面向连接关键词可搜索加密的查询恢复攻击

杜瑞颖，沈蓓，何琨，赵陈斌，王贝宁，陈晶
（武汉大学国家网络安全学院，湖北 武汉 430040）

摘　要：为了恢复连接关键词可搜索加密方案中的用户查询，提出了2种针对连接查询可搜索加密方案的攻击方法，分别是交叉泄露攻击和频率匹配攻击。首先，从泄露中提取候选关键词集合；然后，分别利用关键词对结果模式泄露和查询频率信息进行过滤。结果表明，在交叉泄露攻击中，当攻击者仅掌握10%的数据集时，若关键词在空间为100，查询恢复的准确率可高达90%，将关键词空间扩大至1 000，攻击者依然能够恢复50%以上的查询；在频率匹配攻击中，即使攻击者仅已知不准确的频率分布信息，也至少可以准确恢复70%的查询。

关键词：云存储；可搜索加密；连接关键词查询；查询恢复攻击
中图分类号：TP309
文献标志码：A
DOI：10.11959/j.issn.1000–436x.2024141

Query recovery attacks against conjunctive keyword searchable encryption

DU Ruiying, SHEN Bei, HE Kun, ZHAO Chenbin, WANG Beining, CHEN Jing
School of Cyber Science and Engineering, Wuhan University, Wuhan 430040, China

Abstract: In order to recover user’s queries in conjunctive keyword searchable encryption schemes, two attacks against the conjunctive keyword searchable encryption schemes were proposed, such as cross leakage attack and frequency matching attack. Firstly, a set of candidate keywords were extracted from the leakage. Then the keywords were filtered according to the keyword pair result pattern leakage and query frequency information respectively. Results show that in the cross leakage attack, with knowledge of only 10% of the dataset, the accuracy of query recovery can reach up to 90% if the keyword space is 100. And more than 50% of the queries are still able to recovered by the attacker if the keyword space is expanded to 1 000. In frequency matching attack, even with only inaccurate frequency distribution information known to the attacker, at least 70% of queries can be accurately recovered.

Keywords: cloud storage, searchable encryption, conjunctive keyword search, query recovery attack

0　引言

随着云存储服务的不断扩展，用户能够随时在线访问存储在云服务器的数据。对称可搜索加密（SSE, symmetric searchable encryption）技术允许用户将加密数据外包给云存储提供商，同时保留用户对数据的检索功能。这一概念由Song等[1]首次提

收稿日期：2024–03–26；修回日期：2024–06–28
通信作者：何琨，hekun@whu.edu.cn
基金项目：国家重点研发计划基金资助项目（No.2021YFB2700200）；中央高校基本科研业务费专项资金资助项目（No.2042022kf1195）；国家自然科学基金资助项目（No.62172303）；湖北省重点研发计划基金资助项目（No.2021BAA190, No.2022BAA039）；山东省重点研发计划基金资助项目（No.2022CXPT055）
Foundation Items：The National Key Research and Development Program of China (No.2021YFB2700200), The Fundamental Research Funds for the Central Universities (No.2042022kf1195), The National Natural Science Foundation of China (No.62172303), The Key Research and Development Program of Hubei Province (No.2021BAA190, No.2022BAA039), The Key Research and Development Program of Shandong Province (No.2022CXPT055)

出。之后，Curtmola等[2]给出了SSE的正式安全定义，并提出了逆向索引的存储结构。在典型的SSE方案中，用户首先使用对称加密技术对数据库加密，同时生成搜索索引，将索引和密文数据一起发送给服务器。用户通过生成查询令牌来执行查询，服务器计算与令牌匹配的索引，然后返回用户查询的加密文档。

SSE的理想目标是高效、安全地支持与纯文本数据库一样丰富的查询类型。统计数据显示，40%的美国网民在在线搜索中使用了包含2个关键词的查询，查询中包含3个关键词的占比为22.74%，均高于19.46%的单关键词查询的占比。因此，实用的SSE方案至少应该支持连接关键词查询，简称连接查询，即给定一组关键词，方案能够找到并返回包含所有这些关键词的条目。Cash等[3]提出了第一个支持次线性时间内搜索的连接查询SSE方案，称为不经意交叉标签（OXT, oblivious cross-tag）方案。OXT中包含TSet和XSet这2个存储结构，Lai等[4]指出在索引过程中XSet结构存在关键词对结果模式（KPRP, keyword pair result pattern）泄露，并在此基础上提出交叉隐藏标签（HXT, hidden cross-tag）方案，提高了连接查询的安全性。

为了平衡安全性和效率，SSE方案在执行查询时，即使数据库和查询令牌是加密的，也会向服务器泄露某些信息。例如，搜索模式揭示哪些查询涉及相同的关键词，访问模式揭示匹配查询的所有文档标识符。通常SSE方案在搜索模式和访问模式中泄露信息以提高效率，这些模式对数据隐私并不构成直接威胁，但攻击者仍能利用它们进行攻击，还原查询甚至数据集本身。为了抵御这些攻击，研究人员提出了隐私保护的SSE方案。例如，基于不经意随机访问机（ORAM, oblivious RAM）的方案[5-6]能够完全隐藏搜索模式，但需要昂贵的带宽、计算和存储成本，并且仍然可能泄露响应量，即查询结果中包含的文档个数。

根据攻击者能力，当前利用访问模式和搜索模式的攻击可以分为2种类型：主动攻击[7]，又称注入攻击，攻击者拥有向数据库中注入特定内容的能力；推理攻击[8-14]，攻击者可以在连续的时间周期内观察泄露模式，结合对数据集的背景知识进行攻击。当攻击目标为用户查询时，推理攻击也称查询恢复攻击。

自Islam等[8]提出了首个面向单关键词SSE的查询恢复攻击以来，许多攻击者在不同的假设下提出了相似的攻击。攻击者利用访问模式和搜索模式泄露[9-13]及用户的查询频率[14]，不断推理出查询的底层关键词。

具体而言，在单关键词查询方案中，每个关键词对应的查询令牌相同。通常，攻击者可以观察查询令牌及其对应的加密文档索引，并构建2个矩阵：令牌共现矩阵，记录不同令牌在同一文档中出现的次数；关键词共现矩阵，记录不同明文关键词在同一文档中出现的次数。然后利用模拟退火[15]等多目标优化算法将查询令牌和明文关键词进行匹配。然而，连接查询方案中的查询令牌和搜索结果文档均包含多个关键词的信息，攻击者也无法根据数据库构建多个关键词的共现矩阵。基于上述考虑，现有的单关键词查询恢复攻击方案均不适用于连接查询场景。与此同时，连接查询SSE方案中存在特有的可利用泄露[3-4,16]，但迄今为止尚未提出针对连接查询SSE的攻击方案。

本文主要研究针对连接查询SSE方案的查询恢复攻击。攻击者是一个诚实但好奇的服务器，遵循协议但希望通过被动观察系统来推断用户查询的关键词。

本文的主要贡献如下。

1) 利用KPRP泄露，分离出连接查询访问模式中单个关键词的泄露，提出面向连接关键词查询方案的查询恢复攻击，称为交叉泄露攻击。

2) 进一步假设攻击者未知KPRP泄露，通过将连接查询的查询频率信息与背景频率信息进行匹配，提出另一种面向连接关键词查询方案的查询恢复攻击，称为频率匹配攻击。

3) 对上述2种攻击进行了实际数据集的评估。实验结果显示，即使在仅已知10%的数据集和背景知识中频率分布不准确的情况下，交叉泄露攻击和频率匹配攻击依然具有较高的攻击准确率。

1 相关工作

1.1 连接查询可搜索加密

SSE是一种搜索保护技术[2]，可以在支持加密数据检索的同时保护用户的隐私。针对SSE逐渐多样化的应用场景，单关键词检索已经不能满足用户的检索需求，因此支持多模式的SSE备受关注，包

括动态性[17-20]、模糊搜索[21]、多用户[22-23]和范围查询[24-25]等。

现有的连接查询 SSE 方案基于 OXT 方案[3]和 HXT 方案[4]实现，其区别在于 HXT 方案利用向量隐藏加密（HVE, hidden vector encryption）技术消除了 OXT 方案中的 KPRP 泄露。Wang 等[26]将 OXT 扩展为多用户场景，Patranabis 等[16]将 OXT 方案扩展为动态版本，Yuan 等[20]将 HXT 方案扩展为动态版本，并提出了 KPRP 隐藏的连接关键词查询方案，然而访问模式和搜索模式泄露仍然对连接查询 SSE 方案构成了重大威胁。

1.2　查询恢复攻击

推理攻击是一种针对 SSE 的被动攻击类型，根据攻击目标不同可以分为数据库恢复攻击和查询恢复攻击：数据库恢复攻击针对范围查询方案，过去的研究着重于如何利用基于范围查询的访问模式泄露来恢复数据集中的属性值[27-28]；查询恢复攻击大致分为真实数据攻击和统计数据攻击 2 类，前者了解真实数据库的全部或部分内容，后者只拥有关于数据库的统计信息，例如一组非索引文档。

1) 真实数据攻击。针对单关键词查询 SSE 方案，IKK 攻击[8]使用访问模式泄露来恢复用户查询。它假设攻击者拥有完整数据集和部分已知查询，利用访问模式泄露来计算体积共现矩阵，并利用特征比较函数解决二次优化问题。Cash 等[12]证明，当关键词集合很大，如包含 2 500 个关键词时，IKK 表现不佳，并提出了一种计数攻击，该攻击只需部分数据集知识，基于响应量（即查询匹配的文档数量）来恢复关键词。Blackstone 等[13]提出了一种基于子图的攻击，采用了与计数攻击不同的细化启发式算法，在精确度上优于计数攻击。Ning 等[9]提出了一种真实数据攻击，同时实现了关键词和文档的恢复。

2) 统计数据攻击。Liu 等[14]提出的攻击仅依赖于搜索模式泄露，该攻击为它观察到的每个不同的查询令牌分配一个标签，并利用搜索模式泄露监控每个标签的查询频率。攻击者可以通过比较标签查询频率分布和辅助文档中的关键词查询频率分布来恢复每个标签的底层关键词。Oya 等[10]指出，可以同时利用访问模式和搜索模式信息，使用最优求解器[29]解决关键词线性分配的问题，达到更好的攻击效果。Xu 等[30]在动态场景下提出了一种查询恢复攻击，利用更新前后同一个关键词的对应文档个数和大小的差值，结合查询频率信息恢复查询。Gui 等[31]从 SSE 系统的角度重新定义泄露，并指出现有的访问模式隐藏方案只关注索引检索阶段，而忽略了文档索引阶段的泄露。他们提出的统计数据攻击方案可以忽略大部分抑制泄露的 SSE 方案，实现更实际有效的攻击。

统计数据攻击看似对攻击者的假设较弱，但在现实中通常不适用，因为获得一个独立但在“统计上接近”目标数据库的相似数据库相当困难。如引言中所述，现有的查询恢复攻击方案均不支持连接查询。本文将针对这些问题展开研究，提出合理的攻击假设和模型，达到恢复连接查询的目的。

2　理论基础

2.1　连接查询可搜索加密系统模型

连接查询可搜索加密系统模型由用户端和服务器端组成。考虑以下场景，为了节省存储空间，用户将隐私数据库加密后上传到不受信任的服务器进行存储，并仍然保留对该数据库进行查询的能力。在整个过程中，用户期望保持每次查询的关键词和数据库内容的保密性。

形式上，连接查询可搜索加密协议 $\sum$ 的语法由 Setup 算法和 Search 协议组成。

$(\mathrm{key},\sigma,\mathrm{EDB}) \leftarrow \mathrm{Setup}(\mathrm{DB},1^{\lambda})$ 是一种由用户运行的概率多项式时间算法，以数据库 DB 和安全参数 λ 作为输入，为用户输出密钥 key、状态 σ 和加密后的数据库 EDB，用户保存密钥 key 并将 EDB 上传至服务器。

$(\mathrm{DB}(q);\perp) \leftarrow \mathrm{Search}(\sigma,\mathrm{key},q;\mathrm{EDB})$ 是一个在用户和服务器之间运行的协议，用户以状态 σ、密钥 key 和查询 q 作为输入，服务器以 EDB 作为输入。协议结束时，用户收到一组包含 q 中所有关键词的文档标识符集合 DB(q)。本文用 w 表示关键词，连接查询 $\psi(q)=w_1 \wedge w_2 \wedge \cdots \wedge w_n$，在下文中简单表示为 $q=(w_1,w_2,\cdots,w_n)$。

如果对任意数据库 DB 和任意查询 q，Search 协议返回匹配查询的所有文档，则该 SSE 方案是完全正确的，本文只关注完全正确的 SSE 方案。

表 1 给出了本文用到的参数及其含义。攻击者拥有以下背景知识：关键词空间 Δ；文档 id_i 中包含的关键词 $W(\mathrm{id}_i)$；包含关键词 w 的所有文档标识符

$\mathrm{DB}(w)=\{\mathrm{id}_1,\mathrm{id}_2,\cdots,\mathrm{id}_{\mathrm{SP}(w)}\}$，其中，$\mathrm{SP}(w)=|\mathrm{DB}(w)|$表示$w$对应的文档个数。攻击者的目标是恢复查询$q$中的所有关键词$(w_1,w_2,\cdots,w_n)$。

表1　参数及其含义

参数	含义
w	关键词
K	关键词空间大小
Δ	关键词空间$\Delta=\{w_1,w_2,\cdots,w_K\}$
q	查询$q=(w_1,w_2,\cdots,w_n)$
n	查询中关键词个数
id_i	第i个文档的标识符

2.2　目标方案

实现连接查询的一种直接方法是对每个关键词单独执行搜索，然后由服务器或用户处理结果文档之间的交集。将连接查询简化为单关键词的情况，并对查询结果进行合取操作。这种方法的查询复杂度为$\sum_{i=1}^{n}\mathrm{DB}(w_i)$。

然而，上述方法有2个缺点：一是低效，如果其中一个连接词是“性别=女性”，则会得到一半数据库大小的中间结果；二是信息泄露严重，该方法暴露查询中每个关键词的访问模式和匹配文档的数量。

2.2.1　OXT

Cash等[3]首次提出查询复杂度为次线性的连接查询方案OXT。在查询$q=(w_1,w_2,\cdots,w_n)$中，w_1是查询频率最小的关键词（在所有查询关键词中，对应文档数量最少），记作s项，那么查询q可以写成$q=(s,w_2,\cdots,w_n)$。

OXT方案包含2个存储结构：TSet和XSet。TSet是一种用于高效SSE的扩展加密倒排索引数据结构，记录了每个关键词与包含该关键词文档索引的对应关系，且已经在单关键词SSE方案中充分实例化。XSet存储数据库中每个关键词文档对(w,ind)的交叉索引标签。具体来说，用户执行查询时，生成用于检索s项对应文档的检索陷门$\mathrm{stoken}(s)$，以及用于过滤文档的交叉陷门$\mathrm{xtoken}(s,w_i),i=2,3,\cdots,n$。

执行查询时，用户使用$\mathrm{stoken}(s)$在TSet中检索出对应的文档集合$\mathrm{DB}(s)$，再用交叉陷门$\mathrm{xtoken}(s,w_i)$和XSet过滤出$\mathrm{DB}(s)$中包含w_i的文档$\mathrm{DB}(s)\cap\mathrm{DB}(w_i)$。根据用户发送的所有$\mathrm{xtoken}(s,w_i)$，服务器过滤出最终的搜索结果$\mathrm{DB}(s)\cap\cdots\cap\mathrm{DB}(w_n)$。OXT方案如图1所示，用户分别生成包含$s$项的对应文档$(\mathrm{id}_1,\mathrm{id}_4)$和其他关键词信息$(w_2,w_3)$的4个交差陷门并发送给服务器，服务器则根据这些陷门和XSet结构依次判断$(w_2,\cdots,w_n)$是否包含在s项对应的文档中。

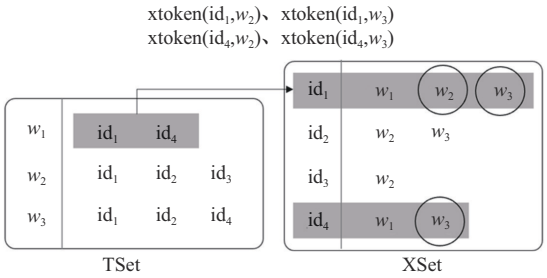


图1　OXT方案

2.2.2　HXT

Lai等[4]指出，OXT方案会泄露KPRP，KPRP泄露查询中频率最小的关键词对应的每一个文档是否包含其他关键词。为了减轻上述泄露，他们提出了HVE技术和概率布隆过滤器索引，并基于这2种加密原语构建了一种泄露隐藏的HXT方案。OXT方案的KPRP泄露主要来自XSet结构，它需要利用单个关键词文档对(w,ind)进行判断并过滤。例如，当用户发起查询$q=(w_1,w_2,w_3)$时，OXT方案会泄露id_4中包含w_1和w_3，而不包含w_2。

HXT方案如图2所示，HVE技术可以利用布隆过滤器一次性判断多个元素是否在一个集合中，以此来对w_1对应的文档进行关键词成员检测，判定其中是否包含所有查询的关键词，且不会产生KPRP泄露。

2.3　目标方案泄露

SSE协议中的信息泄露可以分为3种类型：存储泄露、访问模式泄露和搜索模式泄露。其中，访问模式泄露又称为查询结果模式泄露。

SSE方案的安全性是通过对泄露函数的正式定义来评估的，泄露函数指的是攻击者可以从加密数据库EDB和一系列查询Q中所获得的信息。本文着重关注后2种类型。

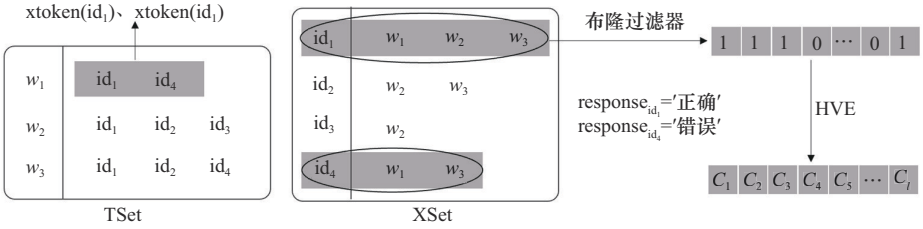


图2　HXT 方案

访问模式：给定查询 q，泄露对应的一组响应文档标识 $\mathrm{ids}(q)$。

搜索模式：给定一组查询 $Q=(q_1,\cdots,q_m)$，泄露其中 2 个查询是否相同，即泄露一个大小为 $m\times m$ 的二进制矩阵 $\boldsymbol{M}$，当 $q_i=q_j$ 时，$\boldsymbol{M}[i,j]=1$，否则 $\boldsymbol{M}[i,j]=0$。通过搜索模式，攻击者可以确定查询数量，从而获取查询频率信息。

本文定义了 2 种不同的泄露场景。这 2 种场景分别从第 2.2 节中介绍的 OXT 和 HXT 方案中抽象出来。至少存在这 2 种泄露的所有 SSE 方案都可能受到本文在该假设下提出的攻击。

在 HXT 方案中，查询 $q=(s,w_2,\cdots,w_n)$，本文关注的泄露函数 $\mathcal{L}_{\mathrm{HXT}}(\mathrm{DB},q)$ 详情定义如下。

查询大小模式：$\mathrm{SP}(s)=|\mathrm{DB}(s)|$，泄露 s 项匹配的文档个数。

查询结果模式：$\mathrm{RD}(q)=\mathrm{DB}(s)\bigcap_{i=2}^{n}\mathrm{DB}(w_i)$，即访问模式，泄露查询 q 匹配的所有文档标识符。

除上述泄露之外，OXT 方案的泄露 $\mathcal{L}_{\mathrm{OXT}}(\mathrm{DB},q)$ 中增加了 KPRP，泄露了 s 项对应文档和其他关键词的交叉关系，因此本文又将其简称为交叉模式泄露。

交叉模式：$\mathrm{KPR}_i=\{\mathrm{DB}(s)\cap\mathrm{DB}(w_i),\ i\in[2,n]\}$，泄露 s 项对应的文档是否包含其他关键词。

3　攻击概述

本文以半诚实的云服务器作为攻击者，攻击者会诚实地执行搜索协议，但会因“好奇”而利用搜索协议的信息泄露挖掘用户的隐私，同时攻击者可能具备用户数据集相关的先验知识。攻击者被允许监控用户和服务器之间的交互，并利用其背景知识恢复查询。遵循柯克霍夫原则，本文假设攻击者了解 SSE 方案的参数和算法。

本文假设攻击者拥有部分真实数据集或查询频率信息，目标是通过这些信息恢复连接查询背后的所有关键词。根据不同的攻击设置、所需的辅助数据和利用的泄露模式，本文的攻击可以分为以下 2 种。

1) 交叉泄露攻击。交叉泄露攻击针对与 OXT 方案[3]有相同泄露的方案。在这种攻击中，攻击者利用交叉模式进行过滤，以恢复查询。交叉泄露攻击假设攻击者已知全部或部分加密文档。实际应用中，可以合理考虑攻击者能够访问数据库的背景知识。

2) 频率匹配攻击。频率匹配攻击主要针对与 HXT 方案[4]有相同泄露的方案。一定时间段内，给定包含所有目标查询的查询分布，频率匹配攻击利用搜索模式来恢复查询信息，并假设攻击者已知目标查询的真实或偏移的频率分布。攻击者仅利用查询结果模式泄露和搜索模式泄露。目前，所有 SSE 方案都无法彻底消除这 2 种泄露，因此频率匹配攻击可以扩展到其他所有连接查询方案。

本文假设攻击者已知全部数据集合或其子集，用现有的单关键词查询恢复攻击方法恢复出查询 q 中频率最小的关键词 s 项。表 2 总结了针对单关键词查询的真实数据攻击方法，以及它们利用的泄露模式。

表 2　针对单关键词查询的真实数据攻击方法

攻击方法	利用的泄露模式	辅助信息
IKK[8]	查询结果模式(共现矩阵)	已知部分查询
Count[12]	查询大小模式	已知部分查询
BKM20[13]	查询结果模式(共现矩阵)	—
SELVOLAN[13]	查询大小模式	—
LEAP[9]	查询结果模式(共现矩阵)	—

根据可搜索加密方案的不同实例，恢复方法也不尽相同，为了评估攻击的有效性和鲁棒性，本文列举了 2 个方法来恢复 s 项。

观察单关键词查询。通常情况下，支持连接查

询的SSE方案同样也支持单关键词查询。攻击者只需观察到足够多的单关键词查询，就可通过访问模式构建共现矩阵，从而恢复出s项。

结合查询大小模式和查询结果模式。根据2.2节中的定义，OXT方案和HXT方案都会泄露这2种模式，攻击者也可以根据这些泄露信息，结合表2中的方法恢复出s项。

4 交叉泄露攻击

攻击假设。q表示在加密数据库EDB上执行的查询，对于$q=(w_1,w_2,\cdots,w_n)$的连接查询。本文假设w_1是查询q中频率最小的关键词，记作s项。攻击目标为恢复q背后的所有关键词$(w_1,w_2,\cdots,w_n)$。本文首先考虑已知文档攻击，即攻击者已知全部加密文档，将该假设作为基准，随后限制这个假设，以设计更实际的攻击。

攻击描述。交叉泄露攻击具体内容如算法1所示，输入加密数据库EDB、查询q、关键词w对应的文档标识符列表DB和文档id中包含的所有关键词集合W。

算法1 交叉泄露攻击

输入 加密数据库EDB，查询q，DB，W

输出 恢复出的查询Pre_q

1) w_1 = single_attack$(s$,EDB$)$
2) add w_1 to Pre_q
3) KPR$_i$ = $\{\mathrm{DB}(s)\cap\mathrm{DB}(w_i),i\in[2,n]\}$//交叉模式
4) Record_single = $[w_1]$//记录已经确定匹配的单词
5) for i in range(n): //逐个关键词恢复
6) $C_q[i]$ = Word_inter(KPR_i)//获取候选关键词集合
7) $C_{\mathrm{filter}}[i]$ = Word_union$(\mathrm{DB}(s)-\mathrm{KPR}_i)$//一定不包含$w$的文档关键词集合
8) for Pre_w in $C_q[i]$:
9) if Pre_w in$C_{\mathrm{filter}}[i]$:
10) remove Pre_w from $C_q[i]$
11) end if
12) end for
13) if#$(C_q[i])$=1: //候选关键词仅剩一个元素，即确定恢复出的关键词
14) add $C_q[i][0]$to Record_single
15) end if
16) add $C_q[i]$to Pre_q$[i]$//记录最终恢复结果
17) end for
18) repeat:
19) Flag = False
20) for i in range(n):
21) if len$(\mathrm{Pre_q}[i])>1$:
22) Pre_q$[i]$.difference$(\mathrm{Record_single})$//去除确定恢复的关键词
23) if len$(\mathrm{Pre_q}[i])=1$:
24) Flag = True
25) Record_single + = Pre_q$[i]$
26) end if
27) end if
28) end for
29) until Flag = False
30) return Pre_q
31) function Word_union(ids): //输出一组文档中包含的关键词并集
32) $C_{\mathrm{kws}}\leftarrow[\,]$
33) for id in ids:
34) C_{kws}.union$(W(\mathrm{id}))$
35) end for
36) return unique_elements(C_{kws})
37) function Word_inter(ids): //输出一组文档中包含的关键词交集
38) $C_{\mathrm{kws}}\leftarrow W(D[0])$
39) for id in ids:
40) C_{kws}.intersection$(W(\mathrm{id}))$
41) end for
42) return unique_elements(C_{kws})

首先，选用第3节列举的方法恢复连接查询中频率最小的关键词s项（第1行），并从已知文档中获取s项对应的关键词列表DB$(s)=\{\mathrm{id}_1,\mathrm{id}_2,\cdots,\mathrm{id}_{\mathrm{SP}(w)}\}$。根据已知的交叉模式KPR$_i$，判断DB$(s)$是否包含关键词$(w_2,w_3,\cdots,w_n)$，从中分别提取出候选关键词集合$C_q[i],i\in[2,n]$，集合中元

素个数表示为$\#\left(C_q[i]\right)$。

然后，对$C_q[i]$进行过滤。除了交叉模式KPR_i中的文档之外，w_i一定不出现在$\mathrm{DB}(s)$包含的其他文档中。因此再次利用交叉模式泄露分别对$(w_2,w_3,\cdots,w_n)$进行过滤，一定不包含w_i的文档可以表示为$\mathrm{DB}(s)-\mathrm{KPR}_i$。

最后，假设$q=(w_1,w_2,\cdots,w_n)$中不含重复关键词，分别恢复出$(w_2,w_3,\cdots,w_n)$的候选关键词后，将只剩一个元素的候选集合Pre_w视为确定恢复出的关键词，并将其记录在Record_single中，将Record_single中的元素从其他关键词的候选集合中除去。循环上述步骤，直到Record_single中没有新增的元素，输出恢复结果Pre_q。

交叉泄露攻击描述了攻击者在已知所有加密文档情况下的基准攻击。然而，攻击者通常很难获得全部非公开加密数据集文档。因此，接下来本文放宽这一假设，使攻击更加实际。

假设攻击者只已知部分加密文档$\mathrm{DB}'\in\mathrm{DB}$，那么攻击输入将为部分文档标识符集合$\mathrm{DB}'$，其中只包含关键词对应的部分已知文档标识符。

此时，交叉模式相应地表示为$\mathrm{KPR}_i'=\left\{\mathrm{DB}'(s)\cap\mathrm{DB}'\left(w_i\right),i\in[2,n]\right\}$。在此假设下，攻击者从已知文档中获得的信息不足，只拥有部分文档的攻击者无法进行精确匹配（第6~7行），这会造成过滤完成后仍存在多个候选结果的情况。

该场景下，攻击者仍能观察到正确的交叉模式长度，记为$\#\left(\mathrm{KPR}_i\right)$。它们之间存在关系$\#\left(\mathrm{KPR}_i'\right)\leqslant\#\left(\mathrm{KPR}_i\right)$。因此，攻击者只已知部分加密文档时，补充算法1的过滤方式（第9~10行）如下。

1) $\mathrm{KPR}_i'=\left\{\mathrm{DB}'(s)\cap\mathrm{DB}'\left(w_i\right),i\in[2,n]\right\}$

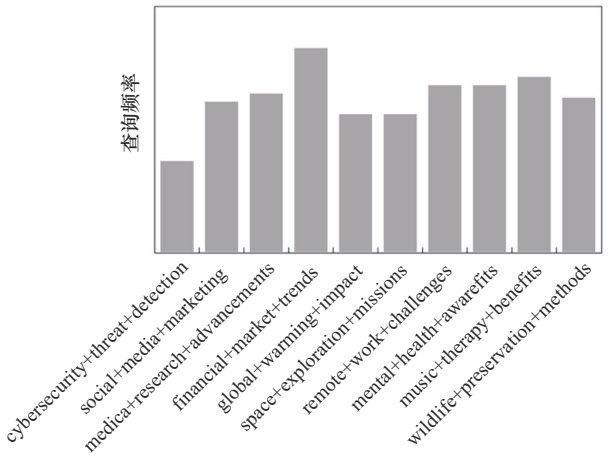
2) if $\#\left(\mathrm{KPR}_i'\right)>\#\left(\mathrm{KPR}_i\right)$:

3)　remove Pre_w from $C_q[i]$

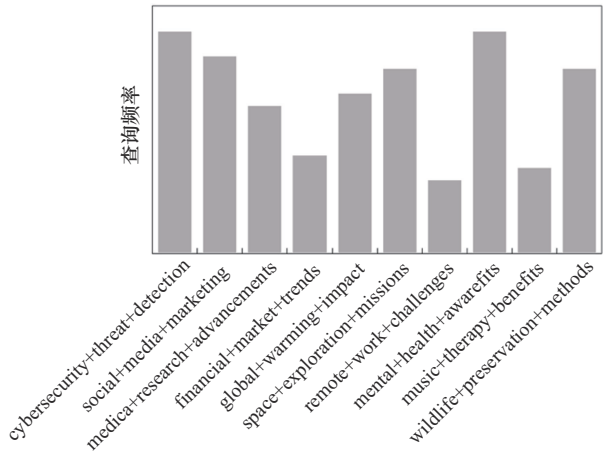
4) end if

5　频率匹配攻击

由于受到季节性、热门话题、新闻事件、一周中的某天和一年中的某月等因素的影响，用户查询频率通常会随着时间的推移而变化，从而提供必要的多样性。图3展示了随机选取的10组连接查询在2023年7月和10月的查询频率分布。由图3可知，同一查询在不同时段的查询频率有很大差异，从而使得查询分布更容易具有唯一性。频率匹配攻击通过将收集到的用户查询频率分布与已知的连接查询频率分布进行匹配，以实现查询恢复。攻击的详细过程如下。



(a) 2023年7月



(b) 2023年10月

图3　随机选取的10组连接查询在2023年7月和10月的查询频率分布

攻击假设。对于$q=\left(w_1,w_2,\cdots,w_n\right)$的连接查询，频率匹配攻击假设一个被动且持续观察的攻击者，他同样了解加密文档的内容，但无法获得交叉模式泄露的信息。攻击者只能观察到查询结果模式，即查询q最终的返回文档。

假设攻击者已知查询辅助频率信息，即q背后的所有关键词$\left(w_1,w_2,\cdots,w_n\right)$中的任意元素在$\tau$个时间区间同时被查询的频率。查询$q$在$\tau$个时间区间的真实频率（即攻击者观测值）记作$\boldsymbol{f}[q]$，攻击

目标为恢复q背后的所有关键词$(w_1,w_2,\cdots,w_n)$。

攻击描述。频率匹配攻击的具体内容如算法2所示，输入包括加密数据库EDB、查询$q=(w_1,w_2,\cdots,w_n)$、关键词w对应的文档标识符列表DB(w)、文档id中包含的关键词集合列表W(id)和查询q的频率辅助信息$\bar{\boldsymbol{f}}[q]$。

算法2 频率匹配攻击

输入 加密数据库EDB，查询q，DB(w)，W(id)，频率辅助信息$\bar{\boldsymbol{f}}[q]$

输出 恢复出的查询Pre_q

1) $w_1=\text{single\_attack}(s,\text{EDB})$

2) $C_q=W\left[\text{RD}[q]\right]-w_1$

3) $C_{\text{q\_candi}}=w_1\left\|P\left(w_2,w_3,\cdots,w_n;\#\left(C_q\right)\right)\right.$

4) $\text{Pre\_q}=\arg\min_{\text{Pre\_q}\in C_{\text{q\_candi}}}\left\|\boldsymbol{f}[q]-\bar{\boldsymbol{f}}[\text{Pre\_q}]\right\|_2$

首先，用第3节列举的方法恢复连接查询中频率最小的关键词s。随后，从查询q的返回结果模式RD[q]包含的文档中提取关键词候选集合，去除元素w_1后表示为C_q。

将该集合中元素个数表示为$\#\left(C_q\right)$，并从中选取$n-1$个元素进行排列，作为查询q的第2~n位候选关键词，记为排列$P\left(w_2,w_3,\cdots,w_n;\#\left(C_q\right)\right)$，结合已经恢复出的$w_1$，候选查询可以表示为

$$C_{\text{q\_candi}}=s\left\|P\left(w_2,w_3,\cdots,w_n;\#\left(C_q\right)\right)\right.$$

攻击目标是在候选连接查询中选择一个已知频率和观测频率分布最接近的元素作为预测值

$$\text{Pre\_q}=\arg\min_{\text{Pre\_q}\in C_{\text{q\_candi}}}\left\|\boldsymbol{f}[q]-\bar{\boldsymbol{f}}[\text{Pre\_q}]\right\|_2$$

其中，$\|\cdot\|_2$代表欧几里得范数，对于每个可能的候选连接查询，攻击者计算查询q的观测频率和候选关键词辅助频率之间的欧氏距离。选取$C_{\text{q_candi}}$中查询频率分布最接近真实情况的元素作为q的预测值Pre_q。

6 实验评估

本节分别在不同的假设下评估了交叉泄露攻击和频率匹配攻击的性能，并对实验结果进行了解释。与之前的研究相似，本文以连接查询恢复的准确率作为衡量攻击准确性的标准，即正确恢复连接查询中每个关键词的查询比例。测试数据集从常用的电子邮件系统Enron数据集中提取，其中包含Enron公司的30 109封电子邮件，每封电子邮件作为数据集中的一个文档。关键词列表是电子邮件主体中的单词（不包含停顿词，如“a”“do”）。本文使用Python的NLTK语料库来获取所有英语单词和停顿词的列表。

本文从Enron数据集中提取出2 000个使用最频繁的关键词形成一个关键词列表，并从中随机选择Δ个使用最频繁的关键词用于生成连接查询q，然后从Google Trends中下载2022年12月之后连续的48周查询频率进行实验。本文提出的2种攻击方法独立恢复不同查询，每次实验随机生成500个查询用于恢复，正确恢复连接查询中每个关键词记作一次正确恢复，攻击准确率即正确恢复率。

实验环境如下：Intel(R) Core(TM) i7-8700的CPU，主频率为3.20 GHz，运行内存为16 GB，操作系统为Ubuntu20.04，编程语言为Python3.7。

6.1 交叉泄露攻击结果

假设攻击者拥有可查询文档的子集，首先进行初步实验，观察已知文档率α对攻击准确率的影响。实验假设攻击者能直接获得连接查询中频率最小的关键词，实际应用场景中，该信息可以通过第3节中的方法推理获得。

假设关键词空间$\Delta\in\{100,500,1\,000,2\,000\}$，每个查询包含的关键词个数$n$为3。已知文档率$\alpha$对交叉泄露攻击准确率的影响如图4所示。当关键词空间小时，恢复率总体较高。即使在仅已知10%文档的情况下，关键词空间$\Delta=100$时仍能保持90%以上的恢复率。这是因为获取候选关键词集合的本质是不同文档中关键词的合取操作，当关键词空间较小时，取少量已知文档中关键词的交集也容易得出唯一的候选关键词。在固定关键词空间的情况下，恢复率随已知文档率α的下降呈下降趋势，关键词空间越大，这种趋势越明显，当α从0.5下降到0.2时，$\Delta=2\,000$下的恢复率从81%下降到23%。

关键词个数n对交叉泄露攻击准确率的影响如图5所示。本文在关键词空间$\Delta=2\,000$下随机抽取n个关键词生成连接查询进行实验，分别设置2个已知文档率$\alpha=0.5$和$\alpha=0.2$。

由图5可以看出，$\alpha=0.5$时的攻击准确率明显高于$\alpha=0.2$，这与图4中的结论一致。另外，攻击准确率与关键词个数呈正相关，这是因为交叉泄露

攻击独立恢复查询中每个关键词，并且获取候选关键词步骤和筛选步骤均与关键词个数无关。由于查询$(w_1,w_2,\cdots,w_n)$中没有重复元素，在确定恢复项之后，系统会在候选关键词中删除已经确认的结果。因此，关键词个数越多，就越容易在候选关键词中删除至只保留一个正确结果。

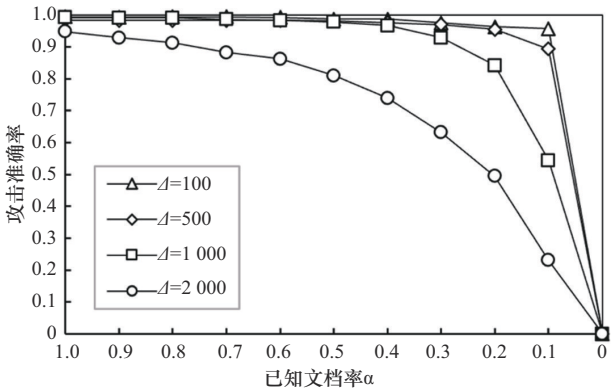


图4　已知文档率α对交叉泄露攻击准确率的影响

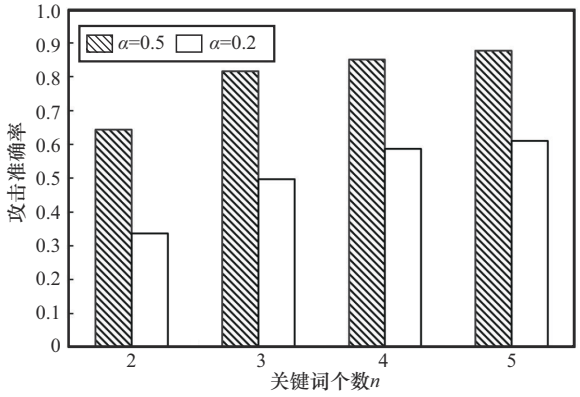


图5　关键词个数n对交叉泄露攻击准确率的影响

6.2　频率匹配攻击结果

本节对第 5 节中介绍的频率匹配攻击进行评估，其中每个实验运行 10 次，最终的结果为 10 次运行结果的均值。每个实验使用不同的随机种子，这种随机性影响噪声矩阵的生成。

频率匹配攻击利用查询频率信息恢复查询。本实验假设攻击者已知全部文档，即$\alpha = 1.0$，已知目标查询分布和候选查询，攻击者选择与目标查询分布最接近的候选查询作为结果。

在实际情况中，攻击者已知的查询分布辅助信息可能不够准确，这会影响攻击的有效性。为了评估这种情况下的攻击效果，本文引入高斯噪声来扰动真实查询，并将其作为攻击者的输入。设置高斯噪声为$\epsilon \sim \mathcal{N}(0,\sigma^2)$，其中噪声指数$\sigma \in \{0,5,10,20,40\}$。同样设置每个查询包含的关键词个数$n = 3$，在不同的关键词空间$\Delta \in \{100,500,1\,000,2\,000\}$下进行评估，噪声指数$\sigma$对频率匹配攻击结果的影响如图 6 所示。

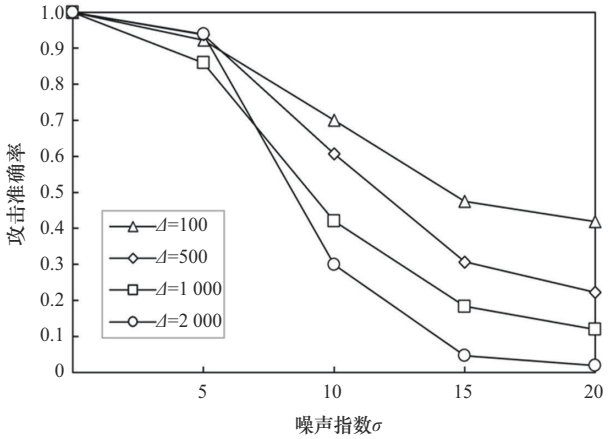


图6　噪声指数σ对频率匹配攻击结果的影响

图 6 结果表明，频率匹配攻击准确率随着噪声指数的上升而下降。当噪声指数σ从 5 上升到 40 时，$\Delta = 2\,000$下的准确率从 94% 下降到 2%。相同噪声指数下，攻击准确率随关键词空间Δ的增大而降低，因为有更多关键词可供选择时，准确拟合查询中每组关键词变得更困难。即使在$\sigma = 40$、$\Delta = 100$的情况下，频率匹配攻击仍能保持 42% 的恢复率。因此，当搜索频率与 Google Trends 的统计结果吻合较好，且用户查询中包含 3 个及以上的关键词时，频率匹配攻击的准确率能达到 80% 以上。由于向攻击者提供真实的频率信息是不现实的，本文在剩余评估中选取噪声指数$\sigma = 5$进行实验。

频率区间个数τ对频率匹配攻击结果的影响如图 7 所示。本实验假设σ为 5，关键词空间Δ的取值为$\{100,500,1\,000,2\,000\}$，区间个数$\tau$为$\{6,12,24,48\}$。

由图 7 可知，当τ<48 时，攻击准确率随关键词空间Δ的增大而降低，这与图 6 的测试结果一致；当$\tau = 48$时，在不同关键词空间下，查询恢复准确率均能达到 90% 左右。

本节实验证明了攻击准确率随着频率区间个数的增加而上升。以$\Delta = 2000$为例，当τ从 12 上升到

48时，攻击准确率从11%增加到93%。结果表明，即使在存在噪声的情况下，只要对频率区间进行足够精细的划分，频率匹配攻击依然能够有效地恢复出80%以上的查询，随着关键词空间的增大，频率匹配攻击的优势更加明显。

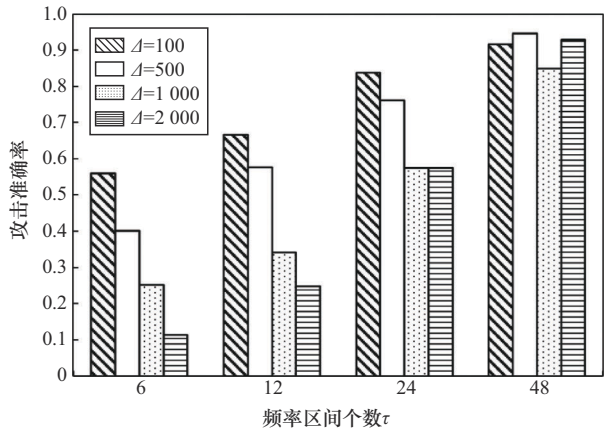


图7 频率区间个数τ对频率匹配攻击结果的影响

关键词个数n对频率匹配攻击结果的影响如图8所示。本实验同样假设σ为5，固定区间个数$\tau = 48$，关键词空间Δ的取值为$\{100,500,1\,000,2\,000\}$。

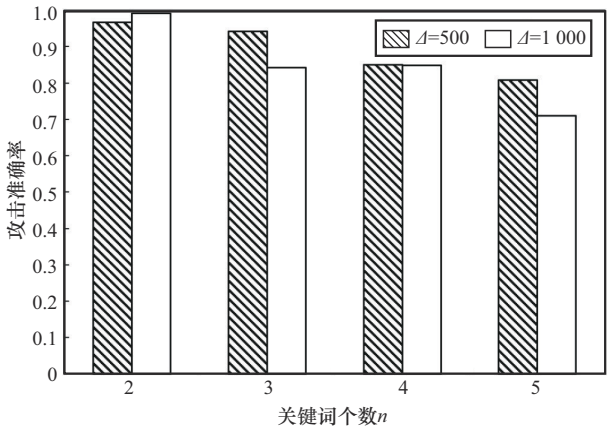


图8 关键词个数n对频率匹配攻击结果的影响

从图8中可以看出，攻击准确率随关键词个数的增多而降低。然而，在查询中包含5个关键词的情况下，关键词空间$\Delta = 500$仍有80%的恢复率。另外，在关键词个数$n = 2$的场景下，攻击者从频率匹配攻击和交叉泄露攻击协议本身获取的信息完全相同，因此，攻击者在实施攻击时可以根据辅助信息的种类选择合适的攻击，以达到更好的攻击效果。

7 结束语

本文详细分析了当前连接关键词可搜索加密方案的泄露问题，提出了面向连接关键词可搜索加密的交叉泄露攻击和频率匹配攻击。实验结果表明，即使攻击者仅已知10%的数据集或者不准确的频率背景信息，上述2种攻击仍能达到较高的恢复准确率。

参考文献：

[1] 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.

[2] 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.

[3] CASH D, JARECKI S, JUTLA C, et al. Highly-scalable searchable symmetric encryption with support for Boolean queries[C]//Annual Cryptology Conference. Berlin: Springer, 2013: 353-373.

[4] LAI S Q, PATRANABIS S, SAKZAD A, et al. Result pattern hiding searchable encryption for conjunctive queries[C]//Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security. New York: ACM Press, 2018: 745-762.

[5] DEMERTZIS I, PAPADOPOULOS D, PAPAMANTHOU C, et al. SEAL: attack mitigation for encrypted databases via adjustable leakage[C]//29th USENIX Security Symposium (USENIX Security 20). Berkeley: USENIX Association, 2020: 2433-2450.

[6] GARG S, MOHASSEL P, PAPAMANTHOU C. TWORAM: efficient oblivious RAM in two rounds with applications to searchable encryption[C]//Annual International Cryptology Conference. Berlin: Springer, 2016: 563-592.

[7] ZHANG Y, KATZ J, PAPAMANTHOU C. All your queries are belong to us: the power of file-injection attacks on searchable encryption[C]// 25th USENIX Security Symposium (USENIX Security 16). Berkeley: USENIX Association, 2016: 707-720.

[8] ISLAM M S, KUZU M, KANTARCIOGLU M. Access pattern disclosure on searchable encryption: ramification, attack and mitigation[C]// Proceedings of the 19th Annual Network and Distributed System Security Symposium. Reston: Internet Society, 2012: 12.

[9] NING J, HUANG X, POH G S, et al. LEAP: leakage-abuse attack on efficiently deployable, efficiently searchable encryption with partially known dataset[C]//Proceedings of the 2021 ACM SIGSAC Conference on Computer and Communications Security. New York: ACM Press, 2021: 2307-2320.

[10] OYA S, KERSCHBAUM F. Hiding the access pattern is not enough: Exploiting search pattern leakage in searchable encryption[C]//30th USENIX Security Symposium (USENIX Security 21). Berkeley: USENIX Association, 2021: 127-142.

[11] OYA S, KERSCHBAUM F. IHOP: improved statistical query recovery against searchable symmetric encryption through quadratic optimization[J]. arXiv Preprint, arXiv: 2110.04180, 2021.

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

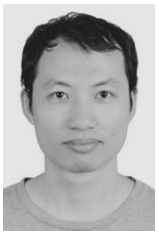
[13] BLACKSTONE L, KAMARA S, MOATAZ T. Revisiting leakage abuse attacks[C]//Proceedings of the 2020 Network and Distributed System Security Symposium. Reston: Internet Society, 2020: 1-18.

[14] 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.
[15] KIRKPATRICK S, GELATT C D Jr, VECCHI M P. Optimization by simulated annealing[J]. Science, 1983, 220(4598): 671-680.
[16] PATRANABIS S, MUKHOPADHYAY D. Forward and backward private conjunctive searchable symmetric encryption[C]//Proceedings of the 2021 Network and Distributed System Security Symposium. Reston: Internet Society, 2021: 1-52.
[17] BOST R, MINAUD B, OHRIMENKO O. Forward and backward private searchable encryption from constrained cryptographic primitives[C]//Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security. New York: ACM Press, 2017: 1465-1482.
[18] CHAMANI J G, PAPADOPOULOS D, KARBASFORUSHAN M, et al. Dynamic searchable encryption with optimal search in the presence of deletions[J]. IACR Cryptol EPrint Arch, 2022, 2022: 648.
[19] CHEN T Y, XU P, PICEK S, et al. The power of bamboo: on the post-compromise security for searchable symmetric encryption[C]//Proceedings of the 2023 Network and Distributed System Security Symposium. Reston: Internet Society, 2023: 1-18.
[20] YUAN D D, ZUO C, CUI S J, et al. Result-pattern-hiding conjunctive searchable symmetric encryption with forward and backward privacy[J]. Proceedings on Privacy Enhancing Technologies, 2023(2): 40-58.
[21] WANG B, YU S C, LOU W J, et al. Privacy-preserving multi-keyword fuzzy search over encrypted data in the cloud[C]//Proceedings of the IEEE Conference on Computer Communications. Piscataway: IEEE Press, 2014: 2112-2120. .
[22] SUN S F, ZUO C, LIU J K, et al. Non-interactive multi-client searchable encryption: realization and implementation[J]. IEEE Transactions on Dependable and Secure Computing, 2022, 19(1): 452-467.
[23] WANG J, CHOW S S M. Omnes pro uno: practical multi-writer encrypted database[C]//31st USENIX Security Symposium (USENIX Security 22). Berkeley: USENIX Association, 2022: 2371-2388.
[24] RIZOMILIOTIS P, MOLLA E, GRITZALIS S. REX: a searchable symmetric encryption scheme supporting range queries[C]//Proceedings of the 2017 on Cloud Computing Security Workshop. New York: ACM Press, 2017: 29-37.
[25] ZHENG Y D, LU R X, ZHANG S N, et al. PMRQ: achieving efficient and privacy-preserving multidimensional range query in eHealthcare[J]. IEEE Internet of Things Journal, 2022, 9(18): 17468-17479.
[26] WANG Y L, WANG J F, SUN S F, et al. Towards multi-user searchable encryption supporting Boolean query and fast decryption[C]//International Conference on Provable Security. Berlin: Springer, 2017: 24-38.
[27] GRUBBS P, LACHARITÉ M S, MINAUD B, et al. Learning to reconstruct: statistical learning theory and encrypted database attacks[C]//Proceedings of the 2019 IEEE Symposium on Security and Privacy (SP). Piscataway: IEEE Press, 2019: 1067-1083.
[28] GUI Z, JOHNSON O, WARINSCHI B. Encrypted databases: new volume attacks against range queries[C]//Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security. New York: ACM Press, 2019: 361-378.
[29] FREDMAN M L, TARJAN R E. Fibonacci heaps and their uses in improved network optimization algorithms[J]. Journal of the ACM (JACM), 1987, 34(3): 596-615.
[30] XU L, ZHENG L Q, XU C Z, et al. Leakage-abuse attacks against forward and backward private searchable symmetric encryption[C]//Proceedings of the 2023 ACM SIGSAC Conference on Computer and Communications Security. New York: ACM Press, 2023: 3003-3017.
[31] GUI Z C, PATERSON K G, PATRANABIS S. Rethinking searchable symmetric encryption[C]//Proceedings of the 2023 IEEE Symposium on Security and Privacy (SP). Piscataway: IEEE Press, 2023: 1401-1418.

[作者简介]

杜瑞颖（1964– ），女，河南新乡人，博士，武汉大学教授、博士生导师，主要研究方向为网络安全、隐私保护等。

沈蓓（2001– ），女，湖北赤壁人，武汉大学硕士生，主要研究方向为网络安全、应用密码学等。



何琨（1986– ），男，湖北武汉人，博士，武汉大学副教授、博士生导师，主要研究方向为应用密码学、网络安全、云计算安全、人工智能安全、区块链安全等。

赵陈斌（1996– ），男，安徽六安人，武汉大学博士生，主要研究方向为网络安全、应用密码学等。

王贝宁（1998– ），女，湖北武汉人，武汉大学博士生，主要研究方向为可搜索加密、应用密码学等。

陈晶（1981– ），男，湖北武汉人，博士，武汉大学教授、博士生导师，主要研究方向为网络安全、应用密码学、分布式系统安全等。