Improving performance of decoy-state free-space QKD using information on fluctuating transmittance in turbulent channel

Wenyuan Wang,[1] Feihu Xu,[2] and Hoi-Kwong Lo[1]

[1]*Centre for Quantum Information and Quantum Control (CQIQC), Dept. of Electrical & Computer Engineering and Dept. of Physics, University of Toronto, Toronto, Ontario, M5S 3G4, Canada*

[2]*Research Laboratory of Electronics, Massachusetts Institute of Technology, 77 Massachusetts Avenue, Cambridge, Massachusetts 02139, USA*

Quantum key distribution (QKD) allows two parties to share a random secret key with unconditional security. There has been increasing interest in implementing QKD through free-space channels, and over the past decade multiple demonstrations for free-space QKD have been made, such as [1–4], through ground-ground and even ground-satellite channels. A major characteristic of a free-space channel is its time-dependent transmittance fluctuations due to *atmospheric turbulence*. This fluctuation can be modeled as a probability distribution of transmission coefficient (PDTC) $p(\eta)$, a function of the transmittance η (the level of turbulence is characterized by the *scintillation index*, σ, as a parameter of the PDTC)

In previous literature discussing free-space QKD, such as [1, 2], the time variance of the channel is ignored, i.e. the secure key rate is calculated based on the time-average of channel transmittance η_0 only. Having knowledge of the PDTC, however, Vallone *et al.* proposed a method named adaptive real-time selection (ARTS) [5] that acquires information about real-time transmittance fluctuation due to turbulence, and makes use of this information to perform post-selection and improve the key rate. The proposed method is to use a classical probe signal (a strong laser beam) alongside the quantum channel. Bob can gain information of the periods of high transmittance by observing the classical signal. Combined with a threshold, he can post-select only those signals received during high transmittance periods, thus increasing the average transmittance and the secure key rate among post-selected signals. However, as one increases the threshold, the number of signals also decreases. Therefore, an optimization of post-selection threshold is necessary in order to acquire the maximal key rate. This approach can significantly increase the secure key rate under high turbulence and high loss.

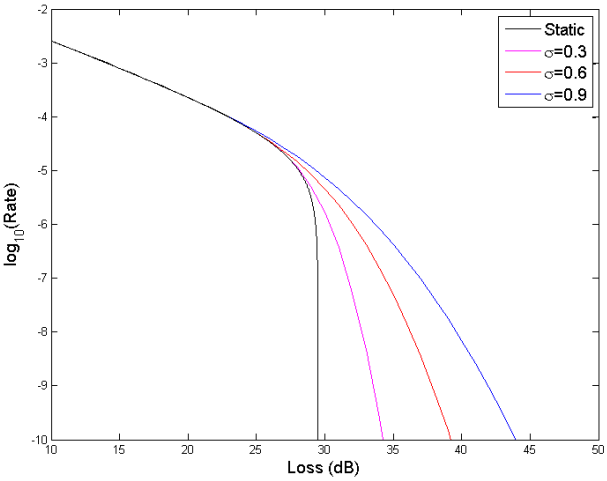

FIG. 1: Comparison of ARTS vs non-ARTS decoy-state BB84 under different levels of turbulence, using $\sigma = 0.3, 0.6, 0.9$ (0.3 for weak turbulence, while 0.9 for relatively strong turbulence) Rate is calculated using experimental parameters from [2]. Here we have already chosen an optimal threshold. We see that the improvement in rate from using ARTS increases with the level of turbulence, and has a significant improvement over static model for high-loss region. For $\sigma = 0.9$, for the same loss=29dB, with ARTS we can achieve as much as 278% increase over the case without ARTS. Also, for a minimum rate of $R = 10^{-7}$, with ARTS we can support a 7.5dB increase in maximum tolerated loss.

In our work, we generalize the proposal of ARTS method, which was only discussed for single-photon case, to practical decoy-state BB84 [6–8] protocol with WCP source. We follow the decoy state setup in [7], and use secure key rate given by GLLP formula [9]. We notice that when all experimental parameters are fixed (including signal intensities, detector dark count rate, detector efficiency and optical misalignment), the rate can be expressed by $R(\eta)$, a function of the transmittance η. When estimating the performance of post-selection with ARTS, a threshold η_T is applied for η of the signals, and we calculate the average transmittance among post-selected signals. We use this

new transmittance to estimate the rate, while combining it with the loss of signals due to post-selection.

Moreover, we showed that the upper bound of the key rate that makes use of all PDTC information can be expressed with the expected value (integral) of $R(\eta)$ with respect to the PDTC, $\langle R(\eta)\rangle$, and that the performance of ARTS can acheive this upper bound with an optimized threshold, i.e., the upper bound is tight. Meanwhile, the actual amount of maximal improvement we can have depends on the PDTC - the stronger the turbulence, the more rate improvement we can gain from using ARTS.

We performed computer simulations for decoy-state BB84 in a turbulent channel, and estimate the improvements from using ARTS. We use the experimental parameters from Ref. [2]. Using the optimized threshold, we generate the rate vs loss for different levels of turbulence, as shown in Fig.1. We see that ARTS provides drastic improvements in high-loss region, and that the stronger the turbulence is, the larger performance gain we have.

[1] RJ Hughes et al. New Journal of Physics, Vol. 4 (2002)

[2] Schmitt-Manderbach, Tobias, et al. Physical Review Letters 98.1 (2007): 010504.

[3] Capraro, Ivan, et al. Physical review letters 109.20 (2012): 200502.

[4] Liao, Sheng-Kai, et al. arXiv preprint arXiv:1707.00542 (2017).

[5] G Vallone et al. Phys. Rev. A 91, 042320 (2015)

[6] Hwang, Won-Young. Physical Review Letters 91.5 (2003): 057901.

[7] Lo, Hoi-Kwong, Xiongfeng Ma, and Kai Chen. Physical review letters 94.23 (2005): 230504.

[8] Wang, X.-B. Physical review letters 94.23 (2005): 230503.

[9] Gottesman, Daniel, et al. Information Theory, 2004. ISIT 2004. Proceedings. International Symposium on. IEEE, 2004.