Spatial-mode detector efficiency mismatch security loophole in free-space QKD

Poompong Chaiwongkhot,[1,2] Shihan Sajeed,[1,3] Jean-Philippe Bourgoin,[1,2]
Thomas Jennewein,[1,2,4] Norbert Lütkenhaus,[1,2] and Vadim Makarov[1,2,3]

[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, ON, N2L 3G1 Canada*
[4] *Quantum Information Science Program, Canadian Institute for Advanced Research, Toronto, ON, M5G 1Z8 Canada*

Introduction. Recent studies show that free-space quantum key distribution has an ability to distribute secret keys over hundreds of kilometers above the ground. In addition, with current technology it is the only channel that can be employed for quantum key distribution on the global scale, via satellite-based systems. Although QKD protocols and security analysis have been developed in theory, deviation of the actual behavior of the devices from the ideal behavior expected in theory presents a major challenge in physical implementation. Thus, to guarantee the security, it is of utmost importance to scrutinize the practical device behaviors for possible deviations, and develop necessary countermeasures to any loophole that can be exploited.

In this submission based on our recent preprint [1], we focus on one such deviation inherent to free-space QKD receivers. We experimentally characterize it, and propose and characterize a countermeasure. We explore a violation of detection efficiency symmetry among all quantum states in Bob's receiver. If this violation exists, an adversary Eve can send light to Bob in different spatial modes so that one detector has a relatively higher probability of click than the other detectors. In this way, she can exploit the mismatch in efficiency [2] and make Bob's measurement outcome dependent on his measurement basis and correlated to Eve, which breaks the assumptions of typical security proofs. In this work, we investigate how crucial this can be to the security of QKD. (While finishing our paper, we became aware of a recent similar work [3].)

We study a receiver designed for polarization encoding free-space QKD, described in the experiment section. We begin by sending an attenuated laser beam to the receiver with various angle offsets and recording the relative detection probability in each channel, to find incidence angles with high efficiency mismatch. With these data, we show by numerical modeling that an eavesdropper attack exists that enables Eve to steal the secret key. Lastly, we discuss a countermeasure.

Experiment. The receiver we test is a prototype for a quantum communication satellite [4] with polarization encoding. It is a passive basis choice receiver operating at 532 nm wavelength [Fig. 1(a,c)]. 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**, $+45°$ **D** and $-45°$ **A**. In order to exploit the mismatch in efficiency, Eve needs to know the efficiency of the four detectors as a function of Bob's input illumination angle. Hence, our first step was to scan Bob's receiver for possible efficiency mismatch. Eve's source consists of a fiber-coupled 532 nm laser, attenuator A, polarization controller PC, and a collimating lens L4 mounted on a two-axis motorised translation stage. In Fig. 1a, green marginal rays denote the initial alignment from Eve, replicating the alignment from Alice to Bob. As we moved the stage in the transversal plane, it allows changing the beam's incidence angle and lateral displacement at Bob's front lens L1 simultaneously. This is shown by the red marginal rays in Fig. 1, representing a beam from Eve coming at an angle (ϕ, θ) relative to the reference beam.

At first, we did a preliminary scan using optical power meters that revealed several features which should be causes of efficiency mismatch, highlighted in Fig. 1(b). Around $\phi = \theta = 0$, maximum light coupling resulted in the central peak ❶. With increasing scanning angle, the focused beam started missing the fiber core, and the detector count dropped off ❷. A region was found when the beam reflected off the polished edge of PBS2 back into the fiber core, causing the peak ❸. Increasing the angle further made the beam hit the anodized aluminum mount of L1 and possibly edges of other lens mounts and round elements in the optical assembly. It was scattered at these edges, producing two ring-like features ❹. Beyond these features, there were no noticeable power readings, as the beam completely missed the receiver aperture.

We then adjusted the receiver setup to minimize peak ❸, and performed final scans at 26.1 m distance using Bob's single-photon detectors. Before scanning, the optics in Bob's apparatus was aligned to maximize coupling into all four detectors at normal incidence, which is the standard alignment procedure for QKD. We then started the scanning procedure that involved first, changing the outgoing beam's angle $\{\phi, \theta\}$, and then recording the corresponding count rate at all four detectors of Bob. Then during post-processing, for each data point for each detector, we subtracted the corresponding detector's background count rate, and then normalized it by dividing by the maximum count rate in that detector. The result is shown in Fig. 2.

Attack model. We numerically model and optimize a practical faked-state attack, using our experimental data and the following assumptions. Alice and Bob perform

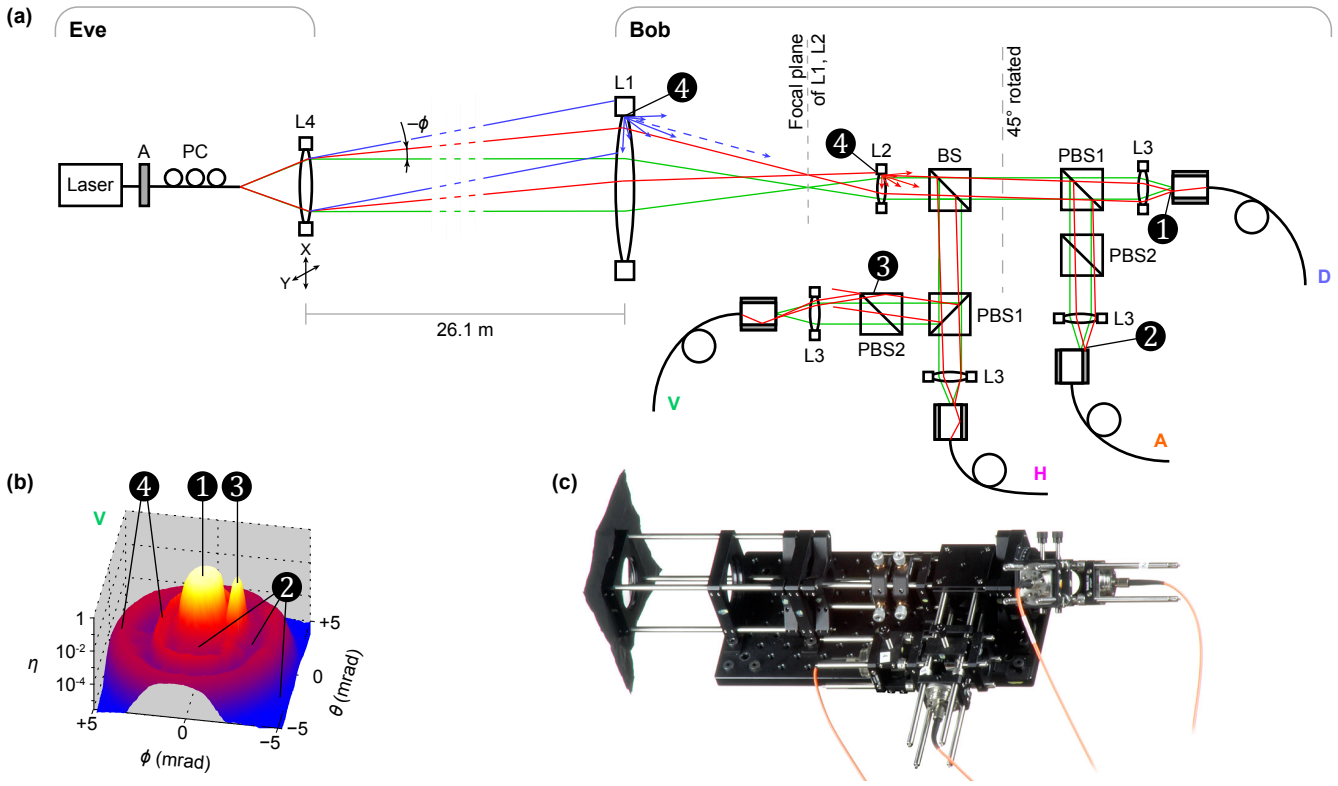

FIG. 1. Experimental setup. (a) Scheme of the experimental apparatus, top view (drawing not to scale). Eve's source consists of a fiber-coupled 532 nm laser, attenuator A, polarization controller PC, and a collimating lens mounted on a two-axis motorised translation stage. The latter allows changing the beam's incidence angle and lateral displacement at Bob's front lens L1 simultaneously. Green marginal rays denote the original alignment of Alice's beam to Bob. Red and blue marginal rays show a scanning beam from Eve tilted at an angle (ϕ, θ) relative to the original beam. Features ❶–❹ mark different transmission paths for light inside Bob. (b) Normalized detection efficiency η in channel V versus the illumination angle (ϕ, θ). This scan was taken to show the features clearly by placing Eve at a closer distance. (c) Photograph of Bob's receiver.

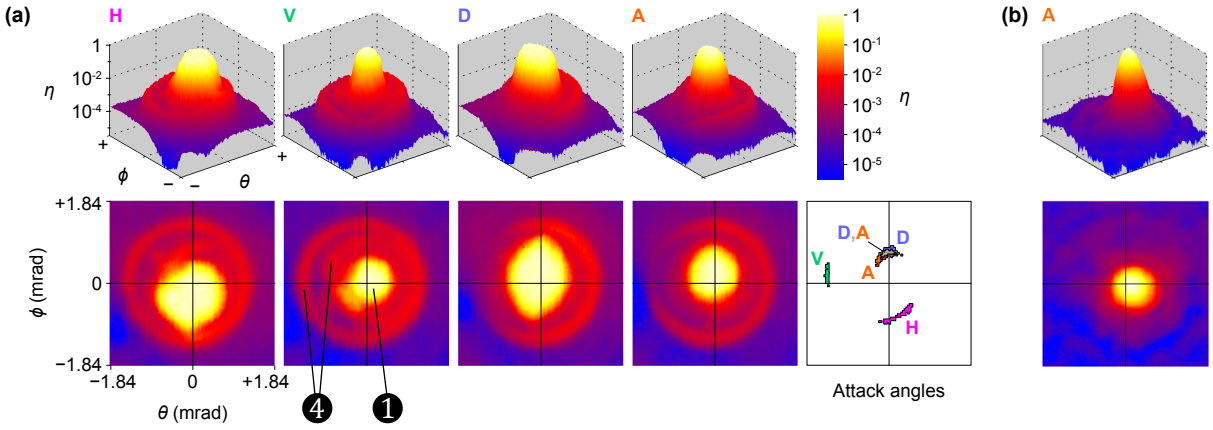

FIG. 2. Angular efficiency scan of the receiver, and points of interest. (a) Four pair of plots **H, V, D, A** shown in both 3D and 2D represent normalized detection efficiency in the four receiver channels versus illuminating beam angle (ϕ, θ). The angle $\phi = \theta = 0$ is the initial angle of QKD operation. The last plot shows angle ranges with a high mismatch, usable in our attack. (b) An example of scanning result in polarization channel **A** with 25 µm diameter pinhole at the focal plane of L1. The plots for the other three receiver channels in this case were very similar; all features that caused the efficiency mismatch disappeared.

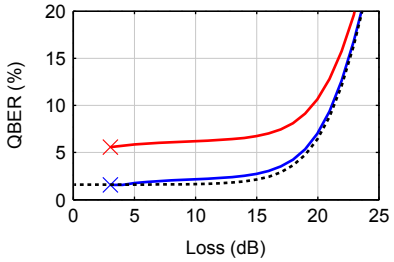

FIG. 3. Modeled QBER observed by Bob versus line loss. The dotted curve shows QBER without Eve. At lower line loss, the QBER is due to imperfect fidelity, while at higher line loss Bob's detector background counts become the dominant contribution. The lower solid curve (blue) shows QBER_e under our attack when only the total Bob's sifted key rate R_e is matched. The upper solid curve (red) additionally keeps his four channel rates equal.

non-decoy-state Bennett-Brassard 1984 (BB84) protocol using polarization encoding. Eve intercepts and measures every signals from Alice using an active basis choice receiver with high-efficiency single-photon detectors. For each successful detection, Eve sends to Bob a faked-state signal which is a weak coherent pulse with polarization matching her measurement result. For each of the four polarizations, she sends at a specific angle and mean photon number. Our next task is to find these parameters, with the goal of Eve to maintain Bob's detection rate and minimize QBER.

Our experimental attack angles are shown in the rightmost plot in Fig. 2(a). For example, the H attack angles were composed of points for which the probability of detection in H channel was 75 times more than the other two non-orthogonal channels (D and A), and the normalized detection probability was at least 0.25. The thresholds used here to find the attack angles were not optimal, and were picked manually. With this information, the detection rate and QBER of Bob can be calculated. From these data, we then ran an optimization program to find optimal mean photon numbers for each attack angle. This optimization was conditioned to minimize QBER and match the total detection rate expected by Alice and Bob (calculated from the parameters at the reference angle).

Our optimization shows that it is possible for Eve to pick appropriate mean photon numbers and successfully attack the system for Alice–Bob channel loss ≥ 3 dB if they are willing to accept a slight increase of QBER by less than 0.7% (see Fig. 3), if Alice and Bob monitor only the total key rate. Furthermore, the attack is still successful at QBER $< 6.82\%$ in 3–15 dB line loss range even when Alice and Bob monitor the equality of detection rates in each channel. Similar QBER values are typical for outdoor channels, because of background light. Eve could shield Bob from the latter to hide QBER resulting from her attack.

Countermeasure. In our attack, Eve has broken a fundamental assumption of security proofs: detection probabilities are independent of detection basis. We propose to restore this assumption by placing a spatial filter (pinhole) at the focal plane of Bob's L1 and L2 [Fig. 1(a)]. We have tested several pinhole sizes, and found that 25 μm diameter pinhole eliminates any visible mismatch as shown in Fig. 2(b). Hence, we conclude that a 25 μm pinhole may be an efficient countermeasure for the current setup.

Discussion and conclusion. Since our analysis implies that data obtained during a QKD session can be explained by an intercept-resend attack exploiting the spatial mode side-channels, there is no postprocessing or privacy amplification that can eliminate Eve's knowledge without sacrificing all key [5]. Although our practical attack should work, and the physical countermeasure seems promising, there is still room for improvement on both the attack scheme and countermeasures. The effect of atmospheric turbulence on both scanning and signal transmission needs to be studied. The resilience of pinhole against laser damage needs to be tested. At last, all these tests need to be performed again on the compact receiver with integrate optics that is going to be installed in the satellite.

Our study summarised here [1] is an excellent example of deviation in device's behavior that is not predicted in theory but affects the security of the protocol. The practical results of this study are applicable to most free-space quantum communication systems. We hope that this work will emphasise the necessity of investigating physical side-channels in every implementation of QKD. Iterations of finding vulnerabilities and testing countermeasures should eventually guarantee the high level of security promised by the theory of QKD.

[1] S. Sajeed, P. Chaiwongkhot, J.-P. Bourgoin, T. Jennewein, N. Lütkenhaus, and V. Makarov, arXiv:1502.02785 [quant-ph].
[2] C.-H. F. Fung, K. Tamaki, B. Qi, H.-K. Lo, and X. Ma, Quant. Inf. Comp. **9**, 131 (2009).
[3] M. Rau, T. Vogl, G. Corrielli, G. Vest, L. Fuchs, S. Nauerth, and H. Weinfurter, IEEE J. Quantum. Electron. **21**, 6600905 (2015).
[4] J.-P. Bourgoin, N. Gigov, B. L. Higgins, Z. Yan, E. Meyer-Scott, A. Khandani, N. Lütkenhaus, and T. Jennewein, (manuscript in preparation).
[5] M. Curty, M. Lewenstein, and N. Lütkenhaus, Phys. Rev. Lett. **92**, 217903 (2004).