Superadditivity of a reverse private capacity in quantum channels

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

Unconditionally secure information sharing of private information against an eavesdropper can be achieved with a quantum key distribution (QKD) protocol. A theoretical bound on a secure key rate of a QKD protocol is known to be realized by a reverse private capacity such as with a reverse reconciliation. We show theoretically that a reverse private capacity has a property of superadditivity, with an example consisting of two quantum channels which are a pure loss channel and an 100% erasure channel. This implies that a tighter bound for a secure key rate exists than the previously known bound based on analysis of a reverse private capacity in a single channel.

I. Introduction

Private communication has become important as personal information is immensely shared over the Internet. Quantum key distribution (QKD) is suitable for private secure communication because it guarantees unconditional security by its physical properties such as no cloning theorem [1].

An objective of QKD is to make two remote parties share a random bit sequence which is not uncovered to an eavesdropper in a probabilistic manner. Then, one can have a fundamental question: what is the maximum generation rate for the shared random bit sequence called as a secure key. Researches to find an answer to the question has been conducted [2]–[4]. The corresponding results provide upper and lower bounds for the maximum secure key rate. The upper and lower bounds are based on quantum relative entropy [4] and a reverse private capacity [2], respectively. In case of the lower bound, the authors in [2] reveled that there exists possibility of a tighter lower bound since the proposed lower bound does not utilize a property of a reverse private capacity. That is, a property of a reverse private capacity should be carefully investigated to find a tighter lower bound.

A reverse private capacity is defined as the maximum secure key rate generated by a QKD protocol with reverse reconciliation through a quantum channel [2]. As aforementioned, the proposed lower bound does not utilize a property of a reverse private capacity which is superadditivity due to lack of its proof. Superadditivity means that a secure key capacity where quantum channels are independently used is less than the capacity where quantum channels are used together. This implies an existence of a tighter lower bound because the proposed lower bound is based on a single channel capacity. In this paper, we show a reverse private capacity has superadditivity by showing a counter example. In that case, two quantum channels are modeled as a pure loss channel and a 100% erasure channel.

This paper will be organized as follows. First, we explain a reverse private capacity with a simple system diagram in Section II. In Section III, we then provide a detailed procedure for proof about superadditivity of a reverse private capacity. We finally conclude our presentation as in Section IV.

II. Reverse private capacity

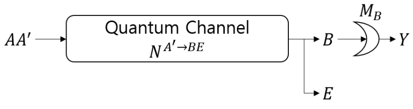

Figure 1: QKD for reverse reconciliation.

By [2], a reverse private capacity, $P_R(N)$, means the maximum secure key rate achieved by a QKD with reverse reconciliation. $P_R(N)$ is expressed as follows:

$$P_R(N^{A'\to BE}) = \lim_{n\to\infty} \frac{1}{n} P_R^{(1)}((N^{A'\to BE})^{\otimes n}), \tag{1}$$

where

$$P_R^{(1)}(N^{A'\to BE}) = \max_{\rho^{AA'}, M_B} I(Y;A) - I(Y;E). \tag{2}$$

Here, $P_R^{(1)}(N)$ is defined as a reverse private capacity for a single channel use. $P_R^{(1)}(N)$ describes a capacity of the QKD with reverse reconciliation as shown in Fig.1. A transmitter, Alice, prepares a pure entangled quantum state AA' of two qubits

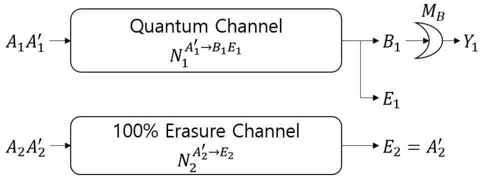

Figure 2: QKD for reverse reconciliation in two quantum channels which are a arbitrary quantum channel and an 100% erasure channel.

for which a density matrix is given $\rho^{AA'}$ provided by a purification of a quantum state A'. Then, she sends a quantum state A' with $\rho^{A'} = \mathrm{Tr}_A(\rho^{AA'})$ to a receiver, Bob, through a quantum channel $N^{A'\to BE}$ which is a completely positive and trace preserving (CPTP) map. During transmission, some of the transmitted quantum state can be absorbed by an environment, which is represented as a quantum state E with the corresponding density matrix ρ^E. Here, the absorbed quantum state by the environment is conservatively assumed to be leaked to an eavesdropper, Eve. Bob measures his received quantum state with positive operator valued measure (POVM), M_B. Then, he obtains a measurement result which is a classical state Y. Based on this, $P_R^{(1)}(N)$ is obtained from difference between quantum mutual information as in Eq.(2).

III. Superadditivity of a reverse private capacity

To show superadditivity, we use two quantum channels which are a pure loss channel and an 100% erasure channel. First, we show a theorem which is helpful to show superadditivity.

Theorem 1. *As shown in Fig.2, Alice prepares a quantum state $A_1A'_1A_2A'_2$ with $\rho^{A_1A'_1A_2A'_2}$ where quantum states $A_1A'_1$ and $A_2A'_2$ are pure entangled states. Then, she sends a quantum state $A'_1A'_2$ with $\rho^{A'_1A'_2} = Tr_{A_1A_2}(\rho^{A_1A'_1A_2A'_2})$ through an arbitrary quantum channel $N_1^{A'_1\to B_1E_1}$ and 100% erasure channel $N_2^{A'_2\to E_2}$. After transmission, Bob measures a quantum state B_1 with POVM M_B to obtain a classical state Y_1. In this case, the following relation is established.*

$$Q_R^{(1)}(N_1^{A'_1\to B_1E_1} \otimes N_2^{A'_2\to E_2}) \geq I(Y_1; A_1), \tag{3}$$

where

$$Q_R^{(1)}(N^{A'\to BE}) = H(A) - H(E). \tag{4}$$

Proof. Given a quantum state $A_1A'_1$ with $\rho^{A_1A'_1}$, by choosing a specific quantum state $A_2A'_2$ with $\rho^{A_2A'_2}$, consider a quantum state $A_1A'_1A_2A'_2$ with $\rho^{A_1A'_1A_2A'_2}$ which satisfies the following conditions.

$$A_1 \perp A_2, \tag{5}$$

$$H(A_2) \geq H(Y_1), \tag{6}$$

$$\rho^{A_1Y_1E_1A'_2} = |\psi^{A_1Y_1E_1A'_2}\rangle\langle\psi^{A_1Y_1E_1A'_2}|. \tag{7}$$

Eq.(5) means that we consider a quantum states A_2 which is independent to a quantum state A_1, i.e., $H(A_1|A_2) = H(A_1)$ where $H(\cdot)$ represents von Neumann entropy. Since Bob's POVM, M_B, is known to Alice, we can find a quantum state A_2 satisfying Eq.(6). To show existence of a quantum state satisfying Eq.(7), assume that a quantum state $A_1Y_1E_1$ with $\rho^{A_1Y_1E_1}$ is given, which can be obtained by a quantum channel, $N_1^{A'_1\to B_1E_1}$. Then, by purification, there exists a pure quantum state $A_1Y_1E_1A'_2$ with $\rho^{A_1Y_1E_1A'_2}$ purified by a quantum state A'_2. This provides that we can find the quantum state satisfying Eq.(7) by controlling a quantum state $A_2A'_2$.

With the aforementioned conditions, the following can be established.

$$\begin{aligned}
Q_R^{(1)}(N_1^{A'_1\to B_1E_1} \otimes N_2^{A'_2\to E_2}) &= \max_{\rho^{A_1A'_1A_2A'_2}} [H(A_1A_2) - H(E_1E_2)], && (8)\\
&\geq H(A_1A_2) - H(E_1E_2), && (9)\\
&= H(A_1A_2) - H(E_1A'_2), && (10)\\
&= H(A_1) + H(A_2) - H(E_1A'_2), && (11)\\
&\geq H(A_1) + H(Y_1) - H(E_1A'_2), && (12)\\
&= H(A_1) + H(Y_1) - H(Y_1A_1), && (13)\\
&= I(Y_1; A_1). && (14)
\end{aligned}$$

Eq.(8) comes from the definition of a reverse quantum capacity in [2]. Eq.(9) is caused by the fact that we consider the specific input quantum state having assumptions in Eqs.(5)-(7). By the 100% erasure channel, a quantum state E_2 is the same as a quantum state A'_2, which provides Eq.(10). Eqs.(11) and (12) are satisfied by Eqs.(5) and (6), respectively. In case of Eq.(13), by the Schumidt decomposition, we can easily check that $H(E_1A'_2) = H(Y_1A_1)$ if a quantum state $A_1Y_1E_1A'_2$ is pure. □

By the fact that a reverse private capacity is bounded by a reverse quantum capacity [2], the result of Theorem 1 provides the following.

$$P_R^{(1)}(N_1^{A_1'\to B_1E_1} \otimes N_2^{A_2'\to E_2}) \geq Q_R^{(1)}(N_1^{A_1'\to B_1E_1} \otimes N_2^{A_2'\to E_2}) \geq I(Y_1;A_1). \tag{15}$$

Next, consider an arbitrary quantum channel $N_1^{A_1'\to B_1E_1}$ in Eq.(15) as a pure loss channel with transmittance $0<\eta<1$. In this channel, a reverse private capacity can be achieved by using an input Gaussian state and a rank one measurement [4]. The corresponding reverse private capacity is as follows:

$$P_R^{(1)}(N_1^{A_1'\to B_1E_1}) = H(A_1) - H(E_1). \tag{16}$$

By the fact that $P_R^{(1)}(N_1^{A_1'\to B_1E_1}) > 0$ when $0<\eta<1$ [4], $H(A_1) > H(E_1) \geq 0$. Since an input quantum state A_1 is a Gaussian state, output quantum states B_1 and E_1 are also Gaussian states in a pure loss channel [2]. Assume that the average photon number in the quantum state A_1 is N_A. Then, by von Neumann entropy of a Gaussian state [5],

$$H(A_1) = (N_A+1)\log_2(N_A+1) - N_A\log_2 N_A, \tag{17}$$

$$H(E_1) = ((1-\eta)N_A+1)\log_2((1-\eta)N_A+1) - (1-\eta)N_A\log_2(1-\eta)N_A. \tag{18}$$

By Eqs.(17) and (18), $H(A_1) > H(E_1) > 0$ if $N_A \neq 0$.

Next, consider a rank-one measurement to calculate conditional von Neumann entropy. One property of a rank-one measurement is the following [2].

$$H(A_1E_1|Y_1) = \sum_y P(y)H(A_1E_1|Y_1=y) = 0, \tag{19}$$

$$H(A_1|Y_1) = H(E_1|Y_1). \tag{20}$$

By the chain rule, $H(A_1E_1|Y_1)$ can be expressed as follows:

$$H(A_1E_1|Y_1) = H(E_1|Y_1) + H(A_1|E_1Y_1). \tag{21}$$

Note that $H(A_1|E_1Y_1)$ and $H(E_1|Y_1)$ act as the Shannon entropy by a classical state Y_1, i.e., $H(A_1|E_1Y_1) \geq 0$ and $H(E_1|Y_1) \geq 0$ [6]. By this property, Eqs.(19) and (21) can be expressed as follows:

$$H(E_1|Y_1) = -H(A_1|E_1Y_1) \leq 0. \tag{22}$$

Since $H(E_1|Y_1) \geq 0$, Eq.(22) indicates $H(E_1|Y_1) = 0$. Furthermore, by Eq.(20), $H(A_1|Y_1) = 0$. Therefore, for the maximizer of a reverse quantum capacity in a pure loss channel, i.e., an input Gaussian state and a rank-one measurement,

$$I(Y_1;A_1) = H(A_1) - H(A_1|Y_1) = H(A_1), \tag{23}$$

$$I(Y_1;E_1) = H(E_1) - H(E_1|Y_1) = H(E_1). \tag{24}$$

By Eq.(16) and the fact that $H(E_1) > 0$ if $0<\eta<1$ as in Eq.(18), for the maximizer of a reverse private capacity,

$$I(Y_1;A_1) > P_R^{(1)}(N_1^{A_1'\to B_1E_1}). \tag{25}$$

Finally, by Theorem 1 and Eq.(25),

$$P_R^{(1)}(N_1^{A_1'\to B_1E_1} \otimes N_2^{A_2'\to E_2}) > P_R^{(1)}(N_1^{A_1'\to B_1E_1}) = P_R^{(1)}(N_1^{A_1'\to B_1E_1}) + P_R^{(1)}(N_2^{A_2'\to E_2}). \tag{26}$$

In Eq.(26), equality holds because a reverse private capacity is zero in an 100% erasure channel.

IV. Conclusion

We prove superadditivity of a reverse private capacity in two quantum channels which are a pure loss channel and an 100% erasure channel. This is, based on our knowledge, the first ever proven for a reverse private capacity. Therefore, it provides the possibility to find a tighter lower bound for a secret key capacity of a secret system such as a QKD system.

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]

References

[1] W. K. Wootters and W. H. Zurek, "A single quantum cannot be cloned," *Nature*, vol. 299, no. 5886, pp. 802–803, 1982.

[2] S. Pirandola, R. García-Patrón, S. L. Braunstein, and S. Lloyd, "Direct and reverse secret-key capacities of a quantum channel," *Physical review letters*, vol. 102, no. 5, p. 050503, 2009.

[3] S. Pirandola, "Quantum discord as a resource for quantum cryptography," *arXiv preprint arXiv:1309.2446*, 2013.

[4] S. Pirandola, R. Laurenza, C. Ottaviani, and L. Banchi, "The ultimate rate of quantum cryptography," *arXiv preprint arXiv:1510.08863*, 2015.

[5] 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.

[6] M. M. Wilde, *Quantum information theory*. Cambridge University Press, 2013.