Phase-matching quantum key distribution protocol based on orbital angular momentum

Zhigang Shen[1] * Shengmei Zhao[1] † Le Wang[1] ‡ Qianping Mao[2] §

[1] *Institute of Signal Processing Transmission, Nanjing University of Posts and Telecommunications, Nanjing, 210003, China*

[2] *College of computer science and technology, Nanjing Tech University, Nanjing 211800, China*

Abstract. A phase-matching quantum key distribution (PM-QKD) based on orbital angular momentum (OAM) protocol is proposed in the paper, named OAM-PM-QKD protocol, where the OAM of photon is used as an information carrier to implement the PM-QKD protocol. Moreover, the key generation rate performance of OAM-PM-QKD influenced by atmospheric turbulence is analyzed. The results show that the proposed OAM-PM-QKD protocol is able to exceed the linear key-rate bound when transmission distance exceeds $230km$, and its key generation rate is slightly larger than the original PM-QKD protocol, and the maximum secure transmission distance is also longer.

Keywords: Quantum key distribution, phase modulation, orbital angular momentum, secret key rate

1 Introduction

The transmission loss of photons is still a major challenge in the practical implementations of quantum key distribution (QKD) protocol. In 2018, Lucamarini *et al.* proposed a twin-field QKD (TF-QKD) protocol [1] to overcome the rate-distance limits of point to point QKD protocol without quantum repeaters, and subsequently a lot variant of TF-QKD was proposed, such as 'sending or not sending TF-QKD' protocol [2] and phase-matching quantum key distribution (PM-QKD) protocol [3].

At present, phase is often used as the information carrier for PM-QKD protocol. Like phase, orbital angular momentum (OAM) is also an information carrier of quantum state, and has high-dimensionality, orthogonality, and rotational symmetry properties [4, 5]. There are infinite OAM eigenstates in a single photon in theory, thus transmitting more information per photon. OAM state is invariant under rotations about the propagation direction, which further makes the sender and receiver avoid the reference frame misalignment. Until now, OAM states has been widely used as the information carriers in QKD protocol. For example, Mirhosseini [6] verified the high-dimensional QKD experiments encoded by OAM and weakly coherent states. We proposed the theoretical analysis of MDI-QKD protocol based on OAM [7] and round-robin differential-phase-shift quantum key distribution (RRDPS-QKD) protocol based on OAM [8]. Meng *et al.* [9] improved TF-QKD with the photon OAM to overcome the reference frame dependence. However, the PM-QKD based on OAM states has been so far much less analyzed and reported.

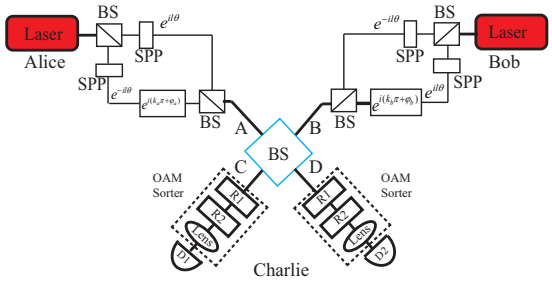

Figure 1: The schematic diagram of the proposed OAM-PM-QKD protocol. SPP: spiral phase plate. BS: 50 : 50 beam splitter. $R1$ and $R2$: two static optical elements. OAM sorter: to efficiently differentiate the different OAM state. $D1$, $D2$,: to detect OAM state $| +l >$ and $| -l >$.

2 Phase-matching quantum key distribution protocol based on orbital angular momentum

Fig.1 shows the schematic diagram of the proposed OAM-PM-QKD protocol. Both Alice and Bob generate pulses with a laser and modulate the photons of pulses to be the OAM states by emitting the pulses to a spiral phase plate (SPP). The OAM state is related to the azimuth phase of the photon, and it could be given as

$$| l >= R(r) \exp(il\theta). \tag{1}$$

where $R(r)$ is the amplitude, r and θ are the radial and azimuthal index, respectively. l is the topological charge of the OAM, whose value is an arbitrary integer. i is an image unit $i = \sqrt{(-1)}$. The OAM states prepared by Alice and Bob are superposition states of two opposite

*shenzg@126.com
†zhaosm@njupt.edu.cn
‡njwanglele@163.com
§maoqp@163.com

topological charges. Then, Alice and Bob send their pulses carrying OAM states to Charlie through free-space. In the protocol, Charlie is the only one who operates measurements. Then Alice and Bob could generate the key based on Charlies successful measurement results.

The details of the proposed OAM-PM-QKD protocol are listed below.

Step 1. Alice first randomly generates a binary key k_a and a random phase φ_a, $\varphi_a \in [0, 2\pi)$. Then, Alice prepares two SPPs to generate OAM states $e^{il\theta}$ and obtains her state as $|A>=|\frac{\mu}{\sqrt{2}}e^{il\theta}> \otimes|\frac{\mu}{\sqrt{2}}e^{-il\theta}e^{i(k_a\pi+\varphi_a)}>$, based on k_a and φ_a. Similarly, Bob randomly generates a binary key k_b and a random parameter φ_b, $\varphi_b \in [0, 2\pi)$, and then he generates a state of OAM state $|B>$. That is,

$$\begin{aligned} |A> &= |\tfrac{\mu}{\sqrt{2}}e^{il\theta}> \otimes|\tfrac{\mu}{\sqrt{2}}e^{-il\theta}e^{i(k_a\pi+\varphi_a)}> \\ &= |\tfrac{\mu}{\sqrt{2}}(e^{il\theta}+e^{i(k_a\pi+\varphi_a-l\theta)})> \\ |B> &= |\tfrac{\mu}{\sqrt{2}}e^{-il\theta}> \otimes|\tfrac{\mu}{\sqrt{2}}e^{il\theta}e^{i(k_b\pi+\varphi_b)}> \\ &= |\tfrac{\mu}{\sqrt{2}}(e^{-il\theta}+e^{i(k_b\pi+\varphi_b+l\theta)})> . \end{aligned} \tag{2}$$

Step 2. Alice and Bob send their signal pulses carrying OAM information to the untrusted third party, Charlie, through a free-space quantum channel.

Step 3. Charlie performs a measurement and records the detection results. The signal pulses sent by Alice and Bob first enter into a 50:50 beam splitter (BS) and then enter into OAM sorters. By calculation, the left output of the BS should be

$$\begin{aligned} |C> &= \tfrac{1}{\sqrt{2}}(|A>+|B>) \\ &= |\tfrac{\mu}{2}[2e^{-il\theta}+e^{i(k_a\pi+\varphi_a+l\theta)}+e^{i(k_b\pi+\varphi_b+l\theta)}]> \\ &= |\tfrac{\mu}{2}[2e^{-il\theta}+(e^{i(k_a\pi+\varphi_a)}+e^{i(k_b\pi+\varphi_b)})e^{il\theta}]> \\ &= |\mu e^{-il\theta}> \otimes|\tfrac{\mu}{2}(e^{i(k_a\pi+\varphi_a)}+e^{i(k_b\pi+\varphi_b)})e^{il\theta}> . \end{aligned} \tag{3}$$

Note that there is an reflection from A to C in BS, and each reflection changes the sign of the topological charge of OAM mode. With the same way, the right output of the BS should be

$$\begin{aligned} |D> &= \tfrac{1}{\sqrt{2}}(|A>-|B>) \\ &= |\tfrac{\mu}{2}[e^{i(k_a\pi+\varphi_a-l\theta)}-e^{i(k_b\pi+\varphi_b-l\theta)}]> \\ &= |\tfrac{\mu}{2}[(e^{i(k_a\pi+\varphi_a)}-e^{i(k_b\pi+\varphi_b)})e^{-il\theta}]> . \end{aligned} \tag{4}$$

Similarly, there is an reflection from B to D in BS.

Here, the OAM sorter is an efficient OAM separation device based on the coordinate transformation method, which is composed of two optical elements R_1, R_2 and a lens to achieve coordinate transformation from Cartesian coordinate (x, y) to logarithmic polar coordinate, The first optical element R_1 is with the transformation phase $\phi_1(x, y)$, where $\phi_1(x, y) = \frac{2a\pi}{f\lambda}[y\arctan(\frac{y}{x}) - x\ln(\frac{\sqrt{x^2+y^2}}{b})+x]$, and a and b are scaling constants [10]. This transformation would introduce some distortions, which can be corrected by the second optical element R_2 [10]. The corrected phase $\phi_2(u, v)$ is expressed as $-\frac{2ab\pi}{f\lambda}\exp(-\frac{u}{a})\cos(\frac{v}{a})$. With the OAM sorter, the OAM modes ℓ and $-\ell$ are separated. Here, only OAM mode ℓ in the detectors D_1 and OAM mode $-\ell$ in D_2 are detected.

Step 3. After Charlie announces the detection result (D_1 click or D_2 click), Alice and Bob declare their random phases φ_a and φ_b.

Step 4. Only if $|\varphi_a - \varphi_b| = 0$ or π, then Alice and Bob retain the result of this communication and generate raw key. When $|\varphi_a - \varphi_b| = 0$, if D_1 click, then $k_a = k_b$; and if D_2 click, then $k_a =!k_b$; On the contrary, when $|\varphi_a - \varphi_b| = \pi$, if D_1 click, then $k_a =!k_b$, and if D_2 click, then $k_a = k_b$.

Step 5. Alice and Bob repeat the above steps until enough raw keys are generated. Then Alice and Bob perform error correction and privacy amplification on the raw key to generate secure key.

The proposed OAM-PM-QKD is a more practical version of PM-QKD. Hence, the key generation rate of the proposed OAM-PM-QKD protocol could be given by the same formula of the PM-QKD [3].

$$R = Q_\mu[1 - f \cdot h(E_\mu) - h(E_\mu^X)]. \tag{5}$$

where Q_μ is the total gain of pulses; E_μ is the total quantum bit error rate(QBER)of pulses; E_μ^X is the phase error rate representing the information leakage; $h(x) = -x\log x-(1-x)\log(1-x)$ is the binary Shannon entropy function; μ is the light intensity; f is the error correction efficiency.

We simulate the performance of OAM-PM-QKD protocol with the parameters given in Table 1.

Table 1: The parameters of the numerical simulation.

Y_0	η_B	f	D	λ	a
8×10^{-8}	14.5%	1.15	$15cm$	$1550nm$	$0.2dB/km$

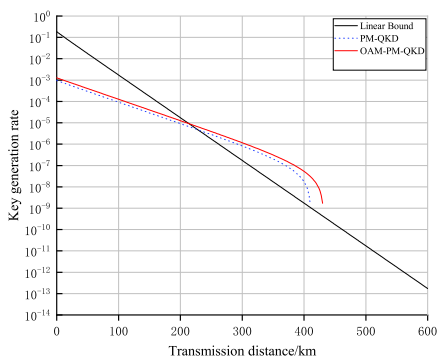

Figure 2: Key generation rate of the proposed OAM-PM-QKD protocol versus the transmission distances, compared with those for original PM-QKD protocol.

The simulation results are shown in Fig.2. The results show the key generation rate of the proposed OAM-PM-QKD protocol versus transmission distance, and com-

pares them with the original PM-QKD protocol under the same conditions without the influence of atmospheric turbulence. From Fig.2, we can find that OAM-PM-QKD is able to exceed the linear key-rate bound when transmission distance exceeds $230km$, and its key generation rate is slightly larger than the original PM-QKD protocol, and the maximum secure transmission distance is also longer.

3 Conclusions

In this paper, We have proposed the PM-QKD protocol based on OAM, where the OAM of photon is used as an information carrier to implement the PM-QKD protocol. We also have analyzed the transmission characteristics of the protocol in atmospheric turbulent channels. Simulation results have shown that the proposed OAM-PM-QKD protocol is able to exceed the linear key-rate bound when transmission distance exceeds $230km$, and its key generation rate is slightly larger than the original PM-QKD protocol, and the maximum secure transmission distance is also longer.

References

[1] Lucamarini M, Yuan Z L, Dynes J F, and Shields A J, Overcoming the rate-distance barrier of quantum key distribution without using quantum repeaters, *Nature*, 557, 400-403 (2018)

[2] Wang X-B, Yu Z-W, and Hu X-L, Twin-field quantum key distribution with large misalignment error, *Phys. Rev. A* 98, 062323 (2018)

[3] Ma X-F, Zeng P, and Zhou H, Phase-matching Quantum Key Distribution, *Phys. Rev. X*, 8, 031043 (2018)

[4] Federico M, and Spedalieri, Quantum key distribution without reference frame alignment:Exploiting photon orbital angular momentum, *Opt. Commun.*, 260(1):340-346 (2006)

[5] Bouchard Frdric, Alicia S, and Khabat H, Round-robin differential-phase-shift quantum key distribution with twisted photons, *Phys. Rev. A*, 98(1):010301 (2018)

[6] Mirhosseini M, Magaa-Loaiza O S, and O'Sullivan M N, High-dimensional quantum cryptography with twisted light, *New J. Phys.*, 17(3):033033 (2015)

[7] Wang L, and Zhao S-M, Free-space measurement-device-independent quantum-key-distribution protocol using decoy states with orbital angular momentum, *Chin. Phys. B*, 24(12):242-249 (2015)

[8] Shen Z-G, Wang L, and Mao Q-P, Round-Robin differential phase shift quantum key distribution protocol based on orbital angular momentum, *Opt. J.*, 39(02):368-376 (2019)

[9] Meng, Zelin, and Hong Lai. Twin-field quantum key distribution based on twisted photon. *Phys. Lett. A*,384(16): 126322 (2020)

[10] Berkhout G C.G, Lavery M P.J, Courtial J and Beijersbergen M W. Efficient separating of orbital angular momentum states of light. *Phys. Rev. Lett.* 105:153601 (2010)