支持模式隐藏的多关键词公钥可搜索加密方案

聂旭云[1,2]，成驰[1]，耿聪[1]，廖泽宇[1]，焦丽华[1]，陈瑞东[3]，陈大江[1,2]
（1.电子科技大学信息与软件工程学院，四川 成都 610054；2.网络与数据安全四川省重点实验室，四川 成都 611731；
3.电子科技大学计算机科学与工程学院，四川 成都 611731）

摘　要：为了解决现有多用户可搜索加密方案无法隐藏访问模式和搜索模式、抵抗关键词猜测等攻击的问题，提出了一种全新的支持多用户、多关键词搜索的公钥可搜索加密方案。该方案能够在分布式系统中支持多写者/多读者功能，并利用安全比特分解（SBD）协议，多密钥隐私保护外包计算（EPOM）和随机引入假阳性的方法，实现对访问模式与搜索模式的隐藏。同时，该方案支持多写者/多读者表示每个用户加密和上传数据，并搜索所有经授权的加密数据。该方案可通过在多个服务器上并行搜索来加速搜索处理，并仅需为所有读者维护一份加密索引。理论分析和实验结果表明，所提方案在满足陷门和密文的不可区分、多类布尔搜索、搜索和访问模式隐私的前提下，执行效率接近同类型的公钥可搜索加密最优方案。

关键词：模式隐藏；多关键词；多写者/多读者；公钥可搜索加密；数据共享安全
中图分类号：TP309
文献标志码：A
DOI：10.11959/j.issn.1000–436x.2025036

Multi-keyword public key searchable encryption scheme with pattern hiding

NIE Xuyun[1,2], CHENG Chi[1], GENG Cong[1], LIAO Zeyu[1], JIAO Lihua[1], CHEN Ruidong[3], CHEN Dajiang[1,2]
1. School of Information and Software Engineering, University of Electronic Science and Technology of China, Chengdu 610054, China
2. Sichuan Provincial Key Laboratory of Network and Data Security, Chengdu 611731, China
3. School of Computer Science & Engineering, University of Electronic Science and Technology of China, Chengdu 611731, China

Abstract: To address the limitations of existing multi-user searchable encryption (SE) schemes that fail to hide access patterns, search patterns, and resist keyword guessing attacks, a novel public-key searchable encryption scheme was proposed supporting multi-user and multi-keyword searches. Multi-writer/multi-reader functionality was enabled in distributed systems and employed three key techniques: the secure bit decomposition (SBD) protocol, efficient privacy-preserving outsourced calculation framework with multiple key (EPOM), and randomly introducing false positives to achieve access pattern and search pattern hiding. Each user was allowed to encrypt/upload data and search all authorized encrypted data by the multi-writer/multi-reader capability. The search processing through parallel search across multiple servers was accelerated while maintaining only one encrypted index for all readers. Theoretical analysis and experimental results demonstrate that the proposed scheme satisfies the indistinguishability of trapdoors and ciphertext, supports multi-type Boolean searches, preserves search and access pattern privacy, and achieves execution efficiency comparable to state-of-the-art public-key SE schemes.

Keywords: pattern hiding, multi-keyword, multi-writer/multi-reader, public key searchable encryption, data sharing security

收稿日期：2024–10–23；修回日期：2025–02–18
通信作者：陈瑞东，crdchen@163.com
基金项目：国家重点研发计划基金资助项目（No.2023YFB3106402）
Foundation Item：The National Key Research and Development Program of China (No.2023YFB3106402)

0 引言

云存储因其相比传统数据存储的显著优势，已成为工业和个人用户必不可少的基础服务之一。随着云计算的广泛应用，数据存储与共享跨越组织边界愈发频繁，由此引发的数据隐私和安全问题也愈加凸显。因此，使用加密方法确保云存储中敏感信息的隐私成为必然[1]。然而，简单的加密方法会使用户丧失对数据进行快速检索的能力。为解决该问题，Song等[2]引入了可搜索加密方案，能够对加密数据进行直接检索，然而该方案仅支持对称可搜索加密，且无法为数据交换共享提供有效安全保障。

Boneh等[3]开创性引入了公钥可搜索加密（PEKS, public-key encryption with keyword search）方案。通常PEKS方案包括数据拥有者（DO, data owner）（写者）、数据用户（读者）和存储服务器。数据拥有者从数据中提取关键词，利用自己的公钥生成可搜索索引。可搜索索引连同加密后的实际数据（通过对称加密）一同上传至存储服务器。仅指定的用户能够基于私钥和感兴趣的关键词创建搜索陷门，并将其上传给存储服务器。存储服务器通过计算搜索陷门与可搜索索引是否匹配来进行密文数据检索，并返回检索结果。在此模型下，如果数据拥有者需要与多个用户共享同一数据，就必须为每个用户生成一个可搜索索引，这在分布式环境中会造成巨大的计算开销和存储开销。因此，为适应多用户数据交换场景，需要一个高效的可搜索加密方案，使单一的可搜索索引能与多个授权用户的搜索陷门相匹配。

多关键词搜索同样是公钥可搜索加密的一个重要功能。对于包含多个关键词的数据文档，普通的PEKS方案要求生成等同于搜索关键词数量的搜索陷门，每个搜索陷门又需要反复地与文档关联的所有可搜索索引进行匹配。因此，一个支持多关键词搜索的更高效的可搜索加密方案是非常需要的。

对于一个可搜索加密方案而言，需解决的安全问题不仅是数据隐私，还涉及数据搜索隐私。这通常被称为访问模式隐私（即一个关键词所对应的实际文档集合）和搜索模式隐私（SPP, search pattern privacy）（即2次搜索请求是否搜索了同样的关键词）。Islam等[4]基于访问模式泄漏提出了第一个强大的攻击方法（称为IKK攻击）。在具有一些背景知识（关键词共现矩阵）的前提下，通过构建陷门共现矩阵并将其与关键词共现矩阵进行匹配。在文献[4]的实验中，一个半诚实的服务器能以90%的准确率恢复出文档包含哪些关键词。基于此，Cash等[5]通过观察检索文档的数量引入了计数攻击，他们通过搜索到的文档数量的辅助得到了更高的准确度。Pouliot等[6]提出了图形攻击，使得使用带有噪声的辅助信息也能恢复出关键词，并且能保证一定的准确度。Zhang等[7]设计了一种文件注入攻击，该攻击向服务器策略性上传精心构造的文件，并通过观察与这些文件相关的访问模式来恢复查询的底层关键词。Liu等[8]将用户搜索行为作为背景知识，并利用搜索模式泄漏来恢复每个查询的底层关键词。尽管这类攻击的目的是获取用户每次查询的内容，但通过统计分析也能获得每个文档的底层关键词。以上攻击均建立在已知一定背景知识的前提之上，而这些背景知识大多由访问模式和搜索模式推导而来，由此可见隐藏访问模式和搜索模式是可搜索加密方案尤为重要的安全属性。

设计一个同时满足多关键词搜索、隐藏访问/搜索模式和支持多写者/多读者功能的PEKS方案是当前的研究热点。文献[9-11]均提出了支持多关键词搜索的方案，但却不能支持多写者/多读者。文献[10]的公钥大小与关键词集数量，文献[9]和文献[11]的可搜索索引与搜索陷门的大小与处理的关键词数量均成线性关系。当处理的关键词数量较大时，带来的计算开销和通信开销会无法实用。为了实现多用户访问同一加密文件，需要为每个用户生成独有的可搜索索引，但这样会大大增加计算开销和存储开销。例如，文献[12]使用广播加密实现一个写入者和多个读取者的PEKS方案。伍祈应等[13]基于线性秘密共享实现了多数据拥有者认证和多关键词搜索，但存储开销会随着查询关键词的增多迅速增大。Sun等[14]利用基于属性的密文策略加密（CP-ABE, ciphertext-policy attribute-based encryption）提出的方案，除了支持多关键词搜索功能外，还支持多用户访问，但是方案中每个文件可能会拥有多份可搜索索引，会造成巨大的存储开销。杨旸等[15]基于CP-ABE实现了对隐藏关键词可搜索加密方案的细粒度访问控制，但伴随着巨大的计算开销。文献[16-18]设计的方案没有解决访问模式和搜索模式的隐私问题。Wang等[19]使用倒排索引构建的方案虽然可以保证访问模式的安全，但搜索模式的泄露问题仍然存在。在此基础上，文献[20]提

出了一个改进方案，能隐藏访问模式。且部分隐藏搜索模式，其原因是该方案搜索关键词时，为本次没有搜索的关键词用 0 占位，从而造成了搜索模式的泄露。Liu 等[21]提出的方案实现了多写者/多读者、多关键词搜索和搜索模式隐私，但仅部分实现访问模式隐私，需通过在搜索过程中加密测试结果来实现。Tian 等[22]提出的方案支持多写者/多读者，且具有亚线性的搜索复杂度，但同样没有解决搜索模式和访问模式的隐私问题。尽管采用不经意随机访问机（ORAM, oblivious random-access machine）[23]和私有信息检索（PIR, private information retrival）[24]可同时防止访问模式和搜索模式的泄露，但同时也引入了高昂的计算开销和通信开销。

基于此，本文基于同态公钥加密构建了一种新的隐藏模式的多关键词公钥可搜索加密（MPKSE-PH, multi-keyword public key searchable encryption with pattern hiding）方案，该方案在分布式系统下满足上述功能性、安全性、隐私性等问题。在分布式环境下，该方案又可以部署多个辅助服务器（SS, support server）来协助云服务器（CS, cloud server）并行执行关键词搜索，提高效率。本文的主要贡献如下。

1) 提出了一个多关键词公钥可搜索加密方案。该方案在分布式环境下支持多写者/多读者的同时，隐藏了访问模式和搜索模式，进而抵抗了关键词猜测攻击（KGA, keyword guessing attack）。

2) 在分布式环境下，本文方案可由并行服务器进行搜索处理以加快响应速度，其中，多写者/多读者意味着支持每个用户加密和上传数据，并搜索存储的所有经授权的加密数据。区别于其他方案为每个读者生成对应的加密索引，且本文方案对所有读者仅会生成一份加密索引。

3) 安全性分析表明，本文方案满足陷门和密文的不可区分性、搜索模式和访问模式的隐私性，并对其计算开销和通信开销进行了实验分析。实验结果表明，本文方案具有可行性，并在个人医疗信息数据查询等高安全需求、执行时间非高度敏感的场景下具有实用性。

1　基础知识

关键词集合表示为 $\mathcal{W}=\{w_{\mu-1},\cdots,w_0\}$，其中 μ 为关键词总数。每个文档用二进制 $F_{\mu-1},\cdots,F_0$ 表示，其中，每一位为 1 表示该文档包含对应的关键词，为 0 表示不包含，用 F 表示 $F_{\mu-1},\cdots,F_0$ 的十进制。一次搜索的关键词集用二进制表示为 $t_{\mu-1},\cdots,t_0$，其中，每一位为 1 表示本次搜索包含对应的关键词，为 0 表示不包含，用 t 表示 $t_{\mu-1},\cdots,t_0$ 的十进制。$\mathcal{W}_F=\{w_i|w_i\in\mathcal{W},F_i=1\}$ 表示文档 F 的关键词集，$\mathcal{W}_t=\{w_i|w_i\in\mathcal{W},t_i=1\}$ 表示搜索关键词集。本文讨论 3 种类型的布尔多关键词搜索，分别为 AND 搜索、OR 搜索和 NOT 搜索。1) AND 搜索。如果 $\mathcal{W}_t\subset\mathcal{W}_F$（即 $\mathcal{W}_t\cap\mathcal{W}_{\neg F}=\varnothing$）成立，那么 t 匹配了 F。2) OR 搜索。如果 $\mathcal{W}_t\cap\mathcal{W}_F\neq\varnothing$ 成立，那么 t 匹配了 F。3) NOT 搜索。如果 $\mathcal{W}_t\subset\mathcal{W}_{\neg F}$（即 $\mathcal{W}_t\cap\mathcal{W}_F=\varnothing$）成立，那么 t 匹配了 F。表 1 给出了本文所用到的符号及其含义。

表 1　　符号及其含义

符号	含义
DB	文档集
DB[w]	包含关键词 w 的所有文档
$\mathcal{W}_s$	s 表示的关键词集合
$\mathcal{W}_{\mathrm{id}}$	第 id 个文档中包含的所有关键词集合
w	一个关键词
$(s_{\mu-1},\cdots,s_0)$	十进制整数的无符号二进制表示
μ	s 的二进制长度，$\mathcal{W}$ 中的关键词个数
$\neg s$	s 的补数
F	十进制整数，其二进制表示文档包含的关键词信息
t	十进制整数，其二进制表示一次搜索的关键词信息
SUM	十进制整数 $2^{\mu-1}$，即长度为 μ 的全 1 二进制数
td	陷门
I	可搜索索引 $I=[F]_{\mathrm{pk}}$
$\mathrm{PK}_i,\mathrm{pk}_i$	i 方的公钥
$\mathrm{SK}_i,\mathrm{sk}_i$	i 方的私钥
ct	密文
$[\cdot]_{\mathrm{pk}}$	在公钥 pk 下的密文
$\mathcal{L}(\cdot)$	长度

安全比特分解（SBD, secure bit-decomposition）协议[25]把某个值‘s’的加密转换成其各比特的加密，可以描述为

$$\mathrm{SBD}\left([s]_{\mathrm{pk}}\right)=\left([s_{\mu-1}]_{\mathrm{pk}},\cdots,[s_0]_{\mathrm{pk}}\right)\tag{1}$$

多密钥隐私保护外包计算（EPOM, efficient

privacy-preserving outsourced calculation framework with multiple keys）[26]基于部分同态加密（PHE, partial homomorphic encryption）[27]和阈值密码系统[28]，提供了一种分布式双陷门公钥密码系统，可确保常用的整数运算可以在加密的情况下进行，而且不会将隐私数据泄露给未授权方。与全同态加密（FHE, fully homomorphic encryption）方案[29]相比，计算开销更小。EPOM 接受 2 个参与方的输入$[x]_{\mathrm{pk}_a}$和$[y]_{\mathrm{pk}_b}$，部分强密钥$\mathrm{SK}^{(1)}$和$\mathrm{SK}^{(2)}$，2 个参与方的公钥pk_a和pk_b，还有系统公钥pk_c实现跨域安全加法算法（SAD），输出加法结果的密文$[x+y]_{\mathrm{pk}_c}$；实现跨域安全乘法算法（SMD），输出乘法结果的密文$[x\times y]_{\mathrm{pk}_c}$；实现跨域安全相等算法（SEQ），输出相等结果的密文$[z]_{\mathrm{pk}_c}$，解密后若z=0，则$x=y$，反之，$x\neq y$。

2 基本方案

2.1 系统模型

密钥生成中心（KGC, key generation center）：生成系统参数、系统密钥以及云服务器和辅助服务器的公钥对，并将相应的密钥分发给 CS 和 SS。一般来说，管理员扮演 KGC 的角色。云服务器负责存储由数据拥有者上传的文档和相应的可搜索索引。它在 SS 的协助下进行搜索操作，最后生成加密的搜索结果并返回给搜索用户（SU, search user）。辅助服务器同 CS 一同进行搜索操作。在分布式环境下，SS 可以是组织内部指定的服务器，或者是其他云服务器。每个数据拥有者拥有 KGC 基于系统参数生成的属于自己的公私钥对，根据文档关键词生成可搜索索引，并将可搜索索引和对应的加密文档存储在 CS 上。每个搜索用户类似 DO，拥有 KGC 生成的 SU 的公私钥对，并为搜索关键词生成搜索陷门。经管理员授权解密来自 CS 的搜索结果，获取满足搜索查询的文档索引。

本文假设 KGC 是诚实的，CS 和 SS 均为诚实且好奇的，他们会遵循方案进行存储、搜索等操作，并试图获取密文信息或者底层关键词信息。DO 也被认为是诚实且好奇的，其遵循协议但试图获取其他参与方的隐私。

2.2 方案构造

如图 1 所示，本文的系统模型由一个 KGC、一个 CS、若干个 SS、若干个 DO 和若干个 SU 组成。KGC 将全局初始化时生成的强密钥分割成独立的密钥对分发给每个 CS 和 SS。有新的参与方加入时，KGC 只需独立为新的参与方再次生成。

若文档关键词集为$\mathcal{W}_F$，可搜索索引为$I=[F]_{\mathrm{pk}_a}$，搜索关键词集为$\mathcal{W}_t$，搜索陷门为$\mathrm{td}=[t]_{\mathrm{pk}_b}$。所以，当$t$与$F$匹配时，那么$\mathcal{W}_t$的所有关键词包含在$\mathcal{W}_F$中，即$\mathcal{W}_t$为$\mathcal{W}_F$的子集。

本文方案先将每个文档的关键词提取出来，形成一个二进制表示的数，进而转换为十进制数F和t来进行后续方案的执行。本文方案应用于分布式环境，CS 可以请求一个或多个 SS 协助处理相同的搜索查询，其中每个 SS 处理一部分关键词。例如，匹配 60 个索引，CS 可以同其他 2 个 SS 为同一匹配，每台服务器匹配 20 个索引。在分布式系统下，使用的 SS 越多，查询响应速度就越快。此外，它还可以有效支持负载平衡，即如果一个 SS 下线或负载过重，其他 SS 可以分享工作负荷。为了简化方案描述，本文将重点阐述如何部署一个 SS 的方案。方案中的$\mathrm{pk}_{\sum \mathrm{SU}}=\left(N,g,h_{\sum \mathrm{SU}}=g^{\theta_{\mathrm{SU}}+\sum_{j=1,\cdots,K}\theta_j}\right)$对应的私钥可由 SU 向 KGC 申请。

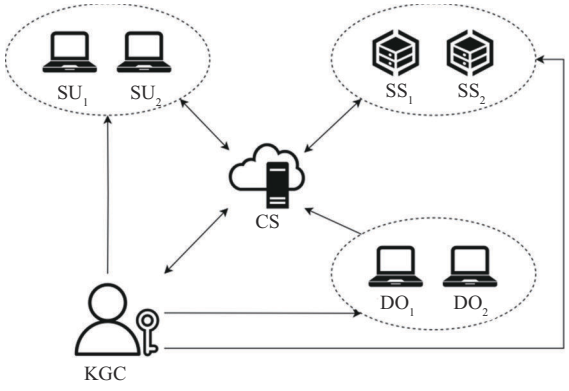


图 1 系统模型

2.2.1 形式化定义

本文方案由下列 4 个算法组成。

1) $\mathrm{KeyGen}(1^k)\rightarrow(\mathrm{PK}_{\mathrm{DO}},\mathrm{SK}_{\mathrm{DO}},\mathrm{PK}_{\mathrm{SU}},\mathrm{SK}_{\mathrm{SU}},\mathrm{SK}_{\mathrm{CS}},\mathrm{SK}_{\mathrm{SS}})$。由 KGC（一般由系统管理者担任）执行，以安全参数k作为输入，初始化公共参数，并为每个参与方生成对应的公私钥对。

2) $\mathrm{BuildIndex}(\mathrm{PK}_{\mathrm{DO}},\mathcal{W}_F)\rightarrow I$。由 DO 执行，DO 使用自己的公钥$\mathrm{PK}_{\mathrm{DO}}$加密文档关键词集$\mathcal{W}_F$，

生成可搜索索引 I，再将文档使用对称加密算法加密后一并上传到云服务器CS上存储。

3) Trapdoor$\left(\mathrm{PK_{SU}},\mathcal{W}_t\right)\rightarrow$ td。由SU执行，SU使用其公钥$\mathrm{PK_{SU}}$加密搜索关键词集$\mathcal{W}_t$生成搜索陷门td并发送至CS。

4) Search$\left(\mathrm{PK_{DO}},\mathrm{SK_{CS}},\mathrm{SK_{SS}},\mathrm{PK_{SU}},\mathrm{SK_{SU}},\mathrm{td},I\right)\rightarrow$ 0/1。由CS联合SS执行，CS接收到搜索陷门td后，使用td与存储在本地的可搜索索引I进行匹配，并返回结果。其中1表示匹配成功，0表示匹配失败。

2.2.2 *详细步骤*

1) 密钥生成。KeyGen $(1^k)\rightarrow(\mathrm{PK_{DO}},\mathrm{SK_{DO}},\mathrm{PK_{SU}},\mathrm{SK_{SU}},\mathrm{SK_{CS}},\mathrm{SK_{SS}})$。给定安全参数$k$、KGC、DO和SU，执行以下操作。

① KGC生成大素数p和q，使$\mathcal{L}(p)=\mathcal{L}(q)=k$。然后KGC运行EPOM.KG算法获取强私钥$\mathrm{SK}=\lambda$，并运行EPOM.SKeyS算法生成2个部分强私钥$\mathrm{SK}^{(1)}=\lambda_1,\mathrm{SK}^{(2)}=\lambda_2$。KGC初始化一个含$\mu$个关键字的词集$\mathcal{W}$作为关键词总集，公开参数$\mathrm{PP}=\left(\mathcal{W},\mu,N,g\right)$，将$\mathrm{SK_{CS}}=\mathrm{SK}^{(1)}=\lambda_1$发送给CS，将$\mathrm{SK_{SS}}=\mathrm{SK}^{(2)}=\lambda_2$发送给SS，并保持SK的机密性。

② 每个DO执行EPOM.KG算法生成公钥$\mathrm{pk_{DO}}=\left(N,g,h_{\mathrm{DO}}\right)$和弱私钥$\mathrm{sk_{DO}}=\theta_{\mathrm{DO}}$，然后公开$\mathrm{pk_{DO}}$并保持$\mathrm{sk_{DO}}$的机密性。每个DO（即写者）对应的所有SU（即读者）用EPOM.KG算法生成公钥$\mathrm{pk_{SU}}=\left(N,g,h_{\mathrm{SU}}\right)$和弱私钥$\mathrm{sk_{SU}}=\theta_{\mathrm{SU}}$，将$\mathrm{pk_{SU}}$公开，并保持$\mathrm{sk_{SU}}$的机密性。

2) 索引建立。BuildIndex$\left(\mathrm{PK_{DO}},\mathcal{W}_F\right)\rightarrow I$。给定DO的公钥$\mathrm{PK_{DO}}=\mathrm{pk_{DO}}$和上传文档的关键词集合$\mathcal{W}_F$。DO在本地计算相应的索引$F$，其二进制为$\left(F_{\mu-1},\cdots,F_0\right)$，采用EPOM.Enc算法获取加密可搜索索引$[F]_{\mathrm{pk_{DO}}}$并发送给CS。

3) 陷门生成。Trapdoor$\left(\mathrm{PK_{SU}},\mathcal{W}_t\right)\rightarrow$ td。给定SU的公钥$\mathrm{PK_{SU}}=\mathrm{pk_{SU}}$和搜索关键词集合$W_t$，计算相应的陷门$t\in\left\{0,\cdots,2^{\mu}-1\right\}$，其二进制表示为$\left(t_{\mu-1},\cdots,t_0\right)$。为了在搜索结果中引入假阳性，SU根据搜索类型的不同，随机选取k个比特位翻转为0/1，从而使每次的返回结果都包含一些原本不匹配的冗余项，以保证访问模式的隐私。具体而言，对于AND搜索和NOT搜索，翻转为0，对于OR搜索，则翻转为1。最后，采用EPOM.Enc算法获取加密陷门$[t]_{\mathrm{pk_{SU}}}$并发送给CS。

4) 搜索。Search $(\mathrm{PK_{DO}},\mathrm{SK_{CS}},\mathrm{SK_{SS}},\mathrm{PK_{SU}},\mathrm{SK_{SU}},\mathrm{td},I)\rightarrow$ 0/1。给定DO的公钥$\mathrm{PK_{DO}}=\mathrm{pk_{DO}}$、CS的秘密密钥$\mathrm{SK_{CS}}=\mathrm{SK}^{(1)}$、SS的秘密密钥$\mathrm{SK_{SS}}=\mathrm{SK}^{(2)}$、SU的公钥$\mathrm{PK_{SU}}=\mathrm{pk_{SU}}$、SU的加密陷门$[t]_{\mathrm{pk_{SU}}}$和加密可搜索索引$[F]_{\mathrm{pk_{DO}}}$，CS和SS执行后续的4个步骤，即算法1~算法4。

算法1。给定$[t]_{\mathrm{pk_{SU}}}$和$[F]_{\mathrm{pk_{DO}}}$，CS根据搜索类型联合SS计算$\neg F$和t或F和t密文的每一位。

算法1　MPKSE_PH搜索算法步骤1

输入　$[t]_{\mathrm{pk_{SU}}},[F]_{\mathrm{pk_{DO}}},\mathrm{pk_{DO}},\mathrm{pk_{SU}},\mathrm{sk_{CS}},\mathrm{sk_{SS}}$

输出　$[\neg F]_{\mathrm{pk_{DO}}},\left[t_i\right]_{\mathrm{pk_{SU}}},i\in\left\{0,\cdots,\mu-1\right\}$

1) 如果搜索类型为AND搜索，那么

2) CS计算：

$$[\mathrm{SUM}]_{\mathrm{pk_{DO}}}=[2^{\mu}-1]_{\mathrm{pk_{DO}}}$$

$$[\neg F]_{\mathrm{pk_{DO}}}=[\mathrm{SUM}]_{\mathrm{pk_{DO}}}([F]_{\mathrm{pk_{DO}}})^{N-1}$$

3) 同SS使用SBD算法：

$$\mathrm{SBD}([\neg F]_{\mathrm{pk_{DO}}})\rightarrow\left(\left[\neg F_{\mu-1}\right]_{\mathrm{pk_{DO}}},\cdots,\left[\neg F_0\right]_{\mathrm{pk_{DO}}}\right)$$

$$\mathrm{SBD}([t]_{\mathrm{pk_{SU}}})\rightarrow([t_{\mu-1}]_{\mathrm{pk_{SU}}},\cdots,[t_0]_{\mathrm{pk_{SU}}})$$

4) 如果搜索类型为OR搜索或NOT搜索，那么

5) CS同SS使用SBD算法：

$$\mathrm{SBD}([F]_{\mathrm{pk_{DO}}})\rightarrow\left(\left[F_{\mu-1}\right]_{\mathrm{pk_{DO}}},\cdots,\left[F_0\right]_{\mathrm{pk_{DO}}}\right)$$

$$\mathrm{SBD}([t]_{\mathrm{pk_{SU}}})\rightarrow([t_{\mu-1}]_{\mathrm{pk_{SU}}},\cdots,[t_0]_{\mathrm{pk_{SU}}})$$

算法2。给定$[F_i]_{\mathrm{pk_{DO}}}$（或$[\neg F_i]_{\mathrm{pk_{DO}}}$）和$\left[t_i\right]_{\mathrm{pk_{SU}}}$，其中$i\in\{0,\cdots,\mu-1\}$，CS联合SS计算$e_i$的密文。

算法2　MPKSE_PH搜索算法步骤2

输入　$[F_i]_{\mathrm{pk_{DO}}}$（或$[\neg F_i]_{\mathrm{pk_{DO}}}$）和$\left[t_i\right]_{\mathrm{pk_{SU}}}$，其中$i\in\{0,\cdots,\mu-1\}$，$\mathrm{pk_{DO}},\mathrm{pk_{SU}},\mathrm{sk_{CS}},\mathrm{sk_{SS}}$

输出　$[e_i]_{\mathrm{pk}_{\sum\mathrm{SU}}}$

1) 如果搜索类型为AND搜索，那么

2) CS联合SS运行SMD算法：

$$[e_i]_{\mathrm{pk}_{\sum\mathrm{SU}}}=\neg\,\mathrm{SMD}([\neg F_i]_{\mathrm{pk_{DO}}},[t_i]_{\mathrm{pk_{SU}}})$$

3) 如果搜索类型为OR搜索或NOT搜索，那么

4) CS联合SS运行SMD算法：

$$[e_i]_{\mathrm{pk}_{\sum \mathrm{SU}}} = \neg \mathrm{SMD}([F_i]_{\mathrm{pk}_{\mathrm{DO}}}, [t_i]_{\mathrm{pk}_{\mathrm{SU}}})$$

算法3。给定$[e_i]_{\mathrm{pk}_{\sum \mathrm{SU}}}$，CS联合SS计算所有$e_i$的乘积，其中$i \in \{0,\cdots,\mu-1\}$。然后再引入随机性$r$，最后得到$[f]_{\mathrm{pk}_{\sum \mathrm{SU}}}$。

算法3 MPKSE_PH搜索算法步骤3

输入 $[e_i]_{\mathrm{pk}_{\sum \mathrm{SU}}}$，对于$i \in \{0,\cdots,\mu-1\}$，$\mathrm{pk}_{\mathrm{SU}}$，$\mathrm{sk}_{\mathrm{CS}}$,$\mathrm{sk}_{\mathrm{SS}}$

输出 $[e_i]_{\mathrm{pk}_{\sum \mathrm{SU}}}$

1) CS初始化

2) $[R]_{\mathrm{pk}_{\sum \mathrm{SU}}} = 1$，$i = 1$

3) CS同SS执行SMD算法

4) 当$i < \mu$时

5) $[R]_{\mathrm{pk}_{\sum \mathrm{SU}}} = \mathrm{SMD}([R]_{\mathrm{pk}_{\sum \mathrm{SU}}}, [e_i]_{\mathrm{pk}_{\sum \mathrm{SU}}})$

6) 结束循环

7) CS随机选择$r \xleftarrow{R} \mathbb{Z}_N^*$且$\gcd(r,N)=1$并计算：

8) $[f]_{\mathrm{pk}_{\sum \mathrm{SU}}} = [rR]_{\mathrm{pk}_{\sum \mathrm{SU}}} = [R]^r_{\mathrm{pk}_{\sum \mathrm{SU}}}$

算法4。给定$[f]_{\mathrm{pk}_{\sum \mathrm{SU}}}$，针对不同类型的搜索，SU输出0表示该文档不匹配当前搜索，输出1表示该文档匹配当前搜索，随后SU向CS请求当前文档。

算法4 MPKSE_PH搜索算法步骤4

输入 $[f]_{\mathrm{pk}_{\sum \mathrm{SU}}}$和$\mathrm{sk}_{\sum \mathrm{SU}}$

输出 0或1

1) SU用私钥$\mathrm{sk}_{\sum \mathrm{SU}}$解密$[f]_{\mathrm{pk}_{\sum \mathrm{SU}}}$

$$\mathrm{D}_{\mathrm{sk}_{\sum \mathrm{SU}}}([f]_{\mathrm{pk}_{\sum \mathrm{SU}}}) \to f$$

2) 如果搜索类型为AND搜索，那么

3) 若$f \neq 0$那么

4) 返回1

5) 如果搜索类型为OR搜索，那么

6) 若$f = 0$那么

7) 返回1

8) 如果搜索类型为NOT搜索，那么

9) 若$f \neq 0$那么

10) 返回1

11) 否则

12) 返回0

2.3 正确性

在本文方案中，最终匹配结果返回1表示本次搜索匹配了对应的文档，返回0表示文档没有匹配本次搜索的关键词。这里以AND搜索为例，其余搜索类似，返回1代表算法4中$f \neq 0$，即$[f]_{\mathrm{pk}_{\sum \mathrm{SU}}} \neq [0]_{\mathrm{pk}_{\sum \mathrm{SU}}}$，说明算法3中每个$[e_i]_{\mathrm{pk}_{\sum \mathrm{SU}}}$都不为$[0]_{\mathrm{pk}_{\sum \mathrm{SU}}}$，进一步说明在算法2中，$[\neg F]_{\mathrm{pk}_{\mathrm{DO}}}$与$[t]_{\mathrm{pk}_{\mathrm{SU}}}$没有交集，这表明如果搜索了文档中不包含的关键词，就不会匹配该文档，也就是说$[t]_{\mathrm{pk}_{\mathrm{SU}}}$是$[F]_{\mathrm{pk}_{\mathrm{DO}}}$的子集，故只有搜索了文档中包含的关键词，才会匹配该文档。反之，若没有搜索该文档包含的关键词，或者搜索了该文档不包含的关键词，搜索算法将会返回结果0，表明没有匹配该文档。

3 安全性分析

3.1 陷门不可区分性

作为PEKS中关注的安全之一，陷门隐私是指隐藏陷门底层关键字的信息。对于本文的系统模型，考虑到多关键字搜索，这意味着CS不能从SU接收到的陷门中了解任何关键字的信息。与先前的安全要求类似，不考虑陷门查询和密文查询。然而，本文允许CS与SS进行通信，执行搜索操作并获取中间结果。陷门不可区分性游戏可以描述如下。

攻击者选择2个不同的感兴趣的关键字集合并将它们发送给挑战者，挑战者随机选择其中一个来生成相应的陷门并返回。然后攻击者尝试猜测挑战陷门的底层关键字集合中的哪一个。

IND-TD定义了描述安全要求的不可区分性游戏，其定义如下。

Setup。在这一阶段，由一个挑战者$\mathcal{C}$运行$\mathrm{KeyGen}(1^k) \to (\mathrm{PK}_{\mathrm{DO}},\mathrm{SK}_{\mathrm{DO}},\mathrm{PK}_{\mathrm{SU}},\mathrm{SK}_{\mathrm{SU}},\mathrm{SK}_{\mathrm{CS}},\mathrm{SK}_{\mathrm{SS}})$，发送$(\mathrm{PK}_{\mathrm{DO}},\mathrm{PK}_{\mathrm{SU}},\mathrm{SK}_{\mathrm{CS}})$给一个敌手$\mathcal{A}$，并保持对$(\mathrm{SK}_{\mathrm{DO}},\mathrm{SK}_{\mathrm{SU}},\mathrm{SK}_{\mathrm{SS}})$的机密性。

Challenge。敌手$\mathcal{A}$选择2个不同的关键词集$\mathcal{W}_0,\mathcal{W}_1 \subseteq \mathcal{W}$。$\mathcal{A}$发送$\mathcal{W}_0$和$\mathcal{W}_1$给挑战者$\mathcal{C}$。$\mathcal{C}$选择$b \in_R \{0,1\}$，运行$\mathrm{Trapdoor}(\mathrm{PK}_{\mathrm{SU}},\mathcal{W}_t) \to \mathrm{td}_b$，并发送$\mathrm{td}_b$给敌手$\mathcal{A}$。

Query。敌手$\mathcal{A}$被允许与挑战者$\mathcal{C}$进行交互，$\mathcal{C}$在这里充当SS的角色。

Output。敌手 $\mathcal{A}$ 给定它的猜测 b'，如果 $b'=b$，则它赢得游戏。

定义 1　MPEKS-PH 满足上述游戏的不可区分性，如果对所有概率多项式时间（PPT, probabilistic polynomial time）的敌手，优势为

$$\mathrm{Adv}^{\text{IND-TD}}_{\text{MPKSE-PH},\mathcal{A}}(\lambda)=\left|\Pr\left[\mathcal{A}^{b=0}\ \text{wins}\ \right]-\Pr\left[\mathcal{A}^{b=1}\ \text{wins}\ \right]\right| \tag{2}$$

则该优势是可忽略的。

3.2　密文不可区分性

当一个加密文档被上传到 CS，DO 还应附上相应的可搜索索引，并要求可搜索索引不泄露任何关于其底层关键字的信息。值得注意的是，尽管 CS 可以与 SS 交互以运行搜索，但最终的搜索结果只能由 SU 访问。另一个考虑因素是陷门是基于 SU 的公钥加密的，可搜索索引是基于 DO 的公钥加密的，攻击者可以使用自己的公钥生成任意关键字集合的搜索陷门和可搜索索引。由于本文系统模型具有多关键字搜索功能，可以描述区分游戏如下。

攻击者选择 2 个不同的感兴趣的关键字集合并将它们发送给挑战者，挑战者随机选择其中一个生成相应的加密可搜索索引并返回。然后攻击者尝试猜测哪个是底层关键字集合。

IND-I 定义了描述安全要求的不可区分性游戏，其定义如下。

Setup。在这一阶段，由一个挑战者 $\mathcal{C}$ 运行 $\mathrm{KeyGen}\left(1^k\right)\rightarrow\left(\mathrm{PK_{DO}},\mathrm{SK_{DO}},\mathrm{PK_{SU}},\mathrm{SK_{SU}},\mathrm{SK_{CS}},\mathrm{SK_{SS}}\right)$，发送 $\left(\mathrm{PK_{DO}},\mathrm{PK_{SU}},\mathrm{SK_{CS}}\right)$ 给敌手 $\mathcal{A}$，并保持对 $\left(\mathrm{SK_{DO}},\mathrm{SK_{SU}},\mathrm{SK_{SS}}\right)$ 的机密性。

Challenge。敌手 $\mathcal{A}$ 选择 2 个不同的关键词集 $\mathcal{W}_0,\mathcal{W}_1\subseteq\mathcal{W}$。$\mathcal{A}$ 发送 $\mathcal{W}_0$ 和 $\mathcal{W}_1$ 给挑战者 $\mathcal{C}$。$\mathcal{C}$ 选择 $b\in_R\{0,1\}$，运行 $\mathrm{BuildIndex}\left(\mathrm{PK_{DO}},\mathcal{W}_b\right)\rightarrow\mathrm{SC}_b$ 并发送 SC 给敌手 $\mathcal{A}$。

Output。敌手 $\mathcal{A}$ 给定它的猜测 b'，如果 $b'=b$，则它赢得游戏。

定义 2　MPEKS-PH 满足上述游戏的不可区分性，如果对所有概率多项式时间（PPT）的敌手，优势为

$$\mathrm{Adv}^{\text{IND-I}}_{\text{MPKSE-PH},\mathcal{A}}(\lambda)=\left|\Pr\left[\mathcal{A}^{b=0}\ \text{wins}\ \right]-\Pr\left[\mathcal{A}^{b=1}\ \text{wins}\ \right]\right| \tag{3}$$

则该优势是可忽略的。

3.3　搜索模式隐私

当 SU 发出 2 个搜索查询时，CS 不能够确定这 2 个查询是否具有相同的底层关键词集。这种安全要求被称为搜索模式隐私[30]。由于 SE-EPOM 的语法，这意味着在给定 2 个陷门的情况下，对手不能确定它们的基础关键词集是否相同。类似于先前的安全要求，陷门查询和密文查询不被考虑在内。受文献[30]中对 PEKS 安全定义的启发，本文在以下游戏中制定了搜索模式隐私。

Setup。在这一阶段，由一个挑战者 $\mathcal{C}$ 运行 $\mathrm{KeyGen}\left(1^k\right)\rightarrow\left(\mathrm{PK_{DO}},\mathrm{SK_{DO}},\mathrm{PK_{SU}},\mathrm{SK_{SU}},\mathrm{SK_{CS}},\mathrm{SK_{SS}}\right)$，发送 $\left(\mathrm{PK_{DO}},\mathrm{PK_{SU}},\mathrm{SK_{CS}}\right)$ 给敌手 $\mathcal{A}$，并保持对 $\left(\mathrm{SK_{DO}},\mathrm{SK_{SU}},\mathrm{SK_{SS}}\right)$ 的机密性。

Challenge。敌手 $\mathcal{A}$ 选择 2 个不同的关键词集 $\mathcal{W}_0,\mathcal{W}_1\subseteq\mathcal{W}$。$\mathcal{A}$ 发送 $\mathcal{W}_0$ 和 $\mathcal{W}_1$ 给挑战者 $\mathcal{C}$。$\mathcal{C}$ 选择 $b\in_R\{0,1\}$，运行 $\mathrm{Trapdoor}\left(\mathrm{PK_{SU}},\mathcal{W}_b\right)\rightarrow\mathrm{td}_b$ 和 $\mathrm{Trapdoor}\left(\mathrm{PK_{SU}},\mathcal{W}_0\right)\rightarrow\mathrm{td}_0$，并发送 td_b 和 td_0 给敌手 $\mathcal{A}$。

Output。敌手 $\mathcal{A}$ 给定它的猜测 b'，如果 $b'=b$，则它赢得游戏。

定义 3　MPEKS-PH 满足上述搜索模式隐私，如果对所有概率多项式时间（PPT）的敌手，优势为

$$\mathrm{Adv}^{\text{IND-TD}}_{\text{MPKSE-PH},\mathcal{A}}(\lambda)=\left|\Pr\left[\mathcal{A}^{b=0}\ \text{wins}\ \right]-\Pr\left[\mathcal{A}^{b=1}\ \text{wins}\ \right]\right| \tag{4}$$

则该优势是可忽略的。

3.4　访问模式隐私

访问模式表示一个文档包含哪些关键词。访问模式的泄露通常来自以下 2 个方面：1) 由 CS 执行搜索算法的输出；2) SU 得到搜索结果后访问的文档。这要求对手无法从文档密文、搜索索引和搜索返回的文档集中获得访问模式。

一方面，本文方案通过语义安全加密 EPOM 保护结果，使 CS 无法了解与搜索查询对应的匹配文档标识符。本文的陷门不可区分性（定义 2）说明了此特性。如果对手可以判断可搜索密文与挑战性陷门之间的匹配结果，则对手可以赢得游戏。因此，本文方案在搜索过程中实现了访问模式隐私保护。而文档密文通过语义安全的对称加密进行加密，同样不会泄露其他相关信息。

另一方面，当用户后续检索与搜索结果相对应的文档时，访问模式也可能泄露给 CS。如果每次都检索相同的文档，那么大概率会让敌手猜测搜索了相同的关键词。然而，本文在陷门生成

$\text{Trapdoor}\left(\text{PK}_{\text{SU}},\mathcal{W}_t\right)\rightarrow \text{td}$过程中通过将$\left(t_{\mu-1},\cdots,t_0\right)$的$k$个比特位翻转为0/1，使实际与陷门不匹配的文档所对应的索引发生匹配，以此引入假阳性，在目标文档之外访问一些无关紧要的文档，以混淆云服务的视图，这让本文很好地隐藏了访问模式。

以AND搜索为例，当陷门中原本为1的t_i被翻转为0后，在算法2中会发生以下变化。若$F_i=1$，则对应的e_i由0翻转为1，进而导致算法3和算法4得到的f可能由0翻转为1，使原本不匹配的索引项产生匹配，引入假阳性。若$F_i=0$，则对应的e_i保持为1，不发生翻转，且不对搜索结果产生影响。

同时，翻转为0/1的操作并不会影响原本为0/1的比特位，因此不会对原本匹配的索引项产生影响而导致搜索错误，即不会引入假阴性。此处以AND搜索为例，对比特翻转的方法不会导致搜索错误（即不会引入假阴性）进行说明。

将陷门t的随机k个比特位翻转为0后得到的新陷门记为t^{mask}，由于t_i为0表示搜索关键词集合$\mathcal{W}_t$中不包含t_i所对应的关键词，于是有$\mathcal{W}_{t^{\text{mask}}}\subset\mathcal{W}_t$。因此，当$\mathcal{W}_t\subset\mathcal{W}_F$时，一定有$\mathcal{W}_{t^{\text{mask}}}\subset\mathcal{W}_F$，即不会引入假阴性。根据以上逻辑不难得到，OR搜索和NOT搜索同样不会引入假阴性。

3.5 陷门不可区分性与搜索模式隐私的关联

根据本文的安全定义，IND-TD游戏和SPP游戏的攻击者都旨在收集有关陷门底层关键字的信息。因此，本节讨论它们的关联。

定理1 如果方案满足陷门不可区分性，那么方案就能满足搜索模式隐私。

证明 假设MPEKS-PH不满足搜索模式隐私。本文将证明它也不满足陷门不可区分性。

当MPEKS-PH不满足搜索模式隐私时，意味着存在一个攻击者$\mathcal{B}$，可以以不可忽略的概率赢得SPP游戏。假设存在一个攻击者$\mathcal{A}$，在IND-TD游戏中将$\mathcal{B}$作为子程序运行，游戏描述如下。

Setup。在这一阶段，首先由一个挑战者$\mathcal{C}$运行$\text{KeyGen}\left(1^k\right)\rightarrow\left(\text{PK}_{\text{DO}},\text{SK}_{\text{DO}},\text{PK}_{\text{SU}},\text{SK}_{\text{SU}},\text{SK}_{\text{CS}},\text{SK}_{\text{SS}}\right)$，发送$\left(\text{PK}_{\text{DO}},\text{PK}_{\text{SU}},\text{SK}_{\text{CS}}\right)$给敌手$\mathcal{A}$，并保持$\left(\text{SK}_{\text{DO}},\text{SK}_{\text{SU}},\text{SK}_{\text{SS}}\right)$的机密性。然后敌手$\mathcal{A}$将$\mathcal{B}$当作一个子程序运行，$\mathcal{B}$选择2个不同的关键词集$\mathcal{W}_0,\mathcal{W}_1\subseteq\mathcal{W}$并发送给$\mathcal{A}$。

Challenge。敌手$\mathcal{A}$发送$\mathcal{W}_0,\mathcal{W}_1$给挑战者$\mathcal{C}$。$\mathcal{C}$选择$b\in_R\{0,1\}$，运行$\text{Trapdoor}\left(\text{PK}_{\text{SU}},\mathcal{W}_b\right)\rightarrow\text{td}_b$，并发送$\text{td}_b$给$\mathcal{A}$。$\mathcal{A}$运行$\text{Trapdoor}\left(\text{PK}_{\text{SU}},\mathcal{W}_0\right)\rightarrow\text{td}_0$，并发送$\text{td}_0,\text{td}_b$给$\mathcal{B}$。在$\mathcal{B}$的视角下，$\text{td}_0,\text{td}_b$对应着SPP游戏中的$\text{td}_0,\text{td}_b$。鉴于以上假设，$\mathcal{B}$输出$b'$并有$b'=b$的情况，以一个不可忽略的概率超过$\frac{1}{2}$。

Query。敌手$\mathcal{A}$可以通过直接将相同的查询转发给挑战者$\mathcal{C}$来回答$\mathcal{B}$的查询。

Output。当且仅当$\mathcal{B}$输出b'时，敌手$\mathcal{A}$输出b'。如果$b'=b$，则敌手赢得游戏。

因此，敌手$\mathcal{A}$显然有不可忽略的概率赢得这场游戏。即MPEKS-PH不满足陷门不可区分性。证毕。

3.6 安全模型定义

本文考虑面向非共谋诚实且好奇攻击者的基于模拟的安全模型定义[26]，在MPEKS-PH中，本文有数据提供方（DO）作为D_a、云服务器（CS）作为S_1和辅助服务器（SS）作为S_2，详情参考文献[26]。

$\mathcal{P}=(D_a,S_1,S_2)$是所有协议参与方的集合，同时存在3种类型的对手$\mathcal{A}_{\mathcal{D}_a},\mathcal{A}_{\mathcal{S}_1},\mathcal{A}_{\mathcal{S}_2}$分别攻击$D_a,S_1,S_2$。

在真实世界中，D_a带着输入x,y运行（还有额外的辅助输入z_x,z_y），而S_1,S_2分别接收辅助输入z_1,z_2。$\mathcal{H}\subset\mathcal{P}$表示诚实参与方的集合，如果$P$是诚实的，即$P\in\mathcal{H}$，则$\text{out}_p$是参与方$P$的输出。若$P$被攻破，即$P\in\mathcal{P}/H$，则$\text{out}_p$是在协议期间$P$的视图。

真实世界中在各方$\mathcal{P}=(D_a,S_1,S_2)$和攻击者$\mathcal{A}=\left(\mathcal{A}_{\mathcal{D}_a},\mathcal{A}_{\mathcal{S}_1},\mathcal{A}_{\mathcal{S}_2}\right)$下，执行协议$\Pi$得到的每个部分视图$P^*\in\mathcal{P}$定义为

$$\text{REAL}_{\Pi,\mathcal{A},\mathcal{P},z}^{P^*}(k,x,y)=\left\{\text{output}_P:P\in H\right\}\cup\text{out}_{P^*}\quad(5)$$

在理想世界中，所有参与方与一个可信方交互，该可信方评估函数为f。挑战者DP_a将发送x,y给f。如果x或y中有一个是$\perp$，那么f返回$\perp$。最后，f返回$f\left(x,y\right)$给挑战者DP_a。如果P是诚实的，即$P\in\mathcal{H}$，则out_p为f返回参与方P的输出。如果P被攻破，即$P\in\mathcal{P}/H$，则out_p成为参与方P输出的值。理想世界中在各方$\mathcal{P}=(D_a,S_1,S_2)$和模拟器$\mathcal{S}=\left(\mathcal{S}_{\mathcal{D}_a},\mathcal{S}_{\mathcal{S}_1},\mathcal{S}_{\mathcal{S}_2}\right)$下，执行协议$\Pi$得到的每个部分视图$P^*\in\mathcal{P}$定义为

$$\text{IDEAL}_{f,\mathcal{S},\mathcal{P},z}^{P^*}(k,x,y)=\left\{\text{output}_P:P\in H\right\}\cup\text{out}_{P^*}\quad(6)$$

如果一个协议Π在真实世界中部分模拟了理想世界中函数f的执行，且对手是不串通，诚实且好

奇的，那么认为一个协议是安全的。

定义 4　令f为一个各方$\mathcal{P}=\left(D_a,S_1,S_2\right)$确定的功能函数，$\Pi$为一个$\mathcal{P}=\left(D_a,S_1,S_2\right)$下的协议。此外，$\mathcal{H}=\varnothing$，即集合$P$中的每个参与方$P\in\mathcal{P}$都是诚实且好奇的不串通方。$f$是$\Pi(\mathcal{P})$安全的，如果对所有诚实且好奇的不串通敌手$\mathcal{A}=\left(\mathcal{A}_{\mathcal{D}_a},\mathcal{A}_{\mathcal{S}_1},\mathcal{A}_{\mathcal{S}_2}\right)$、所有$x,y\in\left\{0,2^{\mu}-1\right\},z\in\left\{0,2^{\mu}-1\right\}$和所有组织$P\in\mathcal{P}$，存在一组概率多项式时间的模拟器$\mathrm{Sim}=\left(\mathrm{Sim}_{D_a},\mathrm{Sim}_{S_1},\mathrm{Sim}_{S_2}\right)$，使得

$$\left\{\mathrm{REAL}^{P^*}_{\Pi,\mathcal{A},\mathcal{P},z}(k,x,y)\right\}_{k\in\mathbb{N}}\approx\left\{\mathrm{IDEAL}^{P^*}_{f,\mathcal{S},\mathcal{P},z}(k,x,y)\right\}_{k\in\mathbb{N}}\tag{7}$$

其中，$\mathcal{S}=\left(\mathcal{S}_{D_a},\mathcal{S}_{S_1},\mathcal{S}_{S_2}\right)$，且$\mathcal{S}_{D_a}=\mathrm{Sim}_{D_a}\left(\mathcal{A}_{D_a}\right)$，$\mathcal{S}_{S_1}=\mathrm{Sim}_{S_1}\left(\mathcal{A}_{S_1}\right)$，$\mathcal{S}_{S_2}=\mathrm{Sim}_{S_2}\left(\mathcal{A}_{S_2}\right)$。

定理 2　如果MPEKS-PH能安全地实现定义4面向$\mathcal{A}=\left(\mathcal{A}_{\mathcal{D}_a},\mathcal{A}_{\mathcal{S}_1},\mathcal{A}_{\mathcal{S}_2}\right)$的基于模拟的安全，则该方案满足密文不可区分性和陷门不可区分性。

证明　假设MPEKS-PH不满足密文不可区分性或陷门不可区分性。本文证明MPEKS-PH不能根据定义4安全地实现。

假设有一个区分器$\mathcal{Z}$尝试去区分真实世界与理想世界。

1) 假设MPEKS-PH不满足密文不可区分性，也就是说，存在一个敌手$\mathcal{B}$，使式(3)是不可忽略的。$\mathcal{Z}$使$\mathcal{A}$或$\mathcal{S}$去攻破S_1(CS)。S_1是诚实的，$\mathcal{Z}$内部运行$\mathcal{B}$，$\mathcal{B}$将$\mathcal{W}_{\mathcal{F},0},\mathcal{W}_{\mathcal{F},1}\subseteq\mathcal{W}$发送给挑战者。

① $\mathcal{Z}$用$\left(\mathrm{BuildIndex}(),\mathcal{W}_{\mathcal{F},b}\right)$与$D_a$交互，其中$b\in 0,1$是一个随机比特。

② 在真实世界中，D_a发送I给$\mathcal{S}_1(\mathcal{A})$，然后$\mathcal{S}_1(\mathcal{A})$再发送给$\mathcal{Z}$。在理想世界中，$D_a$发送$\left(\mathrm{BuildIndex}(),\mathcal{W}_{\mathcal{F},b}\right)$给$f$，$f$发送$\left|\mathcal{W}_{\mathcal{F},b}\right|$给$\mathcal{S}$，$\mathcal{S}$计算出$I'$并发送给$\mathcal{Z}$。

当且仅当$\mathcal{B}$输出1时，$\mathcal{Z}$输出1。如果$\mathcal{Z}$与协议Π交互，那么$\mathcal{B}$会模拟I，因为$\mathcal{A}$扮演$\mathcal{A}_{\mathcal{S}_1}$的角色。如果$\mathcal{Z}$与$\mathcal{S}_{\mathcal{S}_1}$交互，那么$\mathcal{B}$会模拟$I'$，因为理想世界的对手$\mathcal{S}$扮演$\mathcal{S}_{\mathcal{S}_1}$的角色。

根据本文假设，在真实世界中存在一个攻击者$\mathcal{B}$，可以在区分陷门方面以不可忽略的优势输出1，而在理想世界中则以概率$\frac{1}{2}$输出1。显然，运行$\mathcal{B}$作为子程序的区分器$\mathcal{Z}$可以区分在真实世界执行中S_1方的部分视图与理想世界执行中的部分视图。也就是说，MPEKS-PH无法安全地实现。

2) 假设MPEKS-PH在定义1中不满足陷门不可区分性，也就是说，存在一个敌手$\mathcal{B}'$，使式(2)是不可忽略的。$\mathcal{Z}$使$\mathcal{A}$或$\mathcal{S}$去攻破S_1(CS)。S_1是诚实的，$\mathcal{Z}$内部运行$\mathcal{B}'$。

① $\mathcal{Z}$用$\left(\mathrm{Trapdoor}(),\mathcal{W}_{t,b}\right)$与$D_a$交互，其中$b\in 0,$是一个随机比特。

② 在真实世界中，SU发送td给$\mathcal{S}_1(\mathcal{A})$，然后$\mathcal{S}_1(\mathcal{A})$再发送给$\mathcal{Z}$。在理想世界中，SU发送$\left(\mathrm{Trapdoor}(),\mathcal{W}_{t,b}\right)$给$f$，$f$发送$|\mathcal{W}_{t,b}|$给$\mathcal{S}$，$\mathcal{S}$计算出td′并发送给$\mathcal{Z}$。

当且仅当$\mathcal{B}'$输出1时，$\mathcal{Z}$输出1。如果$\mathcal{Z}$与协议Π交互，那么$\mathcal{B}'$会模拟td，因为$\mathcal{A}$扮演$\mathcal{A}_{\mathcal{S}_1}$的角色。如果$\mathcal{Z}$与$\mathcal{S}_{\mathcal{S}_1}$交互，那么$\mathcal{B}'$会模拟td′，因为理想世界的对手$\mathcal{S}$扮演$\mathcal{S}_{\mathcal{S}_1}$的角色。

根据本文的假设，存在一个对手$\mathcal{B}'$能够在真实世界中区分陷门，以不可忽略的优势输出1，而在理想世界中以概率$\frac{1}{2}$输出1。显然，作为子程序运行$\mathcal{B}'$的区分器$\mathcal{Z}$能够区分参与方S_1的部分视图是在真实世界执行还是在理想世界执行。也就是说，该协议无法安全地实现MPEKS-PH。证毕。

3.7　MPEKS-PH安全证明

定理 3　本文提出的MPEKS-PH方案满足面向$\mathcal{A}=\left(\mathcal{A}_{\mathcal{D}_a},\mathcal{A}_{\mathcal{S}_1},\mathcal{A}_{\mathcal{S}_2}\right)$的基于模拟的安全。

证明

1) Sim_{D_a}模拟$\mathcal{A}_{\mathcal{D}_a}$的流程如下。首先随机选择$T$，然后计算$[T]_{\mathrm{pk}_{\mathrm{DO}}}\leftarrow\mathrm{Enc}_{\mathrm{pk}_a}(F)$，将$[F]_{\mathrm{pk}_{\mathrm{DO}}}$发送给$\mathcal{A}_{\mathcal{D}_a}$并输出$\mathcal{A}_{\mathcal{D}_a}$的全部视图。$\mathcal{A}_{\mathcal{D}_a}$的视图包含$[F]_{\mathrm{pk}_{\mathrm{DO}}}$。因为EPOM的语义安全[26]，$\mathcal{A}_{\mathcal{D}_a}$的视图在真实世界和理想世界中是不可区分的。

2) Sim_{S_1}模拟$\mathcal{A}_{S_1}$的流程如下。首先随机选择$\hat{F},\hat{t}\in\left\{0,\cdots,2^{\mu}-1\right\}$，通过运行$\mathrm{Enc}_{\mathrm{pk}_{\mathrm{DO}}(\hat{F})}$和$\mathrm{Enc}_{\mathrm{pk}_{\mathrm{SU}}(\hat{t})}$生成虚构的密文输入$[\hat{F}]_{\mathrm{pk}_{\mathrm{DO}}},[\hat{t}]_{\mathrm{pk}_{\mathrm{SU}}}$，并计算$[\mathrm{SUM}]_{\mathrm{pk}_{\mathrm{DO}}}$，$[\neg\hat{F}]_{\mathrm{pk}_{\mathrm{DO}}}$。随后根据$\mathrm{SBD}(\cdot)$生成$\hat{F},\hat{t}$的中间值

$[\neg\hat{F}]_{pk_{DO}}$,$[\hat{t}_i]_{pk_{SU}}$的密文，其中$i\in\{0,\cdots,\mu-1\}$。然后对于$i\in\{0,\cdots,\mu-1\}$，使用本文相同的算法计算$[\hat{d}_i]_{pk_{\sum SU}}$,$[\hat{e}_i]_{pk_{\sum SU}}$，随后根据随机选择的$\hat{r}$计算$[\hat{f}_i]_{pk_{\sum SU}}$，$[\hat{g}_i]_{pk_{\sum SU}}$。$Sim_{S_1}$将执行过程中所有的加密后的中间值发送给$\mathcal{A}_{S_1}$。如果$\mathcal{A}_{S_1}$返回⊥，则$\mathcal{A}_{S_1}$返回⊥。$\mathcal{A}_{S_1}$的视图包含其创建的加密值，$\mathcal{A}_{S_1}$都会收到$\hat{f}$，$\hat{g}$的加密。因为DO是诚实且好奇的，且EPOM是语义安全的，所以在真实世界和理想世界中，$\mathcal{A}_{S_1}$的视图是无法区分的。

3) Sim_{S_2}模拟$\mathcal{A}_{S_2}$的流程如下。首先在随机选择的数上计算并加密生成SBD(·)、SAD(·,·)和SMD(·,·)的加密中间值。Sim_{S_2}将这些加密中间值发送给$\mathcal{A}_{S_2}$。如果$\mathcal{A}_{S_2}$返回⊥，则Sim_{S_2}返回⊥。$\mathcal{A}_{S_2}$的视图包含其生成的加密值。在真实世界和理想世界中，$\mathcal{A}_{S_2}$都会收到执行过程中的中间值。在真实世界和理想世界的执行中，由于DO是诚实且好奇的以及EPOM的语义安全性，$\mathcal{A}_{S_2}$的视图是无法区分的。证毕。

根据定理1~定理3，本文有以下推论。

推论1 MPEKS-PH满足密文不可区分性、陷门不可区分性和搜索模式隐私。

4 实验及性能分析

4.1 性能对比

本文的MPEKS-PH方案使用Java进行模拟，采用分布式系统架构。KGC、CS、DO、SS和SU部署在配备2.7 GHz八核处理器和16 GB RAM的个人计算机上。对于支持多关键字搜索的比较方案PKE-FET[11]和IMPEKS[19]，服务器端和客户端均部署在配备2.7 GHz八核处理器和16 GB RAM的个人计算机上。与文献[26]类似，所有实验均在80 bit安全性下进行，其中N是一个1 024 bit长度的正整数[31]。系统中关键字的最大数量为4 000、6 000、8 000、10 000或12 000。本文对上述3种方案进行了计算开销和通信开销的评估。

图2展示了索引构建计算开销。由图2可知，IMPEKS方案使用倒排索引构建多项式作为索引生成的算法，其计算开销在关键词总数较少的情况下比本文方案小，但随着关键词总数的不断增加，本文方案几乎和IMPEKS方案的计算开销持平。PKE-FET方案的时间成本与最大关键词数量呈线性关系，在12 000个关键词时约为18.96 s。相比之下，本文方案的成本仅为9.24 s生成一个密文。

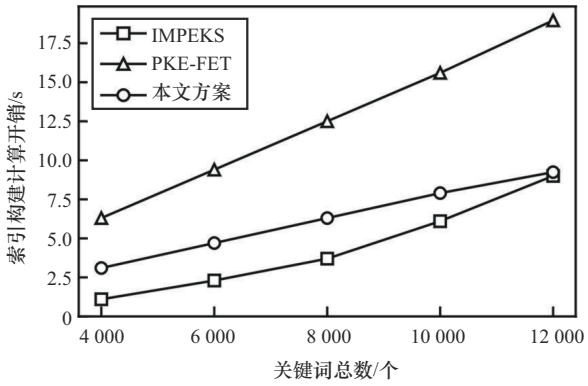


图2 索引构建计算开销

图3展示了陷门构建计算开销。由图3可知，IMPEKS[19]方案的时间成本几乎不与系统中的关键词总数相关，维持在2 s左右。PKE-FET方案使用多项式插值来计算陷门，导致随着最大关键词数量的增加呈现二次曲线，需要大约100 s来为12 000个关键词生成陷门。相比之下，本文方案的计算开销在12 000个关键词下约为13 s。

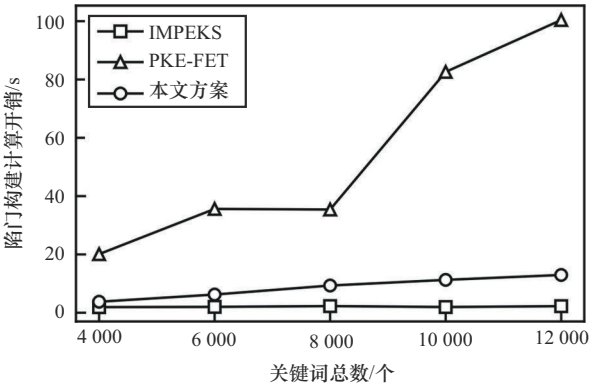


图3 陷门构建计算开销

图4展示了搜索计算开销。由图4可知，PKE-FET和IMPEKS方案的搜索计算开销比本文方案稍好，因为本文方案的测试需要多轮交互，并且网络时延严重影响了时间消耗。然而，随着关键词总数的增加，PKE-FET和IMPEKS方案的性能会下降，而本文方案的性能几乎保持恒定，这是因为本文采用了分布式系统架构，测试由多个并行的辅助服务器SS执行。随着关键词总数的增加，响应时间的差异将变得越来越小。同时，EPOM的执行效率与

其采用的同态加密算法的效率高度相关，这意味着随着同态加密领域的持续发展，本文方案能够通过更换EPOM所基于的PHE和FHE算法来获得更高的执行效率。

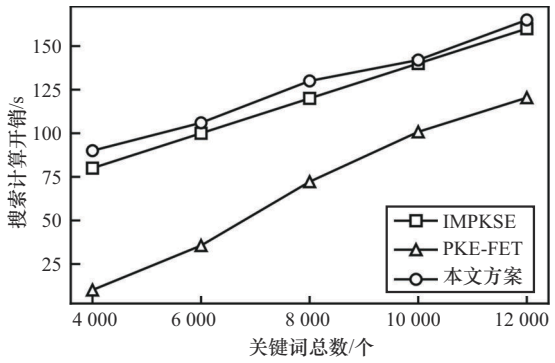


图4　搜索计算开销

图5展示了通信开销。由图5可知，本文在关键词总数设定为2 000个的情况下，通过改变搜索关键词数来比较3个方案的通信开销。IMPEKS方案的通信开销极大，这是因为其使用的倒排索引，需要为每个关键词生成匹配倒排索引的陷门，这会产生极大的通信开销。PKE-FET方案在搜索少量关键词的时候表现良好，但是通信开销会随着搜索关键词数的增大而增大。本文方案的通信开销是固定的，即无论搜索多少个关键词，本文生成的陷门大小是不变的。虽然在搜索关键词数较小的情况下本文方案较PKE-FET更差，但是本文方案通信开销与搜索关键词数无关，随着搜索关键词数的增加，本文方案的通信开销将会逐渐优于PKE-FET。

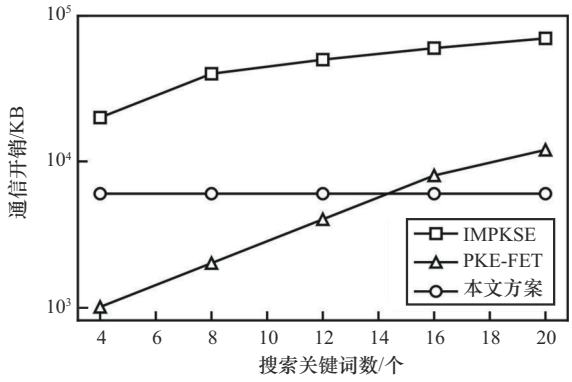


图5　通信开销

4.2　功能对比

本文方案与现有方案的功能对比如表2所示。单读者/单写者设置[9]只允许写者（所有者）自己发起查询，并指的是对称可搜索方案，其中写者和读者是同一方。单写者/多读者设置[14]指的是允许多个用户在特定写者生成的加密数据上进行搜索的方案。多写者/多读者设置支持每个用户加密并上传数据，并在所有用户的存储加密数据上进行搜索。

对于多关键字可搜索加密方案，陷门和密文大小是效率的重要指标。文献[9]的陷门和密文大小与$\mathcal{W}_{\mathrm{id}}$大小成线性关系，用户需保存搜索文档的关键字数量。文献[10]和文献[11]的陷门和密文大小随系统中关键字的最大数量$\mathcal{W}$增加而增加。文献[14]建立了文档及其每个包含的关键字之间的连接，因此密文大小与$\mathcal{W}_{\mathrm{id}}$成线性关系。这些搜索陷门是生成查询中每个关键字与存储的所有文档的每个标识符之间可能连接的指针。因此，这种连接的

表2　　**各方案功能对比**

方案	多读者	多写者	多关键词	抵抗KGA	索引大小	陷门大小	密文大小	分布式系统	搜索模式隐私	多类布尔搜索	访问模式隐私
本文方案	√	√	√	√	$\mathcal{O}(\lvert\mathcal{W}\rvert)$	$\mathcal{O}(\lvert\mathcal{W}\rvert)$	—	√	√	√	√
文献[9]	×	×	√	√	$\mathcal{O}(\lvert\mathcal{W}_{\mathrm{id}}\rvert)$	$\mathcal{O}(\lvert\mathcal{W}_{\mathrm{id}}\rvert)$	—	×	×	×	×
文献[10]	×	√	√	×	$\mathcal{O}(\lvert\mathcal{W}\rvert)$	$\mathcal{O}(\lvert\mathcal{W}\rvert)$	—	×	×	×	×
文献[11]	×	√	√	×	$\mathcal{O}(\lvert\mathcal{W}\rvert)$	$\mathcal{O}(\lvert\mathcal{W}\rvert)$	—	×	×	×	×
文献[14]	√	×	√	√	$\sum_{w\in\mathcal{W}}\lvert\mathrm{DB}[w]\rvert$	$\mathcal{O}(\lvert\mathrm{DB}\rvert\lvert Q\rvert)$	$\mathcal{O}(\lvert\mathcal{W}_{\mathrm{id}}\rvert)$	×	√	√	√
文献[19]	√	√	√	×	$\mathcal{O}(\lvert\mathcal{W}\rvert^3)$	$\mathcal{O}(\lvert\mathcal{W}\rvert^2)$	—	×	√	√	√
文献[21]	√	√	√	√	$\mathcal{O}(\lvert\mathcal{W}\rvert)$	$\mathcal{O}(1)$	—	√	√	×	√
文献[22]	√	√	×	√	$\mathcal{O}(\lvert\mathcal{W}\rvert)$	$\mathcal{O}(1)$	—	√	×	×	×

数量与查询中关键字数量$|Q|$和存储中文档数量|DB|均成线性关系。本文的陷门和密文都是一个十进制整数的同态加密，其长度与关键字数量无关。每个文档只需要一个可搜索密文来表示其所有基础关键字，因此存储在云中的可搜索密文数量为|DB|。此外，本文方案基本上支持多读者访问，而文献[10]和文献[11]中的方案需要为每个读者准备一个单独的密文以实现多读者访问，即$l \times |\mathrm{DB}|$个密文，其中l是读者数量。

由于传统PEKS方案中已知预期读者的公钥，这些方案不可避免地会受到KGA的影响。文献[10]利用第三类双线性映射来降低KGA的成功概率。文献[9]实际上是一个对称方案，其中密文和陷门的生成都需要用户的秘密密钥，因此除用户外的攻击者无法为测试生成密文。文献[11]通过将服务器的秘密密钥作为输入将测试能力委托给服务器，以防止外部攻击者自由测试，但仍然容易受到好奇的服务器内部KGA的影响。文献[14]是一个单写者/多读者方案，这意味着只有写者可以生成密文。然而基于倒排索引方案的文献[19]，其生成索引时需要为每个关键词链接文档，所以索引大小与陷门大小都较大，且与关键词数量成3次$\mathcal{O}\left(|\mathcal{W}|^3\right)$或2次$\mathcal{O}\left(|\mathcal{W}|^2\right)$关系。

本文方案将CS和SS的私钥作为测试的输入，因此包括CS或一组SS在内的攻击者无法自由测试并获取有关底层关键字的任何信息，从而抵抗KGA。并且索引大小与陷门大小仅与总关键词数量$|\mathcal{W}|$成线性关系。总而言之，本文方案从功能和性能综合来看，优于相关工作。

5 结束语

本文设计了一个隐藏模式的多关键词公钥可搜索加密方案。该方案基于公钥同态密码算法EPOM构建。多关键词搜索、多类布尔搜索、恒定大小的可搜索索引与搜索陷门满足了方案的功能性和实用性。而且本文方案在分布式环境下实现了多写者/多读者的存储访问模式，使拥有权限的用户可以在负载均衡的情况下查看其他数据拥有者的文档信息。然后本文对该方案进行了严格的安全证明，证明了该方案能够隐藏访问模式与搜索模式。最后将本文方案与相关公钥可搜索加密方案进行了实验评估，结果表明，本文所提分布式隐藏模式的多关键词公钥可搜索加密方案具有可行性，并在高安全需求、执行时间非高度敏感的场景下具有实用性。此外，本文虽然通过同态加密提升了方案的安全性，但是同态加密带来的低执行效率与引入假阳性带来的额外开销导致本文方案无法在时耗敏感型场景下进行实际应用，在应用场景上具有一定的局限性。

参考文献：

[1] CHEN D J, LIAO Z Y, XIE Z D, et al. MFSSE: multi-keyword fuzzy ranked symmetric searchable encryption with pattern hidden in mobile cloud computing[J]. IEEE Transactions on Cloud Computing, 2024, 12(4): 1042-1057.

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

[3] BONEH D, CRESCENZO G D, OSTROVSKY R, et al. Public key encryption with keyword search[C]//Advances in Cryptology-EUROCRYPT 2004. Berlin: Springer, 2004: 506-522.

[4] ISLAM M S, KUZU M, KANTARCIOGLU M. Access pattern disclosure on searchable encryption: ramification, attack and mitigation[C]// Proceedings of 19th Annual Network and Distributed System Security Symposium. Piscataway: IEEE Press, 2012: 1-15.

[5] CASH D, GRUBBS P, PERRY J, et al. Leakage-abuse attacks against searchable encryption[C]//Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security. New York: ACM Press, 2015: 668-679.

[6] POULIOT D, WRIGHT C V. The shadow nemesis: inference attacks on efficiently deployable, efficiently searchable encryption [C]//Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security. New York: ACM Press, 2016: 1341-1352.

[7] ZHANG Y P, KATZ J, PAPAMANTHOU C. All your queries are belong to us: the power of file-injection attacks on searchable encryption [C]// Proceedings of the 25th USENIX Conference on Security Symposium. Berkeley: USENIX Association, 2016: 707-720.

[8] LIU C, ZHU L H, WANG M Z, et al. Search pattern leakage in searchable encryption: attacks and new construction[J]. Information Sciences, 2014, 265: 176-188.

[9] WANG P S, WANG H X, PIEPRZYK J. Keyword field-free conjunctive keyword searches on encrypted data and extension for dynamic groups[C]// International Conference on Cryptology and Network Security. Berlin: Springer, 2008: 178-195.

[10] ZHANG B, ZHANG F G. An efficient public key encryption with conjunctive-subset keywords search[J]. Journal of Network and Computer Applications, 2011, 34(1): 262-267.

[11] HUANG K B, TSO R, CHEN Y C. Somewhat semantic secure public key encryption with filtered-equality-test in the standard model and its extension to searchable encryption[J]. Journal of Computer and System Sciences, 2017, 89: 400-409.

[12] FIAT A, NAOR M. Broadcast encryption[C]//Advances in Cryptology-CRYPTO'93: 13th Annual International Cryptology Conference. Ber-

lin: Springer, 1994: 480-491.

[13] 伍祈应, 马建峰, 苗银宾, 等. 多数据拥有者认证的密文检索方案[J]. 通信学报, 2017, 38(11): 161-170.
WU Q Y, MA J F, MIAO Y B, et al. Multi-owner accredited keyword search over encrypted data[J]. Journal on Communications, 2017, 38(11): 161-170.

[14] SUN S F, LIU J K, SAKZAD A, et al. An efficient non-interactive multi-client searchable encryption with support for Boolean queries[C]// Computer Security-ESORICS 2016. Berlin: Springer, 2016: 154-172.

[15] 杨旸, 林柏钢, 马懋德. 具有细粒度访问控制的隐藏关键词可搜索加密方案[J]. 通信学报, 2013, 34(S1): 92-100.
YANG Y, LIN B G, MA M D. Secure hidden keyword searchable encryption scheme with fine-grained and flexible access control[J]. Journal on Communications, 2013, 34(S1): 92-100.

[16] 宋衍, 韩臻, 李建军, 等. 支持安全共享的云存储系统研究[J]. 通信学报, 2017, 38(S1): 88-96.
SONG Y, HAN Z, LI J J, et al. Research on cloud storage systems supporting secure sharing[J]. Journal on Communications, 2017, 38(S1): 88-96.

[17] CHEN R M, MU Y, YANG G M, et al. Server-aided public key encryption with keyword search[J]. IEEE Transactions on Information Forensics and Security, 2016, 11(12): 2833-2842.

[18] CHEN R M, MU Y, YANG G M, et al. Dual-server public-key encryption with keyword search for secure cloud storage[J]. IEEE Transactions on Information Forensics and Security, 2016, 11(4): 789-798.

[19] WANG B, SONG W, LOU W J, et al. Inverted index based multi-keyword public-key searchable encryption with strong privacy guarantee[C]//Proceedings of the 2015 IEEE Conference on Computer Communications (INFOCOM). Piscataway: IEEE Press, 2015: 2092-2100.

[20] WANG Y L, SUN S F, WANG J F, et al. Achieving searchable encryption scheme with search pattern hidden[J]. IEEE Transactions on Services Computing, 2022, 15(2): 1012-1025.

[21] LIU X Q, YANG G M, SUSILO W, et al. Privacy-preserving multi-keyword searchable encryption for distributed systems[J]. IEEE Transactions on Parallel and Distributed Systems, 2021, 32(3): 561-574.

[22] TIAN P X, GUO C, JIE Y M, et al. Scan-free verifiable public-key searchable encryption supporting efficient user updates in distributed systems[J]. Journal of Information Security and Applications, 2023, 74: 103471.

[23] GOLDREICH O, OSTROVSKY R. Software protection and simulation on oblivious RAMs[J]. Journal of the ACM, 1996, 43(3): 431-473.

[24] CHOR B, KUSHILEVITZ E, GOLDREICH O, et al. Private information retrieval[J]. Journal of the ACM, 1998, 45(6): 965-981.

[25] SAMANTHULA B K K, CHUN H, JIANG W. An efficient and probabilistic secure bit-decomposition[C]//Proceedings of the 8th ACM SIGSAC Symposium on Information, Computer and Communications Security. New York: ACM Press, 2013: 541-546.

[26] LIU X M, DENG R H, CHOO K K R, et al. An efficient privacy-preserving outsourced calculation toolkit with multiple keys[J]. IEEE Transactions on Information Forensics and Security, 2016, 11(11): 2401-2414.

[27] BRESSON E, CATALANO D, POINTCHEVAL D. A simple public-key cryptosystem with a double trapdoor decryption mechanism and its applications[C]//Advances in Cryptology-ASIACRYPT 2003. Berlin: Springer, 2003: 37-54.

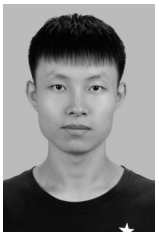
[28] FOUQUE P A, POINTCHEVAL D. Threshold cryptosystems secure against chosen-ciphertext attacks[C]//Advances in Cryptology-ASIACRYPT 2001.Berlin: Springer, 2001: 351-368.

[29] GENTRY C. A fully homomorphic encryption scheme[D]. Stanford: Stanford University, 2009.

[30] NISHIOKA M. Perfect keyword privacy in PEKS systems[C]//Proceedings of the 6th International Conference on Provable Security. New York: ACM Press, 2012: 175-192.

[作者简介]

聂旭云（1975– ），男，江西井冈山人，博士，电子科技大学教授，主要研究方向为密码学、网络安全、隐私保护等。



成驰（2002– ），男，河南济源人，电子科技大学硕士生，主要研究方向为可搜索加密、隐私计算等。

耿聪（2000– ），男，安徽滁州人，电子科技大学硕士生，主要研究方向为网络安全、互联网测量和审查等。

廖泽宇（1998– ），男，四川成都人，电子科技大学硕士生，主要研究方向为网络安全、可搜索加密等。

焦丽华（2002– ），女，四川成都人，电子科技大学硕士生，主要研究方向为数据安全、隐私保护等。

陈瑞东（1985– ），男，山西朔州人，博士，电子科技大学副研究员、硕士生导师，主要研究方向为软件漏洞挖掘、虚拟化安全与数据保护、匿名通信保护、安全开发等。

陈大江（1982– ），男，四川南充人，博士，电子科技大学副教授，主要研究方向为物联网安全、物理层安全、数据安全、隐私计算。