QUIC 安全研究综述：协议、实现和生态

张麟康[1,2]，程逸飞[1,2]，朱宇佳[1,2]，刘庆云[1,2]
（1. 中国科学院信息工程研究所，北京 100084；2. 中国科学院大学网络空间安全学院，北京 100049）

摘　要：随着快速 UDP 网络连接（QUIC）在互联网中的加速部署，其在快速握手、加密集成和多路复用方面的设计推动了现代网络通信的高效与安全。然而，受协议持续演进、实现差异以及网络生态复杂性的影响，多类安全风险仍在实际环境中出现。为应对这些问题，对 QUIC 的关键安全机制与演化路径进行了系统梳理，并构建了涵盖协议机理安全、实现安全与生态安全三大维度、共 18 个子类的研究框架，用于刻画当前安全问题的整体结构。同时，通过对协议草案的纵向分析识别了安全风险的时效性特征，并评估了主要威胁的持续性与缓解措施的有效性。研究结果表明，QUIC 安全研究正从早期的握手与密码机制分析扩展至跨层防护、隐私增强与生态治理等方向，未来趋势集中在协议可观测性提升、安全自动化测试以及后量子安全集成等领域。

关键词：QUIC；机理安全；实现安全；生态安全；安全时效性
中图分类号：TN915.08
文献标志码：A
DOI：10.11959/j.issn.1000–436x.2025210

Survey of QUIC security: protocol, implementation, and ecosystem

ZHANG Linkang[1,2], CHENG Yifei[1,2], ZHU Yujia[1,2], LIU Qingyun[1,2]
1. Institute of Information Engineering, Chinese Academy of Sciences, Beijing 100084, China
2. School of Cyber Security, University of Chinese Academy of Sciences, Beijing 100049, China

Abstract: As quick UDP Internet connection (QUIC) is increasingly deployed across the Internet, its designs in rapid handshakes, integrated encryption, and multiplexing enhance the efficiency and security of modern communication. However, continuous protocol evolution, heterogeneous implementations, and complex interactions with network infrastructure expose multiple security risks in practice. To address these issues, the key security mechanisms and evolutionary developments of QUIC were systematically reviewed, and a research framework consisting of three dimensions—protocol-mechanism security, implementation security, and ecosystem security—with 18 subcategories was constructed to outline the overall structure of current security challenges. A longitudinal analysis of protocol drafts further identified the temporal characteristics of security risks, enabling an assessment of threat persistence and mitigation effectiveness. The results indicate that QUIC security research is expanding from foundational analyses of handshakes and cryptographic mechanisms toward cross-layer defenses, privacy enhancement, and ecosystem governance, with future trends focusing on observability improvement, automated security testing, and integration of post-quantum security.

Keywords: QUIC, mechanism security, implementation security, ecosystem security, security timeliness

收稿日期：2025–08–05；**修回日期：**2025–11–03
通信作者：朱宇佳，zhuyujia@iie.ac.cn
基金项目：中国科学院信息工程研究所攀登计划基金资助项目（No.E3Z0191101,No.E3Z0041101）
Foundation Items：The Scaling Program of Institute of Information Engineering, CAS (No.E3Z0191101, No.E3Z0041101)

0　引言

随着互联网技术的迅猛发展，网络通信的效率与安全性已成为全球范围内关注的核心问题。快速UDP网络连接（QUIC, quick UDP Internet connection）[1]作为谷歌提出的新一代传输层协议，因其融合了传输控制协议（TCP, transmission control protocol）的可靠性、传输层安全（TLS , transport layer security）协议的安全性以及HTTP/2的多路复用能力而受到广泛关注。该协议通过快速连接建立、前向纠错（FEC, forward error correction）与头部加密等机制，显著提升了数据传输的效率与安全性[2]。自2021年5月QUIC被互联网工程任务组（IETF, Internet Engineering Task Force）正式标准化以来，其推广与应用进入快速增长阶段[3-6]。

在现代互联网生态系统中，QUIC的应用日益广泛，诸多技术平台与服务提供商的积极支持进一步加速了其普及进程。例如，Chrome与Firefox等主流浏览器通过集成QUIC实现了更高效的连接性能；YouTube等多媒体服务平台采用QUIC以提升内容传输效率；Cloudflare等网络基础设施提供商则借助QUIC优化整体网络性能。上述应用不仅展示了QUIC在提升通信效率和增强安全性方面的技术潜力，也反映出互联网基础设施在持续演进与创新。尤其是在被HTTP/3指定为核心传输协议[7]之后，QUIC逐渐发展为对传统TCP的重要补充，在低时延与快速连接等应用场景中展现出独特优势，并被广泛部署于域名系统、视频传输及对等网络服务（P2P, peer-to-peer）等多个关键领域[8-10]。

随着QUIC在全球范围内的广泛部署，其潜在的安全问题也日益受到关注。这不仅是技术实现层面的挑战，更是保障现代网络环境与用户数据安全的关键要求。尽管QUIC在设计初期充分考虑了安全机制，但其实际应用过程中仍面临诸多复杂风险。例如，为提升连接效率所引入的零往返时延（0-RTT, zero round trip time）连接建立与连接迁移机制，可能引发重放攻击或会话劫持等安全隐患；同时，QUIC实现高度依赖开源社区，不同实现间的成熟度差异也显著增加了漏洞产生的可能性。此外，QUIC在与现有网络架构的兼容性方面仍存在诸多挑战，可能带来新的安全威胁。上述问题凸显出对QUIC安全性开展系统性研究与持续优化的紧迫需求。

近年来，学术界围绕QUIC的安全性展开了大量研究并取得了丰硕成果。这些研究不仅识别并分析了QUIC的关键安全特性，还为识别潜在威胁与制定对策提供了理论基础与技术指导。尽管已有若干综述性文献涉及QUIC，但大多数研究聚焦于协议的性能优化、部署实现，或特定应用场景如卫星网络与触觉互联网等方面。与安全性相关的综述工作则或因发表时间较早，未能涵盖最新研究进展，或较少关注安全，或在内容上缺乏系统性与全面性，具体如表1所示。在当前网络环境快速演进的背景下，已有综述参考价值已显不足。

本文从网络协议全生命周期的视角出发，基于对2014年以来120余篇相关文献的系统梳理，构建了一套系统化的QUIC安全问题分类框架。该框架将QUIC安全性问题划分为三大类：协议机理安全、协议实现安全与协议生态安全，并进一步细化为18个子类别，实现了从协议设计到应用部署阶

表1　已有综述文章总结

基本属性			安全覆盖面				安全扩展项
类型	相关工作	时间	文献数量*/篇	机理安全	实现安全	生态安全	区分时效性
综合	文献[11]	2019年	9	◐	○	○	○
安全	文献[12]	2025年	48	●	◐	◐	○
	文献[13]	2025年	159	●	◐	◐	○
	文献[14]	2022年	15	◐	○	○	○
	文献[15]	2022年	70	●	◐	◐	○
	文献[16]	2023年	12	◐	◐	○	○
	文献[17]	2024年	15	●	○	○	○
	文献[18]	2024年	86	●	●	◐	○
	文献[19]	2025年	55	◐	◐	○	○

注:●表示满足该标准要求,◐表示部分满足,○表示未满足,*仅统计安全相关文献数。

段的全覆盖，有助于后续开展分层次、系统性的研究分析。

此外，本文特别关注安全问题的时效性。鉴于QUIC的快速演进与版本迭代，诸多早期暴露的安全问题已在标准更新或实际部署中得到规避或缓解。因此，本文引入安全问题时效性视角，动态评估各类安全威胁在当前网络环境中的实际影响力，旨在更加准确地判断问题优先级并提升安全策略的适应性与有效性。

在总结已有研究成果的基础上，本文进一步探讨了QUIC安全性研究所面临的关键挑战与未来发展方向，期望为学术界与工业界提供具有指导意义的深度洞见，并激发对QUIC安全性的持续关注与创新。

1 协议的制定与发展

1.1 QUIC发展历程

QUIC作为新一代传输层协议，其设计理念源于对传统TCP/UDP局限性的突破性思考。在互联网应用层加密已成主流的背景下（HTTPS加密流量占比超97%），QUIC创新性地采用UDP作为底层传输，实现了用户态协议栈的加密与功能更新，有效规避了传统协议依赖操作系统内核更新的部署瓶颈。

QUIC的发展经历了2个关键阶段：谷歌在2012年提出原型并在内部测试后，于2015年提交IETF标准化。这一时期恰逢HTTP/2标准完成[20]，为协议演进提供了新思路。IETF在2016年成立专门工作组，通过对谷歌原始设计（gQUIC, Google QUIC）的优化改进，最终形成IETF标准版本（iQUIC, IETF QUIC），并于2021年5月发布t 9000[4]。2023年推出的QUICv2[21]主要作为版本协商框架，未涉及核心技术变更。协议标准化推动了应用层生态的繁荣发展。HTTP/3[7]和基于QUIC的DNS协议（DoQ, DNS over QUIC）[8]的相继标准化，以及安全隧道[22]、流媒体分发[23]等扩展应用的探索，标志着QUIC在互联网核心协议中的深度整合。产业界的大力支持加速了这一进程，谷歌、Cloudflare等科技巨头的推动与mvfst、quiche等开源项目的广泛实践共同促成了完善的协议生态。

最新统计显示，截至2025年11月，基于QUIC的HTTP/3已承载全球36.4%的网站访问流量，充分证明了其在提升网络性能与安全方面的实际价值。这一发展态势预示着QUIC将继续重塑互联网传输架构的未来格局。

1.2 协议安全性迭代与安全问题时效性

在QUIC的设计过程中，安全性始终是一个核心议题。本文首次深入研究了相关的时间连续的34个草案版本，其中涉及的关键安全更新如表2所示，以追踪安全性的迭代更新，重点关注协议设计过程中对于安全性的迭代更新，旨在揭示QUIC在安全性方面的演进和成熟过程。

同时，在下文总结讨论QUIC的安全性问题，

表2 QUIC版本迭代涉及的关键安全更新总结

草案版本	时间	更新内容及影响	安全属性提升			
			机密性	完整性	可用性	其他
32	2021年	定义拒绝服务攻击（DoS, denial of service）保护措施，保护客户端在握手期间的安全			√	
30	2020年	添加错误代码AEAD_LIMIT_REACHED，以避免冲突并增强安全性				√
29	2020年	允许使用连接ID进行地址验证，增强了身份验证过程的安全性		√		
28	2020年	扩大CONNECTION_CLOSE适用范围，并指定处理应用错误的响应				√
26	2020年	改变传输参数的格式，使用可变长度整数，减少传输参数的预测性和篡改风险		√		
25	2020年	添加HANDSHAKE_DONE帧，用于信号握手确认，确保握手过程的完整性和安全性		√		
23	2019年	为连接ID的相关性制定更严格的规则，防止流量分析攻击				√
20	2019年	错误代码现在被编码为可变长度整数，减少错误代码的预测性和篡改风险		√		
18	2019年	流相关错误现在使用STREAM_STATE_ERROR，更精确地处理流状态相关安全问题				√
17	2018年	使用探测超时代替重传超时，这有助于防止某些类型的拒绝服务攻击			√	
13	2018年	允许在收到版本协商或重试响应后进行0-RTT，这有助于提高握手过程的安全性				√
12	2018年	进行TLS握手的集成变更，使用CRYPTO帧，加强加密握手过程的安全性	√			
7	2017年	使用高级加密标准GCM模式代替FNV-1a（fowler noll vo-1a）哈希算法对所有数据包进行加密，提高数据包加密强度和安全性	√			

注：√表示该版本更新对相应安全属性（机密性、完整性、可用性或其他安全能力）产生正向增强。

尤其是安全威胁时，本文特别关注它们的时效性。安全问题时效性指的是安全威胁或防护机制在协议规范的演进、软件实现的更新以及外部环境变化中的持续有效性。为确保本文的讨论能够反映最新的安全态势，本文采用了一种动态的分析方法，将安全问题时效性划分为有效、部分有效和失效 3 个层次。通过追踪 QUIC 草案的版本变迁，审视后续研究工作，并结合必要的实验验证，本文能够评估每个安全问题在当前网络环境中的实际状态。这种方法不仅揭示了当前的安全态势，而且为未来可能出现的安全挑战提供了预警，增强了研究的实用性和指导价值。

2　QUIC 安全概览

2.1　关键安全机制 1:握手安全性

QUIC 通过创新的握手机制在提高连接建立效率的同时确保安全性。如图 1(a)所示，相较于传统 TCP 的 3 次握手，QUIC 将传输握手与加密握手合并，能够在 1-RTT 内完成连接建立，并在重复连接中借助 0-RTT 技术实现数据的即时传输。这一性能提升主要得益于对 TLS 1.3 的集成，该协议支持会话恢复、快速握手，并为每个连接生成独立的密钥，从而增强通信的安全性与隐私保护。

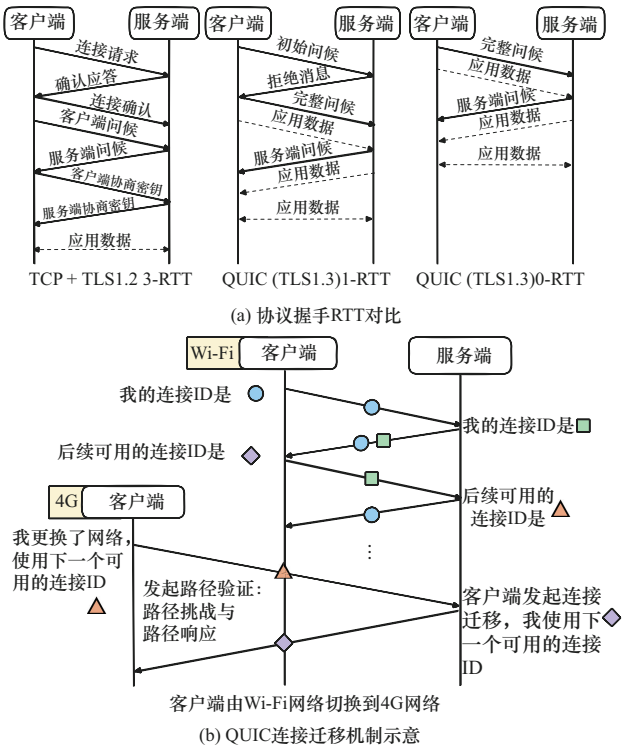


图 1　QUIC 关键机制介绍

在握手过程中，QUIC 实现了认证密钥交换，确保服务器的强认证和客户端的可选认证。同时，QUIC 对传输参数和应用协议使用应用层协议协商（ALPN, application-layer protocol negotiation）机制进行认证协商，有效避免了协议不一致问题。加密数据通过 CRYPTO 帧传输，在不同的数据包编号空间中组织，并借助偏移量保证有序性。

为抵御源地址伪造，QUIC 在握手开始前必须执行地址验证，以确保通信对端真实可达。QUIC 引入的连接 ID 机制保障了数据包的路由一致性，即使在 IP 地址变化时也能维持连接，支持无中断的连接迁移。客户端和服务器通过交换初始包和握手包协商并验证连接 ID，增强了连接的稳定性与抗篡改能力。

2.2　关键安全机制 2:受保护数据包安全性

QUIC 旨在提供一个高效且安全的传输信道，其数据包加密机制是实现该目标的核心。根据 RFC 9000，QUIC 采用端到端加密方式，确保数据传输过程中的机密性与完整性。继承自 TLS 1.3 的密钥交换机制进一步提升了认证强度，有效防御中间人攻击等威胁。

通过认证加密，QUIC 实现了数据包的抗重放和抗篡改能力，仅有合法通信方能够生成与解密有效的数据包。此外，该协议具备良好的网络适应性，在应对网络地址转换（NAT, network address translation）穿透与连接迁移等复杂网络环境时，仍能保障数据包的安全传输。

2.3　关键安全机制 3:连接迁移安全性

作为基于 UDP 的多路复用与加密传输协议，QUIC 在设计上强调低时延连接建立与高效连接迁移。连接迁移允许通信端在不中断传输的前提下，从一种网络平滑切换至另一种网络如 Wi-Fi 到蜂窝，通过最长 64 位的连接 ID 维持连接的标识一致性，如图 1(b)所示。

在安全性方面，QUIC 明确规定连接迁移必须在握手完成之后进行，以防未认证状态下的迁移风险。路径验证机制用于确认新路径的可达性与归属权，端点通过 PATH_CHALLENGE 与 PATH_RESPONSE 帧完成验证。

为防范放大攻击与地址欺骗，QUIC 引入反放大限制机制，规定端点对未验证地址的响应数据量不得超过接收量的 3 倍。在连接迁移过程中，端点

必须验证新地址的有效性，验证失败则恢复使用最后一个有效路径，或在无可用路径的情况下关闭连接，从而确保通信安全与资源控制。

2.4　QUIC 安全研究三分类法

随着互联网服务对高性能与低时延传输的需求不断增长，QUIC 作为新一代传输层协议，已逐步成为取代传统 TCP/UDP 的关键候选。其广泛部署使其承载了大量核心数据流量，成为现代网络通信的基础组件之一。在此背景下，QUIC 的安全性不仅关系到单一连接的保密性与完整性，更直接影响整个互联网服务的稳定性与可信性。因此，系统性研究 QUIC 的安全问题，对于保障网络基础设施的安全具有重要理论与实践意义。

QUIC 的快速发展主要得益于 2 个因素：一是 IETF 的标准化推进与科技企业的技术投入，二是其用户态实现方式所带来的灵活性与高可扩展性。这一架构不仅加速了协议的演进，也降低了开发与部署门槛，促进了广泛的技术创新和社区参与。

然而，QUIC 在快速演进的同时引发了一系列安全挑战。一方面，短周期设计可能导致部分安全机制尚未充分验证；另一方面，多样化的实现方式增加了在规范一致性与安全保障方面的差异，扩大了潜在攻击面。此外，QUIC 与现有网络协议生态的适配也面临新型安全问题，亟需业界与学界的持续关注与深入研究。

在对已有研究工作的系统梳理与归纳基础上，本文构建了 QUIC 安全研究的初步主题划分，如图 2 所示。从研究视角出发，QUIC 的安全问题可划分为协议逻辑层与部署实施层 2 个维度。前者关注协议本身的设计与机制安全，后者则聚焦于协议在现实网络环境中的应用安全。进一步地，部署实施层又可细分为协议实现安全与协议生态安全 2 个子方向。

基于该结构，本文提出了 QUIC 安全研究的三大核心类别：协议机理安全、协议实现安全与协议生态安全。协议机理安全研究致力于分析协议运行机制的安全性，识别潜在威胁并提出改进策略；协议实现安全强调对协议软件实现的安全测试与风险评估，以保障其在部署过程中的鲁棒性；协议生态安全则关注 QUIC 在多样化网络环境中的适配与应用安全，包括其与现有基础设施的交互安全以及在具体应用场景中的安全性保障。图 3 展示了 QUIC 安全研究分类框架，将 QUIC 生命周期中的安全问题系统化划分为协议机理安全、协议实现安全和协议生态安全三大类别及其 18 个子方向全面覆盖协议设计、实现与生态适配等关键领域，为后续研究提供了清晰的结构指引与问题导向，帮助研究者更有针对性地识别并应对 QUIC 在不同场景下所面临的安全挑战。其中，协议机理安全侧重于 QUIC 自身（如请求注解（RFC, request for comment））的设计与规范，指导安全评估与增强；协议实现安全关注客户端与服务器端在实际开发与运行中的安全测试和风险识别；而协议生态安全则着眼于 QUIC 在更广阔网络环境中的安全挑战，例如与现有基础设施如域名系统（DNS, domain name system）和内容

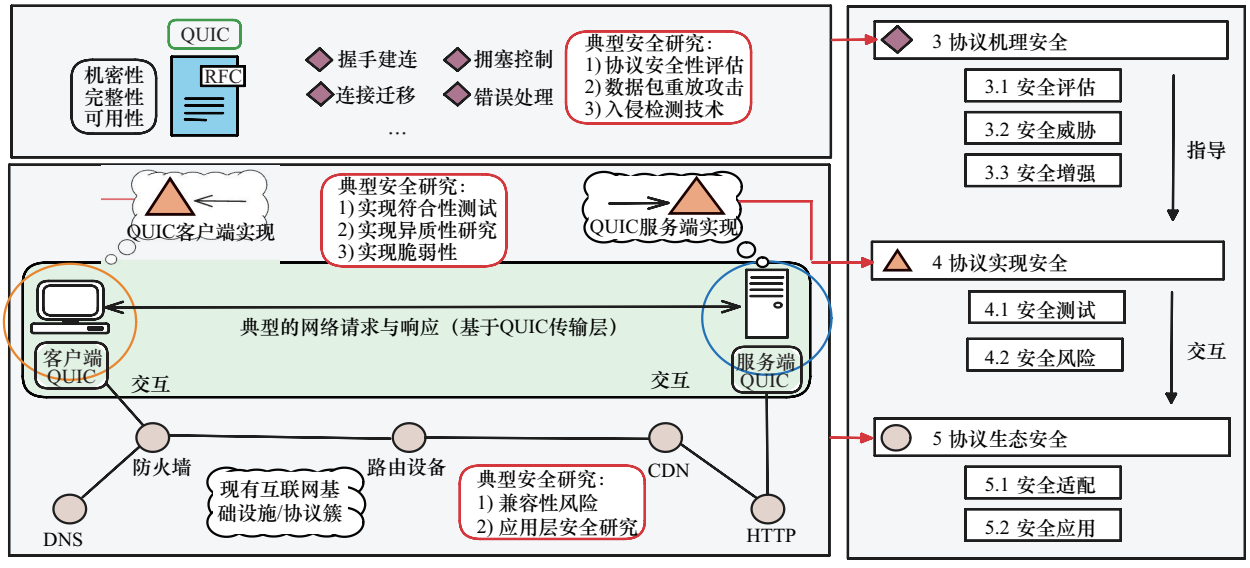


图2　安全研究主题划分示意

分发网络（CDN, content delivery network）的兼容性与安全应用。该框架通过指导和交互两条主线，全面覆盖了从顶层设计到中间实现再到底层环境的全部安全要素，为研究者提供了一个全面的分析蓝图。

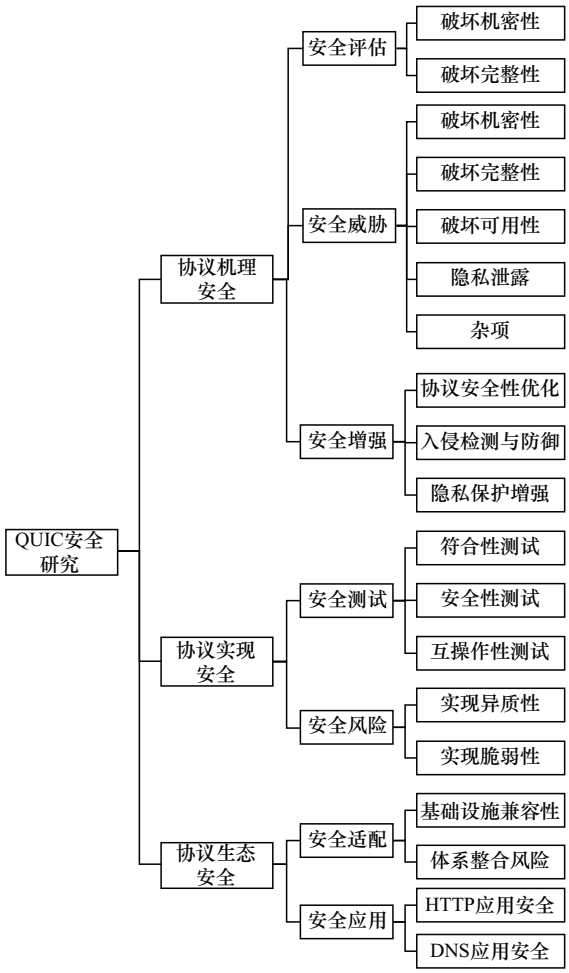


图3　QUIC 安全研究分类框架

3　QUIC 机理安全研究

3.1　安全评估

现有的 QUIC 安全评估工作主要聚焦于密钥交换、握手安全、加密机制及隐私保护等方面，这些研究共同构成了对 QUIC 机理安全性的系统化理解。整体上，安全评估可分为 2 类：握手协议安全分析与记录协议安全分析，分别对应协议在连接建立与数据传输阶段的安全保障机制。

3.1.1　握手协议安全分析

握手阶段的核心任务是密钥交换与身份验证，其安全性直接决定后续通信的可信性与机密性。

Fischlin 等[24]对 gQUIC 的密钥交换机制进行了形式化安全证明，提出了适应多阶段密钥交换的分析框架，为理解 QUIC 在 0-RTT 场景下的安全性提供了理论支撑。

Lychev 等[25]构建了 QUIC 认证与机密通道建立（QACCE, QUIC authenticated and confidential channel establishment）模型，该模型适应 QUIC 的独特握手设计并对其安全属性进行了严格证明。然而，后续研究[26]基于 ProVerif 工具[27]进行验证后发现该模型在实际部署中存在一定局限，促使研究者进一步修正安全假设并改进模型结构。

此外，Gagliardi 等[28]对多个 QUIC 版本的握手过程进行系统测试，揭示了协议规范中的潜在风险并提出优化建议。Zhang 等[29]则采用形式化符号分析方法，对 QUIC 握手协议进行了建模与验证，发现部分设计缺陷，并利用 SPIN 与 ProVerif 工具提出修正方案。这些研究共同推动了 QUIC 握手阶段在密钥安全性、前向安全性及抗重放能力方面的完善。

3.1.2　记录协议安全分析

记录协议主要承担数据加密与隐私防护任务，其安全性关系通信内容的机密性与完整性。

Delignat-Lavaud 等[30]针对 QUIC 记录层提出了新的加密安全模型，对其加密构造及潜在漏洞进行了系统分析，指出 QUIC 在随机数（Nonce, number used once）保密性方面存在一定限制，并提出强化加密鲁棒性的改进思路。

Turner 等[31]从隐私角度评估了 QUIC 在用户跟踪与指纹识别场景下的潜在风险，发现动态连接 ID 机制可在一定程度上缓解跨会话追踪，但传输参数仍可能成为用户指纹识别的载体。

在鲁棒性评估方面，Fischlin 等[32]提出了一种新的加密信道鲁棒性概念，并通过与 DTLS 1.3 的对比分析发现，QUIC 利用滑动窗口机制能够有效抵御数据包重放与乱序问题，从而在不稳定网络环境中保持数据传输的安全与稳定。

综上，记录协议层的安全研究揭示了 QUIC 在机密性、完整性、隐私保护及鲁棒性方面的优势与挑战，为协议的后续安全增强与标准化提供了参考。

3.2　安全威胁

3.2.1　破坏机密性

机密性是指防止未授权方获取或泄露数据的能

力。QUIC通过集成并扩展TLS 1.3的加密机制，在数据包层面提供端到端加密，从而实现机密性保护。与传统TLS结合方式不同，QUIC在密钥交换和数据传输过程中引入了更紧凑的消息结构与独立的帧编号空间，既减少了握手延迟，又提高了密钥更新和重放防护的效率。然而，由于网络环境的复杂性及攻击手段的不断演进，QUIC仍需面对诸如中间人攻击（MITM, man-in-the-middle attack）和密钥泄露等挑战，以确保数据在整个传输周期内的持续安全。

Jäger等[33]针对早期gQUIC版本中TLS-RSA服务器实现对PKCS#1 v1.5弱点的利用进行了深入分析。研究表明，攻击者可借由构造伪造的服务器配置（SCFG, server configuration）消息签名，发起长期中间人攻击，从而相当于掌握服务器的长期私钥，进而在不被检测的情况下解密或篡改传输数据，严重破坏机密性与完整性。然而，随着QUIC在IETF标准化进程中对加密模式及密钥管理方案的全面改进，该攻击已不再适用。

总体而言，QUIC机密性依赖于底层加密算法与密钥管理策略的设计完善。尽管密码学领域对加密算法本身的研究对于提高协议安全至关重要，但其关注点多为通用性问题而非QUIC特有机制，故在本文不作单独赘述。仅当研究直接针对QUIC的加密框架或协议实现中的机密性挑战时，本文才予以重点讨论。

3.2.2 破坏完整性

完整性旨在防止数据在传输过程中被未授权修改、伪造或破坏。QUIC面临的完整性威胁主要包括重放攻击和操纵攻击。

1) 重放攻击

重放攻击是QUIC的重要安全挑战。Lychev等[25]提出2类典型攻击：服务器配置重放和源地址令牌重放。前者通过重放过期的服务器配置参数，诱使客户端使用旧密钥连接，导致连接失败；后者则利用源地址令牌重复发起连接请求，消耗服务器资源，造成拒绝服务。需要强调的是，这些攻击虽针对完整性，但实际效果主要体现为可用性的破坏，因此在表3中额外标注了其属性。Fischlin等[34]进一步指出，尽管QUIC通过击打寄存器机制缓解0-RTT模式下的密钥重放风险，但仍无法彻底防止数据层面的重放，因0-RTT限制服务器对初始密钥生成的参与，增加了参数被重放的可能性。

2) 操纵攻击

操纵攻击同样威胁QUIC安全。Lychev等[25]提出连接ID操纵攻击，攻击者篡改连接ID（CID, connection ID）导致双方计算出不同密钥，从而使连接失败。QUIC中的源地址令牌（STK, source-address token）也可能被篡改，影响握手流程。Chen等[35]指出这种攻击既可能导致拒绝服务（DoS, denial of service），也可能降级连接，具体效果依赖于QUIC草案版本：早期版本中STK参与密钥派生，后期版本仅用于认证。

随着IETF接手标准化进程，QUIC草案v2[36]删除了STK字段和服务器配置（SCFG, server configuration）字段，并将其功能整合进加密保护字段，从而增强了协议的完整性。此外，QUIC安全规范中的安全性考量部分还指出，攻击者可能通过流分段与重组攻击使通信双方资源耗尽，例如恶意发送方不传输完整数据，或接收方故意不确认包，诱发重复传输。

总体来看，尽管早期QUIC存在上述操纵与重放风险，但随着IETF的持续完善，这些攻击方式在当前标准中已难以奏效。

表3 QUIC破坏完整性相关工作

文献	时间	攻击类型	攻击对象	攻击者位置	攻击效果	时效性
文献[25]	2015年	重放攻击	服务器配置参数	旁路	连接建立失败	○
文献[25]	2015年	重放攻击	源地址令牌	旁路	服务端资源消耗	○
文献[25]	2015年	操纵攻击	连接ID	路径中	连接建立失败	◐
文献[25]	2015年	操纵攻击	源地址令牌	路径中	连接建立失败	○
文献[34]	2021年	操纵攻击	源地址令牌	路径中	0-RTT握手降级	○
文献[35]	2021年	操纵攻击	数据流	路径中	服务端资源消耗	◐

注：时效性中○表示已失效，◐表示部分失效。

3.2.3 破坏可用性

可用性是指系统或服务在需要时能够被授权用户正常访问和使用的能力。对于QUIC而言，可用性的破坏主要表现为DoS攻击，这些攻击通过消耗资源或中断服务，使得合法用户无法访问或使用服务。本节将集中讨论针对QUIC的拒绝服务攻击，根据攻击目标的不同，本文将破坏可用性的攻击分为服务端侧和客户端侧两大类。同时，反射放大型攻击虽然不直接针对QUIC的可用性，但却利用QUIC作为攻击载体，可能对其他系统的可用性构成威胁。因此，在集中讨论QUIC的可用性威胁相关研究时，也将其纳入考虑范围。

1) 服务端侧拒绝服务攻击

服务端侧拒绝服务攻击是QUIC的核心安全问题之一。Lychev等[25]提出的源地址令牌重放攻击可耗尽服务器资源，导致合法请求无法响应。Nawrocki等[37]提出的状态溢出攻击模拟大量未验证客户端，强制服务器分配资源，类似TCP SYN泛洪，专门针对QUIC握手流程。尽管QUIC引入了重试机制（RETRY）以限制该类攻击，但实际部署中应用较少。Teyssier等[38]实验验证了状态溢出攻击的有效性，并指出CPU资源最易成为瓶颈，同时提出缓解建议。Cui等[39]设计了操纵客户端初始（MCI, manipulated client initial）攻击，通过篡改初始数据包标签并伪造校验码，使服务器在握手阶段大量消耗资源。Hisasue等[40]则评估了QUIC在低速拒绝服务（LDoS, low-rate denial-of-service）攻击下的脆弱性，指出如Shrew[41]和RoQ[42]等传统攻击手段对QUIC同样有效，并提出新型针对QUIC上BBR的RoQ（RABQ）攻击，在保持高隐蔽性的同时显著降低通信吞吐。

2) 客户端侧拒绝服务攻击

客户端侧拒绝服务攻击也构成严重隐患。Lychev等[25]指出，服务器配置重放攻击可导致客户端延迟和资源浪费；未受保护的连接ID和stk字段亦可被篡改，分别造成密钥不一致和令牌验证失败，进而中断连接。文献[25]还提出了加密流偏移攻击，攻击者通过篡改流偏移破坏握手，甚至发起大规模DoS攻击，Saverimoutou等[43]对此进行了形式化分析，评估其对用户体验质量（QoE, quality of experience）与服务质量（QoS, quality of service）的影响。Cao等[44]补充提出QUIC重置攻击（QUIC RST Attack, QUIC reset attack）与版本协商请求伪造（VNRF, version negotiation request forgery），前者误导客户端认为连接被拒绝，后者通过伪造版本协商迫使客户端断连，暴露连接建立阶段的安全漏洞。

3) 反射放大型拒绝服务攻击

反射放大型拒绝服务攻击利用QUIC作为放大工具。Nawrocki等[37]首次揭示QUIC初始包可能引发反射攻击，攻击者伪造源IP诱导服务器发送大量TLS握手消息。尽管QUIC通过限制未验证响应大小和压缩证书内容降低了风险，后续研究[45]表明约35%的服务器证书仍超出放大阈值，尤其非标准实现更易超标。Gbur等[46]分析了多种基于QUIC的客户端请求伪造攻击，其中服务器初始请求伪造（SIRF, server initial request forgery）和连接迁移请求伪造（CMRF, connection migration request forgery）可引发高达374.44倍和22.1倍的流量放大。Kampanakis等[47]则进一步指出，未来引入后量子签名算法将增加证书长度，可能导致QUIC放大因子提升至5~20倍，带来新的挑战。

本节深入探讨了QUIC在通信可用性方面面临的威胁，这些威胁对用户服务的连续性和可靠性构成了严重影响。如表4时效性标志所示，部分攻击手段如利用源地址令牌重放引发拒绝服务攻击[25]已经因协议更新而失效，但仍有其他攻击，例如QUIC洪水攻击[37-38]和客户端初始操纵攻击[39]，因其对服务器资源的巨大消耗而持续构成实际威胁。此外，针对客户端侧的攻击虽然大部分已失效，但伪造协议版本的攻击手段仍然存在，并且反射放大型拒绝服务攻击利用协议中地址验证的缺陷，显示出其持续的时效性。面对这些挑战，未来的研究需要继续关注QUIC的安全演进，同时开发更为有效的防御机制，以确保网络通信的稳定性和安全性，保障用户利益不受损害。

3.2.4 用户隐私泄露

QUIC旨在通过加密保障用户隐私，但随着加密流量分析技术发展，即便通信内容被加密，用户隐私仍可能泄露。本节探讨QUIC中3类主要的隐私泄露问题：网站指纹（WF, website fingerprinting）攻击、视频流量识别和服务识别。这些问题在QUIC日益普及背景下受到广泛关注并推动相关

表4 QUIC破坏可用性相关工作

相关工作	攻击实施			攻击属性			攻击影响	
	攻击目标	攻击方法	攻击者位置	攻击特性	具体脆弱性	时效性	客户端	服务端
文献[25]	服务端	源地址令牌重放	旁路	重放	状态管理缺陷	○	—	资源耗尽
文献[37-38]		洪水攻击	任意	洪水	握手脆弱性	◐	—	资源耗尽
文献[39]		客户端初始操纵	旁路/任意	操纵/伪造	握手脆弱性	●	—	资源耗尽
文献[40]		慢速攻击控制算法	任意	慢速	状态管理缺陷	●	—	资源耗尽
文献[25]	客户端/连接建立	服务器配置重放	旁路	重放	状态管理缺陷	○	握手失败	握手失败
文献[25]		连接ID篡改	路径中	操纵	未受保护协议字段	◐	握手失败	握手失败
文献[25]		源地址令牌篡改	路径中	操纵	未受保护协议字段	○	握手失败	握手失败
文献[25]		加密流偏移	路径中	注入	消息流处理缺陷	◐	握手失败	握手失败
文献[44]		伪造公共重置包	旁路	伪造	未受保护协议字段	○	主动断连	—
文献[44]		伪造协议版本	旁路	伪造	未受保护协议字段	●	主动断连	—
文献[37,44-46]	其他–反射放大载体	伪造首包地址	任意	反射放大	地址验证缺陷	◐	—	资源消耗
文献[46]		伪造连接迁移	任意	反射放大	地址验证缺陷	●	—	资源消耗

注：标记下划线的文献表示同时破坏了完整性和可用性；时效性中○表示已失效，◐表示部分失效，●表示始终有效。

研究的深入开展。表5总结了近年来对QUIC的相关研究[48-78]，显示其在防御WF攻击方面的薄弱环节。由于QUIC与HTTP/3紧密关联，本文不作严格区分，统一讨论其在WF攻击中的作用和影响。尽管这些技术提升了网络管理与评估能力，但也伴随潜在安全挑战，需在实际应用中权衡风险。

1) 网站指纹攻击

网站指纹攻击是一种被动流量分析手段，攻击者通过分析加密流中的元数据（如数据包大小、传输间隔和顺序）推断用户访问的具体网站或服务。尽管加密隐藏了通信内容，WF攻击仍能通过流量模式识别破坏加密协议的隐私保护机制[48]，对用户隐私构成严重威胁。随着QUIC作为HTTP/3的底层协议广泛应用，WF攻击研究逐渐聚焦于QUIC。

在QUIC早期发展阶段，Zhan等[49]比较了gQUIC、iQUIC和传统HTTPS在WF攻击下的表现，揭示了早期流量的隐私风险。Smith等[50]分析了QUIC与TCP共存环境下WF攻击的适应性，提出2种攻击方法用于识别混合流量，并指出QUIC在抗攻击性上不优于TCP。

在真实网络环境中，Siby等[51]从多维度评估了QUIC面临的WF攻击风险，尤其在缺乏洋葱路由（Tor, the onion router）和虚拟专用网络（VPN, virtual private network）等隐私增强技术的场景下。基于QUIC的Tor传输（Tor over QUIC）被认为是提高匿名性和用户体验的关键解决方案[52]，相关研究[53-54]进一步分析了其对WF攻击的防护能力。

在技术优化层面，Ha等[55]借助自动化机器学习工具提升WF攻击的效率和准确性，降低了攻击实施门槛。Zhan等[56]利用迁移学习在数据有限的情况下显著增强了WF攻击性能，为后续研究提供新方向。大多数研究[48,53-54,56]均在开放世界环境中评估了WF攻击效果[57]，有助于理解其在实际场景中的潜在威胁，并合理评估隐私风险。

2) 视频流量识别

随着视频内容在网络流量中占比持续增长，视频服务商（如YouTube、爱奇艺）逐步采用QUIC作为基于HTTP的动态自适应流媒体传输（DASH, dynamic adaptive streaming over HTTP）协议，以提升传输效率和用户隐私。然而，QUIC的特性使传统基于TCP的视频识别方法难以直接应用。对此，研究者提出了多种基于QUIC的视频流量识别方法。Tang等[58]设计了Shrink方法，通过全局–局部桶机制（GLB）算法实现基于QUIC视频指纹的实时识别。Feng等[59]利用应用数据单元（ADU）组合特征及双向长短期记忆网络–注意力机制（BiLSTM-Attention, bidirectional long short-term memory with attention）网络识别加密视频内容。Wu等[60]结合控制信息特征与明文指纹库，提出面向HTTP/3

表5　　QUIC用户隐私泄露相关工作

基本属性				数据集			流量表示							分类方法		实验评估		
分类	文献	时间	特点	规模	加密	来源	粒度	形式	长度	方向	时间	其他	类别	分类器	封闭	开放	效率
网站指纹攻击	文献[49]	2021年	早期流量指纹	92个网站	HTTPS	自建	会话	⊕	√	√	√	√	ML	RF等	√		
	文献[50]	2021年	混合TCP	100个网站	VPN	自建	会话	⊕	√	√	√	√	DL	CNN等	√	√	
	文献[53]	2023年	无代理场景	150个网站	HTTPS	自建	会话	统计	√	√	√	√	ML	RF	√		
	文献[54]	2022年	Tor over QUIC	248个网站	Tor	自建	会话	序列	√	√			DL	CNN	√	√	√
	文献[55]	2023年	Tor over QUIC	100个网站	Tor	自建	会话	序列		√			⊕	CNN等	√	√	
	文献[51]	2023年	自动机器学习	88个网站	HTTPS	自建	会话	⊕	√	√	√	√	ML	Autogluon-Tabular	√	√	
	文献[56]	2023年	迁移学习	100个网站	VPN	自建	会话	序列		√			DL	MLP	√	√	
视频流量识别	文献[58]	2023年	轻量级	1 000个视频	HTTPS	自建	块	序列				√	AL	AL	√		√
	文献[59]	2022年	多场景设计	10个视频	HTTPS	⊕	块	⊕	√		√	√	⊕	LCSS/Attention	√		
	文献[60]	2024年	精确指纹	10万+视频	HTTPS	自建	块	序列	√			√	ST	HMM	√		√
	文献[61]	2024年	视频分辨率	500个视频	HTTPS	自建	块	序列	√			√	AL	AL	√		√
	文献[62]	2020年	自适应比特率	—	HTTPS	自建	块	序列	√		√	√	AL	Dijkstra算法	√		√
	文献[63]	2018年	QoE识别	1万+视频	HTTPS	自建	流	统计	√	√	√	√	ML	AdaBoost	√		
	文献[64]	2021年	QoE识别	—	HTTPS	自建	流	统计	√	√	√	√	DL	DSOM/MLP	√		
服务识别	文献[73]	2022年	多任务学习	5类服务	HTTPS	公开	流	序列	√	√	√		DL	CNN	√		
	文献[70]	2022年	多模态	6类服务	HTTPS	⊕	流	⊕	√		√	√	DL	CNN	√		
	文献[74]	2023年	集成学习	5类服务	HTTPS	公开	流	序列	√	√	√		ML	XGBT等	√		√
	文献[68]	2019年	半监督学习	5类服务	HTTPS	公开	流	⊕	√	√	√	√	DL	CNN	√		
	文献[67]	2018年	典型	5类服务	HTTPS	公开	流	统计	√	√			DL	CNN	√		
	文献[77]	2022年	典型	6类服务	HTTPS	公开	流	⊕	√	√	√		⊕	CNN/Bayes	√		√
	文献[75]	2024年	集成学习	5类服务	HTTPS	公开	流	序列	√	√	√		ML	RF等	√		
	文献[71]	2024年	频域变换	5类服务	HTTPS	公开	流	统计				√	ML	RF	√		
	文献[76]	2024年	典型	17类服务	HTTPS	公开	流	⊕	√	√	√	√	⊕	CNN/LightGBM	√		
	文献[78]	2023年	典型	5类服务	HTTPS	公开	流	序列	√	√	√		DL	CNN	√		
	文献[72]	2022年	联邦学习	5类服务	HTTPS	公开	流	统计	√		√		DL	MLP	√		√

注:⊕表示混合了多种形式或类别;分类方法类别有机器学习(ML)、深度学习(DL)、启发式算法(AL)、统计方法(ST);所列分类器包括随机森林(RF)、卷积神经网络(CNN)、Autogluon表格模型(Autogluon-Tabular)、多层感知机(MLP)、注意力机制(Attention)、隐马尔可夫模型(HMM)、自适应提升(AdaBoost)、深度自组织映射与多层感知机(DSOM/MLP)、极端梯度提升树(XGBT)、贝叶斯分类器(Bayes)、轻量梯度提升机(LightGBM)等。

的视频流识别方法。尽管这些技术可提升识别准确性和效率，但也可能被攻击者用于推测用户视频偏好，带来隐私风险。

在识别细粒度特征方面，Zhao等[61]提出方法识别视频分辨率，通过序列校正和特征匹配处理平台片段随机组合的情况。Xu等[62]开发CSI系统，基于流量特征推断自适应比特率（ABR, adaptive bitrate）行为，为第三方优化服务质量提供支持。Mazhar等[63]基于机器学习监测HTTPS与QUIC下的QoE，评估启动延迟和重缓冲等指标。TisAselmA等[64]结合DSOM与MLPB方法实现QoE指标的实时精准推断。

3) 服务识别

服务识别是加密流量分析中的核心问题，旨在构建能够识别加密通信中具体服务类型（如聊天、传输、音视频等）的分类模型[65]。QUIC的引入使现有识别模型面临适应性挑战，必须调整以维持识别准确率[66]。

Tong等[67]构建了一个涵盖5类Google服务的QUIC数据集，并提出结合网络流量监控标准

（NetFlow）和包级特征的CNN模型，显著提升分类性能。Rezaei等[68]收集了融合真实用户行为的QUIC数据集，并提出半监督学习方法，在标签不足时仍取得接近监督模型的表现。捷克教育和科学网络（CESNET, czech education and scientific network）协会发布的CESNET-QUIC22数据集[69]，覆盖一个月内的骨干网络流量，细分为102个服务类别，是当前研究的重要基础。

基于上述数据集，大量数据驱动的研究不断涌现。在流量表示方面，研究者采用多模态特征融合[70]、NetFlow增强表示[67]、频域特征提取[71]及互信息特征选择方法[72]。在分类建模方面，提出了多任务学习[73]、集成学习、半监督学习[68,72]、两阶段分类[67]、多模型并行预测[76]及联邦学习方法[72]，以应对数据稀缺、隐私保护和任务差异性等挑战。

尽管现有研究取得初步成果，但仍面临两大局限：其一，多数研究基于早期草案版本的QUIC数据，存在概念漂移问题；其二，缺乏对未知类别流量的识别能力，限制了模型的泛化性与实用性。

综上所述，本节深入探讨了QUIC中用户隐私泄露问题，揭示了即便在强化的加密措施下，攻击者仍可通过流量分析技术对用户行为进行推断。这类安全威胁的攻击面主要涉及服务侧内容的独特性，难以通过单一手段来规避，因此目前仍然具有时效性。随着QUIC的广泛应用，这些攻击手段的现实意义愈发显著，进一步强调了对现有隐私保护策略进行持续评估和改进的必要性。

3.2.5 安全威胁杂项

在深入分析了QUIC的机密性、完整性和可用性方面所面临的安全威胁，以及用户隐私泄露问题之后，接下来本文将探讨一系列重要但不易归类的安全威胁研究。这些研究涵盖了QUIC的多个层面，它们对于理解协议的整体安全性同样至关重要。

1) 隐蔽信道攻击

Sudhan等[79]提出通过QUIC的自旋位构建隐蔽信道。自旋位原本用于延迟监控，但研究表明，它可被用来传输秘密信息。在禁用状态下，自旋位提供单比特的存储空间，可在1-RTT短头部数据包中传输隐蔽信息。实验显示，在1 Gbit/s链路上，隐蔽信道可实现89~255 kbit/s的带宽，足以传输大量隐蔽数据，构成实质性安全威胁。该研究指出，隐蔽信道可能被滥用，如用于传输秘密消息或跟踪数据，可能绕过防火墙检测。

2) 协议伪装攻击

Gbur等[46]提出QUIC的请求伪造攻击，尤其是基于版本协商的请求伪造攻击（VNRF）。此攻击允许QUIC报文被伪装为另一种协议的合理报文，因QUIC版本协商包中的连接ID等字段可由客户端自由设置，攻击者得以利用这一可控空间构造伪装的DNS查询请求。这种协议伪装攻击可能使攻击者绕过安全限制，威胁内部网络或服务[80]。

3) 浏览器指纹识别

Turner等[31]探讨了QUIC的传输参数在浏览器指纹识别中的潜在用途，比较了Chrome、Firefox、Safari、Brave和Opera等主流浏览器在QUIC连接时的传输参数，发现Chrome和Opera使用相同的参数，而Firefox则表现出独特值。这一发现显示，QUIC初始数据包中的传输参数可以部分区分不同浏览器，助力浏览器指纹识别。尽管Safari未纳入分析，但Chrome和Firefox的可区分性为指纹识别提供了证据。为应对这一挑战，JA3推出升级版JA4+，全面支持QUIC，对适应HTTP/3协议起到重要作用。JA4+通过分析不同浏览器的默认传输参数生成高度区分的指纹，展现出较高性能，能有效识别主流和小众浏览器。流量分析软件Wireshark在4.2.0及更高版本中已集成对JA4+的支持，进一步推动其在网络安全中的应用。

4) 用户追踪

Sy等[81]研究了QUIC的隐私问题，特别是用户追踪。源地址令牌和服务器配置可被用来唯一识别客户端。源地址令牌包含公网IP地址和时间戳，服务器配置则有16字节标识符。这些信息使得服务器能够跨连接跟踪用户，且相比传统浏览器指纹或HTTP Cookie（HTTP会话凭证），具有更高的效率和更低的时延，尤其适用于实时出价等场景。Turner等[31]进一步指出，QUIC中的地址验证令牌（AVT, address validation token）也可能被利用进行用户跟踪。尽管AVT的目的是加速连接建立，它可在后续连接中被重用，第三方可通过监测这些AVT实现跨站跟踪。随着通用数据保护条例[82]等法律对个人隐私保护的加强，QUIC的某些特性可能为绕过隐私保护提供新手段，这使得对QUIC隐私保护机制的深入研究和相关政策的制定显得尤为重要。

5) 服务侧信息泄露

QUIC 的某些机制被识别为可能导致服务侧信息泄露。Thimmaraju 等[83]发现 QUIC 的 CID 机制存在规范不足，攻击者可利用此漏洞确定负载均衡器背后的服务器实例数量。他们发现约 25% 的 QUIC 实现易受枚举攻击，攻击者可利用这些行为统计服务器实例，为分布式拒绝服务（DDoS, distributed denial of service）攻击做好准备。此外，Mücke 等[84]通过网络望远镜流量分析了 QUIC 部署的高级知识，发现 QUIC 源连接 ID（SCID, source connection ID）、数据包合并和长度等特征，识别了超大型互联网企业的不同离网部署。他们指出 Facebook 和谷歌在重传超时和最大重传次数上的配置差异，SCID 也可进一步了解负载均衡器部署情况。

以上研究揭示了 QUIC 面临的安全威胁复杂性，强调了对现有防护措施持续审视和改进的必要性。

3.3　安全增强

3.3.1　协议安全性优化

尽管 QUIC 本身具有较高的安全性，但随着网络环境和威胁的不断演进，研究者持续探索增强其安全性的技术。

Hall-Andersen 等[85]基于噪声协议框架提出了针对信任原始公钥系统设计的 QUIC-TLS 变体 nQUIC（noise-based QUIC），支持强制服务器认证和可选客户端认证，能够抵御密钥泄露伪装攻击，并在长期连接中实现优于 QUIC-TLS 的前向及未来保密性，其握手时延与 QUIC-TLS 相当。Delignat-Lavaud 等[30]提出新的安全模型和经过验证的实现方法，提升了 IETF QUIC 记录层的安全性和隐私保护，构建了一个高性能且符合规范、内存安全的记录层，为 QUIC 的标准化和广泛应用奠定了基础。Kempf 等[86]系统评估了 QUIC 在不同密码学算法下的性能，探讨了后量子密码学算法的集成，验证了这些算法在握手阶段的可行性及其性能影响，为 QUIC 的安全优化和未来量子安全网络协议的发展提供了重要参考。

3.3.2　入侵检测与防御

本节将对协议的入侵检测与防御技术进行深入总结，旨在从协议层面出发，探讨如何通过数据驱动的方法和创新策略，强化网络安全防护。

1) 入侵检测技术

QUIC 凭借其高效性和安全性已成为 Web 等高价值服务的核心传输协议，但也因此成为拒绝服务攻击的主要目标。

针对 QUIC 洪水攻击的检测方法，Teyssier 等[87]设计了基于布隆过滤器的 QUICShield 机制，通过概率数据结构快速识别异常握手流量，并采用变化检测技术应对攻击模式演化。Kadi 等[88]则采用机器学习方法分析 HTTP/3 流量特征，实现了洪水攻击的有效检测。此外，Kadi 等[89]通过构建新型数据集与特征选择策略，使用监督学习方法检测 DDoS 攻击中的异常流，重点针对 QUIC 流量的流级统计特征，构建 2 个标签数据集，并在多个主流模型上进行实验对比，验证模型在处理加密传输协议时的入侵检测能力，为 QUIC 安全分析提供了参考。

对于反射放大攻击，Chen 等[90]提出了主被动结合的检测方案，通过双重阈值判定和多元特征匹配提升 UDP 反射攻击的检测效率。Dey 等[91]提出 iQUIC 框架，融合行动者–评论家强化学习机制与生成式网络流量构建，用于识别并缓解基于 QUIC 连接 ID 的 DoS 攻击。通过模拟真实攻击流量场景，框架能在不立即断开连接的情况下做出更柔性的响应决策，实现服务连续性与安全性的平衡。

在攻击特征分析方面，Chatzoglou 等[92]系统研究了 QUIC 与 HTTP 协议的攻击流量特征，并构建了包含多种攻击类型的 H23Q 数据集。基于该数据集，研究者评估了从传统机器学习到深度学习的检测方法，验证了数据驱动方法的有效性，同时揭示了特定攻击类型识别的技术挑战。

针对更广泛的流量异常检测，研究者提出了基于流量特性的创新方法。Teyssier 等[38]利用 QUIC 流量的自相似性，结合经验模态分解技术构建了异常检测模型，通过信号处理方法有效识别流量异常。Špaček 等[93]则专注于 HTTP/3 流量，改进事件流相关性方法并在真实数据集上验证了其在攻击检测中的有效性。这些研究为 QUIC 的安全防护提供了多维度的技术支撑。

2) 防御技术

针对 QUIC 的拒绝服务攻击防御，研究者从不同技术角度提出了创新解决方案。在硬件加速方面，Cui 等[39]利用英特尔 Snow Ridge 系统级芯片的

网络加速复合体实现了高达67 Gbit/s的内联硬件卸载防御，有效平衡了低时延与高安全性的需求。Lee等[94]则提出了基于网络层的双重防护机制：一方面通过动态速率限制适配接收方拥塞窗口，另一方面采用主动丢弃与显式拥塞通知标记相结合的方式精准区分合法QUIC流与恶意UDP攻击流。

在协议特性利用方面，Sudhan等[79]创新性地开发了基于自旋位的防御机制，通过建立隐蔽通信通道有效抵御中间人攻击和数据包伪装攻击。Govil等[95]提出的基于迁移掩码IP的QUIC缓解机制则充分利用QUIC连接迁移特性，通过动态IP跳变干扰攻击者的流量分析能力。Zhang[96]在此基础上改进了地址分配机制，进一步提升了Govil等[95]提出的基于迁移掩码IP的QUIC缓解机制的安全性和效率。

针对隐私保护问题，Smith等[97]设计了客户端网站指纹防护框架，通过生成掩护流量和混淆连接特征，在不修改服务器端的情况下有效抵御基于机器学习的流量分析攻击。实验基于超过10万次网页加载的真实数据验证了其防护效果。

这些研究展示了从硬件加速、协议特性挖掘到隐私保护等多维度的安全防御思路，不仅提升了QUIC的安全防护能力，也为未来网络通信安全研究提供了重要参考。

3.3.3 隐私保护增强

随着网络通信技术的发展，隐私保护成为用户关注的焦点。QUIC以高效的传输特性和安全性，为增强网络隐私提供了新的解决方案。本节将概述QUIC相关的隐私保护增强研究进展。

1) VPN技术融合

虚拟私人网络技术通过加密隧道保护用户隐私， QUIC的应用显著提升VPN隐私保护的效率和抗审查能力。开源VPN框架v2ray自4.7版本起采用QUIC作为传输层，优化了拥塞控制并缩短了连接建立时间。商业应用如IVPN进一步结合v2ray的混淆模式，利用QUIC增强抗审查能力。IETF提出的多路复用应用基质协议（MASQUE）[22]基于QUIC实现了高效的网络代理服务，支持隧道传输功能，避免了数据重封装和重复加密，从而降低时延并提升传输效率。实验研究表明，MASQUE在隐私保护和性能优化方面表现优异[98-99]，并已被Cloudflare和苹果等公司应用[100]。此外，QUIC在卫星VPN领域展现出独特优势。QUIC性能增强代理（QPEP, QUIC performance enhancing proxy）利用QUIC增强卫星通信的加密能力，有效缓解高时延和低吞吐量问题。测试数据表明，相较于传统VPN方案，QPEP在页面加载速度和吞吐量方面具有显著提升[101-102]。这些研究为QUIC在隐私敏感场景下的应用提供了重要参考。

2) Tor网络革新

Tor网络通过洋葱路由为用户提供匿名通信，但面临性能瓶颈。QUIC为改善Tor的高时延问题提供了新的方向。当前研究提出了2种架构设计：端到端设计通过简化链路结构改善拥塞控制，但面临安全风险；逐跳设计则保持了Tor的多路复用能力，并通过使用QUIC替代TCP解决了队头阻塞问题[103-104]。尽管Tor over QUIC初步测试结果令人鼓舞，但进一步研究和评估仍然必要[52,105-106]。

3) 抵抗网络审查

QUIC在抗网络审查方面展现出独特优势，这主要得益于其内置加密机制和快速连接建立特性。作为基于UDP的传输层协议，QUIC的加密设计使得传统基于TCP流量分析的审查技术难以有效识别和阻断其通信。Gbur等[107]的研究进一步指出，QUIC的无状态重置预言机机制增强了抗审查性，使审查者难以主动终止连接。实证研究也验证了QUIC在严格审查环境中的有效性。在伊朗和哈萨克斯坦等网络审查严格的国家进行的测试表明，相较传统TCP连接，QUIC能显著降低HTTP请求被阻断的概率[108-110]。这些发现证实了QUIC在高审查区域的规避潜力，其持续的技术演进有望进一步强化这一特性。

4) 其他隐私保护应用

QUIC在隐私保护领域的应用已从VPN和Tor网络扩展到更广泛的场景。在安全远程访问方面，Michel等[111]提出的SSH3架构将安全外壳（SSH, secure shell）协议重构于QUIC之上，充分利用QUIC的低时延特性和抗TCP重置攻击能力，显著提升了连接稳定性和隐私保护水平，特别适用于高安全要求的远程访问场景。在物联网安全领域，QUIC为解决设备识别漏洞提供了创新方案。Coninck等[112]开发的URLink架构利用QUIC的加密特性，通过隐藏服务的实际网络位置，有效规避了传统基于IP/端口识别的扫描攻击。这种设计不

仅增强了物联网设备的隐私保护能力，还降低了被恶意探测的风险，为物联网安全提供了新的技术路径。

研究表明，QUIC 凭借其加密特性和协议设计优势，已在多个隐私保护场景展现出显著价值。随着技术持续演进，QUIC 有望在网络隐私保护体系中发挥更加关键的作用。

4　QUIC 协议实现安全研究

4.1　安全测试

4.1.1　符合性测试

符合性测试是确保软件实现是否遵循特定标准或规范的重要手段。在 QUIC 背景下，符合性测试旨在验证其实现是否遵守 IETF 规范以确保协议安全性和互操作性。

McMillan 等[113]率先提出基于形式化规范的测试方法，通过自动生成的随机测试用例检测 QUIC 实现与规范的偏差，不仅识别出多个实现错误，还促进了规范的完善。Crochet 等[114]在此基础上扩展研究，利用 Ivy 工具重点关注草案−18~草案−29，对 7 个 QUIC 实现进行测试，揭示了规范中的歧义以及实现间的差异性。

尽管这些研究为草案阶段的 QUIC 实现提供了有效的测试框架，但随着协议正式标准化，针对最新标准版本的符合性测试仍需进一步完善。持续开发更全面的测试方法对于确保 QUIC 实现严格遵循最新规范至关重要。

4.1.2　安全性测试

安全性测试旨在通过模拟攻击者的行为，发现并预防潜在的安全漏洞。在网络协议测试中，重点在于确保协议实现能妥善应对各种异常或恶意输入以保护系统免遭攻击。

QUIC 的安全性测试研究已形成系统化的方法论，主要包括基于扩展工具的精确测试和模糊测试两大方向。Goel 等[115]通过改进 packetdrill 工具，实现了对 QUIC 数据包格式和 TLS 1.3 集成的深度测试，该方法虽能精准控制测试过程，但在扩展性方面存在局限。模糊测试方面，DPIFuzz[116]和 Bleem[117]框架代表了 2 种创新思路：前者通过深度包检测技术比较不同 QUIC 实现的异常处理差异，后者采用定向模糊测试发现包括堆缓冲区溢出在内的严重漏洞。Chatzoglou 等[15]进一步运用模糊测试工具 Mutiny-fuzzer 和网络模糊框架 Fuzzotron 对主流 QUIC/HTTP3 服务器进行测试，揭示了多个可导致资源耗尽的零日漏洞。Ang 等[118]则针对 QUIC 的加密性与状态性导致模糊测试困难的问题，开发了一种专用灰盒模糊器 QUIC-Fuzz。该工具结合状态感知输入生成与高效反馈收集机制，可自动发现协议实现中的潜在安全漏洞，为 QUIC 安全测试提供了系统化工具支持。

尽管 QUIC 日趋成熟，其实现仍存在安全隐患。随着网络威胁不断演变，持续完善安全性测试方法对保障协议健壮性至关重要。现有工作不仅提升了 QUIC 的安全水平，也为网络协议安全评估提供了重要参考。

4.1.3　互操作性测试

互操作性测试通过模拟不同网络条件下的交互来验证协议的一致性和兼容性。QUIC 的互操作性测试研究在保障协议安全性和功能性方面发挥着关键作用。

Seemann 等[119]开发的 QUIC 互操作性运行器（QIR, QUIC interop runner）框架通过容器化环境和网络仿真器 3 网络模拟工具，实现了自动化、可重复的测试环境。QIR 支持从基础握手到复杂多路复用等多种测试场景，能够有效评估不同 QUIC 实现在各类网络条件下的表现，包括面对异常流量时的鲁棒性。

这种系统化的测试方法不仅提升了协议实现的一致性检测效率，也为识别潜在安全漏洞提供了有效手段。相关研究成果为 QUIC 在实际部署中的安全性优化奠定了重要基础。

4.2　安全风险

本节将深入分析 QUIC 软件实现在生产环境中的安全风险，特别是由 RFC 规范不明确性所引发的异质性和脆弱性问题。这种协议规范的模糊性不仅会导致实现间的不一致，也增加了误解规范造成安全漏洞的风险。

4.2.1　实现异质性

随着 QUIC 的发展，其各种不同实现也处于持续演进中。尽管各实现都基于相同标准，但在网络行为、性能和安全性上仍存在显著差异。实现异质性可能带来安全隐患、性能差异，甚至难以预测的网络交互行为，进而影响用户体验和网络的整体稳定性。

Marx等[120]的研究表明，尽管各实现遵循相同协议标准，但在流控制、拥塞控制等核心功能上仍存在行为差异，这主要源于协议规范的开放性解释空间。为应对这一问题，qlog和qvis等工具提供了可视化分析手段[121]，辅助开发者优化实现。

深入研究显示，差异广泛存在的直接原因是规范模糊性。Völker等[122]在路径最大传输单元发现（PMTUD, path maximum transmission unit discovery）机制研究中观察到显著差异，而Sander等[123]发现部分实现为兼容性考虑刻意省略显式拥塞通知（ECN, explicit congestion notification）等标准功能。这些差异不仅影响互操作性，更可能引入安全隐患。

此外，实现异质性催生了新的识别技术。Zirngibl等[124]开发的QUIC Hunter通过分析响应模式特征，实现了QUIC实现的精准识别。该工具的大规模扫描结果既展现了QUIC生态的多样性，也暴露了基于实现特征的潜在攻击面。

这些发现表明，QUIC实现异质性在体现技术创新的同时，也构成了新的安全挑战，持续监测和规范实现差异对保障协议安全性至关重要。

4.2.2 实现脆弱性

QUIC虽然在理论上提供了诸多优势，但其在现实世界的部署中却暴露出了一些实现上的脆弱性。这些脆弱性通常源于对协议规范的不完整实现或实现方式的缺陷，可能导致性能下降甚至安全风险。

QUIC在实际部署中暴露出若干关键实现缺陷，影响了其理论性能优势的充分发挥。研究表明，PMTUD机制在现有QUIC实现中存在显著不足，Völker等[122]发现多数实现无法准确探测网络路径最大传输单元，为此提出的新型搜索算法通过模拟验证可有效改善这一状况。

协议实现缺陷还体现在数据包过大（PTB, packet too big）消息处理方面，当前QUIC普遍缺乏有效的PTB响应机制。针对此问题，研究者开发了参数化PTB检测算法，其模拟测试结果证实了该方案在不同网络条件下的适用性[125]。此外，尽管QUIC标准强制要求ECN支持，Sander等[123]的大规模测量显示实际部署中ECN验证不足且采用率低，严重制约了该机制在拥塞控制方面的潜力。

这些发现凸显了QUIC实现审查与改进的紧迫性。未来研究应着重解决这些实现层面的脆弱性，以确保协议的安全性和性能优势得到充分发挥。

5 QUIC生态安全研究

5.1 安全适配

5.1.1 基础设施兼容性

QUIC的快速发展对现有网络基础设施提出了新的兼容性要求。QUIC的创新设计在提升通信效率的同时，也给传统网络安全设备带来了适配挑战。

早期研究[126]表明，由于QUIC的高度加密特性，多数网络监控工具（如Wireshark在3.0.3版本前）无法有效解析QUIC流量，导致入侵检测系统面临可见性缺失的问题。这一特性已被恶意软件如Merlin利用，通过QUIC建立隐蔽的指挥与控制通信信道。

针对基础设施兼容性问题，近期研究提出了多种解决方案。Franzil[127]改进了基于签名的入侵检测系统对QUIC流量的识别能力。Gbur等[107]评估了QUIC与传统防火墙的交互，发现加密特性在提升安全性的同时影响了流量监控功能。Hilal等[128]则指出中间盒设备可能干扰QUIC的数据包传输，导致通信异常。

这些研究表明，虽然QUIC的部署带来了新的兼容性挑战，但通过持续的技术改进，可以实现安全性与性能的平衡。未来研究需要进一步优化网络基础设施对QUIC的支持能力。

5.1.2 体系整合风险

QUIC与现有互联网体系的整合带来了一系列独特的安全挑战。

在TLS证书兼容性方面，Nawrocki等[45]发现QUIC的3倍放大限制与现有Web证书尺寸存在冲突，导致部分连接无法实现单RTT握手，这不仅削弱了QUIC的低时延优势，还可能迫使采用安全性较低的小型证书。

在网络性能监控方面，QUIC的加密特性阻碍了传统的RTT测量方法，虽然协议设计spin bit机制作为替代方案，但Trammell等[129-130]的研究显示其实际部署率仅约10%，且存在测量精度问题，显著影响了网络性能监测的有效性。

这些体系整合问题虽不构成系统性风险，但确实影响了网络运营商的监控能力和性能优化。针对

这些问题的持续研究对 QUIC 的长期稳定部署具有重要意义。

5.2　安全应用

5.2.1　HTTP 应用安全

IETF 于 2022 年 6 月正式发布了 HTTP/3[7]，该应用层协议明确规定仅使用 QUIC 作为其传输层协议。QUIC 的引入为 HTTP 带来了显著的安全性提升和更高的传输效率，标志着超文本传输协议的一次重要演进。鉴于 HTTP/3 在互联网业务中的核心地位及其广阔的应用前景，其安全性问题自然成为学术界和工业界广泛关注的重点。

Chatzoglou 等[15]通过构建测试平台，系统评估了 HTTP/2 安全威胁向 HTTP/3 的迁移性，发现部分攻击在新协议环境下仍然有效，这为后续安全研究提供了重要基准。

在性能与安全协同优化方面，Sander 等[131]和 Li 等[132]的研究表明，QUIC 的多路复用机制通过缓解队头阻塞问题，不仅提升了传输效率，还增强了抵御网络拥塞攻击的能力。实验数据显示，HTTP/3 服务器在面对脉冲式拒绝服务攻击时，展现出比 HTTP/2 更高的稳定性。

此外，Zhang 等[133]提出的加密流量分析方法，虽然为网络管理提供了新思路，但也引发了隐私保护方面的讨论。该方法通过分析数据包元数据推断 HTTP/3 流量特征，揭示了加密协议在提供隐私保护时面临的新挑战。

5.2.2　DNS 应用安全

随着 QUIC 的兴起，DNS 体系也迎来一系列变革 DoQ[8]为 DNS 查询提供了以 QUIC 为基础的加密传输通道，有效降低了中间人攻击风险。同时，基于 HTTPS 的 DNS（DoH, DNS over HTTPS）[134]的技术积累，业界正逐步向 DNS over HTTP/3 过渡，利用现有 HTTP/3 协议栈简化实现并提高兼容性。此外，HTTPS 资源记录的引入进一步促进了协议升级的平滑过渡。

然而研究表明，仅依靠传输层加密无法完全解决隐私保护问题。针对传统加密 DNS 协议（如 DoT 和 DoH）的流量分析攻击[135-137]在 DoQ 环境下同样存在。同时，已有研究工作证明，即便采用了 QUIC 传输层的填充机制，DoQ 仍然面临着类似的隐私泄露风险。Hu 等[138]通过实验证实，攻击者仍可通过流量特征识别网站类别，其后续研究[139]进一步探讨了不同场景下的隐私泄露风险及填充机制的防护效果。

这些发现凸显了基于 QUIC 的应用层协议在业务安全方面面临的长期挑战。持续的安全研究对于保障现代网络业务的安全高效运行至关重要。

6　发展趋势与展望

自 2021 年标准化以来，QUIC 在网络通信中的广泛应用使其安全性备受关注。随着 QUIC 的不断演进与广泛部署，其安全性研究正逐步从早期的机制探索向更系统、更深入的方向发展。当前研究已在协议机理、实现方式与生态适配等多个方面取得初步成果，但仍存在诸多挑战和亟待拓展的研究空间。

本文系统梳理了 QUIC 安全研究的主要成果，将其划分为协议安全、实现安全和生态安全三大类。从年发文量统计可见，如图 4 所示，QUIC 安全研究整体呈上升趋势，其中协议安全研究持续领先，而实现安全和生态安全研究虽起步较晚但发展迅速，展现出广阔的研究前景。

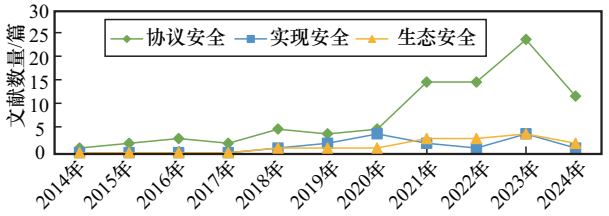


图 4　QUIC 安全研究工作发文量统计

国内外研究对比显示，国内在 QUIC 领域的研究投入与国际先进水平仍存在差距。本文收录的研究中，国内机构主导的仅占 15%。在开源实现方面，国内主要依靠阿里巴巴 XQUIC 和腾讯 TQUIC 等有限项目，且 QUIC/HTTP3 的国内使用率显著低于全球平均水平。鉴于 QUIC 作为新一代传输协议的重要性，亟需加强国内相关研究投入。

未来的 QUIC 安全研究需进一步系统化、精细化发展，重点从协议机理、协议实现和协议生态 3 个层面展开，构建多维度的安全防护体系。

在协议机理方面，QUIC 的加密握手、0-RTT 传输、连接迁移等机制虽有效提升性能，但也带来新的攻击面。已有研究揭示其在会话重放、身份伪造、参数操控等方面的潜在风险。为应对这些挑

战，未来需进一步推动协议安全性的形式建模与验证方法发展，特别是针对0-RTT模式下的数据完整性保护、多路径连接下的验证一致性等问题，仍缺乏系统性解决方案。此外，随着后量子密码算法逐步成熟，QUIC如何集成轻量高效的抗量子密钥协商机制也将成为下一阶段的重要研究方向之一。在保证协议机密性与隐私性的同时，如何平衡性能与安全的权衡关系，是后续机制优化的重要课题。

在协议实现方面，当前多种QUIC实现已广泛应用于浏览器、内容分发网络、边缘计算与物联网系统中，不同代码库之间存在实现差异，成为安全问题频发的主要诱因。尽管现有模糊测试框架在漏洞发现方面取得显著进展，但针对协议状态机、加密上下文与传输路径的深层联动尚缺乏系统支持。未来应加强状态感知的自动化测试工具研究，提升模糊测试的覆盖率与漏洞发现能力；同时结合形式化方法与协议版本迭代历史，构建长期可维护的符合性与安全性验证体系，助力QUIC实现的标准一致性与稳健性增强。此外，针对实现部署中常见的异常处理差异、错误状态触发逻辑等问题，也应纳入未来测试规范与工程实践优化范畴。

在协议生态方面，QUIC在CDN、视频分发、Web代理、加密隧道等复杂场景中的快速部署引发了广泛的安全关注。一方面，其流量特征虽被端到端加密所隐藏，但研究表明仍可通过元数据分析进行网站指纹、浏览器识别及服务分类，隐私保护面临严峻挑战。另一方面，QUIC在连接迁移、CID管理、版本协商等机制中暴露出的中继可识别性与端口行为差异，也使其成为指纹追踪与负载识别攻击的潜在目标。随着MASQUE、Tor over QUIC等新型隐私增强协议的快速发展，QUIC的生态风险管理逐渐从单一链路安全向多跳信任体系、端到端隐私建模扩展，要求研究者从更系统的视角评估其跨域部署带来的安全影响。与此同时，QUIC在反射放大、状态保持等方面的攻击潜力也需进一步遏制，建议围绕部署规范、响应策略与中间件行为构建统一的生态安全防控框架。

综上，QUIC安全研究正逐步进入多维融合与长期演进的阶段。协议层面需增强安全机制的理论支撑与适应性设计，实现层面需推动测试自动化与规范一致性，生态层面则需构建可协同的风险治理体系。未来应加强标准组织、工业界与学术界的深度合作，推动构建以机制安全为核心、实现安全为基础、生态安全为导向的多层次保障体系，为新一代网络传输架构的安全性与可信性提供坚实支撑。

7 结束语

QUIC在提升网络通信效率和安全性方面展现了巨大的潜力，但其在实际应用中仍面临诸多挑战。通过对QUIC安全机制的详细分析及相关研究的梳理，本文为理解和应对这些挑战提供了新的视角和思路。未来，随着技术的不断进步和互联网环境的动态变化，QUIC的安全性研究将继续深化，驱动更安全、更高效的网络通信发展。

参考文献：

[1] LANGLEY A, RIDDOCH A, WILK A, et al. The QUIC transport protocol: design and Internet-scale deployment[C]//Proceedings of the Conference of the ACM Special Interest Group on Data Communication. New York: ACM Press, 2017: 183-196.

[2] RÜTH J, POESE I, DIETZEL C, et al. A first look at QUIC in the wild[C]// Passive and Active Measurement. Berlin: Springer, 2018: 255-268.

[3] THOMSON M. Version-independent properties of QUIC[S]. 2021.

[4] IYENGAR J, THOMSON M. QUIC: a UDP-based multiplexed and secure transport[S]. 2021.

[5] THOMSON M, TURNER S. Using TLS to secure QUIC[S]. 2021.

[6] IYENGAR J, SWETT I. QUIC loss detection and congestion control[S]. 2021.

[7] BISHOP M. HTTP/3[S]. 2022.

[8] HUITEMA C, DICKINSON S, MANKIN A. DNS over dedicated QUIC connections[S]. 2022.

[9] CURLEY L. Media over QUIC-Transfork[R]. 2024.

[10] YIN C Q, CHEN Z H, HU Y H, et al. Fine-grained transmission optimization of large-scale web VR scenes[C]//Proceedings of the 2018 IEEE International Conference on Progress in Informatics and Computing (PIC). Piscataway: IEEE Press, 2018: 209-214.

[11] 李学兵, 陈阳, 周孟莹, 等. 互联网数据传输协议QUIC研究综述[J]. 计算机研究与发展, 2020, 57(9): 1864-1876.
LI X B, CHEN Y, ZHOU M Y, et al. Internet data transfer protocol QUIC: a survey[J]. Journal of Computer Research and Development, 2020, 57(9): 1864-1876.

[12] JOARDER Y A, FUNG C. A survey on the security issues of QUIC[C]// Proceedings of the 2022 6th Cyber Security in Networking Conference (CSNet). Piscataway: IEEE Press, 2022: 1-8.

[13] 苏金树, 宋丛溪, 计晓岚, 等. 多径传输技术研究综述[J]. 软件学报, 2025, 36(1): 289-320.
SU J S, SONG C X, JI X L, et al. Research review on multipath transmission technology [J]. Journal of Software, 2025, 36(1): 289-320.

[14] ORAN S, KOÇAK A, ALKAN M. Security review and performance analysis of QUIC and TCP protocols[C]//Proceedings of the 2022 15th International Conference on Information Security and Cryptography (ISCTURKEY). Piscataway: IEEE Press, 2022: 25-30.

[15] CHATZOGLOU E, KOULIARIDIS V, KAROPOULOS G, et al. Revisiting QUIC attacks: a comprehensive review on QUIC security and a hands-on study[J]. International Journal of Information Security,

2023, 22(2): 347-365.
[16] TATSCHNER S, PETERS S N, EMEIS D, et al. A quick security overview: a literature research on implemented security recommendations[C]// Proceedings of the 18th International Conference on Availability, Reliability and Security. New York: ACM Press, 2023: 1-8.
[17] SENGUPTA J, DEY D, FERLIN S, et al. Accelerating tactile Internet with QUIC: a security and privacy perspective[J]. arXiv Preprint, arXiv: 2401.06657, 2024.
[18] JOARDER Y A, FUNG C. Exploring QUIC security and privacy: a comprehensive survey on QUIC security and privacy vulnerabilities, threats, attacks, and future research directions[J]. IEEE Transactions on Network and Service Management, 2024, 21(6): 6953-6973.
[19] HUANG J N, LIU W W, LIU G J, et al. QuicCourier: leveraging the dynamics of QUIC- based website browsing behaviors through proxy for covert communication[J]. IEEE Transactions on Dependable and Secure Computing, 2025, 22(5): 4516-4533.
[20] BELSHE M, PEON R, THOMSON M. Hypertext transfer protocol version 2 (HTTP/2)[S]. 2015.
[21] DUKE M. QUIC version 2[S]. 2023.
[22] PAULY T, ROSENBERG E, SCHINAZI D. QUIC-aware proxying using HTTP[R]. 2023.
[23] OTT J, ENGELBART M, DAWKINS S. RTP over QUIC (RoQ) [R]. 2023.
[24] FISCHLIN M, GÜNTHER F. Multi-stage key exchange and the case of google's QUIC protocol[C]//Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security. New York: ACM Press, 2014: 1193-1204.
[25] LYCHEV R, JERO S, BOLDYREVA A, et al. How secure and quick is QUIC? provable security and performance analyses[C]//Proceedings of the 2015 IEEE Symposium on Security and Privacy. Piscataway: IEEE Press, 2015: 214-231.
[26] SAKURADA H, YONEYAMA K, HANATANI Y, et al. Analyzing and fixing the QACCE security of QUIC[C]//Security Standardisation Research. Berlin: Springer, 2016: 1-31.
[27] BLANCHET B, CHEVAL V. ProVerif: cryptographic protocol verifier in the formal model[R]. 2016.
[28] GAGLIARDI E, LEVILLAIN O. Analysis of QUIC session establishment and its implementations[C]//Information Security Theory and Practice. Berlin: Springer, 2020: 169-184.
[29] ZHANG J J, YANG L, GAO X M, et al. Formal analysis of QUIC handshake protocol using symbolic model checking[J]. IEEE Access, 2021, 9: 14836-14848.
[30] DELIGNAT-LAVAUD A, FOURNET C, PARNO B, et al. A security model and fully verified implementation for the IETF QUIC record layer[C]//Proceedings of the 2021 IEEE Symposium on Security and Privacy (SP). Piscataway: IEEE Press, 2021: 1162-1178.
[31] TURNER A, ATHAPATHU R, KHARBANDA C. Evaluating QUIC for privacy improvements over its predecessors[R]. 2022.
[32] FISCHLIN M, GÜNTHER F, JANSON C. Robust channels: handling unreliable networks in the record layers of QUIC and DTLS 1.3[J]. Journal of Cryptology, 2024, 37(2): 9.
[33] JÄGER T, SCHWENK J, SOMOROVSKY J. On the security of TLS 1.3 and QUIC against weaknesses in PKCS#1 v1.5 encryption[C]//Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security. New York: ACM Press, 2015: 1185-1196.
[34] FISCHLIN M, GÜNTHER F. Replay attacks on zero round-trip time: the case of the TLS 1.3 handshake candidates[C]//Proceedings of the 2017 IEEE European Symposium on Security and Privacy (EuroS&P). Piscataway: IEEE Press, 2017: 60-75.
[35] CHEN S, JERO S, JAGIELSKI M, et al. Secure communication channel establishment: TLS 1.3 (over TCP fast open) versus QUIC[J]. Journal of Cryptology, 2021, 34(3): 26.
[36] IYENGAR J, THOMSON M. Draft-IETF-quic-transport-02[R]. 2017.
[37] NAWROCKI M, HIESGEN R, SCHMIDT T C, et al. QUICsand: quantifying QUIC reconnaissance scans and DoS flooding events[C]// Proceedings of the 21st ACM Internet Measurement Conference. New York: ACM Press, 2021: 283-291.
[38] TEYSSIER B, JOARDER Y A, FUNG C. An empirical approach to evaluate the resilience of QUIC protocol against handshake flood attacks[C]//Proceedings of the 2023 19th International Conference on Network and Service Management (CNSM). Piscataway: IEEE Press, 2023: 1-9.
[39] CUI B, LI Z X, YU F. Manipulated client initial attack and defense of QUIC[C]//Proceedings of the 2022 IEEE 24th Int Conf on High Performance Computing & Communications; 8th Int Conf on Data Science & Systems; 20th Int Conf on Smart City; 8th Int Conf on Dependability in Sensor, Cloud & Big Data Systems & Application (HPCC/DSS/SmartCity/DependSys). Piscataway: IEEE Press, 2022: 611-618.
[40] HISASUE R, KAWAUCHIYA A, INAMURA H, et al. Experimental evaluation of LDoS attacks on QUIC[C]//Proceedings of the 2023 Fourteenth International Conference on Mobile Computing and Ubiquitous Network (ICMU). Piscataway: IEEE Press, 2023: 1-4.
[41] KUZMANOVIC A, KNIGHTLY E W. Low-rate TCP-targeted denial of service attacks: the shrew vs. the mice and elephants[C]//Proceedings of the 2003 Conference on Applications, Technologies, Architectures, and Protocols for Computer Communications. New York: ACM Press, 2003: 75-86.
[42] GUIRGUIS M, BESTAVROS A, MATTA I, et al. Reduction of quality (RoQ) attacks on Internet end-systems[C]//Proceedings of the Proceedings IEEE 24th Annual Joint Conference of the IEEE Computer and Communications Societies. Piscataway: IEEE Press, 2005: 1362-1372.
[43] SAVERIMOUTOU A, MATHIEU B, VATON S. Which secure transport protocol for a reliable HTTP/2-based web service: TLS or QUIC? [C]// Proceedings of the 2017 IEEE Symposium on Computers and Communications (ISCC). Piscataway: IEEE Press, 2017: 879-884.
[44] CAO X D, ZHAO S R, ZHANG Y Q. 0-RTT attack and defense of QUIC protocol[C]//Proceedings of the 2019 IEEE Globecom Workshops (GC Wkshps). Piscataway: IEEE Press, 2019: 1-6.
[45] NAWROCKI M, TEHRANI P F, HIESGEN R, et al. On the interplay between TLS certificates and QUIC performance[C]//Proceedings of the 18th International Conference on Emerging Networking EXperiments and Technologies. New York: ACM Press, 2022: 204-213.
[46] GBUR Y, TSCHORSCH F. QUICforge: client-side request forgery in QUIC[C]//Proceedings of the 2023 Network and Distributed System Security Symposium. Berlin: Springer, 2023: 23072.
[47] KAMPANAKIS P, LEPOINT T. Vision paper: do we need to change some things? open questions posed by the upcoming post-quantum migration to existing standards and deployments[C]//Security Standardisation Research. Berlin: Springer, 2023: 78-102.
[48] SHEN M, YE K, LIU X T, et al. Machine learning-powered encrypted network traffic analysis: a comprehensive survey[J]. IEEE Communications Surveys & Tutorials, 2023, 25(1): 791-824.
[49] ZHAN P, WANG L, TANG Y. Website fingerprinting on early QUIC traffic[J]. Computer Networks, 2021, 200: 108538.
[50] SMITH J P, MITTAL P, PERRIG A. Website fingerprinting in the age of QUIC[J]. Proceedings on Privacy Enhancing Technologies, 2021, 2021(2): 48-69.
[51] SIBY S, BARMAN L, WOOD C, et al. Evaluating practical QUIC

website fingerprinting defenses for the masses[J]. Proceedings on Privacy Enhancing Technologies, 2023, 2023(4): 79-95.

[52] BASYONI L, ERBAD A, ALSABAH M, et al. QuicTor: enhancing tor for real-time communication using QUIC transport protocol[J]. IEEE Access, 2021, 9: 28769-28784.

[53] NIE M J, ZOU F T, QIN Y, et al. QUIC-CNN: website fingerprinting for QUIC traffic in tor network[C]//Proceedings of the 2022 IEEE 24th Int Conf on High Performance Computing & Communications; 8th Int Conf on Data Science & Systems; 20th Int Conf on Smart City; 8th Int Conf on Dependability in Sensor, Cloud & Big Data Systems & Application (HPCC/DSS/SmartCity/DependSys). Piscataway: IEEE Press, 2022: 663-671.

[54] TRAP C. Impact of replacing TCP by QUIC in Tor on website fingerprinting resistance[R]. 2023.

[55] HA J, ROH H. QUIC website fingerprinting based on automated machine learning[J]. ICT Express, 2024, 10(3): 594-599.

[56] ZHAN M Q, LI Y, ZHU Y C, et al. Website-aware protocol confusion network for emergent HTTP/3 website fingerprinting[J]. IEEE Transactions on Information Forensics and Security, 2023, 18: 2427-2439.

[57] JUAREZ M, AFROZ S, ACAR G, et al. A critical evaluation of website fingerprinting attacks[C]//Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security. New York: ACM Press, 2014: 263-274.

[58] TANG W T, DU M J, LI Z, et al. Shrink: identification of encrypted video traffic based on QUIC[C]//Proceedings of the 2023 IEEE International Performance, Computing, and Communications Conference (IPCCC). Piscataway: IEEE Press, 2023: 140-149. [LinkOut]

[59] 冯子玄 . QUIC 协议下的加密视频内容识别研究[D]. 南京: 东南大学, 2021.
FENG Z X. Research on encrypted video content identification under QUIC protocol[D]. Nanjing: Southeast University, 2021.

[60] 吴桦, 倪珊珊, 罗浩, 等 . 基于 HTTP/3 传输特性的加密视频识别方法[J]. 计算机学报, 2024, 47(1): 190-205.
WU H, NI S S, LUO H, et al. An encrypted video recognition method based on the transmission characteristics of HTTP/3 [J]. Chinese Journal of Computers, 2024, 47(1): 190-205.

[61] ZHAO Y J, WU H, CHEN L, et al. Identifying video resolution from encrypted QUIC streams in segment-combined transmission scenarios[C]//Proceedings of the 34th Workshop on Network and Operating System Support for Digital Audio and Video. New York: ACM Press, 2024: 50-56.

[62] XU S C, SEN S, MAO Z M. CSI: inferring mobile ABR video adaptation behavior under HTTPS and QUIC[C]//Proceedings of the Fifteenth European Conference on Computer Systems. New York: ACM Press, 2020: 1-16.

[63] MAZHAR M H, SHAFIQ Z. Real-time video quality of experience monitoring for HTTPS and QUIC[C]//Proceedings of the IEEE INFOCOM 2018 - IEEE Conference on Computer Communications. Piscataway: IEEE Press, 2018: 1331-1339.

[64] TISA-SELMA, BENTALEB A, HAROUS S. Video QoE inference with machine learning[C]//Proceedings of the 2021 International Wireless Communications and Mobile Computing (IWCMC). Piscataway: IEEE Press, 2021: 1048-1053.

[65] 陈子涵, 程光, 徐子恒, 等 . 互联网加密流量检测、分类与识别研究综述[J]. 计算机学报, 2023, 46(5): 1060-1085.
CHEN Z H, CHENG G, XU Z H, et al. A survey on Internet encrypted traffic detection, classification and identification[J]. Chinese Journal of Computers, 2023, 46(5): 1060-1085.

[66] GUI X L, CAO Y L, HUANG L J, et al. A survey of QUIC-based network traffic identification[C]//Mobile Networks and Management. Berlin: Springer, 2023: 365-372.

[67] TONG V, TRAN H A, SOUIHI S, et al. A novel QUIC traffic classifier based on convolutional neural networks[C]//Proceedings of the 2018 IEEE Global Communications Conference (GLOBECOM). Piscataway: IEEE Press, 2018: 1-6.

[68] REZAEI S, LIU X. How to achieve high classification accuracy with just a few labels: a semi-supervised approach using sampled packets[J]. arXiv Preprint, arXiv: 1712.09761, 2018.

[69] LUXEMBURK J, HYNEK K, ČEJKA T, et al. CESNET-QUIC22: a large one-month QUIC network traffic dataset from backbone lines[J]. Data in Brief, 2023, 46: 108888.

[70] 袁越 . 基于多模态深度学习的QUIC流量分类方法的设计与实现[D]. 北京: 北京邮电大学, 2022.
YUAN Y. Design and implementation of QUIC traffic classification method based on multimodal deep learning[D]. Xi'an: Xidian University, 2022.

[71] DILLBARY N, YOZEVITCH R, DVIR A, et al. Hidden in time, revealed in frequency: spectral features and multiresolution analysis for encrypted Internet traffic classification[C]//Proceedings of the 2024 IEEE 21st Consumer Communications & Networking Conference (CCNC). Piscataway: IEEE Press, 2024: 266-271.

[72] BANO S, MACHUMILANE A, VALERIO L, et al. Federated feature engineering for semi-supervised classification of QUIC flows [C]//Proceedings of the 2022 IEEE 21st Mediterranean Electrotechnical Conference (MELECON). Piscataway: IEEE Press, 2022: 165-170.

[73] 黄凯 . 基于多任务深度学习的 QUIC 流量分类方法研究[D]. 哈尔滨: 哈尔滨理工大学, 2025.
HUANG K. Research on QUIC traffic classification method based on multi-task deep learning[D]. Harbin: Harbin University of Science and Technology, 2025.

[74] ALMUHAMMADI S, ALNAJIM A, AYUB M. QUIC network traffic classification using ensemble machine learning techniques[J]. Applied Sciences, 2023, 13(8): 4725.

[75] MERLIN C, PAULRAJ G J L, JEBADURAI I J, et al. Hyper parameter optimization for ensemble techniques in classifying QUIC traffic[C]//Proceedings of the 2024 International Conference on Cognitive Robotics and Intelligent Systems (ICC-ROBINS). Piscataway: IEEE Press, 2024: 621-626.

[76] LUXEMBURK J, HYNEK K, ČEJKA T. Encrypted traffic classification: the QUIC case[C]//Proceedings of the 2023 7th Network Traffic Measurement and Analysis Conference (TMA). Piscataway: IEEE Press, 2023: 1-10.

[77] 周宇迪 . 基于机器学习的 QUIC 加密流量分类方法研究[D]. 北京: 北京邮电大学, 2021.
ZHOU Y D. Research on QUIC encrypted traffic classification method based on machine learning[D]. Beijing: Beijing University of Posts and Telecommunications, 2021.

[78] ANWAR M A, AGRAWAL M, SAROHA N, et al. Attention to traffic: network traffic classification using attention-based CNNs[C]//Proceedings of the 2023 14th International Conference on Computing Communication and Networking Technologies (ICCCNT). Piscataway: IEEE Press, 2023: 1-6.

[79] SUDHAN S H H, KULKARNI S G. Security and service vulnerabilities with HTTP/3[C]//Proceedings of the 2024 16th International Conference on Communication Systems & Networks (COMSNETS). Piscataway: IEEE Press, 2024: 55-60.

[80] PRYNN T. Cross-protocol request forgery [R]. 2018.

[81] SY E, BURKERT C, FEDERRATH H, et al. A QUIC look at web

tracking[J]. Proceedings on Privacy Enhancing Technologies, 2019, 2019(3): 255-266.

[82] EUROPEAN UNION. General data protection regulation (GDPR)[R]. 2016.

[83] THIMMARAJU K, SCHEUERMANN B. Count me if you can: enumerating QUIC servers behind load balancers[J]. Electronic Communications of the European Association for Software Science and Technology, 2021, 8: 80.

[84] MÜCKE J, NAWROCKI M, HIESGEN R, et al. Waiting for QUIC: on the opportunities of passive measurements to understand QUIC deployments[J]. arXiv Preprint, arXiv: 2209.00965, 2022.

[85] HALL-ANDERSEN M, WONG D, SULLIVAN N, et al. nQUIC: noise-based QUIC packet protection[C]//Proceedings of the Workshop on the Evolution, Performance, and Interoperability of QUIC. New York: ACM Press, 2018: 22-28.

[86] KEMPF M, GAUDER N, JAEGER B, et al. A quantum of QUIC: dissecting cryptography with post-quantum insights[C]//Proceedings of the 2024 IFIP Networking Conference (IFIP Networking). Piscataway: IEEE Press, 2024: 195-203.

[87] TEYSSIER B, JOARDER Y A, FUNG C. QUICShield: a rapid detection mechanism against QUIC-flooding attacks[C]//Proceedings of the 2023 IEEE Virtual Conference on Communications (VCC). Piscataway: IEEE Press, 2023: 43-48.

[88] KADI A, KHOUKHI L, VIINIKKA J, et al. Machine learning for QUIC traffic flood detection[C]//Proceedings of the 2024 Global Information Infrastructure and Networking Symposium (GIIS). Piscataway: IEEE Press, 2024: 1-6.

[89] KADI A, KHOUKHI L, VIINIKKA J, et al. Adapting to the evolution: enhancing intrusion detection through machine learning in the QUIC protocol era[J]. IEEE Transactions on Network and Service Management, 2025, 22(2): 1929-1944.

[90] 陈宏伟, 尹小康, 盖贤哲, 等. 基于主动-被动结合的新型 UDP 反射放大协议识别方法[J]. 计算机科学, 2023, 50(1): 224-230.
CHEN H W, YIN X K, GAI X Z, et al. New type of UDP reflection amplification protocol recognition method based on active-passive combination [J]. Computer Science, 2023, 50(1): 224-230.

[91] DEY D, GHOSH N. IQUIC: an intelligent framework for defending QUIC connection ID-based DoS attack using advantage actor – critic RL[J]. Computers & Security, 2025, 155: 104463.

[92] CHATZOGLOU E, KOULIARIDIS V, KAMBOURAKIS G, et al. A hands-on gaze on HTTP/3 security through the lens of HTTP/2 and a public dataset[J]. Computers & Security, 2023, 125: 103051.

[93] ŠPAČEK S, VELAN P, HOLKOVIČ M, et al. Event-flow correlation for anomaly detection in HTTP/3 web traffic[C]//Proceedings of the NOMS 2023-2023 IEEE/IFIP Network Operations and Management Symposium. Piscataway: IEEE Press, 2023: 1-6.

[94] LEE J, KIM M, SONG W, et al. Rescuing QUIC flows from countermeasures against UDP flooding attacks[C]//Proceedings of the 39th ACM/SIGAPP Symposium on Applied Computing. New York: ACM Press, 2024: 1072-1080.

[95] GOVIL Y, WANG L, REXFORD J. MIMIQ: masking IPs with migration in QUIC[C]//Proceedings of the 10th USENIX Workshop on Free and Open Communications on the Internet (FOCI 20). Berkeley: USENIX Association, 2020: 19-25.

[96] ZHANG W. Secure address allocation mechanism in QUIC-based protocols[R]. 2023.

[97] SMITH J P, DOLFI L, MITTAL P, et al. QCSD: a QUIC client-side website-fingerprinting defence framework[C]//Proceedings of the USENIX Security Symposium. Berkeley: USENIX Association, 2022: 2347-2364.

[98] KÜHLEWIND M, CARLANDER-REUTERFELT M, IHLAR M, et al. Evaluation of QUIC-based MASQUE proxying[C]//Proceedings of the 2021 Workshop on Evolution, Performance and Interoperability of QUIC. New York: ACM Press, 2021: 29-34.

[99] DIKSHIT P, SENGUPTA J, BAJPAI V. Recent trends on privacy-preserving technologies under standardization at the IETF[J]. ACM SIGCOMM Computer Communication Review, 2023, 53(2): 22-30.

[100] HALL D. Zero Trust WARP: tunneling with a MASQUE[R]. 2024.

[101] PAVUR J, STROHMEIER M, LENDERS V, et al. QPEP: an actionable approach to secure and performant broadband from geostationary orbit[C]//Proceedings 2021 Network and Distributed System Security Symposium. Internet Society, 2021: 24074.

[102] HUWYLER J, PAVUR J, TRESOLDI G, et al. QPEP in the real world: a testbed for secure satellite communication performance[C]//Proceedings 2023 Workshop on Security of Space and Satellite Systems. Internet Society, 2023: 239792.

[103] GHARAM M M, STEGER L. Survey on the current state of Tor over QUIC[R]. 2023.

[104] PERRY D. The case for Tor-over-QUIC[R]. 2018.

[105] HEIJLIGERS J. Tor over QUIC[D]. Nederland: Delft University of Technology, 2021.

[106] HOGAN K. Security analysis of Tor over QUIC[D]. Cambridge: Massachusetts Institute of Technology, 2020.

[107] GBUR K Y, TSCHORSCH F. A quick way through your firewall[J]. arXiv Preprint, arXiv: 2107.05939, 2021.

[108] LORIMER A H, FEAMSTER N, MITTAL P. Poster: investigating QUIC's potential impact on censorship circumvention[C]//Proceedings of the 2022 ACM SIGSAC Conference on Computer and Communications Security. New York: ACM Press, 2022: 3403-3405.

[109] ELMENHORST K, SCHÜTZ B, ASCHENBRUCK N, et al. Web censorship measurements of HTTP/3 over QUIC[C]//Proceedings of the 21st ACM Internet Measurement Conference. New York: ACM Press, 2021: 276-282.

[110] FILASTO A, APPELBAUM J. OONI: open observatory of network interference[C]//Proceedings of the 2nd USENIX Workshop on Free and Open Communications on the Internet. Berkeley: USENIX Association, 2012: 6.

[111] MICHEL F, BONAVENTURE O. Towards SSH3: how HTTP/3 improves secure shells[J]. arXiv Preprint, arXiv: 2312.08396, 2023.

[112] CONINCK Q D, KALANTARI S, SION L, et al. URLink: using names as sole Internet addresses to tackle scanning attacks in IoT[C]//Proceedings of the First International Workshop on Security and Privacy of Sensing Systems. New York: ACM Press, 2023: 15-21.

[113] MCMILLAN K L, ZUCK L D. Formal specification and testing of QUIC[C]//Proceedings of the ACM Special Interest Group on Data Communication. New York: ACM Press, 2019: 227-240.

[114] CROCHET C, ROUSSEAUX T, PIRAUX M, et al. Verifying QUIC implementations using ivy[C]//Proceedings of the 2021 Workshop on Evolution, Performance and Interoperability of QUIC. New York: ACM Press, 2021: 35-41.

[115] GOEL V, PAULO R, PAASCH C. Testing QUIC with packetdrill[C]//Proceedings of the Workshop on the Evolution, Performance, and Interoperability of QUIC. New York: ACM Press, 2020: 1-7.

[116] REEN G S, ROSSOW C. DPIFuzz: a differential fuzzing framework to detect DPI elusion strategies for QUIC[C]//Proceedings of the 36th Annual Computer Security Applications Conference. New York: ACM Press, 2020: 332-344.

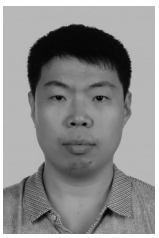
[117] LUO Z X, YU J Z, ZUO F L, et al. Bleem: packet sequence oriented fuzzing for protocol implementations [C]//Proceedings of the USENIX Security Symposium. Berkeley: USENIX Association, 2023: 4481-4498.
[118] ANG K, RANASINGHE D. QUIC-Fuzz: an effective greybox fuzzer for the QUIC protocol[J]. arXiv Preprint, arXiv: 2503.19402, 2025-03-25.
[119] SEEMANN M, IYENGAR J. Automating QUIC interoperability testing[C]//Proceedings of the Workshop on the Evolution, Performance, and Interoperability of QUIC. New York: ACM Press, 2020: 8-13.
[120] MARX R, HERBOTS J, LAMOTTE W, et al. Same standards, different decisions: a study of QUIC and HTTP/3 implementation diversity[C]//Proceedings of the Workshop on the Evolution, Performance, and Interoperability of QUIC. New York: ACM Press, 2020: 14-20.
[121] MARX R, LAMOTTE W, REYNDERS J, et al. Towards QUIC debuggability[C]//Proceedings of the Workshop on the Evolution, Performance, and Interoperability of QUIC. New York: ACM Press, 2018: 1-7.
[122] VÖLKER T, TÜXEN M, RATHGEB E P. The search of the path MTU with QUIC[C]//Proceedings of the 2021 Workshop on Evolution, Performance and Interoperability of QUIC. New York: ACM Press, 2021: 22-28.
[123] SANDER C, KUNZE I, BLÖCHER L, et al. ECN with QUIC: challenges in the wild[C]//Proceedings of the 2023 ACM on Internet Measurement Conference. New York: ACM Press, 2023: 540-553.
[124] ZIRNGIBL J, GEBAUER F, SATTLER P, et al. QUIC hunter: finding quic deployments and identifying server libraries across the internet[C]// Passive and Active Measurement. Berlin: Springer, 2024: 273-290.
[125] VÖLKER T, TÜXEN M. Packet too big detection and its integration into QUIC[C]//Proceedings of the 2023 16th International Conference on Signal Processing and Communication System (ICSPCS). Piscataway: IEEE Press, 2023: 1-10.
[126] DECKER L. QUIC & the dead: which of the most common IDS/IPS tools can best identify QUIC traffic[R]. 2020.
[127] FRANZIL M. Real-time monitoring of the QUIC protocol[D]. Trento: University of Trento, 2022.
[128] HILAL F, GASSER O. Yarrpbox: detecting middleboxes at Internet-scale[J]. Proceedings of the ACM on Networking, 2023, 1(CoNEXT1): 1-23.
[129] TRAMMELL B, KÜHLEWIND M. Revisiting the privacy implications of two-way Internet latency data[C]//Passive and Active Measurement. Cham: Springer, 2018: 73-84.
[130] KUNZE I, SANDER C, WEHRLE K. Does it spin? on the adoption and use of QUIC's spin bit[C]//Proceedings of the 2023 ACM on Internet Measurement Conference. New York: ACM Press, 2023: 554-560.
[131] SANDER C, KUNZE I, WEHRLE K. Analyzing the influence of resource prioritization on HTTP/3 HOL blocking and performance[C]// Proceedings of the Network Traffic Measurement and Analysis Conference. Geneva: IFIP Newsletter, 2022: 1-10.
[132] LI X, WU D S, DUAN H X, et al. DNSBomb: a new practical-and-powerful pulsing DoS attack exploiting DNS queries-and-responses[C]// Proceedings of the 2024 IEEE Symposium on Security and Privacy (SP). Piscataway: IEEE Press, 2024: 4478-4496.
[133] ZHANG Q Q, SU C J. Application-layer characterization and traffic analysis for encrypted QUIC transport protocol[C]//Proceedings of the 2023 IEEE Conference on Communications and Network Security (CNS). Piscataway: IEEE Press, 2023: 1-9.
[134] HOFFMAN P, MCMANUS P. DNS queries over HTTPS (DoH)[S]. 2018.
[135] 张曼, 姚健康, 李洪涛, 等. DNS 信道传输加密技术: 现状、趋势和挑战[J]. 软件学报, 2024, 35(1): 309-332.
ZHANG M, YAO J K, LI H T, et al. Encryption technologies for DNS channel transmission: status, trends and challenges[J]. Journal of Software, 2024, 35(1): 309-332.
[136] HOUSER R, LI Z, COTTON C, et al. An investigation on information leakage of DNS over TLS[C]//Proceedings of the 15th International Conference on Emerging Networking Experiments and Technologies. New York: ACM Press, 2019: 123-137.
[137] SIBY S, JUAREZ M, DIAZ C, et al. Encrypted DNS - privacy a traffic analysis perspective[J]. arXiv Preprint, arXiv: 1906.09682, 2019.
[138] HU G N, FUKUDA K. An analysis of privacy leakage in DoQ traffic[C]// Proceedings of the CoNEXT Student Workshop. New York: ACM Press, 2021: 7-8.

[作者简介]

张麟康（2000– ），男，山东临沂人，中国科学院大学博士生，主要研究方向为网络空间测绘、域名安全、网络流量分析等。

程逸飞（1999– ），男，江苏徐州人，中国科学院大学博士生，主要研究方向为新型加密网络协议分析、网站指纹识别等。

朱宇佳（1984– ），女，江苏无锡人，博士，中国科学院信息工程研究所副研究员、硕士生导师，主要研究方向为网络空间测绘、域名安全、网络大数据分析等。



刘庆云（1980– ），男，河北衡水人，博士，中国科学院信息工程研究所正研级高级工程师、博士生导师，主要研究方向为网络空间测绘、网络空间安全等。