The effect of turbulence on entanglement-based free-space quantum key distribution with photonic orbital angular momentum

2016 J. Opt. 18 064002

(http://iopscience.iop.org/2040-8986/18/6/064002)

IOP Publishing Journal of Optics
J. Opt. 18 (2016) 064002 (7pp) doi:10.1088/2040-8978/18/6/064002

The effect of turbulence on entanglement-based free-space quantum key distribution with photonic orbital angular momentum

Sandeep K Goyal[1,2], Alpha Hamadou Ibrahim[3], Filippus S Roux[3,4], Thomas Konrad[2,5] and Andrew Forbes[4]

[1] Institute of Quantum Science and Technology, University of Calgary, Alberta T2N 1N4, Canada
[2] School of Chemistry and Physics, University of Kwazulu-Natal, Private Bag X54001, Durban 4000, South Africa
[3] CSIR National Laser Centre, PO Box 395, Pretoria 0001, South Africa
[4] School of Physics, University of the Witwatersrand, Private Bag 3, Wits 2050, South Africa
[5] National Institute of Theoretical Physics, University of Kwazulu-Natal, Private Bag X54001, Durban 4000, South Africa

E-mail: andrew.forbes@wits.ac.za

Received 26 November 2015, revised 14 February 2016
Accepted for publication 2 March 2016
Published 5 April 2016

Abstract

Using an experimental setup that simulates a turbulent atmosphere, we study the secret key rate for quantum key distribution (QKD) protocols in orbital angular momentum based free space quantum communication. The QKD protocols under consideration include the Ekert 91 protocol for different choices of mutually unbiased bases and the six-state protocol. We find that the secret key rate of these protocols decay to zero, roughly at the same scale where the entanglement of formation decays to zero.

Keywords: quantum communication, orbital angular momentum, atmospheric turbulence

(Some figures may appear in colour only in the online journal)

1. Introduction

Quantum key distribution (QKD) is the first cryptographic method that is based on the laws of quantum mechanics. In principle, it provides a means to communicate securely against eavesdropping, by establishing a secret key between two authenticated parties that can be used for secret communication. This is the first experimentally realizable application of quantum information processing and has drawn the attention of a large community in both theory [1–8] and experiment [9–16].

To replace classical cryptographic technology, which are in general not secure against attacks using nascent quantum computing technology (with the exception of a few protocols such as lattice-based cryptography [17–20]), methods are sought to achieve QKD with high transmission rates over large distances. Even though the implementation technique for QKD has reached the commercial level (see for example Quintessence Labs (www.quintessencelabs.com), MagiQ Technologies (www.magiqtech.com), idQuantique (www.idquantique.com), and SeQureNet (www.sequrenet.fr)), the transmission distances and rates, are still comparatively small. The most robust quantum channels for QKD are currently based on optical fibers, with transmission distances of between 20 and 150 km and maximal bit rates of between 10 kbit and 1 Mbit s^{-1}[21]. There have been a few experiments where they have achieved the secure QKD up to 336 km with a few bits per second transmission [22, 23].

The free space implementation of QKD could enable intercontinental transmission channels using satellites [24]. A possible candidate as information carrier with high information capacity is the orbital angular momentum (OAM) modal basis of photons [25]. QKD protocols using qubit or multi-dimensional mutually unbiased bases (MUBs) encoded by means of OAM modes were recently tested experimentally [26–28] in the laboratory under ideal conditions. However, while the existence of infinitely many OAM modes, in principle, allows one to encode an arbitrary amount of

information in a single photon, these modes are susceptible to the influence of atmospheric turbulence. Apart from its adverse effect on spatial modal multiplexing in free space optical communication [29–32], the distortion of spatial modes also causes the decay of coherence and reduces the transmission rate of secure keys in free space quantum communication. In other words, the effect of turbulence on the propagation of OAM modes decides whether these modes can contribute to efficient quantum key generation over large distances.

Various aspects of OAM modes propagating through turbulence have been considered theoretically, including the detection probability of OAM modes [33–35], attenuation and crosstalk among multiple OAM channels [36], the decay of entanglement for bipartite qubits [37, 38], and the quantum channel capacity [39]. A few experimental studies of the effect of turbulence on the OAM modes have also been reported [40, 41]. Some groups proposed methods to overcome the effect of turbulence on free space optical or quantum communication. These include, the use of post-processing (adaptive optics) [42, 43] and pre-processing (robust states [44] and optimal encoding [45]) schemes.

In this article, we report on an experimental study of the influence of turbulence on the secret key rate for QKD. For this purpose we prepare two photons in a maximally entangled state, using spontaneous parametric down-conversion (SPDC). We restrict the number of OAM modes to two (qubits) and simulate the effect of atmospheric turbulence on both photons through phase modulation by a single phase screen in each of the beam paths. We study two QKD protocols: E91 [46] with different sets of MUBs and the six-state protocol [47]. These protocols are realized by performing measurements in the eigenbasis of the Pauli matrices on both photons. Since there are three MUBs for two-dimensions one has three ways to select two sets of MUBs for the E91 protocol. For the six-state protocol we perform measurements in all three MUBs (the complete set for qubits) [48]. We find that secure QKD is possible over distances up to where entanglement decays to zero, but with lower secret key rate than entanglement of formation (EoF). Finally, we comment on the potential issues in using OAM as an encoding basis for free space QKD.

2. Theory

For qubits (two-dimensional systems) the sets of eigenstates of the respective Pauli operators form MUBs. The three Pauli operators can be expressed as

$$\hat{\sigma}_{\mathrm{x}} = |1\rangle\langle 0| + |0\rangle\langle 1|, \tag{1}$$

$$\hat{\sigma}_{\mathrm{y}} = \mathrm{i}(|1\rangle\langle 0| - |0\rangle\langle 1|), \tag{2}$$

$$\hat{\sigma}_{\mathrm{z}} = |0\rangle\langle 0| - |1\rangle\langle 1|. \tag{3}$$

The corresponding bases (sets of eigenstates) that are associated with the respective Pauli operators, are

$$\mathcal{M}_x = \left\{\frac{1}{\sqrt{2}}(|0\rangle \pm |1\rangle)\right\}, \tag{4}$$

$$\mathcal{M}_y = \left\{\frac{1}{\sqrt{2}}(|0\rangle \pm \mathrm{i}\,|1\rangle)\right\}, \tag{5}$$

$$\mathcal{M}_z = \{|0\rangle, |1\rangle\}. \tag{6}$$

These bases are mutually unbiased in that the measurement of a basis vector of one of these sets (say $\mathcal{M}_x$) in terms of another one of these bases (say $\mathcal{M}_y$) leads to equi-probable outcomes.

The first QKD protocol was developed by Bennett and Brassard in 1984 (BB84 protocol) [49]. The entanglement-based version of the BB84 protocol was developed by Ekert in 1991 (E91 protocol) [46]. In this protocol, the two parties, Alice and Bob, each obtain one subsystem of a maximally entangled state. In this study we use the Bell state

$$|\Phi^+\rangle = \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle). \tag{7}$$

Each of the two parties, Alice and Bob, then randomly chooses a measurement basis from a set of two MUBs, $\{\mathcal{M}_1, \mathcal{M}_2\}$, which could be any two of the bases shown in equations (4)–(6), and perform a measurement on its respective subsystems in the chosen basis. The two parties repeat this process for a large number n of quantum states and keep a record of their respective measurement outcomes, as well as the basis in which the measurements were performed. Alice and Bob, then publicly compare their measurement bases and keep only those results for which their bases matched, discarding the rest. This so-called sifting process would ideally result in an identical key for both parties although reducing the efficiency by half as each of the party keeps on average only half of the measurement results.

Another QKD protocol of interest is the six-state protocol [47], which is a straight-forward generalization of E91. The six-state protocol uses three orthonormal MUBs $\{\mathcal{M}_1, \mathcal{M}_2, \mathcal{M}_3\}$ (the three MUBs shown in equations (4)–(6)), instead of just two. The rest of the protocol is analogous to E91. In the six-state protocol, Alice and Bob choose on average only in one third of the cases the same measurement bases which leads to a removal of two thirds of the received data during sifting.

In the ideal scenario the protocols discussed above generate identical keys for Alice and Bob. However, differences between both keys can arise from disturbances due to eavesdropping, but also from imperfections in the state preparation, the transmission and the measurement process. It is rather difficult to differentiate between the error caused by eavesdropping and the errors of other origins. Therefore, it is safest to assign all the differences to eavesdropping. To estimate the average error, both parties compare a small portion of their measurements (after sifting) and calculate the so-called quantum bit error rate Q. It is given by the probability that Alice sends the state $|\psi\rangle$ and Bob projects, in an ideal measurement, onto an orthogonal state $|\psi_\perp\rangle$. In the

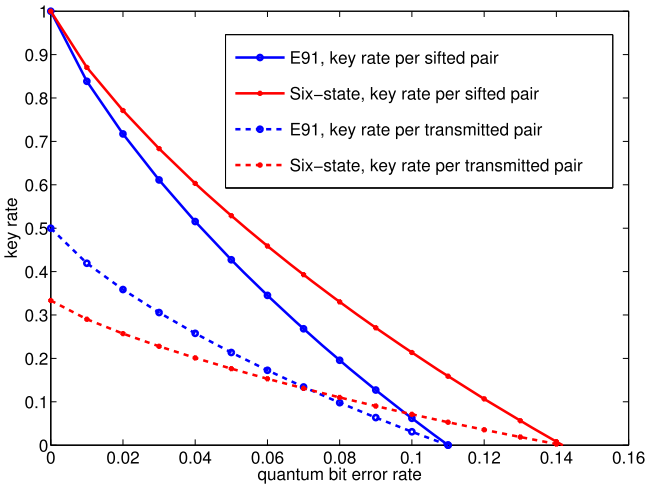

Figure 1. Comparison of the secret key rates of the E91 protocol and the six-state protocol, as a function of the quantum bit error rate.

entanglement-based protocols, the quantum bit error rate Q is

$$Q = \frac{1}{\mathcal{L}} \sum_{\beta=1}^{\mathcal{L}} \sum_{k \neq k'} \mathrm{tr}(|\psi_k^\beta\rangle\langle\psi_k^\beta| \otimes |\psi_{k'}^\beta\rangle\langle\psi_{k'}^\beta| \, \rho_{AB}), \tag{8}$$

where ρ_{AB} is the combined state of the system shared by Alice and Bob, whereas $|\psi_k\rangle$ and $|\psi_{k'}\rangle$ are the states on which their measurements project in case they chose the same basis. The index β numerates the chosen bases and $\mathcal{L}$ is the number of bases available in the protocol: $\mathcal{L} = 2$ and $\mathcal{L} = 3$, for E91 and the six-state protocols, respectively.

The efficiency of the protocol is quantified by the secret key rate r, which represents the average number of secret key bits that can be distilled from each sifted system, i.e., each pair of information carriers that was measured by both parties with respect to the same basis. Distillation is accomplished by means of privacy amplification [50]. The maximum number of secret key bits per sifted pair of two-level systems is given by $r = 1$. However, the expression of the minimum number of secret key bits $r_{\min}$ for a given value of the quantum bit error rate Q, for E91 (and BB84) reads [50, 51]

$$r_{\min} = 1 + 2(1 - Q)\log_2(1 - Q) + 2Q\log_2(Q) \tag{9}$$

and for the six-state protocol it is given by

$$r_{\min} = 1 + \frac{3}{2}Q\log_2\left(\frac{Q}{2}\right) + \left(1 - \frac{3}{2}Q\right)\log_2\left(1 - \frac{3}{2}Q\right). \tag{10}$$

In a comparison of key rates, the six-state protocol produces a higher secret key rate per sifted qubit pair than E91 for the same quantum bit error rate, as shown in figure 1. Since the sifting process reduces the number of usable subsystems by half for the E91 protocol and by two-third for the six-state protocol, the key rate per transmitted qubit pair for the six-state protocol is lower than that of E91 protocol, for small but not for high quantum bit error rates. In the following we study the secret key rate per sifted qubit pair and refer to it simply as secret key rate. Because it is normalised to a maximal value of 1 for qubits, this rate is suited to compare different protocols and find effects other than the random disagreement in the measurement bases.

While the secret key rate is a measure for the efficiency of a particular QKD protocol, the amount of entanglement (quantified by the EoF) between the pairs of photons that arrive at Alice and Bob quantifies the quantum correlations that could be used to generate secret key bits shared by Alice and Bob [52]. The EoF between two two-level photonic systems is calculated from the average joint density matrix of this bipartite system as [53]

$$E = h\left(\frac{1 + \sqrt{1 - \mathcal{C}^2}}{2}\right), \tag{11}$$

where $h(\cdot)$ is the binary entropy function, given by

$$h(x) = -x\log_2 x - (1 - x)\log_2(1 - x) \tag{12}$$

and $\mathcal{C}$ is the concurrence, which is defined as

$$\mathcal{C} = \max\{0, \sqrt{\lambda_1} - \sqrt{\lambda_2} - \sqrt{\lambda_3} - \sqrt{\lambda_4}\}. \tag{13}$$

In equation (13) the λ_n's are the eigenvalues, in decreasing order, of the matrix $\tilde{\rho} = \rho(\sigma_y \otimes \sigma_y)\rho^*(\sigma_y \otimes \sigma_y)$, where * represents the complex conjugate and σ_y is the Pauli spin matrix.

3. Experiment

We implement these protocols in terms of the OAM degree of freedom of entangled photons. Entangled pairs of photons are prepared with the aid of spontaneous parametric down-conversion (SPDC), as explained below. These entangled pairs are then distributed through noisy channels (simulated turbulence) to two projective measurement setups (Alice and Bob). The projective measurements are made in terms of the helical modal basis (approximating Laguerre–Gaussian modes with radial index $p = 0$). We will denote this basis by $\{|\ell\rangle\}$, where ℓ represents the OAM index of the mode. For the purpose of the QKD protocols, we define the MUBs by replacing $|0\rangle \rightarrow |-\ell\rangle$ and $|1\rangle \rightarrow |\ell\rangle$ in equations (4)–(6), giving

$$\mathcal{M}_1 = \{|-\ell\rangle, |\ell\rangle\}, \tag{14}$$

$$\mathcal{M}_2 = \left\{\frac{1}{\sqrt{2}}(|-\ell\rangle \pm |\ell\rangle)\right\}, \tag{15}$$

$$\mathcal{M}_3 = \left\{\frac{1}{\sqrt{2}}(|-\ell\rangle \pm \mathrm{i}\,|\ell\rangle)\right\}. \tag{16}$$

We perform these measurements for $\ell = 1$, 3, 5 and 7.

Our aim to study the effect of atmospheric turbulence on the secret key rate r is realized in the laboratory by simulating the propagation of the photons in a turbulent atmosphere, using spatial light modulators (SLMs). The influence of atmospheric turbulence on an optical beam, in weak scintillation conditions, can be simulated by an SLM that is encoded with a random phase function (as caused by fluctuations of the refractive index of turbulent air) in a single transversal plane of the beam [33]. To simulate the turbulent atmosphere,

in agreement with the Kolmogorov theory of turbulence [54], we compute the random phase function on the SLM as [55, 56]

$$\theta(x, y) = \frac{k_0\sqrt{2\pi L}}{\Delta_k}\mathcal{F}^{-1}\{\chi(k_\perp)\sqrt{\Phi_n(|k_\perp|)}\}, \quad (17)$$

where k_0 is the wavenumber ($=2\pi/\lambda$, where λ is the wavelength of the light), L is the propagation distance, Δ_k is the sampling interval in the spatial frequency domain, $\mathcal{F}^{-1}\{\cdot\}$ is the two-dimensional inverse Fourier transform, $k_\perp$ is the two-dimensional wave vector in the transverse Fourier domain, and $\chi(k_\perp)$ is a frequency domain delta-correlated zero-mean Gaussian pseudo-random complex function, obeying $\chi^*(k_\perp) = \chi(-k_\perp)$, because $\theta(x, y)$ is real-valued. The refractive index power spectral density is expressed as [54, 57, 58]

$$\Phi_n(k) = 0.033C_n^2k^{-11/3}, \quad (18)$$

where C_n^2 is the refractive index structure constant, which determines the strength of the turbulence and k is the magnitude of the spatial frequency vector.

In our simulated turbulence experiment, the turbulence strength is combined with the wavelength and the propagation distance into the Fried parameter, which, for plane waves, is given by

$$r_0 = 0.185\left(\frac{\lambda^2}{C_n^2L}\right)^{3/5}. \quad (19)$$

One can define a dimensionless quantity

$$\mathcal{W} = \frac{w_0}{r_0}, \quad (20)$$

where w_0 is the beam radius of the measurement basis. Since $\mathcal{W}$ contains the propagation distance, it can be regarded as an indication of scintillation strength rather than turbulence strength. It was found [37] that, under weak scintillation conditions, the evolution of the entanglement of a photon pair that is entangled in its spatial degrees of freedom (such as OAM), is completely determined by $\mathcal{W}$. In our experiment we assume weak scintillation and simulate the turbulence with a single phase screen. As a result the parameter that we use to quantify the strength of the scintillation/turbulence is $\mathcal{W}$. Weak scintillation exists when the Rytov variance, which is given by

$$\sigma_R^2 = 1.23C_n^2k_0^{7/6}L^{11/6}, \quad (21)$$

is smaller than approximately 1.

Our experimental setup is shown diagrammatically in figure 2. Entangled photon pairs are generated, using SPDC, by pumping a type-I Barium borate (BBO) crystal with a 355 nm laser. The collinear, degenerate down-converted photons are imaged via a 4f-system from the BBO crystal plane to the two separate SLMs. These HoloEye SLMs consist of 1920 × 1080 pixels, with a pixel size of 8 μm. The photon pairs are projected onto particular helical modes, depending on the helical phase functions that are encoded onto the SLMs. The expression for the transmission (reflection) function of the SLMs encoded with these helical phase

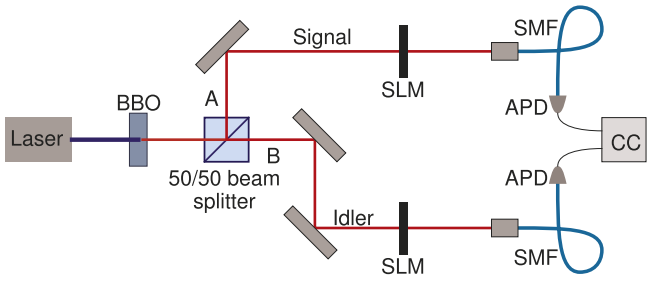

Figure 2. Experimental setup to generate and measure entangled photon pairs. A UV laser source pumps a type-I BBO crystal to produce pairs of entangled photons via SPDC. The crystal plane is imaged onto the SLMs and each SLM plane is imaged onto the input of a SMF.

functions is

$$t(\phi) = \exp(i\ell\phi), \quad (22)$$

where ϕ is the azimuthal coordinate and ℓ is the OAM index (an integer). Random phase functions are added to each SLM to simulate propagation through atmospheric turbulence. The resulting optical fields after the SLMs are then imaged via a 4f-system onto the input facet of single-mode fibers (SMFs). The single photons are detected with avalanche photo diodes (APDs), which are connected to a coincidence counter (CC) with a gating time of 12.5 ns.

4. Results and discussion

Prior to the quantum experiment we employ the technique of back projection [59] to observe the turbulence-distorted mode, for various levels of turbulence and for various OAM values. In this classical experiment one of the APD detectors was replaced by a diode laser and the classical light propagated backwards through the experimental set-up until detection at the second APD. The mode could then be imaged on a CCD detector at any plane along the path. The measured back projected modes at the plane of the BBO crystal are shown in figure 3. The distortion that is introduced by the modulation of the optical beam by the random phase functions on the SLMs leads to crosstalk between OAM modes. One can observe this crosstalk in terms of the decay of correlations between the OAM modes for a down-converted pair of photons. It is well known now that the anti-correlation between the OAM index of the two down-converted photons deteriorates with increasing scintillation, as introduced by the random phase function on the SLMs, and has been reported previously in both classical [60] and quantum studies [41]. The back projection experiment serves to visualize the perturbations of the turbulence screen.

Next, using the projective measurements in the helical basis, we perform quantum state tomography to reproduce the density matrices for the observed quantum states in the two-qubit–Hilbert spaces given by the particular value of ℓ. Such a quantum state tomography is performed by cycling through the different bases composed of the OAM modes in the restricted Hilbert space on each SLM and recording the

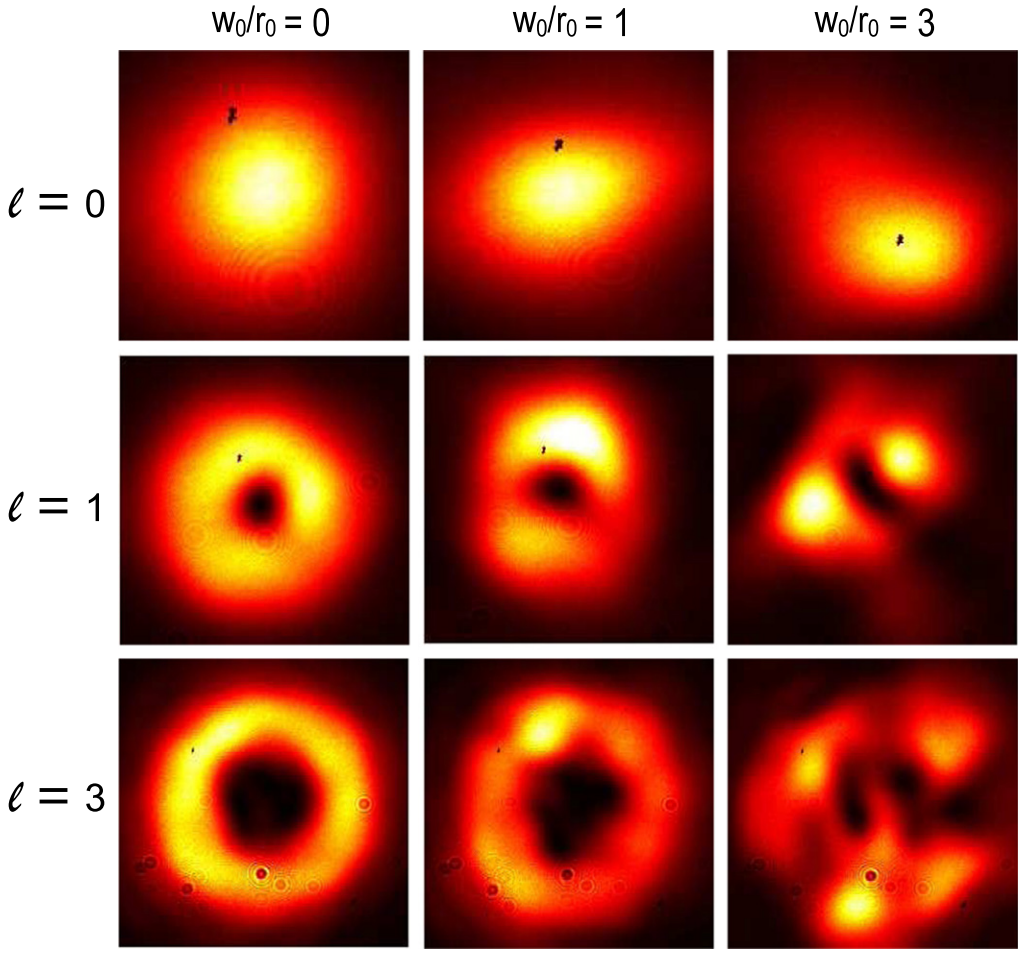

Figure 3. Experimentally measured effect of turbulence on the intensity distributions of OAM modes for $\ell = 0$, 1, 3. First column without turbulence ($\mathcal{W} = 0$). Second and third columns with progressively more severe turbulence conditions ($\mathcal{W} = 1$ and 3, respectively).

coincidence count rates. This quantum state tomography is repeated 30 times, with different sets of random phase functions (different realizations of the turbulent medium), for each value of $\mathcal{W}$, within the range $0 \leqslant \mathcal{W} \leqslant 4$, and for each of the four values of $\ell = 1$, 3, 5, and 7. The resulting density matrices are averaged to obtain a mean density matrix for a given $\mathcal{W}$ and ℓ.

These mean density matrices are used to calculate the quantum bit error rate Q, with the aid of equation (8), and then the minimal secret key rates $r_{\min}$ for the E91 protocol, using equation (9), and for the six-state protocol, using equation (10). The mean density matrices are also used to compute the EoF with the aid of equation (11). These minimal secret key rates $r_{\min}$ are shown, together with the EoF, as a function of $\mathcal{W}$ in figure 4. The calculation of $r_{\min}$ for the E91 protocol is done for all three different ways of choosing the two MUBs from those in equations (14)–(16). The curves denoted by E91 (a), (b) and (c) in figure 4 represent the three cases where the chosen MUBs are $\{\mathcal{M}_1, \mathcal{M}_3\}$, $\{\mathcal{M}_1, \mathcal{M}_2\}$ and $\{\mathcal{M}_2, \mathcal{M}_3\}$, respectively. All the MUBs in equations (14)–(16) are used for the six-state protocol.

Although the qualitative behavior of $r_{\min}$ and the EoF is the same, the former is lower than the latter and the former also decays to zero at a smaller value of $\mathcal{W}$ than the latter. This could be caused by a non-optimal choice of the measurement bases in the experiment. By choosing bases that are more optimal, one may be able to increase the minimal secret key rate $r_{\min}$.

Comparing the secret key rate of the different QKD protocols, as shown in figure 4, we find that the secret key rate in the E91 protocols are in general lower than that of the six-state protocol. This result is to be expected, since the six-state protocol is known to produce a higher secret key rate than E91 for the same quantum bit error rate (see figure 1). However, since the quantum bit error rate depends on the choice of the bases, the said quantity may differ for the E91 and the six-state protocols. This results in occasional better performance by the E91 protocols, as we see in figure 4. Moreover, the choice of MUBs for the E91 protocol makes a slight difference in the performance: the set $\{\mathcal{M}_2, \mathcal{M}_3\}$ gives slightly better performance than the other two choices for larger values of $\mathcal{W}$.

The aim of our experiment is to simulate the effect of atmospheric turbulence on down-converted pairs of photons, which are entangled in their spatial degrees of freedom. This allows us to study the security of QKD protocols that employ

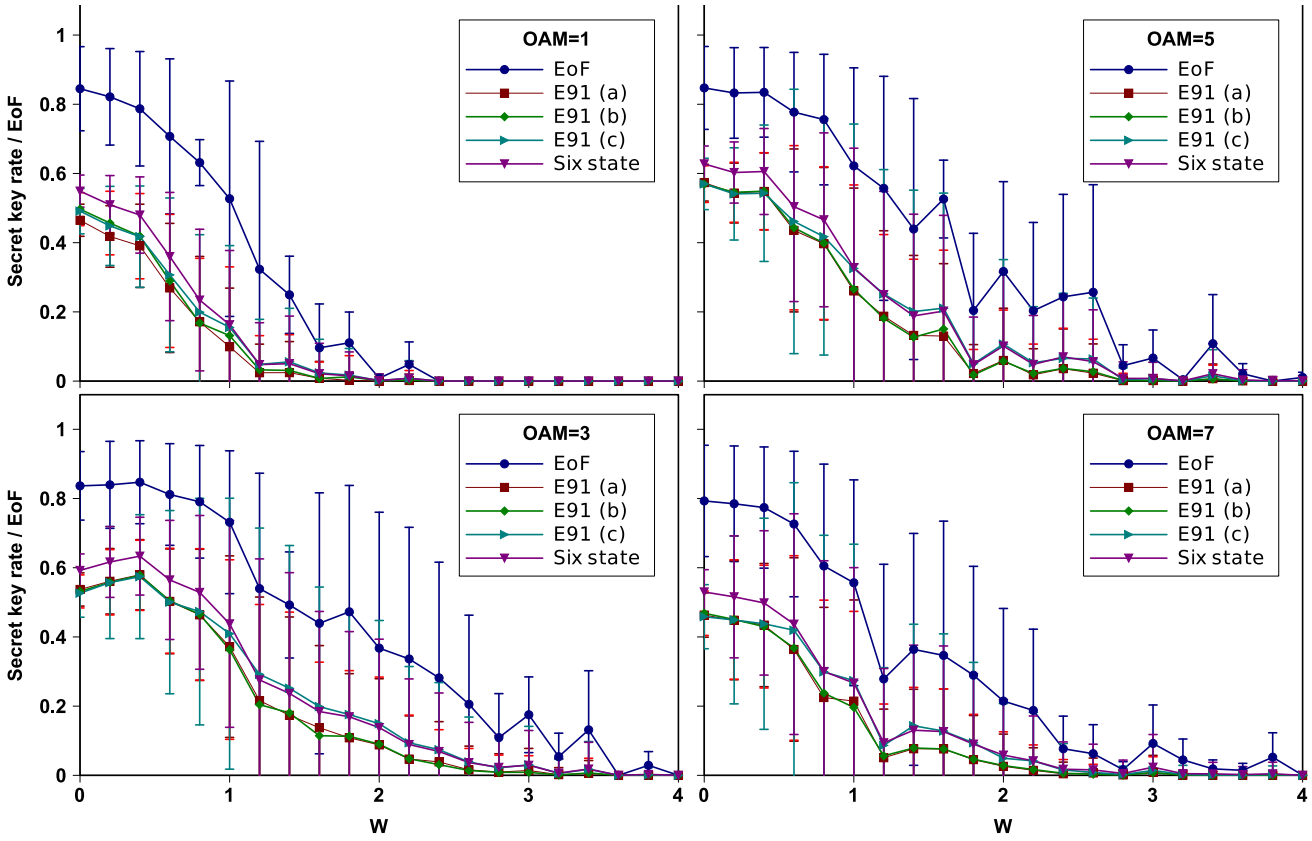

Figure 4. Measured secret key rates of E91 for three different possible choices of the two bases, secret key rate for six-state protocol, and the EoF as a function of $\mathcal{W} = w_0/r_0$ for different OAM encodings. The secret key rates are calculated using the quantum bit error rate Q using equation (8) from the measured density matrix and further using equations (9) and (10). The measured density matrix is used to calculate the EoF with the help of equations (11) and (13).

this type of entanglement resource in free space communication. Under weak scintillation conditions (as assumed in our experiment), the distance scale at which the concurrence decays to zero can be estimated from the observation (see figure 4) that, up to some numerical factor of order 1, the EoF decays to zero when $\mathcal{W} \approx 1$. According to numerical simulation results, the relationship is actually $\mathcal{W} \approx \sqrt{\ell}$ [61, 62], i.e., the larger the value of ℓ, the more tolerant the entanglement is against the turbulence. This can be explained as follows: the states $|\ell\rangle$ and $|-\ell\rangle$ scatter to nearby OAM modes due to the random fluctuations in the turbulent environment. These scattered subspaces corresponding to $|\ell\rangle$ and $|-\ell\rangle$ stay orthogonal for longer distance if the ℓ value is high. Therefore, the two photon states with higher ℓ value retains the entanglement for longer distance. The resulting concurrence decay distance scale is then given by [41]

$$L_{\mathrm{dec}} \approx \frac{0.06\lambda^2\ell^{5/6}}{w_0^{5/3}C_n^2}, \tag{23}$$

where the numerical constant can vary within an order of magnitude. Hence, the distance over which QKD can be operated successfully through a free space channel, depends on the dimension parameters and the OAM index, as shown in equation (23).

As an example, consider the challenge of replicating a previous reported free space QKD experiment with polarization entangled photons over a distance of 144 km [10]. Here $C_n^2 \approx 5 \times 10^{-16}$ m$^{-2/3}$ and $w_0 \approx 50$ mm for a photon wavelength of 710 nm. If an $\ell = 1$ qubit basis was used, the transmission distance for the same experimental parameters would be a little less than 10 km, or roughly an order of magnitude less than for polarization. The 144 km distance could only be reached (under the same experimental conditions) by using large OAM values, $\ell > 25$ due to the robustness of the large OAM modes against turbulence, but this is impractical due to other propagation considerations. This reinforces the very motivation for OAM as a basis for encoding information: its value lies in realizing higher dimensional states and not in replicating qubit states.

It should be noted that distance estimations are here made under the assumption of weak scintillation conditions, which require that the Rytov variance, given in equation (21), is smaller than 1, and which places a limit on the maximum distance. However, by varying some of the parameters, one can obtain larger decay distances, but one would then enter a region where the weak scintillation condition does not apply anymore. As a result the predicted distance would not be reliable. To obtain reliable predictions of operating distances

under strong scintillation conditions, one needs to employ multiple phase screen methods [63].

5. Conclusion

We performed an experimental study of the effect of atmospheric turbulence on the security of certain QKD protocols: E91 with different choices of MUBs and the six-state protocol. We found that, in the weak scintillation limit, one can distribute a quantum key securely over distances comparable to those over which the entanglement survives, but at a slightly lower secret key rate compared to the EoF.

References

[1] Lo H K 1998 *Introduction to Quantum Computation and Information* (Singapore: World Scientific)
[2] Ekert A K, Gisin N, Huttner B, Inamori H and Weinfurter H 2001 *The Physics of Quantum Information* (London: Springer)
[3] Gisin N, Ribordy G, Tittel W and Zbinden H 2002 *Rev. Mod. Phys.* **74** 145–95
[4] Scarani V 2006 *Quantum Physics—A First Encounter* (Oxford: Oxford University Press)
[5] Bellac M L 2006 *A Short Introduction to Quantum Information and Quantum Computation* (Cambridge: Cambridge University Press)
[6] Dušek M, Lütkenhaus N and Hendrych M 2006 *Prog. Opt.* **49** 381
[7] Lo H K and Zhao Y 2009 *Encyclopedia of Complexity and System Science* vol 8 (New York: Springer) p 7265
[8] Scarani V, Bechmann-Pasquinucci H, Cerf N J, Dušek M, Lütkenhaus N and Peev M 2009 *Rev. Mod. Phys.* **81** 1301–50
[9] Gröblacher S, Jennewein T, Vaziri A, Weihs G and Zeilinger A 2006 *New J. Phys.* **8** 75
[10] Ursin R *et al* 2007 *Nat. Phys.* **3** 481
[11] Erven C, Couteau C, Laflamme R and Weihs G 2008 *Opt. Express* **16** 16840–53
[12] Peev M *et al* 2009 *New J. Phys.* **11** 075001
[13] Peloso M P, Gerhardt I, Ho C, Lamas-Linares A and Kurtsiefer C 2009 *New J. Phys.* **11** 045007
[14] Jin X M *et al* 2010 *Nat. Photon.* **4** 376
[15] Sasaki M *et al* 2011 *Opt. Express* **19** 10387–409
[16] Erven C, Heim B, Meyer-Scott E, Bourgoin J P, Laflamme R, Weihs G and Jennewein T 2012 *New J. Phys.* **14** 123018
[17] Regev O 2004 *J. ACM* **51** 899–942
[18] Regev O 2006 Lattice-based cryptography *Advances in Cryptology—CRYPTO 2006* (Berlin: Springer) pp 131–41
[19] Micciancio D 2011 Lattice-based cryptography *Encyclopedia of Cryptography and Security* (Berlin: Springer) pp 713–5
[20] Güneysu T, Lyubashevsky V and Pöppelmann T 2012 Practical lattice-based cryptography: a signature scheme for embedded systems *Cryptographic Hardware and Embedded Systems—CHES 2012* (Berlin: Springer) pp 530–47
[21] Dixon A R, Yuan Z L, Dynes J F, Sharpe A W and Shields A J 2008 *Opt. Express* **16** 18790–979
[22] Shibata H, Honjo T and Shimizu K 2014 *Opt. Lett.* **39** 5078
[23] Korzh B, Lim C C W, Houlmann R, Gisin N, Li M J, Nolan D, Sanguinetti B, Thew R and Zbinden H 2015 *Nat. Photon.* **9** 163–8
[24] Boone K, Bourgoin J P, Meyer-Scott E, Heshami K, Jennewein T and Simon C 2015 *Phys. Rev.* A **91** 052325
[25] Allen L, Beijersbergen M, Spreeuw R and Woerdman J 1992 *Phys. Rev.* A **45** 8185–9
[26] Mafu M, Dudley A, Goyal S, Giovannini D, McLaren M, Padgett M J, Konrad T, Petruccione F, Lütkenhaus N and Forbes A 2013 *Phys. Rev.* A **88** 032305
[27] Vallone G, D'Ambrosio V, Sponselli A, Slussarenko S, Marrucci L, Sciarrino F and Villoresi P 2014 *Phys. Rev. Lett.* **113** 060503
[28] Mirhosseini M, Magaña-Loaiza O S, O'Sullivan M N, Rodenburg B, Malik M, Gauthier D J and Boyd R W 2014 arXiv:1402.7113
[29] Malik M, OSullivan M, Rodenburg B, Mirhosseini M, Leach J, Lavery M P, Padgett M J and Boyd R W 2012 *Opt. Express* **20** 13195–200
[30] Rodenburg B, Lavery M P J, Malik M, OSullivan M N, Mirhosseini M, Robertson D J, Padgett M and Boyd R W 2012 *Opt. Lett.* **37** 3735
[31] Rodenburg B *et al* 2014 *New J. Phys.* **16** 033020
[32] Rodenburg B *et al* 2014 *New J. Phys.* **16** 089501(E)
[33] Paterson C 2005 *Phys. Rev. Lett.* **94** 153901
[34] Gapaul C and Andrews R 2007 *New J. Phys.* **9** 94
[35] Tyler G A and Boyd R W 2009 *Opt. Lett.* **34** 142
[36] Anguita J A, Neifeld M A and Vasic B V 2008 *Appl. Opt.* **47** 2414
[37] Smith B J and Raymer M G 2006 *Phys. Rev.* A **74** 062104
[38] Roux F S 2011 *Phys. Rev.* A **83** 053822
[39] Zhang Y, Djordjevic I B and Gao X 2012 *Opt. Lett.* **37** 3267
[40] Pors B J, Monken C H, Eliel E R and Woerdman J P 2011 *Opt. Express* **19** 6671–83
[41] Hamadou I A, Roux F S, McLaren M, Konrad T and Forbes A 2013 *Phys. Rev.* A **88** 012312
[42] Zhao S M, Leach J, Gong L Y, Ding J and Zheng B Y 2012 *Opt. Express* **20** 452
[43] Ren Y *et al* 2014 *Optica* **1** 376–82
[44] Brünner T and Roux F S 2013 *New J. Phys.* **15** 063005
[45] Gonzalez A J R and Brun T A 2013 *Phys. Rev.* A **88** 022326
[46] Ekert A 1991 *Phys. Rev. Lett.* **67** 661–3
[47] Bruß D 1998 *Phys. Rev. Lett.* **81** 3018–21
[48] Schwinger J 1960 *Proc. National Academy of Sciences of the United States Of America* vol 46, p 570
[49] Bennett C *et al* 1984 Quantum cryptography: public key distribution and coin tossing *Proc. IEEE Int. Conf. on Computers, Systems and Signal Processing (Bangalore, India)* vol 175
[50] Ferenczi A and Lütkenhaus N 2012 *Phys. Rev.* A **85** 052310
[51] Sheridan L and Scarani V 2010 *Phys. Rev.* A **82** 030301
[52] Horodecki R, Horodecki P, Horodecki M and Horodecki K 2009 *Rev. Mod. Phys.* **81** 865–942
[53] Wootters W K 1998 *Phys. Rev. Lett.* **80** 2245
[54] Kolmogorov A N 1941 *Dokl. Akad. Nauk SSSR* **30** 301–5
[55] Martin J M and Flatté S M 1988 *Appl. Opt.* **27** 2111
[56] Martin J M and Flatté S M 1990 *J. Opt. Soc. Am.* A **7** 838
[57] Knepp D L 1983 *Proc. IEEE* 71, 722
[58] Lane R G, Glindemann A and Dainty J C 1992 *Waves Random Media* **2** 209
[59] McLaren M, Romero J, Padgett M J, Roux F S and Forbes A 2013 *Phys. Rev.* A **88** 033818
[60] Trichili A, Mhlanga T, Ismail Y, Roux F S, McLaren M, Zghal M and Forbes A 2014 *Opt. Express* **22** 17553
[61] Ibrahim A H, Roux F S and Konrad T 2014 *Phys. Rev.* A **90** 052115
[62] Leonhard N D, Shatokhin V N and Buchleitner A 2015 *Phys. Rev.* A **91** 012345
[63] Roux F S, Wellens T and Shatokhin V N 2015 *Phys. Rev.* **92** 012326