A generalized efficiency mismatch attack to bypass detection-scrambling countermeasure

M A Ruhul Fatin[1,2] and Shihan Sajeed[3,4,5]

[1]Department of Electrical and Electronic Engineering, Bangladesh Univ. of Engineering and Technology, Dhaka, Bangladesh
[2]Carleton University, Ottawa, ON, K1S 5B6, Canada
[3] Institute of Quantum Computing, University of Waterloo, ON, N2L 3G1 Canada
[4]Department of Physics and Astronomy, University of Waterloo, ON, N2L 3G1 Canada
[5]Department of Electrical and Computer Engineering, University of Toronto, M5S 3G4, Canada

Introduction

- In theory, an ideal QKD system can guarantee unconditional security. However, in practice, imperfections in the receiver setup of quantum cryptography systems may allow an eavesdropper to use it as a control parameter to attack the system.
- Mismatch of sensitivity in the receiver's photodetectors is one of the imperfections that can potentially be exploited by an eavesdropper.
- Published researches have shown that scrambling the role of the photodetectors in the receiver can be one of the countermeasure strategies to protect the system.
- In spatial-mode-efficiency-mismatch [1] type attacks an eavesdropper can compromise the security of the system by changing the angle of the incoming light.
- In Ref. [2], a countermeasure to this type of attacks was proposed but it is not clear how effective the countermeasure is when one considers that detectors operate on optical modes rather than on single-photon signals.

Objectives

- Investigate the effectiveness of proposed detector scrambling countermeasure against spatial-mode-efficiency mismatch type attacks.
- Explore an attack strategy that can bypass the detector scrambling countermeasure.

Method

- Using experimental results from existing publications, it is shown that detector randomization effectively prevents the initial attack but fails to do so when Eve generalizes her attack strategy. Figure 1 shows the simulated QBER vs line loss with the bypass strategy.
- The generalized attack strategy brings new free parameters into the optimization which Eve could adjust to her advantage. Figure 2 shows the scatter plot of the probabilities and mean photon number per pulse that are optimized to formulate the bypass attack.
- For a certain channel loss, Eve must follow a specific blueprint to attack the system. For different channel loss the value of the optimized free parameters will be different.

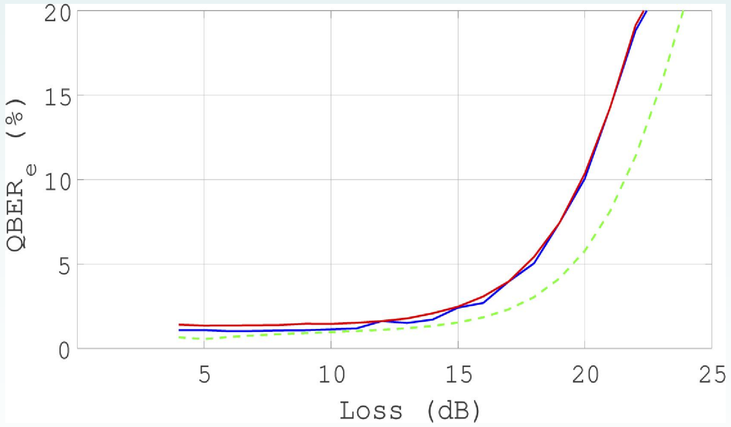

Figure 1: QBER versus line loss with Eve's improved attack. The dotted green curve shows QBER without EVE. The blue and red curves indicate QBER when Bob matches the Alice-Bob key rate with total sifted key rate and individual channel rates respectively. If Alice and Bob are willing to accept a slight increase of QBER by less than 1%, 2% and 5%, Eve can manipulate the mean photon numbers to attack the system for a line loss upto 16 dB, 17 dB and 20 dB respectively.

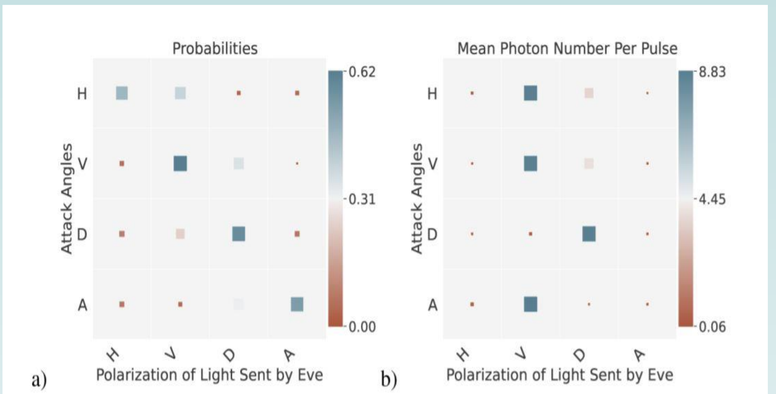

Figure 2: a) Scatter plot of optimized probabilities and b) mean photon number per pulse chosen by Eve for a channel loss of 6 dB respectively.

Results and Conclusion

- This work [3] shows that randomizing the roles of the detectors cannot function as an efficient countermeasure against detector-efficiency-mismatch type attacks.
- The general strategy works even when Bob uses any non-uniform a priori scrambling probabilities.
- The result and methodology can be used to scrutinize a free-space quantum communication receiver against detector-efficiency-mismatch type attacks

References

[1] S. Sajeed, P. Chaiwongkhot, J.-P. Bourgoin, T. Jennewein, N. Lutkenhaus, and V. Makarov, Phys. Rev. A 91, 062301 (2015).
[2] T. F. da Silva, G. C. do Amaral, G. B. Xavier, G. P. Temporao, and J. P. von der Weid, IEEE Journal of Selected Topics in Quantum Electronics 21, 159 (2014).
[3] M. A. R. Fatin and S. Sajeed, Opt. Express 29, 16073 (2021).