Generalized spatial-mode detection efficiency mismatch in a free-space QKD system with Zernike polynomials

Poompong Chaiwongkhot,[1, 2, *] Katanya B. Kuntz,[1, 2] Jean-Philippe Bourgoin,[1, 2]
Norbert Lütkenhaus,[1, 2] Vadim Makarov,[3, 2] and Thomas Jennewein[1, 2, 4]

[1] *Institute for Quantum Computing, University of Waterloo, Waterloo, ON, N2L 3G1 Canada*
[2] *Department of Physics and Astronomy, University of Waterloo, Waterloo, ON, N2L 3G1 Canada*
[3] *Russian Quantum Center and MISIS University, Moscow*
[4] *Quantum Information Science Program, Canadian Institute for Advanced Research, Toronto, ON, M5G 1Z8 Canada*

(Dated: June 29, 2018)

Quantum cryptography promises a high level of security. However, practical quantum key distribution (QKD), it is important to look for exploitable loopholes and implement proper countermeasures to prevent attacks. It is equally important to verify the effectiveness of countermeasure implementation against the attack it is designed to counter, as well as other variants. Detection efficiency mismatch is a class of attack where eavesdropper (Eve) alters the state of the the signal sent to Bob in order to force a specific detection outcome. Our previous study [1] shows that by altering the angle of signal sent to Bob, Eve could bias the detection probability in a free-space QKD receiver, enabling intercept and resend attack. A pinhole was proposed as a countermeasure.

Here, we propose a more general method of characterizing the spatial-mode detection efficiency mismatch in a free-space QKD system using a phase-only spatial light modulator (SLM). We use a SLM to manipulate the phase wavefront of the attack beam. The wavefront consists of a combination of Zernike polynomials Zi [2]. Each Zernike polynomial represents a different optical aberration, including tip-tilt components (Z2 and Z3) which were used in the previous study [1]. We adjust the weightings of each polynomial to produce the optimal wavefront to attack the free-space QKD receiver.

Our experiments are divided into two parts: first, we characterize the detection efficiency mismatch apparatus with SLM and explore the effect of higher order Zernike polynomials on detection efficiency mismatch. Second, we verify the effectiveness of spatial filter against both original tip-tilt as well as using more complex wavefront.

We replace the mechanical scanning apparatus in Ref. 1 with an SLM, as shown in Fig. 1. The test of far-field characteristics of the beam generated by the SLM matches the theoretical simulation throughout the beam path. Limited by stability of the setup, it is impossible to measure all possible Zernike polynomials combinations. The value of Z_i in this study is limited to ±20 for Z2 and Z3 (tip-tilt), and ±8 for higher order Z_i.

The receiver we test is a prototype for a quantum communication satellite [3] with polarization encoding. It is a passive basis choice receiver operating at 532 nm wavelength. In this type of receiver, the input light is split by a 50:50 beamsplitter (BS) and polarizing beamsplitters (PBS) into four multimode fibers leading to four single-photon detectors. The detectors receive photons polarized horizontally H, vertically V, +45 deg D and −45 deg A. The efficiency mismatch ratio (δ_k) means that a detector in channel $k \subset H, V, D, A$ has a probability to click at least δ_k times higher than the detectors in the other basis.

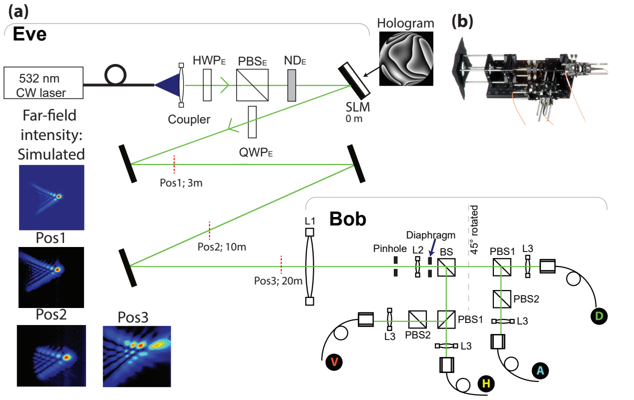

FIG. 1. (a)Experimental setup, and (b)Picture of receiver under test.

The experiment is done by sending circularly polarized light from the source with the wave-front controlled by weight terms Z_i of the hologram on the SLM. The goal here is to find a combination of Z_i that cause highest δ_k for each k channel. Our test of tip-tilt (Z_2, Z_3) scanning shows similar result as [1] (see Fig. 2 (b)). This tip-tilt-only case gave δ_k varying between 1.5–17.7. The higher-order scan of $Z_4 - Z_7$ showed values of δ_k varying between 1.3–4.7, which is not high enough for Eve to exploit. However, when we combine tip-tilt with polynomials Z4 to Z7 , we can significantly increase the mismatch ratio up to 7 times higher than the tip-tilt-only case; the highest value of δ_k obtained is 52.3. In addition to flexibility, the SLM also provides better precision and stability over mechanical scanning setup. It also eliminates distortion caused by tilting the scanning lens.

We also use the setup to verify the effectiveness of spatial filter (25 µm pinhole). The result in Fig. 2 (b) shows that the pinhole can only block the translational modes and small-angle reflection from beamsplitters. However,

[*] poompong.ch@gmail.com

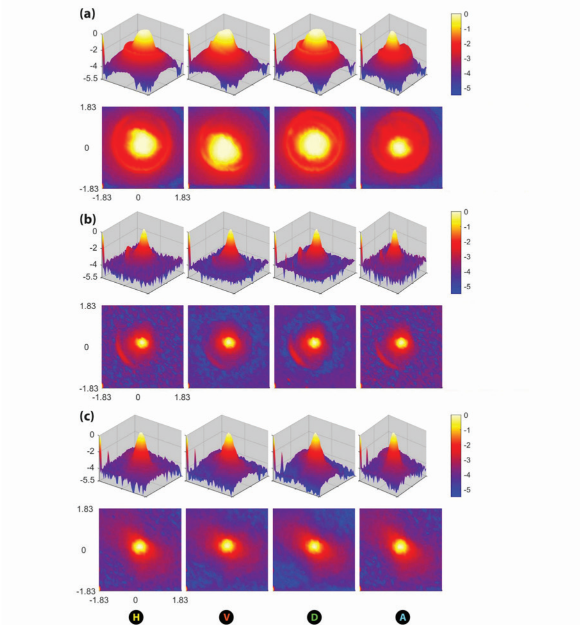

FIG. 2. Tip-tilt scanning result shows normalized detection probability of each detector at different incoming beam angle in mrad on three different scenarios; (a) without pinhole, (b) with pinhole, and (c) with pinhole and diaphragm.

TABLE I. Efficiency mismatch ratio and corresponding weight value of Zernike polynomial weights of V channel under different cases.

Cases	Optimal weight combination				Mismatch ratio (δ)
	Z4	Z5	Z6	Z7	
No pinhole	-8	2	4	4	4.7
Pinhole	8	0	8	4	15.0
Pinhole+diaphragm	-2	6	6	0	15.9

it could not reliably block high-angle trajectory (i.e. lens edge scattering). To counter high-angle scattering, we add a diaphragm behind the collimating lens (L2) in the receiver. The result in Fig. 2 (c) shows that diaphragm and pinhole together help prevent most of the efficiency mismatch from tip-tilt mode. The only feature left is the translational shift of fiber coupler, which causes mismatch angle close to the original beam path in channel H ($\delta_H = 4.5$) and channel V ($\delta_V = 16.9$). These are preliminary results and could be caused by a non-optimal choice of diaphragm size and position. Furthermore, additional iteration of tip-tilts scanning and fine alignment of fiber coupler's position in the alignment procedure of Alice and Bob might help mitigate remaining mismatch. We also test this setup against the attack with higher order Zernike polynomial $Z_4 - Z_7$. As shown in Table I, there exists new combinations of $Z_4 - Z_7$ that could cause higher δ_V than the case without countermeasure. Similar behavior appears in all other channels.

Conclusion In this study, we present a new method to characterize the spatial-mode detection efficiency mismatch using SLM. This provides us both flexibility and precision, which reveals some exploitable features obscured in previous setup. We show that by including higher-order Zernike polynomials, Eve could increase detection efficiency mismatch. This, along with the failure of diaphragm and pinhole to prevent the higher-order attack signifies the importance of including all possible combinations of Zernike polynomials in the characterization of detection efficiency mismatch in free space. The exploitable features shown demonstrates the importance of including a tip-tilt scan while adjusting the alignment between Alice and Bob, as these features could not be seen in the normal alignment procedure. Further study on characterization and finding a better countermeasure against spatial-mode detection efficiency mismatch is highly encouraged.

[1] S. Sajeed, P. Chaiwongkhot, J.-P. Bourgoin, T. Jennewein, N. Lütkenhaus, and V. Makarov, Phys. Rev. A **91**, 062301 (2015).

[2] R. J. Noll, J. Opt. Soc. Am. **66**, 207 (1976).

[3] J.-P. Bourgoin, E. Meyer-Scott, B. L. Higgins, B. Helou, C. Erven, H. Hübel, B. Kumar, D. Hudson, I. D'Souza, R. Girard, R. Laflamme, and T. Jennewein, New J. Phys. **15**, 023006 (2013).