计算机研究与发展
Journal of Computer Research and Development
DOI:10.7544/issn1000-1239.2017.20161024
54(4):711-719,2017

面向能源互联网的电力量子保密通信系统性能评估

陈智雨[1,2] 高德荃[1,2] 王 栋[1,2] 李国春[1] 魏晓菁[3]
[1](国家电网公司信息通信分公司 北京 100761)
[2](国家电网公司电力信息通信系统运行技术实验室 北京 100761)
[3](国家电网公司 北京 100031)
(zhiyu-chen@sgcc.com.cn)

Performance Evaluation of Power Quantum Secure Communication System for Energy Internet

Chen Zhiyu[1,2], Gao Dequan[1,2], Wang Dong[1,2], Li Guochun[1], and Wei Xiaojing[3]
[1](*State Grid Information & Telecommunication Branch*, *Beijing* 100761)
[2](*Electric Power Information & Telecommunication System Operational Technology Laboratory of State Grid Corporation of China*, *Beijing* 100761)
[3](*State Grid Corporation of China*, *Beijing* 100031)

Abstract With the rapid development of energy Internet, more and more distributed energy systems are accessed. The demand for network and information security of energy information is increasingly urgent. Theoretically, quantum secure communication can achieve unconditional and absolute security in information communication. However, its application in power grid is still in the stage of exploring. This paper focuses on the performance evaluation of power quantum secure communication in the global energy Internet field. Firstly, considering the diversity of the grid business scenario and transmission loss, the system architecture diagram of power quantum secure communication is proposed. Then, through the simulation of the power communication transmission environment and actual business scenario, indicators that quantum channel and data exchange channel of power quantum secure communication system are evaluated in six aspects (e.g. distance loss, pendulum loss and connection loss). Finally, the feasibility and security of quantum secure communication technology in power communication field are verified by simulation experiments, and the development of energy Internet can be effectively assured.

Key words energy Internet; quantum secure communication; performance evaluation; transmission loss; power communication security

摘 要 随着全球能源互联网的快速发展,越来越多分布式能源系统接入,对于能源信息的网络与信息安全关注和需求日益迫切.量子保密通信技术在原理上可实现信息通信的无条件绝对安全,其在电网中的应用尚处于探索试点阶段.围绕全球能源互联网环境下的电力量子保密通信性能进行评估分析研究,1)考虑到电网环境的复杂性和电力通信传输损耗的多样性,提出电力量子保密通信系统性能评估的架构图;2)通过仿真模拟电力通信传输环境、电网实际业务环境,从距离损耗、舞动损耗、接续损耗等6个

收稿日期:2016-12-21;**修回日期**:2017-01-18
基金项目:北京市科技计划项目
This work was supported by the Program of Beijing Municipal Science & Technology.
通信作者:王栋(dong-wang@sgcc.com.cn)

方面测试评估电力量子保密通信系统中的量子信道和数据交互通道的各项性能指标;3)通过仿真实验验证了该技术在电力通信领域应用的可行性及安全性,有效地支撑能源互联网的发展.

关键词 能源互联网;量子保密通信;性能评估;传输损耗;电力通信安全

中图法分类号 TP391

随着"互联网+"模式的提出,各行各业与互联网的融合日益加深,网络安全和信息化已成为互联网经济发展的两大基石.2016 年 4 月 19 日,习近平主席在《在网络安全和信息化工作座谈会上的讲话》里指出:"国家关键信息基础设施面临较大风险隐患,加快构建关键信息基础设施安全保障体系.金融、能源、电力、通信、交通等领域的关键信息基础设施是经济社会运行的神经中枢,是网络安全的重中之重,也是可能遭到重点攻击的目标."能源互联网作为能源与信息技术的融合,构建了一个新的经济发展模式.如何构建能源互联网作为一个全球性的问题,各行各业都在寻求能源互联网发展价值的最大化.在绿色能源、智能发电-变电-输电-配电-用电、储能和电动汽车等新能源技术的发展与大数据分析、物联网以及移动互联网等新技术的碰撞下,构建大规模能源互联网为第三次工业革命的发展提供了有效的支撑.当前,我国在国家层面上提出了能源互联网的发展战略,并开展了相关基础性研究.随着能源互联网的不断发展,信息系统接入越来越多,对信息交互的安全级别提出了更高的要求[1].

能源互联网正在改变电力行业的生态环境,形成了由传统电力系统、分布式能源和信息通信系统等互联而成的交互式电网信息系统.新的电网信息系统具有广泛互联、开放互动、高度智能和灵活服务等特点.随着电网信息系统规模的不断扩大,各项电力业务系统的运行与控制越来越依赖于信息交互式通信传输.通过对近 2 年国内外信息泄露事件进行分析,网络环境的不断恶化以及快速衍变的网络攻击技术更加突显了电力信息通信安全的重要性.我国电力系统信息随着能源互联网的发展不断扩大,网络结构日益复杂,网络边界愈发模糊,中间人欺骗、网络嗅探分析、数据爆破等攻击方式严重挑战现有的数据安全防护手段,电力系统主要包括发电、输电、变电、配电、用电和调度 6 个环节,其中输电操作、配电自动化、高级量测体系、需求响应及用户交互等方面均存在网络安全威胁.因此在能源互联网大环境下,保障电力信息通信安全是一项新的挑战[2-3].量子保密通信技术受各行各业的关注,并在银行和通信运营商等网络进行验证测试.通过对已有量子通信网的分析,该技术理论上可以支撑电力信息通信技术的发展,并搭建电力量子保密通信网络.

量子保密通信是以量子密钥分发(quantum key distribution, QKD)技术为基础的加密通信技术,是最先得到实用化的量子信息技术.量子密钥分发利用单光子不可分割、量子态不可克隆定理和海森堡测不准原理来实现通信双方间的安全密钥分发,解决对称加密算法中密钥分发的安全性问题,实现安全加密通信.与传统加密通信技术不同,量子保密通信的安全性由量子物理原则保障,它是至今为止唯一得到严格证明,从原理上确保通信无条件安全的加密通信技术[4].量子保密通信可以极大地提高国防、政务、金融、电力和能源等领域的信息通信安全,是事关国家安全的战略性高新技术,已成为欧盟、美国和日本等发达国家重点关注的前沿科技热点,国际竞争非常激烈.

量子保密通信技术不断被改进,世界各国将这一技术作为重点发展科技之一.2008 年欧洲 SECOQC 网络、2009 年美国国防部 DARPA QKD 网络和 2010 年日本 Tokyo QKD Network 等提出了国家层面上的量子保密通信研究计划.AT&T、Bell 实验室和 IBM 等世界著名公司对量子保密通信技术投入了大量研发资本,并启动了产业化发展.从 2012 年起,美国军方筹划并部署了针对空间尺度达到 5 000 公里量级的广域量子保密通信网络.欧盟于 2016 年 5 月发布了《量子宣言》,发起一项十亿欧元的量子技术实施计划,项目将于 2018 年启动,目标是促进包括安全的通讯网络和通用量子计算机等在内的多项量子技术的发展,并借此成为第 2 次量子革命的领头羊.日本国家信息通信研究院发布了量子信息通信技术发展蓝图,计划在 2020 年实现量子中继,到 2040 年建成无条件安全、极限容量和超高精度的广域光纤与自由空间量子保密通信网络.英国政府公布了投资 2.7 亿英镑的 5 年专项计划,将量子保密通信、量子测量、量子传感、量子模拟和量子计算等作为重点发展的量子技术.量子保密通信作为我国重点发展的前沿技术之一被列入《国家中长期科学

和技术发展规划纲要(2006—2020 年)》[5]. 2016 年 3 月,《中华人民共和国国民经济和社会发展第十三个五年规划纲要》发布,其中量子通信和天地一体化信息网成为十大重点推进项目,预计两大专项基金支持力度接近千亿. 2016 年 4 月,国家发改委和国家能源局发布《能源技术革命创新行动计划(2016—2030 年)》,明确指出:"重点在电力系统量子通信技术应用、电力设备在线监测先进传感技术、推动电力系统与信息系统深度融合等方面开展研发与攻关."

在国内,我国已经在光量子通信、量子纠缠分发等关键技术取得了一系列国际先进科研成果,率先发射了"墨子号"量子科学实验卫星以开展星地纠缠量子技术研究,并且于 2015 年启动 2000 多公里的"京沪干线"量子通信保密干线工程建设,同时开展了重大工程应用实践,量子保密通信技术已经在我国的银行业和国防等领域得到部分试点应用. 然而,与电力行业通信环境和业务场景相比,现有的量子保密通信技术试点应用工程的业务应用相对单一,量子通道主要以地埋光纤为主,稳定性较好,评估指标主要以量子密钥的成码率为主. 而电力通信网络具有架空线路空间跨度大、强电磁干扰环境、跳接点多等特点,电力调度等生产控制业务对电力通信的时延、可靠性有极高的要求,弱单光子信号在复杂电力应用环境下是否能可靠安全稳定运行需要进行严格的测试与验证,现有的评估指标难以全面衡量复杂电网环境下的电力量子保密通信系统性能.

基于电力行业通信安全传输的考虑,结合量子技术发展趋势和电力业务安全保障迫切需求,本文对量子保密通信技术和电力行业的实际应用场景进行深入研究. 为了满足电力信息量子保密通信系统安全运维和技术发展需求,需要对量子保密通信应用在电力行业进行评估,验证以量子保密通信为基础的电力关键信息基础设施是否安全可靠,能否提升电网调度、系统保护、灾备数据和视频会商等业务的安全保障级别. 本文主要研究在模拟电网业务环境下量子设备的运行状况和性能指标,构建符合电网业务的量子保密通信评估模型.

本文的主要贡献有 2 点:

1) 我们提出了一种电力行业内量子保密通信的评估模型,通过对实验数据分析进行应用场景建模.

2) 搭建不同模拟环境下,对量子保密通信系统进行验证测试,并提出具体的评估指标. 基于本文的工作,我们设计一套视频会议保障量子保密通信系统,首次在电力行业中搭载实际业务.

1 量子保密通信原理

量子技术在传感、通信以及高性能计算等方面有着很强的应用前景. 量子保密通信作为当前量子领域最热门的应用技术之一,具有理论上无条件的安全性和高效性,有着传统通信难以比拟的优势. 由于量子保密通信过程中所传输的信息受干扰时会被不可逆地改变,因此很容易发现窃听行为.

量子保密通信技术的发展建立在通信理论和量子力学之上,构筑了量子信息理论,并形成多种量子保密通信协议. 一个完整的量子保密通信系统以量子编码理论为基础,以量子保密通信协议为核心,通过量子信号的产生、调制和探测等技术,实现信息的传送. 量子保密通信协议有 3 种,分为基于纠缠光子信号、单光子信号和连续变量信号. 本节主要对基于单光信号的量子保密通信协议进行分析.

BB84 协议是最早提出的量子保密通信协议,是其他协议的基础并且最接近实用化. 协议中使用光子的水平偏振态、垂直偏振态和±45 偏振态来实现编码. 图 1 和表 1 分别描述了量子密钥分发工作原理和量子密钥的形成过程. 首先对量子信号进行调制、测量和比对,通信双方建立安全密钥;然后采用一次一密的加密方式加密并传输密文,形成安全通信. 实际应用中,图 1 中的经典公共信号可以采用同一条[6]. 随着研究的不断深入,多种基于 BB84 协议的量子保密通信协议被提出. B92 协议对 BB84 协议进行了简化,但降低了通信效率和实用性. 六态协议在 BB84 协议的基础上进行扩展,提升了量子误码率的上限. 限于现有单光子源技术无法得到理想的单光子,诱骗态协议被提出完善非理想单光子源 BB84 协议,解决了"光子数分离攻击"的问题[7-10].

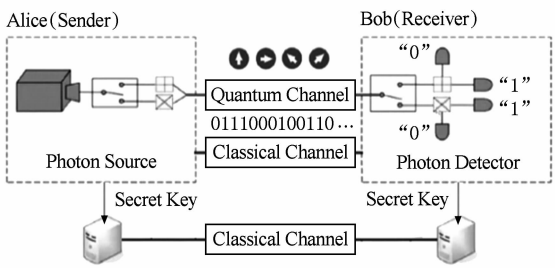

Fig. 1 The framework of quantum key distribution

图 1 量子密钥分发工作原理

Table 1 Quantum Key Generation of BB84 Protocol

表 1 量子密钥生成

QKD	Examples of QKD							
Alice's Bit Sequence	0	1	0	0	1	1	0	1
Alice's Basis	+	+	×	×	+	+	×	×
Alice's Polarization	↑	→	↗	↗	→	→	↗	↘
Bob's Basis	×	+	×	+	×	+	+	×
Bob's Measurement	↗ or ↘	→	↗	↑ or→	↗ or ↘	→	↑ or→	↘
Shared Sifted key		1	0			1		1

Notes: + and × denote basis; arrows denote photon polarization.

目前,单光子量子保密通信系统主要基于偏振调制和相位调制 2 种. 基于偏振调制具有编码/解码简单、光程控制不需十分精确、器件差损小及可进行被动调制等优点,偏振式量子密钥分发系统被不断完善. 本次实验采用单光子偏振式量子密钥分发系统对电力量子保密通信安全传输技术进行研究分析.

2 电力量子保密通信信道特性

对于光信号传输,量子光信号与强光信号一样受各种因素的影响. 在本节中,我们分析量子保密通信传输在电力通信系统中的损耗参数及性能指标.

2.1 光纤损耗[11]

量子保密通信系统传输达到无中继最大距离取决于损耗的程度. 损耗主要受 4 方面的影响:

1) 吸收损耗. 吸收损耗主要包括:材料的本征吸收、杂质吸收和原子缺陷吸收.

2) 散射损耗. 由光的散射引起的损耗主要有:瑞利散射、受激拉曼散射和受激布里渊散射. 瑞利散射是固有损耗(线性散射),决定了光纤损耗的最低理论值. 损耗与波长的四次方成正比(A/λ^4),其中 A 为瑞利散射系数,受纤芯与包层折射率差影响. 另外 2 种散射属于非线性散射,会导致频率的变化.

3) 辐射损耗. 光纤在实际铺设过程中弯曲产生的损耗分为:微弯损耗、过渡弯曲损耗和宏弯损耗.

4) 连接损耗. 在实际链路中,光纤与光钎/光系统连接时产生的损耗. 波长为 1550 nm 时损耗最小,约 0.2 dB/km.

2.2 光纤散射[11]

色散是指由于传输时间的延迟导致脉冲展宽引起的信号失真. 一般情况,量子光脉冲被认为是方差宽度为 σ_T 的近似高斯形. 输出随时间变化的光功率归一化后表达式为

$$p_0(t)=\exp\left(-\frac{t^2}{2\sigma_T^2}\right),$$

其傅立叶变换为

$$P(\omega)=\sqrt{2\pi}\sigma_T\exp\left(-\frac{\omega^2\sigma_T^2}{2}\right).$$

色散分为模式色散、材料色散和波导色散,后两者跟波长有关,被合称为模内色散. 通常量子保密通信中采用单模光纤,本文只讨论模内色散.

1) 材料色散与波长和光纤材料的折射率有关. 光脉冲不是单一色光源,不同波长的传播速度不一样,沿着光纤传输时会展宽脉冲. 因材料色散导致的脉冲展宽的均方差为

$$\sigma_m=\left|\frac{\sigma_\lambda L}{c_0}\lambda\frac{\mathrm{d}^2n_1}{\mathrm{d}\lambda^2}\right|, \tag{1}$$

其中,σ_λ 是谱宽的均方差,c_0 是光速,L 是光纤长度,n_1 是折射率,λ 是波长. 材料色散参数 D 可以表示为

$$D=\left|\frac{\lambda}{c_0}\frac{\mathrm{d}^2n_1}{\mathrm{d}\lambda^2}\right|. \tag{2}$$

通常材料色散参数表示为 ps/(nm·km). 结合式(1)(2),$\sigma_m=\sigma_\lambda LD$.

2) 波导色散受基模能量在芯和包层之间的分布影响. 在单模的情况下($v<2.405$),随着光波长的增加,模场向包层扩展,导致传播常数(α/λ)的增大,使得传输速度变低. 因此,光源波长的不同导致波导色散的产生,光纤的工艺决定着色散的大小.

2.3 电力量子保密通信性能指标

2.1 节和 2.2 节对光纤固有的特性及损耗进行了分析,量子保密通信应用于电力通信系统需要结合实际链路的情况评估. 电力通信线路模式分为架空式和地埋式光缆,线路环境复杂度高. 电力环境中量子保密通信技术的应用受到自然环境(风、雨、雪和温度等)和人工环境(电磁、加密算法和传输数据

量等)的影响.如何评估电力量子保密通信的性能成为当前亟需解决的问题之一.针对实际链路中可能出现的情况,本实验室提出了电力量子保密通信系统性能评估框架,如图 2 所示,并分别对密钥层和业务层构建评估指标体系.密钥层评估指标体现在量子信道中影响量子密钥成码率的因素;业务层评估指标关注经典信道采用量子 VPN 加密传输时系统的传输性能及稳定程度.为了测试不同环境下量子设备成码率及量子 VPN 性能的情况,实验室依据实际线路模拟不同的环境.

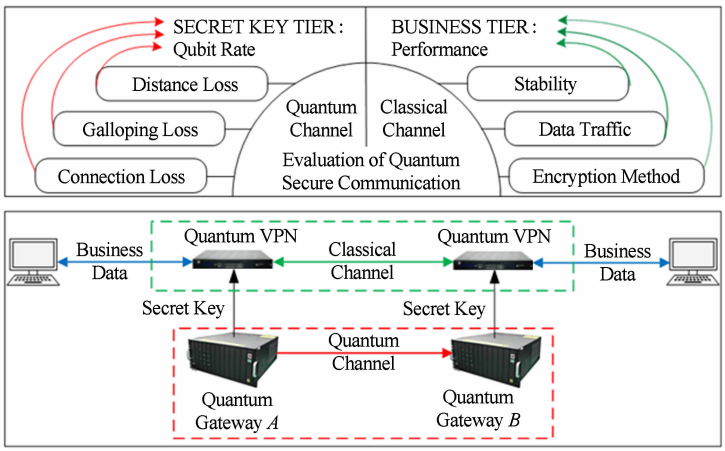

Fig. 2 Evaluation of power quantum secure communication

图 2 电力量子保密通信性能评估

1) 密钥层

① 距离损耗测试.通过搭建不同传输距离的光纤环境,测试不同距离衰减条件下量子设备成码率情况,并记录稳定成码后 1 h 内成码曲线.实际环境(地埋光缆 16.58 km)、模拟环境(裸纤 10 km,20 km,30 km,40 km).

② 舞动损耗测试.在距离测试的基础上,建立电力 OPGW 舞动模拟测试环境.测试传输距离内不同风力级别环境下,量子设备成码率情况并统计稳定成码后 1 h 内成码曲线.风级:稳态(无风)、一级风、二级风、三级风、四级风,如表 2 所示:

Table 2 Wind Scale and Wind Speed List

表 2 风速级别对照表

Wind Scale	Wind Speed/(m·s^{-1})
Light Air	0.3-1.6
Light Breeze	1.6-3.4
Gentle Breeze	5.8-8.0
Moderate Breeze	3.4-5.5

③ 接续损耗测试.在固定传输距离内,通过接入不同损耗的熔接光纤,测试不同熔接损耗下光纤线路环境对量子设备的成码率情况的影响.本次采用 3 根不同的熔接光纤接入模拟线路测试.

2) 业务层

① 数据流量测试.通过在业务两端加载网络性能测试仪,测试经典信道采用量子 VPN 加密传输时的网络时延、抖动、吞吐量、丢包率等传输性能参数.

② 加密算法测试.采用网络性能测试仪测试量子 VPN 采用不同的加密算法对业务数据进行加密传输时量子 VPN 的数据传输性能参数.量子 VPN 支持 IKE 自协商(无量子密钥)、国密 SM4+量子密钥和 AES+量子密钥这 3 种加密方式.

③ 系统稳定性测试.通过接入实际回环光纤线路,测试量子设备在实际传输环境下 7×24 h 内的成码率情况.

3 实验环境及用例

3.1 实验系统架构

图 3 展示了测试系统的网络拓扑图.本次实验中,量子信道采用模拟光纤线路和实际光纤线路进行测试.模拟光纤线路测试中,量子链路使用不同公里数光纤盘作为传输介质.实际光纤线路测试中,量子链路采用实际环境中的地埋式光缆.系统中经典信道使用通用网线模拟搭建.硬件设备如表 3 所示.量子保密通信系统正常运行需满足量子信道衰减小于 13 dB,且两终端间的量子密钥平均成码率(average qubit rate,AQR)不低于 2 Kbps.

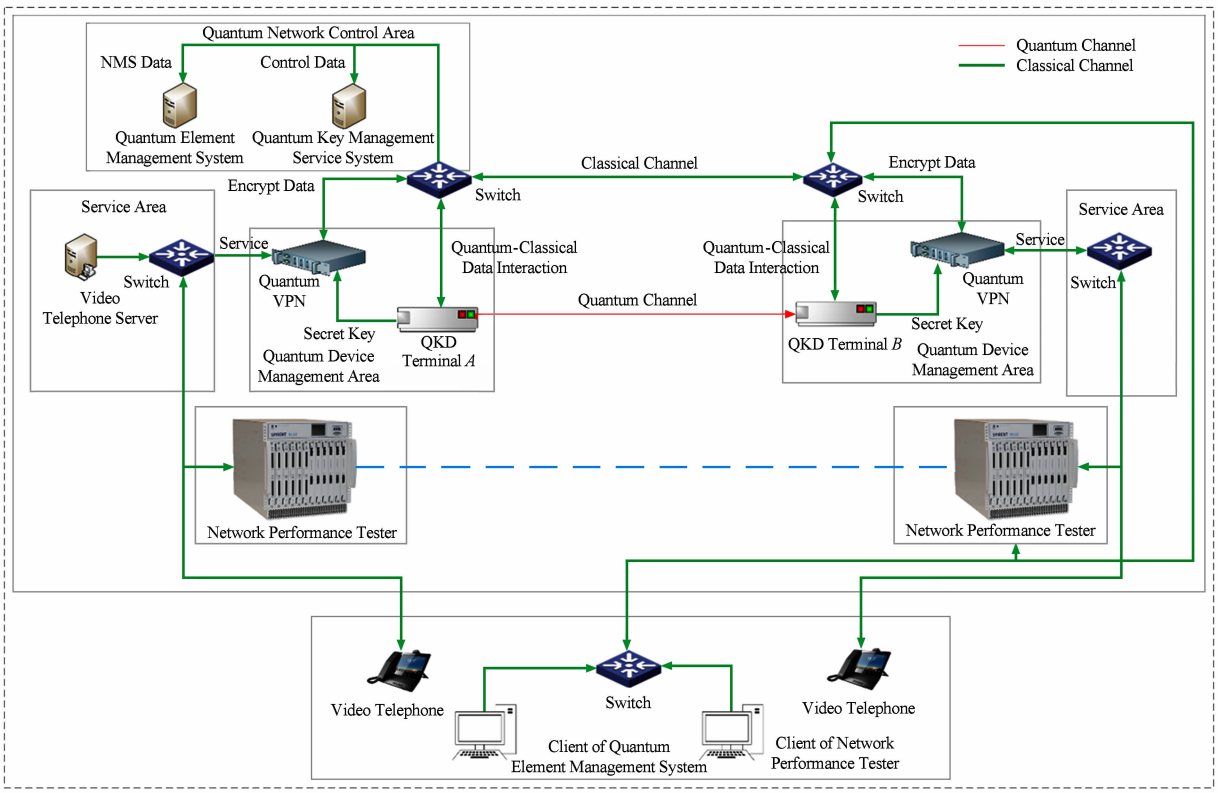

Fig. 3 The network topology of test system

图 3 测试系统网络拓扑图

Table 3 Experimental Equipment

表 3 实验设备

Name of Equipment	Model of Equipment
QKD Terminal *A*	QKDM-POL40A-24G4
QKD Terminal *B*	QKDM-POL40B-24G4
Quantum Key Management Service System	NF-5270 M3
Quantum Network Management System	NF-5270 M3
Video Telephone Server	eSpace U1910
QuantumVPN	SJJ1529 IPsec VPN-Q
Switch	s5700
Video Telephone	espace8950
Network Performance Tester	N11U
OTDR	FTB-200
Optical Fiber Power Meter	JW3116/JW3216A
Digital Anemometer	HT-628
Optical Fiber Tray	2#(10 km),3#(10 km),6#(20 km)
Fused Fiber	1*,2*,3*

3.2 实验用例

本次实验测试不同情况下量子设备的成码性能.

通过对实验结果的分析,评估量子设备对电力通信环境的适应性.对本次实验的用例进行说明:

1) 距离损耗测试.测试在 10 km,20 km,30 km,40 km 以及实际链路下的成码率.

2) 舞动损耗测试.测试在不同风动级别下,10 km,20 km,30 km 和 40 km 的成码率.

3) 接续损耗测试.检测熔接光纤损耗对光信号(1 550 nm)传输及成码率的影响.

4) 加密算法测试.测试不同加密算法对成码率的影响.

5) 数据流量测试.测试不同数据流量对成码率的影响及设备支持的最大数据流量.

6) 稳定性测试.测试在二级风的情况下,实际链路的成码率.

4 实验结果分析

本节对实验结果进行分析,评估量子保密通信在电力环境下的性能.图 4 和图 5 分别是距离损耗测试和舞动损耗测试的实验结果.图 4 所示,随着量子信道光纤线路长度增加,线路距离损耗增大,量子

密钥成码率下降.图 4 中空心圆点为实际链路的实验结果,平均成码率约 6.2 Kbps,大于量子密钥生成终端成码限值(2 Kbps).图 5 显示量子设备成码率在二级风和三级风时波动较大;四级风将光纤吹起使摆动幅度减小,成码率有所升高;40 km 光纤盘受线路衰减和摆动的双重影响,成码率急剧下降,且在二级以上风力的情况下无法成码.综合图 4 和图 5 分析,距离衰减大于 6 dB 导致架空线路成码率出现急剧下降,无风扰动时量子密钥生成终端满足成码限值;当线路受风力扰动时,量子密钥生成终端无法再进行成码.实际应用中需考虑设备的抗干扰能力及量子中继技术的应用.

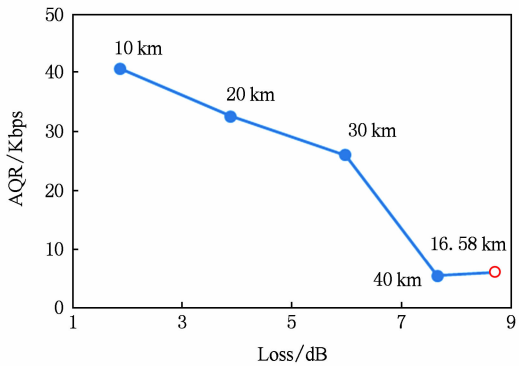

Fig. 4 Test of distance loss

图 4 距离损耗测试

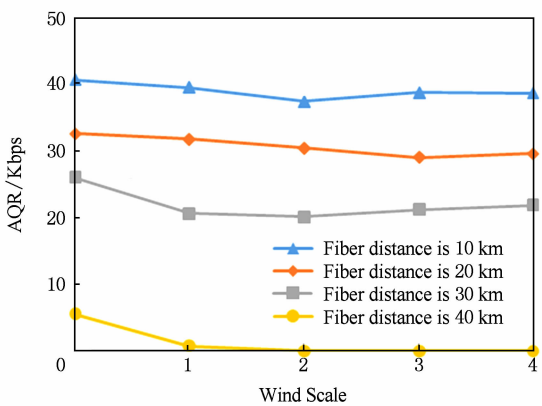

Fig. 5 Test of galloping loss

图 5 舞动损耗测试

图 6 和图 7 分别展示了 10 km 级和 20 km 级光纤分别接续不同熔接光纤的测试结果.从图 6 中可以看出,接续损耗不仅受不同熔接光纤接续的影响,而且受熔接节点数量的影响;节点数的增多导致传输过程中光散射程度增加,接续损耗也随之增大.图 7 所示,2#光纤盘加 3#光纤盘与 6#光纤盘对比,使用 1 根熔接光纤、2 根熔接光纤和 3 根熔接光纤接续分别增加了 1.243 dB,1.566 dB 和 1.897 dB 的损耗.同时,2#光盘与 3#光纤盘接续时,宏弯曲半径小于 4 cm 将导致线路无法正常通信.从表 4 可以得出,在衰耗变化不大的情况下,平均成码率有较大的起伏,侧面论证了风力的不稳定对量子架空线路成码率有较大的影响;同时,较不接续熔接光纤的场合平均成码率分别降低了 11.285 Kbps,13.103 Kbps 和 1.489 Kbps.

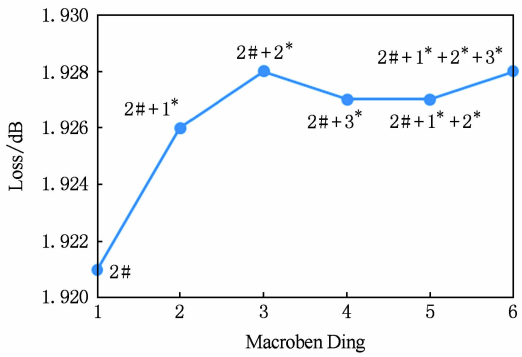

Fig. 6 Test of connection loss (2#)

图 6 接续损耗测试(2#)

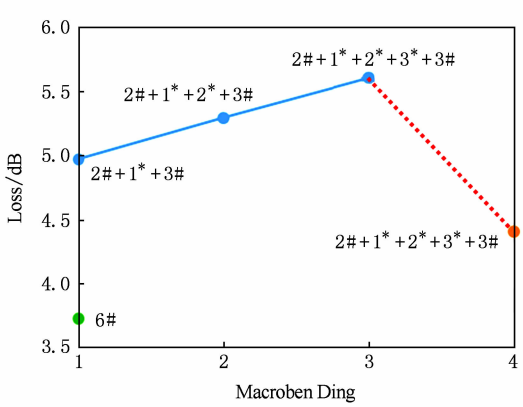

Fig. 7 Test of connection loss (2#+3#,6#)

图 7 接续损耗测试(2#+3#,6#)

Table 4 Test of Connection Loss based on Light Breeze

表 4 二级风接续损耗测试

Test Case	Loss/dB	AQR/Kbps
6#+1*	3.736	20.194
6#+2*	3.738	18.376
6#+3*	3.737	29.990

图 8 描述了不同加密算法下量子 VPN 单向传输吞吐量的测试结果,除了在字节大小为 1 280 B 以外,使用量子密钥的 AES-128 算法是 3 种算法中性能最优的算法.包字节大小影响设备的吞吐量,对实验结果分析,本次实验采用的 VPN 在包字节大小

为 1 280 B 时,对 AES-128 算法支持有所不足. 在字节大小为 64 B 时,使用量子密钥的国密 SM4 算法取得了与 IKE 自协商加密算法同等的网络吞吐量性能. 在其他字节大小的场合,国密 SM4 算法吞吐量性能低于 IKE 自协商加密算法. 国密 SM4 作为与 AES-128 同等量级的算法,且在安全性上更高,本次实验中使用量子密钥的国密 SM4 算法在 3 种方法中吞吐量性能最低. 考虑到算法高效率实施需要软硬件协同工作,量子 VPN 对于国密 SM4 的算法的支持,需从架构上寻求解决方案.

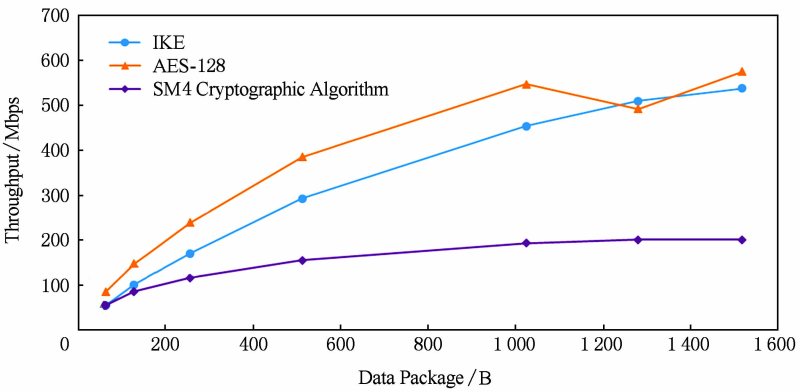

Fig. 8 Test of encryption algorithm

图 8 加密算法测试

采用量子国密 SM4 算法与量子 AES-128 算法对数据进行加解密,国密 SM4 算法较 AES-128 算法对业务数据传输性能影响较大,性能下降范围约 40%～50%. 同时,采用网络性能测试仪分别对不同规模的业务数据流量(范围为 50～500 Mbps)进行测试,结果表明在采用 IKE 自协商加密算法时,量子 VPN 单向传输最大吞吐量为 538 Mbps. 在国密 SM4 算法的条件下,量子 VPN 支持的单向最大吞吐量为 201 Mbps. 对于 AES-128 算法,量子 VPN 支持的单向最大吞吐量为 575 Mbps. 在不超过各加密算法最大吞吐量的条件下,量子 VPN 可稳定传输. 表 5 总结了量子保密通信安全传输系统的稳定性测试结果. 在实际线路环境下,量子设备可长期稳定成码,控制系统运行流畅,网管系统数据上报正常,可以确认量子保密通信系统可长时间稳定运行.

Table 5 Stability Test (7 d)

表 5 7 天稳定性测试

Test Case	Environment	AQR/Kbps
1st day		21.220
2nd day		22.385
3rd day	16.58 km	22.277
4th day	8.72 dB	23.456
5th day	Light Breeze	20.277
6th day		20.281
7th day		22.023

5 总 结

针对量子保密通信技术在电网应用中的复杂性,本文从与电力量子保密通信系统的密钥层和业务层相关的性能参数去分析系统的可行性. 验证方案从距离损耗、舞动损耗、接续损耗、数据流量、加密算法和稳定性 6 个方面提出了性能评估架构,对量子成码率的性能仿真测试数据进行测试评估.

从距离衰减的量子成码率性能测试来看,偏振调制的量子保密通信系统量子信号传输距离为 40 km(通道传输损耗为 7.65 dB)时的量子平均成码率为 5.562 Kbps 传输最大距离在 40 km 左右. 为此在实际应用中,需要综合考虑量子信道的距离与衰减情况,在传输通道上设计部署量子中继站点. 同时,针对 OPGW 在通道受大风影响的情况下,40 公里级量子信道无法成码. 下一步需要开展快速纠偏研究,实现在量子信道受风力干扰的情况,依然能保证电力量子保密通信的稳定运行. 针对量子设备对不同环境的适配性,后续需要进一步结合电网业务场景开展广域范围的量子网络组网研究. 实验结果表明,电力量子保密通信系统中量子信号传输性能显著受到光纤的接续损耗影响. 光通道的偏振和弯曲在很大程度上影响了量子信号传输的性能,因此在工程建设中需要精确熔纤,并且减少光纤通道的接续次数.

通过对业务层性能指标的分析,量子 VPN 对 AES-128 算法的支持高于国密 SM4 算法.从理论上分析,国密 SM4 算法的安全性优于 AES-128 算法.随着国密算法的不断升级,信息通信网络的安全级别也随之提高,量子 VPN 需要从软硬件方面提高对国密算法的优化支持.同时,在量子城域网和广域网建设过程中,各业务系统所处环境、采用的设备和业务需求不尽相同.因此,在满足业务正常运行的条件下,根据电网调度、系统保护、容灾备份和保密会商等实际业务需求合理选择加密算法,构建多种加密算法并存的高效量子保密通信网.

参 考 文 献

[1] Liu Zhenya. Global Energy Internet [M]. Beijing: China Electric Power Press, 2015 (in Chinese)
(刘振亚. 全球能源互联网[M]. 北京: 中国电力出版社, 2015)

[2] Wang Jiye, Guo Jinghong, Cao Junwei, et al. Review on information and communication key technologies of energy Internet [J]. Smart Grid, 2015, 3(6): 473-485 (in Chinese)
(王继业, 郭经红, 曹军威, 等. 能源互联网信息通信关键技术综述[J]. 智能电网, 2015, 3(6): 473-485)

[3] Cao Junwei, Yang Mingbo. Energy Internet—Towards smart grid 2.0 [C] //Proc of the 4th Int Conf on Networking and Distributed Computing. Piscataway, NJ: IEEE, 2013: 105-110

[4] Charles H B, Gilles B. Quantum cryptography: Public-key distribution and coin tossing [C] //Proc of IEEE Int Conf on Computers, Systems and Signal Processing. Piscataway, NJ: IEEE, 1984: 175-179

[5] Zhang Yiying, Zhang Suxiang. Quantum communication and its application in power communication [J]. Electric Power Information and Communication Technology, 2016, 14(9): 7-11 (in Chinese)
(张翼英, 张素香. 量子通信及其在电力通信的应用[J]. 电力信息与通信技术, 2016, 14(9): 7-11)

[6] Yin Hao, Han Yang. Quantum Communication Theory and Technology [M]. Beijing: Publishing House of Electronics Industry, 2013 (in Chinese)
(尹浩, 韩阳. 量子通信原理与技术[M]. 北京: 电子工业出版社, 2013)

[7] Charles H B. Quantum cryptography using any two nonorthogonal states [J]. Physical Review Letters, 1992, 68(2): 3121-3124

[8] Brassard G, Lutkenhaus N, Mor T, et al. Limitations on practical quantum cryptography [J]. Physical Review Letters, 2000, 85(6): 1330-1333

[9] Wang Xiangbin. Beating the photo-number-splitting attack in practical quantum cryptography [J]. Physical Review Letters, 2005, 94(23): 230503

[10] Peng Chengzhi, Zhang Jun, Yang Dong, et al. Experimental long-distance decoy-state quantum key distribution based on polarization encoding [J]. Physical Review Letters, 2007, 98(1): 010505

[11] Pei Changxing, Zhu Changhua. Modern Communication System and Network Measurement [M]. Beijing: Posts & Telecom Press, 2008 (in Chinese)
(裴昌幸, 朱畅华. 现代通信系统与网络测量[M]. 北京: 人民邮电出版社, 2008)

Chen Zhiyu, born in 1987. PhD. His main research interest is signal processing.

Gao Dequan, born in 1975. PhD. His main research interests include the Internet of things and data analytics in smart grid.

Wang Dong, born in 1985. Senior engineer. His main research interest is information security.

Li Guochun, born in 1961. Senior engineer. His main research interest is information and communication technology.

Wei Xiaojing, born in 1971. Senior engineer. Her main research interest is power enterprise information management and technology.