航空科学技术
Aeronautical Science & Technology
Mar. 25 2021 Vol. 32 No.03 71-78

基于斐波那契编码的测量设备无关量子密钥分发方案

尚涛[1,*]，孙海正[2]，刘建伟[1]

1.北京航空航天大学 空天网络安全工业与信息化部重点试验室，北京 100083

2.北京航空航天大学，北京 100083

摘　要：随着量子密钥分发(QKD)技术的飞速发展，为了确保航空通信的安全性，研究人员开始逐步对航空机载平台的量子通信技术进行相关研究和试验。在自由空间试验中，测量设备无关量子密钥分发(MDI-QKD)协议虽然消除了对于探测器边信道的攻击，但是受到大气湍流等干扰因素的影响，其密钥生成率仍然偏低。本文利用斐波那契数列与卢卡斯数列之间存在的关系，对光子轨道角动量(OAM)进行密钥信息编码，提出了一种基于斐波那契编码的MDI-QKD方案。该方案在不影响原始MDI-QKD协议安全性的基础上，单次量子信息传输容量增加。分析了在自由空间中存在噪声的情况下大气湍流对光子OAM的散射效应，得到了探测端检测到不同OAM态的概率，以及使用OAM编码量子信息的MDI-QKD方案的密钥生成率与最大传输距离的关系。当光信号在大气信道传输时，随着光信号的径向强度逐渐增大，大气湍流对光子OAM态的散射效应逐渐增强，原始OAM态发散为相邻OAM态并趋于无规则分布，探测端检测到原始OAM态的概率不断减小。基于OAM编码的MDI-QKD方案的最大传输距离要比基于偏振编码的MDI-QKD方案增加20km。

关键词：航空机载通信技术；测量设备无关；量子密钥分发；轨道角动量；斐波那契数列；大气湍流

中图分类号：TN918　　**文献标识码：**A　　DOI：10.19452/j.issn1007-5453.2021.03.011

量子信息技术的飞速发展给传统航空电子与通信等相关领域带来了挑战，同时也带来了新的研究方向，例如，量子导航、量子成像、量子加密以及量子通信等方向[1]。量子信息技术为未来航空产业的发展带来了新动力，促使航空技术更加高效地为人类服务。量子密钥分发(quantum key distribution, QKD)作为量子信息中最接近实用化的技术，具有理论上绝对安全的特性。该技术经过几十年的发展，正进行着由理论走向实际应用的过程。目前，有些地方已经搭建了一些小型化QKD网络用于试验和研究[2]。量子保密通信相比经典保密通信传输容量更大，复杂度更低。这些特点使得它更适用于航空机载通信技术，所以要发展航空机载量子通信技术，则其面临的相关问题亟待解决。面向航空测试的机载量子通信技术主要对机载量子通信方案的有效性和安全性进行分析研究，研究成果和分析方法有助于航空试验和高性能机载设备的设计开发，为以后建设全覆盖量子通信网络提供重要参考依据[3]。

现阶段，QKD主要面临安全传输距离短和密钥生成率低的实际问题。随着量子卫星的成功发射，研究人员提出了基于卫星的QKD网络方案，该方案可以有效减弱远距离光子的损耗，从而极大提升密钥信息的安全传输距离。但是构建全球的量子星地网络通信需要在各方面耗费大量资源，这些因素限制了其实际应用范围[4]。近些年，航空器的发展突飞猛进，尤其是无人机设备，其在性能、载重及易操作等方面有了很大提升[5]。飞行器中机载通信技术的安全性更是重中之重，甚至关系到国家的安全。因此研究人员尝试将QKD技术引入到航空机载通信平台中，并进行了诸

收稿日期：2020-11-01；退修日期：2020-12-12；录用日期：2021-01-25
基金项目：航空科学基金(2018ZC51016)；国家自然科学基金(61971021，61571024)；国家重点研发计划(2016YFC1000307)
*通信作者：Tel：010-82317222　E-mail：shangtao@buaa.edu.cn
引用格式：Shang Tao，Sun Haizheng，Liu Jianwei.Measurement-device independent quantum key distribution scheme based on Fibonacci coding[J].Aeronautical Science & Technology，2021，32(03)：71-78. 尚涛，孙海正，刘建伟. 基于斐波那契编码的测量设备无关量子密钥分发方案[J]. 航空科学技术，2021，32(03)：71-78.

多试验[6-7]。

光具有自旋角动量(spin angular momentum, SAM)和轨道角动量(orbital angular momentum, OAM)[8]。使用光子的OAM编码信息具有两个优势:一是OAM态在传输方向上具有旋转不变性,因此发送方和接收方不必实时调整参考系统;二是理论上,OAM存在无限维度的本征态,在信息编码过程中,通过对OAM态进行高维编码可以有效提升编码过程的效率[9]。OAM具有的这两个优势,可以减少航空机载量子通信平台的复杂度,以及提升处理数据的效率。

光子的OAM通过纳米等离子体螺旋阵列可以产生具有多个分布在斐波那契数值之间的OAM值。本文基于光子OAM的特点提出了一种利用斐波那契数列(Fibonacci)与卢卡斯(Lucas)数列之间关系编码的MDI-QKD (Measuvement-Device Independent QKD)方案。在保证方案安全性的前提下,通过改变量子信息的编码方式,提升单次量子密钥分发的信息传输容量,从而提升方案的密钥生成率。同时,仿真分析表明了方案的抗干扰能力和整体性能。

1 自由空间中QKD技术的发展现状

在自由空间中,光信号存在的双折射现象基本可以忽略,其退相干效应也比较小,这些优势使得量子密钥分发的安全传输距离得到提升。但是受到自由空间中大气湍流以及近地地形等干扰因素的影响,QKD的传输距离仍然受到限制,误码率也会增加。参考文献[10]中给出了一种空地量子密钥分发网络的数据协调方案,使用该方案可以减少QKD系统复杂度,便于部署在机载平台上。

自由空间中的量子密钥分发技术研究已经取得了一些进展。2012年,德国航空航天中心联合慕尼黑大学在飞机与地面站之间进行了BB84协议的测试试验,首次将QKD系统部署到移动机载平台上,试验结果给出系统的误码率为4.8%,密钥生成率为145bit/s[6]。2016年,“墨子号”量子科学试验卫星在中国成功发射,该卫星也是世界上首颗量子通信卫星[11]。2019年,南京大学科研人员使用无人机建立了两条空对地量子链路,并测试了基于量子纠缠的空地QKD[7]性能,该研究给未来量子通信网络的建设带来新选择。2020年,中国科学技术大学研究团队利用“墨子号”试验卫星在国际上首次实现千公里级基于纠缠的量子密钥分发[11],该研究成果进一步提升了无中继量子保密通信的空间传输距离。

近年来,一些研究人员转向针对高维系统的量子密钥分发方案进行研究,并取得了一定进展。通过发展高维希尔伯特空间来研究高容量量子密钥分发方案的研究有两方面主要优势:一方面加密密钥的多个比特可以编码在一个量子上,另一方面高维系统对某些类型的噪声具有更强的抗干扰性。该方案的两个特点与航空机载量子通信平台的需求相吻合,适合在自由空间中进行量子密钥信息的分发。

2013年,D.S.Simon等提出了一种高容量、高效率形式的量子密钥分发协议[9]。他们利用专门设计的光子的OAM纠缠态和斐波那契数列来实现密钥分发,但是其协议的高容量特性仍然受到实现困难、编码不够灵活的限制。原因主要是增加信息容量依赖于具有更大带宽的OAM和用于编码的方法。因此,由于实际带宽的限制,它不可能同时满足较长的距离和较低的误码率。其次,虽然Simon等已经提出OAM-QKD协议的理论分析,但由于所使用的硬件设备存在缺陷,仍可能遭受针对探测器端的攻击。其实,在2012年,Lo等[12]提出了使用测量设备独立性的方法来解决该问题。在MDI-QKD协议中,通信双方(Alice和Bob)将量子信息发送给第三方(Charlie)完成测量,即使Charlie是不可信的,也可以完成一个安全的QKD过程。而且,在该方案中,Alice或Bob信息的传输距离只是Alice或Bob的信息到探测器的距离,因此,Alice和Bob之间的通信距离是QKD中实际传输距离的两倍。

2 基本理论

斐波那契数列:$F_k = F_{k-1} + F_{k-2}, k \geqslant 2, k$为整数

卢卡斯数列:$L_k = L_{k-1} + L_{k-2}, k \geqslant 2, k$为整数

它们之间存在的关系:

$$L_k = F_{k+1} + F_{k-1}, \quad F_{2k} = F_k \times L_k \tag{1}$$

构造矩阵[13]:

$$\boldsymbol{Q}_1^{2k} = \begin{pmatrix} F_{2k-1} & F_{2k} \\ F_{2k} & F_{2k+1} \end{pmatrix}, \tag{2}$$

$$\boldsymbol{Q}_1^{-2k} = \begin{pmatrix} F_{2k+1} & -F_{2k} \\ -F_{2k} & F_{2k-1} \end{pmatrix}$$

$$\det\left(Q_1^{2k}\right) = (-1)^{2k} = 1 \tag{3}$$

构建斐波那契对角线密钥矩阵:

$$\boldsymbol{D}_{2k} = \begin{pmatrix} Q_1^{2k} & 0 & \cdots & 0 \\ 0 & Q_1^{2k-2} & & \vdots \\ \vdots & & \vdots & 0 \\ 0 & \cdots & 0 & Q_1^{2} \end{pmatrix}_{2k \times 2k}$$

$$\boldsymbol{D}_{2k}^{-1} = \begin{pmatrix} Q_1^{-2k} & 0 & \cdots & 0 \\ 0 & Q_1^{-(2k-2)} & & \vdots \\ \vdots & & & 0 \\ 0 & \cdots & 0 & Q_1^{-2} \end{pmatrix}_{2k \times 2k} \tag{4}$$

密钥矩阵对应的行列式：

$$\det(D_{2k}) = (-1)^{k(k+1)} \tag{5}$$

3 基于斐波那契编码的MDI-QKD方案

3.1 设计思路

光子的OAM具有高维度特性，并且其通过纳米等离子体螺旋阵列可以产生具有多个分布在斐波那契数值之间的OAM值。本文基于光子OAM态的特点使用斐波那契数值编码密钥信息。通过利用式(1)~式(5)中斐波那契数列和卢卡斯数列存在的关系，以及构建密钥矩阵的规则，在原始MDI-QKD方案的框架下对密钥信息编码方式和测量过程进行了设计。本文提出的基于斐波那契编码的MDI-QKD方案，既保留了原方案消除探测器边信道的攻击的特点，也提升了单次量子密钥分发的信息传输容量。

3.2 具体步骤

Alice和Bob是需要建立安全密钥的通信双方，Charlie是一个不可信的第三方，负责检测由Alice和Bob传输的纠缠光子。试验主要设备：单光子探测器L_{C1}、D_{C1}、L_{C2}、D_{C2}；光子OAM态分选机Sorter；分束器BS；诱骗态强度调制器Decoy-IM；空间光调制器SLM；Alice端和Bob端分选器L_A和L_B。具体步骤为：

(1) Alice使用斐波那契数值编码OAM纠缠光子对，记为$|\varphi\rangle$。Bob使用卢卡斯数值编码OAM纠缠光子对，记为$|\phi\rangle$。OAM纠缠态中存在的两种光子分别命名为斐波那契数值的信号光子态和辅助光子态，其中信号光子态记为$|F_k\rangle_s$，辅助光子态记为$|F_k\rangle_i$，其中k为正整数。斐波那契数值和卢卡斯数值的OAM纠缠态如下所示：

$$|\varphi\rangle = \sum_4^9 (|F_{k-1}\rangle_s |F_{k-2}\rangle_i + |F_{k-2}\rangle_s |F_{k-1}\rangle_i) \tag{6}$$

$$|\phi\rangle = \sum_4^9 (|F_{k+1}\rangle_s |F_{k-1}\rangle_i + |F_{k-1}\rangle_s |F_{k+1}\rangle_i) \tag{7}$$

Alice和Bob分别将纠缠对中信号光子留给自己。与此同时，Alice和Bob分别将调制好的辅助光子通过自由空间信道发送给第三方测量设备Charlie。试验原理如图1所示。

(2) 在Charlie的测量设备中，首先使用两个静态光学OAM分选机(Sorter)以及一个透镜分别过滤出叠加态$\frac{1}{\sqrt{2}}(|F_{k-2}\rangle + |F_k\rangle)$和$\frac{1}{\sqrt{2}}(|F_{k-1}\rangle + |L_k\rangle)$，并阻止任何非斐波那契数值的OAM态通过。$L_{C1}$、$D_{C1}$、$L_{C2}$和$D_{C2}$是4个单光子探测器，用于检测斐波那契数值的OAM态，其中L_{C1}用于检测OAM态$|F_{k-2}\rangle / |F_{k-1}\rangle$；$L_{C2}$用于检测OAM态$|F_{k-1}\rangle / |F_{k+1}\rangle$；$D_{C1}$用于检测OAM叠加态$\frac{1}{\sqrt{2}}(|F_{k-2}\rangle + |F_k\rangle)$；$D_{C2}$用于检测OAM叠加态$\frac{1}{\sqrt{2}}(|F_{k-1}\rangle + |L_k\rangle)$。然后，仅当$L_{C1}$和$L_{C2}$、$L_{C1}$和$D_{C2}$、$D_{C1}$和$L_{C2}$、$D_{C1}$和$D_{C2}$这4种情况中任一种情况下的两个探测器同时触发时，本次测量成功。最后，Charlie完成了对辅助光子的Bell态测量，并将测量结果通过经典公开信道发送给Alice和Bob。

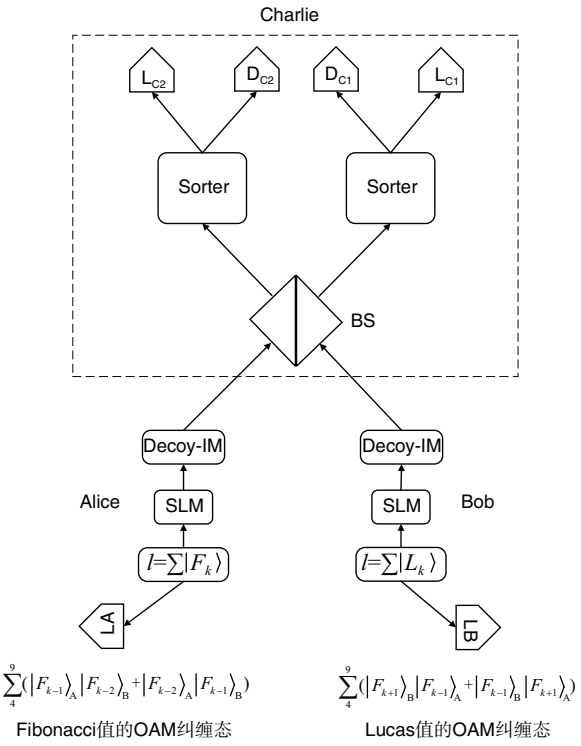

图1 基于斐波那契编码的MDI-QKD方案的试验原理图

Fig.1 Experimental schematic diagram of the MDI-QKD scheme based on Fibonacci coding

在表1中，Charlie进行Bell态测量时，T表示探测器L_{C1}和L_{C2}同时响应；U表示探测器L_{C1}和D_{C2}同时响应；V表示探

表1 基于斐波那契编码的MDI-QKD方案中可能的测量结果

Table 1 Possible measurement results of MDI-QKD scheme based on Fibonacci coding

发送的纠缠态		可能的测量结果			
Alice	Bob	T	U	V	W
$\|\varphi\rangle$	$\|\phi\rangle$	1	0	0	0
$\|\varphi\rangle$	$\|\phi\rangle$	0	1	0	0
$\|\varphi\rangle$	$\|\phi\rangle$	0	0	1	0
$\|\varphi\rangle$	$\|\phi\rangle$	0	0	0	1

测器 L_{C2} 和 D_{C1} 同时响应；W 表示探测器 D_{C1} 和 D_{C2} 同时响应。

（3）根据表 1 所示，Alice 和 Bob 保留所有结果中对应于 Charlie 成功测量的情况（T、U、V 和 W）。然后，Alice 将本地保留的信号光子调制后传输到本方的 L_A 探测器中，同时 Bob 也将本地保留的信号光子调制后传输到本方的 L_B 探测器中。Alice 和 Bob 分别使用 OAM 分选器 L_A 和 L_B 对信号光子态进行检测。如果 Alice（或 Bob）发现 Charlie 发布的结果与他们检测到的结果不匹配，通信双方将终止通信。否则，他们继续执行以下操作。

在通信双方中，当一方检测到确定的斐波那契数值时，另一方检测到的斐波那契数值还仍然无法确定。通过分析图 1、通信双方的 OAM 纠缠态和 Charlie 的测量结果，双方可以得到确定的斐波那契数值。例如，如果 Alice 和 Bob 检测到的结果分别是 $\left|F_{k-1}\right\rangle$ 和 $\left|F_{k-1}\right\rangle$，而 Charlie 中产生响应的探测器为 L_{C1} 和 L_{C2}，测量结果为 $\left|F_{k-2}\right\rangle$ 和 $\left|F_{k+1}\right\rangle$，对应表 1 中 T 的情况。Alice 方拥有的斐波那契数值为 F_{k-1}，根据 OAM 纠缠态 $|\varphi\rangle=\sum_{4}^{9}(\left|F_{k-1}\right\rangle_s\left|F_{k-2}\right\rangle_i+\left|F_{k-2}\right\rangle_s\left|F_{k-1}\right\rangle_i)$，可知发送的辅助光子的值为 F_{k-2}，对比 Charlie 公布的测量结果和响应的探测器，此次通信正常。Alice 根据公式 $F_k=F_{k-1}+F_{k-2}$，$k\geqslant 2$ 可以求出斐波那契数值 F_k。同理，Bob 方拥有的斐波那契数值为 F_{k-1}，根据 OAM 纠缠态 $|\phi\rangle=\sum_{4}^{9}(\left|F_{k+1}\right\rangle_s\left|F_{k-1}\right\rangle_i+\left|F_{k-1}\right\rangle_s\left|F_{k+1}\right\rangle_i)$，可知发送的辅助光子的数值为 F_{k+1}，对比 Charlie 公布的测量结果和响应的探测器，此次通信正常。Bob 根据公式 $L_k=F_{k+1}+F_{k-1}$，$k\geqslant 2$ 可以求出卢卡斯数值 L_k。然后，Alice 和 Bob 根据斐波那契数列和卢卡斯数列可以同时得到 F_k 和 L_k，进一步得到密钥种子 $F_{2k}=F_k\times L_k$。该过程不需要交换经典信息，也不需要进行经典比特位翻转。当 Alice 和 Bob 检测到的结果为其他情况时见表 1，通信双方也可以使用相同的方法得到密钥种子 F_{2k}。

（4）Alice 和 Bob 重复步骤（1）~步骤（3），直到获得足够长的密钥种子。

（5）根据 Charlie 的探测器的结果，Alice 和 Bob 得到斐波那契密钥矩阵的密钥种子 F_{2k}。他们使用随机数生成器生成相同秩的斐波那契密钥矩阵，如式（4）所示。

（6）Alice 和 Bob 可以通过对应的行列式 $\det(D_{2k})=1$，验证密钥矩阵是否正确。如果行列式不等于 1，则中止通信。否则，他们可以使用斐波那契对角线密钥矩阵通过矩阵乘法对数字消息进行加密。

3.3 方案的特点

（1）不需要实时调整系统参考系

OAM 状态的波函数表达式可以表示为[8,14]：

$$u_{lp}^{LG}(r,\alpha,z)=\frac{A(r,z)}{\sqrt{2\pi}}\exp(il\alpha) \tag{8}$$

z 轴方向的 OAM 算子可以在柱坐标系中表示为：

$$\hat{L}_z=-i\frac{\partial}{\partial\alpha} \tag{9}$$

当进行测量时，假设系统旋转角度为 θ，则 OAM 处于的控制区域为：

$$e^{i\theta\hat{L}_z}\left|u_{lp}^{OAM}\right\rangle=e^{il\theta}\left|u_{lp}^{OAM}\right\rangle \tag{10}$$

由式（10）可知，等式两边只是常数因子不同，量子状态并没有发生改变。

（2）不需要对经典比特进行翻转

通过观察试验原理图（见图 1）可知，Alice 和 Bob 可以依据自身所处实验室的分选机 L_A 和 L_B 获得密钥种子，并从 Charlie 得知测量的结果，而不是原始 MDI-QKD 协议中使用的比特翻转方法。

（3）编码能力更强

在所提出方案中，使用获得的斐波那契数值作为斐波那契对角线密钥矩阵的种子，然后可以使用矩阵乘法对数字消息序列进行加密。在 Simon 等[9]提出的 QKD 协议中，使用 3~89 之间的 8 个斐波那契数值分别用来表示一个三位二进制字符串，从而提升单个量子比特携带的信息量。而在本文方案中，如步骤（3）所描述，合法通信双方在密钥分发完成后，可以同时得到斐波那契数值 F_k 和卢卡斯数值 L_k，通过计算进一步得到密钥种子 F_{2k}。假设生成的密钥种子分别为 $F_4=3$ 和 $F_6=8$，当它们表示三位二进制字符串时，生成密钥序列的长度为 6 位；当使用它们构建斐波那契对角线密钥矩阵 $\boldsymbol{D}_4$ 时，如式（11）所示，该方案可以生成一个由 4×4 矩阵表示的密钥数据。

$$\boldsymbol{D}_4=\begin{pmatrix}2&3&0&0\\3&5&0&0\\0&0&5&8\\0&0&8&13\end{pmatrix}_{4\times4} \tag{11}$$

由式（11）可知，斐波那契对角线密钥矩阵 $\boldsymbol{D}_4$ 所表示的密钥数据长度明显比编码为三位二进制字符串要长，该方法提高了量子比特的编码能力。

（4）高效的数据传输速率

在本文提出的方案中，将分选器 L_A 和 L_B 分别放置在 Alice 和 Bob 的实验室中，并放置两对检测器，即 L_{C1} 和 D_{C1}、

L_{C2}和D_{C2}在Charlie的测量设备中。与现有的MDI-QKD协议不同，每种纠缠态都会产生密钥信息，不会丢弃任何一种类型的纠缠态。在Charlie的测量设备中，当L_{C1}和L_{C2}、L_{C1}和D_{C1}、L_{C2}和D_{C2}、D_{C1}和D_{C2}中，每一对中两个探测器同时响应时，Alice和Bob都可以获得密钥种子。将本文方案的数据传输速率定义为：

$$R_F = q \times f_{\text{rep}} \times \mu \times t_{\text{link}} \times \eta \times c \tag{12}$$

式中：q为整体方案的效率因子，在Ekert91方案中[15]，q=1/2，在本文方案中$q=1$。f_{rep}为光源脉冲的重复频率，μ为表每脉冲光子的平均数量，t_{link}为单个光子在传输链路上的传输系数，η为单光子探测器的探测效率，c为携带光子的能力。此外，由于改变了信息编码方式，新方案中光子携带的信息容量有了很大提高，与现有方案相比[12]，本文提出的方案允许更高的数据传输速率。

4 仿真分析

采用MATLAB工具对提出的量子密钥分发方案进行仿真分析。通信过程中各通信方的仿真参数如下：Charlie的仿真参数：e_d=1.5%，P_d=3×10^{-6}，f=1.6。Alice(Bob)的仿真参数：l=10，R=0.075m，λ=1.55μm，β=0.6(dB/km)，C_n^2=1(10^{-15}m$^{-2/3}$)。

4.1 大气湍流对OAM态的影响

在自由空间信道中，大气湍流是光信号OAM态的主要干扰因素。信道中传输的有限维OAM态受到大气湍流干扰会散射到邻近OAM态上[16]。假设发射端光子OAM态为$l_0\hbar$(l_0为量子数)，当光信号经过大气湍流传输时，接收端探测到的光子OAM态为$l_1\hbar$(l_1为量子数，且$l_1 \neq l_0$)。收发两端光子OAM态的量子数差值为$\Delta l = l_1 - l_0$，参考文献[17]可得接收端探测得相邻阶OAM态的概率为：

$$P(l_0 + \Delta l) = \frac{1}{2\pi^2 R^2}\int_0^R r\mathrm{d}r \int_0^{2\pi}\mathrm{d}\theta_1 \int_0^{2\pi} \exp\{-\frac{1}{2}\times [\varphi(r,\theta_1) - \varphi(r,\theta_2)]^2\} + [i\Delta l(\theta_1 - \theta_2)]\mathrm{d}\theta_2 \tag{13}$$

式中：R为接收孔径半径；r和θ分别为径向系数和方位角系数；φ为相位。将Δl = 0,1,2,3分别代入式(13)进行画图处理，可得光信号经过Kolmogorov大气湍流模型后光子OAM态的概率分布图，如图2所示。其中r_0为大气相干长度。

由图2可知，光信号在大气湍流中传播时，发送端光子原有的OAM态有可能会被散射到相邻的OAM态上。当接收端进行探测时，得到原有OAM态的概率随r/r_0参数逐渐变小。同时，接收端检测到光子原有OAM态相邻态的概率先变大后变小。导致该情况的原因是光信号在大气传播过程中，闪烁现象会随着传输距离的增加而逐渐严重，最后会使得所有OAM态趋向于随机分布[17]。

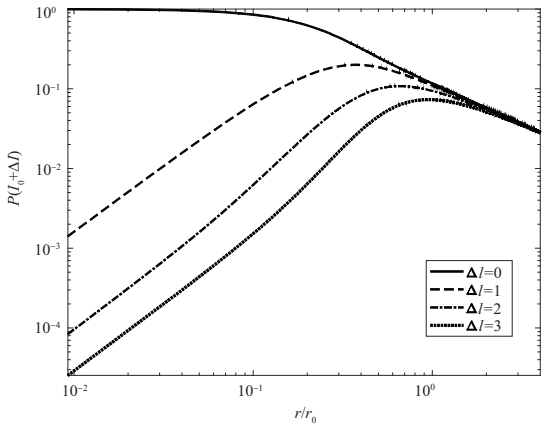

图2 错误概率$P(l_0 + \Delta l)$随r/r_0的变化趋势

Fig. 2 Trend of error probability $P(l_0 + \Delta l)$with r/r_0

在本文方案中，将斐波那契数值编码到光子OAM态上。设原始光子OAM态对应斐波那契数值为5，Δl = 0,3,8,16。将Δl分别代入式(13)，可以得到具有斐波那契数值特征的光信号经过Kolmogorov模型湍流后光子OAM态的概率分布图，如图3所示。

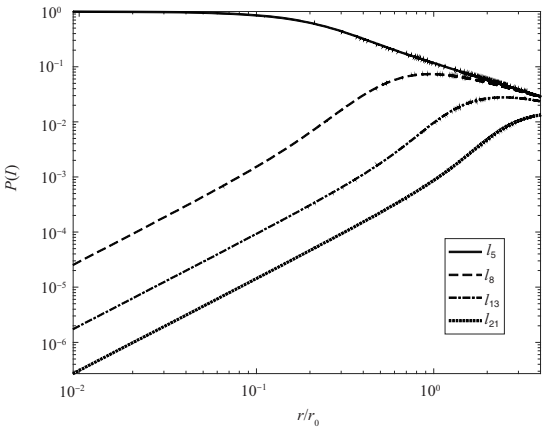

图3 错误概率$P(l)$随r/r_0的变化趋势

Fig. 3 Trend of error probability $P(l)$with r/r_0

在图3中，可以看出原始OAM态散射到相邻具有斐波那契数值特征的OAM态的概率更小，并且斐波那契数值越大的OAM态散射到邻近态的概率更低。所以使用斐波那契数列编码密钥信息到OAM态上，可以减小大气湍流对密钥信息误码率的影响。

4.2 密钥生成率与传输距离的关系

密钥生成率的公式为[10]：

$$R = \mu v \exp[-(\mu+v)] Y_{\mathrm{OAM}}^{1,1}[1-H(e_{\mathrm{SUP}}^{1,1})] - Q_{\mathrm{OAM}}^{\mu v} f(E_{\mathrm{OAM}}^{\mu v}) H(E_{\mathrm{OAM}}^{\mu v})] \quad (14)$$

$$H(x)=H_2(x)=-x\log_2(x)-(1-x)\log_2(1-x) \quad (15)$$

式中：μ和v分别为Alice和Bob发送信号态时的平均光子数；$Y_{\mathrm{OAM}}^{1,1}$为OAM基下的单光子计数率；$e_{\mathrm{SUP}}^{1,1}$为SUP基下的单光子误码率；$f(E_{\mathrm{OAM}}^{\mu v})>1$为低效率纠错函数；$Q_{\mathrm{OAM}}^{\mu v}$和$E_{\mathrm{OAM}}^{\mu v}$分别为量子密钥分发过程中通信双方都选择OAM基时发送量子态的总增益和总误码率；$H_2(x)$为香农二元熵函数。参考文献[18]中给出了对$Y_{\mathrm{OAM}}^{1,1}$，$e_{\mathrm{SUP}}^{1,1}$，$Q_{\mathrm{OAM}}^{\mu v}$和$E_{\mathrm{OAM}}^{\mu v}$的取值的估计方法。由式(14)和式(15)以及仿真参数可得仿真结果如图4所示。

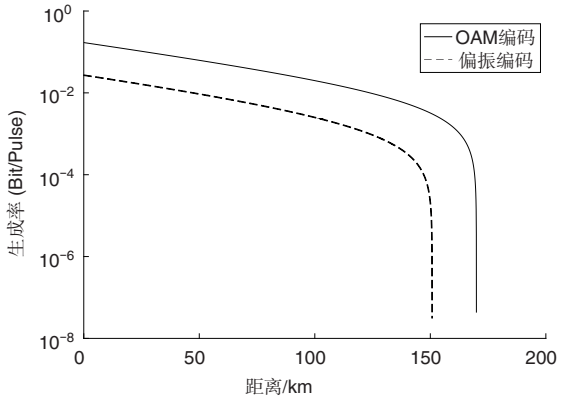

图4 密钥生成率与传输距离的变化趋势

Fig. 4 Trend of key generation rate with transmission distance

图4中是偏振编码与OAM编码方式下的密钥生成率随传输距离的变化关系。如图4所示，与偏振编码QKD方案相比，使用OAM编码的QKD方案的安全传输距离更长，传输距离增加约20km。在采用OAM编码的MDI-QKD方案中，OAM态在传输方向上具有旋转不变性，该特性减小了由于参考系未对准而引起的量子误码率，使得密钥的安全传输距离增加[18]。

5 安全性分析

本文在基于偏振编码的MDI-QKD方案基础上提出了基于斐波那契编码的MDI-QKD方案。该方案与原有方案存在两方面不同。

(1)编码方式

本文方案利用光子OAM态的多维特性来编码密钥信息，编码方式更加灵活，每个光子能够编码的经典信息也更多。参考文献[19]给出了光子OAM态在量子密钥分发中的安全性证明。

(2)第三方测量后的处理

本文方案中通信双方将具有斐波那契特征的数值编码到光子OAM态上，经过第三方测量后，通信双方根据测量结果各自生成斐波那契对角线密钥矩阵。通过验证密钥矩阵对应行列式是否为1，检测是否存在窃听。本文方案中测量设备与原始MDI-QKD方案具有等同的作用，通过后选择(post-select)和密钥矩阵的验证保证方案的安全性。

在本文方案实际应用过程中，需要引入诱骗态技术解决非理想光源面临的安全问题。该过程的安全性可根据GLLP[20]、Shor-Preskill[21]等理论来保证。

6 结论

本文重点分析了利用斐波那契数列与卢卡斯数列之间存在的关系对密钥信息进行编码的MDI-QKD的方案。相较于Simon等[9]提出的使用斐波那契数列编码三位二进制量子信息，该方案编码的信息容量得到提升，并且安全性与原始MDI-QKD协议相同。航空机载量子通信技术传输信息容量的提升，可以加快该技术实际应用的步伐。同时，使用光子OAM编码量子信息，光信号在传输方向上具有旋转不变性，因此发送方和接收方不必实时调整对准参考系统，该特点可以降低航空机载量子通信设备的复杂度，使其部署更方便，实现成本也更低。通过仿真分析了在大气湍流存在的情况下，噪声对相邻OAM态的干扰情况。并且对比了采用OAM编码和偏振编码的MDI-QKD方案的密钥传输距离。由结果可知，本文提出的方案在密钥信息容量和传输距离方面都有了提升。自由空间中多维量子密钥分发方案的研究也对未来实现全球量子通信具有重要推动作用。

AST

参考文献

[1] Bi S W, Henri J, Chandra S R. Quantum remote sensing: review and perspective[J]. Journal of Global Change Data & Discovery, 2019, 3(4): 317-325.

[2] 陈非凡,胡鑫煜,赵英浩,等.全球量子保密通信网络发展研究[J].计算机科学与应用, 2018,8(10):1628-1641.
Chen Feifan, Hu Xinyu, Zhao Yinghao, et al. Development analysis on global quantum secure communication network [J]. Computer Science and Application, 2018, 8(10): 1628-1641.(in Chinese)

[3] 胡丽华,钟志珊,杜鑫,等. 基于仿真技术的机载电子设备结构设计[J].航空电子技术, 2012,43(3):44-49.
Hu Lihua, Zhong Zhishan, Du Xin, et al. Structure design of airborne electronic equipment based on simulation technology [J]. Avionics Technology, 2012, 43(3): 44-49.(in Chinese)

[4] Mitch L. Quantum cryptography via satellite[J]. Engineering, 2019, 5(3):353-354.

[5] 尹文强,孙健. 高空长航时无人机实用升限试飞技术研究[J]. 航空科学技术, 2020, 31(2): 25-30.
Yin Wenqiang, Sun Jian. Research on service ceiling flight test technology in high altitude long endurance UAV[J]. Aeronautical Science & Technology, 2020, 31(2): 25-30.(in Chinese)

[6] Nauerth S, Moll F, Rau M, et al. Air-to-ground quantum communication[J]. Nature Photonics, 2013, 7(5):382-386.

[7] Liu Huaying, Tian Xiaohui, Gu Changsheng, et al. Drone-based entanglement distribution towards mobile quantum networks[J]. National Science Review, 2020, 7(5):921-928.

[8] 郑凤, 陈艺戬, 冀思伟,等. 轨道角动量通信技术的研究[J]. 通信学报, 2020 (5):150-158.
Zheng Feng, Chen Yijian, Ji Siwei, et al. Research on orbital angular momentum communication technology[J]. Acta Optica Sinica, 2020 (5):150-158.(in Chinese)

[9] Simon D S, Lawrence N, Trevino J, et al. High-capacity quantum Fibonacci coding for key distribution[J]. Physical Review A, 2013, 87(3):032312.

[10] 孙海正,尚涛,刘建伟,等. 空地量子密钥分发网络中数据协调方案[J/OL]. (2020-02-10) [2020-11-13]. 北京航空航天大学学报, https://doi.org/10.13700/j.bh.1001-5965.2019.0599.
Sun Haizheng, Shang Tao, Liu Jianwei, et al. Data reconciliation scheme for space-ground quantum key distribution network [J/OL]. (2020-02-10) [2020-11-13]. Journal of Beijing University of Aeronautics and Astronautics, https://doi.org/10.13700/j.bh.1001-5965.2019.0599.(in Chinese)

[11] Yin J, Li Y H, Liao S K, et al. Entanglement-based secure quantum cryptography over 1, 120 kilometres[J]. Nature, 2020, 582(7813):1-5.

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

[13] Esmaeili M, Moosavi M, Gulliver T A. A new class of Fibonacci sequence based error correcting codes [J]. Cryptography and Communications, 2017, 9(3): 379-396.

[14] Heim B, Elser D, Bartley T J, et al. Atmospheric channel characteristics for quantum communication with continuous polarization variables [J]. Applied Physics B, 2009, 98(4): 635-640.

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

[16] Pugh C J, Kaiser S, Bourgoin J P, et al. Airborne demonstration of a quantum key distribution receiver payload [J].Quantum Science and Technology, 2017, 2(2):024009.

[17] Wang Le, Zhao Shengmei, Gong Longyan, et al. Free-space measurement-device-indepen dentquantum-key-distribution protocol using decoy states with orbital angular momentum [J]. Chinese Physics B, 2015, 24(12):242-249.

[18] Gibson G, Courtial J, Padgget M, et al. Free-space information transfer using light beam scarrying orbital angular momentum [J]. Optics Express, 2004, 12(22): 5448-5456.

[19] Grcher S, Jennewein T, Vaziri A, et al. Experimental quantum cryptography with qutrits [J]. New Journal of Physics, 2006, 8(5): 75.

[20] Gottesman D, Lo H K, Lutkenhaus N, et al. Security of quantum key distribution with imperfect devices [J]. Quantum Information and Computation, 2004, 4(5):325-360.

[21] Hwang W Y, Wang X B, Matsumoto K, et al. Shor-Preskill-type security proof for quantum key distribution without public announcement of bases [J]. Physical Review A, 2003, 67(1): 012302.

（责任编辑 陈东晓）

作者简介

尚涛(1976-)男,副教授,博士生导师。主要研究方向:量子密码和量子网络编码。

Tel: 010-82317222

E-mail: shangtao@buaa.edu.cn

孙海正(1993-)男,硕士研究生。主要研究方向:量子密钥分发。

E-mail: sunhaizh@qq.com

刘建伟(1964-)男,教授,博士生导师。主要研究方向:密码学和网络安全。

E-mail:liujianwei@buaa.edu.cn

Measurement-device Independent Quantum Key Distribution Scheme Based on Fibonacci Coding

Shang Tao[1,*], Sun Haizheng[2], Liu Jianwei[1]

1. Key Laboratory of Aerospace Network Security, Ministry of Industry and Information Technology, Beihang University, Beijing 100083, China

2. Beihang University, Beijing 100083, China

Abstract: With the rapid development of quantum key distribution (QKD) technology, in order to ensure the security of aviation communication, researchers began to gradually carry out relevant research and experiments on the quantum communication technology of aviation airborne platform. In the free space experiment, the measurement device independent quantum key distribution (MDI-QKD) protocol eliminates the attack on the detector's side channel, but its key generation rate is still low due to the influence of atmospheric turbulence and other interference factors. Based on the relationship between Fibonacci sequence and Lucas sequence, this paper encodes the key information of photonic orbital angular momentum (OAM), and proposes an MDI-QKD scheme based on Fibonacci coding. The encoded quantum key distribution scheme increases the single quantum information transmission capacity without affecting the security of the original MDI-QKD protocol. The scattering effect of atmospheric turbulence on photonic OAM in the presence of noise in free space is analyzed, and the probability of detecting different OAM states at the detection end is obtained. And the relationship between the key generation rate and the maximum transmission distance of the MDI-QKD scheme that uses OAM to encode quantum information is established. When the beam propagates in the atmospheric channel, the radial intensity of the beam gradually increases, and the scattering effect of the turbulence on the photonic OAM gradually increases. The original OAM state diverges into adjacent OAM states and tends to be irregularly distributed. The probability of detecting the original OAM state at the detection end continues to decrease. The maximum transmission distance of the MDI-QKD scheme based on OAM coding is 20km longer than that of the MDI-QKD scheme based on polarization coding.

Key Words: aviation airborne communication technology; measurement equipment independent; quantum key distribution; orbital angular momentum; Fibonacci sequence; atmospheric turbulence

Received: 2020-11-01； **Revised:** 2020-12-12； **Accepted:** 2021-01-25

Foundation item: Aeronautical Sicence Foundation of China (2018ZC51016)；National Nature Science Foundation of China (61971021,61571024); National Key Research and Development plan of China(2016YFC1000307)

***Corresponding author.Tel.**：010-82317222 **E-mail**：shangtao@buaa.edu.cn