Comment on "Performance improvement of continuous-variable quantum key distribution via photon subtraction"

Kyongchun Lim, Changho Suh and June-Koo Kevin Rhee*
School of Electrical Engineering, KAIST, Republic of Korea

(Dated: May 16, 2018)

Huang *et al.* proposed a continuous variable quantum key distribution (CVQKD) protocol with photon subtraction at a transmitter, where the proposed protocol is asserted to enhance the transmission distance of secure keys. However, the result in the paper was evaluated under less fair conditions in terms of modulation variance, which misled the conclusion of the paper. This comment pints out that the result in the paper needs to be reevaluated for a broad range of modulation variance. We also argue a comment of the authors that photon subtraction at transmitter not only improve entanglement degree in terms of logarithmic negativity, but also performance of CVQKD. Based on the reevaluated result, we report that even if a large entanglement degree may improve correlation between key information, it does not necessarily guarantee improvement of security.

The authors in [1] proposed a continuous variable quantum key distribution (CVQKD) protocol with a non-Gaussian state made by photon subtraction at a transmit side. Through numerical analyses, they also showed the proposed protocol outperforms a conventional CVQKD protocol in terms of transmission distance because photon subtraction improves entanglement degree. However, we argue that the conclusion of the paper should be reconsidered because the investigation for secure key rate with respect to distance was incomplete, lacking investigation of secure key rate under optimal modulation variance.

The main result shown in Fig. 3 of [1] shows secure key rates with respect to distance, where the proposed protocol outperforms the conventional scheme under all simulated excess noises. Here, we point out modulation variance. In the evaluation, the authors in [1] apply the same modulation variances on the proposed and conventional schemes. However, modulation variance can be freely controlled by a system designer, and thus modulation variance can be optimized for distance. Therefore, it is natural that the performance comparison is conducted with optimized modulation variance.

In order to prove misunderstanding introduced by the result data in Fig. 3 of [1], as a counter example, we simulate the same simulation as in [1] with different modulation variances. Under the same simulation parameters, only modulation variance changes to 5 for the conventional and the proposed schemes. The corresponding result is shown in Fig. 1, where the proposed scheme shows lower performance than that of the conventional scheme under all simulated excess noises. This result requires a reevaluation of the performance comparison in Fig. 3 of the original paper.

For fairer comparison, we perform the simulation with the optimized modulation parameters in terms of distance. The corresponding result is shown in Fig. 2. For excess noises 0.01, 0.02, 0.03, and 0.05, optimal modulation variances of the conventional scheme are found to be 2.2, 2.2, 2.2, and 2.3. In case of the proposed scheme, there are two control parameters which are modulation variance and μ of a beam splitter for photon subtraction. These parameters (V_A, μ) are optimized to (3.7, 0.6), (3.6, 0.6), (5, 0.6), and (7.5, 0.7) for excess noises 0.01, 0.02, 0.03, and 0.05. From the result, we find that the proposed scheme cannot beat the performance of the conventional scheme. This contradicts the argument that increase of entanglement degree affects improvement of security of CVQKD as in [1].

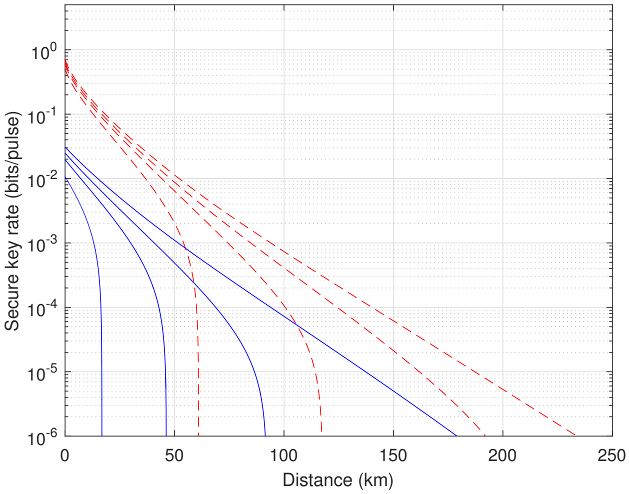

Figure 1. Asymptotic secret key rate $\widetilde{K}_N$ of the EB scheme with photon subtraction with modulation variance as 5 (solid curves), and K_G of the conventional scheme with modulation variance as 5(dotted curves) as a function of distance for different values of the excess noise ϵ. From top to bottom, $\epsilon = 0.01$, 0.02, 0.03, and 0.05, respectively.

In this comment, we point out need for optimal system comparisons to avoid misleading of the conclusion in [1]. The paper conducts the performance comparison under the same modulation variances for the conventional and the proposed scheme. However, modulation vari-

* Email: rhee.jk@kaist.ac.kr

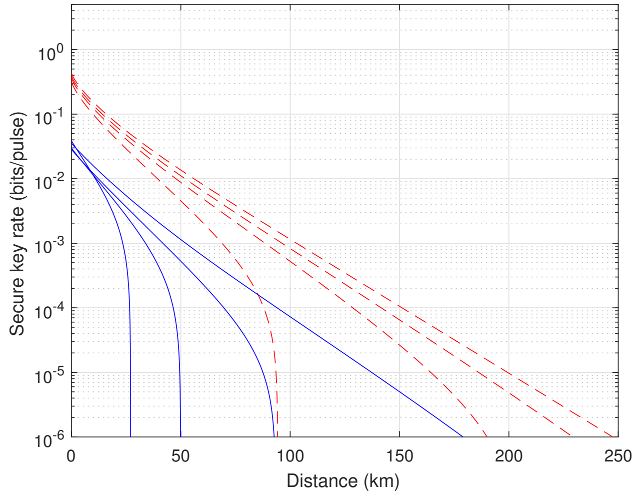

Figure 2. Asymptotic secret key rate $\widetilde{K}_N$ of the EB scheme with photon subtraction with optimized parameters (solid curves), and K_G of the conventional scheme with optimized modulation variance (dotted curves) as a function of distance for different values of the excess noise ϵ. From top to bottom, $\epsilon = 0.01$, 0.02, 0.03, and 0.05, respectively.

ance should be optimized because it is a system control parameter. We reevaluate the performance comparison and find that the conventional scheme outperforms the proposed scheme. This requires a complete reconsideration of the concluding analysis of the proposed scheme. Furthermore, the modified result provides different opinion against that of the original paper, which even if a large entanglement degree improve correlation between key information, it does not necessarily guarantee improvement of security. This implies that we also consider Eve's information caused by an additional operation instead of considering just information of Alice and Bob when we consider security.

This work was supported by the ICT R&D program of MSIP/IITP [1711057505, Reliable crypto-system standards and core technology development for secure quantum key distribution network].

[1] P. Huang, G. He, J. Fang, and G. Zeng, Phys. Rev. A **87**, 012317 (2013).