隐匿信息检索技术现状与展望

杜瑞颖,黄正帝,石 闽,周尔俊,何 琨,陈 晶*
(空天信息安全与可信计算教育部重点实验室,武汉大学国家网络安全学院,湖北武汉 430072)

摘 要: 在数据驱动决策的时代,大数据分析与云计算的深度融合在释放数据价值的同时,也将数据安全与隐私保护推向了核心挑战的前沿. 隐匿信息检索作为关键的多方安全计算技术,允许用户从远程数据库中检索特定信息而完全不泄露查询目标,为不可信环境下的数据查询提供了坚实的隐私保障. 该技术已在医疗、金融等诸多领域展现出应用潜力,持续受到学术界与工业界的广泛关注. 然而,随着数据规模与用户数量的激增,现有方案面临着效率与实用性之间的显著矛盾. 早期基于信息论安全的多服务器方案依赖多不合谋的强安全假设,而基于计算安全的单服务器方案则在通信、计算和存储开销上面临严峻挑战. 因此,在确保安全的前提下,如何全面提升检索效率已成为推动该技术落地的核心问题. 本文系统性地梳理与总结了隐匿信息检索技术的研究现状. 首先,我们明确了隐匿信息检索的形式化定义及其核心属性,并概述了实现该技术的主流密码学原语. 其次,本文构建了一个以服务器数量为依据的技术分类框架,将现有方案划分为多服务器与单服务器两大脉络,并深入剖析了基于函数秘密共享、可穿刺伪随机函数、同态加密及不经意传输等不同技术路线的设计原理与性能权衡. 进一步地,本文探讨了为适应具体功能要求而衍生的多种实用变体,包括批处理隐匿信息检索、对称隐匿信息检索、关键字隐匿信息检索和可更新隐匿信息检索,分析了它们各自解决的问题与设计特点. 在应用层面,本文通过社交发现、匿名通信和广告投递等典型场景,具体阐述了隐匿信息检索如何解决实际的隐私保护痛点. 最后,基于全面的综述分析,本文展望了该领域的未来发展趋势,指出研究重点应聚焦于进一步优化理论开销、设计支持多功能的统一灵活框架,以及通过系统级创新解决实际部署难题,从而推动隐匿信息检索技术从理论走向广泛的实际应用.

关键词: 隐匿信息检索;安全多方计算;隐私保护;同态加密;函数秘密共享

基金项目: 国家重点研发计划(No.2022YFB3102100);国家自然科学基金(No.62076187);湖北省重点研发计划(No.2024BAB018);武汉市知识创新专项(No.2023010201010062)

中图分类号: TP309 **文献标识码:** A **文章编号:** 0372-2112(2025)12-4719-21

电子学报 URL:http://www.ejournal.org.cn **DOI:**10.12263/DZXB.20250525

Private Information Retrieval: Current Status and Future Prospects

DU Rui-ying, HUANG Zheng-di, SHI Min, ZHOU Er-jun, HE Kun, CHEN Jing*
(*Key Laboratory of Aerospace Information Security and Trusted Computing*, *Ministry of Education*, *School of Cyber Science and Engineering*, *Wuhan University*, *Wuhan*, *Hubei* 430072, *China*)

Abstract: In the era of data-driven decision making, the deep integration of big data analytics and cloud computing has pushed data security and privacy protection to the forefront of core challenges while unleashing the value of data. As a key multi-party secure computing technology, private information retrieval allows users to retrieve specific information from remote databases without revealing the query target at all, providing a solid privacy guarantee for data query in untrustworthy environments. The technology has demonstrated its application potential in many fields, such as healthcare and finance, and continues to receive extensive attention from both academia and industry. However, with the proliferation of data size and number of users, the existing schemes face a significant contradiction between efficiency and practicality. Early multi-server schemes based on information-theoretic security rely on the strong security assumption of multiple non-collusion, while single-server schemes based on computational security face severe challenges in communication, computation, and storage overheads. Therefore, how to comprehensively improve the retrieval efficiency under the premise of ensuring security has become a core issue to drive the technology to the ground. In this paper, we systematically sort out and summarize the current research status of private information retrieval technology. First, we clarify the formal definition of private

收稿日期:2025-06-19;录用日期:2025-12-10;责任编辑:覃怀银
*通讯作者:陈晶

information retrieval and its core attributes, and outline the mainstream cryptographic primitives that realize the technology. Second, this paper constructs a technology categorization framework based on the number of servers, divides the existing schemes into two main vectors: multi-server and single-server, and deeply analyzes the design principles and performance trade-offs of different technology routes based on function secret sharing, puncturable pseudorandom function, homomorphic encryption and oblivious transfer. Further, this paper explores various practical variants derived to meet specific functional requirements, including batch private information retrieval, symmetric private information retrieval, keyword private information retrieval and updatable private information retrieval, and analyzes their respective problems and design features. At the application level, this paper specifically illustrates how private information retrieval can address practical privacy protection pain points through typical scenarios such as social discovery, anonymous communication and ad delivery. Finally, based on the comprehensive review and analysis, this paper looks forward to the future development trend of this area, pointing out that research should focus on further optimizing the theoretical overhead, designing a unified and flexible framework to support multi-functionality, and solving practical deployment challenges through system-level innovation, so as to promote private information retrieval technology from theory to a wide range of practical applications.

Key words: private information retrieval; secure multiparty computation; privacy protection; homomorphic encryption; function secret sharing

Foundation Item(s): National Key Research and Development Program of China (No.2022YFB3102100); National Natural Science Foundation of China (No. 62076187); Key Research and Development Program of Hubei Province (No.2024BAB018); Wuhan Knowledge Innovation Project (No.2023010201010062)

1 引言

随着互联网的高速发展,从公共数据库下载数据已经成为用户获取信息的重要途径之一. 然而,拥有数据库的服务器可以轻松地追踪和了解用户的访问记录. 在医院档案查阅、股票数据获知等场景下,用户不愿泄露自身的查询意图,这给用户隐私保护带来了新的挑战. 为应对这一挑战,Chor等[1]在1995年首次提出隐匿信息检索(Private Information Retrieval,PIR),允许客户端从大小为n的数据库中获得第i个记录,同时不向数据库服务器泄露任何有关索引i的信息. 隐匿信息检索技术允许用户在隐藏目标记录的同时完成对公共数据库的信息查询,为不受信环境下用户的安全信息访问提供了全新解决方案,目前已经在医疗、金融、法律、教育等各领域得到广泛应用,如社交发现[2~5],匿名通信[6~9]和广告投递[10~13].

在Chor等最早的方案中,用户需要与多个拥有相同数据库副本的服务器进行通信以完成数据查询,这类需要依赖多个服务器不合谋安全假设的方案被称为多服务器隐匿信息检索方案. 尽管多服务器方案可以实现查询索引的隐藏,但多不合谋服务器的强安全假设限制了其在现实场景中的应用. 1997年,Chor等[14]将隐匿信息检索方案的隐私要求由信息论安全放宽到计算安全,并以此为代价实现了更低的通信开销. 同年,Kushilevitz等[15]利用二次剩余假设(Quadratic Residuosity,QR)[16]提出了首个单服务器计算隐匿信息检索方案,在不增加通信开销的前提下,避免使用多不合谋服务器的安全假设. 总体而言,多服务器方案通常具备更优的理论性能,而单服务器方案的优势在于无需多不合谋服务器的强安全假设. 此后,隐匿信息检索朝低开销[17,18]、多功能[19,20]、易部署[21,22]的方向不断发展. 在低开销方面,研究聚焦于显著降低协议的通信带宽与计算时间成本,以提升其效率;在多功能方面,技术在保障客户端查询隐私的基本前提下不断拓展,衍生出如保护数据库内容机密性、支持批量查询等增强功能;而在易部署方面,探索则集中于弱化安全假设、简化方案流程等,旨在克服实际应用中的障碍,全面提升技术的实用性与普及度. 尽管如此,目前隐匿信息检索尚未满足大规模商业的性能需求,研究者仍需探究高效解决方案.

在隐匿信息检索领域,许多学者已对其技术发展进行了深入的综述和研究. 2004年,Gasarch[23]回顾了隐匿信息检索研究的起源,给出了隐匿信息检索的基本模型定义,并按照时间顺序综述了隐匿信息检索从信息论安全到计算安全的演进,同时按照不同应用场景将隐匿信息检索进行分类. 2007年,Ostrovsky等[24]着眼于单服务器隐匿信息检索,根据实现的技术将其分成基于同态加密、基于Φ-隐藏假设和基于单向陷门置换的隐匿信息检索方案,并讨论了隐匿信息检索与不经意传输、抗碰撞哈希函数和可搜索公钥加密的密切联系. 2023年,Gianira等[25]构建了基于编码理论的单服务器隐匿信息检索统一分析框架,并将隐匿信息检索分成基于有限域同态、基于扩展域同态[26]、基于Lee重量变换[27]和基于容错学习(Learning With Errors,LWE)[28]等四类进行介绍. 2023年,Vithana等[29]侧重于综述隐匿信息检索的概念扩展,系统分析了隐私集合求交、隐私集合求并和隐私数据更新,探讨了隐匿信息

检索在联邦学习和隐私计算中的应用. 2025年,Kim等[30]将基于全同态加密的隐匿信息检索方案按照超立方体结构和树结构进行分类,并结合私有数据库和公共数据库两个实际应用场景对二者的性能进行分析. 在私有数据库上,基于树结构的方案在通信和计算上均优于基于超立方体结构;在公共数据库上,基于超立方体结构的方案在参数选择上表现出更大灵活性,同时能展现出更佳实际性能.

综上所述,虽然学术界对隐匿信息检索方案已进行了一定的研究,但仍存在综述方案过时、综述角度不全面等问题,无法对目前最新隐匿信息检索的研究成果[30~32]进行全面总结与分析. 因此,通过查阅并整理近年来学术界在密码学、信息安全等相关领域的国际会议和学术期刊中发表的研究成果,本文以隐匿信息检索的实际发展趋势为依据,将这些成果按照多服务器和单服务器方案分类,这一分类体系不仅能覆盖基于同态加密、函数秘密共享等密码学工具的最新研究成果,更可容纳恒重码字等基于全新方法实现的隐匿信息检索方案. 在具体分析层面,本文进一步按实例化方法进行细粒度划分,确保对各类技术路线的创新点实现精准追踪. 同时,本文对隐匿信息检索针对批处理、服务器隐私保护、关键字查询和数据库更新等不同功能需求的变体进行了详细介绍,拓展其技术边界. 此外,本文还介绍了包括社交发现、匿名通信和广告投递等目前隐匿信息检索的主要应用场景,最后对未来隐匿信息检索的研究趋势进行总结与展望.

2　隐匿信息检索

介绍隐匿信息检索之前,首先对本文使用的符号进行说明:$\mathbb{N}$表示正整数集合;$\mathrm{negl}(\lambda)$表示关于λ的可忽略函数;$\tilde{O}(\cdot)$表示省略安全参数λ和对数多项式因子.

如图1所示,在隐匿信息检索方案中,服务器拥有一个大小为n的数据库D,客户端拥有目标索引$i\in\{1,2,\cdots,n\}$. 客户端的目标是从服务器获取第i个记录$D[i]$,同时不向服务器泄露任何关于i的相关信息. 在理论分析中,数据库记录的具体表示形式不会影响隐匿信息检索方案的性质,因而常被抽象化处理.

定义1　隐匿信息检索方案. 该方案包括以下4个多项式时间算法.

(1)$p\leftarrow\mathrm{Setup}(1^{\lambda})$:初始化算法. 该算法由客户端和服务器共同执行. 输入安全参数λ,输出公共参数p. 公共参数p隐含在所有后续算法的输入中.

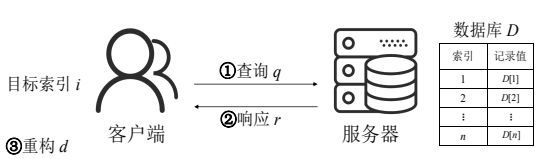

图1　隐匿信息检索

(2)$q\leftarrow\mathrm{Query}(i)$:查询算法. 该算法由客户端执行. 输入目标索引$i\in\{1,2,\cdots,n\}$,输出查询$q$.

(3)$r\leftarrow\mathrm{Answer}(q,D)$:响应算法. 该算法由服务器执行. 输入查询$q$和数据库$D$,输出响应$r$.

(4)$d\leftarrow\mathrm{Reconstruct}(r)$:重构算法. 该算法由客户端执行. 输入响应$r$,输出查询结果$d$.

一个隐匿信息检索方案需要满足以下属性:

(1)正确性. 若对任意安全参数λ、数据库D及其大小$n\in\mathbb{N}$和目标索引$i\in\{1,2,\cdots,n\}$,满足以下条件:

$$\Pr\left[d=D[i]:\begin{array}{c}p\leftarrow\mathrm{PIR.Setup}(1^{\lambda})\\ q\leftarrow\mathrm{PIR.Query}(i)\\ r\leftarrow\mathrm{PIR.Answer}(q,D)\\ d\leftarrow\mathrm{PIR.Reconstruct}(r)\end{array}\right]\geqslant 1-\mathrm{negl}(\lambda)\tag{1}$$

则称该隐匿信息检索方案是正确的.

(2)安全性. 若对任意的安全参数λ、数据库D及其大小$n\in\mathbb{N}$和目标索引$i\in\{1,2,\cdots,n\}$,定义分布:

$$\mathcal{P}(i):=\left\{q:\begin{array}{c}p\leftarrow\mathrm{PIR.Setup}(1^{\lambda})\\ q\leftarrow\mathrm{PIR.Query}(i)\end{array}\right\}\tag{2}$$

若对于任意使用概率多项式时间算法的敌手$\max\limits_{i,j\in[n]}\left\{\Pr\left[\mathcal{A}\left(\mathcal{P}(i)\right)=1\right]-\Pr\left[\mathcal{A}\left(\mathcal{P}(j)\right)=1\right]\right\}\leqslant\mathrm{negl}(\lambda)$,满足以下条件:

$$\max_{i,j\in[n]}\left\{\Pr\left[\mathcal{A}\left(\mathcal{P}(i)\right)=1\right]-\Pr\left[\mathcal{A}\left(\mathcal{P}(j)\right)=1\right]\right\}\leqslant\mathrm{negl}(\lambda)\tag{3}$$

则称该隐匿信息检索方案是安全的.

(3)非平凡性. 为了从服务器获取目标索引对应的记录而不泄露任何信息,一种直观的解决方法是从服务器下载整个数据库,但该做法带来的通信开销为$O(n)$,在实际应用中通常不可接受,需降低通信开销以增强其实用性. 若一个隐匿信息检索方案的通信开销低于线性级,则称该方案是非平凡的.

如图2所示,本文构建了一套隐匿信息检索方案的分类体系,将现有研究方案划分为多服务器和单服务器两大类别. 多服务器模型指客户端需要与多个服务器交互方可完成隐私查询的方案;若客户端仅与单一服务器交互即可完成隐私查询,则属于单服务器模型. 多服务器模型中,方案进一步细化为基于函数秘密共享的方案、基于可穿刺伪随机函数的方案以及其他实现方式;单服务器模型中,则以基于同态加密和基于不经意传输为代表,同时涵盖其他替代性方法. 同时,以上框架中列举出了各种细粒度分类方法的代表性实例.

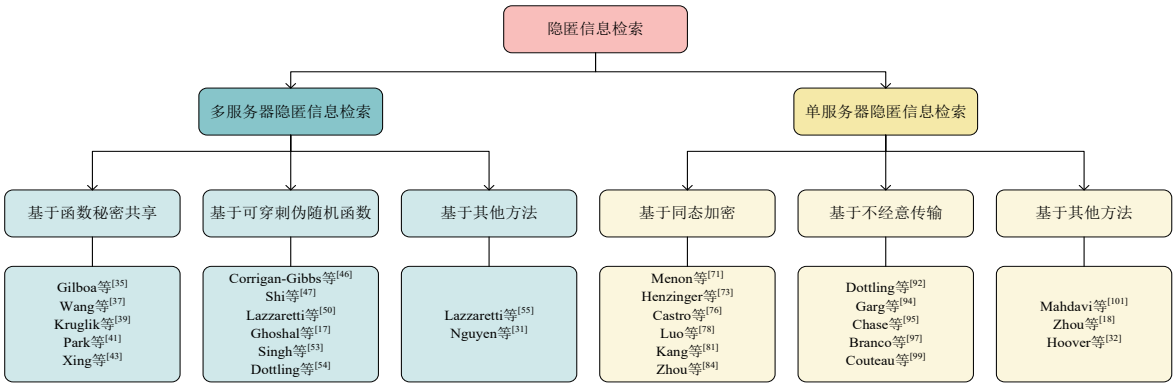

图2 隐匿信息检索分类框架

3 多服务器隐匿信息检索

1995年Chor等[1]在信息论背景下提出了隐匿信息检索的概念，要求客户端查询不能泄露任何关于目标索引i的信息. 为降低通信开销，Chor等提出通过在多个彼此独立、不可通信的服务器之间复制数据库以实现优化. 具体而言，当数据库被复制$k\geqslant 2$次时，隐匿信息检索方案的通信开销可以降低至次线性级，这类方案被称为多服务器隐匿信息检索方案(multi-server private information retrieval).

自隐匿信息检索提出以来，多服务器方案便一直是相关领域研究的热点. 尽管此类方案依赖于强安全假设，即假定多个服务器之间不存在合谋，这一假设通常要求跨组织的协调部署，在实际应用中难以满足，但其提供的高性能是绝大多数单服务器方案难以比拟的.

如图3所示，在多服务器隐匿信息检索方案中，完成初始化设置后，客户端将生成不同的查询请求并发送至对应的服务器. 各服务器根据相同的数据库副本生成相应的响应结果并返回客户端. 最终，客户端运行重构算法，恢复得到查询结果d.

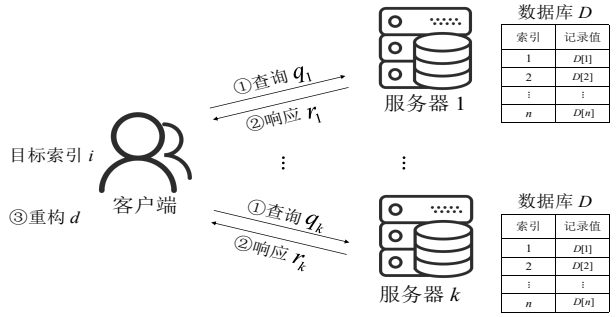

图3 多服务器隐匿信息检索

从实现原语的角度来看，可以将主流多服务器隐匿信息检索方案分为基于函数秘密共享(Function Secret Sharing，FSS)和基于可穿刺伪随机函数(Puncturable PseudoRandom Function，PPRF)的方案. 前者以函数秘密共享为核心，多数方案在实现时无需额外需求，但基本都存在实际性能瓶颈；而后者基于可穿刺伪随机函数及其相关密码学原语构建，并通过引入预处理机制在效率上实现优化. 然而，预处理方法一般需在客户端或服务器上存储辅助信息，但该设计也引入了额外的存储开销. 图4展示了多服务器隐匿信息检索的分类和代表性文献.

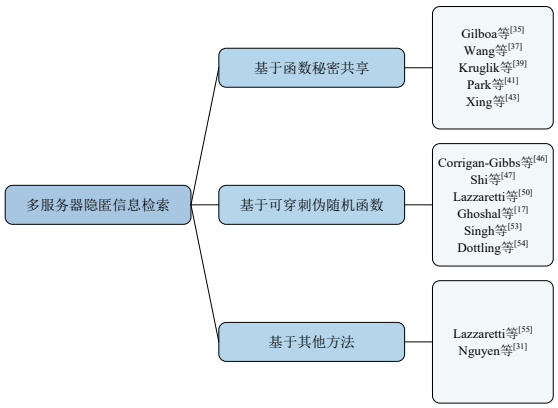

图4 多服务器隐匿信息检索分类图

3.1 基于函数秘密共享的隐匿信息检索

函数秘密共享[31~34]通过将目标函数拆分为多个份额，每个份额独立存储和计算，确保只有在所有份额的结果汇总后才能恢复原函数的输出. 该特性使得计算可在不可信方仅接触局部份额的条件下完成，从而规避在计算过程中暴露敏感信息. 基于这一特性，函数秘密共享技术已广泛应用于隐匿信息检索等领域，其优势在于有效提升查询过程中的隐私保护，同时减少通信和计算开销，尤其适用于需要跨多个服务器协作处理的场景.

如图5所示，在基于函数秘密共享的隐匿信息检索方案中，完成初始化设置后，客户端首先选定一个函数f，使其在目标索引i处取值为1，其余位置均为0. 然后，

客户端将该函数拆分为k个函数分片$(f_1,f_2,\cdots,f_k)$并发送至对应服务器. 服务器将数据库D作为输入计算得到函数评估$f_j(D)$,并将其返回至客户端. 客户端在得到所有服务器的响应结果后,便可以重构得到函数f在数据库D上的评估值$f(D)$,并根据所选的特定函数获得查询结果d. 该类方案采用结构对等的服务器架构,其安全性核心机制在于各服务器所持密钥的异构性与计算过程的互补性. 鉴于此,增加服务器数量虽会引入额外的系统开销,但可显著提高共谋容忍阈值,并增强其服务于复杂查询的能力.

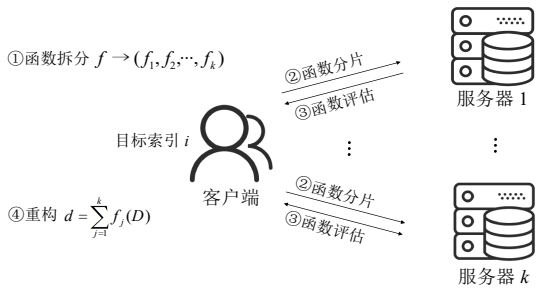

图5　基于函数秘密共享的隐匿信息检索

2014年Gilboa等[35]提出了基于分布式点函数的双服务器隐匿信息检索方案,具有对数多项式级的查询成本,且响应成本仅为一比特. Gilboa等将分布式点函数生成的参与方密钥k_b作为查询发送至对应服务器,服务器计算以k_b为根节点的伪随机函数(PseudoRandom Function,PRF)[36]树的所有节点,然后将计算得到的奇偶校验值作为响应返回给客户端. 在客户端多次使用相同查询的场景中,该方案的单比特响应特性具有较高的实用价值,不过相当于产生n个伪随机比特的计算开销限制了实际应用,为进一步提升方案的计算效率,可以在未来引入并行计算或者借助高性能硬件加速.

2017年Wang等[37]提出了面向公共数据库查询的解决方案Splinter,该方案将函数秘密共享拓展到TOPK和MAX等非可加聚合的复杂查询策略,且在只有一台诚实服务器时即可保证查询的隐私性. 该方案在性能上实现了$O(n\log n)$的服务器计算开销和$O(\log n)$的通信开销,在安全性上完成了对用户查询敏感参数的隐藏,使客户端能进行参数化查询,且参数和查询结果均不会泄露给服务器. 此外,方案利用AES-NI[38]和多核CPU(Central Processing Unit)优化了函数秘密共享的具体实现,在航班搜索、地图路由等实际应用中实现了秒级的端到端延迟. 然而,该方案仅支持SQL(Structured Query Language)中的部分查询策略,且只能在连接条件公开时连接新表,同时不支持数据库更新,未来可探索如何扩展查询支持和完善动态数据一致性机制,进一步扩展其实际应用的功能.

2024年,Kruglik等[39]针对当前多数函数秘密共享方案仅支持计算安全性的研究现状,提出了一种信息论安全的函数秘密共享方案,通过将多项式隐匿信息检索[40]查询转化为多项式曲线的函数秘密共享密钥,实现了信息论安全下的多服务器隐私查询. 方案引入了可验证性机制,利用离散对数假设确保服务器返回结果的正确性,防止恶意篡改. 相比传统方案,工作在保持信息论安全的同时显著提升了客户端查询效率,但在实际部署时仍需权衡多项式次数与计算开销的关系. 然而,方案仅支持点函数与比较函数,未扩展至如非线性函数等的更复杂的函数,且所需服务器数量较多,后续研究可聚焦于减少服务器依赖及扩展支持函数类型,以提升方案实用性与灵活性.

2024年,Park等[41]针对多服务器框架中存在恶意服务器的场景,利用分布式点函数(Distributed Point Function,DPF)和纠删码(erasure code)设计了新的容错隐匿信息检索协议. 通过将输出转换为适用于查询纠删码存储的代数结构,Park等使协议在仅增加少量服务器的条件下实现有效容错功能,同时通过压缩PIR查询显著降低协议的实际开销. 为使DPF具备容错能力,Park等提出了三种解决方法:一是将基于树结构的双服务器DPF方案[31]扩展至多服务器,二是利用覆盖设计来改进基于异或共享的多服务器DPF方案[34],三是设计了一种基于沙米尔秘密共享[42]的容错信息论DPF方案. 尽管如此,部分方案的参数选择依赖于如覆盖设计等的特定数学结构,下一步需探索更通用的参数选择方法,以提升隐匿信息检索方案的灵活性和适用性.

2025年,Xing等[43]聚焦于现有函数秘密共享方案依赖可信第三方生成密钥的问题,提出了首个支持算术共享的无第三方函数秘密共享协议,实现了高效的数学函数计算框架. Xing等设计了无需可信第三方的两方计算协议,使方案支持分布式生成函数秘密共享密钥,并基于去中心化函数秘密共享构建了高效基础组件. 此外,方案针对科学计算中的复杂函数,利用周期性特性减少输入比特的长度,并结合查找表和样条多项式逼近方法[44]提升性能,同时验证其在隐私保护生物认证和邻近性测试等实际场景中的适用性. 不过,方案中离线通信轮数与输入比特长度呈线性关系,且方案仅针对半诚实模型设计,未来需借助信息论消息验证码(Message Authentication Code,MAC)和高效零知识证明验证输入和输出的一致性,完善方案在恶意模型下的安全防护和高效查询.

3.2　基于可穿刺伪随机函数的隐匿信息检索

自可穿刺伪随机函数的概念提出以来,该原语凭借其能够隐藏穿刺点对应取值的特性,已经被广泛应用于多种隐匿信息检索方案中. 这类方案通常与2000

年 Beimel 等[45]提出的预处理方法结合使用，该方法的核心在于在协议执行之前，各服务器预先完成与数据库内容相关的多项式级辅助信息的计算与存储，从而提升协议执行时服务器响应的计算效率.

如图6所示，在基于可穿刺伪随机函数的隐匿信息检索方案中，客户端在离线预处理阶段生成次线性数量的伪随机集合 S，服务器1接收后计算集合元素对应记录的奇偶校验 p 并返回给客户端. 在在线查询阶段，客户端找到包含目标索引 i 的集合 S_k 并将该索引穿刺，生成穿刺集合 S' 后发送至服务器2，服务器2计算对应的奇偶校验 r 后返回. 客户端将离线预处理阶段获得的奇偶校验 p_k 和在线查询返回的响应 r 异或，以获得最终查询结果 d. 在此架构中，各服务器职责明确、功能互补：离线服务器承担预处理职责，为客户端生成提示信息；在线服务器则负责响应在线查询请求. 同时，此类方案的安全性根植于密码学假设与非共谋前提. 在此框架下，增加服务器数量并非其设计目标，且无法为现有安全模型带来实质提升. 此外，不同方案在在线查询时所需的服务器数量也存在差异，部分方案需和多个服务器交互才能完成查询.

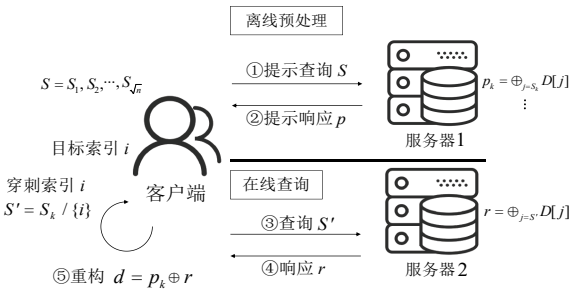

图6 基于可穿刺伪随机函数的隐匿信息检索

2020年，Corrigan-Gibbs 等[46]基于可穿刺伪随机函数构造了可穿刺伪随机集合，并在此基础上提出了具有次线性级服务器计算开销的隐匿信息检索方案. 该方案在离线阶段通过可穿刺伪随机集合对若干次线性大小的索引集合进行随机采样并计算奇偶校验，再将索引集合压缩表示为密钥以减少通信开销. 与此同时，该方案以一定概率选择目标索引 i 作为穿刺点进行穿刺，并通过运行多个副本后投票的方式得到目标索引对应的记录值. 然而，在该方案中穿刺密钥等同于集合 S 减去穿刺元素 x，导致方案的在线通信开销达到 $\tilde{O}(\sqrt{n})$ 级，较未使用预处理的方案在渐进复杂度上更差，后续研究可聚焦于密钥表示的紧凑化设计或压缩技术的引入.

2021年，Shi 等[47]提出了私有可穿刺伪随机集合的全新原语，并借此构造了双服务器的隐匿信息检索方案. 该方案在保持对数多项式级通信开销的基础上，实现了 $\tilde{O}(\sqrt{n})$ 在线计算和 $\tilde{O}(\sqrt{n})$ 客户端存储，且仅依赖于标准 LWE 假设. 为实现该原语，Shi 等选定了特殊采样分布来加快采样效率，且只需满足“偶然正确性”：穿刺算法仅需以较高概率移除穿刺点即可. Shi 等的原语构造依赖于私有可穿刺伪随机函数，并受到伪随机函数设计中分组密码和格式保留加密工作[48,49]的启发. 尽管该方案在通信带宽上的理论效率已接近最优，但由于穿刺算法的内部结构过于复杂，目前尚无研究者提供代码实现，下一步工作可围绕方案的代码实例化展开.

2023年，Lazzaretti 等[50]引入了一种名为弱私有可穿刺伪随机函数（Weak Privately Puncturable Pseudo-Random Function，WPPRF）的原语，并基于此提出了一种双服务器隐匿信息检索方案 TreePIR，具有次线性级摊销的计算开销和对数多项式级的通信开销，其安全性仅基于决策迪菲-赫尔曼（Decision Diffie-hellman，DDH）假设[51]. Lazzaretti 等通过将 WPPRF 的域和范围设定为 $\sqrt{n}$ 来构建伪随机集合，并利用其在穿刺前后的简洁性及支持快速成员检测的高效性，将隐匿信息检索问题从 n 个元素简化为 $\sqrt{n}$ 个元素，然后递归使用另一种隐匿信息检索方案，使整体方案能够兼容其余非预处理方案. 不过，TreePIR 要求客户端存储大量的密钥和提示信息，未来需研究更紧凑的密钥表示或压缩技术以降低客户端的存储开销.

2024年，Ghoshal 等[17]针对现有模型普遍依赖公钥密码操作的不足，提出了具有次线性级带宽和次线性级计算开销的隐匿信息检索方案，仅需额外的次线性级客户端存储，其核心是带列表解码的私有可编程伪随机集合：给定密钥 sk，可将其扩展为一个 $\sqrt{n}$ 大小的伪随机集合，且能在常数级时间判断 $\{1,2,\cdots,n\}$ 中的任一元素是否在集合中. 此外，通过调用编程算法，客户端可将指定元素替换掉集合中某个元素，同时不影响集合中其余元素，且不会泄露被编程元素. 与2023年 Zhou 等[52]不同的是，Ghoshal 等只要求解码时输出一个候选集合列表，使该原语只可通过单向函数构造. 然而，由于在核心原语构建时放宽了安全性约束，该方案并未能实现标准密码学要求的可忽略安全，未来可探究在仅依赖单向函数的条件下实现完全安全的私有可穿刺伪随机函数.

2024年，Singh 等[53]针对当前高效隐匿信息检索方案通常依赖单向函数或公钥假设，提出了一种信息论安全的多服务隐匿信息检索方案，通过引入私有多穿刺伪随机集合（Privately Multi-Puncturable Random Set，PMPRS），首次在不依赖任何密码学假设的情况下实现了高效的预处理. Singh 等设计了基于 d-ary 树的 PMPRS 结构，将传统单点穿刺操作扩展为多点并行穿刺，大幅提升了处理效率. 方案采用多服务器架构实现

负载均衡,使在线阶段的通信开销和计算开销均降至$\tilde{O}(\sqrt{n})$级,同时保证信息论安全,证明了信息论安全方案可以达到密码学方案的性能水平,具有重要的理论意义和实际应用价值.

2025年,Dottling等[54]着眼于批处理场景,将批处理中单个查询的摊销复杂度降低至$\tilde{O}(\sqrt{n})$的计算开销和$\tilde{O}(1)$的通信开销,其中单次批处理大小为$\sqrt{n}$. 为保护客户端隐私的同时提升多目标查询的实际性能,Dottling等提出了可穿刺伪随机集合和批量无偏采样(batch unbiased sampling). 前者可支持高效的成员检测和紧凑的穿刺集合表示,后者借助替换采样避免向采样池中引入偏差. 此外,方案通过共享的伪随机函数密钥来掩盖服务器响应实现服务器端的隐私保护. 尽管如此,方案仅在理论上实现高效批量隐私查询,并未实例化可穿刺伪随机集合及隐匿信息检索方案,未来需完善分析其实际部署性能.

3.3　基于其他方法的多服务器方案

除上述两类方案外,还有部分多服务器方案基于其他密码学原语进行实例化,能够满足多种实际应用场景中的特定需求.

2024年,Lazzaretti等[55]提出了隐匿信息检索方案SinglePass,预处理性能能够达到实际应用的最优水平. 在离线预处理时,方案利用费雪耶茨洗牌算法[56,57]为数据库每行生成随机置换,并与服务器1通信获取每列元素对应的奇偶校验. 在在线查询时,客户端利用随机元素在目标列中替换原目标索引位置,并将修改后的列作为查询请求发送至服务器2. 根据服务器2返回的记录值和离线提示信息,客户端便可得到目标结果. 最后,为保持提示信息的可用性,客户端利用从服务器1获得的随机元素交换查询元素. 此外,虽然SinglePass支持以常数级开销更新数据库,但仅限于在数据库末尾添加数据,未来可探索支持完备动态更新操作的机制.

2025年,Nguyen等[31]提出了具有半诚实安全性的双服务器隐匿信息检索方案Pirex,能够在维持次线性级计算开销的同时,实现最小的客户端通信开销和存储成本,且大部分都是异或、伪随机函数和模运算等低成本操作. 方案通过从随机分区中检索记录来隐藏目标索引,并利用随机异或和私有分区检索恢复目标记录,同时利用刷新机制[58]保持提示信息的可用性. 为进一步优化系统性能,Nguyen等提出增强方案Pirex+,利用加法同态加密[59]在服务器上远程存储提示信息,使其更适合资源受限环境下的系统部署,但在数据库更新阶段,客户端需传输加法同态加密的二进制向量,后续研究可聚焦于增量更新等更高效的更新机制设计和实现.

3.4　多服务器方案小结

多服务器方案作为隐匿信息检索的重要组成部分,在近些年来取得一系列的研究进展,表1对前述方案进行分析比较,主要从安全假设、通信开销、计算开销和是否有额外需求等方面,对多服务器隐匿信息检索方案的代表性实例进行对比分析.

表1　多服务器隐匿信息检索方案对比

分类	方案	安全假设	服务器安全模型	通信开销	计算开销	存储开销
基于函数秘密共享	Gilboa等[35]	OWF	半可信	$O(\log n^{\log 3})$	$O(n)$	0
	Wang等[37]	OWF	半可信	$O(\log n)$	$O(n\log n)$	0
	Kruglik等[39]	DLP	恶意	$O(n^{1/d})$	$O(n^{1/d})$	$O(n^{1/d})$
	Park等[41]	OWF	半可信/恶意	$O(\log n)$	$O(n)$	0
	Xing等[43]	OWF	半可信	$O(\log n)$	$O(n)$	0
基于可穿刺伪随机函数	Corrigan-Gibbs等[46]	OWF	半可信	$O(\sqrt{n})$	$O(\sqrt{n})$	$O(\sqrt{n})$
	Shi等[47]	LWE	半可信	$\tilde{O}(1)$	$\tilde{O}(\sqrt{n})$	$O(\sqrt{n}\log n)$
	Lazzaretti等[50]	DDH	半可信	$\tilde{O}(1)$	$O(\sqrt{n}\log^2 n)$	$O(\sqrt{n})$
	Ghoshal等[17]	OWF	半可信	$\tilde{O}(n^{1/4})$	$\tilde{O}(\sqrt{n})$	$\tilde{O}(\sqrt{n})$
	Singh等[53]	NONE	半可信	$\tilde{O}(\sqrt{n})$	$\tilde{O}(\sqrt{n})$	$\tilde{O}(\sqrt{n})$
	Dottling等[54]	OWF	半可信	$\tilde{O}(1)$	$\tilde{O}(\sqrt{n})$	$\tilde{O}(1)$
基于其他方法	Lazzaretti等[55]	OWF	半可信	$O(\sqrt{n})$	$O(\sqrt{n})$	$O(n\log n)$
	Nguyen等[31]	OWF	半可信	$\tilde{O}(\sqrt{n})$	$O(\sqrt{n})$	$O(\lambda\sqrt{n})$

考虑多服务器隐匿信息检索方案基于的安全假设,基于函数秘密共享的方案通常依赖于如单向函数(One Way Function,OWF)的简单密码学假设,而基于可穿刺伪随机函数的方案还依赖于DDH、LWE等更复杂的密码学假设. 隐匿信息检索方案的成本主要考虑通信开销和计算开销,通信开销指客户端在查询时发送的查询成本和服务器返回的响应成本,而计算开销指服务器在接收查询后计算响应花费的时间成本. 尽

管基于函数秘密共享的方案在通信开销上可达次线性级,但其在计算开销上仍停留在线性级. 而得益于与预处理方法的结合,基于可穿刺伪随机函数的方案目前已能实现对数多项式级的通信开销和次线性级的通信开销,其中Dottling等[54]的开销为批处理中单个查询的摊销复杂度. 受限于预处理方法,基于可穿刺伪随机函数的方案均需额外客户端存储等要求. 除Park等[41]需将数据库以纠删码的形式存储在服务器及Kruglik等[39]将函数份额存储在服务器并将数据库编码表示外,基于函数秘密共享的方案均无特殊要求.

当前多服务器隐匿信息检索方案主要沿函数秘密共享和可穿刺伪随机函数两条技术路径演进,并在安全性、计算效率和适用场景等方面展现出显著差异. 前者通过将目标查询函数分解为多个可独立计算的函数份额来实现隐私保护,具有通信开销低和安全假设低的安全优势,但存在计算开销高和功能受限的缺点;后者利用穿刺操作隐藏查询目标,并结合预处理技术,能够实现次线性级的在线计算效率,但需要额外存储开销并依赖更强的密码学假设. 为缓解上述方案面临的局限性,基于函数秘密共享的方案正尝试通过硬件加速(如AES-NI指令集[38])和新型函数构造(如Xing等[43]提出的算术共享方案)突破计算瓶颈,基于可穿刺伪随机函数的方案则聚焦于存储优化(如Ghoshal等[17]的列表解码技术)和假设弱化(如Singh等[53]的信息论安全方案).

4 单服务器隐匿信息检索

为规避对多个不合谋服务器的强安全假设依赖,1997年Kushilevitz等[15]基于QR构建了首个单服务器计算隐匿信息检索方案,其通信复杂度为$O(n^{\varepsilon})$,其中$\varepsilon>0$. 该工作首次证明,在无需依赖多方非合谋假设的前提下,可基于标准密码学假设构建单服务器隐匿信息检索方案,奠定了此类方案发展的理论基础.

图1中,定义1界定的隐匿信息检索方案在默认情况下对应于单服务器场景. 在单服务器隐匿信息检索方案中,完成初始化设置后,客户端根据查询索引i生成查询请求q并发送至服务器,服务器根据数据库生成响应结果r并返回客户端. 最终,客户端运行重构算法恢复得到查询结果d.

根据实现的密码学工具,主流单服务器隐匿信息检索方案可分为基于同态加密(Homomorphic Encryption,HE)和基于不经意传输(Oblivious Transfer,OT)的方案. 基于同态加密的方案允许服务器直接在加密数据上执行运算并生成密文响应,适用于服务器计算能力较强、但通信资源有限的应用场景,缺点是整体计算开销较高;后者借助不经意传输协议完成隐私查询,产生的通信开销高于前者,但在使用不经意传输扩展(Oblivious Transfer extension,OTe)后可以进一步降低计算开销,适用于低延迟需求的应用场景. 图7展示了单服务器隐匿信息检索的分类和代表性文献.

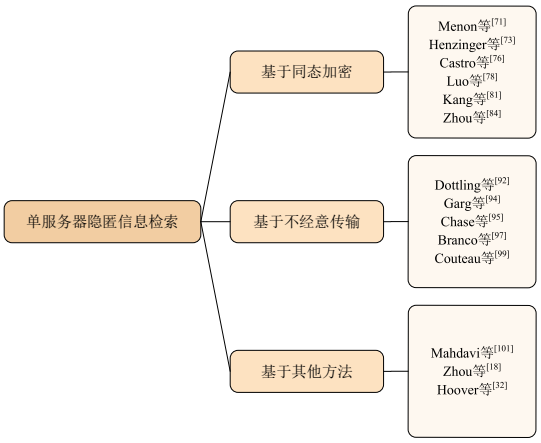

图7 单服务器隐匿信息检索分类图

4.1 基于同态加密的隐匿信息检索

相较于多服务器方案,单服务器隐匿信息检索方案无需依赖多不合谋服务器的强安全假设,从而显著降低部署复杂度,拓展了其在实际应用中的可行性. 其中,基于同态加密的方案因其良好的计算隐私性和协议简洁性而被广泛应用.

同态加密技术[60]允许用户在密文上执行运算,使得解密后所得结果等同于对明文执行相应运算所得结果,这一特性使得不可信第三方在无需访问明文的情况下即可完成加法、乘法等计算,有效防止敏感信息在运算过程中的泄露[61]. 基于这一特性,同态加密已经被广泛应用于包括安全多方计算[62~67]、云计算安全[68~70]等领域.

如图8所示,在基于同态加密的隐匿信息检索方案中,完成初始化设置后,客户端首先生成一个长度为n的向量,该向量在目标索引位置取值为1,其余位置取值为0. 客户端加密该向量后将其发送给服务器,服务器随后将其与数据库D进行同态明文-密文乘法计算,并将结果返回至客户端,最终客户端通过解密得到查询结果d.

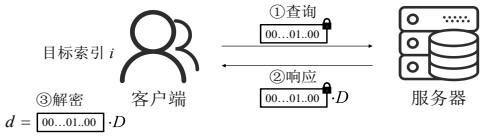

图8 基于同态加密的隐匿信息检索

2023年,Menon等[71]借助Regev[28]加法同态方案和GSW[72]全同态方案提出了SPIRAL,并通过引入新型密文转换技术实现了高效查询. 在查询发起前,客户端向

服务器发送与查询无关的公共参数;在查询生成阶段,客户端使用查询打包方法,并通过密文转换算法将查询压缩为单标量密文;在查询扩展阶段,服务器将查询扩展为包含矩阵Regev密文和GSW密文的集合,随后用矩阵Regev密文将数据库映射到相应子数据库,并对加密后续查询的GSW密文计算同态乘法,最终生成目标记录的加密矩阵Regev密文. 尽管SPIRAL通过引入更大规模的公共参数以实现密文转换程序,优化了在线阶段的通信开销,但这加重了公共参数的存储和传输负担,下一步可借助高效压缩技术降低实际开销.

2023年,Henzinger等[73]基于LWE提出了SimplePIR,在单服务器框架下展现出接近机器内存带宽的性能,但缺点在于通信成本较高. 方案建立在Kushilevitz等[15]早期工作的基础上,其中服务器的吞吐量受限于明文矩阵和密文向量乘积的计算速度. 为突破这一瓶颈,Henzinger等借助Regev[28]加法同态方案,让服务器能在客户端查询之前完成大部分矩阵向量乘积的计算. 这些预处理只和数据库和Regev加法同态算法的公共参数相关,因此可在多个客户端的查询中重复使用. SimplePIR可结合一种专为近似集合成员检测设计的新型数据结构,共同应用于证书透明中的隐私审核任务[74,75],但在方案设计时数据结构的误报率高达1/2,下一步可通过优化哈希策略的方式降低误报率,提高其可用性.

2024年,Castro等[76]针对现有隐匿信息检索方案依赖离线预处理来提高效率的问题,提出了一种完全无状态的隐匿信息检索方案WhisPIR. 在方案中,客户端只在查询时才与服务器交互,不会产生额外离线通信,故适用于大规模客户端和频繁数据库更新的场景. Castro等优化了索引扩展算法,通过动态选择密文旋转生成器来降低计算开销,并利用非紧凑BGV全同态算法[77]省略重线性化来降低通信开销,同时利用参数可调性实现通信与计算的灵活权衡. 不过WhisPIR性能上受限于大记录数据库,且索引扩展的优化依赖经验选择,缺乏理论的封闭解以覆盖所有情况,未来可探究封闭解或提出更精确的噪声管理策略以进一步优化索引扩展.

2024年,Luo等[78]提出了名为KsPIR的单服务器隐匿信息检索方案,其核心围绕高效同态加密计算和分阶段处理优化展开. Luo等提出了维度折叠方法,将数据库编码为二维矩阵,利用环容错学习(Ring Learning With Error,RLWE)[79]和GSW[72]全同态加密方案对目标索引进行加密,并通过结构化的同台操作直接提取目标数据,避免了传统方案中复杂的密文扩展步骤. 同时,KsPIR在离线阶段预计算数据库相关的同态运算中间结果,在在线阶段仅需轻量级的合成计算,并针对实时性要求高的情况下引入BSGS算法[80],将矩阵-向量乘法分解为并行的"小步-大步"同态运算. 不过,KsPIR对超大规模数据库的处理效率存在缺陷,同时查询产生的通信开销略逊色于当前最优方案,下一步可利用更紧凑的查询编码方法和流式传输技术,以支持更灵活的记录大小.

2025年,Kang等[81]聚焦当前隐匿信息检索协议通信开销过大的问题,利用全同态加密方案提出了一种无需转密(transciphering)的高效隐匿信息检索方案Pirouette,借助RLWE密文和LWE密文间的转化降低通信开销,并依托层次化结构和算法设计支持服务器计算的高度并行. Kang等以LWE密文作为查询,并用伪随机生成器(PseudoRandom Generator,PRG)[82]压缩查询大小,客户端仅需发送LWE密文的最后一个分量和PRG种子,将查询大小从KB级降至36 B. 同时,Kang等提出一种高效同态比特分解算法,可将多比特LWE密文转换为多个单比特LWE密文,并借助RLWE密文优化噪声增长. 此外,Pirouette能以部分计算性能为代价直接将应用场景扩展至加密数据库,未来可依托NTRU方案的盲旋转方法[83]进一步降低计算开销.

2025年,Zhou等[84]针对当前方案忽略数据完整性保护的情况,提出了一种可验证的单服务器隐匿信息检索方案VHE-PIR,能够在恶意服务器存在的情况下保护查询隐私和检索结果的完整性. 依托零知识证明[85]和容错学习全同态加密方案,Zhou等构造了可验证的全同态加密原语,可通过加密和密文评估来生成可验证的证明. 为优化计算效率,VHE-PIR利用加速模块[86]将矩阵乘法分解为多线程并同时执行,但尚未在大规模数据集上验证其扩展性能,未来可探索其实际部署能力与系统兼容性.

4.2　基于不经意传输的隐匿信息检索

尽管基于同态加密的隐匿信息检索方案在通信开销方面表现优异,但其较高的计算复杂度限制了实际部署. 相比之下,基于不经意传输的隐匿信息检索方案借助高效的OT协议,在低延迟数据服务场景中展现出更强的实用性和可扩展性.

作为密码学中的基本原语,不经意传输最早由1981年Rabin[87]基于二次剩余求解困难性假设提出,并以2取1OT[88]的形式实现:接收方可从发送方的两个消息中私密选择并接收其中一个,且发送方无法得知接收方的选择. 通过递归调用或者直接构造,这一概念可自然扩展为更通用的n取1OT[89],使接收方能在n个消息中选择目标项且不泄露选择信息. 正是这种特性,使不经意传输[90,91]成为实例化隐匿信息检索的理想工具.

如图9所示,在典型的基于不经意传输的隐匿信息检索流程中,完成初始化设置后,客户端首先根据目标索引i构造查询索引q^i,并将其发送给服务器;服务器将

该索引与数据库D一同输入到不经意传输协议中，返回对应记录r^i给客户端，最终客户端重构得到查询结果d.

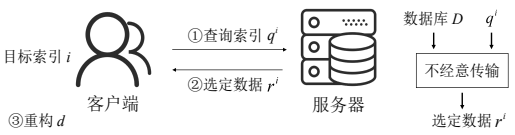

图9 基于不经意传输的隐匿信息检索

2019年，Dottling等[92]基于DDH、QR、决策复合残差(Decision Composite Residuosity，DCR)[93]等多种假设，构建了提示长度为1比特的陷门哈希函数(Trapdoor Hash Function，TDH)，并以此构建了首个rate-1字符串OT协议，其中rate指提示长度的倒数，从而实现了首个具有最优下载速率和对数多项式级通信开销的单服务器隐匿信息检索方案，为隐私数据查询提供全新技术路径. 不过，方案主要关注线性谓词和索引谓词，对更复杂的函数类的支持有限，未来可结合混淆电路技术以扩展到更通用的计算模式和组合任务.

2020年，Garg等[94]提出一种新型范围陷门哈希函数，成功突破传统OT方案中公钥长度过大的技术瓶颈. 该构造基于无双线性对群中幂决策迪菲-赫尔曼(power-DDH)假设，将群求值运算的开销从$O(n^2)$级显著降低至$O(n\log n)$级，并将上传速率从$\lambda^2\tilde{O}(n)$优化至$\lambda\tilde{O}(n)$. 然而，方案基于的安全假设为实际应用带来了更高的安全性要求和实现复杂度，未来可探索在标准DDH、LWE等假设下实现类似的效率提升，降低对强安全假设的依赖.

2021年，Chase等[95]针对客户端通信开销较高的问题，在双线性群上的标准假设[96]的基础上提出了摊销rate-1OT的密码学原语，并以此构造了客户端通信开销为$O(\lambda\log n)$个群元素的rate-1隐匿信息检索方案. 该协议一经初始化，后续的隐匿信息检索查询只需要$O(\log n)$个群元素的通信开销. 摊销rate-1OT实现了接近理论最优的服务器响应，并具备良好的可扩展性，可适配不平衡私集合交等计算场景. 然而，协议仍需较多配对运算，后续研究可进一步优化配对计算性能以降低总计算开销.

2023年，Branco等[97]提出了一种基于统计发送方隐私的不经意传输框架，能够在标准DDH和LPN(Learning Parity with Noise)[98]假设实现渐进最优的摊销通信开销. 框架的核心是co-PIR，即一种具有特殊统计安全特性的公钥加密方案，允许客户端选择性擦除数据库的特定位置，并确保被擦除的位置信息对服务器具有统计安全性. Branco等利用基于扩展域的线性同态加密实现高效批量查询，并设计递归式co-PIR协议实现多位置擦除，为构建高效、安全的隐私保护查询系统提供了实用工具. 不过，方案主要针对批量OT场景，可能无法直接适用于其他更复杂的场景，未来可将其扩展到支持动态数据库更新等更广泛的应用场景.

2024年，Couteau等[99]针对当前OT扩展协议不支持非交互式公钥设置的限制，提出了QuietOT框架，结合对称密钥原语和公钥设置，实现高效的OT扩展. 通过将基础OT替换为基于RLWE假设的公钥设置，方案支持非交互式生成OT实例，并提出可平移的约束伪随机函数[100]，允许主密钥持有者在评估时高效平移约束条件，从而支持更高效的OT扩展. 此外，Couteau等首次形式化公钥OT在多实例场景下的安全性定义，确保在多方计算中公钥的重复使用不会破坏安全性. 然而，QuietOT的公钥尺寸较大，下一步可研究公钥压缩技术或分层密钥派生方法以降低存储和通信开销.

4.3 基于其他方法的单服务器方案

除了基于同态加密和不经意传输的两大主流方案外，学术界还探索了多种创新技术路径来构建隐匿信息检索协议，这些方案在计算复杂度、通信效率和安全保障等方面呈现出不同的权衡与特性.

2022年，Mahdavi等[101]提出了一种基于恒重码字的相等运算符方法，展现出优于传统同态加密方法的计算效率. 恒重码字特指具有相同汉明权重的二进制字符串. 针对此类码字，Mahdavi等设计了一种独特的相等运算符，其乘法深度仅取决于码字的汉明权重，而非传统方法中的元素比特长度. 根据这种特性，Mahdavi等构建了恒重PIR，具备通信和计算开销增长速度缓慢的优势. 恒重PIR能兼容包含大量有效载荷的数据库，且能应用于通信和计算开销较低的流数据场景. 然而，方案对恒重编码过程中可能引入的冲突缺乏深入分析，未来应评估其对安全性造成的影响并提出相应缓解机制.

2024年，Zhou等[18]设计了一种高效且轻量的隐匿信息检索方案Piano，其核心安全基础仅依赖于伪随机函数. Piano将数据库分割为一系列次线性规模的数据块，并利用PRF密钥标识索引集合，从而有效减轻客户端存储负担. 离线预处理时，Piano通过流式传输将数据库内容发送至客户端，客户端随后计算每个集合元素对应记录值的奇偶校验，用于加速在线查询. 在线查询时，客户端将移除目标索引对应的集合元素，并将剩余集合发送至服务器. 服务器枚举所有可能情况并执行奇偶校验计算后将结果返回客户端. 客户端结合接收的响应及本地的提示信息，即可恢复目标索引对应的记录值. Piano利用分层数据结构[102]支持动态数据库更新，但是这一机制可能给方案引入额外的性能开销，未来可探索更灵活的数据组织形式以优化数据更新成本.

2025年,Hoover等[32]提出Plinko,能够在任意参数设置下实现客户端存储和查询时间的最佳权衡. 对于任意客户端存储大小r,Plinko都能实现$t=\tilde{O}(n/r)$的查询时间,而之前的工作只能达到$r=\tilde{O}(\sqrt{n})$的下界. 此外,Plinko能够在最差$\tilde{O}(1)$的时间内完成对单个数据库记录的更新. 为实现以上目标,Hoover等将标准的伪随机函数推广到具备高效反演的情况,提出了可逆伪随机函数的概念,其正向计算能够在$\tilde{O}(1)$时间内完成,反向计算时间与反向集合大小线性相关. 借助可逆伪随机函数,Plinko能够在$\tilde{O}(1)$时间内找到一条包含目标索引i的提示信息,并在更新过程中只需在对应索引处进行PRF反向计算,即可定位需更新的提示信息.

4.4　单服务器方案小结

与依赖多不合谋服务器假设的多服务器方案不同,单服务器隐匿信息检索方案凭借更广泛的应用场景与更低的部署门槛,逐渐成为该领域的研究热点. 表2对前述方案整体进行分析比较,主要从安全假设、通信开销、计算开销和是否有额外需求等方面,对单服务器隐匿信息检索方案的代表性实例进行对比分析.

表2　单服务器隐匿信息检索方案对比

分类	方案	安全假设	服务器安全模型	通信开销	计算开销	存储开销
基于同态加密	Menon等[71]	LWE	半可信	$\tilde{O}(1)$	$O(n)$	$O(1)$
	Henzinger等[73]	LWE	半可信	$\tilde{O}(1)$	$O(n)$	$\tilde{O}(\sqrt{n})$
	Castro等[76]	RLWE	半可信	$\tilde{O}(1)$	$O(n)$	$O(1)$
	Luo等[78]	RLWE	半可信	$O(1)$	$O(n)$	$O(1)$
	Kang等[81]	RLWE	半可信	$O(1)$	$O(\log n)$	$O(1)$
	Zhou等[84]	LWE	恶意	$\tilde{O}(n)$	$O(\log n)$	$O(1)$
基于不经意传输	Dottling等[92]	DDH/QR	半可信/恶意	$\tilde{O}(1)$	$O(\log n)$	$O(n)$
	Garg等[94]	Power-DDH	半可信	$\tilde{O}(1)$	$O(n)$	$\tilde{O}(1)$
	Chase等[95]	SXDH	半可信	$O(\log n)$	$O(n)$	$O(1)$
	Branco等[97]	DDH	恶意	$\tilde{O}(1)$	$O(n^{1+\varepsilon})$	0
	Couteau等[99]	RLWE	半可信/恶意	$\tilde{O}(1)$	$O(n)$	$O(n)$
基于其他方法	Mahdavi等[101]	NONE	半可信	$O(\log n)$	$O(n)$	0
	Zhou等[18]	LWE	半可信	$\tilde{O}(1)$	$\tilde{O}(\sqrt{n})$	$\tilde{O}(\sqrt{n})$
	Hoover等[32]	OWF	半可信	$O(\log n)$	$\tilde{O}(n/r)$	$\tilde{O}(r)$

在安全假设上,不同于多服务器方案,单服务器方案多基于同态加密和不经意传输,并主要依赖LWE假设和DDH类假设. 理论性能上,目前两种方案在通信开销均能够达到对数多项式级的理论最优水准,然而在计算开销上,两类方案仍处于线性级别,这对其实际应用造成一定制约,且后者往往会产生不低的客户端计算开销. 从额外需求的角度来看,基于同态加密的方案多使用预处理架构以分摊在线阶段的计算成本,但相应要求在客户端存储额外信息. 基于不经意传输的方案多数无需额外存储,但部分方案存在显著额外开销. Dottling等[92]的方案需在服务器上存储默克尔树,带来线性级的服务器额外存储开销,而Couteau等[99]则要求服务器存储主密钥、客户端存储约束密钥,导致通信双方均需承担额外线性级存储开销.

单服务器隐匿信息检索的核心挑战在于如何在保障查询隐私的同时,实现计算、通信与存储开销之间的合理平衡. 当前主流路径围绕密码学基础工具展开,通过同态加密或不经意传输机制构建隐私保护方案,实质是在不同数学结构中权衡隐私保障与系统效率. 基于同态加密的方案利用密文空间的代数结构特性,通过同态乘法、密文旋转等操作实现服务器在不解密的前提下处理加密查询,核心思路是“以计算换通信”,最大限度减少在线交互负担. 而基于不经意传输的方案则凭借OT协议的选择隐私特性,通过“茫然传输”使服务器无法获知客户端偏好,其本质是“以通信换计算”,用轻量的协议设计替代昂贵的同态运算. 此外,近期研究已开始突破同态加密与不经意传输两种范式的框架限制,尝试解耦隐私保护与传统计算结构的强绑定,探索具备更高效率的新型隐私计算范式,为未来构建更实用的隐匿信息检索方案奠定了方向基础.

5　隐匿信息检索变体

在阐明标准隐匿信息检索方案之后,本文转向讨论隐匿信息检索方案面对实际应用场景中更加复杂和多变需求时的局限性. 伴随数据规模的迅猛增长和密码学技术的突破,标准隐匿信息检索方案在某些场景中可能存在效率、安全或者功能上的挑战. 为克服这些挑战,研究者们提出了多种隐匿信息检索方案变体.

5.1 批处理隐匿信息检索

在特定场景中,用户希望从同一数据库中获得多个记录,然而多次运行标准隐匿信息检索方案产生的开销巨大,无法满足实际查询的效率需求.

为进一步降低多目标索引查询的计算开销,2004年Ishai等[103]引入了批处理编码(batch codes)的概念.在实际查询中,服务器先将数据库编码为固定数量的批处理编码,并在接收到客户端的批量查询请求时对每个查询应用批处理解码过程,即对每个编码块应用标准隐匿信息检索方案来检索所需记录.2016年,Henry[104]系统总结并扩展了先前的批处理技术,提出了全新的批量编码技术.通过引入分级编码,该技术能够显著提升多条数据检索的效率,且其成本低于传统非批量查询时的单条查询.2018年,Angel等[22]设计了一个高效转换框架,能够将任意单查询隐匿信息检索方案转化为批处理方案,同时显著降低了服务器的总计算开销.2023年,Mughees等[105]受Angel等[22]方法的启发,结合一种RLWE同态加密的向量化变体,设计出一种能够借助单一密文检索多个数据库条目的密文合并策略,进而提出了一种兼具低通信开销与低计算开销的隐匿信息检索方案.2024年,Liu等[106]将Mahdavi等[101]方案中的同态相等运算符替换为基于SIMD[107]的运算符,使得方案能够只通过一次密文-密文乘法便能执行N个等式检查,其中N为SIMD密文的槽数,并由此构建了一个低开销的批处理隐匿信息检索协议PIRANA.

批处理编码技术显著提升了多条数据库记录的查询效率,降低了计算和通信开销.然而,在超大规模数据库和高频查询场景下,现有方法仍存在瓶颈.未来的研究应着眼于进一步优化批量查询效率,以提升批处理隐匿信息检索的性能.

5.2 对称隐匿信息检索

隐匿信息检索的核心目标是确保服务器无法获取关于客户端目标索引的任何信息.然而,在实际应用中,许多商业模式往往要求运营商根据用户的检索数据量收费.因此,除了保护客户端隐私之外,服务器的隐私保护同样至关重要.

针对上述挑战,Gertner等[108]于1998年提出了对称隐匿信息检索(Symmetrically Private Information Retrieval,SPIR)的概念.该方案不仅需要保护客户端的隐私,使服务器无法得知客户端的目标索引,同时也要确保客户端只能访问特定的数据项,而无法获取除目标数据外的任何额外信息.Gertner等进一步指出,任何隐匿信息检索方案均可转换为与之轮数相同、线性共享随机性、只增加额外对数因子通信开销的SPIR方案.2022年,Wang等[109]通过向客户端提供数据库不可知的共享随机子集,提出了一种全新的SPIR方案.在特定的参数设置下,该方案能够达到与标准隐匿信息检索相同的容量,从而证实了单服务器SPIR的理论可行性.2022年,Lin等[110]构造了名为XSPIR的对称隐匿信息检索方案,实现了针对半诚实客户端的数据隐私保护.XSPIR引入了一种名为“不经意遮蔽”的技术,能够在密文打包的同时有效删除打包密文中不必要的数据项,且不向服务器泄露保留数据项的相关信息.此外,通过密文净化技术[111],XSPIR能够确保客户端在拥有密钥时也无法获取除目标消息外的额外密文信息.为实现批量查询场景下的服务器隐私保护,2025年Li等[112]提出了名为BitBatSPIR的高效批处理对称隐匿信息检索方案,通过将比特数据库检索问题转化为隐私集合求交问题来实现客户端和服务器隐私,并采用窗口化和分区等优化技术实现了次线性的通信开销,有助于其在大规模数据库和广域网环境中的实际应用.

对称隐匿信息检索旨在同时保护客户端和服务器的隐私,解决在查询过程中双方数据泄露的问题.但在复杂的实际应用中,对称隐匿信息检索的性能优化与隐私保护仍面临挑战.未来对称隐匿信息检索将集中于进一步优化计算和通信开销,提升其在云存储和隐私保护电子商务等领域的适用性.

5.3 关键字隐匿信息检索

在隐匿信息检索的应用场景中,用户需要知道目标记录的索引才能发起查询,此类依赖于索引检索机制的方案被称为索引隐匿信息检索方案(Index PIR).然而,在实际应用中,用户往往掌握的只是数据项的关键字,而非其具体的索引.

为应对这一场景,Chor等[20]于1998年提出了关键字隐匿信息检索方案(Keyword PIR).此方案巧妙地将隐匿信息检索和支持搜索操作的数据结构相结合,旨在实现基于关键字模型的信息私密检索.在查询过程中,任何服务器均无法获取关于编历过程的信息,确保了查询关键字的隐私.2023年,Patel等[113]针对稀疏数据库提出了SparsePIR,其核心是利用编码技术将键值对编码为多个数据库记录的函数.该编码技术不仅可以将稀疏数据库记录编码为线性组合,还兼容包括递归在内的多种PIR优化技术.2024年,Celi等[114]将基于容错学习的隐匿信息检索与二进制融合过滤器[115]结合,提出了ChalametPIR.ChalametPIR能够将支持索引查询的容错学习隐匿信息检索方案转化为支持键值对查询的关键字隐匿信息检索方案,并通过过滤器结构将关键字映射到固定索引集实现隐私查询.2025年,Xu等[116]基于二叉搜索树和全同态加密提出了BstPIR,通过将服务器数据库重构为二叉搜索树,并利用三路同态比较和多路选择器,在加密状态下实现从根节点到目

标节点的盲路径选择. 2025年,Hao等[117]通过构建高效的关键字-索引映射,将关键字隐匿信息检索问题有效转化为索引隐匿信息检索问题,提出了基于稀疏键值对存储、哈希分桶和近似映射三种实用关键字方案,并在实验中展现出超越现有最优方案的性能优势.

关键字隐匿信息检索通过保护用户关键字隐私,满足了非索引查询的实际需求. 然而随着数据库规模扩大和需求复杂化,现有方案在效率和扩展性上仍面临挑战. 未来研究应重点提升各方案在大规模数据库中的效率和隐私保护能力,以适应更多应用场景.

5.4　可更新隐匿信息检索

为有效保护用户的目标查询索引不被泄露,隐匿信息检索方案需要遍历数据库的所有记录以生成响应. 针对这一限制,2000年Beimel等[45]提出了预处理方法作为一种解决方案,此方法显著降低了隐匿信息检索方案的在线开销,但前提是数据库不支持更新操作. 而与此同时,许多依赖于隐匿信息检索的应用程序均存在对数据库内容适度更新的内在需求. Popcorn[118]作为一个基于隐匿信息检索的私有视频服务,其客户端需要处理不定期被添加、删除或修改的电影;在Pung[6]和Talek[119]等匿名消息传递系统中,数据库每隔几分钟便会添加新内容. 因此,如何在保持数据库内容适度更新的同时实现高效的隐匿信息检索,成为一个亟待解决的难题.

2021年,Kogan等[120]提出了一个名为Checklist的私有块列表查找系统,该系统允许客户端在不向服务器暴露其查询字符串的前提下,验证该字符串是否存在于服务器所持有的加密块列表中. 此外,Kogan等通过将原始块列表巧妙地分割为一系列精细管理的较小块列表,有效应对了块列表内容频繁变动的挑战. 2022年,Ma等[121]引入增量预处理的概念,并提出一种名为增量伪随机集合的全新原语,使预处理隐匿信息检索方案能够支持内容动态变化的数据库环境. 该方案减少了因数据库内容更新而需进行重新预处理的需求,代之以与变化频率线性相关的提示信息更新开销. 不过,该方案还存在添加位置受限、删除数据不完全等局限. 2024年,Zhou等[18]基于伪随机函数构建了名为Piano的轻量隐匿信息检索方案,并引入分层数据结构技术[102]以支持数据库的动态更新. 此外,Piano的设计允许客户端在不长期在线的情况下进行操作,从而将定期重构的成本摊销到整个更新周期内,这提升了系统的灵活性和实用性.

可更新隐匿信息检索旨在解决动态数据库中频繁更新的需求,确保在不泄露用户查询信息的同时,支持数据库的高效修改. 然而,现有方案在应对频繁数据增减时仍面临效率和安全上的挑战. 未来研究应聚焦于如何在保持高效查询的同时,提升系统对数据添加、删除和修改的支持,确保在动态环境下实现更灵活安全的隐匿信息检索.

5.5　隐匿信息检索变体小结

根据应用场景的不同实际需求,隐匿信息检索方案可以引申出包含批处理模型、对称模型、关键字模型和可更新模型等变体,展现出隐匿信息检索方案的多样化设计和强适用性. 表3对前述方案整体进行比较,主要从服务器数量、是否满足自适应查询和方案特点等方面,对隐匿信息检索变体的代表性实例进行对比分析.

表3　隐匿信息检索变体对比

分类	方案	服务器数量	服务器安全模型	自适应查询	特点
批处理模型	Henry[104]	多	半可信	不满足	利用分级秘密共享机制构建批量编码计数
	Angel等[22]	单	半可信	不满足	提出通用批处理模型转换框架
	Mughees等[105]	单	半可信	不满足	单一密文实现对多个数据库条目的检索
	Liu等[106]	单	半可信	不满足	借助同态相等运算符加快同态乘法的密文检查
对称模型	Wang等[109]	单	半可信	满足	给出单服务器下服务器隐私保护的证明
	Lin等[110]	单	半可信	满足	实现针对半诚实客户端的数据隐私保护
	Li等[112]	单	半可信	不满足	将对称隐私问题转化为隐私集合求交问题
关键字模型	Patel等[113]	单	半可信	满足	利用编码技术满足稀疏数据库的查询需求
	Celi等[114]	单	半可信	满足	利用过滤器结构将关键字映射至索引集
	Xu等[116]	单	半可信	满足	将数据库重构为二叉搜索树进行查询
	Hao等[117]	单	半可信	满足	提出稀疏键值对存储、哈希分桶和近似映射三种关键字方案
可更新模型	Kogan等[120]	多	半可信	满足	分割较小块以应对列表内容频繁变动的挑战
	Ma等[121]	多	半可信	满足	更新开销与变化频率而非数据库大小线性相关
	Zhou等[18]	单	半可信	满足	借助分层数据结构进行定期重构

考虑服务器数量的设置,不同变体模型针对不同的实际应用场景,对服务器数量的要求不尽相同. 对于隐匿信息检索方案而言,自适应查询指的是客户端可以决定查询的数量、内容,与之相对的是批量查询,使

用批处理操作的隐匿信息检索方案均不满足客户端自适应查询的要求.

6 应用场景

在信息爆炸的时代背景下,隐私保护意识日益增强,如何在享受数据便利的同时确保个人隐私的安全与尊重,成为社会各界关注的焦点. 隐匿信息检索技术的应运而生,为这一问题提供了全新解决思路. 该技术以其独特的加密查询机制,使用户能在不泄露自身查询意图的情况下,从数据库中检索所需信息,极大地拓宽了信息获取的安全边界,为数据库隐私保护[122]、大数据计算安全[123~125]等领域提供了切实有效的解决途径. 其应用场景广泛而深远,特别是在社交发现、匿名通信以及精准广告投递等领域,展现出非凡的潜力和价值.

6.1 关键组件

在实时在线通信场景中,诸多互联网组织使用XMPP(eXtensible Messaging and Presence Protocol)协议[126]向用户提供在线状态通知和好友关系服务. 这类机制虽然实现简单,但普遍存在隐私泄露风险,服务器可轻易掌握用户的社交关系图谱及在线行为状态.

为解决服务器通过监控查询行为窥探用户社交关系这一痛点,2015 年 Borisov 等[2]将隐匿信息检索技术引入在线状态指示服务,提出了一种名为 DP5 的加密服务,用户可通过隐匿信息检索从数据库中检索得到朋友的状态信息,而无需透露查询的具体内容. 此外,DP5 无需保存长期秘密,且在妥协时可提供完美前向保密. 然而,DP5 在用户规模扩大时面临严重的可扩展性问题,使得直接应用隐匿信息检索带来的高昂开销成为其实际应用的新瓶颈. 为此,2018 年 Parhi 等[3]提出了 MP3 协议,采用动态广播加密技术来减少在线数据库的规模,从而有效降低应用隐匿信息检索协议时用户注册和查询操作的带宽消耗,还使得 MP3 拥有优于 DP5 的客户端体验. 面对在双方不暴露各自联系人列表的前提下找到共同好友的挑战,2018 年 Demmler 等[4]结合隐匿信息检索和隐私集合求交[127]的最新进展,设计了一个名为 PIR-PSI 的社交发现系统,通过对布谷鸟哈希表位置掩码结果的私密查询,使客户端仅能获取其联系人与系统中用户集合的交集,而服务器则仅掌握客户端查询规模的粗略估计. 为进一步提升隐匿信息检索在大规模用户场景中的可行性,2023 年 Hetz 等[5]通过引入数据库分区和高效用户查询调度来提高整体性能,同时利用隐匿信息检索代替昂贵的布谷鸟过滤器[128]下载,实现了通信与计算开销的次线性增长,标志着大规模移动社交发现系统的实际可用性迈出了关键一步.

隐匿信息检索在社交发现中的应用能够有效保护用户的好友关系和在线状态,避免服务器获取敏感信息. 然而,随着用户规模的增长,如何在保障隐私的同时提升系统的可扩展性和效率已成为关键问题. 未来的研究应聚焦于在大规模社交场景中进一步优化隐匿信息检索技术,确保在隐私保护和系统性能之间取得更好的平衡.

6.2 匿名通信

在当前大规模监控与网络攻击频发的背景下,保障通信的私密性已成为亟需解决的重要问题. 匿名通信领域面临的核心挑战,是如何在隐藏通信内容及其元数据的同时,支持高并发通信. 这一挑战中的隐私保护痛点,正是隐匿信息检索技术所要解决的核心问题.

2016 年,Angel 等[6]提出了名为 Pung 的通信系统,允许用户在包括 Pung 服务器在内的所有参与方均不知情的情况下存储和检索信息,从而保护通信内容及元数据的隐私,并有效防御全局敌手的攻击. 2021 年,Ahmad 等[7]构造了首个在完全不可信的基础设施上,支持隐藏元数据并扩展至数万用户的语音通信系统 Addra. 在隐私保护上,Addra 借助隐匿信息检索隐藏访问的邮箱 ID,令敌手无法检测系统中任意两个用户之间是否存在通信关系. 2022 年,Vadapalli 等[8]提出了一个匿名消息传递协议 Sabre,利用隐匿信息检索在公告板中隐匿地检索消息,同时借助其变体将消息随机写入,使服务器无法追踪写入者身份. 此外,Sabre 在面对资源耗尽型 Dos 攻击时能够提供渐进加速,且提升了方案在理想环境下的具体性能. 2024 年,Tovey 等[9]提出了一种元数据匿名消息传递架构 DPIR,该方案通过将大部分计算转移到客户端来应对可扩展的挑战,并利用 Freivalds 概率算法[129]对客户端结果高效验证,确保用户免受恶意客户端和非法服务器的攻击.

在匿名通信领域中,隐匿信息检索能够有效保护通信内容和元数据隐私. 但现有系统在面对高并发请求及大规模用户环境时,仍存在性能瓶颈与成本过高的问题. 未来研究应聚焦于协议效率和可扩展性的进一步优化,以在复杂网络环境中实现更高水平的通信安全保障.

6.3 广告投递

在线行为广告通过跟踪网络用户的在线活动以提供定制化广告,已成为众多 Web 服务的重要收入来源. 然而,这种跟踪往往在用户无感知的情况下进行,导致个人兴趣、行为等敏感信息被广告平台收集,构成严重的隐私泄露. 在此场景中,隐匿信息检索能够保护用户在广告数据库中的查询隐私. 用户通过隐匿信息检索协议向广告平台隐匿地检索目标广告,使服务器无法获知用户的具体选择,从而切断从查询行为到个人兴趣画像的推断链路.

为防止广告平台通过广告分发行为推断出用户的个人兴趣,2016年Green等[10]基于Adnostic[130]提出的同态加密算法思路,提出了AdScale隐私广告投放方案. 该方案结合加法同态投票方案和新的密码学证明技术,利用隐匿信息检索使用户在不泄露隐私的条件下获取广告内容,实现了对数十亿级广告印象高效且安全的报告功能,并在无需对可信第三方施加高负载的情况下展现出良好的扩展能力. 2021年,Mughees等[11]设计了名为PrivateFetch的新框架,利用本地偏好计算和高性能的单服务器隐匿信息检索来确保客户端能从服务器预获取广告内容,并防止服务器根据客户端的请求模式推断其偏好. 然而,由于PrivateFetch无法直接与批处理隐匿信息检索方案兼容,其系统延迟仍保持在较高水平. 2021年,Servan-Schreiber等[12]构建了广告系统AdVeil,旨在应对不可信广告网络中进行私人定向而不泄露用户特征的挑战,通过结合隐匿信息检索和局部敏感哈希[131]来实现最近邻搜索,并通过匿名代理和不可链接的匿名令牌[132]来识别和防止广告欺诈. 2022年,Zhong等[13]提出了广告投递系统Ibex,减少了收集的用户数据,同时仍允许广告商在实时广告中出价,并衡量其广告活动的有效性. 在Ibex中,广告平台通过隐匿信息检索获取竞买数据库中对应用户组的加密竞买份额,隐藏用户的实际组别和竞买内容的关联. 但系统仍需向拍卖方揭示获胜广告商身份,可能造成用户隐私泄露的风险.

隐匿信息检索在广告投递领域提供了有效的用户隐私保护机制,使广告商能够在不直接接触用户数据的前提下实现个性化推荐. 然而,当前系统仍面临在提升广告精准度与保护用户隐私之间的权衡难题. 未来的研究应进一步优化系统结构与协议效率,以实现更高性能的广告投递服务,满足不断增长的市场需求的同时,强化对用户隐私的保护能力.

7　总结与展望

本文综述了隐匿信息检索技术的研究现状,介绍了隐匿信息检索的详细定义及属性,列举了现有方案使用的密码学原语,同时以服务器数量为划分对当前代表性成果进行论述,阐述现有研究成果的设计思路和优缺分析,最后展望隐匿信息检索在社交发现、匿名通信和广告投递等不同领域的应用.

在当前隐匿信息检索技术的发展基础上,本文进一步讨论隐匿信息检索的未来研究点,希望能够激发研究者们设计更完备隐匿信息检索方案的灵感,主要包含以下三个方面.

(1)降低隐匿信息检索的理论开销,实现更加高效的信息查询. 在实际场景中,用户对不同数据的查询频率往往存在差异,如用户对微博榜前的访问偏好远高于其他数据;另外,部分场景中用户并不要求查询过程对服务器完全保密,如公共推荐系统中用户仅希望自己不被明确识别. 基于此,未来研究可将计算资源向高流行数据倾斜,以降低低流行数据的响应准确性为代价提高方案整体效率;或根据实际场景的安全需求适时调整隐私保护强度,为低安全要求用户提供更高效的信息查询服务.

(2)扩展隐匿信息检索的应用场景,探索其在诸多领域的应用潜力. 现有方案大多在单一目标进行优化,缺乏对实际系统中多样化需求的整体适配能力,如许多预处理方案难以支持高效数据更新,或不具备对关键字等结构化内容的灵活查询能力. 因此,未来研究可聚焦于构建一种统一的隐匿信息检索架构,通过引入增量更新、索引映射等技术,在保持低通信复杂度和计算开销的同时,融合包括动态更新、结构化搜索等多种核心功能.

(3)解决隐匿信息检索在实际系统中的部署问题,确保其高效且稳定地运行. 预处理隐匿信息检索方案往往依赖客户端具备一定计算与存储能力,但该前提在资源受限的移动或嵌入式环境中难以满足,从而限制了其现实可行性. 此外,部分方案虽已在理论上实现接近最优的性能,但由于实现方法复杂、对内在安全性要求较高,当前难以在实际环境中部署. 因此,未来研究可探索融合边缘计算架构,将部分中间计算任务转移至边缘节点,以适配移动终端和嵌入式设备的资源约束;同时,通过根据应用场景灵活调整方案的隐私保护强度和系统性能,方案的实际可用性将得到进一步提升.

参考文献

[1] CHOR B, GOLDREICH O, KUSHILEVITZ E, et al. Private information retrieval[C]//Proceedings of IEEE 36th Annual Foundations of Computer Science. Piscataway: IEEE, 2002: 41-50.

[2] BORISOV N, DANEZIS G, GOLDBERG I. DP5: A private presence service[J]. Proceedings on Privacy Enhancing Technologies, 2015, 2015(2): 4-24.

[3] PARHI R, SCHLIEP M, HOPPER N. MP3: A more efficient private presence protocol[M]//Financial Cryptography and Data Security. Berlin, Heidelberg: Springer, 2018: 38-57.

[4] DEMMLER D, RINDAL P, ROSULEK M, et al. PIR-PSI: Scaling private contact discovery[J]. Proceedings on Privacy Enhancing Technologies, 2018, 2018(4): 159-178.

[5] HETZ L, SCHNEIDER T, WEINERT C. Scaling mobile private contact discovery to billions of users[C]//Computer Security-ESORICS 2023. Cham: Springer, 2024: 455-476.

[6] ANGEL S, SETTY S. Unobservable communication over fully untrusted infrastructure[C]//Proceedings of the 12th USENIX Conference on Operating Systems Design and Implementation. New York: ACM, 2016: 551-569.

[7] AHMAD I, YANG Y T, AGRAWAL D, et al. Addra: metadata-private voice communication over fully untrusted infrastructure[C]//Proceedings of 15th USENIX Symposium on Operating Systems Design and Implementation. Berkeley: USENIX Association, 2021: 313-329.

[8] VADAPALLI A, STORRIER K, HENRY R. Sabre: Sender-anonymous messaging with fast audits[C]//2022 IEEE Symposium on Security and Privacy. Piscataway: IEEE, 2022: 1953-1970.

[9] TOVEY E, WEISS J, GILAD Y. Distributed PIR: Scaling private messaging via the users' machines[C]//Proceedings of the 2024 on ACM SIGSAC Conference on Computer and Communications Security. New York: ACM, 2024: 1967-1981.

[10] GREEN M, LADD W, MIERS I. A protocol for privately reporting ad impressions at scale[C]//Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security. New York: ACM, 2016: 1591-1601.

[11] MUGHEES M H, PESTANA G, DAVIDSON A, et al. PrivateFetch: Scalable catalog delivery in privacy-preserving advertising[EB/OL]. (2021-09-16) [2025-06-19]. https://arXiv.org/abs/2109.08189.

[12] SERVAN-SCHREIBER S, HOGAN K, DEVADAS S. Adveil: A private targeted advertising ecosystem[EB/OL]. (2022-03-08)[2025-06-19]. https://eprint.iacr.org/2021/1032.

[13] ZHONG K, MA Y P, ANGEL S. Ibex: Privacy-preserving ad conversion tracking and bidding[C]//Proceedings of the 2022 ACM SIGSAC Conference on Computer and Communications Security. New York: ACM, 2022: 3223-3237.

[14] CHOR B, GILBOA N. Computationally private information retrieval (extended abstract)[C]//Proceedings of the Twenty-Ninth Annual ACM Symposium on Theory of Computing. New York: ACM, 1997: 304-313.

[15] KUSHILEVITZ E, OSTROVSKY R. Replication is not needed: Single database, computationally-private information retrieval[C]//Proceedings 38th Annual Symposium on Foundations of Computer Science. Piscataway: IEEE, 2002: 364-373.

[16] GOLDWASSER S, MICALI S. Probabilistic encryption[J]. Journal of Computer and System Sciences, 1984, 28(2): 270-299.

[17] GHOSHAL A, ZHOU M X, SHI E. Efficient pre-processing PIR without public-key cryptography[C]//Advances in Cryptology-EUROCRYPT 2024. Cham: Springer, 2024: 210-240.

[18] ZHOU M X, PARK A, ZHENG W T, et al. Piano: Extremely simple, single-server PIR with sublinear server computation[C]//2024 IEEE Symposium on Security and Privacy. Piscataway: IEEE, 2024: 4296-4314.

[19] ALBAB K D, ISSA R, VARIA M, et al. Batched differentially private information retrieval[C]//Proceedings of the 31st USENIX Security Symposium. Berkeley: USENIX Association, 2022:3327-3344.

[20] CHOR B, GILBOA N, NAOR M. Private information retrieval by keywords[EB/OL]. (1998-02-03) [2025-06-19]. http://eprint.iacr.org/1998/003.

[21] AGUILAR-MELCHOR C, BARRIER J, FOUSSE L, et al. XPIR: Private information retrieval for everyone[J]. Proceedings on Privacy Enhancing Technologies, 2016, 2016(2): 155-174.

[22] ANGEL S, CHEN H, LAINE K, et al. PIR with compressed queries and amortized query processing[C]//2018 IEEE Symposium on Security and Privacy. Piscataway: IEEE, 2018: 962-979.

[23] GASARCH W I. A survey on private information retrieval[J]. Bulletin of EATCS, 2004, 82: 72-107.

[24] OSTROVSKY R, SKEITH W E III. A survey of single-database private information retrieval: Techniques and applications[M]//Public Key Cryptography - PKC 2007. Berlin, Heidelberg: Springer, 2007: 393-411.

[25] ALFARANO G N, KHATHURIA K, WEGER V. A survey on single server private information retrieval in a coding theory perspective[J]. Applicable Algebra in Engineering, Communication and Computing, 2023, 34(3): 335-358.

[26] HOLZBAUR L, HOLLANTI C, WACHTER-ZEH A. Computational code-based single-server private information retrieval[C]//2020 IEEE International Symposium on Information Theory. Piscataway: IEEE, 2020: 1065-1070.

[27] AGUILAR MELCHOR C, GABORIT P. A fast private information retrieval protocol[C]//2008 IEEE International Symposium on Information Theory. Piscataway: IEEE, 2008: 1848-1852.

[28] REGEV O. On lattices, learning with errors, random linear codes, and cryptography[C]//Proceedings of the Thirty-Seventh Annual ACM Symposium on Theory of Computing. New York: ACM, 2005: 84-93.

[29] VITHANA S, WANG Z S, ULUKUS S. Private information retrieval and its extensions: An introduction, open problems, future directions[J]. IEEE BITS the Informa-

tion Theory Magazine, 2023, 3(4): 67-85.

[30] KIM J, PARK J, SUNG H M. Private information retrieval based on homomorphic encryption, revisited[J/OL]. IACR Cryptology ePrint Archive, 2025: 729. https://eprint.iacr.org/2025/729.

[31] NGUYEN H D, GUAJARDO J, HOANG T. Client-efficient online-offline private information retrieval[J]. Proceedings on Privacy Enhancing Technologies, 2025(3): 192-212.

[32] HOOVER A, PATEL S, PERSIANO G, et al. Plinko: Single-server PIR with efficient updates via invertible PRFs[C]// Advances in Cryptology-EUROCRYPT 2025. Cham: Springer, 2025: 3-33.

[33] BOYLE E, GILBOA N, ISHAI Y. Function secret sharing[M]//Advances in Cryptology - EUROCRYPT 2015. Berlin, Heidelberg: Springer, 2015: 337-367.

[34] BOYLE E, GILBOA N, ISHAI Y. Function secret sharing: Improvements and extensions[C]//Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security. New York: ACM, 2016: 1292-1303.

[35] GILBOA N, ISHAI Y. Distributed point functions and their applications[C]//Advances in Cryptology-EUROCRYPT 2014. Berlin: Springer, 2014: 640-658.

[36] GOLDREICH O, GOLDWASSER S, MICALI S. How to construct random functions[J]. Journal of the ACM, 1986, 33(4): 792-807.

[37] WANG F, YUN C, GOLDWASSER S, et al. Splinter: practical private queries on public data[C]//Proceedings of the 14th USENIX Symposium on Networked Systems Design and Implementation. Berkeley: USENIX Association, 2017: 299-313.

[38] Corporation Intel. Advanced encryption standard instructions (AES-NI) [EB/OL]. (2012-02-02)[2025-06-19]. https://www. intel. cn/content/www/cn/zh/developer/articles/technical/advanced-encryption-standard-instructions-aes-ni.html.

[39] KRUGLIK S, DAU S H, KIAH H M, et al. Verifiable information-theoretic function secret sharing[EB/OL]. (2024-03-18)[2025-06-19]. https://eprint.iacr.org/2024/453.

[40] KRUGLIK S, DAU S H, KIAH H M, et al. Querying twice to achieve information-theoretic verifiability in private information retrieval[J]. IEEE Transactions on Information Forensics and Security, 2024, 19: 8172-8187.

[41] PARK A, LEONG T, MATURANA F, et al. Communication-efficient, fault tolerant PIR over erasure coded storage[C]//2024 IEEE Symposium on Security and Privacy. Piscataway: IEEE, 2024: 4331-4347.

[42] SHAMIR A. How to share a secret[J]. Communications of the ACM, 1979, 22(11): 612-613.

[43] XING P Z, LI H W, HAO M, et al. Distributed function secret sharing and applications[EB/OL]. (2025)[2025-06-19]. https://www. ndss-symposium. org/wp-content/uploads/2025-2233-paper.pdf.

[44] KIM D, SON Y, KIM D, et al. Privacy-preserving approximate GWAS computation based on homomorphic encryption[J]. BMC Medical Genomics, 2020, 13(7): 77.

[45] BEIMEL A, ISHAI Y, MALKIN T. Reducing the servers computation in private information retrieval: PIR with preprocessing[C]//Advances in Cryptology - CRYPTO 2000. Berlin: Springer, 2000: 55-73.

[46] CORRIGAN-GIBBS H, KOGAN D. Private information retrieval with sublinear online time[C]//Advances in Cryptology-EUROCRYPT 2020. Cham: Springer, 2020: 44-75.

[47] SHI E, AQEEL W, CHANDRASEKARAN B, et al. Puncturable pseudorandom sets and private information retrieval with near-optimal online bandwidth and time[C]//Advances in Cryptology - CRYPTO 2021. Cham: Springer, 2021: 641-669.

[48] RISTENPART T, YILEK S. The mix-and-cut shuffle: Small-domain encryption secure against N queries[C]//Advances in Cryptology - CRYPTO 2013. Berlin: Springer, 2013: 392-409.

[49] STEFANOV E, SHI E. FastPRP: Fast pseudo-random permutations for small do-mains[EB/OL]. (2012-06-15)[2025-06-19]. https://eprint.iacr.org/2012/254.

[50] LAZZARETTI A, PAPAMANTHOU C. TreePIR: Sublinear-time and polylog-bandwidth private information retrieval from DDH[C]//Advances in Cryptology - CRYPTO 2023. Cham: Springer, 2023: 284-314.

[51] BONEH D. The decision diffie-Hellman problem[C]//Algorithmic Number Theory. Berlin: Springer, 1998: 48-63.

[52] ZHOU M X, LIN W K, TSELEKOUNIS Y, et al. Optimal single-server private information retrieval[C]//Advances in Cryptology-EUROCRYPT 2023. Cham: Springer, 2023: 395-425.

[53] SINGH J, WEI Y, ZIKAS V. Information-theoretic multi-server private information retrieval with client preprocessing[C]// Theory of Cryptography. Cham: Springer, 2025: 423-450.

[54] DOTTLING N, DUJMOVIC J, LOSS J, et al. Minicrypt PIR for big batches[EB/OL]. (2025-02-21) [2025-06-19]. https://eprint.iacr.org/2025/317.

[55] LAZZARETTI A, PAPAMANTHOU C. Single pass client-preprocessing private information retrieval[C]//Proceedings of the 33rd USENIX Conference on Security Symposium. New York: ACM, 2024: 5967-5984.

[56] DURSTENFELD R. Algorithm 235: Random permutation[J]. Communications of the ACM, 1964, 7(7): 420-421.

[57] KNUTH D E. The Art of Computer Programming, Volume II: Seminumerical Algorithms[M]. Massachusetts: Addison-Wesley, 1997.

[58] ROCHE D S, AVIV A, CHOI S G, et al. Deterministic, stash-free write-only ORAM[C]//Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security. New York: ACM, 2017: 507-521.

[59] CRAMER R, GENNARO R, SCHOENMAKERS B. A secure and optimally efficient multi-authority election scheme[C]//Advances in Cryptology - EUROCRYPT'97. Berlin: Springer, 1997: 103-118.

[60] 刘明洁, 王安. 全同态加密研究动态及其应用概述[J]. 计算机研究与发展, 2014, 51(12): 2593-2603.
LIU M J, WANG A. Fully homomorphic encryption and its applications[J]. Journal of Computer Research and Development, 2014, 51(12): 2593-2603. (in Chinese)

[61] 杨亚涛, 赵阳, 张卷美, 等. 同态密码理论与应用进展[J]. 电子与信息学报, 2021, 43(2): 475-487.
YANG Y T, ZHAO Y, ZHANG J M, et al. Theory and application progress of homomorphic cryptography[J]. Journal of Electronics & Information Technology, 2021, 43(2): 475-487. (in Chinese)

[62] 周素芳, 窦家维, 郭奕旻, 等. 安全多方向量计算[J]. 计算机学报, 2017, 40(5): 1134-1150.
ZHOU S F, DOU J W, GUO Y M, et al. Secure multi-party vector calculation[J]. Chinese Journal of Computers, 2017, 40(5): 1134-1150. (in Chinese)

[63] 李顺东, 赵雪玲, 家珠亮, 等. 集合交集元素和的保密计算[J]. 电子学报, 2023, 51(1): 86-92.
LI S D, ZHAO X L, JIA Z L, et al. Secure calculation of the sum of elements in the intersection of sets[J]. Acta Electronica Sinica, 2023, 51(1): 86-92. (in Chinese)

[64] 马秀莲, 张倦倦, 李顺东, 等. 保密计算交集对应元素和的最大值[J]. 电子学报, 2023, 51(7): 1835-1841.
MA X L, ZHANG J J, LI S D, et al. The maximum value of the sum of elements corresponding to the intersection of secret computation[J]. Acta Electronica Sinica, 2023, 51(7): 1835-1841. (in Chinese)

[65] 窦家维, 刘旭红, 周素芳, 等. 高效的集合安全多方计算协议及应用[J]. 计算机学报, 2018, 41(8): 1844-1860.
DOU J W, LIU X H, ZHOU S F, et al. Efficient set security multiparty computing protocol and its application[J]. Chinese Journal of Computers, 2018, 41(8): 1844-1860. (in Chinese)

[66] 巩林明, 李顺东, 窦家维, 等. 同态加密方案及安全两点直线计算协议[J]. 软件学报, 2017, 28(12): 3274-3292.
GONG L M, LI S D, DOU J W, et al. Homomorphic encryption scheme and secure two-point straight line calculation protocol[J]. Journal of Software, 2017, 28(12): 3274-3292. (in Chinese)

[67] 陈振华, 李顺东, 陈立朝, 等. 点和区间关系的全隐私保密判定[J]. 中国科学(信息科学), 2018, 48(2): 187-204.
CHEN Z H, LI S D, CHEN L C, et al. Full privacy and confidentiality judgment of the relationship between point and interval[J]. Science in China (Information Sciences), 2018, 48(2): 187-204. (in Chinese)

[68] 李宗育, 桂小林, 顾迎捷, 等. 同态加密技术及其在云计算隐私保护中的应用[J]. 软件学报, 2018, 29(7): 1827-1851.
LI Z Y, GUI X L, GU Y J, et al. Homomorphic encryption technology and its application in privacy protection of cloud computing[J]. Journal of Software, 2018, 29(7): 1827-1851. (in Chinese)

[69] 李顺东, 窦家维, 王道顺, 等. 同态加密算法及其在云安全中的应用[J]. 计算机研究与发展, 2015, 52(6): 1378-1388.
LI S D, DOU J W, WANG D S, et al. Homomorphic encryption algorithm and its application in cloud security[J]. Journal of Computer Research and Development, 2015, 52(6): 1378-1388. (in Chinese)

[70] 李占利, 陈立朝, 陈振华, 等. 云环境下多方保密计算最大值、最小值及其统计学应用[J]. 密码学报, 2019, 6(2): 219-233.
LI Z L, CHEN L C, CHEN Z H, et al. Maximum and minimum values of multi-party secret calculation in cloud environment and its statistical application[J]. Journal of Cryptologic Reseatch, 2019, 6(2): 219-233. (in Chinese)

[71] MENON S J, WU D J. SPIRAL: Fast, high-rate single-server PIR via FHE composition[C]//2022 IEEE Symposium on Security and Privacy. Piscataway: IEEE, 2022: 930-947.

[72] GENTRY C, SAHAI A, WATERS B. Homomorphic encryption from learning with errors: Conceptually-simpler, asymptotically-faster, attribute-based[M]//Advances in Cryptology. Berlin, Heidelberg: Springer, 2013: 75-92.

[73] HENZINGER A, HONG M M, CORRIGAN-GIBBS H, et al. One server for the price of two: simple and fast single-server private information retrieval[C]//Proceedings of the 32nd USENIX Security Symposium. Berkeley: USENIX Association, 2023: 3889-3905.

[74] LAURIE B. Certificate transparency[J]. Communications of the ACM, 2014, 57(10): 40-46.

[75] MEIKLEJOHN S, DEBLASIO J, O'BRIEN D, et al. SoK: SCT auditing in certificate transparency[J]. Proceedings on

Privacy Enhancing Technologies, 2022, 2022(3): 336-353.

[76] CASTRO D L, LEWI K, SUH E. WhisPIR: Stateless private information retrieval with low communication[EB/OL]. (2024-02-19)[2025-06-19]. https://eprint.iacr.org/2024/266.

[77] BRAKERSKI Z, GENTRY C, VAIKUNTANATHAN V. (leveled) fully homomorphic encryption without bootstrapping[J]. ACM Transactions on Computation Theory (TOCT), 2014, 6(3): 1-36.

[78] LUO M, LIU F H, WANG H. Faster FHE-based single-server private information retrieval[C]//Proceedings of the 2024 on ACM SIGSAC Conference on Computer and Communications Security. New York: ACM, 2024: 1405-1419.

[79] LYUBASHEVSKY V, PEIKERT C, REGEV O. On ideal lattices and learning with errors over rings[C]//Advances in Cryptology - EUROCRYPT 2010. Berlin: Springer, 2010: 1-23.

[80] HALEVI S, SHOUP V. Faster homomorphic linear transformations in HElib[C]//Advances in Cryptology - CRYPTO 2018. Cham: Springer, 2018: 93-120.

[81] KANG J Y, SCHILD L. Pirouette: Query efficient single-server PIR[J]. IACR Cryptol. EPrint Arch., 2025, 2025: 680.

[82] CHILLOTTI I, GAMA N, GEORGIEVA M, et al. Faster fully homomorphic encryption: Bootstrapping in less than 0.1 seconds[C]//Advances in Cryptology - ASIACRYPT 2016. Berlin: Springer, 2016: 3-33.

[83] KLUCZNIAK K. NTRU-v-um: Secure fully homomorphic encryption from NTRU with small modulus[C]//Proceedings of the 2022 ACM SIGSAC Conference on Computer and Communications Security. New York: ACM, 2022: 1783-1797.

[84] ZHOU F C, SUN J T, WANG Q, et al. Efficient private information retrievals for single-server based on verifiable homomorphic encryption[J]. Computer Standards & Interfaces, 2025, 93: 103961.

[85] PARNO B, HOWELL J, GENTRY C, et al. Pinocchio: Nearly practical verifiable computation[J]. Communications of the ACM, 2016, 59(2): 103-112.

[86] YU Q, MADDAH-ALI M ALI, AVESTIMEHR A S. Polynomial codes: An optimal design for high-dimensional coded matrix multiplication[EB/OL]. (2018-01-24) [2025-06-19]. https://arXiv.org/abs/1705.10464.

[87] RABIN M O. How to exchange secrets with oblivious transfer[EB/OL]. (2011-10-18) [2025-06-19]. https://eprint.iacr.org/2005/187.

[88] BELLARE M, MICALI S. Non-interactive oblivious transfer and applications[C]//Advances in Cryptology - CRYPTO' 89 Proceedings. New York: Springer, 1990: 547-557.

[89] BRASSARD G, CREPEAU C, ROBERT J M. All-or-nothing disclosure of secrets[M]//Advances in Cryptology - CRYPTO'86. Berlin, Heidelberg: Springer, 2007: 234-238.

[90] 石润华, 仲红, 崔杰, 等 . 具有统计特性的不经意传输协议[J]. 电子学报, 2014, 42(11): 2273-2279.
SHI R H, ZHONG H, CUI J, et al. Unintentional transport protocol with statistical characteristics[J]. Acta Electronica Sinica, 2014, 42(11): 2273-2279. (in Chinese)

[91] 冯涛, 马建峰, 李凤华, 等 . UC 安全的高效不经意传输协议[J]. 电子学报, 2008, 36(1): 17-23.
FENG T, MA J F, LI F H, et al. Efficient and casual transport protocol for UC security[J]. Acta Electronica Sinica, 2008, 36(1): 17-23. (in Chinese)

[92] DÖTTLING N, GARG S, ISHAI Y, et al. Trapdoor hash functions and their applications[C]//Advances in Cryptology - CRYPTO 2019. Cham: Springer, 2019: 3-32.

[93] LIPMAA H. An oblivious transfer protocol with log-squared communication[C]//Information Security. Berlin: Springer, 2005: 314-328.

[94] GARG S, HAJIABADI M, OSTROVSKY R. Efficient range-trapdoor functions and applications: Rate-1 OT and more[C]//Theory of Cryptography. Cham: Springer, 2020: 88-116.

[95] CHASE M, GARG S, HAJIABADI M, et al. Amortizing rate-1 OT and applications to PIR and PSI[C]//Theory of Cryptography. Cham: Springer, 2021: 126-156.

[96] BALLARD L, GREEN M, MEDEIROS B D, et al. Correlation-resistant storage via key-word-searchable encryption [EB/OL]. (2005-11-22)[2025-06-19]. https://eprint.iacr.org/2005/417.

[97] BRANCO P, DÖTTLING N, SRINIVASAN A. A framework for statistically sender private OT with optimal rate[C]//Advances in Cryptology - CRYPTO 2023. Cham: Springer, 2023: 548-576.

[98] BITANSKY N, FREIZEIT S. Statistically sender-private OT from LPN and derandomization[C]//Advances in Cryptology - CRYPTO 2022. Cham: Springer, 2022: 625-653.

[99] COUTEAU G, DEVADAS L, DEVADAS S, et al. QuietOT: Lightweight oblivious transfer with a public-key setup[C]//Advances in Cryptology - ASIACRYPT 2024. Singapore: Springer, 2025: 197-231.

[100] SERVAN-SCHREIBER S. Constrained pseudorandom functions for inner-product predicates from weaker assumptions[C]//Advances in Cryptology - ASIACRYPT 2024. Singapore: Springer, 2025: 232-265.

[101] MAHDAVI R A, KERSCHBAUM F. Constant-weight PIR: Single-round keyword PIR via constant-weight equality operators[EB/OL]. (2022-02-16) [2025-06-19]. https://arXiv.org/abs/2202.07569.

[102] BENTLEY J L, SAXE J B. Decomposable searching problems I. Static-to-dynamic transformation[J]. Journal of Algorithms, 1980, 1(4): 301-358.

[103] ISHAI Y, KUSHILEVITZ E, OSTROVSKY R, et al. Batch codes and their applications[C]//Proceedings of the Thirty-Sixth Annual ACM Symposium on Theory of Computing. New York: ACM, 2004: 262-271.

[104] HENRY R. Polynomial batch codes for efficient IT-PIR[J]. Proceedings on Privacy Enhancing Technologies, 2016(4): 202-218.

[105] MUGHEES M H, REN L. Vectorized batch private information retrieval[C]//2023 IEEE Symposium on Security and Privacy. Piscataway: IEEE, 2023: 437-452.

[106] LIU J, LI J Y, WU D, et al. PIRANA: Faster multi-query PIR via constant-weight codes[C]//2024 IEEE Symposium on Security and Privacy. Piscataway: IEEE, 2024: 4315-4330.

[107] SMART N P, VERCAUTEREN F. Fully homomorphic SIMD operations[J]. Designs, Codes and Cryptography, 2014, 71(1): 57-81.

[108] GERTNER Y, ISHAI Y, KUSHILEVITZ E, et al. Protecting data privacy in private information retrieval schemes[C]//Proceedings of the Thirtieth Annual ACM Symposium on Theory of Computing. New York: ACM, 1998: 151-160.

[109] WANG Z S, ULUKUS S. Symmetric private information retrieval at the private information retrieval rate[J]. IEEE Journal on Selected Areas in Information Theory, 2022, 3(2): 350-361.

[110] LIN C Y, LIU Z Y, MALKIN T. XSPIR: Efficient symmetrically private information retrieval from ring-LWE[C]//Computer Security - ESORICS 2022. Cham: Springer, 2022: 217-236.

[111] DUCAS L, STEHLÉ D. Sanitization of FHE ciphertexts[C]//Advances in Cryptology - EUROCRYPT 2016. Berlin: Springer, 2016: 294-310.

[112] LI S S, PENG L Q, LIU W R, et al. BitBatSPIR: Efficient batch symmetric private information retrieval from PSI[J]. IEEE Transactions on Dependable and Secure Computing, 2025, 22(6): 6028-6039.

[113] PATEL S, SEO J Y, YEO K. Don´t be dense: Efficient keyword PIR for sparse databases[C]//Proceedings of the 32nd USENIX Security Symposium. Berkeley: USENIX Association, 2023: 3853-3870.

[114] CELI S, DAVIDSON A. Call me by my name: Simple, practical private information retrieval for keyword queries[C]//Proceedings of the 2024 on ACM SIGSAC Conference on Computer and Communications Security. New York: ACM, 2024: 4107-4121.

[115] GRAF T M, LEMIRE D. Binary fuse filters: Fast and smaller than xor filters[J]. Journal of Experimental Algorithmics (JEA), 2022, 27: 1-15.

[116] XU K X, SU L, HE S, et al. BstPIR: Keyword private information retrieval based on binary search trees[J]. IEEE Internet of Things Journal, 2025, 12(12): 21304-21314.

[117] HAO M, LIU W R, PENG L Q, et al. Practical keyword private information retrieval from key-to-index mappings[C]//Proceedings of the 34th USENIX Security Symposium. Berkeley: USENIX Association, 2025: 3397-3416.

[118] GUPTA T, CROOKS N, MULHERN W, et al. Scalable and private media consumption with Popcorn[C]//Proceedings of the 13th Usenix Conference on Networked Systems Design and Implementation. New York: ACM, 2016: 91-107.

[119] CHENG R, SCOTT W, MASSEROVA E, et al. Talek: Private group messaging with hidden access patterns[C]//Proceedings of the 36th Annual Computer Security Applications Conference. New York: ACM, 2020: 84-99.

[120] KOGAN D, CORRIGAN-GIBBS H. Private blocklist lookups with checklist[C]//Proceedings of the 30th USENIX Security Symposium. Berkeley: USENIX Association, 2021: 875-892.

[121] MA Y P, ZHONG K, RABIN T, et al. Incremental offline/online PIR[C]//Proceedings of the 31st USENIX Security Symposium. Berkeley: USENIX Association, 2022: 1741-1758.

[122] 田秀霞, 王晓玲, 高明, 等. 数据库服务: 安全与隐私保护[J]. 软件学报, 2010, 21(5): 991-1006.
TIAN X X, WANG X L, GAO M, et al. Database service-security and privacy protection[J]. Journal of Software, 2010, 21(5): 991-1006. (in Chinese)

[123] 孟小峰, 张啸剑. 大数据隐私管理[J]. 计算机研究与发展, 2015, 52(2): 265-281.
MENG X F, ZHANG X J. Big data privacy management[J]. Journal of Computer Research and Development, 2015, 52(2): 265-281. (in Chinese)

[124] 钱文君, 沈晴霓, 吴鹏飞, 等. 大数据计算环境下的隐私保护技术研究进展[J]. 计算机学报, 2022, 45(4): 669-701.
QIAN W J, SHEN Q N, WU P F, et al. Research progress of privacy protection technology in big data computing environment[J]. Chinese Journal of Computers,

2022, 45(4): 669-701. (in Chinese)
[125] 曹珍富, 董晓蕾, 周俊, 等. 大数据安全与隐私保护研究进展[J]. 计算机研究与发展, 2016, 53(10): 2137-2151. CAO Z F, DONG X L, ZHOU J, et al. Research progress of big data security and privacy protection[J]. Journal of Computer Research and Development, 2016, 53(10): 2137-2151. (in Chinese)
[126] SAINT-ANDRE P, SMITH K, TRONCON R. XMPP - The Definitive Guide: Building Real-Time Applications with Jabber Technologies[M]. California: O'Reilly, 2009.
[127] PINKAS B, SCHNEIDER T, ZOHNER M. Scalable private set intersection based on OT extension[J]. ACM Transactions on Privacy and Security (TOPS), 2018, 21(2): 1-35.
[128] EPPSTEIN D. Cuckoo filter: Simplification and analysis[EB/OL]. (2016-04-20) [2025-06-19]. https://arxiv.org/abs/1604.06067.
[129] FREIVALDS R. Probabilistic machines can use less running time[EB/OL]. (1977) [2025-06-19]. https://www.semanticscholar.org/paper/Probabilistic-Machines-Can-Use-Less-Running-Time-Freivalds/4d7756df23e6162994de1806761d8e3afcb9aac4.
[130] TOUBIANA V, NARAYANAN A, BONEH D, et al. Adnostic: Privacy preserving targeted advertising[C]// Proceedings of the Network and Distributed System Security Symposium. California: Internet Society, 2010.
[131] GIONIS A, INDYK P, MOTWANI R. Similarity search in high dimensions via hashing[C]//Proceedings of the 25th International Conference on Very Large Data Bases. New York: ACM, 1999: 518-529.
[132] KREUTER B, LEPOINT T, ORRÙ M, et al. Anonymous tokens with private metadata bit[C]//Advances in Cryptology - CRYPTO 2020. Cham: Springer, 2020: 308-336.

作者简介

杜瑞颖　女,1964年5月出生于河南省新乡市. 博士. 现为武汉大学教授、博士生导师. 主要研究方向为网络安全、隐私保护、云安全和移动安全等.
E-mail: duraying@whu.edu.cn

周尔俊　男,1998年3月出生于湖南省岳阳市. 现为武汉大学国家网络安全学院博士研究生. 主要研究方向为安全多方计算、隐私计算.
E-mail: sanfeng@whu.edu.cn

黄正帝　男,2001年7月出生于江西省抚州市. 现为武汉大学在读硕士生. 主要研究方向为隐私保护、应用密码学.
E-mail: rechardhuang@whu.edu.cn

何　琨　男,1986年10月出生于湖北省武汉市. 现为武汉大学副教授、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、人工智能安全和区块链安全等. 中国电子学会会员编号:E190156480M.
E-mail: hekun@whu.edu.cn

石　闽　男,1993年3月出生于安徽省安庆市. 现为武汉大学国家网络安全学院博士后研究员. 主要研究方向为密码协议与形式化方法.
E-mail: itachi@whu.edu.cn

陈　晶　男,1981年3月出生于湖北省武汉市. 现为武汉大学教授、博士生导师. 主要研究方向为网络安全、人工智能安全、分布式系统安全和区块链等.
E-mail: chenjing@whu.edu.cn