PHOTONICS Research

Integrating deep learning to achieve phase compensation for free-space orbital-angular-momentum-encoded quantum key distribution under atmospheric turbulence

Xingyu Wang,[1,2] Tianyi Wu,[2] Chen Dong,[2,*] Haonan Zhu,[1] Zhuodan Zhu,[3] and Shanghong Zhao[1]

[1]School of Information and Navigation, Air Force Engineering University, Xi'an 710077, China
[2]Information and Communication College, National University of Defense Technology, Xi'an 710006, China
[3]No. 94782 Unit of PLA, Hangzhou 310021, China
*Corresponding author: dongchengfkd@163.com

A high-dimensional quantum key distribution (QKD), which adopts degrees of freedom of the orbital angular momentum (OAM) states, is beneficial to realize secure and high-speed QKD. However, the helical phase of a vortex beam that carries OAM is sensitive to the atmospheric turbulence and easily distorted. In this paper, an adaptive compensation method using deep learning technology is developed to improve the performance of OAM-encoded QKD schemes. A convolutional neural network model is first trained to learn the mapping relationship of intensity profiles of inputs and the turbulent phase, and such mapping is used as feedback to control a spatial light modulator to generate a phase screen to correct the distorted vortex beam. Then an OAM-encoded QKD scheme with the capability of real-time phase correction is designed, in which the compensation module only needs to extract the intensity distributions of the Gaussian probe beam and thus ensures that the information encoded on OAM states would not be eavesdropped. The results show that our method can efficiently improve the mode purity of the encoded OAM states and extend the secure distance for the involved QKD protocols in the free-space channel, which is not limited to any specific QKD protocol.   © 2021 Chinese Laser Press

https://doi.org/10.1364/PRJ.409645

1. INTRODUCTION

Quantum key distribution (QKD) can provide information theoretic security to share keys between two distant parties [1–3]. Currently, free-space quantum communication has progressed out of laboratories into real-world scenarios [4–8], which paves the way towards global-scale and highly secure quantum communication networks. However, most experiments mainly rely on either the polarization [9,10] or phase [11] of faint laser pulses as information carriers, where the typical two-dimensional encoding scheme limits the capacity of QKD systems due to an intrinsically bounded Hilbert space.

Unlike the limited degree of freedom on polarization or phase states, the orbital angular momentum (OAM) is a high-dimensional encoding scheme for free-space QKD owing to an infinite number of available OAM eigenstates in principle. Recently, Refs. [12–15] implemented OAM-encoded QKD experiments, and Ref. [16] realized OAM-based entanglement distribution over a free-space optical (FSO) channel of more than 143 km. Furthermore, OAM has been experimentally

demonstrated to be rotational invariant in the propagation direction, which can remove the error caused by reference frame misalignment [17]. These outstanding properties make OAM states useful in both classical communication [18–22] and high-dimensional quantum cryptography [23–31].

Nonetheless, it has been shown that the helical phase of a vortex beam that carries OAM is sensitive to the transmission environment and easily distorted [32–34]. Particularly in a free-space optical channel, the atmospheric turbulence resulting from the inhomogeneity of temperature and pressure in the atmosphere will lead to severe wavefront distortion and coherence destruction of the beam, which will directly increase the crosstalk among the adjacent OAM modes [35,36] and further influence the performance of the key rate in OAM-encoded QKD schemes. Some meaningful methods, such as a post-selection of the data or an increase in the mode spacing, which are usually used in OAM-encoded QKD systems to improve the stability of vortex beams against atmospheric turbulence, will lead to a reduction of single-photon gain and coding dimension. In addition, an adaptive optics (AO) system is often

applied in the classical OAM-encoded communications to implement the phase compensation [37–39]. In such scenarios, the compensation accuracy depends on the convergence of algorithms used in AO systems, which requires relatively more processing time. Especially for the satellite-based QKD system with time-varying channel conditions, the AO systems may not be fully adequate for an efficient turbulence correction. Therefore, methods for quickly compensating for the turbulence-distorted vortex beams are still urgently needed for practically applying OAM-encoded QKD systems, especially for satellite-based QKD applications with the limited link durations.

In this paper, we propose a fast and efficient method to adaptively compensate for the atmospheric turbulence effects, which borrows the ideas of deep learning technology. Deep learning technology is one of the most popular artificial intelligence (AI) tools, and it shows extraordinary ability in image recognition [40], optical fields [41], and even parameter optimization for QKD [42,43]. In our proposed method, a convolutional neural network (CNN) model is first designed to predict phase distortion information of atmospheric turbulence. Then CNN combined with common setups is integrated as an accurate and stable phase feedback module to generate a phase screen [44–46] and correct the distorted vortex beam in our free-space OAM-encoded QKD scheme. Our results show that the compensation ability of our method is independent of the turbulence intensity and only relies on the structure of the CNN. In addition, our method can efficiently eliminate the turbulence distortion and improve the mode purity of OAM states compared to the OAM-encoded QKD scheme without compensation, which extends the secure distance for the involved QKD protocols in the free-space channel.

The organization of the article is as follows. In Section 2, a CNN is presented for estimating phase distortion induced by atmospheric turbulence. Then, in Section 3, we describe the components and phase compensation operation of our free-space OAM-encoded QKD scheme and show the improvement of mode purity of OAM states at different situations to verify the effectiveness of our method. In Section 4, we analyze the performance of the involved OAM-encoded QKD scheme with the decoy-state method. The article is ended in Section 5 with concluding remarks.

2. DEEP LEARNING FOR PHASE DISTORTION PREDICTION IN THE TURBULENCE CHANNEL

When the vortex beam transmits through atmospheric turbulence, the refractive index fluctuation causes the helical phase wavefront distortion. In our work, the phase screen produced by the Kolmogorov model [47], which has been widely used to model the phase distortion information over the propagating beam, is adopted to provide quantitative agreement with analytical results. In parallel, in order to simulate the atmospheric turbulence using the random phase screen located in front of the receiver, the propagation of the optical beam through the atmospheric turbulence channel is usually divided into two processes: vacuum transmission and phase modulation by the turbulence phase screen (details in Appendix A). Consequently, we first need to predict the phase screen containing the distortion information induced by the atmospheric turbulence to perform the phase compensation for correcting the distorted vortex beam.

The CNN is composed of multiple-layered structures built from human-brain-like behavior (i.e., neurons), which can learn data with multiple levels of abstraction and can extract high-level abstract features. Based on the universal approximation theorem of a neural network, it is possible to infinitely approximate any complicated but smooth functions on a defined domain with a CNN. Stated differently, it can be applied to accept new incoming data x and predict the corresponding $\hat{y}$ after adequate iterations. Here we designed a CNN to learn the phase screen in our atmospheric turbulence prediction work as illustrated in Fig. 1. The CNN structure consists of 15 learned layers, including 12 convolutional layers and 3 deconvolutional layers. The first convolutional layer uses 5×5 convolutional kernels, and the other layers use 3×3 convolutional kernels.
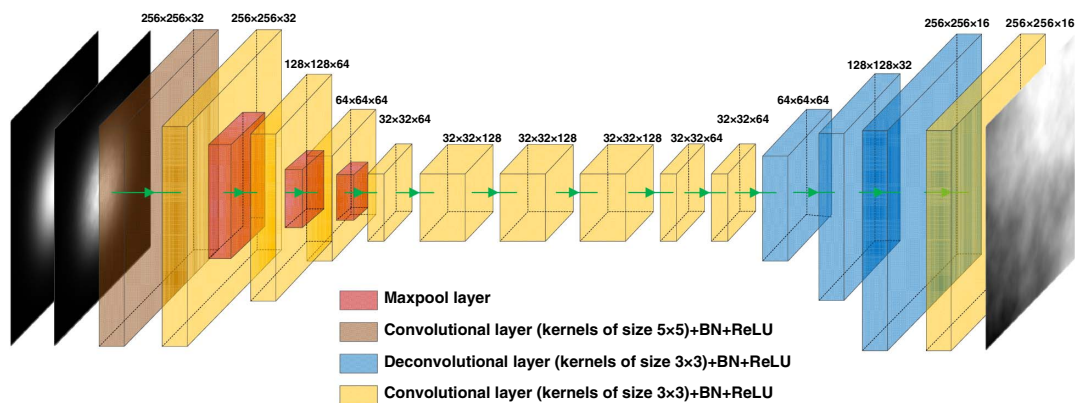

Fig. 1. CNN structure is used to predict the phase distortion in atmospheric turbulence channel. BN, batch normalization; ReLU, rectified linear unit. We consider the encoder-decoder architecture of SegNet [48], since the prediction of the turbulent phase screen belongs to the pixel-by-pixel prediction tasks. The encoder part includes the convolutional layers, pooling layers, etc., where the three maxpool layers make the resolution of the feature map 8 times lower than that of the original image to perform nonlinear upsampling. In the decoder part, three deconvolutional layers are used for upsampling by a factor of 8, so as to keep the size of the original input image consistent. Note that the CNN can be changed according to the needs of specific prediction tasks.

The CNN is trained with a set of training data. This set contains N mappings $(x_i^T, y_i^T), i = 1, 2, \ldots, N$. Specifically, y_i^T is a gray image of the random phase screen produced by the Kolmogorov model in different turbulence intensities, and the input x_i^T represents the two gray images, i.e., the intensity distribution of the Gaussian probe beam (GPB) affected by turbulence and that without turbulence. Namely, the network can analyze distortion information in the form of images, which can automatically find the characterization of turbulence to generate a predicted phase screen for the subsequent phase compensation.

In our CNN, a loss function mean squared error (MSE) is defined on the output layer between the network's calculated outputs $\hat{y}_i = f(x_i^T, w)$ on a set of input data x_i^T, versus the set of desired output y_i^T. The loss function MSE takes the form

$$\mathrm{MSE} = \frac{1}{N} \sum_i^N [f(X, w) - Y]^2. \tag{1}$$

Here we take a linear combination of inputs x_i^T, with weight w and constant factor b, and the activation in each neuron can be expressed as

$$
\begin{aligned}
l_1[f(x_i^T, w), y_i] &= (y_i - \hat{y}_i)^2, \\
l_2[f(x_i^T, w), y_i] &= \mathrm{ReLU}(y_i - \hat{y}_i - b), \\
l_3[f(x_i^T, w), y_i] &= \mathrm{ReLU}(\hat{y}_i - y_i - b),
\end{aligned}
\tag{2}
$$

where ReLU represents rectified linear unit function [i.e., $\max(0, x)$]. We use the backpropagation algorithm [49] to quickly compute the partial derivatives of the loss function to the internal weight w in our CNN. Simultaneously, we adjust the weight w accordingly via the mini-batch gradient descent (MBGD) algorithm [50] to minimize the loss function and make $\hat{y}_i$ approach y_i^T as much as possible. Finally, by substituting Eq. (2) into Eq. (1), the loss function MSE between the estimated value and actual value of phase information is calculated as follows:

$$
\begin{aligned}
\mathrm{MSE} &= \frac{1}{N} \sum_{i=1}^N \{ l_1[f(x_i^T, w), y_i] + l_2[f(x_i^T, w), y_i] \\
&\quad + l_3[f(x_i^T, w), y_i] \} \\
&= \frac{1}{N} \sum_{i=1}^N [(y_i - \hat{y}_i)^2 + \mathrm{ReLU}(y_i - \hat{y}_i - b) \\
&\quad + \mathrm{ReLU}(\hat{y}_i - y_i - b)].
\end{aligned}
\tag{3}
$$

To achieve the trained CNN with a better generalization ability to prevent overfitting, we use an amount of training data to decrease the training error and the model complexity. Here we use 84,000 GPB intensity images with specified turbulence (i.e., the atmospheric refractive index structure constant C_n^2) ranging from $[10^{-15}, 10^{-13}]$, where the size of each image is fixed at 256×256 and the gray values are normalized into $[0, 1]$. In detail, 80,000 of them are used as the training data, 2000 are for the test data, and the remaining 2000 are for the validation data. Figure 2 shows the loss function, where the yellow and blue curves represent the loss value of the validation data set and training data set, respectively. The loss value of the
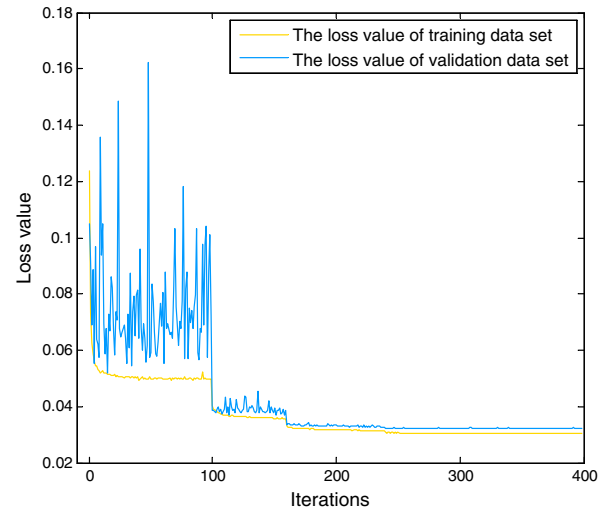

Fig. 2. Loss values of the validation data set and training data set against the iterations of the algorithm. Here we dynamically tune the learning rate at every 10 epochs. As the number of iterations increases, the learning rate is gradually reduced in the process of approaching the optimal solution, which shows drops of the loss value at 100 iterations.
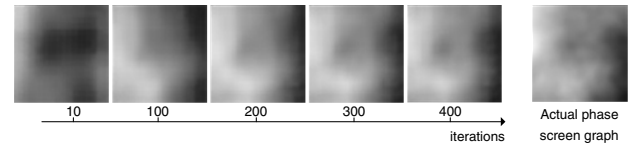

Fig. 3. Atmospheric turbulence phase graphs predicted by the CNN different training iterations. The five images from left to right represent the phase screens that are predicted by the validation data set at 10, 100, 200, 300, and 400 iterations, and the rightmost one is the one corresponding to the actual phase screen.

validation data set is very close to that of training data set, and both converge to be stable. After 400 iterations, the loss value of the validation data set dropped to 0.03, which demonstrated that the CNN at this time has a good performance of prediction on turbulence and no overfitting occurred.

To reflect the trend of the loss curve more intuitively, Fig. 3 presents the phase images predicted by our CNN. From the images, we can see that when the number of iterations is sufficient, the predicted phase images are almost the same as the real phase screens. In detail, the time required for the iterations and processing is about 0.1 ms per image by using an i9-8950 CPU, which is much lower than the turbulent freezing time (10 ms) [51], and thus it brings advantages to optimize the performance of the OAM-encoded QKD scheme.

3. DEEP-LEARNING-BASED PHASE COMPENSATION IN THE FREE-SPACE OAM-ENCODED QKD SCHEME

We use the trained CNN for phase compensation in our OAM-encoded QKD scheme. Figure 4 shows the schematic diagram of an OAM-encoded QKD system with decoy-state method, which contains the real-time atmospheric turbulence
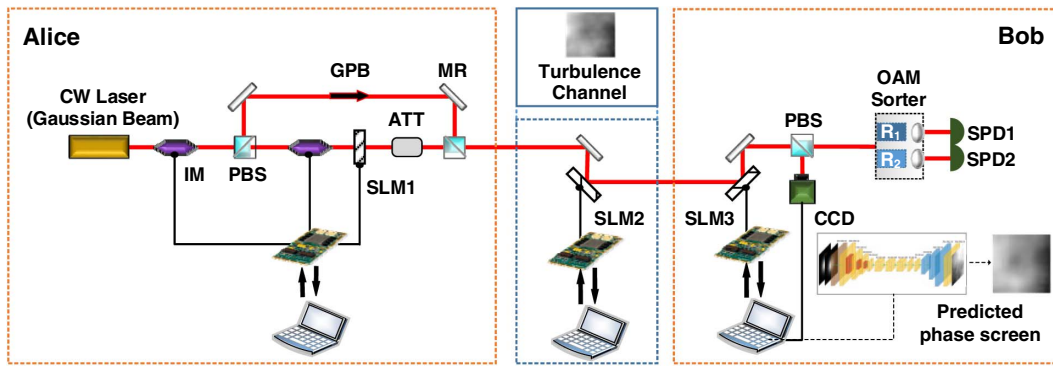
Fig. 4.   Schematic diagram of an OAM-encoded QKD with decoy-state method. CW laser, continuous-wave laser; GPB, Gaussian probe beam; IM, intensity modulator; PBS, polarization beam splitter; SLM, spatial light modulator; ATT, attenuator; MR: mirror; CCD, charge-coupled device; SPD, single-photon detector. At Alice's side, the signal pulses (a CW laser beam modulated by an IM) are separated to two parts by a PBS. The x-polarized GPB is modulated to produce a decoy state and encoded to load the spatially helical phase wavefront (or OAM) by an IM and SLM1, respectively. The y-polarized GPB is then combined with the encoded OAM signal pulses by another PBS and transmitted together through turbulence channel simulated by SLM2. Both the y-polarized GPB and the encoded OAM signal pulses will get phase distortion when transmitted through the simulated turbulence channel. The phase distortion of the y-polarized GPB is detected by a CCD, and the corresponding reverse phase screen will be produced by SLM3 to compensate for the phase distortion of the OAM-encoded signal pulses. After compensation, the OAM-encoded signal pulses will be classified by the OAM sorter and received by different SPDs.

compensation feedback at Bob's side. In detail, at Alice's side, a Gaussian beam from a continuous-wave (CW) laser (operating at 1550 nm) is modulated into a pulse train with a 1 MHz repetition rate. A polarization beam splitter (PBS) is utilized to separate the pulses into two subpulses, where the signal pulses are linearly polarized in the x direction and the Gaussian probe pulses are linearly polarized in the y direction. In practice, it is usually difficult to create a perfect vacuum state in the decoy-state QKD experiments [52]. To realize the preparation of decoy states, an intensity modulator is used to modulate the signal pulses into different intensities. When the gain of a state is modulated to be close (a finite extinction ratio below 30 dB) to the dark count rate of our single-photon detector, the state will be regarded as the "vacuum state." After that, the signal pulses are converted by spatial light modulator (SLMs) to carry OAM-encoded qubit signal and then attenuated to a single-photon level signal by an attenuator. By using a polarizing beam splitter (PBS), the quantum signals together with the Gaussian probe pulses are sent to Bob through a simulated free-space channel.

In the free-space channel, the equivalent phase screens are produced by SLM2 under the Kolmogorov model. At Bob's side, the compensation feedback is used to perform phase compensation, among which SLM3 is only sensitive to x polarization and a CCD is utilized to extract the intensity distribution of Gaussian probe pulses, which is used as the input of a laptop PC with our CNN to predict a real-time atmospheric turbulence phase screen. Thus, by getting a reversed phase of the predicted phase screen on SLM3, the phase distortion of the only vortex pulses induced by atmospheric turbulence can be restored. After these operations, the OAM states are differentiated by employing the OAM sorter [12], which consists of two static optical transformations [unwrapper (R1) and phase corrector (R2) shown in Fig. 4] and a lens. Finally, two single-photon detectors are adopted to detect the results.

Note that the measurement probabilities of the desired OAM state relate directly to the probabilities of obtaining correct or incorrect measurements of a transmitted "symbol." Therefore, for quantitative analysis of the correction effect in terms of the measurement probability, we now need to compare the mode purity of the OAM states before and after compensation. The mode purity, which can be regarded as the normalized power, is an important parameter describing the crosstalk between different spatial modes. Specifically, we assume that the receiver may measure a photon with the adjacent OAM mode $l' = l_0 + \Delta l, \Delta l = 0, 1, 2, \dots$. Thus, the mode purity of OAM states can be estimated by taking ratio $s_\Delta = P_\Delta / P$ between the power contained in each OAM mode and the total power collected by the receiver. Without loss of generality, we are only interested in the ensemble average of this quantity (i.e., $\langle s_\Delta \rangle$). Meanwhile, the OAM topological charge is set as $l_0 = 1$. For Kolmogorov turbulence theory, the mode purity of an OAM state propagating through turbulence can be written as [34]

$$\langle s_\Delta \rangle = \frac{1}{\pi} \int_0^1 \frac{r}{R} d\frac{r}{R} \int_0^{2\pi} \exp\left[-6.88 \times 2^{2/3} \left(\frac{r}{r_0}\right)^{5/3} \left|\sin\frac{\Delta\theta}{2}\right|^{5/3}\right] \times \exp(-i\Delta l \Delta\theta) d\Delta\theta, \tag{4}$$

where r and θ are the radial coordinates and the azimuthal coordinates, respectively; r_0 is the Fried parameter [10]; and R is the radius of a receiving aperture. By substituting $\Delta l = 0$ into Eq. (4), we can get the mode purity of the receiving initial OAM state $l_0 = 1$ without phase compensation:

$$\langle s_0 \rangle = \frac{1}{\pi} \int_0^1 \frac{r}{R} d\frac{r}{R} \int_0^{2\pi} \exp\left[-6.88 \times 2^{2/3} \left(\frac{r}{r_0}\right)^{5/3} \left|\sin\frac{\Delta\theta}{2}\right|^{5/3}\right] d\Delta\theta. \tag{5}$$

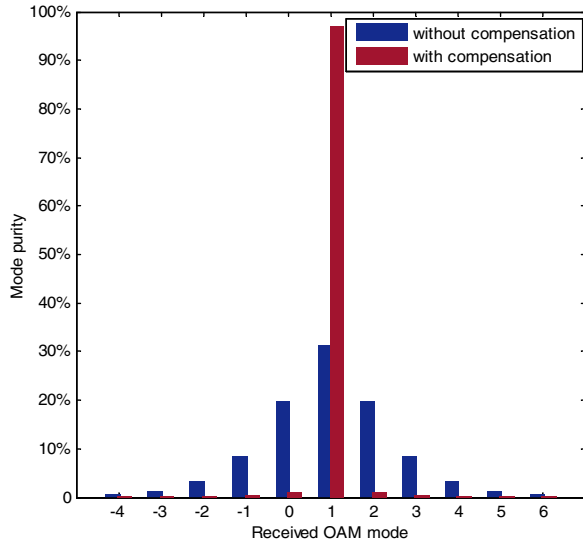On the other hand, as discussed in Ref. [53], the effect of our phase compensation feedback on OAM modes can also be

Fig. 5. Mode purity of the received OAM states with and without compensation.

Fig. 6. Mode purity of the received OAM state in the different situations.

described by the Strehl ratio [54], whose calculation is based on the root mean square (RMS) of the residual wavefront aberration. In our case, the correction errors caused by the system are all attributed to the accuracy of the algorithm in our CNN. Therefore, combined with the performance indices of our CNN, i.e., the MSE value $\chi = 1$, the mode purity of the receiving initial OAM state with phase compensation can be estimated:

$$\langle s_0 \rangle' = \exp(-\chi). \tag{6}$$

By numerical simulation, we present the mode purity of the received OAM states with and without compensation in Fig. 5. Here the beam wavelength $\lambda = 1550$ nm, the waist radius $\omega_0 = 0.002$ m, and the radius of receiving aperture $R = 0.075$ m. The propagation distance Δz is set as 50 m, and the atmospheric refractive index structure constant $C_n^2 = 10^{-14}$ m$^{-2/3}$. It is clear from Fig. 5 that the probabilities for an OAM mode scattering to adjacent OAM modes are greatly reduced, and the mode purity of the initial OAM state $l_0 = 1$ is significantly improved from 32.5% to 97.1%.

To show the applicability of our method in various environments, we update the training data set for our CNN, where the ranges of Δz and C_n^2 are set as $[1 \times 10^3, 1 \times 10^5]$ m and $[10^{-14}, 10^{-13}]$ m$^{-2/3}$, respectively. In particular, we generate 70,000 GPB images every 10 km to form the final data set, i.e., a total of $10 \times 70{,}000$ pieces of data set to train the CNN, where the entire process from generating the data set to training the CNN took about 6 h. After retraining, we show the mode purity of OAM state $l_0 = 1$ at different situations. As shown in Fig. 6, the mode purity can always be well recovered under a wide range of parameter combinations of the intensity of turbulence and the distance. Although the prediction effect under strong turbulence or long distance is reduced (some pixels of the phase screen are out of the gray value range, which leads to the reduction of effective information during the normalization process), the mode purity values in different situations are still
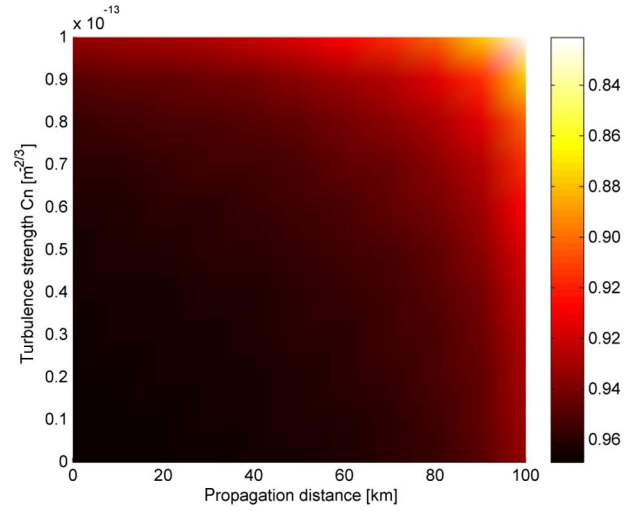
improved to above 0.82. This is because the most key working mechanism of the proposed CNN is to find the mapping relationship between inputs and outputs. Next, we will discuss the key rate performance optimization of the OAM-encoded QKD system.

4. PERFORMANCE OPTIMIZATION OF THE FREE-SPACE OAM-ENCODED QKD

To further evaluate the performance of the deep-learning-based phase compensation in improving the performance of the OAM-encoded QKD scheme with the decoy-state method, we discuss the secret key rate of the involved system. For simplicity and generality, a two-dimensional OAM-QKD protocol is discussed, where the OAM basis and superposition basis (SUP) [12] are both used in the OAM-QKD protocol. In such a decoy-state QKD, Alice randomly chooses an OAM basis $(|-l_0\rangle |l_0\rangle)$ or the SUP basis consisting of $\frac{1}{\sqrt{2}}(|l_0\rangle + e^{in\pi}|-l_0\rangle)$, where $n = 0, 1$ is the encoding bit. 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.

We follow the decoy-state QKD theory from Ref. [55]. Using the Gottesman–Lo–Lutkenhaus–Preskill (GLLP) formula [56], the secure key rate of decoy-state OAM-QKD in the asymptotic case is given by

$$R_{\text{GLLP}} = q\{-f_e(E_\mu^{\text{OAM}}) Q_\mu^{\text{OAM}} h_2(E_\mu^{\text{OAM}}) + \mu e^{-\mu} Y_1^{\text{OAM}}[1 - h_2(e_1^{\text{SUP}})]\}, \tag{7}$$

where q depends on the implementation (1/2 for the BB84 protocol due to the fact that half of the time Alice and Bob disagree with the bases, and if one uses the efficient BB84 protocol, $q \approx 1$); f_e is the error correction inefficiency function, μ is the intensity of the signal state, and h_2 is the binary entropy function. Q_μ^{OAM} and E_μ^{OAM} are the total gain and error rate

Table 1.   List of Parameters Used in the Simulations

Experimental Parameters	Value
Radius of the receiving aperture R_r (cm)	7.5
Signal wavelength λ (nm)	1550
Refraction structure constant C_n^2	10^{-14}
Error rate of dark count e_0	0.5
Misalignment error e_d	0.015
Error correction inefficiency f_e	1.22
Background dark count rate Y_0	3×10^{-6}
Detection efficiency of the SPD η_d	50%
Finite size of data N	10^{14}

under the OAM basis, which can be theoretically calculated by the standard channel model [57] using a transmittance of η.

Here the transmittance consists of the probabilities of obtaining correct and incorrect initial OAM states. As discussed in the below section, the probability of obtaining a correct state can be expressed as

$$\eta_0 = e^{-\beta L} \langle s_0 \rangle', \qquad (8)$$

where β is the link attenuation coefficient. Correspondingly, the other one, the transmission error probability, is $\bar{\eta}_0 = 1 - \eta_0$. Thus, Q_μ^{OAM} can be calculated by

$$Q_\mu^{OAM} = Y_0 + 1 - e^{-\mu \cdot \eta \eta_d}. \qquad (9)$$

Similarly, the gain Q_μ^{SUP} in the SUP basis can also be estimated in a similar way. Therefore, $Q_\mu^{SUP} = Q_\mu^{OAM}$. Note that, considering the errors are induced by misalignment and crosstalk between states, E_μ^{OAM} in the OAM basis can be given as

$$E_\mu^{OAM} = \frac{e_0 Y_0 + t \cdot e_d (Q_\mu^{OAM} - Y_0)}{Q_\mu^{OAM}}, \qquad (10)$$

where e_0 is the error rate of the dark count, Y_0 is the background count rate for the detector, and $t = \bar{\eta}_0$ is the crosstalk probability. Similarly, the total errors $E_\mu^{SUP} = E_\mu^{OAM}$. By using decoy-state technique to combine Q_μ^{OAM} and E_μ^{SUP} for different intensities, we can estimate the yield and the error rate of the single-photon states Y_1^{OAM} and e_1^{SUP}, which can be written as

$$Y_1^{OAM} = \frac{\mu}{\mu v - v^2} \left(Q_v^{OAM} e^v - Q_\mu^{OAM} e^\mu \frac{v^2}{\mu^2} - e^\mu \frac{\mu^2 - v^2}{e_0 \mu^2} \right), \qquad (11)$$

$$e_1^{SUP} = \frac{E_v^{SUP} Q_v^{SUP} e^v - e_0 Y_0}{Y_1^{SUP} v}. \qquad (12)$$

For a fair comparison, we consider the same free-space channel model proposed in Ref. [12], where the link attenuation β is set to 1.38×10^{-4} (0.6 dB/km). The radius of receiving aperture R_r is 7.5 cm, and the refraction structure constant C_n^2 is fixed at 10^{-14} m$^{-2/3}$. Other experimental parameters are taken directly from Ref. [7] as listed in Table 1.

In Fig. 7, we compare the secret key rates versus propagation distance for the situation with perfect phase compensation (i.e., $\chi = 1$), the practical situation with phase compensation feedback based on the learned CNN (i.e., the value of χ is
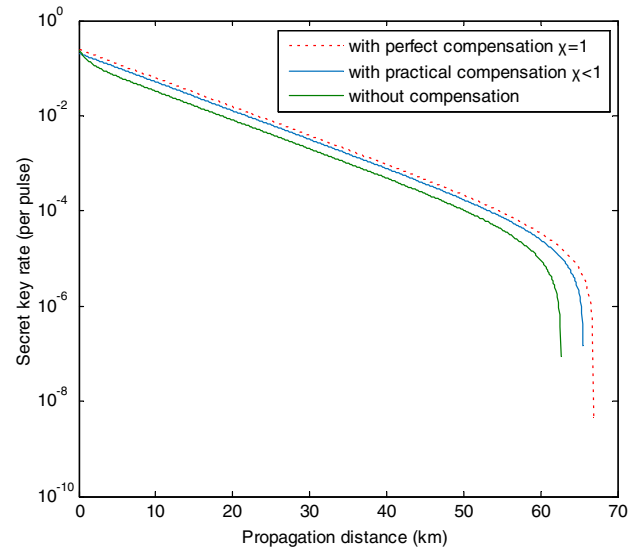

Fig. 7. Secret key rate performance of the OAM-encoded QKD versus propagation distance for different schemes. From top to bottom, the curves represent the secret key rates in the perfect phase compensation (red dotted line, $\chi = 1$), the practical situation with the phase compensation feedback supported by the learned CNN (blue solid line, $\chi < 1$), and the situation without phase compensation (green dashed line, $\chi = 0$). Note that we fix the signal and decoy intensities to $\mu = 0.3$, $v = 0.05$. Therefore, by scanning through the decoy-state intensities and probabilities, the key rate can be further optimized.

dependent on the transmission distance), and the situation without phase compensation. As shown in Fig. 7, our method offers a higher key rate than that of no compensation. Even if the learned CNN is not perfect, the curves of the practical situation for the secret key rates are quite close to the perfect phase compensation, where the situation of perfect phase compensation can be regarded as having no turbulence effects. This means that our proposed method can be applied in the free-space OAM-encoded QKD system to mitigate the turbulence phase distortion.

5. CONCLUSIONS

In this work, considering that the helical phase wavefront induced by the turbulence distortion has significant influence on the performance of a free-space OAM-encoded QKD scheme with the decoy-state method, we integrate the deep learning technology to achieve phase compensation to optimize the involved system. Here a well-trained CNN is designed to predict an equivalent turbulent phase screen. Combined with the commonly used optical devices, fast and accurate phase compensation feedback can be achieved in our experimental scheme. Furthermore, we use the mean-squared error (MSE) between the predicted phase values and original phase values as a performance index for assessing our system. The results show that our scheme can effectively increase the key rate owing to improving the mode purity of OAM states. Our proposed work can provide an efficient solution for a free-space high-dimensional QKD using OAM states.

Note that, considering the time-varied atmospheric turbulence, we use a charge-coupled device (CCD) to extract the real-time turbulence distortions from the intensity distribution of the Gaussian probe beam, which has no coding information. By employing an SLM, a generated compensated phase screen can be directly loaded on the OAM-encoded beams, and thus there is no need to monitor the OAM-encoded signals. In experiments, limited by the response speed of devices such as the SLM, our experimental scheme may degrade the compensation effect, but it can reduce the number of qubits used to estimate channel conditions. Moreover, attacks due to the loopholes of the phase compensation module can also be resisted. In addition, placing the phase compensation module on the measurement side [i.e., measurement-device-independent (MDI)-QKD protocol] can further ensure its safety. Therefore, the experimental and security analysis of the MDI-QKD system integrated with our method will be the subject of our future studies.

APPENDIX A

When the vortex beam transmits through atmospheric turbulence, the refractive index fluctuation causes helical phase wavefront distortion. To simulate the atmospheric turbulence, we model the atmospheric channel using a phase screen located in front of the receiver. Thus, the propagation of the optical beam through the atmospheric turbulence channel with a length $z + \Delta z$ can be divided into two processes: a vacuum transmission channel with a length z and a phase modulation process by the turbulence phase screen with a width Δz. The phase screen method involves the filtering of a complex Gaussian random field using the phase's power spectral density (PSD) function of the atmospheric turbulence, where the phase's PSD function $\Phi(k_x, k_y)$ can be calculated by the Kolmogorov model:

$$\Phi(k_x, k_y) = 2\pi k_0^2 \Delta z \cdot 0.033 C_n^2 \sqrt{k_x^2 + k_y^2}^{-11/3}, \quad \textbf{(A1)}$$

where k_0 is the wavenumber and k_x and k_y are the components of k_0 in the x-axis and y-axis directions, respectively. C_n^2 is the refractive index structure constant, representing the turbulence intensity. Subsequently, the variance of the phase spectrum can be written as

$$\sigma^2(k_x, k_y) = \left(\frac{2\pi}{N\Delta L}\right)^2 \Phi(k_x, k_y), \quad \textbf{(A2)}$$

where ΔL is the grid spacing. Therefore, using the fast Fourier transform (FFT), realization of the corresponding phase screen in the time domain can be represented as

$$\phi(x, y) = \text{FFT}[\mathbf{C} \cdot \sigma(k_x, k_y)]. \quad \textbf{(A3)}$$

Here $\phi(x, y)$ is an $N \times N$ phase screen, and $\mathbf{C}$ is an $N \times N$ dimensional complex Gaussian random number array with a variance of 1. According to the diffraction angular spectrum theory, when the vortex beam $E(z, x, y)$ propagates in atmospheric turbulence over Δz, the optical field at $z + \Delta z$ can be approximately described by

$$E(z + \Delta z, x, y) = \text{FFT}^{-1}\{\exp(iA\Delta z)$$
$$\cdot \text{FFT}\{\exp[i\phi(x, y)]\} \cdot E(z, x, y)\}, \quad \textbf{(A4)}$$

where $\exp(iA\Delta z)$ is the transfer function of Fresnel propagation.

In our work, we choose one of the vortex beam forms, i.e., a Laguerre–Gaussian (LG) beam, making OAM eigenstates correspond to the LG mode set. Here we use the intensity and phase profiles of an LG01 beam after 500 m atmospheric propagation with different C_n^2. Here the beam waist radius w_0 is set as 0.002 m. The phase screen is set with a numerical grid of $N \times N = 512 \times 512$ points and a grid spacing of $\Delta L = 5$ mm.

REFERENCES

1. N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, "Quantum cryptography," Rev. Mod. Phys. **74**, 145–195 (2002).
2. C. H. Bennett, G. Brassard, and N. D. Mermin, "Quantum cryptography without Bell's theorem," Phys. Rev. Lett. **68**, 557–559 (1992).
3. D. Mayers, "Unconditional security in quantum cryptography," J. ACM **48**, 351–406 (2001).
4. W. T. Buttler, R. J. Hughes, P. G. Kwiat, S. K. Lamoreaux, G. G. Luther, G. L. Morgan, J. E. Nordholt, C. G. Peterson, and C. M. Simmons, "Practical free-space quantum key distribution over 1 km," Phys. Rev. Lett. **81**, 3283–3286 (1998).
5. C. Z. Peng, T. Yang, X. H. Bao, J. Zhang, X. M. Jin, F. Y. Feng, B. Yang, J. Yang, J. Yin, Q. Zhang, N. Li, B. L. Tian, and J. W. Pan, "Experimental free-space distribution of entangled photon pairs over 13 km: towards satellite-based global quantum communication," Phys. Rev. Lett. **94**, 150501 (2005).
6. J. Yin, J. G. Ren, H. Lu, Y. Cao, H. L. Yong, Y. P. Wu, C. Liu, S. K. Liao, F. Zhou, Y. Jiang, X. D. Cai, P. Xu, G. S. Pan, J. J. Jia, Y. M. Huang, H. Yin, J. Y. Wang, Y. A. Chen, C. Z. Peng, and J. W. Pan, "Quantum teleportation and entanglement distribution over 100-kilometre free-space channels," Nature **488**, 185–188 (2012).
7. T. Schmitt-Manderbach, H. Weier, M. Fürst, R. Ursin, F. Tiefenbacher, T. Scheidl, J. Perdigues, Z. Sodnik, C. Kurtsiefer, J. G. Rarity, A. Zeilinger, and H. Weinfurter, "Experimental demonstration of free-space decoy-state quantum key distribution over 144 km," Phys. Rev. Lett. **98**, 010504 (2007).
8. S. K. Liao, W.-Q. Cai, W.-Y. Liu, L. Zhang, Y. Li, J.-G. Ren, J. Yin, Q. Shen, Y. Cao, Z.-P. Li, F.-Z. Li, X.-W. Chen, L.-H. Sun, J.-J. Jia, J.-C. Wu, X.-J. Jiang, J.-F. Wang, Y.-M. Huang, Q. Wang, Y.-L. Zhou, L. Deng, T. Xi, L. Ma, T. Hu, Q. Zhang, Y.-A. Chen, N.-L. Liu, X.-B. Wang, Z.-C. Zhu, C.-Y. Lu, R. Shu, C.-Z. Peng, J.-Y. Wang, and J.-W. Pan, "Satellite-to-ground quantum key distribution," Nature **549**, 43–47 (2017).
9. A. Carrasco-Casado, H. Kunimori, H. Takenaka, T. Kubo-Oka, M. Akioka, T. Fuse, Y. Koyama, D. Kolev, Y. Munemasa, and M. Toyoshima, "LEO-to-ground polarization measurements aiming for space QKD using small optical transponder (SOTA)," Opt. Express **24**, 12254–12266 (2016).
10. G. Vallone, D. Daniele, M. Tomasin, M. Schiavon, F. Vedovato, D. Bacco, S. Gaiarin, G. Bianco, V. Luceri, and P. Villoresi, "Satellite quantum communication towards GEO distances," Proc. SPIE **9900**, 99000J (2016).

11. C. Zhou, W. S. Bao, W. Chen, and H. W. Li, "Phase-encoded measurement-device-independent quantum key distribution with practical spontaneous-parametric-down-conversion sources," Phys. Rev. A **88**, 052333 (2013).

12. L. Wang, S. M. Zhao, L. Y. Gong, and W. W. Cheng, "Free-space measurement-device-independent quantum-key-distribution protocol using decoy states with orbital angular momentum," Chin. Phys. B **24**, 120307 (2015).

13. M. Mafu, A. Dudley, S. Goyal, D. Giovannini, M. McLaren, M. J. Padgett, T. Konrad, F. Petruccione, N. Lütkenhaus, and A. Forbes, "Higher-dimensional orbital-angular-momentum-based quantum key distribution with mutually unbiased bases," Phys. Rev. A **88**, 032305 (2013).

14. S. Zhao, W. Li, Y. Shen, Y. Yu, X. Han, H. Zeng, M. Cai, T. Qian, S. Wang, Z. Wang, Y. Xiao, and Y. Gu, "Experimental investigation of quantum key distribution over a water channel," Appl. Opt. **58**, 3902–3907 (2019).

15. Q. H. Lai, M. X. Luo, C. Zhan, J. Pieprzyk, and M. A. Orgun, "An improved coding method of quantum key distribution protocol based on Fibonacci-valued OAM entangled states," Phys. Lett. A **381**, 2922–2926 (2017).

16. M. Krenn, J. Handsteiner, M. Fink, R. Fickler, R. Ursin, M. Malik, and A. Zeilinger, "Twisted light transmission over 143 km," Proc. Natl. Acad. Sci. USA **113**, 13648–13653 (2016).

17. J. L. Liu and C. Wang, "Six-State quantum key distribution using photons with orbital angular momentum," Phys. Rev. A **27**, 110303 (2010).

18. X. Zhang, Y. He, Y. Cai, M. Su, X. Zhou, Y. Chen, S. Chen, Y. Xiang, L. Chen, C. Su, Y. Li, and D. Fan, "Coherent separation detection for orbital angular momentum multiplexing in free-space optical communications," IEEE Photon. J. **9**, 7903811 (2017).

19. J. Wang, J. Y. Yang, I. M. Fazal, N. Ahmed, Y. Yan, H. Huang, Y. Ren, Y. Yue, S. Dolinar, M. Tur, and A. E. Willner, "Terabit free-space data transmission employing orbital angular momentum multiplexing," Nat. Photonics **6**, 488–496 (2012).

20. A. E. Willner, H. Huang, Y. Yan, Y. Ren, N. Ahmed, G. Xie, C. Bao, L. Li, Y. Cao, Z. Zhao, J. Wang, M. P. J. Lavery, M. Tur, S. Ramachandran, A. F. Molisch, N. Ashrafi, and S. Ashrafi, "Optical communications using orbital angular momentum beams," Adv. Opt. Photon. **7**, 66–106 (2015).

21. Y. Zhang, P. Wang, L. Guo, W. Wang, and H. Tian, "Performance analysis of an OAM multiplexing-based MIMO FSO system over atmospheric turbulence using space-time coding with channel estimation," Opt. Express **25**, 19995–20011 (2017).

22. M. Krenn, R. Fickler, M. Fink, J. Handsteiner, M. Malik, T. Scheidl, R. Ursin, and A. Zeilinger, "Communication with spatially modulated light through turbulent air across Vienna," New J. Phys. **16**, 113028 (2014).

23. M. Malik, M. O'sullivan, B. Rodenburg, M. Mirhosseini, J. Leach, M. Lavery, M. J. Padgett, and R. W. Boyd, "Influence of atmospheric turbulence on optical communications using orbital angular momentum for encoding," Opt. Express **20**, 13195–13200 (2012).

24. F. Bouchard, K. Heshami, D. England, R. Fickler, R. W. Boyd, B.-G. Englert, L. L. Sánchez-Soto, and E. Karimi, "Experimental investigation of high-dimensional quantum key distribution protocols with twisted photons," Quantum **2**, 111 (2018).

25. G. Vallone, V. D'Ambrosio, A. Sponselli, S. Slussarenko, L. Marrucci, F. Sciarrino, and P. Villoresi, "Free-space quantum key distribution by rotation-invariant twisted photons," Phys. Rev. Lett. **113**, 060503 (2014).

26. J. P. Zhao, Y. Y. Zhou, B. Braverman, C. Liu, K. Pang, N. Steinhoff, G. Tyler, A. Willner, and R. Boyd, "Performance of real-time adaptive optics compensation in a turbulent channel with high-dimensional spatial-mode encoding," Opt. Express **28**, 15376–15391 (2020).

27. A. Sit, F. Bouchard, R. Fickler, J. Gagnon-Bischoff, H. Larocque, K. Heshami, D. Elser, C. Peuntinger, K. Günthner, B. Heim, C. Marquardt, G. Leuchs, R. Boyd, and E. Karimi, "High-dimensional intracity quantum cryptography with structured photons," Optica **4**, 1006–1010 (2017).

28. C. Daniele, D. Bacco, B. D. Lio, K. Ingerslev, and L. K. Oxenløwe, "Orbital angular momentum states enabling fiber-based high-

29. C. Daniele, B. D. Lio, D. Bacco, and L. K. Oxenløwe, "High-dimensional quantum communication: benefits, progress, and future challenges," Adv. Quantum Technol. **2**, 1900038 (2019).

30. F. Bouchard, A. Sit, F. Hufnagel, A. Abbas, Y. Zhang, K. Heshami, R. Fickler, C. Marquardt, G. Leuchs, R. W. Boyd, and E. Karimi, "Quantum cryptography with twisted photons through an outdoor underwater channel," Opt. Express **26**, 22563–22573 (2018).

31. F. Hufnagel, A. Sit, F. Grenapin, F. Bouchard, K. Heshami, D. England, Y. Zhang, B. J. Sussman, R. W. Boyd, G. Leuchs, and E. Karimi, "Characterization of an underwater channel for quantum communications in the Ottawa River," Opt. Express **27**, 26346–26354 (2019).

32. N. D. Leonhard, V.-N. Shatokhin, and A. Buchleitner, "Universal entanglement decay of photonic- orbital-angular-momentum qubit states in atmospheric turbulence," Phys. Rev. A **91**, 012345 (2015).

33. Y. X. Ren, H. Huang, G. D. Xie, N. Ahmed, Y. Yan, B. I. Erkmen, N. Chandrasekaran, M. P. J. Lavery, N. K. Steinhoff, M. Tur, S. Dolinar, M. Neifeld, M. J. Padgett, R. W. Boyd, J. H. Shapiro, and A. E. Willner, "Atmospheric turbulence effects on the performance of a free space optical link employing orbital angular momentum multiplexing," Opt. Lett. **38**, 4062–4065 (2013).

34. X. Y. Wang, S. H. Zhao, C. Dong, Z. D. Zhu, and W. Y. Gu, "Orbital angular momentum-encoded measurement device independent quantum key distribution under atmospheric turbulence," Quantum Inf. Process. **18**, 304 (2019).

35. C. Paterson, "Atmospheric turbulence and orbital angular momentum of single photons for optical communication," Phys. Rev. Lett. **94**, 153901 (2005).

36. G. A. Tyler and R. W. Boyd, "Influence of atmospheric turbulence on the propagation of quantum states of light carrying orbital angular momentum," Opt. Lett. **34**, 142–144 (2009).

37. M. Li, M. Cvijetic, Y. Takashima, and Z. Yu, "Evaluation of channel capacities of OAM-based FSO link with real-time wavefront correction by adaptive optics," Opt. Express **22**, 31337–31346 (2014).

38. X. Yin, H. Chang, X. Cui, J. Ma, Y. Wang, G. Wu, L. Zhang, and X. Xin, "Adaptive turbulence compensation with a hybrid input-output algorithm in orbital angular momentum-based free-space optical communication," Appl. Opt. **57**, 7644–7650 (2018).

39. H. Chang, X. Yin, X. Cui, X. Chen, Y. Su, J. Ma, Y. Wang, L. Zhang, and X. Xin, "Performance analysis of adaptive optics with a phase retrieval algorithm in orbital-angular-momentum-based oceanic turbulence links," Appl. Opt. **58**, 6085–6090 (2019).

40. K. He, X. Zhang, S. Ren, and J. Sun, "Deep residual learning for image recognition," in *Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition* (IEEE, 2016), pp. 770–778.

41. Y. Zhai, S. Fu, J. Zhang, X. Liu, H. Zhou, and C. Gao, "Turbulence aberration correction for vector vortex beams using deep neural networks on experimental data," Opt. Express **28**, 7515–7527 (2020).

42. W. Y. Wang and H.-K. Lo, "Machine learning for optimal parameter prediction in quantum key distribution," Phys. Rev. A **100**, 062334 (2019).

43. W. Q. Liu, P. Huang, J. Y. Peng, J. P. Fan, and G.-H. Zeng, "Integrating machine learning to achieve an automatic parameter prediction for practical continuous-variable quantum key distribution," Phys. Rev. A **97**, 022316 (2018).

44. P. Chaiwongkhot, K. B. Kuntz, Y. B. Zhang, A. Q. Huang, J. P. Bourgoin, S. H. Sajeed, N. Lütkenhaus, T. Jennewein, and V. Makarov, "Eavesdropper's ability to attack a free-space quantum-key-distribution receiver in atmospheric turbulence," Phys. Rev. A **99**, 062315 (2019).

45. Z. Q. Wang, R. Malane, and B. Burnett, "Satellite-to-Earth quantum key distribution via orbital angular momentum," Phys. Rev. Appl. **14**, 064031 (2020).

46. J. Liu, P. Wang, X. Zhang, Y. He, X. Zhou, H. Ye, Y. Li, S. Xu, S. Chen, and D. Fan, "Deep learning based atmospheric turbulence compensation for orbital angular momentum beam distortion and communication," Opt. Express **27**, 16671–16688 (2019).

47. L. C. Andrews, R. L. Phillips, C. Y. Hopen, and M. A. Al-Habash, "Theory of optical scintillation," J. Opt. Soc. Am. A **16**, 1417–1429 (1999).

48. V. Badrinarayanan, A. Kendall, and R. Cipolla, "SegNet: a deep convolutional encoder-decoder architecture for image segmentation," IEEE Trans. Pattern. Anal. **39**, 2481–2495 (2017).

49. F. C. Chen, "Back-propagation neural networks for nonlinear self-tuning adaptive control," IEEE Contr. Syst. Mag. **10**, 44–48 (1990).

50. S. Ruder, "An overview of gradient descent optimization algorithms," arXiv:1609.04747 (2016).

51. C. Liu, K. Pang, Z. Zhao, P. Liao, R. Zhang, H. Song, Y. Cao, J. Du, L. Li, H. Song, Y. Ren, G. Xie, Y. Zhao, J. Zhao, S. M. H. Rafsanjani, A. N. Willner, J. H. Shapiro, R. W. Boyd, M. Tur, and A. E. Willner, "Single-end adaptive optics compensation for emulated turbulence in a bi-directional 10-Mbit/s per channel free-space quantum communication link using orbital-angular-momentum encoding," Research **2019**, 8326701 (2019).

52. D. Rosenberg, C. Peterson, J. Harrington, P. Rice, N. Dallmann, K. Tyagi, K. McCabe, S. Nam, B. Baek, R. Hadeld, R. J. Hughes, and J. E. Nordholt, "Practical long-distance quantum key distribution system using decoy levels," New J. Phys. **11**, 045009 (2009).

53. R. Neo, M. Goodwin, J. Zheng, J. Lawrence, S. Leon-Saval, J. Bland-Hawthorn, and G. Molina-Terriza, "Measurement and limitations of optical orbital angular momentum through corrected atmospheric turbulence," Opt. Express **24**, 2919–2930 (2016).

54. V. N. Mahajan, "Strehl ratio for primary aberrations in terms of their aberration variance," J. Opt. Soc. Am. **73**, 860–861 (1983).

55. H. K. Lo, X. Ma, and K. Chen, "Decoy-state quantum key distribution," Phys. Rev. Lett. **94**, 230504 (2005).

56. D. Gottesman, H. K. Lo, N. Lutkenhaus, and J. Preskill, "Security of quantum key distribution with imperfect devices," Quant. Inf. Comp. **4**, 325–360 (2004).

57. W. Wang, F. Xu, and H. K. Lo, "Prefixed-threshold real-time selection method in free-space quantum key distribution," Phys. Rev. A **97**, 032337 (2018).