方法, 但要求数据拥有者实时在线, 以便与数据使用者共享会话密钥。林鹏等^[8]通过指定搜索服务器, 提出了一种可抵抗外部 KGA 的 ABKS 方案, 但方案假设搜索服务器是完全可信的, 无法抵抗内部 KGA。Chen 等^[9]提出一种基于双搜索服务器的 PEKS 方案, 通过将测试任务交给相互独立的前端和后端服务器处理, 实现同时抵抗内部和外部 KGA, 但该方案的构造基于同态加密, 计算复杂度较高。Qiu 等^[10]基于隐藏访问结构的 CP-ABE 方案, 提出了一个抵抗内部

KGA 和外部 KGA 的 ABKS 方案, 但需采用受限的“多值与门”作为访问结构, 并且存在与文献[7]相似的问题, 即要求数据拥有者实时在线。

2004 年, Golle 等^[11]首次提出支持连接关键词搜索的可搜索加密方案, 但由于指定了关键词域且关键词位置固定, 搜索的灵活性较差。Zhang 等^[12]基于多项式函数理论, 提出一种支持连接子集关键词公钥可搜索加密 (PECSK, public key encryption with conjunctive-subset keywords search) 方案, 支持动态关键词域。基于 PECSK 方案的思想, Yang 等^[13]提出一种适用于 E-Health 云系统的支持多关键词连接搜索的 PEKS 方案。宋衍等^[14]提出了一种支持关键词任意连接的 ABKS 方案, 可灵活地支持一对多应用场景中的多关键词搜索。

随着移动设备的普及, Dong 等^[15]参考 Hohenberger 等^[16]提出的在线/离线属性基加密方案, 将索引算法和陷门算法分为 2 个阶段, 并在离线阶段完成大部分的运算工作, 有效降低在线阶段的计算负担。陈冬冬等^[17]通过引入在线/离线技术和外包解密技术, 设计了一种高效的可搜索加密方案, 但对方案的安全性没有进行形式化证明。

针对公钥可搜索加密技术中支持一对多应用场景、抵抗内部外部 KGA、支持连接关键词搜索和在线/离线问题, 学术界展开了大量研究, 但现有的方案不能同时解决上述问题。

1.2 本文主要工作

本文首次提出一种适应于云端数据共享的安全、高效、灵活的 ABKS 方案——O²ABCSKS (online/offline attribute based conjunctive-subset keywords search), 方案具有以下 4 点优势。

1) 抵抗内部 KGA: 设计了一种需要数据拥有者私钥参与的索引生成机制, 排除了恶意搜索服务器构造伪造索引的可能。

2) 支持一对多应用场景: 采用具有强表达力的线性秘密共享 (LSSS, linear secret sharing scheme) 访问结构描述用户的搜索权限, 支持一对多的应用场景。

3) 搜索灵活性较高: 支持连接关键词搜索, 提供灵活的多关键词搜索功能。

4) 用户计算开销低: 较其他访问结构, 采用

LSSS 访问结构系统开销有所增加,为降低用户端的开销,引入离线在线思想,将索引和陷门算法分为在线和离线 2 个阶段执行。离线阶段中索引和陷门算法使用的关键词、属性列表或访问结构等信息未知,该阶段承担算法中大部分的计算量;在线阶段已知关键词、属性列表或访问结构等信息后,仅需少量计算即可完成索引和陷门算法。离线阶段可在设备空闲时执行,大大降低了在线阶段的运算量。

2 预备知识

2.1 双线性映射及困难性假设

定义 1 双线性映射。

G, G_T 表示阶为素数 p 的乘法循环群, $g \in G$ 为群 G 的生成元。若映射 $e: G \times G \rightarrow G_T$ 满足下述要求,则其为有效的双线性映射。

双线性: $\forall h_1, h_2 \in G, a, b \in \mathbb{Z}_p, e(h_1^a, h_2^b) = e(h_1, h_2)^{ab}$ 。

非退化性: $e(g, g) \neq 1$ 。

可计算性: $\forall h_1, h_2 \in G$, 存在多项式时间算法计算 $e(h_1, h_2)$ 。

定义 2 q -DPBDHE (q -decisional parallel bilinear Diffie-Hellman exponent assumption) 假设^[18]。

令 G, G_T 表示阶为素数 p 的乘法循环群, $g \in G$ 为生成元, $e: G \times G \rightarrow G_T$ 为有效的双线性映射, 随机选取 $a, s \in \mathbb{Z}_p, T \in G_T$ 。给定元组

$y = \{g, g^s, \forall_{1 \leq i \leq 2q, i \neq q+1} g^{a^i}, g^{sb_j}, \forall_{1 \leq i \leq 2q, i \neq q+1, 1 \leq j \leq q} g^{\frac{a^i}{b_j}}, \forall_{1 \leq i, j, k \leq q, k \neq j} g^{\frac{a^i s b_k}{b_j}}, T\}$, 判定 $T = e(g, g)^{a^{q+1}s}$ 是否成立。

定义 3 DDDH (divisible decisional Diffie-Hellman assumption) 假设^[19]。

令 G 表示阶为素数 p 的乘法循环群, $g \in G$ 为生成元, 随机选取 $a, b \in \mathbb{Z}_p, T \in G$ 。给定元组

$y = \{g, g^a, g^b, T\}$, 判定 $T = g^{\frac{a}{b}}$ 是否成立。

2.2 线性秘密共享方案

定义 4 线性秘密共享方案^[18]。

若在一组参与方 P 上的线性秘密共享方案 Π 满足下述条件, 那么它是线性的。

1) 每个参与方的线性共享份构成一个 $\mathbb{Z}_p$ 上

的向量。

2) 对于秘密共享方案 Π , 存在秘密共享份生成矩阵 $M_{l \times n}$ 。函数 $\rho: \{1, \dots, l\} \rightarrow P_i$ 将矩阵 $M_{l \times n}$ 中的第 i 行映射到参与方集合中。令 $s \in \mathbb{Z}_p$ 表示待共享秘密值, 随机选取 $\forall_{2 \leq i \leq n} r_i \in \mathbb{Z}_p$ 组成向量 $v = (s, r_2, \dots, r_n)$ 。 Mv^T 表示秘密值 s 的 l 个共享份, 其中 $\lambda_i = (Mv^T)_i$ 表示第 i 个共享份, 将 λ_i 分配给参与方 $\rho(i)$ 。

秘密共享方案满足线性重构性质: 令 Π 表示访问策略 ($M_{l \times n}, \rho$) 上的线性秘密共享方案, S 为访问策略的一个授权集, 集合 I 定义为 $I = \{i: \rho(i) \in S\} \subseteq \{1, \dots, l\}$, 存在多项式时间算法计算 $\{w_i \in \mathbb{Z}_p\}_{i \in I}$, 使对 Π 上的有效共享份 λ_i ,

$\sum_{i \in I} w_i \lambda_i = s$ 成立。

3 算法定义及安全模型

3.1 系统模型

系统中有 4 类实体: 云服务提供商 (CSP, cloud service provider)、授权机构 (AA, authorized authority)、数据拥有者 (DO, data owner) 以及数据使用者 (DU, data user)。

1) 云服务提供商

CSP 为系统中的用户提供数据存储、关键词搜索等服务。在本文方案中, CSP 是“诚实但具有好奇心的”, CSP 会如实执行既定的操作, 但它也可能攻击云端存储的数据以获取其中的信息。

2) 授权机构

AA 负责系统建立、用户密钥等生成工作, 是系统中唯一的可信第三方。

3) 数据拥有者

DO 可加密数据, 生成关键词索引, 并将其数据密文及关键词索引上传至云端。

4) 数据使用者

DU 可向 CSP 请求关键词搜索服务, 并从 CSP 处获取搜索结果。

在云存储环境中, 使用本方案进行数据共享的工作流程如图 1 所示。

1) AA 建立系统。

2) DO 在 AA 处注册, AA 生成用户密钥并发送给 DO。

3) DO 加密待上传云端的数据, 在数据中挑

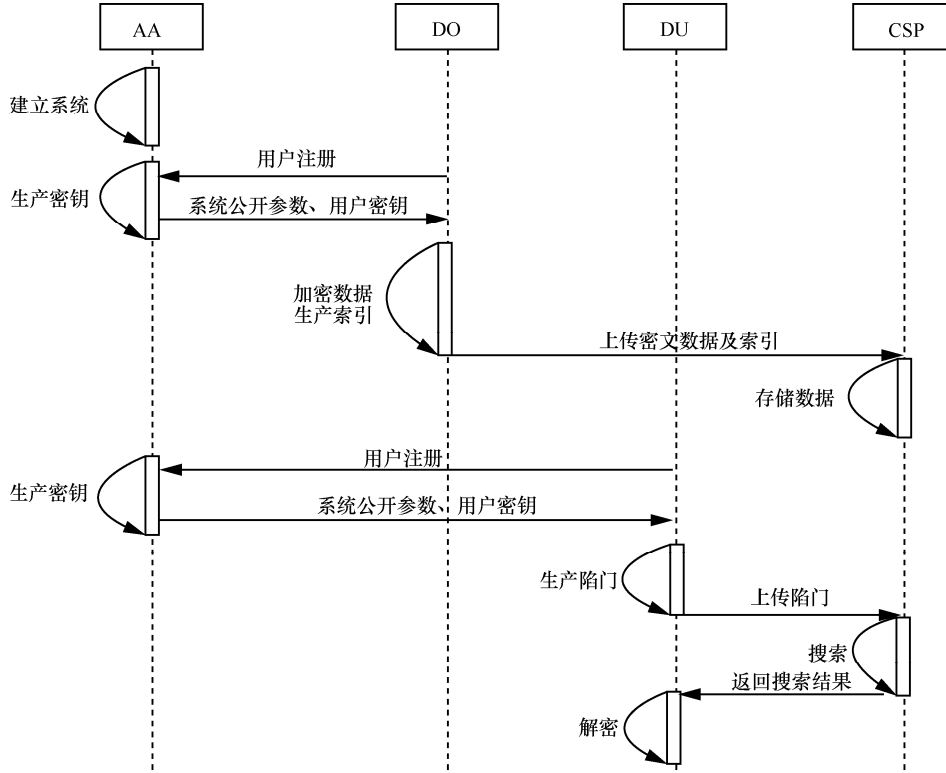


图1 工作流程

选关键词并生成关键词索引。

4) DO 将密文及索引上传至云端。CSP 存储密文及相应的关键词索引。

5) DU 在 AA 处注册。AA 生成用户密钥并发送给 DU。

6) DU 选取待搜索数据集及待搜索关键词，生成搜索陷门。

7) DU 将搜索陷门上传至搜索服务器，搜索服务器执行搜索操作并将结果发送给 DU。

8) DU 解密密文数据得到明文。

3.2 算法定义

定义 5 本文提出的方案包括 7 个算法，算法定义如下。

$\text{Setup}(1^\lambda) \rightarrow (PP, MSK)$ 系统建立算法由 AA 运行。算法输入为安全参数，输出为系统公开参数 PP 及系统主密钥 MSK 。

$\text{KeyGen}(PP, MSK, S) \rightarrow SK$ 密钥生成算法由 AA 运行。算法输入为系统公开参数 PP ，系统主密钥 MSK 以及用户属性集 S ，输出为用户密钥 SK 。

$\text{Offline.Index}(PP) \rightarrow IX$ 离线关键词索引算法由 DO 运行，在此阶段，待加密的关键词集合

及其访问结构是未知的。算法输入为系统公开参数 PP ，算法输出为中间索引 IX 。

$\text{Online.Index}(PP, SK_{sid}, IX, KW, (M_{l \times n}, \rho)) \rightarrow$

Index 在线关键词索引算法由 DO 运行。算法输入为系统公开参数 PP ，数据拥有者的私钥 SK_{sid} 、中间索引 IX 、为数据选取的关键词集合 KW 以及制定的访问结构 $(M_{l \times n}, \rho)$ ，算法输出为最终的索引 Index 。

$\text{Offline.Trapdoor}(PP, SK) \rightarrow IT$ 离线陷门算法由 DU 运行，在此阶段，待搜索的关键词集合及待搜索数据集是未知的。算法输入为系统公开参数 PP 以及 DU 的密钥 SK ，算法输出为中间陷门 IT 。

$\text{Online.Trapdoor}(PP, IT, SK, PK_{sid}, SKW) \rightarrow$

Trapdoor 在线陷门算法由 DU 运行。算法输入为系统公开参数 PP 、中间陷门 IT 、用户密钥 SK 、待搜索数据集的 DO 公钥 PK_{sid} 以及待搜索的关键词集合 SKW ，算法输出为陷门 Trapdoor 。

$\text{Search}(\text{Index}, \text{Trapdoor}) \rightarrow SR$ 搜索算法由 CSP 运行。算法输入为关键词索引 Index 及陷门 Trapdoor ，算法输出为搜索结果 SR 。

3.3 安全模型

定义 6 索引保密性。

考虑数据所有者存储在云端数据的安全性，保证索引不会泄露其为数据选取的关键词信息，方案需要达到选择关键词明文攻击的不可区分性安全(IND-CKA)。攻击者和挑战者之间在选择模型下的攻击游戏定义如下。

初始化：敌手 $\mathcal{A}$ 选取待挑战的访问结构 $(M_{1 \times n}^*, \rho^*)$ 。

系统建立：挑战者 $\mathcal{C}$ 运行系统建立算法，生成系统公开参数以及主密钥，将公开参数发送给敌手 $\mathcal{A}$ ，并秘密地保存主密钥。

阶段 1 $\mathcal{A}$ 对下述预言机进行多项式次数的询问， $\mathcal{C}$ 按照下述方法回答 $\mathcal{A}$ 的查询。

$\mathcal{O}_{\text{KeyGen}}(S)$ $\mathcal{A}$ 将其属性集合 S 提交给 $\mathcal{C}$ 。若 S 满足访问结构 $(M_{1 \times n}^*, \rho^*)$ ，则终止；否则， $\mathcal{C}$ 运行密钥生成算法，产生相应的密钥并发送给 $\mathcal{A}$ 。

$\mathcal{O}_{\text{Trapdoor}}(S, SKW)$ $\mathcal{A}$ 将属性集合 S 、关键词集合 SKW 提交给 $\mathcal{C}$ 。 $\mathcal{C}$ 运行离线陷门算法和在线陷门算法，生成相应的陷门并将其发送给 $\mathcal{A}$ ，将 $\mathcal{A}$ 提交的关键词集合 SKW 添加到关键词集合列表 L_{SKW} 中。

挑战： $\mathcal{A}$ 提交待挑战的关键词集合 KW_1, KW_2 ，要求 L_{SKW} 中没有集合 $(KW_1^* \setminus KW_2^*)$ 或集合 $(KW_2^* \setminus KW_1^*)$ 的子集。可构造仿真器 Σ 随机选取 $rand \in \{0, 1\}$ ，生成挑战索引 $Index_{KW_{rand}}$ ，并将其发送给 $\mathcal{A}$ 。

阶段 2 与阶段 1 相同， $\mathcal{A}$ 可对 KeyGen 陷门和 Trapdoor 陷门进行多项式次的查询，但当查询 KeyGen 陷门时， $\mathcal{A}$ 提交的属性集合不能满足 $(M_{1 \times n}^*, \rho^*)$ ；查询 Trapdoor 陷门时， $\mathcal{A}$ 不能查询 KW_1, KW_2 对应的陷门，其提交的属性集合满足 $(M_{1 \times n}^*, \rho^*)$ 。

猜测： $\mathcal{A}$ 输出对 $rand$ 的猜测，并将其表示为 $rand'$ 。若 $rand' = rand$ ， $\mathcal{A}$ 赢得游戏。 $\mathcal{A}$ 在该游戏中的优势被定义为 $\text{Adv} := |\Pr(rand = rand') - \frac{1}{2}|$ 。

定义 7 陷门保密性。

考虑数据使用者搜索过程的安全性，保证其生成的陷门不会泄露当前搜索关键词信息，方案需要达到选择关键词明文攻击的不可区分性安

全。攻击者和挑战者之间在选择模型下的攻击游戏定义如下。

系统建立：挑战者 $\mathcal{C}$ 运行系统建立算法，生成系统公开参数以及主密钥，将公开参数发送给敌手 $\mathcal{A}$ ，秘密地保存主密钥。

阶段 1 $\mathcal{A}$ 对 Trapdoor 陷门进行多项式次的查询， $\mathcal{C}$ 按照下述方法回答 $\mathcal{A}$ 的查询。

$\mathcal{O}_{\text{Trapdoor}}(S, SKW)$ $\mathcal{A}$ 将属性集合 S 、关键词集合 SKW 以及数据拥有者的公钥提交给 $\mathcal{C}$ 。 $\mathcal{C}$ 运行离线陷门算法和在线陷门算法，生成相应的陷门并将其发送给 $\mathcal{A}$ ，将 $\mathcal{A}$ 提交的关键词集合 SKW 添加到列表 L_{SKW} 中。

挑战： $\mathcal{A}$ 提交待挑战的关键词集合 SKW_1, SKW_2 ，包含 SKW_1, SKW_2 的集合都未曾出现在 L_{SKW} 中。 Σ 随机选取 $rand \in \{0, 1\}$ ，生成挑战索引 $\text{Trapdoor}_{SKW_{rand}}$ ，并将其发送给 $\mathcal{A}$ 。

阶段 2 与阶段 1 相同， $\mathcal{A}$ 可对 Trapdoor 陷门进行多项式次的查询，但若 $\mathcal{A}$ 提交的属性集合满足访问结构 $(M_{1 \times n}^*, \rho^*)$ ，则其不能查询 SKW_1, SKW_2 对应的陷门。

猜测： $\mathcal{A}$ 输出对 $rand$ 的猜测，并将其表示为 $rand'$ 。若 $rand' = rand$ ， $\mathcal{A}$ 赢得游戏。 $\mathcal{A}$ 在该游戏中的优势被定义为 $\text{Adv} := |\Pr(rand = rand') - \frac{1}{2}|$ 。

4 O²ABCSKS 方案

ABKS 方案的主要应用场景如下^[18]：为提高数据共享效率，数据所有者为其数据挑选关键词，并生成关键词索引，使预期的接收者可以安全高效地实施密文搜索。因此，在实际搜索过程中，数据使用者获取数据拥有者的公钥信息是可行的。基于上述分析，本文构造了一种可抵抗内部 KGA 和外部 KGA 的索引生成机制，该机制的实施方法如下。授权机构在用户注册时为用户产生包括一个公私钥对在内的搜索密钥；数据所有者生成索引时使用自己私钥签名生成的关键词索引；而数据使用者在搜索过程中指定待搜索数据集的数据所有者，并使用该数据拥有者的公钥加密搜索陷门。

基于上述索引生成机制，构造用来对 O²ABCSKS 方案发起 KGA 的伪造索引，需要数据拥有者的私钥。对于外部关键词猜测攻击，发起 KGA 的敌手为恶意用户，它可截获陷门信息，

但是它无法从中猜测出指定的待搜索数据集的数据拥有者,因此无法构造可有效发起攻击的伪造索引。对于内部关键词猜测攻击,发起 KGA 的敌手为恶意搜索服务器,它可截取陷门信息,并通过执行搜索算法可猜测出陷门中指定的数据拥有者信息以及执行算法过程中产生的中间参数,但是除非搜索服务器可攻破离散对数假设,否则无法获取数据拥有者的私钥,因此也无法构造可有效进行 KGA 的伪造索引。

4.1 具体构造

方案中使用的部分符号描述如表 1 所示。

表 1 符号定义

符号	描述
$(M_{l \times n}, \rho)$	数据访问结构
$PK_{s_{id}}, SK_{s_{id}}$	数据拥有者的公私钥对
KW	数据拥有者挑选的关键词集合
m	数据拥有者选取的关键词个数
S	用户的属性集合
$PK_{u_{id}}, SK_{u_{id}}$	数据使用者的公私钥对
SKW	数据使用者搜索的关键词集合

1) Setup(1^λ) $\rightarrow$ (PP, MSK)

系统属性集合为 U , 输入安全参数后, 授权机构按照下述步骤执行系统建立算法。

①选取阶为素数 p 的乘法循环群 G, G_T , 双线性映射 $e: G \times G \rightarrow G_T$, 生成元 $g_1 \in G$ 。

②随机选取 $a, b, \alpha \in \mathbb{Z}_p$, 计算 $g_2 = g_1^b$, $Y = e(g_1, g_2)^\alpha$, $f_1 = g_1^a$, $f_2 = g_2^a$ 。

③对属性集合中的所有属性, 随机选取 $\forall_{x \in U} h_x \in \mathbb{Z}_p$, 计算 $h_{1,x} = g_1^{h_x}$ 以及 $h_{2,x} = g_2^{h_x}$ 。

④选取密码学散列函数: $H: \{0,1\}^* \rightarrow \mathbb{Z}_p$ 。

⑤授权机构公布系统公开参数为 $PP = \{G, G_T, e, g_1, g_2, Y, f_1, f_2, \{h_{2,x}\}_{x=1}^u, H\}$, 并秘密保存系统主密钥 $MSK = \{\alpha, \{h_{1,x}\}_{x=1}^u\}$ 。

2) KeyGen(PP, MSK, S) $\rightarrow$ SK

授权机构审核用户提交的属性集合 S , 若通过审核, 授权机构按照下述步骤执行密钥生成算法。

①随机选取 $r_{id} \in \mathbb{Z}_p$, 用户私钥为 $SK_{r_{id}} = r_{id}$, 并计算 $PK_{r_{id}} = g_1^{r_{id}}$ 作为用户的公钥。

②随机选取 $t \in \mathbb{Z}_p$, 计算 $K = g_1^\alpha g_1^{at}$, $L = g_1^t$,

对用户属性集合 S 中的属性, 计算 $\forall_{x \in S} K_x = h_{1,x}^t$ 。

③随机选取 $z \in \mathbb{Z}_p$, 为用户生成搜索密钥

$$K' = g_1^a g_1^{z^2}, L' = L^z, K'_x = K_x^{\frac{1}{z}}.$$

④授权机构通过安全信道将密钥 $SK = \{SK_{r_{id}}, K', L', \{K'_x\}_{x \in S}\}$ 发送给用户。

3) Offline.Index(PP) $\rightarrow$ IX

此阶段由于需加密的数据集是未知的, 数据拥有者无法精确地选定关键词以及访问结构, 数据属性按照下述步骤执行该算法。

①随机选取 $s \in \mathbb{Z}_p$, 计算 $C = e(g_1, g_2)^{as}$, $C' = g_2^s$ 。

②令集合 K_{att} 表示离线阶段需计算的属性密钥的属性集合, 首次执行离线索引算法时 $K_{att} = U$ 。对属性 $x \in K_{att}$, 随机选取 $r_x \in \mathbb{Z}_p$, 计算 $C'_x = h_{2,x}^{-r_x}, D'_x = g_2^{r_x}$, 执行上述运算后, 将该属性从 K_{att} 中删除。

③输出中间索引 $IX = \{s, C, C', C'_0, \{C'_x, D'_x\}_{x \in U}\}$ 。

4) Online.Index(PP, SK_{s_{id}}, IX, KW, (M_{l×n}, ρ)) $\rightarrow$

Index

数据拥有者输入为数据集选定的关键词集合 $KW = \{KW_1, KW_2, \dots, KW_m\}$, 以及为其制定的访问结构 $(M_{l \times n}, \rho)$, 其中 ρ 表示将 M 中的行映射到属性的函数。数据拥有者按照下述步骤执行该算法。

①将 $(M_{l \times n}, \rho)$ 中用到的属性记录到集合 K_{att} 中。

②随机选取向量 $v = (s, y_2, \dots, y_n)$, 其中 $y_i \in \mathbb{Z}_p, 1 \leq i \leq n$, 计算 $\lambda_i = M_i v^T$, 其中 M_i 表示 $M_{l \times n}$ 的第 i 行。计算 $C_i = g_2^{a\lambda_i} C'_{\rho(i)}$, $D_i = D'_{\rho(i)}$ 。

③随机选取 $d \in \mathbb{Z}_p$, 构造 m 级多项式 $f(x) = d(x - H(KW_1))(x - H(KW_2)) \cdots (x - H(KW_m)) + s = d_m x^m + d_{m-1} x^{m-1} + \cdots + d_1 x + d_0$, 其中 $H(KW_1), H(KW_2), \dots, H(KW_m)$ 为方程 $f(x) - s = 0$ 的 m 个根。对 $d_i, 0 \leq i \leq m$, 计算 $E_i = g_2^{s_{id} d_i}$ 。

④输出索引 $Index = \{C, C', \{C_i, D_i\}_{i=1}^l, \{E_j\}_{j=0}^m\}$ 。

5) Offline.Trapdoor(PP, SK) $\rightarrow$ IT

此阶段搜索的关键词是未选定的, 数据使用者选取 $k \in \mathbb{Z}_p$, $F = g_1^{\frac{k}{u_{id}}}$, 输出 $IT = \{L', \{K'_x\}_{x \in S}, F\}$ 。

6) Online.Trapdoor(PP, IT, SK, PK_{s_{id}}, SKW) $\rightarrow$

Trapdoor

数据使用者选定待搜索关键词集合 $SKW = \{SKW_1, SKW_2, \dots, SKW_m\}$ 及待搜索数据集的数据拥有者。计算 $K'' = K'(g_1^{s_{id}})^{\frac{k}{u_{id}}}$ ，对 $0 \leq i \leq m$ ，计算 $F_i = F^{\frac{H(SKW_1)^i + H(SKW_2)^i + \dots + H(SKW_m)^i}{m^i}}$ ，输出陷门 $Trapdoor = \{K'', L', \{K'_x\}_{x \in S}, \{F_i\}_{i=0}^m\}$ 。

7) Search(Index, Trapdoor) $\rightarrow SR$

假设数据使用者的属性集合 S 满足访问结构 $(M_{l \times n}, \rho)$ 。令 $I = \{I : \rho(i) \in S\}$ 表示满足访问结构 $(M_{l \times n}, \rho)$ 的最小属性集合，云服务提供商计算 $T_1 = \prod_{i \in I} [e(C_i, L') e(D_i, K'_{\rho(i)})]^{w_i}$ ，其中 $\sum_{i \in I} w_i M_i = (1, 0, \dots, 0)$ ， $T_2 = e(K'', C')$ ， $T_3 = C \prod_{i=0}^m e(E_i, F_i)$ 。测试 $T_2 = T_1 T_3$ 是否成立，若成立，则当前测试索引对应的密文为数据使用者查找的；反之，则不是数据使用者查找的。

4.2 算法一致性

若数据使用者的属性集满足数据拥有者制定的访问结构，则

$$\begin{aligned} T_1 &= \prod_{i \in I} [e(C_i, L') e(D_i, K'_{\rho(i)})]^{w_i} \\ &= \prod_{i \in I} \left[e(g_2^{a \lambda_i} g_2^{-h_{\rho(i)} r_{\rho(i)}}, g_1^{\frac{t}{z}}) e(g_2^{r_{\rho(i)}}, g_1^{\frac{h_{\rho(i)} t}{z}}) \right]^{w_i} \\ &= e(g_1, g_2)^{\frac{at \sum_{i \in I} \lambda_i w_i}{z}} = e(g_1, g_2)^{\frac{ats}{z}} \end{aligned}$$

若数据使用者选取的关键词都在数据拥有者设置的关键词集合内，则

$$\begin{aligned} T_3 &= C \prod_{i=0}^m e(E_i, F_i) = e(g_1, g_2)^{as} \\ &= \prod_{i=0}^m e(g_2^{s_{id} d_i}, g_1^{\frac{k(H(SKW_1)^i + H(SKW_2)^i + \dots + H(SKW_m)^i)}{u_{id} m^i}}) \\ &= e(g_1, g_2)^{as} e(g_1, g_2)^{\frac{k s_{id} \sum_{i=0}^m \sum_{j=1}^m d_i H(SKW_j)^i}{u_{id} m^i}} \\ &= e(g_1, g_2)^{as} e(g_1, g_2)^{\frac{k s_{id} \sum_{j=1}^m (d_m H(SKW_j)^m + d_{m-1} H(SKW_j)^{m-1} + \dots + d_1 H(SKW_j) + d_0)}{u_{id} m^i}} \\ &= e(g_1, g_2)^{as} e(g_1, g_2)^{\frac{k s_{id} s}{u_{id}}} \\ T_1 T_3 &= e(g_1, g_2)^{\frac{ats}{z}} e(g_1, g_2)^{as} e(g_1, g_2)^{\frac{k s_{id} s}{u_{id}}} \\ T_2 &= (K'', C') = e(g_1^{\frac{a}{z}} g_1^{\frac{k s_{id}}{u_{id}}}, g_2^s) \\ &= e(g_1, g_2)^{as} e(g_1, g_2)^{\frac{ats}{z}} e(g_1, g_2)^{\frac{k s_{id} s}{u_{id}}} \end{aligned}$$

故本方案满足计算一致性。

5 方案分析

5.1 安全性证明

定理 1 若 q -DPBDHE 假设成立，则方案满足索引保密性。

证明 若存在多项式时间敌手 $\mathcal{A}$ 以 ε 优势攻破该方案在选择模型下的 CKA 安全性，则可构造仿真器 Σ 以 $\frac{1}{2}\varepsilon$ 优势攻破 q -DBDHE 假设。

初始化：挑战者 $\mathcal{C}$ 将 q -DBDHE 数组发送给仿真器 Σ ，敌手 $\mathcal{A}$ 将待挑战的访问结构 $(M_{l \times n}^*, \rho^*)$ 提交给 Σ 。

系统建立： Σ 运行 Setup 算法，令 $g_1 = g$ ， $g_2 = g^b$ ，随机选取 $\alpha' \in \mathbb{Z}_p$ ，令 $\alpha = \alpha' + a^{q+1}$ 。计算 $Y = e(g, g^b)^{\alpha'} e(g^a, (g^a)^b)$ 。对于属性 $x \in U$ ， Σ 随机选取 $h_x \in \mathbb{Z}_p$ ，若 $\rho^*(i) = x$ ，令 X 表示所有 $x = \rho^*(i)$ 属性的集合， $h_{1,x} = g^{h_x} \prod_{i \in X, 1 \leq j \leq n^*} g^{a^j M_{i,j}^* / b_i}$ ， $h_{2,x} = (h_{1,x})^b$ ；否则，令 $h_{1,x} = g^{h_x}$ ， $h_{2,x} = g^{b h_x}$ 。 Σ 公布公开参数 PP 。

阶段 1 密钥查询： $\mathcal{A}$ 提交它的属性集，若属性集满足待挑战的访问结构，算法终止；否则 Σ 随机选取密钥 $SK_{id} = u_{id}$ 作为用户的私钥，计算 $PK_{id} = g_1^{u_{id}}$ 作为其公钥，并将公钥添加到公开参数中。选取 $r, z \in \mathbb{Z}_p$ ， $W = (w_1, w_2, \dots, w_{n^*})$ ，其中 $w_1 = -1$ 且 $M_i^* W = 0$ 。令 $t/z = r + w_1 a^q + w_2 a^{q-1} + \dots + w_{n^*} a^{q-n^*+1}$ ，计算 $K' = g^{\alpha'} g^{ar} \prod_{2 \leq i \leq n^*} (g^{a^{q+2-i}})^{w_i}$ ， $L' = g^r \prod_{1 \leq i \leq n^*} (g^{a^{q-i+1}})^{w_i}$ ，对 $\mathcal{A}$ 属性集中的属性 x 计算

$$K'_x = (L')^{h_x} \prod_{i \in X} \prod_{1 \leq j \leq n^*} \left(g^{r_i a^j / b_i} \prod_{1 \leq k \leq n^*, k \neq j} g^{\frac{w_k a^{j-k+q+1}}{b_i}} \right)^{M_{i,j}^*},$$

由于 $M_i^* W = 0$ ， $g^{\frac{a^{q+1}}{b_i}}$ 项可消去。将搜索密钥发送给 $\mathcal{A}$ 。

陷门查询： $\mathcal{A}$ 提交属性集，关键词集合 $SKW = \{SKW_1, SKW_2, \dots, SKW_m\}$ 以及待搜索属性集的数据所有者的公钥。 Σ 运行密钥生成算法，随机选取密钥 $SK_{r_{id}} = r_{id}$ 作为用户的私钥，计算 $PK_{r_{id}} = g_1^{r_{id}}$ 作为其公钥，并将公钥添加到公开参

数中。按照密钥查询阶段方法生成密钥, 随后运行陷门算法, 计算 $K'' = Kg^{\frac{k}{u_{id}}}$, $F = g^{\frac{k}{u_{id}}}$, $F_i = F^{\frac{H(SKW_1)^i + H(SKW_2)^i + \dots + H(SKW_m)^i}{m}}$ 。将生成的陷门发送给 $\mathcal{A}$, 将关键词集合 SKW 添加到列表 L_{SKW} 中。

挑战: $\mathcal{A}$ 将关键词集合 KW_1^* , KW_2^* 提交给 Σ , 要求 L_{SKW} 中没有集合 $(KW_1^* \setminus KW_2^*)$ 或集合 $(KW_2^* \setminus KW_1^*)$ 的子集。 Σ 选取随机值 $rand \in \{0, 1\}$, 随机选取 $y'_2, \dots, y'_{n^*}, r'_1, \dots, r'_{l^*} \in \mathbb{Z}_p$, 令 $v = (s, sa + y'_2, \dots, sa^{n^*-1} + y'_{n^*})$, 计算 $C = T^b e(g^s, g)^{a'b}$, $C' = (g^s)^b$ 。令 R 表示集合 $i \neq k, \rho(i) \neq \rho(k)$, 计算 $D_{\rho^*(i)} = g^{\frac{r'_{\rho^*(i)}}{\rho^*(i)}} (g^{-sb_i})^b$, $C_{\rho^*(i)} = h_{\rho^*(i)}^{br'_{\rho^*(i)}} (\prod_{2 \leq j \leq n^*} (g^a)^{bM^*_{i,j} y'_j}) \cdot (g^{b_i s})^{-bh_{\rho(i)}} (\prod_{k \in R, 1 \leq j \leq n^*} (g^{a^j s (b_i / b_k)})^{bM^*_{k,j}})$, 对关键词集合 $KW_{rand}^* = \{KW_1^*, \dots, KW_m^*\}$, 计算 $f(x) = d(x - H(KW_1^*))(x - H(KW_2^*)) \dots (x - H(KW_m^*)) + s = \sum_{i=0}^m d_i x^i$, $E_0 = (g^s)^{s_{id} b} g^{s_{id} b \prod_{i=1}^m -H(KW_i^*)}$, $E_i = g^{s_{id} d_i b}, 1 \leq i \leq m$ 。将待挑战索引 $Index_{KW_{rand}^*} = \{C, C', \{C_i, D_i\}_{i=1}^l, \{E_j\}_{j=0}^m\}$ 发送给 $\mathcal{A}$ 。

阶段 2 阶段 2 与阶段 1 相同。但在陷门查询过程中, 当提交的属性集合满足 $(M_{l \times n}^*, \rho^*)$ 时, $\mathcal{A}$ 查询的关键词集合不能是集合 $(KW_1^* \setminus KW_2^*)$ 或集合 $(KW_2^* \setminus KW_1^*)$ 的子集。

猜测: $\mathcal{A}$ 输出对随机数 $rand$ 的猜测, 用 $rand'$ 表示猜测的结果。基于 $\mathcal{A}$ 的猜测, Σ 回答 q -DBDHE 问题。若 $rand = rand'$, Σ 回答 $T = e(g, g)^{a^{q+1}s}$; 否则, Σ 回答 T 是随机选取的。

若 $T = e(g, g)^{a^{q+1}s}$, $Index_{KW_{rand}^*}$ 是有效的索引,

$$\Pr \left[\mathcal{B}(\vec{y}, T = e(g, g)^{a^{q+1}s}) = 0 \right] = \frac{1}{2} + \varepsilon。$$

若 $T = R$, $Index_{KW_{rand}^*}$ 是无效的索引,

$$\Pr \left[\mathcal{B}(\vec{y}, T = e(g, g)^{a^{q+1}s}) = 0 \right] = \frac{1}{2}。$$

定理 2 若 DDDH 假设成立, 则方案满足陷门保密性。

证明 若存在多项式时间敌手 $\mathcal{A}$ 以 ε 优势攻破该方案在选择模型下的 IND-KGA 安全性, 则

可构造仿真器 Σ 以 $\frac{1}{2}\varepsilon$ 优势攻破 DDDH 假设。

初始化: 挑战者 $\mathcal{C}$ 将 DDDH 数组发送给仿真器 Σ 。

系统建立: Σ 为用户选取 $u'_{id} \in \mathbb{Z}_p$, 将其私钥设为 $u_{id} = bu'_{id}$, 公钥为 $PK_{id} = (g^b)^{u'_{id}}$ 。

阶段 1 陷门查询: 敌手 $\mathcal{A}$ 将属性集、关键词集合 $SKW = \{SKW_1, SKW_2, \dots, SKW_m\}$, 以及待搜索数据集的数据拥有者公钥 s_{id} 提交给 Σ , Σ 选取随机值 $t, k' \in \mathbb{Z}_p$, $k = bk'$ 计算 $K' = g^a g^{\frac{a't}{z}} (g^b)^{\frac{k' s'_{id}}{u'_{id}}}$, $L' = g^{\frac{t}{z}}$, $K'_x = g^{\frac{t}{z} h_x}$, 对 $0 \leq i \leq m$, 令 $F_i = (g^b)^{\frac{k' \cdot H(SKW_1)^i + H(SKW_2)^i + \dots + H(SKW_m)^i}{u'_{id} m}}$, 将其发送给 $\mathcal{A}$, 并将关键词集合 SKW 添加到列表 L_{SKW} 中。

挑战: $\mathcal{A}$ 将关键词集合 SKW_1^* , SKW_2^* 提交给 Σ , 要求 L_{SKW} 中没有包含关键词集合 SKW_1^* , SKW_2^* 的集合。 Σ 选取随机数 $rand \in \{0, 1\}$, 产生挑战陷门 $Trapdoor_{SKW_{rand}^*}$, 其中 $SKW_{rand}^* = \{SKW_1^*, SKW_2^*, \dots, SKW_m^*\}$ 。 Σ 随机选取 $k' \in \mathbb{Z}_p$, 令 $k = ak'$, 计算 $K' = g^a g^{\frac{a't}{z}} (g^a)^{\frac{k' s'_{id}}{u'_{id}}}$, $L' = g^{\frac{t}{z}}$, $K'_x = g^{\frac{t}{z} h_x}$, 对 $0 \leq i \leq m$, $F_i = T^{\frac{k' \cdot H(SKW_1^*)^i + H(SKW_2^*)^i + \dots + H(SKW_m^*)^i}{u'_{id} m}}$ 。

阶段 2 与阶段 1 相同, 但若 $\mathcal{A}$ 提交的属性集合满足 $(M_{l \times n}^*, \rho^*)$, 则其不能查询 SKW_1 、 SKW_2 对应的陷门。

猜测: $\mathcal{A}$ 输出对随机数 $rand$ 的猜测, 用 $rand'$ 表示猜测的结果。基于 $\mathcal{A}$ 的猜测, Σ 回答 DDDH 问题。若 $rand = rand'$, Σ 回答 $T_1 = g^{\frac{a}{b}}$; 否则, Σ 回答 T 是随机选取的。

若 $T_1 = g^{\frac{a}{b}}$, $Trapdoor_{SKW_{rand}^*}$ 是有效的陷门,

$$\Pr \left[\mathcal{B} \left(\mathbf{y}, T = g^{\frac{a}{b}} \right) = 0 \right] = \frac{1}{2} + \varepsilon。$$

若 $T_1 = R$, $Trapdoor_{SKW_{rand}^*}$ 是无效的陷门,

$$\Pr \left[\mathcal{B} \left(\mathbf{y}, T = g^{\frac{a}{b}} \right) = 0 \right] = \frac{1}{2}。$$

因此, $\mathcal{A}$ 在安全性游戏中的优势是可忽略的。

5.2 理论分析

Sun 等^[3]、林鹏等^[8]、宋衍等^[14]以及 Qiu 等^[10]提出的方案是近年来较为著名的 ABKS 方案，本节从功能和效率方面将本文提出的方案与上述方案进行对比。

功能对比如表 2 所示，本文提出的方案采用的是 LSSS 访问结构，具有较好的表达能力，而文献[3]与文献[10]中的方案采用 AND 访问结构，表达能力较弱；本文方案与文献[14]的方案支持连接关键词搜索，具有较高的灵活性；本文中的方案与文献[10]方案可抵抗外部与内部 KGA，具有较高的安全性。

表 2 功能对比结果

方案	访问结构	连接关键词	外部 KGA	内部 KGA
Sun ^[3]	AND	否	否	否
林鹏 ^[8]	TREE	否	是	否
宋衍 ^[14]	TREE	是	否	否
Qiu ^[10]	AND	否	是	是
O ² ABCSKS	LSSS	是	是	是

效率对比如表 3 所示， E_1, E_2 分别表示群 G, G_T 上的指数运算， H 表示从 Z_p 到群 G 中的散列运算，上述运算的计算复杂度远高于算法中的其他运算，因此算法的复杂度主要考虑上述运算。 N 表示用户属性个数， M_1 表示数据拥有者中选取的关键词数量， M_2 表示数据使用者搜索的关键词数量，若 M_2 大于 M_1 ，则当前搜索的文档必然不满足搜索要求，因此 $M_2 \leq M_1$ 。由于文献[3,8,10]方案仅支持单关键词搜索，为了便于对比搜索算法效率，本文按照多轮搜索方式计算算法复杂度，其中， $A(M_1, M_2) = \frac{M_1!}{(M_1 - M_2)!}$ 为排列组合公式。由于本文采用离线/在线技术，

离线阶段可在设备空闲时执行，故 O²ABCSKS 方案中索引和陷门算法的计算复杂度仅考虑在线阶段的算法复杂度。如表 3 所示，相较于其他方案，本文方案与文献[8]中的方案具有较高的效率，较文献[8]，本文方案也有一定的优势。

5.3 实验评估

本文通过实验对本文提出的算法与文献[14]中的算法进行进一步的性能评估。实验的硬件环境为 Intel Core i5, 2.4 GHz 处理器，操作系统为环境为 64 bit Ubuntu 操作系统。实验基于 Charm 架构，选用 MNT224 椭圆曲线。

图 2 为属性数量对各算法运行时间的影响。在实验中，令属性数量 N 为 1~20，数据拥有者为每个文档选取的关键词数量为 $M_1=5$ 。可以看出，在线索引算法（Index）和搜索算法（Search）的运行时间随着属性数量的增长呈线性增长趋势，在线陷门算法（Trapdoor）的运行时间与属性数量无关。本文中的索引及搜索算法效率较文献[14]中的算法具有一定的优势。

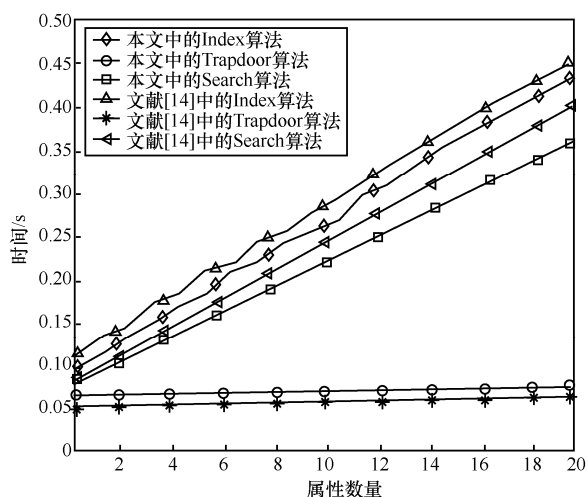


图 2 属性数量对运行时间的影响

表 3 效率对比结果

方案	索引	陷门	搜索
Sun ^[3]	$(NM_1 + 1)E_1 + E_2$	$(2NM_2 + 1)E_1$	$A(M_1, M_2)((N + 2)P + E_2)$
林鹏 ^[8]	$(2N + M_1 + 3)E_1 + (N + M_1)H_1$	$(M_2 + 3N + 4)E_1 + (M_2 + N)H_1$	$A(M_1, M_2)((2N + M_1 + 2)P + E_1 + (2N + M_1 + 1)E_2)$
宋衍 ^[14]	$(2N + M_1 + 3)E_1$	$(M_1 + 1)E_1$	$(2N + M_1 + 3)P + (2N + M_1 + 1)E_2$
Qiu ^[10]	$(2N + M_1)E_1 + 2E_2$	$(M_2 + 2N)E_1$	$A(M_1, M_2)((2N + 1)P + E_2)$
O ² ABCSKS	$(2N + M_1 + 1)E_1$	$(M_1 + 2)E_1$	$(2N + M_1 + 2)P + (N + M_1 + 3)E_2$

图3为关键词数量对各算法运行时间的影响。在实验中,令关键词数量 M_1 为1~20,用户的属性数量为 $N=10$ 。可以看出,在线索引算法,在线陷门算法和搜索算法的运行时间随着属性数量的增长呈线性增长趋势。本文中的索引及搜索算法效率较文献[14]中的算法具有一定的优势。

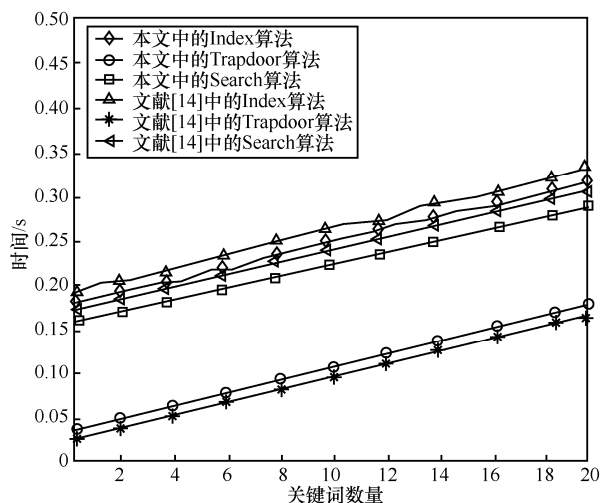


图3 关键词数量对运行时间的影响

6 结束语

本文针对关键词猜测攻击、连接关键词搜索以及效率问题,提出一种适合云存储环境的基于属性的关键词搜索方案,该方案可抵抗内部和外部关键词猜测攻击,采用具有强表达力的 LSSS 访问结构,支持连接关键词搜索,支持在线/离线。理论分析和实验评估表明,本文提出的方案是实用、安全且高效的。下一步将在此方案的基础上,对搜索结果的可验证性以及方案的效率进行研究,使方案更加实用。

参考文献:

- [1] 李经纬, 贾春福, 刘哲理, 等. 可搜索加密技术研究综述[J]. 软件学报, 2015, 26(1):109-128.
LI J W, JIA C F, LIU Z L, et al. Survey on the searchable encryption [J]. Journal of Software, 2015, 26(1): 109-128.
- [2] ZHENG Q, XU S, ATENIESE G. VABKS: verifiable attribute-based keyword search over outsourced encrypted data[C]//IEEE Conference on Computer Communications. 2014: 522-530.
- [3] SUN W, YU S, LOU W, et al. Protecting your right: attribute-based keyword search with fine-grained owner-enforced search authorization in the cloud[C]//IEEE Conference on Computer Communications. 2014: 226-234.
- [4] JIN W B, RHEE H S, PARK H, et al. Off-line keyword guessing attacks on recent keyword search schemes over encrypted data[C]//The Third VLDB Workshop Secure Data Management. 2006: 75-83.
- [5] FANG L, SUSILO W, GE C, et al. Public key encryption with keyword search secure against keyword guessing attacks without random oracle[J]. Information Sciences an International Journal, 2013, 238(7): 221-241.
- [6] WANG C H, TU T Y. Keyword search encryption scheme resistant against keyword-guessing attack by the untrusted server[J]. Journal of Shanghai Jiaotong University (Science), 2014, 19(4): 440-442.
- [7] LI C T, LEE C W, SHEN J J. An extended chaotic maps-based keyword search scheme over encrypted data resist outside and inside keyword guessing attacks in cloud storage services[J]. Nonlinear Dynamics, 2015, 80(3): 1601-1611.
- [8] 林鹏, 江颀, 陈铁明. 云环境下关键词搜索加密算法研究[J]. 通信学报, 2015, 36(s1):259-265.
LIN P, JIANG J, CHEN T M. Application of keyword searchable encryption in cloud[J]. Journal of Communications, 2015, 36 (s1): 259-265.
- [9] CHEN R, MU Y, YANG G, et al. Dual-server public-key encryption with keyword search for secure cloud storage[J]. IEEE Transactions on Information Forensics & Security, 2016, 11(4):789-798.
- [10] QIU S, LIU J, SHI Y, et al. Hidden policy ciphertext-policy attribute-based encryption with keyword search against keyword guessing attack[J]. Science China Information Sciences, 2017, 60(5).
- [11] GOLLE P, STADDON J, WATERS B. Secure conjunctive keyword search over encrypted data[C]//The Second International Conference on Applied Cryptography and Network Security(ACNS 2004). 2004: 31-45.
- [12] ZHANG B, ZHANG F. An efficient public key encryption with conjunctive subset keywords search[J]. Journal of Network & Computer Applications, 2011, 34(1): 262-267.
- [13] YANG Y, MA M. Conjunctive keyword search with designated tester and timing enabled proxy re-encryption function for e-health clouds[J]. IEEE Transactions on Information Forensics & Security, 2016, 11(4):746-759.
- [14] 宋衍, 韩臻, 陈栋, 等. 支持关键词任意连接搜索的属性加密方案[J]. 通信学报, 2016, 37(8):77-85.
SONG Y, HAN Z, CHEN D, et al. Attribute-based encryption supporting arbitrary conjunctive key word search[J]. Journal of Communications, 2016, 37(8):77-85.
- [15] DONG Q, GUAN Z, CHEN Z. Attribute-based keyword search efficiency enhancement via an online/offline approach[C]//The International Conference on Parallel and Distributed Systems. 2015: 298-305.
- [16] HOHENBERGER S, WATERS B. Online/offline attribute-based encryption[C]//Public Key Cryptography (PKC 2014). 2014: 293-310.
- [17] 陈冬冬, 曹珍富, 董晓蕾. 在线/离线密文策略属性基可搜索加密[J]. 计算机研究与发展, 2016, 53(10):2365-2375.
CHEN D D, CAO Z F, DONG X L. Online/offline ciphertext policy attribute-base searchable encryption[J]. Journal of Computer Research and Development, 2016, 53 (10): 2365-2375.
- [18] WATERS B. Ciphertext-policy attribute-based encryption: an expressive, efficient, and provably secure realization[C]//Public Key Cryptography(PKC 2011). 2011: 53-70.
- [19] WU Y, LU X, SU J, et al. An efficient searchable encryption against keyword guessing attacks for sharable electronic medical records in cloud-based system[J]. Journal of Medical Systems, 2016, 40(12): 258.

作者简介：

朱智强（1961-），河南驻马店人，博士，信息工程大学教授，主要研究方向为信息安全。



孙磊（1973-），河南洛阳人，博士，信息工程大学研究员，主要研究方向为信息安全。



苏航（1994-），女，湖北随州人，信息工程大学硕士生，主要研究方向为信息安全。



李作辉（1981-），湖南衡阳人，博士，信息工程大学副研究员，主要研究方向为公钥密码。