Classical-Quantum Arbitrarily Varying Wiretap Channel—A Capacity Formula with Ahlswede Dichotomy—Resources

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

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

†Christian Deppe
Lehrstuhl für Theoretische
Informationstechnik,
Technische Universität München,
München, Germany,
Email: christian.deppe@tum.de

***Abstract*—We establish the Ahlswede Dichotomy for arbitrarily varying classical-quantum wiretap channels, i.e., either the deterministic secrecy capacity of an arbitrarily varying classical-quantum wiretap channel is zero, or it equals its randomness assisted secrecy capacity. We analyze the secrecy capacity of arbitrarily varying classical-quantum wiretap channels when the sender and the receiver use various resources. It turns out that having randomness, common randomness, and correlation as resources are very helpful for achieving a positive deterministic secrecy capacity of arbitrarily varying classical-quantum wiretap channels. We prove the phenomenon "super-activation" for arbitrarily varying classical-quantum wiretap channels, i.e., two arbitrarily varying classical-quantum wiretap channels, both with zero deterministic secrecy capacity, if used together allow perfect secure transmission.**

I. Introduction

The development in modern communication systems are rapid, especially quantum communication systems which set new kinds of limitations and offer new possibilities. We consider classical-quantum channels, i.e., the sender's inputs are classical data and the receiver's outputs are quantum systems. The capacity of classical-quantum channels has been determined in [15] and [18].

Channel robustness and security are two of the basic features of many information processing systems, since many modern communication systems are often not perfect, but vulnerable to jamming and eavesdropping.

In the model of an classical arbitrarily varying channel we consider channel uncertainty, i.e., transmission over a channel which is not stationary, but can change with every use of the channel. We interpret it as a channel with an evil jammer. The arbitrarily varying channel was first introduced [7]. Ahlswede showed in [1] the surprising result that either the deterministic capacity of an arbitrarily varying channel is zero, or it equals its randomness assisted capacity (Ahlswede Dichotomy). A classical-quantum channel with a jammer is called an arbitrarily varying classical-quantum channel. In [3], the capacity of arbitrarily varying classical-quantum channels is analyzed. A lower bound of the capacity has been given. An alternative proof of [3]'s result and a proof of the strong converse is given in [5]. In [2], 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 [11], a simplification of this condition for the arbitrarily varying classical-quantum channels is given.

In the model of a classical wiretap channel we consider communication with security. This was first introduced in [22] (in this paper we will use a stronger security criterion than [22]). We interpret the wiretap channel as a channel with an evil eavesdropper. A classical-quantum channel with an eavesdropper is called a classical-quantum wiretap channel, its secrecy capacity has been determined in [14] and [13].

In the model of an classical arbitrarily varying wiretap channel, we consider transmission with both a jammer and an eavesdropper. Its secrecy capacity has been analyzed in [6]. A lower bound of the randomness assisted secrecy capacity has been given. 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 $\{(W_t, V_t) : t = 1, \cdots, T\}$ with a common input alphabet and possibly different output alphabets, connecting a sender with two receivers, a legal one and a wiretapper, where t is called a channel state of the channel pair. The legitimate receiver accesses the output of the first part of the pair and the wiretapper observes the output of the second part, respectively. A channel state t, which varies from symbol to symbol in an arbitrary manner, 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 the sense of the stronger security criterion. This

*Project "Informationstheorie des Quanten-Repeaters, Teilprojekt Mehrwegkommunikationsprotokolle für Quanten-Repeater" supported by the Federal Ministry of Education and Research (Ref. No. 01BQ1050)

†Project "Informationstheorie des Quanten-Repeaters, Teilprojekt Robustheit und Sicherheit des Quanten-Repeaters" supported by the Federal Ministry of Education and Research (Ref. No. 01BQ1052)

978-1-4799-5186-4/14/$31.00 ©2014 IEEE

is a generalization of compound classical-quantum wiretap channels in [9] to the case when the channel states are not stationary, but can change over the time. The secrecy capacity of the arbitrarily varying classical-quantum wiretap channels has been analyzed in [8]. A lower bound of the randomness assisted capacity has been given, and it has been shown that this is either a lower bound for the deterministic capacity, or the deterministic capacity is equal to zero.

Assume that a bipartite source, modeled by an i.i.d. random variable (X, Y) with values in some finite set $\mathbf{X} \times \mathbf{Y}$, is observed by the sender and (legal) receiver. The sender has access to the random variable X, and the receiver to Y. We call (X, Y) a correlation. The capacity of an classical arbitrarily varying channel assisted by the correlation as resource has been discussed in [4]. The capacity of an arbitrarily varying quantum channel assisted by the correlation as resource has been discussed in [11].

In Section III we will generalize the result of [8] by establishing the Ahlswede Dichotomy for the arbitrarily varying classical-quantum wiretap channels, i.e., either the deterministic secrecy capacity of an arbitrarily varying classical-quantum wiretap channel is zero, or it equals its randomness assisted secrecy capacity.

In Section IV we will analyze the secrecy capacity of an arbitrarily varying classical-quantum wiretap channel assisted by the correlation as resource. We will show that the correlation is a helpful resource for the secure information transmission through an arbitrarily varying classical-quantum wiretap channel. We will give an example in which both cases of the Ahlswede Dichotomy for the arbitrarily varying classical-quantum wiretap channels actually occur.

In Section V we will present a new discovery for the arbitrarily varying classical-quantum wiretap channels which is followed by the Ahlswede Dichotomy for the arbitrarily varying classical-quantum wiretap channels. This phenomenon is called "super-activation", i.e., two arbitrarily varying classical-quantum wiretap channels, both with zero deterministic secrecy capacity, if used together allow perfect secure transmission.

II. Communication Scenarios and Resources

Let A be a finite set. Let H be a finite-dimensional complex Hilbert space. We denote the sets of probability distributions on A by $P(A)$. We denote the space of density operators on H by $\mathcal{S}(H)$.

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 mutual information between X and Y by $I(X;Y)$ ([21]).

For a quantum state $\rho \in \mathcal{S}(H)$, we denote the von Neumann entropy of ρ by $S(\rho) = -\mathrm{tr}(\rho \log \rho)$. Let $\Phi := \{\rho_x : x \in A\}$ be a set of quantum states on $\mathcal{S}(H)$ labeled by elements of A. For a probability distribution P on A, we denote the Holevo χ quantity by

$$\chi(P; \Phi) := S\left(\sum_{x\in A} P(x)\rho_x\right) - \sum_{x \in A} P(x) S\left(\rho_x\right) \ .$$

A classical-quantum channel is a map $W : A \rightarrow \mathcal{S}(H)$, $A \ni a \rightarrow W(a) \in \mathcal{S}(H)$.

Definition 2.1: Let $\theta := \{1, \cdots, T\}$ be a finite set. For every $t \in \theta$ let W_t be a quantum channel $A \rightarrow \mathcal{S}(H)$. We call the set of the quantum channels $(W_t)_{t\in\theta}$ an **arbitrarily varying classical-quantum channel** when the state t varies from symbol to symbol in an arbitrary manner.

We say that $(W_t)_{t\in\theta}$ is **symmetrizable** if there exists a parametrized set of distributions $\{\tau(\cdot \mid a) : a \in A\}$ on θ such that for all a, $a' \in A$,

$$\sum_{t\in\theta} \tau(t \mid a) W_t(a') = \sum_{t\in\theta} \tau(t \mid a') W_t(a) \ .$$

Definition 2.2: Let A be a finite set. Let H and H' be finite-dimensional complex Hilbert spaces. Let $\theta := \{1, \cdots, T\}$ be a finite set. For every $t \in \theta$ let W_t be a quantum channel $A \rightarrow \mathcal{S}(H)$ and V_t be a quantum channel $A \rightarrow \mathcal{S}(H')$. We call the set of the quantum channel pairs $(W_t, V_t)_{t\in\theta}$ an **arbitrarily varying classical-quantum wiretap channel**. The legitimate receiver accesses the output of W_t and the wiretapper observes the output V_t, respectively, when the state t varies from symbol to symbol in an arbitrary manner.

Definition 2.3: An (n, J_n) **(deterministic) code** C for $(W_t, V_t)_{t\in\theta}$ consists of a stochastic encoder E : $\{1, \cdots, J_n\} \rightarrow P(A^n)$, specified by a matrix of conditional probabilities $E(\cdot|\cdot)$, and a collection of positive semi-definite operators $\{D_j : j \in \{1, \cdots, J_n\}\}$ on $H^{\otimes n}$ such that $\sum_{j=1}^{J_n} D_j = \mathrm{id}_{H^{\otimes n}}$.

R is an achievable **(deterministic) secrecy rate** for the arbitrarily varying classical-quantum wiretap channel $(W_t, V_t)_{t\in\theta}$ if for every positive ϵ, δ, ζ, and sufficiently large n there exist an (n, J_n) code $C = \big\{(E^n, D_j^n) : j = 1, \cdots J_n\big\}$ such that $\frac{\log J_n}{n} > R - \delta$, and

$$\max_{t^n \in \theta^n} P_e(C, t^n) < \epsilon \ , \tag{1}$$

$$\max_{t^n \in \theta^n} \chi\left(R_{uni}; Z_{t^n}\right) < \zeta \ , \tag{2}$$

where R_{uni} is the uniform distribution on $\{1, \cdots J_n\}$. Here $P_e(C, t^n) := 1 - \frac{1}{J_n} \sum_{j=1}^{J_n} \sum_{a^n \in A^n} E(a^n|j) \mathrm{tr}(W_{t^n}(a^n) D_j)$, and Z_{t^n} is the resulting quantum state at the output of the wiretap channel. The largest achievable (deterministic) secrecy rate of $(W_t, V_t)_{t\in\theta}$ is called the (deterministic) secrecy capacity of $(W_t, V_t)_{t\in\theta}$, denoted by $C_s((W_t, V_t)_{t\in\theta})$.

Definition 2.4: Let $\mathbf{X}$ and $\mathbf{Y}$ be finite sets. We denote the sets of joint probability distributions on $\mathbf{X}$ and $\mathbf{Y}$ by $P(\mathbf{X}, \mathbf{Y})$. Let (X, Y) be a random variable distributed to a joint probability distribution $p \in P(\mathbf{X}, \mathbf{Y})$. An (X, Y)**-correlation assisted** (n, J_n) **code** $C(X, Y)$ for the arbitrarily varying classical-quantum wiretap channel $(W_t, V_t)_{t\in\theta}$ consists of a set of stochastic encoders $\{E_{\mathbf{x}^n} : \{1, \cdots, J_n\} \rightarrow P(A^n) : \mathbf{x}^n \in \mathbf{X}^n\}$, and a set of collections of positive semi-definite operators $\Big\{\{D_j^{(\mathbf{y}^n)} : j = 1, \cdots, J_n\} : \mathbf{y}^n \in \mathbf{Y}^n\Big\}$ on $\mathcal{S}(H^{\otimes n})$ which fulfills $\sum_{j=1}^{J_n} D_j^{(\mathbf{y}^n)} = \mathrm{id}_{H^{\otimes n}}$ for every $\mathbf{y}^n \in \mathbf{Y}^n$.

R is an achievable (X,Y) **secrecy rate** for $(W_t,V_t)_{t\in\theta}$ if for every positive ϵ, δ, ζ and sufficiently large n there exist an (X,Y)-correlation assisted (n,J_n) code $C(X,Y) = \left\{\left(E_{\mathbf{x}^n}, D_j^{(\mathbf{y}^n)}\right) : j \in \{1,\cdots,J_n\},\ \mathbf{x}^n \in \mathbf{X}^n,\ \mathbf{y}^n \in \mathbf{Y}^n\right\}$ such that $\frac{\log J_n}{n} > R-\delta$, and

$$\max_{t^n\in\theta^n} \sum_{\mathbf{x}^n\in\mathbf{X}^n} \sum_{\mathbf{y}^n\in\mathbf{Y}^n} p(\mathbf{x}^n,\mathbf{y}^n) P_e(C(\mathbf{x}^n,\mathbf{y}^n),t^n) < \epsilon \ ,$$

$$\max_{t^n\in\theta^n} \sum_{\mathbf{y}^n\in\mathbf{Y}^n} p(\mathbf{x}^n,\mathbf{y}^n)\chi\left(R_{uni}; Z_{t^n,\mathbf{x}^n}\right) < \zeta \ ,$$

where $P_e(C(\mathbf{x}^n,\mathbf{y}^n),t^n) := 1- \frac{1}{J_n}\sum_{j=1}^{J_n}\sum_{a^n\in A^n} E_{\mathbf{x}^n}(a^n|j)\mathrm{tr}(W_{t^n}(a^n)D_j^{(\mathbf{y}^n)})$. The largest achievable (X,Y) secrecy rate of is called the (X,Y) secrecy capacity.

Definition 2.5: Let $\Lambda := \left\{(P_j^n,\rho_j^{\otimes n})_{j=1,\cdots,J_n} \in (P(A^n)\times\mathcal{S}(H^{\otimes n}))^{J_n} : \sum_{j=1}^{J^n}\rho_j^{\otimes n} = \mathrm{id}_{H^{\otimes n}}\right\}$. Every element $\gamma = (P_j^n,\rho_j^{\otimes n})_{j=1,\cdots,J_n} \in \Lambda$ canonically defines an (n,J_n) deterministic code $C^\gamma = \{(E^\gamma, D_j^\gamma) : j=1,\cdots,J_n\}$ by setting $E^\gamma(\cdot \mid j) = P_j^n$ and $D_j^\gamma = \rho_j^{\otimes n}$. An (n,J_n) **randomness assisted quantum code** for the arbitrarily varying classical-quantum wiretap channel $(W_t,V_t)_{t\in\theta}$ is a distribution G on (Λ,σ), where σ is a sigma-algebra such that the functions $\gamma \to P_e(C^\gamma,t^n)$ and $\gamma \to \chi\left(R_{uni}; Z_{C^\gamma,t^n}\right)$ are both G-measurable with respect to σ for every $t^n \in \theta^n$. Here Z_{C^γ,t^n} is the wiretapper's resulting quantum state.

R is an achievable **secrecy rate for** $(W_t,V_t)_{t\in\theta}$ **under randomness assisted quantum coding** if for every positive δ, ζ, ϵ, and sufficiently large n, there is an (n,J_n) randomness assisted quantum code $(\{C^\gamma : \gamma\in\Lambda\},G)$ such that $\frac{\log J_n}{n} > R-\delta$, and

$$\max_{t^n\in\theta^n}\int_\Lambda P_e(C^\gamma,t^n)dG(\gamma) < \epsilon \ ,$$

$$\max_{t^n\in\theta^n}\int_\Lambda \chi\left(R_{uni}, Z_{C^\gamma,t^n}\right)dG(\gamma) < \zeta \ .$$

The largest achievable secrecy rate under random assisted quantum coding is called the random assisted secrecy capacity.

Definition 2.6: Let Λ and C^γ for $\gamma\in\Lambda$ be defined as in Definition 2.5. An (n,J_n) **common randomness assisted quantum code** for the arbitrarily varying classical-quantum wiretap channel $(W_t,V_t)_{t\in\theta}$ is a set $\Gamma = \{\gamma^1,\cdots,\gamma^{|\Gamma|}\}\subset\Lambda$ such that $|\Gamma|$ is in polynomial order of n. As in Definition 2.5, every element $\gamma^i = (P_j^n,\rho_j^{\otimes n})_{j=1,\cdots,J_n}\in\Gamma$ canonically defines an (n,J_n) deterministic code $C^{\gamma^i} = \{(E^{\gamma^i},D_j^{\gamma^i}) : j=1,\cdots,J_n\}$ by setting $E^{\gamma^i}(\cdot\mid j) = P_j^n$ and $D_j^{\gamma^i} = \rho_j^{\otimes n}$.

R is an achievable **secrecy rate for the** $(W_t,V_t)_{t\in\theta}$ **under common randomness assisted quantum coding** if for every positive δ, ζ, ϵ, and sufficiently large n, there is an (n,J_n) common randomness assisted quantum code $(\{C^\gamma : \gamma\in\Gamma\})$ such that $\frac{\log J_n}{n} > R-\delta$, and

$$\max_{t^n\in\theta^n}\frac{1}{|\Gamma|}\sum_{\gamma=1}^{|\Gamma|} P_e(C^\gamma,t^n) < \epsilon \ ,$$

$$\max_{t^n\in\theta^n}\frac{1}{|\Gamma|}\sum_{\gamma=1}^{|\Gamma|}\chi\left(R_{uni}, Z_{C^\gamma,t^n}\right) < \zeta \ .$$

The largest achievable secrecy rate under common randomness assisted quantum coding is called the common randomness assisted secrecy capacity.

The entanglement generating capacity of an arbitrarily varying quantum channel describes the maximal amount of entanglement that we can generate or transmit over the channel. For the sender and the receiver, the objective is to share a nearly maximally entangled state on a Hilbert space by using a large number instances of the quantum channel. This state is needed as an important resource in the quantum information theory. The entanglement generating capacity of the arbitrarily varying quantum channels has been analyzed in [2]. The authors of [2] made the following Conjecture 2.7, which is still unsolved.

Conjecture 2.7: The entanglement generating capacity of an arbitrarily varying quantum channel is equal to the entanglement generating capacity of an arbitrarily varying quantum channel under randomness assisted quantum coding.

A code for the secure message transmission over a classical-quantum wiretap channel can be used to build a code for the entanglement transmission over a quantum channel ([14]). But it seems that the technique of [14] does not work if we consider channel uncertainty (Remark 1).

III. Ahlswede Dichotomy

First we analyze the secrecy capacities of various coding schemes with resource assistance. Our goal is to see what the effects on the secrecy capacities of an arbitrarily varying classical-quantum wiretap channel are if we use deterministic code, randomness assisted code, or common randomness assisted code.

Theorem 3.1 (Ahlswede Dichotomy): Let $(W_t,V_t)_{t\in\theta}$ be an arbitrarily varying classical-quantum wiretap channel.

3.1.1: 1) If the arbitrarily varying classical-quantum channel $(W_t)_{t\in\theta}$ is not symmetrizable, then $C_s((W_t,V_t)_{t\in\theta})$ is equal to the random assisted secrecy capacity of $(W_t,V_t)_{t\in\theta}$.

2) If $(W_t)_{t\in\theta}$ is symmetrizable,

$$C_s((W_t,V_t)_{t\in\theta}) = 0 \ . \tag{3}$$

3.1.2: The common randomness assisted secrecy capacity of $(W_t,V_t)_{t\in\theta}$ is equal to the random assisted secrecy capacity of $(W_t,V_t)_{t\in\theta}$.

Sketch of Proof: Our proof is similar to the proof of the Ahlswede Dichotomy for arbitrarily varying classical-quantum channels in [3]. The difference between our proof and the proofs in [3] is that we have to include security. We use random encoding technique to show that for any (n,J_n) randomness assisted quantum code there exists an (n,J_n) common randomness assisted code $(\{C^\gamma : \gamma\in\Gamma\})$ with the same secrecy rate, where $|\Gamma|$ is in polynomial order of n. This proves 3.1.2. Assuming that $(W_t)_{t\in\theta}$ is not symmetrizable we show the lower bound in 3.1.1 1) by building two-part deterministic code words. By 3.1.2 there is a common randomness assisted code $(\{C^{\gamma} : \gamma \in \Gamma\})$ with the same secrecy rate as the (n, J_n) randomness assisted quantum code. Using the result of [3] we can build an insecure deterministic code to create the common randomness for the sender and the legal receiver. Since $|\Gamma|$ is in polynomial order of n, the length of the insecure code words can be ignored. The two-part deterministic code word is a composition of the insecure code word and the common randomness assisted code word. Even when the first part is not secure against wiretapping, the two-part code word itself is secure against wiretapping. The proof for the upper bound in 3.1.1 1) and the proof for 3.1.1 2) are similar to the methods in [3].

There are indeed arbitrarily varying classical-quantum wiretap channels which have zero deterministic secrecy capacity and positive random secrecy capacity (the example in Section IV). Therefore, as Theorem 3.1.1 shows, randomness is indeed a very helpful resource for the secure message transmission through an arbitrarily varying classical-quantum wiretap channel.

Common randomness is a less "strong" resource than randomness. Here we say "strong" in the sense of [11]. Theorem 3.1.2 shows that the common randomness capacity is always equal to the random secrecy capacity. Therefore, common randomness is an equally helpful resource for the secure message transmission through an arbitrarily varying classical-quantum wiretap channel. However, as [11] showed, common randomness is still a very "strong" resource. As Theorem 3.1 shows, for the transmission of common randomness we have to require that the deterministic capacity for message transmission of the sender's and legal receiver's channel be positive. In the following, we will see that the much "weaker" resource, the (X, Y) correlation, is also an equally helpful resource for the message transmission through an arbitrarily varying classical-quantum channel. The advantage here is that we do not have to require that the deterministic capacity for message transmission of the sender's and legal receiver's channel be positive.

IV. Arbitrarily Varying Classical-Quantum Wiretap Channel with Correlation Assistance

The (X, Y) correlation is a weaker resource than common randomness. We can simulate any (X, Y) correlation by common randomness asymptotically, but there exists a class of sequences of bipartite distributions which cannot model common randomness (cf. Lemma 1 of [11]). Our following Theorem 4.1 shows that also in the case of secure message transmission through an arbitrarily varying classical-quantum wiretap channel, the (X, Y) correlation assistance is an equally helpful resource as common randomness.

Theorem 4.1: Let $(W_t, V_t)_{t\in\theta}$ be an arbitrarily varying classical-quantum wiretap channel. Let $\mathbf{X}$ and $\mathbf{Y}$ be finite sets. If $I(X, Y) > 0$ holds for a random variable (X, Y) which is distributed to a joint probability distribution $p \in P(\mathbf{X}, \mathbf{Y})$, then the randomness assisted secrecy capacity of $(W_t, V_t)_{t\in\theta}$ is equal to the (X, Y) correlation assisted secrecy capacity of $(W_t, V_t)_{t\in\theta}$.

Sketch of Proof: By 3.1.2 there is a common randomness assisted code $(\{C^{\gamma} : \gamma \in \Gamma\})$ with the same secrecy rate as the (n, J_n) randomness assisted quantum code. If the randomness assisted secrecy capacity of $(W_t, V_t)_{t\in\theta}$ is positive, we build a new arbitrarily varying classical-quantum channel $\{f : f \text{ is a function } \mathbf{X} \rightarrow A\} \rightarrow \mathcal{S}(H) \otimes H_{\mathbf{Y}}$ with positive deterministic insecure capacity. Similar to proof of 3.1.1 we build a two-part deterministic code word which consists of a common randomness assisted code word and a code word for the new arbitrarily varying classical-quantum channel. We use th latter one to create common randomness for the sender and the legal receiver. We show that a code for the new arbitrarily varying classical-quantum channel does not have to be secure to be useful for a secure code for the original arbitrarily varying classical-quantum wiretap channel. If the randomness assisted secrecy capacity of $(W_t, V_t)_{t\in\theta}$ is equal to zero, with a technique similar to the techniques in [4] and [11] we show that the (X, Y) correlation assisted secrecy capacity of $(W_t, V_t)_{t\in\theta}$ is also equal to zero.

The following example shows an arbitrarily varying classical-quantum wiretap channel which has zero deterministic secrecy capacity, but positive random secrecy capacity.

Let $\theta = \{1, 2\}$ and $A = \{0, 1\}$. Let $H = H'$ be spanned by the orthonormal vectors $|0\rangle$ and $|1\rangle$. We define $(W_t, V_t)_{t\in\theta}$ by $W_1(0) = |0\rangle\langle 0|$, $W_1(1) = \frac{1}{2}|0\rangle\langle 0| + \frac{1}{2}|1\rangle\langle 1|$, $W_2(0) = \frac{1}{2}|0\rangle\langle 0| + \frac{1}{2}|1\rangle\langle 1|$, $W_2(1) = |1\rangle\langle 1|$, $V_1(0) = |0\rangle\langle 0|$, $V_1(1) = |0\rangle\langle 0|$, $V_2(0) = |0\rangle\langle 0|$, $V_2(1) = |0\rangle\langle 0|$.

$(W_t, V_t)_{t\in\theta}$ is an example that a "useless" arbitrarily varying classical-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 — either randomness, common randomness, or even an insecure and weak correlation (i.e. $I(X, Y)$ needs only to be slightly larger than zero). Thus the "weak" correlation is a very helpful resource for the secure message transmission through an arbitrarily varying classical-quantum wiretap channel. Having weak public signals can be very useful for secure communication in practice.

While in classical information theory single-letter formulas are available for most capacities results, one of the main features in quantum information theory is that for the quantum channels, most of the capacities results can only be expressed in multi-letter formulas. Unlike most capacities results for quantum channels, however, we have the surprising fact that the condition for the zero deterministic security capacity of an arbitrarily varying classical-quantum wiretap channel can be expressed in a single-letter formula (cf. Definition 2.1). Furthermore, the Ahlswede Dichotomy shows that the deterministic capacity for secure message transmission is, in general, not specified by entropy quantities. This is a new behavior in communication due to active wiretap attacks.

V. Super-Activation

One of the properties of classical channels is that in the majority of cases if we have a channel system where two sub-channels are used together, the capacity of this channel system is the sum of the two sub-channels' capacities. Particularly, a 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 ("$0+0=0$").

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 where 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.

Particularly, in the quantum information theory there are examples of two quantum channels W_1 and W_2 with zero capacity that allow perfect transmission if they are used together, i.e., the capacity of their product $W_1 \otimes W_2$ is positive ("$0 + 0 > 0$"). 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" (cf. [20], [19], [17] and also [12] for a rare case result when this phenomenon occurs using two classical arbitrarily varying wiretap channels).

It is known that arbitrarily varying classical-quantum wiretap channels with positive secrecy capacities are super-additive, in sense of the product $W_1 \otimes W_2$ of two arbitrarily varying classical-quantum wiretap channels W_1 and W_2, both with positive secrecy capacities are larger than the sum of the capacity of W_1 and the capacity of W_2 ([16]).

Using Theorem 3.1, we demonstrate the following Theorem:

Theorem 5.1: The super-activation occurs for arbitrarily varying classical-quantum wiretap channels.

Note that super-additivity does not imply super-activation, since here we consider channels with zero secrecy capacity.

We prove Theorem 5.1 by giving an example. Let $\theta = \{1,2\}$ and $A = \{0,1\}$. Let $H = H'$ be spanned by the orthonormal vectors $|0\rangle$ and $|1\rangle$. We define $(W_t, V_t)_{t\in\theta}$ as in the example in Section IV. We define $({W'}_t, {V'}_t)_{t\in\theta}$ by ${W'}_1(0) = \frac{3}{4}|0\rangle\langle 0| + \frac{1}{4}|1\rangle\langle 1|$, ${W'}_1(1) = \frac{1}{4}|0\rangle\langle 0| + \frac{3}{4}|1\rangle\langle 1|$, ${W'}_2(0) = \frac{3}{4}|0\rangle\langle 0| + \frac{1}{4}|1\rangle\langle 1|$, ${W'}_2(1) = \frac{1}{4}|0\rangle\langle 0| + \frac{3}{4}|1\rangle\langle 1|$, ${V'}_1(0) = |0\rangle\langle 0|$, ${V'}_1(1) = |1\rangle\langle 1|$, ${V'}_2(0) = |0\rangle\langle 0|$, ${V'}_2(1) = |1\rangle\langle 1|$.

Applying the Ahlswede Dichotomy we can obtain the following result. Although both $(W_t, V_t)_{t\in\theta}$ and $({W'}_t, {V'}_t)_{t\in\theta}$ have zero deterministic secrecy capacity, $(W_{t_1} \otimes {W'}_{t_2}, V_{t_1} \otimes {V'}_{t_2})_{(t_1,t_2)\in\theta^2}$ has a positive deterministic secrecy capacity. This shows that the research in quantum channels with channel uncertainty and eavesdropping can lead to some promising applications. This result sets a new challenging task for the design of media access control.

Remark 1: A preprint of the extended version of this paper can be found at arxiv [10]. Furthermore, to find a result similar to the Ahlswede Dichotomy for the entanglement generating capacity of an arbitrarily varying quantum channel, the results of this paper are applied to Devetak's method for entanglement generation. Some difficulties which occur are discussed in the extended version (cf. Conjecture 2.7 and the discussion in Section II).

References

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

[2] 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.

[3] R. Ahlswede and V. Blinovsky, Classical capacity of classical-quantum arbitrarily varying channels, IEEE Trans. Inform. Theory, Vol. 53, No. 2, 526-533, 2007.

[4] R. Ahlswede and N. Cai, Correlation sources help transmission over an arbitrarily varying channel, IEEE Trans. Inform. Theory, Vol. 43, No. 4, 1254-1255, 1997.

[5] 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.

[6] I. Bjelaković, H. Boche, and J. Sommerfeld, Capacity results for arbitrarily varying wiretap channels, Classical-quantum arbitrarily 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, 114-129, `arXiv:1209.5213`, 2012.

[7] 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.

[8] V. Blinovsky and M. Cai, Classical-quantum arbitrarily 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, 197-206, `arXiv:1208.1151`, 2012.

[9] H. Boche, M. Cai, N. Cai, and C. Deppe, Capacities of classical compound quantum wiretap and classical quantum compound wiretap channels, `arXiv:1202.0773v1`, to be pubilshed in Phys. Rev. A, 2012.

[10] H. Boche, M. Cai, and C. Deppe, Classical-Quantum Arbitrarily Varying Wiretap Channel—A Capacity Formula with Ahlswede Dichotomy—Resources, `arXiv:1307.8007` , 2013.

[11] H. Boche and J. Nötzel, Arbitrarily small amounts of correlation for arbitrarily varying quantum channel, accepted for publication in J. Math. Phys, `arXiv 1301.6063`, 2013.

[12] H. Boche and R. F. Wyrembelski, Capacity results and super-activation for wiretap channels with active wiretappers, IEEE Transactions on Information Forensics and Security, Vol. 8, No. 8, 1397-1408, 2013.

[13] 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.

[14] 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.

[15] A. S. Holevo, The capacity of quantum channel with general signal states, IEEE Trans. Inform. Theory, Vol. 44, 269-273, 1998.

[16] K. Li, A. Winter, X. B. Zou, G. C. Guo, Private capacity of quantum channels is not additive, Physical Review Letters, Vol. 103, No. 12, 120501, 2009.

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

[18] B. Schumacher and M. D. Westmoreland, Sending classical information via noisy quantum channels, Phys. Rev., Vol. 56, 131-138, 1997.

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

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

[21] M. Wilde, Quantum Information Theory, Cambridge University Press, 2013.

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