Continuous variable quantum key distribution protocol with photon subtraction at receiver

Kyongchun Lim, Changho Suh, and June-Koo Kevin Rhee
School of Electrical Engineering, KAIST, Daejeon, South Korea
{lim.kc, chsuh, rhee.jk}@kaist.ac.kr

Abstract

Continuous variable quantum key distribution (CVQKD) has attracted interests of researchers since it is known that a CVQKD protocol outperforms a discrete quantum key distribution (DVQKD) in terms of the secure key rate. In this work, we develop a novel CVQKD scheme that introduces photon subtraction operation, thus yielding a better performance compared to the state of the art. In particular, we demonstrate through numerical analyses that the proposed protocol supports a longer transmission distance of secure keys.

I. Introduction

The importance of personal privacy drives the need for secure communication. Quantum key distribution (QKD) has received considerable attention due to its unconditional security [1]. QKD protocols are categorized into two parts depending on the type of the distribution of quantum keys: (1) discrete variable QKD (DVQKD); (2) continuous variable QKD (CVQKD). CVQKD has received more attention as it is shown to outperform an existing DVQKD protocol [2].

In this paper, we propose a CVQKD protocol utilizing photon subtraction to ensure a longer transmission distance. The key feature of our protocol is to perform photon subtraction at a receiving end. We find that the photon subtraction operation plays a role to remove photons induced by an eavesdropper, thus yielding a higher performance. We also evaluate the performance of the proposed protocol with simulation results and demonstrate that our proposed protocol outperforms a conventional CVQKD protocol.

We expect that the photon subtraction in a receiver partially removes photons added by an eavesdropper. We also evaluate performance of the proposed protocol with results of numerical analyses and verify our proposed protocol outperforms a conventional CVQKD protocol.

II. General CVQKD

We first review a conventional CVQKD protocol. A general CVQKD protocol utilizes p and q quadratures to express continuous variables. In the protocol, a transmitter (Alice) generates a two-mode squeezed vacuum (TMSV) state. Here, p and q quadratures of a TMSV state have the same variance $V = V_A + 1$ in shot noise unit where V_A is a variance of Alice's Gaussian modulation. One half of the TMSV state is captured in a quantum memory. The other half of the TMSV state is transmitted to a receiver (Bob) through a quantum channel characterized by transmittance T and noise variance V_N. Then, Bob performs homodyne detection with respect to p or q quadrature and announces his choices of quadratures to Alice through a public channel. After the announcement, Alice performs homodyne detection with respect to the announced quadratures on the half of the TMSV captured in a quantum memory. This leads Alice and Bob to share Gaussian correlated data. The data become final secure key after post processing consisting of error correction and privacy amplification.

III. CVQKD with photon subtraction in a receiver

Our proposed model has an additional beam splitter having transmittance T_1 and a photon resolving detector in Bob for photon subtraction as shown in Fig. 1. The model generates single photon subtracted quantum states by collecting states corresponding to single photon detection of the photon resolving detector. In order to analyze security of the model, we first consider a quantum state generated by the proposed model.

At first, a TMSV state $|\psi\rangle_{AB}$ prepared by Alice can be represented as follows:

$$|\psi\rangle_{AB_0} = \sum_{n=0}^{\infty} \alpha_n |n, n\rangle_{AB_0}, \tag{1}$$

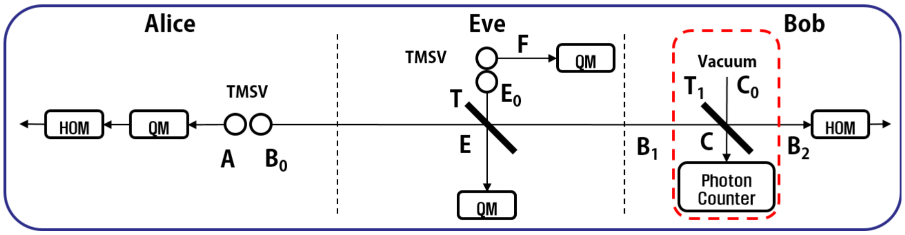

Figure 1: Model for CVQKD with photon subtraction in Bob. HOM and QM stand for homodyne detection and quantum memory, respectively.

where $\alpha_n = \sqrt{\frac{\alpha^{2n}}{(1+\alpha^2)^{n+1}}}$ and α^2 denotes the mean photon number of the TMSV state. In a similar way, a channel characterized by an Eve's TMSV state having mean photon number β^2 can be expressed as follows:

$$|\psi\rangle_{E_0F} = \sum_{m=0}^{\infty} \beta_m \, |m,m\rangle_{E_0F} \, , \tag{2}$$

where $\beta_m = \sqrt{\frac{\beta^{2m}}{(1+\beta^2)^{m+1}}}$. Then, a quantum state after a channel having transmittance T can be represented as follows:

$$|\psi\rangle_{AB_1EFC} = \sum_{n=0}^{\infty} \alpha_n \sum_{k=1}^{n} (-1)^k \gamma_{n,k} \sum_{m=0}^{\infty} \beta_m \sum_{l=0}^{m} \gamma_{m,l} \sum_{s=0}^{n-k+l} (-1)^s \epsilon_{n-k+l,s} K \, |n, n-k+l, k+m-l, m, s\rangle_{AB_1EFC} \tag{3}$$

where $\gamma_{i,j} = \sqrt{\binom{i}{j} T^{i-j} (1-T)^j}$, $\epsilon_{i,j} = \sqrt{\binom{i}{j} T_1^{i-j} (1-T_1)^j}$, and $K = \sqrt{\binom{n-k+l}{l}} \sqrt{\binom{k+m-l}{k}}$. Applying single photon subtraction on the quantum state represented as in Eq. (3),

$$|\psi_1\rangle_{AB_2EFC} = -\frac{1}{P_1} \sum_{n=0}^{\infty} \alpha_n \sum_{k=1}^{n} (-1)^k \gamma_{n,k} \sum_{m=0}^{\infty} \beta_m \sum_{l=0}^{m} \gamma_{m,l} \sum_{s=0}^{n-k+l} \epsilon_{n-k+l,1} K \, |n, n-k+l, k+m-l, m, 1\rangle_{AB_2EFC} \tag{4}$$

where

$$P_1 = \sum_{n=0}^{\infty} \alpha_n^2 \sum_{m=0}^{\infty} \beta_m^2 \sum_{k=0}^{n} \sum_{l=0}^{m} K \left(\sum_{j=0}^{\min\{n-k,m-l\}} (-1)^j \gamma_{n,k} \gamma_{n,k+j} \gamma_{m,l} \gamma_{m,l+j} K_+ + \sum_{j=1}^{\min\{k,l\}} (-1)^j \gamma_{n,k} \gamma_{n,k-j} \gamma_{m,l} \gamma_{m,l-j} K_- \right), \tag{5}$$

and $K_\pm = \sqrt{\binom{n-k+l}{l \pm j}} \sqrt{\binom{k+m-l}{k \pm j}}$.

Based on the quantum state represented in Eq. (4), we can build a covariance matrix $\mathbf{V}_{AB}$ and $\mathbf{V}_{EFB}$ by using a method in [3] (due to the page limit, we omit explicit expression), which is used to calculate secure key rate K_S of the proposed model as follows:

$$K_S = P_1 \left(f I_{AB} - \chi_{BE} \right), \tag{6}$$

where f, I_{AB}, and χ_{BE} are the efficiency of error correction, mutual information between Alice and Bob, and quantum mutual information between Bob and Eve. However, since the quantum state in Eq. (4) is a non-Gaussian state, it is not tractable to calculate Eq. (6). For the purpose of a tractable calculation, here we utilize the Gaussian optimality theorem [4]. Specifically we assume that a Gaussian state is generated by the model having the same covariance matrix of the quantum state in Eq. (4). This then yields a lower bound of secure key rate obtained by the proposed model. This can be done by changing the photon subtraction operation to a certain Gaussian operation providing the same covariance matrix of the quantum state in Eq. (4). This makes the calculation of the mutual information in Eq. (6) tractable.

For the computation of I_{AB}, we calculate $V_A = \langle\psi_1|\hat{q}_A^2|\psi_1\rangle$, $V_B = \langle\psi_1|\hat{q}_{B_2}^2|\psi_1\rangle$, and $C_{AB} = \frac{1}{2}\langle\psi_1|\hat{q}_A\hat{q}_{B_2} + \hat{q}_{B_2}\hat{q}_A|\psi_1\rangle$ representing the variance of Alice's data obtained by measuring a quantum state A, the variance of Bob's data

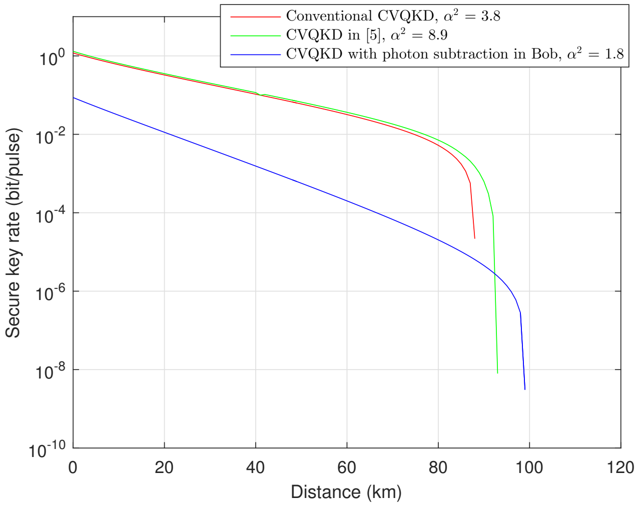

Figure 2: Comparisons for secure key rate of CVQKD protocols.

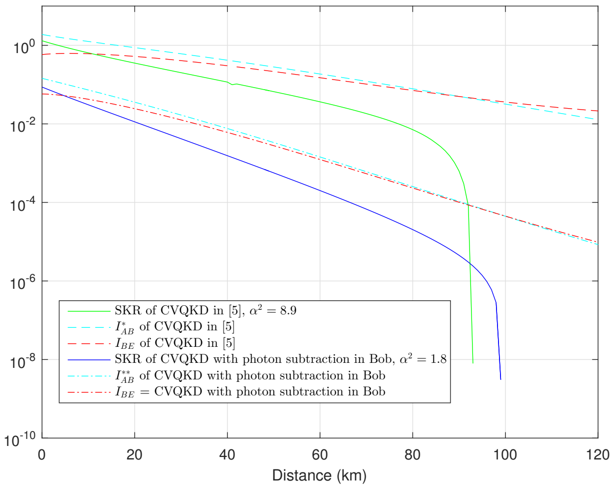

Figure 3: Comparisons for mutual information of CVQKD protocols. SKR stands for secure key rate. $I^*_{AB} = fI_{AB}$ and $I^{**}_{AB} = P_1 f I_{AB}$

obtained by measuring a quantum state B, and the correlation between Alice and Bob, respectively. With the variances, we can calculate I_{AB} as follows:

$$I_{AB} = \frac{1}{2}\log_2 \frac{V_A}{V_{A|B}}, \tag{7}$$

where $V_{A|B}$ is the conditional variance expressed as $V_{A|B} = V_A - C^2_{AB}/V_B$.

In case of χ_{BE}, we calculate it by applying a method in [5] on $\mathbf{V}_{EFB}$ (although we omit explicit expression due to the page limit, χ_{BE} can be calculated with $\mathbf{V}_{EFB}$).

IV. Numerical analysis results and conclusion

For simulations, we set error correction efficiency f, detector efficiency, and mean photon number of channel β as 0.95, 0.68, and 0.001, respectively. In addition, transmittance T_1 of the beam splitter in Bob set as 0.9. For performance comparison, we simulate secure key rates of a conventional CVQKD and a CVQKD proposed in [5]. The corresponding result is plotted in Fig. 2 where mean photon number of Alice for each protocol is optimized. From the result, we find that our proposed model can transmit secure keys at a longer distance. Fig. 3 shows I_{AB} and χ_{BE} with respect to distance. At around 100km, even if I_{AB} of the proposed model becomes lower than that of [5], χ_{BE} of the proposed model becomes much lower than that of [5]. This yields a longer secure key transmission.

Acknowledgment

This work was supported by the ICT R&D program of MSIP/IITP. [1711028311, Reliable crypto-system standards and core technology development for secure quantum key distribution network] and the MSIP(Ministry of Science, ICT and Future Planning), Korea, under the ITRC(Information Technology Research Center) support program (IITP-2017-2015-0-00385) supervised by the IITP(Institute for Information & communications Technology Promotion)".

References

[1] H.-K. Lo and H. F. Chau, "Unconditional security of quantum key distribution over arbitrarily long distances," *science*, vol. 283, no. 5410, pp. 2050–2056, 1999.

[2] S. Pirandola, R. Laurenza, C. Ottaviani, and L. Banchi, "Fundamental limits of repeaterless quantum communications," *Nature Communications*, vol. 8, 2017.

[3] C. Weedbrook, S. Pirandola, R. García-Patrón, N. J. Cerf, T. C. Ralph, J. H. Shapiro, and S. Lloyd, "Gaussian quantum information," *Reviews of Modern Physics*, vol. 84, no. 2, p. 621, 2012.

[4] R. García-Patrón and N. J. Cerf, "Unconditional optimality of gaussian attacks against continuous-variable quantum key distribution," *Phys. Rev. Lett.*, vol. 97, p. 190503, Nov 2006. [Online]. Available: https://link.aps.org/doi/10.1103/PhysRevLett.97.190503

[5] C. Ottaviani, R. Laurenza, T. P. Cope, G. Spedalieri, S. L. Braunstein, and S. Pirandola, "Secret key capacity of the thermal-loss channel: Improving the lower bound," in *SPIE Security+ Defence*. International Society for Optics and Photonics, 2016, pp. 999 609–999 609.