Li et al. *EPJ Quantum Technology* (2024) 11:40
https://doi.org/10.1140/epjqt/s40507-024-00251-z

EPJ Quantum Technology
a SpringerOpen Journal

EPJ.org

RESEARCH Open Access

An intelligent threshold selection method to improve orbital angular momentum-encoded quantum key distribution under turbulence

Jia-Hao Li[1,3], Jie Tang[1], Xing-Yu Wang[1], Yang Xue[2], Hui-Cun Yu[1], Zhi-Feng Deng[1], Yue-Xiang Cao[1], Ying Liu[1], Dan Wu[1], Hao-Ran Hu[1], Ya Wang[1], Hua-Zhi Lun[1], Jia-Hua Wei[1], Bo Zhang[1], Bo Liu[3*] and Lei Shi[1*]

*Correspondence:
liubo08@nudt.edu.cn;
slfly2012@163.com
[3]College of Advanced Interdisciplinary Studies, National University of Defense Technology, Changsha, China
[1]Information and Navigation College, Air Force Engineering University, Xi'an, China
Full list of author information is available at the end of the article

Abstract

High-dimensional quantum key distribution (HD-QKD) encoded by orbital angular momentum (OAM) presents significant advantages in terms of information capacity. However, perturbations caused by free-space atmospheric turbulence decrease the performance of the system by introducing random fluctuations in the transmittance of OAM photons. Currently, the theoretical performance analysis of OAM-encoded QKD systems exists a gap when concerning the statistical distribution under the free-space link. In this article, we analyzed the security of QKD systems by combining probability distribution of transmission coefficient (PDTC) of OAM with decoy-state BB84 method. To address the problem that the invalid key rate is calculated in the part transmittance interval of the post-processing process, an intelligent threshold method based on neural network is proposed to improve OAM-encoded QKD, which aims to conserve computing resources and enhance system efficiency. Our findings reveal that the ratio of root mean square (RMS) OAM-beam radius to Fried constant plays a crucial role in ensuring secure key generation. Meanwhile, the training error of neural network is at the magnitude around 10^{-3}, indicating the ability to predict optimization parameters quickly and accurately. Our work contributes to the advancement of parameter optimization and prediction for free-space OAM-encoded HD-QKD systems. Furthermore, it provides valuable theoretical insights to support the development of free-space experimental setups.

Keywords: Statistical distribution; High-dimensional quantum key distribution; Threshold selection; Neural network

1 Introduction

By utilizing the principles of quantum mechanics, quantum cryptography ensures secure key distribution by focusing on physical properties rather than computational complexity. Unlike traditional cryptographic approaches, quantum cryptography achieves provable security at the level of information theory. As the core of quantum cryptography, quantum key distribution (QKD) establishes a bit string of common true random bits between two legitimate parties, to realize secure communication combined with One-Time Pad (OTP) Vernam encryption algorithm [1–3]. Currently, most practical QKD uses the degree of

Springer

freedom such as polarization and phase of photon, the information capacity is limited to 1 bit per photon due to the intrinsically bounded Hilbert space [4–8]. To break through the system information entropy threshold, high-dimensional QKD (HD-QKD) offers improved communication capacity and enhanced noise resilience [9–14]. One common approach to achieve HD-QKD is through the utilization of the orbital angular momentum (OAM) of photons [15–19]. The OAM freedom allows photons to be mapped to an infinite dimensional Hilbert space, providing an effective resource for implementing HD-QKD.

Optical waves carrying OAM in the form of a helical phase front can be adversely affected by turbulence, leading to distortions. These distortions cause the transmission coefficient of the optical OAM channel to fluctuate randomly, resulting in random degradation of the transmitted signal. However, the existing statistical distribution models primarily focus on describing the intensity fluctuations of optical waves, which is insufficient for accurately representing the complex nature of the transmission coefficient fluctuations in turbulent optical OAM channels. Characterizing these fluctuations in the transmission coefficient is crucial for analyzing the security of OAM-encoded QKD systems [20].

Currently, there is a notable absence of comprehensive theoretical analysis on the integration of the probability distribution of transmission coefficient (PDTC) of OAM and QKD in atmospheric turbulence. The fluctuations in transmittance resulting from atmospheric turbulence lead to time-varying quantum bit error rate (QBER), posing a significant challenge in quantum communication systems [21, 22]. In order to address the challenge, enhancing the signal-to-noise ratio (SNR) through post-selection with high transmittance has been proposed as a solution [23–26]. This approach involves optimizing the transmittance threshold after receiving all signals. However, the calculation method often imposes a substantial computational burden due to its complexity. To mitigate the computational challenge and enhance system performance, optimizing QKD system parameters through machine learning techniques has emerged as a promising strategy [27–29]. By utilizing neural network methods for parameter optimization, it becomes possible to improve operational efficiency, facilitate parameter prediction, and ultimately enhance the overall performance of the system [30]. Under the grand vision of promoting the realization of global quantum Internet [31–33], the intelligent methodology holds particular significance for applications such as airborne free space QKD missions, where speed, accuracy, and reliability are paramount considerations.

The paper is organized as follows: In Sect. 2, we begin by generating random samples of transmission coefficients using Monte Carlo simulation. Based on these samples, a suitable transmission coefficient statistical distribution model is proposed which accurately captures the characteristics of turbulent optical OAM channels. Subsequently, we establish a basic framework for calculating the key rate of OAM-encoded QKD systems in Sect. 3. Finally, an artificial neural network method is used to forecast the optimal transmittance threshold to improve system in Sect. 4. The conclusions of the present paper are given in Sect. 5.

2 Preliminaries

Characterization of the statistical distribution of OAM transmission in turbulence is the primary task of studying OAM-encoded QKD. In this section, we will use Monte Carlo simulation and dual Johnsom S_B distribution to get the PDTC model of OAM.

2.1 Instantaneous transmittance of OAM channels

Given the initial normalization of light intensity, the transmission coefficient of OAM is directly correlated with the received optical power. However, it is essential to note a fundamental distinction between the mathematical models for detecting power in OAM optical channels and traditional free-space channels. The variance implies that the probability distribution function governing light intensity fluctuations induced by atmospheric turbulence may not be applicable when describing the fluctuation of transmission coefficients in turbulent OAM optical channels. Unlike classical Gaussian light, the transmission of OAM in turbulent conditions does not conform to the commonly employed log-normal and Gamma-Gamma distribution models.

In general, establishing a statistical distribution model directly tailored for turbulent optical OAM channel transmission coefficients through analytical mathematical derivation poses significant challenges. To overcome the limitation, our approach involves utilizing Monte Carlo simulation to generate a random sample of transmission coefficients. This methodology enables us to propose a suitable distribution model that accurately reflects the fluctuations in the transmission coefficient. Drawing insights from existing Ref. [20], we begin by theoretically deriving the instantaneous transmission coefficient:

$$\eta(t) = \int_0^\infty \hat{\rho}(\hat{r}) W(\hat{r} r_0)\, d\hat{r}, \tag{1}$$

with

$$\hat{\rho}(\hat{r}) = \hat{r}\left(\frac{2\sqrt{|l|+1}}{\Omega}\right)^2 \frac{1}{|l|!}\left[\frac{\hat{r}\sqrt{2(|l|+1)}}{\Omega}\right]^{2|l|} \exp\left[-\frac{2(|l|+1)\hat{r}^2}{\Omega^2}\right] \tag{2}$$

$$W(r) = (2\pi)^{-2}\left|\int_0^{2\pi} d\theta \exp\left[i\varphi(r,\theta)\right]\right|^2, \tag{3}$$

where $\hat{r} = r/r_0$ represents the ratio of Laguerre-Gaussian (LG) beam width r to the Fried constant r_0, $\Omega = w_z\sqrt{(|l|+1)}/r_0$ denotes the nondimensional ratio between the root-mean-square(RMS) OAM-beam radius and the Fried constant, and the RMS OAM-beam radius reflects the divergence characteristic [34]. l is the OAM index. The OAM beam under consideration has a radial index set to zero. $w_z = w_0\sqrt{1 + z^2/z_R^2}$, w_0 is the beam waist, $z_R = 0.5kw_0^2$ is the Rayleigh range (here $k = 2\pi/\lambda$, k and λ represent wavenumber and wavelength respectively).

The aforementioned data can be provided based on the actual scenario. The crucial aspect revolves around the implementation of the random phase screen $\varphi(r,\theta)$. The random generation of phase screens based on sparse spectrum is a commonly employed method due to its ability to be easily adapted to uniform spatial sampling in polar coordinates. The procedure for realizing $\varphi(r,\theta)$ through sparse-spectrum-based method and Monte Carlo simulation is detailed in Appendix A.1.

2.2 Model of PDTC

In order to conduct a mathematical characterization of the PDTC, a dual Johnson S_B distribution with four independent control parameters is fitted to the random fluctuations of the measured signal in the turbulent optical OAM channel. The probability density func-

tion (PDF) of dual Johnson S_B distribution can be expressed as:

$$P_d(\eta|\gamma_1,\delta_1,\gamma_2,\delta_2) = \frac{1}{2}\left[P_J(\eta|\gamma_1,\delta_1) + P_J(\eta|\gamma_2,\delta_2)\right], \tag{4}$$

with

$$P_J(\eta|\gamma,\delta) = \frac{\delta}{\sqrt{2\pi}}\frac{1}{\eta(1-\eta)}\exp\left\{-\frac{1}{2}\left[\gamma + \delta\ln\left(\frac{\eta}{1-\eta}\right)\right]^2\right\}, \tag{5}$$

where $P_J(\eta|\gamma,\delta)$ is the PDF of Johnson S_B distribution. The four independent control parameters $\gamma_1,\gamma_2,\delta_1,\delta_2 > 0$, statistically characterize the simulated samples. For practical application of the dual Johnson S_B distribution, it is advisable to establish a direct correlation between four control parameters and the propagation conditions along with OAM modes. The connection between (Ω, l, r_0) and $(\gamma_1,\delta_1,\gamma_2,\delta_2)$ can be perceived as a mapping from three to four dimensions. While formulating a mathematical expression to articulate the mapping remains challenges, Monte Carlo simulations and probability distribution fitting utilizing maximum likelihood estimation (MLE) can elucidate the relationship.

To further investigate the mechanism of how Ω and r_0 influence the PDTC, we analyze the PDF of transmission coefficients under different Ω and r_0 conditions. As shown in Fig. 1, when keeping Ω constant and varying r_0, the PDF curve of the transmission coefficient exhibits a similar trend with slight differences. However, when keeping r_0 constant and varying Ω, there is a significant discrepancy in the PDF curve. It indicates that the impact of Ω on the PDF of the transmission coefficient is stronger than r_0. Moreover, as Ω increases, the PDF curve's "peak" gradually shifts to the left, indicating a decrease in the probability of achieving high transmittance η. It suggests that turbulence-induced channel attenuation is intensified. Notably, when Ω is close to 1 (as depicted in Fig. 1(b)), the PDF curve exhibits a pronounced tailing phenomenon that is difficult to describe with existing mathematical models.

Considering the transport properties of OAM in the atmosphere and practical implementation, it is more reasonable to set $r_0 = 10$ cm. As depicted in Fig. 2(a), the PDF curves of different OAM indices are essentially merged, suggesting that when Ω is small, l has no discernible influence on the PDF. However, in Fig. 2(b) and Fig. 2(c), when $\Omega \geq 1$, differences between the curves are evident, indicating that the PDTC of OAM exhibits a notable state-dependent effect. The state-dependent turbulence in this scenario comes from two

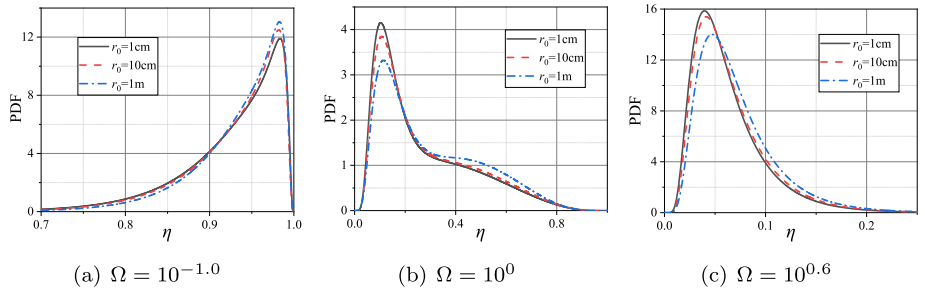
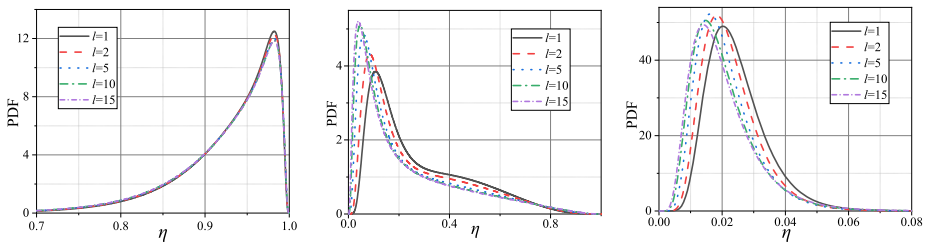


Figure 1 PDFs of transmission coefficient η with $l \equiv 1$ and different Ω and r_0. (a) $\Omega = 10^{-1.0}$; (b) $\Omega = 10^{0}$; (c) $\Omega = 10^{0.6}$



(a) $\Omega = 10^{-1.0}$ (b) $\Omega = 10^{0}$ (c) $\Omega = 10^{0.6}$

Figure 2 PDFs of transmission coefficient η with $r_0 \equiv 10$ cm and different Ω and l. (a) $\Omega = 10^{-1.0}$; (b) $\Omega = 10^{0}$; (c) $\Omega = 10^{0.6}$

folds: (1) high order OAMs have larger beam cross section which leads to a worse turbulence; (2) high order OAMs have multi-fold phase structures which are more sensitive to phase distortions.

3 Secure key rate analysis

Currently, the relationship between the security key generation rate R and the transmittance coefficient η in turbulent optical OAM channels lacks theoretical substantiation. Under the premise of fixed QKD system parameters, building upon the analysis in Sect. 2 and incorporating the Gottesman-Lo-Lütkenhaus-Preskill (GLLP) formula, we formulate the key rate of the decoy-state BB84 protocol as a function of $R(\eta)$. Consequently, assessing the system security rate in turbulent channels involves determining the integral of $R(\eta)$ over the probability distribution of η.

Ratewise integration is a prevalent method for determining the secure key rate, involving the integration of $R(\eta)$ over the entire range of the PDF, incorporating all available information regarding the channel transmission probability distribution. Initially, we examine the asymptotic scenario of transmitting an infinite number of pulses. As depicted in Fig. 1 and Fig. 2, we have measured the channel transmittance η corresponding to each signal transmission period and acquired comprehensive transmittance information. The rate of the ratewise integration model can be expressed as:

$$R^{\text{Ratewise}} = \int_0^1 R(\eta)P(\eta)\,d\eta. \tag{6}$$

As the spatial degree of freedom of the light field, OAM possesses the ability to map an infinite-dimensional Hilbert space. In the quantum state space of high dimensions, the SUP basis and the OAM basis form two mutually unbiased bases (MUBs), which guarantees the unconditional security of QKD. OAM basis is composed of different OAM states, and the Fourier conjugate SUP basis consists of an equal superposition of OAM states with fixed relative phase between adjacent OAM components. The OAM basis and SUP basis can be represented as:

$$\begin{aligned} \{|\varphi_{\text{OAM}}\rangle\} &= \{|-l\rangle, |-l+1\rangle, \ldots, |0\rangle, \ldots, |l-1\rangle, |l\rangle\} \\ \{|\psi_{\text{SUP}}\rangle\} &= \left\{ \frac{1}{\sqrt{d}} \sum_{l=-L}^{L} \exp\left(i\frac{jl2\pi}{d}\right) |\varphi_{\text{OAM}}\rangle \right\} \end{aligned} \tag{7}$$

Table 1 Parameters used for the numerical simulation of OAM-encoded HD-QKD

Parameters	Value
Dark count rate Y_0	1×10^{-5} (per signal)
Detector efficiency η_d	0.25
Misalignment e_d	0.03
Error-correction efficiency f	1.22
Signal wavelength λ	1550 nm
Signal state intensity μ	0.3
Decoy state intensity v	0.05

where d is the dimension of the Hilbert space and L is the maximum OAM quantum number in use, which satisfies the relation $2L + 1 = d$. Subsequently, Bob uses the results with OAM basis as the key bits and the results with SUP basis as the testing bits, and then they testify the security of the key distribution. After error correction and privacy amplification, they can distill a secure key [35]. For weak coherent sources (WCS), the secure key rate of decoy-state HD-QKD can be estimated by [16]:

$$R \geq q_m \left\{ -f_{\mathrm{EC}}\left(E_\mu^{\mathrm{OAM}}\right) Q_\mu^{\mathrm{OAM}} H_d\left(E_\mu^{\mathrm{OAM}}\right) + Q_1^{\mathrm{OAM}}\left[\log_2 d - H_d\left(e_1^{\mathrm{SUP}}\right)\right] \right\} \tag{8}$$

where q_m represents the probability of choosing basis and depends on the QKD protocol. $f_{\mathrm{EC}}(E_\mu^{\mathrm{OAM}})$ is the error correction efficiency of the signal state. Q_μ^{OAM} and E_μ^{OAM} are the gain and QBER of the signal states, respectively. Q_1^{OAM} and e_1^{SUP} are the gain and the error rate of the single-photon states, which can be estimated using decoy-state, see Appendix A.2 for detailed analysis. $H_d(x) = -(1-x)\log_2(1-x) - x\log_2[x/(d-1)]$ is the d-dimensional Shannon entropy.

Due to the rotation invariance of the vortex light field, it effectively avoids the problem of the reference frame alignment, and provides a new coding scheme for the construction of high-speed and stable mobile quantum communication networks. The most likely application in the future is, for example, the scenario of drone-based quantum communication, with a typical distance range of kilometers. According to the above theoretical analysis, targeting 10 km free space link scenarios, the simulation method is used to analyze the performance of OAM-encoded HD-QKD system. The settings of the QKD system parameters [36] are outlined in Table 1.

We initially simulate the impact of the OAM index on the security key rate. Figure 3 illustrates the correlation between Ω and the security key rate R. As Ω increases, the security key rate exhibits a gradual decline, suggesting that Ω to some degree reflects the disturbance and attenuation characteristics of atmospheric turbulence channel. Nonetheless, variations in the OAM index l result in negligible effects on the secure key rate. Therefore, it can be further considered to apply a high-dimensional quantum system to improve the information capacity under the condition of changing Ω, especially when $\Omega \leq 1$.

Figure 4 depicts the correlation between the security key rate R and Ω within a d-dimensional QKD system. The figure exclusively illustrates the trend in the variation of the security key rate surface for d-dimensional QKD as Ω changes. From the visualization, it is evident that with an increase in the dimensionality of the QKD system, both the security key rate and the transmission distance rise. The observation suggests that the QKD system can effectively leverage the benefits of high-dimensional coding when Ω is considered a variable. Due to the existence of state-dependent diffraction (SDD) [35] and other effects in high-dimensional QKD system transmission in the atmosphere, the receiving efficiency

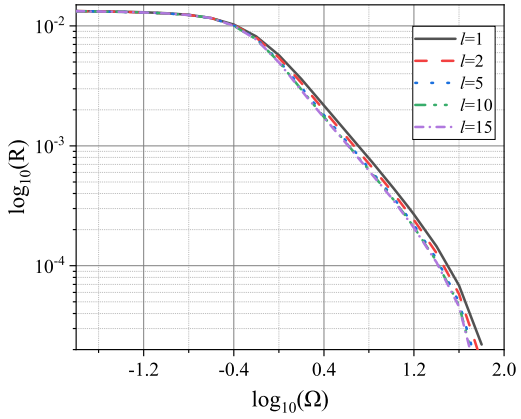


Figure 3 Secure key rate R of Ω with different l

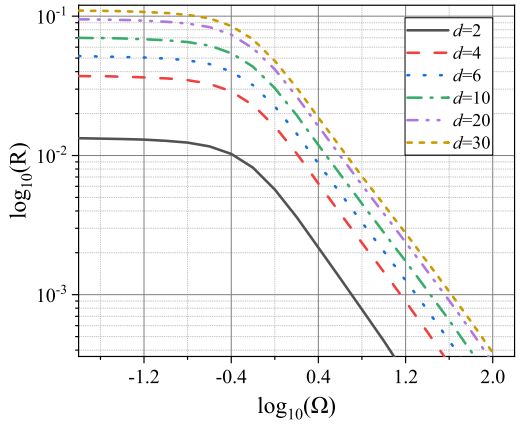


Figure 4 Secure key rate R of Ω with different dimension d

mismatch leads to security vulnerabilities and security key rate decrease. According to the results of Fig. 3 and Fig. 4, we can use more high-dimensional quantum systems in the scenarios of minor Ω, because OAM index l has a subtle influence on key generation at this time. To get closer to practicality, the finite-size effect is analyzed in Appendix A.3.

The above analysis provides a theoretical basis for the performance optimization method of threshold selection. First, by combining the transmission PDF of OAM with HD-QKD, a theoretical model is found for the statistical distribution of OAM-encoded QKD; Second, the advantages of HD-QKD encoding are explored in incorporating the finite-size effects, and a theoretical reference is provided for the practical airborne application of OAM-encoded QKD.

4 Performance optimization

In addressing the challenges posed by random fluctuations in channel transmission and low key generation rates resulting from atmospheric turbulence in free-space experiments, this section presents strategies and recommendations aimed at enhancing system performance. Through the implementation of optimal threshold selection, computational

resource consumption is minimized. Additionally, a neural network model is employed to train and predict discrete datasets, thereby enhancing operational efficiency.

4.1 Threshold selection method

During the process of ratewise integration method, there are instances where key generation can be negligible under certain transmission efficiency conditions due to the PDTC in turbulent OAM optical channels. However, in practical scenarios, the data segment necessitates post-processing, leading to a squandering of computational resources. Considering the time-varying transmission characteristics induced by free-space atmospheric turbulence, employing threshold selection method as a simplified method to filter information and post-selection becomes imperative. This approach helps diminish the volume of data computation, thereby enhancing the secure key rate per pulse and overall system performance. The simplified security key rate for threshold selection can be expressed as follows:

$$R^{\text{Simplified}} = \int_{\eta_T}^{1} R(\eta)P(\eta)\,d\eta. \tag{9}$$

According to the Eq. (9), adjusting the threshold value η_T and observing the resultant alteration in the security key generation rate is imperative. As depicted in Fig. 5, when the OAM index $l = 1$, the security key rate that we set the threshold is almost the same as the static value obtained by the ratewise integration in the initial range, followed by a marked decline. We can find an optimal η_T according to the actual scenario to simplify the calculation, for example, in the scenarios of minor Ω, opting for a higher threshold can be advantageous in enhancing the efficiency of data processing.

In order to further depict the selection of thresholds more vividly, we set up three-dimensional images of Ω, l and η_T to visually observe the effects of different variables on η_T. As illustrated in Fig. 6(a), it is evident that the impact of Ω on η_T surpasses that of l, with the optimal threshold gradually diminishing as Ω increases, aligning with the findings in Fig. 5. However, when Ω exceeds 1, a more intricate relationship among the

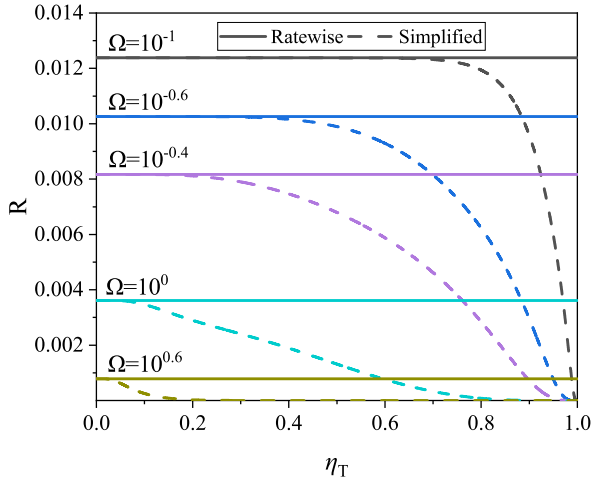
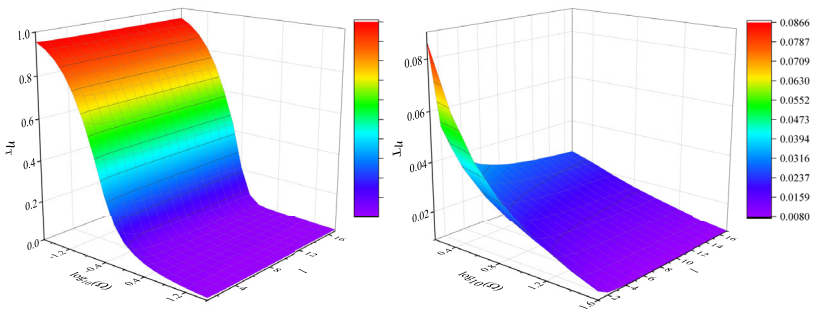


Figure 5 Secure key rate R of ratewise integration method and threshold selection simplified method



(a) $-2 \leq \log_{10}(\Omega) \leq 2$ (b) $0 \leq \log_{10}(\Omega) \leq 2$

Figure 6 Optimal threshold η_T under different Ω and l conditions. (a) $-2 \leq \log_{10}(\Omega) \leq 2$; (b) $0 \leq \log_{10}(\Omega) \leq 2$

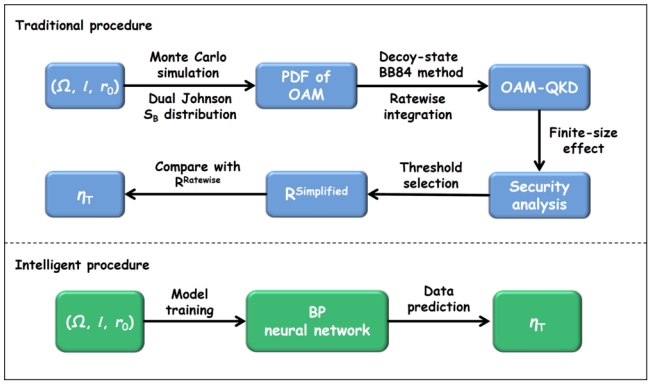


Figure 7 A comparison of traditional and intelligent procedures

three variables is discerned, as depicted in Fig. 6(b), signifying a shift in their interplay. At this juncture, both l and Ω exert a significant influence on the determination of η_T, and with the escalation of l, the selection of the optimal threshold declines correspondingly. Consequently, when Ω is less than 1, the influence of l on the selection of the optimal threshold may be disregarded. Conversely, when Ω surpasses 1, due consideration must be given to the impact of l on the optimal threshold selection.

4.2 Neural network method

The PDTC of OAM in turbulence is based on data obtained through Monte Carlo simulation, which is discrete and exhibits a degree of volatility. To further enhance the optimization of the threshold, an adaptive threshold selection method employing an artificial neural network is proposed. The error back propagation (BP) neural network, as a widely utilized model, has been chosen for optimization and prediction.

Based on the analysis in Sect. 2, 3 and 4.1, Fig. 7 shows the procedure of obtaining the optimal threshold η_T from the initial parameters (Ω, l, r_0). This procedure involves a clear concept, but it entails significant computational complexity. By employing intelligent methods to train the initial parameters, it is possible to not only obtain the final result η_T but also achieve data prediction, showcasing its practical advantages.

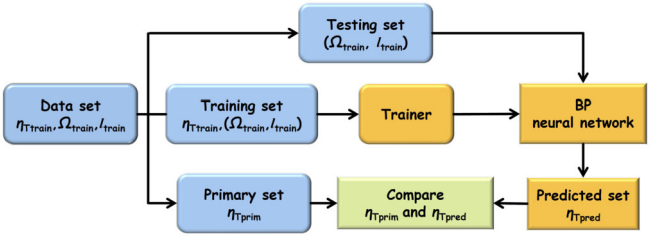


Figure 8 The process of model training and parameter prediction by BP neural network

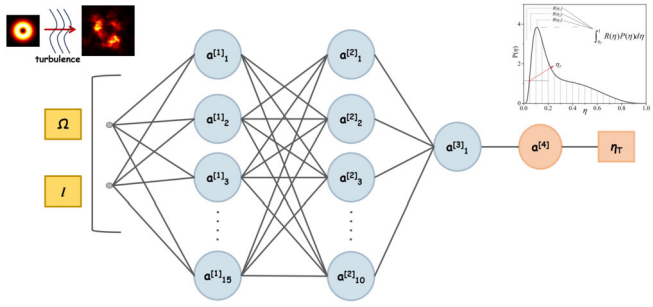


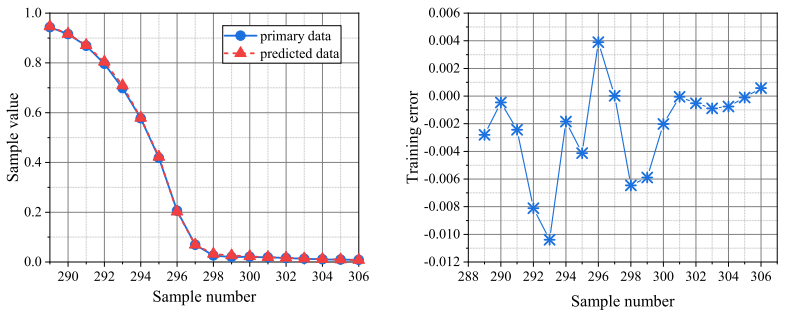
Figure 9 The structure of BP neural network

The process of using BP neural network to achieve model training and parameter prediction is shown in Fig. 8. First, the data set is divided into three parts, the training set, the testing set, and the primary set. The BP neural network model is obtained by inputting the large-capacity data which can embody the data characteristics into the trainer. In order to verify the performance of the model, the testing set is brought into the network for calculation, and the predicted set is obtained. Finally, the data of the predicted set and the primary set are compared to judge the performance of the system.

The network architecture, as illustrated in Fig. 9. The parameters of the input layer represent the main characteristics of OAM and turbulence, which shows the effect of random disturbance. The number of hidden layers is 3, and the number of neurons is 15, 10 and 1, respectively. The data of the output layer is the optimal threshold η_T. The transfer function for the hidden layer is the tansig transfer function, while the output layer employs a purelin function. The learning algorithm employed is the Levenberg-Marquardt (LM) variable gradient algorithm, with the mean square error (MSE) function used as the performance metric. The training process includes 2000 iterations, with a learning rate set at 0.01.

The dataset with the optimal threshold η_T of 18*17 samples has been constructed, where the ratio Ω of the RMS OAM-beam radius and Fried constant ranges from 10^{-2} to $10^{1.4}$ and the OAM index l varies from 0 to 16. (η_T, Ω, l) $(2 \times 18 \times 16)$ is selected as the training set to train the neural network model. The last 18 data $[l = 16, \Omega = 10^{-2.0} \sim 10^{1.4}]$ are selected for prediction. The Imitative effect and training error between the predicted data and the primary data are compared, as shown in Fig. 10.

Figure 10(a) shows the fitting curve. The horizontal axis represents the number of samples selected by the neural network, while the vertical axis illustrates the sample value of the optimal threshold selection. By standardizing the data in training, normalization fa-



(a) Imitative effect (b) Training error

Figure 10 Optimal threshold prediction results using BP neural network. (a) Imitative effect; (b) Training error

cilitates effective data processing and contributes to faster convergence during program execution. The practice is fundamental for ensuring that the neural network can efficiently learn and adapt to the given dataset, ultimately improving its performance in prediction and analysis tasks. The solid blue line with dots corresponds to the primary data, whereas the solid red lines with triangles depict the predicted data. Figure 10(b) shows the training error curve, and the ordinate represents the training error between the model's predicted value and the primary data value.

From Fig. 10(a), it can be analyzed that the change pattern of the primary data and the predicted data follows a periodic trend. The imitative effect can be attributed to the method of selecting the optimal threshold during the collection of original data, where the thresholds are chosen in increasing order of the same OAM index l. In other words, when selecting Ω for a specific OAM index, the subsequent OAM index with Ω values is considered until 18 OAM index points have been covered.

The fitting curve effect of the predicted data generated by the BP neural network aligns closely with the primary data curve, underscoring the model's accuracy in capturing and predicting the trends within the dataset. Moreover, Fig. 10(b) reveals that the training error of the sample set is around 10^{-3}, indicating the high prediction accuracy of the neural network. It should be noted that in the scenario of high Ω, the optimal threshold accuracy at this time reaches 1×10^{-2}, so the training error at this time is also an important basis for judging the network performance. The training error of the last three predicted data is in the order of 10^{-4}, which proves the training effect of the network. The intelligent model can effectively support the adaptive optimal threshold selection in the OAM-encoded QKD system, enhancing data processing speed and providing valuable guidance for system parameter prediction and optimization.

5 Conclusion

The analysis of the statistical distribution of OAM transmission characteristics in the atmosphere plays a pivotal role in advancing high-dimensional quantum communication. The benefits offered by OAM-encoded QKD, such as communication capacity and rotationally invariant property, have propelled its application in short-distance information transmission within local hotspots. Due to the complex attenuation and disturbance caused by OAM transmission in atmospheric turbulence, it is difficult to use classical mathematical models to characterize the statistical distribution of transmission charac-

teristics at the receiver. Currently, there remains a gap in comprehensive theoretical analysis concerning the statistical distribution of OAM-encoded QKD in free space. In this paper, the transmittance PDF of OAM transmitted in the atmosphere is integrated with the HD-QKD secure key rate formula, incorporating the finite-size effects to effectively evaluate system performance. The results show that the ratio Ω of RMS OAM-beam radius to Fried constant plays the most prominent role in determining control parameters and security key generation. If the value of Ω exceeds 1, the effect of OAM index l cannot be ignored. Furthermore, the study briefly explores the coding advantages of HD-QKD, shedding light on the potential benefits and applications of high-dimensional quantum key distribution in secure communication protocols. The comprehensive analysis contributes valuable insights into the optimization and performance enhancement of OAM-encoded QKD systems in challenging atmospheric environments.

Aiming at the problem of the free space OAM-encoded QKD system that the invalid key rate is calculated in the part transmittance interval of the post-processing process and the high-dimensional protocol needs to accumulate a large amount of data, the method combining threshold selection and neural network is used to train discrete data points. The results indicate a close alignment between the original data curve and the predicted data, with a training error around 10^{-3}. This achievement signifies the model's capability to perform intelligent parameter prediction effectively. Furthermore, the model's success in achieving high accuracy showcases its potential to enhance system running speed and key distribution performance. Ultimately, this approach offers a practical solution for the intelligent advancement of quantum secure communication systems.

Appendix

A.1 Generation of random phase screen

It should be emphasized that $\varphi(r,\theta)$ in Eq. (3) actually denotes the phase perturbation described via a random phase screen, resulting in $\eta(t)$ taking on a random value. Clearly, the key to obtaining random samples of $\eta(t)$ is to acquire a random implementation of the phase screen $\varphi(r,\theta)$. Due to the advantageous feature of integration over θ, we have opted for sparse-spectrum-based method [37] to generate the phase screen:

$$\varphi(\vec{r}) = \mathrm{Re}\left[\sum_{n=1}^{N} a_n \exp(i\vec{K}\cdot\vec{r})\right], \tag{A1}$$

where a_n represents a random complex amplitude, $\vec{r} = (r,\theta)$ is a position vector in a two-dimensional plane, and Re(z) denotes the real part of z. $\vec{K}$ signifies a random wavenumber vector, the probability density function (PDF) for the magnitude of vector $\vec{K}$ is:

$$p_n(K) = \frac{5}{3}\frac{1}{K_{n-1}^{-5/3} - K_n^{-5/3}} K^{-8/3}, \tag{A2}$$

where $K_{n-1} \le K \le K_n$, $K_n = \kappa_0 \exp[(n/N)\ln(\kappa_m/\kappa_0)]$ and $1 \le n \le N$, $\kappa_0 = 2\pi/L_0$, $\kappa_m = 2\pi/l_0$, l_0 and L_0 are the inner and outer scales of turbulence, respectively. The direction angle of vector $\vec{K}$ is assumed to follow a uniform distribution between π and $-\pi$. Moreover, a_n is a random complex amplitude that follows a normal distribution and obeys:

$$\langle a_n\rangle = 0, \langle a_n a_m\rangle = 0, \left\langle a_n a_m^*\right\rangle = 3.695 r_0^{-5/3}\left(K_{n-1}^{-5/3} - K_n^{-5/3}\right)\delta_{mn}, \tag{A3}$$

where the angle brackets indicate statistical averages, and $\delta_{mn} = 1$ if $m = n$ and $\delta_{mn} = 0$ otherwise. By utilizing N to generate a random implementation of a_n and $\vec{K}$, it becomes straightforward to calculate $\varphi(r,\theta)$ at any given position $\vec{r} = (r,\theta)$ based on Eq. (A1).

It is noteworthy that in the Monte Carlo simulation, to align our spectral intervals with the standard pure Kolmogorov spectrum, we have set the inner and outer scales of the turbulence to 1 mm and 100 m, respectively.

A.2 Decoy-state HD-QKD rate model

For decoy-state HD-QKD system, the total system transmittance η_{sys} of single photon signal consists of the transmission efficiency η and detector efficiency η_d. Thus, Q_μ^{OAM} can be calculated by:

$$Q_\mu^{\text{OAM}} = Y_0 + 1 - \mathrm{e}^{-\mu\eta_{\text{sys}}}, \tag{B1}$$

where $Y_0 = 2p_d$ is the yield when Alice does not send a photon. p_d is the dark count of the detector. μ and ν are the mean photon number of signal state and decoy state respectively. Meanwhile, E_μ^{OAM} can be given as

$$E_\mu^{\text{OAM}} = \frac{e_0 Y_0 + e_d(Q_\mu^{\text{OAM}} - Y_0)}{Q_\mu^{\text{OAM}}}. \tag{B2}$$

Different from the general two-dimensional QKD system, $e_0 = (d-1)/d$ is the error rate of the dark count in HD-QKD. By using "vacuum + weak decoy state" method, the yield and the error rate of the single-photon states Y_1^{OAM} and e_1^{SUP} can be estimated by:

$$Y_1^{\text{OAM}} \geq \frac{\mu}{\mu\nu - \nu^2}\left(Q_\nu^{\text{OAM}} e^\nu - Q_\mu^{\text{OAM}} e^\mu \frac{\nu^2}{\mu^2} - \frac{\mu^2 - \nu^2}{\mu^2} Y_0\right), \tag{B3}$$

$$e_1^{\text{SUP}} \leq \frac{E_\nu^{\text{SUP}} Q_\nu^{\text{SUP}} e^\nu - e_0 Y_0}{Y_1^{L,\nu,0}\nu}. \tag{B4}$$

A.3 Finite-size analysis

Due to the disparity between HD-QKD and 2D-QKD in terms of key analysis, we conducted a security analysis of HD-QKD under asymptotic conditions. However, in practical QKD systems, the number of pulses transmitted by the quantum signal is limited, leading to statistical fluctuations between observed and measured values. To further validate the security of the HD-QKD system, it becomes crucial to analyze the finite-size effects resulting from statistical fluctuations. To obtain the expected confidence interval of the observed parameter, the Chernoff inequality is employed [38]. The upper and lower limits of the confidence interval $E^U[\zeta]$ and $E^L[\zeta]$ can be expressed as:

$$E^L[\zeta] = \frac{\zeta}{1+\delta^L}, \qquad E^U[\zeta] = \frac{\zeta}{1-\delta^U}, \tag{C1}$$

with

$$\left[\frac{\mathrm{e}^{\delta^L}}{(1+\delta^L)^{1+\delta^L}}\right]^{\frac{\zeta}{1+\delta^L}} = \frac{\varepsilon}{2}, \qquad \left[\frac{\mathrm{e}^{-\delta^U}}{(1-\delta^U)^{1-\delta^U}}\right]^{\frac{\zeta}{1-\delta^U}} = \frac{\varepsilon}{2}, \tag{C2}$$

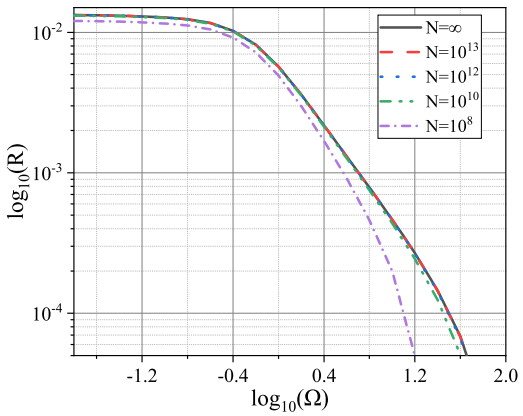


Figure 11 Secure key rate R of Ω with finite-size effects

where $\zeta > 0$ is an observed value, δ is the statistical fluctuation which used to represent the estimated interval of the expected value. ε is the failure probability to estimate the confidence interval of the expected value.

Based on Eq. (C1)-(C2) and Eq. (B3)-(B4), the upper and lower bounds of the statistical fluctuations for Y_1^{OAM} and e_1^{SUP} can be obtained. The security key length of OAM-basis of HD-QKD system under finite-size effect is obtained:

$$[K^{\mathrm{OAM},L} \geq M_{1\mu}^{\mathrm{OAM},L}\left[1 - H_d\left(e_{1\mu}^{\mathrm{SUP},U}\right)\right] - M_{\mu}^{\mathrm{OAM}} f_{\mathrm{EC}}\left(E_{\mu}^{\mathrm{OAM},U}\right) H_d\left(E_{\mu}^{\mathrm{OAM},U}\right) \tag{C3}$$

where $M_{1\mu}^{\mathrm{OAM},L}$ is the lower limit number of OAM-basis sifted key from the single-photon signal state. M_{μ}^{OAM} is the number of OAM-basis sifted key from the overall signal state. $e_{1\mu}^{\mathrm{SUP},U}$ is the upper limit of the phase error rate. $E_{\mu}^{\mathrm{OAM},U}$ is the upper limit of the QBER in the OAM-basis sifted key. Therefore, for a given data size N, the final secret key rate of the practical HD-QKD system is:

$$R^{\text{Finite-size}}(\eta, N) \geq \frac{K^{\mathrm{OAM},L}}{N}. \tag{C4}$$

Consequently, the formula for the security key rate of the system with finite-size effects can be recalculated:

$$R^{\text{Finite-size}} = \int_0^1 R^{\text{Finite-size}}(\eta, N) P(\eta)\, d\eta. \tag{C5}$$

Figure 11 examines the security key rate under finite-size effects. The figure presents a comparison of key rate curves across various data sizes and asymptotic ($N = \infty$) conditions. It is evident from the illustration that as the data size gradually increases, the security key rate follows suit. When the number of quantum pulses N reaches or exceeds 10^{12}, the key rate curve closely aligns with the asymptotic case. Taking into account practical implementation and cost optimization, we can select $N = 10^{12}$ as the pulse transmission scheme for the HD-QKD system in practical scenarios to conserve photon resources.

Author contributions
The model design and simulations were done by JHL and YX and BL. The background was analysed by HCY and YXW. JT and ZFD handled the verification of manuscript. The effort was conceived and supervised by BL and co-supervised by LS. JHL and BL wrote the draft and all authors reviewed the manuscript.

Funding
This work is supported by the National Natural Science Foundation of China (Grants No. 61971436, No. 62073338); Science and technology innovation program of Hunan Province (Grants No. 2023RC3003).

Data Availability
No datasets were generated or analysed during the current study.

Declarations

Competing interests
The authors declare no competing interests.

Author details
[1]Information and Navigation College, Air Force Engineering University, Xi'an, China. [2]Chinese Academy of Military Science, Beijing, China. [3]College of Advanced Interdisciplinary Studies, National University of Defense Technology, Changsha, China.

Received: 28 March 2024 Accepted: 30 May 2024 Published online: 06 June 2024

References

1. Gisin N, Ribordy G, Tittel W, Zbinden H. Quantum cryptography. Rev Mod Phys. 2002;74:145–95. https://doi.org/10.1103/RevModPhys.74.145.
2. Bennett CH, Brassard G. Quantum cryptography: public key distribution and coin tossing. Theor Comput Sci. 2014;560:7–11.
3. Scarani V, Bechmann-Pasquinucci H, Cerf NJ, Dušek M, Lütkenhaus N, Peev M. The security of practical quantum key distribution. Rev Mod Phys. 2009;81:1301–50. https://doi.org/10.1103/RevModPhys.81.1301.
4. Chen W, Han Z-F, Zhang T, Wen H, Yin Z-Q, Xu F-X, Wu Q-L, Liu Y, Zhang Y, Mo X-F, Gui Y-Z, Wei G, Guo G-C. Field experiment on a "star type" metropolitan quantum key distribution network. IEEE Photonics Technol Lett. 2009;21(9):575–7. https://doi.org/10.1109/LPT.2009.2015058.
5. Wang S, Chen W, Yin Z, Li H-W, He D-Y, Li Y-H, Zhou Z, Song X-T, Li F-Y, Wang D, Chen H, Han Y, Huang J, Guo J-F, Hao P-L, Li M, Zhang C-M, Liang W-Y, Han Z-F. Field and long-term demonstration of a wide area quantum key distribution network. Opt. Express. 2014;22. https://doi.org/10.1364/OE.22.021739.
6. Sasaki M, Fujiwara M, Ishizuka H, Klaus W, Wakui K, Takeoka M, Miki S, Yamashita T, Wang Z, Tanaka A, Yoshino K, Nambu Y, Takahashi S, Tajima A, Tomita A, Domeki T, Hasegawa T, Sakai Y, Kobayashi H, Asai T, Shimizu K, Tokura T, Tsurumaru T, Matsui M, Honjo T, Tamaki K, Takesue H, Tokura Y, Dynes JF, Dixon AR, Sharpe AW, Yuan ZL, Shields AJ, Uchikoga S, Legré M, Robyr S, Trinkler P, Monat L, Page J-B, Ribordy G, Poppe A, Allacher A, Maurhart O, Länger T, Peev M, Zeilinger A. Field test of quantum key distribution in the Tokyo qkd network. Opt Express. 2011;19(11):10387–409. https://doi.org/10.1364/OE.19.010387.
7. Peev M, Pacher C, Alléaume R, Barreiro C, Bouda J, Boxleitner W, Debuisschert T, Diamanti E, Dianati M, Dynes JF, Fasel S, Fossier S, Fürst M, Gautier J-D, Gay O, Gisin N, Grangier P, Happe A, Hasani Y, Hentschel M, Hübel H, Humer G, Länger T, Legré M, Lieger R, Lodewyck J, Lorünser T, Lütkenhaus N, Marhold A, Matyus T, Maurhart O, Monat L, Nauerth S, Page J-B, Poppe A, Querasser E, Ribordy G, Robyr S, Salvail L, Sharpe AW, Shields AJ, Stucki D, Suda M, Tamas C, Themel T, Thew RT, Thoma Y, Treiber A, Trinkler P, Tualle-Brouri R, Vannel F, Walenta N, Weier H, Weinfurter H, Wimberger I, Yuan ZL, Zbinden H, Zeilinger A. The secoqc quantum key distribution network in Vienna. New J Phys. 2009;11(7):075001. https://doi.org/10.1088/1367-2630/11/7/075001.
8. Courtland R. China's 2,000-km quantum link is almost complete [news]. IEEE Spectr. 2016;53(11):11–2. https://doi.org/10.1109/MSPEC.2016.7607012.
9. Bechmann-Pasquinucci H, Peres A. Quantum cryptography with 3-state systems. Phys Rev Lett. 2000;85:3313–6. https://doi.org/10.1103/PhysRevLett.85.3313.
10. Cerf NJ, Bourennane M, Karlsson A, Gisin N. Security of quantum key distribution using *d*-level systems. Phys Rev Lett. 2002;88:127902. https://doi.org/10.1103/PhysRevLett.88.127902.
11. Wang F, Zeng P, Zhao J, Braverman B, Zhou Y, Mirhosseini M, Wang X, Gao H, Li F, Boyd RW, Zhang P. High-dimensional quantum key distribution based on mutually partially unbiased bases. Phys Rev A. 2020;101:032340. https://doi.org/10.1103/PhysRevA.101.032340.
12. Gröblacher S, Jennewein T, Vaziri A, Weihs G, Zeilinger A. Experimental quantum cryptography with qutrits. New J Phys. 2006;8(5):75. https://doi.org/10.1088/1367-2630/8/5/075.
13. Mirhosseini M, Magaña-Loaiza OS, O'Sullivan MN, Rodenburg B, Malik M, Lavery MPJ, Padgett MJ, Gauthier DJ, Boyd RW. High-dimensional quantum cryptography with twisted light. New J Phys. 2015;17(3):033033. https://doi.org/10.1088/1367-2630/17/3/033033.
14. Krenn M, Handsteiner J, Fink M, Fickler R, Ursin R, Malik M, Zeilinger A. Twisted light transmission over 143 km. Proc Natl Acad Sci. 2016;113(48):13648–53. https://doi.org/10.1073/pnas.1612023113.
15. Sit A, Bouchard F, Fickler R, Gagnon-Bischoff J, Larocque H, Heshami K, Elser D, Peuntinger C, Günthner K, Heim B, Marquardt C, Leuchs G, Boyd RW, Karimi E. High-dimensional intracity quantum cryptography with structured photons. Optica. 2017;4(9):1006–10. https://doi.org/10.1364/OPTICA.4.001006.
16. Wang F-X, Chen W, Yin Z-Q, Wang S, Guo G-C, Han Z-F. Characterizing high-quality high-dimensional quantum key distribution by state mapping between different degrees of freedom. Phys Rev Appl. 2019;11:024070. https://doi.org/10.1103/PhysRevApplied.11.024070.
17. Molina-Terriza G, Torres JP, Torner L. Management of the angular momentum of light: preparation of photons in multidimensional vector states of angular momentum. Phys Rev Lett. 2001;88:013601. https://doi.org/10.1103/PhysRevLett.88.013601.

18. Chang Z, Wang Y, Guo Z, An M, Qu R, Jia J, Wang F, Zhang P. Compact implementation of high-dimensional mutually partially unbiased bases protocol. Quantum Sci Technol. 2023;8(3):035028. https://doi.org/10.1088/2058-9565/acdd91.
19. Sun Z, Li Y, Ma H. Experimental high-dimensional quantum key distribution with orbital angular momentum. J Opt Soc Am B. 2024;41(2):351–5. https://doi.org/10.1364/JOSAB.507195.
20. Chen C, Yang H. Characterizing the statistical distribution for transmission coefficient of turbulent optical orbital-angular-momentum channels. Opt Express. 2019;27:28968. https://doi.org/10.1364/OE.27.028968.
21. Gyongyosi L. Multicarrier continuous-variable quantum key distribution. Theor Comput Sci. 2020;816:67–95. https://doi.org/10.1016/j.tcs.2019.11.026.
22. Paterson C. Atmospheric turbulence and orbital angular momentum of single photons for optical communication. Phys Rev Lett. 2005;94:153901. https://doi.org/10.1103/PhysRevLett.94.153901.
23. Vallone G, Marangon DG, Canale M, Savorgnan I, Bacco D, Barbieri M, Calimani S, Barbieri C, Laurenti N, Villoresi P. Adaptive real time selection for quantum key distribution in lossy and turbulent free-space channels. Phys Rev A. 2015;91:042320. https://doi.org/10.1103/PhysRevA.91.042320.
24. Erven C, Heim B, Meyer-Scott E, Bourgoin JP, Laflamme R, Weihs G, Jennewein T. Studying free-space transmission statistics and improving free-space quantum key distribution in the turbulent atmosphere. New J Phys. 2012;14(12):123018. https://doi.org/10.1088/1367-2630/14/12/123018.
25. Wang W, Xu F, Lo H-K. Prefixed-threshold real-time selection method in free-space quantum key distribution. Phys Rev A. 2018;97:032337. https://doi.org/10.1103/PhysRevA.97.032337.
26. Xu F, Zhang Y-Z, Zhang Q, Pan J-W. Device-independent quantum key distribution with random postselection. Phys Rev Lett. 2022;128:110506. https://doi.org/10.1103/PhysRevLett.128.110506.
27. Wang X, Wu T, Dong C, Zhu H, Zhu Z, Zhao S. Integrating deep learning to achieve phase compensation for free-space orbital-angular-momentum-encoded quantum key distribution under atmospheric turbulence. Photon Res. 2021;9(2):9–17. https://doi.org/10.1364/PRJ.409645.
28. Kang J-L, Zhang M-H, Liu X-P, Xie J-H. Machine learning with neural networks for parameter optimization in twin-field quantum key distribution. Quantum Inf. Process. 2023;22. https://doi.org/10.1007/s11128-023-04063-5.
29. Wang L, Dong Q, Jiao R. Parameter optimization in decoy-state phase-matching quantum key distribution. Quantum Inf. Process. 2023;22. https://doi.org/10.1007/s11128-023-04130-x.
30. Gyongyosi L, Imre S. Training optimization for gate-model quantum neural networks. Sci Rep. 2019;9(1):12679.
31. Popkin G. The Internet goes quantum. Science. 2021;372(6546):1026–9. https://doi.org/10.1126/science.372.6546.1026.
32. Gyongyosi L, Imre S. Advances in the quantum Internet. Commun ACM. 2022;65(8):52–63. https://doi.org/10.1145/3524455.
33. Gyongyosi L, Imre S, Nguyen HV. A survey on quantum channel capacities. IEEE Commun Surv Tutor. 2018;20(2):1149–205. https://doi.org/10.1109/COMST.2017.2786748.
34. Padgett MJ, Miatto FM, Lavery MPJ, Zeilinger A, Boyd RW. Divergence of an orbital-angular-momentum-carrying beam upon propagation. New J Phys. 2015;17(2):023011. https://doi.org/10.1088/1367-2630/17/2/023011.
35. Zhao J, Mirhosseini M, Braverman B, Zhou Y, Hashemi Rafsanjani SM, Ren Y, Steinhoff NK, Tyler GA, Willner AE, Boyd RW. Performance analysis of *d*-dimensional quantum cryptography under state-dependent diffraction. Phys Rev A. 2019;100:032319. https://doi.org/10.1103/PhysRevA.100.032319.
36. Charnotskii M. Statistics of the sparse spectrum turbulent phase. J Opt Soc Am A. 2013;30(12):2455–65. https://doi.org/10.1364/JOSAA.30.002455.
37. Zhao L-Y, Wu Q-J, Qiu H-K, Qian J-L, Han Z-F. Practical security of wavelength-multiplexed decoy-state quantum key distribution. Phys Rev A. 2021;103:022429. https://doi.org/10.1103/PhysRevA.103.022429.
38. Ma X, Qi B, Zhao Y, Lo H-K. Practical decoy state for quantum key distribution. Phys Rev A. 2005;72:012326. https://doi.org/10.1103/PhysRevA.72.012326.

Publisher's Note