Effect of atmospheric turbulence on spatial-mode detector-efficiency mismatch

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

[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]*Department of Electrical and Computer Engineering, University of Waterloo, Waterloo, Ontario, N2L 3G1 Canada*
[4]*Quantum Information Science Program, Canadian Institute for Advanced Research, Toronto, ON, M5G 1Z8 Canada*

(Dated: April 26, 2017)

Introduction. In theory, quantum key distribution (QKD) is unconditionally secure; however in practice, a real system is never perfect. Therefore, it is important to study the flaws and vulnerabilities of a system, and find a solution or countermeasure to successful attacks. Recent studies have shown that it is possible to hack a QKD receiver by changing the spatial mode of the incoming beam to the receiver [1]. This attack depends on the ability of the eavesdropper, Eve, to precisely maintain a certain input angle to the receiver. It is well known that turbulence in the transmission channel can, in practice, hinder the performance of both legitimate parties' communication and the adversary's attack. While the assumption of a physical limitation of an eavesdropper (Eve) is not usually part of the security analysis of a QKD system, it is common in practice to have a secure surrounding where Eve could not present, such as in military operation. Therefore, the effect of turbulence on free-space QKD needs to be studied.

We experimentally emulated atmospheric turbulence in the lab using a phase-only spatial light modulator (SLM) to test whether such an attack would still succeed in a turbulent channel. We first verified the accuracy and reproducibility of the atmospheric turbulence emulated by our SLM setup. Then we performed a spatial mode attack for various strengths of the turbulence following a similar procedure as presented in Sajeed *et al.* [1]. From the result, we determined an upper bound on the level of turbulence and distance from adversary where such a spatial mode attack can still succeed on this specific receiver, assuming the adversary only has practical devices with today's technology. Therefore we can determine what atmospheric conditions makes our system safe from this type of attack.

Turbulence emulator. We use a phase-only SLM to emulate atmospheric turbulence in the lab. The advantage of using an SLM as opposed to performing the experiment outside is the ability to generate reproducible turbulence of various strengths without being affected by an unpredictable environment. We chose to generate the phase holograms that represent turbulence based on the Kolmogorov model [2] using a superposition of Zernike polynomials [3]. Zernike polynomials make a convenient basis choice as they directly relate to known optical aberrations, such as tip/tilt, defocus, astigmatism, etc.

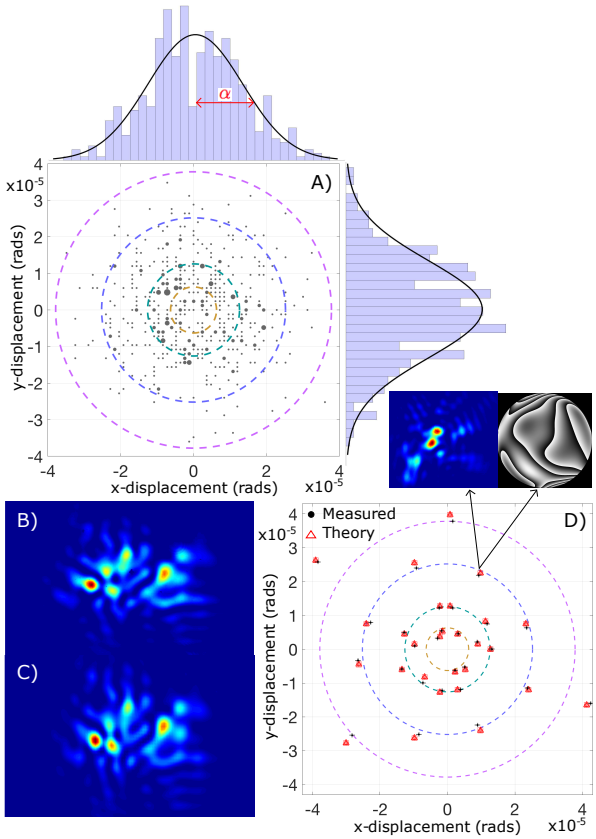

FIG. 1. Turbulence emulator characterization for $r_0 = 1$ cm and $D = 20$ cm. A) Simulated centroid displacements corresponding to 500 phase holograms (α = standard deviation). The size of the data point corresponds to the count frequency. B) Measured and C) Simulated far-field intensity distributions. D) Comparison between measured and simulated centroid displacements for hologram subset.

Another important advantage to using Zernike modes as the basis-set is that their weightings can be analytically calculated based on the strength of turbulence [4]. The radial phase function, $\phi(\rho, \theta)$, that describes each phase hologram is given by a weighted sum of several Zernike polynomials as $\phi(\rho, \theta) = \sum_i c_i Z_i$, where Z_i and c_i are the Zernike polynomial and corresponding coeffi-

* poompong.ch@gmail.com

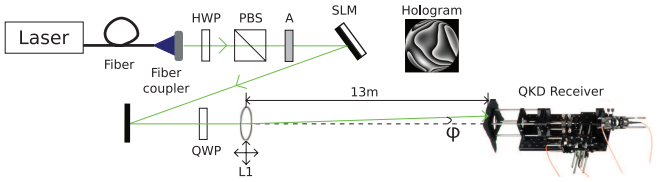

FIG. 2. Experimental setup of our spatial mode attack in a turbulent channel. HWP: half wave-plate, QWP: quarter wave-plate, PBS: polarization beam splitter, A: attenuator, SLM: spatial light modulator, L1: scanning lens, $\phi =$ scanning angle.

cient for the ith mode, respectively, following the Noll labelling convention [3].

We can use simple equations and devices, such as a CCD camera or wavefront sensor, to independently verify and characterize our turbulence emulator. This step is crucial before we can proceed with scanning a QKD receiver in a turbulent channel. It is vital to know whether the emulated turbulence generated by the SLM setup agrees with the predicted strength from theory and simulation results. Therefore, we calculated the theoretical far-field intensity distribution and centroid displacement for comparison with experimental results.

Figure 1 shows both the theoretical and experimental far-field intensity distributions and centroid displacements that emulates strong atmosphere turbulence corresponding to low-altitude sea level ($C_n^2 = 3.67 \times 10^{-14}\,\mathrm{m}^{-2/3}$). Each data point in Fig. 1A and 1D corresponds to a unique phase hologram and far-field distribution. This data illustrates we have excellent agreement between theory and experiment for turbulence emulated using our SLM setup. Therefore, we are confident our setup can accurately emulate reproducible turbulence of various strengths, and we can now attempt a spatial mode attack in a turbulent channel.

Spatial mode attack in a turbulent channel. We use our turbulence emulator to study the effect of turbulence on free-space detection efficiency mismatch. The experimental setup consists of two parts: the turbulence emulator (SLM) and the beam scanning (steering lens, L1), as shown in Fig. 2. Our source is a 532 nm continuous-wave laser that is first sent through polarization optics to generate horizontally-polarized light to ensure phase-only modulation from the SLM. The light after the SLM has a phase wavefront that represents a beam that has travelled through atmospheric turbulence. We use a quarter wave-plate to then rotate the polarization to circularly polarized so there will be a signal on all four detector channels in the QKD receiver. The scanning lens, L1, is mounted on a two-axis motorized translation stage to scan the angle of the outgoing beam. Finally, we place the receiver 13 m away from L1. The QKD receiver under test is a prototype for a quantum communication satellite [6] that has a passive basis choice to detect polarization-encoded light operating at 532 nm on four channels: horizontally **H**, vertically **V**, diagonally at $+45°$ **D** or anti-diagonally at $-45°$ **A**.

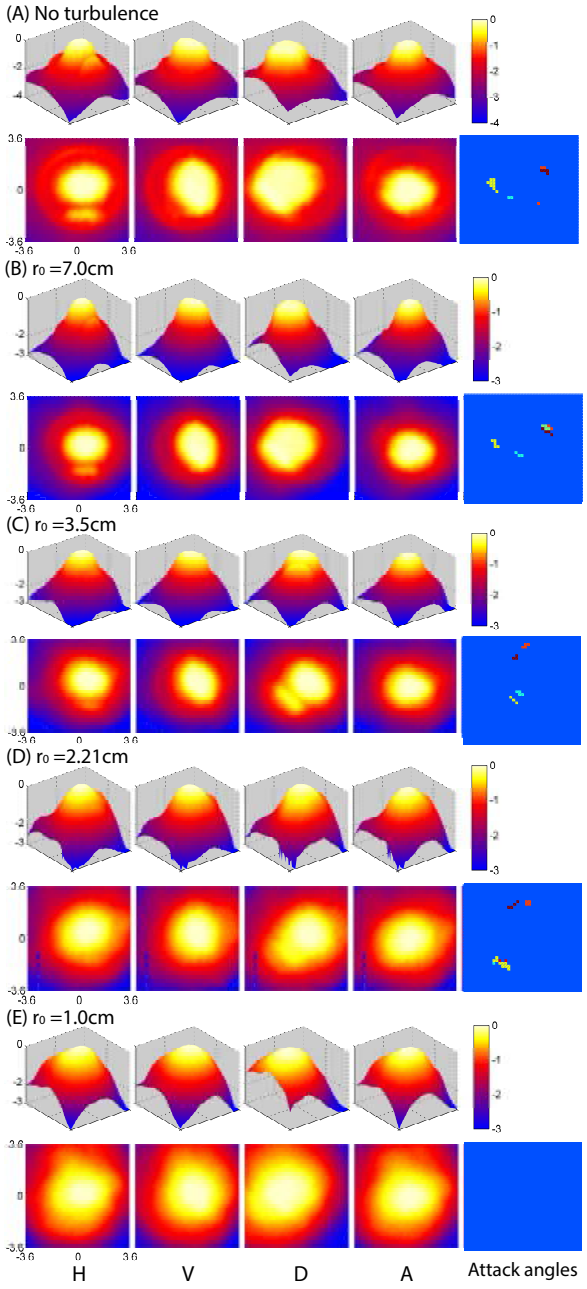

FIG. 3. Normalized count rates for each detector at different incoming beam angles, and the corresponding attack angles for different turbulence strengths. The color of the attack angles denote which detector: dark red: H-detector, red: V, yellow: D, light-blue: A, green: overlap between H and V detectors.

During the receiver alignment procedure, we first send a beam through the center of the lens, L1, to optimize and equalized the detection rates of all four detectors (along dashed line shown in Fig. 2). This initial alignment represents normal operation between Alice (sender) and Bob (receiver). We then adjust the position of lens L1,

TABLE I. Efficiency mismatch parameters for hacking data shown in Fig. 3 and Fig. 4. δ_k = minimum detection efficiency ratio, τ_k = detection efficiency lower bound.

Turbulence r_0	δ_k				τ_k			
	H	V	D	A	H	V	D	A
None	4	4	35	7	0.4	0.08	0.8	0.1
7.0 cm	2	3	30	3	0.4	0.3	0.5	0.5
3.5 cm	1.5	1.5	5	3	0.2	0.1	0.4	0.6
2.21 cm	1.5	1.4	3.5	3	0.2	0.3	0.1	0.5
1.0 cm	1.3	2	1.5	1.5	0.5	0.05	0.4	0.5

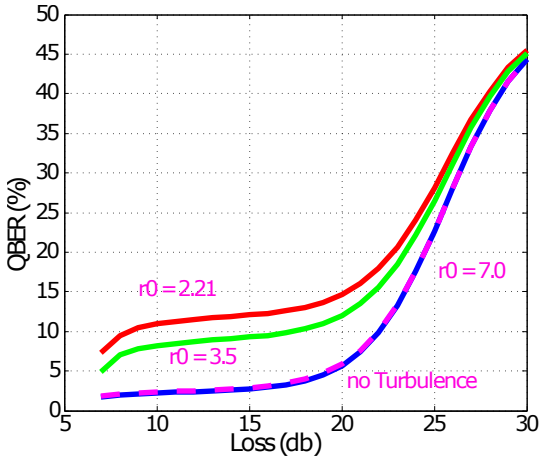

FIG. 4. Optimized quantum bit error rate (QBER) as a function of transmission loss for different turbulence strengths.

and record the detection efficiencies for different angles. The scan is performed in 90 µrad steps covering a range of ±3.6 mrad, which corresponds to a lateral displacement of ±48 mm at the front lens of the QKD receiver.

Our procedure follows the same method as described in [1] to find the potential attack angles where one channel has more probability to click than the other. In our attack model, Eve is restricted to today's technology and using a weak coherent state as her source. The attack angles shows in the right most plot of each sub figure Fig. 3, for example, the scan results without turbulence, Fig.3(A), for the **H** detector, the attack angles are where the **H** detector has a probability of clicking at least 4 times higher than **D** or **A** detectors ($\delta_H = 4$), and the normalized detection probability is greater than 0.4 ($\tau_H = 0.4$). The ratios for the other channels are shown in Tab. I. These parameters were then used in an optimization program to find a set of mean photon numbers that Eve could use for her resent signal to match Bob's expected detection probability while minimizing the quantum bit error rate (QBER).

To simulate the attack under turbulence, we sequentially cycle through a subset of phase holograms on the SLM for each attack angle. We assumed that Eve can measure and correct the tip/tilt component of turbulence using adaptive optics. The final normalized detection efficiency of each detector, η_k, is the weighted sum of the detection rates that resulted from each hologram. We then repeated this process for different turbulence strengths from very weak to strong turbulence corresponding to low-altitude sea level. The attack angles and respective parameters are shown in Fig. 3(B)-(E) and Tab. I.

It can be seen that the stronger turbulence is, the weaker the mismatch ratio (δ_k) and the normalized detection rate at each angle becomes. As a result, the optimized QBER for an attack under strong turbulence is higher overall. The minimized QBER under attack as a function of transmission loss between Alice and Bob is shown in Fig. 4. If we assume that the QBER threshold is 8 %, then the attack without turbulence is successful when the transmission loss between Alice and Bob is less than 22 dB. The weakest turbulence, $r_0 = 7.0$ cm, only slightly affects this result, and looks very similar to the no turbulence case. The strongest turbulence Eve can successfully attack is $r_0 = 3.5$ cm when the transmission loss is lower than 10 dB. This turbulence strength is equivalent to Eve having her resent setup 250 m away from Bob's receiver at sea level. Further more, the result for $r_0 = 2.21$ cm shows that there is no case where the transmission loss between Alice and Bob is low enough where Eve can attack without inducing a QBER that exceeds the threshold. Lastly, for $r_0 = 1.0$ cm, the mismatch ratio is too small ($\delta \leq 2$ for all channels). Therefore, the optimization program could not find a solution for an optimal QBER for any transmission loss.

Conclusion. In this study, we successfully emulated atmospheric turbulence in a lab environment using a phase-only spatial light modulator, and demonstrated a spatial mode detection efficiency mismatch attack in a turbulent channel. We showed the overall trend for the effectiveness of an attack under different turbulence strengths. We found that Eve can attack a free-space non-decoy state BB84 system from up to 250 m away at sea level. Our result implies that if Alice and Bob can establish a secure zone of approximately 250 m around this particular receiver system, then both parties can still exchange a key that is secure from this type of attack.

[1] S. Sajeed *et al.,* Phys. Rev. A **91**, 062301 (2015).
[2] L.C. Andrews and R.L. Phillips, *Laser beam propagation through random media* (SPIE Optical Engineering Press, 1998).
[3] R.J. Noll, J. Opt. Soc. Am., **66**, 207–211 (1976).
[4] L. Burger *et al.,* S. Afr. J. Sci. **104**, 129–134 (2008).
[5] R. Tyson, *Principles of adaptive optics* (CRC Press, 2010).
[6] J.-P. Bourgoin *et al.,* Phys. Rev. A **92**, 052339 (2015).