云环境下安全的可验证多关键词搜索加密方案

张键红[1,2]，武梦龙[1]，王晶[3,4]，刘沛[3,4]，姜正涛[4]，彭长根[2]

（1. 北方工业大学信息学院，北京 100144；2. 贵州大学公共大数据国家重点实验室，贵州 贵阳 550025；
3. 京东集团财税创新部，北京 100176；4. 中国传媒大学计算机与网络空间安全学院，北京 100024）

摘 要：云计算的高虚拟化与高可扩展性等优势，使个人和企业愿意外包加密数据到云端服务器。然而，加密后的外包数据破坏了数据间的关联性。尽管能够利用可搜索加密（SE）进行加密数据的文件检索，但不可信云服务器可能篡改、删除外包数据或利用已有搜索陷门来获取新插入文件相关信息。此外，现有单关键词搜索由于限制条件较少，导致搜索精度差，造成带宽和计算资源的浪费。为了解决以上问题，提出一种高效的、可验证的多关键词搜索加密方案。所提方案不仅能够支持多关键词搜索，也能实现搜索模式的隐私性和文件的前向安全性。此外，还能实现外包数据的完整性验证。通过严格的安全证明，所提方案在标准模型下被证明是安全的，能够抵抗不可信云服务器的离线关键词猜测攻击（KGA）。最后，通过与最近 3 种方案进行效率和性能比较，实验结果表明所提方案在功能和效率方面具有较好的综合性能。

关键词：云计算；q-ABDHE 安全假设；多关键词搜索；安全证明

中图分类号：TP 309

文献标识码：A

DOI: 10.11959/j.issn.1000−436x.2021054

Secure and verifiable multi-keyword searchable encryption scheme in cloud

ZHANG Jianhong[1,2], WU Menglong[1], WANG Jing[3,4], LIU Pei[3,4], JIANG Zhengtao[4], PENG Changgen[2]

1. School of Information Sciences and Technology, North China University of Technology, Beijing 100144, China
2. Guizhou Provincial Key Laboratory of Public Big Data, Guizhou University, Guiyang 550025, China
3. Finance and Tax Innovation Department of JD Group, Beijing 100176, China
4. School of Computer and Cyber Sciences, Communication University of China, Beijing 100024, China

Abstract: Due to the advantages of cloud computing, such as virtualization and high scalability, individuals and enterprises are willing to outsource local data storage and computing to cloud servers. However, encryption breaks the linkability between the data. Although searchable encryption (SE) enables cloud servers to provide retrieval services of the encrypted data for data owners, cloud servers who are untrusted, may tamper and delete data, or learn information of the newly added encrypted files with previous trapdoors. Besides, single-keyword search inevitably incurs many unrelated results, resulting in a waste of bandwidth and computing resources. To address the problems above, an efficient and verifiable multi-keyword search encryption scheme was proposed, which could not only supported multiple-keyword search, but also realized the privacy of search pattern and forward security of the outsourced files. In the meanwhile, it also ensured the integrity check of the outsourced data. Through rigorous security verification, the proposed scheme was proved to be secure under the standard mode, and could resist offline keyword guesswork attack (KGA) on untrusted cloud serv-

收稿日期：2020−12−09；**修回日期**：2021−02−22

通信作者：武梦龙，wumenglong@126.com

基金项目：北京市自然科学基金资助项目（No.4212019, No.L182039）；广西密码学与信息安全重点实验室研究课题基金资助项目（No.GCIS201808）；贵州省公共大数据重点实验室开放课题基金资助项目（No.2019BDKFJJ012）；国家重点研发计划基金资助项目（No.2018YFB0803900）

Foundation Items: The Natural Science Foundation of Beijing (No.4212019, No.L182039), Guangxi Key Laboratory of Cryptography and Information Security (No.GCIS201808), Foundation of Guizhou Provincial Key Laboratory of Public Big Data (No.2019BDKF JJ012), The National Key Research and Development Program of China (No.2018YFB0803900)

ers. Finally, by comparing the efficiency and performance with the recent three searchable encryption schemes, the experimental results show that the proposed scheme has the best comprehensive performance in terms of function and efficiency among the four schemes.

Keywords: cloud computing, q-ABDHE security assumption, multi-keyword search, security proof

1 引言

作为云计算的一种重要服务[1]，云存储[2]为解决企业和个人的海量数据存储提供了一个途径，使用户能够摆脱沉重的本地数据计算和管理负担。然而，将大量敏感数据（如财务文档、电子医疗记录等）以明文形式存储在远程不可信云服务提供商（CSP, cloud service provider）上，会给用户的数据隐私安全带来潜在隐患。为此，在数据外包给远程服务器之前，数据拥有者需要对数据进行加密。这样能够抵制不可信 CSP 的数据泄露，从而实现外包数据的隐私安全[3-5]。然而，加密却破坏了明文间消息的关联性，给数据的搜索带来极大困难。为了解决这个问题，对称可搜索加密（SSE, symmetric searchable encryption）技术[6]被提出，它允许数据所有者根据指定关键词进行搜索。尽管对称可搜索加密能够实现较高的搜索效率，但是并不能提供公开可验证性。为了解决该问题，Boneh 等[7]提出了基于公钥的可搜索加密方案，该方案是一种单关键词可搜索加密。由于该方案只能对单关键词进行搜索，因此搜索精度不高，还可能会返回一些不相关的结果。为了节省带宽和计算资源，缩小查询范围，可搜索加密（SE, searchable encryption）应该支持多关键词搜索，才能避免返回不必要的加密文件。

Golle 等[8]首次提出了基于连接关键词的可搜索加密方案，在该方案中，关键词的陷门长度与加密文档的数量呈线性关系，使搜索的通信开销过高、实用性较低。为了解决该问题，Ballard 等[9]构造了一种基于双线性映射的多关键词可搜索加密方案，在该方案中，尽管关键词陷门具有固定长度，但是搜索每个文档需要执行 2 次双线性映射运算，使方案的计算耗费巨大。Ryu 等[10]提出了一个高效的、基于双线性映射的多关键词可搜索加密方案，在该方案中，关键词陷门具有固定长度，能够降低计算开销。Cao 等[11]利用内积相似性问题提出了一种可排序的多关键词搜索加密方案。该方案能够对搜索结果进行相关度排序，提高了搜索结果的匹配精度。但每一次搜索请求时，存储服务器都需要遍历所有文档索引，使服务器计算负担较重。

理论上，CSP 应该诚实地根据协议规定来保障外包数据的机密性和完整性。然而，在现实中，为了降低管理负担和计算压力，云服务器可能会返回不正确或不完整的搜索结果。这意味着数据所有者的外包数据可能存储在一个不可信的云服务器上。因此，为了保证搜索结果的正确性，可搜索方案应该提供完整性验证机制[12-14]。同时，为了不削弱云存储的优势，应使结果验证的计算开销尽可能小。为了实现以上功能，Miao 等[15]提出了一种新的高效多关键词可搜索加密方案，该方案不仅能实现多关键词搜索，还能实现密文的完整性验证。尽管该方案被证明是安全的，但是该方案不能抵制搜索模式的隐私泄露。已知 2 个搜索令牌 $T=(T_1,T_2)$和 $T'=(T'_1,T'_2)$，云服务器能够通过判定关系式 $e(T_2,\beta_i g_1^{-T'_1})\stackrel{?}{=}e(\beta_i g_1^{T_1},T'_2)$ 是否成立来确定这 2 次的搜索关键词是否一样。

实现文件的前向安全性和搜索模式的隐私性是搜索加密方案亟须解决的 2 个问题，现有大多数搜索方案都不满足这 2 种特性。前向安全性能够确保云服务器不能了解新插入文件的相关信息，也就是说，云服务器不能利用已有的搜索陷门来测试新插入文件是否包含对应的关键词。搜索模式的隐私性能够确保云服务器不能区分数据用户 2 次提交的搜索陷门是否对应于相同的关键词。这 2 个问题的存在给现有可搜索加密方案带来巨大安全隐患。此外，为了确保云端服务器上外包文件的安全性，应该将公开审计技术[16-17]扩展到 SE 方案中来提升方案的安全性。为了解决以上问题，基于分级身份加密、哈希链技术和带密钥的哈希函数[18-19]，本文在云环境下设计了一种高效的可验证多关键词可搜索加密方案，该方案不仅能实现对多关键词搜索，也能实现对云端密文的完整性验证；此外，还能实现搜索模式的隐私保护和文件的前向安全性。

所提可验证多关键词可搜索加密方案本质上是一种连接关键词搜索。具体而言，本文的主要研究工作可概括如下。

1) 多关键词搜索。本文所提方案允许数据拥有

者对多个关键词进行搜索。

2) 搜索结果的完整性验证。本文所提方案满足搜索结果完整性验证，通过结果验证机制，能够防止 CSP 返回不准确的搜索结果。

3) 标准模型下的安全性。通过形式化安全分析，本文所提方案能够在标准安全模型下被证明是安全的，能够抵制抗密钥猜测攻击（KGA, keyword guesswork attack），安全分析表明，本文所提方案是有效的、安全的。

4) 搜索模式隐私保护。本文所提方案能够阻止云服务器通过搜索陷门来猜测关键词的具体信息。

5) 前向安全性。在本文所提方案中，云服务器不能利用已有陷门信息来测试新插入的密文文件是否包含相应的关键词，但仍能利用更新后的陷门信息对原有密文文件和新插入密文文件进行搜索。

2　云环境下多关键词可搜索加密系统

本节将介绍云环境下多关键可搜索加密的系统模型、威胁模型，然后给出最终的安全设计目标。

2.1　系统模型

一个云环境下的多关键词可搜索加密系统包含云服务器、数据拥有者、用户和审计者 4 类实体。其系统模型如图 1 所示。

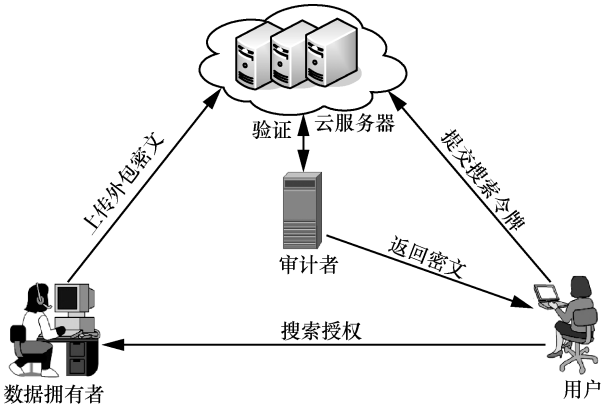

图 1　系统模型

云服务器。云服务器具有丰富的存储空间和强大的计算能力，负责为用户存储数据和执行文件搜索服务。

数据拥有者。数据拥有者希望把数据文件加密后外包到远程云服务器上。

用户。数据使用者需要经数据拥有者授权，并向云服务器提交关键词搜索请求以获取相关文件。

审计者。审计者负责对外包到云服务器的数据进行完整性验证。

2.2　设计目标

为了确保能够对密文进行有效的搜索，本文所提方案的主要目标具体如下。

1) 支持多关键词搜索。为了能够准确地定位相应密文，所提方案应该同时支持多关键词搜索。

2) 抗关键词猜测攻击。当关键词空间较小时，攻击者能够发动关键词猜测攻击，为此，要确保所提方案能够抵制攻击者的猜测攻击。

3) 密文的完整性。确保在不可信云服务器上存储的密文不能被云服务篡改，以确保密文的完整性。

4) 前向安全性。确保不可信云服务器不能通过已有搜索令牌，来获得新插入文件的任何信息。然而，能够利用新的搜索令牌来搜索满足搜索关键词的所有文件。

5) 搜索模式的隐私性。云服务不能通过 2 个搜索令牌来判定所对应的关键词是否一样。

2.3　算法定义

一个多关键词可验证搜索加密方案包括以下几个算法。

Setup(1^k)→(Para)。这是一个确定性算法，输入一个安全参数 k，输出系统公开参数 Para。

KeyGen(Para)→（PK_D,SK_D,PK_C,SK_C）。该算法是一个概率算法，输入系统公开参数 Para，输出数据拥有者的密钥对（PK_D,SK_D）和云服务器的密钥对（PK_C,SK_C）。

Enc(Para,PK_D,SK_D,PK_C,F,W)→ {Sig_F, I_F,π}。该算法是一个概率算法，输入系统公共参数 Para、数据拥有者的密钥对（PK_D,SK_D）、云服务器的公钥 PK_C 以及关键词集 W 和文件集 F，输出签名集 Sig_F、索引集 I_F 和报头 π。

TrapdoorGen(Para,SK_D,W',L)→{T}。该算法是一个概率算法，输入系统参数、数据拥有者的私钥 SK_D 和关键词集 W' 以及关键词的位置信息 L，输出搜索令牌{T}。

Insert(Para,PK_D,SK_D,PK_C,F,W) → {Sig_F,I_F, π}。该算法是一个概率算法，输入公共系统参数 Para、数据拥有者的密钥对（PK_D,SK_D）以及关键词集 W 和新插入的文件集 F，输出签名集 Sig_F、索引集 I_F 和报头 π。

Search(Para,T,L,I_F,SK_C)→(C',FID′)。该算法是一

个概率算法，输入系统参数 Para、云服务器的私钥 SK_C、索引集 I_F、关键词的位置信息 L 和搜索令牌 T，云服务器调用该算法来进行文件匹配，最后，返回满足条件的密文 C'和文件标识 FID。

Verify(Para,C',FID′)→1/0。该算法是一个交互式算法，需要审计者与云服务器执行一个交互过程，与远程数据完整审计方案中的审计过程一样，如果通过验证返回 1；否则，返回 0。

2.4 安全模型

对于一个关键词可搜索加密而言，关键词的空间相对较小，这使许多可搜索加密方案易遭受字典攻击和离线关键词猜测攻击。此外，在一个可搜索加密方案中，由于不可信云服务器拥有密文和搜索陷门信息，它是一个攻击性较强的内部敌手。因而，对于一个可搜索加密方案，如果能够抵抗不可信云服务器的安全攻击，那么该方案就是安全的。下面，给出云服务器关键词猜测攻击的安全模型定义。

定义 1 安全模型。令 k 是一个安全参数，A 是一个多项式时间攻击者，敌手 A 与挑战者$\mathcal{C}$之间的交互游戏定义如下。

系统建立阶段。$\mathcal{C}$输入一个安全参数 k 来调用 Seup 算法和 KeyGen 算法，产生系统公开参数 Para、数据拥有者密钥对（PK_D,SK_D）以及云服务器的密钥对（PK_C,SK_C），发送(Para,PK_D,PK_C,SK_C)给敌手 A。

阶段 1

陷门询问阶段。敌手 A 能够自适应地选择一个关键词集 $\{w_1,\cdots,w_d\}$ 发布陷门询问。$\mathcal{C}$ 调用 TapdoorGen 算法产生陷门（d_0,d_1），并把它返回给敌手 A。

插入询问。敌手 A 能够自适应地选择一个文件 F 和相应的关键集 W 来发起插入询问，$\mathcal{C}$能够利用公共参数 Para 和(PK_D,PK_C)产生一个密文集、索引集和签名集，并把它们返回给敌手 A。

挑战阶段。敌手 A 选择 2 个含有 m 个元素的关键词集(W^*_0,W^*_1)发起挑战。$\mathcal{C}$随机选择一个比特 $b\in\{0,1\}$，并调用 Enc 算法来产生搜索索引 I^*_b。最后，$\mathcal{C}$发送 I^*_b 给敌手 A。

阶段 2

陷门询问阶段。像阶段 1 的挑战阶段一样，敌手 A 能够自适应地选择关键词集$\{w_1,\cdots,w_d\}$发布陷门询问。限制条件为关键词集(W^*_0,W^*_1)不能被发布陷门询问。

猜测阶段。A 返回一个猜测的比特 $b'\in\{0,1\}$。当 $b'=b$ 时，敌手赢得该游戏。敌手 A 能够赢得该游戏的优势定义为 $\mathrm{Adv}_{\mathrm{A}}^{\mathrm{Game}}(1^k)=\Pr[b'=b]-1/2$。

3 具体方案构造

为了方便理解方案的设计，表 1 总结了本文所用符号。

表 1 本文所用符号

符号	描述
F_0	首次外包的文件集
F_i	第 i 次插入的文件集
$F_i=\{F_{i1},\cdots,F_{in}\}$	包含 n 个文件的外包文件集 F_i
$\mathrm{FID}_i=\{\mathrm{FID}_{i1},\cdots,\mathrm{FID}_{in}\}$	文件名称集 FID_i
$C_i=\{C_{i1},\cdots,C_{in}\}$	文件集 F_i 对应的密文集合
$\mathrm{Sig}_i=\{\mathrm{sig}_{i1},\cdots,\mathrm{sig}_{in}\}$	数据拥有者对文件 F_i 的签名集
$I_i=\{I_{i1},\cdots,I_{in}\}$	加密文件的索引集
θ	数据拥有者的哈希密钥

3.1 系统建立阶段（Setup）

输入一个安全参数 k，该阶段调用 setup(1^k)算法输出一组双线对密码参数（G_1,G_2,e,p,g_1,g_2），其中 G_1 和 G_2 是 2 个阶为 p 的乘法循环群，p 是一个大素数，e:$G_1\times G_1\to G_2$ 是一个双线性对映射，g_1 和 g_2 是群 G_1 的 2 个随机生成元。H_1:$\{0,1\}^*\to G_1$，H_2:$\{0,1\}^*\to Z_p$ 和 f:$\{0,1\}^*\to Z_p$ 是 3 个密码哈希函数。然后，随机选择 $r_0\in Z_p$ 和 $h_i\in G_l$（i=0,1,$\cdots$,l），其中 l 表示一个文件所包含关键词的最大个数。最后，系统公开参数被公布为

$$\mathrm{Para}=\{G_1,G_2,e,p,g_1,g_2,f,H_1,H_2,h_0,\cdots,h_l\}$$

3.2 密钥产生（KeyGen）

对于数据拥有者，它随机选择一个数 $d\in Z_p$ 作为密钥，并计算其公钥 $\mathrm{PK_D}=g_1^d$。对于云服务器而言，它也随机选择一个数 $c\in Z_p$ 作为密钥，并计算其公钥

$$\mathrm{PK_C}=g_1^c \tag{1}$$

最后，数据拥有者和云服务器分别保存相应的私钥 SK_D=d 和 SK_C=c。此外，数据拥有者还要选择一个随机数$\theta\in Z_p$ 秘密保存，并且计算一个哈希链（$f_1,f_2,\cdots,f_\chi$），其中 $f_i=f(f_{i-1}(\theta))$ 和 f_0=f(θ)。

3.3 加密和认证标签产生（Enc）

在该阶段，数据拥有者不仅需要对多个关键词加密来建立搜索索引，还需要产生外包文件集 F 的

认证标签。其具体过程如下。

1) 为了方便陈述，假设首次外包文件集 F_0 中包含 n 个文件，并且每个文件都包含 m 个关键词，即 $F_0=\{F_{01},\cdots,F_{0n}\}$，$W=\{w_1,\cdots,w_m\}$。

2) 选择一个安全的对称加密算法 Enc=(E_k,D_k)，并计算文件F_{0j}的密文$C_{0j}=E_k(F_{0j})$，i=1,⋯,n。

3) 随机选择 $s_b\in Z_p$ 计算

$$\mathrm{PK}_s=g_1^{s_b} \tag{2}$$

作为它的签名公钥。接着，对于文件集 F_0 中的所有文件，即对于 $j\in\{1,\cdots,n\}$，计算每个文件 F_{0j} 的认证标签，具体为

$$\mathrm{sig}_{F_{0j}}=(H_1(\mathrm{FID}_{0j})g_2^{H_2(C_{0j})})^{s_b} \tag{3}$$

其中，FID_{0i} 和 C_{0j} 分别表示文件 F_{0j} 的文件标识和相应密文。

4) 在文件集 F_0 中，对于每个文件 F_{0j} 的 m 个关键词 $W=\{w_1,\cdots,w_m\}$，数据拥有者随机选择 2 个数 $x_1,x_2\in Z_p$ 来计算

$$v=e(\mathrm{PK}_\mathrm{D},g_1)^{x_1f_\chi} \tag{4}$$

$$T=\mathrm{PK}_\mathrm{C}^{x_1} \tag{5}$$

$$\pi_0=\mathrm{PK}_\mathrm{D}^{x_2},\pi_1=ve(g_1,h_0)^{x_2},\pi_2=e(g_1,g_1)^{x_2} \tag{6}$$

然后，对于 s=1,⋯,m，数据拥有者计算索引

$$I_s^{F_{0j}}=h_s^{w'_sx_2} \tag{7}$$

其中，$w'_s=H(w_s\|\theta)$。

5) 所产生文件 F_{0j}（j=1,⋯,n）的搜索索引为 $I^{F_{0j}}=(I_1^{F_{0j}},\cdots,I_m^{F_{0j}})$。

6) 数据拥有者上传文件集 F_0 的密文 $(C_0,T,\mathrm{PK}_s,\{\mathrm{sig}_{F_{0j}},I^{F_{0j}}\}_{j=1,\cdots,n},\pi_0,\pi_1,\pi_2)$ 到云端服务器，其中 $C_0=\{C_{01},\cdots,C_{0n}\}$表示文件集 F_0 中对应文件的密文集合。

3.4　文件插入（Insert）

令 F_i 表示第 i 次插入的文件集，为了表述方便，不妨设该文件集也包括 n 个文件，并且每个文件都包含 m 个关键词，即 $F_i=\{F_{i1},\cdots,F_{in}\}$，$W=\{w_1,\cdots,w_m\}$。为了插入该文件集，数据拥有者计算如下。

1) 利用安全对称加密算法 Enc=(E_k,D_k)来计算文件 F_{ij} 的密文 $C_{ij}=E_k(F_{ij})$，i=1,⋯,n。

2) 然后，随机选择 $s_b\in Z_p$ 计算

$$\mathrm{PK}_s=g_1^{s_b} \tag{8}$$

作为签名公钥。接着，对于文件集 F_i 中的文件，即对于 j=1,⋯,n，计算每个文件 F_{ij} 的认证标签

$$\mathrm{sig}_{F_{ij}}=(H_1(\mathrm{FID}_{ij})g_2^{H_2(C_{ij})})^{s_b} \tag{9}$$

其中，FID_{ij} 和 C_{ij} 分别表示文件 F_{ij} 的文件标识和相应密文。

3) 在文件集 F_i 中，对于文件 F_{ij} 的 m 个关键词 $W=\{w_1,\cdots,w_m\}$，数据拥有者随机选择 2 个数 $x_1,x_2\in Z_p$ 来计算

$$v=e(\mathrm{PK}_\mathrm{D},g_1)^{x_1f_{\chi-i}} \tag{10}$$

$$T=\mathrm{PK}_\mathrm{C}^{x_1} \tag{11}$$

$$\pi_0=\mathrm{PK}_\mathrm{D}^{x_2},\pi_1=ve(g_1,h_0)^{x_2},\pi_2=e(g_1,g_1)^{x_2} \tag{12}$$

其中，$f_{\chi-i}$ 表示第 i 次文件集插入时所使用哈希链中的第$\chi-i$ 个哈希值。

接着，对于 s=1,⋯,m，数据拥有者计算

$$I_s^{F_{ij}}=h_s^{w'_sx_2} \tag{13}$$

其中，$w'_s=H(w_s\|\theta)$。

4) 所产生文件 F_{ij} (j=1,⋯,n)的搜索索引为

$$I^{F_{ij}}=(I_1^{F_{ij}},\cdots,I_m^{F_{ij}})$$

5) 数据拥有者上传文件集 F_i 的密文 $(C_i,T,\mathrm{PK}_s,\{\mathrm{sig}_{F_{ij}},I^{F_{ij}}\}_{j=1,\cdots,n},\pi_0,\pi_1,\pi_2)$ 到云端服务器，其中 $C_i=\{C_{i1},\cdots,C_{in}\}$表示对应文件集 F_i 中文件的密文集合。

3.5　陷门产生阶段（TrapdoorGen）

当一个数据用户想访问含有关键词集 $\overline{W}=\{\overline{w}_1,\cdots,\overline{w}_\lambda\}$ 的文件时，其中 $\overline{W}\subseteq W$，数据拥有者需要为其进行授权，具体计算如下。

1) 随机选择$\gamma_1\in Z_p$ 计算

$$d_0=\left(h_0g_1^{-r_0}\right)^{\frac{1}{d}}\left(\prod_{k=1}^{\lambda}h_k^{\overline{w}'}\right)^{\gamma_1} \tag{14}$$

$$d_1=\mathrm{PK}_\mathrm{D}^{\gamma_1} \tag{15}$$

其中，$\overline{w}'_i=H(\overline{w}_i\|\theta)$，$r_0$ 是 Z_p 中的一个随机数。注，为了降低通信费用，令 $r_0=H_2(d_1)$。

2) 所产生的关键词集 $\overline{W}=\{\overline{w}_1,\cdots,\overline{w}_l\}$ 的搜索令牌就是 $T=(d_0,d_1,f_{\chi-i})$。

3) 把 $T=(d_0,d_1,f_{\chi-i})$及相应关键词的位置信息集 $L=\{L_1,\cdots,L_l\}$发送给云服务器，其中 L_i 表示关键词 $\overline{w}_i$ 在关键词集合 W 中的位置。

3.6　搜索阶段（Search）

当接收到用户提交的搜索令牌 $T=(d_0,d_1,f_{\chi-i})$和位置信息 L 后，云服务器执行搜索算法，如算法 1 所示，其具体步骤如下。

算法 1 搜索算法

输入 搜索令牌 $T=(d_0,d_1,f_{\chi-i})$ 、位置信息 L 和所有文件集密文 $(C,T,\mathrm{PK}_s,\{\mathrm{sig}_{F_i},I_{F_i}\}_{i=1,\cdots,n},\pi_0,\pi_1,\pi_2)$

输出 密文集合 $C'=\{C'_1,\cdots,C'_t\}$ 和文件名称集 $\mathrm{FID}=\{\mathrm{FID}'_1,\cdots,\mathrm{FID}'_t\}$

1) do //对最新加入的文件集 F_i 进行搜索
2) $t=f_{\chi-i}$
3) $v'=e(T,\mathrm{PK}_\mathrm{D})^{c^{-1}t}$
4) for j=1 to n do
5) if $\left(\pi_1\dfrac{e\left(d_1,\prod_{k=1}^{\lambda}I_k^{F_{ij}}\right)\pi_2^{-r_0}}{e(\pi_0,d_0)}==v'\right)$ //判断是否满足搜索令牌
6) then
7) $C=C\cup\{C'_{ij}\}$
8) $\mathrm{FID}=\mathrm{FID}\cup\{\mathrm{FID}'_i\}$
9) end if
10) end for
11) i—;
12) $f_{\chi-i}=f(t)$;
13) while (i==0)
14) return C and FID

首先，令 $t=f_{\chi-i}$ 并计算

$$v'=e(T,\mathrm{PK}_\mathrm{D})^{c^{-1}t} \tag{16}$$

然后，利用搜索令牌 T 和位置信息 L 对所有的搜索索引 $\{I_{F_i}\}$ 进行以下匹配

$$\pi_1\frac{e\left(d_1,\prod_{k=1}^{\lambda}I_k^{F_{ij}}\right)\pi_2^{-r_0}}{e(\pi_0,d_0)}=v' \tag{17}$$

接着，计算 $t=f(f_{\chi-i})$，依次循环执行算法 1 的步骤 1)～步骤 11)，直到 i 次。其目的是对第 i 次文件集插入前的文件进行搜索。

最后，把满足式(17)的所有密文集合 $C'=\{C'_1,\cdots,C'_t\}$ 以及对应文件的文件名称标识集 $\mathrm{FID}=\{\mathrm{FID}'_1,\cdots,\mathrm{FID}'_t\}$（$1\leqslant t\leqslant n$）返回给一个审计者。

3.7 验证阶段（Verify）

该阶段的目的是验证外包在云端的密文是否被云服务器篡改。为此，审计者需要与云服务器执行一个交互过程，具体步骤如下。

1) 首先，审计者选择一组随机数 $\{y_1,\cdots,y_d\}$，其中 $y_i\in Z_p$，并且将它们发送给云服务器。

2) 云服务器根据标识集 $\mathrm{FID}=\{\mathrm{FID}'_1,\cdots,\mathrm{FID}'_d\}$ 和随机数集 $\{y_1,\cdots,y_d\}$ 产生一个证明信息 ψ 为

$$\psi=\prod_{i=1}^{t}\mathrm{sig}_i^{y_i} \tag{18}$$

然后，将证明信息 ψ 发送给审计者。

3) 当审计者接收 ψ 以后，首先，计算

$$\rho=\sum_{i=1}^{t}y_iH_2(C'_i) \tag{19}$$

然后，验证

$$e(\psi,g_1)=e\left(\prod_{i=1}^{t}H_1(\mathrm{FID}'_i)^{y_i}g_2^{\rho},\mathrm{PK}_s\right) \tag{20}$$

如果式(20)成立，那么，它就发送密文 $C'=\{C'_1,\cdots,C'_d\}$ 给用户。

4 安全性分析

本节将对本文所提方案的正确性和安全性进行分析。为了方便理解，首先，回顾一下本文方案所基于的数学难题——基于截断决定性双线性 Diffie-Hellman 安全假设（truncated decisional q-augmented bilinear Difffie-Hellman exponent (q-ABDHE) problem）[19]。已知一组元素 $(g_1,g'_1\in G_1,g_1^{\alpha^{q+2}},g_1^{\alpha},\cdots,g_1^{\alpha^q},Z\in G_2)$，判断关系式 $Z=e(g_1,g'_1)^{\alpha^{q+1}}$ 是否成立是一个困难问题。

正确性 对于整个协议，如果每个实体都能按照协议规定正确地执行协议，那么，式(17)和式(20)一定成立。这就意味着，授权用户一定能获取满足关键词的相应密文。

因为对于式(17)，依据算法 1 可知

$$\pi_1\frac{e\left(d_1,\prod_{k=1}^{\lambda}I_k^{F_{ij}}\right)\pi_2^{-r_0}}{e(\pi_0,d_0)}=$$

$$ve(g_1,h_0)^{x_2}\frac{e\left(\mathrm{PK}_\mathrm{D}^{\gamma_1},\prod_{k=1}^{\lambda}I_k^{F_{ij}}\right)e(g_1,g_1)^{-r_0x_2}}{e\left(\pi_0,(h_0g_1^{-r_0})^{\frac{1}{d}}\left(\prod_{k=1}^{\lambda}h_k^{\overline{w}'}\right)^{\gamma_1}\right)}=$$

$$ve(g_1,h_0)^{x_2}\frac{e(g_1,g_1)^{-r_0x_2}}{e\left(\pi_0,(h_0g^{-r_0})^{\frac{1}{d}}\right)}=v=e(T,\mathrm{PK}_\mathrm{D})^{c^{-1}t}$$

因此，当式(17)成立时，这就意味着有效的搜索令牌一定能匹配到满足条件的密文文件。

对于式(20)，依据算法 1 可知

$$e(\psi,g_1)=e\left(\prod_{j=1}^{t}\mathrm{sig}_{ij}^{y_j},g_1\right)=e\left(\prod_{j=1}^{t}(H_1(\mathrm{FID}_{ij})g_2^{H_2(C_{ij})})^{s_by_j},g_1\right)=$$

$$e\left(\prod_{j=1}^{t}(H_1(\mathrm{FID}_{ij}))^{y_j}g_2^{\sum_{j=1}^{t}y_jH_2(C_{ij})},\mathrm{PK}_s\right)=e\left(\prod_{j=1}^{t}H_1(\mathrm{FID}_{ij})^{y_j}g_2^{\rho},\mathrm{PK}_s\right)$$

这意味着，如果所返回的密文没有被篡改，那么，式(20)一定成立。

定理 1　在 q-ABDHE 假设下，本文所提方案能够安全地抵制 KGA。

证明　假设存在一个 PPT 敌手 A 能够以不可忽略的概率击破本文所提方案，那么，本文就能够构造一个多项式算法 B 来求解 q-ABDHE 问题。首先，回顾一下 q-ABDHE 问题。已知一个 q+4 元组 $(g_1', g_1'^{q+2}, g_1, g_1^{\alpha}, \cdots, g_1^{\alpha^q}, Z)$，其中 $g_1, g_1' \in G_1$ 且 $Z \in G_2$ 或者 $Z=e(g_1, g_1')^{\alpha^{q+1}}$，该问题的目的是判断 $Z \in_{\mathrm{R}} G_2$ 还是 $Z=e(g_1, g_1')^{\alpha^{q+1}}$。

为了求解 q-ABDHE 问题，敌手 A 与挑战者$\mathcal{C}$需要执行一个交互游戏，具体如下。

系统建立。挑战者$\mathcal{C}$随机产生一个次数为 q 并且满足 $f(0)\neq 0$ 的多项式 $f(x)$。然后，计算一个多项式 $g(x)=\dfrac{f(x)-f(0)}{x}$，使

$$\mathrm{PK}_{\mathrm{D}}=g_1^{\alpha}, h_0=g_1^{f(\alpha)}, r_0=f(0), h_i=g_1^{\alpha a_i}(i=1,\cdots,l)$$

其中，a_i是一个随机数。同时选择一个$\theta\in Z_p$作为一个哈希密钥并且产生一个哈希链$(f_1, f_2, \cdots, f_\chi)$。接着，选择一个随机数 $c\in Z_p$来设置它的公钥为

$$\mathrm{PK}_{\mathrm{C}}=g_1^{c}$$

阶段 1

陷门询问。当敌手 A 选择一组关键词 $\overline{W}=\{\overline{w}_1, \cdots, \overline{w}_\lambda\}$ 请求陷门询问时，挑战者$\mathcal{C}$计算如下。

1) 对于 i=1,⋯,λ, 挑战者$\mathcal{C}$计算 $w_i'=H_2(\overline{w}_i \| \theta)$。

2) 选择一个 $\gamma_1 \in Z_p$ 来计算

$$d_0=g_1^{g(\alpha)}\left(\prod_{k=1}^{\lambda} h_k^{w_k'}\right)^{\gamma_1}$$

$$d_1=\mathrm{PK}_{\mathrm{C}}^{\gamma_1}$$

并返回（d_0,d_1,$f_{\chi-i}$）给敌手 A。显然，（d_0,d_1,$f_{\chi-i}$）是一个有效的陷门，因为

$$d_0=g_1^{g(\alpha)}\left(\prod_{k=1}^{\lambda} h_k^{w_k'}\right)^{\gamma_1}=g_1^{\frac{f(\alpha)-f(0)}{\alpha}}\left(\prod_{k=1}^{\lambda} h_k^{w_k'}\right)^{\gamma_1}=$$

$$(h_0 g_1^{-r_0})^{\frac{1}{\alpha}}\left(\prod_{k=1}^{\lambda} h_k^{w_k'}\right)^{\gamma_1}$$

$$d_1=\mathrm{PK}_{\mathrm{C}}^{\gamma_1}$$

$$r_0=f(0)$$

插入询问。当敌手用一个含有 n 个文件集 F 和关键词集 W 进行文件插入询问时，$\mathcal{C}$执行 3.4 节中的文件插入算法来得到以下密文

$$(C_i, T, \mathrm{PK}_s, \pi_0, \pi_1, \pi_2, \{\mathrm{sig}_{F_{ij}}, I^{F_{ij}}\}_{j=1,\cdots,n})$$

并将该密文返回给敌手。

挑战阶段。敌手 A 随机选择 2 个关键词个数都是 l 的关键词集（$\overline{W}_0^*$，$\overline{W}_1^*$），然后，挑战者$\mathcal{C}$调用算法 B 随机选择一个比特 $b\in\{0,1\}$来产生搜索索引，具体过程如下。

1) 令 $s=\log_{g_1} g_1'^{\alpha^{q+1}}$。

2) 对于 i=1,⋯,λ，计算 $I_i^*=(g_1'^{\alpha^{q+2}})^{a_i \overline{w}_{bi}'}$，其中 $w_{bi}' \in \overline{W}_b^*$ 且 $\overline{w}_{bi}'=H_2(w_{bi}' \| \theta)$。设置 $I_F^*=\{I_i^*\}_{i=1,\cdots,\lambda}$。

3) 选择一个随机数 $x_1\in Z_p$ 计算

$$T^*=\mathrm{PK}_{\mathrm{C}}^{x_1}$$

$$\pi_0^*=g_1'^{\alpha^{q+2}}$$

$$\pi_1^*=v^* \frac{e(\pi_0^*, d_0^*)}{e\left(d_1^*, \prod_{k=1}^{\lambda} I_k^*\right)\pi_2^{*-r_0}}$$

$$\pi_2^*=Z$$

其中，$v^*=e(\mathrm{PK}_{\mathrm{D}}, g_1)^{x_1 f_\chi}$。

4) 选择一个随机数 $s_b\in Z_p$ 来计算

$$\mathrm{PK}_s=g_2^{s_b}$$

并将其作为签名公钥。接着，对于 i=1,⋯,n，计算每个文件 F_i 的认证标签为

$$\mathrm{sig}_{F_i}=\left(H_1(\mathrm{FID}_i) g_2^{H_2(C_i)}\right)^{s_b}$$

其中，FID_i 表示文件 F_i 的名称，然后，设置 $\mathrm{sig}_F=\{\mathrm{sig}_{F_i}\}_{i=1,\cdots,n}$。

5) （$T^*, \mathrm{PK}_s, \mathrm{sig}_F, I_F^*, \pi_0^*, \pi_1^*, \pi_2^*$）就是所产生挑战元组，并把它返回给敌手。注：密文 C 能够被删除，且不影响方案的安全分析。

阶段 2

敌手 A 仍然可以像阶段 1 的陷门询问阶段一样发布陷门询问。唯一的限制条件是挑战关键词集 $(\overline{W}_0^*, \overline{W}_1^*)$ 不能被用来发起陷门询问。

猜测阶段。在该阶段，敌手 A 输出一个猜测的比特 $b'\in\{0,1\}$。当满足 $b'=b$ 时，敌手赢得该游戏。如果 $\Pr(b'=b)=\xi>1/2$，挑战者$\mathcal{C}$能够利用算法 B 能够以至少 $\xi'=\xi-1/2$ 的优势来求解 q-ABDHE 问题。

当 $Z=e(g_1, g_1')^{\alpha^{q+1}}$ 时，有

$$I_i^*=(g_1'^{\alpha^{q+2}})^{a_i \overline{w}_{bi}'}=(g_1^{\alpha a_i})^{s \overline{w}_{bi}'}=h_i^{s \overline{w}_{bi}'}$$

$$T^*=\mathrm{PK}_{\mathrm{C}}^{x_1}$$

$$\pi_0^*=g_1'^{\alpha^{q+2}}=g_1^{s\alpha}=\mathrm{PK}_\mathrm{D}^s$$

$$\pi_1^*=v^*\frac{e(\pi_0^*,d_0^*)}{e\left(d_1^*,\prod_{k=1}^{\lambda}I_k^*\right)\pi_2^{*-r_0}}$$

$$\pi_2^*=Z=(g_1,g_1')^{\alpha^{q+1}}=e(g_1,g_1)^s$$

成立。其中，$s=\log_{g_1}g_1'\alpha^{q+1}$，显然$(T^*,\mathrm{PK}_s,\mathrm{sig}_F,I_F^*,\pi_0^*,\pi_1^*,\pi_2^*)$是一个有效密文。

定理 2 本文所提方案能够实现搜索模式的隐私保护，也就是说，不可信云服务器不能通过搜索令牌来猜测出与之对应的关键词。

证明 在搜索阶段，云服务器接收到搜索令牌$T=(d_0,d_1,f_{\chi-i})$，其中满足$d_0=(h_0g_1^{-r_0})^{\frac{1}{\bar{d}}}\left(\prod_{k=1}^{\lambda}h_k^{\bar{w}'}\right)^{\gamma_1}$，$d_1=\mathrm{PK}_\mathrm{D}^{\gamma_1}$，然而，$\bar{w}_i'=H(\bar{w}_i\|\theta)$是一个带密钥的哈希函数。由于哈希函数的密钥$\theta$未知，对于任意一个关键词$\bar{w}_i$，云服务器不可能获得该关键词的哈希值$\bar{w}_i'=H(\bar{w}_i\|\theta)$，因而，云服务器不能通过验证

$$e(\mathrm{PK}_\mathrm{D},d_0)=e(h_0g_1^{-r_0},g_1)e\left(\prod_{k=1}^{\lambda}h_k^{\bar{w}'},d_1\right) \quad (21)$$

来猜测出与之对应的关键词。因此，本文所提方案能够实现搜索模式的隐私保护。证毕。

定理 3 在离散对数安全假设下，不可信服务器不能在外包密文被篡改情况下，产生一个证明信息 Prof，使其通过审计者的验证。

证明 因为本文中采用的完整性验证方案是基于 Shacham 和 Waters 的远程数据完整验证方案[12]。而该方案在安全模型下被证明是安全抵制云服务器的篡改和删除攻击，因而，本文所提方案也能够抵制相应攻击。

定理 4 在哈希函数的单向性条件下，本文所提方案能够实现前向安全性。

证明 在本文所提方案中，采用哈希链来实现文件的前向安全性。在第 i 次文件插入时，哈希链中的哈希值$f_{\chi-i}$被嵌入文件密文中，即

$$v=e(\mathrm{PK}_\mathrm{D},g_1)^{x_1f_{\chi-i}}$$

当第 i 次文件被插入以后，用户的搜索令牌是$T=(d_0,d_1,f_{\chi-i})$，其中嵌入了哈希链中的$f_{\chi-i}$哈希值，这使云服务器仅能搜索第 i 次插入文件集。为了实现对第 i 次插入前的文件进行搜索，云服务器需要计算

$$f_{\chi-i+1}=f(f_{\chi-i})$$

然后，利用$T=(d_0,d_1,f_{\chi-i+1})$来搜索第 $i-1$ 次插入的文件集。依次类推，云服务器能够搜索第 i 次前所有满足关键词集的所有文件。

然而，对于云服务器，尽管它拥有第 i 次文件插入前的搜索令牌，例如，第 $i-1$ 次文件插入后的搜索令牌为$T=(d_0,d_1,f_{\chi-i+1})$，它仍然不能利用$(d_0,d_1,f_{\chi-i+1})$来对新插入的文件进行搜索，因为新插入文件的密文中嵌入了哈希值$f_{\chi-i}$，由于哈希函数f的单向性，云服务器不能通过哈希值$f_{\chi-i+1}$来获得$f_{\chi-i}$。因而，它不能通过式(21)来判断搜索令牌是否匹配新插入的文件，从而实现了方案的前向安全性。

5 效率分析

本节将从理论角度来对所提方案的效率和功能进行分析。为了更好地说明本文所提方案的性能，本节将通过与 3 种多关键词搜索加密方案[13-15]比较来分析本文所提方案性能。为了简化分析，在下文的分析中，仅考虑耗时的密码运算。令 E 表示在群 G_1 或 G_2 中的指数运算，M 表示乘法运算，P 表示对运算，H_1 表示一个比特串映射到群 G_1 中元素的 map2point 运算。表 3 给出了本文所提方案与文献[13-15]方案的效率比较，其中，n 表示文件的

表 3 几种方案的效率比较

算法	文献[13]方案	文献[14]方案	文献[15]方案	本文所提方案
KeyGen	4E	3E	2E	2E
Enc	$(2m+1)n$E+mnP	$(m+5)n$E+$2n$P	$(mn+5n+2n)$E+$n\mathrm{H}_1$+3P	$(mn+5n+2n)$E+$n\mathrm{H}_1$+2P
Trapdoor	$(2l+2)$E+H_1	$(l+3)$E	2E	$(l+3)$E
Search	$(l+1)$E+H_1+lP	$(l+4)$E+(l+2)P	2P+3E+lM	2P+2E+lM
Verify	—	—	$(d+1)$E+$d\mathrm{H}_1$+2P	$(d+1)$E+$d\mathrm{H}_1$+2P
security	yes	yes	no	yes
search model	leak	leak	leak	anonymity
forward security	no	no	no	yes

个数，m 表示关键词集中的元素个数，l 表示所询问的关键词个数，d 表示返回的搜索结果，“—”表示不具有该功能，search model 表示搜索模式是否满足隐私性，leak 表示不满足，anonymity 表示满足。forward security 表示方案是否满足前向安全性。

从表 3 可知，就算法 KeyGen、Trapdoor 和 Search 而言，与其他 2 种方案相比，本文所提方案和文献[15]方案具有更小的计算开销。就 Enc 算法而言，本文所提方案是所有方案中计算量最小的方案，这是因为在本文所提方案中最耗时的对运算独立于文件和关键词个数，对运算不会随着关键词的数量和文件的数量的增加而增多。同时，从表 3 中可以发现，本文所提方案和文献[15]方案在效率上基本一致。在陷门产生阶段，本文所提方案比文献[15]方案需要较多的计算量。然而，本文所提方案能够实现搜索模式的隐私保护，具体原因在定理 2 中被分析。但是文献[15]方案不能实现搜索模式的隐私保护，因为在文献[15]方案中，搜索令牌 $T=(T_1,T_2)$ 具有如下形式

$$T_1=\theta$$

$$T_2=(\beta_i g_1^{-\theta})^{\frac{1}{b_i-\sum_{k=1}^{l} w_k'}}$$

因此，对于 2 个搜索令牌 $T=(T_1,T_2)$ 和 $T'=(T'_1,T'_2)$，如果它们包含同一组关键词集 $(w_1',\cdots,w_k')$，那么，云服务器可以通过验证

$$e(\beta_i g_1^{-T_1},T_2')=e(\beta_i g_1^{-T_1'},T_1) \tag{22}$$

来判定这 2 个搜索令牌 T 和 T' 是否包含同样的关键词。从而泄露了搜索模式的相关统计信息。此外，文献[15]方案也不能抵制恶意云服务器的离线猜测攻击，对于含有 n 个元素的关键词集，云服务器能够以概率 $1/C_n^k$ 猜测出相应的关键词集。当关键词空间相对较小、搜索关键词个数较多时，云服务器能够以较大概率猜测出关键词。此外，文献[15]方案不支持文件的前向安全性，这使云服务能够利用已有的搜索令牌来搜索新插入文件是否包含相应关键词，从而泄露新插入文件的相关信息。

本文所提方案通过引入一个带密钥的哈希函数来有效地抵制恶意云服务器的离线关键词猜测攻击，因为云服务器不知道密钥 θ，使它不可能产生一个 $\vec{w}_i'=H(\vec{w}_i\|\theta)$，所以能够阻止云服务器的离线关键词猜测攻击。此外，为了实现前向安全性，本文所提方案采用一个哈希链，然后借助哈希链的单向性来实现本文所提方案的前向安全性。

综上所述，本文所提方案在陷门产生阶段尽管计算量比文献[15]方案大，但也优于文献[13-14]方案，并且所增加的计算量是由计算力丰富的云服务器完成的，而没有增加用户的任何计算负担。此外，就方案的功能而言，本文所提方案不仅能实现搜索模式的隐私保护和文件前向安全性，还能抵制云服务器的离线关键词猜测攻击。而文献[15]方案不能实现搜索模式的隐私性和插入文件的前向安全性，也不能抵制云服务器的离线关键词猜测攻击。通过牺牲一点计算代价换取方案的功能增强和安全性增强是值得的。这就意味着，本文所提方案就综合性能而言是 4 种方案中最好的。

6　实验分析

为了评估本文所提方案的实际性能，本文实验在一台 1.5 GHz 主频、Broadcom BCM2711 处理器、2 GB 内存、Raspbian 操作系统的树莓派上进行。每个算法运行 100 次，最后，通过取平均数来得到以下所有实验数据。

在加密阶段，4 种方案的计算开销与关键词个数和文件个数呈线性相关，如图 2 和图 3 所示。同时，由图 2 和图 3 可知，本文所提方案与文献[15]方案对应的直线斜率都低于文献[13-14]方案所对应的直线斜率，这意味着本文所提方案和文献[15]方案在计算开销上优于文献[13-14]方案。

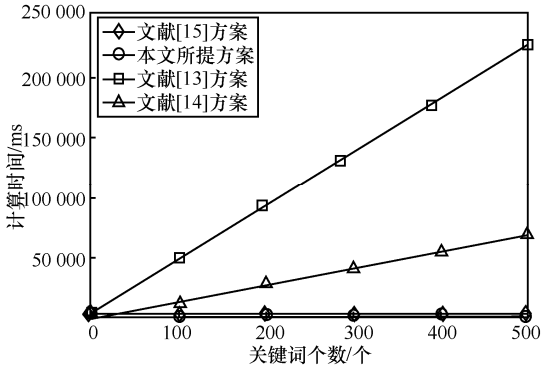

图 2　n=2 000 时加密阶段的计算开销

在陷门产生阶段，本文所提方案与文献[13-15]方案都与关键词的个数呈线性关系，如图 4 所示。由于在文献[15]方案中，所有关键词只是进行加法

运算，而加法的计算开销几乎可以忽略，所以在图 4 中，文献[15]方案的计算量几乎呈一条水平直线。尽管在陷门产生阶段，本文所提方案的计算开销劣于文献[15]方案的计算开销，但本文所提方案仍优于文献[13-14]方案。

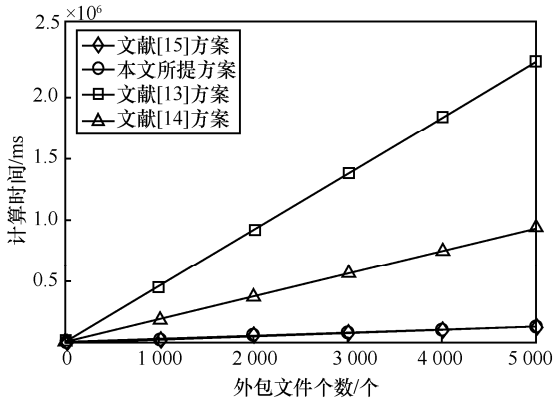

图 3　m=200 时加密阶段的计算开销

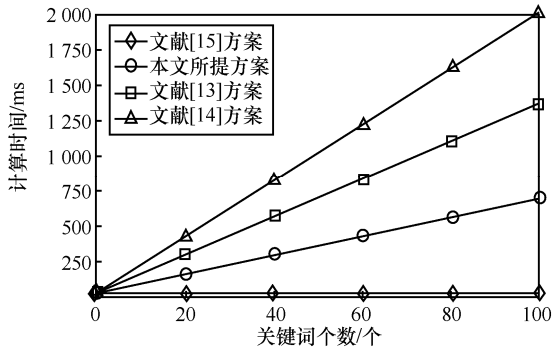

图 4　陷门产生阶段的计算开销

在搜索阶段，本质上，本文所提方案与文献[13-15]方案的计算开销都与关键词个数呈线性关系，如图 5 所示。

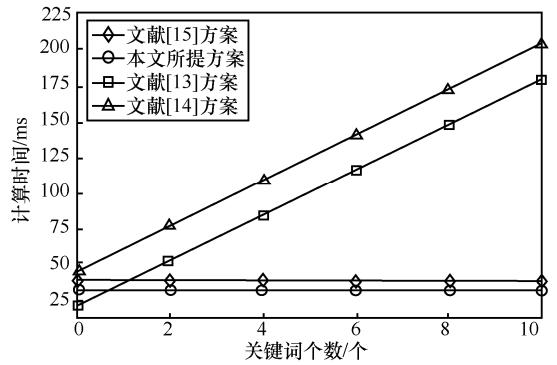

图 5　搜索阶段的计算开销

然而，在文献[15]方案和本文所提方案中，与关键词数量相关的运算只有乘法运算，而乘法运算具有较低的计算开销，因此，在图 5 中，文献[15]方案和本文所提方案几乎呈一条水平直线。同时，由图 5 可知，本文所提方案的计算效率也优于文献[13-15]方案。

7　结束语

本文提出了一种新的可验证多关键词可搜索加密方案，它既能支持密文的完整性验证，又能支持多关键词搜索，同时，还支持文件的前向安全性和搜索模式的隐私保护。与以往的可搜索加密方案相比，本文所提方案能够在标准模型下被证明是安全的，且能够抵制不可信云服务器的离线猜测攻击，并且该方案是一种基于公钥环境下支持文件前向安全的可搜索加密方案。在未来的研究工作中，将探索设计有效地支持更丰富语义表达的密文搜索方案。

参考文献：

[1] AMBRUST M, FOX A, JOSEPH A D, et al. Above the clouds: a berkeley view of cloud computing[R]. California: University of California, UCB/EECS-2009-28, 2009.

[2] MELL P M, GRANCE T. The NIST definition of cloud computing[R]. National Institute of Standards and Technology, 2011.

[3] JULISCH K, HALL M. Security and control in the cloud[J]. Information Security Journal: A Global Perspective, 2010, 19(6): 299-309.

[4] 冯登国, 张敏, 张妍, 等. 云计算安全研究[J]. 软件学报, 2011, 22(1): 71-83.
FENG D G, ZHANG M, ZHANG Y, et al. Study on cloud computing security[J]. Journal of Software, 2011, 22(1): 71-83.

[5] TANG Y, LEE P P C, LUI J C S, et al. Secure overlay cloud storage with access control and assured deletion[J]. IEEE Transactions on Dependable and Secure Computing, 2012, 9(6): 903-916.

[6] SONG D X, WAGNER D, PERRIG A. Practical techniques for searches on encrypted data[C]//Proceeding 2000 IEEE Symposium on Security and Privacy. Piscataway: IEEE Press, 2000: 44-55.

[7] BONEH D, CRESCENZO G, OSTROVSKY R, et al. Public key encryption with keyword search[C]//International Conference on the Theory and Applications of Cryptographic Techniques. Berlin: Springer, 2004: 506-522.

[8] GOLLE P, STADDON J, WATERS B. Secure conjunctive keyword search over encrypted data[C]//Proceedings of the 2nd International Conference on Applied Cryptography and Network Security. Berlin: Springer, 2004: 31-45.

[9] BALLARD L, KAMARA S, MONROSE F. Achieving efficient conjunctive keyword searches over encrypted data[C]//Proceedings of the 7th International Conference on Information and Communications Security. Berlin: Springer, 2005:414-426

[10] RYU E K, TAKAGI T. Efficient conjunctive keyword-searchable

encryption[C]//Proceedings of 21st International Conference on Advanced Information Networking and Applications Workshops. Piscataway: IEEE Press, 2007: 409-414.

[11] CAO N, WANG C, LI M, et al. Privacy-preserving multi-keyword ranked search over encrypted cloud data[C]//Proceedings of IEEE INFOCOM. Piscataway: IEEE Press, 2011: 829-837.

[12] SHACHAM H, WATERS B. Compact proofs of retrievability [J]. Journal of Cryptology, 2013, 26(3): 442-483.

[13] GUO L F, LU B, LI X Y, et al. A verifiable proxy Re-encryption with keyword search without random oracle[C]//2013 Ninth International Conference on Computational Intelligence and Security. Piscataway: IEEE Press, 2013: 474-478.

[14] YANG Y, MA M D. 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.

[15] MIAO Y B, MA J F, LIU X M, 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.

[16] WANG G J, YUE F S, LIU Q. A secure self-destructing scheme for electronic data[J]. Journal of Computer and System Sciences, 2013, 79(2): 279-290.

[17] GUO Y, ZHANG C, JIA X H. Verifiable and forward-secure encrypted search using blockchain techniques[C]//IEEE International Conference on Communications. Piscataway: IEEE Press, 2020: 1321-1329.

[18] BASERI Y, HAFID A, CHERKAOUI S. Privacy preserving fine-grained location-based access control for mobile cloud[J]. Computers & Security, 2018, 73: 249-265.

[19] MIAO Y B, MA J F, LIU X M, et al. Lightweight fine-grained search over encrypted data in fog computing[J]. IEEE Transactions on Services Computing, 2019, 12(5): 772-785.

[作者简介]

张键红（1975− ），男，河北石家庄人，博士，北方工业大学教授，主要研究方向为密码学、云安全、物联网安全。

武梦龙（1972− ），男，山西太原人，博士，北方工业大学副教授，主要研究方向为无线通信、信息安全、信号处理技术等。

王晶（1988− ），男，山东烟台人，京东集团财税创新部工程师，主要研究方向为计算机软件、网络安全、电子商务等。

刘沛（1982− ），男，北京人，京东集团财税创新部工程师，主要研究方向为国家税收治理、区块链、税务数智化转型、财税安全管理。

姜正涛（1976− ），男，山东青岛人，博士，中国传媒大学副教授，主要研究方向为密码学、信息安全、物联网安全等。

彭长根（1963− ），男，贵州锦屏人，博士，贵州大学教授，主要研究方向为密码学、信息安全、物联网安全等。