Performance analysis of d-dimensional quantum cryptography with mode-dependent diffraction

Jiapeng Zhao[1], Mohammad Mirhosseini[2], Yiyu Zhou[1], Seyed Mohammad Hashemi Rafsanjani[1], Yongxiong Ren[3], Nicholas K. Steinhoff[4], Glen A. Tyler[4], Alan E. Willner[3], Robert W. Boyd[1,5]

[1]*The Institute of Optics, University of Rochester, Rochester, New York, 14627, USA*
[2]*California Institute of Technology, Pasadena, California, 91125, USA*
[3]*University of Southern California, Los Angeles, California, 90007, USA*
[4]*The Optical Science Company, Anaheim, California, 92806, USA*
[5]*Department of Physics, University of Ottawa, Ottawa ON K1N 6N5, Canada*

Abstract: We analyze the degraded performance of QKD that results from mode-dependent diffraction in spatial-mode-encoded QKD systems. A pre-compensation method is proposed to solve this problem without sacrificing the security.

OCIS codes: 270.5565, 270.5568.

1. Introduction

The orbital angular momentum (OAM) of light is a promising candidate for d-dimensional quantum key distribution (QKD). The beam has an azimuthally dependent wavefront $\exp(i\ell\theta)$ and carries an OAM of $\ell\hbar$ per photon, where ℓ is the OAM quantum number. One characteristic of an OAM mode is the ℓ-dependent diffraction, which lead to the ℓ-dependent far-field beam size [1] and propagation phase (i.e. the Gouy phase for Laguerre Gaussian states). This will give rise to mode-dependent loss for a given finite size of the receiver's aperture and mode-dependent relative phase. Both effects will lead to an increased error rate at the receiver. We propose a compensation method to overcome this problem without sacrificing the security [2]. The experimental data shows that our approach can significantly reduce the error rate and increase the information capacity without sacrificing the security.

2. Degraded performance of QKD under mode-dependent diffraction

In OAM-based QKD, we use the OAM basis and its Fourier conjugate angular (ANG) basis to encode photons. One particular ANG state j is used to written as:

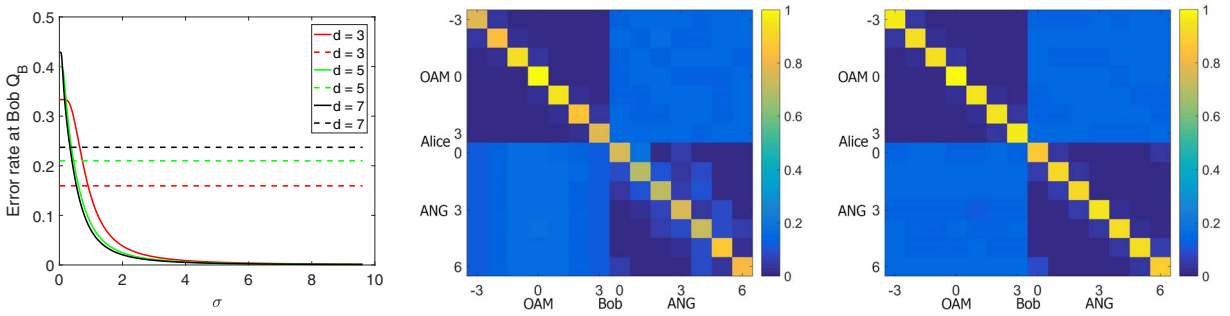
$$|j\rangle = \frac{1}{\sqrt{d}} \sum_{\ell=-L}^{L} |\ell\rangle e^{-i\ell 2\pi j/d}, \tag{1}$$

where $|\ell\rangle$ is the OAM state with quantum number ℓ. d is the dimension of the Hilbert space and L is the maximum OAM quantum number, which satisfies the relation $2L+1=d$. Considering mode-dependent diffraction, the OAM spectrum at the receiver will not be uniform, and the ANG spectrum will be broader. The ANG state j is modified as follows:

$$|j\rangle_B = \frac{1}{\sqrt{\varepsilon_j}} \hat{F}|j\rangle_A = \sum_{p=0}^{d-1} \sqrt{P_{j,p}}|j+p\rangle = \sum_{\ell=-L}^{L} \sqrt{P_\ell}|\ell\rangle_A e^{-i\ell(2\pi j/d-\psi(z))}, \tag{2}$$

where A indicates that this is the ANG mode prepared by Alice, B indicates that the state is received by Bob. $\frac{1}{\sqrt{\varepsilon_j}}$ is the normalization constant representing the efficiency of ANG state j, $\hat{F}$ is the propagation operator including the effect of finite aperture size, $P_{j,p}$ is the probability of finding ANG index $j+p$ in ANG basis, and P_ℓ characterizes the probability of finding the OAM component ℓ in the modified ANG mode j. $\sqrt{P_{j,p}}$ and $\sqrt{P_\ell/d}$ are related by a quantum Fourier transform, and one can also check that $P_{j,p}=P_{j+1,p}=\cdots$. The $\psi(z)$ is the propagation phase acquired by each OAM component during the propagation. One can figure out that the crosstalk has been introduced into the ANG basis by mode-dependent diffraction, and hence the errors will be introduced at the receiver.

To characterize how the quantum symbol error rate (QSER) changes as a consequence of the diffraction, we assume that the probability distribution of P_ℓ has a Gaussian shape with variance σ, which characterizes the degree of crosstalk



(a) (b) (c)

Fig. 1: **(a).** The relation between QBER and σ where dashed lines are upper bounds of QBER while the solid lines are QBER with mode-dependent diffraction. **(b).** The figure gives the crosstalk matrix with no compensation. **(c).** The figure provides the crosstalk matrix with WPC.

induced by diffraction. A highly lossy channel with long propagation distance will lead to a small value of σ, which means that only the fundamental Gaussian mode can be transmitted. This will lead the loss of information so that no secure channel can be established. We have plotted the QSER as the function of the crosstalk parameter σ in Fig.1 (a). For a given dimension d, strong diffraction (i.e. a small σ) can significantly increase the QSER even if there is no quantum attack. This will lead to a lower information capacity, and make the system more vulnerable to eavesdropping and quantum cloning because the upper bound of the QSER is fixed for each given dimension d.

3. Pre-compensation protocol

To reduce the overall loss, we use the minimum energy loss (MEL) modes as the OAM courier [3]. These modes are well-designed self-imaging modes providing a larger spatial bandwidth than conventional top-hat OAM modes or Laguerre-Gaussian (LG) modes. The efficiency of a MEL mode only depends on the Fresnel number N_f and the OAM quantum number ℓ. We propose a pre-compensation methods using MEL modes to overcome the diffraction-induced defects: *Waist pre-compensation (WPC)*: The transmitter carefully selects her OAM modes so that each mode with different OAM value has different sizes of beam waist but similar loss for the given link, and then use these selected OAM modes to construct the ANG basis. After that, each OAM component will be pre-compensated with an extra propagation phase so that the relative phase between two adjacent OAM states is $exp(-i2\pi j/d)$.

The experimental verification of the WPC has been performed in a link with $N_f = 3.96$. The crosstalk matrices are shown in Fig.1 (c) and (d). One can see that the crosstalk in the ANG basis is very small, especially compared with the crosstalk matrix without any compensation, which is shown in Fig. 1 (c). The QSER measured from the case of no compensation is 14.2% while the QSER with WPC is 6.7%. Therefore, the compensation protocol can significantly reduce the QSER to a lower level. The mutual information between two legitimate parties calculated with WPC can be found as 2.56 bits per photon which is improved from 2.22 bits per photon for the case of no compensation.

4. Conclusion

We point out that mode-dependent diffraction can introduce defects in a practical QKD system with high-dimensional spatial mode encoding. One pre-compensation method is proposed and verified in the lab. By comparing the performance of no-compensation case with compensated case, we can find the QSER can be significantly reduced so that the information capacity and the robustness against the eavesdropping can be maintained with our WPC protocol even if the mode-dependent diffraction is found.

References

1. M.J.Padgett, F.M.Miatto, M.P.Lavery, A.Zeilinger and R.W.Boyd, New Journal of Physics **17**, 023011, 2015.
2. V.Scarani, S.Iblisdir, N.Gisin and A.Acin, Reviews of Modern Physics **77**, 1225, 2005.
3. G.A.Tyler, Optics letters **36**, 4650–4652, 2011.