电力工程信息安全风险问题及量子加密通信防护策略

王 霞

（雄特建设工程（山东）有限公司，山东 聊城 252000）

摘 要 由于电力系统结构复杂、数据资产价值高，信息安全风险日益凸显，传统加密方式难以有效应对日益频发的网络攻击事件，电力系统面临数据窃取、业务中断等重大安全隐患。基于此，本文分析了电力工程信息安全的现状与挑战，梳理了电力监控、智能电网通信、数据中心等环节的主要风险问题，提出基于量子加密通信的信息安全防护策略，从量子密钥分发、量子安全通信协议、量子加密存储等方面，探讨了量子技术在电力系统入侵检测、数据传输保护、访问控制优化等领域的应用前景，以期为保障电力系统安全运行提供参考。

关键词 电力工程；信息安全；风险防控；量子加密通信

中图分类号：TN91 **文献标志码**：A **DOI**：10.3969/j.issn.2097-3365.2025.24.011

0 引言

电力系统作为国家关键基础设施，其安全稳定运行事关国计民生。随着能源互联网、泛在电力物联网等新型电力系统加速建设，电力工程信息化、自动化、智能化水平不断提升。电力系统规模庞大、结构日趋复杂，数据资产价值也与日俱增，由此衍生出诸多信息安全风险，网络入侵、数据窃取、业务中断等安全事件频发，给电网运行埋下重大隐患。传统加密技术受算法强度所限，难以从根本上解决电力信息安全难题。为破解电力系统面临的信息安全困境，亟需引入新型加密防护技术，筑牢电力系统网络安全防线。量子加密通信技术以其“绝对安全”等独特优势，有望成为保障电力信息安全的“利器”。本文在分析电力工程主要信息安全风险的基础上，重点探讨量子加密通信技术在电力系统信息防护中的应用策略，以期为提升电力工程信息安全性提供参考。

1 电力工程信息安全风险的现状与挑战

1.1 电力系统信息安全威胁的多样性与复杂性

电力系统是一个复杂的网络物理融合系统，涵盖发电、输电、变电、配电、用电等诸多环节，系统架构异常庞杂。随着电力系统向着信息化、自动化、智能化方向发展，信息技术与电力物理设施的融合日益紧密，使得电网暴露在更加广阔的网络空间，信息安全风险不断积聚。电力工业信息化进程加快，企业管理、生产调度、市场交易等各个领域高度依赖信息系统，由此产生海量电力数据资产，数据窃取、篡改的风险大大增加。能源互联网、泛在电力物联网建设提速，海量智能终端接入电网，数据采集、传输环节多，边界防护难度大，网络入侵、恶意代码植入等威胁更加凸显，电力工控系统与IT系统的互联互通，使得工业控制网络与互联网的边界日益模糊，更容易受到来自IT领域的网络攻击。电力系统供电服务与社会民生息息相关。发生大规模信息安全事件，极易在能源电力领域引发连锁反应，对国家能源安全、社会经济稳定造成严重冲击，电力工程信息安全形势日趋严峻，亟需提高风险防控能力[1]。

1.2 传统加密技术面临的局限性与挑战

电力系统大多采用传统密码学技术实现信息加密保护，主要包括对称加密算法（如AES、3DES）和非对称加密算法（如RSA、椭圆曲线），这两类算法在应对一般的网络威胁时，能够发挥一定的作用。但在电力工程的复杂应用场景下，仍面临诸多局限性，传统密码算法的安全性主要依赖于密钥的保密性和算法自身的数学难题，密钥泄露或算法被攻破，加密体系将很快瓦解。随着量子计算、云计算等新型计算模式的发展，传统密码算法面临被破解的风险与日俱增，保障海量电力数据的长期安全，是摆在电力工程信息安全建设面前的一道难题。电力系统终端节点分布广泛、数量庞大，密钥管理的复杂度高，传统的密钥分发方案存在较大局限性，易引发密钥配送失误、私钥复制等问题，增加安全隐患。电力系统对网络通信的高可靠、低时

延也提出了更高要求。传统加密技术在实现大规模组网时，不可避免地会带来通信效率损耗，面对电力系统复杂多变的应用场景需求，传统密码学技术暴露出诸多“短板”，亟需创新性的信息安全防护之策。

1.3 电力信息安全事件的危害与影响分析

电力系统作为国家关键基础设施，遭受网络攻击，极易在能源电力领域引发连锁反应，后果不堪设想。攻击者可能利用系统漏洞，侵入电网调度控制中心，窃取敏感数据，篡改关键参数，下达错误控制指令，导致电网运行严重失衡。变电站可能因此发生爆炸，输电线路过载熔断，大片区域陷入黑暗。电力中断将给工业生产、交通运输、通信网络等各个领域带来灾难性的连锁反应，工厂车间被迫停工，生产线陷入瘫痪，经济损失难以估量，居民日常生活更是困难重重，电梯无法运行，空调制冷系统停摆，自来水供应中断，给人们的衣食住行带来诸多不便。网络攻击导致电力系统大面积停运，将给国计民生带来灾难性影响。现代工业生产线高度自动化，完全依赖于连续稳定的电力供应，若电网瘫痪，工厂车间必然停工，造成的经济损失是惊人的。许多精密仪器设备在突然断电后很容易损坏，重新启动也需要很长时间，生产效率大打折扣。电力中断严重影响城市交通、通信网络、金融数据中心等关键领域，给人们的日常工作生活带来诸多不便。重要民生场所如医院、血库、疫苗冷藏库若是突然断电，将给公众健康安全带来威胁。电力信息安全事件一旦发生，其影响之深远，危害之巨大，实在是不堪设想[2]。

2 电力工程中的主要信息安全风险问题

2.1 电力监控系统的网络入侵与数据窃取风险

电力监控系统是电力系统安全稳定运行的核心枢纽，集中承担电网运行监视、安全分析、故障诊断等任务，掌控着电网的“生命线”。

电力监控系统信息化程度高，外部接口多，易成为网络攻击的“重灾区”，来自互联网的恶意入侵、数据窃取威胁日益凸显，网络入侵者一旦攻破电力监控系统，窃取系统权限，即可任意操纵电网运行，置电网安全于危难之中。监控系统汇聚了海量电网实时工况数据，数据价值高，极易成为攻击者觊觎的目标，数据被非法窃取，不仅会泄露电网运行机密，更可能被对手恶意利用，实施精准打击。数据的恶意篡改也将严重影响监控系统判断，酿成错误控制决策，更有甚者，攻击者还可能借助监控系统进一步渗透发电、输电等更深层次的控制系统，危及电网运行安全。筑牢电力监控系统网络安全防线，对保障整个电力系统安全至关重要[3]。

2.2 智能电网通信环节的信息传输安全隐患

智能电网通过信息通信技术将电网各个环节紧密连接，实现电力系统的高度自动化和智能化。电网通信环节众多，传输距离远，数据资产的机密性、完整性、可用性面临巨大威胁，在发电侧，发电厂监控系统、故障录波装置等智能终端需要与调度控制中心实时通信。传输电厂运行状态、故障告警等关键信息；在输电侧，变电站自动化系统通过光纤、无线等通信方式接入调度数据网，上送电压、电流等海量测量量，通信链路如果被恶意窃听、侦测，电网运行机密将无所遁形，更为严重的是，部分变电站仍采用明文传输控制指令。遭到篡改，变电站将执行错误操作，埋下极大的安全隐患，配电自动化大量采集配电设备的实时运行数据，接入海量智能电表、新能源并网装置，产生的通信流量剧增，数据完整性难以保证。智能电网各个层级均面临数据传输安全风险，在高度互联的通信网络中确保信息高效、安全地流转，是智能电网建设必须考虑的重点问题。

2.3 电力数据中心的信息存储与访问控制风险

电力工程各环节产生海量数据，电力数据中心承担着数据集中存储、管理和应用的重任。当前不少电力数据中心在数据存储与访问控制方面还存在诸多风险。电力系统缺乏统一的数据分级分类标准，对敏感数据的脱敏处理不到位，使得核心数据资产面临较大泄露风险，部分电力部门的数据服务器、存储设备对外开放程度高，防护措施单一，易受外部入侵威胁。电力数据中心普遍存在身份认证、权限管理漏洞，虽然不同业务信息系统之间采取了一定的逻辑隔离，但内部人员一般拥有较高权限，可跨系统调阅数据，对访问行为缺乏细粒度审计约束，极易酿成“超权访问”。个别单位还存在人员私自利用工作便利复制、携带核心数据资产的情况。加强数据中心的安全防护，规范电力数据全生命周期管理，已成当务之急，从源头消除电力数据泄密隐患，最大限度控制信息安全风险，是电力工程必须直面的难题。

3 量子加密通信在电力工程中的防护策略

3.1 量子密钥分发技术应对网络入侵与数据窃取

针对电力系统网络入侵、数据泄露等安全风险，量子密钥分发（QKD）技术能够发挥独特优势。QKD利

用量子态制备、量子测量等物理机制，在通信双方之间建立“一次一密”的随机密钥，任何窃听企图都将引入不可避免的误码，通信双方能够及时发现非法窥探，进而废止密钥，这种基于物理层面的绝对安全保障，从根本上杜绝了窃听风险。电力工程可以将 QKD 技术应用于核心控制区、调度数据网等高安全需求场合，实现发电控制、电网调度系统与主控中心的加密通信，有效抵御网络入侵。在数据存储环节，利用 QKD 为海量电力数据提供端到端的加密保护，即使密文数据库泄露，攻击者也难以在有限时间内破解密文，最大程度规避数据泄密风险。QKD 技术生成的安全密钥可用于保护电力监控、变电站等系统的认证过程，防止内部私钥被复制、滥用。QKD 有望成为应对电力系统信息泄露的“利器”，筑牢电力工程的安全屏障[4]。

3.2 量子安全通信协议保障智能电网信息传输

智能电网通信网络异常庞杂，传输链路交错重叠，传统加密方案难以全面覆盖，量子安全直接通信（QSDC）协议能够通过单光子序列直接传送秘密信息，无需事先分发密钥，简化了密钥管理，是保障智能电网通信安全的理想选择。基于 QSDC 技术，在智能电网部署多用户网络，实现各区域终端与控制中心的机密通信。QSDC 利用非正交量子态编码信息，数据的安全性直接由量子物理定律保证，攻击者无法通过测量获取隐藏信息，通信安全性显著提升。还可进一步采用诱骗态技术，即将部分信息比特编码为正交态，专门用于窃听检测，使得量子信道能够抵御更强的攻击。对于电力调度控制指令等核心数据，采用 QSDC 技术与认证协议相结合，保证指令传输机密性，验证通信双方身份，提供更高等级的安全防护。在智能电表、配电终端接入等场合，QSDC 多用户组网能力可有效支撑海量节点通信需求。QSDC 无需密钥协商、密钥存储等复杂流程，通信效率高，满足智能电网信息传输的低时延需求。量子安全通信有望成为智能电网通信安全的“护身符”。

3.3 量子加密存储技术强化数据中心访问控制

电力数据资产的存储保护与访问管控是确保数据机密性的重中之重。电力工程可以引入量子加密存储技术，利用量子密钥实现更为可靠的数据安全托管。量子加密存储将原始数据在本地利用量子密钥加密，密文数据上传至云端，用户凭借量子密钥才能解密访问。在数据存储阶段，电力部门可放心地将数据委托给第三方管理，即便内部管理人员也难以恶意窃取，数据泄密风险大为降低。在访问控制方面，可基于量子密钥实现细粒度授权，不同部门、岗位人员持有不同的量子密钥，对不同分区的电力数据拥有相应读写权限，系统记录所有外来量子密钥及其操作行为，可溯源性强，配合严格的异常访问审计机制，对越权操作行为进行预警，从而从源头遏制内部人员超权访问、滥用职权等行为[5]。由于量子密钥能够频繁更新，可定期轮换电力数据的加密密钥，使数据更新保护机制常态化，强化系统的长期安全性，量子加密存储技术将为电力数据的长期、可靠保护提供坚实的保障。

4 结束语

电力系统是经济社会运行的重要基础，随着电力工程信息化、网络化进程的不断加快，信息安全风险也日益突出，给电网安全稳定运行带来了严峻的挑战。传统密码学技术受制于自身局限，难以应对日益频发的网络攻击事件，电力系统亟需创新的信息安全防护策略。量子加密通信技术为破解电力工程信息安全困局指明了新路径。量子密码的“不可克隆”特性，信息论意义上的无条件安全，将从根本上消除窃密隐患；量子态易受扰动的敏感性，又使得窃听行为无所遁形，确保通信私密，QKD、QSDC 等量子安全通信协议分别针对电力核心控制系统、智能电网通信场景，有效规避网络入侵、数据泄露风险。量子加密存储进一步强化了电力数据资产的安全托管和精准授权，最大限度地避免了敏感信息泄露。电力工程应积极布局量子密码技术创新，结合行业应用实际，探索量子加密在电网入侵检测、安全通信、访问控制、身份认证等方面的最佳实践，构建一套全方位、纵深化的网络安全防护体系，为电力系统安全运行提供坚实的保障。

参考文献：

[1] 盛佃清.面向数字政府的量子安全加密通信框架[J].山西大学学报(自然科学版),2024,47(04):815-822.

[2] 梁东贵,梁哲辉,李韫莛,等.面向电网服务信息交互的数据通信安全策略研究[J].电子设计工程,2024,32(16):73-77.

[3] 同[1].

[4] 贾耕涛,倪玮栋,吴佳伟,等.面向能源互联网的电力量子保密通信关键技术研究及应用[J].电力信息化,2020,18(07):1-7.

[5] 文涛,李夏,周海鹏,等.基于量子通信的电力系统安全传输机制研究与实现[J].无线互联科技,2024,21(18):1-3.