云环境下对称可搜索加密研究综述

黄一才* 李森森 郁 滨

(信息工程大学 郑州 450001)

摘 要：云存储技术是解决大容量数据存储、交互、管理的有效途径，加密存储是保护远程服务器中用户数据隐私安全的重要手段，而可搜索加密技术能在保证用户数据安全前提下提高系统可用性。对称可搜索加密以其高效的搜索效率得到人们的广泛关注。总体而言，相关研究可归纳为系统模型、效率与安全、功能性3个层次。该文首先介绍了对称可搜索加密(SSE)系统典型模型，然后深入分析了搜索效率优化、安全性分析的常用手段和方法，最后从场景适应能力、语句表达能力、查询结果优化3个方面对方案功能性研究进行了梳理，重点对当前研究的热点和难点进行了总结。在此基础上，进一步分析了未来可能的研究方向。

关键词：对称可搜索加密；安全云存储系统；云计算；前向隐私；后向隐私

中图分类号：TN918.4; TP399 **文献标识码**：A **文章编号**：1009-5896(2023)03-1134-13

DOI: 10.11999/JEIT211572

A Survey of Symmetric Searchable Encryption in Cloud Environment

HUANG Yicai LI Sensen YU Bin

(*Information Engineering University*, *Zhengzhou* 450001, *China*)

Abstract: The technology of cloud storage is an effective way to solve the problems in high-capacity data storage, interaction and management. Using encrypted data in cloud servers is an important means to protect the privacy and security of user data in remote servers. Searchable encryption technology can improve the system availability on the premise of ensuring the security of user data. For its search efficiency, the Symmetric Searchable Encryption (SSE) has become a hot research topic. In general, the related research can be summarized into three aspects: the system model, efficiency and security, and usability. Firstly, the typical models of Symmetric Searchable Encryption(SSE) system are introduced. Then, common methods for search efficiency optimisation and security analysis are analysed in depth in this paper. Finally, from the aspects of scene adaptability, sentence expression ability and query result optimization, the research on scheme usability is combed and the hot spots and difficulties of the current research are summarized. On this basis, the possible research hotspots in the future are further analyzed.

Key words: Symmetric Searchable Encryption(SSE); Security cloud storage system; Cloud compute; Forward private; Backward private

1 引言

云环境下数据与用户分离，导致数据隐私及存储安全问题成为制约其进一步应用的关键因素。安全云存储系统也称加密云存储系统，通过引入高强度密码算法保护云环境下用户数据隐私[1]，而加密是保护用户数据隐私的重要手段。然而，传统的加密方案尽管能有效保证数据机密性，但因无法基于密文数据进行有意义的运算，导致安全云存储系统中用户数据搜索困难。同态加密能够使密文数据保留与明文相似的计算特性，然而设计实用的全同态加密算法是困难的，且存在计算量较大的问题[2]，另一种可行的方法是在密文安全性上作出某种妥协，基于传统密码算法和假设模型设计可搜索加密方案(Searchable Encryption, SE)。

根据搜索时使用的密码算法，SE方案可分为非对称可搜索加密(Asymmetric Searchable Encryption, ASE)和对称可搜索加密(Searchable Symmetric Encryption, SSE)两类[1]。其中SSE因搜索过程采用对称加密算法，具有较高搜索效率，更适合云存储系统中大数据量的应用特点，成

收稿日期：2021-12-27；改回日期：2022-07-07；网络出版：2022-07-19
*通信作者： 黄一才 huangyicai3698@163.com
基金项目：国家自然科学基金(61772547)
Foundation Item: The National Natural Science Foundation of China (61772547)

为当前可搜索加密研究的热点[3,4]。本文的主要贡献包括：

(1)从系统模型、效率与安全、功能性3个方面对当前研究热点问题进行了分类整理，使各研究内容间相互关系更加清晰，同时，结合静态SSE方案定义，给出了一般模型下动态SSE方案的形式化描述。

(2)从方案实现时所采用的关键技术对研究工作进行了整理。不仅仅对方案的实现效果进行了分析，而且从不同方案采用的关键技术角度对方案进行分类整理，更有助于发现不同方案之间的相互关系，为方案的分析和对比研究提供帮助。

(3)整理了动态对称可搜索加密方案安全性定义及典型攻击方式。系统分析与整理安全性方面的研究，将安全性的定义扩展到一般模型，为方案构造中的安全性分析提供重要参考。

(4)分析了近年来国内外有关对称可搜索加密的最新研究成果。

2　系统模型

首先介绍SE加密方案的典型应用场景、安全性假设和方案的形式化定义，并在此基础上整理当前研究的热点问题。

2.1　应用场景描述

SE的典型应用场景涉及云环境下个人敏感数据存储以及医疗、政务、金融、邮件服务等诸多应用领域。文献[4–7]应用SE技术解决了医疗数据共享中个人隐私保护问题。SE适用场景主要包括单写单读(Single writer/Single reader, S/S)、多写单读(Multiwriter/Single reader, M/S)、单写多读(Single writer/Multireader, S/M)以及多写多读(Multiwriter/Multireader, M/M)4种[1]。

一个典型的单写多读可搜索加密云存储系统如图1所示，由数据拥有者(Data Owner, DO)、云服务器(Cloud storage server)和数据使用者(Data User, DU)组成。该场景中，若方案仅支持DO读取数据，即为单写单读(S/S)方案；若同时支持多个DO写入数据，则变成多写方案。尽管多写多读灵活性最高，但方案设计时难度也最大，实际研究中大多数方案属于单写单读(S/S)和单写多读(S/M)方案。

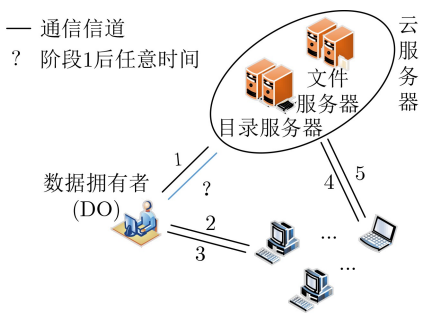

图 1 可搜索加密云存储系统“单写多读”应用场景示意

系统应用场景设定为多个DU访问DO存储在云服务器的文件，其中云服务器由密文目录服务器和文件服务器组成，假定：

(1)服务器为“诚实且好奇(honest but curious)”的。即服务器能忠实运行用户发出的请求，但也会尽可能地窥探用户个人隐私。

(2)只有DO是完全可信的，能够访问系统中所有的明文信息；各实体之间以及云存储服务器内部各通信信道均不可信，可能存在各种网络攻击行为。

(3)DU能够对具有访问权限的文档进行解密；DU在访问服务器前并不确定云服务器中存有哪些文件，以及是否包含其想要的文件。

(4)DO和DU可以为同一实体，也可能为不同实体。

基于以上假设，用户数据存储和搜索访问过程如下：

(1)文件加密前，DO通过计算，提取文档相关索引信息，将抽取到的索引进行盲化(比如编码、单向置换等)，然后使用对称密码算法将文档和索引分别加密后发往云服务器的目录服务器和文件服务器。

(2)DU向DO申请访问凭证。DO为每个DU_i $(i\in 1,2,\cdots,n)$生成不同的访问凭证。

(3)DO根据相关信息，为DU生成搜索凭证信息。

(4)DU利用搜索凭证，根据搜索关键词生成搜索陷门，并将搜索信息发送至目录服务器。

(5)目录服务器根据搜索陷门，对文档索引进行密文搜索，并将匹配文档索引发送至文件存储服务器，文件存储服务器读取相关密文文件发送至DU。DU采用与DO共享的文件加密密钥完成解密。

(6)数据上传服务器后，在协议运行的任一阶段，DO可以随时向云存储服务器申请对存储在服务器上的数据持有性和完整性进行验证。

2.2　形式化描述

若可搜索加密方案不支持密文数据的更新操作(如插入、删除等)，也称静态可搜索加密方案，反之称为动态可搜索加密方案。

假设数据库由$\mathbf{DB}=(\mathrm{id}_i,W_i)_{i=1}^{d}$文档地址/关键词集构成，其中$\mathrm{id}_i$为第$i$文档，$W_i$为文档$i$包含的关键词集合，$d$为数据库中文档的数量。参照文献[3, 8]给出的静态SSE方案形式化定义，动态SSE方案可用一个5元组来描述，即$\boldsymbol{\Pi}=(\mathrm{KenGen},\mathrm{Setup},\mathrm{Trapdoor},\mathrm{Search},\mathrm{Update})$，具体定义如下：

(1)$\mathrm{KenGen}\left(1^k\right)$。密钥生成算法。算法中，DO输入安全参数$k$，输出密钥$K$；

(2)Setup $(K, \mathbf{DB})$。索引生成算法。DO使用该算法生成密文的检索索引，输入密钥K和明文数据库$\mathbf{DB}$，输出密文索引I。在动态SSE方案中，通常设$I=\Phi$；

(3)Trapdoor (K, w, ind)。陷门生成算法。该算法包括检索陷门生成算法$\mathrm{Trapdoor}_{\mathrm{search}}(K, w)$和更新陷门生成算法$\mathrm{Trapdoor}_{\mathrm{update}}(K, w)$。无论静态或动态SSE方案均需包含$\mathrm{Trapdoor}_{\mathrm{search}}(K, w)$，一般由DU生成，输入密钥$K$和检索关键词$w$，输出检索陷门$T_w$；$\mathrm{Trapdoor}_{\mathrm{update}}(K, w, \mathrm{ind})$通常由DO生成，输入密钥$K$、更新关键词$w$和更新索引ind，输出检索陷门$T_u$，用于向服务器密文索引$I$添加或删除索引。

(4)Search (I, T_w)。搜索算法。该算法在服务器上执行，输入密文索引I和检索陷门T_w，输出包含检索关键词w的所有文档标识$\mathbf{DB}(w)$。其中SSE方案的正确性需要满足如下式所示的性质[3]，对于所有的$\mathbf{DB}$和$\boldsymbol{W}$，对任意的$w \in W$，满足

$$\mathrm{Search}(I, T_w) = \mathbf{DB}(w)$$

(5)Update $(\mathrm{I}, \mathrm{T}_u, \mathrm{op})$。更新算法。该算法大多需要在服务器上执行，输入密文索引I、检索陷门T_u和更新操作类型op，其中$\mathrm{op} \in \{\mathrm{add}, \mathrm{del}\}$，输出更新后的密文索引数据库$I'$。

2.3 研究热点

图2将当前对称可搜索加密的相关研究热点概括为系统模型、效率与安全、功能性3个方面。其中模型研究主要用于分析可搜索加密的不同应用场景及方案形式化描述方法。保证正确性的前提下，SE的研究大多包括方案的搜索效率及安全性两个方面，提高实际应用效果。同时通过提高查询语句的表达能力可进一步降低方案的计算和通信开销，优化查询结果(如对查询结果按照相关性排序)可使方案更易于使用。

(1)系统模型。研究不同应用场景下各参与实体的安全假设、系统结构、相互关系及方案形式化定义。

(2)效率优化。主要包括提高算法的搜索速度、减少存储开销和网络开销等内容，提高方案的实用性。

(3)安全性研究。主要包括以下两个方面，一是利用泄露函数对方案安全级别进行分析，并在此基础上，给出方案查询模式、访问模式及前/后向安全性定义。二是研究针对当前方案的有效攻击方式，通过引入新的技术手段改善方案抵抗某种攻击的能力。

(4)场景适应能力扩展。主要通过引入新的技术或优化系统结构，使原有方案支持“多写”或“多读”应用场景，并对该场景下方案的执行性能、安全性进行分析。

(5)查询语句表达能力扩展。实现通过一次查询搜索出更准确的查询结果，涉及单关键词搜索、连接关键词搜索、模糊搜索及语义搜索等热点问题。

(6)查询结果优化。根据文档与结果相关性对查询结果分级，提高查询结果的可用性，减少系统开销，同时基于恶意服务器假设，对查询结果的完整性、完备性和新鲜性进行验证。

尽管云服务器具有较强的计算资源，但在大数据量上的频繁数据搜索操作，服务器的搜索响应时间往往随着用户数量和存储数据量的增大急剧增加。在方案效率、安全性及功能性间寻找平衡点，是构造可搜索加密方案的关键和核心。

3 搜索效率优化

搜索特指在数据存储服务器接收数据使用者发送的查询请求后，在服务器中寻找匹配文档的过程。通过搜索效率优化即需要通过特殊结果或算法使搜索时计算度不与文件大小、匹配文档数据相关。

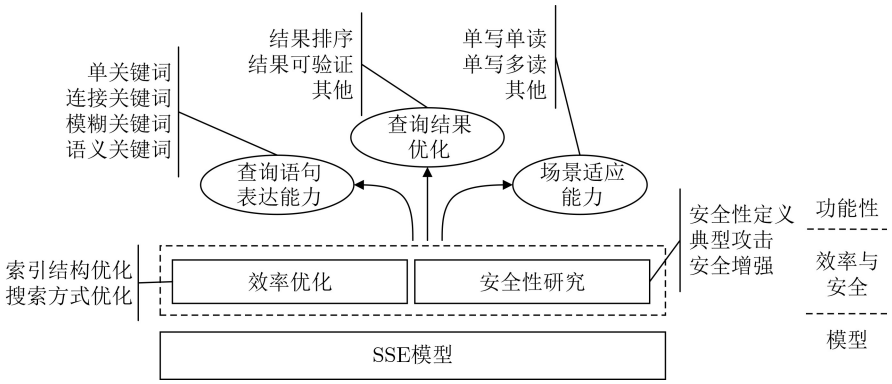

图 2 当前研究热点和关键问题

3.1 优化索引结构

Song等人[9]首次提出了可搜索加密的概念，并构造了对称可搜索加密方案，即SWP方案。方案在搜索过程采用对称加密算法实现，然而每次查询均需要遍历整个密文文件，且搜索时间与文件大小相关，搜索效率较低。同时泄露了关键词访问频次信息。Xu等人[10]指出这类方法尽管在搜索效率、动态更新等方面存在不足，但却不用提前构建索引，且在抵抗攻击方面具有特殊的优势。

在文档加密前为其建立关键词索引列表，搜索时只对索引进行操作可大大降低搜索复杂度，当前绝大部分可搜索加密方案均采用索引结构来实现。按照索引的组织方式，可以分为正排索引(the forward index)和倒排索引(the inverted index)两类。

正排索引是为每个文档建立一个关键词列表，这使得搜索时搜索复杂度与文档个数相关。Goh[11]为文档中搜索关键词映射为一个搜索矩阵，建立每一个文档的盲化搜索索引，构造了抗自适应选择关键词攻击(INDexes of semantic security against adaptive Chosen Keyword Attack, IND-CKA)的Z-IDX方案。

倒排索引是为每个关键词建立一个包含该关键词的文档列表，搜索复杂度与关键词个数相关。相比正排索引，倒排索引具有更好的搜索效率。Curtmola等人[8]构造了基于倒排索引的SSE方案。该方案的搜索复杂度与关键词个数相关，且检索过程只需要解密关键词对应文档节点。刘政等人[12]提出一种聚合索引结构的可搜索加密方案，通过减少关键词查询比较次数，提高倒排索引查询效率。

文献[13,14]提出采用结合正向和倒排两种索引结果的双向索引，提高了搜索效率。相比线性索引结构，文献[2]使用两个OMAP(Oblivious Map)结构，隐藏了服务器上存储器访问位置信息，构建树形索引搜索方案。研究表明，树形索引通常具有更好的搜索效率。

3.2 优化搜索方式

利用Bloom Filter能够快速查找集合元素的特点，可以降低搜索复杂度。Goh[11]利用Bloom Filter构建的Z-IND方案，提高了搜索效率，且搜索复杂度与文档关键词总长度无关。由于Bloom Filter在集合元素查找方面的显著优势，此后多个典型SSE方案均采用这一技术来实现。Suga等人[15]、Lai等人[16]分别采用Bloom Filter设计了支持模糊关键词查询和连接关键词查询的可搜索加密方案。然而Bloom Filter假阳性也会影响搜索结果的正确性。

将搜索操作拆分为多个子集上的并发操作，可大大减少搜索时间。文献[17]在不向云端透露语义数据的情况下将中心加密索引拆分为基于主题的碎片，提高搜索时并发性，从而显著改善了大数据量时算法的响应速度。文献[18]通过优化IO效率，提出了一种支持前向安全的SSE方案。

另一种解决思路是提前根据文档主题相关性，对文档进行分类存储，并在实际搜索时只对相关文档进行搜索，减少实际搜索的文档范围，从而提高搜索效率。文献[19]将关键词进行分类存储，对包含相同关键词文件采用隐藏结构相互关联，提高密文搜索时间。文献[20–22]采用聚类算法构造支持隐私保护和排序的密文检索方案。文献[6]首次介绍了一种采用专用硬件实现的可搜索加密方法，用于个人医疗数据隐私保护。

建立加密文档索引将文档内容与索引分开处理，在搜索效率和安全性上具有明显优势。数据量较大的云存储系统中，文档一般存储在多个服务器节点，引入支持并发计算的搜索算法，可极大提高实际搜索效率。

4 安全性研究

安全性研究通常包括以下两种思路：一是利用泄露函数对方案安全性进行理论分析，二是针对某类特殊的攻击对方案的构造过程进行优化。

4.1 安全性定义

Curtmola等人[8]首次给出了自适应安全SSE方案的正式定义，并广泛用于各类SSE方案的安全性分析。不失一般性，仿照Curtmola等人[8]自适应安全定义，设$\mathcal{A}$表示攻击者，$\mathcal{S}$表示模拟器，给出真实游戏$\mathrm{Real}_{\mathrm{A}}^{\Pi}$和理想游戏$\mathrm{Idea}_{\mathrm{A,S}}^{\Pi}$的工作过程。

$\mathrm{Real}_{\mathcal{A}}^{\Pi}(k)$。攻击者选择数据库$\mathbf{DB}$，DO运行$\mathrm{Setup}(\mathbf{DB})$算法生成检索索引$I$并发送给$\mathcal{A}$。攻击者A按一定规则选择一系列查询$q$，DO运行$\mathrm{Trapdoor}(q)$算法生成的$T_q$并发送给A。服务器运行$\mathrm{Search}(I,T_q)$，将运行的所有结果发送给A。最后，A输出一个比特$b$。

$\mathrm{Idea}_{\mathcal{A},\mathcal{S}}^{\Pi}$。模拟器初始化查询数组$q$。攻击者选择数据库$\mathbf{DB}$，DO运行$\mathcal{S}(\mathcal{L}(\mathrm{DB}))$算法生成检索索引I并发送给A。接着，攻击者A按一定的规则选择查询q。模拟器记录下查询$q[i]$，运行$\mathcal{S}(\mathcal{L}(q,\mathrm{DB}))$。最后，A输出一个比特$b$。

(1)泄露函数。泄露函数$\mathcal{L}$表示SSE方案在搜索过程中信息的具体泄露程度。

定义1　泄露函数$\mathcal{L}$定义为

$$\mathcal{L}=\Pr\left[\mathrm{Real}_{\mathcal{A}}^{\Pi}(k)=1\right]-\Pr\left[\mathrm{Idea}_{\mathcal{A},\mathcal{S}}^{\Pi}=1\right]$$

即真实游戏$\mathrm{Real}_{\mathcal{A}}^{\Pi}(k)$和理想游戏$\mathrm{Idea}_{\mathcal{A},\mathcal{S}}^{\Pi}$中A最终输出比特$b$相同的概率差值。A无法判断正在和真实游戏还是模拟游戏交互，证明攻击者除获得泄露函数$\mathcal{L}$外，无法获得关于用户数据的其他任何信息。

一个SSE方案Π，若攻击者A一次性产生所有查询q，则称攻击者A为非自适应的。若攻击者A能根据历史查询结果自适应选择查询q，且对于所有的多项式概率时间攻击者$\mathcal{A}$，存在一个高效的模拟器$\mathcal{S}$和一个可忽略函数negl，使得$\mathcal{L}<\mathrm{negl}(k)$，则$\Pi$是$\mathcal{L}$-自适应安全的。

(2)查询模式。查询模式也称检索模式，指询语句与关键词之间的对应关系，检索模式泄露即泄露了用户的两次查询是否相同。

定义2[3] 检索模式定义为一个$t\times t$的矩阵$\mathbf{SP}$

$$\left.\begin{array}{l}\mathbf{SP}[i,j]=1,\ Q_i=Q_j\\ \mathbf{SP}[i,j]=0,\ Q_i\neq Q_j\end{array}\right\}$$

其中，Q_i为第i次查询，t为总查询次数。

显然矩阵$\mathbf{SP}$满足$\mathrm{SP}[i,j]=1$(若$i=j$)，且$\mathbf{SP}$为对称矩阵，即$\mathrm{SP}[i,j]=\mathrm{SP}[j,i]$。当且仅当矩阵$\mathbf{SP}$为单位矩阵时，方案不泄露有关检索模式任何信息。

(3)访问模式。访问模式指查询结果包含了哪些文档，访问模式泄露即泄露了用户的检索到的文档标识。

定义3[3] 访问模式$\mathbf{AP}$定义为

$$\mathbf{AP}=\{\mathbf{DB}(Q_1),\mathbf{DB}(Q_2),\cdots,\mathbf{DB}(Q_t)\}$$

其中，$\mathbf{DB}(Q_i)$表示第i次查询时返回的查询结果。

访问模式和检索模式是两类重要的信息。攻击表明[23–25]利用访问模式和检索模式可以快速恢复出用户的查询关键词。采用ORAM技术隐藏访问模式和搜索模式具有理论安全性，但存在检索效率低，实际应用效果差的问题。Liu等人[23]在搜索关键词中加入多个伪关键词，达到隐藏搜索模式的目的。但引入大量伪关键词，也会导致搜索效率降低。Chen等人[26,27]基于d-隐私和差分隐私思想，设计了可搜索对称加密的差异私有访问模式，保护搜索时访问模式特征信息。Fu等人[28]提出有选择地增加特定的扰乱关键词，并在最终结果中删除扰乱结果，保护文档访问特征。但这实际上将导致服务器的搜索工作量和通信开销大幅提高，且剔除时处理实际结果和扰乱结果中相同文档将影响搜索结果准确性。文献[14]提出一种固定大小索引构造方案，隐藏返回索引大小信息。Shrishti等人[29]提出通过周期更新关键词索引向量表，使同一关键词在不同时间查询陷门不同，破坏查询特征及访问特征。然而，当系统中用户较多、索引规模较大时，周期性更新带来的巨大计算和通信开销将是一个不容忽视的问题。

(4)前向/后向隐私。如果更新查询不泄露正在更新的关键字/文档对中所涉及的关键字信息，则SSE方案是前向隐私(或前向安全)的。

定义4[30] 若更新泄露函数$\mathcal{L}^{\mathrm{Updt}}$表示为

$$\mathcal{L}^{\mathrm{Updt}}=\mathcal{L}'(\mathrm{op},\{(\mathrm{ind}_i,\mu_i)\})$$

如果op表示更新操作，集合$\{(\mathrm{ind}_i,\mu_i)\}$表示所有更新的文档中关键词$\mu_i$对文档$\mathrm{ind}_i$更新的次数。若$\mathcal{L}^{\mathrm{Updt}}$是状态无关的，则称一个$\mathcal{L}$-自适应安全SSE方案是前向隐私的。

后向隐私方案要求是搜索和更新泄露仅是$\mathrm{DB}(w)$的函数，仅泄露数据库中当前文档(不包括已删除的文档)。根据插入和删除条目泄露数据信息多少定义了安全强度由高至低的3种后向隐私。

定义5-1[30] 若查询$\mathcal{L}^{\mathrm{Srch}}$和更新$\mathcal{L}^{\mathrm{Updt}}$泄露函数写为

$$\mathcal{L}^{\mathrm{Updt}}(\mathrm{op},w,\mathrm{ind})=\mathcal{L}'(\mathrm{op})$$

$$\mathcal{L}^{\mathrm{Srch}}(w)=\mathcal{L}''(\mathrm{TimeDB}(w),a_w)$$

其中，$\mathcal{L}'$和$\mathcal{L}''$是无状态的，则称一个$\mathcal{L}$-自适应-安全SSE方案是插入特征泄露后向隐私的，通常也称Type I后向隐私。

目前，Moneta方案[30]、Orion方案[2]基于ORAM技术构建了该安全级别的可搜索加密方案。

定义5-2[30] 若查询$\mathcal{L}^{\mathrm{Srch}}$和更新$\mathcal{L}^{\mathrm{Updt}}$泄露函数写为

$$\mathcal{L}^{\mathrm{Updt}}(\mathrm{op},w,\mathrm{ind})=\mathcal{L}'(\mathrm{op},w)$$

$$\mathcal{L}^{\mathrm{Srch}}(w)=\mathcal{L}''(\mathrm{TimeDB}(w),\mathrm{Updates}(w))$$

其中，$\mathcal{L}'$和$\mathcal{L}''$是无状态的，则称一个$\mathcal{L}$-自适应-安全SSE方案是更新特征泄露后向隐私的，通常也称Type II后向隐私。

Mitra方案[2]、$\mathrm{Diana}_{\mathrm{del}}$方案[30]、Fides方案[30]，Aura方案[31]均构造了这一安全级别的可搜索加密方案。

定义5-3[30] 若查询$\mathcal{L}^{\mathrm{Srch}}$和更新$\mathcal{L}^{\mathrm{Updt}}$泄露函数写为

$$\mathcal{L}^{\mathrm{Updt}}(\mathrm{op},w,\mathrm{ind})=\mathcal{L}'(\mathrm{op},w)$$

$$\mathcal{L}^{\mathrm{Srch}}(w)=\mathcal{L}''(\mathrm{TimeDB}(w),\mathrm{DelHist}(w))$$

其中，是$\mathcal{L}$’和$\mathcal{L}$”是无状态的，则称一个$\mathcal{L}$-自适应-安全SSE方案是弱后向隐私的，通常也称Type III后向隐私。

Horus方案[2]、Janus方案[30]、Janus++方案[32]均属于这类安全级别的安全方案。

从定义看出，Type I安全性最强，Type III安全性最弱，且Type I后向隐私也必须是前向隐私的。如果一个方案同时满足前向隐私和Type III后向隐私，则更新查询泄露既不能与更新关键词(前向隐私定义要求)相关，也不能与更新文档索引(Type III后向隐私定义要求)相关，因此泄露只能限制在操作本身。

检索模式、访问模式、前向/后向安全性也是方案进行安全性分析的理论基础。各定义间相互关系如图3所示，其中前向隐私和后向隐私主要用于分析动态可搜索加密方案在更新(添加或删除)索引时的安全性。

表1为几种典型对称可搜索加密方案在前向/后安全性对比，其中**DB**表示整个文档集合，D为文档数，a_w为关键词w的匹配文档数，d_w表示关键词w的删除文档数，$n_w = a_w - d_w$。

4.2 常见攻击方式

由于可搜索加密本质上需要向服务器泄露某些明文特征或信息[4]，利用哪些泄露信息可以开展有效的攻击是当前方案设计与分析关注的重点问题。

(1)选择关键词攻击。文献[9]最早将可搜索加密的安全性定义为抗选择明文攻击安全，要求不可信服务器无法仅通过密文了解明文的任何的信息。然而研究表明，该模型不能满足可搜索加密实际应用中的安全需求。2003年，Goh[11]提出攻击者除以前的查询结果或其他渠道外，不能从其索引推断文件内容信息，并正式定义了安全索引，给出了抗选择关键词攻击语义安全(IND-CKA)的概念。

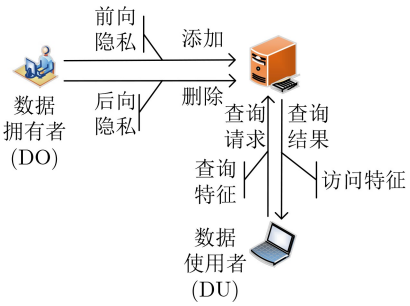

图 3 各安全定义之间的相互关系

Goh[11]通过改变IND – CKA游戏的挑战阶段，定义了增强模型，称为IND2 – CKA。Curtmola等人[8]指出IND2-CKA模型也只分析了那些不考虑以前的搜索陷门和搜索结果的对手，称为非自适应的。为此，通过在自适应下引入不可分辨性和基于仿真的定义，给出了抗选择关键词攻击的自适应安全概念。

Kurosawa等人[34]指出对于主动攻击者，如恶意服务器，可能伪造或删除加密文档的内容。文献[34]在抗选择关键词攻击的自适应安全模型下，基于UC(Universal Composability)安全模型定义了安全强度更高的UC-安全模型，使得协议在与其他协议任意组合的情形下，依然是安全的。

(2)文件注入攻击(file-injected Attacks)。文件注入攻击也称已知文件攻击，是恶意服务器假设条件下，利用SE方案泄露文件的访问特征恢复查询关键词的一类重要攻击方法。文献[35]通过文件注入攻击，服务器在已知关键词空间和具备文件注入能力的情况下，可以轻易恢复出文件关键词明文信息，通过进一步实验证明了采用简单安全增强方法均无法有效抵抗这种攻击。Wang等人[36]提出了一种基于有限集的改进文件注入攻击方法，进一步减少了服务器注入文件数目。文献[21]基于可搜索加密方案中文件访问特征信息泄露问题，提出了一种攻击方法，并针对该攻击，提出在向返回结果中适当添加噪声信息抵抗这种攻击。

文件注入攻击是搜索服务器利用可搜索加密的访问模式泄露信息恢复出查询关键词的一种有效攻击方式[35]，其成功的关键在于能够使用旧的陷门得到新注入文件的响应。而前向安全要求旧陷门无法查询到新的更新文件，因此满足前向安全就能够保证抵抗文件注入攻击[37]。

(3)推理攻击。文献[24]首次介绍了一种基于一定先验知识、利用数据访问模式泄露实施的通用攻击模型。攻击过程实际上是将用户搜索时行为模式和搜索习惯作为服务器额外信息。如通过监视用户与服务器之间的数据交互，记录搜索结果集合与陷

表 1　典型SSE方案对比

方案	特点	通信开销	计算开销	前向隐私	后向隐私
Song等人[9]	SWP	$O(n_w)$	$O(\mathrm{DB})$	×	×
Goh[11]	Bloom Filter	$O(n_w)$	$O(D)$	×	×
Sophos[33]	单向陷门置换	$O(n_w)$	$O(a_w + d_w)$	√	×
Diana $_{\mathrm{del}}$[30]	约束PRFs	$O(n_w + d_w \log_2 a_w)$	$O(a_w)$	√	Type III
Janus++[32]	SPE	$O(n_w)$	$O(n_w d_w)$	√	Type III
Aura[31]	SRE	$O(n_w)$	$O(n_w)$	√	Type II

门之间进行频率统计分析，结合公开数据库信息或已泄露文档信息进行比较，从而推理出更多有用信息。实验结果表明，攻击恢复关键词的成功率能够达到60%～80%，若对根据过程对方法进行调整，还能达到更好的攻击效果。利用类似的思想，文献[25,38]分别提出了多种具体的攻击方案，刘文心等人[37]将这类攻击统称为推理攻击。

抵抗推理攻击最有效的方式是隐藏返回结果中文件大小和数量信息。文献[26]使用HVE(Hiden Vector Encryption)方法设计了隐藏结果大小的SSE方案。

此外，关键词猜测攻击[39]、共谋攻击等也是当前可搜索加密方案安全分析中的常见攻击方式。随着攻击技术的不断成熟，某类典型攻击方式下方案安全性分析也逐渐成为近年来方案构造需要考虑的重要因素。

5 功能性扩展

除对方案的搜索效率和安全性进行研究外，构造SE方案中还需要针对其场景适应能力、查询语句表达能力和查询结果优化分别进行专门设计，以提高方案的实用性。

5.1 场景适应能力扩展

单写单读(S/S)一般适用于个人小规模数据加密存储，重点对正确性、安全性、搜索效率等方面进行分析[1, 11,13,33]。一种更实用的方案是支持S/M和M/M的可搜索加密方案，如医疗中多位医生共享病例信息，警察共享案件信息等。将传统S/S方案扩展至S/M场景，关键在于如何为多个DU安全构造查询陷门。

多用户可搜索加密方案的解决思路大体可以分为以下几类。

(1)引入密钥共享机制实现[8]。方案无须额外运行认证授权协议就可进行搜索，具有更高的执行效率。但多个用户共享加密密钥，易增加系统主密钥面临的风险，且难以区分各客户端数据访问权限。

(2)DU每次查询均向DO申请访问凭证。但这类方案每次搜索查询均需要在DU与DO之间进行交互，增加了搜索时的通信开销，且要求DO必须始终在线，另外相对DO，泄露了各DU使用数据时的查询特征。

(3)由DU和DO共同生成查询陷门。Sun等人[40]方案在陷门生成过程仍需DO参与。Kermanshahi等人[41]在Cash的OXT方案基础上，引入随机分布式密钥同态伪随机函数，使得在部分客户端参与下，就可生成查询令牌，而不要求DO始终在线。方案还同时支持授权撤消、抵抗服务器和DU子集间被动或主动合谋攻击等。

(4)引入第三方服务器参与陷门生成和用户管理。文献[42–45]提出通过引入可信的第三方服务器用于管理用户授权和撤消。但引入完全可信的第三方服务器对用户访问权限进行管理，在一定程度上影响了方案实用性。文献[46,47]引入“诚实且好奇”的代理服务器，构造了一种支持多用户且前向安全的动态可搜索加密方案。服务器直接参与搜索令牌生成，能够较好地保护访问特征信息，提高了方案安全性。但方案运行过程涉及公钥运算，方案执行效率影响不容忽视。提高多客户端与可信第三方之间通信效率，进而降低对原有可搜索加密方案效率的影响是一个难点问题。

当前满足“多写多读”应用场景的SSE方案及其可证明安全性方面的研究较少。值得一提的是，Wang等人[47]对多用户环境下DO使用不同密钥加密的索引进行搜索的应用场景进行了研究，提出了一种自适应令牌搜索方案。方案通过设计两层加密结构，保证多用户间密钥分享安全。当对多个不同密钥加密的索引进行搜索时，只需要向第三方服务器发送单个搜索令牌，由授权服务器生成各加密索引对应真实搜索令牌。方案也可推广至共享同一代理服务器的“多写多读”应用场景，可惜文中并未对具体过程进行深入研究。

由于引入多个DU，方案安全性上面临更多安全威胁，比如多读方案更易于遭受服务器或客户端子集的共谋攻击，访问权限的撤消、令牌信息泄露等。另外，将多用户环境下安全方案构造与传统方案中查询特征和访问特征保护、前/后向隐私等结合，构造新的安全方案将是值得研究的问题。

5.2 查询语句表达能力扩展

查询语句指DU向云服务器发送搜索请求时使用的陷门或令牌，其中包含DU想要查询关键词信息。查询语句表达能力影响着方案使用的便捷性，方便灵活的查询语句能够帮助用户更快找出想要的数据集合。

文献[8,11,30,32]等均属于支持单关键词的可搜索加密方案。这类方案更易于构建，便于分析，多以方案的安全性和搜索效率为研究重点。文献[40,48–50]研究了支持布尔运算的连接关键可搜索加密实现方案。但以上方案要求查询关键词必须与索引中的值完全一致，否则将无法搜索到正确的结果。

模糊关键词搜索加密是一类在输入搜索关键出现一定拼写错误的情况下，仍能够搜索出包含想要结果文档集合的可加密搜索方案。文献[51]基于关

键词之间的可编辑距离提出允许一定字符错误的模糊关键词加密方案。文献[17,52,53]构建了支持通配符查询的可搜索加密方案。文献[54]提出一种基于正则表达关键词搜索算法。以上方案本质上均是通过在构造关键词索引时，提前存储该关键的所有可能形式，并在搜索时对关键词的可能形式进行比对，达到模糊匹配的效果。但这要求预先存储所有关键词的各种组合，随着支持关键词长度的增加，索引规模将迅速扩大。为此，文献[55]利用局部敏感Hash函数相似输出会得到相似输出的特点，构建了关键词模糊搜索方案。文献[56]通过为每个关键词生成特征“指纹”，索引结构存储为指纹特征，由于指纹信息允许一定噪声，构造了一种基于关键词“指纹”特征的模糊关键词搜索方案。

模糊关键词搜索大多关注搜索词形差异，然而许多单词尽管词形相差较大，但从语义上却是相关的。2014年，文献[57]通过构造基于向量空间模型，比较文档索引向量空间模型与查询向量之间的相似度，返回分级的查询结果。该文献也被视为真正意义上基于语义的关键词可搜索加密方案。文献[58]采用语义关系数据库来评估语义距离实现了语义搜索加密，文献[59]使用关键词提取算法，动态建立词典，并基于词频信息返回分级查询结果，并在此基础上构建了基于语义的加密演示系统。文献[17]在文献[59]基础上，通过将搜索操作缩小到只与用户查询相关的物理存储空间，提高搜索时的并行执行能力，从而提高语义搜索操作的实时性。文献[60]使用主题模型(topic model)[61]实现文档语义关联，使用乘法同态加密算法构造了语义搜索方案。但搜索过程需要进行大量计算，存在大数据集上搜索效率不高的问题。设计语句表达能力更好的语义搜索SSE方案及其安全性分析尚待进一步深入研究。

5.3 查询结果优化

查询结果优化主要包括对搜索结果进行分级排序和不可信服务器，甚至恶意服务器假设下对搜索结果进行验证两个方面的研究内容。

(1)结果排序。结果排序是指将查询结果根据与查询关键词的匹配程度进行优化，使得用户能够迅速找到符合要求的文档，减少实际系统中网络传输开销，增加可用性。2014年Cao等人[62]采用基于“坐标匹配”的相似度测量和内积运算，提出了支持多关键词分级的可搜索加密方案。该方案提升了查询的隐私性，首次做到了多关键字可排序，但方案无法区分各个关键词的权重，且搜索阶段依然使用线性扫查询结果，搜索效率较低[63]。

在此基础上，文献[63,64]对搜索阶段进行优化，获得了亚线性时间的搜索复杂度，且方案支持文档更新操作。牛淑芬等人[65]在Xia等人[63]方案的基础上，使用加权统计算法衡量加密文件与搜索陷门之间的相似度，降低了传输过程的通信开销，并提高了密文检索的精确度和用户的查找效率。Dai等人[66]构造了高效多关键字排序搜索方案。Dai等人[67]结合可搜索加密中用户搜索意图的语义特征，提出了一种基于语义感知的加密云数据多关键字排序搜索方案。该方案在时间开销和空间利用上都优于现有的可搜索加密方案。Guo等人[68]提出了一种支持结果级的动态多步搜索方案。

根据相关性对查询结果排序可以提高系统实用性，但目前在可加密搜索结果排序的研究方面仍存在排序因素单一化、排序结果准确性不高以及方案实际执行开销过大等问题。

(2)结果可验证。云服务提供商可能因系统硬件故障，成本、计算资源等因素，向用户提供过期或不准确数据，甚至基于恶意服务器假设，服务器可能通过发送特殊消息序列(如文件注入攻击)破坏方案安全性。在这种假设下，需要对查询结果进行验证。可验证性研究主要包含如下几个方面[3,69]：(a)完整性：结果中的数据均应符合查询条件。(b)完备性：检索结果应包含全部满足查询条件的数据。(c)新鲜性：搜索结果应反映服务器中存储数据当前状态。

一种可行的方法是对搜索结果进行随机抽样，并对抽样结果进行完整校验。Chai等人[70]首次构造了可验证对称可搜索加密方案，防止服务器仅“诚实”运行部分数据集上的搜索而返回结果片段。Sun等人[71]提出了一种支持连接关键词查询的多关键词可验证方案，但搜索效率随着关键词数量增多而下降。Najafi等人[69]首次构造了一个支持动态数据更新和多关键词分级搜索的可验证搜索方案。Najafi等人[72]构造了支持多关键词查询的结果可验证对称可搜索加密方案。方案在计算复杂度、搜索效率等方面与通用方案相差不大，提高了验证方案的实用性。张中俊[73]设计一种支持结果完整性和完备性验证的对称可搜索加密方案，实验证明方案具有较高效更新和验证效率。

6 总结与展望

总体来看，近年来国内研究更多集中于方案安全性和功能性，而系统模型和搜索效率优化方面的研究还相对较少。对称可搜索加密的相关研究成果及未来研究热点梳理如表2所示。

相比同类研究，搜索效率是SSE方案的突出优

表 2 领域内研究方向的代表性研究成果及热点问题

方向		代表性研究成果	难点问题	未来值得关注的研究热点
系统模型	模型描述	方案形式化描述[3, 8]	更通用模型及模型的分析	通用模型不同场景下相互转化的方法和条件。
	应用场景	医疗、政务、通用存储等[4-7]	安全性、效率、功能性平衡	国内较成熟、影响力较大的应用较少
搜索效率优化	索引结构	正排索引[11]，倒排索引[8]，双向索引[13]、树形索引[14]，非索引结构搜索[9, 10]	索引准确性和适应未来应用的能力，索引安全对文件内容安全的影响	非索引结构中搜索效率优化及应用研究
	搜索方式	Bloom过滤器[15, 16]，并行搜索[17]，分类存储[19-22]	结果精确的SSE方案及云环境下性能测试与分析	结合磁盘数据存取特点或特殊硬件的索引结构优化；云环境下分布式数据存储效率优化
安全性研究	安全性分析	安全性定义[3, 8, 30]，前向/后向隐私[2, 30, 31]，其他典型方案[14, 23, 26, 28]	动态方案安全性分析、通信开销与安全性平衡问题	动态SSE方案安全性定义和分析方法；采用新技术设计安全性更高SSE方案
	攻击方式	选择关键词攻击[8, 11, 34]，文件注入攻击[35, 36]，推理攻击[24, 37]	推理攻击的预防问题	恶意服务器假设下方案抵抗攻击的能力研究
	场景适应能力	S/S[1, 11, 13, 33]，S/M[40-42, 44, 45, 47]	多用户场景下安全性研究	采用新技术实现的S/S方案；“多读”场景中不可信服务器假设下的安全性研究
功能性扩展	语句表达能力	单关键词[9, 11, 30-33]，连接关键词[40, 48, 50, 52]，模糊关键词[53, 55, 56]，语义关键词[57, 59, 61]	非集合扩展的模糊关键词搜索，现有语义模型应用于SSE方案的安全性分析	更灵活地模糊关键词搜索方案或语义关键词搜索方案研究
	结果优化	结果排序[65]，结果可验证[69-72]	空结果校验，动态方案验证，排序准确性等	实现大多依赖公钥算法，优化后对原SSE方案性能的影响值得关注

势，但研究发现SSE方案在加密数据共享、访问特征隐藏、抵抗可能存在的共谋攻击等方面也面临诸多挑战。保持对称加密效率的同时，结合非对称算法、同态加密、多方计算等，在效率、安全性和功能性之间寻找新的平衡点，对推动SSE方案进入实际应用具有重要意义。

参 考 文 献

[1] KAMARA S and LAUTER K. Cryptographic cloud storage[C]. Financial Cryptography and Data Security, Islands, Spain, 2010: 136–149. doi: 10.1007/978-3-642-14992-4.

[2] GHAREH CHAMANI J, PAPADOPOULOS D, PAPAMANTHOU C, *et al*. New constructions for forward and backward private symmetric searchable encryption[C]. 2018 ACM SIGSAC Conference on Computer and Communications Security, Toronto, Canada, 2018: 1038–1055. doi: 10.1145/3243734.3243833.

[3] 王赟玲, 陈晓峰. 对称可搜索加密技术研究进展[J]. 电子与信息学报, 2020, 42(10): 2374–2385. doi: 10.11999/JEIT190890.
WANG Yunling and CHEN Xiaofeng. Research on searchable symmetric encryption[J]. *Journal of Electronics & Information Technology*, 2020, 42(10): 2374–2385. doi: 10.11999/JEIT190890.

[4] ZHANG Rui, XUE Rui, and LIU Ling. Searchable encryption for healthcare clouds: A survey[J]. *IEEE Transactions on Services Computing*, 2018, 11(6): 978–996. doi: 10.1109/TSC.2017.2762296.

[5] LI Hongwei, YANG Yi, DAI Yuanshun, *et al*. Achieving secure and efficient dynamic searchable symmetric encryption over medical cloud data[J]. *IEEE Transactions on Cloud Computing*, 2020, 8(2): 484–494. doi: 10.1109/TCC.2017.2769645.

[6] YOSHIKAWA M, IKEZAKI Y, and NOZAKI Y. Implementation of searchable encryption system with dedicated hardware and its evaluation[C]. The 2018 9th IEEE Annual Ubiquitous Computing, Electronics & Mobile Communication Conference, New York, USA, 2018: 218–221. doi: 10.1109/UEMCON.2018.8796620.

[7] 刁冲. 可搜索加密在脑卒中电子病历数据共享隐私保护中的应用[D]. 北京: 北京交通大学, 2021. doi: 10.26944/d.cnki.gbfju.2021.003312.
DIAO Chong. The application of searchable encryption in data sharing privacy protection of cerebral apoplexy electronic medical record[D]. Beijing: Beijing Jiaotong University, 2021. doi: 10.26944/d.cnki.gbfju.2021.003312.

[8] CURTMOLA R, GARAY J, KAMARA S, *et al*. Searchable symmetric encryption: Improved definitions and efficient constructions[J]. *Journal of Computer Security*, 2011, 19(5): 895–934. doi: 10.3233/JCS-2011-0426.

[9] SONG D X, WAGNER D, and PERRIG A. Practical techniques for searches on encrypted data[C]. 2000 IEEE Symposium on Security and Privacy, Berkeley, USA, 2000: 44–55. doi: 10.1109/SECPRI.2000.848445.

[10] XU Min, NAMAVARI A, CASH D, *et al*. Searching encrypted data with size-locked indexes[C/OL]. Proceedings of USENIX Security Symposium, 2021: 4025–4042.

[11] GOH E J. Secure indexes[J]. *Cryptology ePrint Archive*, 2003, 2003: 216.

[12] 刘政, 王瑾璠, 齐竹云, 等. 一种高效的基于聚合索引的可搜索加密方案[J]. 计算机技术与发展, 2020, 30(12): 112–117. doi:

10.3969/j.issn.1673-629X.2020.12.020.

LIU Zheng, WANG Jinfan, QI Zhuyun, *et al*. An efficient searchable aggregated-indexing-based encryption scheme[J]. *Computer Technology and Development*, 2020, 30(12): 112–117. doi: 10.3969/j.issn.1673-629X.2020.12.020.

[13] HAHN F and KERSCHBAUM F. Searchable encryption with secure and efficient updates[C]. 2014 ACM SIGSAC Conference on Computer and Communications Security, Scottsdale, USA, 2014: 310–320. doi: 10.1145/2660267.2660297.

[14] KIM K S, KIM M, LEE D, *et al*. Forward secure dynamic searchable symmetric encryption with efficient updates[C]. 2017 ACM SIGSAC Conference on Computer and Communications Security, Dallas, USA, 2017: 1449–1463. doi: 10.1145/3133956.3133970.

[15] SUGA T, NISHIDE T, and SAKURAI K. Secure keyword search using bloom filter with specified character positions[C]. The 6th International Conference on Provable Security, Chengdu, China, 2012: 235–252. doi: 10.1007/978-3-642-33272-2_15.

[16] LAI Shangqi, PATRANABIS S, SAKZAD A, *et al*. Result pattern hiding searchable encryption for conjunctive queries[C]. 2018 ACM SIGSAC Conference on Computer and Communications Security, Toronto, Canada, 2018: 745–762. doi: 10.1145/3243734.3243753.

[17] WOODWORTH J W and SALEHI M A. S3BD: Secure semantic search over encrypted big data in the cloud[J]. *Concurrency and Computation:Practice and Experience*, 2019, 31(11): e5050. doi: 10.1002/cpe.5050.

[18] SONG Xiangfu, DONG Changyu, YUAN Dandan, *et al*. Forward private searchable symmetric encryption with optimized I/O efficiency[J]. *IEEE Transactions on Dependable and Secure Computing*, 2020, 17(5): 912–927. doi: 10.1109/TDSC.2018.2822294.

[19] 郑东, 王清瀚, 秦宝东. 一种轻量级的对称可搜索加密方案[J]. 西安邮电大学学报, 2020, 25(3): 1–6. doi: 10.13682/j.issn.2095-6533.2020.03.001.

ZHENG Dong, WANG Qinghan, and QIN Baodong. A lightweight symmetric searchable encryption scheme[J]. *Journal of Xi'an University of Posts and Telecommunications*, 2020, 25(3): 1–6. doi: 10.13682/j.issn.2095-6533.2020.03.001.

[20] NIRMALA E, MUTHURAJKUMAR S, and SUBITHA D. An efficient privacy-preserving ranked keyword search method[J]. *IOP Conference Series:Materials Science and Engineering*, 2017, 1084: 012103. doi: 10.1088/1757-899X/1084/1/012103.

[21] FREY B J and DUECK D. Clustering by passing messages between data points[J]. *Science*, 2007, 315(5814): 972–976. doi: 10.1126/science.1136800.

[22] CHEN Chi, ZHU Xiaojie, SHEN Peisong, *et al*. An efficient privacy-preserving ranked keyword search method[J]. *IEEE Transactions on Parallel and Distributed Systems*, 2016, 27(4): 951–963. doi: 10.1109/TPDS.2015.2425407.

[23] LIU Chang, ZHU Liehuang, WANG Mingzhong, *et al*. Search pattern leakage in searchable encryption: Attacks and new construction[J]. *Information Sciences*, 2014, 265: 176–188. doi: 10.1016/j.ins.2013.11.021.

[24] ISLAM M S, KUZU M, and KANTARCIOGLU M. Access pattern disclosure on searchable encryption: Ramification, attack and mitigation[C]. The 19th Annual Network and Distributed System Security Symposium, San Diego, USA, 2012.

[25] CASH D, GRUBBS P, PERRY J, *et al*. Leakage-abuse attacks against searchable encryption[C]. The 22nd ACM SIGSAC Conference on Computer and Communications Security, Denver, USA, 2015: 668–679. doi: 10.1145/2810103.2813700.

[26] CHEN Guoxing, LAI T H, REITER M K, *et al*. Differentially private access patterns for searchable symmetric encryption[C]. IEEE INFOCOM 2018 - IEEE Conference on Computer Communications, Honolulu, USA, 2018: 810–818. doi: 10.1109/INFOCOM.2018.8486381.

[27] 赵梓婷, 徐银, 宋祥福, 等. 基于差分隐私的多模式隐藏动态对称可搜索加密方案[J]. 计算机研究与发展, 2021, 58(10): 2287–2299. doi: 10.7544/issn1000-1239.2021.20210614.

ZHAO Ziting, XU Yin, SONG Xiangfu, *et al*. A multi-pattern hiding dynamic symmetric searchable encryption based on differential privacy[J]. *Journal of Computer Research and Development*, 2021, 58(10): 2287–2299. doi: 10.7544/issn1000-1239.2021.20210614.

[28] FU Zhangjie, LIU Yangen, SUN Xingming, *et al*. Confusing-keyword based secure search over encrypted cloud data[J]. *Mobile Networks and Applications*, 2020, 25(1): 125–132. doi: 10.1007/s11036-018-1195-8.

[29] SHRISHTI, BURRA M S, MAURYA C, *et al*. Leakage resilient searchable symmetric encryption with periodic updation[C]. The 2019 3rd International Conference on Trends in Electronics and Informatics, Tirunelveli, India, 2019: 22–29. doi: 10.1109/ICOEI.2019.8862626.

[30] BOST R, MINAUD B, and OHRIMENKO O. Forward and backward private searchable encryption from constrained cryptographic primitives[C]. 2017 ACM SIGSAC Conference on Computer and Communications Security, Dallas, USA, 2017: 1465–1482. doi: 10.1145/3133956.3133980.

[31] SUN Shifeng, STEINFELD R, LAI Shangqi, *et al*. Practical non-interactive searchable encryption with forward and backward privacy[C/OL]. The 28th Annual Network and

Distributed System Security Symposium, 2021. doi: 10.14722/ndss.2021.24162..

[32] SUN Shifeng, YUAN Xingliang, LIU J K, *et al*. Practical backward-secure searchable encryption from symmetric puncturable encryption[C]. 2018 ACM SIGSAC Conference on Computer and Communications Security, Toronto, Canada, 2018: 763–780. doi: 10.1145/3243734.3243782.

[33] BOST R. $\sum o\phi o\varsigma$: Forward secure searchable encryption[C]. 2016 ACM SIGSAC Conference on Computer and Communications Security, Vienna, Austria, 2016: 1143–1154. doi: 10.1145/2976749.2978303.

[34] KUROSAWA K and OHTAKI Y. UC-secure searchable symmetric encryption[C]. The 6th International Conference on Financial Cryptography and Data Security, Kralendijk, Bonaire, 2012: 285–298. doi: 10.1007/978-3-642-32946-3_21.

[35] ZHANG Yupeng, KATZ J, and PAPAMANTHOU C. All your queries are belong to us: The power of file-injection attacks on searchable encryption[C]. The 25th USENIX Security Symposium, Washington, USA, 2016: 707–720.

[36] WANG Gaoli, CAO Zhenfu, and DONG Xiaolei. Improved file-injection attacks on searchable encryption using finite set theory[J]. *The Computer Journal*, 2021, 64(8): 1264–1276. doi: 10.1093/comjnl/bxaa161.

[37] 刘文心, 高莹. 对称可搜索加密的安全性研究进展[J]. 信息安全学报, 2021, 6(2): 73–84. doi: 10.19363/J.cnki.cn10-1380/tn.2021.03.05.

LIU Wenxin and GAO Ying. A survey on security development of searchable symmetric encryption[J]. *Journal of Cyber Security*, 2021, 6(2): 73–84. doi: 10.19363/J.cnki.cn10-1380/tn.2021.03.05.

[38] LACHARITÉ M S, MINAUD B, and PATERSON K G. Improved reconstruction attacks on encrypted data using range query leakage[C]. 2018 IEEE Symposium on Security and Privacy, San Francisco, USA, 2018: 297–314. doi: 10.1109/SP.2018.00002.

[39] BYUN J W, RHEE H S, PARK H A, *et al*. Off-line keyword guessing attacks on recent keyword search schemes over encrypted data[C]. The 3rd Secure Data Management, Seoul, Korea, 2006: 75–83. doi: 10.1007/11844662_6.

[40] SUN Shifeng, LIU J K, SAKZAD A, *et al*. An efficient non-interactive multi-client searchable encryption with support for Boolean queries[C]. The 21st European Symposium on Research in Computer Security, Heraklion, Greece, 2016: 154–172. doi: 10.1007/978-3-319-45744-4_8.

[41] KERMANSHAHI S K, LIU J K, STEINFELD R, *et al*. Multi-client cloud-based symmetric searchable encryption[J]. *IEEE Transactions on Dependable and Secure Computing*, 2021, 18(5): 2419–2437. doi: 10.1109/TDSC.2019.2950934.

[42] BAO Feng, DENG R H, DING Xuhua, *et al*. Private query on encrypted data in multi-user settings[C]. The 4th International Conference on Information Security Practice and Experience, Sydney, Australia, 2008: 71–85. doi: 10.1007/978-3-540-79104-1_6.

[43] 曹素珍, 郎晓丽, 刘祥震, 等. 抗关键词猜测的授权可搜索加密方案[J]. 电子与信息学报, 2019, 41(9): 2180–2186. doi: 10.11999/JEIT181103.

CAO Suzhen, LANG Xiaoli, LIU Xiangzhen, *et al*. Delegate searchable encryption scheme resisting keyword guess[J]. *Journal of Electronics & Information Technology*, 2019, 41(9): 2180–2186. doi: 10.11999/JEIT181103.

[44] BAKAS A and MICHALAS A. Power range: Forward private multi-client symmetric searchable encryption with range queries support[C]. 2020 IEEE Symposium on Computers and Communications, Rennes, France, 2020: 1–7. doi: 10.1109/ISCC50000.2020.9219739.

[45] BAKAS A and MICHALAS A. Nowhere to leak: Forward and backward private symmetric searchable encryption in the multi-client setting (Extended Version)[J]. *Cryptology ePrint Archive*, 2021, 2021: 903.

[46] 卢冰洁, 周俊, 曹珍富. 一种增强的多用户前向安全动态对称可搜索加密方案[J]. 计算机研究与发展, 2020, 57(10): 2104–2116. doi: 10.7544/issn1000-1239.2020.20200439.

LU Bingjie, ZHOU Jun, and CAO Zhenfu. A multi-user forward secure dynamic symmetric searchable encryption with enhanced security[J]. *Journal of Computer Research and Development*, 2020, 57(10): 2104–2116. doi: 10.7544/issn1000-1239.2020.20200439.

[47] WANG Guofeng, LIU Chuanyi, DONG Yingfei, *et al*. IDCrypt: A multi-user searchable symmetric encryption scheme for cloud applications[J]. *IEEE Access*, 2018, 6: 2908–2921. doi: 10.1109/ACCESS.2017.2786026.

[48] WANG Jianfeng, CHEN Xiaofeng, SUN Shifeng, *et al*. Towards efficient verifiable conjunctive keyword search for large encrypted database[C]. The 23rd European Symposium on Research in Computer Security, Barcelona, Spain, 2018: 83–100. doi: 10.1007/978-3-319-98989-1_5.

[49] WU Zhiqiang and LI Kenli. VBTree: Forward secure conjunctive queries over encrypted data for cloud computing[J]. *The VLDB Journal*, 2019, 28(1): 25–46. doi: 10.1007/s00778-018-0517-6.

[50] WANG Yunling, WANG Jianfeng, SUN Shifeng, *et al*. Toward forward secure SSE supporting conjunctive keyword search[J]. *IEEE Access*, 2019, 7: 142762–142772. doi: 10.1109/ACCESS.2019.2944246.

[51] LI Jin, WANG Qian, WANG Cong, *et al*. Fuzzy keyword search over encrypted data in cloud computing[C]. 2010 Proceedings IEEE INFOCOM, San Diego, USA, 2010: 1–5. doi: 10.1109/INFCOM.2010.5462196.

[52] 于文. 支持通配符搜索的安全可搜索加密方案研究[D]. [硕士论文], 大连理工大学, 2019.
YU Wen. Research on secure searchable encryption scheme supporting wildcard search[D]. [Master dissertation], Dalian University of Technology, 2019.

[53] LIU Qin, PENG Yu, PEI Shuyu, *et al*. Prime inner product encoding for effective wildcard-based multi-keyword fuzzy search[J]. *IEEE Transactions on Services Computing*, 2022, 15(4): 1799–1812. doi: 10.1109/TSC.2020.3020688.

[54] SALEHI M A, CALDWELL T, FERNANDEZ A, *et al*. RESeED: Regular expression search over encrypted data in the cloud[C]. The 2014 IEEE 7th International Conference on Cloud Computing, Anchorage, USA: 2014, 673–680. doi: 10.1109/CLOUD.2014.95.

[55] 魏国富, 葛新瑞, 于佳. 支持数据去重的可验证模糊多关键词搜索方案[J]. 密码学报, 2019, 6(5): 615–626. doi: 10.13868/j.cnki.jcr.000327.
WEI Guofu, GE Xinrui, and YU Jia. Verifiable and fuzzy multi-keyword search scheme over encrypted cloud data supporting data deduplication[J]. *Journal of Cryptologic Research*, 2019, 6(5): 615–626. doi: 10.13868/j.cnki.jcr.000327.

[56] LIU Guoxiu, YANG Geng, BAI Shuangjie, *et al*. FSSE: An effective fuzzy semantic searchable encryption scheme over encrypted cloud data[J]. *IEEE Access*, 2020, 8: 71893–71906. doi: 10.1109/ACCESS.2020.2966367.

[57] FU Zhangjie, SUN Xingming, LINGE N, *et al*. Achieving effective cloud search services: Multi-keyword ranked search over encrypted cloud data supporting synonym query[J]. *IEEE Transactions on Consumer Electronics*, 2014, 60(1): 164–172. doi: 10.1109/TCE.2014.6780939.

[58] SUN Xingming, ZHU Yanling, XIA Zhihua, *et al*. Privacy-preserving keyword-based semantic search over encrypted cloud data[J]. *International Journal of Security and its Applications*, 2014, 8(3): 9–20. doi: 10.14257/ijsia.2014.8.3.02.

[59] WOODWORTH J, SALEHI M A, and RAGHAVAN V. S3C: An architecture for space-efficient semantic search over encrypted data in the cloud[C]. 2016 IEEE International Conference on Big Data, Washington, USA, 2016: 3722–3731. doi: 10.1109/BigData.2016.7841040.

[60] FU Zhangjie, XIA Lili, SUN Xingming, *et al*. Semantic-aware searching over encrypted data for cloud computing[J]. *IEEE Transactions on Information Forensics and Security*, 2018, 13(9): 2359–2371. doi: 10.1109/TIFS.2018.2819121.

[61] WANG Peng and RAVISHANKAR C V. On masking topical intent in keyword search[C]. The 2014 IEEE 30th International Conference on Data Engineering, Chicago, USA, 2014: 256–267. doi: 10.1109/ICDE.2014.6816656.

[62] CAO Ning, WANG Cong, LI Ming, *et al*. Privacy-preserving multi-keyword ranked search over encrypted cloud data[J]. *IEEE Transactions on Parallel and Distributed Systems*, 2014, 25(1): 222–233. doi: 10.1109/TPDS.2013.45.

[63] XIA Zhihua, WANG Xinhui, SUN Xingming, *et al*. A secure and dynamic multi-keyword ranked search scheme over encrypted cloud data[J]. *IEEE Transactions on Parallel and Distributed Systems*, 2016, 27(2): 340–352. doi: 10.1109/TPDS.2015.2401003.

[64] 李宇溪, 周福才, 徐剑, 等. 双服务器模型下支持相关度排序的多关键字密文搜索方案[J]. 计算机研究与发展, 2018, 55(10): 2149–2163. doi: 10.7544/issn1000-1239.2018.20180433.
LI Yuxi, ZHOU Fucai, XU Jian, *et al*. Multiple-keyword encrypted search with relevance ranking on dual-server model[J]. *Journal of Computer Research and Development*, 2018, 55(10): 2149–2163. doi: 10.7544/issn1000-1239.2018.20180433.

[65] 牛淑芬, 王金风, 王伯彬, 等. 区块链上基于B+树索引结构的密文排序搜索方案[J]. 电子与信息学报, 2019, 41(10): 2409–2415. doi: 10.11999/JEIT190038.
NIU Shufen, WANG Jinfeng, WANG Bobin, *et al*. Ciphertext sorting search scheme based on B+ tree index structure on blockchain[J]. *Journal of Electronics & Information Technology*, 2019, 41(10): 2409–2415. doi: 10.11999/JEIT190038.

[66] DAI Hua, DAI Xuelong, LI Xiao, *et al*. A multibranch search tree-based multi-keyword ranked search scheme over encrypted cloud data[J]. *Security and Communication Networks*, 2020, 2020: 7307315. doi: 10.1155/2020/7307315.

[67] DAI Xuelong, DAI Hua, YANG Geng, *et al*. An efficient and dynamic semantic-aware multikeyword ranked search scheme over encrypted cloud data[J]. *IEEE Access*, 2019, 7: 142855–142865. doi: 10.1109/ACCESS.2019.2944476.

[68] GUO Cheng, CHEN Xue, JIE Yingmo, *et al*. Dynamic multi-phrase ranked search over encrypted data with symmetric searchable encryption[J]. *IEEE Transactions on Services Computing*, 2020, 13(6): 1034–1044. doi: 10.1109/TSC.2017.2768045.

[69] NAJAFI A, JAVADI H H S, and BAYAT M. Verifiable ranked search over encrypted data with forward and

backward privacy[J]. *Future Generation Computer Systems*, 2019, 101: 410–419. doi: 10.1016/j.future.2019.06.018.

[70] CHAI Qi and GONG Guang. Verifiable symmetric searchable encryption for semi-honest-but-curious cloud servers[C]. 2012 IEEE International Conference on Communications, Ottawa, Canada, 2012: 917–922. doi: 10.1109/ICC.2012.6364125.

[71] SUN Wenhai, LIU Xuefeng, LOU Wenjing, *et al*. Catch you if you lie to me: Efficient verifiable conjunctive keyword search over large dynamic encrypted cloud data[C]. 2015 IEEE Conference on Computer Communications, Hong Kong, China, 2015: 2110–2118. doi: 10.1109/INFOCOM.2015.7218596.

[72] NAJAFI A, JAVADI H H S, and BAYAT M. Efficient and dynamic verifiable multi-keyword searchable symmetric encryption with full security[J]. *Multimedia Tools and Applications*, 2021, 80(17): 26049–26068. doi: 10.1007/s11042-021-10844-w.

[73] 张中俊. 前向安全的可验证对称可搜索加密方案研究[D]. [硕士论文], 西安电子科技大学, 2020.
ZHANG Zhongjun. Research on verifiable forward secure searchable symmetric encryption[D]. [Master dissertation], Xidian University, 2020.

黄一才：男，讲师，博士生，主要研究方向为安全云存储系统、移动存储、短距离无线通信安全等.

李森森：男，讲师，硕士，研究方向为物联网安全、安全云存储系统等.

郁 滨：男，教授，博士生导师，主要研究方向为信息安全、无线网络安全、视觉密码等.

责任编辑：马秀强