

科技评论

量子保密通信与5G融合的探索实践

缪亚军¹, 武俊¹, 戚海洋², 汤静¹, 李明翰¹

摘要 在量子信息技术与信息通信技术融合背景下,面向提升信息通信安全性和便携性的迫切需求,采用了理论分析和实际应用案例结合的方式,探讨了量子保密通信与5G融合的探索实践,展示了量子保密通信在5G网络中的融合策略与应用成效。量子保密通信正携手5G在承载网络、网络切片等基础设施层面探索融合,同时催生出量子加密通话、量子加密对讲等融合创新应用。展望了量子保密通信与5G融合的未来发展:随着量子保密通信和5G在基础设施、应用场景等方面不断深度融合,将共同构筑高速泛在、自主可控的数字基础设施,为数字经济的蓬勃发展提供坚实而强大的安全保障,有力推动产业数字化转型升级,助力数字经济持续发展。

关键词 量子保密通信;5G;网络基础设施安全;融合应用安全

2021年12月,国际电信联盟发布了《量子保密通信网络应用用例》报告^[1],提出了量子保密通信与5G(第5代移动通信技术)等电信网络、密码原语、TCP/IP协议(transmission control protocol/ internet protocol,传输控制协议/网络协议)、移动终端和垂直行业融合等6大类应用用例。2023年8月,我国首个面向应用的量子保密通信标准《量子保密通信应用基本要求》(GB/T42829-2023)^[2]正

式发布,标准给出了多个应用场景,包括电信接入网络、骨干网络和移动应用等。国内国际相关标准的陆续出台,为量子保密通信与5G在网络、应用等方面的融合提供了重要指引。

1 量子保密通信与5G融合满足日益增强的安全需求

随着5G向经济社会多个领域渗透,5G在数字化转型发展中的基础性地位、全局性影响愈发突出,同时5G网络基础设施安全和数据、应用安全也越来越重要。以我国为例,2019年6月,工业和信息化部正式向中国电信集团公

司、中国移动通信集团公司(中国移动)、中国联合网络通信集团有限公司(中国联通)、中国广播电视网络集团有限公司发放5G商用牌照,我国正式进入5G商用元年。经过4年左右的发展,截至2023年6月,我国建成5G基站约290万个,5G用户已超过6.7亿^[3],5G应用正向工业、交通、能源、医疗等领域加速推进。为进一步加强5G安全保障能力体系建设,2021年11月,工业和信息化部发布《“十四五”信息通信行业发展规划》,并明确要求“打造包括5G网络基础设施和5G应用安全的国际领先的5G安全保障能力,形成技术领先、应用丰富、可持续发

1. 国科量子通信网络有限公司,
上海 201315
2. 菏泽市产品检验检测研究院,
菏泽 274000

收稿日期:2022-12-14;修回日期:2024-03-18

基金项目:浙江省软科学项目(2024C35052)

作者简介:缪亚军,博士,研究方向为量子信息科技产业化、量子保密通信应用与标准化,电子信箱:miaoyajun@qtict.com;李明翰(通信作者),高级工程师,研究方向为量子通信及标准化研究,电子信箱:liminghan@qtict.com

引用格式:缪亚军,武俊,戚海洋,等.量子保密通信与5G融合的探索实践[J].科技导报,2025,43(4):14-18;doi:10.3981/j.issn.1000-7857.2023.12.01895

展的5G应用安全保障生态”。

面对应用层面日益增强的安全需求和不断演进的网络攻击,5G安全体系需要不断迭代升级,一方面,既有的网络安全保障需要逐步健全,例如,承载网普遍未启用加密技术,业务数据流量保护依赖上层应用的加密手段。另一方面,随着量子计算技术快速发展,主要通过经典密码保护身份认证和通信安全的5G网络和应用,需要更安全的技术手段增强安全性。量子保密通信与5G融合能够为5G构建更高等级的安全屏障提供重要支撑。

根据《量子保密通信应用基本要求》^[2],量子保密通信是指以量子密钥分发(quantum key distribution, QKD)作为密钥分发功能组件,结合适当的密钥管理、密码算法和协议而形成的保密通信解决方案。QKD的安全性由量子物理原理保证,能够提供具有信息论安全性的通信手段,在量子密钥协商过程中,窃听者无法做到既偷看又不留下痕迹。量子保

密通信并不是要替代经典通信方式,而是一种增强经典通信安全的技术,同时量子保密通信的规模化应用也需要与经典通信技术相融合,构建广域量子保密通信网络体系。得益于国家的前瞻部署和长期支持,国科量子通信网络有限公司在全球率先初步建成了星地一体广域量子保密通信骨干网络,总长超过1万km,覆盖京津冀、长三角、粤港澳大湾区、成渝、东北等区域,并与“墨子号”、量子微纳卫星成功对接,具备全球量子密钥投送能力。网络成码率、可用性、可运营性等关键指标均处于全球领先地位,这为量子保密通信与5G技术的融合提供了条件和可能(图1)。

2 量子保密通信提升5G网络基础设施安全

量子保密通信与5G融合为增强网络基础设施安全提供了重要的技术手段,国内外电信运营商已在5G承载网和5G网络切片

中开展量子保密通信融合试点^[4]。

1) 量子保密通信提升5G承载网的安全性。5G承载网是为5G无线接入网和核心网提供网络连接的基础网络,根据不同部署场景及业务需求,可分为前传、中传和回传,前传和中传分别连接无线接入网的不同网元,回传连接无线接入网和核心网。目前量子保密通信与5G承载网络的前传、回传及设备层面的融合已经取得积极成果。

在5G前传网络方面,2023年英国布里斯托大学研究团队在英国5G国家测试网5GUK上成功验证了量子保密通信技术保护5G前传网络的可行性,支持加密和传输速率达100 Gbps,不仅提升了5G前传网络的安全性,同时对网络时延几乎无影响,满足了前传网络大带宽、低时延的要求^[5]。

在5G回传网络方面,韩国最大的电信运营商SK Telecom在将量子保密通信与4G网络融合提供回传加密服务的基础上,于2019年在首尔经大田至太平的5G回传网络中应用量子保密通信保护数据安全,该网络承载了约30%的5G核心网流量,SKT沿5G回传网络部署了超过300 km的量子保密通信网络,用量子保密通信取代原有传输层安全性协议(transport layer security, TLS)/IPsec(IKEv2)等加密通信协议,使得回传网络安全性得到了进一步增强^[1]。

在5G承载网络设备方面,近年来主流设备商,如思科公司^[6]、诺基亚公司^[7]、Juniper网络公司^[8]等陆续开始将量子保密通信与其

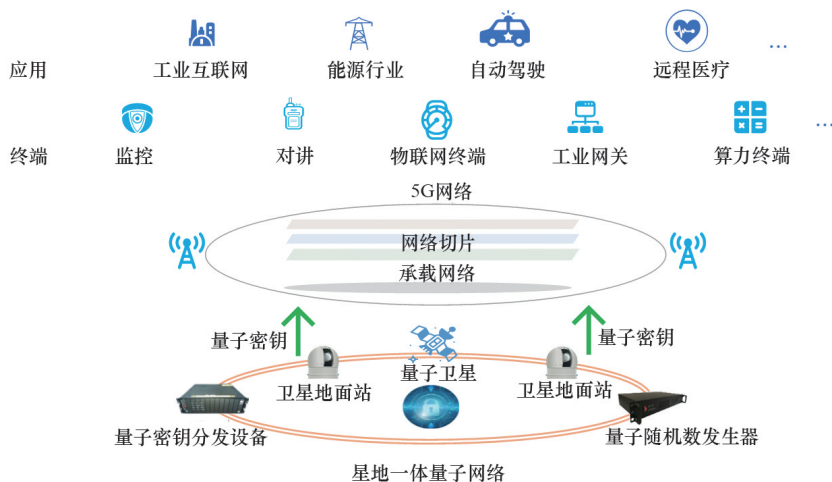


图1 量子保密通信与5G融合增强网络和应用安全

路由器和光传输设备融合,分别开发出相应的接口技术,支持在路由器或光传输设备中利用量子密钥加密传输增强网络连接的安全性,为量子保密通信与承载网络快速全面融合奠定了基础。目前相关设备已在欧盟 OPENQKD (开放量子密钥分发)项目和欧洲运营商网络中成功验证。

2) 量子保密通信能增强 5G 网络切片隔离和数据传输的安全。5G 引入了网络切片技术,通过网络切片,运营商能够在一个通用的物理网络之上构建多个专用的、虚拟化的、互相隔离的逻辑网络,满足不同客户对网络能力的差异化要求。为不同切片之间提供有效的安全隔离措施和加密措施来确保不同切片之间数据传输的安全性是网络切片的重要关注点。

目前利用量子保密通信增强 5G 网络切片安全性的研究和试点工作正在加快推进,例如,国家电网有限公司、中国移动通信集团公司和国科量子通信网络有限公司(国科量子)等在电力领域开展了融合量子保密通信与 5G 切片专网的现网试验,利用量子保密通信加密传送电力配网(在 5G 网络上利用切片技术形成的专网)控制信息,时延和安全性满足电网电力生产、调度、巡检、管理等重要业务的需求^[9]。英国电信公司和约克大学等合作,利用量子进行保密通信,在英国电信创新基地 Adastral Park 和剑桥间的网络上建立了动态、安全增强的端到端 5G 网络切片^[10]。

3 量子保密通信提供 5G 应用安全保障、推动融合创新

量子保密通信与 5G 融合,形成了量子加密通话和量子对讲等新产品、新业务,并且正在车联网、工业互联网等场景中开展试点应用。

1) 量子加密通话/加密对讲。量子加密通话利用量子密钥增强 5G VoIP/VoLTE 的身份认证安全和通信安全,通话建立前使用符合商密要求的 TF 卡(Trans-flash Card)/SIM (Subscriber Identity Module),卡内预置量子密钥先进行身份认证,在身份认证完成后,手机终端获取量子会话密钥,对通话内容进行加密保护,能够有效防止用户重要信息在通话过程中被窃听、泄露(图 2)。量子加密通话具有密钥“真随机”、端到端加密、“一话一密”等特点,同时支持高清语音,具有良好的应用体验。中国电信 2021 年以来陆续发布了量子密话业务和天翼量子高清密话,目前总用户已突破 100 万。2022 年 5 月,中国移动和信通数智量子科技有限公司(信通数智量子)、国科量子等联合推出

了量子加密通话业务,正在雄安等地推进商用落地使用。韩国运营商韩国电信正在进行量子+5G 密话试点项目。

量子加密对讲是将量子安全能力融入现有基于 5G 网络的对讲业务产品,其采用“一次一密”的加密方式,实现对讲终端身份认证、网络与通信数据加密,能够有效防止信息窃听和身份冒用,提供安全、稳定、可靠的对讲调度服务。2023 年 5 月,中国移动和信通数智量子、国科量子等合作伙伴联合推出了量子加密对讲业务,为杭州第十九届亚运会赛事提供了增强的安全保障服务;中国电信 2022 年推出了量子加密对讲业务,在 2022 年北京冬奥会中为现场交通、车队、人员的统一调度指挥提供通信安全保障。

2) 量子保密通信+5G 车联网应用。量子保密通信与 5G 的融合可同时满足车辆控制信息传输的高安全性和低时延需求,提高自动驾驶系统的安全性和可靠性(图 3)。中国联通在北京的车联网示范基地验证了量子密钥云平台与 5G 车联网的应用,加密时延等性能指标满足了远程驾驶和自

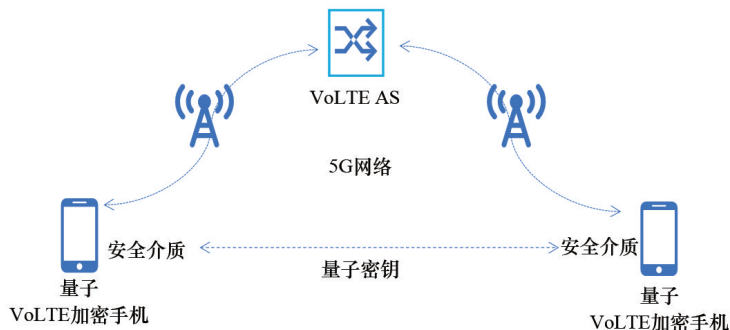


图2 量子加密通话示意

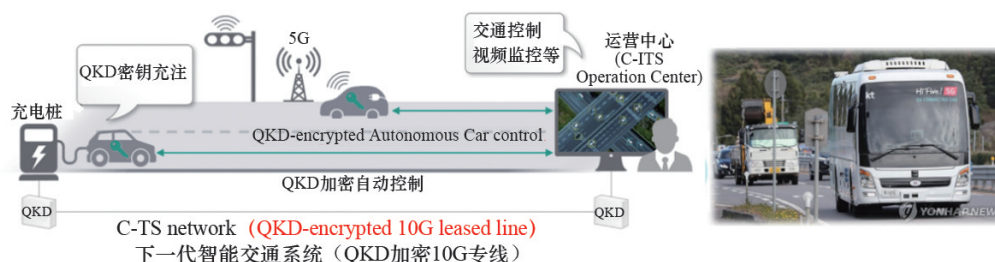


图3 量子保密通信+5G车联网应用示意

自动驾驶等多种场景的需求。韩国电信在济州岛无人驾驶试验中,利用量子密钥加密实时交通信息、突发路况等重要数据,通过5G网络传输至自动驾驶汽车,以便自动驾驶汽车及时反应并采取相应措施。

3) 基于量子保密通信和5G的产品质量实时检测。基于量子保密通信和5G的产品质量实时检测和优化方案通过将量子保密通信、5G、机器视觉、边缘计算等技术结合,可实现产品质量的实时高精度检测,能够满足实时性的同时保障了产品数据的安全(图4)。在数据传输方面,量子保密通信与5G融合,在实时性、安全性方面更好满足工业应用需要;在数据存储方面,量子保密通信增强了边缘云和公有云上产品数据存储安全。方案的实施有助于企业提高检测效率,节省生产成本。

当前,量子保密通信与5G融合正处于探索和发展阶段,并已取得了一系列积极进展,但仍面临着标准指导不足、应用案例不足和市场对新技术接受度低等挑战。例如,由于缺少技术融合对接标准规范,量子保密通信与5G网络基础设施对接时往往需要解决多项互通和互操作问题,增加了技术实施的难度和部署成本;目前融合应用仍局限于部分企业的点状探索,缺乏对融合发展经验的积累提炼,尚未形成可复制、可推广的路径模式;新一代安全技术投入较高,收益难以量化,部分企业难免存在“不愿”“不敢”“不会”的困境。

从行业发展角度来看,量子保密通信与5G融合所面临的挑战正迎来更多的关注和举措。在标准规范方面,2023年6月国际电信联盟(International Telecommunication Union, ITU)正式通过

了《IMT-2030(全球6G愿景)框架建议书》,明确提出要抵御量子计算威胁。中国电信、华为公司等34家单位参与的中国IMT-2030(6G)网络技术组及海外多个运营商通过《6G白皮书》形式,支持在6G网络中引入量子通信等增强的密码技术来实现量子安全。在市场推广方面,杭州亚运会、北京冬奥会等大型活动的量子+5G成功应用案例正在发挥引领示范作用,辐射带动千行百业关注并了解量子+5G技术,在工业、能源、医疗等领域为工业互联网企业、电网、医院等关键基础设施提供安全服务。

2021年7月,工业和信息化部、中央网络安全和信息化委员会办公室、国家发展和改革委员会等10个部门联合印发“5G应用‘扬帆’行动计划”,明确要求“加快跨领域融合创新发展……打好技术‘组合拳’,不断培育5G应用新蓝海”,鼓励相关行业和企业先行先试量子保密通信与5G融合技术,不仅有助于构筑更加安全高效的数字基础设施,而且能为数字经济的健康发展提供强大的技术支撑和安全保障,推动产业数字化转型升级,助力数字经济迈向新的高峰。

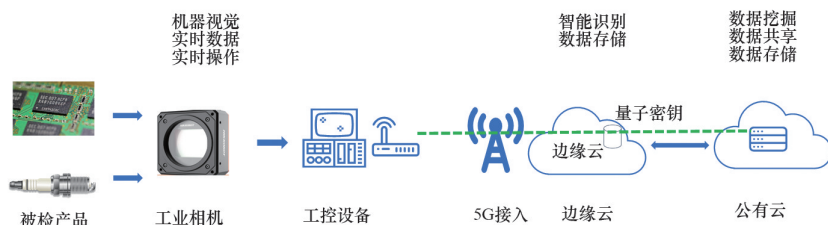


图4 基于量子保密通信和5G产品质量实时检测示意

参考文献(References)

- [1] ITU-T Focus Group on Quantum Information Technology for Networks (FG QIT4N). Technical report FG QIT4N D2.2: Quantum information technology for networks use cases: Quantum key distribution network [R]. Geneva: ITU, 2021.
- [2] 国家市场监督管理总局, 国家标准化管理委员会. 量子保密通信应用基本要求: GB/T 42829—2023[S]. 北京: 中国标准出版社, 2023.
- [3] 工业和信息化部. 2023年上半年通信业经济运行情况[EB/OL]. (2023-07-20)[2023-11-01]. https://wap.miit.gov.cn/gxsj/tjfx/txy/art/2023/art_75d835da87d24c13aa5dc752-b901aca7.html
- [4] 赵勇. 量子通信技术助力“新基建”信息安全[J]. 中国信息安全, 2020(7): 33-35.
- [5] Arabul E, Oliveira R D, Emami A, et al. 100 Gbps quantum-secured and O-RAN-enabled programmable optical transport network for 5G fronthaul[J]. Journal of Optical Communications and Networking, 2023, 15(8): C223-C231.
- [6] Cisco. Security and VPN configuration guide[EB/OL]. (2021-01-11)[2023-11-01]. <https://www.cisco.com/c/en/us/td/docs/routers/ios/config/17-x/sec-vpn/b-security-vpn/m-sec-cfg-quantum-encryption-ppk.html#cisco-secure-key-integration-protocol-and-dynamic-ppk>.
- [7] Nokia. Quantum safe networks[EB/OL]. (2023-01-01) [2023-11-01]. https://onestore.nokia.com/asset/213258?_ga=2.113724935.1866941391.1701932016-1472546916.1691049144.
- [8] Juniper. Validation of a quantum safe MACSEC implementation[EB/OL]. (2022-07-01) [2023-11-01]. <https://www.juniper.net/content/dam/www/assets/white-papers/us/en/2022/validation-of-quantum-safe-macsec-white-paper.pdf>.
- [9] 吴忠平, 王路杰, 许佳诺, 等. 基于量子保密通信及5G硬切片专网的配网应用研究[J]. 电信科学, 2022, 38(1): 159-169.
- [10] Wright P, White C, Parker R C, et al. 5G network slicing with QKD and quantum-safe security[J]. Journal of Optical Communications and Networking, 2021, 13(3): 33-40.

Exploration and practice of quantum secure communication and 5G integration

MIAO Yajun¹, WU Jun¹, QI Haiyang², TANG Jing¹, LI Minghan^{1*}

1. Chinese Academy of Sciences Quantum Network Co., Ltd., Shanghai 201315, China
2. Heze Product Inspection and Testing Research Institute, Heze 274000, China

Abstract In the context of the integration of quantum information technology and information communication technology, and in response to the urgent need to enhance the security and portability of information communication, in this paper, theoretical analysis and practical application cases were combined to explore the integration practices of quantum secure communication and 5G, and the integration strategies and application effects of quantum secure communication in 5G networks were demonstrated. Quantum secure communication, enabled by 5G, has been used to explore the integration at the infrastructure level, such as bearer networks and network slicing. Meanwhile innovative applications like quantum-encrypted calls and quantum-encrypted intercom have been fostered. The future development of the integration of quantum secure communication and 5G were forecasted: enabled by quantum secure communication and 5G which have been integrated continuously and deeply at infrastructure and application scenarios, a high-speed, ubiquitous, and autonomously controllable digital infrastructure will be built. It will provide a solid security guarantee for the vigorous growth of digital economy, promote the digital transformation and upgrading of industries and support the sustained development of the digital economy.

Keywords quantum secure communication; 5G; network infrastructure security; converged application security ●



(责任编辑 王微)