电网中的量子技术与边缘设备：机遇、挑战与未来方向

Marjorie Hoegen [1], * Ren´e Glebke [2], * M. Sahnawaz Alam [1], † Alessandro David [3] Juan Navarro Adenas [4,5] Nikolaus Wirtz [6] Mario Albanese [7] Daniele Carta [7] Felix Motzoi [3,8] Antonello Monti [1] Carsten Schuck [4,5] Andrea Benigni [7,9] Klaus Wehrle [2] 和 Ferdinanda Ponci [1]

[1] *Institute for Automation of Complex Power Systems,RWTH Aachen University, 52074 Aachen, Germany*

[2] *Communication and Distributed Systems, RWTH Aachen University, 52074 Aachen, Germany*

[3] *Forschungszentrum Jülich GmbH, Peter Grünberg Institute, Quantum Control (PGI-8) 52425 Jülich Germany „ , , 48149 Münster, Germany*

[4] *Department for Quantum Technology University of Münster*

[5] *Center for NanoTechnology – CeNTech, 48149 Münster, Germany*[6] *Department of Digital Energy, Fraunhofer Institute for Applied Information Technology, Aachen 52074, Germany*[7] *ICE-1 Energy Systems Engineering, Forschungszentrum Jülich, 52428 Jülich, Germany*[8] *Institute for Theoretical Physics, University of Cologne, 50937 Köln, Germany*[9] *JARA-Energy, 52425 Jülich, Germany*

arXiv:2603.06783v1 [eess.SY] 6 Mar 2026

在现代电力系统中，边缘设备充当本地枢纽，负责收集数据、进行现场计算、感知电气参数、执行控制操作，并作为更大电网的一部分与邻近的边缘设备通信。然而，随着监测节点和控制回路数量不断增加，传统边缘设备面临着严重的局限。复杂的信号处理和决策任务可能使其不堪重负，导致延迟增加、能源消耗上升。标准传感器会受到噪声底的限制，无法检测微小变化，因此更难发现故障或不稳定性的早期迹象。同时，传统通信链路难以应对带宽限制、安全风险和日益增长的加密需求，这些因素共同拖慢并削弱了关键信息在电网中的传输。Quantum 技术有望克服这些挑战。量子计算机能够为优化和机器学习任务带来指数级加速，处理普通处理器无法应对的问题。量子传感器能够以原子级精度感知信号，使边缘设备得以更精确地了解电网动态。量子通信技术（包括量子密钥分发）提供了实现信息论安全的方法，并确保信息快速、无篡改地传送。我们探讨如何将量子技术集成到边缘设备中，并着重介绍其中的机遇与挑战。

关键词：Quantum 技术；边缘设备；Quantum 计算；Quantum 传感；Quantum 通信；电力系统网络安全

1. 引言

在物联网（IoT）和边缘设备 [1, 2] 的支持下，近年来电力系统这一大型、复杂的非线性系统正经历着转型。可再生能源（RES）和电力电子接口资源的接入加快了系统动态变化，因此需要对这些资源进行密切监测和广泛控制。完全集中式地实施这些监测与控制功能要求很高，几乎难以实现。因此，在能够通信与协作的本地设备之间分配智能和计算能力，正逐渐成为更可行的选择。边缘设备负责采集数据（传感）、执行计算，并与其他设备安全通信 [3–6]。然而，随着电网边缘设备的规模和复杂性不断增加，边缘设备越来越难以跟上发展步伐。首先，随着监测节点数量增加，本地信号处理和决策的计算负担可能迅速超出传统微控制器的能力，导致时延和能耗增加。其次，传统电磁传感器的灵敏度对噪声环境中的原子级扰动构成了严格限制，使得难以追踪那些预示故障状态或不稳定性的细微波动。第三，与边缘设备进行传统的双向通信面临带宽约束、拦截脆弱性以及日益增长的加密需求，这些因素共同损害了电网状态信息的及时性和完整性 [7–9]。

量子技术提供了一条极具前景的发展路径。从理论上讲，量子计算架构能够针对特定类别的问题实现指数级加速，例如边缘侧的机器学习任务，从而实现电网功率流的实时路径寻优和异常检测，而这些任务对于当前设备而言根本无法实现 [10–12]。例如，金刚石中的氮空位中心磁力计等量子传感器，可在实验室实验中提供纳米级空间分辨率 [13, 14], ；随着这些平台不断发展，边缘节点或许能够

* 这些作者对本研究的贡献相同。

† 通讯作者：sahnawaz.alam@eonerc.rwth-aachen.de

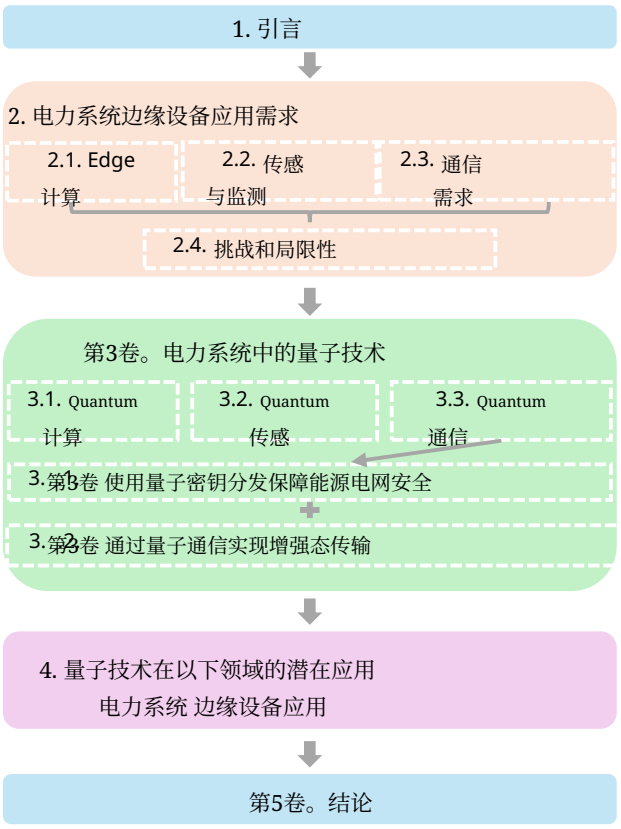

图1. 本文结构。

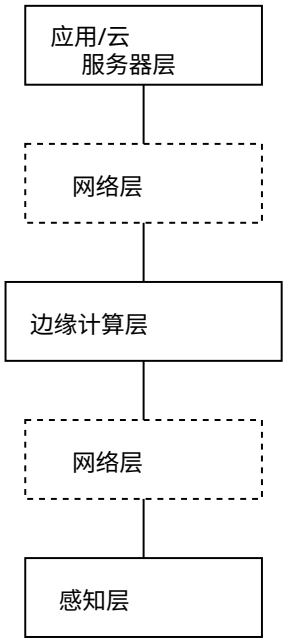

图2. 边缘计算系统的四层架构。三个主要层（感知、计算和应用）以实线框表示，网络层以虚线框表示。

分辨电网量中更微小的变化。最后，量子通信方法，尤其是量子密钥分发（QKD），能够为传输的数据提供信息论安全，确保控制命令和测量数据即使面对强大的对手也能受到保护 [15]。

在本文中，我们综述电网中边缘设备应用面临的当前挑战，并阐述量子计算、传感和通信等量子技术如何应对这些挑战。接下来，我们描述新兴量子模态，概述将其集成到下一代边缘设备中的路线图，并讨论为实现未来电力系统中所谓基于量子的边缘智能而必须应对的挑战。

如图1所示，本文的综述内容安排如下。第2节介绍边缘设备的若干需求，包括计算、传感和通信应用，以及其面临的挑战和局限性。随后，第3节介绍用于解决这些挑战的量子边缘设备相关 Quantum 技术。第4节讨论量子边缘设备的应用与挑战。最后，第5节对全文进行总结。

2. 电力系统边缘设备应用需求

2.1. 边缘计算系统

边缘计算系统的架构（图2）通常包含三个主要层级：感知层或边缘设备层、边缘计算层或边缘服务器层，以及应用层或云服务器层（图2中的实线框）。这些层级通过网络层（图2中的虚线框）相连，从而实现层间数据传输 [5, 16, 17]。各层使用的设备具有不同的特性，因为每一层的用途各不相同。靠近边缘的感知层包含负责感知并从物理环境中收集数据的边缘设备。在较高层级，边缘计算设备或边缘服务器设备具有更强的计算能力，能够预处理从终端设备收集的数据，并执行一些计算任务[4, 16]。

在 Ojo 等人 [18], 的研究中，对可用于边缘计算层的物联网设备进行了调查。这些设备分为低端、中端和高端设备，并列出和比较了它们的主要规格。低端设备被描述为资源受限设备，主要用于基本的传感和执行应用，属于边缘

计算系统的较低层。它们的时钟速度通常在 MHz 范围内，随机存取存储器（RAM）和板载存储的容量则在 kB 量级。高端物联网设备拥有更强的资源，例如强大的处理单元、大容量 RAM 和良好的板载连接。介于两者之间的是中端设备，其资源少于高端设备，但计算能力强于低端设备。中端和高端设备的时钟速度可达 GHz 范围，RAM 和板载存储的容量则可达 GB 量级。

2.2. 边缘设备中的传感与监测

用于电网监测和控制的数据由传感器采集，而传统传感器通常是体积庞大的设备，且一般仅限于变电站使用，例如仪用互感器。然而，对紧凑型传感器的需求日益增长。为了实现高效的实时监测和控制，这些传感器应能够实时测量数据，同时具备高能效。边缘设备持续测量本地电气参数（电压、电流、频率等）和设备状态，且测量粒度很高。例如，边缘的馈线传感器和智能电表能够实时检测异常或电能质量问题，从而细致呈现电网状况 [19]。这种高分辨率监测为现代电网的预测性维护和快速故障检测提供了基础。然而，边缘级电气传感器，即仪用互感器（电流互感器和电压互感器）、霍尔效应器件和罗氏线圈，其准确度等级通常为：电流互感器/电压互感器的误差范围为 0.1%–1%，罗氏线圈约为 0.5%；而开环霍尔效应传感器的满量程误差通常约为 ±3–5% [20, 21]。这些设备还可能因铁芯饱和、绝缘击穿、热漂移、接线故障以及无法检测直流分量而随时间性能下降或发生故障 [22, 23]。

2.3. 电力系统应用的通信要求

边缘设备在数据源附近处理数据，可减少对远程云服务器和控制中心的依赖，从而加快响应速度并避免网络负担 [29]。智能电网要求连接到电网发电、输电和配电环节的不同类型组件之间进行双向通信。边缘设备使用量的增加，也使通信基础设施及其要求在智能电网中发挥基础性作用，因为如此庞大的信息流必须通过可靠、安全的信道传输。

智能电网通信网络可以表示为一种分层多层架构，该架构包括短距离网络、中距离网络和长距离网络。短距离网络位于客户场所内，包括家庭区域网、楼宇区域网和工业区域网，覆盖范围可达100米。这类网络在智能电网中的一个应用示例是家庭或楼宇自动化系统。中距离网络包括邻域网和现场区域网，覆盖范围可达10公里。抄表和配电自动化可视为这类网络中的应用示例。长距离网络是广域网（WAN），覆盖范围为100公里或更远（例如，涉及同步相量的应用会使用广域网 [30]）。

智能电网各类应用在不同通信网络层中通常需要考虑的要求包括时延、数据速率、可靠性和安全性，相关内容已在 Kuzlu 和 Pipattanasomporn [30], Gungor 等人 [24], Ghorbanian等人 [25]等文献中得到综述。表 I 总结了部分应用对时延和数据速率的要求。时延要求因应用而异，范围从 12 毫秒到数分钟。对于实时感知，时延至关重要，应控制在 12 至 20 毫秒之间。广域态势感知系统和配电自动化系统也要求时延较低，通常为毫秒级。对时延要求不高、可容忍约 2 至 15 秒时延的应用包括高级计量基础设施（AMI）和家庭能源管理系统（HEMs）。数据速率要求范围为 9.6 kbit/s 至 10 Mbit/s。广域态势感知系统需要较高的数据速率，以实现准确、可靠的数据传输。其他应用（如 AMI、家庭与楼宇自动化以及配电自动化）的数据速率要求可以较低，通常低于 100 kbit/s。

智能电网高度依赖信息与通信技术（ICT），并且极易受到网络攻击，因为每个网络连接都可能成为攻击目标 [31]。考虑到这些系统彼此互联，且包含终端用户和电力系统组件的敏感信息，针对智能电网的网络攻击可能造成严重后果，例如停电。因此，为几乎所有智能电网应用提供可靠的端到端安全至关重要。

2.4. 挑战和局限性

尽管边缘设备的现代发展取得了显著进步，但近期综述指出，仍有若干瓶颈亟待解决 [29]。智能电网的复杂性给计算和通信基础设施以及感知协议的设计带来了挑战。

物联网设备在计算和存储特性方面的局限性会影响其运

应用	理想时延	数据速率	覆盖范围
输电线路监测	15 - 200 毫秒	9.6 - 56 kbit/s	最长可达 100 km
变电站自动化	3毫秒 [a] / 15 - 200 毫秒	9.6 - 100 kbit/s	最长可达 10 km
广域态势感知	15 - 200 毫秒	600 -1500 千比特/秒	100 千米或以上
配电自动化	20 - 200 毫秒	9.6 - 100 千比特/秒	最长可达 10 km
家庭能源管理	300 - 2000 毫秒	9.6 - 56 千比特/秒	最长可达 100 m
灵活性供给	500 毫秒至数分钟	14 至 100 千比特/秒	最远 10 公里
停电管理	2 s	56 千比特/秒	最远 10 公里
高级计量基础设施	12 毫秒 [b] - 15 秒	10 - 100 千比特/秒	最长 10 千米
分布式能源资源/储能	300 毫秒 - 2 秒	0.6 - 56 kbps	最远 10 km

[a] 保护系统中断路器的跳闸信号[b] 若用于实时运行

表 I. 基本智能电网应用的通信要求，数据基于 [24–28]。时延为端到端时延，数据速率为单个节点的数据速率。

行复杂算法的能力 [32, 33]。然而，电网相关应用（如需求响应 [34], 保护 [35],等多个领域 [33, 36]）对人工智能（AI）算法的需求日益增长。但由于边缘设备的整体计算能力较弱，直接在边缘运行人工智能模型在实际应用中可行性较低 [33]。训练人工智能模型所需的计算性能也会带来不可忽视的功耗，因此，在要求边缘设备自行训练的情况下，可能会受到限制。联邦学习等分布式人工智能方案 [37] 可通过引入由中心实例协调的全局模型和学习过程，减轻单个设备的工作负载，使单个设备只需基于各自的数据子集进行训练。这种协作方法使设备能够在计算或功耗负担与通信需求之间进行权衡。不过，这也使相关实体之间可靠、安全的通信变得更加重要，因为做出明智决策所需的数据并非总能在本地获取。

就边缘设备的感知要求而言，智能电网在各种环境条件下运行，这可能导致数据含噪且可靠性较低。然而，在实际环境条件下，所采集数据的高精度、高可靠性和高可用性是人们所期望的 [32]。

安全对于保障系统的可靠性以及数据隐私日益重要，但在边缘设备中也可能构成挑战，因为随着设备数量增加，攻击入口点也随之增多，而资源约束也可能限制安全性 [17]。智能电网中的数据传感和通信可能带来越来越多的入侵和攻击入口，使网络安全的重要性日益凸显。为了确保现代电网正常运行，许多系统需要互连，这也带来了新的可能性和网络安全威胁

性 [27]。考虑到物联网和边缘设备在智能电网中的应用（例如智能电表、光伏系统控制器、电池或车辆充电系统，以及变电站中的设备），这类设备大多受到资源约束，因此其能够实现的安全机制复杂度也受到影响 [38]。物联网恶意软件攻击数量不断增加；据 Analytics [39] 数据，2022年至2023年，物联网相关网络攻击增长了400%。这些设备的可维护性，以及设备所有者或运营者无需亲自接触设备即可应对新出现威胁的能力，也给保障网络安全带来了挑战 [40, 41]。传统上用于保护系统的加密算法大多无法有效抵御量子计算攻击，因此产生了新的漏洞 [42]。这意味着，最终不仅机密的个人或商业数据可能在未经同意的情况下被解密和使用，设备之间为电网运行而交换的控制数据也可能遭到拦截或篡改，从而危及电网稳定性或安全。

3. 电力系统中的量子技术

建立在经典物理学之上的现代技术能够捕捉日常宏观系统的行为，但在微观领域却失效；在这一领域，量子原理成功描述了这些原子尺度系统，并反过来推动宏观工程不断向更快、更准确、更高效的方向发展。量子世界由波粒二象性、不确定性原理以及物理性质的量子化等基本原理所定义。在这一领域，电子和光子等粒子同时呈现波状和粒子状行为，而它们的行为只能用概率来描述 [43]。这标志着我们从经典物理学的确定性本质，明确转向了量子物理的概率性框架；量子物理已显著改变了我们对宇宙的理解，

量子物理也通过解释物质和能量在极小尺度下的行为，构成了许多现代技术的基础。这种早期理解促成了第一次量子革命，并推动了激光器、晶体管和半导体等技术的发展 [45]。近年来取得的进展通常被称为第二次量子革命，涉及对量子系统的操控，并促成了量子计算、传感和通信领域的新兴应用 [46–48]。

在这一基础及其成功之上，近期研究探索如何在更广泛的应用中利用其潜力，尤其是在电力系统等高度复杂的工程基础设施中。尽管大规模电网坚定地运行于宏观范畴，规划、运行、传感和通信中的若干子问题仍暴露出计算、精度或安全方面的局限性，而量子技术可能在这些方面带来优势。特别是，源自第二次量子革命的进展，使得人们能够初步探索将量子计算用于电力系统应用中的优化、学习和仿真任务 [12, 49, 50]。与此同时，量子传感技术已展现出对电场和磁场的原子尺度灵敏度，从而能够实现与电网监测和诊断相关的高分辨率电流、电压和场测量数据 [13, 51], ，这超出了经典传感器的能力范围。此外，量子通信协议，尤其是量子密钥分发，已被提出用于增强智能电网及未来电力系统中通信链路的安全与韧性 [42, 52]。尽管其中许多方法仍处于早期或实验阶段，功能有限，但它们共同表明，评估量子技术在哪些方面能够切实补充现代电力系统的研究工作正在不断增长，后续各节将对此作更详细的讨论。表 II 简要概述了这些研究方向及其挑战。

3.1. Quantum 计算

量子计算利用叠加和纠缠等量子现象执行计算；对于某些问题，其速度比经典计算机快几个数量级。这一能力为密码学、优化、量子模拟和机器学习等领域带来了新的发展机遇 [53, 54]。

自1982 [10, 11], 引入量子计算以来，自20世纪90年代起，人们提出了许多新的量子算法，其应用领域涵盖量子化学到金融 [55]。总体而言，这些算法可分为三大类：（i）用于更高效地仿真量子力学的算法，主要旨在推动科学发现取得突破、改进理论模型，并实现最佳药物设计和深入了解分子化学；（ii）用于改进优化和解决难题的全局搜索算法，借助量子态的叠加（包括 Grover搜索或振幅放大等通用算法、变分量子求解器、加速线性代数和量子机器学习）；以及（iii）用于破解密码的工具。在这三类中，我们认为第二类（ii）是探索电力系统应用的正确方向。第三类（iii）会对系统的安全运行构成威胁，我们将在第3.3节进一步讨论这一方面。

在类别 (ii) 中，量子机器学习 (QML) 利用量子并行性，相较于经典机器学习技术，有望在数据密集型机器学习任务中实现加速 [56]。变分量子算法，包括量子支持向量机、量子神经网络及相关模型，构成了当前 QML 研究的基石，在理论与当今可用的含噪中等规模量子 (NISQ) 设备实践之间架起桥梁。表 III 展示了文献 [57] 及其中所引文献报告的若干重要经典与量子机器学习算法时间复杂度随数据集大小变化的比较 N 。这份线性代数和 QML 量子算法清单，可能对能源电网的分析与优化产生重要影响。Ganeshamurthy 等人[12]介绍了量子计算和 QML 在电力系统中的潜力与应用，涉及系统监测、控制、优化和保护等领域。

在考察量子计算所带来的性能提升时，需要牢记一个重要的注意事项（见参考文献 [58]）：在大多数情况下，算法加速仅在处理所涉问题的量子态这一层面得到保证，但通常需要先制备量子态，以适当地表示数据，之后还需要将其读出。特别是当问题使用经典数据时，将数据加载到量子态中的过程会引入线性（对于向量）和二次（对于矩阵）开销，从而抵消二次加速的优势 [59]。因此，最具前景的算法是那些涉及三次、四次甚至更高次加速的算法。在输出/读出方面，解决方案通常被编码到过多的概率幅中，因而只能高效地提取全局性质，例如偶性或奇性，或确认解是否相同。在输入方面，如果待处理数据可以通过算法生成，或者数据已经编码在量子态中，则性能可以得到提升。从这个意义上说，研究使用传感器来采集电网状态，并将其编码到量子信息载体（光子、自旋等）中的方法，将是值得的。

应用	研究方向 tion	与电力系统的相关性	研究挑战
Quantum 计计算	(i) 改进优化和全局搜索复杂问题。 (ii) 用于密码学破解—ing	(i) 电网运行与规划、基于 Quantum 的机器学习。(ii) 潜在威胁包括加密，因此也为安全运行能源系统提供保障。	(i) 转换信息 to 量子态可抵消计算方面的加速，直接使用量子测量会受到测量误差的影响，并且会发生退相干。 (ii) 长期安全通信即使面临量子威胁，大型电网中的通信仍可保持安全量子威胁
Quantum 传感-ing	高精度 mea-量	通过磁场测量电流-场、温度测-量；可应用于边缘设备由于微型化	NV 已在高精度应用
Quantum 计算通信	(i) Quantum 密钥分发贡献。 (ii) 增强态传输	(i) 保护关键电力系统通信信道，例如，控制中心与现场设备之间设备。 (ii) Quantum 量子隐形传态朝向电网控制机制量子SDN／路径内信号处理，以实现共识分布式控制中的鲁棒性。	（i）真实智能电网中的部署复杂性；鲁棒、节能且经济高效的边缘系统；与经典信道 to 避免拒绝服务攻击期间 QKD 受损所导致的服务中断。（ii）控制策略的实际实施需要额外的通信传输通道，并意味着复杂性增加

表 I I. 电力系统中的量子技术研究方向与挑战概述。

算法	经典	Quantum
线性回归	$\mathcal{O}(N)$	$\mathcal{O}$(对数 N)
高斯过程回归	$\mathcal{O}(N)$	$\mathcal{O}$(对数 N)
集成方法	$\mathcal{O}(N)$	$\mathcal{O}(\sqrt{N})$
支持向量机	$\mathcal{O}(N^2-N^3)$	$\mathcal{O}$（日志 N）
贝叶斯网络	$\mathcal{O}(N)$	$\mathcal{O}(\sqrt{N})$
k 均值聚类	$\mathcal{O}(kN)$	$\mathcal{O}(k$ 对数 $N)$
主成分分析	$\mathcal{O}(N)$	$\mathcal{O}$(对数 N)
持久同调	$\mathcal{O}$(指数 N)	$\mathcal{O}(N^2)$
高斯混合模型	$\mathcal{O}$（对数 N）	$\mathcal{O}$（多对数 N）
卷积神经网络	$\mathcal{O}(N)$	$\mathcal{O}$（对数 N）
贝叶斯深度学习	$\mathcal{O}(N)$	$\mathcal{O}(\sqrt{N})$
生成对抗网络	$\mathcal{O}(N)$	$\mathcal{O}$(polylog N)
玻尔兹曼机	$\mathcal{O}(N)$	$\mathcal{O}(\sqrt{N})$

表 III. 不同机器学习算法的经典与量子时间复杂度比较，时间复杂度是数据集大小 N 的函数。

不过，根据具体场景，由此类传感器编码的量子态可能需要从电网内的不同位置采集，然后传输到某些量子计算设备进行进一步处理。由于这些位置之间的距离可能达到几十至数百千米，量子态需要通过经典方式（即通过光纤或自由空间发送光子）或量子隐形传态（即借助纠缠效应并结合经典通信 [60]）进行传输。这两种方法都容易受到测量误差和退相干的影响，而且距离越长、时间跨度越大，这种影响越严重 [61]。

因此，量子传感器的布设及其与量子算法流程的集成需要仔细规划，以避免计算输入出现过高的错误率，即便量子通信的进展（参见第3.3节）可能缓解此类问题。

在此背景下，量子–经典混合架构提供了一种务实途径，可利用新兴的量子能力，同时避免与完整量子态制备、远距离量子传输和噪声读出相关的诸多瓶颈。这些架构将量子子程序集成到负责数据采集、大规模计算和实时控制的经典工作流中。尽管存在上述挑战，早期实验工作表明，此类混合方法已能在能量和物联网应用中带来实际效益。例如，最近的一项演示展示了面向5G基站和太阳能光伏系统的机器学习模型，其中量子退火机执行组合选址步骤，而经典优化器（数据包络分析）负责运行规划 [62]。同样，2025年的一份报告展示了用于电动公交车队管理的混合工作流：量子例程离线训练风险分类器，所得压缩模型则以经典神经网络的形式部署在物联网边缘控制器上，用于实时充电决策 [63]。

尽管取得了这些进展，但要在机器学习中明确展示量子优势仍然是一个悬而未决的问题，这主要是因为当前硬件存在噪声且容易出错 [64]。当前的含噪中等规模量子设备面临着各种来源的错误，从量子门不保真度到测量误差、无意的环境耦合和串扰不等[65]。尽管完整容错量子

芯片的路线图已经明确 [66], ，但能够支持所需数量物理量子比特的可扩展架构尚未得到验证。替代方法包括接受当前的错误率，并应用错误缓解技术，以便迅速提高结果的质量 [67]。然而，由于边缘设备的计算资源有限，将 Quantum 计算，尤其是量子机器学习，集成到边缘环境中仍然是一项重大挑战 [68]。

3.2. 量子传感

量子传感利用量子系统或现象，以高精度测量物理量，从而能够检测场或力中微小的变化，而这些变化往往是经典传感器无法感知的 [69]。这种能力具有广泛的社会应用；例如，检测载流设备产生的磁场波动，可以通过这些扰动所产生的电磁场揭示电力系统中的异常。然而，对于电力系统应用而言，采用能够在室温下运行的量子系统至关重要。诸如金刚石中带负电的氮空位（NV）中心等量子传感器对磁场、电场、温度和压力敏感，可以前所未有的精度检测这些物理量的细微变化 [13, 70–72] ，并能在室温下运行。NV 中心已被用于探测凝聚态物质系统，研究静态和动态磁结构及电流分布 [73]。此外，NV 中心还用于纳米尺度测温，以测量微小的温度变化 [74] 以及晶体形变或应变的微观变化 [14, 70, 75]。值得注意的是，NV 中心能够同时检测磁场和温度变化 [76]。这些能力使量子传感成为少数几种在电力系统边缘侧的实际硬件限制下，已可部署于电力系统应用的量子技术之一。

通过准确估算电流，可以确定电力系统的某些特性，例如电池的充放电电流。测量这些系统产生的磁场，即可精确测定电流。传统系统能够以毫安量级的精度测定电流；然而，要更精确地测定功率流，即使在噪声环境中，NV 中心等量子传感器也具有显著优势 [51]。近期发展使 NV 传感器实现了显著微型化，器件尺寸可小至 0.42cm^3 [77], ，因此很适合集成到边缘设备中，其性能优于基于经典传感器的现有技术。

3.3. 量子通信

量子通信利用量子物理效应，增强两个或多个参与方之间的数据交换。通过在量子对象中编码信息，并利用量子系统特有的现象（例如态叠加和纠缠），量子通信能够以经典系统无法实现的方式共享信息。相关发展涉及电力系统应用的两个重要方面：（数据）安全和增强态传输，以下各节将对此展开讨论。

3.3.1. Securing energy grids with quantum key distribution

针对能源电网中的数据安全问题， [42] 回顾了当前分布式能源资源（DER）系统面临量子网络攻击的漏洞。文中指出了量子安全威胁可能出现的时间，并提到 IBM 的量子计算路线图 [78]显示， 10^6量子比特的量子计算机可能会在 2026 年之后的某个时候问世。不到十年间，量子计算系统已从仅有几十个量子比特的芯片发展至今；这类系统距离能够在数小时内破解官方认可的加密方法（如密钥长度为2048 [79]位或 3000 [80]位的 Rivest–Shamir–Adleman（RSA））所需的量子比特数量仅差一个数量级 [81], 。而近期使用经典方法取得的成果，要破解密钥长度仅为 829 位的密钥，也需要在当前可用的经典硬件上运行数千个核心年 [82]。然而，具体到不同应用场景，能源电网的加密需求主要涉及保密期限较短的数据，任何合理的加密方案都会为每对通信实体使用独立密钥。这意味着，量子计算能力发展所带来的一些可能令人担忧的密码学条件会有所缓解；此外，通常还必须针对电力系统中的每条独立连接重复发起攻击，因此潜在攻击者若想全面控制系统，就需要付出巨大努力。尽管如此，鉴于能源电网作为关键基础设施可能存在的漏洞，亟需采取主动措施应对未来威胁。

量子密钥分发（QKD）提出了这样一种解决方案。它依靠实用量子力学的基本原理（例如海森堡不确定性原理、不可克隆定理和光子偏振），通过联合生成对称密钥，在网络中空间分离的参与方之间建立可证明安全的 [15] 通信。在QKD环境中，即使拥有无限计算能力的对手，也不可避免地会以某种方式扰动传输的量子比特状态，从而暴露其试图窃听量子信道的行为；因此，希望进行私密通信的参与方可以丢弃通过该信道建立的密钥，避免在使用该密钥编码私密信息之前使用它——

在实际应用中，QKD迄今主要以两种方式实现：适用于数百千米以内距离的光纤实现 [84, 85]，以及用于长距离/全球密钥分发的自由空间实现，例如通过卫星 [86, 87]。尽管这两种方案都曾被考虑用于保障智能电网中的通信 [88], ，但光纤方案尤其适用于电力电网应用，因为变电站与控制中心之间的典型距离与当前最先进的电力设施光纤量子密钥分发实现所覆盖的$10-100$ 千米距离十分匹配。

第2.3节中介绍的智能电网基础设施通信需求，与当前最先进的量子密钥分发系统已能实现的能力相比，通常较为适中。智能电网通信系统虽然必须支持广泛的应用，但与电信标准相比，其时延、带宽和链路距离要求相对较低（参见表 I）。现代光纤量子密钥分发技术可可靠地产生数 kbit/s（>200 km）至百 Mbps（<10 km）的密钥率，具体取决于距离和硬件配置。新型光子集成量子密钥分发发射器在 50 km 距离上实现了 1.82 Mbps 的密钥率，并可将密钥生成距离维持在 250 km 以内 [90], ，从而满足智能电网中绝大多数通信需求。此外，基于光纤的量子密钥分发几乎不会引入传输时延，并能使密钥生成与应用层时序解耦，因此与对时延敏感的电网功能高度兼容。

量子密钥分发硬件在技术上已可视为成熟且适用于现场部署，尤其是与量子处理器等技术相比。因此，它能在近期切实增强关键电力系统通信信道的安全性，例如广域监测、保护与控制（WAMPAC）系统所使用的信道；通过强化现场设备与控制中心之间交换的测量数据的机密性和真实性，以及发回电网的控制信号的完整性，提升其安全性。电网领域已实现的应用示例包括Alshowkan等人 [91] 的研究，该研究展示了如何在电力设施光纤网络中，实现在配电中心与变电站之间的 3.4 km 链路上分发量子密钥。该演示系统与运行网络隔离，采用商用量子密钥分发硬件，并在网络协议栈的上层使用发布—订阅消息队列遥测传输（MQTT）协议。同样，量子密钥分发也被部署于一套用于实时电网分布式能源资源的控制系统中，展示了其在抵御欺骗攻击和截获方面增强的韧性 [92]。中国电网实施了一种卫星量子密钥分发方案，用于保障电网通信安全 [93]。作为空间尺度量子实验（QUESS）任务的一部分，该方案旨在展示远距离量子安全，并推动量子互联网的发展。

在文献 [94] 和 [95], 中，研究人员通过商用实时数字仿真器（RTDS）模拟的实时环境，重现了控制中心与微电网之间基于模拟量子密钥分发协议的通信。

尽管这些进展和实例令人鼓舞，但智能电网和电力系统中量子密钥分发应用的研究仍然有限 [52], ，尚未实现大规模的实际部署。要在布局类似于智能电网的大型网络中保障通信安全，也面临着额外挑战。除了在智能电网中通过量子信道连接设备所需的暗光纤链路的成本和可用性之外 [52, 96], ，现有能源控制设备种类繁多，也使得在异构网络中实现可扩展的量子密钥分发集成颇为困难。因此，相比通用型量子密钥分发实现，智能电网更适合采用定制化解决方案，以优化适用于能源系统变电站与控制中心之间通信的特定用例。此类面向具体应用的量子密钥分发解决方案必须确保硬件子系统、协议和接口之间的兼容性，从而保障整个系统的最佳性能和安全性 [97]。在规划量子密钥分发系统时，考虑电网各区段的电气关联和控制结构，可降低部署复杂性。文献 [98] 例如探讨了电力系统中的半量子密钥分发（semi-QKD）概念，即只有部分节点需要具备完整的量子能力。该研究旨在优化资源分配，同时维持安全性，并提出了一种在电网中部署量子服务器的贪心算法，且在 IEEE 14节点系统上对其进行了验证。

要实现大规模实际部署并覆盖网络边缘，当前量子密钥分发设备的尺寸、功耗和成本，以及此类系统的运行环境条件，可能都需要进一步改进。在这方面，基于芯片的光子集成量子密钥分发收发器有助于缩小密码模块的尺寸，并带来了令人振奋的可能性；与此同时，密钥生成速率和链路距离也在迅速提升。超导纳米线单光子探测器（超导纳米线单光子探测器）彻底革新了量子密钥分发接收技术，因为它们能够实现接近 100% 的探测效率、皮秒级时间抖动，以及接近 GHz 范围的计数率 [99], ，性能远超传统雪崩光电二极管（雪崩光电二极管）。这些进展共同展现了构建高速率、经济高效的光纤量子密钥分发系统的前景，使其能够满足未来智能电网对规模和可靠性的需求。

需要指出的是，尽管使用 QKD 确实能为传输的数据提供可靠的额外安全保障，但它并不能阻止针对加密机制的攻击，而此类攻击可能会对运行性能造成负面影响。尤其是，对量子信道的窃听会带来拒绝服务攻击的风险 [100, 101], ，因为量子物理定律决定了，窃听传输会在原通信双方之间的通信中引入扰动，

因此，攻击期间可能无法建立或更新密钥。对于依赖持续交付或更新密钥材料的系统（例如，一次一密的朴素实现），服务可能会因此受损，直至窃听事件结束。因此，识别电力系统各部分在何种时间范围内能够使用可能未改变的密钥对运行（即保护暂时减弱），以及潜在攻击成功所带来的影响，十分重要。例如，在远方保护场景中发出紧急命令的应用被视为高度关键，因为信令机制遭到滥用可能造成大范围影响。然而，此类信号很可能不受突发攻击影响，因为用于跳闸信号等场景的 IEC 68150 GOOSE / R-GOOSE 信令机制会在事件发生时采用突发式信令机制（即连续快速发送消息），而在没有变化时则改为缓慢的周期性重复发送 [102]。因此，可利用事件发生前未遭窃听的时段预先建立足够的密钥材料，以应对紧急情况下产生的信号突发；事件发生后，密钥则可以延迟一段时间再更新。类似地，高级计量基础设施的快速数据更新乍看之下似乎需要频繁重新生成密钥，因而依赖 QKD 资源的稳定供应。然而，测量的规模庞大且分布广泛，因此这类应用更难遭受攻击，因为攻击者需要实际攻击更多系统；此外，还可采用在不完全可观测性条件下进行状态估计等方法 [103]，弥补因新的量子密钥材料暂时不可用而造成的数据缺失。此外，现代数据驱动型入侵检测技术，例如 [104]，提出的基于贝叶斯生成对抗网络的虚假数据注入检测方案，可用于识别遭到篡改的测量数据。评估应用或控制场景失效前遭到破坏的程度和持续时间，有助于确定密码保护机制需要满足哪些保证，而不论该机制基于量子效应还是经典技术。在这方面，欧洲电信标准协会（ETSI）制定的标准，尤其是其关于量子密钥分发密钥管理接口 [105] 和网络架构 [106]，的规范，使 QKD 能够集成到 IEC 61850 环境中，作为现有基于 IEC 62351 的保护配置文件（例如，采用传输层安全协议或互联网协议安全保护的客户端/服务器流量，以及用于 GOOSE / R-GOOSE 和采样值的组密钥）的高保障对称密钥来源，而非独立的安全孤岛；其配置规模可根据底层应用的关键程度和时间范围进行调整。

3.3.2. Enhanced state transfer via quantum communication

除了为密码学功能提供必要的增强外，量子通信还可助力开发新型控制方法。利用成组的预纠缠量子比特可用于在远程创建这些量子比特状态的副本（“量子隐形传态”）这一效应 [60]，，无需在该时刻实际传输量子信息载体（例如光子），即可在不同位置之间传递量子状态信息。尽管此类隐形传态仍需要在发送方完成必要的测量过程后传输额外信息，因此其速度并不快于光速 [107, 108]，，但量子信息理论上无损且（在一定程度上）与量子信道状态无关的通信能力，为在电网不同区域之间共享信息开辟了新的可能性。

文献 [109, 110] 提出利用量子隐形传态，在能源电网上部署的分布式能源资源（DER）系统控制器之间实现共识，并模拟了该机制在微电网中的交流频率控制和直流电压控制应用。然而，Ahmad等 [111]近期对微电网分布式控制策略的综述发现，除上述方法外，涉及量子通信的研究仍十分有限，但采用纠缠量子比特和/或隐形传态量子比特或许能够带来更多研究机会。

尤其是将量子隐形传态应用于电网控制，看来颇具吸引力；然而，量子物理的一些基本原理，例如不可克隆定理 [112, 113]和不可通信定理 [108] ，分别排除了某些应用场景，也使量子通信在其他场景中的应用更加复杂。发送方持有的状态信息会在隐形传态过程中不可避免且不可逆地被销毁，因此无法通过这种方法复制信息，只能传输信息。这会影响控制算法的工作机制以及通信协议，因为仅凭量子隐形传态无法实现共享状态（即双方都能获得相同信息）。如第3.3.1节所述，元信息需要通过附加信道传输，这又增加了控制机制的复杂性，因为两个信道必须协同运行才能发挥优势。

4. Quantum 技术在电力系统边缘设备中的潜在应用

量子技术已成功应用于应对现代

电网面临的部分挑战和局限性，并支持建设和维护可靠、安全电网的工作。大多数理论量子计算模型的计算速度都优于经典模型 [114] ，且有研究表明，与经典计算相比，量子计算的能耗更低 [115]。量子计算、量子机器学习和量子密钥分发已应用于电力系统领域，相关综述包括 Golestan等 [115], Eskandar- pour 等 [116], Zhou 等 [114], Ganeshamurthy等[12], 。现有应用主要涵盖电网分析、优化、运行和安全等电力系统问题，例如功率流、状态估计、事故分析、电磁暂态仿真、稳定性评估、故障诊断与管理、机组组合、设施选址与分配、PMU布点、电力系统控制、网络安全和预测。本文探讨量子技术与边缘设备的潜在集成方式。

尽管大规模量子处理器仍受量子比特相干性、噪声和物理尺寸的限制，但若干电力系统任务已经能够从现阶段的量子技术中受益。首先，浅层电路变分量子算法能够支持小规模优化和机器学习任务，例如降阶分类或局部优化。在 [114] 中，详细综述了在含噪中等规模量子（NISQ）约束下仍具可行性的量子算法，并重点说明了其对能源系统优化的具体相关性。其次，室温NV中心量子传感器能够对磁场、电流、温度和应变进行高精度测量，从而改善边缘侧的异常检测和设备诊断。第三，量子密钥分发（QKD）已经在电力公用事业光纤网络中得到验证，可为保护、控制和分布式能源资源（DER）协调提供实用的量子安全通信。在 [91] 中，展示了一种通过3.4公里在运行中的电力公用事业光纤部署的QKD方案，用于保障变电站与配电中心之间基于MQTT的SCADA通信。同样，在 [92], 中，展示了将QKD集成到某供应商的三节点系统中，并采用基于暗光纤的通信。第四，即使没有完全纠错的网络，有限形式的量子通信（例如纠缠辅助同步）也能够支持分布式协调和故障转移功能。例如，在 [109]中已证明，基于隐形传态的信息共享能够支持分布式微电网控制器。该方案通过在每个节点部署一台量子计算机组成量子分布式控制器（ QDC），并在各节点之间建立量子通信来实现。同一组作者还在 [110], 中表明，相互作用量子比特能够在现实噪声条件下使DER控制器保持同步。最后，后量子密码学（PQC）可立即用于资源受限的边缘设备。

如 [117], 中所示，基于格的后量子密码算法非常适合低功耗嵌入式硬件，并可集成到物联网安全架构和微控制器中。在 [118], 中，提出了两种不同的架构，既支持在功能强大的边缘物联网设备中采用PQC，也支持在资源受限的物联网节点中采用PQC。总体而言，这些应用代表了在当前硬件约束下量子技术的现实用例。

在传感器方面，基于 NV 中心的量子传感器能够在室温下以极高的精度和空间分辨率测量磁场、电场、温度和压力场 [70, 77]。这些设备属于固态设备，体积小巧，并且可以在噪声环境中运行 [77]。此类微型低功耗传感器可以直接嵌入电网边缘硬件（例如输电线路、变压器或物联网设备中），从而对局部电流、场和环境条件提供丰富的实时监测数据。新兴研究还在探索分布式量子传感，即在传感器网络中使用纠缠粒子，以实现超越经典精度极限的集体测量。例如，连续变量多方纠缠网络已被证明能够在灵敏度方面达到海森堡极限标度，其性能优于可分方案[119]。除传感外，研究人员还在设计可部署于分布式边缘网络的轻量级量子算法，并提出利用量子通信链路来同步传感任务、通过纠缠辅助协议确保边缘设备之间的安全协调，以及执行纠缠辅助数据融合和决策 [89]。

在边缘设备的通信技术方面，人们正日益探索将量子密钥分发直接集成到电网边缘的量子传感器和处理器中。集成光子学的进步使量子密钥分发系统得以微型化，从而能够将紧凑、低功耗的量子密钥分发模块直接部署在智能电表、变压器和物联网传感器等边缘硬件中。这些集成光子量子密钥分发设备利用片上光源、探测器和调制器，以极小的占用空间和成本，通过现有光纤或自由空间链路安全地生成和分发量子密钥 [97]。近期在光子集成和封装方面的演示展示了扩大量子密钥分发在边缘网络中部署规模的可行途径，有望在无需大量专用基础设施的情况下，实现边缘节点之间实时的量子安全通信 [99]。

除了 QKD，后量子密码学（PQC）算法还提供了互补的软件安全解决方案，可部署在资源受限的边缘设备上，以保护数据免受量子赋能攻击。Liu等人 [117], Ebrahimi等人 [118], 和 Sch¨offel 等人 [120] 的研究表明，基于格和基于编码的后量子密码算法可针对低功耗物联网环境进行优化。随着边缘设备逐渐发展为量子传感器和处理器，

建立稳健且可扩展的量子通信基础设施，对于协调这些设备至关重要[89]。此类边缘设备将集成必要的物理组件，以便在分布式节点之间建立并维护纠缠链路：纠缠光子源、量子中继器和量子路由器。借助集成光子学，量子通信技术能够以较低成本扩展至分布式电网边缘环境。

电网控制中心可能需要处理大量信息，同时控制信号又有实时需求；因此，一旦这些控制中心自身的运行出现中断（例如硬件故障），就会产生问题。如果电网数据无法再在某一地点得到妥善处理，就需要尽快将控制系统的当前状态转移至备用控制中心，以便在那里恢复控制。即使不需要发送方介入，信息中的经典部分也可以分发到不同地点，例如采用软件定义网络（SDN）方案； [121, 122]等文献就曾建议在智能电网中采用此类方案。在这种情形下，数据既可以直接在网络中复制，同时发送至主控制中心和备用站点；也可以在主设施出现故障时重新路由至备用站点。触发重新路由的问题甚至可以由网络硬件本身检测，从而将延迟降至最低；近期的硬件发展使其能够以接近线路速率收集必要的统计数据（例如发往控制中心和由控制中心发出的数据包），或对传输中的数据进行计算（例如阈值分析），前提是这些计算足够简单 [123]。此类硬件与量子密钥分发（QKD）结合后，还可以在数据传输过程中对其执行特定的密码功能，从而免去边缘设备实现这类功能的需要。例如，一次一密（可利用QKD生成密钥）在加密和解密时只需对数据和密钥执行异或运算，而可编程网络设备能够高速完成这类运算。如果边缘设备无法改造，或出于经济原因不适合改造（例如近期安装的智能电表或小型设备），且相较于保护电网核心内部的数据（可能经过聚合），对产消者至电网运营商“第一英里”上各条数据的保护或认证不那么重要，那么这些方案可能切实可行。

基于第3.3.2节所述的原因，无法预先提供特定量子态的副本。因此，运行于特定位置的量子算法只有在收到特定通知后，才能将其状态传输至另一位置。纠缠量子比特的隐形传态或许可以在无损的情况下实现这一点，但在算法设计中，必须考虑此类故障转移场景完全被动响应的特性。

另一种可能的做法是，让量子传感器以轮询方式将各自的读数发送到位于不同位置的量子算法副本；这样，对于 n个算法副本，每个副本所处理的数据副本最多只会滞后n 次传感迭代。发生故障时，便可建立备用控制，系统状态虽会存在细微偏差，但无需先启动完整的态传送。与经典数据一样，这种温备/热备策略不一定要由量子传感器或算法副本本身实现，也可以在量子网络内部实现。特别是，当借助量子中继器 [124], 将点对点量子信道替换为交换式量子网络时，这些中继器便可支持“量子SDN”。量子信息在多大程度上可用于控制交换过程，以及由此产生的、实质上基于欠采样的控制策略对电网运行的影响，仍有待确定。然而，类似这一策略的方法或许能为解决将分布式量子数据集成到控制场景中所带来的一些不那么直观的影响提供有意思的途径。

量子技术要在现实世界的智能电网中得到应用，需要具备互操作性和适应性的经典系统。这些系统不仅是快速集成量子技术所必需的，也有助于量子技术与传统应用并行、协同运行，在两者之间切换，并使用后备方案。一个例子是 SOGNO [125] 和 MCCS [126], 等控制系统的模块化方法，它们简化了新功能（包括基于量子技术的功能）作为服务的集成，因此可作为赋能技术。

最后，我们考察了影响当前观点的实际工程限制，这些限制关系到在电力和能源系统的边缘部署量子能力是否可行。大型稀释制冷机体现了集成量子技术所面临的挑战。低温恒温器可能高达数米，重达数百千克，因此需要专用的多相电源和占地空间。另一方面，超导电路中的约瑟夫森结对磁场极其敏感，因此需要厚重的屏蔽层。囚禁离子系统同样需要超高真空泵、稳频激光器和隔振平台，而这些设备有时会超出电网变电站的环境和基础设施承受限度 [127]。即便是室温金刚石氮空位平台，也需要严格的环境控制，并需要昂贵的封装、温度稳定装置以及 ∼100 毫瓦级光泵浦激光器。具有代表性的商用设备功耗为 ∼17 瓦，远高于经典磁场或电流传感器 [128]。

这些物理限制为将量子元件直接嵌入相量测量单元、保护继电器或分布式控制器带来了不小的障碍。量子传感器和通信模块目前的资本成本较高，主要受专用光学器件、精确热控以及小批量制造的影响。

运营支出也较高：校准间隔较短；光子源、探测器和光耦合器会随时间推移而出现明显性能退化；低温或激光组件则需要定期维护、重新校准或更换。因此，其总拥有成本仍显著高于传统边缘设备（公用事业设备的典型生命周期为10–20年）。尽管如此，变电站具有固定不动的特点，可接入公用事业级电力，且可以采用将量子模块隔离起来的混合架构。这些因素表明，与其他边缘计算用例相比，电网应用或许会率先在技术和经济层面妥善应对这些限制。

5. 结论

将量子计算、量子传感和量子通信等量子技术集成到边缘设备中，可能代表着电网领域的一种新范式。本文介绍了量子赋能边缘设备克服当前边缘设备能力关键局限的可能途径。量子计算以叠加和纠缠原理为基础，在电网边缘侧能够应对大规模复杂优化问题，并实时更新控制系统；例如，实时功率流优化对于经典处理器而言可能难以实现。类似地，量子传感能够高精度测量电磁信号等物理量，即使在噪声环境中，也能检测到经典传感器设备无法察觉的微小场变化。利用这些量子传感协议，可以监测电网状况，并在故障或扰动超出传统经典传感器的灵敏度范围时发出预警。此外，量子通信利用量子系统传输信息，速度更快且安全性更高。例如，量子密钥分发能够实现经典加密方案无法提供的、从根本上安全的信息交换。因此，这些量子技术有望将边缘设备提升为一种快速、响应灵敏且高度安全的新型节点，从而增强未来电力系统的整体韧性和效率。短期内，鉴于当前硬件的限制，量子传感、量子密钥分发、后量子密码学以及小规模适用于含噪中型量子设备的算法，是应用于电力系统边缘设备最现实且最有益的量子工具。

尽管存在这些潜在机遇，但在基于量子的边缘设备能够在电网中得到实际应用之前，仍需克服重重障碍。例如，当前的量子硬件受资源密集型需求的限制，并且存在噪声。同样，基于 NV 的微型量子传感器也必须经过校准以消除噪声，从而保持准确性。此外，系统互操作性仍是一个悬而未决的问题：量子组件需要与经典电网基础设施和通信协议实现无缝对接。如果缺乏针对量子—经典混合运行的明确定义的标准和架构，量子边缘设备的优势就无法得到充分发挥。

针对这些挑战，若干新兴研究方向有助于指导量子赋能边缘设备的实际发展。首先，量子硬件的小型化亟需取得重大进展，因为现有系统可能仍无法满足变电站的环境和运行要求；集成光子学、紧凑型低温技术以及面向特定应用的量子传感器均代表着前景广阔的发展路径 [129]。其次，迫切需要开展定性成本—生命周期评估，因为量子组件目前的采购、校准和维护成本均高于经典同类组件，从而影响其现场部署的经济可行性。第三，未来的实现方式将依赖混合量子—经典架构，将量子传感器和后量子密码学/量子密钥分发模块与含噪中等规模量子时代的处理器相结合，因此必须开发新的软件框架、编排机制和互操作性标准。

通过持续研究应对这些挑战，将有助于在实践中实现基于量子的边缘设备。一些国家级倡议已认识到量子技术在电力系统中的重要性，其中包括 QuGrids项目。该项目旨在探索量子解决方案，构建基于量子的能源基础设施，以提升未来电力系统的韧性和智能化水平。总而言之，实现这一基于量子的边缘设备愿景不仅是一项技术挑战，更是战略上的必然要求，旨在打造安全、坚韧且智能的新一代智能电网，以应对能源系统格局不断演变所带来的挑战。

致谢

我们感谢北莱茵-威斯特法伦州文化与科学部（MKW NRW）在“Profilbildung 2022”项目框架内，为“基于量子的能源电网（QuGrids）”项目提供的支持。

附录A：基础量子物理及其应用

量子物理描述了最微观尺度上的自然界，而量子系统受概率、复振幅以及测量引发的随机性支配。在第二次量子革命中，量子物理的主要应用包括量子计算、传感和通信。量子叠加原

理和纠缠是这些应用的基础。本节将对它们作简要介绍，并说明其与经典物理学的区别。

1. 量子叠加原理与纠缠

叠加原理指出，一个量子系统可以同时处于多个经典态，并且有效量子态的任意线性组合本身也是一个有效量子态。从物理上讲，这意味着一个量子比特（qubit）可以处于 $|0\rangle$与 $|1\rangle$的相干混合中，而不是仅占据一种（0或1）经典构型。在数学上，它可以表示为

$$|\psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle\,. \tag{A1}$$

其中，$|\alpha|^2$ 和 $|\beta|^2$ 是将系统测量为态 $|0\rangle$和 $|1\rangle$的概率。与非0即1的经典比特不同，量子比特同时存储两者的概率幅。

而量子纠缠则出现在复合系统的量子态无法写为其子系统的张量积之时。例如，双量子比特态 $|\Psi\rangle \in \mathbb{C}^2 \otimes \mathbb{C}^2$ 在以下情况下处于纠缠：

$$|\Psi\rangle \neq |\psi_1\rangle \otimes |\psi_2\rangle. \tag{A2}$$

一个典型例子是贝尔态

$$|\Phi^+\rangle = \frac{|00\rangle + |11\rangle}{\sqrt{2}}. \tag{A3}$$

该态表现出完美关联：对一个量子比特的测量会确定另一个量子比特的结果，而与距离无关。纠缠是量子算法、通信和传感的基本资源。

2. 量子计算

量子计算利用量子态和幺正演化来执行超出经典系统能力的计算。信息的基本单位是量子比特，即由该态描述的二能级量子系统

$$|\psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle\,, \tag{A4}$$

其中复振幅满足 $|\alpha|^2 + |\beta|^2 = 1$。计算通过量子门实现，每个量子门均由幺正算子 U 表示，并服从

$$U^\dagger U = I, \tag{A5}$$

这保证了量子演化的可逆性。一个典型示例是哈达玛门，

$$H = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}, \tag{A6}$$

它作用于计算基并生成叠加，形式如下：

$$H|0\rangle = \frac{|0\rangle + |1\rangle}{\sqrt{2}}, \tag{A7}$$

$$H|1\rangle = \frac{|0\rangle - |1\rangle}{\sqrt{2}}. \tag{A8}$$

对于初始化为态 $|0\rangle^{\otimes n}$的 n量子比特寄存器，施加算子 $H^{\otimes n}$ 会在全部 2^n 个计算基态上产生均匀叠加，

$$H^{\otimes n}|0\rangle^{\otimes n} = \frac{1}{\sqrt{2^n}} \sum_{x\in\{0,1\}^n} |x\rangle, \tag{A9}$$

这构成了量子并行性的结构起源。因此，量子计算被描述为排列在电路中的一系列幺正操作，

$$|\psi_{\text{out}}\rangle = U_n U_{n-1} \cdots U_1\,|\psi_{\text{in}}\rangle\,, \tag{A10}$$

随后进行测量，该测量以概率方式将最终的量子态振幅转换为经典输出。

a. Unitary encoding of a function

作用于 n 输入比特并得到m 输出比特的任何函数，都可以分解为基本布尔运算（与、或 以及非）。这些布尔运算无法由量子系统直接实现，因为它们不可逆，即无法根据其输出重构其输入。由于量子演化是幺正的，因而可逆，我们必须使用反映这一性质的逻辑门。这由托福利门表示，它具有三个输入和三个输出，

$$T(a,b,c) = \{a, b, (a \text{ and } b) \text{ xor } c\}, \tag{A11}$$

其中异或 是异或（或差）算子。该门能够可逆地实现任何基本布尔运算。

已经证明，托福利门可以进一步分解为每次作用于单个量子比特和两个量子比特的基本量子操作 [130]。这构成了将函数 f 实现为一系列简单量子门并产生总幺正门 U_f的理论基础。幺正 U_f 针对编码为由多个量子比特构成的量子态的给定输入值，计算 f 的值。

聚焦于具有 n 个输入比特和一个输出比特的函数，$f:\ \{0,1\}^{\times n} \to \{0,1\}$ （通过向量化可扩展至多个输出），幺正U_f 具有以下行为，

$$U_f\,|x\rangle\,|y\rangle = |x\rangle\,|y \oplus f(x)\rangle\,, \quad x \in \{0,1\}^n. \tag{A12}$$

将这一作用与幺正门的线性性质相结合，我们便能看到量子并行性的真正体现：当U_f 作用于如式（A9）所示生成的态叠加时，

$$\begin{aligned} & U_f\left(\frac{1}{\sqrt{2^n}}\sum_{x\in\{0,1\}^n}|x\rangle\right)\otimes|y\rangle \\ &= \frac{1}{\sqrt{2^n}}\sum_{x\in\{0,1\}^n}|x\rangle\otimes|y\oplus f(x)\rangle\,. \end{aligned} \tag{A13}$$

函数 f 在所有可能的输入上被同时求值。结果是一个纠缠（不可分离）态，其概率幅编码了 f的全部输出。完全解码 f 极为低效，因为测量量子比特每次至多得到 $n+1$ 比特信息，且所需重复次数随 n呈指数增长。一般而言，更方便的做法是像Deutsch-Jozsa 算法[131]那样，利用相长干涉与相消干涉来提取 f 的全局性质。

3. 量子传感

量子传感利用受控的量子演化，以达到基本量子极限的精度测量物理参数。关于未知参数的信息通过其哈密顿量编码于系统动力学中；具体而言，若物理参数 θ 与生成元 G耦合，则哈密顿量可写为

$$H=\theta G, \tag{A14}$$

从而使系统按如下方式演化

$$|\psi(\theta)\rangle = e^{-i\theta G t}\,|\psi(0)\rangle\,. \tag{A15}$$

量子传感协议通过态制备、信号相关演化和测量的重复循环进行。传感器被初始化为已知参考态 $|0\rangle$ ，并经由相干控制变换为敏感的叠加态 $|\psi_0\rangle$，从而最大化对目标参数的响应。在询问时间 t内，系统在信号相关哈密顿量作用下演化，将参数 θ 以相对相位或布居转移的形式印刻到量子态中。最后一次控制运行将这一编码信息映射到测量基上，随后投影测量产生由演化后的态所决定的概率的经典结果。重复该序列并对结果进行统计平均，可得到信号相关概率 $p(t)$，由此推断物理参数的估计值，其精度受量子噪声和可用询问资源的限制。

4. 量子通信

Quantum 通信利用量子态和量子纠缠，通过量子信道传输信息。量子信道将经典通信信道推广到传输量子比特而非经典比特的系统。在这一框架中，信息被编码在非正交量子态中，其传输和操控遵循量子物理规律，从而实现经典系统所不具备的通信协议能力。量子通信的一个核心应用是量子密钥分发，它使两个参与方能够建立共享密钥，其安全性由基本物理原理保证：任何窃听行为都会扰动传输中的量子态，从而暴露窃听者的存在。这种安全性还进一步由不可克隆定理提供保障。该定理禁止创建未知量子态的完全相同副本，并确保量子信息无法在不被检测到的情况下被截获、复制或转发。综合而言，这些特性实现了内在安全的通信，并构成量子网络和长距离量子信息传输的基础。下文将进一步阐述不可克隆理论：

假设一个任意纯量子态 $|\psi\rangle$ 和一个已知空白态 $|0\rangle$。可以证明 [112, 113]，不存在酉操作 U （如附录第2卷中所介绍）能够完美克隆 $|\psi\rangle$:

$$\nexists U \text{ unitary}, |0\rangle: \quad U(|\psi\rangle\otimes|0\rangle) = |\psi\rangle\otimes|\psi\rangle \quad \forall\ |\psi\rangle \tag{A16}$$

因此，与经典情形不同，已传输到其他位置的量子信息不可能保留副本。这意味着，既无法在同一时间、不同地点处理同一份量子信息；而且，只要量子信息在传输过程中或传输后受到外部因素（例如与环境相互作用）的扰动，原发送方就无法重新传输它。因此，量子信息需要通过其他机制加以保护。这些机制包括量子纠错码（QECCs）[132], , 其基本原理是将一个逻辑量子比特的信息分散到多个物理量子比特中，从而能够检测并纠正该特定量子纠错码设计范围内的特定扰动，但代价是：传输和存储一份“真正的”量子信息需要多个物理量子比特。另一种相关方法是纠缠纯化（或蒸馏）[133], ，它同样利用多个不完美纠缠对、对纠缠粒子进行局部运行以及经典通信，以概率性地保留保真度更高（即更接近最大纠缠态）、更适于量子信息传输的纠缠对。

[1] G. Bedi、G. K. Venayagamoorthy、R. Singh、R. R. Brooks 和 K.-C. Wang，《电力与能源系统中的物联网综述》，IEEE Inter- net of Things Journal **第5卷**，847（2018）。[2] M. Capra、R. Peloso、G. Masera、M. Ruo Roch 和 M. Martina，《边缘计算：物联网领域的硬件需求综述》，Fu- ture Internet **11**，10.3390/fi11040100（2019）。[3] C. Feng、Y. Wang、Q. Chen、Y. Ding、G. Strbac 和 C. Kang，《智能电网邂逅边缘计算：机遇与应用》，Advances in Applied Energy **1**，100006（2021）。[4] M. Y. Mehmood、A. Oad、M. Abrar、H. M. Munir、S. F. Hasan、H. A. u. Muqeet 和 N. A. Golilarz，《面向物联网智能电网的边缘计算》，Security and commu- nication networks **2021年**，5524025（2021）。[5] J. Li、C. Gu、Y. Xiang 和 F. Li，《面向智能电网的边缘云计算系统：最新进展、架构与应用》，Journal of Modern Power Syste ms and Clean Energy **第10卷**，805（2022）。[6] J. Gedeon、F. Brandherm、R. Egert、T. Grube 和 M. M¨ uhlh¨auser，《雾是什么？重新审视边缘计算：愿景、应用与未来挑战》，IEEE Access **7**，152847（2019）。[7] M. M. Hussain 和 M. S. Beg，《面向物联网辅助智能电网架构的雾计算》，Big Data and Cognitive Computing **第3卷**，10.3390/bdcc3010008（2019）。[8] P. Sun、S. Shen、Y. Wan、Z. Wu、Z. Fang 和 X.-Z. Gao，《物联网隐私安全综述：架构、技术、挑战与趋势》，IEEE Internet of Things Journal **11**，34567（2024）。[9] M. Khanafer、I. Al-Anbagi 和 H. T. Mouftah，《面向时延关键型智能电网应用的优化无线传感器网络设计》，Journal of Sensors **2017年**，5274715（2017）。[10] R. P. Feynman，《用计算机模拟物理》，In- ternational Journal of Theoretical Physics **21**，467–488（1982）。[11] P. Shor，《量子计算算法：离散对数与因式分解》，载于 *Proceedings 35th Annual Symposium on Foundations of Computer Science*（1994），第124–134页。[12] P. A. Ganeshamurthy、K. Ghosh、C. O'Meara、G. Cor- tiana 和 J. Schiefelbein-Lach，《借助量子计算弥合新一代电力系统规划与运行的差距》（2024）。[13] M. W. Doherty、N. B. Manson、P. Delaney、F. Jelezko、J. Wrachtrup 和 L. C. Hollenberg，《金刚石中的氮-空位色心》，Phys. Rep. **528**，1（2013）。[14] J. F. Barry、J. M. Schloss、E. Bauch、M. J. Turner、C. A. Hart、L. M. Pham 和 R. L. Walsworth，《NV金刚石磁力测量的灵敏度优化》，Reviews of Modern Physics **92**，10.1103/revmodphys.92.015004（2020）。[15] D. Gottesman、H.-K. Lo、N. L¨utkenhaus 和 J. Preskill，《不完美设备下量子密钥分发的安全性》，Quantum Info. Comput. **4**，325–360（2004）。[16] S. Liang、S. Jin 和 Y. Chen，《边缘计算技术及其在电力系统中的应用综述》，Energies **17**，10.3390/en17133230（2024）。[17] Y. Xiao、Y. Jia、C. Liu、X. Cheng、J. Yu 和 W. Lv，边缘计算安全：现状与挑战，IEEE 会议录 **107**，1608（2019年）。[18] M. O. Ojo、S. Giordano、G. Procissi 和 I. N. Seitani-dis，低端、中端和高端物联网设备综述，IEEE Access **6**，70528（2018年）。[19] R. Moghe、F. C. Lambert 和 D. Divan，面向智能电网的智能"贴附式"传感器，IEEE 智能电网汇刊 **3**，241（2012年）。[20] C. Xu、J.-G. Liu、Q. Zhang、C. Xu 和 Y. Yang，开环霍尔效应电流传感器热漂移研究及其改进，载于 *2015 IEEE International Workshop on Applied Measurements for Power Systems (AMPS)* 2015 1 6（IEEE，）第–页。[21] I. Metwally，用于高冲击电流测量的自积分罗氏线圈，IEEE 仪器与测量汇刊 **59**，353（2010年）。[22] D. Gazivoda、I. Ziger、I. Novko 和 T. Zupan，采用分段式有源部件对仪用互感器进行内部故障测试的方法，IEEE Access **9**，143295（2021年）。[23] E. O. Schweitzer 和 B. Kasztenny，距离保护：我们为何从圆形特性开始？这重要吗？还有哪些其他方案？，载于 *2018 71st Annual Conference for Protective Relay Engineers (CPRE)*（IEEE，2018年）第1–19页。[24] V. C. Gungor、D. Sahin、T. Kocak、S. Ergut、C. Buccella、C. Cecati 和 G. P. Hancke，智能电网潜在应用与通信需求综述，IEEE Transactions on Industrial Informatics **9**，28（2013年）。[25] M. Ghorbanian、S. H. Dolatabadi、M. Masjedi 和 P. Siano，智能电网中的通信：现有及未来通信和信息基础设施综合综述，IEEE Systems Journal **13**，4001（2019年）。[26] M. Ghorbanian、S. H. Dolatabadi、M. Masjedi 和 P. Siano，智能电网中的通信：现有及未来通信和信息基础设施综合综述，IEEE Systems Journal **13**，4001（2019年）。[27] Y. Yan、Y. Qian、H. Sharif 和 D. Tipper，智能电网通信基础设施综述：动因、需求与挑战，IEEE Communications Surveys & Tutorials **15**，5（2013年）。[28] N. Myoung、Y. Kim 和 S. Lee，智能配电自动化系统和高级计量基础设施的通信基础设施设计，载于 *2010 International Conference on Information and Communication Technology Convergence (ICTC)*（2010年）第461–462页。[29] F. Yıldırım、Y. Yalman、K. u. Bayındır 和 E. Terciyanlı，电力系统边缘计算综合综述：现状、架构与应用，《应用科学》**15**，4592（2025年）。[30] M. Kuzlu 和 M. Pipattanasomporn，评估不同智能电网应用的通信技术与网络需求，载于 *2013 IEEE PES Innovative Smart Grid Technologies Conference (ISGT)*（2013年）第1–6页。[31] ETSI，*Draft TR 102 935, Version: 0.1.3 Machine to Machine Applicability of M2M Architecture to Smart Grid Networks* 2010，技术报告（ETSI，）。

[32] Y. Saleem、N. Crespi、M. H. Rehmani 和 R. Copeland，物联网辅助智能电网：技术、架构、应用、原型与未来研究方向，IEEE Access **7**，62962（2019年）。[33] H. B. Gooi、T. Wang 和 Y. Tang，面向智能电网的边缘智能：应用潜力综述，CSEE电力与能源系统期刊 **9**，1623（2023年）。[34] M. A. Khan、A. M. Saleh、M. Waseem 和 I. A. Sajjad，人工智能赋能的需求响应：智能电网环境中的前景与挑战，IEEE Access **11**，1477（2023年）。[35] M. Bakkar、S. Bogarra、F. C´ orcoles、A. Aboelhas-san、S. Wang 和 J. Iglesias，基于人工智能的智能电网保护，Energies **15**，10 3390 15134933 2022 . /en（）。[36] O. A. Omitaomu 和 H. Niu，智能电网中的人工智能技术：综述，Smart Cities **4**，548（2021年）。[37] L. U. Khan、W. Saad、Z. Han、E. Hossain 和 C. S. Hong，物联网联邦学习：最新进展、分类体系与开放挑战，IEEE Communications Surveys & Tutorials **23**，1759（2021年）。[38] M. Adam、M. Hammoudeh、R. Alrawashdeh 和 B. Alsulaimy，物联网系统中的安全、隐私、信任与架构挑战综述，IEEE Access **12**，57128（2024年）。[39] I. Analytics，2024年物联网现状：全球联网物联网设备数量增长至130亿（2024年）。[40] A. Kolehmainen，物联网安全固件更新：综述，载于 *2018 IEEE iThings / GreenCom / CPSCom / SmartData* 2018 112 117 （）第–页。[41] K. Arakadakis、P. Charalampidis、A. Makrogiannakis 和 A. Fragkiadakis，物联网网络固件空中编程技术综述，ACM Comput. Surv. **54**，10.1145/3472292（2021年）。[42] J. Ahn、H.-Y. Kwon、B. Ahn、K. Park、T. Kim、M.-K. Lee、J. Kim 和 J. Chung，迈向量子安全的分布式能源资源：采用后量子密码学（PQC）和量子密钥分发（QKD），Energies **15**，714（2022年）。[43] R. P. Feynman、R. B. Leighton 和 M. Sands，*The Feynman Lectures on Physics* ，*Vol. I: Mainly Mechanics Radiation and Heat* ，1963（Addison-Wesley，）。[44] D. Halliday、R. Resnick 和 J. Walker，*Fundamentals of Physics* 10 2014 ，第版（Wiley，）。[45] D. Kleppner 和 R. Jackiw，量子物理学百年，《科学》**289**，893–898（2000年）。[46] J. P. Dowling 和 G. J. Milburn，量子技术：第二次量子革命，《英国皇家学会哲学汇刊》A辑：数学、物理与工程科学 **361**，1655–1674（2003年）。[47] H. M. Wiseman 和 G. J. Milburn，*Quantum Measurement and Control* 2009 （剑桥大学出版社，）。[48] I. H. Deutsch，驾驭第二次量子革命的力量，PRX Quantum **1**，10.1103/prxquantum.1.020101（2020年）。[49] B. Sævarsson、S. Chatzivasileiadis、H. J´ ohannsson 和 J. Østergaard，电力流算法的量子计算：在真实量子计算机上进行测试（2022年）。[50] P. A. Ganeshamurthy、K. Ghosh、C. O'Meara、G. Cortiana、J. Schiefelbein-Lach 和 A. Monti，基于量子多输出高斯过程的机器学习及其在电网线路参数估计中的应用（2024年）。[51]Y. Hatano、J. Shin、J. Tanigawa、Y. Shigenobu、A. Nakazono、T. Sekiguchi、S. Onoda、T. Ohshima、K. Arai、T. Iwasaki 和 M. Hatano，《利用金刚石量子传感器在宽动态范围内高精度、稳健地监测电动汽车电池的充放电电流》，Scientific Reports 第12卷，10 1038 41598 022 18106 2022 . /s - - -x ( ). [52] P.-Y. Kong，《智能电网通信安全视角下的量子密钥分发协议综述》，IEEE Systems Journal 第16卷，41 (2022)。[53] E. Chae、J. Choi 和 J. Kim，《量子计算量子比特基本原理与发展的入门综述》，Nano Convergence 第11卷，10.1186/s40580-024-00418-5 (2024)。[54] Z. Yang、M. Zolanvari 和 R. Jain，《量子计算与通信中的重要问题综述》，IEEE Communications Surveys & Tutorials 第25卷，1059 2023( )。[55] A. M. Dalzell、S. McArdle、M. Berta、P. Bienias、C.- F. Chen、A. Gily´en、C. T. Hann、M. J. Kastoryano、E. T. Khabiboulline、A. Kubica、G. Salton、S. Wang 和 F. G. S. L. Brand˜ao，《量子算法：应用与端到端复杂度综述》(2023)。[56] J. Biamonte、P. Wittek、N. Pancotti、P. Rebentrost、N. Wiebe 和 S. Lloyd，量子机器学习，Nature 第549卷，195–202 (2017)。[57] A. K. Fedorov、N. Gisin、S. M. Beloussov 和 A. I. Lvovsky，《量子计算迈向量子优势阈值：务实综述》(2022)。[58] S. Aaronson，《细读条款》，Nature Physics 第11卷，291 293 2015– ( )。[59] T. Hoefler、T. H¨aner 和 M. Troyer，《剥离炒作，回归实际：如何切实实现量子优势》，Communications of the ACM 第66卷，82–87 (2023)。[60] C. H. Bennett、G. Brassard、C. Cr´epeau、R. Jozsa、A. Peres 和 W. K. Wootters，《通过经典与爱因斯坦-波多尔斯基-罗森双通道传送未知量子态》，Phys. Rev. Lett. 第70卷，1895 (1993)。[61] M. Schlosshauer，量子退相干，《物理评论》831，1 (2019)。[62] Y. Xu、X. Han、R. Luo 和 Z. Li，面向城市社区5G基站与光伏电站联合规划的混合量子-经典随机规划，Scientific Reports 第15卷，42642 (2025)。[63] M. Moniruzzaman、C. Lu 和 M. S. Hossain，面向节能型电动公交车充电优化的混合量子-经典机器学习，SSRN (2025)。[64] Z. Zimbor´as、B. Koczor、Z. Holmes、E.-M. Borrelli、A. Gily´en、H.-Y. Huang、Z. Cai、A. Ac´ın、L. Aolita、L. Banchi、F. G. S. L. Brand˜ao、D. Cavalcanti、T. Cubitt、S. N. Filippov、G. Garc´ıa-P´erez、J. Goold、O. K´alm´an、E. Kyoseva、M. A. C. Rossi、B. Sokolov、I. Tavernelli 和 S. Maniscalco，《完全容错实现之前关于量子计算的迷思：不可行定理排除了什么，又没有排除什么》(2025)。[65] T. Patel、A. Potharaju、B. Li、R. B. Roy 和 D. Tiwari，《含噪中等规模量子计算机的实验评估：误差测量、表征及其影响》，载于 *SC20: International Conference for High Performance Computing, Networking, Storage and Analysis* (2020)，第1–15页。[66] A. G. Fowler、M. Mariantoni、J. M. Martinis 和 A. N. Cleland，表面码：迈向实用的大规模

量子计算，Physical Review A **86**，032324 (2012)，出版方：美国物理学会。[67] Z. Cai、R. Babbush、S. C. Benjamin、S. Endo、W. J. Huggins、Y. Li、J. R. McClean 和 T. E. O'Brien，量子误差缓解，《现代物理评论》**95**，045005 (2023)，出版方：美国物理学会。[68] S. Herbst、V. De Maio 和 I. Brandic，流式物联网数据与量子边缘：经典/量子机器学习应用案例，载于 *Euro-Par 2023: Parallel Pro-cessing Workshops* (Springer Nature Switzerland, 2024)，第177–188页。[69] C. L. Degen、F. Reinhard 和 P. Cappellaro，量子传感，《现代物理评论》**89**，10.1103/revmod- phys.89.035002 (2017)。[70] M. W. Doherty、V. V. Struzhkin、D. A. Simpson、L. P. McGuinness、Y. Meng、A. Stacey、T. J. Karle、R. J. Hemley、N. B. Manson、L. C. Hollenberg 和 S. Prawer，压力下金刚石 NV⁻ 中心的电子特性与计量应用，Phys. Rev. Lett. **112**，10.1103/PHYSREVLETT.112.047601 (2014)。[71] J. Fang、W. Wang、Y. Zhou、J. Li、D. Zhang、B. Tang、J. Zhong、J. Hu、F. Zhou、X. Chen、J. Wang 和 M. Zhan，经典与原子重力测量，Remote Sensing **16**，2634 (2024)。[72] E. Oh、M. D. Gregoire、A. T. Black、K. Jeramy Hughes、P. D. Kunz、M. Larsen、J. Lautier-Gaud、J. Lee、P. D. D. Schwindt、S. L. Mouradian、F. A. Narducci 和 C. A. Sackett，量子传感器展望：从基础研究到商业应用，AIAA Journal **第62卷**，4029 4053 2024– ( )。[73] F. Casola、T. van der Sar 和 A. Yacoby，利用基于金刚石氮-空位中心的磁测量探测凝聚态物理，Nature Reviews Materials **第3卷**，10.1038/natrevmats.2017.88 (2018)。[74] K. Hayashi、Y. Matsuzaki、T. Taniguchi、T. Shimo-Oka、I. Nakamura、S. Onoda、T. Ohshima、H. Morishita、M. Fujiwara、S. Saito 和 N. Mizuochi，利用氮-空位中心系综的光探测磁共振谱优化温度灵敏度，Phys. Rev. Appl. **第10卷**，034009 (2018)。[75] M. S. Alam、F. Gorrini、M. Gawe-lczyk、D. Wig-ger、G. Coccia、Y. Guo、S. Shahbazi、V. Bharadwaj、A. Kubanek、R. Ramponi、P. E. Barclay、A. J. Bennett、J. P. Hadden、A. Bifone、S. M. Eaton 和 P. Mach-nikowski，根据金刚石波导中带负电氮-空位中心系综的零场光探测磁共振谱确定应变分量，Phys. Rev. Appl. **第22卷**，024055 (2024)。[76] Y. Hatano、J. Shin、D. Nishitani、H. Iwatsuka、Y. Ma-suyama、H. Sugiyama、M. Ishii、S. Onoda、T. Ohshima、K. Arai、T. Iwasaki 和 M. Hatano，利用光纤耦合量子金刚石传感器同时进行温度测量和磁测量，Applied Physics Letters **第118卷**，10 1063 5 0031502 2021 . / . ( )。[77] J. Pogorzelski、L. Horsthemke、J. Homrighausen、D. Stiegek¨otter、M. Gregor 和 P. Gl¨osek¨otter，基于金刚石 NV 中心的紧凑型全集成 LED 量子传感器，Sensors **第24卷**，743 (2024)。[78]IBM，IBM 构建开放量子软件生态系统的路线图 (2025)，存档/最后访问日期：2025-04-04。[79] E. Barker 和 A. Roginsky，*Transitioning the Use of Cryptographic Algorithms and Key Lengths*，技术报告。

NIST特别出版物（SP）800-131A，第2版（美国国家标准与技术研究院，马里兰州盖瑟斯堡，2019年）。[80] 德国联邦信息安全局，*Cryptographic Mechanisms: Recommendations and Key Lengths Version: 2025-1* ，，技术报告 BSI TR- -02102 1（德国联邦信息安全局，德国波恩，2025年）。[81] C. Gidney 和 M. Eker˚å，《如何利用2000万个含噪量子比特在8小时内分解2048位RSA整数》，《Quantum》**第5卷**，433（2021年）。[82] F. Boudot、P. Gaudry、A. Guillevic、N. Heninger、E. Thom´é 和 P. Zimmermann，《比较因数分解与离散对数的难度：一项240位数实验》，载于 *Advances in Cryptology – CRYPTO 2020*，D. Micciancio 和 T. Ristenpart 编（施普林格国际出版公司，查姆，2020年），第62–91页。[83]S. Pirandola、U. L. Andersen、L. Banchi、M. Berta、D. Bunandar、R. Colbeck、D. Englund、T. Gehring、C. Lupo、C. Ottaviani、J. L. Pereira、M. Razavi、J. Shamsul Shaari、M. Tomamichel、V. C. Usenko、G. Vallone、P. Villoresi 和 P. Wallden，《量子密码学进展》，《光学与光子学进展》**第12卷**，1012（2020年）。[84] P. Sharma、A. Agrawal、V. Bhatia、S. Prakash 和 A. K. Mishra，《量子密钥分发保护的光网络：综述》，IEEE通信学会开放期刊**第2卷**，2049–2083（2021年）。[85] Y. Cao、Y. Zhao、Q. Wang、J. Zhang、S. X. Ng 和 L. Hanzo，《量子密钥分发网络的演进：迈向量子互联网》，IEEE通信调查与教程**第24卷**，839（2022年）。[86] Z. C. M. Davidson、E. Hugues-Salas、G. M. Bonner、B. E. Jones、J. Prentice、S. Kariappa、D. S. Fowler、R. D. Oliveira、P. Zhang、Y. Andersson、E. A. Kosmatos、A. Stavdas 和 A. Lord，《AirQKD：自由空间光学量子密钥分发在实现务实、安全且可扩展的通信中的作用》，IEEE通信杂志**第62卷**，40（2024年）。[87] R. Bedington、J. M. Arrazola 和 A. Ling，《卫星量子密钥分发的进展》，npj量子信息**第3卷**，30（2017年）。[88] H. Dai、X. Sun、B. Lv、H. Wang 和 L. Tong，《面向电网终端的多场景量子密钥分发机制》，载于 *2024 12th International Conference on Information Systems and Computing Technology (ISCTech)* 2024 1 5 ()，第–页。[89] Z. Li、K. Xue、J. Li、L. Chen、R. Li、Z. Wang、N. Yu、D. S. L. Wei、Q. Sun 和 J. Lu，《纠缠辅助量子网络：机制、使能技术、挑战与研究方向》，IEEE通信调查与教程**第25卷**，2133–2189（2023年）。[90] J. A. Dolphin、T. K. Para¨íso、H. Du、R. I. Woodward、D. G. Marangon 和 A. J. Shields，《混合集成量子密钥分发收发器芯片》，npj量子信息**第9卷**，84（2023年）。[91] M. Alshowkan、P. G. Evans、M. Starke、D. Earl 和 N. A. Peters，《利用量子密钥分发对智能电网通信进行身份验证》，Scientific Reports**第12卷**，12731（2022年）。[92] P. G. Evans、M. Alshowkan、D. Earl、D. D. Mulkey、R. Newell、G. Peterson、C. Safi、J. L. Tripp 和 N. A. Peters，《电力公司中的可信节点量子密钥分发》，IEEE Access**第9卷**，105220（2021年）。

[93] AZO Quantum, 《莫子卫星如何从太空提供量子安全》（2022年）。[94] Z. Tang、P. Zhang 和 W. O. Krawec, 《微电网安全的量子飞跃：量子安全微电网的前景》, IEEE Electrification Magazine 第9卷，66 73 2021–（）。[95] Z. Tang、Y. Qin、Z. Jiang、W. O. Krawec 和 P. Zhang, 《量子安全网络化微电网》, 载于 *2020 IEEE Power & Energy Society General Meeting (PESGM)*（2020年）, 第1–5页, ISSN：1944-9933。[96] W. Grice、M. Olama、A. Lee 和 P. G. Evans, 《量子密钥分发在智能电网网络安全系统中的适用性》, IEEE Access 第13卷，17398（2025年）。[97] E. Diamanti、H.-K. Lo、B. Qi 和 Z. Yuan, 《量子密钥分发的实际挑战》, npj量子信息 第2卷，16025（2016年）。[98] M. Gado、M. Ismail 和 W. O. Krawec, 《升级电力系统的网络层以支持半量子密钥分发》, 载于 *2024 IEEE Power & Energy Society Innovative Smart Grid Technologies Conference (ISGT)*（2024年）, 第1–5页, ISSN：2472-8152。[99] F. Beutel、H. Gehring、M. A. Wolff、C. Schuck 和 W. Pernice, 《适用于GHz时钟速率的探测器集成片上量子密钥分发接收器》, npj量子信息 第7卷，40（2021年）。[100] I. Astaburuaga、S. Rath 和 S. Sengupta, 《揭示BB84的漏洞：量子密钥分发仿真库》, 载于 *2025 IEEE 22nd Consumer Communications & Networking Conference (CCNC)* 2025 （）, 第1–8页。[101] A. B. Price、J. G. Rarity 和 C. Erven, 《一种用于快速拒绝服务检测的量子密钥分发协议》, EPJ Quantum Technology 第7卷，8（2020年）。[102] A. Apostolov, 《广域GOOSE及其在系统完整性保护方案中的应用》, 载于2021 *74th Conference for Protective Relay Engineers (CPRE)*（2021年）, 第1–5页。[103] M. Buechel、M. Zimmer、D. Carta 和 A. Benigni, 《利用相关高斯过程估计配电网电压》, 载于 *2025 IEEE 15th International Workshop on Applied Measurements for Power Systems (AMPS)*（2025年）, 第1–6页。[104] J. Xie、A. Rahman 和 W. Sun, 《基于贝叶斯生成对抗网络的虚假数据注入攻击检测：面向含分布式能源资源的主动配电网》, IEEE 智能电网汇刊 第15卷，3223（2024年）。[105] ETSI, *GS QKD 004; Version: 2.1.1 Quantum Key Distribution (QKD); Application Interface*, 技术报告（ETSI，2020年）。[106] ETSI, *Draft GR QKD 017; Version: 0.1.13 Quantum Key Distribution (QKD); Analysis of QKD Network architectures* 2025, 技术报告（ETSI，）。[107] A. Peres 和 D. R. Terno, 《量子信息与相对论》, 《现代物理评论》第76卷，93（2004年）。[108] P. H. Eberhard, 《贝尔定理与定域性的不同概念》, 《新物理学杂志》B辑第11系列 第46卷，392 419 1978–（）。[109] P. Babahajiani 和 P. Zhang, 《量子分布式微电网控制》, 载于 *2022 IEEE Power & amp; Energy Society General Meeting (PESGM)* 2022 （IEEE, ）, 第1–5页。[110] P. Babahajiani、P. Zhang、T.-C. Wei、J. Liu 和 X. Lu, 《利用相互作用量子比特实现分布式微电网控制》, IEEE电力系统汇刊，第1页（2022年）。

[111] G. Ahmad、A. Hassan、A. Islam、M. Shafiullah、M. A. Abido和M. Al-Dhaifallah, 《微电网分布式控制策略：技术与挑战的批判性综述》, IEEE Access **13**，60702（2025年）。[112] W. K. Wootters和W. H. Zurek, 《单个量子不可克隆》, Nature **299**，802（1982年）。[113] D. Dieks, 《利用EPR装置进行通信》, Physics Letters A **92**，271（1982年）。[114] Y. Zhou、Z. Tang、N. Nikmehr、P. Babahajiani、F. Feng、T.-C. Wei、H. Zheng和P. Zhang, 《电力系统中的量子计算》, iEnergy **1**，170（2022年）。[115] S. Golestan、M. Habibi、S. Mousazadeh Mousavi、J. Guerrero和J. Vasquez, 《电力系统中的量子计算：近期进展综述》, Energy Reports **第9卷**，584（2023年）。[116] R. Eskandarpour、K. J. Bahadur Ghosh、A. Khodaei、A. Paaso和L. Zhang, 《未来的量子增强型电网：入门读本》, IEEE Access **8**，188993（2020年）。[117] Z. Liu、K.-K. R. Choo和J. Grossschadl, 《使用基于格的密码学保障后量子物联网中边缘设备的安全》, IEEE Communications Magazine **56**，158（2018年）。[118] S. Ebrahimi、S. Bayat-Sarmadi和H. Mosanaei-Boorani, 《面向物联网中边缘与资源受限设备优化的后量子密码处理器》, IEEE Internet of Things Journal**6**，5500（2019年）。[119] Q. Zhuang、Z. Zhang和J. H. Shapiro, 《利用连续变量多体纠缠的分布式量子传感》, Physical Review A**97**，10.1103/phys-reva.97.032329（2018年）。[120] M. Sch¨offel、F. Lauer、C. C. Rheinl¨ander和N. Wehn, 《量子计算机时代的安全物联网——瓶颈何在？》, Sensors **22**，10.3390/s22072484（2022年）。[121] T. Duan和V. Dinavahi, 《智能电网中支持SDN的广域测量系统基于数据平面的快速故障切换》, IEEE Transactions on Industrial Informatics **19**，8148（2023年）。[122] A. Goodney、S. Kumar、A. Ravi和Y. H. Cho, 《利用软件定义网络实现高效的相量测量单元组网》, 载于*2013 IEEE International Conference on Smart Grid Communications (SmartGridComm)* 2013 378 ()第–383页。[123] I. Kunze、R. Glebke、J. Scheiper、M. Bodenbenner、R. H. Schmitt和K. Wehrle, 《网内计算在工业场景中适用性的研究》, 载于*2021年4th IEEE International Conference on Industrial Cyber-Physical Systems (ICPS)* 2021 334 340 ()第–页。[124] K. Azuma、S. E. Economou、D. Elkouss、P. Hilaire、L. Jiang、H.-K. Lo和I. Tzitrin, 《量子中继器：从量子网络到量子互联网》, 《现代物理评论》**95**，045006（2023年）。[125] Linux Foundation / SOGNO成员与贡献者，SOGNO - LF Energy（2025年）。[126] 50Hertz, MCCS（2025年）。[127] E. I. Malevannaya、I. A. Polozov、Vikto...ov、A. V. Andriyash和I. A. Rodionov, 《超导量子电路屏蔽工程指南》, Applied Physics Reviews **第12卷**，031334（2025年）, https://pubs.aip.org/aip/apr/article-pdf/doi/10.1063/5.0250262/20708867/031334_1_5.025026"

[128] X. P. Le, L. Mayer, S. Magaletti, M. Schmidt, J.-F. Roch 和 T. Debuisschert，基于全碳肖特基接触的金刚石中氮空位中心场效应检测磁共振，Communications 第2卷. pdf。

Engineering **4**，209（2025年）。[129] S. E. Crawford、R. A. Shugayev、H. P. Paudel、P. Lu、M. Syamlal、P. R. Ohodnicki、B. Chorpening、R. Gentry 和 Y. Duan，能源应用中的量子传感：综述与展望，Advanced Quantum Technologies **4**，2100049（2021年），https://advanced.onlinelibrary.wiley.com/doi/pdf/10.1002/qute.202100049。[130] A. Barenco、C. H. Bennett、R. Cleve、D. P. DiVincenzo、N. Margolus、P. Shor、T. Sleator、J. A. Smolin 和 H. Weinfurter，量子计算的基本门，Physical Review A **第52卷**，3457（1995），编号：5。[131] D. Deutsch 和 R. Jozsa，量子计算快速解决问题，伦敦皇家学会会刊 A 辑 **439**，553（1992），出版者：英国皇家学会。[132] E. Knill 和 R. Laflamme，量子纠错码理论，Physical Review A **55**，900（1997）。[133] W. Dur 和 H. J. Briegel，纠缠纯化与量子纠错，Reports on Progress in Physics **70**，1381（2007）。