www.nature.com/scientificreports

scientific reports

OPEN

Measurement device-independent quantum key distribution with vector vortex modes under diverse weather conditions

Comfort Sekga[1] & Mhlambululi Mafu[2]✉

Most quantum key distribution schemes exploiting orbital angular momentum-carrying optical beams are based on conventional set-ups, opening up the possibility of detector side-channel attacks. These optical beams also suffer from spatial aberrations due to atmospheric turbulence and unfavorable weather conditions. Consequently, we introduce a measurement device-independent quantum key distribution implemented with vector vortex modes. We study the transmission of vector vortex and scalar beams through a turbulent atmospheric link under diverse weather conditions such as rain or haze. We demonstrate that a maximum secure key transmission distance of 178 km can be achieved under clear conditions by utilizing the vector vortex beams, which have been mainly ignored in the literature. When raindrops have a diameter of 6 mm and fog particles have a radius of 0.5 µm, the signals can reach 152 km and 160 km, respectively. Since these distances are comparable, this work sheds light into the feasibility of implementing measurement device-independent quantum key distribution using vector vortex modes under diverse weather conditions. Most significantly, this opens the door to practical secure quantum communications.

Quantum key distribution (QKD) allows sharing of information-theoretic cryptographic keys by distant users, even in the presence of a third party with unlimited computational power[1]. Over the past few years, there have been significant advances in the implementation of QKD[2–4] . Even though QKD has reached this milestone, challenges still need to be overcome before the technology can be fully adopted in real-world applications[5]. Among others, challenges relate to optimal secret key rate-transmission distance limit, infrastructure size and costs, imperfect physical devices, signal-to-noise ratio, and practical security[6–9]. A more practical solution for wide deployment of QKD is chip-based devices which offer advantages such as low cost, low power consumption, well-established batch fabrication techniques, improved performance, miniaturization, and enhanced functionality[10–12]. Other challenges concern imperfections in communication channels, for example, quantum data communications and networking, underwater communication, satellite communication, and fiber-optic communication[1,13–16]. A QKD protocol is ideally secure only when it utilizes perfect single-photon sources and detectors, which are currently unavailable[5,17]. Thus, device imperfections may expose security loopholes or allow side-channel attacks by an eavesdropper, compromising the security of practical implementations. Thus, it is imperative to design protocols robust against device imperfections, such as decoy-state QKD[18,19] and protocols that are tolerant to reference frame misalignment[20,21]. Another bottleneck to large-scale QKD deployment is high channel loss and decoherence, which results in a relatively low secret key rate[2,16]. Developing efficient methods and models that address these challenges is critical to achieving full-scale practical QKD for secure everyday communications. Therefore, a novel approach, measurement-device-independent QKD (MDI-QKD), was proposed to overcome the communication distance barrier between the participants[22,23]. The scheme allows two users (Alice and Bob) to send their optical signals to an untrusted intermediate node, i.e., Charlie, who performs the measurement, doubling the distance conventional QKD schemes can cover. Most significantly, MDI-QKD removes all detector side-channels from the measurement unit, widely recognized as one of the most vulnerable parts of QKD systems. Remarkably, a variant of the MDI-QKD, named the twin-field QKD[16], was discovered which is capable of scaling quadratically with channel transmittance marking another milestone towards the

[1]Department of Physics and Astronomy, Botswana International University of Science and Technology, P/Bag 16, Palapye, Botswana. [2]Department of Physics, Case Western Reserve University, Cleveland, OH 44106, USA. ✉email: mhlambululi.mafu@gmail.com

realization of long-distance quantum communications. The protocol has been studied in both theory[24–26] and experimentally[27] demonstrate its unique advantages.

The MDI-QKD has been extensively studied with optical signals encoded with polarization and phase characteristics of photons[28–35]. Although these degrees of freedom are more suitable for implementations with optical fibers, they are prone to birefringence effects that induce decoherence of signals and require interferometric stability[36]. Therefore, free-space optical links are generally preferred for long-distance QKD communications, especially in areas where fiber installation is not feasible, such as satellite-to-ground links[37–40]. Most significantly, the orbital angular momentum (OAM) states have recently attracted attention in free-space QKD owing to their rotational invariance in the transmission direction, eliminating error rates caused by misalignment of reference frames[41–46]. Furthermore, the OAM theoretically spans infinite Hilbert space, thereby enabling more information to be encoded per photon[47]. Despite this, under bad weather conditions or a turbulent atmosphere, the OAM beam experiences additional broadening, absorption, and backscattering due to random scattering on dust particles, aerosols, and/or precipitation, resulting in the loss of information[48–56]. While there is very limited study on the impact of other weather conditions, such as fog and rain on OAM beams, numerous studies exist regarding quantum optical beam propagation in turbulent atmospheres in the presence of haze and fog[37,57–66]. We highlight that OAM and the vector vortex modes have been recently exploited to analyse the performance of MDI-QKD[67–69]. While these studies are of great importance for QKD, they need more consideration of other practical scenarios that might limit the performance of QKD. For instance, Wang et al.[67] proposed a MDI-QKD that employs only OAM degree of freedom as carrier of information. However, OAM-carrying beams are more susceptible to losses in the turbulent atmosphere, especially those generated from the superposition of two OAM values. A more promising solution is coupling of polarization and OAM degrees of freedom which has proved to be more resilient to misalignment as they propagate through the turbulent environment. The MDI-QKD employing vortex beams, a hybrid of polarization and OAM degree of freedom, has been introduced in Ref.[68] . The performance of the protocol was analysed by considering the optical fiber channel. However, transmission of OAM carrying beams via conventional fiber is faced with a challenge of spatial-mode mixing which result in OAM mode information loss. More recently, Li et al.[69] proposed a similar work on hybrid polarization-OAM MDI-QKD. Their proposed protocol exploits high dimensional vector vortex beams to encode information and further employs a filter-based detection of Bell state set up which utilises six beam-splitters and eight detectors. The use of such detection method would result in lower signal-to-noise ratio due to the losses at the beam-splitters and low detection efficiency attributed to many detectors. In the context of QKD, such a loss would lead to lower yield and effective key rates, jeopardising the advantage provided hybrid polarization-OAM modes. Most significantly, in contrast, our proposed MDI-QKD protocol utilises a simple and easy to implement deterministic method of sorting the vector vortex mode which relies on interference of modes. The method is more efficient to filter based technique in terms of number resources and complexity of the scheme used in Charlie's measurement site. Notably, this has been demonstrated experimentally to perform better than filter based technique[70]. Another noticeable difference is that in our work, we emulate real-world conditions, particularly by simulating the performance of the protocol under diverse weather conditions. On a daily basis, communication under these weather conditions is inevitable, thus it is vital to evaluate the feasibility of MDI-QKD with vector vortex beams under such conditions. Also, in our protocol we consider the free-space link, which makes our protocol applicable to ground-satellite stations communication. While the work in Ref.[69] is a significant advance, it only provides the achievable key rates and transmission distances under consideration of optical fiber channel which is susceptible to losses induced by spatial-mode mixing.

Real-world deployment of QKD protocols often entails operating in diverse environments, including turbulent weather conditions. Diverse weather conditions cause interference in communication channels, causing fluctuations in the received signal quality, errors and inadvertently enhancing the potential for eavesdropping. As a result, demonstrating MDI-QKD security under such adverse scenarios provides assurance to withstand the challenges encountered during implementation. This validation is crucial for building trust in QKD systems and encouraging the widespread adoption of secure communication applications. Demonstrating the security of QKD protocols under turbulent weather conditions is a substantial advance toward advancing quantum communication in real-world scenarios. Besides aiding the development of robust QKD systems, this work also lays the foundation for exploring new, efficient, secure quantum communication protocols resilient to adverse weather conditions. Therefore, as a critical aspect of our contribution, we close this gap by proposing an MDI-QKD scheme implemented with vector vortex and scalar beams. This approach maximizes the advantages of both OAM states and MDI-QKD. A specific combination of OAM and polarization modes (hybrid states) provides these optical beams. As a result, any perturbation caused by misalignment of the polarization is precisely compensated for by an identical effect caused by misalignment of the OAM modes. This results in rotationally-invariant photon states. Another novel key aspect of this work is that we examine the performance of the proposed MDI-QKD scheme under diverse weather conditions to determine its viability since communicating information under varied weather conditions is necessary for real-world applications. We do this by evaluating key figures of merit, i.e., secure key rate and transmission distance. These results are of central importance, as they provide valuable insights into the feasibility of MDI-QKD based on vector vortex beams and pave the way for long-distance quantum secure communication.

Results

Operation of the OAM based MDI-QKD protocol.

We propose an MDI-QKD scheme implemented with vector vortex and scalar beams. Typically, in quantum optics, optical fields can be manipulated to create vector vortex or scalar beams. Vector vortex beams are states of light with spatially varying polarization in the transverse plane, i.e., inhomogeneous polarization states. The spatial and polarization degrees of freedom

(DoFs) are coupled in a non-separable manner, reminiscent of entanglement in quantum mechanics. Scalar beams, on the other hand, are completely separable in spatial and polarization modes, i.e., the spatial properties are not affected by changes in the polarization state of the photon. Specifically, vector vortex beams are defined by utilizing the notation adopted from quantum mechanics as[71]:

$$|\psi\rangle_{\theta,\ell} = \frac{1}{\sqrt{2}}(|\mathrm{R}\rangle|\ell\rangle + e^{i\theta}|\mathrm{L}\rangle|-\ell\rangle), \tag{1}$$

and the mutually unbiased bases (MUB) scalar beams are expressed as

$$|\phi\rangle_{\theta,\ell} = \frac{1}{\sqrt{2}}(|\mathrm{R}\rangle + e^{i\theta}|\mathrm{L}\rangle)|\pm\ell\rangle, \tag{2}$$

where R and L correspond to the right and left circular polarization states of light, and $|\pm\ell\rangle$ is an OAM state that carries $\pm\ell\hbar$ quanta of OAM. This quantity can be represented as

$$|\ell\rangle = A(r,z)W(r/R)\exp(i\ell\phi), \tag{3}$$

where A corresponds to an amplitude of the beam, r and ϕ are the radial and azimuthal coordinates, respectively. The term ℓ denotes an OAM topological charge, and it is an integer, while $W(r/R)$ denotes an aperture function with radius R expressed as[50]

$$W(r/R) = \begin{cases} 1, & \text{if } |r| < R \\ 0, & \text{otherwise.} \end{cases} \tag{4}$$

State preparation. The OAM based MDI-QKD is realized by manipulating the vector vortex and scalar beams in Eqs. (1) and (2) an with intra modal phase $\theta = 0$ or π to generate two mutually unbiased bases (MUB), vector basis $\mathbf{V} \in \{V_0 = \frac{1}{\sqrt{2}}(|\mathrm{R}\rangle|\ell\rangle + |\mathrm{L}\rangle|-\ell\rangle), V_1 = \frac{1}{\sqrt{2}}(|\mathrm{R}\rangle|\ell\rangle - |\mathrm{L}\rangle|-\ell\rangle)\}$ and the scalar basis $\mathbf{S} \in \{S_0 = \frac{1}{\sqrt{2}}(|\mathrm{R}\rangle + |\mathrm{L}\rangle)\||\ell\rangle, S_1 = \frac{1}{\sqrt{2}}(|\mathrm{R}\rangle - |\mathrm{L}\rangle)|-\ell\rangle\}$. The two communication parties, Alice and Bob randomly and independently choose a basis ($\mathbf{V}$ or $\mathbf{S}$), and a bit $r \in \{0,1\}$ where $r = 0 \in \{V_0, S_0\}$ and $r = 1 \in \{V_1, S_1\}$.

Next, they generate optical signals of intensity $\gamma \in \{\mu, \nu, 0\}$ (where μ is the intensity for signal states, ν for decoy states, and ω for vacuum states) prepared in the basis state of $\beta \in \{\mathbf{V}, \mathbf{S}\}$. Alice and Bob send their states to Charlie via the quantum channel.

Measurement. Charlie let the two optical pulses interfere in the symmetric beam splitter (BS) and performs mode sorting and Bell state measurement. When the photons carrying OAM states from Alice and Bob arrive at 50:50 BS, a Hong-Ou-Mandel (HOM) effect occurs. In particular, according to the HOM effect, two indistinguishable photons incident at each input port of BS will exit at the same output port of BS. However, four distinct possibilities exist with distinguishable photons: the two photons exit the BS together through the same output port, or the photons exit the BS separately through different output arms. Precisely, for the initial state $|\Psi\rangle = |1\rangle_{1,\mathbf{M}}|1\rangle_{2,\mathbf{N}} = |\mathbf{M}\rangle_1|\mathbf{N}\rangle_2 = \hat{a}^{\dagger}_{1,\mathbf{M}}\hat{b}^{\dagger}_{2,\mathbf{N}}|0\rangle$, the transformation relations of the two photons incident at the two inputs of BS can be described as

$$\begin{aligned} \hat{a}^{\dagger}_{1,\mathbf{M}}\hat{b}^{\dagger}_{2,\mathbf{N}}|0\rangle &\overset{BS}{\mapsto} \frac{1}{2}(\hat{c}^{\dagger}_{3,\mathbf{M}} + \hat{d}^{\dagger}_{4,\mathbf{M}})(\hat{c}^{\dagger}_{3,\mathbf{N}} - \hat{d}^{\dagger}_{4,\mathbf{N}})|0\rangle \\ &= \frac{1}{2}(\hat{c}^{\dagger}_{3,\mathbf{M}}\hat{c}^{\dagger}_{3,\mathbf{N}} - \hat{c}^{\dagger}_{3,\mathbf{M}}\hat{d}^{\dagger}_{4,\mathbf{N}} + \hat{c}^{\dagger}_{3,\mathbf{N}}\hat{d}^{\dagger}_{4,\mathbf{M}} - \hat{d}^{\dagger}_{4,\mathbf{N}}\hat{d}^{\dagger}_{4,\mathbf{N}})|0\rangle, \end{aligned} \tag{5}$$

where $\hat{a}^{\dagger}, \hat{b}^{\dagger}, \hat{c}^{\dagger}$ and $\hat{d}^{\dagger}$ are creation operators at input and output ports 1,2 and 3,4, respectively. The notations $\mathbf{M}$ and $\mathbf{N}$ correspond to the degree of freedom, such as polarization and orbital angular momentum. For the two input photons with the same degree of freedom that are identical, the second and third terms in Eq. (5) disappears. For simplicity, for initial states, $|\psi\rangle$ and $|\varphi\rangle$ the action of the beam-splitter can also be illustrated as

$$|\psi\rangle_1|\varphi\rangle_2 \overset{BS}{\mapsto} \frac{1}{2}(|\psi\rangle_3|\overline{\varphi}\rangle_3 - |\psi\rangle_3|\varphi\rangle_4 + |\overline{\psi}\rangle_4|\overline{\varphi}\rangle_3 - |\overline{\psi}\rangle_4|\varphi\rangle_4) \tag{6}$$

where $|\bar{x}\rangle$ is the reflected state. Based on the beam-splitter interactions, we describe observations from each basis as follows.

Vector basis

Based on a method described in Ref.[71], two vector vortex states are sorted by combining geometric phase control and multipath interference (see Fig. 1). Once photons exit the first BS, they pass through a polarization grating. This separates left and right circularly polarized photons into two paths based on their polarization according to

$$|\psi\rangle_{\theta,\ell} = \frac{1}{\sqrt{2}}(|\mathrm{R}\rangle_a|\ell\rangle_a + e^{i\theta}|\mathrm{L}\rangle_b|-\ell\rangle_b). \tag{7}$$

As a result of interference between the photons in paths a and b at the second BS, the resultant state is expressed as follows

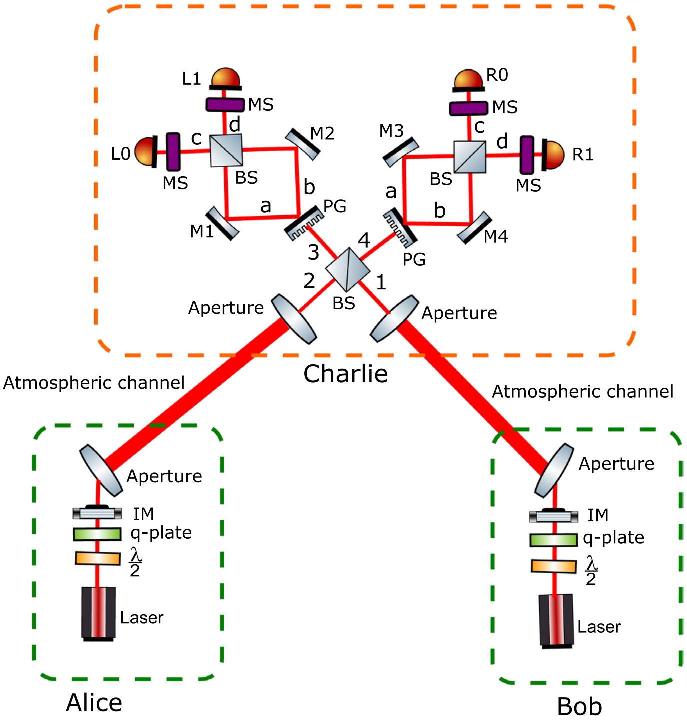

Figure 1. An illustration of the proposed OAM-based MDI-QKD. Alice and Bob prepare two mutually unbiased basis states (**V**, **S**) and send them to Charlie through the unsecure channel. The $\lambda/2$ plate and the q-plate are used to generate a set of vector and scalar modes, which are then attenuated to intensity $\gamma \in \{\mu, \nu, 0\}$ using intensity modulator IM. Next, the telescope collimates the quantum states with a finite aperture. They are then sent through a free atmospheric space link to the measurement site controlled by Charlie. The optical states are then collected by the telescope and allowed to interfere with the symmetric beam splitter (BS). Next, the photons are passed through the polarization grating that separates the left and right circularly polarized photons, then guided by mirrors (M1, M2, M3, M4) towards a beam-splitter (BS). As a result, the photons are then measured using the mode sorters (MS) that map OAM to position and then detected by the detectors (L0, R0, L1, R1). This illustration was generated using Inkscape 1.1 software.

$$|\psi'\rangle_{\theta,\ell} = \frac{1-e^{i\theta}}{2}|\ell\rangle_c + i\frac{1+e^{i\theta}}{2}|-\ell\rangle_d. \tag{8}$$

Note that due to parity differences in the reflections in each input port, the polarisation of the two paths is inherently reconciled in each output port of the beam splitter. Also, it is worth stating that at this stage, it is not essential to keep the polarisation in the expression of the photon state since the polarisation details are defined in the path. The OAM carrying photons from the outputs c and d are then measured by passing them through the OAM mode sorter and coincidently detected by two detectors L0 and L1 or R0 and R1. According to Eq. (8) when Alice and Bob prepare the same vector states, we observe a click from one detector along the same path (3 or 4) from the output ports of the first BS. An error corresponds to a click from two detectors within the same path (3 or 4) when the same states are sent by two parties . However, if Alice and Bob prepare vector vortex beams of different states, two detectors are triggered at opposite ends, that is, (L0, R1) or (L1, R0) or within the same path (3 or 4), i.e., (L0, L1) or (R0, R1). For instance, suppose that Alice sent $|\varphi\rangle_2 = \frac{1}{\sqrt{2}}(|\mathrm{R}\rangle|\ell\rangle - |\mathrm{L}\rangle|-\ell\rangle)$ and Bob sent vector vortex state $|\psi\rangle_1 = \frac{1}{\sqrt{2}}(|\mathrm{R}\rangle|\ell\rangle + |\mathrm{L}\rangle|-\ell\rangle)$, then based on the first BS interactions we have

$$\begin{aligned}|\psi\rangle_1|\varphi\rangle_2 \overset{BS}{\mapsto} \frac{1}{2}([&\frac{1}{\sqrt{2}}(|\mathrm{R}\rangle|\ell\rangle + |\mathrm{L}\rangle|-\ell\rangle)]_3 \otimes [\frac{1}{\sqrt{2}}(|\mathrm{R}\rangle|\ell\rangle - |\mathrm{L}\rangle|-\ell\rangle)]_3 - [\frac{1}{\sqrt{2}}(|\mathrm{R}\rangle|\ell\rangle + |\mathrm{L}\rangle|-\ell\rangle)]_3 \\ &\otimes [\frac{1}{\sqrt{2}}(|\mathrm{R}\rangle|\ell\rangle - |\mathrm{L}\rangle|-\ell\rangle)]_4 + [\frac{1}{\sqrt{2}}(|\mathrm{R}\rangle|\ell\rangle + |\mathrm{L}\rangle|-\ell\rangle)]_4 \otimes [\frac{1}{\sqrt{2}}(|\mathrm{R}\rangle|\ell\rangle \\ &- |\mathrm{L}\rangle|-\ell\rangle)]_3 - [\frac{1}{\sqrt{2}}(|\mathrm{R}\rangle|\ell\rangle + |\mathrm{L}\rangle|-\ell\rangle)]_4 \otimes [\frac{1}{\sqrt{2}}(|\mathrm{R}\rangle|\ell\rangle - |\mathrm{L}\rangle|-\ell\rangle)]_4).\end{aligned} \tag{9}$$

From the above result, we observe that there are four distinct probable scenarios; 25% probability that both $|\psi\rangle_1$ and $|\varphi\rangle_2$ will exit at output port 3; 25% probability that $|\psi\rangle_1$ exit at port 3 and $|\varphi\rangle_2$ leaves at port 4; 25% chance that $|\psi\rangle_1$ exit at port 4 and $|\varphi\rangle_2$ exit at output arm 3; 25% probability that both states leave the BS at output arm

4. Without loss of generality, let us consider a case where $|\psi\rangle_1$ exit at port 4 and $|\varphi\rangle_2$ exit at port 3, which is indicated by the third term in Eq. (9). After going through a polarization grating, the states transform as follows

$$\frac{1}{\sqrt{2}}(|\mathrm{R}\rangle_3|\ell\rangle_3 + e^{i\theta}|\mathrm{L}\rangle_3|-\ell\rangle_3)\; PG\; \frac{1}{\sqrt{2}}(|\mathrm{R}\rangle_{3,a}|\ell\rangle_{3,a} + e^{i\theta}|\mathrm{L}\rangle_{3,b}|-\ell\rangle_{3,b}). \tag{10}$$

Note that we have introduced a phase factor $e^{i\theta}$, with $\theta = \pi$. After passing through the second BS we obtain

$$|\psi\rangle_{\theta,\ell} = \frac{1-e^{i\theta}}{2}|\ell\rangle_{3,c} + i\frac{1+e^{i\theta}}{2}|-\ell\rangle_{3,d}, \tag{11}$$

Now, substituting back $\theta = \pi$ into Eq. (11) we obtain

$$|\psi\rangle_{\pi,\ell} = |\ell\rangle_{3,c}. \tag{12}$$

For the photon leaving through port 4, we have

$$\frac{1}{\sqrt{2}}(|\mathrm{R}\rangle_4|\ell\rangle_4 + e^{i\theta}|\mathrm{L}\rangle_4|-\ell\rangle_4)\; PG\; \frac{1}{\sqrt{2}}(|\mathrm{R}\rangle_{4,a}|\ell\rangle_{4,a} + e^{i\theta}|\mathrm{L}\rangle_{4,b}|-\ell\rangle_{4,b}), \tag{13}$$

where $\theta = 0$. After passing through the BS, we obtain

$$|\psi\rangle_{\theta,\ell} = \frac{1-e^{i\theta}}{2}|\ell\rangle_{4,c} + i\frac{1+e^{i\theta}}{2}|-\ell\rangle_{4,d}, \tag{14}$$

Substituting $\theta = 0$ into Eq. (14) we obtain

$$|\psi\rangle_{0,\ell} = i|-\ell\rangle_{4,d}. \tag{15}$$

Therefore, this scenario will lead to click in detectors L0 and R1. Table 1 depicts the results of other probable occurrences.

Scalar basis

Scalar modes are sorted in an analogous manner to vector modes. As a result, the two states that form the basis can be described as follows

$$|\phi\rangle_{\theta,\ell} = \frac{1}{\sqrt{2}}(|\mathrm{R}\rangle_a|\ell\rangle_a + e^{i\theta}|\mathrm{L}\rangle_b|\ell\rangle_b) \tag{16}$$

and

$$|\phi\rangle_{\theta,-\ell} = \frac{1}{\sqrt{2}}|\mathrm{R}\rangle_a|-\ell\rangle_a + e^{i\theta}|\mathrm{L}\rangle_b|-\ell\rangle_b. \tag{17}$$

The modes are separated into two paths a and b using a polarization grating and then allowed to interfere in the BS. The output state for Eq. (16) is given by

$$|\psi'\rangle_{\theta,\ell} = \frac{1-e^{i\theta}}{2}|\mathrm{R}\rangle_c|\ell\rangle_c + i\frac{1+e^{i\theta}}{2}|\mathrm{L}\rangle_d|\ell\rangle_d. \tag{18}$$

and the output state for Eq. (17) is

$$|\psi'\rangle_{\theta,-\ell} = \frac{1-e^{i\theta}}{2}|\mathrm{R}\rangle_c|-\ell\rangle_c + i\frac{1+e^{i\theta}}{2}|\mathrm{L}\rangle_d|-\ell\rangle_d. \tag{19}$$

			Charlie's measurement results			
			$\|\Psi\rangle^+$		$\|\Psi\rangle^-$	
Basis	**Alice**	**Bob**	**L0, L1**	**R0, R1**	**L0, R1**	**L1, R0**
Vector basis	V_0	V_0	0	0	0	0
	V_0	V_1	0.25	0.25	0.25	0.25
	V_1	V_0	0.25	0.25	0.25	0.25
	V_1	V_1	0	0	0	0
Scalar basis	S_0	S_0	0	0	0	0
	S_0	S_1	0.25	0.25	0.25	0.25
	S_1	S_0	0.25	0.25	0.25	0.25
	S_1	S_1	0	0	0	0

Table 1. Probability distribution for Bell state measurement results announced by Charlie when both Alice and Bob choose the same basis.

The intramodal phases are chosen to be $\theta = 0$ and $\theta = \pi$ for states in Eq. (18) and Eq. (19), respectively. Therefore, the output states can be reduced to $|\psi'\rangle_{\pi,\ell} = |\mathrm{R}\rangle|\ell\rangle$ and $|\psi'\rangle_{0,-\ell} = i|\mathrm{L}\rangle|-\ell\rangle$. These results indicate that when Alice and Bob prepare the same scalar states, only one detector will be triggered within the relay. Alternatively, if two parties prepare scalar states with opposite OAM, this will result in the click of two detectors in different output paths of the first BS, i.e., a combination of either (L0, R1) or (R0, L1) or the two detectors triggered within the same path from the first BS, that is, (L0, L1) or (R0, R1). There is also an error in this basis if both detectors within the same path (path 3 or 4) are triggered when the same states are sent.

Announcement. Following photon detection, Charlie announces successful measurement events. A successful detection event corresponds to a coincidence click in two detectors (associated with orthogonal OAM). In the proposed protocol, the detectors L0 and R0 are used to detect OAM state $|\ell\rangle$ while L1 and R1 are used to detect OAM state $|-\ell\rangle$. Thus, a combination of (L0, L1), (R0, R1) , (L0, R1) and (R0, L1) corresponds to successful detection. We define a click in detectors (L0,L1) or (R0, R1) to indicate projection into Bell state $|\Psi\rangle^{+} = \frac{1}{\sqrt{2}}(|01\rangle_{\mathrm{LL}} + |10\rangle_{\mathrm{RR}})$, while a click in detectors (L0, R1) or (R0, L1) correspond to Bell state $|\Psi\rangle^{-} = \frac{1}{\sqrt{2}}(|01\rangle_{\mathrm{LR}} - |10\rangle_{\mathrm{LR}})$.

Sifting. When Charlie announces a successful Bell state measurement result, Alice and Bob publish their basis choices and intensity over an authenticated public channel. Bob flips his key bits to match Alice's as illustrated in Table 2.

The random bit values $r \in \{0, 1\}$ in each basis are assigned as $r = 0 \in \{V_0, S_0\}$ and $r = 1 \in \{V_1, S_1\}$. The random bits obtained from the vector basis are then exploited by Alice and Bob in order to form a raw key. The random bits from the scalar basis are used to estimate the upper bound in eavesdropper's information. Then, the two communicating parties perform error correction and privacy amplification in order to obtain a secret key that can be used for secure communication.

Security analysis. We provide a security analysis for our scheme along the lines of Ref[29], which makes use of a photon-number channel model and the Gottesman-Lo-Lütkenhaus-Preskill (GLLP) security proof[72]. In particular, the security proof is based on time-reversed EPR-based QKD protocol and the notion of virtual protocol. In this virtual setting, it is assumed that Alice possesses a virtual qubit, and she entangles it with a quantum signal she prepared before sending it to Charlie. Similarly, Bob uses a virtual qubit to prepare an entangled state with the quantum signal he sends to Charlie. Now, in principle, the two could rather store their virtual qubits in her quantum memory and wait for the announcement of successful Bell state measurements by Charlie. The successful measurements of the signals sent by Alice and Bob automatically imply that their virtual qubits are entangled by virtue of entanglement swapping. After that, Alice and Bob can now perform a measurement on their virtual qubits to determine which state they are sending to Charlie. In such virtual qubits setting, the protocol is directly equivalent to an entanglement-based protocol and its security can be proved following the technique proposed in Ref[73]. The key rate formula for the proposed MDI-QKD is given by

$$K \geq q\{Q^{\mathbf{V}}_{\mu_a\mu_b} f_{\mathrm{EC}} H(E^{\mathbf{V}}_{\mu_a\mu_b}) + Q^{\mathbf{V}}_{11}(1 - H(e^{\mathbf{S}}_{11}))\}, \tag{20}$$

where q is the basis sift factor; parameter μ denotes the signal intensity; $Q^{\mathbf{V}}_{\mu_a\mu_b}$ and $E^{\mathbf{V}}_{\mu_a\mu_b}$ are the overall gain and quantum bit error rate (QBER) in the vector basis, respectively. The quantities $Q^{\mathbf{V}}_{11}$ and $e^{\mathbf{S}}_{11}$ indicate the gain and error rate of individual photon components. We evaluate these parameters using the decoy state theory presented in the "Methods" section.

Propagation through perturbing media. We examine how the OAM-carrying optical beams employed in our proposed protocol are affected by various weather conditions during their propagation through the free space link. When OAM beams propagate through atmospheric channels, they undergo aberrations, primarily caused by beam extinction and turbulence effects. Extinction occurs due to absorption and scattering by molecules and aerosols, as opposed to the latter caused by changes in the refractive index of the atmosphere. Atmospheric effects are strongly related to the transmittance, η, which is defined as the probability of a photon being successfully transmitted through the channel and being detected. This is a critical factor in evaluating QKD protocol performance. To study the influence of various weather conditions on the transmission of OAM signals in the MDI-QKD protocol, we make use of some well-developed atmospheric optical communications models.

Alice and Bob	Charlie's measurement results	
	$\|\Psi\rangle^{+}$	$\|\Psi\rangle^{-}$
Vector basis	Bit flip	Bit flip
Scalar basis	Bit flip	Bit flip

Table 2. Post-processing of raw key in the sifting step. Bob flips his bits to ensure correct correlation with Alice's bit.

OAM carrying photons through turbulence. As OAM states propagate through free space, their purity is compromised due to the turbulence that occurs in the atmosphere. As a result of fluctuations in the refractive index of the atmosphere caused by turbulence, a propagating optical beam will exhibit random phase aberrations. Based on the methods described in Ref.[50], we investigate the effects of random phase aberrations on the received OAM state. First, the original optical field at the transmitter is assumed to be given by

$$A(\mathbf{r}) = A_0 W(r/R) e^{i\ell\phi}, \tag{21}$$

where A_0 is the (spatially uniform) field amplitude, and other parameters are defined as in Eq. (3). After undergoing scrambling in the turbulent atmosphere, the field at the receiver aperture can be represented as

$$V(\mathbf{r}) = A_0 W(r/R) e^{i\ell\phi} e^{i\vartheta(\mathbf{r})}, \tag{22}$$

where $\vartheta(\mathbf{r})$ represents the turbulence-induced wavefront distortion at the receiver. Notably, the quantity $\exp(i\vartheta(\mathbf{r}))$ can be expanded in the Fourier series as

$$e^{i\vartheta(r,\phi)} = \sum_{\ell=-\infty}^{\infty} C_k(r) e^{ik\phi}, \tag{23}$$

where the expansion coefficients $C_k(r)$ are given by

$$C_k(r) = \frac{1}{2\pi} \int_0^{2\pi} \mathrm{d}^{\mathrm{i}\vartheta(\mathrm{r},\phi)} \mathrm{e}^{-\mathrm{ik}\phi}. \tag{24}$$

The received field $V(\mathbf{r})$ can be expanded in a similar manner as $V(r,\phi) = \sum_{\ell=-\infty}^{\infty} V_n(r)\exp(in\phi)$, where each Fourier component $V_n(r)$ is given by

$$V_n(r) = \frac{1}{2\pi} \int_0^{2\pi} \mathrm{d}\phi \mathrm{V}(\mathrm{r},\phi) \mathrm{e}^{-\mathrm{in}\phi}. \tag{25}$$

By substituting Eqs. (22) and (23) into Eq. (25) yields

$$V_n(r) = \frac{A_0}{2\pi} W(r/R) \sum_{\ell=-\infty}^{\infty} C_\ell(r) \int_0^{2\pi} \mathrm{d}\phi \mathrm{e}^{-\mathrm{i}(\mathrm{n}-\ell-\mathrm{m})\phi}. \tag{26}$$

The above expression can be further reduced to

$$V_n(r) = \frac{A_0}{2\pi} W(r/R) C_\Delta(r), \tag{27}$$

by considering that the integral in Eq. (25) equals 2π when $m - k - \ell = 0$ and vanishes otherwise. The last expression defines Δ as $\Delta = m - \ell$. The connection between azimuthal Fourier components $C_\Delta(r)$ associated with atmospheric turbulence and the OAM state of the received field emanating from Eq. (27) allows one to determine the amount of radiation that remains in the initial OAM state based on the spatial component of the azimuthal Fourier spectrum $\exp(i\vartheta(\mathbf{r}))$. Practically, this radiation is determined in terms of power contained in each OAM state of the received field. The total power collected by the receiver is given by

$$P = \frac{1}{2}\epsilon_0 \int \mathrm{d}\mathbf{r} \mathrm{W}(\mathrm{r}/\mathrm{R}) \mathrm{V}^*(\mathbf{r}) \mathrm{V}(\mathbf{r}) = \frac{1}{2}\epsilon_0 |\mathrm{A}_0|^2 \pi \mathrm{R}^2, \tag{28}$$

Accordingly, this power is constituted by a combination of different (orthogonal) modes of OAM modes of the field according to

$$P = \sum_{\Delta=-\infty}^{\infty} P_\Delta, \text{ where } \mathrm{P}_\Delta = 2\pi |\mathrm{A}_0|^2 \int_0^{\mathrm{R}} \mathrm{drr} \mathrm{C}_\Delta^*(\mathrm{r}) \mathrm{C}_\Delta(\mathrm{r}). \tag{29}$$

An important parameter of interest is the ratio $\eta_{\text{turb}} = P_\Delta / P$ of the power contained in each OAM mode given by

$$\eta_{\text{turb}} = \frac{2}{R^2} \int_0^R \mathrm{drr} \mathrm{C}_\Delta^*(\mathrm{r}) \mathrm{C}_\Delta(\mathrm{r}). \tag{30}$$

Using this parameter, we can determine the probability that the OAM quantum number m of the received state differs from that of the transmitted state ℓ by the amount $\Delta = m - \ell$. The result presented in Eq. (30) applies to any realization of atmospheric turbulence. Generally, η_{turb} is described as an ensemble average according to the form

$$\eta_{\text{turb}} = K \int_0^R \mathrm{drr} \int_0^{2\pi} \mathrm{d}\phi_1 \int_0^{2\pi} \mathrm{d}\phi_2 \langle \mathrm{e}^{-[\vartheta(\mathrm{r},\phi_1) - \vartheta(\mathrm{r},\phi_2)]} \rangle \times e^{i\Delta(\phi_1 - \phi_2)}, \tag{31}$$

where $K = 1/(2\pi^2 R^2)$. By considering the Kolmogorov turbulence theory, the above expression can be further reduced to

$$\eta_{\text{turb}} = \frac{1}{\pi}\int_0^1 \mathrm{d}\rho\rho \int_0^{2\pi} \mathrm{d}\phi \mathrm{e}^{-3.44(\mathrm{D}/\mathrm{r}_0)^{5/3}(\rho\sin(\phi/2))^{5/3}} \\ \times \cos(\Delta\phi), \tag{32}$$

where $\rho = r/R$. Here D denotes the receiver aperture diameter, and the parameter r_0 corresponds to Fried's coherence diameter, which is described as

$$r_0 = 0.1853\left(\frac{\lambda^2}{C_n^2 L}\right), \tag{33}$$

where λ is the wavelength of the optical beam, L is the transmission distance and C_n^2 is the refractive-index structure parameter, which gives the strength of atmospheric turbulence.

OAM carrying photons through rain. OAM carrying beams are also highly susceptible to adverse weather conditions, such as rain. Generally, rain attenuates beam energy in free space link QKD due to the absorption and scattering of rain droplets. The phenomenon is known as rain extinction[62]. An empirical formula has been developed to measure rain extinction in relation to rainfall intensity, and is defined as[62,74]:

$$\alpha_{\text{rain}} = 1.45 I_{\text{rain}}^{0.64}, \tag{34}$$

where I_{rain} is the rainfall intensity, and α_{rain} is the rain extinction. Using Law-Parsons raindrop size distribution, rainfall intensity is also related to raindrop size as[59,62]:

$$I_{\text{rain}} = 6\pi \times 10^{-4}\int_0^{\infty} n(D_{\text{rain}})D_{\text{rain}}^3 v(D_{\text{rain}})dD_{\text{rain}}. \tag{35}$$

The above expression can be further simplified by dropping the integral and expressed analytically as

$$I_{\text{rain}} = \frac{6\pi\, n(D_{\text{rain}})D_{\text{rain}}^3 v(D_{\text{rain}})}{10^4 m(D_{\text{rain}})}, \tag{36}$$

where D_{rain} denotes diameter of the rain droplet, $n(D_{\text{rain}})$ corresponds to the number of rain-droplets, $v(D_{\text{rain}})$ is terminal velocity of rain-droplets and $m(D_{\text{rain}})$ is percentage of volume.

The transmittance associated with rain extinction for horizontal paths with length L is given by

$$\eta = e^{-\alpha_{\text{rain}} L}. \tag{37}$$

OAM carrying photons through a foggy atmosphere. This section examines the effects of foggy weather conditions on free space QKD. In general, fog is composed of a large number of small water droplets suspended in the air. Beam degradation caused by fog particles is largely reflected in scattering and absorption contributions, which is known as beam extinction. There are two main factors that influence the extinction effects: the radius of the fog particle and the wavelength of the beam. For modeling the scattering and absorption effect, we consider the Mie scattering theory[75], which is more appropriate for evaluating the scattering of particles approximately the wavelength of a beam of light. The Mie theory uses Maxwell equations to characterize beam extinction induced by fog particles. We consider the case of a beam perturbed by homogeneous spherical particles that are isotropic. According to Ref.[76], the relationship between scattered and incident beams is defined as a function of the amplitudes of electric field components as

$$\begin{bmatrix} E_S^V \\ E_S^H \end{bmatrix} = \frac{\exp(ikr)}{-ikr}\begin{bmatrix} S_1 & S_3 \\ S_2 & S_4 \end{bmatrix}\begin{bmatrix} E_V^i \\ E_H^i \end{bmatrix}. \tag{38}$$

The subscripts V and H refer to the vertical and polarization components of the electric field, respectively. The parameter k represents the wave number, and the element S_i represents the scattering matrix. Its value is determined by particle diameter, refractive index, beam wavelength, and scattering polar angle. According to the scattering matrix, the value is determined by the particle shape, scale, and refractive index. In the case of spherical particles, $S_3 = 0$, $S_4 = 0$, and the complex solution of the other elements, S_1 and S_2, can be written as follows

$$\begin{aligned} S_1(\theta) &= \sum_{n=1}^{\infty}\frac{2n+1}{n(n+1)}(a_n\pi_n + b_n\tau_n), \\ S_2(\theta) &= \sum_{n=1}^{\infty}\frac{2n+1}{n(n+1)}(b_n\pi_n + a_n\tau_n), \end{aligned} \tag{39}$$

where

$$\pi_n = \frac{P_n^1(\cos\theta)}{\sin\theta} = \frac{dP_n(\cos\theta)}{d(\cos\theta)} \tag{40}$$

$$\tau_n = \frac{dP_n^1(\cos\theta)}{d(\cos\theta)}. \tag{41}$$

According to the above expressions, $P_n^1(\cos\theta)$ is the first kind of Legendre function of order n. The scattering polar angle is defined by the parameter θ. The Mie scattering quantities a_n and b_n defined in Eq. (39) are obtained from the Bessel functions as

$$a_n = \frac{\psi_n(x)\psi_n'(mx) - m\psi_n'(x)\psi_n(mx)}{\xi_n(x)\xi_n'(mx) - m\xi_n'(x)\xi_n(mx)}, \tag{42}$$

$$b_n = \frac{m\psi_n(x)\psi_n'(mx) - \psi_n'(x)\psi_n(mx)}{m\xi_n(x)\xi_n'(mx) - \xi_n'(x)\xi_n(mx)}, \tag{43}$$

where for some variables y, $\psi_n(y) = \sqrt{\frac{\pi y}{2}}J_{n+1/2}(y)$, $\xi_n(y) = \sqrt{\frac{\pi y}{2}}H_{n+1/2}(y)$ and $J_{n+1/2}(X)$, $H_{n+1/2}(X)$ denote the first and second kind of semi-integral order Bessel function and Hankel function, respectively. The parameter m represents the refractive index of fog particles, which is estimated as $m = 1.33 + i0.003$, while the quantity x is related to the particle's circumference and wavelength λ according to

$$x = \frac{2\pi R_{\text{fog}}}{\lambda}, \tag{44}$$

where R_{fog} is the particle's radius.

The coefficients a_n and b_n are useful for determining the extinction efficiency factor caused by fog particles, which can be obtained by[75]

$$Q_{\text{ext}} = \frac{\lambda^2}{2\pi}\sum_{n=1}^{\infty}(2n+1)\text{Re}(a_n + b_n). \tag{45}$$

Thus, the beam attenuation coefficient of fog can be calculated as follows

$$\alpha_{\text{fog}} = \pi R_{\text{fog}}^2 Q_{\text{ext}} N_{\text{fog}}, \tag{46}$$

where N_{fog} denotes the number of particles per unit volume.

Simulation. Based on the simulation parameters provided in Table 3, we analyze the performance of OAM-based MDI-QKD under various weather conditions. To begin with, we examine what impact turbulent atmospheric conditions have on the transmitted OAM states. We evaluate the probabilities of obtaining different OAM measurements, η_{turb} for OAM beams propagating under Kolmorogov turbulence using Eq. (32).

According to Fig. 2, as the receiver aperture diameter D becomes comparable to the Fried parameter r_0, the probability of obtaining the original OAM states ($\Delta\ell = 0$) at the receiver aperture decreases asymptomatically. When $D \leq r_0$ is small, phase aberrations are weak, and OAM scattering is small, but as the Fried parameter approaches the receiver aperture diameter, it becomes more likely that OAM scattering will occur. The curves showing the probability of receiving scrambled OAM states i.e., $\Delta\ell > 0$ initially increase with increasing turbulence levels and ultimately decrease with further increase. At high turbulence levels, optical power is spread across various OAM modes, resulting in a decreased probability of detecting a specific OAM value.

Figure 3 shows a relationship between key rate and transmission distance for different deviations $\Delta\ell$ from original OAM states induced by turbulence. The results demonstrate that the key rate and maximum transmission distance decrease with increasing deviation from originally transmitted OAM states. Notably, we observe that the achievable key rate remains comparable to the normal condition without deviation of transmitted OAM states for a lower aberration of OAM states, e.g., for $\Delta\ell = 1$.

In Fig. 4, we analyze the impact of rain droplet size on transmittance based on the Law-Parson model depicted in Eq. (36). The transmittance decreases as the size of the rain droplets increases. As the size of rain droplets increases from 3 mm onwards, a sharp drop in transmittance is observed. In Fig. 5, we plotted the achievable key rate against the transmission distance for various sizes of rain droplets. As can be seen from the results, larger rain droplets (which are directly proportional to rainfall intensity) negatively influence key rate and transmission distance. Also, we observe that with a clear atmosphere, the maximum transmission distance is approximately 178 km, while with a rainfall of 2 mm diameter droplets, the maximum distance is 160 km. It should be noted that the distance is further reduced with an increase in the diameter of the rain droplets. A further study was carried out to evaluate the influence of fog particle size on the extinction of optical signals in Fig. 6 based on Eq. (46). Based on the results, the extinction coefficient increases as the fog particle radius increases, indicating an increase in optical absorption and scattering. In Fig. 7, we generated curves for key rates against transmission distances for different sizes of fog particles. Clearly, the achievable key rate and maximum transmission distance decrease as the fog particle size increases. However, we discover that the protocol's performance under foggy conditions is still comparable to the performance under typical atmospheric conditions. For instance, if we set

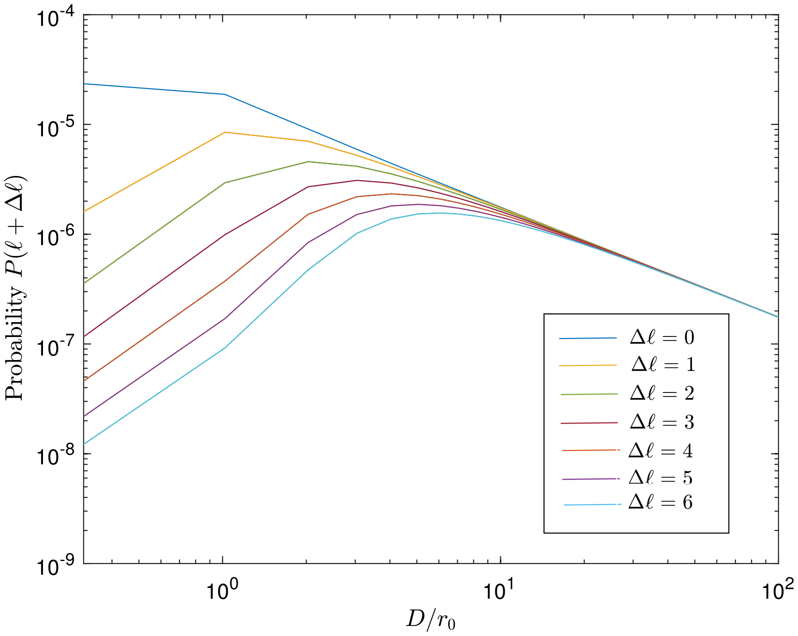

Figure 2. This plot illustrates the probability of receiving adjacent OAM states (Transmittance), η_{turb} against the ratio of the aperture diameter D to the Fried parameter r_0.

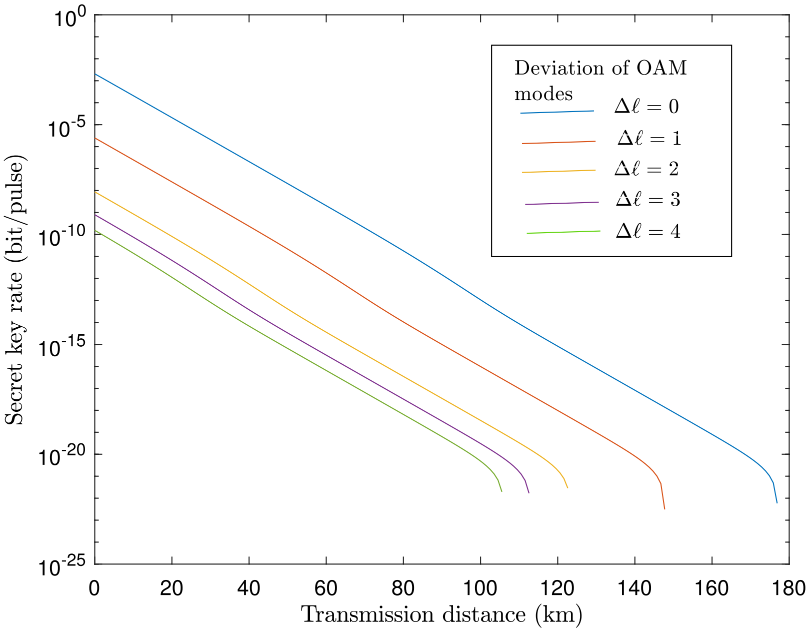

Figure 3. A plot of the secret key generation rate, K, versus transmission distance when atmospheric turbulence is varied as measured by the deviation of OAM modes, $\Delta\ell$.

the real-life parameters for the key rate, $R = 10^{-10}$, then the maximum transmission distance under fog particles of size 1 μm is 80 km, and under normal conditions, the maximum attainable transmission distance is 100 km.

Discussion

We have demonstrated free space MDI-QKD using vector vortex and scalar beams. Due to the rotational invariance property of the beams, two communicating parties can generate secret keys without having to align the reference frames of the transmitting and receiving units. Additionally, we evaluated the performance of the proposed protocol under a variety of weather conditions that approximate the realistic conditions of everyday communications. We observed that propagation of OAM carrying beam under turbulent conditions may result

Parameters						Values
Background count rate						8×10^{-6}
Error correction efficiency f						1.15
Detector efficiency						14.5%
Aperture diameter, D						15×10^{-2} m
C_n^2						$10^{-14}\mathrm{m}^{-2/3}$
Wavelength of the beam, λ						1550 nm
Terminal velocity of rain, $v\ (D_{\text{rain}})$						9 m/s
Rain-drop size distribution , $n\ (D_{\text{rain}})$						10^5
Percentage rain volume, $m\ (D_{\text{rain}})$						1
Number of particles per unit volume, N_{fog}						10^{15}

Table 3. Parameters used for simulation.

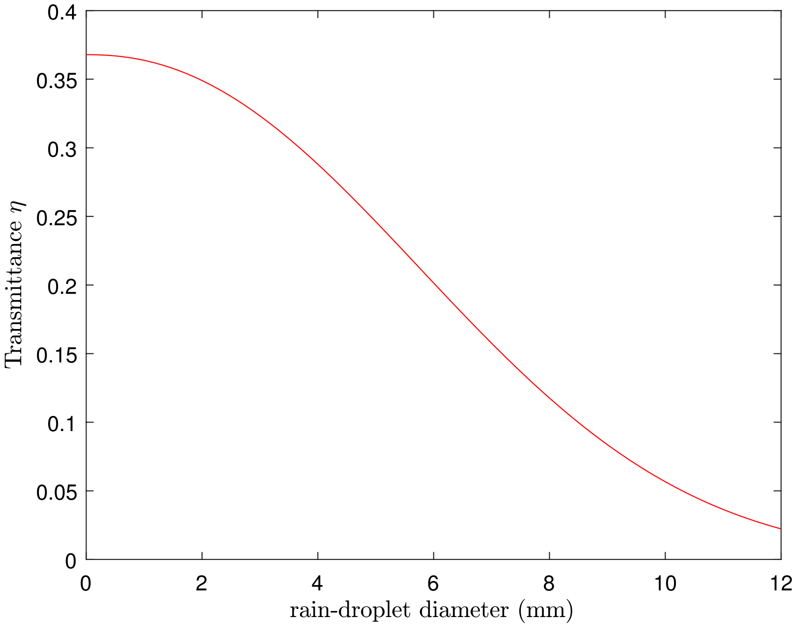

Figure 4. A plot of transmittance, η, against the diameter of raindrops, D_{rain}.

in scrambling of the OAM state of the beam, and the probability of scrambling increases as the strength of the turbulence increases. Results indicate that large deviations in originally transmitted OAM states of the vortex and scalar beams lead to reduced achievable key rates and maximum transmission distances. In particular, in a weak turbulence regime, i.e., with a small $\Delta\ell$, the achievable distance is comparable to that under normal atmospheric conditions. Notably, we have also demonstrated that, under clear atmospheric conditions, our proposed scheme can transmit signals up to 178 km. In constrast, with rainfall of 6 mm diameter droplets, the distance to which the signals can be transmitted is 152 km. It should be noted that in foggy conditions with fog particles with a radius of 0.5 μm, the maximum attainable distance is 160 km, which is still comparable to the maximum distance reached under clear conditions. These results demonstrate the robustness of MDI-QKD implementation using vector vortex and scalar beams to generate secure keys over long transmission distances in adverse weather conditions. As a result, this study is of central importance as it opens up the intriguing possibility of utilizing these beams in future QKD applications.

Methods

This section presents the derivation of the parameters used to estimate the MDI-QKD secret key rate. The gain for single photon states $Q_{11}^{\mathbf{V}}$, which represents the probability of Alice and Bob sending out single photon states on a vector basis and obtaining successful detection results, is expressed as follows

$$Q_{11}^{\mathbf{V}} = \mu_a \mu_b e^{-\mu_a - \mu_b} Y_{11}^{\mathbf{V}}. \tag{47}$$

The quantity $Y_{11}^{\mathbf{V}}$ corresponds to the yield of single photons in the vector basis and is given by

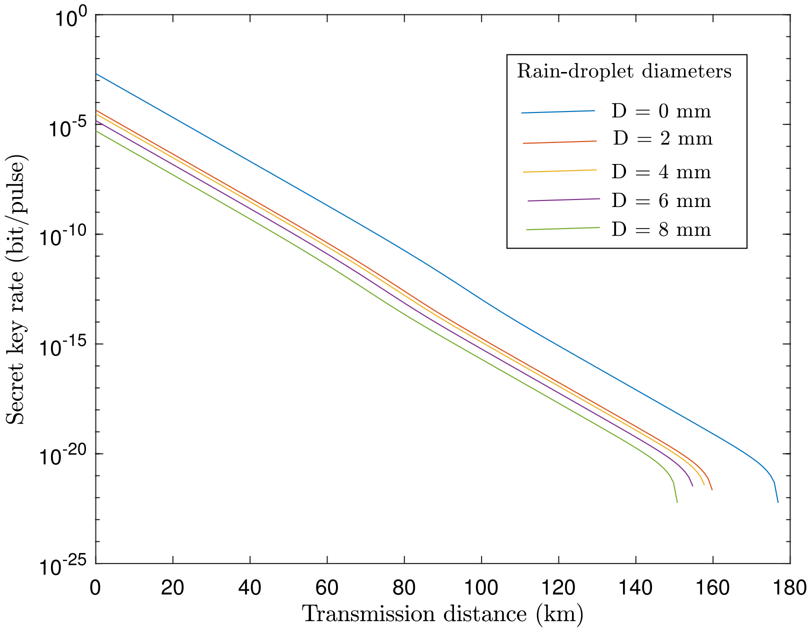

Figure 5. Plot of the secret key generation rate, K, against transmission distance in km for a range of raindrop diameters.

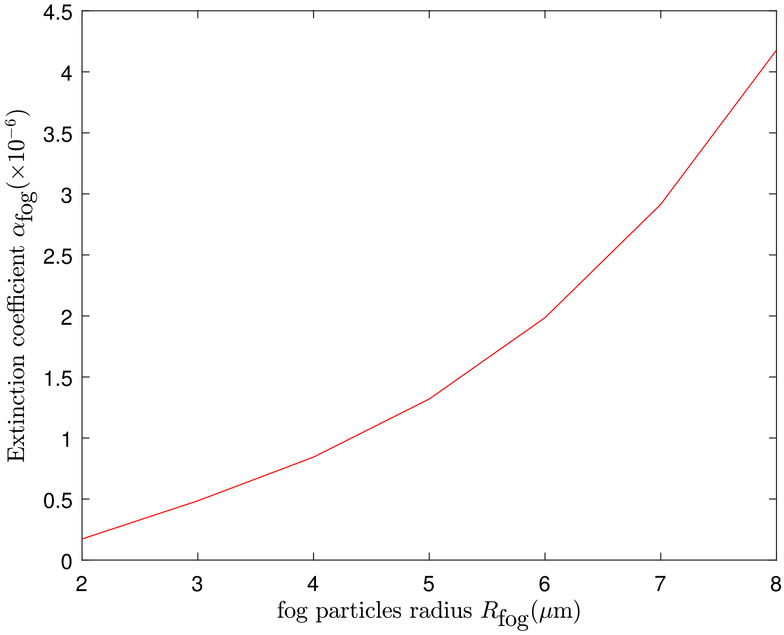

Figure 6. An illustration showing the relation between the beam extinction coefficient, α_{fog}, and the radius of the fog particles, R_{fog}.

$$Y_{11}^{\text{V}} = Y_{11}^{\text{L0R1}} + Y_{11}^{\text{L1R0}} + Y_{11}^{\text{L0L1}} + Y_{11}^{\text{R0R1}} + Y_{11}^{\text{L0R0}} + Y_{11}^{\text{L1R1}}. \tag{48}$$

Without a loss of generality, here we show how to obtain Y_{11}^{L0R1}, and owing to symmetry, other terms are deduced similarly. After propagating through a lossy channel modeled by transmittance η_a, η_b, the initial state of Alice and Bob can be described as a mixed state

$$\frac{\eta_a\eta_b}{4}|\psi_{11}\rangle\langle\psi_{11}| + \frac{\eta_a(1-\eta_b)}{2}|\psi_{10}\rangle\langle\psi_{10}| + \frac{(1-\eta_a)\eta_b}{2}|\psi_{01}\rangle\langle\psi_{01}| + (1-\eta_a)(1-\eta_b)|\psi_{00}\rangle\langle\psi_{00}| \tag{49}$$

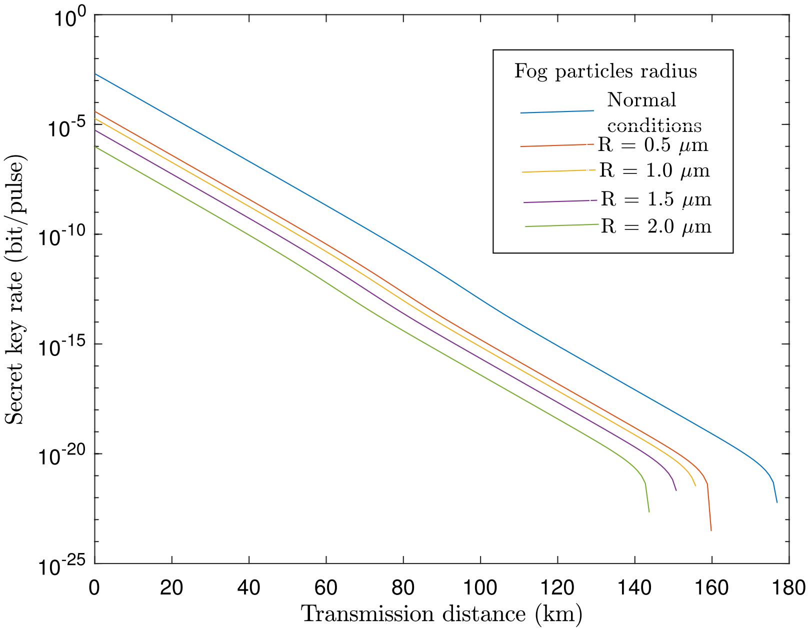

Figure 7. A plot of the secret key generation rate, *K*, against transmission distance in km for various values of the radius of the fog particles.

where $|\psi_{00}\rangle = |00\rangle_{ab}, |\psi_{01}\rangle = |01\rangle_{ab}, |\psi_{10}\rangle = |10\rangle_{ab}, |\psi_{11}\rangle = |11\rangle_{ab}$ and $|0\rangle, |1\rangle$ represent vacuum and one photon states. After passing through a BS, the states in Eq. (49) transform to

$$\begin{aligned} |11\rangle_{12} &\longmapsto \frac{1}{\sqrt{2}}(|0\rangle_3|2\rangle_4 - |2\rangle_3|0\rangle_4), \\ |10\rangle_{12} &\longmapsto \frac{1}{\sqrt{2}}(|0\rangle_3|1\rangle_4 - |1\rangle_3|0\rangle_4), \\ |01\rangle_{12} &\longmapsto \frac{1}{\sqrt{2}}(|1\rangle_3|0\rangle_4 - |0\rangle_3|1\rangle_4), \\ |00\rangle_{12} &\longmapsto |0\rangle_3|0\rangle_4, \end{aligned} \tag{50}$$

where we assume the case of indistinguishable photons. For distinguishable photons the state $|11\rangle$ can also be represented by the transformations

$$|11\rangle_{12} \longmapsto |1\rangle_3|1\rangle_4 \tag{51}$$

$$|11\rangle_{12} \longmapsto \frac{1}{\sqrt{2}}(|0\rangle_3|2\rangle_4 - |2\rangle_3|0\rangle_4). \tag{52}$$

The Bell state measurement is considered successful when exactly one of the two detectors is triggered in each OAM mode. By taking into account the effects of detector dark counts p_d, we obtain the photon detection probabilities by conditioning on the following events;

Dark counts

In a case where no photons reach the input ports of the beam splitter, detection events can only result from detector noise. In this case, the detection probability is given by

$$P_{\text{det}}(|00\rangle) = (1-\eta_a)(1-\eta_b)p_d^2(1-p_d)^2. \tag{53}$$

One-photon case Consider a case where only one photon form the two parties reach the input port of the beam splitter, then detection probability is given by

$$P_{\text{det}}(|01\rangle) = (1-\eta_a)\eta_b(1-p_d)p_d(1-p_d)^2 \tag{54}$$

$$P_{\text{det}}(|01\rangle) = \eta_a(1-\eta_b)(1-p_d)p_d(1-p_d)^2 \tag{55}$$

Two-photon case We now determine detection events emanating from two photons entering the beam splitter. The two photons can leave the BS at different ports or they may exit from the same port, and the detection probabilities are respectively given by

$$P_{\text{det}}(|11\rangle) = \eta_a\eta_b(1-p_d)^2(1-p_d)^2 \tag{56}$$

$$P_{\text{det}}(|11\rangle) = \eta_a\eta_b(1-p_d)p_d(1-p_d)^2. \tag{57}$$

Thus, the yield Y_{11}^{L0R1} is given by

$$Y_{11}^{\text{L0R1}} = (1-p_d)^2[\eta_a\eta_b + (\eta_b+\eta_a-4\eta_a\eta_b)p_d + (1-2\eta_a-2\eta_b+4\eta_a\eta_b)p_d^2]. \tag{58}$$

An error is obtained in the cases where L0 and R0 or L1 and R1 click. The detection probabilities for these events is given by

$$Y_{11}^{\text{L0R0(L1R1)}} = (1-p_d)^2[(\eta_b+\eta_a-\eta_a\eta_b)p_d + (1-2\eta_a-2\eta_b+2\eta_a\eta_b)p_d^2] \tag{59}$$

Thus, an error rate $e_{11}^{\mathbf{S}}$ is given by

$$\begin{aligned} e_{11}^{\mathbf{S}}Y_{11} &= Y_{11}^{\text{L0R0}} + Y_{11}^{\text{L1R1}} \\ &= 2(1-p_d)^2[(\eta_a+\eta_b-\eta_a\eta_b)p_d + (1-2\eta_a-2\eta_b+2\eta_a\eta_b)p_d^2] \\ &= e_0(1-p_d)^2[(\eta_a+\eta_b-\eta_a\eta_b)p_d + (1-2\eta_a-2\eta_b+2\eta_a\eta_b)p_d^2] \end{aligned} \tag{60}$$

where $e_0 = \frac{1}{2}$ corresponds to the error rate of random erroneous detection. The overall gain $Q_\mu^{\mathbf{V}}$ and the QBER, $E_\mu^{\mathbf{V}}$ are evaluated in accordance with the method in Ref.[29] with modifications as follows

$$\begin{aligned} Q_\mu^{\mathbf{V}} = {} & [D_{\text{L0}}(1-D_{\text{L1}}) + (1-D_{\text{L0}})D_{\text{L1}}][D_{\text{R1}}(1-D_{\text{R0}}) + (1-D_{\text{R1}})D_{\text{R0}}] + [D_{\text{L0}}D_{\text{L1}}(1-D_{\text{R0}})(1-D_{\text{R1}})] \\ & + [D_{\text{R0}}D_{\text{R1}}(1-D_{\text{L0}})(1-D_{\text{L1}})]. \end{aligned} \tag{61}$$

Here, the detection probabilities for the four detectors are given by

$$D_{\text{L0(R0)}} = 1-(1-p_d)\exp\left(-\left|e^{i\theta_a}\frac{\sqrt{\eta_a\mu_a}}{2} + e^{i\theta_b}\frac{\sqrt{\eta_b\mu_b}}{2}\right|\right), \tag{62}$$

$$D_{\text{L1(R1)}} = 1-(1-p_d)\exp\left(-\left|e^{i\theta_a}\frac{\sqrt{\eta_a\mu_a}}{2} - e^{i\theta_b}\frac{\sqrt{\eta_b\mu_b}}{2}\right|\right). \tag{63}$$

We adopt the following notation to simplify our analysis;

$$\begin{aligned} \lambda &= \eta_a\mu_a + \eta_b\mu_b, \\ \Delta\theta &= \theta_b - \theta_a, \\ x &= \sqrt{\eta_a\mu_a\eta_b\mu_b}/2, \\ y &= (1-p_d)e^{-\lambda/4}, \end{aligned}$$

where λ denotes the average number of photons after interference in the BS, and $\Delta\theta$ corresponds to the difference between Alice's and Bob's random overall phases. As a result, the probability of detection simplifies as follows

$$D_{\text{L0(R0)}} = 1 - ye^{-x\cos\Delta\theta}, \tag{64}$$

$$D_{\text{L1(R1)}} = 1 - ye^{x\cos\Delta\theta}. \tag{65}$$

The QBER, $E_\mu^{\mathbf{V}}$ is expressed as

$$E_\mu^{\mathbf{V}}Q_\mu^{\mathbf{V}} = 2D_{\text{L0}}(1-D_{\text{L1}})(1-D_{\text{R1}})D_{\text{R0}}. \tag{66}$$

Data availability

The datasets generated during and/or analysed during the current study are available from the corresponding author on reasonable request.

Received: 22 May 2023; Accepted: 14 August 2023
Published online: 11 September 2023

References

1. Gisin, N., Ribordy, G., Tittel, W. & Zbinden, H. Quantum cryptography. *Rev. Mod. Phys.* **74**, 145 (2002).
2. Pirandola, S. *et al.* Advances in quantum cryptography. *Adv. Opt. Photonics* **12**, 1012–1236 (2020).
3. Mao, Y., Zeng, P. & Chen, T.-Y. Recent advances on quantum key distribution overcoming the linear secret key capacity bound. *Adv. Quantum Technol.* **4**, 2000084 (2020).
4. Xu, F., Ma, X., Zhang, Q., Lo, H.-K. & Pan, J.-W. Secure quantum key distribution with realistic devices. *Rev. Mod. Phys.* **92**, 025002 (2020).
5. Scarani, V. & Kurtsiefer, C. The black paper of quantum cryptography: real implementation problems. *Theor. Comput. Sci.* **560**, 27–32 (2014).

6. Takeoka, M., Guha, S. & Wilde, M. M. Fundamental rate-loss tradeoff for optical quantum key distribution. *Nat. Commun.* **5**, 5235 (2014).
7. Diamanti, E., Lo, H.-K., Qi, B. & Yuan, Z. Practical challenges in quantum key distribution. *npj Quantum Inf.* **2**, 1–12 (2016).
8. Mafu, M. & Senekane, M. Security of quantum key distribution protocols. In *Advanced Technologies of Quantum Key Distribution* (IntechOpen, 2018).
9. Mafu, M., Sekga, C. & Senekane, M. Loss-tolerant prepare and measure quantum key distribution protocol. *Sci. Afr.* **14**, e01008 (2021).
10. Sibson, P. *et al.* Chip-based quantum key distribution. *Nat. Commun.* **8**, 13984 (2017).
11. Semenenko, H. *et al.* Chip-based measurement-device-independent quantum key distribution. *Optica* **7**, 238–242 (2020).
12. Kwek, L.-C. *et al.* Chip-based quantum key distribution. *AAPPS Bull.* **31**, 1–8 (2021).
13. Bedington, R., Arrazola, J. M. & Ling, A. Progress in satellite quantum key distribution. *npj Quantum Inf.* **3**, 30 (2017).
14. Zhang, Q., Xu, F., Chen, Y.-A., Peng, C.-Z. & Pan, J.-W. Large scale quantum key distribution: challenges and solutions. *Opt. Express* **26**, 24260–24273 (2018).
15. McCutcheon, W. *et al.* Experimental verification of multipartite entanglement in quantum networks. *Nat. Commun.* **7**, 13251 (2016).
16. Lucamarini, M., Yuan, Z. L., Dynes, J. F. & Shields, A. J. Overcoming the rate-distance limit of quantum key distribution without quantum repeaters. *Nature* **557**, 400–403 (2018).
17. Pereira, M., Kato, G., Mizutani, A., Curty, M. & Tamaki, K. Quantum key distribution with correlated sources. *Sci. Adv.* **6**, eaaz4487 (2020).
18. Ma, X., Qi, B., Zhao, Y. & Lo, H.-K. Practical decoy state for quantum key distribution. *Phys. Rev. A* **72**, 012326 (2005).
19. Liu, B. *et al.* Decoy-state method for quantum-key-distribution-based quantum private query. *Sci. China Phys. Mech. Astron.* **65**, 240312 (2022).
20. She, L.-G. & Zhang, C.-M. Reference-frame-independent quantum key distribution with modified coherent states. *Quantum Inf. Process.* **21**, 161 (2022).
21. Nie, Y.-F. & Zhang, C.-M. Afterpulse analysis for reference-frame-independent quantum key distribution. *Quantum Inf. Process.* **21**, 340 (2022).
22. Lo, H.-K., Curty, M. & Qi, B. Measurement-device-independent quantum key distribution. *Phys. Rev. Lett.* **108**, 130503 (2012).
23. Sekga, C., Mafu, M. & Senekane, M. High-dimensional quantum key distribution implemented with biphotons. *Sci. Rep.* **13**, 1229 (2023).
24. Maeda, K., Sasaki, T. & Koashi, M. Repeaterless quantum key distribution with efficient finite-key analysis overcoming the rate-distance limit. *Nat. Commun.* **10**, 3140 (2019).
25. Currás-Lorenzo, G. *et al.* Tight finite-key security for twin-field quantum key distribution. *npj Quantum Inf.* **7**, 22 (2021).
26. Yin, Z.-Q. *et al.* Twin-field protocols: towards intercity quantum key distribution without quantum repeaters. *Fundam. Res.* **1**, 93–95 (2021).
27. Wang, S. *et al.* Twin-field quantum key distribution over 830-km fibre. *Nat. Photonics* **16**, 154–161 (2022).
28. Tamaki, K., Lo, H.-K., Fung, C.-H.F. & Qi, B. Phase encoding schemes for measurement-device-independent quantum key distribution with basis-dependent flaw. *Phys. Rev. A* **85**, 042307 (2012).
29. Ma, X. & Razavi, M. Alternative schemes for measurement-device-independent quantum key distribution. *Phys. Rev. A* **86**, 062319 (2012).
30. Wang, Q. & Wang, X.-B. Efficient implementation of the decoy-state measurement-device-independent quantum key distribution with heralded single-photon sources. *Phys. Rev. A* **88**, 052332 (2013).
31. Da Silva, T. F. *et al.* Proof-of-principle demonstration of measurement-device-independent quantum key distribution using polarization qubits. *Phys. Rev. A* **88**, 052303 (2013).
32. Tang, Z. *et al.* Experimental demonstration of polarization encoding measurement-device-independent quantum key distribution. *Phys. Rev. Lett.* **112**, 190503 (2014).
33. Yin, H.-L. *et al.* Measurement-device-independent quantum key distribution over a 404 km optical fiber. *Phys. Rev. Lett.* **117**, 190501 (2016).
34. Gu, J. *et al.* Experimental measurement-device-independent type quantum key distribution with flawed and correlated sources. *Sci. Bull.* **67**, 2167–2175 (2022).
35. Primaatmaja, I. W., Lavie, E., Goh, K. T., Wang, C. & Lim, C. C. W. Versatile security analysis of measurement-device-independent quantum key distribution. *Phys. Rev. A* **99**, 062332 (2019).
36. Boileau, J.-C., Laflamme, R., Laforest, M. & Myers, C. Robust quantum communication using a polarization-entangled photon pair. *Phys. Rev. Lett.* **93**, 220501 (2004).
37. Liorni, C., Kampermann, H. & Bruß, D. Satellite-based links for quantum key distribution: beam effects and weather dependence. *New J. Phys.* **21**, 093055 (2019).
38. Chen, Y.-A. *et al.* An integrated space-to-ground quantum communication network over 4,600 kilometres. *Nature* **589**, 214–219 (2021).
39. Wang, X.-F. *et al.* Transmission of photonic polarization states from geosynchronous earth orbit satellite to the ground. *Quantum Eng.* **3**, e73 (2021).
40. Sidhu, J. S. *et al.* Advances in space quantum communications. *IET Quantum Commun.* **2**, 182–217 (2021).
41. Vallone, G. *et al.* Free-space quantum key distribution by rotation-invariant twisted photons. *Phys. Rev. Lett.* **113**, 060503 (2014).
42. Krenn, M. *et al.* Communication with spatially modulated light through turbulent air across Vienna. *New J. Phys.* **16**, 113028 (2014).
43. Mirhosseini, M. *et al.* High-dimensional quantum cryptography with twisted light. *New J. Phys.* **17**, 033033 (2015).
44. Sit, A. *et al.* High-dimensional intracity quantum cryptography with structured photons. *Optica* **4**, 1006–1010 (2017).
45. Bouchard, F. *et al.* Quantum cryptography with twisted photons through an outdoor underwater channel. *Opt. Express* **26**, 22563–22573 (2018).
46. Otte, E. *et al.* High-dimensional cryptography with spatial modes of light: tutorial. *J. Opt. Soc. Am. B* **37**, A309–A323 (2020).
47. Mafu, M. *et al.* Higher-dimensional orbital-angular-momentum-based quantum key distribution with mutually unbiased bases. *Phys. Rev. A* **88**, 032305 (2013).
48. Paterson, C. Atmospheric turbulence and orbital angular momentum of single photons for optical communication. *Phys. Rev. Lett.* **94**, 153901 (2005).
49. Gbur, G. & Tyson, R. K. Vortex beam propagation through atmospheric turbulence and topological charge conservation. *J. Opt. Soc. Am. A* **25**, 225–230 (2008).
50. Tyler, G. A. & Boyd, R. W. Influence of atmospheric turbulence on the propagation of quantum states of light carrying orbital angular momentum. *Opt. Lett.* **34**, 142–144 (2009).
51. Roux, F. S. Infinitesimal-propagation equation for decoherence of an orbital-angular-momentum-entangled biphoton state in atmospheric turbulence. *Phys. Rev. A* **83**, 053822 (2011).
52. Sanchez, D. J. & Oesch, D. W. Orbital angular momentum in optical waves propagating through distributed turbulence. *Opt. Express* **19**, 24596–24608 (2011).

53. Rodenburg, B. *et al.* Influence of atmospheric turbulence on states of light carrying orbital angular momentum. *Opt. Lett.* **37**, 3735–3737 (2012).
54. Ren, Y. *et al.* Atmospheric turbulence effects on the performance of a free space optical link employing orbital angular momentum multiplexing. *Opt. Lett.* **38**, 4062–4065 (2013).
55. Chandrasekaran, N. & Shapiro, J. H. Photon information efficient communication through atmospheric turbulence-part i: Channel model and propagation statistics. *J. Light. Technol.* **32**, 1075–1087 (2014).
56. Li, J. *et al.* Mitigation of atmospheric turbulence with random light carrying OAM. *Opt. Commun.* **446**, 178–185 (2019).
57. Liu, C. & Yeh, K. Propagation of pulsed beam waves through turbulence, cloud, rain, or fog. *J. Opt. Soc. Am.* **67**, 1261–1266 (1977).
58. Yura, H., Barthel, K. & Büchtemann, W. Rainfall-induced optical phase fluctuations in the atmosphere. *J. Opt. Soc. Am.* **73**, 1574–1580 (1983).
59. de Wolf, D. A. On the laws-parsons distribution of raindrop sizes. *Radio Sci.* **36**, 639–642 (2001).
60. Piazzolla, S. & Slobin, S. Statistics of link blockage due to cloud cover for free-space optical communications using NCDC surface weather observation data. In *Free-Space Laser Communication Technology XIV*, vol. 4635, 138–149 (SPIE, 2002).
61. Lukin, I., Rychkov, D. S., Falits, A. V., Lai, K. S. & Liu, M. R. A phase screen model for simulating numerically the propagation of a laser beam in rain. *Quantum Electron.* **39**, 863 (2009).
62. Uijlenhoet, R., Cohard, J.-M. & Gosset, M. Path-average rainfall estimation from optical extinction measurements using a large-aperture scintillometer. *J. Hydrometeor.* **12**, 955–972 (2011).
63. Grabner, M. & Kvicera, V. Multiple scattering in rain and fog on free-space optical links. *J. Light. Technol.* **32**, 513–520 (2013).
64. Mori, S. & Marzano, F. S. Microphysical characterization of free space optical link due to hydrometeor and fog effects. *Appl. Opt.* **54**, 6787–6803 (2015).
65. Vasylyev, D. *et al.* Free-space quantum links under diverse weather conditions. *Phys. Rev. A* **96**, 043856 (2017).
66. Lu, Q.-H. *et al.* Quantum key distribution over a channel with scattering. *Phys. Rev. Appl.* **17**, 034045 (2022).
67. Wang, L., Zhao, S.-M., Gong, L.-Y. & Cheng, W.-W. Free-space measurement-device-independent quantum-key-distribution protocol using decoy states with orbital angular momentum. *Chin. Phys. B* **24**, 120307 (2015).
68. Chen, D., Zhao, S.-H., Shi, L. & Liu, Y. Measurement-device-independent quantum key distribution with pairs of vector vortex beams. *Phys. Rev. A* **93**, 032320 (2016).
69. Li, Y. *et al.* Polarization and orbital angular momentum coupling for high-dimensional measurement-device-independent quantum key distribution protocol. *Quantum Inf. Process.* **22**, 147 (2023).
70. Ndagano, B., Nape, I., Cox, M. A., Rosales-Guzman, C. & Forbes, A. Creation and detection of vector vortex modes for classical and quantum communication. *J. Light. Technol.* **36**, 292–301 (2018).
71. Ndagano, B. *et al.* A deterministic detector for vector vortex states. *Sci. Rep.* **7**, 13882 (2017).
72. Gottesman, D., Lo, H.-K., Lutkenhaus, N. & Preskill, J. Security of quantum key distribution with imperfect devices. In *International Symposium on Information Theory*, 2004. ISIT 2004. Proceedings, 136 (IEEE, 2004).
73. Shor, P. & Preskill, J. Simple proof of security of the bb84 quantum key distribution protocol. *Phys. Rev. Lett.* **85**, 441–444 (2000).
74. Ulbrich, C. W. & Atlas, D. Extinction of visible and infrared radiation in rain: Comparison of theory and experiment. *J. Atmos. Ocean. Technol.* **2**, 331–339 (1985).
75. Bohren, C. F. & Huffman, D. R. *Absorption and Scattering of Light by Small Particles* (Wiley, 2008).
76. Hulst, H. C. & van de Hulst, H. C. *Light Scattering by Small Particles* (Courier Corporation, 1981).

Author contributions

Conceptualization, C.S. and M.M.; methodology, C.S.; software, C.S.; validation, C.S. and M.M.; formal analysis, C.S. and M.M.; writing-original draft preparation, C.S.; writing-review and editing, M.M.; supervision, M.M.; project administration, M.M. All authors have read and agreed to the published version of the manuscript.

Competing interests

The authors declare no competing interests.

Additional information

Correspondence and requests for materials should be addressed to M.M.

Reprints and permissions information is available at www.nature.com/reprints.

Publisher's note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.