Secret Message Transmission over Quantum Channels under Adversarial Quantum Noise: Secrecy Capacity and Super-Activation

Holger Boche
Lehrstuhl für Theoretische Informationstechnik,
Technische Universität München,
Munich, Germany
boche@tum.de

Minglai Cai
Lehrstuhl für Theoretische Informationstechnik,
Technische Universität München,
Munich, Germany
minglai.cai@tum.de

Christian Deppe
Lehrstuhl für Nachrichtentechnik,
Technische Universität München,
Munich, Germany
christian.deppe@tum.de

Janis Nötzel
Technische Universität Dresden
Dresden, Germany,
janis.noetzel@tu-dresden.de

December 18, 2017

Abstract

We determine the secrecy capacities of arbitrarily varying quantum channels. Both secrecy capacity with average error probability and with maximal error probability are derived. The code we construct fulfills a stringent secrecy requirement, which is called the strong code concept. We determine when the secrecy capacity is a continuous function of the system parameters and completely characterize its discontinuity points both for average error criterion and for maximal error criterion. Furthermore, we prove the phenomenon “super-activation” for secrecy capacities of arbitrarily varying quantum channels, i.e., two quantum channels both with zero secrecy capacity, if used together, allow secure transmission with positive capacity.
1 Introduction

In the last few years the developments in modern communication systems have produced many results in a short amount of time. Quantum communication systems especially, allow us to exploit new possibilities while at the same time impose fundamental limitations.

Quantum mechanics differs significantly from classical mechanics, it has its own laws. Quantum information theory unifies information theory with quantum mechanics, generalizing classical information theory to the quantum world. The unit of quantum information is called the "qubit", the quantum analogue of the classical "bit". Unlike a bit, which is either “0” or “1”, a qubit can be in a “superposition”, i.e., two states at the same time. This property has turned into one of the fundamental resources of quantum information processing.

A quantum channel is a communication channel which can carry quantum information, e.g., photons. In general, there are two ways to represent a quantum channel with linear algebraic tools, either as a sum of several transformations, or as a single unitary transformation, which explicitly includes the unobserved environment.

A quantum channel can transmit both classical and quantum information. If the sender wants to transmit a classical message of a finite set $A$ to the receiver using a quantum channel $N$, his encoding procedure will include a classical-to-quantum encoder to prepare a quantum message state $\rho$ suitable as an input for the channel. If the sender’s encoding is restricted to transmit an indexed finite set of quantum states $\{\rho_x : x \in A\}$, then we can consider the choice of the signal quantum states $\rho_x$ as a component of the channel. This is equivalent to considering the classical capacity of quantum channels.

Our goal is to investigate communication that takes place over a quantum channel which is, in addition to the noise from the environment, subjected to the
action of a jammer who actively manipulates the states. The messages should also be kept secret from an eavesdropper.

A channel with a jammer is called an arbitrarily varying channel, where the jammer may change his input in every channel use and is not restricted to use a repetitive probabilistic strategy. In this model we consider a channel which is not stationary and can change with every use. It works as follows: At first the sender and the receiver have to select their coding scheme. After that, the jammer makes his choice of the channel state to sabotage the message transmission. However, due to the physical properties, we assume that the jammer’s changes only take place in a set which is known to the sender and the receiver.

The arbitrarily varying channel was first introduced in [12]. [2] showed a surprising result which is known as the Ahlswede Dichotomy: Either the capacity of an arbitrarily varying channel is zero or it equals its shared randomness assisted capacity. After the discovery in [12] it has remained an open question as to when the deterministic capacity is positive. In [25], a sufficient condition for that has been given, and in [23], it is proved that this condition is also necessary. The Ahlswede Dichotomy demonstrates the importance of shared randomness for communication in a very clear form.

A quantum channel with a jammer is called an arbitrarily varying quantum channel. It is defined as a family of indexed channels \( \{N_\theta : \theta = 1, \ldots, T \} \), where \( \theta \) is called a channel state of the channel pair. This channel state \( \theta \), which varies from symbol to symbol in an arbitrary manner, governs the channel. In [4], the classical capacity of arbitrarily varying quantum channels is analyzed, and a lower bound on the capacity has been given. An alternative proof and a proof of the strong converse are both given in [11]. In [3], the Ahlswede Dichotomy for the arbitrarily varying classical-quantum channels is established, and a sufficient and necessary condition for the zero deterministic capacity is given. In [18], a simplification of this condition for the arbitrarily varying classical-quantum channels is given. [3] and [15] complete the characterization of message transmission capacity for the arbitrarily varying channel. In [3], message transmission, key transmission, and strong subspace transmission have been considered. A full description of these transmission tasks have been completely established. In [18] an example has been given showing there are indeed arbitrarily varying classical-quantum channels which have zero deterministic capacity and positive random capacity. In this work we rendered these results to secrecy message transmission over arbitrarily varying quantum channels, which is the full description of secure message transmission and key transmission through arbitrarily varying quantum wiretap channels.

For a noisy quantum channel, its noise can be interpreted as interaction with the environment. Following the general protocol of [24], we say the environment is completely under the control of the eavesdropper. Secure communication over a classical channel with an eavesdropper was first introduced in [41]. A classical-quantum channel with an eavesdropper is called a classical-quantum wiretap channel. The secrecy capacity for classical-quantum channel with an eavesdropper has been determined in [24] and [22].

This work is a furtherance of our previous papers [15], [16], and [17], where we considered channel robustness against jamming, and concurrently security against eavesdropping for classical-quantum channels (cf. Section 2.2), where classical-quantum channels are quantum channels whose sender’s inputs are classical variables. In our earlier works [15], [16], and [17], we investigated the
secrecy message transmission over a classical-quantum channel. The messages were kept secret from an eavesdropper. Communication took place over a quantum channel which was, in addition to noise from the environment, subjected to the action of a jammer, which actively manipulated the states. A classical-quantum channel with both a jammer and an eavesdropper is called an arbitrarily varying classical-quantum wiretap channel. It is defined as a family of pairs of indexed channels \( \{ (W_\theta, V_\theta) : \theta = 1, \ldots, T \} \) with a common input alphabet and possibly different output systems, connecting a sender with two receivers, a legal one and a wiretapper. The legitimate receiver accesses the output of the first channel \( W_\theta \) in the pair, and the wiretapper observes the output of the second channel \( V_\theta \), respectively. \( \theta \) governs both the legal receiver’s channel and the wiretap channel. A code for the channel conveys information to the legal receiver such that the wiretapper knows nothing about the transmitted information. In [15], [16], and [17], the Ahlswede Dichotomy for arbitrarily varying classical-quantum wiretap channels is established, i.e. either the deterministic capacity of an arbitrarily varying channel is zero or is equal to its shared randomness assisted capacity. We delivered the formula for secrecy capacity of the arbitrarily varying classical-quantum wiretap channel. A full description of the arbitrarily varying classical-quantum wiretap channels is thus established when we combine the results of [15], [16], and [17].

In this work we determine the secrecy capacities of arbitrarily varying quantum channels. We also give an example showing that there are indeed arbitrarily varying quantum channels which have zero deterministic secrecy capacity and positive randomness assisted secrecy capacity.

The capacities of classical arbitrarily varying channel under maximal error criterion and under the average error criterion are in general, not equal, where the capacity formula of classical arbitrarily varying channels under maximal error criterion is still an open problem. Interestingly, [15] shows that the capacities of arbitrarily varying quantum channel under maximal error criterion and under the average error criterion are equal (cf. Remark 2.6, Remark 4.7, and Remark 4.8). In this work we extend this observation: We show that the secrecy capacities of arbitrarily varying quantum channel under maximal error criterion and under the average error criterion are equal.

As an application of our results, we turn to the question: Is the secrecy capacity a continuous function of the system parameters? The analysis of the continuity of capacities of quantum channels is motivated by the question of whether small changes in the channel system are able to cause dramatic losses in the performance. The continuity of the message and entanglement transmission capacity of a stationary memoryless quantum channel has been listed as an open problem in [12] and was solved in [31]. Considering quantum channels with active jamming faces an especially new difficulty. The reason is that the capacity in this case is, in general, not solely specified by entropy quantities. In [19] it has been shown when the message transmission capacity of an arbitrarily varying quantum channels is continuous. The condition for continuity of message transmission capacity of a classical arbitrarily varying wiretap channel has been given in [40].

The continuity of the secrecy capacity of a classical arbitrarily varying channel under randomness assisted quantum coding has been shown in [21]. This proof is still capable of improvements since in general, the legal channel users do not have control over the the eavesdropper’s channel. However, this proof
requires that the output alphabet of the eavesdropper’s channel is of finite cardinality. In this work we show that the continuity of the secrecy capacity of an arbitrarily varying quantum channel under randomness assisted quantum coding only depends on the legal channel. Moreover we improve the result of [21] when we give a generalized control function. This control function only depends on the legal channel.

Furthermore, we show as a consequence of our results that there is a phenomenon called “super-activation” for the secrecy capacity of arbitrarily varying quantum channels, i.e., two arbitrarily varying quantum channels, each useless for secure message transmission, can be super-activated to acquire positive secrecy capacity when used together.

2 Preliminaries

2.1 Basic properties, Communication Scenarios, and Notations

For a finite set \( A \) we denote the set of probability distributions on \( A \) by \( P(A) \). Let \( \rho_1 \) and \( \rho_2 \) be Hermitian operators on a finite-dimensional complex Hilbert space \( G \). We say \( \rho_1 \geq \rho_2 \) and \( \rho_2 \leq \rho_1 \) if \( \rho_1 - \rho_2 \) is positive-semidefinite. For a finite-dimensional complex Hilbert space \( G \), we denote the (convex) space of density operators on \( G \) by \( S(G) := \{ \rho \in L(G) : \rho \text{ is Hermitian, } \rho \geq 0 \text{ on } G, \text{ tr}(\rho) = 1 \} \), where \( L(G) \) is the set of linear operators on \( G \), and \( 0 \) is the null matrix on \( G \). Note that any operator in \( S(G) \) is bounded.

For any finite set \( A \), any finite-dimensional complex Hilbert space \( H \), and \( n \in \mathbb{N} \), we define \( A^n := \{(a_1, \cdots, a_n) : a_i \in A \forall i \in \{1, \cdots, n\}\} \), and \( H^\otimes n := \text{span}\{v_1 \otimes \cdots \otimes v_n : v_i \in H \forall i \in \{1, \cdots, n\}\} \). We write \( a^n \) for the elements of \( A^n \).

We denote the identity operator on a space \( H \) by \( \text{id}_H \) and the symmetric group on \( \{1, \cdots, n\} \) by \( S_n \). For a set \( A \) on an Euclidean space \( G \) we define the convex hull of \( A \) by \( \text{Conv}(A) \).

For a discrete random variable \( X \) on a finite set \( A \) and a discrete random variable \( Y \) on a finite set \( B \), we denote the Shannon entropy of \( X \) by \( H(X) = -\sum_{x \in A} p(x) \log p(x) \) and the mutual information between \( X \) and \( Y \) by \( I(X;Y) = \sum_{x \in A} \sum_{y \in B} p(x,y) \log \left( \frac{p(x,y)}{p(x)p(y)} \right) \). Here \( p(x,y) \) is the joint probability distribution function of \( X \) and \( Y \), and \( p(x) \) and \( p(y) \) are the marginal probability distribution functions of \( X \) and \( Y \) respectively, and “log” means logarithm to base 2.

For a quantum state \( \rho \in S(H) \) we denote the von Neumann entropy of \( \rho \) by \( S(\rho) = -\text{tr}(\rho \log \rho) \).

Let \( \mathfrak{H} \) and \( \Omega \) be quantum systems. We denote the Hilbert space of \( \mathfrak{H} \) and \( \Omega \) by \( G^\mathfrak{H} \) and \( G^\Omega \), respectively. Let \( \phi^{\mathfrak{H}\Omega} \) be a bipartite quantum state in \( S(G^\mathfrak{H}\Omega) \).
We denote the partial trace over $G^\mathcal{P}$ by
\[
\text{tr}_\mathcal{P}(\phi^{G^\mathcal{P}}) := \sum_l \langle l|\phi^{G^\mathcal{P}}|l\rangle ,
\]
where $\{|l\rangle : l\}$ is an orthonormal basis of $G^\mathcal{P}$. We denote the conditional entropy by
\[
S(\mathcal{P} | \Omega)_\rho := S(\phi^{G^\mathcal{P}}) - S(\phi^\mathcal{P}) .
\]
Here $\phi^\mathcal{P} = \text{tr}_\mathcal{P}(\phi^{G^\mathcal{P}})$.

Let $\Phi := \{\rho_x : x \in A\}$ be a set of quantum states labeled by elements of $A$. For a probability distribution $Q$ on $A$, the Holevo quantity $\chi$ is defined as
\[
\chi(Q; \Phi) := S\left(\sum_{x \in A} Q(x) \rho_x\right) - \sum_{x \in A} Q(x) S(\rho_x) .
\]
Note that we can always associate a state $\rho^{XY} = \sum_{x} Q(x)|x\rangle\langle x| \otimes \rho_x$ to $(Q; \Phi)$ such that $\chi(Q; \Phi) = I(X; Y)$ holds for the quantum mutual information.

For a probability distribution $P$ on a finite set $A$ and a positive constant $\delta$, we denote the set of typical sequences by
\[
\mathcal{T}_{P,\delta} := \left\{a^n \in A^n : \left|\frac{1}{n} N(a' | a^n) - P(a')\right| \leq \frac{\delta}{|A|} \forall a' \in A\right\} ,
\]
where $N(a' | a^n)$ is the number of occurrences of the symbol $a'$ in the sequence $a^n$.

For finite-dimensional complex Hilbert spaces $G$ and $G'$, a quantum channel $N : S(G) \rightarrow S(G')$, $S(G) \ni \rho \rightarrow N(\rho) \in S(G')$ is represented by a completely positive trace-preserving map which accepts input quantum states in $S(G)$ and produces output quantum states in $S(G')$.

**Definition 2.1.** Let $\mathcal{P}$ and $\Omega$ be quantum systems. We denote the Hilbert space of $\mathcal{P}$ and $\Omega$ by $H^\mathcal{P}$ and $H^\Omega$, respectively, and let $\Theta := \{1, \cdots , T\}$ be a finite set.

For every $\theta \in \Theta$, let $N_\theta$ be a quantum channel $S(H^\mathcal{P}) \rightarrow S(H^\Omega)$. We call the set of the quantum channels $\{N_\theta : \theta \in \Theta\}$ an **arbitrarily varying quantum channel** when the state $\theta$ varies from symbol to symbol in an arbitrary manner.

The following Definition 2.2 plays a very important role for the characterization of the capacity of arbitrarily varying quantum channels.

**Definition 2.2.** Let $L \in \mathbb{N}$. We say that the arbitrarily varying quantum channel $\{N_\theta : \theta \in \Theta\}$ is $L$-symmetrizable if for every $\rho^L$, $\rho'^L \in S(H^{G^\mathcal{P}})$ there exists a map $\tau$ which maps from $\{|\rho^L, \rho'^L\rangle\}$ to the set of distributions on $\Theta^L$ such that
\[
\sum_{\theta L \in \Theta^L} \tau(\rho^L)(\theta^L) N_{\theta L}(\rho'^LL) = \sum_{\theta L \in \Theta^L} \tau(\rho'^L)(\theta^L) N_{\theta L}(\rho^L) .
\] (1)

**Remark 2.3.** In [15] the $L$-symmetrizability was defined as follows: We say that $\{N_\theta : \theta \in \Theta\}$ is $L$-symmetrizable if for every finite set $\{\rho_1^L, \cdots , \rho_K^L\} \subset$
S(H^\Omega) there exists a \tau such that for all \rho^L, \rho'^L \in \{\rho^L_1, \ldots, \rho^L_K\}, (1) holds. The authors then showed that we might limit the cardinality K to K = 2, which is the condition for L-symmetrizability defined in [7]. Thus the two conditions for L-symmetrizability are equivalent.

2.2 Problem Definition and Basic Definitions

In general, there are two ways to represent a quantum channel, i.e. a completely positive trace-preserving map \( H^\Psi \rightarrow H^\Omega \), with linear algebraic tools.

1. Operator sum decomposition (Kraus representation)

\[ N(\rho) = \sum_{i=1}^{K} A_i \rho A_i^* , \quad (2) \]

where \( A_1, \ldots, A_K \) (Kraus operators) are linear operators \( S(H^\Psi) \rightarrow S(H^\Omega) \) (cf. [29], [7], and [33]). They satisfy the trace-preserving relation \( \sum_{i=1}^{K} A_i^* A_i = \text{id}_{H^\Psi} \). The representation of a quantum channel \( N \) according to (2) is not unique. Let \( A_1, \ldots, A_K \) and \( B_1, \ldots, B_K \) be two sets of Kraus operators (by appending zero operators to the shorter list of operation elements we may ensure that \( K' = K \)). Suppose \( A_1, \ldots, A_K \) represents \( N \), then \( B_1, \ldots, B_K \) also represents \( N \) if and only if there exists a \( K \times K \) unitary matrix \((u_{ij})_{i,j=1,2,\ldots,K}\) such that for all \( i \) we have \( A_i = \sum_{j=1}^{K} u_{ij} B_j \) (cf. [33]).

2. Isometric extension (Stinespring dilation)

\[ N(\rho) = \text{tr}_\mathcal{E} (U_N \rho U_N^* ) , \quad (3) \]

where \( U_N \) is a linear operator \( S(H^\Psi) \rightarrow S(H^\Omega) \) such that \( U_N^* U_N = \text{id}_{H^\Psi} \), and \( \mathcal{E} \) is the quantum system of the environment (cf. [39], [7], and also cf. [39] for a more general Stinespring dilation theorem). \( H^\mathcal{E} \) can be chosen such that \( \dim H^\mathcal{E} < (\dim H^\Psi)^2 \). The isometric extension of a quantum channel \( N \) according to (3) is not unique either. Let \( U \) and \( U' \) be two linear operators \( S(H^\Psi) \rightarrow S(H^\Omega) \). Suppose \( U \) represents \( N \), then \( U' \) also represents \( N \) if and only if \( U \) and \( U' \) are unitarily equivalent.

It is well known that we can reduce each of these two representations of the quantum channel from the other one. Let \( A_1, \ldots, A_K \) be a set of Kraus operators which represents \( N \). Let \( \{|j\rangle : j = 1, \ldots, K\} \) be an orthonormal system on \( H^\mathcal{E} \). Then \( U_N = \sum_{j=1}^{K} A_j \otimes |j\rangle^\mathcal{E} \) is an isometric extension which represents \( N \), since \( \left( \sum_{j=1}^{K} A_j \otimes |j\rangle^\mathcal{E} \right)^\dagger \rho \left( \sum_{k=1}^{K} A_k \otimes |k\rangle^\mathcal{E} \right) = \sum_{j=1}^{K} A_j \rho A_j^* \) and \( \left( \sum_{j=1}^{K} A_j \otimes |j\rangle^\mathcal{E} \right)^\dagger \left( \sum_{k=1}^{K} A_k \otimes |k\rangle^\mathcal{E} \right) = \sum_{j=1}^{K} A_j^* A_j \). For the other way around, every isometric extension \( U_N \) that represents \( N \) can be written in the form \( U_N = \sum_{j=1}^{K} A_j \otimes |j\rangle^\mathcal{E} \), i.e. if the sender sends \( \rho \), and if the environment’s measurement gives \(|i\rangle^\mathcal{E}\), the receiver’s outcome will be \( A_i \rho A_i^* \). Here \( A_1, \ldots, A_K \) is a set of Kraus operators which represents \( N \), and \( \{|j\rangle^\mathcal{E} : j = 1, \ldots, K\} \) is an orthonormal system on \( H^\mathcal{E} \).
We aim to analyze secret message transmission over a quantum channel. This channel connects the sender and the legal receiver, conveying information from the former to the latter. It is subject to active attacks: A jammer may change his input in every channel use and is not restricted to use a repetitive probabilistic strategy. If we do not consider security, we have a situation as shown in Figure 1, where public messages are transmitted. This scenario is described by a tripartite system with the sender, the legal receiver, and the jammer.

Following [24] we now define the secret message transmission protocol when we assume that the environment is completely under the control of the eavesdropper.

**Definition 2.4.** Let $\mathcal{P}$ and $\Omega$ be quantum systems and $\Theta := \{1, \ldots , T\}$ be a finite set. Let $\mathcal{I} = \{N_\theta : \theta \in \Theta\}$ be an arbitrarily varying quantum channel. Following [24] we assume that the environment $\mathcal{E}$ is completely under the control of the eavesdropper in the following sense:

Let $\rho^\mathcal{P} \to U_{N_\theta}\rho^\mathcal{P}U_{N_\theta}^*$ be an isometric transformation which represents $N_\theta$, where $U_{N_\theta}$ is a linear operator $\mathcal{S}(H^\mathcal{P}) \to \mathcal{S}(H^\mathcal{E} \oplus \mathcal{Q})$, and $\mathcal{Q}$ is the quantum system of the environment. $H^\mathcal{E}$ can be chosen such that $\dim H^\mathcal{E} \leq (\dim H^\mathcal{P})^2$. Fix a $\rho^\mathcal{P}$ with eigen-decomposition $\sum_{x \in \mathcal{X}} p(x) \left| \psi_x \right\rangle \left\langle \psi_x \right|_\mathcal{P}$. If the channel state is $\theta$, the local output density matrix seen by the receiver is

$$\text{tr}_\mathcal{E} \left( \sum_{x} p(x) U_{N_\theta} \left| \psi_x \right\rangle \left\langle \psi_x \right|_\mathcal{P} U_{N_\theta}^* \right),$$

and the local output density matrix seen by the environment (which we interpret as the wiretapper) is

$$\text{tr}_\mathcal{Q} \left( \sum_{x} p(x) U_{N_\theta} \left| \psi_x \right\rangle \left\langle \psi_x \right|_\mathcal{P} U_{N_\theta}^* \right).$$

Therefore $\{V_\theta : \theta \in \Theta\}$ defines an arbitrarily varying wiretap quantum channel $\{(N_\theta, V_\theta) : \theta \in \Theta\}$, where $N_\theta : H^\mathcal{P} \to H^\mathcal{P} \oplus \sum_{x \in \mathcal{X}} p(x) \left| \psi_x \right\rangle \left\langle \psi_x \right|_\mathcal{P} \to \text{tr}_\mathcal{E} \left( \sum_{x} p(x) U_{N_\theta} \left| \psi_x \right\rangle \left\langle \psi_x \right|_\mathcal{P} U_{N_\theta}^* \right)$, and $V_\theta : H^\mathcal{P} \to H^\mathcal{Q} \oplus \sum_{x \in \mathcal{X}} p(x) \left| \psi_x \right\rangle \left\langle \psi_x \right|_\mathcal{P} \to \text{tr}_\mathcal{E} \left( \sum_{x} p(x) U_{N_\theta} \left| \psi_x \right\rangle \left\langle \psi_x \right|_\mathcal{P} U_{N_\theta}^* \right)$. 

---

**Figure 1:** Arbitrarily varying quantum channel
The jammer and the eavesdropper here act as two additional channel users. Instead of the tripartite system of Figure 1 we now have a quadripartite system in Figure 2. The quantum channel used by the legal parties (sender and receiver) is subject to two attacks at the same time: one passive (eavesdropping), and one active (jamming). The task for the legal transmitters is to transmit private information (secret messages or secret keys) despite the jamming attacks and at the same time to kept it secret against eavesdropping.

We consider the secrecy capacity of quantum channels carrying private information. We assume that the jammer is an additional hostile channel user. It is effectively given by an interference channel where the legal sender and the jammer are allowed to make inputs to the system and the legal receiver as well as the eavesdropper receive the corresponding outputs. Furthermore, we assume that the eavesdropper controls the complete environment. The jammer and the eavesdropper aim to prevent the legal parties from privately communicating, each with their own attacking strategies, respectively.

Quantum channels can transmit both classical and quantum information. For the transmission of classical information via a quantum channel, we first have to convert a classical message into a quantum state. We assume that the states to be produced in the input system are given by the set \( \{\rho_x : x \in A\} \subset S(G) \), where \( A \) is a finite set of letters. By Section 2.1 we can define the map \( F : A \rightarrow H^\Omega \), which is defined by \( A \ni x \rightarrow F(x) = \rho_x \in H^\Omega \), meaning that each classical input of \( x \in A \) leads to a distinct quantum output \( \rho_x \in H^\Omega \). \( F \) defines a linear map (a classical-quantum channel) \( N \circ F := W : P(A) \rightarrow S(H^\Omega) \),

\[
P(A) \ni P \mapsto W(P) = \sum_x P(x)N(\rho_x) \in S(H^\Omega) .
\]

In view of this, we have the following definition.

**Definition 2.5.** An \((n, J_n)\) (deterministic) code \( C \) for an arbitrarily varying quantum channel \( J = \{N_\theta : \theta \in \Theta\} \) with classical input \( F : A \rightarrow H^\Omega \) consists of a stochastic encoder \( E : \{1, \cdots, J_n\} \rightarrow P(A^n) \), \( j \rightarrow E(j) \), specified by a
matrix of conditional probabilities $E(\cdot | \cdot)$, and a collection of positive-semidefinite operators $\{D_j : j \in \{1, \ldots, J_n\}\}$ on $H^\otimes n$, which is a partition of the identity, i.e., $\sum_{j=1}^{J_n} D_j = \text{id}_{H^\otimes n}$. We call these operators the decoder operators.

The average probability of the decoding error of a deterministic code $C$ is defined as

$$P_e(C, \theta^n) := 1 - \frac{1}{J_n} \sum_{j=1}^{J_n} \text{tr}(N_{\theta^n} \circ F^n(E(\cdot | j))D_j) .$$

The maximal probability of the decoding error of a deterministic code $C$ is defined as

$$P_e^{(\max)}(C, \theta^n) := 1 - \min_{j \in \{1, \ldots, J_n\}} \text{tr}(N_{\theta^n} \circ F^n(E(\cdot | j))D_j) .$$

A code is created by the sender and the legal receiver before the message transmission starts. The sender uses the encoder to encode the message that he wants to send, while the legal receiver uses the decoder operators on the channel output to decode the message.

In [24] it has been shown that codes for the secure message transmission over a classical-quantum wiretap channel can be used to build codes for the entanglement transmission over a quantum channel. Please see [14] for a discussion of entanglement generation over compound quantum channels, which are channels with channel uncertainties.

**Remark 2.6.** For classical arbitrarily varying channels, capacities under the average error criterion and under maximal error criterion are distinguished from each other. The capacity formula for the latter one is still unknown (cf. [2]). This statement is not true for the capacities of arbitrarily varying classical-quantum channel under maximal error criterion and under the average error criterion (cf. Remark [7], Remark [8] and [11]).

We now consider, in addition to a faithful message transmission, the security, i.e., a code for the channel conveying private information to the legal receiver such that the wiretapper’s knowledge of the transmitted information can be kept arbitrarily small.

**Definition 2.7.** Let $\mathcal{J} = \{N_\theta : \theta \in \Theta\}$ be an arbitrarily varying quantum channel. A non-negative number $R$ is an achievable (deterministic) secrecy rate for the arbitrarily varying quantum channel $\mathcal{J}$ under the average error criterion if for every $\epsilon > 0$, $\delta > 0$, $\zeta > 0$ and sufficiently large $n$ there exists a finite set $A$, a map $F : A \to H^\psi$, and an $(n, J_n)$ code $C = (E, \{D^\theta_j : j = 1, \ldots, J_n\})$ such that

$$\frac{\log J_n}{n} > R - \delta,$$

and

$$\max_{\theta^n \in \Theta^n} P_e(C, \theta^n) < \epsilon ,$$

$$\max_{\theta^n \in \Theta^n} \chi (R_{\text{uni}}; Z_{\theta^n}) < \zeta .$$

Here $R_{\text{uni}}$ is a random variable uniformly distributed on $\{1, \ldots, J_n\}$ and

$$Z_{\theta^n} = \{V_{\theta^n} \circ F^n(E(\cdot | i)) : i \in \{1, \ldots, J_n\}\} ,$$

10
where $V'^{\theta}$ is the channel to the environment defined by $N^{\theta}$.

The supremum on achievable (deterministic) secrecy rates of $I$ under the average error criterion is called the (deterministic) secrecy capacity of $I$ under the average error criterion, denoted by $C_s(I)$.

**Remark 2.8.** A weaker and widely used security criterion is obtained if we replace (5) with
\[
\max_{\theta^n \in \Theta} \frac{1}{n} \chi (R_{\text{uni}}^{\theta^n}; Z_{\theta^n}) < \zeta.
\]
In this paper we will follow [10] and use (5).

**Remark 2.9.** It is understood that the sender and the receiver have to select their coding scheme first. We assume that this coding scheme is known by the jammer and the eavesdropper. The jammer can make use of this knowledge to advance his attacking strategy. Our Definition 4 for the criterion of decoding error probability and Definition 5 for the security criterion require that a private information transmission can be guaranteed even in the worst case, i.e., under the assumption that the jammer and the eavesdropper know the complete coding scheme and will choose attacking strategies which are most advantageous for themselves.

**Definition 2.10.** Let $I = \{N^\theta : \theta \in \Theta\}$ be an arbitrarily varying quantum channel. A non-negative number $R$ is an achievable (deterministic) secrecy rate for the arbitrarily varying quantum channel $I$ under the maximal error criterion If for every $\epsilon > 0$, $\delta > 0$, $\zeta > 0$ and sufficiently large $n$ there exists a finite set $A$, a map $F : A \rightarrow H^n$, and an $(n, J_n)$ code $C = (E, \{D^j_n : j = 1, \ldots, J_n\})$ such that $\frac{\log J_n}{n} > R - \delta$, and
\[
\max_{\theta^n \in \Theta} P^{(\text{max})}(C, \theta^n) < \epsilon,
\]
\[
\max_{\theta^n \in \Theta} \chi (R_{\text{uni}}^{\theta^n}; Z_{\theta^n}) < \zeta.
\]
Here $R_{\text{uni}}$ and $Z_{\theta^n}$ are defined as in Definition 2.7.

The supremum on achievable (deterministic) secrecy rates of $I$ under the maximal error criterion is called the (deterministic) secrecy capacity of $I$ under the maximal error criterion, denoted by $C_{s,\text{max}}(I)$.

The maximal error criterion is the strongest error criterion in the sense that when we consider secret message transmission under the maximal error criterion, we assume that the jammer not only knows the coding scheme of the legal channel users (cf. Remark 2.9), but also the actual message. Definition 2.10 requires that a private information transmission can be guaranteed even under the assumption that the jammer, knowing both the complete coding scheme and the message, will choose the most advantaged jamming attacking strategy depending on this knowledge.

**Definition 2.11.** Let $I = \{N^\theta : \theta \in \Theta\}$ be an arbitrarily varying quantum channel. We denote the set of $(n, J_n)$ deterministic codes for $I$ by $\Lambda$.

A non-negative number $R$ is an achievable secrecy rate for the arbitrarily varying quantum channel $I$ under randomness assisted coding if for every
\[
\delta > 0, \ \zeta > 0, \ \text{and} \ \epsilon > 0, \ \text{if} \ n \ \text{is sufficiently large, there is a finite set} \ \mathbf{A}, \ \text{a map} \ F : \mathbf{A} \to H^\mathcal{G}, \ \text{and a distribution} \ G \ \text{on} \ (\Lambda, \sigma) \ \text{such that} \ \frac{\log J_n}{n} > R - \delta, \ \text{and}
\]
\[
\max_{\theta^n \in \Theta^n} \int_{\Lambda} P_\gamma^e(C^n, \theta^n) dG(\gamma) < \epsilon, \\
\max_{\theta^n \in \Theta^n} \int_{\Lambda} \chi(R_{\text{uni}}; Z_{C^n, \theta^n}) dG(\gamma) < \zeta.
\]

Here \( \sigma \) is a sigma-algebra, so chosen such that the functions \( \gamma \to P_\gamma^e(C^n, \theta^n) \) and \( \gamma \to \chi(R_{\text{uni}}; Z_{C^n, \theta^n}) \) are both \( G \)-measurable with respect to \( \sigma \) for every \( \theta^n \in \Theta^n \).

The supremum on achievable secrecy rates for \( \mathcal{I} \) under randomness assisted coding is called the randomness assisted secrecy capacity of \( \mathcal{I} \), denoted by \( C_s(\mathcal{I}, r) \).

**Definition 2.12.** Let \( \mathcal{I} = \{N_\theta : \theta \in \Theta \} \) be an arbitrarily varying quantum channel. We denote the set of \((n, J_n)\) deterministic codes for \( \mathcal{I} \) by \( \Lambda \).

A non-negative number \( R \) is an achievable secrecy rate for the arbitrarily varying quantum channel \( \mathcal{I} \) under randomness assisted classical coding and the maximal error criterion if for every \( \delta > 0, \ \zeta > 0, \ \text{and} \ \epsilon > 0, \ \text{if} \ n \ \text{is sufficiently large, there is a finite set} \ \mathbf{A}, \ \text{a map} \ F : \mathbf{A} \to H^\mathcal{G}, \ \text{and a distribution} \ G \ \text{on} \ (\Lambda, \sigma) \ \text{such that} \ \frac{\log J_n}{n} > R - \delta, \ \text{and}
\]
\[
\max_{\theta^n \in \Theta^n} \int_{\Lambda} P_\gamma^e(C^n, \theta^n) dG(\gamma) < \epsilon, \\
\max_{\theta^n \in \Theta^n} \int_{\Lambda} \chi(R_{\text{uni}}; Z_{C^n, \theta^n}) dG(\gamma) < \zeta.
\]

Here \( \sigma \) is a sigma-algebra, so chosen such that the functions \( \gamma \to P_\gamma^e(C^n, \theta^n) \) and \( \gamma \to \chi(R_{\text{uni}}; Z_{C^n, \theta^n}) \) are both \( G \)-measurable with respect to \( \sigma \) for every \( \theta^n \in \Theta^n \).

The supremum on achievable secrecy rates for \( \mathcal{I} \) under randomness assisted classical coding and the maximal error criterion is called the randomness assisted secrecy classical capacity under the maximal error criterion of \( \mathcal{I} \), denoted by \( C_{s, \text{max}}(\mathcal{I}, r) \).

**Definition 2.13.** The code concept for arbitrarily varying wiretap quantum channels is similar to the code concept for arbitrarily varying classical-quantum wiretap channels in [15] and [17]. We build a two-part code word, the first part is used to create the randomness for the sender and the legal receiver, the second is used to transmit the message to the legal receiver. We call it a weak code concept when the first part to synchronize the second part is public, and a strong code concept when the first part is secure.

**Definition 2.14.** Let \( \{N_\theta : \theta \in \Theta \} \) and \( \{N_{\theta'} : \theta' \in \Theta' \} \) be two arbitrarily varying quantum channels.

We say super-activation occurs to the secrecy capacity for two arbitrarily varying classical-quantum wiretap channels \( \{N_\theta : \theta \in \Theta \} \) and \( \{N_{\theta'} : \theta' \in \Theta' \} \) when the following hold:
\[
C_s(\{N_\theta : \theta \in \Theta \}) = 0,
\]

12
\[ C_a(\{\tilde{N}_{\theta'} : \theta' \in \Theta'\}) = 0, \]

and
\[ C_a(\{N_\theta \otimes \tilde{N}_{\theta'} : (\theta, \theta') \in \Theta \times \Theta'\}) > 0. \]

Definition 2.15. Let \( I = \{N_\theta : \theta \in \Theta\} \) be an arbitrarily varying quantum channel. We define
\[ \mathcal{C}(I) = \lim_{n \to \infty} \sup \frac{1}{n} \left( \sup_{A, F, P, q' \in P(\Theta)} \inf_{\theta'' \in \Theta^n} \chi(P, B^n_{q'}) - \max_{\theta'' \in \Theta^n} \chi(P, Z_{\theta''}) \right). \]  

The supremum is taken over all chosen finite sets \( A \), maps \( F : A \to H^Y \), and probability distributions \( P \) on the input quantum states \( \{F(x) : x \in A\} \). Here \( B_q \) and \( Z_{\theta''} \) are the resulting quantum states at the output of \( N_\theta \) and \( V_\theta \), respectively, where \( V_\theta \) is the channel to the environment defined by \( N_\theta \).

Let \( \Sigma = (W_{\theta}, V_{\theta})_{\theta \in \Theta} \) be an arbitrarily varying classical-quantum wiretap channel. We define
\[ \mathcal{C}(\Sigma) := \lim_{n \to \infty} \frac{1}{n} \max_{U \to A \to \{B_{\theta}, Z_{\theta}, q, \theta\}} \left( \inf_{B_q \in \text{Conv}(\{B_{\theta} : \theta \in \Theta\})} \chi(p_U, B^n_{q}) - \max_{\theta'' \in \Theta^n} \chi(p_U, Z_{\theta''}) \right). \]

Here \( B_{\theta} \) are the resulting quantum states at the output of the legitimate receiver’s channels. \( Z_{\theta''} \) are the resulting quantum states at the output of wiretap channels. The maximum is taken over all random variables that satisfy the Markov chain relationships: \( U \to A \to B_{\theta} Z_{\theta} \) for every \( B_{\theta} \in \text{Conv}(\{B_{\theta} : \theta \in \Theta\}) \) and \( \theta \in \Theta \). Here \( A \) is a random variable taking values on \( A \), and \( U \) a random variable taking values on some finite set \( U \) with probability distribution \( p_U \).

Definition 2.16. For finite sets \( A \) and \( B \), we define a (discrete) classical channel \( V : P(A) \to P(B) \), \( P(A) \ni p \to V(p) \in P(B) \) to be a system characterized by a probability transition matrix \( V(\cdot | \cdot) \). For \( p \in P(A) \) and \( y \in B \), \( V(y | p) \) expresses the probability of the output symbol \( y \) when we send the symbol \( x \) through the channel. The channel is said to be memoryless if the probability distribution of the output depends only on the input at that time and is conditionally independent of previous channel inputs and outputs. Further, we can extend this definition when we define a classical channel to a map \( V : P(A) \to P(B) \) by denoting \( V(y | p) := \sum_{x \in A} p(x)V(y | x) \).

Definition 2.17. Let \( A, B, \) and \( C \) be finite sets. Let \( \Theta : = \{1, \ldots, T\} \) be a finite set. For every \( \theta \in \Theta \), let \( W_{\theta} \) be a classical channel \( P(A) \to P(B) \) and \( V_{\theta} \) be a classical channel \( P(A) \to P(C) \).

We call the set of the classical channel pairs \( \{(W_{\theta}, V_{\theta}) : \theta \in \Theta\} \) a (classical) arbitrarily varying wiretap channel when the channel state \( \theta \) varies from symbol to symbol in an arbitrary manner. When the sender inputs \( p \in P(A) \) into the channel, the receiver receives the output \( y \in B \) with probability \( \sum_{x \in A} p(x)W_{\theta}(y | x) \), while the wiretapper receives the output \( z \in Z \) with probability \( \sum_{x \in A} p(x)V_{\theta}(z | x) \).
Definition 2.19. Let $\mathcal{R} = \{(W_\theta, V_\theta) : \theta \in \Theta\}$ be a classical arbitrarily varying wiretap channel. An $(n, J_n)$ code for $\mathcal{R}$ consists of a stochastic encoder $E : \{1, \ldots, J_n\} \to P(A^n)$, specified by a matrix of conditional probabilities $E(\cdot|\cdot)$, and a collection of mutually disjoint sets $\{D_j \subseteq B^n : j \in \{1, \ldots, J_n\}\}$ (decoding sets).

The average probability of the decoding error of a deterministic code $C$ is defined as

\[ P_e(C, \theta^n) := \frac{1}{J_n} \sum_{j=1}^{J_n} E(x^n|j)W_\theta^n(D_j^n|x^n). \]

Definition 2.18. Let $\mathcal{R} = \{(W_\theta, V_\theta) : \theta \in \Theta\}$ be a classical arbitrarily varying wiretap channel. An $(n, J_n)$ code for $\mathcal{R}$ consists of a stochastic encoder $E : \{1, \ldots, J_n\} \to P(A^n)$, specified by a matrix of conditional probabilities $E(\cdot|\cdot)$, and a collection of mutually disjoint sets $\{D_j \subseteq B^n : j \in \{1, \ldots, J_n\}\}$ (decoding sets).

The average probability of the decoding error of a deterministic code $C$ is defined as

\[ P_e(C, \theta^n) := \frac{1}{J_n} \sum_{j=1}^{J_n} E(x^n|j)W_\theta^n(D_j^n|x^n). \]

Definition 2.19. Let $A$ and $B$ be finite sets, and $H$ be a finite-dimensional complex Hilbert space. Let $\Theta := \{1, 2, \cdots\}$ be an index set. For every $\theta \in \Theta$, let $W_\theta$ be a classical channel $P(A) \to P(B)$ and $V_\theta$ be a classical-quantum channel $P(A) \to S(H)$. We call the set of the classical channel/classical-quantum channel pairs $\{(W_\theta, V_\theta) : \theta \in \Theta\}$ a classical arbitrarily varying quantum wiretap channel when the state $t$ varies from symbol to symbol in an arbitrary manner, while the legitimate receiver accesses the output of $W_\theta$, and the wiretapper observes the output of $V_\theta$, respectively.

Definition 2.20. Let $\mathcal{J} = \{(W_\theta, V_\theta) : \theta \in \Theta\}$ be a classical arbitrarily varying quantum wiretap channel. An $(n, J_n)$ code $C$ for the classical arbitrarily varying quantum wiretap channel $\mathcal{J}$ consists of a stochastic encoder $E : \{1, \cdots, J_n\} \to P(A^n)$, $j \to E(\cdot|j)$, specified by a matrix of conditional probabilities $E(\cdot|\cdot)$, and a collection of mutually disjoint sets $\{D_j \subseteq B^n : j \in \{1, \ldots, J_n\}\}$ (decoding sets).

Definition 2.21. A non-negative number $R$ is an achievable secrecy rate for the classical arbitrarily varying quantum wiretap channel $\mathcal{J} = \{(W_\theta, V_\theta) : \theta \in \Theta\}$ under the maximal error criterion if for every $\epsilon > 0$, $\delta > 0$, $\zeta > 0$ and sufficiently large $n$ there exist an $(n, J_n)$ code $C = \{E, \{D_j : j = 1, \cdots, J_n\}\}$ such that $\log J_n > R - \delta$, and

\[ \max_{j \in \{1, \cdots, J_n\}} \max_{\theta \in \Theta} W_\theta^n(D_j^n|E(\cdot|j)) \leq \epsilon, \]  

and

\[ \max_{\theta \in \Theta^{\alpha}} \sum_{n=1}^{\alpha} (R_{uni} ; Z_{\theta^n}) \leq \zeta. \]

The supremum on achievable secrecy rates for $\mathcal{J}$ is called the secrecy capacity of $\mathcal{J}$ under the maximal error criterion, denoted by $C_{s,\text{max}}(\mathcal{J})$.

Definition 2.22. Let $\mathcal{F}$ and $\mathcal{Q}$ be quantum systems. We denote the Hilbert space of $\mathcal{F}$ and $\mathcal{Q}$ by $H^\mathcal{F}$ and $H^\mathcal{Q}$, respectively. Let $\Theta := \{1, \ldots, T\}$ be a finite set. For every $\theta \in \Theta$, let $N_\theta$ be a quantum channel $S(H^\mathcal{F}) \to S(H^\mathcal{Q})$.

We call the set of the quantum channel $\{N_\theta : \theta \in \Theta\}$ a quantum compound channel. When the channel state is $t$ and the sender inputs a quantum state $\rho^\mathcal{F} \in S(H^\mathcal{F})$ into the channel, the receiver receives an output quantum state $N_\theta(\rho^\mathcal{F}) \in S(H^\mathcal{Q})$.

Definition 2.23. An $(n, J_n)$ code $C$ for the classical-quantum compound wiretap channel $\{N_\theta : \theta \in \Theta\}$ consists of a stochastic encoder $E : \{1, \cdots, J_n\} \to$
\[ P(A^n), j \to E(|j) \] and a collection of positive-semidefinite operators \( \{D_j : j \in \{1, \cdots, J_n\} \} \) on \( H^\otimes n \), which is a partition of the identity.

We deal with two communication scenarios. In the first one, only the sender is informed about the index \( t \), or in other words, has CSI, where CSI is an abbreviation for “channel state information”. In the second scenario, neither sender nor receiver has any information about that index at all.

**Definition 2.24.** A non-negative number \( R \) is an achievable secrecy rate having CSI at the encoder for the compound wiretap quantum channel \( \{N_\theta : \theta \in \Theta\} \) if for every \( \epsilon > 0, \delta > 0, \zeta > 0 \) and sufficiently large \( n \) there exist a finite set \( A \), a map \( F : A \to H^\otimes n \) and an \((n, J_n)\) code \( C_\theta = (E_\theta, \{D_j^{(\theta)} : j = 1, \cdots, J_n\}) \) for each \( \theta \in \Theta \) such that \( \log J_n > R - \delta \), and

\[
\max_{\theta \in \Theta} 1 - \frac{1}{J_n} \sum_{j=1}^{J_n} \text{tr}(N_\theta^\otimes n \circ F_n(E_\theta(|j))D_j^{(\theta)}) < \epsilon ,
\]

\[
\max_{\theta \in \Theta} \chi(R_\text{uni}; Z_\theta^\otimes n) < \zeta .
\]

Here
\[
Z_\theta = \left\{V_\theta' \circ F_n(E(|i)) : i \in \{1, \cdots, J_n\}\right\} ,
\]

where \( V_\theta' \) is the channel to the environment defined by \( N_\theta \).

A non-negative number \( R \) is an achievable secrecy rate having no CSI at the encoder for the compound wiretap quantum channel \( \{N_\theta : \theta \in \Theta\} \) if for every \( \epsilon > 0, \delta > 0, \zeta > 0 \) and sufficiently large \( n \) there exist an \((n, J_n)\) code \( C = (E, \{D_j : j = 1, \cdots, J_n\}) \) such that \( \log J_n > R - \delta \), and

\[
\max_{\theta \in \Theta} 1 - \frac{1}{J_n} \sum_{j=1}^{J_n} \text{tr}(N_\theta^\otimes n \circ F_n(E(|j))D_j) < \epsilon ,
\]

\[
\max_{\theta \in \Theta} \chi(R_\text{uni}; Z_\theta^\otimes n) < \zeta .
\]

The supremum of all secrecy rates having CSI at the encoder is called the secrecy capacity of \( \{N_\theta : \theta \in \Theta\} \) with CSI, denoted by \( C_s,\text{csi}(\{N_\theta : \theta \in \Theta\}) \). The supremum of all secrecy rates having no CSI at the encoder is called the secrecy capacity of \( \{N_\theta : \theta \in \Theta\} \) (with no CSI), denoted by \( C_s(\{N_\theta : \theta \in \Theta\}) \).

### 3 Main Results

Our main results are included in the following theorems and corollaries:

**Theorem 3.1.** Let \( \mathcal{I} = \{N_\theta : \theta \in \Theta\} \) be an arbitrarily varying quantum channel

1) If the arbitrarily varying quantum channel \( \mathcal{I} \) is not \( L \)-symmetrizable for some \( L \in \mathbb{N} \), then the deterministic secrecy capacity under the strong code concept and under the average error criterion of \( \{N_\theta : \theta \in \Theta\} \) is given by

\[
C_s(\mathcal{I}) = \mathcal{C}(\mathcal{I}) .
\]
2) If $\mathcal{I}$ is $L$-symmetrizable for all $L \in \mathbb{N}$, then the deterministic secrecy capacity under strong code concept and under the average error criterion of $\{N_\theta : \theta \in \Theta\}$ is equal to zero.

**Corollary 3.2.** Let $\mathcal{I} = \{N_\theta : \theta \in \Theta\}$ be an arbitrarily varying quantum channel. We have

$$C_s(\mathcal{I}, r) = \mathcal{C}(\mathcal{I}) \ .$$

(17)

**Lemma 3.3.** Let $\mathcal{I} = \{N_\theta : \theta \in \Theta\}$ be an arbitrarily varying quantum channel. We have $C_{s,\max}(\mathcal{I}, r) = C_s(\mathcal{I}, r)$. In other words

$$C_{s,\max}(\mathcal{I}, r) = \mathcal{C}(\mathcal{I}) \ .$$

(18)

We distinguish here message transmission under maximal error criterion and under the average error criterion. The capacities under these two error criteria are not equal for classical arbitrarily varying channels, but equal for arbitrarily varying classical-quantum channels. The capacity formula of classical arbitrarily varying channels under maximal error criterion is still an open problem (cf. Remark 4.8).

**Theorem 3.4.** Let $\mathcal{I} = \{N_\theta : \theta \in \Theta\}$ be an arbitrarily varying quantum channel.

1) If the arbitrarily varying quantum channel $\mathcal{I}$ is not $L$-symmetrizable for some $L \in \mathbb{N}$, then the deterministic secrecy capacity under strong code concept and under the maximal error criterion of $\{N_\theta : \theta \in \Theta\}$ is given by

$$C_{s,\max}(\mathcal{I}) = \mathcal{C}(\mathcal{I}) \ .$$

(19)

2) If $\mathcal{I}$ is $L$-symmetrizable for all $L \in \mathbb{N}$, then the deterministic secrecy capacity under strong code concept and the maximal error criterion of $\{N_\theta : \theta \in \Theta\}$ is equal to zero.

**Remark 3.5.** Theorem 3.4 states that when an arbitrarily varying quantum channel is not $L$-symmetrizable for some $L \in \mathbb{N}$, then secret message transmission is possible even when the coding scheme of the legal transmitters is known by the jammer and the eavesdropper.

Theorem 3.4 states that when an arbitrarily varying quantum channel is not $L$-symmetrizable for some $L \in \mathbb{N}$, then secret message transmission is possible even when the coding scheme of the legal transmitters is known by the jammer and the eavesdropper and, additionally, the jammer know the actual message the legal channel users want to communicate (cf. 2.9).

**Corollary 3.6.** Let $\Theta$ be a finite set and $\mathcal{J} = \{N_\theta, V_\theta : \theta \in \Theta\}$ be a classical arbitrarily varying quantum wiretap channel. If $\mathcal{J}$ is not symmetrizable, then

$$C_{s,\max}(\mathcal{J}) = \lim_{n \to \infty} \frac{1}{n} \left( \max_{U \to A^n \to \{B_q^n, Z_{g^n}, q^n\}} \min_{q \in P(\Theta)} I(p_U, \hat{B}_q^n) - \max_{\theta \in \Theta^n} \chi(p_U; Z_{\theta^n}) \right) .$$

(20)
Here $\hat{B}_0$ are the resulting classical random variables at the output of the legitimate receiver’s channels and $Z_{0n}$ are the resulting quantum states at the output of wiretap channels. The maximum is taken over all random variables that satisfy the Markov chain relationships: $U \rightarrow A^n \rightarrow \{B_q^{\otimes n}, Z_{0n} : q, \theta^n\}$ for every $\hat{B}_q \in \text{Conv}(\{B_q\}_{\theta \in \Theta})$ and $\theta \in \Theta$. $A$ is here a random variable taking values on $\mathcal{A}$, and $U$ a random variable taking values on some finite set $\mathcal{U}$ with probability distribution $p_U$.

In [21] it has been shown that the secrecy capacity of a classical arbitrarily varying channel under randomness assisted coding is continuous if the eavesdropper’s output can be described by a finite alphabet set.

In Section 5.1 we will show that the secrecy capacity of an arbitrarily varying quantum channel $\mathcal{S}$ under randomness assisted quantum coding is continuous if the receiver’s system can be described by a finite dimensional Hilbert space in the following sense:

**Corollary 3.7.** Let $\{N_0 : \theta \in \Theta\}$ be an arbitrarily varying quantum channel $\mathcal{S}(H^\mathcal{A}) \rightarrow \mathcal{S}(H^{\mathcal{Q}})$. Let $\dim \mathcal{H}^{\mathcal{Q}}$ be finite. For a positive $\delta$, let $C_\delta$ be the set of all arbitrarily varying quantum channels $\{\hat{N}_0 : \theta \in \Theta\}$ such that

$\max_{\rho \in \mathcal{S}(H^{\mathcal{Q}})} \|N_0(\rho) - \hat{N}_0(\rho)\|_1 < \delta$

for all $\theta \in \Theta$. $\| \cdot \|_1$ denotes here the trace norm.

For any positive $\epsilon$ there is a positive $\delta$ such that for all $\{\hat{N}_0 : \theta \in \Theta\} \in C_\delta$ we have

$|C_\delta(\{N_0 : \theta \in \Theta\}, r) - C_\delta(\{\hat{N}_0 : \theta \in \Theta\}), r) | \leq \epsilon$ .  \hfill (21)

**Corollary 3.8.** Let $L \in \mathbb{N}$. For a finite set $\Theta$ and an arbitrarily varying quantum channel $\{N_0 : \theta \in \Theta\}$, we define

$F_L(\{N_0 : \theta \in \Theta\})$

$:= \min_{\tau \in C(\Theta^L | \mathcal{A}^L)} \max_{a L, a' L} \left\| \sum_{\theta L \in \Theta^L} \tau(| a L \rangle | a' L \rangle) N_{0\theta L}(a' L) - \sum_{\theta L \in \Theta^L} \tau(| a L \rangle | a' L \rangle) \hat{N}_{0\theta L}(a' L) \right\|_1$, \hfill (22)

where $C(\Theta^L | \mathcal{A}^L)$ is the set of parametrized distributions sets $\{\tau(\cdot | a L \rangle : a L \in \mathcal{A}^L\} on \Theta^L$ and

$F(\{N_0 : \theta \in \Theta\}) := \sum_{L \in \mathbb{N}} \frac{1}{2L} F_L(\{N_0 : \theta \in \Theta\})$ . \hfill (23)

The statement $F_L(\{N_0 : \theta \in \Theta\}) = 0$ is equivalent to $\{N_0 : \theta \in \Theta\}$ being $L$-symmetrizable. The statement $F(\{N_0 : \theta \in \Theta\}) = 0$ is equivalent to $\{N_0 : \theta \in \Theta\}$ being $L$-symmetrizable for every $L \in \mathbb{N}$.

$C_\delta(\{N_0 : \theta \in \Theta\})$, the deterministic secrecy capacity of arbitrarily varying quantum channel is discontinuous at $\{N_0 : \theta \in \Theta\}$, if and only if the following hold:

1) The secrecy capacity of $\{N_0 : \theta \in \Theta\}$ under randomness assisted quantum coding is positive;

2) $F(\{N_0 : \theta \in \Theta\}) = 0$, but for every positive $\delta$ there is a $\{N'_{0} : \theta \in \Theta\} \in C_\delta$ such that $F(\{N'_{0} : \theta \in \Theta\}) > 0$.
Remark 3.9. The function $F$ is defined as a uniformly convergent series of continuous functions on the set of arbitrarily varying quantum channels. Thus $F$ itself is also a continuous function on the set of arbitrarily varying quantum channels.

The following Corollary 3.10 is a consequence of Corollary 3.8. Corollary 3.10 shows that the positive values of the secrecy capacity of an arbitrarily varying quantum wiretap channel are stable in the sense that when the secrecy capacity of an arbitrarily varying quantum wiretap channel takes a positive value in an interval of the domain, then all arbitrarily varying quantum wiretap channels in a sufficiently small neighborhood also have positive secrecy capacities.

Corollary 3.10. Let $\Theta$ be a finite set and $\{N_\theta : \theta \in \Theta\}$ be an arbitrarily varying quantum wiretap channel. When the secrecy capacity of $\{N_\theta : \theta \in \Theta\}$ is positive, then there is a $\delta$ such that for all $\{N'_\theta : \theta \in \Theta\} \in C_\delta$ we have

$$C_s(\{N'_\theta : \theta \in \Theta\}) > 0.$$

Corollary 3.11. The deterministic secrecy capacity of an arbitrarily varying quantum channel is in general not continuous.

Corollary 3.12. Super-activation occurs for secrecy capacities of arbitrarily varying quantum channels.

In [21] it has been shown that the secrecy capacity of a classical arbitrarily varying wiretap channel under randomness assisted coding is continuous in the sense of the following Lemma:

Lemma 3.13. For a classical arbitrarily varying wiretap channel $\{(W_\theta, V_\theta) : \theta \in \Theta\}$, where $W_\theta : P(A) \to P(B)$ and $V_\theta : P(A) \to P(C)$, and a positive $\delta$ let $C_\delta$ be the set of all classical arbitrarily varying wiretap channels $\{(W'_\theta, V'_\theta) : \theta \in \Theta\}$, where $W'_\theta : P(A) \to P(B)$ and $V'_\theta : P(A) \to P(C)$, such that

$$\max_{a \in A} \|W_\theta(a) - W'_\theta(a)\|_1 < \delta$$

and

$$\max_{a \in A} \|V_\theta(a) - V'_\theta(a)\|_1 < \delta$$

for all $\theta \in \Theta$.

When $|A|$ is finite, then for any positive $\epsilon$ there is a positive $\delta$ such that for all $\{(W'_\theta, V'_\theta) : \theta \in \Theta\} \in C_\delta$ we have

$$|C_s(\{(W_\theta, V_\theta) : \theta \in \Theta\}; r) - C_s(\{(W'_\theta, V'_\theta) : \theta \in \Theta\}; r)| \leq \epsilon. \quad (24)$$

However, the proof for Lemma 3.13 in [21] requires the outputs of the eavesdropper’s channel to be include in a finite alphabet. Since in general, the legal channel users do not have control over the the eavesdropper’s channel, this proof is still capable of improvements nonetheless. We will give an alternative proof
for Lemma 3.13 such that the continuity does not depend on the alphabet of the eavesdropper.

In our earlier work [14] we determined the secrecy capacity of the classical-quantum compound wiretap channel. Now we are going to consider the secrecy capacity of the compound wiretap quantum channel.

**Corollary 3.14.** The secrecy capacity of the compound quantum channel \( \{ N_\theta : \theta \in \Theta \} \) in the case with CSI is given by

\[
C_{S,CSI}(\{ N_\theta : \theta \in \Theta \}) = \min_{\theta \in \Theta} \lim_{n \to \infty} \frac{1}{n} \max_{U \to A \to \{(BZ)_{\theta} \}} \chi(p_U; B_\theta^n) - \chi(p_U; Z_\theta^n).
\]

(25)

Here \( B_\theta \) are the resulting random variables at the output of legal receiver channels, and \( Z_\theta \) are the resulting random quantum states at the output of wiretap channels.

The secrecy capacity of the compound quantum channel \( \{ N_\theta : \theta \in \Theta \} \) in the case with CSI is given by

\[
C_S(\{ N_\theta : \theta \in \Theta \}) = \lim_{n \to \infty} \frac{1}{n} \max_{U \to A \to \{(BZ)_{\theta} \}} \left( \min_{\theta \in \Theta} \chi(p_U; B_\theta^n) - \max_{\theta \in \Theta} \chi(p_U; Z_\theta^n) \right).
\]

(26)

4 Complete Characterization of Secrecy Capacity of Quantum Channels

4.1 Previous Works and the Strong Code Concept

In our previous works [15], [16], and [17] we considered that the sender’s encoding is restricted to transmitting an indexed finite set of quantum states \( \{ \rho_x : x \in A \} \subset \mathcal{S}(G) \) as a component of the channel. We obtained a channel \( \sigma_x := N(\rho_x) \) with classical inputs \( x \in A \) and quantum outputs, which we call a classical-quantum channel.

In [15], the Ahlswede Dichotomy for arbitrarily varying classical-quantum wiretap channels has been established, i.e. either the deterministic capacity of an arbitrarily varying channel was zero or equal to its shared randomness assisted capacity. Our proof was similar to the proof of the Ahlswede Dichotomy for arbitrarily varying classical-quantum channels in [4]: We built a two-part code word, the first part was used to create randomness for the sender and the legal receiver, the second was used to transmit the message to the legal receiver. Here we use the weak code concept (cf. Definition 2.13).

**Lemma 4.1 (Ahlswede Dichotomy under weak code concept).** Let \( \mathcal{R} = \{ (W_\theta, V_\theta) : \theta \in \Theta \} \) be an arbitrarily varying classical-quantum wiretap channel.

1. If the arbitrarily varying classical-quantum channel \( \{ W_\theta : \theta \in \Theta \} \) is not symmetrizable, then

\[
C_\ast(\mathcal{R}) = C_s(\mathcal{R}; r).
\]

(27)
2. If \( \{W_\theta : \theta \in \Theta\} \) is symmetrizable,

\[
C_s^*(\mathcal{R}) = 0 .
\]  

(28)

Here \( C_s^*(\mathcal{R}) \) and \( C_s(\mathcal{R}; r) \) are the secrecy capacity under weak code concept and random assisted secrecy capacity of \( \mathcal{R} \), respectively (cf. [15] and [17]).

We also analyzed the secrecy capacity when the sender and the receiver used various resources. In [16] we determined the secrecy capacities under randomness assisted coding of arbitrarily varying classical-quantum wiretap channels.

**Lemma 4.2.** Let \( \Theta := \{1, \cdots, T\} \) be a finite index set. Let \( \mathcal{L} = (W_\theta, V_\theta)_{\theta \in \Theta} \) be an arbitrarily varying classical-quantum wiretap channel. We have

\[
C_s(\mathcal{L}; r) = C(\mathcal{L}) .
\]  

(29)

We also examined in [16] when the secrecy capacity is a continuous function of the system parameters. Furthermore, we proved the phenomenon “super-activation” for arbitrarily varying classical-quantum wiretap channels. Combining the results of these two papers we obtain the formula for deterministic secrecy capacity of the arbitrarily varying classical-quantum wiretap channel.

However, that formula is still capable of improvement when we explicitly allow the eavesdropper to have a small part of the code word be non-secure. This reduces the generality of the code concept. The code word we built was a composition of a public code word to synchronize the second part and a randomness assisted code word to transmit the message. We only required security for the last part. As we have shown in [17], when the jammer had access to the first part, the code would be rendered completely useless. Thus the code concept only works when the jammer is limited in his action, e.g., when the eavesdropper cannot send messages towards the jammer. Nevertheless, this code concept with weak criterion could be useful when a small number of public messages were desired, e.g. when the receiver used it to estimate the channels.

For classical arbitrarily varying wiretap channels the authors of [34] developed a new method to overcome this problem: Applying a technique introduced in [23], they made the first part secure and used it to send the message instead of just the randomness. The code they constructed is thus a one-part deterministic secure code. However, it is technically difficult to extend the random classical code technique introduced in [23] to classical-quantum channels, thus we have to come up with a different construction.

Therefore, in [17] we considered a general code concept when we constructed a code in such a way that every part of it is secure. We call it the strong code concept (cf. Definition 2.13). The main results of [17] are included in the following two lemmata:

**Lemma 4.3.** Let \( \mathcal{L} = (W_\theta, V_\theta)_{\theta \in \Theta} \) be an arbitrarily varying classical-quantum wiretap channel. If the arbitrarily varying classical-quantum channel \( \{W_\theta : \theta \in \Theta\} \) is not symmetrizable, then

\[
C_s(\mathcal{L}) = C(\mathcal{L}) ,
\]  

(30)
when we use a two-part code word where both parts are secure.

Here \( B_\theta \) are the resulting quantum states at the output of the legitimate receiver’s channels, \( Z_\theta \) are the resulting quantum states at the output of wiretap channels. The maximum is taken over all random variables that satisfy the Markov chain relationships: \( U \to A \to B_\theta \) for every \( B_\theta \in \text{Conv}(B_\theta) \) and \( \theta \in \Theta \). Here \( A \) is a random variable taking values on \( A \), and \( U \) a random variable taking values on some finite set \( U \) with probability distribution \( p_U \).

**Lemma 4.4 (Ahlswede Dichotomy under strong code concept).** Let \( \Theta \) be a finite set and \( \leq = \{(W_\theta, V_\theta) : \theta \in \Theta\} \) be an arbitrarily varying classical-quantum wiretap channel.

1) If the arbitrarily varying classical-quantum channel \( \{W_\theta : \theta \in \Theta\} \) is not symmetrizable, then

\[
C_s(\leq) = C_s(\leq; r). \tag{31}
\]

2) If \( \{W_\theta : \theta \in \Theta\} \) is symmetrizable, then

\[
C_s(\leq) = 0. \tag{32}
\]

Here \( C_s(\leq) \) is the secrecy capacity under the strong code concept (cf. [17]).

These lemmata show that when the legal channel is not symmetrizable, the sender can send a small number of secure transmissions which push the secure capacity to the maximally attainable value. Thus, complete security is granted.

### 4.2 Proof of the Main Results

Corollary 3.2 follows immediately from the definition of the randomness assisted secrecy capacity and Lemma 4.4.

The following proof of Corollary 3.6 is almost exact the same as our proof of the capacity formula of classical arbitrarily varying quantum wiretap channels in [16], when we apply the coding technique of [18] for the maximal error criterion instead of coding techniques for the average error criterion.

**Proof.** We fix a probability distribution \( p \in P(A) \) and choose an arbitrarily positive \( \delta \). Let

\[
J_n = \left[ 2^{\inf_{\theta \in \Theta} \chi(p; Z_\theta)} - \max_{\theta \in \Theta} \chi(p; Z_\theta) - n\delta \right] ,
\]

and

\[
L_n = \left[ 2^{\max_{\theta \in \Theta} \chi(p; Z_\theta) + n\delta} \right] .
\]

Let \( p'(x^n) := \begin{cases} p^n(x^n) / p^n(T_{p,\delta}) & \text{if } x^n \in T_{p,\delta} \\ 0 & \text{else} \end{cases} \) and \( X^n := \{X_{j,l} \}_{j \in \{1, \ldots, J_n\}, l \in \{1, \ldots, L_n\}} \) be a family of random matrices whose components are i.i.d. according to \( p' \).

By [18], [4] and the Alternative Covering Lemma in [16], if \( n \) is sufficiently large with a positive probability there exist a realization \( \{x_{j,l} \}_{j \in \{1, \ldots, J_n\}, l \in \{1, \ldots, L_n\}} \)
of $X^n$, a set of mutually disjoint sets $\{D_{j,l} : j \in \{1, \cdots, J_n\}, l \in \{1, \cdots, L_n\}\}$ on $B^n$ such that for all positive $\epsilon, \lambda \theta^n \in \Theta^n, j \in \{1, \cdots, J_n\}, \text{ } \text{ and } l \in \{1, \cdots, L_n\}$

$$W_{\theta^n}(D_{j,l} | x_{j,l}) \leq \epsilon , \quad (33)$$

and

$$\chi (R_{uni}; Z_{\theta^n}) \leq \lambda . \quad (34)$$

The following proof of Corollary 3.3 is similar to our proof of the formula for randomness assisted capacity of classical arbitrarily varying quantum wiretap channels.

Proof. When we apply the coding technique of [18] where it has been shown that the randomness assisted capacity of an arbitrarily varying quantum channel under the maximal error criterion is equal to its the randomness assisted capacity under the average error criterion, and the Alternative Covering Lemma in [16] to our proof for the capacity formula of classical arbitrarily varying quantum wiretap channels in [16], we obtain: If $n$ is sufficiently large with a positive probability there exist an $$(n, J_n)$$ code $C_{\gamma} = (E_{\gamma}, \{D_{\gamma j,l} : j \in \{1, \cdots, J_n\}, l \in \{1, \cdots, L_n\}\})$ for $\gamma = 1, \cdots, n^3$ and a $F$ such that for all positive $\epsilon, \lambda \theta^n \in \Theta^n, j \in \{1, \cdots, J_n\}, \text{ and } l \in \{1, \cdots, L_n\}$

$$1 - \frac{1}{n^3} \sum_{\gamma=1}^{n^3} N_{\theta^n} \circ F^n(D_{\gamma j,l} | E^n(\cdot | j, l)) \leq \epsilon , \quad (35)$$

and

$$\frac{1}{n^3} \sum_{\gamma=1}^{n^3} \chi (R_{uni}; Z_{C_{\gamma}, \theta^n}) \leq \lambda . \quad (36)$$

Here for $\theta^n \in \Theta^n$ and $C_{\gamma} = \{(w(j)^{n,\gamma}, D_{\gamma j}) : j = 1, \cdots, J_n\}$, $Z_{C_{\gamma}, \theta^n} := \{V_{\theta^n}(w(1)^{n,\gamma}), V_{\theta^n}(w(2)^{n,\gamma}), \cdots, V_{\theta^n}(w(n)^{n,\gamma})\}$.

Now we will deliver the proof for Theorem 3.1

Proof. i) Proof of 2)

In [19], the following was shown: When $I$ is $L$-symmetrizable for all $L \in \mathbb{N}$, then for any chosen $A$ and $F : A \rightarrow H^P$, the arbitrarily varying classical-quantum channel $\{N_\theta \circ F : \theta \in \Theta\}$ is symmetrizable. By Lemma 4.4, the secrecy capacity concept of $\{N_\theta : \theta \in \Theta\}$ with any classical input is equal to zero. Thus 2) holds.

ii) Converse for 1)

Now let us assume that there is a $L' \in \mathbb{N}$ such that $I$ is $L'$-symmetrizable.

We fix a finite set $A$, and a map $F : A \rightarrow H^P$. By Lemma 4.4 the secrecy capacity under strong code for the arbitrarily varying classical-quantum wiretap
channel \{(N_\theta \circ F, V_\theta' \circ F) : \theta \in \Theta\} under strong code concept cannot exceed 
\limsup_{n \to \infty} \frac{1}{n} \sup_{p} \inf_{q \in P(\Theta)} (\chi(P, B^n_\theta) - \max_{\theta' \in \Theta} \chi(P, Z_{\theta'})). Thus
\[ C_s(\mathcal{J}) \leq \limsup_{n \to \infty} \frac{1}{n} \sup_{A,F,P} \left( \inf_{q \in P(\Theta)} \chi(P, B^n_\theta) - \max_{\theta' \in \Theta} \chi(P, Z_{\theta'}) \right). \tag{37} \]

iii) Achievement for 1)

We assume that there is a \( L' \in \mathbb{N} \) such that \( \mathcal{J} \) is not \( L' \)-symmetrizable.

When
\[ \limsup_{n \to \infty} \frac{1}{n} \sup_{A,F,p} \left( \inf_{q \in P(\Theta)} \chi(P, B^n_\theta) - \max_{\theta' \in \Theta} \chi(P, Z_{\theta'}) \right) \leq 0 \]
holds, we have \( C_s(\mathcal{J}) = 0 \) by (37), and there is nothing to prove.

Now we assume there is a finite set of letter \( \mathcal{A}' \), a map \( F' : \mathcal{A}' \to \mathcal{S}(H) \), and a distribution \( p' \) on \( \{F'(x) : x \in \mathcal{A}'\} \) such that for sufficiently large \( n \) we have
\[ \frac{1}{n} \inf_{B' \in \text{Conv}(B_q \circ a)_{a \in \Theta}} \left( \chi(p'; B'^{\otimes n}_q) - \max_{\theta' \in \Theta} \chi(p'; Z'_{\theta'}) \right) > 0, \tag{38} \]
where \( B'_{\theta} \) and \( Z'_{\theta} \) are the resulting quantum states at the outputs of \( N_\theta \circ F' \) and \( V'_\theta \circ F' \), respectively.

In [19] a technique has been introduced to construct an arbitrarily varying classical-quantum channel by means of an arbitrarily varying quantum channel. However this technique does not work for the classical arbitrarily varying quantum wiretap channel since it cannot provide security. We have to find a more sophisticated way.

a) Definition of an arbitrarily varying classical-quantum channel which is not symmetrizable

When \( \{N_\theta : \theta \in \Theta\} \) is not \( L' \)-symmetrizable, then it is also not \( L \)-symmetrizable for all \( L > L' \) (cf. [19]). We choose a \( L \geq L' \) such that
\[ \frac{1}{L} \inf_{B' \in \text{Conv}(B'_q \circ a)_{a \in \Theta}} \left( \chi(p'; B'^{\otimes L}_q) - \max_{\theta' \in \Theta} \chi(p'; Z'_{\theta'}) \right) = C_1 > 0. \tag{39} \]

We now combine the idea of [19] and the trick we used for the proof of Lemma 4.3 in [17] to define a set of classical-quantum channels.

We denote the dimension of \( H^3 \) by \( d' \). Now choose arbitrarily \( dL^2 \) density operators \( \tilde{M}_i, i = 1, \ldots, dL^2 \) which span the space of Hermitian operators on \( H^3 \). We define a new set of letters \( \mathcal{A}_1 := \mathcal{A}' \cup \{1, \ldots, d^2\} \) and a map \( F : \mathcal{A}_1 \to \mathcal{S}(H) \) by
\[ F(a) = \begin{cases} F'(a) & \text{if } a \in \mathcal{A}'; \\ \tilde{M}_a & \text{if } a \in \{1, \ldots, d^2\}. \end{cases} \]

When \( \{N_{\theta L} \circ F_{\theta L} : \theta L \in \Theta^L\} \) is symmetrizable then there is a \( \{\tau(\cdot | aL) \circ aL \in U^L\} \) on \( \Theta^L \) such that
\[ \sum_{\theta \in \Theta^L} \tau(\theta L | aL)N_{\theta L} \circ F_{\theta L}(aL) = \sum_{\theta \in \Theta^L} \tau(\theta L | aL)N_{\theta L} \circ F_{\theta L}(aL) \]
\[ (\text{38}) \]
\[ (\text{39}) \]
\[ (\text{37}) \]
for all $a, a' \in A_1$.

This implies that

$$
\sum_{\theta L \in \Theta L} \tau(\theta L | i L) N_{\theta L}(M_i) = \sum_{\theta L \in \Theta L} \tau(\theta L | i' L) N_{\theta L}(M_{i'})
$$

for all $i, i' \in \{1, \ldots, d L^2\}$.

Since $\{M_i : i = 1, \ldots, d L^2\}$ spans the space of Hermitian operators on $H^{\Theta L}$, $\{N_{\theta L} : \theta L \in \Theta L\}$ is $L$-symmetrizable. This is a contradiction to our assumption. Therefore $\{N_{\theta L} \circ F L : \theta L \in \Theta L\}$ is not symmetrizable.

b) The secure transmission of the message with a deterministic code

We define a distribution $p$ on $\{F L(a L) : a L \in A_1^L\}$ by

$$
p(F L(a L)) = \begin{cases} p'(F L(a L)) & \text{if } a L \in A_1^L, \\ 0 & \text{else}. \end{cases}
$$

By (39)

$$
\frac{1}{L} \left( \inf_{B'_q \in \text{Conv}((B'_q)_{\theta \in \Theta})} \chi(p; B'_q) - \max_{\theta L \in \Theta L} \chi(p; Z_{\theta L}) \right)
= \frac{1}{L} \left( \inf_{B'_q \in \text{Conv}((B'_q)_{\theta \in \Theta})} \chi(p'; B'_q) - \max_{\theta L \in \Theta L} \chi(p'; Z_{\theta L}) \right)
= C_1, \tag{40}
$$

where $B_{\theta}$ and $Z_{\theta}$ are the resulting quantum states at the outputs of $N_{\theta} \circ F$ and $V_{\theta} \circ F$, respectively.

We apply block coding and regarding $L$ uses of the quantum channel as a single quantum channel. Since $\{N_{\theta} \circ F L : \theta L \in \Theta L\}$ is not symmetrizable, by Lemma 4.3 (40) implies that

$$
C_s (\{(N_{\theta} \circ F L, V_{\theta} \circ F L) : \theta L \in \Theta L\}) = C_1 > 0.
$$

Since $(\log n)^2 \gg 3 \log n$ we can build a $((\log n)^2, n^3)$ code $(\hat{E}_L(\log n)^2, \hat{D}_L(\log n)^2 : i \in \{1, \ldots, n^3\})$ such that for any positive $\varepsilon$ when $n$ is sufficiently large we have

$$
1 - \min_{\theta L(\log n)^2 \in \hat{E}_L(\log n)^2} \min_{i \in \{1, \ldots, n^3\}} N_{\theta L(\log n)^2} \circ F L(\log n)^2 \left( \hat{E}_L(\log n)^2 (\cdot | i) \right) \hat{D}_L(\log n)^2 \\
\leq \varepsilon \tag{41}
$$

and

$$
\max_{\theta L(\log n)^2 \in \hat{E}_L(\log n)^2} \left\| V_{\theta L(\log n)^2} \circ F L(\log n)^2 \left( \hat{E}_L(\log n)^2 (\cdot | i) \right) - \Xi_{\theta L(\log n)^2} \right\|_1 \leq \varepsilon, \tag{42}
$$

where $\Xi_{\theta L(\log n)^2}$ is a quantum state which is independent of $i$ (cf. [14]).

**Remark 4.5.** Note that each code word of this $((\log n)^2, n^3)$ secret deterministic code itself is actually a composition of a $((\log \log n)^3, (\log n)^3)$ secret deterministic code word and a $((\log n)^2 - (\log \log n)^3, n^3)$ secret random code word (cf. [17]).
Recall that by (40),
\[
\frac{1}{n} \left\{ \inf_{B_q \in \text{Conv}((B_q)_{q \in \Theta})} \chi(p; B_q^\otimes n) - \max_{\theta \in \Theta_n} \chi(p; Z_\theta) \right\} = \frac{1}{n} \left\{ \inf_{B_q' \in \text{Conv}((B_q')_{q \in \Theta})} \chi(p'; B_q'^\otimes n) - \max_{\theta \in \Theta_n} \chi(p'; Z_\theta') \right\}
\]
where $B_\theta$ and $Z_\theta$ are the resulting quantum states at the outputs of $N_\theta \circ F$ and $V^\theta_\rho \circ F$, respectively.

We choose an arbitrary positive $\delta$. Let
\[
J_n = \frac{1}{n} \left\{ \inf_{B_q \in \text{Conv}((B_q)_{q \in \Theta})} \chi(p; B_q^\otimes n) - \max_{\theta \in \Theta_n} \chi(p; Z_\theta) \right\} - \delta.
\]

By Lemma 4.2 (cf. [16] for details), if $n$ is sufficiently large we can construct an $(n, J_n)$ randomness assisted quantum code $\left\{ \left( E^n, \{ D^n_{j,i} : j \in \{1, \ldots, J_n\} \} \right) : i \in \{1, \ldots, n^3\} \right\}$, and positive $\lambda$, $\zeta$, such that for all $\theta \in \Theta^n$
\[
\frac{1}{n} \frac{1}{J_n} \sum_{j=1}^{J_n} \sum_{\pi \in S_n} \sum_{i=1}^{n^3} \text{tr} \left( (N_\theta \circ F^n (\pi(E^n(\cdot|j))) P_{\pi_i} D^n_{j,i} P^n_{\pi_i} ) \right) \geq 1 - 2^{-n^{1/16}\lambda}, \tag{43}
\]
and for all $\theta \in \Theta^n$, $j \in \{1, \ldots, J_n\}$ and all $i \in \{1, \ldots, n^3\}$
\[
\| V^\theta_\rho \circ F^n (\pi(E^n(\cdot|j))) - P_{\pi_i} \Xi_{\pi_i^{-1}(\theta_\rho)} P^n_{\pi_i} \|_1 < 2^{-\sqrt{n}\zeta}, \tag{44}
\]
where $\Xi_{\theta_\rho} \in \mathcal{S}(H^n)$ is a quantum state which is independent of $j$ and $i$ (cf. [17]).

Using the technique of Lemma 4.1 (cf. [15] for details) to reduce the amount of randomness if $n$ is sufficiently large, we can find a set $\{\pi_1, \ldots, \pi_{n^3}\} \subset S_n$ such that
\[
\frac{1}{n} \frac{1}{J_n} \sum_{i=1}^{n^3} \sum_{j=1}^{J_n} \text{tr} \left( (N_\theta \circ F^n (\pi_i(E^n(\cdot|j))) P_{\pi_i} D^n_{j,i} P^n_{\pi_i} ) \right) \geq 1 - 2^{-n^{1/16}\lambda}, \tag{45}
\]
and for all $\theta \in \Theta^n$, $j \in \{1, \ldots, J_n\}$ and all $i \in \{1, \ldots, n^3\}$
\[
\| V^\theta_\rho \circ F^n (\pi_i(E^n(\cdot|j))) - P_{\pi_i} \Xi_{\pi_i^{-1}(\theta_\rho)} P^n_{\pi_i} \|_1 < 2^{-\sqrt{n}\zeta}, \tag{46}
\]
where $\Xi_{\theta_\rho} \in \mathcal{S}(H^n)$ is a quantum state which is independent of $j$ and $i$ (cf. [17]).

Furthermore, by the permutation-invariance of $p$ we also have $\Xi_{\theta_\rho} = P_{\pi_i} \Xi_{\pi_i(\theta_\rho)} P^n_{\pi_i}$ for all $\pi \in S_n$.

We now define our secure $(L \log n)^2 + n, J_n + n^3)$ code for $\{(N_\theta \circ F, V^\theta_\rho \circ F) : \theta \in \Theta \}$ by
\[
E^{(L \log n)^2 + n} \{ (a^{L \log n})^2 + n \mid i, j \} := \hat{E}(L \log n)^2 \left(a^{L \log n}\right)^2 (a^{L \log n})^2 \cdot E^n(\pi_i(a^n)|j), \tag{47}
\]
for every $a^{(\log n)^{3+n}} = \{a^{(\log n)^{3}}, a^n\} \in U^{(\log n)^{3+n}}$ and

$$D^{(\log n)^{3+n}}_{i,j} := \hat{D}^{(\log n)^{3}}_i \otimes (P_{\pi, D^n_j} P^\dagger_{\pi, i}) \ . \quad (48)$$

By (41) and (45), for every $\theta^{L(\log n)^{2+n}} = (\theta^{L(\log n)^{2}}, \theta^n) \in G^{L(\log n)^{2+n}}$, we have

$$\frac{1}{n^3} \sum_{i=1}^{n^3} \sum_{j=1}^{J_n} \sum_{i=1}^{J_n} \text{tr} \left( N_{\theta^{L(\log n)^{2}}} \circ F^{L(\log n)^{2}}(\hat{E}^{L(\log n)^{2}}(\cdot | i)) \hat{D}^{(\log n)^{2}}_i \right)$$

$$= \frac{1}{n^3} \sum_{i=1}^{n^3} \sum_{j=1}^{J_n} \sum_{i=1}^{J_n} \text{tr} \left( \left[ N_{\theta^{L(\log n)^{2}}} \circ F^{L(\log n)^{2}}(\hat{E}^{L(\log n)^{2}}(\cdot | i)) \hat{D}^{(\log n)^{2}}_i \right] \right)$$

$$= \frac{1}{n^3} \sum_{i=1}^{n^3} \text{tr} \left( \left[ N_{\theta^{L(\log n)^{2}}} \circ F^{L(\log n)^{2}}(\hat{E}^{L(\log n)^{2}}(\cdot | i)) \hat{D}^{(\log n)^{2}}_i \right] \right)$$

$$\geq 1 - \frac{1}{n^{4/16}} 2^n - 2 \cdot 2^{-n^{1/16}} \lambda$$

$$\geq 1 - \varepsilon \quad (49)$$

for any positive $\varepsilon$ when $n$ is sufficiently large.

By (42) and (46), for every $\theta^{L(\log n)^{2+n}} = (\theta^{L(\log n)^{2}}, \theta^n) \in G^{L(\log n)^{2+n}}$ and $i \in \{1, \ldots, n^3\}$ and $j \in \{1, \ldots, J_n\}$, we have

$$\|V'_{\theta^{L(\log n)^{2+n}}} \circ F^{L(\log n)^{2+n}}(\hat{E}^{L(\log n)^{2+n}}(\cdot | i, j)) - \Xi_{\theta^{L(\log n)^{2}}} \otimes \Xi_{\theta^n}\|_1$$

$$= \|V'_{\theta^{L(\log n)^{2}}} \hat{E}^{L(\log n)^{2}}(\cdot | i) \otimes V'_{\pi^n}(\pi(E^n(\cdot | j))) - \Xi_{\theta^{L(\log n)^{2}}} \otimes \Xi_{\theta^n}\|_1$$

$$< \frac{1}{\sqrt{n}} 2^n + 2 \cdot 2^{-n^{3/4}} \ . \quad (50)$$

**Lemma 4.6 (Fannes-Audenaert Ineq., cf. [26, 3]).** Let $\Phi$ and $\Psi$ be two quantum states in a $d$-dimensional complex Hilbert space and $\|\Phi - \Psi\| \leq \mu < \frac{1}{2}$, then

$$|S(\Phi) - S(\Psi)| \leq \mu \log(d - 1) + h(\mu) \ , \quad (51)$$

where $h(\nu) := -\nu \log \nu - (1 - \nu) \log(1 - \nu)$ for $\nu \in [0, 1]$.  

26
The Fannes Inequality was first introduced in [26], where it has been shown that \(|S(X) - S(Y)| \leq \mu \log d - \mu \log \mu\). In [6] the result of [26] has been improved, and it has been proved.

Let \(R_n\) be the uniform distribution on \(\{1, \cdots, n^3\}\). We define a random variable \(R_{n, uni}\) on the set \(\{1, \cdots, n^3\} \times \{1, \cdots, R_n\}\) by \(R_{n, uni} := R_n \times R_{uni}\). Applying Lemma 4.6 we obtain

\[
\frac{\max}{gL(\log n)^2 + n \in gL(\log n)^2 + n} \chi \left( R_n^3, j_n ; Z_{gL(\log n)^2 + n} \right)
\leq \frac{\max}{gL(\log n)^2 + n \in gL(\log n)^2 + n} \chi \left( R_n^3, Z_{gL(\log n)^2 + n} \right)
\]

\[
+ \frac{1}{n^3} \sum_{i=1}^{n^3} \max_{\theta^n \in \theta^n} \chi \left( R_{uni} ; V'_{gL(\log n)^2} \left( \hat{E}L(\log n)^2 \left( \cdot \right) \right) \otimes Z_{\theta^n, \pi_i} \right)
\]

\[
= \frac{\max}{gL(\log n)^2 + n \in gL(\log n)^2 + n} \left( S \left( \frac{1}{n^3} \sum_{i=1}^{n^3} \sum_{j=1}^{J_n} V'_{gL(\log n)^2 + n} \circ F_{gL(\log n)^2 + n} \left( \cdot \mid i, j \right) \right) \right)
\]

\[
- \frac{1}{n^3} \sum_{i=1}^{n^3} S \left( \frac{1}{J_n} \sum_{j=1}^{J_n} V'_{gL(\log n)^2 + n} \circ F_{gL(\log n)^2 + n} \left( \cdot \mid i, j \right) \right)
\]

\[
\leq \frac{\max}{gL(\log n)^2 + n \in gL(\log n)^2 + n} \left( S \left( \frac{1}{n^3} \sum_{i=1}^{n^3} \sum_{j=1}^{J_n} V'_{gL(\log n)^2 + n} \circ F_{gL(\log n)^2 + n} \left( \cdot \mid i, j \right) \right) \right)
\]

\[
- \left| \Xi_{gL(\log n)^2} \otimes \Xi_{\theta^n} \right|
\]

\[
+ \left| \Xi_{gL(\log n)^2} \otimes \Xi_{\theta^n} \right|
\]

\[
+ \frac{1}{n^3} \sum_{i=1}^{n^3} S \left( \frac{1}{J_n} \sum_{j=1}^{J_n} V'_{gL(\log n)^2 + n} \circ F_{gL(\log n)^2 + n} \left( \cdot \mid i, j \right) \right)
\]

\[
\leq \frac{\max}{gL(\log n)^2 + n \in gL(\log n)^2 + n} \left( S \left( \frac{1}{J_n} \sum_{j=1}^{J_n} V'_{gL(\log n)^2 + n} \circ F_{gL(\log n)^2 + n} \left( \cdot \mid i, j \right) \right) \right)
\]

\[
\otimes \left( V'_{\theta^n} \circ F^n \left( \pi_i \left( E^n \left( \cdot \mid j \right) \right) \right) \right)
\]

\[
- \frac{1}{J_n} \sum_{j=1}^{J_n} \left( V'_{gL(\log n)^2 + n} \circ F_{gL(\log n)^2 + n} \left( \cdot \mid i, j \right) \right) \otimes \left( V'_{\theta^n} \circ F^n \left( \pi_i \left( E^n \left( \cdot \mid j \right) \right) \right) \right)
\]

\[
- \left| V'_{gL(\log n)^2 + n} \circ F_{gL(\log n)^2 + n} \left( \cdot \mid i, j \right) \right| \otimes \Xi_{\theta^n}
\]

\[
+ \left| V'_{gL(\log n)^2 + n} \circ F_{gL(\log n)^2 + n} \left( \cdot \mid i, j \right) \right| \otimes \Xi_{\theta^n}
\]

\[
\leq \frac{\max}{gL(\log n)^2 + n \in gL(\log n)^2 + n} \left( S \left( \frac{1}{J_n} \sum_{j=1}^{J_n} V'_{gL(\log n)^2 + n} \circ F_{gL(\log n)^2 + n} \left( \cdot \mid i, j \right) \right) \right)
\]

\[
- \left| V'_{gL(\log n)^2 + n} \circ F_{gL(\log n)^2 + n} \left( \cdot \mid i, j \right) \right| \otimes \Xi_{\theta^n}
\]

\[
+ \left| V'_{gL(\log n)^2 + n} \circ F_{gL(\log n)^2 + n} \left( \cdot \mid i, j \right) \right| \otimes \Xi_{\theta^n}
\]

\[
\leq 27
\]
\[-\frac{1}{J_n} \sum_{j=1}^{J_n} S\left(V_{\theta,\pi(L\log n)^2}^{\log n} \circ P^{(L\log n)^2} (E^{(L\log n)^2} (\cdot | i)) \otimes (V_{\theta,\pi(L\log n)^2}^{\log n} (E^{(L\log n)^2} (\cdot | j)))\right)\]
\[\leq \left(\frac{1}{\sqrt{n}} 2^\epsilon + 2 \cdot 2^{-\sqrt{n} \epsilon} \right) \log (d^{(L\log n)^2} - 1) + h\left(\frac{1}{\sqrt{n}} 2^\epsilon + 2 \cdot 2^{-\sqrt{n} \epsilon}\right) + 2 \cdot 2^{-\sqrt{n} \epsilon} \log (d^n - 1) + h(2 \cdot 2^{-\sqrt{n} \epsilon}) \leq \epsilon \]
\[\text{(52)}\]

for any positive \(\epsilon\) when \(n\) is sufficiently large. Here \(Z_{\theta,\pi}\) denotes the resulting quantum state at \(V_{\theta,\pi}^{\log n}\) after \(i \in \{1, \cdots, n^3\}\) has been sent with \(E^{(L\log n)^2}\).

For any positive \(\delta\), if \(n\) is sufficiently large, we have \(\frac{1}{n} \log J_n - \frac{1}{L,\log n\log n + n} \log J_n \leq \delta\). Thus
\[C_s(\mathcal{J}) \geq \limsup_{n \to \infty} \frac{1}{n} \left( \sup_{A, F, P} \inf_{q \in P(\Theta)} \chi(P, B_q^n) - \max_{\theta^n \in \Theta^n} \chi(P, Z_{\theta^n}) \right) - 2\delta \]  
\[\text{(53)}\]

Next we will deliver the proof for Theorem 3.4

**Proof.** Let \(\Theta := \{1, \cdots, T\}\) be a finite index set. Let \(\{N_{\theta}, V_{\theta}'\} : \theta \in \Theta\) be an arbitrarily varying wiretap quantum channel defined by an arbitrarily varying quantum channel \(\mathcal{J} = \{N_{\theta} : \theta \in \Theta\}\).

\[C_s(\mathcal{J}) \geq C_{s,\max}(\mathcal{J}) \]  
\[\text{(54)}\]

follows directly from the definitions. Thus the converse is trivial.

Now we are going to prove the achievability. When \(\mathcal{J}\) is \(L\) symmetrizable for all \(L \in \mathbb{N}\), then by Theorem 3.1 we have \(C_s(\mathcal{J}) = 0\). When
\[\limsup_{n \to \infty} \frac{1}{n} \sup_{A, F, P} \left( \inf_{q \in P(\Theta)} \chi(P, B_q^n) - \max_{\theta^n \in \Theta^n} \chi(P, Z_{\theta^n}) \right) \leq 0 \]
holds, we also have \(C_s(\mathcal{J}) = 0\). By [54], there is nothing to prove in this case.

We assume that there is a \(L' \in \mathbb{N}\) such that \(\mathcal{J}\) is not \(L'\) symmetrizable, and
\[\limsup_{n \to \infty} \frac{1}{n} \sup_{A, F, P} \left( \inf_{q \in P(\Theta)} \chi(P, B_q^n) - \max_{\theta^n \in \Theta^n} \chi(P, Z_{\theta^n}) \right) > 0 \]
holds.

Now we assume there is a finite set of letters \(A'\), a map \(F' : A' \to S(H)\), and a distribution \(p'\) on \(F'(x) : x \in A'\) such that for sufficiently large \(n\) and some \(p' \in P(A')\) we have
\[\frac{1}{n} \inf_{B'q_{\Theta}} \chi(p'; B'^{\otimes n}) - \max_{\theta^n \in \Theta^n} \chi(p'; Z_{\theta^n}) > c \]  
\[\text{(55)}\]
for a positive \(c\). Here \(B'_{\theta}\) and \(Z'_{\theta}\) are the resulting quantum states at the outputs of \(N_{\theta} \circ F'\) and \(V'_{\theta} \circ F'\), respectively.

We choose an arbitrary positive \(\mu\) and define
\[J'_m := \left\lfloor \exp\left( \inf_{q \in P(\Theta)} \chi(P, B_q^n) - 2\mu n \right) \right\rfloor.\]
By Corollary 3.3 if \( m \) is sufficiently large we can find a \((m, J'_m)\) randomness assisted quantum code \( \left\{ \left( E^\gamma, \{ D_j^\gamma : j \in \{ 1, \ldots, J'_m \} \} \right) : \gamma \in \Gamma \right\} \) and positive \( \lambda, \zeta \) such that for all \( \theta^m \in \Theta^m \)

\[
\min_{j \in \{1, \ldots, J'_m\}} \frac{1}{|\Gamma|} \sum_{\gamma \in \Gamma} \text{tr} \left( N_{\theta^m} \circ F^{m}( E^\gamma( \{ j \}) D_j^\gamma) \right) \geq 1 - 2^{-m^{1/16} \lambda}. \tag{56}
\]

When \( \Theta \) is not \( L' \)-symmetrizable for some \( L' \in \mathbb{N} \), by [3] if \( m \) is sufficiently large, there exist quantum stats \( \sigma_1, \sigma_2 \in \mathcal{S}(H^m) \) and positive-semidefinite operators \( \tilde{D}_1, \tilde{D}_2 \) on \( H^\otimes m \), where \( \tilde{D}_1 + \tilde{D}_2 = 1_{H^\otimes m} \), such that for all \( \theta^m \in \Theta^m \) and \( i \in \{1, 2\} \)

\[
\text{tr} \left( N_{\theta^m}(\sigma_i) \tilde{D}_i \right) > \frac{1}{2}. \tag{57}
\]

We define a new set of letters \( A_2 \) by \( A_2 := A' \cup \{ 1, 2 \} \) and for every \( \theta^m \in \Theta^m \) a classical-quantum channel \( \tilde{N}_{\theta^m} : A_2 \to \mathcal{S}(H^m) \) by

\[
	ilde{N}_{\theta^m}(a) = \begin{cases} 
N_{\theta^m}(F^m(a)) & \text{if } a \in A'; \\
N_{\theta^m}(\sigma_a) & \text{if } a \in \{1, 2\}.
\end{cases}
\]

We define a \( p \in P(A_2) \) by

\[
p(a) = \begin{cases} 
p'(a) & \text{if } a \in A'; \\
0 & \text{if } a \in \{1, 2\}.
\end{cases}
\]

By \( \text{(55)} \) and \( \text{(56)} \) it holds

\[
\frac{1}{m} \left( \inf_{B_q \in \text{Conv}(B_q) \in A_2} \chi(p; B_q^\otimes m) - \max_{\theta^m \in \Theta^m} \chi(p; Z^\theta_{\theta^m}) \right) > c,
\]

where \( \tilde{B}_{\theta^m} \) are the resulting quantum states at the outputs of \( \tilde{N}_{\theta^m} \).

By Theorem 1 of [16], if \( m' \) is sufficiently large we can find a \((m', 2)\) code \( (\tilde{E}, \{ \tilde{D}_j : j \in \{3, 4\} \}) \) and positive \( \lambda, \zeta \) such that for all \( \theta^{mm'} \in \Theta^{mm'} \)

\[
\min_{j \in \{3, 4\}} \text{tr} \left( \tilde{N}_{\theta^{mm'}}(\tilde{E}( \{ j \}) \tilde{D}_j) \right) \geq 1 - 2^{-m'^{1/16} \lambda}. \tag{59}
\]

and

\[
\max_{j \in \{3, 4\}} \| V'_{\theta^{mm'}} \circ F^{mm'}( \tilde{E}( \{ j \}) ) - \Xi_{\theta^{mm'}} \|_1 < 2^{-\sqrt{m'}/\zeta}, \tag{60}
\]

for a \( \Xi_{\theta^{mm'}} \in \mathcal{S}(H^{mm'}) \) which is independent of \( j \).

Now for every \( \theta^{mm'} \in \Theta^{mm'} \) we construct a classical channel \( \tilde{N}_{\theta^{mm'}} : P(\{1, 2, 3, 4\}) \to P(\{1, 2, 3, 4\}) \) by

\[
\tilde{N}_{\theta^{mm'}}(a | b) := \begin{cases} 
\frac{1}{2} \text{tr} \left( N_{\theta^{mm'}}(\sigma_{b}^\otimes m') \tilde{D}_a^\otimes m' \right) & \text{if } a \in \{1, 2\}; \\
\frac{1}{2} \text{tr} \left( N_{\theta^{mm'}}(\tilde{E}^m( \{ b \}) \tilde{D}_a) \right) & \text{if } a \in \{3, 4\}.
\end{cases}
\]

29
part code words for \( \rho \). The deterministic secrecy capacity of the classical-arbitrarily varying channel under the maximal error criterion is positive.

By Corollary 3.4, the deterministic secrecy capacity of the classical-arbitrarily varying quantum wiretap channel \( \{ (\tilde{N}_{g:mm}, V'_{g:mm} \circ F^{mm'}) : \theta^{mm'} \in \Theta^{mm'} \} \) under the maximal error criterion is positive.

A secure deterministic code \( (E, \{ S_j : j \}) \) for the classical-arbitrarily varying wiretap channel \( \{ (\tilde{N}_{g:mm}, V'_{g:mm} \circ F^{mm'}) : \theta^{mm'} \in \Theta^{mm'} \} \) defines a secure deterministic code \( (E, \{ D_j : j \}) \) for \( \{ (N_{g:mm} \circ F^{mm'}, V'_{g:mm} \circ F^{mm'}) : \theta^{mm'} \in \Theta^{mm'} \} \) when we define \( D_j := \tilde{D}_j^{mm'} \) for \( j \in \{ 1, 2 \} \) and set

\[
\frac{1}{2} \sum_{a \in S_j} \tilde{D}_a^{mm'} .
\]

Here, for \( a^{mm'} = (a_1, \cdots, a_{mm'}) \), we set \( \tilde{D}_a^{mm'} = \tilde{D}_{a_1} \otimes \cdots \otimes \tilde{D}_{a_{mm'}} \). Thus the deterministic secrecy capacity of the arbitrarily varying classical-quantum wiretap channel \( \{ (\tilde{N}_{g:mm}, V'_{g:mm} \circ F^{mm'}) : \theta^{mm'} \in \Theta^{mm'} \} \) under the maximal error criterion is positive.

Similar to the proof of Theorem 3.4, we can construct a code with two-part code words for \( \{ (N_{\theta}, V'_{\theta}) : \theta \in \Theta \} \). The first parts of the code words are used to send the randomization index to the legal receiver such that the eavesdropper knows nothing about the randomness such that the maximal probability of the decoding error can be kept arbitrarily small. The second parts are randomness assisted secure code words transmitting the actual secret message such that the maximal probability of the decoding error can be kept arbitrarily small. By Corollary 3.3 there exists a randomness assisted secure code such that its secure deterministic capacity under strong code concept and the maximal error criterion is large or equal to \( \frac{1}{n} \left( \inf_{B' \in Conv((B_{\theta})_{\theta \in \Theta})} \chi(p'; B'_{\theta^{mm'}}) - \max_{\theta \in \Theta} \chi(p'; Z_{\theta^{mm'}}) \right) \). This shows the direct part of Theorem 3.4. 1).

Remark 4.7. In [30], where arbitrarily varying quantum channels were analyzed, actually the following result has been shown:

The deterministic capacity of an arbitrarily varying quantum channel \( \{ N_{\theta} : \theta \in \Theta \} \) under the average error criterion is zero if and only if for every \( L \in \mathbb{N} \) and every finite set \( \{ \rho^L_1, \cdots, \rho^L_K \} \subset S(H^{\otimes L}) \) there exists a \( \tau \) such that for all \( \rho^L, \rho^L' \in \{ \rho^L_1, \cdots, \rho^L_K \} \), we have

\[
\sum_{\rho^L \in \Theta^L} \tau(\rho^L)(\Theta^L)N_{\Theta^L}(\rho^L) = \sum_{\rho^L' \in \Theta^L} \tau(\rho^L)(\Theta^L)N_{\Theta^L}(\rho^L') .
\]
The deterministic capacity of an arbitrarily varying quantum channel \{N_\theta : \theta \in \Theta\} under the maximal error criterion is zero if and only if for every \(L \in \mathbb{N}\) and every \(\{\rho_1^L, \rho_2^L\} \subset S(H^{PL})\), we have

\[
\text{Conv} \left( \{N_{\theta^L}(\rho_1^L) : \theta^L \in \Theta^L\} \right) \cap \text{Conv} \left( \{N_{\theta^L}(\rho_2^L) : \theta^L \in \Theta^L\} \right) \neq \emptyset.
\] (63)

In [3] the authors then showed that the zero-capacity-condition for \(\{N_\theta : \theta \in \Theta\}\) under the maximal error criterion (63) and the \(L\)-symmetrizability in sense of Definition 2.2 are equivalent.

In [18] the authors showed that the zero-capacity-condition for \(\{N_\theta : \theta \in \Theta\}\) under the maximal error criterion (63) and the \(L\)-symmetrizability in the sense of Definition 2.2 is equivalent (cf. Remark 2.3). This is one of the key statements by the authors of [18] to show the equality of the capacity of an arbitrarily varying quantum channel under the maximal error criterion and its capacity under the average error criterion.

Remark 4.8. Interestingly, unlike for arbitrarily varying classical-quantum channels, for classical arbitrarily varying channels, the capacities under maximal error criterion and under the average error criterion are not equal. See [2] for a discussion of the zero-capacity-condition for classical arbitrarily varying channel under maximal error criterion and under the average error criterion.

The capacity formula of classical arbitrarily varying channels under maximal error criterion is still an open problem. In [11] the equality of the zero-error capacity of a classical arbitrarily varying channel and its capacity under maximal error criterion has been demonstrated. In [11] it has been shown that this equality does not hold for arbitrarily varying classical-quantum channels.

5 Applications

5.1 Investigation of Secrecy Capacity’s Continuity

In this section we give the proof to Corollary 3.7. This shows the continuity of the secrecy capacity of an arbitrarily varying quantum channel \(\mathcal{I}\) under randomness assisted quantum coding when the receiver’s system can be described by a finite dimensional Hilbert space.

Proof. [39] shows that for a noisy quantum channel \(N_\theta\), when we consider interactions with the environment as an external system, it is possible to express it as \(\text{tr}_\mathcal{E}(U_N p U_N^\dagger)\), where \(U_N\) is a linear operator \(S(H^\mathcal{P}) \to S(H^\mathcal{E})\) such that \(U_N U_N^\dagger = \text{id}_{H^\mathcal{P}}\), and \(\mathcal{E}\) is the quantum system of the environment. By our assumption, where we follow [24] using a most general protocol, the environment is completely under the control of the eavesdropper. A continuity theorem for Stinespring Dilation has been shown in [39]. This continuity theorem is one of the tools our proof is based on.

By [39], when

\[
\max_{\rho \in S(H^\mathcal{P})} \|N_\theta(\rho) - \hat{N}_\theta(\rho)\|_1 < \delta,
\]

there exist Stinespring Distillations \(U_{N_\theta}\) and \(U_{\hat{N}_\theta}\) for \(N_\theta\) and \(\hat{N}_\theta\) such that

\[
\max_{\rho \in S(H^\mathcal{P})} \|U_{N_\theta}(\rho \otimes \text{id}^{\mathcal{P}}) - U_{\hat{N}_\theta}(\rho \otimes \text{id}^{\mathcal{P}})\|_1 < \delta.
\]
for all \( \theta \in \Theta \).

When there are Stinespring Distillations \( U_N \) and \( U_{N_0} \) for \( N_0 \) and \( N_0 ' \) such that
\[
\max_{\rho \in S(H^P)} \| U_{N_0} (\rho \otimes id^P) - U_{N_0} (\rho \otimes id^P) \|_1 < \delta,
\]
by the triangle inequality, we then have
\[
\max_{\rho \in S(H^P)} \| V'_{N_0} (\rho) - V'_{N_0} (\rho) \|_1 < \delta.
\]

We fix a finite set \( A \), and a map \( F : A \to H^P \). By [10], the secrecy capacity of \( \{(N_0 \circ F, V'_{N_0} \circ F) : \theta \in \Theta \} \in \mathbb{C}_\delta \), its secrecy capacity under randomness assisted quantum coding is
\[
\lim_{n \to \infty} \frac{1}{n} \max_{U \to A \to (B_{N_0}^{\otimes n} : Z_{N_0}, \theta_1, \theta_n)} \left( \inf_{B_{N_0} \in \mathrm{Conv}(\{B_{N_0} \theta_1, \theta_n\})} \chi(p_U ; B_{N_0}^{\otimes n}) - \max_{\theta_n \in \Theta_0} \chi(p_U ; Z_{N_0} \theta_n) \right),
\]
and for every \( \{(\hat{N}_0 \circ F, \hat{V}'_{N_0} \circ F) : \theta \in \Theta \} \in \mathbb{C}_\delta \), its secrecy capacity under randomness assisted quantum coding is
\[
\lim_{n \to \infty} \frac{1}{n} \max_{U \to A \to (B_{N_0}^{\otimes n} : Z_{N_0}, \theta_1, \theta_n)} \left( \inf_{B_{N_0} \in \mathrm{Conv}(\{B_{N_0} \theta_1, \theta_n\})} \chi(p_U ; \hat{B}_{N_0}^{\otimes n}) - \max_{\theta_n \in \Theta_0} \chi(p_U ; \hat{Z}_{N_0} \theta_n) \right),
\]
where \( \hat{B}_{N_0} \) is the resulting quantum state at the output of \( \hat{N}_0 \) and \( \hat{Z}_{N_0}' \) is the resulting quantum state at the output of \( \hat{V}'_{N_0} \).

To analyze \( |\chi(p ; Z_{N_0} \theta_n) - \chi(p ; \hat{Z}_{N_0} \theta_n)| \), we use the technique introduced in [31] and apply the following lemma given in [5].

**Lemma 5.1 (Alicki-Fannes Inequality).** Suppose we have a composite system \( \mathfrak{P} \mathfrak{Q} \) with components \( \mathfrak{P} \) and \( \mathfrak{Q} \). Let \( G^\mathfrak{P} \) and \( G^\mathfrak{Q} \) be the Hilbert space of \( \mathfrak{P} \) and \( \mathfrak{Q} \), respectively. Suppose we have two bipartite quantum states \( \phi^{\mathfrak{P} \mathfrak{Q}} \) and \( \sigma^{\mathfrak{P} \mathfrak{Q}} \) in \( S(G^\mathfrak{P} \mathfrak{Q}) \) such that \( \| \phi^{\mathfrak{P} \mathfrak{Q}} - \sigma^{\mathfrak{P} \mathfrak{Q}} \| \leq \epsilon < 1 \), it holds
\[
S(\mathfrak{P} | \mathfrak{Q})_\rho - S(\mathfrak{P} | \mathfrak{Q})_\sigma \leq 4 \epsilon \log(d - 1) - 2b(\epsilon),
\]
where \( d \) is the dimension of \( G^\mathfrak{P} \) and \( b(\epsilon) \) is defined as in Lemma 4.6.

We fix an \( n \in \mathbb{N} \) and a \( \theta^n = (\theta_1, \cdots, \theta_n) \in \Theta^n \). For any \( a^n \in A^n \) we have
\[
\left| S \left( V'_{\theta^n} (F^n(a^n)) \right) - S \left( \hat{V}'_{\theta^n} (F^n(a^n)) \right) \right|
= \sum_{k=1}^{n} \left| S \left( V'_{(\theta_1, \cdots, \theta_{k-1})} \otimes V'_{(\theta_k, \cdots, \theta_n)} (F^n(a^n)) \right) - S \left( V'_{(\theta_1, \cdots, \theta_{k+1})} \otimes V'_{(\theta_{k+1}, \cdots, \theta_n)} (F^n(a^n)) \right) \right|
\leq \sum_{k=1}^{n} \left| S \left( V'_{(\theta_1, \cdots, \theta_{k-1})} \otimes \hat{V}'_{(\theta_k, \cdots, \theta_n)} (F^n(a^n)) \right) - S \left( V'_{(\theta_1, \cdots, \theta_{k+1})} \otimes \hat{V}'_{(\theta_{k+1}, \cdots, \theta_n)} (F^n(a^n)) \right) \right|.
\]

For a \( k \in \{1, \cdots, n\} \) and \( a^n = (a_1, \cdots, a_n) \in A^n \), by Lemma 5.1 we have
\[
\left| S \left( V'_{(\theta_1, \cdots, \theta_{k+1})} \otimes V'_{(\theta_{k+1}, \cdots, \theta_n)} (F^n(a^n)) \right) - S \left( V'_{(\theta_1, \cdots, \theta_k)} \otimes V'_{(\theta_k, \cdots, \theta_n)} (F^n(a^n)) \right) \right|
= S \left( \hat{V}'_{(\theta_1, \cdots, \theta_k)} \right) - S \left( \hat{V}'_{(\theta_1, \cdots, \theta_k+1)} \right).
\]
\[-S \left(V'_{(\theta_1,\ldots,\theta_{k-1})} \otimes \hat{V}'_{(\theta_{k+1},\ldots,\theta_n)}(F^{n-1}(a_1,\ldots,a_{k-1},a_{k+1},\ldots,a_n)))\right)\]
\[-S \left(V'_{(\theta_1,\ldots,\theta_{k-1})} \otimes \hat{V}'_{(\theta_{k+1},\ldots,\theta_n)}(F^n(a^n))\right)\]
\[+ S \left(V'_{(\theta_1,\ldots,\theta_{k-1})} \otimes \hat{V}'_{(\theta_{k+1},\ldots,\theta_n)}(F^{n-1}(a_1,\ldots,a_{k-1},a_{k+1},\ldots,a_n)))\right)\]
\[= S \left(V'_{\theta_k}(a_k) | V'_{(\theta_1,\ldots,\theta_{k-1})} \otimes \hat{V}'_{(\theta_{k+1},\ldots,\theta_n)}(F^{n-1}(a_1,\ldots,a_{k-1},a_{k+1},\ldots,a_n)))\right)\]
\[= S \left(V'_{\theta_k}(a_k) | V'_{(\theta_1,\ldots,\theta_{k-1})} \otimes \hat{V}'_{(\theta_{k+1},\ldots,\theta_n)}(F^{n-1}(a_1,\ldots,a_{k-1},a_{k+1},\ldots,a_n)))\right)\]
\[\leq 4 \delta \log(\dim H^2 - 1) - 2 \cdot h(\delta)\]
\[= 4 \delta \log(\dim H^2 - 1) - 2 \cdot h(\delta) . \quad (65)\]

Thus,
\[|S \left(V'_{\theta^n}(F^n(a^n)) - S \left(\hat{V}'_{\theta^n}(F^n(a^n))\right)\right| \leq 4n \delta \log(\dim H^2 - 1) - 2n \cdot h(\delta) . \quad (66)\]

For any probability distribution \(p \in P(A)\), \(n \in \mathbb{N}\), and \(\theta^n \in \Theta^n\) we have
\[
|\chi(p; Z'_{\theta^n}) - \chi(p; \hat{Z}'_{\theta^n})| \leq 8n \delta \log(\dim H^2 - 1) - 4n \cdot h(\delta) . \quad (67)\]

We fix a probability distribution \(q\) on \(\Theta\), a probability distribution \(p \in P(A)\), and an \(n \in \mathbb{N}\). By Lemma 4.6 we have
\[
|\chi(p; B_q) - \chi(p; \hat{B}_q)| \leq 8 \delta \log(\dim H^2 - 1) - 4 \cdot h(\delta) . \quad (68)\]

33
Thus for any probability distribution $q$ on $\Theta$, $n \in \mathbb{N}$, $p \in P(A)$, $\theta^n \in \Theta^n$ we have for all $\{N_\theta : \theta \in \Theta\} \in C_\delta$

$$\left| (\chi(p; B_\theta) - \frac{1}{n} \chi(p; Z_{\theta^n})) - (\chi(p; B_\theta) - \frac{1}{n} \chi(p; \hat{Z}_{\theta^n})) \right| \leq 16\delta \log(\dim H^2 - 1) - 8 \cdot h(\delta) . \quad (69)$$

For any positive $\epsilon$ we can find a positive $\delta$ such that $16\delta \log(\dim H^2 - 1) - 8 \cdot h(\delta) \leq \epsilon$.

When $\inf_{q \in P(\theta)} \chi(p; B_\theta) - \max_{\theta^n \in \Theta^n} \chi(p; Z_{\theta^n})$ achieves its maximum in $F$ and $p$, and when $\inf_{q' \in P(\theta)} \chi(p; \hat{B}_{q'}) - \frac{1}{n} \max_{\theta^n \in \Theta^n} \chi(p; \hat{Z}_{\theta^n})$ achieves its maximum in $\hat{F}$ and $\hat{p}$ for some map $\hat{F} : A \to H^2$ and a $\hat{p} \in P(A)$, where $\hat{B}_\theta$ is the resulting quantum state at the output of $N_\theta \circ \hat{F}$ and $\hat{Z}_\theta$ is the resulting quantum state at the output of $\hat{V}_\theta \circ \hat{F}$, the following inequality holds.

For all $n \in \mathbb{N}$ and any positive $\epsilon$ we can find a positive $\delta$ such that for all $\{N_\theta : \theta \in \Theta\} \in C_\delta$

$$\left| \left( \max_p \inf_{q \in P(\theta)} \chi(p; B_\theta) - \max_{\theta^n \in \Theta^n} \chi(p; Z_{\theta^n}) \right) \right|$$
$$- \left( \max_p \left( \left( \min_{q' \in P(\theta)} \chi(p; \hat{B}_{q'}) - \frac{1}{n} \max_{\theta^n \in \Theta^n} \chi(p; \hat{Z}_{\theta^n}) \right) \right) \right| \leq 3\epsilon , \quad (70)$$

since else we would have

$$\inf_{q \in P(\theta)} \chi(p; B_\theta) - \frac{1}{n} \max_{\theta^n \in \Theta^n} \chi(p; \hat{Z}_{\theta^n}) > \inf_{q' \in P(\theta)} \chi(p; \hat{B}_{q'}) - \frac{1}{n} \max_{\theta^n \in \Theta^n} \chi(p; \hat{Z}_{\theta^n}) \quad \text{.}$$

(70) shows Corollary 3.7 \hfill \square

**Remark 5.2.** In [21] the continuity of the secrecy capacity of a classical arbitrarily varying channel under randomness assisted quantum coding has been shown in a similar way (cf. Lemma 3.13). That proof is only valid when the alphabet that the eavesdropper uses is finite. Similarly, our proof of Corollary 3.7 only holds when the quantum system of the environment as eavesdropper has a finite dimension. However, the quantum system of the environment as eavesdropper can be always chosen such that its dimension is upper bounded by the dimension of the receiver’s system (cf. 65).

Since for the classical case we cannot always expect that the eavesdropper is restrict to a finite alphabet, we may use another way to overcome the problem (cf. Remark 5.2) by giving an alternative proof to Lemma 3.13.

**Proof.** For sets $A$, $B$, $C$ and a finite index set $\Theta$, let $\{(W_\theta, V_\theta) : \theta \in \Theta\}$ be a classical arbitrarily varying wiretap channel. Here $W_\theta : P(A) \to P(B)$ and $V_\theta : P(A) \to P(C)$. By [9] we have

$$C_\delta(\{W_\theta, V_\theta\} : \theta \in \Theta; r) = \max_{U \to A \to (BZ), \theta \in \Theta} \min I(p_U; B_\theta) - \max_{\theta \in \Theta} I(p_U; Z_\theta) . \quad (71)$$
The maximum is taken over all random variables that satisfy the Markov chain relationships: $U \rightarrow A \rightarrow (BZ)$. Here $B_t$ are the resulting random variables at the output of legal receiver channels, and $Z_t$ are the resulting random variables at the output of wiretap channels. $U$ is a random variable taking values on some finite set $U$ with probability distribution $p_U$.

Assume we have a classical arbitrarily varying wiretap channel $\{(W'_{\theta}, V'_\theta) : \theta \in \Theta\}$, where $W'_{\theta} : P(A) \rightarrow P(B)$ and $V'_\theta : P(A) \rightarrow P(C)$, and a positive $\delta$ such that
\[
\max_{a \in A} \|W_\theta(a) - W'_\theta(a)\|_1 < \delta
\]
and
\[
\max_{a \in A} \|V_\theta(a) - V'_\theta(a)\|_1 < \delta
\]
for all $\theta \in \Theta$.

We fix a $\theta \in \Theta$ and a random variable $X$ distributed on $A$ according to a probability distribution $p_x$. Let $Z_\theta$ and $Z'_\theta$, distributed on $Z$, be the resulting random variables at the output of $V_\theta$ and $V'_\theta$, respectively. We have
\[
|I(X, Z_\theta) - I(X, Z'_\theta)|
\]
\[
= |H(X) - H(X|Z_\theta) - H(X|Z'_\theta)|
\]
\[
= |H(X|Z_\theta) - H(X|Z'_\theta)|
\]
\[
= \sum_{z \in Z} |V_\theta(z | p_X) - V'_\theta(z | p_X)| \cdot H(X|Z_\theta = z)
\]
\[
\leq \epsilon \max_{z \in Z} H(X|Z_\theta = z)
\]
\[
\leq \epsilon \log |A| .
\]
(72)

Let $B_\theta$ and $B'_\theta$ be the resulting random variables at the output of $W_\theta$ and $W'_\theta$, respectively. Similar to (72), we have
\[
|I(X, B_\theta) - I(X, B'_\theta)| \leq \epsilon \log |A| .
\]
(73)

Combining (71) with (72) and (73) we have
\[
|C_s(\{(W_\theta, V_\theta) : \theta \in \Theta\}; r) - C_s(\{(W'_\theta, V'_\theta) : \theta \in \Theta\}; r) | \leq 2 \epsilon \log |A| .
\]
(74)

This shows that in the classical case also, the continuity does not depend on some unknown strategy of the eavesdropper. \qed

Corollary 3.8 and Corollary 3.10 are direct consequences of Corollary 3.7 when we apply the techniques in [17] for the discontinuity points of classical-quantum channels to Theorem 3.1 and Corollary 3.7.

Now we are going to prove Corollary 3.8.

Proof. At first we assume that the secrecy capacity of $\{N_\theta : \theta \in \Theta\}$ under randomness assisted quantum coding is positive and $F(\{N_\theta : \theta\}) = 0$. We choose a positive $\epsilon$ such that $C_s(\{N_\theta : \theta\}; r) - \epsilon := C > 0$. By Corollary 3.7 the secrecy capacity under randomness assisted quantum coding is continuous. Thus there exist a positive $\delta$ such that for all $\{N'_\theta : \theta \in \Theta\} \in C_\delta$ we have
\[
C_s(\{N'_\theta : \theta \in \Theta\}; r) \geq C_s(\{N_\theta : \theta\}; r) - \epsilon .
\]
Now we assume that there is a \( \{ N'_\theta : \theta \in \Theta \} \in C_\delta \) such that \( F(\{ N'_\theta : \theta \}) > 0 \). This means that \( \{ N'_\theta : \theta \} \) is not symmetrizable. By Theorem 3.1, it holds

\[
C_s(\{ N'_\theta : \theta \in \Theta \}) = C_s(\{ N'_\theta : \theta \}; r) \geq C > 0.
\]

\( \{ N_\theta : \theta \} \) is symmetrizable since \( F(\{ N_\theta : \theta \}) = 0 \). By Theorem 3.1,

\[
C_s(\{ N_\theta : \theta \in \Theta \}) = 0.
\]

Therefore the deterministic secrecy capacity is discontinuous at \( \{ N_\theta : \theta \in \Theta \} \) when 1) and 2) hold.

Now let us consider the case when the deterministic secrecy capacity is discontinuous at \( \{ N_\theta : \theta \in \Theta \} \).

We fix a \( L \in \mathbb{N} \), a \( \tau \in C(\Theta^L | A^L) \), and \( a^L, a^{L'} \in A^L \). The map

\[
\{ N_\theta : \theta \in \Theta \} \rightarrow \frac{1}{2L} \left\| \sum_{\theta^L \in \Theta^L} \tau(\theta^L | a^L)N_{\theta^L}(a^{L'}) - \sum_{\theta^L \in \Theta^L} \tau(\theta^L | a^{L'})N_{\theta^L}(a^L) \right\|_1
\]

is continuous in the following sense: When

\[
\frac{1}{2L} \left\| \sum_{\theta^L \in \Theta^L} \tau(\theta^L | a^L)N_{\theta^L}(a^{L'}) - \sum_{\theta^L \in \Theta^L} \tau(\theta^L | a^{L'})N_{\theta^L}(a^L) \right\|_1 = C
\]

holds, then for every positive \( \delta \) and any \( \{ N'_\theta : \theta \in \Theta \} \in C_\delta \) we have

\[
\left\| \frac{1}{2L} \sum_{\theta^L \in \Theta^L} \tau(\theta^L | a^L)N_{\theta^L}(a^{L'}) - \sum_{\theta^L \in \Theta^L} \tau(\theta^L | a^{L'})N_{\theta^L}(a^L) \right\|_1 \leq 2\delta.
\]

Thus if for a \( \tau \in C(\Theta^L | A) \) we have

\[
\frac{1}{2L} \left\| \sum_{\theta^L \in \Theta^L} \tau(\theta^L | a^L)N_{\theta^L}(a^{L'}) - \sum_{\theta^L \in \Theta^L} \tau(\theta^L | a^{L'})N_{\theta^L}(a^L) \right\|_1 = C > 0
\]

for all \( a, a^{L'} \in A \), we also have

\[
\frac{1}{2L} \left\| \sum_{\theta^L \in \Theta^L} \tau(\theta^L | a^L)N_{\theta^L}(a^{L'}) - \sum_{\theta^L \in \Theta^L} \tau(\theta^L | a^{L'})N_{\theta^L}(a^L) \right\|_1 \geq C - 2\delta.
\]

When \( F(\{ N_\theta : \theta \}) > 0 \) holds, then there is at least one \( L \in \mathbb{N} \) such that \( F_L(\{ N_\theta : \theta \}) > 0 \). We can find a positive \( \delta \) such that \( F_L(\{ W'_\theta : \theta \}) > 0 \), and thus \( F(\{ W'_\theta : \theta \}) > 0 \) holds for all \( \{ N'_\theta : \theta \in \Theta \} \in C_\delta \). By Theorem 3.1, it holds

\[
C_s(\{ N'_\theta : \theta \in \Theta \}) = C_s(\{ N'_\theta : \theta \}; r) \geq C > 0.
\]

By Corollary 3.7, \( C_s(\{ N'_\theta : \theta \}; r) \) is continuous.

Therefore, when the deterministic secrecy capacity is discontinuous at \( \{ N_\theta : \theta \in \Theta \} \), \( F(\{ N_\theta : \theta \}) \) cannot be positive.
We consider now that \( F(\{ N_0 : \theta \}) = 0 \) holds. By Theorem 3.1,
\[
C_s(\{ N_0 : \theta \in \Theta \}) = 0.
\]
When for every \( \{ N'_0 : \theta \in \Theta \} \in C_\delta \) we have \( F(\{ N'_0 : \theta \}) = 0 \), then by Theorem 3.1, \( C_s(\{ N'_0 : \theta \in \Theta \}) = 0 \), and the deterministic secrecy capacity is thus continuous at \( \{ N_0 : \theta \in \Theta \} \).

Therefore, when the deterministic secrecy capacity is discontinuous at \( \{ N_0 : \theta \in \Theta \} \), for every positive \( \delta \) there is a \( \{ N'_0 : \theta \in \Theta \} \in C_\delta \) such that \( F(\{ N'_0 : \theta \}) > 0 \).

When for every positive \( \delta \) there is a \( \{ N'_0 : \theta \in \Theta \} \in C_\delta \) such that \( F(\{ N'_0 : \theta \}) > 0 \) and \( C_s(\{ N_0 : \theta \in \Theta \}, r) = 0 \) holds, then by Theorem 3.1 we have
\[
C_s(\{ N'_0 : \theta \in \Theta \}) = C_s(\{ N'_0 : \theta \in \Theta \}, r),
\]
and the deterministic secrecy capacity is continuous at \( \{ N_0 : \theta \in \Theta \} \).

Therefore, when the deterministic secrecy capacity is discontinuous at \( \{ N_0 : \theta \in \Theta \} \), \( C_s(\{ N_0 : \theta \in \Theta \}, r) \) must be positive. \( \square \)

Corollary 3.11 states that the deterministic secrecy capacity of an arbitrarily varying quantum channel is, in general, not continuous. We show Corollary 3.11 by giving an example.

**Example 5.3.** Let \( \Theta := \{ 1^+, 1^-, 2^+, 2^- \} \) and \( \{ W_\theta : \theta \in \Theta \} \) be defined as in Example 5.4 in Section 5.2. Let \( \{ |0\rangle^3, |1\rangle^3 \} \) be a set of orthonormal vectors on \( H^3 \). Let \( \{ |0\rangle^3, |1\rangle^3, |2\rangle^3, |3\rangle^3, |4\rangle^3, |5\rangle^3 \} \) be a set of orthonormal vectors on \( H^6 \). Let \( \lambda \) be \( \in [0, 1] \). We define a map \( W_{1^+}^\lambda : S(H^3) \to S(H^6) \) by
\[
c_1|0\rangle^3 \langle 0|^3 + c_2|1\rangle^3 \langle 1|^3 + c_3|1\rangle^3 \langle 0|^3 + \overline{c_3}|0\rangle^3 \langle 1|^3
\]
\[
= (1 - \lambda)c_1|0\rangle^3 \langle 0|^3 + (1 - \lambda)c_2|1\rangle^3 \langle 1|^3 + (1 - \lambda)c_3|1\rangle^3 \langle 0|^3 + \lambda(c_1 + c_2)|3\rangle^3 \langle 3|^3,
\]

a map \( W_{1^-}^\lambda : S(H^3) \to S(H^6) \) by
\[
c_1|0\rangle^3 \langle 0|^3 + c_2|1\rangle^3 \langle 1|^3 + c_3|1\rangle^3 \langle 0|^3 + \overline{c_3}|0\rangle^3 \langle 1|^3
\]
\[
= (1 - \lambda)c_1|0\rangle^3 \langle 0|^3 + (1 - \lambda)c_2|1\rangle^3 \langle 1|^3 - (1 - \lambda)c_3|1\rangle^3 \langle 0|^3 + \lambda(c_1 + c_2)|4\rangle^3 \langle 4|^3,
\]

a map \( W_{2^+}^\lambda : S(H^3) \to S(H^6) \) by
\[
c_1|0\rangle^3 \langle 0|^3 + c_2|1\rangle^3 \langle 1|^3 + c_3|1\rangle^3 \langle 0|^3 + \overline{c_3}|0\rangle^3 \langle 1|^3
\]
\[
= (1 - \lambda)c_1|1\rangle^3 \langle 1|^3 + (1 - \lambda)c_2|2\rangle^3 \langle 2|^3 + (1 - \lambda)c_3|2\rangle^3 \langle 1|^3 + \lambda(c_1 + c_2)|5\rangle^3 \langle 5|^3,
\]

and
\[
c_1|0\rangle^3 \langle 0|^3 + c_2|1\rangle^3 \langle 1|^3 + c_3|1\rangle^3 \langle 0|^3 + \overline{c_3}|0\rangle^3 \langle 1|^3
\]
\[
= (1 - \lambda)c_1|1\rangle^3 \langle 1|^3 + (1 - \lambda)c_2|2\rangle^3 \langle 2|^3 + (1 - \lambda)c_3|2\rangle^3 \langle 1|^3 + \lambda(c_1 + c_2)|5\rangle^3 \langle 5|^3,
\]
and a map \( W^{\lambda}_{2;1} : \mathcal{S}(H^3) \rightarrow \mathcal{S}(H^3) \) by
\[
c_1|0\rangle\langle 0|^3 + c_2|1\rangle\langle 1|^3 + c_3|1\rangle\langle 0|^3 + \overline{c_3}|0\rangle\langle 1|^3
\rightarrow (1 - \lambda)c_1|1\rangle\langle 1|^3 + (1 - \lambda)c_2|2\rangle\langle 2|^3
- (1 - \lambda)c_3|2\rangle\langle 1|^3 - (1 - \lambda)\overline{c_3}|1\rangle\langle 2|^3 + \lambda(c_1 + c_2)|6\rangle\langle 6|^3
= (1 - \lambda)W_{2;1}^{-}\left(c_1|0\rangle\langle 0|^3 + c_2|1\rangle\langle 1|^3 + c_3|1\rangle\langle 0|^3 + \overline{c_3}|0\rangle\langle 1|^3 + \lambda(c_1 + c_2)|6\rangle\langle 6|^3 \right).
\]

These maps are obviously linear and trace-preserving. They are also completely positive: When \( \lambda \) is positive semidefinite then all its leading principal minors are non-negative, therefore \( c_1 \) and \( c_2 \) are non-negative.

\[
\begin{pmatrix}
(1 - \lambda)c_1 & (1 - \lambda)c_3 & 0 \\
(1 - \lambda)\overline{c_3} & (1 - \lambda)c_2 & 0 \\
0 & 0 & \lambda(c_1 + c_2)
\end{pmatrix}
\]
is a matrix with positive semidefinite matrices on its diagonal and thus, also positive semidefinite.

i) If \( \lambda \) is not equal to zero, then \( \{W^{\lambda}_{\theta} : \theta \in \Theta\} \) is not symmetric.

Let \( \upsilon \) and \( \phi \) be two arbitrary quantum states \( \in \mathcal{S}(H^3) \). We suppose that there are two distributions \( p_\upsilon \) and \( p_\phi \) on \( \Theta \) such that
\[
\sum_{\theta \in \Theta} p_\phi(\theta) \cdot W^{\lambda}_{\theta}(\upsilon) = \sum_{\theta \in \Theta} p_\upsilon(\theta) \cdot W^{\lambda}_{\theta}(\phi).
\]

We have
\[
(1 - \lambda) \sum_{\theta \in \Theta} p_\upsilon(\theta) W_\theta(\phi) + \lambda \sum_{\theta \in \Theta} p_\upsilon(1^+) |3\rangle\langle 3|^3 + p_\upsilon(1^-) |4\rangle\langle 4|^3
+ p_\upsilon(2^+) |5\rangle\langle 5|^3 + p_\upsilon(2^-) |6\rangle\langle 6|^3
= (1 - \lambda) \sum_{\theta \in \Theta} p_\phi(\theta) W_\theta(\upsilon) + \lambda \sum_{\theta \in \Theta} p_\phi(1^+) |3\rangle\langle 3|^3 + p_\phi(1^-) |4\rangle\langle 4|^3
+ p_\phi(2^+) |5\rangle\langle 5|^3 + p_\phi(2^-) |6\rangle\langle 6|^3.
\]

If \( \lambda \neq 0 \) \( (75) \) implies that
\[
p_\phi(\theta) = p_\upsilon(\theta)
\]
for all \( \theta \in \Theta \).

If \( \{W^{\lambda}_{\theta} : \theta \in \Theta\} \) was symmetric, i.e., if there existed a parametrized set of distributions \( \{p_\rho(\cdot) : \rho \in \mathcal{S}(H^3)\} \) on \( \Theta \) such that for all \( \rho, \rho' \in \mathcal{S}(H^3) \), and if \( \lambda \neq 0 \sum_{\theta \in \Theta} p_\phi(\theta) W^{\lambda}_{\theta}(\rho) = \sum_{\theta \in \Theta} p_\phi(\theta) W^{\lambda}_{\theta}(\rho'), \) by \( (75) \) there would be a distribution \( \rho' \) on \( \Theta \) such that
\[
p'(\theta) = p_\rho(\theta)
\]
for all \( \theta \in \Theta \) and \( \rho \in \mathcal{S}(H^3) \).
But there is clearly no such distribution $p'$ such that $\sum_{\theta \in \Theta} p'(\theta) W_{\theta}^{\lambda}(\rho) = \sum_{\theta \in \Theta} p'(\theta) W_{\theta}^{\lambda}(\rho')$. For example

$$\sum_{\theta \in \Theta} p'(\theta) W_{\theta}^{\lambda}(|0\rangle\langle 0|^{3}) = \sum_{\theta \in \Theta} p'(\theta) W_{\theta}^{\lambda}(|1\rangle\langle 1|^{3})$$

implies that

$$p'(1^{+}) = -p'(1^{-})$$

and

$$p'(2^{+}) = -p'(2^{-})$$

but

$$p'(1^{+})W_{1^{+}}^{\lambda}(|0\rangle\langle 0|^{3}) = p'(1^{+})W_{1^{-}}^{\lambda}(|0\rangle\langle 0|^{3})$$

implies that

$$p'(1^{+}) = -p'(1^{-}) = p'(2^{+}) = -p'(2^{-}) = 0.$$ This is of course a contradiction to the assumption that $p'$ is a distribution on $\Theta$. Thus $\{W_{\theta}^{\lambda} : \theta \in \Theta\}$ is not symmetric.

**ii) There is a positive $\eta$ and a positive $\lambda'$ such that for any positive $\gamma \leq \lambda'$ the randomness assisted secrecy capacity of $\{W_{\theta}^{\lambda} : \theta \in \Theta\}$ is larger than $\eta$.**

Let the sender’s encoding be restricted to $\{|0\rangle^{3}, \{1\rangle^{3}\}$. We have a classical-quantum channel. By [13], the classical-quantum secrecy capacity of $\{W_{\theta}^{\lambda} : \theta \in \Theta\}$ can be lower bounded by

$$\max_{P \text{ on } \{0,1\}} \left( \min_{Q \in \mathcal{Q}} \chi(P, W_{Q}^{\lambda}) - \lim_{n \to \infty} \max_{\theta' \in \Theta^{n}} \frac{1}{n} \chi(P^{n}, V_{\theta'}^{\lambda}) \right),$$

where $\{V_{\theta}^{\lambda} : \theta \in \Theta\}; \mathcal{S}(H^{3}) \to \mathcal{S}(H^{3})$ are the channels where the wiretapper observes the outputs, and $\mathcal{Q}$ is the set of distributions on $\Theta$.

The Kraus representations and the Stinespring dilation of $W_{\theta}^{\lambda}$, $\theta \in \Theta$ are simple. It is easy to verify that following fact holds:

When the sender sends the state $\rho$, and when the legal channel to the receiver can be represented by Kraus matrices $(A_{1}, A_{2}, \cdots)$, the quantum state which the environment obtains can be written in matrix form

$$(A_{i}^{*} \rho A_{j})_{i,j}.$$
Thus for all \( \theta \in \mathcal{Q} \), \( V_\theta^\lambda \left( \begin{array}{cc} c_1 & c_2 \\ \lambda c_3 & c_2 \end{array} \right) \) can be written as (minus the zero rows and columns, and to another set of basis vectors for each \( \theta \in \mathcal{Q} \), of course).

\[
\begin{pmatrix}
(1 - \lambda)(c_1 + c_2) & 0 & 0 \\
0 & \lambda c_1 & \lambda c_3 \\
0 & \lambda c_3 & c_2
\end{pmatrix}.
\]

We assume that \( \theta \), the channel information, is known by a eavesdropper who has access to the complete environment. Thus we may assume that this eavesdropper knows to which basis its output can be represented in the above matrix form, i.e., when \( c_1 |0\rangle |0\rangle^\varepsilon + c_3 |1\rangle |0\rangle^\varepsilon + c_3 |0\rangle |1\rangle^\varepsilon + (1 - c_1) |1\rangle |1\rangle^\varepsilon \) is transmitted, the eavesdropper can find a set of orthonormal vectors \( \{ |0\rangle^\varepsilon, |1\rangle^\varepsilon, |2\rangle^\varepsilon \} \) on \( H^\varepsilon \) and perform a transformation to it’s output such that it obtains \( \lambda c_1 |0\rangle^\varepsilon + \lambda c_3 |1\rangle |0\rangle^\varepsilon + \lambda c_3 |0\rangle |1\rangle^\varepsilon + \lambda (1 - c_1) |1\rangle |1\rangle^\varepsilon \) (1 - \( \lambda \)|1)/2|2\rangle^\varepsilon. If it is not able to do this, the amount of information it gathers will be of course less.

Let \( P \) be a probability distribution on the set \( \{ |0\rangle^A, |1\rangle^A \} \), such that \( P(|0\rangle^A) = a_0 \) and \( P(|1\rangle^A) = a_1 \), \( a_0 + a_1 = 1 \). When the sender’s encoding is restricted to \( \{ |0\rangle^A, |1\rangle^A \} \), then for any \( \theta^n \in \Theta^n \) we have

\[ \frac{1}{n} \chi(P^n, V_\theta^\lambda) = \frac{1}{n} \sum_{0 \leq k_1, k_2, k_3 \leq n; k_1 + k_2 + k_3 = n} \binom{n}{k_1, k_2, k_3} (1 - \lambda)^{k_1} \lambda^{k_2} a_0^{k_2} \lambda^{k_3} a_1^{k_3} \log((1 - \lambda)^{k_1} \lambda^{k_2} a_0^{k_2} \lambda^{k_3} a_1^{k_3}) \]

\[ + \frac{1}{n} \sum_{0 \leq k_1, k_2, k_3 \leq n; k_1 + k_2 + k_3 = n} \binom{n}{k_1, k_2, k_3} (1 - \lambda)^{k_1} \lambda^{k_2} a_0^{k_2} \lambda^{k_3} a_1^{k_3} \log((1 - \lambda)^{k_1} \lambda^{k_2} \lambda^{k_3}) \]

\[ = -\frac{1}{n} \sum_{0 \leq k_1, k_2, k_3 \leq n; k_1 + k_2 + k_3 = n} \binom{n}{k_1, k_2, k_3} (1 - \lambda)^{k_1} \lambda^{k_2} a_0^{k_2} \lambda^{k_3} a_1^{k_3} \log(a_0^{k_2} a_1^{k_3}) \]

\[ \leq -\lambda \frac{1}{n} \sum_{0 \leq k_1, k_2, k_3 \leq n; k_1 + k_2 + k_3 = n} \binom{n}{k_1, k_2, k_3} a_0^{k_2} a_1^{k_3} \log(a_0^{k_2} a_1^{k_3}) \]

\[ \leq \lambda \frac{1}{n} H(P^n) = \lambda . \]

We consider a positive \( \lambda_1 \) such that for any \( 0 < \lambda \leq \lambda_1 \) we have

\[ \lim_{n \to \infty} \frac{1}{n} \chi(P^n, V_\theta^\lambda) \leq \frac{1}{4} C \]

where \( C \) is the random capacity of the arbitrarily varying classical-quantum channel \( (W^\lambda_\theta)_{\theta \in \Theta} \), which is positive by Example 5.4 in Section 5.2.

The function \( [0, 1] \to \mathbb{R}: \lambda \to \min_{Q \in \mathcal{Q}} \chi(P, W^\lambda_Q) \) is continuous. Thus there is a positive \( \lambda_2 \) such that for any \( 0 < \lambda \leq \lambda_2 \), we have

\[ \min_{Q \in \mathcal{Q}} \chi(P, W^\lambda_Q) \geq \frac{3}{4} C . \]
For all $0 < \lambda \leq \min\{\lambda_1, \lambda_2\}$, we have

$$p \max_{Q \in \mathcal{Q}} \left( \min_{\theta \in \Theta} \chi(P, W_Q^\theta) - \lim_{n \to \infty} \max_{\theta' \in \Theta^n} \frac{1}{n} \chi(P^n, V_{\theta'}^n) \right) \geq \frac{1}{4} C. \quad (77)$$

Since the random security capacity of the arbitrarily varying quantum channel $\{W^\theta : \theta \in \Theta\}$ is large or equal to the random security capacity of the arbitrarily varying classical-quantum channel when the sender’s encoding is restricted to $\{|0\rangle^A, \{1\rangle^A\}$, (77) proves ii).

By i) and ii), when $\lambda \in [0, 1]$ approaches zero, the deterministic secrecy capacity of $\{W^\theta : \theta \in \Theta\}$ does not approach zero, which is the deterministic secrecy capacity of $\{W^\theta : \theta \in \Theta\}$ by Example 5.4 in Section 5.2. Thus the deterministic secrecy capacity of $\{W^\theta : \theta \in \Theta\}$ is not continuous at zero.

Now we are going to prove Corollary 3.10

**Proof.** Suppose we have $C_s(\{N_\theta : \theta \in \Theta\}) > 0$. Then $\{N_\theta : \theta \in \Theta\}$ is not symmetrizable, which means that $F(\{N_\theta : \theta \in \Theta\})$ is positive. In the proof of Corollary 3.8 we show that $F$ is continuous. Thus there is a positive $\delta'$ such that $F(\{N_\theta' : \theta \in \Theta\}) > 0$ for all $\{N_\theta' : \theta \in \Theta\} \in C_{\delta'}$. When $\{N_\theta : \theta \in \Theta\}$ is not symmetrizable then we have $C_s(\{N_\theta : \theta \in \Theta\}, r) = C_s(\{N_\theta : \theta \in \Theta\}) > 0$. By Corollary 5.1 in [16], the secrecy capacity under randomness assisted quantum coding is continuous. Thus there is a positive $\delta''$ such that $C_s(\{N_\theta' : \theta \in \Theta\}, r) > 0$ for all $\{N_\theta' : \theta \in \Theta\} \in C_{\delta''}$. We define $\delta := \min(\delta', \delta'')$ and the Corollary is shown.

### 5.2 Further Notes and Super-Activation

Theorem 3.1 states that either the deterministic security capacity of an arbitrarily varying quantum channel is zero, or it equals its randomness assisted security capacity. There are actually arbitrarily varying quantum channels which have zero deterministic security capacity but achieve a positive security capacity, if the sender and the legal receiver can use a resource (cf. Example 5.4). This shows that the Ahlswede Dichotomy is indeed a “dichotomy”, and how helpful a resource can be for the robust and secure message transmission.

Now we give an example when the deterministic secrecy capacity of an arbitrarily varying quantum channel is not equal to its randomness assisted secrecy capacity.

**Example 5.4.** Let the sender’s quantum system be presented by $H^A = \mathbb{C}$. Let the receiver’s quantum system be presented by $H^B = \mathbb{C}$. We choose an orthonormal basis $\{|0\rangle^A, |1\rangle^A\}$ on $H^A$ and an orthonormal basis $\{|0\rangle^B, |1\rangle^B, |2\rangle^B\}$ on $H^B$.

i) **Definition of an arbitrarily varying quantum channel**

Let $\Theta := \{1^{(1)}, 1^{(-1)}, 2^{(1)}, 2^{(-1)}\}$ be a set of indices. We define an arbitrarily varying quantum channel $\{W_\theta : \theta \in \Theta\}$ in the following way: We define a map $W_{1^{(1)}}: \mathcal{S}(H^A) \to \mathcal{S}(H^B)$ by

$$c_1|0\rangle^A\langle 0|^B + c_2|1\rangle^A\langle 1|^B + c_3|1\rangle^A\langle 0|^B + \overline{c_3}|0\rangle^A\langle 1|^B,$$

$$\to c_1|0\rangle^B + c_2|1\rangle^B + c_3|0\rangle^B + \overline{c_3}|1\rangle^B,$$
a map $W_1^{(-)}: S(H^A) \to S(H^B)$ by
\[
\begin{align*}
  & c_1|0\rangle_0|0\rangle^A + c_2|1\rangle_0|1\rangle^A + c_3|1\rangle_0|0\rangle^A + c\rangle_0|0\rangle^A \\
  \Rightarrow & c_1|0\rangle_0|1\rangle^A + c_2|1\rangle_0|2\rangle^A - c_3|1\rangle_0|0\rangle^A - c\rangle_0|0\rangle^A,
\end{align*}
\]
a map $W_2^{(+)}: S(H^A) \to S(H^B)$ by
\[
\begin{align*}
  & c_1|0\rangle_0|0\rangle^A + c_2|1\rangle_0|1\rangle^A + c_3|1\rangle_0|0\rangle^A + c\rangle_0|0\rangle^A \\
  \Rightarrow & c_1|1\rangle_0|1\rangle^A + c_2|2\rangle_0|2\rangle^A + c_3|2\rangle_0|1\rangle^A + c\rangle_0|1\rangle^A,
\end{align*}
\]
and a map $W_2^{(-)}: S(H^A) \to S(H^B)$ by
\[
\begin{align*}
  & c_1|0\rangle_0|0\rangle^A + c_2|1\rangle_0|1\rangle^A + c_3|1\rangle_0|0\rangle^A + c\rangle_0|0\rangle^A \\
  \Rightarrow & c_1|1\rangle_0|1\rangle^A + c_2|2\rangle_0|2\rangle^A - c_3|2\rangle_0|1\rangle^A - c\rangle_0|1\rangle^A.
\end{align*}
\]

It is easy to verify that all these maps are linear and trace preserving, it is also easy to verify that $W_1^{(+)}$ and $W_2^{(+)}$ are complete positive. $W_1^{(-)}$ is complete positive since for any $\rho \in S(H^A)$, $W_1^{(+)}(\rho)$ and $W_1^{(-)}(\rho)$ are unitarily equivalent. Similarly, $W_2^{(-)}(\rho)$ is unitarily equivalent to $W_2^{(+)}(\rho)$ for every $\rho \in S(H^A)$ and therefore $W_2^{(-)}$ is complete positive, too.

$W_1^{(+)}$, $W_1^{(-)}$, $W_2^{(+)}$, and $W_2^{(-)}$ are unitary transformation, they have very simple Kraus representations (consist of only one matrix) and very simple Stinespring dilation (a identity matrix on a subspace). It is easy to verify that there is a vector $|0\rangle|0\rangle^e$ on $H^e$, the environment space, such that the channel $V_\theta$ from the sender to the environment can be described as
\[
c_1|0\rangle_0|0\rangle^A + c_2|1\rangle_0|1\rangle^A + c_3|1\rangle_0|0\rangle^A + c\rangle_0|0\rangle^A \rightarrow (c_1 + c_2)|0\rangle|0\rangle^e
\]
for all four $\theta \in \Theta$.

**ii) L-symmetrizability for all $L \in \mathbb{N}$**

We fix an arbitrary $L \in \mathbb{N}$. For every $\rho^L \in S(H^A^L)$ we define a parametrized set of distributions $\tilde{q}_{\rho^L}$ on $\{\Omega^L : \theta \in [0,1]\}$ by
\[
\tilde{q}_{\rho^L}(\theta^L) := (\otimes_{i=1}^{L} |\theta_i|^A) \rho^L (\otimes_{i=1}^{L} |\theta_i|^A)
\]
for $j^L = (j_1, \cdots, j_L)$.

We define a map $g : \Omega^L \to \{0,1\}^L$ in the following way. For every $\theta^L = (k_1^{(s_1)}, k_2^{(s_2)}, \cdots, k_L^{(s_L)}) \in \Omega^L$, $k_i \in \{1,2\}$, $s_i \in \{+, -\}$, we define
\[
g(\theta^L) := (k_1 - 1, k_2 - 1, \cdots, k_L - 1).
\]

We define a parametrized set of distributions $\{q_{\rho^L} : \rho \in S(H^A^L)\}$ on $\Omega^L$ by
\[
q_{\rho^L}(\theta^L) := \frac{1}{2^n} \tilde{q}_{\rho^L}(g(\theta^L)).
\]
For all $\rho^L, \rho'^L \in \mathcal{S}(H^L)$ it holds

$$
\sum_{\theta^L \in \Theta^L} q_{\theta^L} (\theta^L) W_{\theta^L} (\rho^L) = \\
= \sum_{\theta^L \in \Theta^L} q_{\theta^L} \sum_{j^L \in \{0,1\}^L} (\otimes_{i=1}^L (|j_i| \langle |j_i| \rangle) \rho^L (\otimes_{i=1}^L |j_i| \langle |j_i| \rangle) W_{\theta^L} (\otimes_{i=1}^L |j_i| \langle |j_i| \rangle)$$

$$
= \frac{1}{2^L} \sum_{\theta^L \in \Theta^L} \left( \sum_{j^L \in \{0,1\}^L} (\otimes_{i=1}^L (g(\theta^L)_i \langle |j_i| \rangle) \rho^L (\otimes_{i=1}^L |j_i| \langle |j_i| \rangle) (\otimes_{i=1}^L |j_i| + g(\theta^L)_i) \langle |j_i| + g(\theta^L)_i \rangle) \right)$$

$$
= \sum_{j^L \in \{0,1\}^L} \left( \sum_{j^L \in \{0,1\}^L} \otimes_{i=1}^L (|j_i| \langle |j_i| \rangle) \rho^L (\otimes_{i=1}^L |j_i| \langle |j_i| \rangle) (\otimes_{i=1}^L |j_i| + j_i) \langle |j_i| + j_i \rangle) \right)$$

$$
= \frac{1}{2^L} \sum_{\theta^L \in \Theta^L} \left( \sum_{j^L \in \{0,1\}^L} \otimes_{i=1}^L (g(\theta^L)_i \langle |j_i| \rangle) \rho^L (\otimes_{i=1}^L |j_i| \langle |j_i| \rangle) (\otimes_{i=1}^L |j_i| + g(\theta^L)_i) \langle |j_i| + g(\theta^L)_i \rangle) \right)$$

$$
= \sum_{\theta^L \in \Theta^L} q_{\theta^L} \sum_{j^L \in \{0,1\}^L} \left( \sum_{j^L \in \{0,1\}^L} \otimes_{i=1}^L (|j_i| \langle |j_i| \rangle) \rho^L (\otimes_{i=1}^L |j_i| \langle |j_i| \rangle) W_{\theta^L} (\otimes_{i=1}^L |j_i| \langle |j_i| \rangle) \right)$$

$$
= \sum_{\theta^L \in \Theta^L} q_{\theta^L} (\theta^L) W_{\theta^L} (\rho^L),
$$

where for $j^L = (j_1, \ldots, j_L)$ and $j'^L = (j'_1, \ldots, j'_L) \in \{0,1\}^L$ we define $j^L + j'^L := (j_1 + j'_1, \ldots, j_L + j'_L) \in \{0,1,2\}^L$.

Thus $\{W_{\theta} : \theta \in \Theta\}$ is $L$-symmetrizable.

iii) Positivity of the random security capacity

Let $\Theta' := \{1,2\}$ be a finite set of indices. We define a complete positive trace preserving map $W_1 : \mathcal{S}(H^3) \rightarrow \mathcal{S}(H^3)$ by

$$
c_1 |0\rangle |0\rangle \langle 0| + c_2 |1\rangle |1\rangle \langle 1| + c_3 |0\rangle \langle 0| + \bar{c_3} |0\rangle \langle 0| + c_1 |1\rangle \langle 1| + \bar{c_1} |1\rangle \langle 1|
$$

$$
\rightarrow c_1 |0\rangle |0\rangle + c_2 |1\rangle |1|,
$$
and a complete positive trace preserving map \( W_2 : \mathcal{S}(H^3) \to \mathcal{S}(H^3) \) by
\[
  c_1 |0\rangle\langle 0^3 | + c_2 |1\rangle\langle 1^3 | + c_3 |1\rangle\langle 0^3 | + c_4 |0\rangle\langle 1^3 | \\
  \to c_1 |1\rangle\langle 1^3 | + c_2 |2\rangle\langle 2^3 |.
\]

Let \( \mathcal{T} \) and \( \mathcal{T}' \) be the set of distributions on the index set \( \Theta \) and \( \Theta' \), respectively. We consider the case when the sender’s encoding is restricted to transmitting the indexed finite set of orthogonal quantum states \( \{ |0\rangle\langle 0^3 | , |1\rangle\langle 1^3 | \} \) on \( \mathcal{S}(H^3) \). For any \( \sigma \in \{ |0\rangle\langle 0^3 | , |1\rangle\langle 1^3 | \} \) we have \( W_1(\sigma) = W_{1(+)}(\sigma) = W_{1(-)}(\sigma) \) and \( W_2(\sigma) = W_{2(+)}(\sigma) = W_{2(-)}(\sigma) \).

For any \( p \in \mathcal{T} \) we define a distribution \( q_p \in \mathcal{T}' \) by \( q_p(1) = p(1^{(+)}) + p(1^{(-)}) \) and \( q_p(2) = p(2^{(+)}) + p(2^{(-)}) \). For any \( \sigma \in \{ |0\rangle\langle 0^3 | , |1\rangle\langle 1^3 | \} \) it always holds trivially
\[
  q(1)W_1(\sigma) + q(2)W_2(\sigma) = q_p(1^{(+)})W_{1(+)}(\sigma) + q_p(2^{(+)})W_{2(+)}(\sigma) .
\]

Thus
\[
  \min_{s \in \mathcal{T}} \max_{p \in \mathcal{P}} \chi(p, B_s) = \min_{s' \in \mathcal{T}'} \max_{p \in \mathcal{P}} \chi(p, B'_{s'}) .
\]

Here \( \mathcal{P} \) is the set of distributions on the input set \( \{ |0\rangle\langle 0^3 | , |1\rangle\langle 1^3 | \} \), \( B'_s \) is the quantum output of \( (W_2)_{s \in \Theta'} \), and \( B_s \) is the quantum output of \( \{ W_\theta : \theta \in \Theta \} \).

We denote by \( p' \) the distribution on \( \{ |0\rangle\langle 0^3 | , |1\rangle\langle 1^3 | \} \) such that \( p'(1(0^3)) = p'(1(1^3)) = \frac{1}{2} \). Let \( q \in [0, 1] \). We define \( Q(1) = q, Q(2) = 1 - q \). We have
\[
  \chi \left( p', \{ W_{Q}(a) : a \in A \} \right) \\
  = -\frac{1}{2} q \log \frac{1}{2} q + \frac{1}{2} (1 - q) \log \frac{1}{2} (1 - q) - \frac{1}{2} \log \frac{1}{2} + q \log q + (1 - q) \log (1 - q) .
\]

By the differentiation by \( q \), we obtain
\[
  \frac{1}{\log e} \left( \frac{1}{2} \log \frac{1}{2} q - \frac{1}{2} \log \frac{1}{2} (1 - q) + \frac{1}{2} \log q + 1 - \log (1 - q) - 1 \right) \\
  = \frac{1}{\log e} (\log q - \log (1 - q)) .
\]

This term is equal to zero if and only if \( q = \frac{1}{2} \). By further calculation, one can show that \( \chi \left( p', \{ W_{Q}(\rho) : \rho \in \{ |0\rangle\langle 0^3 | , |1\rangle\langle 1^3 | \} \} \right) \) achieves its minimum when \( q = \frac{1}{2} \). This minimum is equal to \(-\frac{1}{2} \log \frac{1}{4} + \frac{1}{2} \log \frac{1}{2} = \frac{1}{2} > 0 \). Thus
\[
  \max_{p} \min_{q} \chi(p, B_q) \geq \frac{1}{2} .
\]
For any \( n \in \mathbb{N} \), an arbitrary quantum state \( \rho^\otimes n \) in \( S(H^A_n) \), and an arbitrary sequence \( \theta^n \in \Theta^n \), we have \( V_{\theta^n}(\rho^\otimes n) = |0\rangle \langle 0|^E \). This can be easily shown by induction: For any \( m \in \mathbb{N} \), we assume \( \rho^\otimes m \) is an arbitrary quantum state in \( S(H^A_m) \) and \( \theta^m = (\theta_1, \cdots, \theta_m) \) is an arbitrary sequence in \( \Theta \). It holds \( V_{\theta^m}(\rho^\otimes m) = |0\rangle \langle 0|^E \otimes V_{\theta^{m-1}}(\rho^\otimes m-1) \), where \( \rho^\otimes m-1 \) is a quantum state in \( S(H^A_{m-1}) \) and \( \theta^{m-1} = (\theta_2, \cdots, \theta_m) \). Thus for every \( p \in \mathcal{P} \) and \( \theta^n \in \Theta^n \), \( \chi(p^n, Z_{\theta^n}) \) cannot exceed \( 1 \log 1 - 1 \log 1 = 0 \).

Thus

\[
C_s(\{(W_{\theta}, V_{\theta}) : \theta \in \Theta\}, r) \geq \frac{1}{2} > 0 = C_s(\{(W_{\theta}, V_{\theta}) : \theta \in \Theta\}, r).
\]

This gives an example of an arbitrarily varying quantum channel such that its deterministic capacity is zero, but its random capacity is positive.

Thus, a “useless” arbitrarily varying quantum channel, i.e. with zero deterministic secrecy capacity, allows secure transmission if the sender and the legal receiver have the possibility to use a resource.

A common property of classical channels is that where the capacity of two sub-channels, when used together, is the sum of their capacities. Particularly, a channel system consisting of two orthogonal classical channels, where both are “useless” in the sense that they both have zero capacity for message transmission, the capacity for message transmission of the whole system is zero as well (“0+0 = 0”). For the definition of “two orthogonal channels” in classical systems please see [27].

In contrast to the classical information theory, it is known that the capacities of quantum channels can be super-additive, i.e., there are cases in which the capacity of the product \( W_1 \otimes W_2 \) of two quantum channels \( W_1 \) and \( W_2 \) are larger than the sum of the capacity of \( W_1 \) and the capacity of \( W_2 \) (cf. [32] and [28]). “The whole is greater than the sum of its parts” - Aristotle.

Particularly in quantum information theory, there are examples of two quantum channels, \( W_1 \) and \( W_2 \), with zero capacity, which allow positive transmission if they are used together, i.e., the capacity of their product \( W_1 \otimes W_2 \) is positive, (cf. [38], [37], [35] and also [20] for a rare case result when this phenomenon occurs using two classical arbitrarily varying wiretap channels). This is due to the fact that there are different reasons why a quantum channel can have zero capacity. If we have two channels which have zero capacity for different reasons, they can “remove” their weaknesses from each other, or in other words, “activate” each other. We call this phenomenon “super-activation” (“0+0 > 0”).

In our previous work [15] we proved super-activation for arbitrarily varying classical-quantum wiretap channels.

Now we will prove Theorem 3.12, i.e., super-activation of secrecy capacities for arbitrarily varying quantum channels, by giving an example.

**Example 5.5.** Let the sender’s quantum system be presented by \( H^A = \mathbb{C}^4 \) and the receiver’s quantum system be presented by \( H^B = \mathbb{C}^4 \). Let \( \Theta := \{1, 2\} \) be a finite set of indices.
Choosing an orthonormal basis \{0\}^A, 1\}^A, 2\}^A, 3\}^A} on \(H^A\) and an orthonormal basis \{0\}^B, 1\}^B, 2\}^B, 3\}^B} on \(H^B\), we define a complete positive trace-preserving map \(\hat{W}_1 : S(H^A) \to S(H^B)\) with respect to these bases by

\[
\begin{pmatrix}
  c_{00} & c_{01} & c_{02} & c_{03} \\
  c_{01} & c_{11} & c_{12} & c_{13} \\
  c_{02} & c_{12} & c_{22} & c_{23} \\
  c_{03} & c_{13} & c_{23} & c_{33}
\end{pmatrix}
\to
\begin{pmatrix}
  c_{00} & c_{01} & 0 & 0 \\
  0 & 0 & c_{22} + c_{33} & 0 \\
  0 & 0 & 0 & 0 \\
  0 & 0 & 0 & 0
\end{pmatrix},
\]

and a complete positive trace-preserving map \(\hat{W}_2 : S(H^A) \to S(H^B)\) with respect to these bases by

\[
\begin{pmatrix}
  c_{00} & c_{01} & c_{02} & c_{03} \\
  c_{01} & c_{11} & c_{12} & c_{13} \\
  c_{02} & c_{12} & c_{22} & c_{23} \\
  c_{03} & c_{13} & c_{23} & c_{33}
\end{pmatrix}
\to
\begin{pmatrix}
  c_{00} + c_{11} & 0 & 0 & 0 \\
  0 & 0 & 0 & 0 \\
  0 & 0 & c_{22} & c_{23} \\
  0 & 0 & c_{23} & c_{33}
\end{pmatrix}.
\]

With respect to an orthonormal basis \{0\}^E, 1\}^E, 2\}^E, 3\}^E} on \(H^E\), \(\hat{W}_1\) has the Stinespring matrix

\[
\begin{pmatrix}
  1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
  0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
  0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\
  0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
  0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
  0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
  0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
  0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
  0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\
  0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\
  0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\
  0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\
  0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\
  0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\
  0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0
\end{pmatrix}.
\]

The quantum state which the environment obtains is

\[
\begin{pmatrix}
  c_{00} & c_{01} & c_{02} & c_{03} \\
  c_{01} & c_{11} & c_{12} & c_{13} \\
  c_{02} & c_{12} & c_{22} & c_{23} \\
  c_{03} & c_{13} & c_{23} & c_{33}
\end{pmatrix}
\to
\begin{pmatrix}
  c_{00} + c_{11} & 0 & 0 & 0 \\
  0 & 0 & 0 & 0 \\
  0 & 0 & c_{22} & c_{23} \\
  0 & 0 & c_{23} & c_{33}
\end{pmatrix},
\]

with respect to the orthonormal basis \{0\}^E, 1\}^E, 2\}^E, 3\}^E} on \(H^E\).

With respect to an orthonormal basis \{0\}^E, 1\}^E, 2\}^E, 3\}^E} on \(H^E\), \(\hat{W}_2\) has
the Stinespring matrix

\[
\begin{pmatrix}
0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\
0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\
0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
\end{pmatrix}
\]

The quantum state which the environment obtains is

\[
\begin{pmatrix}
c_{00} & c_{01} & c_{02} & c_{03} \\
c_{01} & c_{11} & c_{12} & c_{13} \\
c_{02} & c_{12} & c_{22} & c_{23} \\
c_{03} & c_{13} & c_{23} & c_{33} \\
\end{pmatrix}
\rightarrow
\begin{pmatrix}
c_{00} & c_{01} & 0 & 0 \\
c_{01} & c_{11} & 0 & 0 \\
0 & 0 & c_{22} & c_{33} \\
0 & 0 & 0 & 0 \\
\end{pmatrix}
\]

with respect to a orthonormal basis \{[0]_E, [1]_E, [2]_E, [3]_E\} on \(H_E^\otimes\).

When we interpret the environment as a wiretapper, then the arbitrarily varying wiretap quantum channel \((\hat{W}_{\theta'}, \hat{V}_{\theta'}) : \theta' \in \hat{\Theta}\) has the following property:

\(\hat{W}_1\) and \(\hat{V}_2\) are identical with respect to the corresponding orthonormal bases on \(H_B^\otimes\) and \(H_E^\otimes\), while \(\hat{W}_2\) and \(\hat{V}_1\) are identical with respect to the corresponding orthonormal bases on \(H_B^\otimes\) and \(H_E^\otimes\).

Thus for any input set of quantum states and any probability distribution \(p\) on this set we always have

\[
\min_{\theta' \in \hat{\Theta}} \chi(p, \hat{W}_{\theta'}) - \max_{\theta'' \in \hat{\Theta}} \chi(p, \hat{V}_{\theta''}) = \min_{\theta' \in \hat{\Theta}} \chi(p, \hat{W}_{\theta'}) - \max_{\theta'' \in \hat{\Theta}} \chi(p, \hat{W}_{\theta''}) \leq 0.
\]

The secrecy capacity of this arbitrarily varying wiretap quantum channel is thus always zero: Supposed there is a message set and a code such that for \((\hat{W}_{\theta'}, \hat{V}_{\theta'})\), \(\theta' \in \hat{\Theta}\) the sender is able to convey a secure message to the legal receiver without the wiretapper knowing anything, then the wiretapper can correctly decode the same encoded message, when it is transmitted with the same decoding operator in corresponding orthonormal bases through \((\hat{W}_{\theta''}, \hat{V}_{\theta''})\), \(\theta'' \neq \theta'\), while the legal receiver cannot decode anything.

Let \(\{W_{\theta} : \theta \in \Theta\}\) be defined as in Section 5.2. We now consider \(\hat{W}_{\theta'} \otimes W_{\theta} : (\theta', \theta) \in \hat{\Theta} \times \Theta\). For any \(\sigma \in H_A^\otimes\), when the channel state is \((\theta', \theta)\), the
quantum state which the environment obtains is \( \hat{V}_\theta \otimes V_\theta(\sigma) \). We have

\[
C_s(\{(\hat{W}_\theta \otimes W_\theta, \hat{V}_\theta \otimes V_\theta) : (\theta', \theta) \in \hat{\Theta} \times \Theta\}, r) \\
\geq C_s((W_\theta, V_\theta) : \theta \in \Theta), r) \\
= \frac{1}{2}.
\]

We define

\[
\rho_1 := \frac{1}{2}(|0\rangle + |1\rangle)(|0\rangle + |1\rangle)\hat{a} \otimes \hat{a} |0\rangle |0\rangle^a
\]

and

\[
\rho_2 := \frac{1}{2}(|2\rangle + |3\rangle)(|2\rangle + |3\rangle)\hat{a} \otimes \hat{a} |0\rangle |0\rangle^a.
\]

If \( \{\hat{W}_\theta \otimes W_\theta : (\theta', \theta) \in \hat{\Theta} \times \Theta\} \) is symmetrizable, then there exists a parametrized set of distributions \( \{\tau(\cdot | \sigma) : \sigma \in \mathcal{H}^a \otimes \mathcal{A}\} \) on \( \hat{\Theta} \times \Theta \) such that

\[
\sum_{(\theta', \theta) \in \hat{\Theta} \times \Theta} \tau((\theta', \theta) | \rho_2) \hat{W}_\theta \otimes W_\theta(\rho_1) = \sum_{(\theta', \theta) \in \hat{\Theta} \times \Theta} \tau((\theta', \theta) | \rho_1) \hat{W}_\theta \otimes W_\theta(\rho_2)
\]

\[
\Rightarrow \frac{1}{2}(\tau((1, 1^{(+)} | \rho_2) + \tau((1, 1^{(-)} | \rho_2))(0) + (1)))(|0\rangle + (1))\hat{a} \otimes |0\rangle |0\rangle^a
\]

\[
+ \frac{1}{2}(\tau((2, 1^{(+)} | \rho_2) + \tau((2, 1^{(-)} | \rho_2))(0) + (1))\hat{a} \otimes |0\rangle |0\rangle^a
\]

\[
+ \frac{1}{2}(\tau((1, 2^{(+)} | \rho_2) + \tau((1, 2^{(-)} | \rho_2))(0) + (1))\hat{a} \otimes (0) |1\rangle |1\rangle^a
\]

\[
+ \frac{1}{2}(\tau((2, 2^{(+)} | \rho_2) + \tau((2, 2^{(-)} | \rho_2))(0) + (1))\hat{a} \otimes (0) |1\rangle |1\rangle^a
\]

\[
\Rightarrow \tau((1, 1^{(+)} | \rho_2) + \tau((1, 1^{(-)} | \rho_2)
\]

\[
= \tau((2, 1^{(+)} | \rho_2) + \tau((2, 1^{(-)} | \rho_2)
\]

\[
= \tau((1, 2^{(+)} | \rho_2) + \tau((1, 2^{(-)} | \rho_2)
\]

\[
= \tau((2, 2^{(+)} | \rho_2) + \tau((2, 2^{(-)} | \rho_2)
\]

\[
= 0
\]

\[
\Rightarrow \frac{1}{2}.
\]

(79)

\( \{\hat{W}_\theta \otimes W_\theta : (\theta', \theta) \in \hat{\Theta} \times \Theta\} \) is thus not symmetrizable. By Theorem 3.1

\[
C_s(\{(\hat{W}_\theta \otimes W_\theta, \hat{V}_\theta \otimes V_\theta) : (\theta', \theta) \in \hat{\Theta} \times \Theta\})
\]

\[
= C_s((W_\theta, V_\theta) : (\theta', \theta) \in \hat{\Theta} \times \Theta), r)
\]

\[
\geq \frac{1}{2}.
\]
6 Secrecy Capacity of Quantum Compound Channels

In our earlier work [14] we determined the secrecy capacity of the classical-quantum compound wiretap channel. Our idea for the case with CSI (channel state information) at the transmitter was sending the information in two parts, firstly, the sender sent the state information with finite blocks of finite bits with a public code to the receiver, and then, depending on \( \theta \), the sender sent the message with a secure code in the second part. The following Lemma has been proved in [14].

Lemma 6.1. The secrecy capacity of the compound classical-quantum wiretap channel \( \{(W_\theta, V_\theta) : \theta \in \Theta\} \) in the case with CSI is given by

\[
C_{CSI}(\{(W_\theta, V_\theta) : \theta \in \Theta\}) = \lim_{n \to \infty} \min_{\theta \in \Theta} \max_{P_{inp: wt}} \frac{1}{n} \left( \chi(P_{inp}; B^n_\theta) - \chi(P_{inp}; Z^n_\theta) \right)
\]

where \( B_\theta \) are the resulting random quantum states at the output of legal receiver channels and \( Z_\theta \) are the resulting random quantum states at the output of wiretap channels. The maximum is taken over all probability distributions \( P_{inp} \) on the input quantum states \( w_\theta \).

Assume that the sender’s encoding is restricted to transmitting an indexed finite set of orthogonal quantum states \( \{\rho_x : x \in A\} \subset \mathcal{S}(H_\theta \otimes n) \), then the secrecy capacity of the compound classical-quantum wiretap channel \( \{(W_\theta, V_\theta) : \theta \in \Theta\} \) in the case with no CSI at the encoder is given by

\[
C_S(\{(W_\theta, V_\theta) : \theta \in \Theta\}) = \lim_{n \to \infty} \max_{U \to A \to (BZ)_{\theta \in A}} \left( \frac{1}{n} \min_{\theta \in \Theta} \chi(U; B^n_\theta) - \max_{\theta \in \Theta} \chi(U; Z^n_\theta) \right).
\]

Now we are going to prove Corollary 3.14.

Proof. (26) follows immediately from Lemma 6.1. (25) can be proved in a similar way as Lemma 6.1: The converse is trivial since the secrecy capacity of \( \{(N_\theta \circ F, V_\theta \circ F) : \theta \in \Theta\} \) with CSI is upper bounded by \( \lim_{n \to \infty} \frac{1}{n} \max_{U \to A \to (BZ)_{\theta \in A}} \chi(p_U; B^n_\theta) - \chi(p_U; Z^n_\theta) \leq 0 \). Now we are going to show the achievability. When

\[
\lim_{n \to \infty} \frac{1}{n} \max_{U \to A \to (BZ)_{\theta \in A}} \chi(p_U; B^n_\theta) - \chi(p_U; Z^n_\theta) > 0
\]

holds, the secrecy capacity of \( \{(W_\theta, V_\theta) : \theta \in \Theta\} \) with CSI is zero and there is nothing to prove.

Now we assume that

\[
\lim_{n \to \infty} \frac{1}{n} \max_{U \to A \to (BZ)_{\theta \in A}} \chi(p_U; B^n_\theta) - \chi(p_U; Z^n_\theta) \leq 0
\]

holds. In this case we showed that in [14] the secrecy capacity of \( \{(N_\theta \circ F, V_\theta \circ F) : \theta \in \Theta\} \) without CSI is positive and the sender can build a code \( C_1 = (E^{(1)}, \{D^n_\theta(1) : \theta \in \Theta\}) \) such that the CSI can be sent to the legal receiver with
a block with finite length and the eavesdropper knowing nothing. The first part is of length $O(1)$, which is negligible compared to the second part.

If both the sender and the legal receiver have the full knowledge of $\theta$, then we only have to look at the single wiretap channel $(N_\theta \circ F, V_\theta \circ F)$.

In [22] and [24] it was shown that if $n$ is sufficiently large, there exists an $(n, J_{n,\theta})$ code for the quantum wiretap channel $(N_\theta \circ F, V_\theta \circ F)$ with

$$\log J_{n,\epsilon} = \max_{U \rightarrow A \rightarrow \{(BZ)_{\theta}\}} (\chi(p_U; B_{\theta}^n u) - \chi(p_U; Z_{\theta}^n u)) - \epsilon,$$

for any positive $\epsilon$ and $\zeta$ such that

$$1 - \frac{1}{J_n} \sum_{j=1}^{J_n} \text{tr}(N_{\theta}^n F^n(E_{\theta}(|j|)D_j^{(\theta)})) < \epsilon,$$

and

$$\chi(R_{uni}; Z_{\theta}^n) < \zeta.$$

When the sender and the legal receiver both know $\theta$, they can build an $(n, J_n)$ secure code $C_2^{(\theta)} = (E^{(2)}, \{D^{(2)}_j : j = 1, \cdots, J_n\})$ to send the message, where

$$\log J_n = \min_{\theta \in \Theta} \max_{U \rightarrow A \rightarrow \{(BZ)_{\theta}\}} \chi(p_U; B_{\theta}^n) - \chi(p_U; Z_{\theta}^n) - \epsilon.$$

We define now a code $C := (E^{(1)} E^{(2)}, \{D^{(1)}_j \otimes D^{(2)}_j : \theta \in \Theta, j = 1, \cdots, J_n\}).$

Since the length of $C_1$ can be negligible compared to the second part in asymptotic scenarios, we have

$$C_{S,CSI} \geq \min_{\theta \in \Theta} \lim_{n \rightarrow \infty} \frac{1}{n} \max_{U \rightarrow A \rightarrow \{(BZ)_{\theta}\}} \chi(p_U; B_{\theta}^n) - \chi(p_U; Z_{\theta}^n).$$

Acknowledgment

Support by Bundesministerium für Bildung und Forschung (BMBF) via Grant 16KIS0118K and 16KIS0117K, the German Research Council (DFG) via Grant 1129/1-1 and Bo 1734/20-1, and the ERC via Advanced Grant IRQUAT is gratefully acknowledged.

References

[1] R. Ahlswede, A note on the existence of the weak capacity for channels with arbitrarily varying channel probability functions and its relation to Shannon’s zero error capacity, Annals of Mathematical Statistics, Vol. 41, No. 3, 1970.

[2] R. Ahlswede, Elimination of correlation in random codes for arbitrarily varying channels, Z. Wahrscheinlichkeitstheorie verw. Gebiete, Vol. 44, 159-175, 1978.

[3] R. Ahlswede, I. Bjelaković, H. Boche, and J. Nötzel, Quantum capacity under adversarial quantum noise: arbitrarily varying quantum channels, Comm. Math. Phys. A, Vol. 317, No. 1, 103-156, 2013.
[4] R. Ahlswede and V. Blinovsky, Classical capacity of classical-quantum arbitrarily varying channels, IEEE Trans. Inform. Theory, Vol. 53, No. 2, 526-533, 2007.

[5] R. Alicki and M. Fannes, Continuity of quantum conditional information, J. Phys. A: Math. Gen., Vol. 37, L55, 2004.

[6] K. M. R. Audenaert, A sharp continuity estimate for the von Neumann entropy, J. Phys. A: Math. Theor., Vol. 40, 8127-8136, 2007.

[7] H. Barnum, M. A. Nielsen, and B. Schumacher, Information transmission through a noisy quantum channel, Phys. Rev. A, Vol. 57, 4153, 1998.

[8] I. Bjelaković and H. Boche, Classical capacities of averaged and compound quantum channels, IEEE Trans. Inform. Theory, Vol. 57, No. 7, 3360-3374, 2009.

[9] I. Bjelaković, H. Boche, and J. Sommerfeld, Secrecy results for compound wiretap channels, Problems of Information Transmission, Vol. 49, No. 1, 73-98, 2013.

[10] I. Bjelaković, H. Boche, and J. Sommerfeld, Capacity results for arbitrarily varying wiretap channels, Information Theory, Combinatorics, and Search Theory, in Memory of Rudolf Ahlswede, H. Aydinian, F. Cicalese, and C. Deppe eds., LNCS Vol. 7777, 114-129, arXiv:1209.5213, 2012.

[11] I. Bjelaković, H. Boche, G. Janßen, and J. Nötzel, Arbitrarily varying and compound classical-quantum channels and a note on quantum zero-error capacities, Information Theory, Combinatorics, and Search Theory, in Memory of Rudolf Ahlswede, H. Aydinian, F. Cicalese, and C. Deppe eds., LNCS Vol. 7777, 247-283, arXiv:1209.6325, 2012.

[12] D. Blackwell, L. Breiman, and A. J. Thomasian, The capacities of a certain channel classes under random coding, Ann. Math. Statist. Vol. 31, No. 3, 558-567, 1960.

[13] V. Blinovsky and M. Cai, Arbitrarily classical-quantum varying wiretap channel, Information Theory, Combinatorics, and Search Theory, in Memory of Rudolf Ahlswede, H. Aydinian, F. Cicalese, and C. Deppe eds., LNCS Vol. 7777, 234-246, 2013.

[14] H. Boche, M. Cai, N. Cai, and C. Deppe, Secrecy capacities of compound quantum wiretap channels and applications, Physical Review A, Vol. 89, No. 5, 052320. arXiv:1302.3412, 2016.

[15] H. Boche, M. Cai, C. Deppe, and J. Nötzel, Classical-quantum arbitrarily varying wiretap channel - Ahlswede Dichotomy - positivity - resources - super activation, Quantum Information Processing, Vol. 15, No. 11, 4853-489, arXiv:1307.8007, 2016.

[16] H. Boche, M. Cai, C. Deppe, and J. Nötzel, Classical-quantum arbitrarily varying wiretap channel: Common randomness assisted code and continuity, Quantum Information Processing, Vol. 16, No. 1, 1-48, 2016.
[17] H. Boche, M. Cai, C. Deppe, and J. Nötzel, Classical-Quantum Arbitrarily Varying Wiretap Channel: Secret Message Transmission under Jamming Attacks, Journal of Mathematical Physics, Vol. 58, 102203, 2017.

[18] H. Boche and J. Nötzel, Arbitrarily small amounts of correlation for arbitrarily varying quantum channels, J. Math. Phys., Vol. 54, No. 11, arXiv 1301.6063, 2013.

[19] H. Boche and J. Nötzel, Positivity, discontinuity, finite resources, and nonzero error for arbitrarily varying quantum channels, J. Math. Phys., Vol. 55, No. 122201, 2014.

[20] H. Boche and R. F. Schaefer (Wyrembelski), Capacity results and super-activation for wiretap channels with active wiretappers, Trans. on Inform. Forensics and Security, Vol. 8, No. 9, 2013.

[21] H. Boche, R. F. Schaefer (Wyrembelski), and H. V. Poor, On the continuity of the secrecy capacity of compound and arbitrarily varying wiretap channels, IEEE Trans. on Information Forensics and Security, Vol. 10, No. 12, 2531-2546, 2015.

[22] N. Cai, A. Winter, and R. W. Yeung, Quantum privacy and quantum wiretap channels, Problems of Information Transmission, Vol. 40, No. 4, 318-336, 2004.

[23] I. Csiszár and P. Narayan, The capacity of the arbitrarily varying channel revisited: positivity, constraints, IEEE Trans. Inform. Theory, Vol. 34, No. 2, 181-193, 1988.

[24] I. Devetak, The private classical information capacity and quantum information capacity of a quantum channel, IEEE Trans. Inform. Theory, Vol. 51, No. 1, 44-55, 2005.

[25] T. Ericson, Exponential error bounds for random codes in the arbitrarily varying channel, IEEE Trans. Inform. Theory, Vol. 31, No. 1, 42-48, 1985.

[26] M. Fannes, A continuity property of the entropy density for spin lattice systems, Comm. Math. Phys., Vol. 31, 291-294, 1973.

[27] K. Fazel and S. Kaiser, Multi-Carrier and Spread Spectrum Systems. From OFDM and MC-CDMA to LTE and WiMAX, 2. edition, ISBN 978-0-470-99821-2, John Wiley & Sons, New York, 2008.

[28] G. Giedke and M. M. Wolf, Quantum communication: super-activated channels, Nature Photonics, Vol. 5, No. 10, 578-580, 2011.

[29] K. Kraus, States, Effects, and Operations, Springer, Berlin, 1983.

[30] D. Kretschmanna, D. Schlingemann, and R. F. Werner, A continuity theorem for Stinespring’s dilation, Journal of Functional Analysis, Vol. 255, No. 8, 1889-1904, 2008.

[31] D. Leung and G. Smith, Continuity of quantum channel capacities, Commun. Math. Phys, Vol. 292, No. 1, 201-215, 2009.
[32] K. Li, A. Winter, X. B. Zou, G. C. Guo, Private capacity of quantum channels is not additive, Phys. Rev. Lett., Vol. 103, No. 12, 120501, 2009.

[33] M. Nielsen and I. Chuang, Quantum Computation and Quantum Information, Cambridge University Press, 2000.

[34] J. Nötzel, M. Wiese, and H. Boche, The Arbitrarily Varying Wiretap Channel — Secret Randomness, Stability and Super-Activation, IEEE Trans. Inform. Theory, Vol. 62, No. 6, 3504-3531, [arXiv:1501.07439], 2016.

[35] J. Oppenheim, For quantum information, two wrongs can make a right, Science Magazine, Vol. 321, 1783, 2008.

[36] P. W. Shor, The quantum channel capacity and coherent information, Lecture Notes, MSRI Workshop on Quantum Computation, 2002.

[37] G. Smith, J. A. Smolin, and J. Yard, Quantum communication with Gaussian channels of zero quantum capacity, Nature Photonics, Vol. 5, 624-627, 2011.

[38] G. Smith and J. Yard, Quantum communication with zero-capacity channels, Science Magazine, Vol. 321, No. 5897, 1812-1815, 2008.

[39] W. F. Stinespring, Positive functions on $C^*$-algebras, Proc. Amer. Math. Soc., Vol. 6, 211, 1955.

[40] M. Wiese, J. Nötzel, and H. Boche, The arbitrarily varying wiretap channel-deterministic and correlated random coding capacities under the strong secrecy criterion, IEEE Trans. Inform. Theory, Vol. 62, No. 7, 3844 - 3862, [arXiv:1410.8078], 2016.

[41] A. D. Wyner, The wire-tap channel, Bell System Technical Journal, Vol. 54, No. 8, 1355-1387, 1975.

[42] Quantum information problem page of the ITP Hannover, [http://qig.itp.uni-hannover.de/qiproblems/11](http://qig.itp.uni-hannover.de/qiproblems/11).