研究论文

模式匹配量子密钥分发在无线公网电力业务中的应用

卞宇翔[1,2], 李圆智[3], 吕超[1,2], 李端超[4], 陈伟[4], 冯宝[1,2], 石开毅[5], 李悦[5], 刘畅[5], 马海强[5*]

摘要 量子密钥分发(quantum key distribution, QKD)为解决传统加密技术所面临的安全挑战和量子计算机带来的威胁能够提供信息理论要求的安全性。探究了 QKD 在无线公网电力业务中的应用且兼顾电磁干扰、通信距离等参数,进行建模和仿真,结果表明,模式匹配协议 QKD 在配对间隔数大于 10^4 时展现出很好的性能,超越 PLOB 界且依然达到超过 400 km 的传输距离,保证了通信链路的安全性,为模式匹配协议 QKD 在无线公网电力业务的应用提供了理论支撑。

关键词 无线公网;量子通信;量子密钥分发;电力业务;模式匹配

电力系统中的无线公网依托蜂窝通信技术(如 4G/5G)实现远程监控与控制,支持电力数据的实时传输,具有覆盖广、移动性强等优点,但也面临信息窃听等安全威胁。随着量子计算的发展,传统加密技术的风险日益凸显。量子密钥分发(quantum key distribution, QKD)[1−2]基于量子不可克隆和量子纠缠原理,可提供无条件安全的密钥分发,有效应对未来量子攻击。自 BB84 协议提出以来,QKD 已发展出包括 E91、BBM92、B92 等多种协议[3−6],持续提升安全通信的可行性和多样性。将 QKD 与无线公网业务相结合,能够为电力系统这类关键基础设施构建强安全屏障,保障敏感数据的传输机密性与完整性,具有显著的必要性和紧迫性。

QKD 的理论安全性与实际安全性在实际应用中还存在一些差距,因为实际器件的不理想,对 QKD 系统会引入额外的安全性漏洞。QKD 发展中有十分重要的补偿器件漏洞的协议,测量设备无关协议(measurement device independent QKD, MDI−QKD)可以抵御所有来自探测器端的测信道攻击[7],但其无法突破 PLOB(pirandola−laurenza−ottaviani−bianchi)界;双场协议(twin−field QKD, TF−QKD)可以突破 PLOB 界,由于缺乏全局相位参考导致不稳定的光学干涉,TF 协议的实施挑战性很大;2023 年模式匹配协议(mode pairing QKD, MP−QKD)[8]的提出既可以免疫探测端受到的攻击,又可以突破 PLOB 界,并且相较于 TF−QKD,降低了协议的复杂度,是迄今性能最佳的 QKD 协议。因此本文将该协议应用于无线公网电力系统,并进行了模拟仿真,为 QKD 应用提供成功范例和技术支撑。

1. 南京南瑞信息通信科技有限公司,南京 211106
2. 国网电力科学研究院有限公司,南京 211106
3. 国网安徽省电力有限公司电力科学研究院,合肥 230601
4. 国网安徽省电力有限公司,合肥 230009
5. 北京邮电大学理学院,北京 100876

收稿日期: 2024−04−13; 修回日期: 2025−09−21
基金项目: 国家电网总部科技项目(5700−202319840A−4−3−WL)
作者简介: 卞宇翔, 工程师, 研究方向为电力系统通信, 电子信箱: bianyuxiang@sgepri.sgcc.com.cn; 马海强(通信作者), 教授, 研究方向为量子通信与信息安全, 电子信箱: hqma@bupt.edu.cn
引用格式: 卞宇翔, 李圆智, 吕超, 等. 模式匹配量子密钥分发在无线公网电力业务中的应用[J]. 科技导报, 2025, 43(21): 81−86;
doi:10.3981/j.issn.1000-7857.2024.04.00325

1 模式匹配协议在无线公网电力业务中的应用策略

无线公网电力业务在中国应用十分广泛,中国部分地区的电力业务使用 4G 和 5G 的无线公网进行信息传输,由于该通信需要将大量且分散的用电交互终端(如居民楼、商场大厦等)与主站相连并传输信息,信息量大且分散,在信息传输过程中,可能出现攻击者伪造、仿冒、控制智能用电交互终端非法接入主站,导致主站被非法控制、数据被窃取,或者是恶意窃听者通过获取用户每天的用电量等隐私信息,进而分析用户的用电习惯,导致用户的隐私泄露;若某个地区的大量用电终端的信息被泄露进而被更改,则该地对当前总负荷量和电力需求的计算将会出现差错,天气对无线接入网通信质量影响的指标也会产生一些影响,从而产生重大的交互错误,导致该地区用电不平衡,因此,无线公网通信的加密对整个用电系统至关重要。

当前无线公网电力系统所使用的加密手段大多为传统加密技术,传统加密手段主要依靠在数学计算方面增加复杂度,使其更难被破解,但随着量子计算的兴起,使用量子算法可以在很短时间内解决传统计算机需要计算很久的问题,因此传统加密技术的安全性受到了挑战。量子密钥分发主要依靠量子力学的无条件安全性,在对抗未来计算技术的威胁上,QKD 作为一种量子安全通信的手段,提供了更高级别的保护,因此将 QKD 应用到无线公网中是十分必要的。

MP−QKD 是目前为止 QKD 众多协议中性能最佳的一个协议,具有同 MDI−QKD[9]一样免疫探测器端的测信道攻击的优势,以及 TF−QKD[10]在无量子中继时突破 PLOB 界的性能,模式匹配协议的密钥信息被编码在相对相位或强度中,其稳定性仅取决于局部相位参考和光路的条件,实验实现、数据采集控制与 MDI−QKD 和 TF−QKD 有很多相似之处,而 MDI−QKD 和 TF−QKD 这 2 种方案已在实验室和现场中广泛实施。值得注意的是,为适应不同的硬件条件,可以在数据后处理期间,通过调整脉冲间隔参数在 1 种模式和 2 种模式方案之间自由调整模式配对方案,以优化系统性能。将该协议应用于无线公网电力系统是一个最好的选择,基于该技术可实现变电站与主站之间的点到点、点到多点拓扑组网,全面提升电力调度业务的数据通信安全性,实现 MP−QKD 的组网。配电业务关系到整个配电网运行状态的监视和控制,配电终端多,应用范围广,其通信安全性也有待进一步加强。面对海量的配电终端,可使用量子 Ukey、量子 TF 卡来构建量子密钥无线分发系统,实现配电移动终端的量子安全加密,提高配电业务的安全性和保密强度。

MP−QKD 模型具体实现步骤如下。

1)准备阶段。

在第 i 轮(i=1, 2,⋯, N),Alice 在光学模式 A_i 中制备相干态 $\sqrt{\mu_i^a}\mathrm{e}^{\mathrm{i}\phi_i^b}$,光强范围为 $\{0,\mu\}$,相位范围为 $[0,2\pi)$,Bob 也同理。

2)测量阶段。

Alice 和 Bob 将模式 A_i 和 B_i 发送给 Charlie,Charlie 进行单光子干涉测量。Charlie 向 Alice 和 Bob 公布探测器 L 和 R 的响应情况。Alice 和 Bob 重复上述 2 个步骤 N 轮,之后对数据进行如下后处理。

3)模式配对。

对于所有成功检测到的回合,若其中 2 个检测器中的 1 个且只有 1 个响应,Alice 和 Bob 应用将 2 个响应的回合分组为 1 对的策略。这 2 轮的编码相位和强度形成 1 个数据对。

4)基的筛选。

基于 2 个轮次 i 与 j 的强度,Alice 与 Bob 对其进行定义:若强度为 $(0,\mu)$ 或者 $(\mu,0)$,则这一组被称为 Z 基;若强度为 (μ,μ),则称为 X 基;若为 $(0,0)$,则为 0。Alice 和 Bob 宣布每对数据的基;如果它们都宣布了基 X 或基 Z,它们就维持数据对,否则,数据对就被丢弃。

5)密钥选择。

对于匹配为 Z 基的轮次 i 与 j,若强度满足 $\left(\mu_i^a,\mu_j^a\right)=(0,\mu)$,Alice 将她的密钥设置为 $\kappa^{\mathrm{a}}=0$;若满足 $\left(\mu_i^a,\mu_j^a\right)=(\mu,0)$,则 $\kappa^{\mathrm{a}}=1$。对于匹配为 X 基的轮次,密钥在相对相位 $\left(\phi_j^a-\phi_i^a\right)=\theta^a+\pi\kappa^{\mathrm{a}}$ 中选取:初始密钥为 $\kappa^a=\left\{\left[\left(\phi_j^a-\phi_i^a\right)/\pi \bmod 2\right]\right\}$,对准角度为:$\theta^a=\left(\phi_j^a-\phi_i^a\right) \bmod \pi$。Bob 以同样的方法得到他的初始密钥与角度。对于 Z 基翻转的不同之处在于,若 Bob 的强度为 $\left(\mu_i^{\mathrm{b}},\mu_j^{\mathrm{b}}\right)=(\mu,0)$ 时,编码为 $\kappa^{\mathrm{b}}=0$;若为

$\left(\mu_i^{\mathrm{b}},\mu_j^{\mathrm{b}}\right)=(0,\mu)$，则$\kappa^{\mathrm{b}}=1$。作为$X$基的额外步骤，如果 Charlie 的探测结果是(L, L)或(R, R)，Bob 保持κ^{b}；若为(L, R)或(R, L)，Bob 翻转κ^{b}。对于X基，Alice 和 Bob 宣布对齐角度θ^{a}与θ^{b}，如果$\theta^{\mathrm{a}}=\theta^{\mathrm{b}}$，则保留数据对；否则，数据对将被丢弃。

6) 参数估计。

Alice 和 Bob 估计响应信号的比例$q(1,1)$，以及 Alice 和 Bob 在位置i和j都发射了 1 个光子，使用Z基对和X基对的数据。相应的Z基相位误码率为e_{11}^{Z}以及Z基对的量子比特误码率为$E^{(\mu,\mu),Z}$。

模式匹配原理如图 1 所示，Alice 和 Bob 首先制备具有随机强度与随机相位的相干脉冲，随机强度选自$\{0,\mu\}$，随机相位$\varphi_i^{\mathrm{a(b)}}\in[0,2\pi)$，并将其发送给 Charlie。在干涉测量之后，Charlie 宣布探测结果，基于该探测结果 Alice 和 Bob 对脉冲进行配对并确定它们的编码基。对于X基，他们宣布对准角θ^{a}与θ^{b}，保留$\theta^{\mathrm{a}}=\theta^{\mathrm{b}}$的数据，使用$Z$基对来生成密钥和其他用于参数估计的数据。

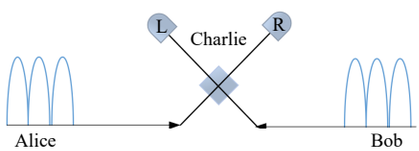

图 1 模式匹配协议原理

无线公网电力业务在电力网络中面临一些安全性风险，由于无线公网电力业务通过 4G 和 5G 来传输信息，而传输信息的终端分布在各个地区，十分地分散，需要对大量且分散的智能用电交互终端通过无线公网向主站传输数据的过程进行防护。在各个用电交互终端接入主站之前，对主站发出接入请求，在该过程中可能有攻击者伪造、仿冒或控制智能用电交互终端非法接入主站，导致主站被非法控制、数据被窃取，对无线公网电力业务进行安全保护的首要目的是为了保证用电交互端的隐私信息安全，防止用户的一些重要信息被泄露。因此，在无线公网通信链路中布署 MP-QKD 能有效保证信息安全，具体实施策略如图 2 所示。

图 2 中一级主站(上级调度中心)下辖二级子站(下级调度中心)和一个直属发电厂与变电站。所有站间实现包括量子和经典 2 条分线路以实现 MP-QKD 协议要求的量子态传输与测量结果，站间直线为经典信道以完成协议要求的信息传输过程，站间虚线为量子信道。图 2 中站间距离以实际线路为准。当存在多个链路时，如果量子密钥不足则系统默认自动切换到其他中继节点进行密钥传输。Alice 和 Bob 先共享密钥，然后将密钥发送给主站，主站将信息加密后完成站间通信。各级发电站相当于位于中继节点的 Charlie，负责对传送的密钥进行探测并公布探测结果，之后 2 个主站对探测结果进行密钥提取以及后处理。该方案实现了在电信系统的无线公网中融合量子保密通信技术以应用于电力系统的输电、变电、配电、调控等，还可以将该方案与软件定义一切(software defined everything, SDX)结合[11]，实现基于 SDX 的资源调度。

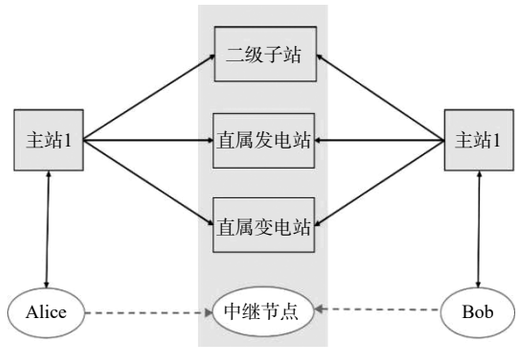

图 2 模式匹配协议在无线公网电力业务中的实施策略

2 无线公网电力业务与量子密钥分发融合

将 MP-QKD 与无线公网电力系统结合的首要问题是复杂的通信损耗，我们主要考虑了无线公网电磁环境下对于信道所产生的影响[12-14]，由于电磁波在自由空间中的传输损耗与其工作频率和传输距离密切相关，并且在实际无线环境中还存在反射、绕射、散射和波导传播等多种机制，这些因素共同导致其传播特性远较自由空间复杂，从而显著增加 QKD 链路的传输损耗。为量化该影响，结合具体环境因素与 QKD 的系统参数，推导出信道损耗的经验公式。考虑具体因素并结合 QKD 的具体参量，得到信道损耗为

$$\eta=m+n\lg d \tag{1}$$

式中，$m=n+k_1\lg d_{\mathrm{a}}$，$n=k_2+\lg d_{\mathrm{b}}$，$d=d_a+d_b$，$d$为 Alice 与 Bob 端的距离，$d_{\mathrm{a}}$与$d_{\mathrm{b}}$分别为 Alice 与 Bob 到

中继节点 Charlie 的距离，k_1与k_2为电磁信号修正因子[12]。

MP−QKD 的密钥率为[8]

$$R = r_p r_s \{ q_{(1,1)} [1 - H(E^X_{(1,1)})] - fH(E^{(\mu,\mu),Z}) \} \quad (2)$$

式中，r_p为在每轮中的配对期望，r_s为每轮响应中脉冲为单光子对的概率，$E^X_{(1,1)}$为单光子对误码率，$E^{(\mu,\mu),Z}$为总误码率(QBER)，$q_{(1,\ 1)}$为单光子信号对的期望配对率，其中[8]

$$r_p = \left\{ \frac{1}{p[1-(1-p)^l]} + \frac{1}{p} \right\}^{-1} \quad (3)$$

式中，p为第 i 轮被成功检测到的概率，每轮响应中脉冲为单光子对的概率r_s为[8]：

$$\begin{aligned} r_s &= \frac{1}{16}\frac{1}{p^2} \sum_{\xi^k \oplus \xi^l = 11} \Pr\left(C^k = 1 \middle| \xi^k\right) \Pr\left(C^l = 1 \middle| \xi^l\right) \\ &= \frac{1}{8}\frac{1}{p^2}[1-(1-2pd)\exp(-\eta_s \mu)]^2 \end{aligned} \quad (4)$$

误码率的表达式为

$$\begin{aligned} E^{(\mu,\mu),Z} &= \frac{1}{16}\frac{1}{r_s p^2} \sum_{[\xi^k,\xi^l] \in \varepsilon} \Pr\left(C^k = 1 \middle| \xi^k\right) \Pr\left(C^l = 1 \middle| \xi^l\right) \\ &= \frac{1}{4}\frac{1}{r_s p^2} pd[1-(1-2pd)\exp(-2\eta_s \mu)] \end{aligned} \quad (5)$$

单光子信号对的期望配对率q_{11}为

$$\begin{aligned} q_{11} &= \frac{1}{16}\frac{1}{r_s p^2} \sum_{\xi^k \oplus \xi^l = 11} \Pr\left(C|S,\xi^k,\xi^l\right) \Pr\left(S|\xi^k,\xi^l\right) \\ &= \frac{1}{16}\frac{P_\mu(1)^2}{r_s p^2} \sum_{\xi^k \oplus \xi^l = 11} \Pr\left(C^k = 1 | n^k = \xi^k\right) \cdot \\ &\quad \Pr\left(C^l = 1 | n^k = \xi^l\right) \\ &= \frac{1}{8}\frac{P_\mu(1)^2}{r_s p^2}[1-(1-2pd)(1-\eta_s)] \end{aligned} \quad (6)$$

式中，协议采用弱相干脉冲作为光源[15−16]，光子数分布遵从$P_\mu(k) = \exp(-\mu)\frac{\mu^k}{k!}$[17]，单光子探测概率以及单光子误码率采用传统 MDI[18−20]协议的探测概率与误码率。

由于密钥率与传输距离是衡量 QKD 性能的重要指标，通过式(4)~式(6)并结合 MP−QKD 无线公网电力业务的特性，仿真了不同配对间隔数 N 时，密钥率随传输距离的变化关系；在无线公网电力系统中 MP−QKD 的密钥率−距离图像，以及与其在理想状态下的对比。图 3 采用不同配对间隔数 N 时 MP−QKD 的密钥率随传输距离的变化关系，该参数直接决定了协议后处理中信号脉冲的配对策略和效率，是影响最终密钥生成性能的核心因素，不同颜色曲线为 MP−QKD 中不同的配对间隔数l。从图 3 中可以看出，当l>10^4 以上时，密钥率可以超越 PLOB 界，当l<10^4 以下时无优越性，l决定了协议的性能，特别是当$l=1$时，MP−QKD 等效为传统的双模 MDI−QKD，因此无法超越 PLOB 界，在l逐渐增大的过程中，$R \sim \sqrt{\eta}$的性质逐渐明显，这一对比也验证了该协议通过后处理优化可实现远超传统无中继 QKD 协议的传输极限。

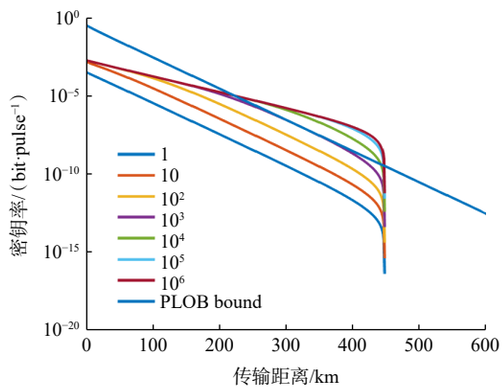

图 3 无线公网电力业务下的 MP−QKD

为评估无线公网电力业务下电磁环境对 MP−QKD 的影响，仿真了理想情况下与电磁干扰情况下的 MP−QKD 的密钥率−距离图像，图 4 为在 MP−QKD 中的配对间隔 10^6 时，理想情况下 MP−QKD 与无线公网电力业务下的 MP−QKD 的对比，仿真结果显示，电磁环境引入的噪声干扰等因素会引入额外损耗，导致最远传输距离较理想情况下降约 40 km。尽管如此，系统仍能保持超过 400 km 的有效传输距离，

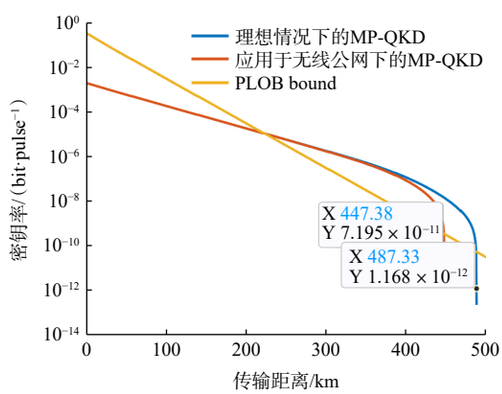

图 4 理想状况下与实际情况下的 MP−QKD 对比

且密钥率在远距离下依旧高于 PLOB 界。这一结果说明,尽管无线公网环境对 QKD 性能存在可见影响,但 MP-QKD 展现出较强的鲁棒性和实用性,足以满足大多数电力广域通信场景的安全传输需求。

图 5 为将 MP-QKD 应用于无线公网电力系统时,系统的误码率随距离的变化图像,可以看出随着距离的增加,误码率也有数量级的变化,在 400 km 范围内,QBER 仍保持在 10^{-3} 量级,处于可接受阈值以内,表明 MP-QKD 在实际无线公网环境下仍具备较好的可靠性。该结果与图 4 的密钥率-距离图像共同说明 MP-QKD 协议在数据后处理阶段能有效处理一定程度的误码,验证了 MP-QKD 在电力无线公网环境中的鲁棒性。

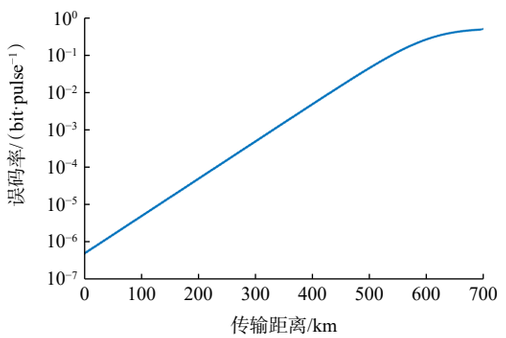

图 5 模式匹配协议误码率图像

3 结论

研究了 MP-QKD 在无线公网电力业务中的应用可行性与实际性能。理论分析与仿真结果表明,MP-QKD 不仅具备测量设备无关的安全性,还能突破无中继量子密钥分发的 PLOB 界,显著提升安全传输距离。在配对间隔数大于 10^4 时系统表现优异,传输距离超过 400 km,误码率保持在较低水平,虽在复杂电磁环境下通信距离较理想情况缩短约 40 km,但仍处于工程可接受范围。

该协议为电力无线公网业务提供了可对抗量子计算攻击的安全通信新路径:在输电环节,MP-QKD 可用于跨区域主干通信网及调度中心之间的敏感指令传输,保障广域电网的实时控制安全;在配电物联网中,可面向智能开关、故障指示器及分布式能源终端的海量接入,提供轻量级量子安全认证与密钥分发机制。此外,MP-QKD 也有望与后量子密码(PQC)融合,构建多层次量子安全防护体系,或结合电力系统新型业务,应用在基于 SDX 的量子密钥分发体系,实现基于无线公网的 SDX 下的资源调度。

参考文献(References)

[1] Bennett C H, Brassard G. Proceedings of the IEEE international conference on computers, systems and signal processing[M]. New York: IEEE, 1984.

[2] Bennett C H, Brassard G. Quantum cryptography: Public key distribution and coin tossing[C]//Proceedings of the IEEE International Conference on Computers, Systems, and Signal Processing, Bangalore, 1984: 175-179.

[3] 彭志刚. 无线公网通信技术在配电自动化系统中的应用[J]. 中小企业管理与科技, 2012, 10(10): 306-307.

[4] 牛佳宁, 赵子岩, 李国春, 等. 新型电力系统配网运行场景下的量子密码技术应用体系架构[J]. 电力信息与通信技术, 2022, 20(11): 65-73.

[5] 刘燕龙, 范群韬. 面向配用电网的无线公网安全检测的研究[J]. 电力系统, 2018, 27(15): 12-16.

[6] 郭弘, 李政宇, 彭翔. 量子密码[M]. 北京: 国防工业出版社, 2016.

[7] 冯晓宁, 吴洪宇. 对称密码体制的量子攻击[J]. 应用科学学报, 2024, 42(1): 39-52.

[8] Zeng P, Zhou H Y, Wu W J, et al. Mode-pairing quantum key distribution[J]. Nature Communications, 2022, 13: 3903.

[9] Ma X F, Razavi M. Alternative schemes for measurement-device-independent quantum key distribution[J]. Physical Review A, 2012, 86(6): 062319.

[10] Lucamarini M, Yuan Z L, Dynes J F, et al. Overcoming the rate-distance limit of quantum key distribution without quantum repeaters[J]. Nature, 2018, 557(7705): 400-403.

[11] 侯杰, 王云升, 王勇, 等. 基于SDN和遗传算法优化的干线数字双链路动态资源调度[J]. 电声技术, 2025, 49(1): 5-8.

[12] 周宇英, 代合鹏, 彭龙军. 电磁环境评估中传播模型的对比分析与修正方法研究[J]. 宇航计测技术, 2009, 29(3): 63-65.

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

[14] Bennett C H, Brassard G, Mermin N D. Quantum cryptography without Bell' s theorem[J]. Physical Review Letters, 1992, 68(5): 557-559.

[15] Bennett C H. Quantum cryptography using any two nonorthogonal states[J]. Physical Review Letters, 1992, 68(21): 3121-3124.

[16] 马永红, 伊利琛, 陈雅琳, 等. MDI-QKD协议性能优化及

电力调度量子密钥应用策略[J]. 电力系统自动化, 2019, 43(14): 182−199.
[17] Boström K, Felbinger T. Deterministic secure direct communication using entanglement[J]. Physical Review Letters, 2002, 89(18): 187902.
[18] Brassard G, Lütkenhaus N, Mor T, et al. Limitations on practical quantum cryptography[J]. Physical Review Letters, 2000, 85(6): 1330−1333.
[19] Gottesman D, Lo H K, Lütkenhaus N, et al. Security of quantum key distribution with imperfect devices[J]. Quantum Information and Computation, 2004, 4(5): 325−360.
[20] Hwang W Y. Quantum key distribution with high loss: Toward global secure communication[J]. Physical Review Letters, 2003, 91(5): 057901.

Research on the application of mode pairing quantum key distribution in wireless public network power service

BIAN Yuxiang[1,2], LI Yuanzhi[3], LÜ Chao[1,2], LI Duanchao[4], CHEN Wei[4], FENG Bao[1,2], SHI Kaiyi[5], LI Yue[5], LIU Chang[5], MA Haiqiang[5*]

1. NARI Information Communication Technology Co., Ltd., Nanjing 211106, China
2. State Grid Electric Power Research Institute Co., Ltd., Nanjing 211106, China
3. State Grid Anhui Electric Power Co., Ltd. Electric Power Science Research Institute, Hefei 230601, China
4. State Grid Anhui Electric Power Co., Ltd., Hefei 230009, China
5. School of Science, Beijing University of Posts and Telecommunications, Beijing 100876, China

Abstract Quantum key distribution (QKD) provides information−theoretic security to address security challenges faced by traditional encryption techniques and threats posed by quantum computers. This paper investigates the application of QKD in wireless public network power services, accounting for parameters such as electromagnetic interference and communication distance through modeling and simulation. Results demonstrate that the pattern matching protocol QKD exhibits excellent performance when the pairing interval exceeds 10^4, surpassing the PLOB boundary while still achieving transmission distances exceeding 400 km. This ensures the security of communication links and provides theoretical support for the application of pattern matching protocol QKD in wireless public network power services.

Keywords wireless public network; quantum communication; quantum key distribution; electricity business; mode pairing

（责任编辑 傅雪）