Capacities of classical compound quantum wiretap and classical quantum compound wiretap channels

Minglai Cai
Department of Mathematics
University of Bielefeld
Bielefeld, Germany
Email: mlcai@math.uni-bielefeld.de

*Ning Cai
The State Key Laboratory of
Integrated Services Networks
University of Xidian
Xian, China
Email: caining@mail.xidian.edu.cn

†Christian Deppe
Department of Mathematics
University of Bielefeld
Bielefeld, Germany
Email: cdeppe@math.uni-bielefeld.de

***Abstract*—We determine the capacity of the classical compound quantum wiretapper channel with channel state information at the transmitter. Moreover we derive a lower bound on the capacity of this channel without channel state information and determine the capacity of the classical quantum compound wiretap channel with channel state information at the transmitter.**

I. Introduction

The compound channel models transmission over a channel that may take a number of states, its capacity was determined by [5]. A compound channel with an eavesdropper is called a compound wiretap channel. It is defined as a family of pairs of channels $\{(W_t, V_t) : t = 1, \cdots, T\}$ with common input alphabet and possibly different output alphabets, connecting a sender with two receivers, one legal and one wiretapper, where t is called a state of the channel pair (W_t, V_t). The legitimate receiver accesses the output of the first channel W_t in the pair (W_t, V_t), and the wiretapper observes the output of the second part V_t in the pair (W_t, V_t), respectively, when a state t governs the channel. A code for the channel conveys information to the legal receiver such that the wiretapper knows nothing about the transmitted information. This is a generalization of Wyner's wiretap channel [14] to the case of multiple channel states.

We will be dealing with two communication scenarios. In the first one only the transmitter is informed about the index t (channel state information (CSI) at the transmitter), while in the second, the legitimate users have no information about that index at all (no CSI). The compound wiretap channels were recently introduced in [8]. An upper bound on the capacity under the condition that the average error goes to zero and the sender has no knowledge about CSI is obtained. The result of [8] was improved in [4] by using the stronger condition that the maximal error should go to zero. Furthermore, the capacity for the case with CSI was derived.

This paper is organized as follows. In Section II we present some known results for classical compound wiretap channel. In Section III we derive the capacity of the classical compound quantum wiretap channel with CSI and give a lower bound of the capacity without CSI. In this channel model the wiretapper uses classical quantum channels. In Section IV we derive the capacity of the classical quantum compound wiretap channel with CSI. In this model both the receiver and the wiretapper use classical quantum channels, and the set of the states can be both finite or infinite.

*the National Natural Science Foundation of China (Ref. No. 60832001)
†Project "Informationstheorie des Quanten-Repeaters" supported by the Federal Ministry of Education and Research (Ref. No. 01BQ1052)

II. Classical Compound Wiretap Channels

Let A, B, and C be finite sets, $P(A)$, $P(B)$, and $P(C)$ be the sets of probability distributions on A, B, and C, respectively. Let $\theta := \{1, \cdots, T\}$. For every $t \in \theta$ let W_t be a channel $A \to P(B)$ and V_t be a channel $A \to P(C)$. We call $(V_t, W_t)_{t\in\theta}$ a compound wiretap channel. W_t^n and V_t^n stand for the n-th memoryless extensions of stochastic matrices W_t and V_t. Here the first family represents the communication link to the legitimate receiver while the output of the latter is under control of the wiretapper. An (n, J_n) code for the compound wiretap channel $(V_t, W_t)_{t\in\theta}$ consists of stochastic encoders $\{E\} : \{1, \cdots, J_n\} \to P(A^n)$ and a collection of mutually disjoint sets $\{D_j \subset B^n : j \in \{1, \cdots, J_n\}\}$ (decoding sets). A non-negative number R is an achievable secrecy rate for the compound wiretap channel (W_t, V_t) in the case with CSI if there is a collection of (n, J_n) codes $(\{E_t : t = 1, \cdots, T\}, \{D_j : j \in \theta\})$ such that $\liminf_{n\to\infty} \frac{1}{n} \log J_n \geq R$, $\lim_{n\to\infty} \max_t \max_j \sum_{x^n\in A^n} E_t(x^n|j) W_t^n(D_j^c|x^n) = 0$, $\lim_{n\to\infty} \max_t I(J; Z_t^n) = 0$, where J is an uniformly distributed random variable with value in $\{1, \cdots, J_n\}$. Z_t^n are the resulting random variables at the output of wiretap channels V_t^n. $I(\cdot, \cdot)$ stands for the mutual information. A non-negative number R is an achievable secrecy rate for the compound wiretap channel (W_t, V_t) in the case without CSI if there is a collection of (n, J_n) codes $(E, \{D_j : j \in \theta\})$ such that $\liminf_{n\to\infty} \frac{1}{n} \log J_n \geq R$, $\lim_{n\to\infty} \max_t \max_j \sum_{x^n\in A^n} E(x^n|j) W_t^n(D_j^c|x^n) = 0$, $\lim_{n\to\infty} \max_t I(J; Z_t^n) = 0$. For $P \in P(A)$, $\delta > 0$ we denote by $\mathcal{T}_{P,\delta}^n$ the set of typical sequences in the sense of [12]. In the case with CSI, let $p_t'(x^n) := \begin{cases} \frac{p_t^n(x^n)}{p_t^n(\mathcal{T}_{p_t,\delta}^n)} , & \text{if } x^n \in \mathcal{T}_{p_t,\delta}^n \\ 0 , & \text{else} \end{cases}$ and $X^{(t)} := \{X_{j,l}^{(t)}\}_{j\in\{1,\cdots,J_n\}, l\in\{1,\cdots,L_{n,t}\}}$ be a family of random matrices whose entries are i.i.d. according to p_t'. For

978-1-4673-2579-0/12/$31.00 ©2012 IEEE

any $\omega > 0$, if we set $J_n = \lfloor 2^{n(\min_{t\in\theta}(I(p_t,V_t)-\frac{1}{n}\log L_{n,t})-\mu}\rfloor$, where μ is a positive constant which does not depend on j or t, and can be arbitrarily small when ω goes to 0, then there are such $\{D_j : j = 1, \cdots, J_n\}$ that for all $t \in \theta$

$$Pr\left(\sum_{j=1}^{J_n}\frac{1}{J_n}\sum_{l=1}^{L_{n,t}}\frac{1}{L_{n,t}}W_t^n(D_j^c|X_{j,l}^{(t)}) > \sqrt{T}2^{-n\omega/2}\right) \leq \sqrt{T}2^{-n\omega/2} . \quad (1)$$

Since here only the error of the legitimate receiver is analyzed, for the result above just the channels V_t, but not those of the wiretapper, are regarded. It was shown in [4] that by (1), the largest achievable rate, called capacity, of the compound wiretap channel with CSI at the transmitter $C_{S,CSI}$, is given by

$$C_{S,CSI} = \min_{t\in\theta}\max_{V\to A\to(BZ)_t}(I(V,B_t) - I(V,Z_t)) , \quad (2)$$

where B_t are the resulting random variables at the output of legal receiver channels. Z_t are the resulting random variables at the output of wiretapper's channels. Analogously, in case without CSI, the idea is similar to the case with CSI: Let $p'(x^n) := \begin{cases}\frac{p^n(x^n)}{p^n(\mathcal{T}_{p,\delta}^n)} & \text{if } x^n \in \mathcal{T}_{p,\delta}^n \\ 0 & \text{else}\end{cases}$ and $X^n := \{X_{j,l}\}_{j\in\{1,\cdots,J_n\},l\in\{1,\cdots,L_n\}}$ be a family of random matrices whose components are i.i.d. according to p'. For any $\omega > 0$ define $J_n = \lfloor 2^{n(\min_{t\in\theta}(I(p_t,V_t)-\frac{1}{n}\log L_n)-\mu}\rfloor$, with some suitable positive constant μ which does not depend on j, t, we can find such $\{D_j\}$ that for all $t \in \theta$

$$Pr\left(\sum_{j=1}^{J_n}\frac{1}{J_n}\sum_{l=1}^{L_n}\frac{1}{L_n}W_t^n(D_j(X)^c|X_{j,l}) > \sqrt{T}2^{-n\omega/2}\right) \leq \sqrt{T}2^{-n\omega/2} . \quad (3)$$

In view of (3) the capacity of the compound wiretap channel without CSI at the transmitter C_S is lower bounded by (see [4]),

$$C_S \geq \max_{V\to A\to(BZ)_t}(\min_{t\in\theta} I(V,B_t) - \max_t I(V,Z_t)) . \quad (4)$$

III. Classical Compound Quantum Wiretap Channels

Let A and B be finite sets, and let H be a finite-dimensional complex Hilbert space. Let $P(A)$ and $P(B)$ be the sets of probability distributions on A and B, respectively, and $\mathcal{S}(H)$ be the space of self-adjoint, positive-semidefinite bounded linear operators with trace 1 on H. Let $\theta := \{1, \cdots, T\}$. For every $t \in \theta$ let W_t be a channel $A \to P(B)$ and V_t be a classical quantum channel, i.e., a map $A \to \mathcal{S}(H)$: $A \ni x \to V_t(x) \in \mathcal{S}(H)$. We define $(V_t, W_t)_{t\in\theta}$ as a classical compound quantum wiretap channel. Associate to V_t is the channel map on n-block $V_t^{\otimes n}$: $A^n \to \mathcal{S}(H^{\otimes N})$ with $V_t^{\otimes n}(x^n) := V_t(x_1)\otimes\cdots\otimes V_t(x_n)$. $S(\cdot)$ denotes the von Neumann entropy and $\chi(\cdot,\cdot)$ denotes the Holevo χ quantity. An (n, J_n) code for the classical compound quantum wiretap channel $(V_t, W_t)_{t\in\theta}$ consists of stochastic encoders $\{E\} : \{1, \cdots, J_n\} \to P(A^n)$ and a collection of mutually disjoint sets $\{D_j \subset B^n : j = 1, \cdots, J_n\}$ (decoding sets). A non-negative number R is an achievable secrecy rate for the classical compound quantum wiretap channel $(W_t, V_t)_{t\in\theta}$ with CSI if there is an (n, J_n) code $(\{E_t : t \in \theta\}, \{D_j : j = 1, \cdots, J_n\})$ such that $\liminf_{n\to\infty}\frac{1}{n}\log J_n \geq R$, $\lim_{n\to\infty}\max_t\max_j\sum_{x^n\in A^n}E_t(x^n|j)W_t^n(D_j^c|x^n) = 0$, and $\lim_{n\to\infty}\max_t\chi(J; Z_t^{\otimes n}) = 0$, where J is an uniformly distributed random variable with value in $\{1, \cdots, J_n\}$. Z_t are the resulting random states at the output of V_t. A non-negative number R is an achievable secrecy rate for the classical compound quantum wiretap channel $(W_t, V_t)_{t\in\theta}$ without CSI if there is an (n, J_n) code $(E, \{D_j : j = 1, \cdots, J_n\})$ such that $\liminf_{n\to\infty}\frac{1}{n}\log J_n \geq R$, $\lim_{n\to\infty}\max_t\max_j\sum_{x^n\in A^n}E(x^n|j)W_t^n(D_j^c|x^n) = 0$ and $\lim_{n\to\infty}\max_t\chi(J; Z_t^{\otimes n}) = 0$.

Theorem 1: The capacity of the classical compound quantum wiretap channel $(W_t, V_t)_{t\in\theta}$ in the case with CSI at the transmitter $C_{S,CSI}$ is given by

$$C_{S,CSI} = \min_{t\in\theta}\max_{P\to A\to B_tZ_t}(I(P,B_t) - \limsup_{n\to\infty}\frac{1}{n}\chi(P, Z_t^{\otimes n})) . \quad (5)$$

Respectively, in the case without CSI, the capacity of the classical compound quantum wiretap channel $(W_t, V_t)_{t\in\theta}$ C_S is lower bounded as follows

$$C_S \geq \max_{P\to A\to B_tZ_t}(\min_{t\in\theta} I(P,B_t) - \max_t\chi(P,Z_t)) , \quad (6)$$

where B_t are the resulting random variables at the output of legal receiver channels. Z_t are the resulting random states at the output of wiretap channels.

Proof: Let p'_t, $X^{(t)}$, and D_j be defined like in classical case. Then (1) still holds since the sender transmits through a classical channel to the legitimate receiver. We abbreviate $\mathcal{X} := \{X^{(t)} : t \in \theta\}$. (Analogously, in the case without CSI, let p', X^n, and D_j be defined like in classical case, then (3) still holds.)

For $\rho \in \mathcal{S}(H)$, and $\alpha > 0$ there exists an orthogonal subspace projector $\Pi_{\rho,\alpha}$ commuting with $\rho^{\otimes n}$ and satisfying (see [12])

$$\mathrm{tr}\left(\rho^{\otimes n}\Pi_{\rho,\alpha}\right) \geq 1 - \frac{d}{\alpha^2} , \quad (7)$$

$$\mathrm{tr}\left(\Pi_{\rho,\alpha}\right) \leq 2^{nS(\rho)+Kd\alpha\sqrt{n}} , \quad (8)$$

$$\Pi_{\rho,\alpha}\cdot\rho^{\otimes n}\cdot\Pi_{\rho,\alpha} \leq 2^{-nS(\rho)+Kd\alpha\sqrt{n}}\Pi_{\rho,\alpha} , \quad (9)$$

where $a := \#\{A\}$, $d := \dim H$, and K is a positive constant. For $P \in P(A)$, $\alpha > 0$ and $x^n \in \mathcal{T}_P^n$ there exists an orthogonal subspace projector $\Pi_{V,\alpha}(x^n)$ commuting with $V_{x^n}^{\otimes n}$ and satisfying (see [12])

$$\mathrm{tr}\left(V^{\otimes n}(x^n)\Pi_{V,\alpha}(x^n)\right) \geq 1 - \frac{ad}{\alpha^2} , \quad (10)$$

$$\mathrm{tr}\left(\Pi_{V,\alpha}(x^n)\right) \leq 2^{nS(V|P)+Kad\alpha\sqrt{n}} , \quad (11)$$

$$\Pi_{V,\alpha}(x^n)\cdot V^{\otimes n}(x^n)\cdot\Pi_{V,\alpha}(x^n)$$
$$\leq 2^{-nS(V|P)+Kad\alpha\sqrt{n}}\Pi_{V,\alpha}(x^n)\ , \tag{12}$$

$$\mathrm{tr}\left(V^{\otimes n}(x^n)\cdot\Pi_{PV,\alpha\sqrt{a}}\right)\geq 1-\frac{ad}{\alpha^2}\ , \tag{13}$$

Let

$$Q_t(x^n):=\Pi_{PV_t,\alpha\sqrt{a}}\Pi_{V_t,\alpha}(x^n)\cdot V_t^{\otimes n}(x^n)\cdot\Pi_{V_t,\alpha}(x^n)\Pi_{PV_t,\alpha\sqrt{a}}$$

where α will be defined later. Let ρ be a state, and X be a positive operator with $X\leq id$ (the identity matrix) and $1-\mathrm{tr}(\rho X)\leq\lambda\leq 1$. It is sown in [13] that

$$\|\rho-\sqrt{X}\rho\sqrt{X}\|\leq\sqrt{8\lambda}\ . \tag{14}$$

It follows from (14), (7), (13), and the fact that $\Pi_{PV_t,\alpha\sqrt{a}}$ and $\Pi_{V_t,\alpha}(x^n)$ are both projection matrices, that for any t and x^n

$$\|Q_t(x^n)-V_t^{\otimes n}(x^n)\|\leq\frac{\sqrt{8(ad+d)}}{\alpha}\ . \tag{15}$$

We set $\Theta_t:=\sum_{x^n\in\mathcal{T}^n_{p_t,\delta}}{p'}^n_t(x^n)Q_t(x^n)$. For given z^n and t, $\langle z^n|\Theta_t|z^n\rangle$ is the expected value of $\langle z^n|Q_t(x^n)|z^n\rangle$ under the condition $x^n\in\mathcal{T}^n_{p_t,\delta}$.

Lemma 1 (see [2]): Let $\mathcal{V}$ be a finite dimensional Hilbert space, $X_1,\cdots,X_L$ be a sequence of i.i.d. random variables with values in $\mathcal{S}(\mathcal{V})$ such that $X_i\leq\mu\cdot id_{\mathcal{V}}$ for all $i\in\{1,\cdots,L\}$, and $\epsilon\in(0,1)$. Let p be a probability distribution on $\{X_1,\cdots,X_L\}$, $\rho:=\sum_i p(X_i)X_i$ be the expected value of X_i, and $\Pi'_{\rho,\lambda}$ be the projector onto the subspace spanned by the eigenvectors of ρ whose corresponding eigenvalues are greater than $\frac{\lambda}{\dim\mathcal{V}}$. Then

$$Pr\left(\|L^{-1}\sum_{i=1}^{L}X_i-\Pi'_{\rho,\lambda}\cdot\rho\cdot\Pi'_{\rho,\lambda}\|>\epsilon\right)$$
$$\leq 2\cdot(\dim\mathcal{V})\exp\left(-L\frac{\epsilon^2\lambda}{2\ln 2(\dim\mathcal{V})\mu}\right)\ . \tag{16}$$

Let $\mathcal{V}$ be the image of $\Pi_{P,\alpha\sqrt{a}}$. By (8) we have $\dim\mathcal{V}\leq 2^{nS(P)+Kd\alpha\sqrt{an}}$. Furthermore, by (12)

$$Q_t(x^n)\leq 2^{-n\cdot S(V_t|P)+Kad\alpha\sqrt{n}}\cdot id_{\mathcal{V}}\ . \tag{17}$$

Thus, by (16) and (17)

$$Pr\left(\|\sum_{l=1}^{L_{n,t}}\frac{1}{L_{n,t}}Q_t(X^{(t)}_{j,l})-\Pi'_{\Theta_t,\lambda}\Theta_t\Pi'_{\Theta_t,\lambda}\|>\frac{1}{2}\epsilon\right)$$
$$\leq 2\cdot 2^{n(S(P)+Kd\alpha\sqrt{an})}$$
$$\cdot\exp\left(-L_{n,t}\frac{\epsilon^2}{8\ln 2}\lambda\cdot 2^{n(-\chi(P,Z_t))+Kd\alpha\sqrt{n}(\sqrt{a}-1)}\right)\ ,$$

since $S(P)-S(V_t|P)=\chi(P,Z_t)$.

Notice that $\|\Theta_t-\Pi'_{\Theta_t,\lambda}\Theta_t\Pi'_{\Theta_t,\lambda}\|\leq\lambda$. Let $\lambda:=\frac{1}{2}\epsilon$ and n large enough, then

$$Pr\left(\|\sum_{l=1}^{L_{n,t}}\frac{1}{L_{n,t}}Q_t(X_{j,l})-\Theta_t\|>\epsilon\right)$$
$$\leq\exp\left(-L_{n,t}\cdot 2^{-n(\chi(P,Z_t)+\zeta)}\right)\ , \tag{18}$$

where ζ is some suitable positive constant, which does not depend on j, t, and can be arbitrarily small when ϵ goes to 0. Let $L_{n,t}=2^{n(\chi(P,Z_t)+2\zeta)}$ and n be large enough, then by (18) for all j the following holds,

$$Pr\left(\|\sum_{l=1}^{L_{n,t}}\frac{1}{L_{n,t}}Q_t(X^{(t)}_{j,l})-\Theta_t\|>\epsilon\right)\leq\exp(-2^{n\zeta})\ , \tag{19}$$

and

$$Pr\left(\|\sum_{l=1}^{L_{n,t}}\frac{1}{L_{n,t}}Q_t(X^{(t)}_{j,l})-\Theta_t\|<\epsilon\ \forall t\right)\geq 1-2^{-n\upsilon}\ , \tag{20}$$

where υ is some suitable positive constant which does not depend on j and t. (Analogously in the case without CSI, let $L_n=2^{n\max_t(\chi(P,Z_t)+\delta)}$ and n be large enough, then we can find some positive constant υ such that

$$Pr\left(\|\sum_{l=1}^{L_n}\frac{1}{L_n}Q_t(X^{(t)}_{j,l})-\Theta_t\|<\epsilon\ \forall t\right)\geq 1-2^{-n\upsilon} \tag{21}$$

for all j.)

From (1) and (20), it follows: For any given $\epsilon>0$, if n is large enough then the event

$$\left(\bigcap_t\left\{\sum_{j=1}^{J_n}\frac{1}{J_n}\sum_{l=1}^{L_{n,t}}\frac{1}{L_{n,t}}W_t^n(D_j^c(\mathcal{X})|X^{(t)}_{j,l})\leq\epsilon\right\}\right)$$
$$\cap\left(\bigcap_j\left\{\|\sum_{l=1}^{L_{n,t}}\frac{1}{L_{n,t}}Q_t(X^{(t)}_{j,l})-\Theta_t\|\leq\epsilon\ \forall t\right\}\right)$$

has a positive probability. This means that we can find a realization $x^{(t)}_{j,l}$ of $X^{(t)}_{j,l}$ with a positive probability such that for all $t\in\theta$, we have

$$\sum_{j=1}^{J_n}\frac{1}{J_n}\sum_{l=1}^{L_{n,t}}\frac{1}{L_{n,t}}W_t^n(D_j^c|x^{(t)}_{j,l})\leq\epsilon\ ,$$

and

$$\|\sum_{l=1}^{L_{n,t}}\frac{1}{L_{n,t}}Q_t(x^{(t)}_{j,l})-\Theta_t\|\leq\epsilon\ \forall j\ .$$

Let $R:=\min_{t\in\theta}\max_{P\to A\to B_tZ_t}\left(I(P,B_t)-\chi(P,Z_t)\right)+\gamma$ for any $\gamma>0$, we have

$$\liminf_{n\to\infty}\frac{1}{n}\log J_n\geq R \tag{22}$$

$$\lim_{n\to\infty}\max_t\max_j\sum_{x^n\in A^n}E_t(x^n|j)W_t^n(D_j^c|x^n)=0\ , \tag{23}$$

where E_t is the random outputs of $(X^{(t)}_{j,l})_l$. Choose a sufficiently large but fixed α in (15) such that for all j it holds $\|V_t^{\otimes n}(x^{(t)}_{j,l})-Q_t(x^{(t)}_{j,l})\|<\epsilon$. In this case for any given $j'\in\{1,\cdots,J_n\}$ we have

$$\|\sum_{l=1}^{L_{n,t}}\frac{1}{L_{n,t}}V_t^{\otimes n}(x^{(t)}_{j',l})-\Theta_t\|\leq 2\epsilon \tag{24}$$

and $\|\mathbb{E}_j \sum_{l=1}^{L_{n,t}} \frac{1}{L_{n,t}} V_t^{\otimes n}(x_{j,l}^{(t)}) - \Theta_t\| \leq \epsilon$ for any probability distribution uniformly distributed on $\{1, \cdots, J_n\}$.

Lemma 2 (Fannes inequality [13]): Let $\mathfrak{X}$ and $\mathfrak{Y}$ be two states in a d-dimensional complex Hilbert space and $\|\mathfrak{X} - \mathfrak{Y}\| \leq \mu < \frac{1}{e}$, then

$$|S(\mathfrak{X}) - S(\mathfrak{Y})| \leq \mu \log d - \mu \log \mu \ . \tag{25}$$

If J is a probability distribution uniformly distributed on $\{1, \cdots, J_n\}$, then from the inequality (24) and Lemma 2 we have $\chi(J; Z_t^{\otimes n}) \leq 3\epsilon \log d - \epsilon \log \epsilon - 2\epsilon \log 2\epsilon$. We have

$$\lim_{n\to\infty} \max_t \chi(J; Z_t^{\otimes n}) = 0 \ . \tag{26}$$

(Analogously there is a realization $x_{j,l}$ of $X_{j,l}$ with a positive probability such that $\sum_{j=1}^{J_n} \frac{1}{J_n} \sum_{l=1}^{L_n} \frac{1}{L_n} W_t^n(D_j^c | x_{j,l}) \leq \epsilon$ for all $t \in \theta$ and $\lim_{n\to\infty} \max_{t\in\theta} \chi(J; Z_t^{\otimes n}) = 0$.) Combining (1) and (26) we obtain the results:

$$C_{S,CSI} \geq \min_{t\in\theta} \max_{V\to A\to B_t Z_t} (I(V, B_t) - \chi(V, Z_t)) \ ,$$

respectively

$$C_S \geq \max_{P\to A\to B_t Z_t} (\min_{t\in\theta} I(P, B_t) - \max_t \chi(P, Z_t)) \ .$$

Consider a sequence of an (n, J_n) code $(\mathcal{C}_n)$ such that $\sup_{t\in\theta} \frac{1}{J_n} \sum_{j=1}^{J_n} \sum_{x^n\in A^n} E(x^n|j) W_t^n(D_j^c|x^n) =: \epsilon_{1,n}$ and $\sup_{t\in\theta} \chi(J; Z_t^{\otimes n}) =: \epsilon_{2,n}$ where $\lim_{n\to\infty} \epsilon_{1,n} = 0$ and $\lim_{n\to\infty} \epsilon_{2,n} = 0$. Let $C(V_t, W_t)$ denote the secretey capacity of the wiretap channel (V_t, W_t) in the sense of [12]. Choose $t' \in \theta$ such that $C(V_{t'}, W_{t'}) = \min_{t\in\theta} C(V_t, W_t)$. It is well-known, in information theory, that even in the case without wiretapper (we have only one classical channel $W_{t'}$), the capacity cannot exceed $I(J; B_{t'}) + \xi$ for any constant $\xi > 0$. Thus, the capacity of a quantum wiretap channel $(W_{t'}, V_{t'})$ cannot be greater than

$$I(J; B_{t'}) + \xi \leq [I(J; B_{t'}) - \limsup_{n\to\infty} \frac{1}{n} \chi(J; Z_{t'}^{\otimes n})] + \epsilon$$

for any $\epsilon > 0$. Since we cannot exceed the capacity of the worst wiretap channel we have

$$C_{S,CSI} \leq \min_{t\in\theta} \max_{V\to A\to B_t Z_t} (I(V, B_t) - \limsup_{n\to\infty} \frac{1}{n} \chi(V, Z_t^{\otimes n})) \ .$$

■

IV. Classical Quantum Compound Wiretap Channel with CSI

Let H be a finite-dimensional complex Hilbert space. Let $\mathcal{S}(H)$ be the space of self-adjoint, positive-semidefinite bounded linear operators on H with trace 1. For every $t \in \theta$ let W_t respectively V_t be quantum channels, i.e., completely positive trace preserving maps $\mathcal{S}(H) \to \mathcal{S}(H)$. An (n, J_n, λ) code for the classical quantum compound wiretap channel $(W_t, V_t)_{t\in\theta}$ consists of a family of vectors $\{w(j) : j = 1, \cdots, J_n\} \subset S(H^{\otimes N})$ and a collection of positive semi-definite operators $\{D_j : j \in \{1, \cdots, J_n\}\} \subset S(H^{\otimes N})$ which is a partition of the identity, i.e. $\sum_{j=1}^{J_n} D_j = id_{H^{\otimes N}}$. A non-negative number R is an achievable secrecy rate for the classical quantum compound wiretap channel $(W_t, V_t)_{t\in\theta}$ with CSI if there is an (n, J_n, λ) code $(\{w_t : t \in \theta\}, \{D_j : j\})$ such that $\liminf_{n\to\infty} \frac{1}{n} \log J_n \geq R$, $\lim_{n\to\infty} \max_t \frac{1}{J_n} \sum_{j=1}^{J_n} \mathrm{tr}\left(W_t^{\otimes n}(w_t(j)) D_j\right) \geq 1 - \lambda$, $\lim_{n\to\infty} \max_t \chi(J; Z_t^{\otimes n}) = 0$, where J is an uniformly distributed random variable with value in $\{1, \cdots, J_n\}$. Z_t are the resulting random states at the output of wiretap channels.

Theorem 2: The capacity of the classical quantum compound wiretap channel in the case with CSI is given by

$$C_{CSI} = \lim_{n\to\infty} \min_{t\in\theta} \max_{P, w_t} \frac{1}{n} (\chi(P, B_t^{\otimes n}) - \chi(P, Z_t^{\otimes n})), \tag{27}$$

where B_t are the resulting random states at the output of legal receiver channels. Z_t are the resulting random states at the output of wiretap channels.

Proof: Our idea is to send the information in two parts, firstly, we send the state information with finite blocks of finite bits with a code C_1 to the receiver, and then, depending on t, we send the message with a code $C_2^{(t)}$ in the second part. We don't require that the first part should be secure against the wiretapper, since we assume that the wiretapper already has full knowledge of the CSI. By ignoring the security against the wiretapper, we have only to consider the compound channel $(W_t)_{t\in\theta}$. Let $W = (W_t)_t$ be an arbitrary compound classical-quantum-channel. Then by [3], for each $\lambda \in (0, 1)$ the λ-capacity $C(W, \lambda)$ equals

$$C(W, \lambda) = \inf_t \max_p \chi(p, W_t) \ . \tag{28}$$

If $\min_t \max_p \chi(p, W_t) > 0$, then for any required upper bound $\lambda > 0$, the sender may send the state to the legal receiver by a code of sufficiently large but constant length such that with the probability at least $1 - \frac{\lambda}{2}$ the legal receiver decodes correctly. In case $\min_t \max_p \chi(p, W_t) = 0$, we need to do nothing because in this case the right hand side of (27) is zero. 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 t, then we only have to consider the single wiretap channel (W_t, V_t). In [6] and [7] it is shown that there exists an (n, J_n, λ) code for the quantum wiretap channel (W, V) with

$$\log J_n = \max_{P,w} (\chi(P, B^{\otimes n}) - \chi(P, Z^{\otimes n})) - \epsilon \ , \tag{29}$$

for any $\epsilon > 0$, where B is the resulting random state at the output of legal receiver channel. Z is the output of the wiretap channel. When the sender and the legal receiver both know t, they can build an $(n, J_{n,t}, \lambda)$ code $C_2^{(t)}$ where

$$\log J_{n,t} = \max_{P,w_t} (\chi(V, B_t^{\otimes n}) - \chi(V, Z_t^{\otimes n})) - \epsilon \ . \tag{30}$$

Thus,

$$C_{CSI} \geq \lim_{n\to\infty} \min_{t\in\theta} \max_{P,w_t} \frac{1}{n} (\chi(P, B_t^{\otimes n}) - \chi(P, Z_t^{\otimes n})) \ . \tag{31}$$

For any $\epsilon > 0$ choose $t' \in \theta$ such that $C(V_{t'}, W_{t'}) \leq \inf_{t\in\theta} C(V_t, W_t) + \epsilon$. From [6] and [7], we know that the

capacity of the quantum wiretap channel $(W_{t'}, V_{t'})$ cannot be greater than $\lim_{n\to\infty} \max_{P,w_{t'}} \frac{1}{n}(\chi(P, B_{t'}^{\otimes n}) - \chi(P, Z_{t'}^{\otimes n}))$. Since we cannot exceed the capacity of the worst wiretap channel, we have

$$C_{CSI} \leq \lim_{n\to\infty} \min_{t\in\theta} \max_{P,w_t} \frac{1}{n}(\chi(P, B_t^{\otimes n}) - \chi(P, Z_t^{\otimes n})). \quad (32)$$

This together with (31) completes the proof of Theorem 2. ■

If for every $t \in \theta$ and $n \in \mathbb{N}$, $I(P, B_t^{\otimes n}) \geq I(P, Z_t^{\otimes n})$ for all $P \in P(A)$ and $\{w_t(j) : j = 1, \cdots, J_n\} \subset \mathcal{S}(H^n)$, we have $C_{CSI} = \min_{t\in\theta} \max_{P,w_t}(\chi(P, B_t) - \chi(P, Z_t))$ (see [11]).

So far, $|\theta|$ was finite. Now we consider the case when $|\theta|$ can be arbitrary.

Theorem 3: For an arbitrary set θ we have

$$C_{CSI} = \lim_{n\to\infty} \inf_{t\in\theta} \max_{P,w_t} \frac{1}{n}(\chi(P, B_t^{\otimes n}) - \chi(P, Z_t^{\otimes n})) \ . \quad (33)$$

Proof: Let $W : \mathcal{S}(H) \to \mathcal{S}(H)$ be a linear map, then let

$$\|W\|_\diamond := \sup_{n\in\mathbb{N}} \max_{a\in S(\mathbb{C}^n\otimes H), \|a\|_1=1} \|(id_n \otimes W)(a)\|_1 \ , \quad (34)$$

where $\|\cdot\|_1$ stands for the trace norm. It is well known (see [10]) that $\|W \otimes W'\|_\diamond = \|W\|_\diamond \cdot \|W'\|_\diamond$.

A τ-net in the space of the completely positive trace preserving maps is a finite set $\left(W^{(k)}\right)_{k=1}^K$ with the property that for each W there is a $k \in \{1, \cdots, K\}$ with $\|W - W^{(k)}\|_\diamond < \tau$.

Lemma 3 (τ−net [9]): For any $\tau \in (0, 1]$ there is a τ-net of quantum-channels $\left(W_t^{(k)}\right)_{k=1}^K$ in the space of the completely positive trace preserving maps with $K \leq (\frac{3}{\tau})^{2d^4}$, where $d = \dim H$.

If $|\theta|$ is arbitrary, then for any $\xi > 0$ let $\tau = \frac{\xi}{-\log \xi}$. By Lemma 3 there exists a finite set θ' with $|\theta'| \leq (\frac{3}{\tau})^{2d^4}$ and τ-nets $(W_{t'})_{t'\in\theta'}$, $(V_{t'})_{t'\in\theta'}$ such that for every $t \in \theta$ we can find a $t' \in \theta'$ with $\|W_t - W_{t'}\|_\diamond \leq \tau$ and $\|V_t - V_{t'}\|_\diamond \leq \tau$. For every $t' \in \theta'$ the legal transmitters build a code $C_2^{(t')} = \{w_{t'}, \{D_{t',j} : j\}\}$. Since by [6], the error of the code $C_2^{(t')}$ decreases exponentially to its length, we can find an $N = O(-\log \xi)$ such that for all $t' \in \theta'$ it holds

$$\frac{1}{J_N} \sum_{j=1}^{J_N} \mathrm{tr}\left(W_{t'}^{\otimes N}(w_{t'}(j)) D_{t',j}\right) \geq 1 - \lambda - \xi \ , \quad (35)$$

$$\chi(J; Z_{t'}^{\otimes N}) \leq \xi \ . \quad (36)$$

The sender sends "t'" if obtaining the state information "t", we have $\mathrm{tr}\left[\left(W_t^{\otimes N} - W_{t'}^{\otimes N}\right)(w_{t'}(j))\right] \leq N\tau$, because we can purificat $w_{t'}(j)$ in $H^{\otimes N} \times H^{\otimes N}$ and then use the definition of $\|\cdot\|_\diamond$. Therefore,

$$\frac{1}{J_N}\left(\sum_{j=1}^{J_N} \mathrm{tr}(W_t^{\otimes N}(w_{t'}(j)) D_{t',j}) - \sum_{j=1}^{J_N} \mathrm{tr}(W_{t'}^{\otimes N}(w_{t'}(j)) D_{t',j})\right) \leq N\tau \ . \quad (37)$$

For any probability distribution J uniformly distributed on $\{1, \cdots, J_N\}$, by Lemma 2 we have

$$\|\chi(J, V_t) - \chi(J, V_{t'})\| \leq 2\tau \log d - 2\tau \log \tau \ , \quad (38)$$

since $\|V_t(\rho) - V_{t'}(\rho)\| \leq \tau$ for all $\rho \in \mathcal{S}(H)$ if $\|V_t - V_{t'}\|_\diamond \leq \tau$. From (37) and (38) we obtain

$$\max_t \frac{1}{J_N} \sum_{j=1}^{J_N} \mathrm{tr}\left(W_t^{\otimes N}(w_{t'}(j)) D_{t',j}\right) \geq 1 - \lambda - \xi - N\tau \ ,$$

$$\chi(J; Z_t^{\otimes N}) \leq \xi + 2\tau \log d - 2\tau \log \tau \ .$$

Since $N\tau$ and $2\tau \log d$ both tend to zero when ξ goes to zero, we have $\lim_{n\to\infty} \max_t \frac{1}{J_n} \sum_{j=1}^{J_n} \mathrm{tr}\left(W_t^{\otimes n}(w_{t'}(j)) D_{t',j}\right) \geq 1-\lambda$, $\lim_{n\to\infty} \chi(J; Z_t^{\otimes n}) = 0$. The bits that the sender uses to transform the CSI is large but constant, so it is still negligible compared to the second part. we have

$$C_{CSI} > \lim_{n\to\infty} \inf_{t\in\theta} \max_{P,w_t} \frac{1}{n}(\chi(P, B_t^{\otimes n}) - \chi(P, Z_t^{\otimes n})) \ . \quad (39)$$

For the converse, we consider a worst t. ■

ACKNOWLEDGMENT

We thank Igor Bjelakovic and Holger Boche for useful discussions. Support by the Bundesministerium für Bildung und Forschung (BMBF) via grant 01BQ1052 is gratefully acknowledged.

REFERENCES

[1] R. Ahlswede, I. Bjelakovic, H. Boche, and J. Nötzel, Quantum capacity under adversarial quantum noise: arbitrarily varying quantum channels, submitted to Communications in Mathematical Physics.

[2] R. Ahlswede and A. Winter, Strong converse for identification via quantum channels, IEEE Trans. Inform. Theory, Vol. 48, No. 3, 569-579, 2002. Addendum: IEEE Trans. Inform. Theory, Vol. 49, No. 1, 346, 2003.

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

[4] I. Bjelakovic, H. Boche, and J. Sommerfeld, Capacity results for compound wiretap channels, CoRR abs, 1103-2013, 2011.

[5] D. Blackwell, L. Breiman, and A. J. Thomasian, The capacity of a class of channels, Ann. Math. Stat. Vol. 30, No. 4, 1229-1241, 1959.

[6] 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.

[7] 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.

[8] Y. Liang, G. Kramer, H. Poor, and S. Shamai, Compound wiretap channels, EURASIP Journal on Wireless Communications and Networking, Article ID 142374, 2008.

[9] V. D. Milman and G. Schechtman, Asymptotic Theory of Finite Dimensional Normed Spaces. Lecture Notes in Mathematics 1200, Springer-Verlag, corrected second printing, Berlin, 2001.

[10] V. Paulsen, Completely Bounded Maps and Operator Algebras, Cambridge Studies in Advanced Mathematics 78, Cambridge University Press, Cambridge, UK, 2002.

[11] S. Watanabe, Remarks on Private and Quantum Capacities of More Capable and Less Noisy Quantum Channels, arXiv:1110-5746, Vol. [quant-ph], 2011.

[12] M. Wilde, From Classical to Quantum Shannon Theory, arXiv:1106-1445, 2011.

[13] A. Winter, Coding theorem and strong converse for quantum channels, IEEE Trans. Inform. Theory, Vol. 45, No. 7, 2481-2485, 1999.

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