SCIENCE CHINA
Information Sciences

• RESEARCH PAPER •

June 2018, Vol. 61 062501:1–062501:11
https://doi.org/10.1007/s11432-017-9291-6

High-rate and high-capacity measurement-device-independent quantum key distribution with Fibonacci matrix coding in free space

Hong LAI[1*], Mingxing LUO[2], Josef PIEPRZYK[3,4], Jun ZHANG[5],
Lei PAN[5] & Mehmet A. ORGUN[6,7*]

[1] *School of Computer and Information Science and Centre for Research and Innovation in Software Engineering (RISE), Southwest University, Chongqing 400715, China;*
[2] *Information Security and National Computing Grid Laboratory, School of Information Science and Technology, Southwest Jiaotong University, Chengdu 610031, China;*
[3] *School of Electrical Engineering and Computer Science, Queensland University of Technology, Brisbane 4000, Australia;*
[4] *Institute of Computer Science, Polish Academy of Sciences, Warsaw 01-248, Poland;*
[5] *School of Information Technology, Deakin University, Geelong 3220, Australia;*
[6] *Department of Computing, Macquarie University, Sydney 2109, Australia;*
[7] *Faculty of Information Technology, Macau University of Science and Technology, Macau 519020, China*

Received 5 June 2017/Revised 29 August 2017/Accepted 26 October 2017/Published online 7 May 2018

Abstract This paper proposes a high-rate and high-capacity measurement-device-independent quantum key distribution (MDI-QKD) protocol with Fibonacci-valued and Lucas-valued orbital angular momentum (OAM) entangled states in free space. In the existing MDI-OAM-QKD protocols, the main encoding algorithm handles encoded numbers in a bit-by-bit manner. To design a fast encoding algorithm, we introduce a Fibonacci matrix coding algorithm, by which, encoded numbers are separated into segments longer than one bit. By doing so, when compared to the existing MDI-OAM-QKD protocols, the new protocol can effectively increase the key rate and the coding capacity. This is because Fibonacci sequences are used in preparing OAM entangled states, reducing the misattribution errors (which slow down the execution cycle of the entire QKD) in QKD protocols. Moreover, our protocol keeps the data blocks as small as possible, so as to have more blocks in a given time interval. Most importantly, our proposed protocol can distill multiple Fibonacci key matrices from the same block of data, thus reducing the statistical fluctuations in the sample and increasing the final QKD rate. Last but not the least, the sender and the receiver can omit classical information exchange and bit flipping in the secure key distillation stage.

Keywords measurement-device-independent quantum key distribution, Fibonacci-matrix coding, free space, orbital angular momentum, bit flipping, misattribution errors

Citation Lai H, Luo M X, Pieprzyk J, et al. High-rate and high-capacity measurement-device-independent quantum key distribution with Fibonacci matrix coding in free space. Sci China Inf Sci, 2018, 61(6): 062501, https://doi.org/10.1007/s11432-017-9291-6

1 Introduction

On August 16, 2016, China launched a satellite from the Jiuquan Satellite Center. The satellite called Micius was designed to conduct a variety of experiments with quantum key distribution (QKD), quantum

[*] Corresponding author (email: hlai@swu.edu.cn, mehmet.orgun@mq.edu.au)

entanglement, quantum non-locality tests and quantum teleportation. One of the main aims of the satellite missions was to investigate the challenges related to the particle entanglement technology. It is known that if two quantum particles are entangled, then a change of the state of one particle causes an instantaneous change of the state of the other particle. In theory, this interaction should be independent from the distance between the two particles. At present, although the main communication medium of quantum secure communication is optical fiber, experiments have confirmed that entanglement work when two particles are not far away from 200 km in optical fiber. While in free space, atmospheric turbulence has little influence on the polarization state of light, and even can be ignored due to a small angle forward scattering of light to atmospheric turbulence. Also, orbital angular momentum (OAM) remains unchanged when rotating, so, the sender and the receiver do not have to adjust the reference system in real time [1–4]. Consequently, developing a satellite-based quantum communication between very distant parties on Earth provides an unexplored opportunity for new applications of quantum technology, which includes an investigation of quantum key distribution (QKD) based on OAM in free space.

In 1992, Allen et al. [5] showed that a single photon can carry a well-defined value of OAM. When the well-defined values are Fibonacci sequence, the ratio of Fibonacci sequence approaches the golden ratio, which leads to distinctive features of the band edge modes [6]. Moreover, golden-angle spirals have been widely discovered in nature, such as the arrangements in sunflower seeds and pine cones [7]. Such patterns do not exhibit clumping in distributions of sunflower seeds. Moreover, spontaneous photometric down conversion (SPDC) processes have been widely used as the OAM entanglement source in QKD protocols. Inspired by nature, golden-angle spiral structures have been explored by Simon et al. [6] to prepare OAM entangled states with SPDC, reducing the misattribution errors in QKD protocols. Furthermore, Simon et al.'s [6] QKD protocol exhibits large birefringence with a tunable dispersion. Most importantly, in contrast to other encoding schemes such as polarization, OAM offers a large state space and allows transmission of much more information per photon. Another advantage of OAM is that its use increases resistance to errors in QKD protocols [8]. The higher dimension of the state space can be more secure against eavesdropping attacks, since the error probability introduced by an eavesdropper will be greatly increased in such a communication protocol [9].

Although the theoretical analysis of Simon et al.'s OAM-QKD protocol [6] has been presented, it may still suffer from "side-channel attacks" because of the flaws of the hardware devices used [10–12]. Actually, in 2012, Lo et al. [10] proposed to use the method of measurement device independence to address it. In the MDI-QKD protocol, the two parties (Alice and Bob) send quantum information to a third party (Charlie) to complete the measurement, and even if Charlie is untrusted, a secure QKD process can be completed. Moreover, in this system, the transmission distance of Alice's or Bob's information is only the distance from Alice's or Bob's information to the detector, so, the communication distance between Alice and Bob is twice as long as the actual transmission distance in QKD [12]. Most importantly, MDI-QKD protocols have been shown to be free from side-channel attacks, since Alice and Bob can distill a secret key in terms of Charlie's measurement outcomes alone. Since the original MDI-QKD protocol was proposed by Lo et al. [10], many revised protocols have been proposed [13–21] and some experiments have already been performed [22–24]. However, until the present time, free-space MDI-QKD protocols with Fibonacci-valued OAM entangled states have not been reported.

In this paper, we present an MDI-OAM-QKD protocol with a photonic system composed of two-particular-sequence beams in free space. Our protocol combines MDI-OAM-QKD with SPDC corresponding to Fibonacci-valued and Lucas-valued OAM entanglements. An entanglement exists between the two beams with two particular sequences without changing the way in which OAM entangled states are prepared. The protocol has the following features: (1) OAM remains constant when a Fibonacci-valued or Lucas-valued OAM entangled state is rotated around the propagation direction. Consequently, two communicating parties do not have to adjust the parameters. (2) Detected Fibonacci and Lucas values can be used to achieve Fibonacci matrix coding, greatly improving the coding capacity of a photon and data transmission rates. (3) Information rates of QKD protocols are improved but with neither classical information exchange nor bit flipping in the secure key distillation stage. And (4) distilled Fibonacci values can be used more than once, thus reducing the statistical fluctuations in the sample.

Table 1 Terms of Fibonacci and Lucas sequences

k	0	1	2	3	4	5	6	7	8	$\cdots$
F_k	0	1	1	2	3	5	8	13	21	$\cdots$
L_k	2	1	3	4	7	11	18	29	47	$\cdots$

In the rest of this paper, Section 2 discusses and uses the relationship between the Fibonacci sequence (F_k) and the Lucas sequence (L_k) to construct block-diagonal Fibonacci matrices. Section 3 describes the new MDI-OAM-QKD protocol. The security analysis and features of the protocol are presented in Sections 4 and 5. Section 6 presents a brief summary four contributions to conclude the work.

2 Fibonacci and Lucas sequences and block-diagonal Fibonacci matrix D_{2k}

In this section, we define the Fibonacci and Lucas sequences and discuss the relationship between them. Next we show how the sequences can be used to create block-diagonal Fibonacci matrix D_{2k}.

2.1 Fibonacci sequence

Definition 1 (Fibonacci numbers [25])**.** The Fibonacci sequence $\{F_k\}_{k=0}^{+\infty}$ of integers is defined by the following recurrence relation:

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

where $F_0 = 0,\ F_1 = 1$. A few elements of the sequence can be seen in Table 1.

2.2 Lucas sequence

Below, we present the definition of the Lucas sequence, and two well-known facts on the Fibonacci and Lucas numbers [25].

Definition 2 (Lucas numbers [25])**.** The Lucas sequence $\{L_k\}_{k=0}^{+\infty}$ of integers is defined by the following recurrence:

$$L_k = L_{k-1} + L_{k-2}, \quad k \geqslant 2, \tag{2}$$

where $L_0 = 2$ and $L_1 = 1$. A few integers of the sequence can be seen in Table 1.

The relationship between the Lucas and Fibonacci sequences is described by the following relations:

$$L_k = F_{k+1} + F_{k-1}, \tag{3}$$

$$F_{2k} = F_k L_k. \tag{4}$$

Table 1 also illustrates the relationship.

2.3 Block-diagonal Fibonacci matrix D_{2k}

A Fibonacci Q-matrix [26] is defined as follows:

$$\overline{Q_1} = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}. \tag{5}$$

According to work by Esmaeili et al. [26], one can write a Fibonacci Q-matrix of dimension 2 as follows:

$$Q_1 = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}. \tag{6}$$

Table 2 Q_1^{2k} and Q_1^{-2k}, where $k=2,3,4,5$

k	2	3	4	5
Q_1^{2k}	$\begin{pmatrix} 2 & 3 \\ 3 & 5 \end{pmatrix}$	$\begin{pmatrix} 5 & 8 \\ 8 & 13 \end{pmatrix}$	$\begin{pmatrix} 13 & 21 \\ 21 & 34 \end{pmatrix}$	$\begin{pmatrix} 34 & 55 \\ 55 & 89 \end{pmatrix}$
Q_1^{-2k}	$\begin{pmatrix} 5 & -3 \\ -3 & 2 \end{pmatrix}$	$\begin{pmatrix} 13 & -8 \\ -8 & 5 \end{pmatrix}$	$\begin{pmatrix} 34 & -21 \\ -21 & 13 \end{pmatrix}$	$\begin{pmatrix} 89 & -55 \\ -55 & 34 \end{pmatrix}$

The following relations can be used to create consecutive Fibonacci matrices:

$$Q_1^{2k} = \begin{pmatrix} F_{2k-1} & F_{2k} \\ F_{2k} & F_{2k+1} \end{pmatrix}. \tag{7}$$

Note that Q_1^{2k} satisfies the following property:

$$\det(Q_1^{2k}) = (-1)^{2k} = 1.$$

Clearly, Q_1^{2k} is invertible and its inverse matrix Q_1^{-2k} can be calculated as follows:

$$Q_1^{-2k} = \begin{pmatrix} F_{2k+1} & -F_{2k} \\ -F_{2k} & F_{2k-1} \end{pmatrix}. \tag{8}$$

By using the above relation, we can obtain Q_1^{-2k} of Q_1^{2k} when $k=2,3,4,5$ (see Table 2).

The process of creating a block-diagonal Fibonacci matrix D_{2k} is performed iteratively as follows. We start from Q_1 and then construct the block-diagonal Fibonacci matrices D_{2k} as follows, where $p=1,2,3,\ldots$

$$D_{2k} = \begin{pmatrix} Q_1^{2k} & 0 & \cdots & 0 \\ 0 & Q_1^{2k-2} & \ddots & \vdots \\ \vdots & \ddots & \ddots & 0 \\ 0 & \cdots & 0 & Q_1^2 \end{pmatrix}_{2k\times 2k}, \tag{9}$$

and

$$\det(D_{2k}) = \det(Q_1^2) \times \det(Q_1^4) \times \cdots \times \det(Q_1^{2k}) = (-1)^{(k+1)k}. \tag{10}$$

According to (9) and (10), D_{2k} is invertible, for all $k=1,2,3,\ldots$. Moreover, from (9), we can easily find its inverse Q_{2p}^{-2k} as follows:

$$D_{2k}^{-1} = \begin{pmatrix} Q_1^{-2k} & 0 & \cdots & 0 \\ 0 & Q_1^{-(2k-2)} & \ddots & \vdots \\ \vdots & \ddots & \ddots & 0 \\ 0 & \cdots & 0 & Q_1^{-2} \end{pmatrix}_{2k\times 2k}. \tag{11}$$

3 High-rate and high-capacity measurement-device-independent QKD protocols

In this section, we use the sources of entangled Fibonacci-valued and Lucas-valued OAM states based on a Vogel spiral as in Simon et al.'s protocol [6]. Simon et al. pointed out that compared with the Fibonacci sequence, though the Lucas sequence starts from different initial values, it still obeys the

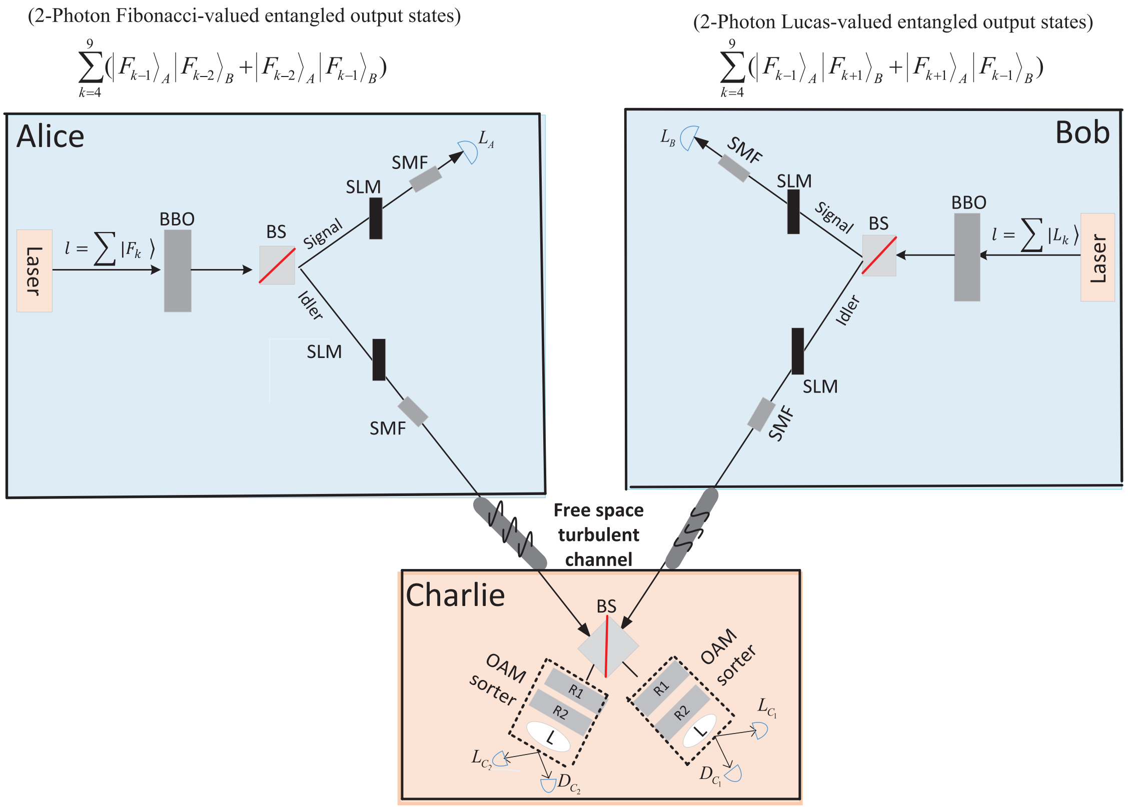
(2-Photon Fibonacci-valued entangled output states)
$\sum_{k=4}^{9}(|F_{k-1}\rangle_A|F_{k-2}\rangle_B+|F_{k-2}\rangle_A|F_{k-1}\rangle_B)$
(2-Photon Lucas-valued entangled output states)
$\sum_{k=4}^{9}(|F_{k-1}\rangle_A|F_{k+1}\rangle_B+|F_{k+1}\rangle_A|F_{k-1}\rangle_B)$
Alice
Laser
$l=\sum|F_k\rangle$
BBO
BS
Signal
Idler
SLM
SMF
L_A
SLM
SMF
Bob
L_B
SMF
SLM
Signal
BS
BBO
$l=\sum|L_k\rangle$
Laser
Idler
SLM
SMF
Free space turbulent channel
Charlie
BS
OAM sorter
R1
R2
L
L_{C_2}
D_{C_2}
OAM sorter
R1
R2
L
L_{C_1}
D_{C_1}

Figure 1 (Color online) The experimental setup of the proposed OAM-MDI-QKD protocol based on a Vogel spiral. The laser sources in Alice's and Bob's labs pump Barium borate (BBO) crystals to prepare Fibonacci- and Lucas-valued pairs of entangled photons with the spontaneous parametric down conversion (SPDC). The crystal planes are imaged onto the spatial light modulators (SLMs), and every SLM is imaged onto the input of a single-mode fiber (SMF). Then single photons are detected with detectors $L_A, L_B, L_{C_1}, L_{C_2}, D_{C_1}, D_{C_2}$ in Alice's, Bob's and Charlie's laboratories. The detectors $L_A, L_B, L_{C_1}, L_{C_2}$ are used only for letting Fibonacci-valued photons reach the arrays of single-photon detectors, while the OAM-sorters R1 and R2 (two static optical elements) and a lens (L) are used for differentiating the superpositions of the form $\frac{1}{\sqrt{2}}(|F_{k-2}\rangle+|F_k\rangle)$ and $\frac{1}{\sqrt{2}}(|F_{k-1}\rangle+|L_k\rangle)$ respectively, and blocking any non-Fibonacci values. D_{C_1}, D_{C_2} can be used to detect the superposition states $\frac{1}{\sqrt{2}}(|F_{k-2}\rangle+|F_k\rangle)$ and $\frac{1}{\sqrt{2}}(|F_{k-1}\rangle+|L_k\rangle)$ respectively. BS denotes beam splitter with 50 : 50.

Fibonacci recursion relations, and therefore their method is also suitable for preparing entangled Lucas-valued OAM states. Then, we exploit the relationships between the Lucas and Fibonacci sequences to encode states according to block-diagonal Fibonacci matrices. The encoding achieves a high-rate and high-capacity measurement-device-independent QKD in free space. The protocol follows the steps described below. Alice and Bob are the two authenticated parties that wish to establish a secure key. Charlie can be an untrusted third party who detects the entangled photons transmitted by them.

Step 1. Using a Barium borate (BBO) crystal via the spontaneous parametric down conversion (SPDC), the two parties Alice and Bob prepare Fibonacci-valued and Lucas-valued OAM entangled photon pairs, named Fibonacci-valued signal photons and Fibonacci-valued idler photons respectively (see Figure 1). The values for the signal and idler are F_{k-1} and F_{k-2}, and F_{k+1} and F_{k-1}. However, for either beam, either value can be, so the Fibonacci and Lucas-valued OAM entangled states are as follows:

$$|\varphi\rangle=\sum_{k=4}^{9}(|F_{k-1}\rangle_s|F_{k-2}\rangle_i+|F_{k-2}\rangle_s|F_{k-1}\rangle_i), \tag{12}$$

$$|\phi\rangle=\sum_{k=4}^{9}(|F_{k+1}\rangle_s|F_{k-1}\rangle_i+|F_{k-1}\rangle_s|F_{k+1}\rangle_i), \tag{13}$$

Table 3 The possible outcomes for key seeds in our MDI-QKD protocol [a)]

The sent entangled states		The probability to the measured outcome				Final key seeds
Alice	Bob	T	U	V	W	
[0.5ex] $\vert\varphi\rangle$	$\vert\phi\rangle$	1	0	0	0	Yes
$\vert\varphi\rangle$	$\vert\phi\rangle$	0	1	0	0	Yes
$\vert\varphi\rangle$	$\vert\phi\rangle$	0	0	1	0	Yes
$\vert\varphi\rangle$	$\vert\phi\rangle$	0	0	0	1	Yes

a) T: Charlie announces that the signal entangled photons from Alice and Bob go to the sorters L_{C_1}, L_{C_2}; U: Charlie announces that the signal entangled photons from Alice and Bob go to the sorters L_{C_1} and D_{C_2}; V: Charlie announces that the signal entangled photons from Alice and Bob go to the sorters L_{C_2} and D_{C_1}; W: Charlie announces that the signal entangled photons from Alice and Bob go to both the sorters D_{C_1} and D_{C_2}.

where i denotes the idler light and s denotes the signal light. Moreover, considering turbulence affects [27–32], we select appropriate Fibonacci values $F_5, F_6, F_7, F_8, F_9, F_{10}$ and Lucas values $L_5, L_6, L_7, L_8, L_9, L_{10}$ as the pump value l for wide-bandwidth communications to achieve longer distances and lower error rates.

Next, Alice and Bob keep the signal photons for themselves, and transmit the idler photons to Charlie through the free-space channel. Both Alice and Bob select computer-controlled spatial light modulators (SLMs) together with single-mode fibers (SMFs) as their sector states for the signal and the idler photons. Then they transmit the modulated signal photons to the detectors L_A and L_B, respectively. At the same time, they send the modulated idler photons to Charlie.

Step 2. First, two static optical OAM-sorters R1 and R2 and a lens (L) are used to filter the superpositions of the form $\frac{1}{\sqrt{2}}(|F_{k-2}\rangle + |F_k\rangle)$ and $\frac{1}{\sqrt{2}}(|F_{k-1}\rangle + |L_k\rangle)$ respectively, and block any non-Fibonacci values against various possible problems. Second, in the focal planes of the lenses, there are four single photon sorters $L_{C_1}, D_{C_1}, L_{C_2}$ and D_{C_2}, which are used to detect two Fibonacci-valued OAM states $|F_{k-2}\rangle/|F_{k-1}\rangle$ and $|F_{k-1}\rangle/|F_{k+1}\rangle$ simultaneously, that is, L_{C_1} or D_{C_1} for the OAM state $|F_{k-2}\rangle/|F_{k-1}\rangle$, L_{C_2} or D_{C_2} for the OAM state $|F_{k-1}\rangle/|F_{k+1}\rangle$. Finally, Charlie carries out the modulated measurements of the idler photons'. He succeeds if and only if two of the four detectors ($L_{C_1}, D_{C_1}, L_{C_2}$ and D_{C_2}) are triggered simultaneously at L_{C_1} and L_{C_2}, L_{C_1} and D_{C_2}, L_{C_2} and D_{C_1}, or D_{C_1} and D_{C_2} (see Table 3).

Step 3. According to Table 3, Alice and Bob keep all the results corresponding to the cases T and U, V and W of Charlie's successful measurements. If Alice or Bob find that Charlie's published outcomes do not match their detected ones, she (he) aborts the communication. Otherwise, they perform the following operations.

Based on the facts that for a definite Fibonacci number detected by one party, there is still a double uncertainty for the Fibonacci number the other party detected [6], in terms of Figure 1, Eq. (12), and Charlie's measured outcomes based on Table 3, Table 4 can be obtained. For example, if Alice's and Bob's detected outcomes are $|F_{k-1}\rangle$ and $|F_{k-1}\rangle$ respectively, Charlie chooses detectors L_{C_1} and L_{C_2} and the matching outcomes are $|F_{k-2}\rangle$ and $|F_{k+1}\rangle$. Therefore, both Alice and Bob can obtain F_k and L_k in a definite way, and further obtain key seeds $F_{2k} = F_k \times L_k$ without exchanging classical messages or by bit flipping. Other cases in Table 4 can be obtained in the same way.

Step 4. Alice and Bob repeat Steps 1–3 until they obtain a long enough key seed.

Step 5. According to the outcomes with detectors, Alice and Bob obtain the key seed F_{2k} for the Fibonacci key matrix as in (9). They use their random number generators to produce the Fibonacci key matrices of the same rank.

Example 1. Given the key seed $F_8 = 21$, $F_{10} = 55$ and $F_{12} = 144$, the generated Fibonacci diagonal

Table 4 The possible outcomes for available Fibonacci key seeds in our MDI-QKD protocol

Alice's detected outcomes	Bob's detected outcomes	Charlie's detected outcomes	Final key seeds
$\|F_{k-1}\rangle$	$\|F_{k-1}\rangle$	$\|F_{k-2}\rangle$ and $\|F_{k+1}\rangle$	F_{2k}
$\|F_{k-2}\rangle$	$\|F_{k-1}\rangle$	$\|F_{k-1}\rangle$ and $\|F_{k+1}\rangle$	F_{2k}
$\|F_{k-1}\rangle$	$\|F_{k+1}\rangle$	$\|F_{k-2}\rangle$ and $\|F_{k-1}\rangle$	F_{2k}
$\|F_{k-2}\rangle$	$\|F_{k+1}\rangle$	$\|F_{k-1}\rangle$ and $\|F_{k-1}\rangle$	F_{2k}
$\|F_{k-2}\rangle$	$\|F_{k-1}\rangle$	$\|F_{k-1}\rangle$ and $\frac{1}{\sqrt{2}}(\|F_{k-1}\rangle+\|L_k\rangle)$	F_{2k}
$\|F_{k-2}\rangle$	$\|F_{k+1}\rangle$	$\|F_{k-1}\rangle$ and $\frac{1}{\sqrt{2}}(\|F_{k-1}\rangle+\|L_k\rangle)$	F_{2k}
$\|F_{k-1}\rangle$	$\|F_{k-1}\rangle$	$\|F_{k-2}\rangle$ and $\frac{1}{\sqrt{2}}(\|F_{k-1}\rangle+\|L_k\rangle)$	F_{2k}
$\|F_{k-1}\rangle$	$\|F_{k+1}\rangle$	$\|F_{k-2}\rangle$ and $\frac{1}{\sqrt{2}}(\|F_{k-1}\rangle+\|L_k\rangle)$	F_{2k}
$\|F_{k-2}\rangle$	$\|F_{k-1}\rangle$	$\frac{1}{\sqrt{2}}(\|F_{k-2}\rangle+\|F_k\rangle)$ and $\|F_{k+1}\rangle$	F_{2k}
$\|F_{k-2}\rangle$	$\|F_{k+1}\rangle$	$\frac{1}{\sqrt{2}}(\|F_{k-2}\rangle+\|F_k\rangle)$ and $\|F_{k-1}\rangle$	F_{2k}
$\|F_{k-1}\rangle$	$\|F_{k-1}\rangle$	$\frac{1}{\sqrt{2}}(\|F_{k-2}\rangle+\|F_k\rangle)$ and $\|F_{k+1}\rangle$	F_{2k}
$\|F_{k-1}\rangle$	$\|F_{k+1}\rangle$	$\frac{1}{\sqrt{2}}(\|F_{k-2}\rangle+\|F_k\rangle)$ and $\|F_{k-1}\rangle$	F_{2k}
$\|F_{k-2}\rangle$	$\|F_{k-1}\rangle$	$\frac{1}{\sqrt{2}}(\|F_{k-2}\rangle+\|F_k\rangle)$ and $\frac{1}{\sqrt{2}}(\|F_{k-1}\rangle+\|L_k\rangle)$	F_{2k}
$\|F_{k-2}\rangle$	$\|F_{k+1}\rangle$	$\frac{1}{\sqrt{2}}(\|F_{k-2}\rangle+\|F_k\rangle)$ and $\frac{1}{\sqrt{2}}(\|F_{k-1}\rangle+\|L_k\rangle)$	F_{2k}
$\|F_{k-1}\rangle$	$\|F_{k-1}\rangle$	$\frac{1}{\sqrt{2}}(\|F_{k-2}\rangle+\|F_k\rangle)$ and $\frac{1}{\sqrt{2}}(\|F_{k-1}\rangle+\|L_k\rangle)$	F_{2k}
$\|F_{k-1}\rangle$	$\|F_{k+1}\rangle$	$\frac{1}{\sqrt{2}}(\|F_{k-2}\rangle+\|F_k\rangle)$ and $\frac{1}{\sqrt{2}}(\|F_{k-1}\rangle+\|L_k\rangle)$	F_{2k}

key matrix is as follows:

$$D_6=\begin{pmatrix} 89 & 144 & 0 & 0 & 0 & 0 \\ 144 & 233 & 0 & 0 & 0 & 0 \\ 0 & 0 & 34 & 55 & 0 & 0 \\ 0 & 0 & 55 & 89 & 0 & 0 \\ 0 & 0 & 0 & 0 & 13 & 21 \\ 0 & 0 & 0 & 0 & 21 & 34 \end{pmatrix}. \tag{14}$$

Step 6. Alice and Bob can verify whether the key matrices are correct with their corresponding determinants $\det(D_6)=1$ in terms of (10). If they are wrong, they abort the communication. Otherwise, they use the Fibonacci diagonal key matrix to encrypt the digital message using matrix multiplication.

4 Security analysis

Below, we analyze the security of the proposed MDI-OAM-QKD protocol, based on the hybrid OAM entangled states of the Lucas-sequence and the Fibonacci-sequence beams. That is, except for Alice and Bob, nobody can obtain the key.

(1) Firstly, both Alice and Bob use the Fibonacci-valued and Lucas-valued-OAM entangled state method, avoiding the photon number splitting attack [33]. Moreover, Alice and Bob send one half of OAM entangled photons to Charlie, while they keep the other half of OAM entangled photons. Given the properties of the sorters L_{C_1}, D_{C_1}, L_{C_2} and D_{C_2} [6], Alice and Bob detect the values carried by photons after Charlie finishes his measurements and announcements. Therefore, the Fibonacci and Lucas values carried by the detected entangled OAM photons could be used as the seed to produce the key. This means that the security of our protocol is similar to that of Ekert91 protocol [34], which has been shown to be unconditionally secure [35].

(2) Secondly, our proposed MDI-OAM-QKD protocol prevents eavesdropping against the detector, since the security of key generation is not guaranteed by Bob's measurement, but the third (untrusted) party's measurement. Moreover, our protocol can omit the use of the authenticated classical channel between Alice and Bob because of the particular design of the experimental setup, i.e., only the detectors L_A and L_B are used in Alice's and Bob's laboratories respectively. Though all the results in the detectors

L_{C_1}, D_{C_1}, L_{C_2} and D_{C_2} from Charlie's laboratory are publicly revealed, all the outcomes in the sorters L_A and L_B in Alice's and Bob's laboratories are undisclosed. More importantly, as we can see from Table 4, suppose that Charlie's detectors that are used to detect the entangled photons from Alice's and Bob's laboratories are L_{C_1} and L_{C_2}. According to the values detected with the sorters L_A and L_B in their laboratories, Alice and Bob can easily obtain the corresponding values for Fibonacci-valued and Lucas-valued OAM entangled states.

However, for the adversary Eve, without the detected outcomes from Alice's and Bob's laboratories, there is double uncertainty in the Fibonacci and Lucas numbers that Alice and Bob receive, which is determined by the principle of OAM sorters. That is, even if Eve knows the values carried by entangled photons, she does not know if Alice and Bob have the preceding or succeeding value of the pumps ($l = F_k$ and $l = L_k$ in our protocol). She can only obtain them with an average probability of 27.08% by guessing [6] respectively. For our protocol, Eve must correctly guess F_k and L_k simultaneously. Consequently, the successful probability to guess is reduced to 7.33%. For the cases L_{C_1} and D_{C_1}, L_{C_2} and D_{C_2}, and D_{C_1} and D_{C_2}, according to our protocol, Alice and Bob can obtain the specific Fibonacci and Lucas values carried by OAM entangled states. Meanwhile the adversary Eve obtains nothing, since in these three cases, Eve obtains the superpositions of the form $\frac{1}{\sqrt{2}}(|F_{k-2}\rangle + |F_k\rangle)$ and $\frac{1}{\sqrt{2}}(|F_{k-1}\rangle + |L_k\rangle)$, and the pump remains in a superposition. Therefore, Eve cannot uniquely determine Alice's and Bob's value or the pump value. Eve can randomly guess with only a chance of $\frac{1}{2}$, which is equivalent to no information.

(3) Most importantly, in our protocol, the actual coding used is the Fibonacci matrix coding corresponding to the pump values F_k and L_k. The ranks of the Fibonacci matrices, are determined by the random number generators in Alice's and Bob's laboratories. So, Eve cannot have any information about the ranks. Even if she guesses the correct F_{2k}, she cannot generate the right Fibonacci key matrix without knowing its rank. In other words, the core security of our protocol lies in two points: the post-selection of the cases on Charlie's announced detectors and the random rank of Fibonacci matrices. Here, post-selection means that Alice and Bob only need to select the desired results or the correct results after Charlie announces his detected outcomes. If there exists eavesdropping or interference during the measurement process, its impact on the measurement results can be divided into the as follows two cases: (i) When the measurement results, even if disturbed, are still within the required range, then the set of data can still be used to produce the key seeds, as the security of our protocol will be guaranteed by the post selection of the ranks of the Fibonacci matrices. (ii) When the measurement results are not within the required range, then Alice and Bob will not choose this set of data, to avoid eavesdropping on the impact of the key seeds. Most importantly, we can achieve eavesdropping detection using the determinants of Fibonacci matrices.

(4) Finally, for free-space orbit-angular-momentum-based communications, turbulence affects must be taken into account [27–32]. In Simon et al.'s protocol [6], it is proven that due to turbulence affects, the higher the pump value l, the lower the error rate, but the shorter the transmitted distance, while the lower the pump value l, the higher the error rate, but the longer the transmitted distance. Therefore, in Section 3, we select Fibonacci values $F_5, F_6, F_7, F_8, F_9, F_{10}$ and Lucas values $L_5, L_6, L_7, L_8, L_9, L_{10}$ as the pump value l to reduce the turbulence affects. Also, the method of increasing the mode-spacing between the OAM sorters introduced by Malik et al. [30] can be used to reduce turbulence affects in our protocol.

5 Features of our proposed protocol

When compared to the existing MDI-OAM-QKD protocols with SPDC [20,21], the encoding and decoding of information in our MDI-OAM-QKD protocol is convenient in free space. In general, our scheme has the following features: (1) There is no requirement to adjust the reference system. (2) It is efficient with a high key rate owing to maintaining the merit of MDI-OAM-QKD with SPDC by using OAM entanglement of pairs of the Fibonacci-valued or Lucas-valued beams and Fibonacci matrix coding. (3) It can reduce misattribution errors due to the golden angle (GA) spirals whose OAM values always sum to a Fibonacci or Lucas number. (4) It can remove the authenticated classical channel between Alice and Bob. (5) It can remove bit flipping operations.

(a) **No requirement to adjust the reference system.** As discussed by Fürst et al. [36] in the coordinate system, the wave function expression of the OAM state can be expressed as

$$u_{lp}^{LG}(r,\alpha,z)=\frac{A(r,z)}{\sqrt{2\pi}}\exp(\mathrm{i}l\alpha). \tag{15}$$

The OAM operator in the z-axis direction can be represented by the following equation in the column coordinate system [36]:

$$\widehat{L}_z=-\mathrm{i}\frac{\partial}{\partial\alpha}. \tag{16}$$

For the measurement, we assume that when the system rotates the angle θ, the OAM states that are into the control area change as follows [36]:

$$\mathrm{e}^{\mathrm{i}\theta\widehat{L}_z}|u_{lp}^{\mathrm{OAM}}\rangle=\mathrm{e}^{\mathrm{i}l\theta}|u_{lp}^{\mathrm{OAM}}\rangle. \tag{17}$$

It can be seen through (17) above, only the constant factors on the both sides of the equation change, and $|u_{lp}^{\mathrm{OAM}}\rangle$ and $\mathrm{e}^{\mathrm{i}l\theta}|u_{lp}^{\mathrm{OAM}}\rangle$ represent the same quantum state. So, in a QKD system based on OAM encoding, it is not necessary to require real-time monitoring and adjust the reference system [36].

(b) **No bit flipping.** By carefully designing the experimental setup (see Figure 1), Alice and Bob can obtain the key seeds in terms of the sorters L_A and L_B in their laboratories and announced outcomes from Charlie, instead of bit flipping used in the existing MDI-OAM-QKD protocols.

(c) **No authenticated classical channel between Alice and Bob.** Likewise, due to the experimental setup (see Figure 1), without exchanging classical messages through the authenticated classical channel between them, Alice and Bob can obtain the key seeds in terms of the sorters L_A and L_B in their laboratories and announced outcomes from Charlie.

(d) **High-capacity coding.** In our protocol, unlike the existing bit encoding method used in other protocols, we use the obtained Fibonacci values as the seeds for block-diagonal Fibonacci matrices, and then the digital message can be encrypted using matrix multiplication. In Simon et al.'s protocol, every Fibonacci number is used to represent a three-bit binary string. While in our proposed protocol, the same Fibonacci number is used to be the seed for constructing a Fibonacci matrix and further for block-diagonal Fibonacci matrices together with the Lucas number from Bob. Let us consider Example 1 given in Section 3, where (c) Fibonacci and Lucas numbers can transmit an 18-bit binary string between Alice and Bob. In contrast, our protocol can use (c) Fibonacci and Lucas numbers to send the data represented by a 6 × 6 matrix:

$$D_6=\begin{pmatrix} 13 & 21 & 0 & 0 & 0 & 0\\ 21 & 34 & 0 & 0 & 0 & 0\\ 0 & 0 & 34 & 55 & 0 & 0\\ 0 & 0 & 55 & 89 & 0 & 0\\ 0 & 0 & 0 & 0 & 89 & 144\\ 0 & 0 & 0 & 0 & 144 & 233 \end{pmatrix}.$$

Then, the key is $13\|21\|0\|0\|0\|0\|21\|34\|0\|0\|0\|0\|\|0\|0\|34\|55\|0\|0\|0\|0\|55\|89|0\|0\|0\|0\|0\|0\|89\|144\|0\|0$ $\|0\|0\|144\|233$, which is significantly longer than 18 bits.

This method greatly improves the coding capacity of an entangled photon. It is especially suitable for the finite-size scenario, because Alice and Bob obtain data for a finite amount of time, until the data block is large enough to guarantee small statistical fluctuations in the parameters estimated from the data set. Then they proceed and obtain the next block of data. The current approach used for OAM-MDI-QKD is to distill a single key bit from every block of data [20, 21]. Therefore, to increase the coding capacity, the data block should be kept as small as possible, so as to have more blocks in a given time interval [37].

(e) **High data transmission rates.** In our protocol, we place the sorters L_A and L_B in Alice's and Bob 's laboratories, and two pairs of detectors, i.e., L_{C_1} and D_{C_1}, L_{C_2} and D_{C_2} in Charlie's laboratory. Different to the existing MDI-OAM-QKD protocols, none of the entangled states are discarded in terms of the possible outcomes listed in Table 4. To be exact, when the detectors L_{C_1} and L_{C_2}, L_{C_1} and D_{C_1}, L_{C_2} and D_{C_2}, and D_{C_1} and D_{C_2} work in Charlie's laboratory, Alice and Bob can obtain the key seeds.

By considering feature (d) stated above, we define the data transmission rate as follows:

$$R_{\rm DT} = q \times f_{\rm rep} \times \mu \times t_{\rm link} \times \eta \times c, \tag{18}$$

where q represents the efficiency factor of a protocol, for example, in the Ekert91 protocol [33], $q = \frac{1}{2}$, while $q = 1$ in our protocol. Here, $f_{\rm rep}$ represents the repetitive frequency of the light source, μ represents the average number of photons per pulse, $t_{\rm link}$ ($0 \leqslant t_{\rm link} \leqslant 1$) represents the transmission coefficient of a single photon on the transmission link, and η represents the detection efficiency of the single photon detector, which are 1 in our protocol. c represents the capacity of a photon carried. Moreover, due to feature (d), the capacity of a photon carried in our protocol is greatly improved. That is, compared with the existing protocols [20, 21], our protocol allows for a higher data transmission rate.

6 Conclusion

In this paper, we have presented a MDI-OAM-QKD protocol with the use of pairs of Fibonacci-valued or Lucas-valued beams. A hybrid entanglement of Fibonacci-valued or Lucas-valued beams is adopted to achieve random rotations in MDI-OAM-QKD with SPDC protocols in free space. Compared to the original MDI-QKD protocols [20, 21], our protocol can reduce the misattribution errors of the entangled states, increase the key rate owing to the design of the experimental setup, and greatly improve the coding capacity of an entangled photon with Fibonacci matrix coding. Moreover, compared to the existing MDI-OAM-QKD protocols with SPDC, our protocol can remove the authenticated classical channel between Alice and Bob, and bit flipping.

Acknowledgements Hong LAI was supported by National Natural Science Foundation of China (Grant No. 61702427), Doctoral Program of Higher Education (Grant No. SWU115091), and financial support in part by 1000-Plan of Chongqing by Southwest University (Grant No. SWU116007). Mingxing LUO was supported by National Natural Science Foundation of China (Grant No. 61772437) and Sichuan Youth Science & Technique Foundation (Grant No. 2017JQ0048). Jun ZHANG was supported by National Natural Science Foundation of China (Grant No. 61401371). Josef PIEPRZYK has been supported by National Science Centre, Poland (Grant No. UMO-2014/15/B/ST6/05130).

References

1 Lai H, Luo M X, Pieprzyk J, et al. An efficient quantum blind digital signature scheme. Sci China Inf Sci, 2017, 60: 082501

2 Spedalieri F M. Quantum key distribution without reference frame alignment: exploiting photon orbital angular momentum. Opt Commun, 2006, 260: 340–346

3 Li J-L, Wang C. Six-state quantum key distribution using photons with orbital angular momentum. Chin Phys Lett, 2010, 27: 110303

4 Zhang C M, Zhu J R, Wang Q. Practical decoy-state reference-frame-independent measurement-device-independent quantum key distribution. Phys Rev A, 2017, 95: 032309

5 Allen L, Beijersbergen M W, Spreeuw R J C, et al. Orbital angular momentum of light and the transformation of Laguerre-Gaussian laser modes. Phys Rev A, 1992, 45: 8185–8189

6 Simon D S, Lawrence N, Trevino J, et al. High-capacity quantum Fibonacci coding for key distribution. Phys Rev A, 2013, 87: 032312

7 Krenn M, Malik M, Erhard M, et al. Orbital angular momentum of photons and the entanglement of Laguerre-Gaussian modes. Phil Trans R Soc A, 2017, 375: 20150442

8 Bechmann-Pasquinucci H, Peres A. Quantum cryptography with 3-state systems. Phys Rev Lett, 2000, 85: 3313–3316

9 Cerf N J, Bourennane M, Karlsson A, et al. Security of quantum key distribution using d-level systems. Phys Rev Lett, 2002, 88: 127902

10 Lo H K, Curty M, Qi B. Measurement-device-independent quantum key distribution. Phys Rev Lett, 2012, 108: 130503

11 Braunstein S L, Pirandola S. Side-channel-free quantum key distribution. Phys Rev Lett, 2012, 108: 130502

12 Ma X, Fung C H F, Razavi M. Statistical fluctuation analysis for measurement-device-independent quantum key distribution. Phys Rev A, 2012, 86: 052305

13 Tamaki K, Lo H K, Fung C H F, et al. Phase encoding schemes for measurement-device-independent quantum key distribution with basis-dependent flaw. Phys Rev A, 2012, 85: 042307

14 Zhang Y C, Li Z, Yu S, et al. Continuous-variable measurement-device-independent quantum key distribution using squeezed states. Phys Rev A, 2014, 90: 052325

15 Tang Y-L, Yin H-L, Chen S-J, et al. Field test of measurement-device-independent quantum key distribution. IEEE J Sel Top Quantum Electron, 2015, 21: 116–122

16 Ma X, Razavi M. Alternative schemes for measurement-device-independent quantum key distribution. Phys Rev A, 2012, 86: 062319

17 Lai H, Luo M X, Zhan C, et al. An improved coding method of quantum key distribution protocols based on Fibonacci-valued OAM entangled states. Phys Lett A, 2017, 381: 2922–2926

18 Zhao S M, Gong L Y, Li Y Q, et al. A large-alphabet quantum key distribution protocol using orbital angular momentum entanglement. Chin Phys Lett, 2013, 30: 060305

19 Mafu M, Dudley A, Goyal S, et al. Higher-dimensional orbital-angular-momentum-based quantum key distribution with mutually unbiased bases. Phys Rev A, 2013, 88: 032305

20 Wang L, Zhao S M, Gong L Y, et al. Free-space measurement-device-independent quantum-key-distribution protocol using decoy states with orbital angular momentum. Chin Phys B, 2015, 24: 120307

21 Chen D, Zhao S H, Shi L, et al. Measurement-device-independent quantum key distribution with pairs of vector vortex beams. Phys Rev A, 2016, 93: 032320

22 Da Silva T F, Vitoreti D, Xavier G B, et al. Proof-of-principle demonstration of measurement-device-independent quantum key distribution using polarization qubits. Phys Rev A, 2013, 88: 052303

23 Tang Z, Liao Z, Xu F, et al. Experimental demonstration of polarization encoding measurement-device-independent quantum key distribution. Phys Rev Lett, 2014, 112: 190503

24 Pirandola S, Ottaviani C, Spedalieri G, et al. High-rate measurement-device-independent quantum cryptography. Nat Photon, 2015, 9: 397–402

25 Vajda S. Fibonacci and Lucas Numbers, and the Golden Section: Theory and Applications. New York: Dover Publications, 2007

26 Esmaeili M, Moosavi M, Gulliver T A. A new class of Fibonacci sequence based error correcting codes. Cryptogr Commun, 2017, 9: 379–396

27 Yan X, Zhang P F, Zhang J H, et al. Effect of atmospheric turbulence on entangled orbital angular momentum three-qubit state. 2017, 26: 064202

28 Fu S, Gao C. Influences of atmospheric turbulence effects on the orbital angular momentum spectra of vortex beams. Photon Res, 2016, 4: 1–4

29 Jurado-Navas A, Tatarczak A, Lu X, et al. 850-nm hybrid fiber/free-space optical communications using orbital angular momentum modes. Opt Express, 2015, 23: 33721–33732

30 Malik M, O'Sullivan M, Rodenburg B, et al. Influence of atmospheric turbulence on optical communications using orbital angular momentum for encoding. Opt Express, 2012, 20: 13195–13200

31 Ren Y, Huang H, Xie G, et al. Atmospheric turbulence effects on the performance of a free space optical link employing orbital angular momentum multiplexing. Opt Lett, 2013, 38: 4062–4065

32 Rodenburg B, Lavery M P J, Malik M, et al. Influence of atmospheric turbulence on states of light carrying orbital angular momentum. Opt Lett, 2012, 37: 3735–3737

33 Huttner B, Imoto N, Gisin N, et al. Quantum cryptography with coherent states. Phys Rev A, 1995, 51: 1863–1869

34 Ekert A K. Quantum cryptography based on Bell's theorem. Phys Rev Lett, 1991, 67: 661–663

35 Lo H K, Ma X, Chen K. Decoy state quantum key distribution. Phys Rev Lett, 2005, 94: 230504

36 Fürst M, Weier H, Schmitt-Manderbach T, et al. Free-space quantum key distribution over 144 km. In: Proceedigns of Society of Photo-Optical Instrumentation Engineers (SPIE), Stockholm, 2006. 63990G

37 Jiang C, Yu Z W, Wang X B. Measurement-device-independent quantum key distribution with source state errors and statistical fluctuation. Phys Rev A, 2017, 95: 032325