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] revealed 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:

\[
P_R(N; A' \rightarrow BE) = \lim_{n \rightarrow \infty} \frac{1}{n} I^{(1)}_R((N; A' \rightarrow BE)\otimes n),
\]

where

\[
P^{(1)}_R(N; A' \rightarrow BE) = \max_{\rho_{A'A'M_B}} I(Y; A) - I(Y; E).
\]

Here, \( P^{(1)}_R(N) \) is defined as a reverse private capacity for a single channel use. \( P^{(1)}_R(N) \) 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 an 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 $\rho^{A'} = \text{Tr}_A(\rho^{AA'})$ to a receiver, Bob, through a quantum channel $N^{A'\rightarrow BE}$ 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 $\rho^E$. 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 $A_1A_1' A_2A_2'$ with $\rho^{A_1A_1' A_2A_2'}$ where quantum states $A_1 A_1'$ and $A_2 A_2'$ are pure entangled states. Then, she sends a quantum state $A_1A_1' A_2 A_2'$ with $\rho^{A_1A_1' A_2A_2'} = \text{Tr}_{A_1A_2} (\rho^{A_1A_1' A_2A_2'})$ through an arbitrary quantum channel $N_1^{A_1 A_1' \rightarrow B_1 E_1}$ and 100% erasure channel $N_2^{A_2 A_2' \rightarrow E_2}$. 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.

$$Q_R^{(1)}(N_1^{A_1 A_1' \rightarrow B_1 E_1} \otimes N_2^{A_2 A_2' \rightarrow E_2}) \geq I(Y_1; A_1),$$

where

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

**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 $A_1A_1' A_2 A_2'$ with $\rho^{A_1A_1' A_2A_2'}$ which satisfies the following conditions.

$$A_1 \perp A_2,$$
$$H(A_2) \geq H(Y_1),$$
$$\rho^{A_1, Y_1, E_1} = \langle \psi_{A_1 Y_1 E_1} | \psi_{A_1 Y_1 E_1} \rangle.$$
By the fact that a reverse private capacity is bounded by a reverse quantum capacity [2], the result of Theorem 1 provides the following.

\[ P_R^{(1)}(N_1^{A_1 \rightarrow B_1 E_1} \otimes N_2^{A_2 \rightarrow E_2}) \geq Q_R^{(1)}(N_1^{A_1 \rightarrow B_1 E_1} \otimes N_2^{A_2 \rightarrow E_2}) \geq I(Y_1; A_1). \]  

(15)

Next, consider an arbitrary quantum channel \( N_1^{A_1 \rightarrow B_1 E_1} \) 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:

\[ P_R^{(1)}(N_1^{A_1 \rightarrow B_1 E_1}) = H(A_1) - H(E_1). \]  

(16)

By the fact that \( P_R^{(1)}(N_1^{A_1 \rightarrow B_1 E_1}) > 0 \) 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],

\[ H(A_1) = (N_A + 1) \log_2 (N_A + 1) - N_A \log_2 N_A, \]  

(17)

\[ H(E_1) = ((1 - \eta)N_A + 1) \log_2 ((1 - \eta)N_A + 1) - (1 - \eta)N_A \log_2 (1 - \eta)N_A. \]  

(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].

\[ H(A_1 E_1 | Y_1) = \sum_y P(y) H(A_1 E_1 | Y_1 = y) = 0, \]  

(19)

\[ H(A_1 | Y_1) = H(E_1 | Y_1). \]  

(20)

By the chain rule, \( H(A_1 E_1 | Y_1) \) can be expressed as follows:

\[ H(A_1 E_1 | Y_1) = H(E_1 | Y_1) + H(A_1 | E_1 Y_1). \]  

(21)

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

\[ H(E_1 | Y_1) = -H(A_1 | E_1 Y_1) \leq 0. \]  

(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,

\[ I(Y_1; A_1) = H(A_1) - H(A_1 | Y_1) = H(A_1), \]  

(23)

\[ I(Y_1; E_1) = H(E_1) - H(E_1 | Y_1) = H(E_1). \]  

(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,

\[ I(Y_1; A_1) > P_R^{(1)}(N_1^{A_1 \rightarrow B_1 E_1}). \]  

(25)

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

\[ P_R^{(1)}(N_1^{A_1 \rightarrow B_1 E_1} \otimes N_2^{A_2 \rightarrow E_2}) > P_R^{(1)}(N_1^{A_1 \rightarrow B_1 E_1}) = P_R^{(1)}(N_1^{A_1 \rightarrow B_1 E_1}) + P_R^{(1)}(N_2^{A_2 \rightarrow E_2}). \]  

(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