引用本文：赵永利，王亚子，刘宇航，等. 量子密钥分发网络国际标准研究进展[J]. 光通信技术，2025，49(5)：1-9.

量子密钥分发网络国际标准研究进展

赵永利，王亚子，刘宇航，郁小松
（北京邮电大学 信息光子学与光通信全国重点实验室，北京 100876）

摘要：为应对量子计算对传统密码体系的威胁并推动量子密钥分发（QKD）网络从实验走向规模化应用，系统梳理了国际QKD标准化组织在协议架构、安全评测与网络互联等方面的最新进展，分析了现有标准在设备无关安全性、跨域互操作性等方面的不足。研究总结了QKD技术在传输距离、成码率及集成化等方面的突破，提出了面向大规模组网的关键标准化路径，包括构建统一接口协议、强化跨组织协同、推进星地一体化标准建设等。最后，展望了QKD组网的未来布局。

关键词：量子密钥分发；标准；量子密钥分发网络
中图分类号：TN256　**文献标志码：**A　**文章编号：**1002-5561(2025)05-0001-09
DOI：10.13921/j.cnki.issn1002-5561.2025.05.001

Research progress on international standards for quantum key distribution networks

ZHAO Yongli, WANG Yazi, LIU Yuhang, YU Xiaosong
（State Key Laboratory of Information Optics and Optical Communications, Beijing University of Posts and Telecommunications, Beijing 100876, China）

Abstract: To address the threat posed by quantum computing to traditional cryptographic systems and to promote the transition of quantum key distribution (QKD) networks from experimental stages to large-scale applications, this paper systematically reviews the latest advancements in protocol architecture, security evaluation, and network interoperability by international QKD standardization bodies. It analyzes the shortcomings of existing standards in areas such as device-independent security and cross-domain interoperability. This paper summarizes breakthroughs in QKD technology regarding transmission distance, key generation rate, and integration, and proposes key standardization pathways for large-scale networking. These include developing unified interface protocols, enhancing cross-organizational collaboration, and advancing integrated space-ground standards development. Finally, the future landscape of QKD networking is outlined.

Key words: quantum key distribution, standard, quantum key distribution network

收稿日期：2025-07-17。
基金项目：国家自然科学基金项目（62350001、62425105、U22B2026、62021005）资助；科技创新重大项目（2021ZD0300701）资助。

作者简介：赵永利（1981—），男，教授，博士生导师，北京邮电大学发展规划处副处长（主持工作）、学术委员会办公室副主任（主持工作），信息光子学与光通信全国重点实验室副主任，通信与网络核心技术国家“111”创新引智基地主任，美国加州大学戴维斯分校访问学者，IET Fellow。国家杰出青年科学基金、国家优秀青年科学基金、中国通信学会青年科技奖获得者。先后主持和参加国家级科研项目20余项，获得国家科技进步二等奖1次，省部级科技奖励20余次。发表高水平期刊论文100余篇，出版学术专著10部，获得授权国家发明专利100余项，提交国际标准建议文稿100余篇。担任《光网络技术手册》主编、《光通信技术》编委。目前主要研究方向包括F5G/F6G、量子互联网、卫星激光组网等。

0 引言

量子计算技术的快速发展对基于计算复杂性的传统非对称密码体系构成了根本性威胁，亟需构建能够抵御量子攻击的新一代信息安全体系[1]。量子密钥分发（QKD）技术利用量子不可克隆原理和测量坍缩特性，在物理层面实现密钥分发的信息理论安全，为未来通信基础设施提供了重要的安全支撑[2]。尽管QKD在原理上具有抗量子计算攻击的潜力，其实际推广应用仍面临传输距离、密钥生成速率、设备成本及系统集成度等多重约束[3]。近年来，随着千公里级光纤传输、卫星量子通信及动态量子网络等关键技术的突破，QKD正从实验走向初步规模化应用，在此过程中，标准化建设成为推动技术成熟与产业互联的关键支撑[4]。

目前，国际主要标准化组织已积极布局QKD相关标准研制，形成了多层次、多方向的协同推进格局。欧洲电信标准化协会（ETSI）自2008年起系统推进QKD组件、协议和网络架构的标准化，并发布了信息安全技能竞赛（ISG）-QKD系列标准[5]；国际电信联盟（ITU-T）于2022年成立量子密钥分发网络联合协调活动（JCA-QKDN）协调组，聚焦天地一体化量子网络的安全机制[6]；国际标准化组织/国际电工委员会（ISO/IEC）则致力于构建一致的安全测试与评估标准，其第27分委会（SC27）工作组已开展QKD安全评测规范研究[7]。此外，国际电气与电子工程师协会（IEEE）、中国通信标准化协会（CCSA）等组织也分别从经典-量子信号共传、协议兼容性及行业应用等角度推进标准制定，共同促进QKD技术的实用化和国际化[8-9]。

然而，现有标准仍未能全面覆盖QKD系统在实际部署中面临的跨学科挑战和动态安全性问题，尤其在设备无关（DI）-QKD安全性认证、网络规模化扩展机制、混合量子-经典协议兼容性等方面尚存规范空白[10-11]。本文旨在系统分析国际QKD标准化现状与发展趋势，总结已有标准在技术要求和安全评测方面的进展与不足，并针对QKD系统互操作、安全验证体系及星地一体化集成等关键问题，提出适用于大规模量子网络应用的标准化路径与实施建议，以助推QKD技术从示范应用走向全面商业化部署。

1 技术研究与产业化进展

1.1 QKD理论研究进展

QKD作为量子密码学的核心应用，通过传输随机生成的候选密钥实现安全协商——该过程仅用于确认密钥安全性，不涉及实质信息传递。其理论起源可追溯至1969年WIESNER S提出的革命性构想：利用单量子态特性构建不可伪造的“量子钞票”。这一开创性理念在沉寂近20年后，于1984年经BENNETT C H与BRASSARD G的深入研究取得突破性进展，二人基于量子态信息传输原理正式提出BB84协议，标志着QKD技术范式的确立[5]。QKD的理论根基植根于量子力学基本原理，即海森堡不确定性原理与量子不可克隆定理：前者指出无法同时精确测量一对共轭物理量，后者表明未知量子态无法被精确复制[6-8]。这些原理保证了量子比特（qubit）的不可复制性，任何窃听行为都会扰动量子态，从而被通信双方检测[9]。

自BB84协议提出以来，QKD协议体系持续演进。EKERT A K[10]于1991年提出了基于Einstein-Podolsky-Rosen（EPR）纠缠粒子对的E91协议，其安全性依托于Bell不等式检验；同年，BENNETT C H团队[11]简化设计，提出了仅需2个非正交态的B92协议。随着技术发展，新一代协议如相干态连续变量（GG02）协议、测量设备无关（MDI）-QKD协议和双场（TF）-QKD协议相继问世，不仅在理论上具备可证明的安全性，也在实验中得到验证[12-13]。在此基础上，量子密钥分发逐渐分化为离散变量（DV）-QKD与连续变量（CV）-QKD两大技术路线。前者以单光子或弱相干光为信号源，通过偏振或相位编码实现比特信息传递；后者则基于量子态的振幅和相位进行高斯调制与解调。DV-QKD的代表性协议包括BB84、E91、B92、MDI-QKD及近年发展的TF-QKD，具备高容错和远距离传输能力，但对器件性能要求较高、系统集成难度较大。相比之下，CV-QKD以GG02协议为代表，采用相干态作为信号源，配合零差或外差检测器对连续变量进行测量，并通过协方差矩阵估计完成安全参数分析。CV-QKD天然兼容经典光通信系统，具备结构简单、频谱效率高、易于芯片集成等优势，近年来在短距离高密度网络和硅光子平台中展现出广泛应用潜力[14]。在具体实现方面，早期QKD系统依赖高性能单光子源与单光子探测器。受限于器件成熟度，现有系统多采用弱相干光源替代，但这类光源会引入光子数分离攻击的安全风险。为此，诱骗态协议与测量设备无关架构等方案被提出，通过提升系统抗干扰和抗侧信道攻击能力，显著增强了QKD的实用性和部署可行性。

QKD可通过自由空间和光纤2种信道实现，其中光纤凭借广泛覆盖和低损耗特性成为主流载体。为实现量子信号与经典光信号的共纤传输，波分复用与时分复用技术被广泛采用：早期实验使用O波段（1 260~1 360 nm）传输量子信号，C波段（1 530~1 565 nm）传输经典信号；后续研究逐步发展出C波段内的多信道复用方案，以提高频谱效率并缓解传输距离限制[15]。具体而言，量子信号通过量子信道与公共交互信道协同传输密钥参数，经典数据则经由经典数据信道独立传输。当前研究聚焦于多节点动态组网与跨介质传输优化，例如通过密集波分复用实现千公里级无中继传输，并结合卫星量子通信构建天地一体化量子网络，为全球量子安全通信奠定基础。

1.2 QKD产业化现状

随着QKD技术从理论走向实用，其产业化进程呈现出“科研突破—试点部署—生态构建”三者融合推进的发展态势。本文整理了量子密钥分发网络（QKDN）若干代表性案例，如表1所示。

表1 典型QKDN部署与性能成果

时间/发布主体	协议/技术类型	传输距离/km	成码率	特点/突破
2023/山西大学，中国	DV-QKD	80	2.11 Mb/s	改进型16-APSK调制
2023/中科大联合团队，中国	DV-QKD	10	115.8 Mb/s	单通道世界纪录
2023/中科大，中国	SNS-TF-QKD	1 002	0.003 4 b/s	突破PLOB极限，创最长距离记录
2023/北京量子院，中国	PMP-QKD	508	42.64 b/s	系统简化设计
2024/瑞士应用物理团队，瑞士	DV-QKD	10	64 Mb/s	多通道超导探测器并行读出
2021/意大利帕多瓦大学团队，意大利	集成硅光子平台	0.145	30 kb/s	自由空间，全天测试
2023/日内瓦大学+IDQ，瑞士	硅光子平台	200.2	1.3 kb/s	误码控制优化
2023/剑桥大学，英国	III-V材料+硅混合集成	50	1.82 Mb/s	双向通信，片上发射+接收
2023/Amazon Web Services，美国	CV-QKD	16	未公开	边缘计算集成VPN，AWS融合QKD
2023/中国电信，中国	DV-QKD	100.96	2.7 kb/s	共纤传输，支持1 Tb/s数据传输下量子成码
2023/IDQ，瑞士	CV-QKD	几十	未公开	与诺基亚合作，连接布鲁塞尔两数据中心
2023/LuxQuanta，中国	CV-QKD	城域	未公开	全球首款CV-QKD系统“NOVA LQ”
2024/Swisscom+Quantum Optics Jena，瑞士、德国	Entanglement-based QKD	未公开	未公开	采用纠缠光子对方案
2025/法国电信+Toshiba Europe，法国	QKD（基于硬件）+PQC（基于软件）	20~80	10~100 kb/s	QKD+PQC多层纵深防御

1.2.1 技术突破：从核心性能迈向工程可用性

QKD协议在理论优化与系统集成方面持续取得进展，推动技术不断向更远传输距离和更高成码率方向演进。CV-QKD凭借其中短距离高成码率的优势，主导城域量子通信应用；DV-QKD则通过协议与器件的持续优化，不断突破性能极限。山西大学[16]采用改进型16个星座点的幅度相位联合键控（16-APSK）调制，在80 km光纤链路中实现2.11 Mb/s的成码率；中国科大联合团队[17]基于诱骗态BB84协议，在10 km光纤链路中创下单通道115.8 Mb/s的世界纪录；瑞士应用物理研究[18]所则借助多通道超导纳米线（SNS）单光子探测器（PD）阵列，在同等距离实现了64 Mb/s的密钥率，标志着QKD技术正向高带宽、远距离应用场景迈进。TF-QKD凭借“双端制备-中心测量”架构突破点对点通信极限，中国科大团队[19]采用SNS-TF-QKD协议，在1 002 km光纤链路中实现0.003 4 b/s的成码率；北京量子信息科学研究院[20]提出开放式相位匹配协议（PMP）-QKD架构，在508 km光纤链路中实现42.64 b/s的成码率，显著降低了系统复杂度。

集成光学平台作为QKD系统硬件形态的重要演进方向，正逐步实现调制器、光源和探测器等核心元器件的片上集成。2021年，意大利帕多瓦大学团队[21]基于集成硅光子平台，研制出1 550 nm波长的自由空间QKD发射芯片，在145 m自由空间链路全天测试中实现30 kb/s密钥率；2023年，日内瓦大学联合IDQ团队[22]构建了基于硅光子芯片的高速QKD系统，在200.2 km光纤链路中实现1.3 kb/s密钥率，误码率控制在0.9%以内；剑桥大学[23]于同年提出一种混合集成QKD收发芯片，将III-V族材料高速电光调制器与硅光波导相融合，在50 km光纤链路中实现1.82 Mb/s密钥率，误码率低于1%，芯片面积仅为10 mm^2。

1.2.2 示范应用：产学研协同驱动落地进程

在关键性能持续提升的基础上，全球QKD系统已逐步进入试点部署与行业验证阶段。2023年，亚马逊量子网络中心在新加坡完成双节点量子安全网络部署，创新融合QKD与 亚马逊云服务（AWS）边缘计算硬件构建虚拟专用网络（VPN）隧道；中国电信团队突破少模光纤（FMF）传输瓶颈，实现100.96 km FMF与经典光通信共纤传输，在1 Tb/s经典带宽下密钥成码率达2.7 kb/s[24]。欧洲方面，瑞士IDQ联合诺基亚完成布鲁塞尔至梅赫伦数据中心间的量子密钥分发试验；西班牙LuxQuanta推出全球首款商用连续变量QKD系统“NOVA LQ”[25]。2024年，瑞士最大电信运营商Swisscom联合德国初创公司Quantum Optics Jena，在现网光纤环境中完成基于纠缠光子对的QKD系统验证测试[26]。该系统通过生成纠缠光子对，在Swisscom商用网络中实现稳定密钥交换。相比传统DV-QKD或CV-QKD，纠缠QKD在抗窃听能力方面具备天然物理安全性优势。2025年，法国电信运营商Orange Business联合东芝在巴黎正式推出“Orange Quantum Defender”量子安全网络服务，标志着法国首个QKD商用网络正式上线[27]。该系统采用东芝研发的高密钥速率

QKD技术，结合后量子密码（PQC）算法构建多层纵深防御架构，已接入法国多个金融企业核心站点。

1.2.3 标准化趋势：构建可持续发展生态

QKD产业链已形成“上游核心元器件—中游设备与网络解决方案—下游行业应用”的完整闭环。上游以光纤光缆、光学芯片及信号处理器为核心，我国烽火通信、亨通光电等企业已实现光纤光缆、传感器件等关键部件的自主可控；中游聚焦QKD终端与网络部署，国盾量子、问天量子等领军企业深耕量子终端研发，九州量子等新兴力量推动多节点组网技术突破；下游应用覆盖政务、金融等高安全需求领域，通过多协议兼容设计满足分级安全需求。国际方面，美国MagiQ、瑞士IDQ等企业持续引领量子随机数发生器、量子交换机等技术迭代；日本东芝与软银共建量子技术中心；韩国SK Broadband推出融合QKD与PQC的专线服务，全球产业链呈现出“技术突破—场景验证—商业落地”协同演进的态势。

随着QKD技术实用化进程加速，标准化建设与跨领域融合成为关键。未来技术将聚焦三大方向：一是提升远距离传输效率，结合波分复用技术优化量子-经典光信号共纤传输性能；二是深化多协议兼容性，推动QKD与PQC、IPSec等加密体系融合；三是完善全球化标准体系，依托ITU-T、ETSI等国际组织的主导作用，参考JCA-QKDN等跨组织协调机制，推动量子网络在体系架构、接口协议、互操作性和性能评估等方面形成国际共识。

1.3 QKDN部署案例

点对点QKD虽已取得显著进展，但其规模化应用仍需依赖网络化部署。自1994年TOWNSEND P团队提出基于无源光网络的多用户扩展方案以来，全球QKDN建设持续推进：1997年实现首个光学节点量子通信网络原型；2002年，美国国防高级研究计划局（DARPA）主导的量子网络部署了跨机构的10节点系统[28]；2008年，欧盟基于量子密码的安全通信（SECOQC）项目在维也纳整合多节点可信中继架构，完成远距离组网验证[29]；中国在该领域成果显著——2016-2019年间，“墨子号”量子科学实验卫星成功发射，京沪、沪杭等量子保密通信干线相继开通，广佛肇量子通信示范网创新融合高精度时间同步技术，成为粤港澳大湾区首条量子通信骨干网络。与此同时，全球多国积极建设QKD测试平台以验证其在真实环境中的性能：瑞士日内瓦SwissQuantum网络[30]、南非德班量子网络[31]及英国剑桥量子网络[32]通过可信中继技术实现了长期稳定运行与分析；日本与欧洲合作在东京建成跨国QKD试验网[33]；中国的芜湖城域量子通信网[34]及北京网通商用光纤骨干量子网络则为行业应用提供了重要验证场景。

随着量子信号与经典光信号共纤传输技术的突破，QKDN正逐步走向实用化。2017年，中国成功实现北京、济南、合肥、上海等城市超过2 000 km的量子链路连接，多家企业基于该基础设施推出专用QKD服务，为政府及企业关键数据提供了量子加密保障。相关技术标准与测试方法也在同步完善，覆盖密钥建立、资源分配、可信中继通信等核心流程。当前，全球量子通信网络正从技术验证阶段迈向与多行业深度融合的新时期。我国凭借政策支持与丰富的应用场景优势，正加速构建从核心器件、关键设备到组网应用的全产业链自主可控体系，为全球量子安全通信网络的发展提供了重要实践范式。

2 标准化组织与标准进展

2.1 ITU-T标准化进展

为推动QKD技术与信息通信技术（ICT）网络的深度融合，ITU-T建立了多层次、分阶段的标准化推进机制。2019年，ITU-T成立量子信息技术网络焦点组（FG-QIT4N），明确了QKD在广域组网和高安全性场景中的关键技术方向，有效促进了跨学科、跨组织的协同研究，其成果为后续标准体系的构建奠定了基础。

当前，QKD标准化工作主要由ITU-T的第11（SG11）、第13（SG13）和第17（SG17）研究组协同推进，分别聚焦于协议测试、网络架构与安全机制等关键领域。SG11负责Q系列建议书，重点开展协议设计、接口定义与互操作性测试，已牵头制定Q.4160－Q.4164等一系列QKDN接口标准；SG13通过Y系列建议书（如Y.3800《QKD网络基础概念》、Y.3801《功能需求》等）系统定义了QKDN的整体架构与功能模型；SG17则通过X系列建议书推进量子安全标准化，内容涵盖安全框架（X.1710）、密钥组合方法及量子噪声随机数生成器架构（X.1702）等关键技术。

为提升标准制定过程中的组织协同效率，ITU-T于2023年启动JCA-QKDN，作为其内部各研究组与外部标准组织（如ETSI、ISO/IEC、IEEE等）之间的协调枢纽。JCA-QKDN虽不直接制定标准，但通过机制化协作促进资源共享、进度同步与标准衔接，有力推动了全球QKDN标准体系的互认与一致性。

截至目前，研究团队在ITU-T已累计牵头制定16

项标准，并深度参与10项标准项目，内容覆盖QKDN互联互通、自主管控和生存性等多个方面，持续推动QKDN标准化进程的完善。图1为ITU-T SG13中QKDN相关标准的进展情况。其中，黄色高亮表示由本文作者研究团队（下文简称为团队）牵头制定的标准，绿色高亮表示团队参与制定的标准。

团队在ITU-T SG13框架下主导构建了QKDN标准体系，取得多项突破性成果。2019年，团队率先启动Y.3805《量子密钥分发网络——软件定义网络控制（SDNC）》[35]，首次建立分层SDN控制器架构与操作规范，实现量子网络控制模块的标准化。2021年，团队联合日本推动Y.3810《量子密钥分发网络互联互通框架》立项[36]，开创了多域互联标准体系，并配套发布Y.3813《互联互通功能需求》[37]与Y.3818《互联互通架构》标准[38]，系统解决了多运营商组网的技术壁垒，填补了多点组网标准的空白。

面向网络智能化发展需求，团队创新地将机器学习引入量子网络管理，于2020年主导制定Supplement 70《量子密钥分发网络机器学习用例》补充标准[39]，系统阐述了机器学习在量子层、密钥管理层及网络控制层的应用范式。2021年发布的Y.3814《机器学习功能需求与架构》标准[40]，构建了涵盖异常检测、资源优化等6大类共23项智能功能的QKDN智能运维体系。在自主运维方面，团队于2023年与韩国电子通信研究院（ETRI）联合推动Y.QKDN-qos-auto-rq标准立项，首次提出基于服务质量（QoS）闭环控制的自主管控模型。

在联邦架构与安全控制方面，团队主导完成了Y.3820《软件定义控制》[41]和Y.3824《联邦模型》[42]等核心标准的制定，突破了多厂商设备互操作的关键难

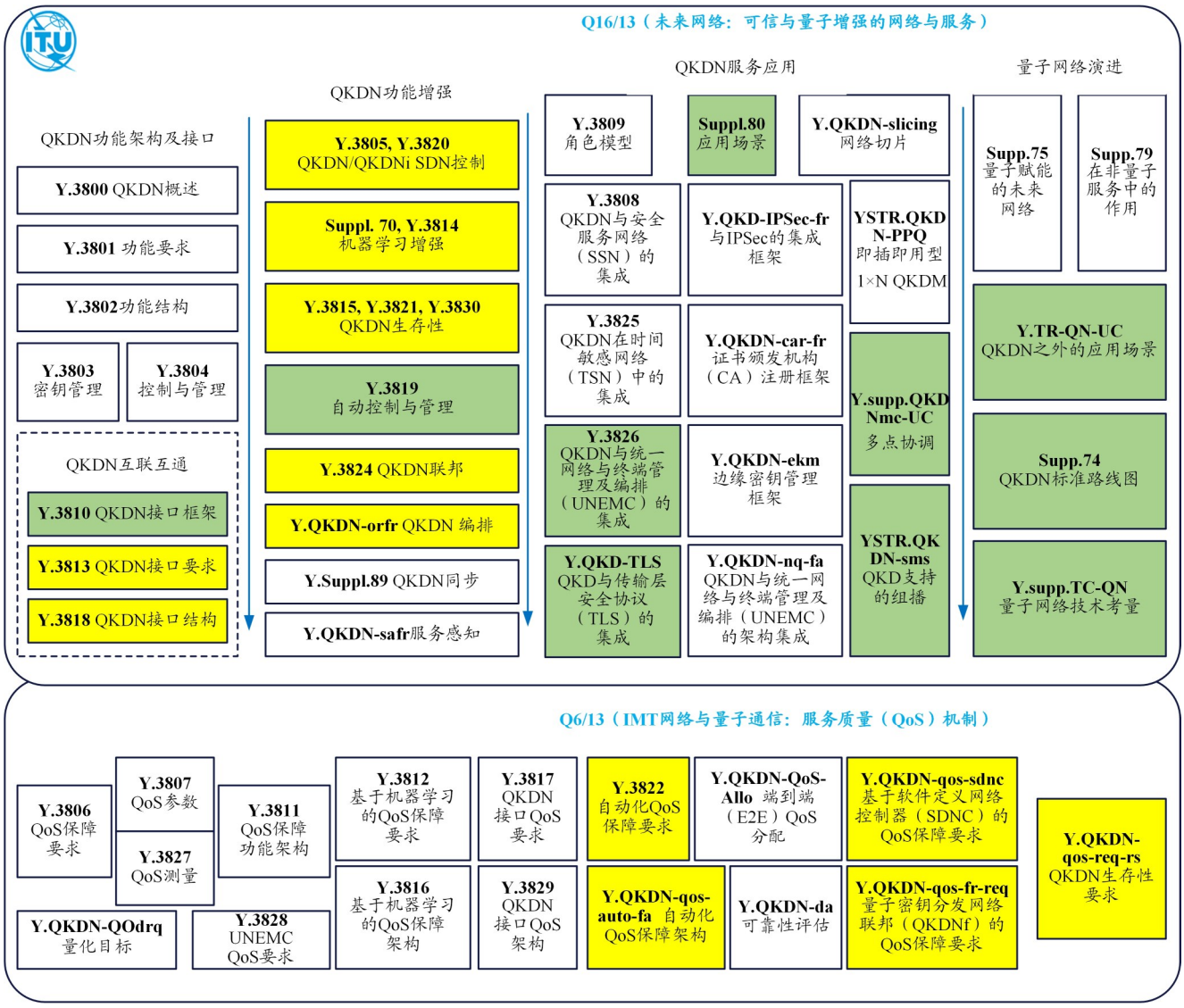

图1 ITU-T SG13 QKDN标准化进展

题。通过构建“基础架构-智能控制-跨域协同”三位一体的标准体系，不仅支撑了CCSA《软件定义量子密钥分发网络研究》技术白皮书的编写，也增强了我国在ITU-T SG13标准制定中的话语权。目前，相关研究成果已形成覆盖标准制定、设备研发与网络部署的完整技术链条，为我国量子通信产业化提供了关键支撑。

随着QKDN应用范围的扩展，网络在故障或异常情况下的持续稳定运行成为关键挑战。2023年，团队发布Y.3815《QKDN生存性概述》标准[43]，系统阐述了QKDN在面对网络故障、攻击或设备失效时的生存性保障模型；2024年发布的Y.3821《QKDN生存性功能需求》标准[44]，明确了多种故障场景下的功能要求；2025年7月通过的Y.3830《支持QKDN生存性保障的密钥供应保护与恢复流程》标准[45]，详细规定了量子密钥供应链的保护与恢复机制，标志着QKDN生存性标准体系的成熟。同期，团队还推动Y.QKDN-qos-req-rs《支持QoS保障的QKDN生存性需求》标准立项，进一步强化了面向业务实际服务质量需求的生存性标准建设。

未来，团队将继续深化与ITU-T SG13的合作，推动量子密钥分发网络与第六代移动通信（6G）、算力网络等前沿技术的融合，为构建安全可控的全球量子通信基础设施提供中国方案。

2.2 ETSI标准化进展

ETSI作为全球信息通信技术标准化的核心组织，通过其特有的“行业规范小组（ISG）”机制有效推动技术快速创新。ETSI汇聚了超过700家成员单位，包括企业、高校及研究机构，其标准制定过程遵循开放共识原则，所有成果均以免费开放形式公开发布。为平衡知识产权保护与技术共享，ETSI实施严格的知识产权（IPR）政策，要求核心专利在公平、合理和非歧视的条件下向所有成员开放。为适应ICT产业研发与标准化同步推进的需求，ETSI创新设立了ISG机制：仅需4家成员单位发起，即可成立专项工作组，在签署相关协议后迅速启动标准化进程。ISG面向全体成员及外部合作方开放，参与者需签署保密协议并遵守IPR管理规定。该机制最终产出为“组规范（GS）”，作为一种开放标准，为全球ICT产业提供统一的技术规范框架。

作为ETSI内首个专注于量子通信标准化的行业规范小组，ISG-QKD已建立起覆盖全产业链的技术标准体系。从基础性文件（如《词汇表组规范》GS QKD 002[46]）到核心技术规范（如密钥提取流程GS QKD 004[47]、安全协议验证GS QKD 011[48]），从安全攻防分析（《QKD安全实施白皮书》）到器件特性标准化（GS QKD 003[49]），该小组已累计发布20余项GS。当前，ISG-QKD的工作重点聚焦于支持大规模量子网络构建的扩展接口标准化，包括密钥供应接口（GS QKD 014[50]）与网络编排协议（GS QKD 018[51]），旨在突破从实验室验证到跨域规模组网的技术瓶颈。通过ISG这一高效机制，ETSI不仅加速了QKD技术从理论研究走向实际应用的进程，也为全球量子通信网络的建设提供了可扩展、可互操作的标准基础。

2.3 ISO/IEC标准化进展

ISO/IEC联合技术委员会（JTC1）下属的SC27工作组WG3“安全评估、测试与规范”专注于QKD系统的安全需求分析、测试方法及评估体系建设，致力于优化QKD设备的设计安全性与实施可靠性，并建立针对QKD模块的安全验证机制。该工作组在ISO/IEC框架下主导量子技术标准化工作，已发布2项核心标准以完善QKD系统安全评估与认证流程，同时负责制定并维护ISO/EN 15408《信息技术安全评估通用准则》，为QKD技术从研发到部署的全生命周期安全提供标准化支撑。

2.4 IEEE标准化进展

IEEE在量子通信标准化领域正推进2项关键标准：P1913标准工作组致力于提出基于YANG模型的动态管理框架，支持通信网络中量子协议与应用的灵活配置、修改及移除，其定义的QKD模块标准化接口可实时捕获设备收发器速率、QKD协议类型等关键参数，但需解决经典通信与量子技术协同演进的技术割裂风险，以及跨标准组织协调不足导致的互操作性冲突；另一项P7130标准聚焦量子技术专用术语定义，通过构建统一概念体系提升技术理解一致性，为多厂商系统互操作奠定基础。此外，P1913标准还创新性地定义了“软件定义量子通信（SDQC）”应用层协议，基于传输控制协议/网际协议（TCP/IP）架构实现对量子端点的动态配置能力，支持量子协议与应用模块的敏捷开发与迭代，进一步拓展了量子通信网络的灵活性与可扩展性。

2.5 CCSA标准化进展

CCSA作为国内信息通信技术领域的核心标准化组织，其下设的量子通信与信息技术特设任务组（ST7）自2017年成立以来，系统构建了覆盖QKD全链条的标准化研究体系，已成为推动我国QKD技术标准化的核心力量。ST7设立量子通信工作组（WG1）与量

子信息处理工作组（WG2），聚焦术语定义、应用场景、网络架构及设备技术要求等关键方向，系统性推进了25项标准研究项目[52-67]。这些项目涵盖国家标准《量子通信术语和定义》《量子保密通信应用场景和需求》，以及多项行业标准，包括QKD系统技术要求（含BB84协议实现规范）、测试方法与应用接口设计，并涉及量子保密通信网络架构优化和QKD安全性验证等15项前沿课题。通过系统性的标准化研究，ST7不仅完成了量子安全通信系统的测试与评估工作并发布多项成果，还积极联合密码标准化技术委员会（CSTC）及其他国家级机构，协同推进QKD技术的标准化进程，逐步构建起覆盖基础规范、技术验证与产业应用的完整标准体系。这为我国量子保密通信实验网络的建设和多厂商设备生态的健康发展奠定了坚实基础。

3 QKD组网技术挑战与未来布局

当前，QKD组网面临两大核心挑战：一是网络互操作性难题，需解决QKD与现有光纤基础设施的深度融合、密钥传输接口标准化，以及量子密钥与经典加密协议的集成问题。ETSI正主导网络层技术攻关，推动量子信号与传统光通信系统的共纤传输优化，但在实际部署中仍面临设备兼容性不足、密钥协商机制碎片化等问题。例如，不同厂商的量子交换机与经典路由器接口协议不兼容，导致组网时需额外部署中间转换设备，增加了系统复杂性与建设成本。此外，QKD终端与现有网络管理系统的数据交互缺乏统一规范，可能引发密钥调用延迟甚至失效的风险。二是网络安全认证挑战。尽管ITU-T SG17已推动QKDN安全性研究，面向多节点动态组网场景的端到端安全认证框架仍待完善。QKD密钥的安全能力边界也在持续拓展，其应用已从早期链路层点对点加密逐步延伸至更复杂、多样化的网络环境，包括云边协同、跨域连接以及面向移动用户的动态密钥服务等场景。2025年7月，韩国代表团在ITU-T SG13中提交《TR.QKDN-nq-ZTA》技术报告草案，提出将QKDN与基于信任增强机制的零信任架构深度融合，构建面向6G的量子安全网络体系，旨在突破传统QKDN在复杂网络中的信任边界限制，打造支持动态认证、信任可扩展和服务可组合的未来网络安全架构。

面向2025年之后的全量子互联网发展目标，QKD组网需构建支持量子计算机互联及量子信息直接传输的新型架构。这要求突破量子中继器的技术瓶颈，实现远距离量子态的无损传输与高效纠缠分发。当前，量子中继器受限于纠缠交换效率和噪声干扰，传输距离普遍低于百公里，亟需研发基于超导量子比特与光子集成芯片的新型中继方案。同时，应制定兼容经典网络协议的混合组网标准，例如将QKD密钥管理协议嵌入SDN架构，实现量子与经典网络资源的统一调度。卫星量子通信模块的标准化也日益迫切，包括光学地面站的性能参数（如单光子探测灵敏度、暗计数率）和卫星光终端接口协议（如编码格式与调制方式）等。例如，低轨卫星组网需解决星间量子信道动态切换时的密钥同步问题，而高轨卫星量子中继则需攻克星地链路时延补偿与多普勒频移校正技术，这些均需通过产学研协同以加速技术转化与生态构建。

在标准化战略层面，应优先完善基础性规范体系，包括制定统一的QKD设备性能指标（如ITU-T Y.3827）、密钥管理协议（如基于BB84的密钥协商流程）及网络控制接口标准（如ETSI GS QKD 018）。ETSI、ITU-T等国际组织应加强协作，推动量子网络架构、密钥传输效率优化等关键技术的全球共识，例如联合制定《量子密钥分发网络互操作性框架》，明确设备接入认证与密钥路由策略等核心规范。同时，建立跨平台互操作性测试框架，开发自动化测试工具链，覆盖量子态制备、传输与测量全流程，为多厂商设备接入提供技术保障。欧洲OPENQKD项目已构建多厂商QKD设备测试床，验证了BB84与E91协议在城域网中的互操作性，此类实践可为标准化进程提供重要参考。

未来布局还需聚焦卫星量子通信网络的标准化建设，重点突破低轨卫星群组网、星地量子信号无缝切换等技术难点。例如，通过部署分布式低轨卫星星座构建全球量子通信网络，需解决卫星轨道参数优化与星间量子链路快速建立等挑战。同时，应推动“量子-经典”混合网络架构的标准化，实现QKD与经典数据传输之间的带宽动态分配。通过与国际伙伴合作开展“OPENQKD”类示范项目，如在金融领域构建跨境量子保密通信专网，在政务领域建立跨部门量子安全云平台，可加速QKD技术在金融、政务等高安全需求领域的规模化应用。此外，应探索量子区块链融合路径，将QKD与分布式账本技术结合，增强数据溯源与防篡改能力。最终，通过构建天地协同的量子通信网络体系，为全球量子互联网发展奠定基础，推动量子技术在数字经济与国家安全等领域的深度应用。

4 结束语

本文系统梳理了QKD领域的技术研发与产业化

进程，聚焦于产业链各核心环节。作为支撑未来产业升级与网络演进的关键基石，标准化体系已成为推动量子通信乃至整体量子网络技术革新的核心驱动力，国际和国内层面均在加速完善相关技术标准的布局。然而，当前量子信息领域的标准体系仍面临覆盖不全面、跨组织协同不足等突出问题，难以适应技术快速迭代和规模化应用的迫切需求。

针对这一现状，本文系统分析了QKD组网面临的主要技术挑战，并据此提出面向未来的发展路径与重点布局方向，旨在为我国量子通信技术的标准化工作提供系统性解决方案，从而助力实现从关键技术突破到产业生态全面落地的跨越式发展。

参考文献：

[1] LADD T D, JELEZKO F, LAFLAMME R, et al. Quantum computers [J]. Nature, 2010, 464(7285): 45−53.

[2] GISIN N, THEW R. Quantum communication[J]. Nature Photonics, 2007, 1(3): 165−171.

[3] LÄNGER T, LENHART G. Standardization of quantum key distribution and the ETSI standardization initiative ISG-QKD[J]. New Journal of Physics, 2009, 11(5): 055051-1−055051-16.

[4] CHEN Y A, ZHANG Q, CHEN T Y, et al. An integrated space-to-ground quantum communication network over 4, 600 kilometres[J]. Nature, 2021, 589(7841): 214−219.

[5] BENNETT C H, BRASSARD G. Quantum cryptography: public key distribution and coin tossing[C]//IEEE. Proceedings of the IEEE International Conference on Computers, Systems and Signal Processing. New York: IEEE, 1984: 175−179.

[6] DIRAC P A M. The principles of quantum mechanics: number 27[M]. Oxford: Oxford university press, 1981.

[7] HEISENBERG W. Über den anschaulichen inhalt der quantentheoretischen kinematik und mechanik[M]. Berlin: Springer, 1985: 478−504.

[8] WOOTTERS W K, ZUREK W H. A single quantum cannot be cloned [J]. Nature, 1982, 299(5886): 802−803.

[9] 张春辉. 新型量子密码的方案设计与实验验证[D]. 南京：南京邮电大学，2021.

[10] EKERT A K. Quantum cryptography based on Bell's theorem[J]. Physical Review Letters, 1991, 67(6): 661−663.

[11] BENNETT C H. Quantum cryptography using any two nonorthogonal states[J]. Physical review letters, 1992, 68(21): 3121−3124.

[12] LUCAMARINI M, YUAN Z L, DYNES J F, et al. Overcoming the rate − distance limit of quantum key distribution without quantum repeaters[J]. Nature, 2018, 557(7705): 400−403.

[13] WANG W, XU F, LO H K. Asymmetric protocols for scalable high-rate measurement-device-independent quantum key distribution networks [J]. Physical Review X, 2019, 9(4): 041012-1−041012-30.

[14] ZHANG Y, BIAN Y, LI Z, YU S, GUO H. Continuous-variable quantum key distribution system: past, present, and future[J]. Applied Physics Reviews, 2024, 11(1): 011318-1−011318-54.

[15] BAHRAMI A, LORD A, SPILLER T. Quantum key distribution integration with optical dense wavelength division multiplexing: a review[J]. IET Quantum Communication, 2020, 1(1): 9−15.

[16] TIAN Y, ZHANG Y, LIU S, et al. High-performance long-distance discrete-modulation continuous-variable quantum key distribution[J]. Optics Letters, 2023, 48(11): 2953−2956.

[17] LI W, ZHANG L, TAN H, et al. High-rate quantum key distribution exceeding 110 Mb/s[J]. Nature Photonics, 2023, 17(5): 416−421.

[18] HAJOMER A A E, BRUYNSTEEN C, DERKACH I, et al. Continuous-variable quantum key distribution at 10 gbaud using an integrated photonic-electronic receiver[J]. Optica, 2024, 11(9): 1197−1204.

[19] LIU Y, ZHANG W J, JIANG C, et al. Experimental twin-field quantum key distribution over 1000 km fiber distance[J]. Physical Review Letters, 2023, 130(21): 210801-1−210801-6.

[20] ZHOU L, LIN J, XIE Y M, et al. Experimental quantum communication overcomes the rate-loss limit without global phase tracking[J]. Physical Review Letters, 2023, 130(25): 250801-1−250801-7.

[21] AVESANI M, CALDERARO L, SCHIAVON M, et al. Full daylight quantum-key-distribution at 1550 nm enabled by integrated silicon photonics[J]. NPJ Quantum Information, 2021, 7(1): 93-1−93-8.

[22] SAX R, BOARON A, BOSO G, et al. High-speed integrated QKD system[J]. Photonics Research, 2023, 11(6): 1007−1014.

[23] DOLPHIN J A, PARAÏSO T K, DU H, et al. A hybrid integrated quantum key distribution transceiver chip[J]. NPJ Quantum Information, 2023, 9(1): 84-1−84-8.

[24] DOU T, GAO S, ZHANG C L, et al. Coexistence of 1 Tbps classical optical communication and quantum key distribution over a 100.96 km few-mode fiber[J]. Optics Letters, 2023, 48: 4905−4908.

[25] IDQ. SK Telecom and Samsung unveil the galaxy quantum 4, providing more safety and performance with IDQ's QRNG chip [DB/OL]. (2023−06−12) [2025−07−17]. https://www. idquantique. com/sk-telecom-and-samsung-unveil-the-galaxy-quantum-4/.

[26] Swisscom und deutsches start-up testen quantum-security-lösung mit verschränkten Photonen [DB/OL]. (2024−04−17) [2025−07−17]. https://www. heise. de/news/Swisscom-und-deutsches-Start-up-testen-Quantum-Security-Loesung-10291699.html.

[27] Toshiba Europe. Toshiba and orange business launch France's first commercial quantum-secure network service [DB/OL]. (2025−06−11) [2025−07−17].https://www.toshiba.eu/quantum/news/toshiba-orange-launch-commercial-quantum-network/.

[28] ELLIOTT C. Building the quantumnetwork[J]. New Journal of Physics, 2002, 4(1): 46-1−46-12.

[29] PEEV M, PACHER C, ALLÉAUME R, et al. The SECOQC quantum key distribution network in Vienna[J]. New Journal of Physics, 2009, 11(7): 075001-1−075001-37.

[30] STUCKI D, LEGRE M, BUNTSCHU F, et al. Long-term performance of the SwissQuantum quantum key distribution network in a field environment[J]. New Journal of Physics, 2011, 13(12): 123001-1−123001-18.

[31] MIRZA A, PETRUCCIONE F. Realizing long-term quantum cryptog-

raphy[J]. Journal of the Optical Society of America B, 2010, 27(6): A185-A188.
[32] YUAN Z L, SHIELDS A J. Continuous operation of a one-way quantum key distribution system over installed telecom fibre[J]. Optics Express, 2005, 13(2): 660−665.
[33] SASAKI M, FUJIWARA M, ISHIZUKA H, et al. Field test of quantum key distribution in the Tokyo QKD Network[J]. Optics Express, 2011, 19(11): 10387−10409.
[34] XU F X, CHEN W, WANG S, et al. Field experiment on a robust hierarchical metropolitan quantum cryptography network[J]. Chinese Science Bulletin, 2009, 54(17): 2991−2997.
[35] ITU-T. QKDNs-software defined networking control: Y. 3805[S]. Genève: ITU-T, 2021.
[36] ITU-T. QKDN interworking-framework: Y.3810[S]. Genève: ITU-T, 2022.
[37] ITU-T. QKDN interworking-functional requirements: Y. 3813[S]. Genève: ITU-T, 2023.
[38] ITU-T. QKDN interworking-architecture: Y.3818 [S]. Genève: ITU-T, 2024.
[39] ITU-T. QKDNs-Applications of machine learning: Y Suppl. 70[S]. Genève: ITU-T, 2021.
[40] ITU-T. QKDNs-Functional requirements and architecture for ML enablement: Y.3814[S]. Genève: ITU-T, 2023.
[41] ITU-T. QKDN interworking-software defined networking control: Y.3820[S]. Genève: ITU-T, 2024.
[42] ITU-T. QKDN federation-reference models: Y.3824[S]. Genève: ITU-T, 2024.
[43] ITU-T. QKDNs-overview of resilience: Y. 3815[S]. Genève: ITU-T, 2023.
[44] ITU-T. QKDNs-requirements for resilience: Y.3821[S]. Genève: ITU-T, 2024.
[45] ITU-T. QKDNs-procedures for key supply protection and recovery for resilience: Y.3830[S]. Genève: ITU-T, 2025.
[46] ETSI. QKD-Use Cases: GS QKD 002 V1.1.1[S]. Sophia Antipolis: ETSI, 2010.
[47] ETSI. QKD-application interface: GS QKD 004 V2.1.1[S]. Sophia Antipolis: ETSI, 2010.
[48] ETSI. QKD-component characterization: characterizing optical components for QKD Systems: GS QKD 011 V1.1.1[S]. Sophia Antipolis: ETSI, 2016.
[49] ETSI. QKD-components and internal interfaces: GS QKD 003 V2.1.1 [S]. Sophia Antipolis: ETSI, 2018.
[50] ETSI. QKD-protocol and data format of REST based key delivery API: GS QKD 014 V1.1.1[S]. Sophia Antipolis: ETSI, 2019.
[51] ETSI. QKD-orchestration interface for software defined networks: GS QKD 018 V1.1.1 [S]. Sophia Antipolis: ETSI, 2022.
[52] CCSA. 量子密钥分发（QKD）系统技术要求第1部分：基于诱骗态BB84协议的QKD系统：YD/T 3834.1 2021[S]. 北京：CCSA，2021.
[53] CCSA. 量子密钥分发（QKD）系统测试方法第1部分：基于诱骗态BB84协议的QKD系统：YD/T 3835.1 2021[S]. 北京：CCSA，2021.
[54] CCSA. 基于BB84协议的量子密钥分发（QKD）用关键器件和模块第3部分：量子随机数发生器（QRNG）：YD/T 3907.3 2021[S]. 北京：CCSA，2021.
[55] CCSA. 基于BB84协议的量子密钥分发（QKD）用关键器件和模块第1部分：光源：YD/T 3907.1 2022[S]. 北京：CCSA，2022.
[56] CCSA. 量子保密通信网络架构：YD/T 4301 2023[S]. 北京：CCSA，2023.
[57] CCSA. 量子密钥分发（QKD）网络管理技术要求第1部分：网络管理系统（NMS）功能：YD/T 4302.1 2023[S]. 北京：CCSA，2023.
[58] CCSA. 基于IPSec协议的量子保密通信网设备技术规范：YD/T 4303 2023[S]. 北京：CCSA，2023.
[59] CCSA. 量子密钥分发（QKD）系统技术要求第2部分：基于高斯调制相干态协议的QKD系统：YD/T 3834.2 2023[S]. 北京：CCSA，2023.
[60] CCSA. 量子密钥分发（QKD）系统测试方法第2部分：基于高斯调制相干态协议的QKD系统：YD/T 3835.2 2023[S]. 北京：CCSA，2023.
[61] CCSA. 量子密钥分发（QKD）网络Ak接口技术要求第1部分：应用程序接口（API）：YD/T 4410.1 2023[S]. 北京：CCSA，2023.
[62] CCSA. 量子密钥分发与经典光通信共纤传输技术要求：YD/T 4632 2023[S]. 北京：CCSA，2023.
[63] CCSA. 量子密钥分发（QKD）设备安全要求第1部分：基于诱骗态BB84协议的QKD设备：YD/T 6059.1 2024[S]. 北京：CCSA，2024.
[64] CCSA. 基于传输层密码协议的量子保密通信应用设备技术规范：YD/T 6265 2024[S]. 北京：CCSA，2024.
[65] CCSA. 量子密钥分发（QKD）网络安全技术要求：YD/T 6309 2024 [S]. 北京：CCSA，2024.
[66] CCSA. 量子保密通信应用基本要求：GB/T 42829 2023 [S]. 北京：CCSA，2023.
[67] CCSA. 量子通信术语和定义：GB/T 43692 2024 [S]. 北京：CCSA，2024.