CAICT 中国信通院

No.202127

量子信息技术发展与应用研究报告

中国信息通信研究院

2021年12月

版权声明

前　言

以量子计算、量子通信和量子测量为代表的量子信息技术可能引发信息技术体系的颠覆性创新与重构，并诞生改变游戏规则的变革性应用，从而推动信息通信技术换代演进和数字经济产业突破发展。2020 年 10 月，习近平总书记在中央政治局第二十四次专题集体学习中，做出把握量子科技大趋势，下好先手棋的系列重要指示，为加快促进我国量子信息技术领域发展提供了战略指引和根本遵循。2021 年 3 月，“十四五”规划正式发布，明确提出量子信息领域组建国家实验室，实施重大科技项目，谋划布局未来产业，加强基础学科交叉创新等一系列规划部署。

近年来，量子计算、量子通信和量子测量三大领域科研探索和技术创新持续活跃，代表性研究成果亮点纷呈，应用场景探索广泛开展，产业生态培育方兴未艾。我国量子信息技术领域具备良好的研究与应用实践基础，三大领域总体发展态势良好，未来有望进一步取得更多技术研究、应用探索与产业培育新成果。

中国信息通信研究院连续三年发布《量子信息技术发展与应用研究报告》，得到主管部门和业内专家广泛认可。为对量子信息技术总体发展态势、三大领域研究与应用进展情况和热点问题，及技术演进和应用前景等进行持续跟踪研判，我们组织研究编写了 2021 年版《量子信息技术发展与应用研究报告》，供业界参考。

目 录

图 目 录

表 目 录

一、量子信息技术总体发展态势

（一）量子科技突破经典极限，打开未来科学新疆域

量子是近原子尺度的微观粒子系统，如光子、电子、离子等，及粒子中蕴含的各类物理量，如自旋、能级等，不可分割的最小单位。量子力学研究和刻画微观粒子系统的结构、性质及其相互作用，与信息论共同奠定了信息获取、处理和传输技术发展与应用的物理和理论基础，成为连接物质、能量和信息三大基本要素的桥梁与纽带，也是推动人类社会从工业时代跨入信息时代的关键使能者。

随着数十年来信息通信技术的飞速发展，经典信息技术的极限和边界，如摩尔定律晶体管制程工艺极限，通信信道香农容量极限和光学测量成像衍射极限等，正被不断逼近并逐步成为未来进一步提升信息运算处理能力、组网传输效率和传感测量精度的重大挑战。虽然技术和工程领域的不断创新仍将推动信息通信技术持续演进，但可带来技术体系重构和极限边界突破的划时代变革，可能需要藉由物理基础和信息理论基础的重大创新才能实现。

量子调控技术，如激光原子冷却、离子阱囚禁和单光子探测等，通过对微观粒子系统的精确操控与观测，为开发和利用量子力学中的叠加态、纠缠态和压缩态等独特物理现象，提供前所未有的新颖物理基础，有望引发颠覆性创新和改变游戏规则的技术应用。量子调控技术赋能信息通信，诞生了以量子计算、量子通信和量子测量为代表的量子信息技术，将成为突破经典信息技术极限，拓展未来科学技术新疆域，推动信息技术和数字经济发展演进的新动能。

量子计算以量子比特为基本单元，利用量子叠加和干涉等原理实现并行计算，能在某些计算困难问题上提供指数级加速，是未来计算能力跨越式发展的重要方向。近年来量子计算科研创新活跃，“悬铃木”“九章”“祖冲之”等原理样机和实验平台，在量子计算优越性实验验证中不断取得突破性成果；IBM、Google 等科技巨头大力推动量子计算软件算法、编译工具和测控系统等软硬件研发；众多初创企业和行业巨头广泛开展量子计算解决实用化问题的应用场景探索；量子计算云平台、软件开源社区、企业联盟组织和竞赛培训推广等应用产业活动兴起；量子计算领域正在形成集科研攻关、工程研发、应用探索和产业生态构建为一体的全方位发展格局。

量子通信利用量子叠加态或纠缠效应，在经典通信辅助下进行量子态信息传输或密钥分发，理论协议层面具有信息论可证明安全性，部分协议可实现经典信息传输。量子通信包括多种协议与应用类型：基于量子隐形传态与量子存储中继等技术，可实现量子态信息传输，进而构建量子信息网络，已成为当前科研热点，但距实用化仍然较远；基于量子密钥分发和对称加密算法的量子保密通信技术初步实用化，在商用设备、实验网络和示范应用等方面取得一定进展，但技术产品工程化水平仍待提升，融合应用场景有待进一步探索；量子安全直接通信近年在样机研发和组网实验方面取得一定进展，但实用化水平仍较为有限；其他协议与应用主要处于学术研究阶段。

量子测量对外界物理量变化导致的微观粒子系统量子态变化进行调控和观测，实现精密传感测量，在精度、灵敏度和稳定性等方面相较传统技术带来数量级提升。主要技术方案包括冷原子干涉测量、

核磁/顺磁共振测量、原子自旋测量、纠缠态/压缩态测量和量子增强测量等。主要发展方向涉及新一代定位/导航/授时的光学原子钟、光学时频传输系统、原子陀螺仪与重力仪等，以及高灵敏度检测与目标识别的光学量子雷达、物质痕量检测、磁场精密测量等。主要应用场景涵盖航空航天、防务装备、地质资源勘测、基础科研和生物医疗等众多领域，应用与产业发展前景广阔。

（二）量子信息技术成为全球各国科技政策布局热点

以量子计算、量子通信和量子测量为代表的量子信息技术已成为未来基础科学研究探索和信息技术产业升级的重点发展方向之一，同时还将在网络信息安全保障、防务技术装备升级和资源勘探开发利用等涉及国家经济和安全的重要领域引发深刻变革。持续加强量子信息领域科研规划与布局投入，掌握关键核心技术，促进应用探索和产业培育，成为全球各主要国家在科技政策领域的关注焦点和普遍共识。近年来，全球各国量子信息领域项目规划布局与投资的情况如表 1 所示，据不完全统计投资总规模已超 130 亿美元[1]。

表 1 近年全球量子信息领域项目规划布局与投资情况[2]

国家	时间	项目/规划	布局方向与要点	金额(亿美元)
英国	2015	国家量子技术计划（一期）	建立量子通信/传感/成像/计算 4 个研发中心	5.24
欧盟	2016	量子旗舰计划	24 国参与，2018 年启动 4 领域 19 个科研项目	11.12
加拿大	2016	——	资助 4 个量子研究中心和 QEYSSat 任务等	1.49
澳大利亚	2017	——	资助 4 个量子研究机构和硅量子计算项目等	1.03
美国	2018	国家量子行动（NQI）立法	设立国家量子协调办，NSF/DoE/NIST 等组织实施	12.75
德国	2018	量子技术-从基础到市场	计算/通信/测量/基础 4 大方向，6 方面推动措施	7.23

[1] https://cifar.ca/wp-content/uploads/2021/05/QuantumReport-EN-May2021.pdf
https://www.qureca.com/overview-on-quantum-initiatives-worldwide-update-mid-2021

[2] 投资金额据公开报道，以美元计价，汇率波动可能导致具体数值变化。

国家	时间	项目/规划	布局方向与要点	金额(亿美元)
日本	2018	光 量子跃迁(Q-LEAP)计划	量子信息处理、量子模拟器和量子计算机等	2.76
英国	2019	国家量子技术计划（二期）	第二阶段拨款，增设国家量子计算中心	4.87
韩国	2019	量子计算技术开发项目	量子计算机硬件、新架构、量子算法和基础软件	3.98
荷兰	2019	量子技术发展国家计划	量子计算/模拟、国家量子网络、量子传感应用	8.68
俄罗斯	2019	量子技术基础与应用研究	量子计算/模拟、量子通信、量子传感、使能技术	6.92
印度	2020	国家量子技术和应用任务	量子计算、通信、密码、传感、时钟、器件材料	10.65
法国	2020	国家量子技术投资计划	开发容错大型量子计算机，量子传感器和量子通信	18.28
以色列	2020	国家量子技术计划	投资量子计算，量子传感和量子材料科研	3.75
加拿大	2021	国家量子战略	支持量子材料和量子设备研究，投资新兴量子产业	3.60
德国	2021	量子计算机研发与应用	开发量子计算机，将量子计算技术推向市场	24.36
奥地利	2021	量子奥地利	加强量子技术基础研究，促进产品服务和市场投放	1.27
新西兰	2021	——	资助多德沃尔斯光子和量子技术中心	0.37
美国	2021	2021 年创新与竞争法案	含《量子网络基础设施和劳动力发展法案》	——

来源：中国信息通信研究院根据公开信息整理（截至 2021 年 10 月）

美国长期高度重视和持续投入支持量子信息领域的科学研究和应用探索，近年来通过《国家量子行动（NQI）》《量子信息科学国家战略概述》《美国量子网络战略规划》等多项立法与规划，明确量子计算机、量子互联网和量子传感器等重点发展方向，对基础科学研究、原理样机研制、网络技术试验和应用场景探索设置分阶段发展目标，进一步开展中长期规划部署。NQI 方案年度报告[3]显示其基础科研和重点发展领域投资规模远超原计划，支持与推动力度正进一步加大。根据 NQI 立法授权，美国白宫国家科学技术委员会成立国家量子协调办公室，牵头组织国家科学基金会（NSF）、能源部（DoE）和国家技术标准局（NIST）等多部门，在基础科学研究、工程技术研发、应用场景探索、人才教育培训和产业链构建等方面，开展全方位体系化布局。NSF 向美国高校优势科研团队注资，新成立三所量子飞跃挑

[3] https://www.quantum.gov/wp-content/uploads/2021/01/NQI-Annual-Report-FY2021.pdf

战研究所，持续支持四家量子信息科学物理前沿中心。DoE 在下属国家实验室体系中成立五个量子信息研究中心，牵头组织量子互联网等技术验证实验，支持基础科研成果的工程研发转化。NIST 开展光钟、量子探测存储和抗量子计算破解加密算法等技术研究与标准化，提供微纳加工平台和超低温测试床等基础设施服务。

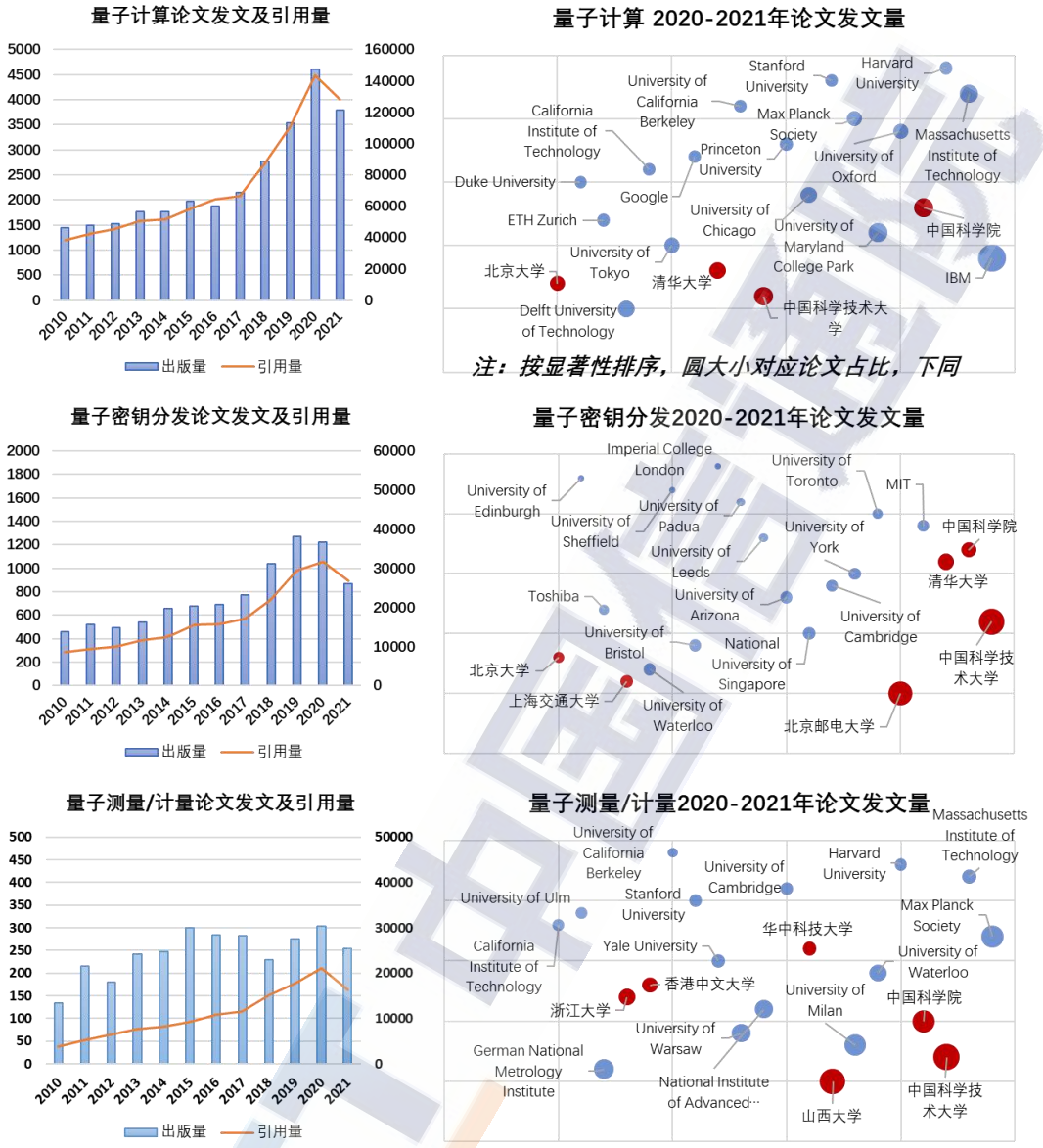
我国高度重视和大力支持量子信息领域的基础研究、科学实验、网络建设和示范应用。2020 年 10 月，习近平总书记在中共中央政治局第二十四次集体学习中，做出把握量子科技大趋势，下好先手棋系列重要指示，为加快促进我国量子信息技术领域发展提供了战略指引和根本遵循。2021 年 3 月，《中华人民共和国国民经济和社会发展第十四个五年规划和 2035 年远景目标纲要》正式发布[4]，明确提出聚焦量子信息等重大创新领域组建一批国家实验室；瞄准量子信息等前沿领域，实施一批具有前瞻性、战略性的国家重大科技项目；在量子信息等前沿科技和产业变革领域，组织实施未来产业孵化与加速计划，谋划布局一批未来产业；加快布局量子计算、量子通信等前沿技术，加强基础学科交叉创新；深化军民科技协同创新，加强量子科技等领域军民统筹发展。2021 年以来，北京、安徽、广东、上海、山东等 21 个省市在地方“十四五”科技与信息技术产业发展规划中，对量子信息领域基础科研、应用探索和产业培育等方面做出具体部署，提供政策引导与项目支持。

[4] http://www.gov.cn/xinwen/2021-03/13/content_5592681.htm

（三）量子信息各领域科研加速发展，技术创新活跃

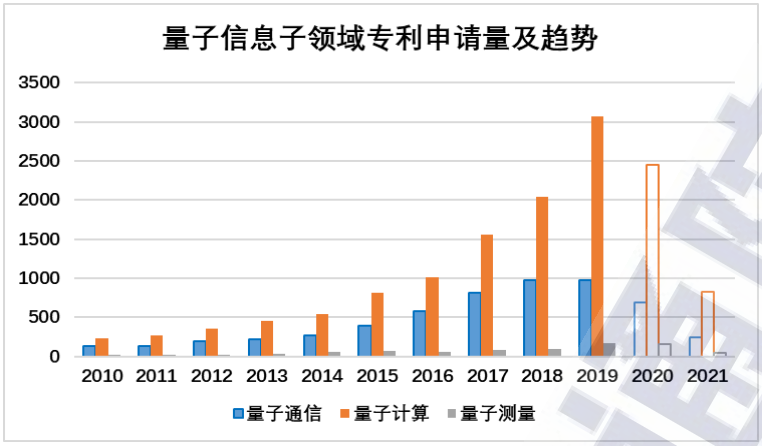
量子信息领域论文主要集中在物理学、光学和工程领域，与计算机、化学、数学等领域也有较多关联。量子计算关联主题主要包括量子比特、量子算法、量子电路、量子纠错、量子网络、量子门、量子态等；量子密钥分发关联主题主要包括量子网络、量子隐形传态、量子密码、量子比特、量子容量等；量子测量关联主题主要包括量子比特、量子态、退相干、量子模拟、量子纠错、腔量子电动力学等；量子信息三大领域的研究主题也存在较多交叉重合。

近年来，量子信息三大领域科研论文发文量持续上升，研究创新活跃，如图 1 所示。量子计算领域研究上升趋势明显，美国量子计算前沿研究领域处于领先地位，学术论文发表量和研究机构数量位列全球第一，我国紧随其后。过去一年中，国内科研和创新活跃机构包括中国科学院、中国科学技术大学、清华大学和北京大学等。量子通信领域，量子密钥分发相关论文数量持续上升，我国量子密钥分发论文量位列第一，欧洲研究也较为活跃。近一年来，中国科学院、中国科学技术大学、清华大学、北京邮电大学、上海交通大学、北京大学等国内机构论文成果较多。外国机构中，麻省理工学院、多伦多大学、剑桥大学、新加坡国立大学、日内瓦大学等亦有较多成果。量子测量领域，美国科研机构发文量位列第一，中、德、日、英等国紧随其后。除上述高校科研机构外，IBM、Google 和东芝等大型企业，在量子信息学术论文发表方面也处于前列。



来源：中国信息通信研究院知识产权中心（2021.9，Microsoft Academic Search）

图 1 量子信息三大领域近年来科研论文发表情况



来源：中国信息通信研究院知识产权中心（截至 2021.9）

图 2 量子信息三大领域近年来专利申请趋势[5]

近十年量子通信、量子计算、量子测量三大领域全球专利申请趋势如图 2 所示，量子计算领域关注度上升最快，尽管量子计算机距离实用化还有一段距离，但科技巨头对知识产权已开展前瞻布局，美国专利总量和申请时间上占有优势，我国量子计算专利申请数量持续上升，增速较快。但值得注意的是，相比于美、日、欧，我国更多专利申请来自高校和科研机构。

来源：中国信息通信研究院知识产权中心（截至 2021.9）

图 3 量子信息三大领域专利聚类分析

[5] 专利申请信息公开存在 18 个月滞后期

三大领域近五年有效专利聚类分析如图 3，各领域间互有交叉。量子计算领域，有越来越多应用主体，如银行、互联网公司、移动支付机构等围绕量子计算与人工智能的交叉领域，提出量子数据分类的模型训练方法，量子数据分类方法，数字签名方法等信息安全领域专利。量子通信领域，相关企业关注连续变量量子密钥分发方法和系统芯片化。量子测量领域侧重消除量子噪声方法和应用领域创新，比如有科研单位提出原子干涉重力仪在地质勘测领域的应用解决方案。

（四）量子信息技术国际国内标准化取得阶段性成果

标准是经济活动和社会发展的技术支撑，标准化在推进国家治理体系和治理能力现代化中发挥着基础性、引领性作用。2021 年 10 月，中共中央、国务院印发《国家标准化发展纲要》[6]，要求在量子信息等关键技术领域加强标准研究；建立重大科技项目与标准化工作联动机制，将标准作为科技计划重要产出；完善科技成果标准化评价机制和服务体系，促进创新成果产业化应用；强化标准实施应用，在认证认可、检验检测、政府采购、招投标等活动中应用先进标准。

随着量子信息技术研究、样机研制、应用探索和产业培育的快速发展，量子信息领域标准体系建设和技术标准研制受到国内外产业界和学术界共同关注。近年来，国际电信联盟电信标准化部门（ITU-T）、欧洲电信标准化协会（ETSI）、国际标准化组织与国际电工委员会第一联合技术委员会（ISO/IEC JTC1）、互联网研究任务组（IRTF）、电气与电子工程师协会（IEEE）等国际和区域性标准化组织布局开展量

[6] http://www.gov.cn/zhengce/2021-10/10/content_5641727.htm

子密钥分发（QKD）、量子密钥分发网络（QKDN）、量子计算、量子互联网等方面研究工作并取得阶段性成果，标准研究工作进展和具体成果如附录 I 中表 2~

表 6 所示。

ETSI 最早开展 QKD 标准研究，关注系统器件、内部接口、应用接口、安全性证明等，发布标准和报告 10 项，在研 6 项，欧洲学术机构和产业公司是主要推动力量。2018 年 ITU-T 启动量子信息技术标准化工作，关注量子密钥分发网络架构、功能、协议、安全性等，发布标准和报告 10 项，在研 28 项，成为量子信息技术国际标准化的重要平台。中日韩等国是其中主要推动力量，我国学术界和产业界在标准研制中发挥重要作用，牵头推动成立网络量子信息技术焦点组（FG-QIT4N），积极开展前沿领域技术研讨与标准化前景分析。ISO/IEC JTC1 开展 QKD 系统安全性标准研制，研究量子计算术语定义，我国成员是重要推动力量。IRTF 和 IEEE 在量子互联网和量子计算等方面初步布局，进展和工作成果较为有限。

我国基于 QKD 的量子保密通信在设备商用化、实验网络建设和示范应用探索等方面发展较快，量子计算原理样机科研成果不断涌现，应用探索初步开展，成为推动量子信息技术标准化研究的重要支撑。中国通信标准化协会（CCSA）、密码行业标准化技术委员会（CSTC）和全国量子计算与测量标准化技术委员会（TC578）等标准组织积极布局和开展量子保密通信、量子计算和测量等领域标准研究，具体工作进展和成果见附录 I 中表 7~表 9。

CCSA 主要关注 QKD、量子保密通信、量子信息处理与组网应

用等领域标准化，已发布 QKD 系统技术要求、测试方法、关键器件等核心行业标准，可为规范和促进我国量子保密通信应用与产业发展提供重要指导，目前立项国家标准 2 项，行业标准 13 项，研究报告 21 项。CSTC 从密码技术、应用与管理角度开展 QKD 和量子密码等领域标准化研究，立项行业标准 5 项，研究报告 6 项，其中已发布行业标准 2 项，经典密码与量子密码领域交流融合有待进一步加强。TC578 布局量子计算术语和量子测量领域研究，已立项 2 项国家标准和 5 项研究报告，标准化工作推动处于起步阶段。

（五）量子信息产业培育起步，政产学研协同成趋势

量子信息技术能够为科技与信息通信等诸多领域发展提供物理基础重大创新驱动。随着量子信息技术逐步从学术研究和实验探索，走向样机研制、产品开发与应用探索，着眼于科研成果转化、行业应用创新、供应链建设、人力资源培养和创业投融资等工作的产业生态培育，已开始成为全球主要国家在量子信息领域的关注热点和发力方向，加强政产学研用各方在量子信息领域的沟通交流与协同创新正逐步形成新趋势。近期，各国成立和推动量子信息技术领域产业联盟的进展概况如图 4 所示。

来源：中国信息通信研究院根据公开信息整理

图 4 近年全球各国量子信息技术领域产业联盟

根据 2018 年美国 NQI 立法授权，NIST 牵头组建美国量子经济发展联盟（QED-C），其目标是在美国建立发展量子技术产业及相关供应链。截至 2021 年 10 月，联盟包含美国高校、研究机构、国家实验室、科技企业、军工企业和众多初创公司在内的各类型成员 176 家。QED-C 含至少五个技术咨询委员会（TAC），其中使能技术 TAC 举办低温技术、超导量子比特材料缺陷、量子赋能激光技术、量子系统电子学和射频/微波控制等研讨会；应用案例 TAC 由 Google 支持开展量子计算市场基准评估；标准化 TAC 推出基于应用算法的量子计算性能原型基准研究开源项目[7]；人力资源 TAC 发布量子技术行业人才需求情况调查报告[8]；国家安全量子技术 TAC 推动量子定位/导航/授时（PNT）相关技术与应用发展。

[7] https://arxiv.org/pdf/2110.03137.pdf

[8] https://arxiv.org/pdf/2109.03601v1.pdf

在欧盟量子旗舰计划支持下，2021 年 4 月，欧盟多国量子信息领域初创企业、研究机构和各领域行业企业，成立了欧洲量子产业联盟（QuIC），总部位于德国尤利希，成员单位超过 100 家。联盟以促进政府、学术界和产业界等量子技术产业利益相关方协调联系；开发探讨量子技术在支持组件/技术、用例、性能、供应链、标准和人力资源等方面和行业和市场要求；明确上述方面的障碍问题并提出解决方案为主要目标。设置 10 个工作组包括：市场趋势和用例、知识产权、教育、标准、行业新技术、行业战略路线图、协调/流程/便利、生态系统、投资、中小型企业和初创企业。

2020 年 10 月，加拿大成立含 24 家企业的量子工业联盟（QIC），加快量子技术创新、实现人才的转化以及推进量子技术商业化进程。2021 年 6 月，德国西门子、默克、SAP 等 10 家大型企业联合成立量子技术与应用联盟（QUTAC），推动量子计算在各行业领域应用探索，构建商用化基础和产业生态。2021 年 9 月，日本东芝、丰田、NEC 等 24 家大型财团企业，行业涉及通信、汽车、保险、金融和化学等领域，组建量子科技新产业创造委员会（Q-STAR），关注量子计算和量子通信应用探索和商业场景开发。

为贯彻落实习近平总书记关于促进量子科技领域产学研协同创新的重要指示精神，在工业和信息化部指导下，中国信息通信研究院联合我国量子信息领域高校、科研机构、初创企业、科技企业和信息通信企业，将共同发起和筹备组建量子信息网络产业联盟（QIIA）。主要计划包括：开展量子计算、量子通信和量子测量三大领域的量子信息网络技术、应用、产业发展趋势问题研讨；组织技术交流研讨，

技术创新与实用化研究，促进应用场景探索与通用共性技术的协同研发；开展产业发展需求与问题分析，促进产业要素聚集和生态培育；推动技术标准前期研究，研制测试测评方法规范，开展测评验证；举办论坛会议、科普培训和竞赛展示等多种形式活动，推广优秀技术产品、解决方案和应用案例，组织开展对外交流合作等。

二、量子计算领域研究与应用进展

（一）多种硬件技术路线并存，工程研发仍面临挑战

量子计算处理器是制备、操作和测量量子比特的物理载体，基于单比特叠加和多比特纠缠的耦合与状态演化实现高效并行计算模拟等功能，是样机研发攻关亟待突破的“核心瓶颈”。根据实现量子比特二能级体系和制备操控方案不同，量子计算处理器存在超导、离子阱、硅基半导体和光量子等多种技术路线，目前仍处并行发展和开放竞争状态，尚未出现技术路线融合收敛趋势。

超导量子处理器基于超导约瑟夫森结形成扩展二能级系统，通常采用超导谐振传输器（Transmon）电路模型电荷量子位构造量子比特。主要优势在于，可实现较高保真度（双比特逻辑门>99%）和快速门操控（数十纳秒），电路设计、制备和测量与集成电路技术兼容，比特数规模暂处领先，比特能级耦合设计与操控灵活，平面二维布局与纠错编码契合度高等。主要局限在于，数十毫开尔文极低温制冷要求对大规模扩展和电子学设计带来工程挑战，人工制造量子位的差异可能导致错误，来源机制尚未明确，比特相干寿命目前仅为百微秒量级，提高相干寿命和保真度需材料科学和电路模型设计等方面的重大突

破。美国科技巨头 Google 和 IBM 样机研发领先，2019 年，Google 报道[9]53 位比特处理器“悬铃木”，量子随机线路采样问题中首次实验验证量子计算优越性。2021 年发布路线图[10]，预测 2029 年实现百万位量子比特和可纠错量子计算。2020 年 IBM 推出 65 位比特样机“蜂鸟”，在德、日、英等国开展部署，通过云平台向部分用户开放，2021 年 11 月，推出 127 位“鹰”平台，计划 2023 年推出 1121 位“秃鹫”平台[11]。我国中科大近期超导量子计算科研取得重要进展，5 月报道[12]62 位“祖冲之”处理器实验演示二维量子随机行走，10 月报道[13]66 位处理器在与 Google 相同问题中，以更大优势验证量子计算优越性。本源量子近期发布超导样机研发计划[14]，预计 2025 年达 1024 位比特。

离子阱量子处理器以微波电场和高精度激光信号对带电离子进行捕获、操控和测量，并以其能级谱中两个长寿命二能级构建量子位。主要优势在于，无需极低温冷却，天然离子量子位具有全同性，保真度高（双比特逻辑门>99.9%），相干寿命长（秒级），纠错编码开销需求低，光子操控、互联与未来量子信息组网兼容等。主要局限在于，需要超高真空环境支持激光冷却，门操作速度慢，单比特多路激光读写需求和线性阱尺度规模制约比特数扩展等。美国 Honeywell 和 IonQ 在离子阱量子计算样机研发方面处于领先。2021 年 Honeywell 报道[15]

[9] https://doi.org/10.1038/s41586-019-1666-5

[10] https://quantumai.google/hardware

[11] https://research.ibm.com/blog/ibm-quantum-roadmap

[12] https://doi.org/10.1126/science.abg7812

[13] https://doi.org/10.1103/PhysRevLett.127.180501

[14] https://app.originqc.com.cn/zh/new_detail.html?newId=171

[15] https://doi.org/10.1038/s41586-021-03318-4

基于电荷耦合器架构的 10 位高保真比特原型机“H1”，预计在 2023 年实现 40 位量子比特原型机“H2”，2030 年实现基于集成光学栅格的模块化百位量子比特样机。2020 年 IonQ 发布[16]32 位比特离子阱样机，预计在 2025 年比特数达到 64 位。

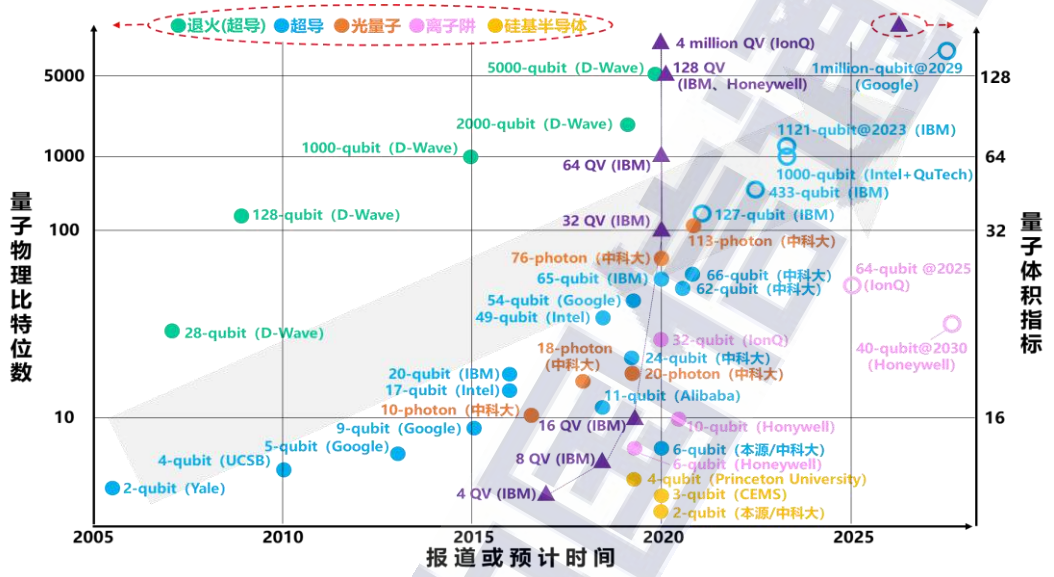
硅基半导体量子处理器通常以硅同位素量子点中电子自旋构建量子比特的二能级系统。主要优势在于，可采用成熟集成电路工艺设计制造，具备潜在扩展性和测控复用优势，门操作速度快（纳秒级）等。主要局限在于，噪声影响明显，保真度较低，需要低温冷却（可运行于 1 开尔文温区），需要高纯度材料提高量子位相干寿命，量子位间串扰难解决，限制比特数扩展。硅基半导体量子计算样机研究近期暂无重大突破，美国 Intel 与荷兰 Qutech 联合团队、澳大利亚 New South Wales 大学和 SQC 公司、加拿大 Photonic 公司、我国中科大和本源量子等高校和企业在该领域具备较强的研发能力。

光量子计算可以使用光子的多种自由度，例如偏振、相位和时间位置等进行量子态编码和量子位构建，这一技术也在量子通信中广泛应用。主要优势在于，室温运行无需真空，保真度高，操控速度快，采用硅光集成技术可以实现大规模扩展等。主要局限在于，光子间相互作用微弱，构建逻辑门困难，光子量子位相干寿命较短（百微秒量级），高品质光源技术尚不成熟，高性能单光子探测需要低温制冷等。我国中科大空间光学量子计算实验处于领先，2020 年 12 月报道[17]，76 光子单模压缩光学实验系统“九章”，在高斯玻色采样问题中实验验

[16] https://ionq.com/posts/december-09-2020-scaling-quantum-computer-roadmap

[17] https://doi.org/10.1126/science.abe8770

证量子计算优越性，2021 年报道[18]进一步提升为 113 光子，在相同问题中更大优势验证量子计算优越性。需要指出，光量子计算领域初创公司，如美国 PsiQ、加拿大 Xanadu 和我国图灵量子等，普遍关注基于集成光学芯片的光量子计算技术方案。



来源：中国信息通信研究院公开材料整理（截至 2021.10）

图 5 量子计算处理器物理比特数和量子体积发展趋势

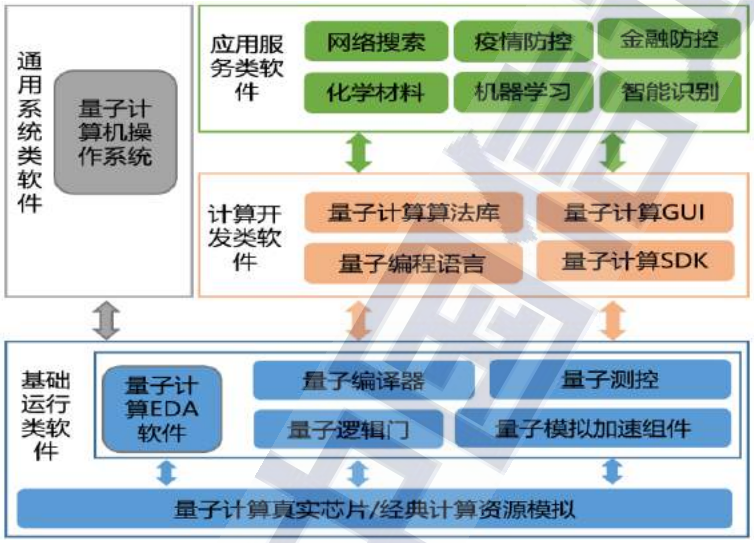
近年来量子计算硬件技术路线发展趋势和主要指标情况如图 5 所示，在量子计算硬件不断发展的过程中，综合评价指标也呈现多元化探讨态势。继 2020 年 IBM 提出量子体积（QV）指标之后，IonQ 基于量子算法在量子计算机上的运行性能，提出算法量子比特的评价指标，美国量子软件初创公司 Zapata 基于 NISQ 计算架构，提出应用基准度量指标等。未来数年，随着量子计算性能基准研究、测评验证和标准化的不断发展，量子计算综合评价体系和测试基准将逐步明确，

[18] https://doi.org/10.1103/PhysRevLett.127.180502

成为衡量量子计算发展水平和计算能力的重要依据。

（二）量子软件与算法研发活跃，开源开放多样发展

量子软件生态目前处于培育初期，业界正在开展软件及算法的体系化设计以及用户培育工作，多种量子计算软件并举研发迭代活跃，开放化和开源化成为量子计算软件发展的主要趋势。



来源：中国信息通信研究院

图 6 量子计算软件分类、定位及现状

量子计算软件分类如图 6 所示，主要分为四种类型：基础运行软件、计算开发软件、应用服务软件以及通用系统软件。

基础运行软件作为量子计算机的核心控制类软件，与硬件紧密相关，是量子计算软件技术的发展核心，也是上层软件开发和应用功能的实现基础。量子编译软件主要规范量子编程的边界，确保量子程序编译执行的正确性，提供完善的语法规则用以协调和约束量子操作、经典操作，典型软件包括 QASM、eQASM、QASM-HL、

Quil、OpenQASM、f-QASM、Jaqal 等。量子测控软件提供测量结果反馈和芯片校准等功能,是量子计算处理器稳定运行的重要保障,包括 LabOne、HVI、Optimus、PyQCat 等。芯片设计 EDA 软件成为量子计算软件发展新亮点,可高效完成量子芯片自动化辅助设计、参数标定优化、芯片封装设计等功能,加速量子计算芯片研发与迭代,目前已有 Qiskit Metal 和 KQCircuits 等。

计算开发软件提供了研究量子算法、开发量子应用的工具体系,主要用来编写运行在量子计算机中的量子算法和程序,经过封装后还可提供常用的量子计算组件和量子算法库,进行量子程序的快速开发。量子汇编类软件与量子计算硬件对接,提供了统一表示量子算法程序的数据及接口。其中典型软件包括 Qiskit、Cirq、QDK、QPanda、ProjectQ、HiQ、Forest 及 SuperstaQ 等。

应用服务软件是量子技术走向应用的关键,匹配行业需求解决特定领域问题,通过上层编程开发,为不同应用领域提供服务,主要包括解决算法、应用程序及云端人机交互环境。典型应用服务软件领域涉及量子化学、量子机器学习和量子组合优化等。

通用系统软件是在对量子计算操作性和兼容性要求提升的背景下出现的,其中通用操作系统的出现成为今年量子计算软件发展的另一亮点,用于实现量子资源系统化管理和自动任务调度,保证量子计算任务高效执行,屏蔽量子计算软硬件的差异性,简化量子计算操控和使用,未来有望加速量子计算高效运行,实现计算资源共建共享,目前公布的量子计算操作系统软件包括英国 Deltaflow.OS、奥地利 ParityOS、中国本源司南等。

量子计算优势的展现离不开基于量子算法对具体问题进行求解，算法的突破将有力推动量子计算领域发展。目前量子算法存在多种技术路线和探索方向，其中 NISQ 条件下经典+混合量子算法、通用量子算法以及量子启发式经典算法是近期业界研究热点。

QAOA 和 VQE 算法是典型经典+混合算法，有望在 NISQ 计算架构下解决化学模拟、组合优化等特定的计算问题。2021 年 5 月，美国 CQC 推出新算法用以加速量子蒙特卡罗积分[19]，缩短获得量子优势的时间，并证实量子计算对金融业尤其重要。

量子机器学习是通用量子算法的研究热点，具备广阔应用潜力，但总体而言存在诸多开放性问题亟需探索和解决，例如，机器学习中的数据与特征的量子编码与量子制备问题，量子版本的机器学习是否能够真实体现优势，量子机器学习任务如何与硬件进行协同适配等。2021 年 7 月 Google 与 MIT 提出一种量子算法[20]，引入神经正切核近似，实现对数时间加速训练深度神经网络。

量子启发式经典算法作为近几年业界提出的新研究方向，以量子计算的数据结构和计算逻辑为视角，可在经典计算机上用以加速解决特定问题，有望成为新的实用化方向。2021 年 10 月，美国 DARPA 推出量子启发经典计算计划[21]，旨在利用从量子算法基准测试中获得的经验，为一系列复杂优化问题开发量子启发求解器。

量子纠错编码是实现可容错通用量子计算的关键要素。由于量子

[19] https://arxiv.org/pdf/2105.09100.pdf

[20] https://arxiv.org/pdf/2107.09200.pdf

[21] https://insidehpc.com/2021/10/darpa-program-aims-to-build-quantum-inspired-solvers/

比特的错误自由度高并具有高度复杂性，量子纠错编码仍是颇具挑战的科研方向。2021 年在改善错误率路径方面取得可喜进展，Google 在 Nature 报道[22]，基于“悬铃木”量子处理器实现嵌入在超导量子比特的二维网格中的一维重复纠错编码，实现位翻转或相位翻转错误抑制的指数提升，逻辑错误减少 100 倍以上，证明了量子纠错可以成功将错误率控制在一定范围内，从而推进容错量子计算机研发进程。

量子编程语言方面，如何从抽象编程范式和模型中发掘和利用量子计算特殊并行优势，并进行工程化设计和软件扩展，是具有挑战性的技术问题。目前，量子编程语言仍处于初级发展阶段，进展包括 Svore 等人提出了分层量子软件架构，可将高级量子程序通过量子汇编语言映射到量子设备上；Nagarajan 等人定义了顺序量子随机访问存储器（SQRAM）模型，进一步设计了 QPL 编译器。近期关于量子编程语言的项目如 Quipper、LIGUi|>、Scaffold 和 QuaFL 逐步开发，量子线路优化与合成取得较大进展。目前在量子编程领域仍然有诸多开放性问题值得业界探讨，如绝热量子计算、拓扑量子计算等物理非标准体系，基于量子线路模型难以编程的问题，量子程序的并发性和分布式计算问题，函数式量子编程问题等。

量子计算的软件生态目前处于体系建立的早期阶段，目前尚未产生统一标准，各类软件开发与应用远远未达到与经典计算软件相媲美的程度。国外量子计算软件布局及生态推广方面，IBM、Google、微软及 Rigetti 等公司在研发和应用领域表现活跃，如图 7 所示，IBM

[22] https://www.nature.com/articles/s41586-021-03588-y

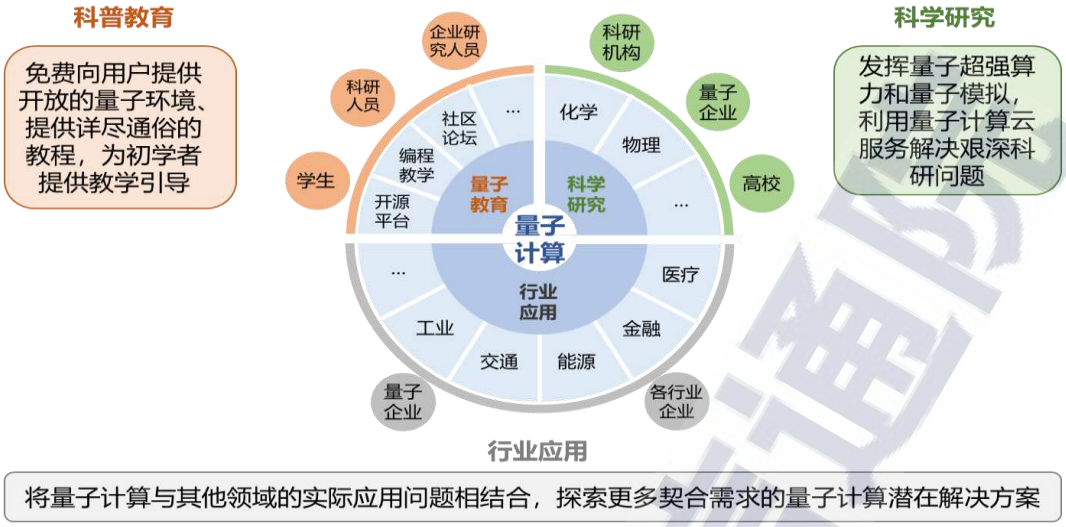
持续积极推行量子计算软件的开源，推动量子计算软件工具生态系统形成，培养解决量子计算问题的开发者社区。阿里巴巴、百度、本源等在量子软件方面也积极布局，推出相关开源软件项目。

来源：中国信息通信研究院根据公开信息整理

图 7 IBM 量子计算软件生态培育推广动态

（三）实用案例成为关注重点，多领域探索蓄势待发

随着量子计算优越性得到实验验证，量子计算已进入实用化优势应用场景探索的新阶段，如图 8 所示，基于专用量子计算机，在不同领域和行业开展了广泛应用探索。近期在科学研究、科普教育、行业应用等多方面开展布局并取得进展。



来源：中国信息通信研究院

图 8 量子计算实用化应用探索发展方向

目前量子计算应用探索主要包括量子模拟和加速优化两大类型。量子模拟在药物研究、材料科学、分子化学等领域，通过量子处理器来模拟量子系统运行状态，具备真实接近系统自然状态原貌的优势。计算层面的加速及优化包括机器学习的加速和大数据处理及优化等，目前在量化金融、航空动力学设计、交通规划等领域探索活跃。

在量子化学模拟场景中，化学反应过程的模拟和分析对于经典计算机来说，由于变量复杂和建模困难，计算难度呈指数级增长，非常具有挑战性。量子化学模拟在化学制剂和生物医药研发等领域具有广阔应用潜力，或将成为未来量子计算可切入市场之一。2020 年 8 月，Google 在量子处理器中实现 Hartree-Fock 状态化学模拟；2021 年 1 月，Google 与 BI 合作研究量子计算药物研发前沿用例；美国芝加哥大学利用 53 位物理比的 IBM“蜂鸟”量子处理器，模拟和制造一种称为激子凝聚态的量子材料。

在量化金融场景探索中，量子计算有望消除数据盲点，开展风险预测，加速资产定价，挖掘最佳投资组合等，量子优化、机器学习、量子加速蒙特卡罗算法有望成为量子金融计算应用探索的三大方向。全世界 20 余家银行正在积极探索量子金融的应用，2020 年 7 月，AlgoDynamix 宣称使用量子退火算法提供用于财务行为分析的预测服务。西班牙对外银行研究结果表明，量子计算可以提升信用评分、发现套利机会，并加速蒙特卡罗模拟，可以用于模拟市场中可能发生的行为。2021 年 2 月，本源量子与建信金科联合发布量子期权定价、量子风险价值计量等算法应用探索案例。2021 年 3 月，英国剑桥量子计算公司推出多个量子机器学习推理方法，在 IBM 量子计算机上，实现贝叶斯网络的随机实例推理，在模拟金融时间序列的隐马尔可夫模型中推断市场条件波动。

在组合优化问题中，搜索空间往往随着搜索规模呈指数级增长，导致有效时间内难以求解，或难以获得全局性最优解，量子退火算法和量子近似优化算法等有希望为超大规模的特定组合优化问题提供解决方案。D-wave 与德国大众合作，基于量子退火算法对北京 1 万辆出租车的交通流向数据进行组合优化求解，探索解决交通阻塞问题的优化方案。2021 年 9 月，日本富士通公司宣布，推出量子启发数字退火技术，大幅简化汽车运输船的配载复杂任务计划。

在航空航天领域，量子计算有助于解决基础材料研究、空气动力学设计、复杂系统优化等方面技术挑战，航空航天领域知名企业开始涉足量子计算软硬件与应用探索研究。美国国家航空航天局（NASA）设立量子人工智能实验室来解决航空、地球和空间科学以及太空探索

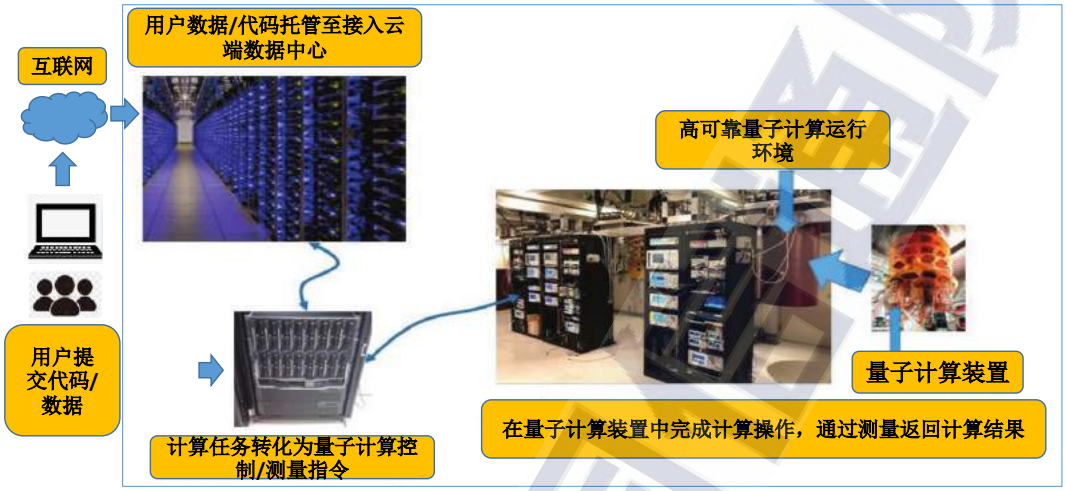
任务中出现计算任务和机器学习优化问题。

在量子计算应用探索发展过程中，算法和编程比赛成为生态培育与推广重要舞台，科技公司和行业企业积极举办赛事，为参赛者提供软件平台、奖金、就业机会、认证证书等多种激励手段，既有助于发现培育量子计算人才，也对软件和云平台进行了有效宣传推广，全面盘活软件生态。科技巨头 IBM 举办的量子计算编程挑战赛，已成为全球最具影响力的量子计算赛事，2021 年挑战赛有超过 1400 支队伍参加，在 IBM 量子计算云平台提交了超过 7000 次的编程计算任务，执行超过 30 亿次。华为多次举办量子计算开发者大赛和量子编程黑客松比赛，为参赛选手提供 HiQ 编程框架和量子计算云平台的编程环境，采取比赛打榜和专家答辩等多种形式进行优秀选手选拔及评比。2020 年 10 月，百度之星大赛上首设量子计算赛题，参赛选手针对量子电路优化设计任务开展激烈竞逐，取得多项创新成果。行业巨头也积极举办量子计算悬赏类竞赛，2020 年欧洲空客公司举办全球量子计算挑战赛，通过采用量子计算这种新型计算能力，为飞机全生命周期的复杂优化和模型化提供解决方案，我国本源量子成功入围决赛。2021 年，德国宝马集团联合 Amazon 发起全球量子计算挑战赛，设立 50 多项挑战任务，来自全球量子计算领域的研究人员和初创企业可向宝马集团量子计算挑战赛提出特定工业挑战的解决方案，并在真实量子计算平台上进行方案验证测试。

（四）量子计算云平台深化发展，各方探索竞争合作

量子计算云平台作为展示量子计算实用化优势和输出能力的途

径之一，成为量子计算领域发展热点。近年来国外科技企业、初创企业与研究机构加速布局，纷纷推出量子计算云平台，为争夺产业生态地位，抢占未来发展先机展开激烈竞争。



来源：中国信息通信研究院根据《Quantum Computing and Prospects》整理

图 9 量子计算云平台服务实现示意图

量子计算云平台集成了量子计算与经典云计算的特点与优势，系统与应用框架示意如图 9 所示。用户在客户端设计量子计算任务，通过互联网提交至云端，由云端服务器转换为量子控制信号后，操控量子计算装置进行运作与测量，最终将得到的计算结果返回给用户。量子计算云平台借助经典云释放出量子计算潜力，可满足量子计算研究、教学、开发等多方需求，同时各方反馈也成为量子计算云平台的贡献者，形成演进闭环，共同促进量子计算技术发展。

国际量子计算云平台服务提供商多元化发展，竞争与合作并存。2017 年 3 月，IBM Q Experience 首次发布量子计算 API，使开发人员能够在基于真实量子比特的量子计算机与经典计算机之间建立接口，IBM Q 量子计算系统和服务通过 IBM 云平台交付并逐步构建量子计

算软件生态系统。2020 年 8 月，Amazon 发布 Braket 作为完全托管的 AWS 服务，可提供开发环境来帮助客户量子计算应用算法，灵活接入多家量子计算公司物理平台后端，也可使用 Amazon EC2 量子计算模拟器运行和验证算法。2020 年 7 月，Honeywell 发布 H0 的 6 量子比特离子阱计算原型机并提供云端访问接入能力，与多种量子软件框架兼容。2020 年 9 月，D-Wave 发布 5000 量子比特系统 D-Wave Advantage，在 Leap 量子云平台中构建和运行量子混合应用程序，提供量子退火服务。为推动欧洲量子技术的发展，2021 年 4 月荷兰 QuTech 开发了公共量子计算云服务平台 Quantum Inspire，与 IBM 类似，Quantum Inspire 包含量子芯片、经典控制、量子编译器、软件层和用户界面，侧重于量子计算教育培训与应用程序开发。

我国量子计算云平台提供企业虽然起步较晚，但紧跟国际企业发展步伐，整体表现活跃，汇集了多家科技企业、初创企业和研究机构，为国内量子计算发展贡献支撑力量。2017 年 10 月，阿里云与中国科学院联合发布了量子计算云平台，并在 2018 年 2 月接入了 11 比特的超导量子计算服务。2017 年 10 月，本源量子上线量子计算云平台，搭建 32 位量子计算模拟机，目前还可提供基于自研超导量子芯片及半导体量子芯片的云平台接入访问。2018 年 10 月，华为发布了量子计算模拟器 HiQ 云服务平台及量子计算软件解决方案，基于 VQE 算法探索量子化学模拟应用场景，2020 年更新 HiQ 3.0 量子计算模拟器及开发者工具，增加量子组合优化求解器和张量网络计算加速器。2020 年百度发布量易伏量子计算云平台，实现 28 位量子比特的量子随机线路模型，并发布了基于百度开源框架 PaddlePaddle 的机器学习

库，支持量子神经网络的搭建与训练，2021 年 10 月发布了云原生量子集成开发环境 YunIDE。2021 年，北京量子信息科学研究院等研究机构也开始提供超导量子计算云平台，为量子算法和量子模拟研究提供了实际物理平台后端的测试场景等。

依托量子计算云平台开展企业多方合作成为该领域发展趋势。2021 年 6 月，IBM 宣布将其所有量子计算系统整合到了 Strangeworks 第三方量子计算云平台，用户可免费访问全部 28 项量子计算服务，包括 9 台免费量子计算机和 5 个托管模拟器，进一步提高 IBM Q Network 生态系统影响力。Honeywell 与 CQC 公司宣布合并，未来依托云平台提供更强的软硬件服务。IonQ 与 Google 开源量子计算框架 Cirq 全面整合，提供多种量子软件框架对 IonQ 样机的访问。

量子计算模拟器成为量子计算云平台能力输出的重要技术特色。一方面，量子计算模拟器缓解了当前量子计算资源的稀缺性问题，在一定程度上降低对真实量子计算物理条件的依赖，促进量子计算科学实验和应用验证在软件和算法层面的顺利进行。另一方面，为复杂含噪环境下的量子计算模拟、量子物理现象推演、量子启发式算法实现、量子芯片设计验证等提供辅助实现工具。近年来，国内外科技企业也加大了量子计算模拟器的研究和应用推广力度，取得了突破性成果。2021 年 5 月，Amazon 在 Braket 量子云平台提供完全托管的密度矩阵模拟器，可模拟最高 17 个量子比特的量子噪声线路。2020 年 9 月，华为队发布 HiQ 3.0 量子计算模拟器及开发者工具，推出了量子组合优化求解器 HiQ Optimizer 和张量网络计算加速器 HiQ Tensor，在天河二号超级计算机上部署 HiQ 模拟器，可进行超大规模的量子计算

模拟仿真任务。2020 年 12 月，阿里巴巴开源了自研量子计算模拟器太章 2.0，对分布式张量网络收缩算法进行了优化改进，支持量子硬件设计、量子算法测试，以及在材料、分子发现，优化问题和机器学习等领域内的探索应用。2021 年 4 月，芯片巨头 NVIDIA 也看好未来量子模拟器的算力需求，推出名为 cuQuantum 的开发工具组，让开发者基于 NVIDIA GPU 对量子计算模拟器进行计算加速。

量子计算云平台商业应用模式探索也在积极开展。2020 年 7 月，Amazon 宣布 Braket 提供量子计算云平台服务，用户可接入 D-wave、Rigetti 等第三方量子计算后端，并可使用 32qubit 托管式量子模拟器，费用为 4.50 美元/小时。Google 云用户可以购买使用 IonQ 量子计算机服务，成为 Google 云市场上首个第三方量子计算机，其中 QPU 操作费用为 1 美元/次。同时，量子计算云平台也在积极探索采用多种新技术提升资源调度和服务访问质量。2021 年 3 月，IBM 发布了 Qiskit Runtime 量子计算容器化服务，采用新软件栈和 OpenShift 运算符使用户能够最大限度地利用计算时间并缩短等待时间，发布全新量子内核对齐算法（QKAA），为用户的算法和计算任务自动匹配最佳量子计算内核，显著提升量子算法实验执行效率。2021 年 3 月，量子计算公司（QCI）发布量子应用加速器 Qatalyst，并在 Amazon 量子云平台上线，有效提升用户在使用量子计算硬件资源效率。

总体而言，量子计算技术产业尚在发展萌芽期，目前国内外开放的量子计算云平台主要提供以展示和验证量子计算运行机理为主的“玩具级”演示应用和服务，以及提供量子算法、量子软件初步运行和验证等“工具级”服务为主，随着未来量子计算软硬件不断发展完善，

“杀手级”和“工业级”应用出现之后，量子计算云平台也将逐步向“商用级”演进，其中云平台标准化、服务服务保障、安全性等仍面临诸多挑战，还需要业界共同研究探讨和持续推进。

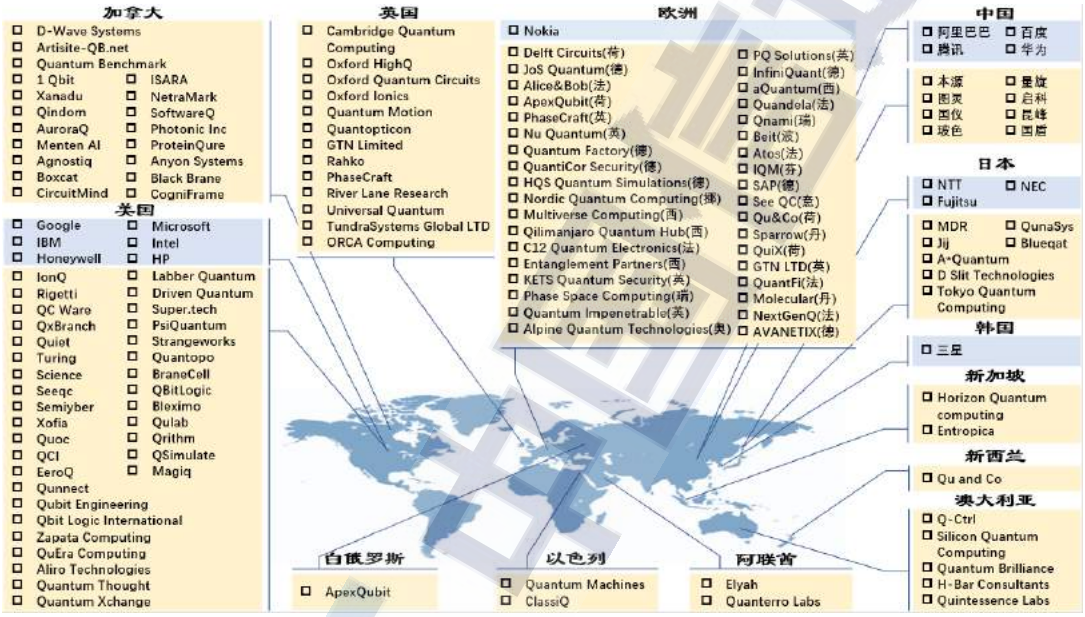
（五）科技巨头与初创公司并进，产业生态逐步培育

在量子计算领域，美国已形成政府部门、科技巨头和行业企业等多方投入推动，高校、科研机构和初创企业协同分工配合发展格局，依托科研项目部署、公司研发计划、开源社区建设和产业联盟组织，在基础科学研究、软硬件工程研发、应用场景探索和产业生态培育等方面全方位推动。在应用场景探索和产业生态培育等方面，科技巨头和初创公司表现活跃，成为主要推动力量。

科技巨头在量子计算领域竞争激烈，是推动量子计算技术与应用加速发展的主要动力。IBM、Google、Microsoft、Intel、Honeywell、Amazon 等美国科技巨头均已进军量子计算领域，具备资金投入雄厚、工程技术成熟、软件能力突出、云计算资源丰富等优势，开展包括量子计算硬件、软件算法、云服务及应用服务在内的全套研发。我国的科技企业进入相对较晚，阿里、百度、腾讯、华为等主要采取与科研机构合作或聘请领军科学家模式，分别成立量子实验室，在量子计算硬件、软件算法、云平台及应用服务等方面进行布局。

初创企业是促进量子计算活跃发展的另一重要组成部分。目前，全球已有百余家量子计算初创企业，如图 10 所示，地域分布以美国、欧洲（含英国）和加拿大最为密集，覆盖量子计算技术栈的各个层级。

最新进展包括，2021 年 10 月 D-Wave 发布路线图[23]，计划开发基于门的量子计算机，提出下一代量子计算平台将包括退火和基于门的量子计算机，致力于成为同时拥有两种技术方案的量子计算硬件公司；2021 年 10 月，Strangeworks 推出后台通行证计划[24]，扩展量子计算技术访问和服务范围；IonQ、Rigetti 和 QCI 等量子计算初创公司，在 2021 年已开始登陆美国纳斯达克资本市场[25]。



来源：中国信息通信研究院根据公开信息整理（截至 2021 年 10 月）

图 10 量子计算领域科技公司和初创企业分布情况

科研机构、科技巨头、初创公司与行业企业开展应用探索合作。2021 年 4 月，D-Wave 与 NEC 和澳大利亚国防部合作开展量子计算计划，优化自动驾驶汽车从中央基地为军队提供补给的解决方案[26]。5

[23]https://www.dwavesys.com/company/newsroom/press-release/let-s-get-practical-d-wave-details-product-expansion-cross-platform-roadmap/

[24] https://strangeworks.com/newsroom/strangeworks-announces-backstage-pass-quantum-hardware-program

[25]https://www.quantumcomputinginc.com/press-releases/quantum-computing-inc-lists-on-nasdaq-capital-market

[26]https://www.dwavesys.com/company/newsroom/press-release/nec-d-wave-and-the-australian-department-of-d

月，Intel 与 QuTech 联合解决控制半导体量子比特低温下高保真度运行技术问题[27]。6 月，IBM 宣布与英国哈特里中心开展建设国家数字创新中心量子计算研究的联合项目，并将 IBM 量子计算系统集成至 Strangeworks 平台[28]。Google 量子计算框架 Cirq 与 IonQ 全面整合[29]。Honeywell 宣布其量子解决方案公司与剑桥量子计算公司合并[30]，旨在提供高性能量子计算机和全套量子软件。7 月，Rigetti 宣布与 Riverlane、Astex Pharmaceuticals 合作开发应用程序用于药物发现[31]。10 月，微软宣布 Azure 支持 IBM Qiskit 以及 Google Cirq。

	IBM	Microsoft	日本企业	德国企业	芬兰企业	加拿大企业	本源量子
联盟名称	IBM Q Network	Microsoft Quantum Network	Northwest Quantum Nexus	Q-STAR	Qutac	BusinessQ	QIC	OQIA
成立时间	2017年12月	2019年3月	2019年3月	2021年9月	2021年6月	2021年9月	2020年10月	2018年7月
联盟成员（部分）	.....	.....	.....	.....	.....	.....	.....	.....
措施	提供量子专业知识与资源，基于云访问先进、可扩展的通用量子计算系统	协作开发实用解决方案，加强教育、精进技能、发展人才	开设课程培训，举办研讨会，量子初创企业孵化和分拆	产学研各界与政府合作，推动应用新技术计划，建立技术平台	明确战略路线图，参与标准化和知识产权制定，确定教育和技能需求	促进各类公司合作，开设论坛，组织产学研研讨会	促进与合作伙伴的交流，培养量子人才，部署和扩展商业途径	与学术界、产业界合作，培育量子软、硬件开发者
目标	培育发展的生态系统，加速并扩展量子计算	开拓型协作社区，构建全球量子合作伙伴生态系统	推进QIS研究，培养受过QIS培训的人才	以量子技术创新为导向，利用量子优势创造新产业	将现有量子计算基础发展为工业应用，为德国和欧洲产业化奠定基础	制定业务路线图，扩大量子技术对芬兰工业和商业的影响	将加拿大量子创新和人才转化为加拿大的成功产业化	推进各行业量子计算发展，拓展量子计算产业生态圈

来源：中国信息通信研究院根据公开信息整理（截至 2021 年 10 月）

图 11 量子计算领域产业联盟发展情况

efence-collaborate-on-quantum-computing-initiative/

[27] https://www.nature.com/articles/s41586-021-03469-4

[28]https://strangeworks.com/newsroom/strangeworks-and-ibm-announce-integration-of-ibm-quantum-cloud-services-into-the-strangeworks-ecosystem

[29] https://ionq.com/news/june-10-2021-2021-06-10-ionq-adds-integration-with-google-cirq

[30]https://www.honeywell.com/us/en/press/2021/06/honeywell-quantum-solutions-and-cambridge-quantum-computing-will-combine-to-form-worlds-largest-most-advanced-quantum-business

[31]https://www.globenewswire.com/news-release/2021/07/13/2261611/0/en/Rigetti-Computing-Partners-with-Riverlane-Astex-Pharmaceuticals-to-Advance-Quantum-Computing-for-Drug-Discovery.html

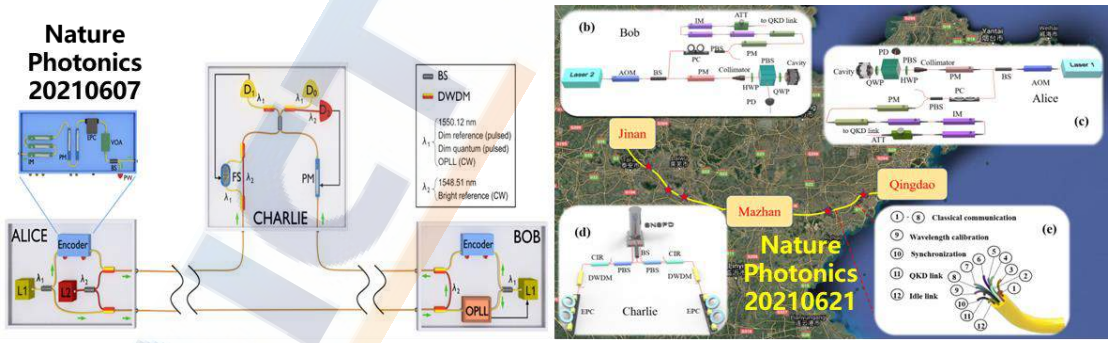
产业联盟成为促进量子计算技术发展和培育产业生态重要手段。全球各国高度重视量子计算发展，通过构建产业联盟来积极推动技术研发和产业发展。目前，全球主要量子计算产业联盟如图 11 所示。IBM 成立 IBM Q Network 目前已有包含政府及科研机构、初创企业、行业应用合作伙伴等在内百余家成员，覆盖航空、汽车、银行、能源等十余个应用领域，致力于推动行业合作，培育量子计算生态系统。微软发起 Microsoft Quantum Network 与 Northwest Quantum Nexus，主要包括解决方案合作方、下游潜在客户及研究机构三类成员，致力于推进量子计算发展并探讨实际应用。日本 24 家企业联合成立量子战略产业革命联盟 Q-STAR，包含不同应用领域企业，与政府和科研机构、产业界充分合作，旨在评估与量子技术相关的基本原则与法律，并就其适用性和必要产业结构提出建议。德国 10 家企业成立量子技术与应用联盟 Qutac，在确定经济中量子计算需求的基础上，明确现阶段可能实现的行业应用，评估量子计算的工业化实施潜力，实现指明行业发展方向和为成员创造价值的目的。芬兰建立量子计算产业联盟项目 BusinessQ，目标在于制定量子商业路线图，扩大量子技术对芬兰工业与商业的影响。加拿大成立量子产业部 QIC，由 20 余家量子企业组成，旨在加速技术创新、实现人才转化及推进量子技术商业化进程。我国本源量子于 2019 年建立本源量子计算产业联盟，加速技术开发和探索应用落地，2021 年联合国内多家生物化学企业组成“量子计算生物化学行业应用生态联盟”。

三、量子通信领域研究与应用进展

（一）量子通信科研多方向不断深化，进展成果丰富

量子通信领域包含量子密钥分发（QKD）、量子隐形传态（QT）、量子安全直接通信（QSDC）、量子数字签名（QDS）等诸多协议与应用，同时 QT 结合量子存储中继和量子态转换等技术，可连接量子计算机等量子信息处理节点，构建量子信息网络。2021 年量子通信各方向科学研究与实验探索持续活跃，取得一系列进展和成果。

在 QKD 研究方面，无存储中继传输距离再创新高，密钥分发传输信道“上天下海”，系统设计实现不断简化。东芝欧研报道[32]实验室环境下双波段参考光相位补偿的 605 公里双场（TF）QKD 传输实验，如图 12（a）所示，成码率为 0.97bit/s。中科大报道[33]在济南-青岛 511 公里超低损现网光纤中基于时频传递方案的 TF-QKD 传输实验，如图 12（b）所示，成码率为 3.45bit/s。



（a）东芝欧研实验室605公里TF-QKD实验　　（b）中科大现网511公里TF-QKD实验

来源：中国信息通信研究院根据公开信息整理

图 12 TF-QKD 传输距离新记录（a）东芝欧研（b）中科大

[32] https://doi.org/10.1038/s41566-021-00811-0

[33] https://doi.org/10.1038/s41566-021-00828-5

南京大学报道[34]基于无人机中继的1公里距离地面站之间空-地量子纠缠分发链路实验，提供自由空间 QKD 灵活组网新方案。美国伊利诺伊大学报道[35]采用 3D 打印光路系统小型化 QKD 设计方案，推动无人机 QKD 实用化发展。上海交大报道[36]在实验室 30 米较浑浊海水（Jerlov III 型）信道中的诱骗态 BB84 协议 QKD 传输实验，量子信道误码率<2.5%，成码率为 220.5bit/s。东芝欧研报道[37]GHz 工作频率，无需波长相位反馈调节简化 MDI-QKD 系统实验，54dB 信道损耗成码率 8bit/s。英国剑桥大学报道[38]500MHz 工作频率，参考光与量子光交替发送，组合参数优化的简化本地本振 CV-QKD 系统实验，15 公里光纤传输成码率为 26.9Mbit/s。

在 QT 实验研究方面，高维与确定性量子态传输是重要发展方向。中科大报道[39]基于光子路径自由度编码和辅助纠缠光子对的六光子系统三维量子隐形传态实验，保真度为 59.6%。美国芝加哥大学报道[40]超导同轴线连接的量子比特节点间的确定性纠缠分发实验，传输保真度达到 91.1%。德国马普所报道[41]基于单光子源的确定性 QT 协议，实现 60 米距离量子存储器间 6 位量子态传输，保真度为 88.3%。荷兰 Delft 报道[42]实现偏振编码光学输入状态到一对纳米机械谐振器的联

[34] https://doi.org/10.1103/PhysRevLett.126.020503

[35] https://doi.org/10.1117/12.2582376

[36] https://doi.org/10.1103/PhysRevApplied.15.024060

[37] https://doi.org/10.1038/s41534-021-00394-2

[38] https://doi.org/10.1038/s41598-021-88468-1

[39] https://doi.org/10.1103/PhysRevLett.127.110505

[40] https://doi.org/10.1038/s41586-021-03288-7

[41] https://doi.org/10.1103/PhysRevLett.126.130502

[42] https://doi.org/10.1038/s41566-021-00866-z

合状态的 QT 传输，开展光-机械量子态转换探索。

量子存储中继是未来拓展量子通信应用，实现量子信息网络的关键使能技术，目前仍处于开放性研究探索阶段，实用化前景不明朗。瑞士日内瓦大学报道[43]稀土晶体中 1338nm 纠缠光子存储和输出测量实验，CHSH 不等式违背 S=2.64，有望成为固态量子存储中继器原型。西班牙 CIFO 报道[44]稀土晶体固态存储器预报式纠缠分发实验，存储时间 25 微秒，使用下转换纠缠光源演示 50 米光纤存储纠缠分发。中科大报道[45]基于吸收型固态量子存储器和光频梳多模存储方案，实现双存储器之间 6000 对光子/秒速率预报式纠缠分发，保真度达 80.4%；还报道[46]基于原子频率梳操控稀土晶体光子存储实验，存储时间达到 1 小时，保真度为 96.4%。清华报道[47]两个数十毫秒存储时间的原子系综量子存储器之间，执行按需交换纠缠扩展性实验。此外，中科大还提出了基于无噪声光子回波（NLPE）固态量子存储的原创性方案[48]，可有效降低光子存储噪声并提高保真度。

[43] https://doi.org/10.1038/nature09662

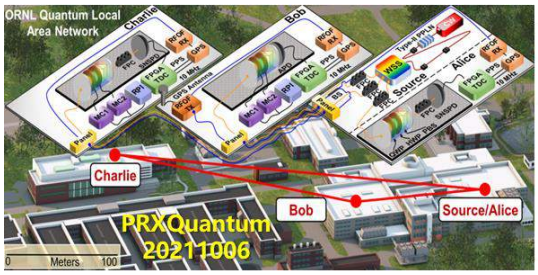
[44] https://doi.org/10.1038/s41586-021-03481-8

[45] https://doi.org/10.1038/s41586-021-03505-3

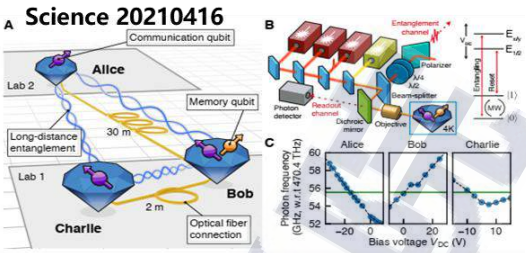
[46] https://doi.org/10.1038/s41467-021-22706-y

[47] https://doi.org/10.1038/s41566-021-00764-4

[48] https://doi.org/10.1038/s41467-021-24679-4



(a) 美国ORNL三节点量子纠缠局域网实验



(b) 荷兰Delft NV色心三节点量子纠缠网络

来源：中国信息通信研究院根据公开信息整理

图 13 量子信息网络原型试验（a）美国 ORNL（b）荷兰 Delft

在量子信息网络（也称量子互联网）的原型组网试验方面，近期欧美发展迅速。美国加州理工、费米实验室和 AT&T 联合团队报道[49]建立量子网络原型实验床，基于 1536.5nm 保真度>90%的光子纠缠源结合全光纤耦合组件进行时间位置编码，实现 44 公里量隐形传态实验，系统频率 90MHz，隐形传输速率 Hz 量级。荷兰代尔夫特（Delft）理工报道[50]基于金刚石色心量子比特的三节点 GHZ 态量子纠缠网络组网如图 13（a）所示，具备确定性纠缠产生和前馈式纠缠操作特性，预报纠缠交换效率达每 40 秒 1 次。美国橡树岭实验室（ORNL）、斯坦福大学和普渡大学联合团队报道[51]三节点量子纠缠局域网原型实验，如图 13（b）所示演示动态重构通道的光子偏振纠缠资源灵活分发和远程状态制备，各节点纠缠保真度>92%。

其他量子通信协议研究方面，2020 中关村论坛发布北京量子院与清华大学研制 QSDC 第二代样机，可实现 10 公里光纤链路中 4kbit/s

[49] https://doi.org/10.1103/PRXQuantum.1.020317

[50] https://doi.org/10.1126/science.abg1919

[51] https://doi.org/10.1103/PRXQuantum.2.040304

信息通信速率和量子加密电话应用。上海交大报道[52]基于时间-能量纠缠与和频产生的 15 用户 QSDC 原理演示组网实验，用户之间可实现保真度>95%的纠缠共享，信息传输速率可达 1kbit/s。南京大学报道[53]基于后匹配处理方法和六态非正交编码的新型 QDS 方案，降低安全分析复杂性，提高数据使用效率。

（二）以星地量子通信为契机促进空间量子科学发展

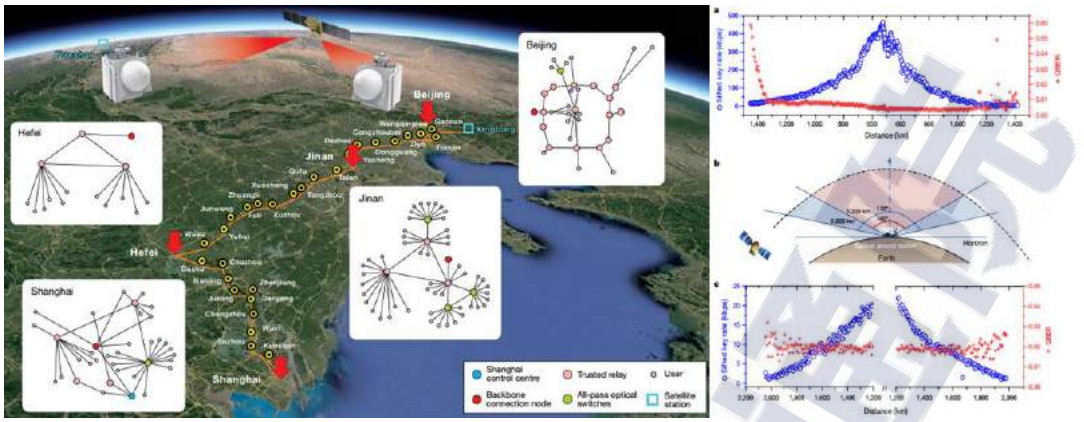
基于卫星平台的星地量子通信方案，具有信道损耗小、接入灵活性高、覆盖面广和生存性强等优点，成为量子通信科学研究和实验探索的热点方向。2016 年 8 月，中科大联合航天科技集团等多家单位，成功发射了全球首颗量子科学实验卫星“墨子号”，并在之后 4 年取得一系列国际领先科研实验成果[54]。2021 年 1 月，中科大 Nature 发文[55]，对基于“墨子号”量子科学实验卫星和量子保密通信“京沪干线”技术验证及应用示范项目，验证天地一体化量子通信组网可行性科研成果进行回顾综述，如图 14 所示。通过提升工作频率、地面站望远镜尺寸和耦合效率，使用非平衡选基新协议等改进措施，在理想气象条件下单轨（约 6 分钟）星地 QKD 密钥成码率比早期结果提升 40 倍，可达 47.8kbit/s，每周密钥生成量的理想化最大值约 36Mbit。

[52] https://doi.org/10.1038/s41377-021-00634-2

[53] https://doi.org/10.1364/OE.433656

[54] http://www.caict.ac.cn/kxyj/qwfb/bps/202012/P020201215373063374434.pdf 第 39 页

[55] https://doi.org/10.1038/s41586-020-03093-8



来源：Nature volume 589, pages214–219 (2021)

图 14 基于“墨子号”卫星和“京沪干线”天地一体化组网验证

虽然“墨子号”卫星高标准、超预期的完成了预定科学实验任务，并在国内外开展了基于星地 QKD 的量子保密通信初步示范应用[56]，但需要指出的是，基于卫星平台的星地 QKD 传输组网要走向实用化，仍面临诸多需要解决的技术和工程挑战。“墨子号”是低地轨道（LEO）卫星，单轨可用传输时间和地面覆盖范围有限，由于工作波长和背景光噪声限制，仅能在夜间工作，同时星地空间光路可用性受地面天气状态影响明显，星地之间实时协商后处理功能尚未完善，上述局限性导致“墨子号”在科学实验价值之外的实用化能力仍较为有限。此外，卫星与地面站的体积、重量、成本，以及任务实施部署费效比，也是开展工程研究和应用探索中不得不考虑的限制因素。

尽管星地量子通信在工程和应用等方面仍面临重重挑战，但相关

[56] https://doi.org/10.1103/PhysRevLett.120.030501
冯宝,李国春,俞学豪,赵子岩,卞宇翔.量子保密通信电网应用情况及研究进展[J].信息通信技术与政策,2021,47(07):39-45.

科研和实验探索也在持续稳步开展和推动。据中科大科研团队报告[57]，在 LEO 量子通信卫星实用化研究方面，开发载荷重量约 30 千克微纳 QKD 卫星，工作频率提升至 625MHz，具备基于激光通信的实时密钥协商后处理功能，同时已研发重量小于 100 千克的可移动式地面接收机，提升地面站部署灵活性，预计未来基于 3-5 颗较低成本微纳卫星或可覆盖全球上百用户，提供 QKD 密钥每周更新服务。针对下一代地球静止轨道（GEO）卫星量子通信需求，中科大报道[58]基于 1550nm 工作波长，在 53 公里距离实现白天条件的地面自由空间 QKD 传输，为突破地影区工作限制开展前期验证；“墨子号”开展了低仰角（5°）远距离（2000 公里）星地 QKD 传输实验，初步验证了万公里距离的星地 QKD 传输可行性。同时，布局 GHz 频率光源系统、高效率背景光噪声抑制、大口径高精度光学系统和自适应光学接收等技术攻关。MDI-QKD 协议系统自由空间传输实验验证取得进展[59]。

基于前期空间量子通信的科研成果和技术积累，推动开展下一代空间量子科学研究和实验探索，将成为未来的发展方向和重要目标。卫星是开展大尺度条件量子科学实验的理想平台，基于 GEO、地月乃至深空卫星，可以开展包含观测者自由意志随机选择的量子力学非定域检验，进一步证明和完善量子物理学基础理论。同时，卫星平台具备的高真空、微重力环境和机动变轨等能力，可支持构建大尺度高精度光量子干涉实验环境，为空间引力波和暗物质探索提供新方案，

[57] 2021 年全国量子信息技术学术交流大会，中国苏州，2021 年 9 月

[58] https://doi.org/10.1038/nphoton.2017.116

[59] https://doi.org/10.1103/PhysRevLett.125.260503

推动基础科学理论验证和发展。此外，新型光学原子钟技术不断发展，稳定度指标进入 10^{-19} 量级，对下一代秒定义中的时频传递精度提出更高要求，地基时频比对由于潮汐效应和环境运动等影响将难以满足需求。基于低引力场噪声卫星平台，一方面可进一步提升光钟稳定度，另一方面结合光梳信号干涉双向比对，可以实现与光钟稳定度匹配的超高精度时频传递，构建未来新一代时间基准与授时网络。

（三）QKD 应用场景持续探索，产业化水平仍待提升

QKD 技术的应用场景和价值主要体现在，或者从严格意义上讲仅限于，为各类对称加密应用提供收发双方的共享密钥。相比传统的基于 RSA 等公钥加密算法的互联网密钥交换（IKE）方案，一方面，QKD 能够提升共享密钥生成过程的安全性，即具备窃听感知能力，需要说明的是，这种量子力学特性和 QKD 协议提供的窃听感知能力仅限于密钥分发过程，并不涉及后续密钥层面存储管理、二次转发和中继组网，以及应用层面的信息加密传输等过程；另一方面，根据 YD/T 3834.1-2021 标准规范[60]，商用化 QKD 设备应具备 kbit/s 量级的密钥生成速率，可为对称加密算法提供更高频率（可达秒级）的初始密钥更新，上述两项特性有望提升对称加密体系安全防护能力。

基于 QKD 的量子保密通信，首先要解决收发双方“密钥可达性”问题。如前节所述，自由空间和卫星 QKD 等方向主要处于科学研究和实验探索阶段，尚无大规模实用化前景。商用 QKD 系统基于光纤信道传输，由于微弱光信号等物理特性和筛选压缩等协议特性限制，

[60] http://www.csres.com/detail/364660.html

现网光纤传输距离约为数十公里量级。城域范围内可以通过光路开关控制，实现时分复用组网，如一收多发轮询成码或多收发交替成码等。由于量子中继尚不可用，商用 QKD 系统长距离传输和大范围组网，需依靠多段光纤信道传输，逐段生成 QKD 密钥，再结合“可信中继”节点的密钥存储和转发中继来实现，该过程已不再具备量子力学特性，只能依靠传统方式，如中继密钥异或处理和站点信息安全等级保护等措施，保护密钥存储和二次转发的安全性。这也是对基于现有 QKD 产品和方案，推动大规模广域网络建设，构建所谓“密钥基础设施”的提法，存在可行性和必要性争议的重要原因之一。

基于 QKD 的量子保密通信在各类场景中的应用，还要探索解决“加密融合性”问题。对于有线通信网络中的量子保密通信，将各类量子加密设备，如 VPN、路由器、OTN 设备等，在原有网络中进行融合组网应用的部署方案主要可分为旁挂、串联和替换三种。其中，旁挂式部署将加密设备与原有设备并联，可以在不改变原有网络拓扑的基础上，通过业务流量引导实现按需加密，同时原有设备可在加密设备故障或密钥资源不足等情况下，提供保护倒换备份。串联式部署则将加密设备在原有设备的客户侧串接，需对网络拓扑进行调整，可通过网关和端口等配置，实现业务按需加密或透传。替换式部署是将原有设备更换为量子加密设备，实现所有业务流量加密，需保证传输性能和稳定性不低于原有设备，加解密时延符合业务场景需求。目前，大多数基于光纤网络的量子保密通信应用场景，如城域政务网、数据中心互联、电力专网通信等，基本采用上述三种部署模式。

在无线通信网络中实现 QKD 密钥的融合加密应用，是量子保密

通信技术拓展应用场景和提升产业发展潜力的重要探索方向。2021年6月，俄罗斯研究团队报道[61]，在自动驾驶车辆上安装QKD设备，在加油或充电期间通过光纤连接与控制中心进行密钥分发，在基于无线通信的车辆软件升级和关键信息传输等过程中，提供量子加密VPN保护，提升自动驾驶车辆的信息安全性，为未来QKD技术在车联网中的应用进行初步探索。但是，对于智能手机等小型无线终端而言，直接集成QKD设备并提供光纤或空间光路连接尚不具备现实可行性。一种退而求其次的解决方案是将QKD密钥通过SIM或存储卡充注等方式，离线加载到无线终端，供通信过程加密使用。近期，国内有相关企业推出上述手机加密解决方案并开展商用探索。需要指出的是，与“可信中继”节点的密钥存储和中继转发类似，QKD 密钥的离线存储充注也不再具有任何量子属性，与传统预置密钥或密钥协商方案的差异性如何体现，应用模式能否得到市场认可，仍有待观察。

量子保密通信技术在工程和应用层面还存在较为明显的局限性[62]，商用化推广和产业化发展仍处于探索培育阶段。2021 年，英国电信（BT）公司与东芝公司合作报道[63]，在国家复合材料中心和建模仿真中心的7公里光纤链路中部署和测试QKD和量子保密通信系统，对工业机器人远程操控通信过程进行保护，初步探索工业互联网加密应用。此外还报道[64]在伦敦建设连接码头区、金融城和 M4 走廊开发区

[61]https://thequantumdaily.com/2021/06/01/qrate-demonstrates-protection-for-autonomous-vehicles-with-qkd-device/

[62] http://www.caict.ac.cn/kxyj/qwfb/bps/202012/P020201215373063374434.pdf 第三章第五节

[63] https://www.eenewseurope.com/news/quantum-network-manufacturing

[64]https://newsroom.bt.com/bt-and-toshiba-to-build-worlds-first-commercial-quantum-secured-metro-network-across-london/

的量子保密通信城域网，探索提供基于 QKD 和抗量子计算破解加密（PQC）的数据保护服务。我国在海口[65]、福州[66]、重庆[67]等地量子保密通信网络建设和示范应用陆续开展。中国电信启动量子铸盾行动[68]，计划在多个城市开展城域量子密钥分发和加密应用探索，并推广移动终端用户的量子加密通话服务等。电信网络运营商的加入有望为提升量子保密通信技术实用化水平，推动商用化发展注入新动力。

（四）PQC 升级成大势所趋，QKD 发展需明确定位

量子计算技术将对以公钥密码体系为基础的信息通信网络安全构成严重威胁，已成为全球各国管理机构、学术界和产业界普遍共识。当前公钥密码体系用于密钥封装和数字签名的公开密钥，安全性普遍基于素数乘积因式分解的计算困难问题。1994 年，快速分解素数乘积的量子多项式 Shor 算法提出，成为量子计算信息安全威胁的发端。随着各类型量子计算原理样机研制工作近年来加速发展，这一威胁正逐步从理论走向现实。2021 年 4 月，Google 报道[69]基于两千万位含噪量子物理比特处理器，可在 8 小时计算破解 RSA-2048 公钥，比之前估计硬件资源减少两个数量级。尽管目前量子计算样机物理比特数仅为百位量级，距离能够有效运行 Shor 算法仍有较大差距，但据近期 IBM 和 Google 发布的量子计算发展路线图显示，预计到 2030 年左右

[65] https://res.hndaily.cn/file/news/20210413/cid_106_232012.html

[66] http://www.szzg.gov.cn/2021/xwzx/fhzx/202105/t20210507_5589895.htm

[67] http://www.bishan.gov.cn/bmjz/bm_97237/fwygwh/dt/202108/t20210818_9593515.html

[68] http://www.chinatelecom.com.cn/news/06/5G/zxdt/xwdt/202011/t20201127_58478.html

[69] https://quantum-journal.org/papers/q-2021-04-15-433/

量子计算样机将达一百万位物理比特规模。美国智库兰德公司预测[70]，能够破解密钥的量子计算机将可能在 2033 年左右出现。

量子计算可能引发信息安全风险包含两方面：一是破坏性风险，量子计算将现有的绕开加密体系，寻找漏洞和后门的迂回攻击模式，升级演变为针对加密体系和密钥进行暴力计算破解的直接攻击模式，将对通信信息安全造成基础性破坏。二是追溯性风险，对于需要长期安全性防护的敏感信息，如解密期限长达数十年的外交军事情报等，可能出现加密信息已被截获存储，目前虽暂时无法破解，但在量子计算技术发展成熟之后，从而产生信息破解泄露的风险。

为应对量子计算带来的通信安全风险，欧美密码学界提出抗量子计算破解加密（PQC）算法，目标是开发面对量子计算和经典计算均能够保证加密安全性的新一代公钥密码体系，主要关注基于格、基于散列、基于编码和基于多变量等新型加密算法，构造方案、性能参数和安全性等方面各有特色，可用于公钥加密、数字签名和密钥封装等不同场景。PQC 标准化以美国为主导，欧洲为主要推动力量。2016 年 12 月，NIST 启动 PQC 算法标准全球公开征集评比，2020 年 7 月进入第三轮评比[71]，对 7 项入围算法进行最终评估，预计在 2023 年左右形成 PQC 算法国际标准。近期，美国国家安全局（NSA）发布 PQC 展望[72]，支持 NIST 标准化研究成果，计划在国家安全信息系统采用

[70] https://www.rand.org/pubs/research_reports/RR3102.html/

[71] https://csrc.nist.gov/News/2020/pqc-third-round-candidate-announcement

[72]https://www.nsa.gov/Cybersecurity/NSAs-Cybersecurity-Perspective-on-Post-Quantum-Cryptography-Algorithms/

基于格的密钥封装和数字签名算法，逐步升级替代 RSA 等算法[73]。

如前节所述，QKD 可以替换基于 RSA 的 IKE 自协商密钥交换，为对称加密算法直接提供共享密钥，在理论协议层面具备信息论可证明安全性，被认为可用于应对量子计算信息安全威胁。但需要指出，第一，QKD 不适用于非对称加密场景，也不能用于数字签名和身份认证，QKD 大规模组网过程中的高效设备身份认证可采用 PQC 算法辅助解决[74]。第二，QKD 技术在系统工程化、建设部署和运行维护的成本与难度等方面存在一定局限性和较高要求，难以支撑在各类信息安全系统中的大规模广泛应用，近期全球多国信息安全管理机构，均就此表明技术立场和观点[75]。第三，QKD 和 PQC 对比中谈论较多的是，PQC 安全性基于新型数学困难问题无法被计算破解的假设，目前量子计算技术和算法研究仍不充分，PQC 难以证明可以抵御未来可能出现的新型攻击，即存在未知风险。而鲜少提及的是，QKD 需要依靠实际物理系统实现，安全性不能仅以理论协议一言蔽之，其系统和组网现实安全性本身也是讨论热点[76]。尚无研究可以证明，实际 QKD 系统或网络中，已不存在任何未知的系统漏洞和被攻击风险。因此，仅从存在未知风险的角度而言，QKD 和 PQC 二者逻辑等同。

面对量子计算可能引发的信息安全威胁，各国管理机构普遍支持 PQC 是未来公钥密码体系升级演进的主流方案，应用推广将是大势

[73] https://media.defense.gov/2021/Aug/04/2002821837/-1/-1/1/Quantum_FAQs_20210804.PDF

[74] https://doi.org/10.1364/OE.432944

[75] http://www.caict.ac.cn/kxyj/qwfb/bps/202012/P020201215373063374434.pdf 第三章第四节 https://www.nsa.gov/Press-Room/News-Highlights/Article/Article/2394053/nsa-cybersecurity-perspectives-on-quantum-key-distribution-and-quantum-cryptogr/

[76] http://www.caict.ac.cn/kxyj/qwfb/bps/201912/P020191226517744813705.pdf 第三章第四节

所趋。对此，我们应进一步加强 PQC 技术和标准研究，争取与国际同步推出自主可控的 PQC 算法、标准和应用产品，针对核心密码、普通密码和商用密码在不同领域面临风险和应用需求，制定分级应对策略，及时部署和推进公钥密码体系的 PQC 升级。

2021 年 6 月，美国 Gartner 公司发布《中国量子通信创新洞察》报告[77]，其中指出中国将量子技术纳入“十四五”规划，在量子通信研究领域处于领先。但是，在能够以现实条件下实现远距离和安全的量子通信之前，QKD 尚不具备商业可行性。此外，量子安全密码学，即 PQC 的发展也挑战了 QKD 的必要性。

未来，QKD 应用探索需进一步明确发展定位，找到区别于 PQC 的差异化发展空间。在有长期保密性需求和高安全性要求的专用通信领域中，基于光纤或空间光信道，直接进行量子态传输和密钥成码，再结合一次一密对称加密算法进行保密通信传输，是真正体现 QKD 技术优势的典型应用场景，可在满足行业需求和管理标准的前提下，率先探索推动。但是，如果 QKD 技术还叠加了“可信中继”组网、密钥存储转发、密钥离线充注、商用加密算法等种种“折中妥协”，则相对 PQC 技术难言明显优势，其商业模式和应用推广能否走通，需要产业界努力开拓和探索，并交由用户和市场来判断和选择。

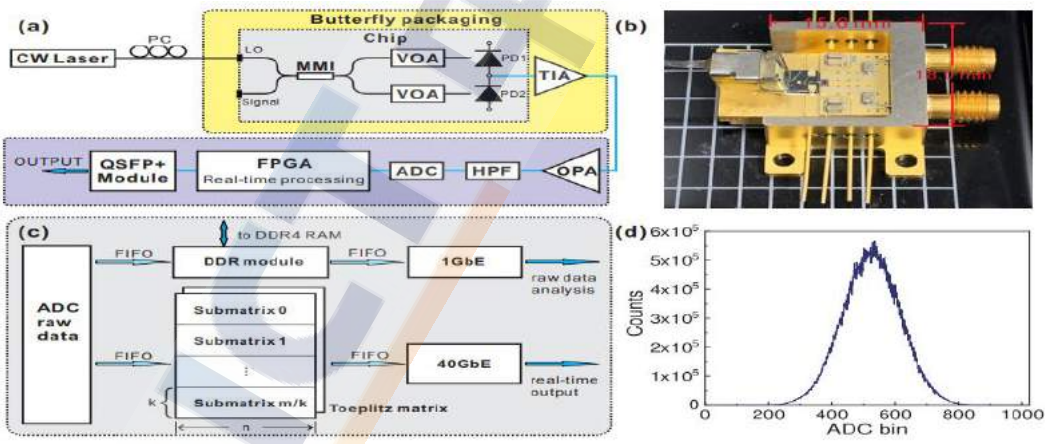
（五）基于 QRNG 的加密应用成为关注与探索新方向

随机数是统计学和密码学等领域的重要资源，在模拟仿真、信息加密、博彩交易等应用场景中发挥着不可替代的作用。能够产生随机

[77] https://www.gartner.com/en/documents/4002882/innovation-insight-for-quantum-communication-in-china

数的机制和设备称为随机数发生器，有多种技术方案，其中基于软件算法，如线性反馈移位寄存器等，生成随机数称为伪随机数发生器（PRNG），优点是简单易行，统计特性能满足初级应用需求，但本原多项式和初值等特性导致不可预测性较差，较难满足密码学等高级应用需求。基于硬件随机过程，如电路噪声和热噪声等来制备随机数，称为真随机数发生器（TRNG），优点是物理随机过程提升不可预测性，但建立严格的随机性理论模型困难，且生成速率较低。

利用量子物理体系的内禀随机性，如量子态坍缩等，进行随机数生成制备，称为量子随机数发生器（QRNG），由量子力学理论模型保证其真随机性，同时随机数生成速率可达更高水平。2021 年中科大报道[78]，基于真空态涨落光子集成电路，如图 15 所示，实现芯片化系统中 18.8Gbit/s 的量子随机数生成速率新纪录。



来源：Appl. Phys. Lett. 118, 264001 (2021)

图 15 中科大基于 PIC 芯片的真空态涨落 QRNG 系统

[78] https://doi.org/10.1063/5.0056027

QRNG 包含量子态制备与测量、后处理信息压缩、以及状态监测等基本功能模块[79]。其中，量子态制备测量产生随机信号熵源可用多种方案，技术成熟度和商用化发展水平较高的是相位涨落、真空态涨落、放大自发辐射噪声等。相位涨落 QRNG 以临界工作状态激光器产生自发辐射光子，通过干涉仪将光子信号中的相位涨落转化为强度涨落，经光电探测后输出熵源信号。真空态涨落 QRNG 通过本地本振激光器对真空态输入信号进行干涉测量和平衡零差探测，获得熵源信号。放大自发辐射 QRNG 对放大自发辐射（ASE）噪声光源，如超辐射二极管等，直接进行光电信号探测得熵源信号。QRNG 信息压缩后处理过程可采用多种随机数提取方案，但推荐用具备量子信息侧信道消除能力的强提取器，如 Toeplitz 提取器和 Trevisan 提取器。此外，QRNG 推荐具备量子熵源状态和输出序列随机性检测等状态监测功能，为系统正常运行和稳定工作提供保障。

与 QKD 相比，QRNG 系统的光电子学组件简单，后处理协议的复杂度低，具备集成度和可靠性高，成本低的优势。但是 QRNG 仅具备本地化的量子随机性提供能力，并不直接生成密钥，而 QKD 能实现更高安全性的量子随机性“拉远”，并在收方双方之间直接生成共享密钥。基于 QRNG 产生高速率、高质量随机数源，可替代传统公钥密码体系的 PRNG，用于数据库加密、用户身份认证、VPN 加密等多种类型加密任务，提升信息系统的整体安全防护水平，有望成为未来量子技术在信息安全领域应用的另一重要发展方向。

[79] http://www.csres.com/detail/367425.html

QRNG 已在国内外实现了多种类型技术方案、系统产品乃至芯片化产品的多厂家商用化。近期，国内外通信运营商、互联网科技企业和行业专网等用户也积极开展基于 QRNG 的加密应用探索。2021 年，美国量子加密应用服务商 Qrypt 报道[80]，与西班牙 Quside 公司合作，通过云服务为企业网和物联网嵌入式系统提供基于 QRNG 和 PQC 的融合加密方案。韩国电信运营商 SKT 报道[81]，联合三星和瑞士 IDQ 公司推出第二款加载芯片化 QRNG 的 Galaxy 手机，并拓展相关加密应用服务。阿里报道[82]，基于多款商用化 QRNG 构建量子随机数云平台，在智能网关和数字金融等场景的 VPN 中，提供密钥随机数源和身份认证等服务。工商银行报道[83]，使用 QRNG 为客户登录、支付结算、资金交易等金融场景，提供客户信息标识和校验。

四、量子测量领域研究与应用进展

（一）量子测量技术发展面向超高精度和超经典能力

量子测量是利用量子特性获得更高性能的测量技术，特性可归纳为“一二三四五”，即一种基础定义、两个核心特征、三种主要类型、四个基本步骤和五大技术方向。基础定义是基于对微观粒子系统的调控和观测，实现对物理量超高精度测量的技术。两个核心特征是测量系统中的操作对象是微观粒子；微观粒子在待测物理场中演化导致量子态的改变，直接或间接地反映待测物理量的大小。三种主要类型包

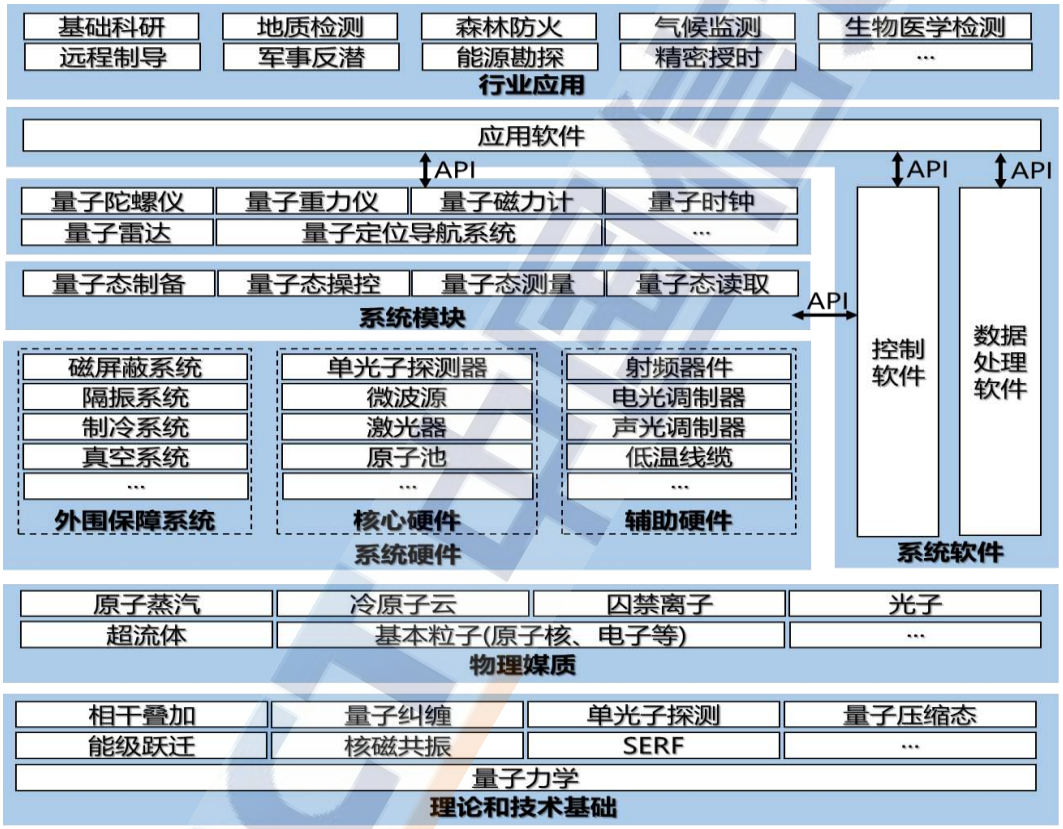
[80] https://www.qrypt.com/qrypt-quside-press-release

[81] https://www.sktelecom.com/en/press/press_detail.do?idx=1503

[82] https://doi.org/10.1038/s41534-021-00442-x

[83] https://www.financialnews.com.cn/yh/sd/202105/t20210511_218309.html

括基于分立能级结构测量、基于量子相干叠加测量和基于量子纠缠/压缩态测量，对应量子测量技术发展演进三个阶段，精度不断提升，可突破标准量子极限（SQL），但系统复杂度和体积成本也相应提升。量子测量的四个基本步骤是：量子态的制备与初始化、量子体系在待测物理场中演化、演化后量子态读取、结果处理输出。五大典型技术方向包括时频基准、磁场测量、重力测量、惯性测量和目标识别。



来源：中国信息通信研究院

图 16 量子测量技术体系框架

近年来，量子测量技术的科学研究不断探索极限，工程样机逐步发展成熟，各领域应用积极探索，产业化发展初步启动。量子测量技术的体系框架如图 16 所示，以量子力学为理论基础，运用相干叠加、

量子纠缠等量子物理特性对原子、离子、光子等基本粒子进行量子态制备、操控、测量和读取；配合数据的处理与转换，实现对角速度、重力场、磁场、频率等物理量的精密探测；之后通过控制处理软件进行信号转换处理，并通过应用层软件将测量结果呈现给用户。

在理论基础方面，量子测量技术的物理理论和原理机制研究基本明确，大量理论和实验证明利用量子能级跃迁、量子相干叠加、量子纠缠等物理特性可实现多种物理量的精密测量。随着激光冷却、磁光阱、光抽运、单光子探测等使能技术的逐渐成熟，量子测量技术优势日益凸显。但需要说明，部分关键技术仍有待突破，如量子纠缠态高效确定性产生方法和远距离分发技术等。

在物理媒质方面，根据测量物理量和技术方案不同，可选用原子、离子、光子，甚至电子、原子核等基本粒子作为物理媒质。热门技术路线包括冷原子干涉、核磁共振、顺磁共振、无自旋交换弛豫原子自旋（SERF）、量子纠缠、量子压缩、量子增强技术等，不同技术路线和物理体系可适用于不同物理量的测量应用场景。例如，自旋原子核具有磁矩，天然地具有测量电磁场和角速度的能力；而物理量“秒”采用铯原子同位素基态超精细能级之间的跃迁频率来定义，因此利用冷原子或囚禁离子能级跃迁是测量优选方案。

在系统硬件方面，大致可以分为核心硬件、辅助硬件和外围保障系统三个部分。核心硬件是实现量子测量过程的最关键元器件，如用于粒子存储保持的原子气室，用于量子态制备和调控的激光器或微波源，用于量子态探测和读取的单光子探测器等。辅助硬件包括射频器件、高频线缆、光电信号放大器、现场可编程逻辑门阵列（FPGA）、

数据采集系统、电光/声光调制器等。此外，量子测量系统对外界环境干扰十分敏感，需要振动隔离、磁屏蔽、温度控制等外围保障。

在样机系统研制方面，不同技术和应用方向的发展水平各异，微波原子钟、冷原子重力仪、SERF 陀螺仪、单光子量子雷达等已经实现系统产品的商用化，光学原子钟、高精度量子磁场测量平台、量子纠缠/照明雷达等尚处于原理样机研制和实验探索阶段。样机系统研发主要集中在高校、科研机构和防务企业，不断探索和刷新性能指标，提升工程化和实用化水平，同时部分成熟技术领域开始孵化初创公司，推出商用产品并开展产业化应用探索。

在系统软件方面，主要包括控制软件、数据处理软件和用户应用软件。控制软件配合系统硬件实现量子态的制备、调控、测量、读取，并且协同各模组之间运作。相关研究表明，控制软件与人工智能或量子计算相结合，在测量过程中对制备的量子态进行优化，可以实现测量性能的提升。量子测量采用原子或者光子级别的载体作为测量“探针”，信号强度弱，易淹没在噪声当中，并且噪声理论模式复杂难以通过信号处理补偿或抑制，因此需要数据处理软件进行后处理。人工智能算法适合解决模型复杂、参数未知的数学问题。通过将量子测量与人工智能技术相结合，提升数据后处理能力，可以提升实用化水平。应用软件通过 API 接口和软件界面将测量结果反馈给用户。

在行业应用层面，量子测量技术积极探索基础科研、航天国防、生物医疗、能源勘探、精密授时等诸多领域的新型应用场景。在新一代定位、导航和授时系统，磁场和重力场高灵敏度监测系统和高精度目标识别系统等方向有望率先获得突破和应用。部分技术已经开展了

试点应用，尚未进入规模商用阶段。量子测量技术需要与垂直行业需求充分融合，才能推动产业化发展。

（二）样机性能指标不断提升，新方向探索取得进展

量子测量一直是量子信息领域科研热点方向。一方面，随着技术成熟和系统优化，量子测量精度、稳定度、环境适应性、体积功耗等性能指标不断提升。另一方面，除了相对成熟的量子频率基准、量子磁力计、量子重力仪、量子陀螺仪和量子目标识别五大方向，新技术方向和应用也不断涌现，拓宽了技术路线，为更多物理量（如温度、应力等）的精密测量奠定了理论和实验基础。

量子时频基准方面，2019 年，第 26 届国际计量大会已将铯-133 原子不受干扰的基态超精细能级跃迁频率定义为常数，原子钟正式成为秒长基准。如果使用激光冷却或离子俘获技术，可将原子钟的理论稳定度进一步提高 2~3 个数量级，并且光频率也比微波频率高 4~5 个数量级，因此与原子微波钟相比，光学原子钟在稳定性和不确定度等指标方面都将有数量级改善。目前，光钟的不确定度和稳定度指标均进入 10^{-19} 量级，其中美国 NIST 的铝离子光钟不确定度极限达到 9.5×10^{-19}，相当于 330 亿年不差一秒。我国量子时频基准科研处于跟跑状态，2020 年中科院精密测量研究院报道钙离子光钟频率不确定度达到 10^{-17} 量级[84]，与国际先进水平尚有差距。国外也开始开展基于量子纠缠的光钟研究，进一步提升准确度。2020 年美国麻省理工报

[84] https://academic.oup.com/nsr/article/7/12/1799/5851766

道成果在 SQL 上实现了 4.4dB 的增益[85]。光钟远程比对方面，2021 年美国博尔德原子钟光学网络联盟通过自由空间和光纤链路两种方式比对三台光钟[86]，实现了创纪录的频率比值测量准确度，为未来秒定义奠定重要基础。高精度时频传递方面，2021 年中科大演示了 16 公里自由空间的光频率信号传递[87]，模拟验证地球静止轨道链路未来可以用于远程光钟的比对。

量子目标识别方面，量子探测技术灵敏度远高于传统方法。探测目标可以是硬目标，如飞行器等，也可以是软目标，比如烟雾、云团、甚至某种气体成分等。进一步利用量子纠缠、量子压缩等性质还可以实现超越经典极限的探测精度，但该技术难度大，远距离传输退纠缠、退压缩现象明显，2020 年报道纠缠量子雷达仅对 1 米处的目标进行了探测[88]，向更远的距离应用扩展困难。量子成像利用光场二阶或高阶关联获得物体图像信息，可实现超分辨、3D、全息或者非视域成像，是近年来研究热点，取得诸多突破性成果。英国格拉斯哥大学首次用量子纠缠光子来将信息编码为全息图，可创建更高分辨率、更低噪声图像。中科大使用集成化同轴单光子雷达，实现 205.1 公里 3D 成像实验[89]；利用上转换单光子探测器实现毫米级空间分辨精度的非视域成像实验[90]。澳大利亚昆士兰大学实现量子增强非线性显微镜[91]。

[85] https://www.nature.com/articles/s41586-020-3006-1

[86] https://www.nature.com/articles/s41586-021-03253-4

[87] https://www.osapublishing.org/optica/fulltext.cfm?uri=optica-8-4-471&id=449900

[88] https://www.science.org/doi/10.1126/sciadv.abb0451

[89] https://doi.org/10.1063/5.0021214

[90] https://doi.org/10.1103/PhysRevLett.127.053602

[91] https://www.nature.com/articles/s41586-021-03528-w

实验证明量子关联信噪比超过传统显微镜极限。中科大与美国麻省理工合作，利用周期极化铌酸锂波导，搭建颜色擦除强度干涉仪，对1.43 公里外相距 4.2 毫米的两个不同波长光源目标进行区分测量[92]。

量子陀螺仪方面，基于量子效应的原子陀螺仪被称为第三代陀螺仪，与传统陀螺仪相比，在测量精度、体积功耗等性能参数方面具有独特优势。冷原子干涉陀螺仪理论精度最高，零偏有望低于 10^{-10} °/h，可实现超高精度的角速度测量。美国斯坦福大学、法国巴黎天文台、中科院精密测量研究院等团队近年取得诸多成果。其中，精密测量院研制的高精度冷原子干涉仪原理样机零偏指标与 2018 年的国际报道水平相当。核磁共振陀螺仪技术相对成熟，体积小成本低，可满足民用场景需求。航天院所自主研发的小型化核磁共振陀螺仪工程样机已通过温循、振动、冲击测试，具备实用化能力。SERF 陀螺仪精度高，可满足未来防务装备惯性指导需求。北航研究团队的 SERF 原子陀螺样机零偏稳定性指标，已优于国际公开报道最好水平。除了以上三类，一些量子陀螺仪新技术路线也被提出和验证。2021 年上海交大团队提出轨道角动量原子-光混合 Sagnac 干涉仪，提高测量旋转的精度[93]。量子陀螺仪与经典陀螺仪各具优势，借鉴组合守时系统和组合导航系统的思路，未来可采用原子陀螺仪驾驭和矫正光纤陀螺仪，抑制误差发散，同时保证导航系统的采样率和长期稳定性。

量子重力仪方面，利用冷原子干涉可实现重力绝对值和重力梯度的精密探测。中科院精密测量院研发冷原子重力梯度仪样机分辨率已

[92] https://journals.aps.org/prl/abstract/10.1103/PhysRevLett.127.103601

[93] https://www.osapublishing.org/oe/fulltext.cfm?uri=oe-29-1-208&id=445046

达 0.9E（1E=$10^{-9}/s^2$），冷原子重力梯度仪是绝对重力梯度仪，无机械磨损，测量频率和时序定位精度高，理论上不存在漂移，将是高精度重力匹配辅助惯性导航与水下大型目标引力场探测的理想技术方案。目前冷原子重力仪、重力梯度仪进入小型化和工程化开发阶段，美国加州大学、法国宇航院、中科院精密测量研究院、浙江工业大学等完成车载/船载等外场测试，验证系统稳定性和实用性。此外一些新技术方案也被提出，2021 年以色列本-古里安大学在原子芯片上实现斯特恩-格拉奇干涉仪，可用于重力检测[94]，基于磁场调控原子量子态，可在短距离用作高精度表面探针，避免激光热效应。

量子磁力计方面，利用原子自旋量子态可以实现磁场的精密测量，特别是基于金刚石 NV 色心的磁场测量技术近年来备受瞩目。中科大基于金刚石固态单自旋体系，在室温环境实现突破 SQL 的磁测量[95]。比利时哈塞尔特大学利用金刚石 NV 色心磁力仪绘制地磁场地图，可提供纳米尺度测量分辨率，响应时间低于百纳秒[96]。目前，欧空局已将其带入国际空间站，用于在太空中测试金刚石量子传感技术。

新型量子测量探索方面，被测物理量进一步扩展到温度、力学量、相位、距离和痕量等。2021 年，之江实验室研制的基于光动量效应量子精密测量装置完成验收[97]，力探测灵敏度达$3.4 \times 10^{-19}\mathrm{N}/\sqrt{\mathrm{Hz}}$，分辨率达$4.6 \times 10^{-21}\mathrm{N}$。中科大用全光激发实现对稀有同位素氪-81 的

[94] https://www.science.org/doi/10.1126/sciadv.abg2879

[95] https://www.science.org/doi/10.1126/sciadv.abg9204

[96]https://www.electronicsweekly.com/blogs/gadget-master/space/picture-day-space-bound-magnetometer-uses-diamond-based-quantum-technology-2021-09/

[97] https://baijiahao.baidu.com/s?id=1693537072203644724&wfr=spider&for=pc

单原子探测[98]，这种原子阱痕量分析的检测方法，对地球与环境科学研究将有推动作用。德国维尔茨堡大学提出一种新型氮化硼原子传感器[99]，展示了原子尺度的磁场、温度、压力测量传感功能。

量子测量技术工程化方面，近年使能组件的研究取得一定进展。英国牛津大学和伯明翰大学研发一种新冷原子源装置[100]，可用于便携式量子技术设备，可用于频率基准、重力测量、惯性导航以及暗物质和引力波探测等领域，由于组件少、安装简单，因此易于规模量产，适合商业应用。美国科罗拉多大学研制时间相关单光子计数器[101]，实现 550fs 单光子定时分辨率，可能推动成像技术的重大改进。

信号处理软件算法方面，亚利桑那大学结合可变量子线路和经典机器学习[102]，训练矢量量化控制模型，定制传感器共享多部分纠缠，解决数据处理问题，数据分类错误率低于经典模型，有望实现超灵敏惯性导航，促进早期疾病医疗诊断。中科大报道结合深度学习和稀疏矩阵补全技术的纳米核磁共振波谱分析成果[103]，10%采样覆盖率下，信噪比提高 5.7dB。美国路易斯安那大学利用人工神经网络自主学习进化特性[104]，在单光子水平校正扭曲的拉盖尔高斯模复杂空间轮廓，对单光子成像的湍流实时校正具有重要意义。

[98] https://journals.aps.org/prl/abstract/10.1103/PhysRevLett.127.023201

[99] https://www.nature.com/articles/s41467-021-24725-1

[100] https://www.osapublishing.org/oe/fulltext.cfm?uri=oe-29-14-21143&id=452608

[101] https://arxiv.org/abs/2009.01069

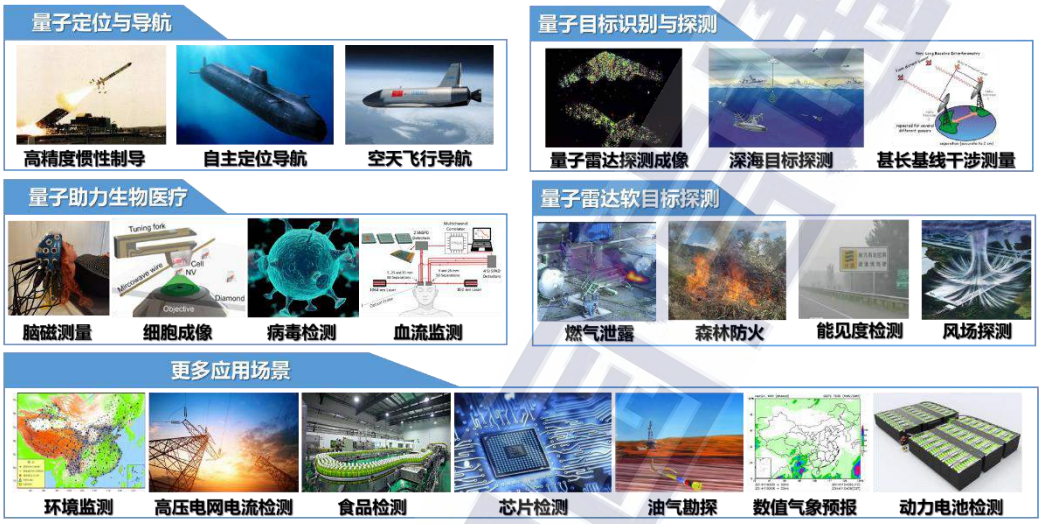
[102] https://journals.aps.org/prx/abstract/10.1103/PhysRevX.11.021047

[103] https://www.nature.com/articles/s41534-020-00311-z

[104] https://onlinelibrary.wiley.com/doi/10.1002/qute.202000103

（三）技术应用场景和领域广泛，多方开拓发展活跃

量子测量技术涵盖多种物理量的精密检测，在各学科和行业领域拥有广泛应用场景，相对于经典测量技术在性能指标上的跨越式提升是加速其应用发展的决定性因素。



来源：中国信息通信研究院

图 17 量子测量技术的典型应用场景

量子测量技术典型应用场景如图 17 所示。基于量子陀螺仪、重力仪、时钟及时频传递技术的新一代定位/导航/授时系统在航天和国防等领域具有重要战略价值，量子磁力计、单光子探测雷达和金刚石色心传感器等则在生物技术科研、心脑磁医疗诊断、大气环境探测和高端工业制造检测等民用领域极具应用前景，近年来技术研究、样机产品研制、以及应用探索发展迅速。

在定位导航应用领域，民用领域定位导航应用主要依靠全球卫星定位导航系统，如 GPS、北斗和 GLONASS，而国防领域定位导航则

需要考虑在卫星定位导航不可用条件下，基于重力和惯性等测量技术的自主定位导航。随着运载工具覆盖范围不断提升，对定位制导精度提出了更高要求，量子陀螺仪角速度测量的零偏稳定度理论极限可达10^{-10}°/h，可实现万公里距离下的米级定位精度。同时，发射平台提高生存性和隐蔽性要求实现长航时高精度自主定位导航，量子重力仪测量精度可达小数点后九位，与量子陀螺仪等配合，可实现米/年精度的自主定位导航。除超高精度之外，量子定位导航技术在体积功耗等方面也有潜在优势，例如量子陀螺仪部分技术方案在具备高精度同时，核心组件尺寸仅为厘米级，同时兼具低功耗优势，将是未来各类自主定位导航应用领域的技术升级演进重要方向。

在目标识别探测领域，雷达利用电磁波进行目标探测识别，对探测距离和分辨率等提出更高要求。单光子探测增强激光雷达通过提升光子探测效率提升雷达探测性能。例如量子激光雷达在百公里低层大气环境外场实验中，相比同参数经典激光雷达，可提升空中目标探测距离一倍以上。在海底目标探测中，微波和光学探测手段受限，高精度磁场探测将成为可选技术方案。量子磁力计具有 fT 量级的超高检测灵敏度，能够对海底金属物体存在和移动导致的地磁场微弱变化进行检测，有望成为提升态势感知能力的重要手段。天文观测中，常常使用长基线干涉测量或者甚长基线干涉测量，基线长度可以从几公里到几千公里甚至洲际距离，可拥有高分辨率，又能敏感捕捉微弱信号，虚拟一个“地球级别”的巨大望远镜。多个天文望远镜的观测数据要进行相干计算，因此需要高精度的时间同步和相位同步。目前，光钟精度已经进入 10^{-18}~10^{-19} 量级，结合量子时频传递技术可支持甚长基线

的干涉测量和深空探测等方面应用。

在生物医疗应用领域，生物体产生的磁场信号携带重要生理和病理信息，但信号强度非常微弱，使用传统测量手段难以有效检测。量子磁测量技术与传统心电图、脑电图、核磁共振成像等技术相比，具备超高测量灵敏度，且对人体无损无创，可用于心磁、脑磁探测，为神经科学、脑科学研究，疾病早期诊断等领域提供全新解决方案。2021年，俄罗斯量子中心报道[105]适用于脑磁图的室温固态量子传感器，理论灵敏度小于 1 fT/√Hz 具有较宽动态范围，使用前不需要校准。英国萨塞克斯大学构建模块化量子大脑扫描仪，记录大脑磁场信号；量子传感与计时技术中心开发可穿戴 SERF 光泵浦磁力计用于脑磁图探测，已安装在多伦多儿童疾病医院，用于自闭症研究。我国北航等团队研制用于心脑磁测量的阵列式小型化原子磁强计探头，与国内十余家医院合作开展临床应用探索，未来进一步提高灵敏度、降低体积，提高实用化水平，可用于辅助重大心脑疾病诊断。

金刚石氮空位（NV）色心技术高空间分辨率和非侵入式探测可以用于活体细胞的检测与成像，对于细胞动力学、癌细胞标记与筛选、药物运输与代谢等方面研究与应用提供了新手段。英国伦敦大学报道[106]，自旋增强纳米金刚石传感器可以用作体外病毒信息检测，对 HIV 病毒检测实验中，比传统使用金纳米颗粒的检测灵敏度提高了九万倍，同时开展了 SARS-CoV-2 新冠病毒检测的实验。

单光子探测技术可以用于非侵入性脑部血流检测。美国马萨诸塞

[105] https://onlinelibrary.wiley.com/doi/10.1002/hbm.25582

[106] https://www.nature.com/articles/s41586-020-2917-1

州综合医院和麻省理工学院报道[107]将超导纳米线单光子探测器应用到扩散相关光谱系统中实现头部脉动血流情况监测，使得光子检测效率提升近 13 倍，获得高频率、低信噪比的脉动血流，未来有可能实现非侵入脉动血流监测诊断颅内压力。利用纠缠光源可实现量子增强型 X 射线显微镜，通过分离光束，研究样品暴露于 X 射线中的剂量较小，由于没有穿过样品的光子与穿过样品的光子是相关的，因此可以保持全剂量 X 射线束的分辨率。美国布鲁克海文国家实验室预计在 2023 年实现 10nm 空间分辨率的微米级物体的 X 射线显微技术。

在大气环境监测领域，单光子激光雷达可以实现烟雾、云团甚至特定气体成分等“软目标”探测，与林业、气象、交通、能源等行业相结合，探索应用场景。与气体光谱学结合，还可实现对二氧化碳或者甲烷等温室气体的分布进行成像，从而可以快速可视化和量化管道或储气设施中的泄漏情况，或者进行环境污染监测。森林防火方面，单光子激光雷达可以对火灾产生的烟尘进行监测，监控火灾异常，与传统雷达相比该技术实时性强扫描时间可由小时级缩减至分钟级，与视频监控技术相比，不受雨雾等恶劣天气和自然背景光影响，昼夜阴晴均可工作。公路、机场和港口航道能见度探测方面，可实时进行路面、航道团雾检测，红外波段对人眼更安全。气象观测方面，可开展高空大气边界层、风场、温湿度等参数观测。

在高端工业检测领域，学术界和产业界也在积极探索更多的潜在用户和应用场景。金刚石 NV 色心量子测量技术广泛开展跨行业应用

[107]https://www.spiedigitallibrary.org/journals/neurophotonics/volume-8/issue-3/035006/Superconducting-nanowire-single-photon-sensing-of-cerebral-blood-flow/10.1117/1.NPh.8.3.035006.full

探索，比如面向锂电池生产厂商的正负极金属残留缺陷的弱电流检测；面向电力行业的高压电网电感圈电流灵敏检测；面向食品安全领域的食品、烟草等材质自由基成分检测；以及面向石油行业的油井开采中的随钻核磁成像检测等。

（四）量子测量产业化尚处起步阶段，产业链待完善

量子测量技术方向众多，应用领域覆盖面广，其中部分成熟技术方向已开始进入从工程样机向商用产品的过渡阶段。近年来，国内外逐步开始出现由高校和科研机构转化，专注于量子测量技术产品研发和应用推广的初创企业，但是总体而言，量子测量商业化应用和产业化规模仍较为有限，发展还处于初级阶段，产业链及生态尚不成熟，量子测量技术产业链和代表性企业，如图 18 所示。

来源：中国信息通信研究院根据公开信息整理

图 18 量子测量技术产业链与代表性企业视图

欧美国家在量子测量领域研究基础深厚，技术产品种类比较丰富，

近年来已出现了十余家专注量子测量技术的初创企业，产品类型包含原子钟、原子重力仪、原子加速度计、量子磁力计、量子激光雷达、量子图像传感器、金刚石色心显微镜等多个技术和应用领域，并积极在通信网络、地质勘探、航天国防、电力能源等领域探索应用。

近期，量子测量技术备受资本市场青睐，公开报道显示，2020 年 11 月，英国 M Squared 公司宣布获得 3250 万英镑新融资，支持量子测量和量子计算等领域研发。2021 年 4 月，英国量子激光雷达公司 QLM 获得 310 万英镑种子融资，支持其扩展下一代温室气体监测的业务。5 月，瑞士金刚石色心量子显微镜公司 Qnami 宣布已完成 A 轮融资，募集资金为 400 万瑞士法郎，用于 ProteusQ 商用量子显微镜系统的量产以及新应用领域探索。法国 iXblue 公司宣布收购量子测量公司 Muquans，希望成为欧洲光子和量子技术领域领导者。

欧美多家量子测量公司近期也推出新产品和方案。2021 年 6 月，美国 Gigajot Technology 公司发布首批量子图像传感器产品，其读出噪声性能比传统 CMOS 成像提升 5~10 倍。8 月，英国量子磁力计公司 Cerca Magnetics 在多伦多儿童医院成功安装了第一套 OPM-MEG 系统，用于自闭症研究。9 月，英国量子激光雷达公司 QLM 与无人机公司 Inzpire 合作，研究基于量子激光雷达探测甲烷排放能力。

总体而言，量子测量产业化处于起步阶段，市场和行业规模不大。主要原因在于，一方面量子测量技术门槛比较高，需要量子物理学和测试计量等领域的知识和技术积累，对高端专业人才素养要求严格。目前大部分量子测量企业都是从高校或者科研院所孵化；另一方面，除了量子雷达和磁力计等具有明确的民用场景外，其他方向主要定位

于航天国防等应用场景，市场相对封闭，难以大规模商业推广。

我国量子测量企业主要由高校和科研院所的科研团队创立，产品主要集中在原子钟、量子雷达、顺磁共振谱仪、量子重力仪等领域，近年来不断扩展市场，探索量子测量技术在不同领域、不同行业的应用场景与解决方案。量子测量技术路线繁多，原理差异性大，产业的上游材料、器件提供商的种类也比较多。并且我国上游产业链仍存在短板和待提升空间。我国量子测量上游产业短板的主要原因大致可以分为以下三类：一是，国内不具备商用化规模生产供给能力或者产品性能不能满足需求；二是，国内具有研发生产能力或潜力，但是产品需要定制或市场规模过小，仅靠市场化供给难以支持相关研发制造需求；三是，需要结合工程设计或应用需求重新定制化开发。总体而言，当前国内外量子测量产业发展在早期阶段，产业资源集中在核心系统设计及整机的工程化开发中，在大规模应用推广到来之前量子测量的应用对上游的牵引力还不足，导致上游有实力的元器件及工艺厂商在面向量子产业的研发投入不足，制约产业整体发展。

量子测量产业的下游目前还没有明确界定。量子测量技术的优势在于超高的测量精度，因此在诸多领域都具有应用前景。然而具体的应用结合点以及解决方案，有赖于量子测量企业与垂直行业用户深入交流合作才能明确。可通过在典型行业试点应用取得一定成果后，让更多用户了解量子测量技术优势，进一步开展跨行业领域推广。目前最具潜力的量子测量行业级产品应用在航空航天、高端材料检测、医疗成像等领域，产品推广面临行业较长的论证和准入周期，这也是建立下游生态需要解决的问题。量子测量技术产品精度已超出传统检测

机构或者第三方认证机构的传统能力范围。需要研究建立量子测量的标准与测评认证体系，明确量子测量产品指标及测试方法，打通检测认证环节，为推动技术产品应用和产业发展提供指导。

五、量子信息技术演进与应用前景展望

（一）各领域研究持续推进，应用产业探索广泛开展

量子计算、量子通信和量子测量为代表的量子信息技术，是未来突破经典技术极限，拓展科学新疆域的重要发展方向，其研究与应用将成为推动基础科学探索、信息技术演进和数字经济发展的“触发器”和“催化剂”。近年来，量子信息技术已经成为全球各主要国家科技政策和发展规划的关注焦点之一，投资支持力度不断加大，科学研究、产品研发、应用探索和产业培育的体系化布局初显。量子信息各领域科研发展迅速，技术创新与知识产权布局活跃，标准化研究取得阶段性成果，将成为推动技术与应用迭代演进的重要支撑。随着量子信息领域样机产品不断涌现和发展成熟，商业化应用探索和产业链构建等工作也开始成为各方关注热点。美、欧、日、德等国家和地区均成立量子信息领域产业培育组织，增进跨领域交流协同，推动应用场景探索，加大投融资支持力度，开展供应链和人力资源建设。

量子计算领域是目前各方关注与期望焦点，科学研究和技术研发亮点纷呈，多领域应用探索蓄势待发，创新创业与投融资增长迅速，发展趋势强劲。超导、离子阱、光量子和半导体等多种技术路线并行发展，量子计算优越性获得实验验证，比特数量规模和质量参数进一步提升，但在可扩展性、操作复杂度、噪声抑制能力和集成化水平等

方面仍有诸多挑战，实现大规模通用量子计算未来仍需长期艰苦努力。NISQ 软件算法研发欣欣向荣，编程语言、编译工具、操作系统、EDA 设计软件等大量出现，处于开放竞争阶段。量子计算/模拟技术在金融、化学和医药等领域应用探索广泛开展，但真正具备实际社会经济价值的“杀手级”应用仍未明确，能否保持发展热度尚待观察。科技巨头和初创企业等通过云平台、开源社区和产业联盟等方式，开展竞争与合作，用户习惯培养和产业生态构建。量子计算领域集科研、工程、应用和产业为一体的发展格局初步显现。

量子通信领域包含多种协议和应用方向，发展和应用程度各异。基于 QT 构建量子信息网络仍是远期发展目标，尚无实用落地前景，近年来欧美在使能组件研究和组网试验验证方面发展较为迅速。基于 QKD 的量子保密通信初步实用化，科研方面持续保持活跃，无存储中继传输距离再创新高，系统设计实现不断简化。与传统 IKE 协商密钥相比，QKD 能提供更高更新速率和安全性的密钥共享，相关应用场景探索持续开展，但在工程和应用层面还存在较为明显的局限性，商用化推广和产业化发展仍处于探索培育阶段。我国在星地量子通信科研实验取得系列重要成果，未来有望进一步研究提升实用化水平，并以此为契机加快推动空间量子科学研究与发展。面对量子计算技术快速发展带来的信息安全威胁，推动 PQC 升级演进已成为共识趋势，我国需加强技术标准研究，掌握自主可控算法和应用升级能力。此外，基于 QRNG 的信息加密应用正逐步成为探索发展新方向。

量子测量技术能够实现超高测量传感精度和灵敏度，具备超越经典技术改变游戏规则的巨大潜力。量子测量包含多种技术方案，发展

方向主要涵盖时间基准、惯性测量、重力测量、磁场测量和目标识别，同时开拓温度、力学量、相位、距离和痕量等新兴方向。基于量子陀螺仪、重力仪、时钟及时频传递技术的新一代定位/导航/授时系统在航天和国防等领域具有重要战略价值。量子磁力计、单光子探测雷达和金刚石色心传感器等在生物技术科研、心脑磁医疗诊断、大气环境探测和高端工业制造检测等领域极具应用前景。近年来，国内外逐步开始出现由高校和科研机构转化，专注于量子测量技术产品研发和应用推广的初创企业。总体而言，量子测量技术方案多元、系统复杂度高、应用场景较为分散，民用推广门槛较高，商业应用和产业化规模目前较为有限，发展处于初级阶段，产业链及生态尚不成熟。

（二）国内外发展态势与促进研究应用发展的关注点

在量子信息技术国际发展态势方面，以下几点值得关注和重视。第一，量子信息技术研究发展与应用探索仍将具有长期性和不确定性。量子计算多种技术路线并存发展尚未收敛，关键实用化应用场景尚未突破落地，量子信息网络研究与试验处于起步阶段，量子保密通信应用场景开拓和产业发展仍面临挑战，量子测量应用和产业化水平有待进一步提升。全球各国的量子信息领域科技政策普遍重视中长期发展规划和全方位体系化布局。第二，欧美在量子信息，尤其是量子计算领域，形成管理部门、科技巨头和行业企业等多方投入推动，高校、科研机构和初创企业等分工协同配合的发展格局。基础科学研究、软硬件工程研发、应用场景探索和产业生态构建培育等方面，可能率先取得突破，未来进一步通过掌控关键使能组件，建立应用先发优势，

培养用户习惯和布局专利标准等举措，可能在应用产业发展过程中形成壁垒和垄断。第三，量子信息技术与应用产业发展亟需高水平科研与技术人才支撑，全球各国都面临量子技术领域高水平科研人员和工程研发人才紧缺的现实问题。当前新冠大流行和少数国家“小院高墙”思维，将会对全球量子信息领域的学术与人员交流，项目合作与产业投融资，国际标准化研究等方面产生负面影响。

习近平总书记重要指示为加快促进我国量子信息领域发展提供了战略指引和根本遵循。落实“十四五”规划中组建量子信息科学国家实验室，实施重大科技项目的布局举措，可进一步加强量子信息技术各领域科研体系化布局和支持投入力度。2021 年以来，中科大增设量子信息科学本科专业，清华大学成立量子信息“姚班”，相关企业推出量子信息教育实验平台等新进展，可对加强我国量子信息领域后备人才培养起到重要支撑作用。筹备组建量子信息网络产业联盟，汇聚国内量子信息学术界与产业界各方力量，有望在促进技术交流研讨、推动应用场景探索、培育构建产业生态等方面发挥积极作用。

我国量子信息技术领域发展总体态势良好，未来进一步促进研究与应用发展主要关注点包括：一是，加强学术产业交流，探索分工协同机制。依托联盟和学会等平台，组织开展应用探索、产业需求、供应链建设等方面深入交流，探索科研、工程和产业各领域的分工合作协同机制。二是，开展核心组件攻关，夯实产业发展基础。梳理总结核心器件材料和装备仪表等方面短板需求，有针对性设立产业基础类攻关项目，突破和掌握核心使能技术，为应用探索和产业化发展奠定基础。三是，推动应用产业研究，加强标准测评引导。组织行业共性

需求研究，提升支撑保障能力，进一步完善技术标准体系，制定产品技术标准，开展测评测试验证，规范引导应用产业发展。四是，拓展国际合作空间，加强海外人才引进。发挥学术团体和联盟协会等平台机构在国际交流合作中的第三方作用，设置和开展量子信息领域的国际学术、应用、产业和标准类交流合作项目，增强对海外高水平科研和工程人才的吸引和支持力度。

附录 I：量子信息技术国际/国内标准化进展

中国信息通信研究院根据公开信息整理，截至 2021 年 10 月。

表 2 ITU-T 量子信息技术标准化进展

No	ITU-T SG11 Q2	Recommendation/Report	Status
1	Q.QKDN_profr	QKDN – Protocol framework	Under development
No	**ITU-T SG13 Q16**	**Recommendation/Report**	**Status**
1	Y.3800	Overview on networks supporting QKD	Published (2019-11)
2	Y.3801	Functional requirement of the QKDN	Published (2020-07)
3	Y.3802	Functional architecture of the QKDN	Published (2021-04)
4	Y.3803	Key management for QKDN	Published (2021-03)
5	Y.3804	Control and Management for QKDN	Published (2021-01)
6	Y.3805	Software defined network control for QKDN	Under development
7	Y.3806	Requirements for QoS assurance of the QKDN	Under development
8	Y.QKDN-bm	Business role-based model in QKDN	Under development
9	Y.QKDN_frint	Framework for integration of QKDN and secure network infrastructures	Under development
10	Y.QKDN-iwfr	QKDN interworking framework	Under development
11	Y.QKDN-ml-fra	QKDN Functional requirements and architecture for machine learning	Under development
12	Y. QKDN-qos-gen	General aspects of QoS on the QKDN	Under development
13	Y.QKDN-qos-fa	Functional architecture of QoS assurance for QKDN	Under development
14	Y.QKDN-qos-ml-req	Requirements of machine learning based QoS assurance for QKDN	Under development
15	Y.QKDN-rsfr	QKDN - resilience framework	Under development
16	Y.sup70	ITU-T Y.3800-series - QKDN - Applications of machine learning	Published (2021-09)
17	Y.supp.QKDN-roadmap	Standardization roadmap on QKDN	Under development
No	**ITU-T SG17 Q4**	**Recommendation/Report**	**Status**
1	X.1702	Quantum Noise Random Number Generator Architecture	Published (2019-11)
2	X.1710	Security framework for QKDN	Published (2020-10)
3	X.1714	Key combination and confidential key supply for QKDN	Published (2020-10)
4	X.1712	Security requirements and measures for QKDN - key management	Under development
5	X.sec_QKDN_aa	Authentication and authorization in QKDN using quantum safe cryptography	Under development
6	X.sec_QKDN_cm	Security requirements and measures for QKDN - control and management	Under development
7	X.sec_QKDN_tn	Security requirements for QKDN - trusted node	Under development
8	X.sec_QKDN_intrq	Security requirements for integration of QKDN and secure network infrastructures	Under development
9	TR.sec-qkd	Technical Report: Security considerations for QKDN	Published (2020-03)
10	TR.hybsec-qkdn	Technical Report: Overview of hybrid security approaches applicable to QKD	Under development
No	**ITU-T FG-QIT4N**	**Report**	**Status**
1	D1.1	QIT4N terminology part 1: Network aspects of QIT	Published (2021-12)
2	D1.2	QIT4N use case part 1: Network aspects of QIT	Published (2021-12)
3	D1.4	QIT4N standardization outlook and technology maturity part 1: Network aspects of QIT	Published (2021-12)
4	D2.1	QIT4N terminology part 2: QKDN	Published (2021-12)
5	D2.2	QIT4N use case part 2: QKDN	Published (2021-12)
6	D2.3.1	QKDN protocols part I: Quantum layer	Published (2021-12)

7	D2.3.2	QKDN protocols part II: Key management, QKDN control layer and management layer	Published (2021-12)
8	D2.4	QKDN transport technologies	Published (2021-12)
9	D2.5	QIT4N standardization outlook and technology maturity part 2: QKDN	Published (2021-12)

表 3 ETSI 量子信息技术标准化进展

No	ETSI ISG-QKD	Group Specification/Report	Status
1	GS QKD 002	QKD Use Cases	Published (2010-06)
2	GS QKD 004	QKD Application Interface	Published (2010-12)
3	GS QKD 005	QKD Security Proofs	Published (2010-12)
4	GS QKD 008	QKD Module Security Specification	Published (2010-12)
5	GS QKD 010	Implementation security: protection against Trojan horse attacks in one-way QKD systems	Under development
6	GS QKD 011	Component characterization: characterizing optical components for QKD systems	Published (2016-05)
7	GS QKD 012	Device and Communication Channel Parameters for QKD Deployment	Published (2019-02)
8	GS QKD 013	Characterisation of Optical Output of QKD transmitter modules	Under development
9	GS QKD 014	QKD Protocol and data format of key delivery API to Applications;	Published (2019-02)
10	GS QKD 015	QKD Control Interface for Software Defined Networks	Published (2021-03)
11	GS QKD 016	Common Criteria Protection Profile for QKD	Under development
12	GS QKD 018	QKD Orchestration Interface of Software Defined Networks	Under development
13	GR QKD 007	QKD Vocabulary	Published (2018-12)
14	GR QKD 003	QKD Components and Internal Interfaces	Published (2018-03)
15	GR QKD 017	QKD Network Architectures	Under development
16	GR QKD 019	Design of QKD interfaces with Authentication	Under development

表 4 ISO/IEC JTC1 量子信息技术标准化进展

No	ISO/IEC JTC1 SC27 WG3	Standard/Report	Status
1	ISO/IEC WD 23837-1	Security requirements, test and evaluation methods for QKD Part 1: requirements	Under development
2	ISO/IEC WD 23837-2	Security requirements, test and evaluation methods for QKD Part 2: test and evaluation methods	Under development
No	**ISO/IEC JTC1 WG14**	**Standard/Report**	**Status**
1	ISO/IEC WD 4879	Information technology — Quantum computing — Terminology and vocabulary	Under development

表 5 IRTF 量子信息技术标准化进展

No	IRTF	Internet-Draft	Status
1	draft-irtf-qirg-principles-03	Architectural Principles for a Quantum Internet	I-D Exists
2	draft-dahlberg-ll-quantum-03	The Link Layer service in a Quantum Internet	I-D Exists
3	draft-kaws-qirg-advent-01	Advertising Entanglement Capabilities in Quantum Networks	I-D Exists
4	draft-van-meter-qirg-quantum-connection-setup-01	Connection Setup in a Quantum Network	I-D Exists
5	draft-wang-qirg-quantum-internet-use-cases-05	Applications and Use Cases for the Quantum Internet	I-D Exists

表 6 IEEE 量子信息技术标准化进展

No	IEEE	Project	Status
1	P1913	Software-Defined Quantum Communication	Approved PAR
2	P2995	Trial-Use Standard for a Quantum Algorithm Design and Development	Approved PAR
3	P7130	Standard for Quantum Computing Definitions	Approved PAR
4	P7131	Standard for Quantum Computing Performance Metrics & Performance Benchmarking	Approved PAR

表 7 CCSA 量子信息技术标准化进展

No	CCSA ST7	国家标准项目	状态
1	国家标准	量子保密通信应用场景和需求	报批
2	国家标准	量子通信术语和定义	在研
No	**CCSA ST7**	**行业/协会标准项目**	**状态**
1	行业标准	量子密钥分发(QKD)系统技术要求 第 1 部分：基于 BB84 协议的 QKD 系统	发布(2021-03)
2	行业标准	量子密钥分发(QKD)系统测试方法 第 1 部分：基于 BB84 协议的 QKD 系统	发布(2021-03)
3	行业标准	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	已报批
4	行业标准	基于 BB84 协议的量子密钥分发（QKD）用关键器件和模块-第 2 部分：单光子探测器	已报批
5	行业标准	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：随机数发生器	发布(2021-05)
6	行业标准	量子密钥分发(QKD)系统应用接口	在研
7	行业标准	量子密钥分发与经典光通信共纤传输技术要求	在研
8	行业标准	量子保密通信网络架构	在研
9	行业标准	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	在研
10	行业标准	量子密钥分发（QKD）网络 密钥管理单元与 QKD 设备间接口要求	在研
11	行业标准	量子密钥分发网络 网络管理系统技术要求	在研
12	行业标准	基于 IPSec 协议的量子保密通信应用设备技术要求	在研
13	协会标准	支持量子波道的 WDM 系统技术要求	在研
No	**CCSA ST7**	**研究课题项目**	**状态**
1	研究报告	量子密钥分发与经典光通信系统共纤传输研究	已完成
2	研究报告	量子保密通信系统测试评估研究	已完成
3	研究报告	量子保密通信网络架构研究	已完成
4	研究报告	量子密钥分发安全性研究	已完成
5	研究报告	量子随机数制备和检测技术研究	已完成
6	研究报告	量子保密通信网络管理研究	已完成
7	研究报告	量子保密通信网络可信中继节点技术研究	已完成
8	研究报告	连续变量量子密钥分发技术研究	已完成
9	研究报告	软件定义的量子密钥分发网络研究	已完成
10	研究报告	量子保密通信组网关键技术研究	已完成
11	研究报告	空间量子保密通信技术研究	已完成
12	研究报告	量子时间同步技术的演进及其在通讯网络中的应用研究	已完成
13	研究报告	连续变量量子密钥分发系统测评研究	在研
14	研究报告	量子保密通信网络中 MPLS 专线承载加密数据要求的研究	在研
15	研究报告	基于诱骗态方法的优化协议研究	在研
16	研究报告	面向量子密钥分发应用的集成光学技术研究	在研
17	研究报告	实用化双场量子密钥分发研究	在研
18	研究报告	量子信息网络物理层基础组件技术研究	在研
19	研究报告	基于高斯调制相干态协议的量子密钥分发系统技术要求及共纤传输研究	在研
20	研究报告	量子密钥分发、量子随机数及后量子密码在信息安全中的融合技术研究	在研
21	研究报告	量子信息网络应用场景研究	在研

表 8 CSTC 量子信息技术标准化进展

No	CSTC	行业标准项目	状态
1	行业标准	诱骗态 BB84 量子密钥分配产品技术规范	发布(2021-10)
2	行业标准	诱骗态 BB84 量子密钥分配产品检测规范	发布(2021-10)
3	行业标准	相干态连续变量量子密钥分发技术规范	在研
4	行业标准	量子密钥分发设备密钥输出接口规范	在研
5	行业标准	量子随机数发生器测评规范	在研
No	**CSTC**	**研究课题项目**	**状态**
1	研究报告	量子随机数制备和测试技术研究	在研
2	研究报告	量子保密通信中继安全性研究	在研
3	研究报告	基于量子密钥分配的网络密码机技术规范研究	结题
4	研究报告	诱骗态 BB84 量子密钥分配系统测评规范研究	结题
5	研究报告	量子随机数研究	在研
6	研究报告	基于量子密钥分发的加密通信技术体系框架研究	在研

表 9 TC578 量子信息技术标准化进展

No	TC578	标准项目	状态
1	国家标准	量子计算 术语和定义	在研
2	国家标准	精密光频测量中光学频率梳性能参数测试方法	在研
No	**TC578**	**研究课题项目**	**状态**
3	研究报告	量子计算发展趋势与标准化需求研究	在研
4	研究报告	量子计算应用场景研究	在研
5	研究报告	量子云计算技术应用发展及测评研究	在研
6	研究报告	NISQ 时代量子程序语言规范标准研究	在研
7	研究报告	超高灵敏原子惯性计量测试标准研究	在研

附录 II：缩略语表

缩略语	英文全称	中文全称
API	Application programming interface	应用编程接口
ASE	Amplified spontaneous emission	放大自发辐射
CV-QKD	Continuous variable quantum key distribution	连续变量量子密钥分发
EDA	Electronic design automation	电子设计自动化
FPGA	Field programmable gate array	现场可编程门阵列
GEO	Geostationary orbit	地球静止轨道
GPS	Global positioning system	全球定位系统
IKE	Internet key exchange	互联网密钥交换
LEO	Low earth orbit	低地球轨道
MDI-QKD	Measurement device independent quantum key distribution	测量设备无关量子密钥分发
NISQ	Noisy intermediate-scale quantum	含噪声中等规模量子处理器
NLPE	Noise-less photon echo	无噪音光子回波
NV	Negatively nitrogen vacancy	金刚石氮空位
OTN	Optical transport network	光传送网
PNT	Positioning/navigation/timing	定位/导航/授时
PQC	Post quantum encryption	抗量子计算破解加密
PRNG	Pseudo random number generator	伪随机数发生器
QAOA	Quantum approximate optimization algorithm	量子近似优化算法
QDS	Quantum digital signature	量子数字签名
QKAA	Quantum kernel alignment algorithm	量子内核对齐算法
QKD	Quantum key distribution	量子密钥分发
QKDN	Quantum key distribution network	量子密钥分发网络
QRNG	Quantum random number generator	量子随机数发生器
QSDC	Quantum secure direct communication	量子安全直接通信
QT	Quantum teleportation	量子隐形传态
SERF	Spin-exchange relaxation free	无自旋交换弛豫原子自旋
SQL	Standard quantum limit	标准量子极限
SQRAM	Sequential quantum random access memory	顺序量子随机访问存储器
TF-QKD	Two field quantum key distribution	双场量子密钥分发
TRNG	True random number generator	真随机数发生器
VPN	Virtual private network	虚拟专用网
VQE	Variational quantum eigen solver	变分量子本征求解器

中国信息通信研究院

地址：北京市海淀区花园北路 52 号

邮编：100191

电话：010-62300592

传真：010-62304980

网址：www.caict.ac.cn