专题:量子保密通信技术及应用

量子保密通信现实安全性与发展前景分析

赖俊森　刘璐　吴冰冰　赵文玉　张海懿

摘要:基于量子密钥分发的量子保密通信技术是未来进一步提升网络信息安全保障能力的可选方案之一。近年来,量子保密通信前沿研究、试点应用和网络建设快速发展,产业化水平不断提升。近期,量子保密通信系统和网络的现实安全性问题引发学术界、产业界和社会舆论的广泛关注与讨论。本文对量子保密通信系统和网络的现实安全性问题进行分析探讨,同时展望量子保密通信技术应用前景并提出相关策略建议。

关键词:量子密钥分发;量子保密通信;现实安全性;发展前景

1　引言

量子是不可分割的微观粒子(如光子和电子等)的统称。量子力学为人类认识和改造自然奠定理论基础,量子物理学的突破和发展是触发科技革命的关键使能要素。随着人类对微观粒子系统观测和调控能力的不断突破和提升,量子科技革命的第二次浪潮即将来临。量子信息技术通过对光子、电子和冷原子等微观粒子系统及其量子态进行精确人工观测和调控,借助量子叠加和量子纠缠等独特物理现象,以经典理论无法实现的方式获取、传输和处理信息,主要包括量子通信、量子计算和量子测量3个技术方向。

量子通信利用微观粒子系统(主要是光子)的量子叠加态或纠缠效应等进行密钥或信息传输,主要包括量子隐形传态(QT)和量子密钥分发(QKD)两类。量子隐形传态在经典通信的辅助下能够实现量子态信息的直接传输,是基础科研领域的前沿热点,但仍处于试验研究和验证阶段,距离实用化仍有明显距离。未来量子隐形传态和量子计算融合形成量子信息互联网是量子通信发展的重要方向,美国和欧盟已经开始进行量子隐形传态试验网络的项目布局和建设。量子密钥分发通过对光子或光场正则分量的量子叠加态制备、传输和测量,首先在收发双方间实现信息论可证明安全性的密钥共享,之后再与传统保密通信技术相结合完成经典信息的加解密和安全传输,基于量子密钥分发的保密通信称为量子保密通信。量子保密通信目前已进入初步实用化阶段,是未来提升信息安全防护能力的可选解决方案之一。

量子保密通信使用QKD提供的密钥并采用对称加密体制实现业务信息的加密传输,系统原理如图1所示。QKD设备结合光开关、波分复用器等传输辅助设备完成量子态光信号物理层传输和点到点QKD密钥生成。量子密钥管理设备负责网元管理、密钥管理和基于可信中继的端到端密钥生成。量子加密应用设备,主要包括量子加密VPN和量子加密路由器等,使用QKD密钥对业务信号进行加密处理和传输接收。量子加密应用设备和传统保密通信设备在加密算法、校验算法、整体功能和性能等方面基本一致,主要区别在于使用QKD密钥替换传统保密通信中双方通过协商得到的加密密钥。

我国量子通信技术研究与国际先进水平基本保持同步,在星地量子通信等领域的研究和应用探索方面处于领先,同时在国家和一些地方政府的支持下,我国在量子保密通信试点应用项目数量、投资金额和网络规模等方面已处于全球领先。2017年,量子保密通信"京沪干线"技术验证与应用示范项目投入使用,总长

超过2000km，接入北京、济南、合肥和上海4地量子保密通信城域网络，采用可信中继方案进行密钥中继。2018年，国家广域量子保密通信骨干网络建设一期工程开始实施，在“京沪干线”基础上增加武汉和广州两个骨干节点，新建北京—武汉—广州线路和武汉—合肥—上海线路，并接入若干已有和新建城域网络。

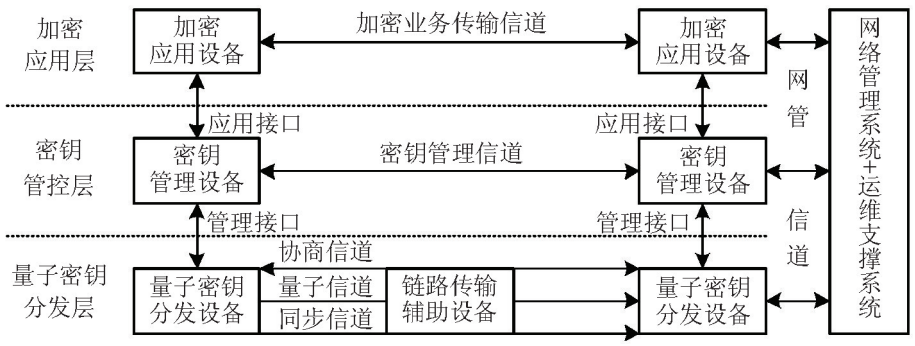

图1 基于量子密钥分发的量子保密通信系统原理框图

在取得可喜的研究与应用成果的同时，学术界、产业界和社会舆论对于量子保密通信技术、系统和网络的现实安全性及其应用价值也一直存在一些关注和讨论。近期，中科大郭光灿院士团队和上海交大金贤敏教授团队发表的量子密钥分发系统现实安全性的研究论文，在社会舆论中引发了关于量子保密通信安全性的争议与讨论。本文对量子保密通信系统和网络的现实安全性问题进行分析探讨，同时展望量子保密通信技术应用前景并提出相关策略建议。

2 量子保密通信的安全性及风险点分析

量子密钥分发技术经过近40年的发展，其中密钥分发的安全性由量子力学的基本原理保证，理论安全性证明也相对完备，量子密钥分发技术在提供对称密钥的安全性方面的价值已经获得全球学术界和产业界的承认和共识。但需要指出的是，基于量子密钥分发的量子保密通信系统和网络的现实安全性仍然存在一定风险，也是各方讨论量子保密通信发展和应用的一个主要关注点。

（1）量子密钥分发只是量子保密通信系统的一个环节，量子保密通信系统满足信息论可证明安全性的前提是需要量子密钥分发、一次一密加密和安全身份认证3个环节，缺一不可。目前，量子密钥分发系统的现网密钥生成速率约为数十kbit/s量级，对于现有信息通信网络中的SDH、OTN和以太网等高速业务，难以采用一次一密加密，只能与传统对称加密算法（如AES、SM1和SM4加密算法）相结合，由量子密钥分发提供对称加密密钥。在此情况下，由于存在密钥的重复使用，不能满足一次一密的加密体制要求，所以此时的量子保密通信系统并不能达到信息论层面的“绝对安全”。但相比传统对称加密体系，量子保密通信仍然能够带来一定程度的安全性提升和应用价值，主要来自于两个方面：一方面，相比原有对称加密算法的收发双发自协商产生加密密钥，量子密钥分发所提供的加密密钥在密钥分发过程的防窃听和破解的能力得到加强；另一方面，量子密钥分发能够提升对称加密体系中的密钥更新速率，从而降低加密数据被计算破解的风险。

（2）量子密钥分发技术能够保障点到点的光纤或自由空间链路中的密钥分发的安全性。由于量子存储和量子中继技术距离实用化仍有一定距离，长距离的量子密钥分发线路和网络需要借助“可信中继节点”技术进行逐段的密钥分发和落地存储中继。密钥一旦落地存储，就不再具备量子态和由量子力学保证的信息论安全性，量子密钥分发线路和网络中的“可信中继节点”需要采用传统信息安全领域的高等级防护来保证节点自身的安全性。目前，针对“可信中继节点”的安全性防护要求、标准和测评等工作正在逐步开展，但尚未正式推出相关标准和要求，测评工作有待完善。未来进一步加强可信中继节点技术要求、安全性分析和测评方法等标准的研究与实施，将是保障量子保密通信网络建设和应用现实安全性的重要措施之一。通过

明确可信中继节点的安全防护要求和实施方案并通过相关测评验证，结合量子密钥分发和符合相应等级要求的密钥中继及安全管理方案，可以实现具有实用化水平和符合安全性等级要求的量子密钥分发网络。

（3）量子密钥分发技术的信息论可证明安全性是指理论证明层面，对于实际量子密钥分发系统而言，由于实际器件（如光源、探测器和调制器等）无法满足理论证明的假设条件，即可能存在安全性漏洞，所以量子密钥分发系统的实际安全性和漏洞攻击与防御，一直是学术界研究的热点之一。前述的中科大郭光灿院士团队和上海交大金贤敏教授团队的研究报道，都是针对量子密钥分发实际系统的安全性漏洞进行攻击和防御改进的学术研究成果。针对量子密钥分发安全性攻防的学术研究成果需要一分为二看待：一方面，这类研究通常在完全控制系统设备的条件下，采用极端条件模拟（如超高光功率注入等方式）来攻击系统获取密钥信息，与实际系统和网络中可行的攻击属于不同层面，并且上述研究报道的出发点和落脚点也是在于改进和提升量子密钥分发系统的实际安全性，通常都会给出针对所提出的攻击方式的系统防御策略和解决方案，而非否定量子密钥分发技术的安全性；另一方面，针对量子密钥分发系统和网络现实安全性的学术研究在未来将会持续进行，从系统实现和实际应用层面而言，量子密钥分发系统和网络需要持续进行现实安全性研究、分析和测评验证。

3 量子保密通信的应用前景分析与展望

目前，学术界和产业界对于量子保密通信网络建设和产业发展的另一个关注点，是对于其技术成熟度、实用化水平和大规模组网应用的社会经济价值方面的讨论。本文结合对量子保密通信的技术产业调研、测评和标准化等方面的工作体会，总结主要观点和分析。

（1）量子密钥分发系统的性能指标和实用化水平仍有提升空间。目前，由于系统协议、关键器件和后处理算法等方面的限制，量子密钥分发系统在光纤现网的单跨段传输距离通常在百公里以内，密钥成码率约为数十kbit/s量级，系统传输能力和密钥成码率有待进一步提高。同时，量子密钥分发设备系统的工程化水平也有一定提升空间，例如偏振调制型设备在抗光纤线路扰动方面存在短板；单光子探测器需要低温制冷，对机房环境温度变化较为敏感；量子密钥分发系统的网管和运维等方面尚未完全成熟。此外，量子保密通信系统和网络需要密钥管理设备和加密通信设备进行联合组网，密钥管理设备属于信息安全领域，加密通信设备属于信息通信领域，目前量子保密通信业界与信息通信行业和信息安全行业的融合与协同配合还比较有限，设备产品工程化和标准化的提升和演进速度较慢。

（2）量子保密通信技术的应用发展还面临加密体制的技术路线竞争。量子保密通信的应用背景主要是面向未来量子计算对于现有公钥加密体系的计算破解威胁。一方面，量子计算的发展目前还处于多种技术路线探索的原理样机试验阶段，尽管近年来发展加速，但是距离实现真正具备破解密码体系的大规模通用量子计算能力仍有很长的距离；另一方面，信息安全行业也在为应对量子计算可能带来的安全性威胁进行积极准备，目前以美国国家标准与技术研究院（NIST）主导的抗量子计算破解的新型加密体系和算法的征集和评比已经完成第一轮筛选，计划在2023年左右完成3轮公开评选，并推出新型加密体制标准，我国上海交大、复旦大学和中科院等单位提交的新型加密方案也参与其中。未来，抗量子计算破解的安全加密体制存在量子密钥分发和后量子安全加密的技术路线竞争。加快提升量子密钥分发技术和设备成熟度、实用化水平和性价比，是赢得加密技术体制竞争的关键。

（3）量子保密通信的商业化应用和市场开拓仍需进一步探索。量子保密通信是对现有的保密通信技术中的对称加密体系的一种安全性提升，能够解决密钥分发部分的安全性问题，提升对称加密通信的安全性水平，但并不能完全解决信息网络中面临的所有安全性问题。量子保密通信主要适用于具有长期性和高安全性需求的保密通信应用场景，例如政务、金融专网以及电力等关键基础设施网络等，其产业规模和市场容量相对有限。我国量子保密通信产业化始于2009年，至今发展已有10年，产业规模仍然较为有限，并且主要依靠国家和地方政府的支持和投入。量子保密通信

技术的商业化应用推广和市场化发展仍然面临技术成熟度、设备可靠性和投入产出性价比等方面的考验，需要产学研用各方共同努力，从设备升级、产业链建设、标准完善和市场探索等多方面进行推动。

4 量子保密通信技术产业发展策略建议

（1）明确概念提法，凝聚各方共识形成合力

量子通信主要包括量子隐形传态和量子密钥分发两类，量子隐形传态是未来量子通信基础性研究的重点和重要发展方向，但是目前距离实用化仍有距离。目前，国内部分媒体所宣传的量子通信实际上只是基于量子密钥分发的量子保密通信。将量子通信和量子保密通信的概念混为一谈，会带来不必要的争议，对于凝聚各方共识，形成合力，推动技术产业发展而言并无益处。同时，量子密钥分发和量子保密通信技术的信息论可证明安全性属于理论层面，在实际系统实现、长距离组网和加密应用等层面无法满足部分媒体所宣传的“绝对安全”，通过炒作大而无当的“绝对安全”概念来推广量子保密通信的做法会引起不必要的反弹和争议，对技术研究和应用推广产生消极负面影响，实则对量子保密通信产业发展有害。明确量子通信和量子保密通信的概念提法，厘清理论安全性与现实安全性的区分界限，有助于凝聚产学研用各方共识，形成推动技术演进、应用推广和产业发展的共识与合力。

（2）加强基础研究，提升工程化实用化水平

我国面临的信息安全形势错综复杂，在政务、金融、外交、国防和关键基础设施等领域，提高信息安全保障能力的需求较为紧迫，对量子保密通信技术带来的长期信息安全保障能力有客观需求和应用前景。同时，量子保密通信技术的产业应用和市场化推广，也需要其自身技术成熟度、设备实用化、现实安全性和可靠性水平的不断提升，以满足规模化现网应用部署和运维管理的要求和条件。针对量子保密通信系统设备的工程化和实用化的关键瓶颈开展基础性共性技术，例如高性能单光子探测器、集成化调制解调器和高性能后处理算法等领域的攻关突破，将政策支持的优势真正转化为核心技术和产品功能与性能的优势，进一步强化关键技术创新和可持续发展能力，是我国量子保密通信技术发展演进和产业做大做强的关键所在。

（3）重视标准测评，引导应用产业健康发展

标准是引导和规范产业发展的重要工具，标准化也是新兴技术在应用和产业发展成熟过程中的必经之路。我国量子保密通信技术研究和应用发展具备良好的实践基础，目前在ITU-T和ISO/IEC等国际标准组织，以及CCSA和密标委等国家和行业标准组织中，已经开始推动量子密钥分发和量子保密通信的标准化研究工作。通过标准规范研究，能够有效保证量子保密通信设备系统的功能与性能一致性、可靠性和互操作性，以及设备系统和网络层面的现实安全性。加强测试评价与认证体系建设，能够为用户提供高实用化水平和安全可靠的量子保密通信系统、网络和应用解决方案，为行业和专网用户的规模化应用部署提供客观中立的技术验证和选型参考，促进量子保密通信商业化应用推广、产业链发展壮大以及产业化健康发展。

参考文献

[1] 赖俊森, 吴冰冰, 李少晖, 等. 量子保密通信研究进展与安全性分析 [J]. 电信科学, 2015, 31(6): 39-45.

[2] 赖俊森, 吴冰冰, 汤瑞, 等. 量子通信应用现状及发展分析 [J].电信科学, 2016, 32(3): 123-129.

[3] 赖俊森, 吴冰冰, 汤瑞, 等. 量子保密通信标准化现状与发展分析 [J]. 电信科学, 2018, 34(1): 1-7.

[4] Qian, Y.-J., et al. Hacking the quantum key distribution system by exploiting the avalanche- transition region of single- photon detectors[J]. Physical Review Applied, 2018. 10(6): 064062.

[5] Pang, X.-L., et al. Hacking quantum key distribution via injection locking. arXiv:1902.10423v2.

作者简介：

赖俊森 中国信息通信研究院技术与标准研究所宽带网络研究部高级工程师

刘 璐 中国信息通信研究院技术与标准研究所宽带网络研究部工程师

吴冰冰 中国信息通信研究院技术与标准研究所宽带

网络研究部高级工程师
赵文玉 中国信息通信研究院技术与标准研究所宽带网络研究部主任，高级工程师
张海懿 中国信息通信研究院技术与标准研究所副所长，高级工程师

Analysis on the security and prospect of quantum secure communication

LAI Junsen, LIU Lu, WU Bingbing, ZHAO Wenyu, ZHANG Haiyi

Abstract: Quantum secure communication (QSC) based on quantum key distribution (QKD) is one of the promising solutions for improving the network information security in the future. In last decade, frontier research, demonstrational application, and network construction of QSC have developed rapidly, the level of industrialization has been determined improved. Recently, the practical security issues of QSC system and network have caused widespread concern and discussion in academia, industry and public opinion. In this paper, the practical security issues of QSC systems and networks are analyzed, the prospects of QSC application and relevant strategies are discussed.

Key words: quantum key distribution; quantum secure communication; practical security; development prospects

（收稿日期：2019-08-25）

罗德与施瓦茨助力爱立信实现开创性的基于无人机的5G覆盖和性能验证

近日，罗德与施瓦茨公司向爱立信公司提供移动网络测试解决方案，基于无人机测试5G网络的覆盖范围、性能和运行情况。这一独特的方式能让测试获得前所未有的3D接入性、位置准确性和可重复性。它还提供了新的可能性，来确保要求严苛的5G用例中的终端用户服务质量（QoS），例如工业4.0、汽车和公共安全。

5G新空口（NR）的部署为用户、政府和行业带来了基于蜂窝网络的新应用。在这一过程中，对网络的正确覆盖范围、性能和运行的验证变得更加重要，从而提高了对传统现场网络测试中准确性和接入性的要求。由爱立信5G Readiness Program RAN技术负责人Richard Wirén领导的项目团队（位于芬兰Jorvas），与芬兰北中部应用科技大学（Centria University of Applied Sciences）共同开发了一种新型系统，用于测试蜂窝移动网络的覆盖范围。新的系统将罗德与施瓦茨的移动网络测试扫频仪和智能手机安装在无人机上，通过对无人机进行编程来进行非常灵活的自动测试，例如可以实现精确的路线选择和无人机速度控制。该解决方案对于工业用例特别有价值。与传统的步行和车载测试相比，它还拥有额外的优势：具有前所未有的可重复性和位置准确性，能够验证波束赋形和3D地图覆盖情况。

爱立信5G Readiness Program RAN技术负责人Richard Wirén说："兑现5G承诺，关键在于对网络的运行和质量进行现场验证，这个系统的开发是确保我们客户获得其所需网络性能的开创性方法。我们很高兴使用罗德与施瓦茨公司提供的测试解决方案，其可靠性已得到验证，并且很高兴我们现在可以使用基于商用5G NR终端的解决方案，例如三星S10 5G。"

罗德与施瓦茨公司的移动网络测试副总裁Hanspeter Bobst说："我们很高兴将行业领先的移动网络测试技术与爱立信悠久的网络创新传统相结合，以确保在5G NR迈向现实之际可以提供终端用户质量体验（QoE）。"