研究论文

高维双场量子密钥分发提升电力系统安全性

韩嘉佳[1],汤亿则[1],戴桦[1],徐思聪[2],吕玉祥[2],马海强[3*]

摘要 采用偏振和纵向动量耦合对单光子进行高维量子编码,使光子能够携带 2 比特信息且仅受到单边信道衰减。仿真结果表明,与传统 2 维协议相比,该协议的安全码率提升近 1 个数量级,并且能够突破无中继密钥率传输距离的限制,同时量子比特误码率仅为 0.04。该解决方案显著提高了无线公网电力系统的安全性,为可靠的电力传输和数据通信提供了新的选择。

关键词 双场;量子保密通信;量子密钥分发;无线公网电力系统

随着信息技术的迅猛发展及电力系统的智能化进程,无线公网电力业务因具有覆盖范围广泛和无线通信的特性被广泛应用。然而该系统面临来自恶意攻击者的安全威胁,传统的加密方法在面对日益复杂的安全威胁时可能存在漏洞,寻求更高级别的安全保障机制势在必行。近年来,量子保密通信作为一种革命性的安全通信技术,引起了广泛的关注和研究。

量子保密通信是利用量子力学的基本原理,如海森堡不确定性原理、不可克隆定理和测量塌缩理论等实现信息的绝对保密性[1]。在无线公网电力业务中,引入量子保密通信技术可以有效应对传统加密方法所面临的挑战,提供更高级别的通信保密性和安全性。量子密钥分发(quantum key distribution, QKD)是基于量子力学的安全通信技术,旨在实现高度安全的密钥交换。自 1984 年 BB84 协议提出以来,QKD 经历了不断改进和发展[2−5]。近年来在理论和实验中均取得了重要的突破,一些国际机构和企业已经展示了在城市范围内的长距离 QKD 通信,甚至还出现了一些商业化的 QKD 系统,为各行各业提供了更安全的通信解决方案[6−8]。

传统的 QKD 协议通常使用 2 维量子态(如光子的偏振)来编码和传输密钥,如 BB84 量子密钥分发协议(BB84 quantum key distribution, BB84−QKD)[9]、测量设备无关量子密钥分发协议(measurement−device−independent quantum key distribution, MDI−QKD)[4]、双场量子密钥分发协议(twin−field quantum key distribution, TF−QKD)[10−13]等。随着不同协议的提出,量子通信取得了较大的进展。2021 年,Pittaluga 等[14]突破了无中继的传输距离记录,达到了 600 km。2022 年,Park 等[15]实现了 TF−QKD 网络方案,该方案利用“即插即用”的结构和 Sagnac 环实现了经济高效的配置,并在 50 km 的光纤上进行了实验,平均密钥率为 1.31×10^{-4} 比特每脉冲。同年,中国科学技术大学韩正甫院士团队通过实验,实现了 830 km 光纤的 TF−QKD[16]。

近年来,研究人员提出了高维量子密钥分发(high−dimensional quantum key distribution, HD−QKD)的概念,利用更高维度的量子态(如光子的轨道角动量、时间、频率等)来编码和传输密钥信息[17−20]。通过使用更多的自由度,HD−QKD 可以携带更多的信息

1. 国网浙江省电力有限公司电力科学研究院,北京 310014
2. 安徽继远软件有限公司,合肥 230000
3. 北京邮电大学理学院,北京 100876

收稿日期:2024−03−23;修回日期:2024−10−16
基金项目:国家电网创新基金项目(B311DS230009)
作者简介:韩嘉佳,高级工程师,研究方向为信息安全,电子信箱:36155384@qq.com;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:韩嘉佳, 汤亿则, 戴桦, 等. 高维双场量子密钥分发提升电力系统安全性[J]. 科技导报, 2025, 43(16): 120−127; doi:10.3981/j.issn.1000-7857.2024.04.00324

量,提高了密钥传输速率和系统的安全性。而 TF-QKD 是利用单光子干涉后的探测作为有效探测事件的测量设备无关量子密钥分发,仅需单个探测器响应,接收方每次产生用来成码的有效探测仅消耗 1 个光子,是传统测量设备无关量子密钥分发探测消耗的双光子的 50%,且该光子仅经历单边信道,衰减是信道总衰减的平方根,安全成码率提升至随信道衰减的平方根下降,其密钥率可以突破无中继密钥率传输距离(pirandola-laurenza-ottaviani-banchi, PLOB)界限[21]。

将 HD-QKD 与 TF-QKD 融合,提出一种新的高维双场量子密钥分发(high-dimensional twin-field quantum key distribution, HD-TF-QKD)协议,兼具高维 QKD 和双场 QKD 的优势,旨在提升 QKD 传输过程中的信息容量和通信安全密钥率,降低误码率。在无线公网电力系统中,通常存在各种噪声和干扰源,如电磁干扰和光学噪声。利用高维度的量子态可以提高通信系统对噪声和干扰的抗性。由于高维度的量子态具有更大的容量,可以通过纠错编码和信道调整的方式来增加系统的容错性,提高通信的可靠性。此外,电力系统通常涉及多个用户和多个通信节点之间的通信需求。采用高维度的量子态可以支持多用户之间的并行通信,提高系统的通信效率和带宽利用率。

1 无线公网电力系统与量子密钥分发

无线公网在电力系统中的应用范围广泛,如智能电网、远程监控、故障诊断等[22]。在无线公网电力系统中,数据安全和隐私保护至关重要,量子密钥分发可以提供更高级别的安全性。量子比特(如光子)的不可伪造性和量子态的特性使 QKD 可以确保在通信双方之间分发的密钥是无条件安全的,可防止未经授权的访问和数据泄露,保护电力数据的机密性[23-25]。在实际应用中,需考虑电力系统的通信需求,确定适当的量子密钥分发速率和密钥长度,以满足实时通信的要求。除了提供量子密钥的保密性,还需要考虑网络的完整性和可用性,采用适当的安全机制和协议,以防止攻击和故障。高维量子密钥分发协议可以提供更高的安全性,抵抗更多种类的攻击,例如基于量子计算的攻击和侧信道攻击。电力系统通常涉及多个用户和多个通信节点,高维 QKD 协议可以支持并行密钥分发,提高系统的通信效率。此外,高维度的量子密钥可以提供更高的容量,适应电力系统中大规模数据传输的需求,提高通信的带宽和效率[26]。

结合电力量子保密通信,将业务系统与业务应用接入现有的电力系统[27-31]。如图 1 所示,卫星通过自由空间信道与 2 个地面 QKD 终端进行通信,这些终端负责生成和分发量子密钥。每个 QKD 终端通过量子 VPN(virtual private network, VPN)设备连接到量子密钥分发管理终端,该终端通过光纤信道与量子 VPN 设备相连,确保量子密钥的安全传输。量子密钥分发管理终端进一步通过经典信道与加密信息分发中心相连,该中心负责将加密后的信息分发给用户。用户终端通过无线公网电力业务终端连接到加密信息分发中心,接收并解密加密信息以获取原始数据。整个系统通过量子密钥提供高级别的安全性,确保数据在传输过程中的保密性和完整性。

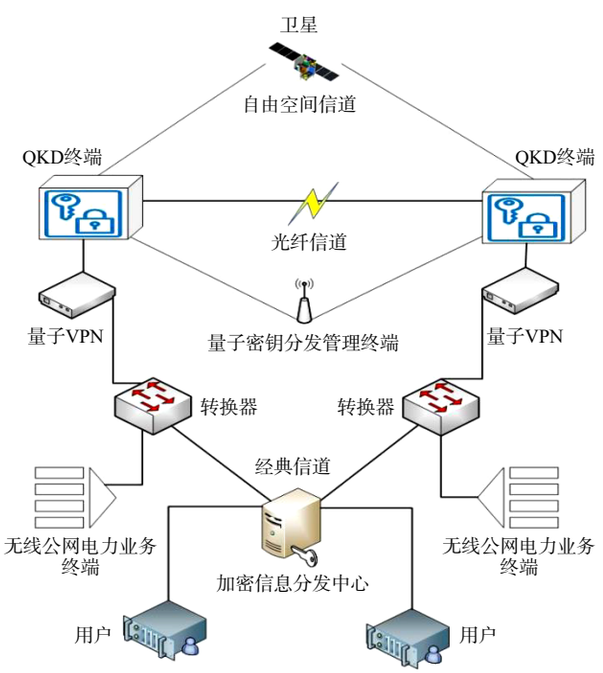

图 1 现有电力系统接入量子保密通信业务

2 高维双场量子密钥分发协议

2.1 HD-TF-QKD 协议介绍

首先,构造多自由度耦合实现 HD-QKD 方案。如图 2 所示,基于N维自由度耦合,建立一个d^2维希尔伯特空间,发送端多自由度的信息在 1 条路径上耦

合,探测端仅需配置 2 个单光子探测器。图 2 中小球表示 Alice 和 Bob 制备量子态的不同自由度,圆柱表示多自由度耦合在一条路径中,D_1、D_2表示位于 Charlie 端的探测器,接收端探测器的数量与维度数N无关。通过不同自由度分离(如状态映射、响应延迟等)进行高维贝尔态的测量。例如,基于时间编码使用不同时隙的 HD−QKD 方案。

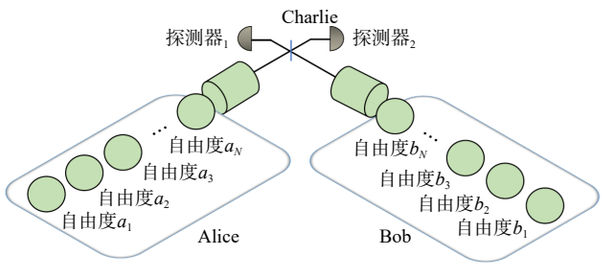

图 2 多自由度编码图

假设 Alice 和 Bob 所选用的d个二维自由度的正交基矢分别为$\boldsymbol{x}_1/\boldsymbol{y}_1,\boldsymbol{x}_2/\boldsymbol{y}_2...\boldsymbol{x}_d/\boldsymbol{y}_d$,则构建的$d^2$维正交基矢可以表示为$|p_1q_2...k_d\rangle\,(p,q,k\in\{x,y\})$,则高维量子态可以表示为$|\psi\rangle=\sum_{k=1}^{d}c_k\,|p_1q_2...k_d\rangle$,其中$c_k$是复数系数,满足归一化条件:$\sum_{k=1}^{d}|c_k|^2=1$。

在该协议中,通过耦合偏振和纵向动量构建了一个 4 维希尔伯特空间来研究 HD−TF−QKD。在每个自由度下,Alice 和 Bob 均使用 2 组基底,水平垂直基和对角基。在偏振自由度中,水平垂直基为$\{|\boldsymbol{H}\rangle,|\boldsymbol{V}\rangle\}$,其中$|\boldsymbol{H}\rangle$和$|\boldsymbol{V}\rangle$分别表示水平偏振和垂直偏振;对角基为$|+\rangle_{\mathrm{p}}=\frac{1}{\sqrt{2}}(|\boldsymbol{H}\rangle+|\boldsymbol{V}\rangle)$,$|-\rangle_{\mathrm{p}}=\frac{1}{\sqrt{2}}(|\boldsymbol{H}\rangle-|\boldsymbol{V}\rangle)$。在纵向动量自由度中,水平垂直基为$\{|\boldsymbol{L}\rangle,|\boldsymbol{R}\rangle\}$,其中,$|\boldsymbol{L}\rangle$和$|\boldsymbol{R}\rangle$分别表示向左和向右的空间模式;对角基为$|+\rangle_{\mathrm{f}}=\frac{1}{\sqrt{2}}(|\boldsymbol{L}\rangle+|\boldsymbol{R}\rangle)$,$|-\rangle_{\mathrm{f}}=\frac{1}{\sqrt{2}}(|\boldsymbol{L}\rangle-|\boldsymbol{R}\rangle)$在以上 2 种自由度编码中$|\boldsymbol{H}\rangle,|+\rangle_{\mathrm{p}},|\boldsymbol{L}\rangle,|+\rangle_{\mathrm{f}}$表示编码为 0,而$|\boldsymbol{V}\rangle,|-\rangle_{\mathrm{p}},|\boldsymbol{R}\rangle,|-\rangle_{\mathrm{f}}$表示编码为 1。

如图 3 所示,Alice(Bob)从激光器发射脉冲光,并使用强度调制器随机调制成不同强度的光脉冲,用于设置信号态、诱骗态和真空态。发送光子的偏振态和纵向动量自由度分别由电偏振控制器和哈达玛门来调控。耦合器将不同自由度的信息耦合到光子中后,被分束器以相等的概率分成 2 条路径,由另一个分束器进行调制和输出。量子态被发送给 Charlie 进行完整的超纠缠贝尔态分析(HBSA),HBSA 可以独立地进行偏振贝尔态分析和空间贝尔态分析,第 1 步用于空间贝尔态分析,第 2 步用于偏振贝尔态分析,在贝尔态分析过程中需要利用量子不破坏探测器(QNDs),该仪器既可以将空间模式中的 4 种贝尔态划分为 2 组,又可以区分相位为 0 的贝尔态和相位为π的贝尔态,因此,可以完全区分每个自由度中的 4 个贝尔态[27−31]。Charlie 基于 Hong−Ou−Mandel(HOM)效应在分束器处进行双光子干涉。然后利用光栅将携带纵向动量的光子模式转换分离形成空间分离的高斯基模,上下两路光子经折反镜后汇聚于偏振分束器来确定偏振信息,最后连接到单光子探测器。

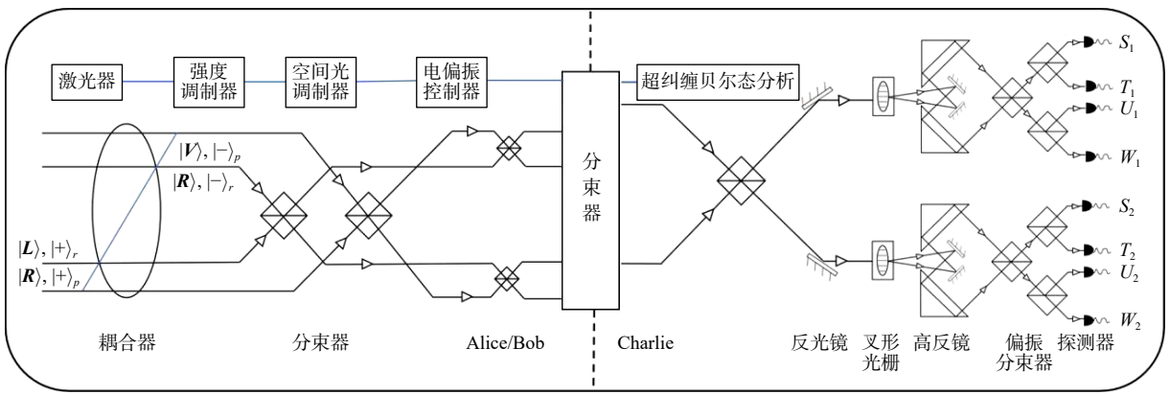

图 3 偏振和纵向动量耦合的 HD−TF−QKD 协议图

基于偏振和纵向动量自由度耦合的 HD−TF−QKD 协议流程如下。

1)初始操作。将相位间隔$[0,2\pi)$分成$M=16$等份,$\Delta k=\frac{2\pi k}{M}$,其中$k=(0,1,...,M-1)$。

2)相位校准。用户首先发送未调制的明亮光脉

冲来校准相位偏移$\delta_{ba}=\delta_b-\delta_a$(角标 a 表示 Alice, b 表示 Bob),随后将光脉冲衰减到单光子级别并对其强度和相位进行调制。

3)量子态制备。首先 Alice 和 Bob 选择强度$\mu_{a,b}\hat{I}\{u/2,v/2,\omega/2\}$的随机值;并选择比特相位$\alpha_{a,b}\hat{I}\{0,2\pi\}$,基相位$\beta_{a,b}\hat{I}\{0,\pi/2\}$,随机相位$\rho_{\alpha,\beta}\in[0,2\pi)$;这些相位值决定了 Alice 和 Bob 的相位所归属的相位片。随后单光子先在电偏振控制器(EPC)实现偏振自由度$\{|\boldsymbol{H}\rangle,|\boldsymbol{V}\rangle\}$编码,再通过分束器(BS)在纵向动量自由度中充当哈达玛门,实现纵向动量自由度$\{|\boldsymbol{L}\rangle,|\boldsymbol{R}\rangle\}$编码。以$\boldsymbol{Z}$基为例,经过多次哈达玛门转换后,光子态最终转换为:$|\boldsymbol{H}\rangle\otimes|\boldsymbol{V}\rangle$,$|\boldsymbol{H}\rangle\otimes|\boldsymbol{R}\rangle$,$|\boldsymbol{V}\rangle\otimes|\boldsymbol{L}\rangle$或$|\boldsymbol{V}\rangle\otimes|\boldsymbol{R}\rangle$。编码后,Alice 和 Bob 制备出具有偏振自由度和动量自由度的相干态脉冲,随后分别通过量子通道将量子比特发送给第三方 Charlie。

4)量子态测量。Charlie 接收到 Alice 和 Bob 发送的光子量子比特后,对光子对进行超纠缠贝尔态分析(hyperentangded-Bell-state analysis, HBSA),可以完全区分每个自由度中的 4 种贝尔态,2 个自由度的贝尔态为

$$\begin{aligned}
|\phi^{\pm}\rangle_p&=\frac{1}{\sqrt{2}}(|\boldsymbol{H}\rangle_a|\boldsymbol{H}\rangle_b\pm|\boldsymbol{V}\rangle_a|\boldsymbol{V}\rangle_b),\\
|\psi^{\pm}\rangle_p&=\frac{1}{\sqrt{2}}(|\boldsymbol{H}\rangle_a|\boldsymbol{V}\rangle_b\pm|\boldsymbol{H}\rangle_a|\boldsymbol{V}\rangle_b)\\
|\phi^{\pm}\rangle_f&=\frac{1}{\sqrt{2}}(|\boldsymbol{L}\rangle_a|\boldsymbol{L}\rangle_b\pm|\boldsymbol{R}\rangle_a|\boldsymbol{R}\rangle_b),\\
|\psi^{\pm}\rangle_f&=\frac{1}{\sqrt{2}}(|\boldsymbol{L}\rangle_a|\boldsymbol{R}\rangle_b\pm|\boldsymbol{R}\rangle_a|\boldsymbol{L}\rangle_b)
\end{aligned}\tag{1}$$

式中,下标 a(b)表示 Alice(Bob)端的编码。测量结束后,Charlie 公布测量结果,所有未响应的情况均舍弃。根据超纠缠贝尔态的分析结果,$|\phi^{\pm}\rangle_p$对应同一 RM 异侧的探测器 $S_1W_1(S_2W_2)$或者 $T_1U_1(T_2U_2)$响应,$|\psi^{\pm}\rangle_p$对应同一 RM 同侧的探测器 $S_1T_1(S_2T_2)$或者 $U_1W_1(U_2W_2)$响应,$|\phi^{\pm}\rangle_f$对应不同 RM 异侧的探测器 $S_1W_2(S_2W_1)$或者 $T_1U_2(T_2U_1)$响应,$|\psi^{\pm}\rangle_f$对应不同 RM 同侧的探测器 $S_1T_2(S_2T_1)$或者 $U_1W_2(U_2W_1)$响应。(S_1 或者 S_2、T_1 或者 T_2、U_1 或者 U_2、W_1 或者 W_2 表示探测器符号)

5)后处理。Alice 和 Bob 通过信道宣布其相位片$\Delta k(a,b)$,用户丢弃所有不在同一相位片上的事件,并在此基础上宣布其选择的自由度和基,根据以下情况进行后处理。

(1)如果选择了不同的自由度或者在同一自由度中选取了不同的基,则丢弃该事件对应的编码信息。

(2)如果在 1 个自由度中选择相同的基,可在该自由度中获取彼此的编码信息。如果 2 者都在 1 个自由度中使用水平垂直基,则 Bob 需要将$|\psi^{\pm}\rangle$对应的数据进行比特翻转,如果 2 者都在 1 个自由度中使用对角基,则 Bob 需要对$|\phi^{-}\rangle$和$|\psi^{-}\rangle$对应的数据进行比特翻转。根据贝尔态测量(Bell-state measurement, BSM)结果和基选择翻转比特的具体操作如表 1 所示。

表 1 测量基选择和贝尔态测量结果

BSM结果	$\|\phi^{+}\rangle$	$\|\phi^{-}\rangle$	$\|\psi^{+}\rangle$	$\|\psi^{-}\rangle$
水平垂直基	不翻转	不翻转	翻转	翻转
对角基	不翻转	翻转	不翻转	翻转

(3)Alice 和 Bob 执行纠错和隐私放大,以完成最终安全密钥的生成。

以具体案例进行分析,假定 Alice 的编码信息是 00,Bob 的编码信息是 10。由于基的选择存在 2 种不同的情况,依次对每种情况进行详细说明。

情况 1:Alice 和 Bob 在所有自由度中基选择相同,假定 Alice 准备的态是$|\boldsymbol{H}\rangle_a|\boldsymbol{L}\rangle_a$,Bob 准备的态是$|\boldsymbol{V}\rangle_b|\boldsymbol{L}\rangle_b$。在这种情况下,发送给 Charlie 的光子的耦合态表示为

$$\begin{aligned}
&|\boldsymbol{H}\rangle_a|\boldsymbol{L}\rangle_a\otimes|\boldsymbol{V}\rangle_b|\boldsymbol{L}\rangle_b=|\boldsymbol{H}\rangle_a|\boldsymbol{V}\rangle_b\otimes|\boldsymbol{L}\rangle_a|\boldsymbol{L}\rangle_b\\
&=\frac{1}{\sqrt{2}}(|\psi^{+}\rangle_p+|\psi^{-}\rangle_p)\otimes\frac{1}{\sqrt{2}}(|\phi^{+}\rangle_f+|\phi^{-}\rangle_f)
\end{aligned}\tag{2}$$

根据测量结果和基选择,Alice 和 Bob 可以知道其在偏振自由度的编码是相反的,在纵向动量自由度的编码是相同的。这样,Bob 只需要在偏振中进行比特翻转。

情况 2:Alice 和 Bob 只在 1 个自由度中基选择相同,假定 Alice 准备的态是$|\boldsymbol{H}\rangle_a|L\rangle_a$,Bob 准备的态是$|\boldsymbol{V}\rangle_b|+\rangle_{fb}$,此时,发送给 Charlie 的光子的耦合态表示为

$$\begin{aligned}
&|\boldsymbol{H}\rangle_a|\boldsymbol{L}\rangle_a\otimes|\boldsymbol{V}\rangle_b|+\rangle_{fb}=|\boldsymbol{H}\rangle_a|\boldsymbol{V}\rangle_b\otimes|\boldsymbol{L}\rangle_a|+\rangle_{fb}\\
&=\frac{1}{\sqrt{2}}(|\psi^{+}\rangle_p+|\psi^{-}\rangle_p)\otimes\frac{1}{2}(|\phi^{+}\rangle_f+|\phi^{-}\rangle_f+|\psi^{+}\rangle_f+|\psi^{-}\rangle_f)
\end{aligned}\tag{3}$$

在这种情况下,经过 HBSA 之后,Alice 和 Bob 可

以知道其极化自由度的编码是相反的,然而,因为Bob在纵向动量自由度中的基选择与Alice不同,导致Bob有50%的概率得到错误的结果,所以Bob需要舍弃该自由度下的编码信息。

情况3:Alice和Bob在2种自由度下选择的基均不相同,例如,Alice准备的态是$|\boldsymbol{H}\rangle_{\mathrm{a}}|\boldsymbol{L}\rangle_{\mathrm{a}}$,Bob准备的态是$|-\rangle_{\mathrm{pb}}|+\rangle_{\mathrm{fb}}$。在这种情况下,其耦合态为式(4)。此时,必须舍弃全部信息。

$$\begin{aligned}&|\boldsymbol{H}\rangle_{\mathrm{a}}|\boldsymbol{L}\rangle_{\mathrm{a}}\otimes|-\rangle_{\mathrm{pb}}|+\rangle_{\mathrm{pb}}=|\boldsymbol{H}\rangle_{\mathrm{a}}|-\rangle_{\mathrm{pb}}\otimes|\boldsymbol{L}\rangle_{\mathrm{a}}|+\rangle_{\mathrm{pb}}\\&=\frac{1}{2}\left(|\phi^{+}\rangle_{\mathrm{p}}+|\phi^{-}\rangle_{\mathrm{p}}-|\psi^{+}\rangle_{\mathrm{p}}-|\psi^{-}\rangle_{\mathrm{p}}\right)\otimes\\&\frac{1}{2}\left(|\phi^{+}\rangle_{\mathrm{f}}+|\phi^{-}\rangle_{\mathrm{f}}+|\psi^{+}\rangle_{\mathrm{f}}+|\psi^{-}\rangle_{\mathrm{f}}\right)\end{aligned}\tag{4}$$

2个不同自由度中可能的贝尔态分析(Bell state analysis, BSA)结果和Bob的后选择操作如表2所示,其中,$\boldsymbol{X}$表示$|\boldsymbol{H}\rangle$或$|\boldsymbol{L}\rangle$,$\boldsymbol{Y}$表示$|\boldsymbol{V}\rangle$或$|\boldsymbol{R}\rangle$,且$|\boldsymbol{H}\rangle$与$|\boldsymbol{V}\rangle$成对出现对应于p,$|\boldsymbol{L}\rangle$与$|\boldsymbol{R}\rangle$成对出现对应于f。

表2 BSA结果和Bob的后选择操作

编码信息		贝尔态测量结果				比特翻转情况
Alice	Bob	+	−	+	−	—
$\boldsymbol{X}$	$\boldsymbol{X}$	1/2	1/2	0	0	否
$\boldsymbol{X}$	$\boldsymbol{Y}$	0	0	1/2	1/2	是
$\boldsymbol{Y}$	$\boldsymbol{X}$	0	0	1/2	1/2	是
$\boldsymbol{Y}$	$\boldsymbol{Y}$	1/2	1/2	0	0	否
$(\boldsymbol{X}+\boldsymbol{Y})/\sqrt{2}$	$(\boldsymbol{X}+\boldsymbol{Y})/\sqrt{2}$	1/2	0	1/2	0	否
$(\boldsymbol{X}+\boldsymbol{Y})/\sqrt{2}$	$(\boldsymbol{X}-\boldsymbol{Y})/\sqrt{2}$	0	1/2	0	1/2	是
$(\boldsymbol{X}-\boldsymbol{Y})/\sqrt{2}$	$(\boldsymbol{X}+\boldsymbol{Y})/\sqrt{2}$	0	1/2	0	1/2	是
$(\boldsymbol{X}-\boldsymbol{Y})/\sqrt{2}$	$(\boldsymbol{X}-\boldsymbol{Y})/\sqrt{2}$	1/2	0	1/2	0	否

2.2 HD-TF-QKD安全密钥率

根据原来的HD-QKD及TF-QKD协议的密钥率分析,可知第i自由度下单光子增益的下界为[4]

$$\begin{aligned}Q_{1_i}=&\frac{\mu_i e^{-\mu_i}\left(\mu_i^{2}Q_{\nu_i}e^{\nu_i}-\mu_i^{2}Q_{\omega_i}e^{\omega_i}\right)}{\mu_i\left(\mu_i\nu_i-\mu_i\omega_i-\nu_i^{2}+\omega_i^{2}\right)}-\\&\frac{\mu_i e^{-\mu_i}\left(\nu_i^{2}-\omega_i^{2}\right)\left(Q_{\mu_i}e^{\mu_i}-y_0\right)}{\mu_i\left(\mu_i\nu_i-\mu_i\omega_i-\nu_i^{2}+\omega_i^{2}\right)}\end{aligned}\tag{5}$$

第i自由度下误码率上界为

$$\bar{e}_{1_i}=\frac{\left(E_{\nu_i}Q_{\nu_i}e^{\nu_i}-E_{\omega_i}Q_{\omega_i}e^{\omega_i}\right)\mu_i e^{-\mu_i}}{\left(\nu_i-\omega_i\right)Q_{1_i}}\tag{6}$$

因此,得到HD-TF-QKD的安全密钥率为

$$R_i=\frac{D}{M}Q_{1_i}\left[1-h\left(\bar{e}_{1_i}\right)\right]-\frac{D}{M}F_iQ_{\mu_i}h\left(E_{\mu_i}\right)\tag{7}$$

式中,μ,ν,ω分别为信号态和诱骗态的强度;$i=\mathrm{p},\mathrm{f}$;D为量子光脉冲与经典光脉冲之间的占空比,Charlie可以使用基于Alice和Bob在经典阶段(TF-QKD协议的第2步)接收到的明亮脉冲的主动反馈程序,用来补偿相位漂移;F_i是第i自由度下的纠错效率;$Q_{x_i}\,(x=\mu,\nu,\omega)$、$E_{\mu_i}$分别为第$i$自由度下探测器的响应率和信号态所对应的量子比特误码率(quantum bit error rate, QBER)。$\mathrm{h}(x)$是高维香农熵函数,表达式为$\mathrm{h}(x)=-(1-x)\log_2(1-x)-x\log_2\frac{x}{d-1}$,其中$d$为维度。

此外,由于2个自由度中的编码是独立的,因此总安全密钥生成速率可表示为

$$\begin{aligned}R=&\frac{D}{M}\left(-F_{\mathrm{p}}Q_{\mu\mathrm{p}}h\left(E_{\mu\mathrm{p}}\right)-F_{\mathrm{f}}Q_{\mu\mathrm{f}}h\left(E_{\mu\mathrm{f}}\right)\right)+\\&\frac{D}{M}Q_{1\mathrm{p}}\left[1-h\left(\bar{e}_{1\mathrm{p}}\right)\right]+\frac{D}{M}Q_{1\mathrm{f}}\left[1-h\left(\bar{e}_{1\mathrm{f}}\right)\right]\end{aligned}\tag{8}$$

当发送1个光子,图3中的4组探测器里,每一组探测器都不响应,每一组中仅有上侧探测器响应,每一组中仅有下侧探测器响应以及每组中2个探测器均响应的概率分别为

$$\begin{aligned}&P_0^{l}=1-\eta,\\&P_U^{l}=\frac{\eta\left(1+\cos\delta_{\Delta}\right)}{2},\\&P_D^{l}=\frac{\eta\left(1-\cos\delta_{\Delta}\right)}{2},\\&P_{U,D}^{l}=0\end{aligned}\tag{9}$$

式中,η是探测效率,$\eta=10^{-\frac{\alpha l}{10}}\eta_d$,$\alpha$为光线损耗,$l$为传输距离,$\eta_d$为探测器检测效率,$\delta_{\Delta}$为全局相位差。

2.3 仿真结果

基于理论分析的基础,进行数值模拟。Alice(Bob)

发送信号态、诱骗态、真空态平均光子数为$\mu=0.4$, $v=10^{-2}$, $\omega=10^{-4}$(单位为个/每脉冲)的脉冲光。仿真参数选取:暗记数率P_d=10^{-8}个/脉冲,信道光学误差率$e=0.03$,光纤损耗因子$\alpha=0.2$ dB/km,探测器检测效率$\eta_d=0.3$,纠错效率$F=1.15$,占空比$D=0.5$。

假设在理想情况下,只增加维度而不考虑设备缺陷等因素影响,通过比较基于偏振和纵向动量自由度的 HD−TF−QKD 协议与 2 维 TF−QKD 协议。仿真结果如图 4 所示,无论是在 2 维还是更高维的情况下,HD−TF−QKD 均保留了 TF−QKD 协议的优势,安全码率均可以超越 PLOB 界限。在同一距离下,HD−TF−QKD 协议在安全码率方面表现更优,比传统 2 维情况下的密钥率提升了近 1 个数量级,而且在同一安全密钥率下 HD−TF−QKD 协议传输的距离更远。此外,将维度扩展到了 8 维,假设在 3 个自由度下编码单光子(如扩展了横向自由度),这种情况下传输距离甚至可以突破 600 km,且其安全码率比其他 2 种情况更高一些。

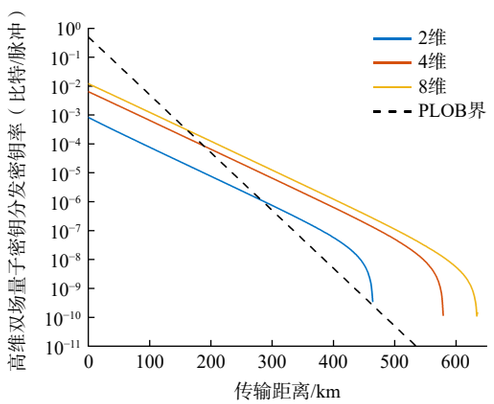

图 4 HD−TF−QKD 在不同维度上的安全密钥率

在无线公网业务中进行量子密钥分发时,信号在自由空间传输中的路径损耗、大气衰减以及无线信号在建筑物或障碍物中的衰减等会降低信号强度。此外,还需考虑无线通信中存在各种噪声和干扰源,如热噪声、射频干扰等。这些噪声和干扰会混入到信号中,使得探测器在检测过程中面临额外的噪声干扰。探测器的检测效率可能会受到这些因素的影响而发生变化。因此,针对不同探测效率情况下的 HD−TF−QKD 在不同维度下的安全码率进行仿真。如图 5 所示,不论在哪种检测效率下,HD−TF−QKD 协议的安全码率曲线始终高于传统 2 维的 TF−QKD。这是因为高维 QKD 可以在单位时间内传输更多的密钥比特。传统的 2 维 QKD 每次只能传输 1 个比特,而高维 QKD 可以同时传输多个维度的信息,从而大幅度提高了密钥传输速率。特别地,如果探测器效率为$\eta_d=0.6$时,HD−TF−QKD 协议的最远传输距离已经突破了 700 km。

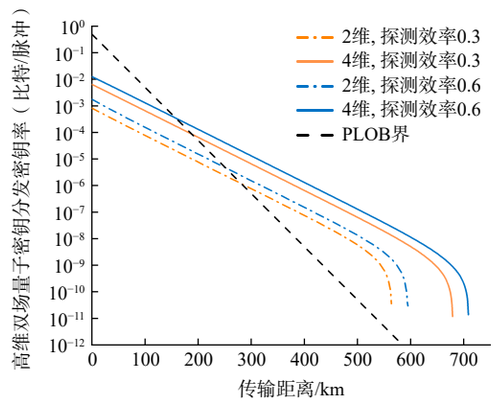

图 5 探测器不同探测效率下 HD−TF−QKD 的安全密钥率

同时,QBER 也是表征协议性能的一个重要参数。对 HD−TF−QKD 协议的 QBER 进行了仿真。如图 6 所示,在有效的通信距离范围内,协议的 QBER 值约为 0.04,远低于 QBER 的上限 0.5。这说明 HD−TF−QKD 协议在量子比特传输过程中仅有很少的比特出现错误,不仅增强了密钥的安全性,也提高了密钥的质量和传输速率。

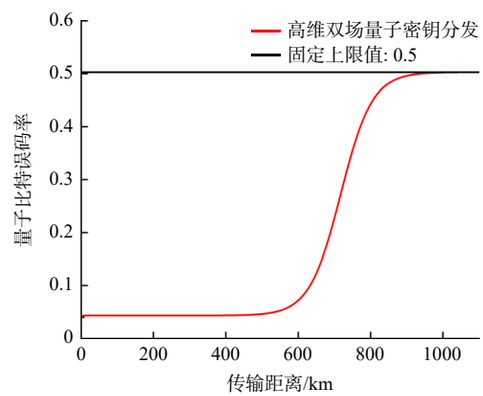

图 6 HD−TF−QKD 的量子比特误码率

3 结论

本文提出的 HD−TF−QKD 协议通过在偏振和纵

向动量 2 个自由度上对单光子进行编码,实现了单光子携带 2 比特信息,显著提升了密钥传输速率和系统安全性。该协议继承了 TF-QKD 的特性,能够突破 PLOB 界限,仿真结果表明其安全码率相比 2 维协议大幅提升,探测器效率为 60% 时最远传输距离可达 700 km,量子比特误码率仅为 0.04。在长距离、高效率量子密钥分发方面展现出巨大潜力,有望应用于金融、军事等对安全性要求极高的领域。然而,当前研究在实验稳定性和理论模型验证方面仍存在不足,未来将致力于优化高维编码的精度和稳定性,并在更多实际场景中验证协议性能。

参考文献(References)

[1] Xu F H, Ma X F, Zhang Q, et al. Secure quantum key distribution with realistic devices[J]. Reviews of Modern Physics, 2020, 92(2): 025002.

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

[3] Lo H K, Ma X F, Chen K. Decoy state quantum key distribution[J]. Physical Review Letters, 2005, 94(23): 230504.

[4] Lo H K, Curty M, Qi B. Measurement-device-independent quantum key distribution[J]. Physical Review Letters, 2012, 108(13): 130503.

[5] 马海强, 杨舜禹, 李振华. 强度波动下参考系无关量子密钥分发对比研究[J]. 量子电子学报, 2021, 38(6): 838-845.

[6] Wang S, Chen W, Yin Z Q, et al. Practical gigahertz quantum key distribution robust against channel disturbance[J]. Optics Letters, 2018, 43(9): 2030-2033.

[7] Lydersen L, Wiechers C, Wittmann C, et al. Hacking commercial quantum cryptography systems by tailored bright illumination[J]. Nature Photonics, 2010, 4(10): 686-689.

[8] 马海强, 冯宝, 赵子岩, 等. 基于波分复用技术的参考系无关量子密钥分发[J]. 量子电子学报, 2021, 38(3): 346-353.

[9] 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: IEEE, 1984: 175-179.

[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] Curty M, Azuma K, Lo H K. Simple security proof of twin-field type quantum key distribution protocol[J]. NPJ Quantum Information, 2019, 5: 64.

[12] Ma X F, Zeng P, Zhou H Y. Phase-matching quantum key distribution[J]. Physical Review X, 2018, 8(3): 031043.

[13] Yu Z W, Hu X L, Jiang C, et al. Sending-or-not-sending twin-field quantum key distribution in practice[J]. Scientific Reports, 2019, 9: 3080.

[14] Pittaluga M, Minder M, Lucamarini M, et al. 600 km repeater-like quantum communications with dual-band stabilization[J]. Nature Photonics, 2021, 15(7): 530-535.

[15] Park C H, Woo M K, Park B K, et al. 2×N twin-field quantum key distribution network configuration based on polarization, wavelength, and time division multiplexing[J]. NPJ Quantum Information, 2022, 8: 48.

[16] Wang S, Yin Z Q, He D Y, et al. Twin-field quantum key distribution over 830-km fibre[J]. Nature Photonics, 2022, 16(2): 154-161.

[17] Sit A, Bouchard F, Fickler R, et al. High-dimensional intracity quantum cryptography with structured photons[J]. Optica, 2017, 4(9): 1006.

[18] Ding Y H, Bacco D, Dalgaard K, et al. High-dimensional quantum key distribution based on multicore fiber using silicon photonic integrated circuits[J]. NPJ Quantum Information, 2017, 3: 25.

[19] Cozzolino D, Da Lio B, Bacco D, et al. High-dimensional quantum communication: Benefits, progress, and future challenges[J]. Advanced Quantum Technologies, 2019, 2(12): 1900038.

[20] Li Y, Sun Z Q, Li P Y, et al. Polarization and orbital angular momentum coupling for high-dimensional measurement--deviceindependent quantum key distribution protocol[J]. Quantum Information Processing, 2023, 22(3): 147.

[21] Pirandola S, Laurenza R, Ottaviani C, et al. Fundamental limits of repeaterless quantum communications[J]. Nature Communications, 2017, 8(1): 1-15.

[22] 苑立民. 电力系统信息通信网络安全及防护措施分析[J]. 数字技术与应用, 2023, 41(9): 240-242.

[23] Gunduz M Z, Das R. Cyber-security on smart grid: Threats and potential solutions[J]. Computer Networks, 2020, 169: 107094.

[24] Majid M, Habib S, Javed A R, et al. Applications of wireless sensor networks and Internet of Things frameworks in the industry revolution 4.0: A systematic literature review[J]. Sensors, 2022, 22(6): 2087.

[25] Feng H, Tavakoli R, Onar O C, et al. Advances in high-power wireless charging systems: Overview and design considerations[J]. IEEE Transactions on Transportation Electrification, 2020, 6(3): 886-919.

[26] Tariq M I, Ahmed S, Memon N A, et al. Prioritization of

information security controls through fuzzy AHP for cloud computing networks and wireless sensor networks[J]. Sensors, 2020, 20(5): 1310.
[27] 张素香, 高德荃, 陈智雨, 等. 面向电网应用的量子保密通信系统VPN实测分析[J]. 电力信息与通信技术, 2017, 15(10): 38−42.
[28] Sikeridis D, Ott D, Huntley S, et al. ELCA: Introducing enterprise−level cryptographic agility for a post−quantum era[J]. Cryptology ePrint Archive, 2023, 10(10): 1539.
[29] 田照宇, 肖磊, 李伯中, 等. 电力通信网络中的量子保密通信示范应用与测评[J]. 中国电力, 2021, 54(1): 175−181.
[30] Huang L L, Feng K, Xie C J. A practical hybrid quantum−safe cryptographic scheme between data centers [C]//Proceedings of Emerging Imaging and Sensing Technologies for Security and Defence V; and Advanced Manufacturing Technologies for Micro− and Nano−systems in Security and Defence III. Washington: SPIE, 2020: 30−35.
[31] Li D D, Zhao M S, Li Z, et al. High dimensional quantum key distribution with temporal and polarization hybrid encoding[J]. Optical Fiber Technology, 2022, 68(1): 102828.

High−dimensional twin−field quantum key distribution improves the security of electric power systems

HAN Jiajia[1], TANG Yize[1], DAI Hua[1], XU Sicong[2], LÜ Yuxiang[2], MA Haiqiang[3*]

1. State Grid Zhejiang Electric Power Research Institute, Beijing 310014, China
2. Anhui Jiyuan Software Co., Ltd., Hefei 230000, China
3. School of Science, Beijing University of Posts and Telecommunications, Beijing 100876, China

Abstract In order to improve the security of wireless public power systems, a solution based on high−dimensional twin−field quantum key distribution is proposed in this study. The scheme employs polarization and longitudinal momentum coupling for high−dimensional quantum coding of a single photon, which enables the photon to carry 2−bits of information and is subject to only one−sided channel attenuation. Simulation results show that compared with the traditional two−dimensional protocol, the security code rate of this protocol is improved by nearly an order of magnitude. Additionally, it has the capability to surpass the transmission distance limitations imposed by relay−free key rates, while the quantum bit error rate is only 0.04. This solution significantly improves the security of the wireless public power system, and provides a new option for reliable power transmission and data communication.

Keywords two−field; quantum secure communications; quantum key distribution; wireless public power systems

（责任编辑 傅雪）