Universal superposition codes: capacity regions of compound quantum broadcast channel with confidential messages

Holger Boche
Munich Center for Quantum Science and Technology (MCQST)
80799 München, Germany
Technische Universität München
Lehrstuhl für Theoretische Informationstechnik
80290 München, Germany
Email: boche@tum.de

Gisbert Janßen, Sajad Saeedinaeeni
Technische Universität München
Lehrstuhl für Theoretische Informationstechnik
80290 München, Germany
Email: (gisbert.janssen sajad.saeedinaeeni)@tum.de

Abstract—We derive universal codes for transmission of broadcast and confidential messages over classical-quantum-quantum and fully quantum channels. These codes are robust to channel uncertainties considered in the compound model. To construct these codes we generalize random codes for transmission of public messages, to derive a universal superposition coding for the compound quantum broadcast channel. As an application, we give a multi-letter characterization of regions corresponding to capacity of the compound quantum broadcast channel for transmitting broadcast and confidential messages simultaneously. This is done for two types of broadcast messages, one called public and the other common.

A full version of this work has been published in Journal of Mathematical Physics 61, 042204 (2020) [13]

I. Introduction

Assuming the state of a channel, connecting two sides of a communication, to be perfectly known by the communicating parties is an idealization that often cannot be realized in real-world applications. The compound channel model, in which the communicating parties only have access to an uncertainty set to which the state of the channel belongs, invokes coding strategies that are robust to such uncertainties. Relaxing the assumption of the perfectly known channel, requires coding strategies that work for all channels belonging to a set of possibly infinite cardinality and are hence, significantly more sophisticated. The compound model consists of an indexed set of channels \( \{ W_s \}_{s \in \mathcal{S}} \). A channel from this uncertainty set is used in a memoryless fashion for communication, requiring the codes to be reliable for the set \( \{ W^{(n)}_s \}_{s \in \mathcal{S}} \), where the channel is used \( n \in \mathbb{N} \) times.

Information theoretically, the compound model has yielded intriguing properties. One of the interesting information theoretic properties of the compound channel, is that in general, a strong converse cannot be established on the capacity of the compound channel for message transmission, when upper-bounding of the average decoding error is considered. This holds even for finite uncertainty sets [1], [2], [9]. This observation implies that a second order capacity theorem cannot be developed in this case. Further, calculation of the so called \( \epsilon \)-capacity of the compound channel under the average error criterion is still an open question. We note however, that determining a second order \( \epsilon \)-capacity for the compound channel is not possible, due to the observation, that there are examples of the compound channel where the optimistic \( \epsilon \)-capacity is strictly larger than its pessimistic one (see [11] Remark 13).

In [4] Section 3, Ahlswede posed the question of whether or not there exist simple recursive formulas for the \( \epsilon \)-capacity of the compound channel. This question, being of great practical significance as discussed in the concluding remarks here, was answered negatively by authors of [11]. The non-computability of \( \epsilon \)-capacity of the compound channel on the set of computable channels and under average error criterion, is implied by non-continuity of this function in its error input. We note also, the importance of codes developed for the compound channel, for another prominent channel model, namely the arbitrarily varying channel (see e.g. [3]), where an active jamming party is present.

We consider the compound quantum broadcast channel, connecting one sender to two receivers of different permissions or priorities. The channel is used to perform an integrated task, in which a confidential message, kept secret from the third party, is communicated simultaneously with a broadcast message available to both receivers. The requirements on the broadcast message, determine two communication scenarios. In the first scenario, we consider the case where both receivers are required to decode the broadcast message. We refer to this message as the common message. In the second scenario the decoding condition is relaxed on one of the receivers. That is, the third party, namely the receiver...
from whom the confidential message is kept secret, may or may not decode the broadcast message, to which, in this scenario, we refer as the public message. We first consider the case where the sender is restricted to classical inputs, namely the classical-quantum-quantum (cqq) broadcast model. This model proves useful for obtaining capacity results for the fully quantum broadcast model, where this restriction is lifted. The classical counterparts of our results were given in [16]. Therein, the authors first derive robust codes for the bidirectional channel, in which both receivers are meant to decode the message. This common message will then piggyback a public message decoded by Bob. The privacy amplification strategies are then applied on part of the public codes to obtain information theoretic security (see [17] for a comparison with cryptography) via equivocation. We follow a similar approach in the context of quantum information theory. We obtain codes for the bidirectional channel (broadcast channel with no security requirement) by generalizing the random codes from [14]. Our generalization of these results (see Appendix B [13]), yields a universal superposition coding for cq channels. Our input structure allows us to use privacy amplification arguments ([10]) on part of the codebook to achieve the desired secrecy rates.

The quantum broadcast model in which the channel is assumed to perfectly known by communicating parties is the (single serving) model. A one-shot dynamic capacity trade o is established a dynamic capacity trade o.

The privacy amplification strategies are then applied on the bidirectional channel, in which both receivers are conditioned on the broadcast message. Proving the existence of capacity achieving codes is done in two steps. First we consider the case where there is no security criterion placed on the messages sent to Bob and Eve. In this case, we have a bidirectional channel, where Alice is sending a message to be decoded by Bob and potentially by Eve (weather Eve decodes this message depends on which scenario is considered, determining in turn our labeling of it as common or public). Conditioned on this message (the corresponding codewords are distributed according to a certain structure), Alice is simultaneously transmitting a second type of message, that is decoded by Bob. The random coding that makes precisely this task possible, is given by Lemma 9 from the full version of this work, [13], which is our universal superposition coding result. Application of this lemma gives us the desired bidirectional codes in forms of Lemma 14 (where the conditioning message is common) and 17 (where the conditioning message is public) from [13]. In the second step, the second type of message described above, is used for privacy amplification. Finally, we give the code definitions and capacity results for the fully quantum channel independently in Section IV.

II. Notation and conventions

All Hilbert spaces are assumed to have finite dimensions and are over the field C. All alphabets are also assumed to have finite dimensions. The set of linear operators from Hilbert space \( \mathcal{H} \) to itself is denoted by \( \mathcal{L}(\mathcal{H}) \). We denote the set of states by \( \mathcal{S}(\mathcal{H}) := \{ \rho \in \mathcal{L}(\mathcal{H}) : \rho \geq 0, \text{tr}(\rho) = 1 \} \). Pure states are given by projections onto one-dimensional subspaces. Given a unit vector \( \mathbf{x} \in \mathcal{H} \), the corresponding pure state will be written as \( | \mathbf{x} \rangle \langle \mathbf{x} | \).

The set of probability distributions on the finite alphabet \( \mathcal{X} \) of cardinality \( | \mathcal{X} | \), will be denoted by \( \mathcal{P}(\mathcal{X}) \). For \( n \in \mathbb{N} \), we define \( \mathcal{X}^n := \{ (x_1, \ldots, x_n) : x_i \in \mathcal{X}, \forall i \in \{1, \ldots, n\} \} \). The sequence \( \mathbf{x} \) will denote elements of \( \mathcal{X}^n \). Also, we use bold letters to denote vectors (sequences with more than one element). The probability distribution \( p^{\otimes n} \in \mathcal{P}(\mathcal{X}^n) \) will be given by \( n \)-fold product of \( p \in \mathcal{P}(\mathcal{X}) \), namely \( p^{\otimes n}(\mathbf{x}) = p(x_1) \cdots p(x_n) \) with \( \mathbf{x} = (x_1, \ldots, x_n) \). For any number \( M \in \mathbb{N} \), we use \( [M] := \{1, \ldots, M\} \).

The classical quantum (cq) channel \( W : \mathcal{X} \to \mathcal{S}(\mathcal{H}) \) is a completely positive trace preserving map from alphabet \( \mathcal{X} \) to the set of states on Hilbert space \( \mathcal{H} \). We denote the set of all such maps by \( \mathcal{CQ}(\mathcal{X}, \mathcal{H}) \). This set is equipped with the norm \( \| \cdot \|_{\mathcal{CQ}} \) defined for \( W \in \mathcal{CQ}(\mathcal{X}, \mathcal{H}) \) by \( \| W \|_{\mathcal{CQ}} := \max_{\mathbf{x} \in \mathcal{X}^n} \| W(\mathbf{x}) \|_1 \), where \( \| \cdot \|_1 \) is the trace norm on \( \mathcal{L}(\mathcal{H}) \). We use the termcq channel for map \( V \in \mathcal{CQ}(\mathcal{X}, \mathcal{H}_1 \otimes \mathcal{H}_2) \) with two outcomes in two sets of states on two Hilbert spaces. A measurement or a positive operator valued measure (POVM) with \( M \in \mathbb{N} \), is the mutual information between Alice and Eve to be arbitrarily small for large numbers of channel uses. As the common or indeed the public messages are available to Eve, we require the mentioned mutual information to be conditioned on the broadcast message. Proving the existence of capacity achieving codes is done in two steps.
outcomes on Hilbert space $\mathcal{H}$, is given by an $M$-tuple $(D_1, \ldots, D_M) : D_i \geq 0, \forall i \in [M]$ and $\sum_{i \in [M]} D_i = 1$. With slight abuse of notation, we write $a^\ell := 1_H - a$ for $a \in L(H)$. We use the base two logarithm denoted by $\log$. The von Neumann entropy of a state $\rho \in S(H)$ is given by $S(\rho) := -\text{tr}(\rho \log \rho)$. Given the state $\omega_{AB} \in S(\mathcal{H}_A \otimes \mathcal{H}_B)$, a closely related quantity, namely the mutual information is given by $I(A; B) := S(A, \omega) + S(B, \omega) - S(AB, \omega)$, where $S(\gamma, \omega)$, indicates the von Neumann entropy of the state $\omega^\gamma$, the marginal state of $\omega$. Consider the ensemble $\{p(x), \omega_{AB}^x\}$ with $\omega_{AB}^x \in S(\mathcal{H}_A \otimes \mathcal{H}_B)$ and $p \in \mathcal{P}(\mathcal{X})$. We can define a classical-quantum (cq) state $\omega_{XAB} \in S(\mathcal{C}^{|X|} \otimes \mathcal{H}_A \otimes \mathcal{H}_B)$, given some ONB $\{e_x\}_{x \in \mathcal{X}} \subset \mathcal{C}^{|X|}$ as

$$\omega_{XAB} := \sum_{x \in \mathcal{X}} p(x)|e_x\rangle\langle e_x| \otimes \omega_{AB}^x$$

(1)

Note that we have used the suffix $X$ to label the Hilbert space corresponding to alphabet $\mathcal{X}$. The conditional mutual information is then defined by

$$I(A; B|X, \omega_{XB}) := \sum_{x \in \mathcal{X}} p(x)I(A; B, \omega_{AB}^x).$$

(2)

We use cl$(A)$ to denote the closure of set $A$ and conv$(A)$ to denote its convex hull.

III. Basic definitions and main results

In this section we state the main results and definitions for the compound classical-quantum-quantum (cqq) broadcast channel. The results and definitions related to the fully quantum broadcast channel are stated in Section IV. For finite alphabet $\mathcal{X}$ and Hilbert spaces $\mathcal{H}_B, \mathcal{H}_E$, let $W := \{W_{i}\}_{i \in S} \subset C(Q(\mathcal{X}, \mathcal{H}_B \otimes \mathcal{H}_E))$ be a set of cqq channels. The compound cqq broadcast channel generated by this set is given by family $\{W_{i}^\otimes n, s \in S\}_{n=1}^\infty$. In other words, using $n$ instances of the compound channel is equivalent to using $n$ instances of one of the channels from the uncertainty set. We consider two closely related communication scenarios of significance, having both appeared in the literature hitherto.

- **Broadcasting Common and Confidential messages** (BCC), where the compound channel is used $n \in \mathbb{N}$ times by the sender Alice in control of the input of the channel, to send two types of messages $(m_0, m_c)$ simultaneously over the channel.
  - $m_0 \in [M_{0,n}]$, called the common message, that has to be reliably decoded by receiver Bob in control of Hilbert space $\mathcal{H}_B$ and Eve in control of Hilbert space $\mathcal{H}_E$.
  - $m_c \in [M_{c,n}]$, called the confidential message, that has to be decoded reliably by Bob while Eve, the wiretapper, is kept ignorant.

- **Transmitting Public and Confidential messages** (TPC), where along with the confidential message $m_c \in [M_{0,n}]$ and instead of the common message, Alice wishes to send a "public" message $m_1 \in [M_{1,n}]$ that is reliably decoded by Bob while it may or may not be decoded by Eve.

We consider the main concepts and results related to each task in the following. We start with the BCC scenario. The precise definition of the BCC codes is given by the following.

**Definition 1** (BCC codes). An $(n, M_{0,n}, M_{c,n})$ BCC code for $W$, is a family $\mathcal{C} = \{E(\cdot|m), D_{B,m}, D_{E,m_0}\}_{m \in \mathbb{M}}$ with $\mathbb{M} := [M_{0,n}] \times [M_{c,n}]$, stochastic encoder $E : M \rightarrow \mathcal{P}(\mathcal{X}^n)$, POVMs $(D_{B,m})_{m \in \mathbb{M}}$ on $\mathcal{H}_B^\otimes n$ and $(D_{E,m_0})_{m_0 \in [M_{0,n}]}$ on $\mathcal{H}_E^\otimes n$.

We define the transmission error functions, for any cq broadcast channel $W : X \rightarrow S(\mathcal{H}_B \otimes \mathcal{H}_E)$ and $n \in \mathbb{N}$ by

$$\tilde{\tau}_B(C, W^\otimes n) := \frac{1}{|\mathbb{M}|} \sum_{m \in \mathbb{M}} \sum_{x \in \mathcal{X}} E(x|m)\text{tr}(D_{E,m_0}(x))$$

and

$$\tilde{\tau}_E(C, W^\otimes n) := \frac{1}{|\mathbb{M}|} \sum_{m \in \mathbb{M}} \sum_{x \in \mathcal{X}} E(x|m)\text{tr}(D_{E,m_0}(x))$$

where, $W^\gamma, \gamma \in \{B, E\}$ are the marginal channels of $W$. Moreover, the security condition will be achieved by upper-bounding

$$I(M_i; E|M_0, \sigma_{s,n}),$$

(3)

where $\sigma_{s,n}$ is the code state defined for all $s \in S$ and $n \in \mathbb{N}$ by

$$\sigma_{s,n} := \frac{1}{|\mathbb{M}|} \sum_{m \in \mathbb{M}} |m\rangle \langle m| \otimes \sum_{x \in \mathcal{X}} E(x|m)W^\otimes n(x).$$

(4)

The conditional mutual information should be understood given (2) and considering ONBs $\{|m_i\}_{m_i \in [M_i]} \subset \mathbb{C}^{M_i}$, for $i \in \{0, c\}$ and $|m| := |m_0\rangle \otimes |m_c\rangle$. Based on this, we define the following achievable rate pairs.

**Definition 2.** (Achievable BCC rate pair) A pair $(R_0, R_c)$ of non-negative numbers is called an achievable BCC rate pair for $W$, if for each $\epsilon, \delta > 0$, exists an $n_0(\epsilon, \delta) \in \mathbb{N}$, such that for all $n > n_0$, we find an $(n, M_{0,n}, M_{c,n})$ BCC code $\mathcal{C} = \{E(\cdot|m), D_{B,m}, D_{E,m_0}\}_{m \in \mathbb{M}}$ such that

$$\frac{1}{2^n} \log M_{i,n} \geq R_i - \delta \quad (i \in \{0, c\}),$$

$$\sup_{s \in S} \tilde{\tau}_i(C, W^\otimes n) \leq \epsilon \quad (\gamma \in \{B, E\}),$$

$$\sup_{s \in S} I(M_i; E|M_0, \sigma_{s,n}) \leq \epsilon,$$

are simultaneously fulfilled.

We define the BCC capacity region of $W$ by

$$C_{\text{BCC}}(W) := \{(R_0, R_c) \in \mathbb{R}_+^2 \times \mathbb{R}_+^2 : (R_0, R_c) \text{ is achievable BCC rate pair for } W\}.$$

(5)

To state our theorem, we define the following regions, given finite alphabets $U, Y, X$ and probability distribution $p = p_{UYX} \in \mathcal{P}(U \times Y \times X^2)$, with the random variables $U, Y, X$ distributed accordingly.

$$\tilde{\mathcal{C}}^{(1)}(W, p, n) := \{(R_0, R_c) \in \mathbb{R}_+^2 \times \mathbb{R}_+^2 :$$

$$R_0 \leq \inf_{s \in S} \{I(U; B, \omega_s) + I(U; E, \omega_s)\} \wedge$$

$$R_c \leq \inf_{s \in S} I(Y; B|U, \omega_s) + \sup_{s \in S} I(Y; E|U, \omega_s)\}.$$
with
\[ \omega_s := \sum_{(u,y,x) \in U \times Y \times X^n} p(u,y,x) |u\rangle \langle u| \otimes |y\rangle \langle y| \otimes W_s \otimes (x). \] (6)

We state the following theorem.

**Theorem 3.** Let \( \mathcal{W} := \{W_s\}_{s \in S} \subset \mathcal{C}(\mathcal{X}, \mathcal{H}_B \otimes \mathcal{H}_E) \) be any compound cq broadcast channel. It holds
\[
C_{\text{BCC}}[\mathcal{W}] = \text{cl} \left( \bigcup_{l=1}^{\infty} \prod_{p=1}^{l} C^{(1)}(W,p,l) \right),
\] (7)

where we have used \( \frac{1}{A} = \{ [\frac{1}{2}x_1, \frac{1}{2}x_2] \mid (x_1, x_2) \in A \} \). The second union is taken over all \( p_{UXY} \in \mathcal{P}(U \times Y \times X^l) \) such that random variables \( U - Y - X \) form a Markov chain and alphabets \( U \) and \( Y \) are finite.

**Remark 4.** The set given on the right hand side of (7) is convex and hence we do not need further convexification here. This results from time sharing arguments applied on the entropic quantities appearing in (7). For a short proof of a similar statement, see [12].

We proceed with the TPC scenario. The precise definition of the TPC codes is given in the following.

**Definition 5 (TPC codes).** An \((n,M_1,m,M_c)\) TPC code for \( W \) is a family \( \mathcal{C} = \{C(\mathcal{X}), \mathcal{D}_B, \mathcal{D}_E\} \) with \( \mathcal{M} := \{M_1, \ldots , M_c\} \) a stochastic encoder \( E : \mathcal{M} \rightarrow \mathcal{P}(\mathcal{X}^n) \) and a POVM \((\mathcal{D}_B, \mathcal{D}_E)\) on \( H_B \).

We define the relevant transmission error function, for any cq broadcast channel \( W : \mathcal{X} \to \mathcal{S}(\mathcal{H}_B \otimes \mathcal{H}_E) \) and \( n \in \mathbb{N} \) by \( \varepsilon_B(C, W^\otimes n) := \sum_{v \in \mathcal{V}} \sum_{y \in \mathcal{X}} E(x|m) \text{tr}(D_B W_s^\otimes n(x)) \). Moreover, the security condition will be achieved by upper-bounding
\[
I(M_s; E|M_1, \sigma_{s,n}), \tag{8}
\]
where \( \sigma_{s,n} \) is the code state defined by
\[
\sigma_{s,n} := \frac{1}{|\mathcal{M}|} \sum_{m \in \mathcal{M}} |m\rangle \langle m| \otimes \sum_{x \in \mathcal{X}^n} E(x|m) W_s^\otimes n(x). \tag{9}
\]

Again, not that the conditional mutual information should be understood given (2) and considering ONBs \(|m_i\rangle_{m_i \in \mathcal{M}} \in \mathbb{C}^{|\mathcal{M}|} \) for \( i \in [1,c] \) and \( |m\rangle := |m_1\rangle \otimes |m_c\rangle \).

Based on this, we define the following achievable rate pairs.

**Definition 6.** (Achievable TPC rate pair) A pair \((R_1, R_2)\) of non-negative numbers is called an achievable TPC rate pair for \( \mathcal{W} \), if for each \( \epsilon, \delta > 0 \), there is a non-negative integer \( n_0(\epsilon, \delta) \in \mathbb{N} \) such that for all \( n > n_0 \), we find an \((n,M_1,m,M_c)\) TPC code \( \mathcal{C} = \{E(\cdot|m), \mathcal{D}_B, \mathcal{D}_E\} \) such that
\begin{enumerate}
\item \( \frac{1}{n} \log M_n \geq R_1 - \delta \) \( (i \in [1,c]) \),
\item \( \sup_{s \in S} \varepsilon_B(C, W^\otimes n) \leq \epsilon \),
\item \( \sup_{s \in S} I(M_s; E|M_1, \sigma_{s,n}) \leq \epsilon \)
\end{enumerate}
are simultaneously fulfilled.

We define the TPC capacity region of \( W \) by
\[
C_{\text{TPC}}[\mathcal{W}] := \{(R_1, R_2) \in \mathbb{R}_+^2 \mid (R_1, R_2) \text{ is achievable TPC rate for } \mathcal{W}\}. \tag{10}
\]

To state our theorem, we define the following sub-regions, given finite alphabets \( \mathcal{V}, \mathcal{Y} \) and probability distribution \( p = p_{UYX} \in \mathcal{P}(\mathcal{V} \times \mathcal{Y} \times \mathcal{X}) \), with the random variables \( V, Y, X \) distributed accordingly.
\[
C^{(1)}(W,p,n) := \{(R_1, R_2) \in \mathbb{R}_+^2 \mid R_1 \leq \inf_{s \in S} I(V; B, \omega_s) \wedge \ R_2 \leq \inf_{s \in S} I(Y; B|V, \omega_s) - \sup_{s \in S} I(Y; E|V, \omega_s)\}, \tag{11}
\]

with
\[
\omega_s := \sum_{(v,y,x) \in V \times Y \times X^l} p(v,y,x) |v\rangle \langle v| \otimes W_s^\otimes (x). \tag{12}
\]

We can state the following theorem.

**Theorem 7.** Let \( \mathcal{W} := \{W_s\}_{s \in S} \subset \mathcal{C}(\mathcal{X}, \mathcal{H}_B \otimes \mathcal{H}_E) \) be any compound cq broadcast channel. It holds
\[
C_{\text{TPC}}[\mathcal{W}] = \text{cl} \left( \bigcup_{l=1}^{\infty} \prod_{p=1}^{l} C^{(1)}(W,p,l) \right). \tag{13}
\]

The second union is taken over all \( p_{UYX} \in \mathcal{P}(\mathcal{V} \times \mathcal{Y} \times \mathcal{X}) \) such that random variable \( V - Y - X \) form a Markov chain and alphabets \( V \) and \( Y \) are finite.

IV. BCC and TPC Capacities of Compound Quantum Broadcast Channels

In this section we extend our results to the "fully quantum" setting where the receivers input quantum systems to the channels, i.e. the transition maps of the channels are c.p.t.p. maps instead of cq channels. Since the message transmission tasks we aim to perform are after all of a classical nature, the corresponding coding theorems can be proven applying the results from earlier chapters. Explicitly we apply the results of the preceding sections to derive codes for fully quantum broadcast channels. For the remainder of this section, we fix an arbitrary set \( \mathcal{J} := \{N_s\}_{s \in S} \), where \( N_s : \mathcal{L}(\mathcal{H}_A) \to \mathcal{L}(\mathcal{H}_B \otimes \mathcal{H}_E) \) is a c.p.t.p. map for each \( s \in S \). Traditionally, the c.p.t.p. map \( N_s \) is assumed to be an isometric channel, namely a Stinespring isometry to a given channel connecting \( A \) and \( B \). This way of defining the channel is fairly justified, since it naturally equips \( E \) with the strongest abilities when attacking the confidential transmission goals of the remaining parties. However, dropping this assumption on the channel does not complicate any subsequent arguments.

In what follows, we consider the BCC scenario. Corresponding considerations regarding the TPC scenario are easily extrapolated and are hence left to the reader.

**Definition 8 (BCC codes).** An \((n,M_0,M_c)\) BCC code for \( \mathcal{J} \) for channels in \( \mathcal{C}(\mathcal{H}_B \otimes \mathcal{H}_E) \) is a family \( \mathcal{C} = (E(\cdot |m), \mathcal{D}_B, \mathcal{D}_E) \) such that
\[
C_{\text{BCC}}[\mathcal{W}] = \text{cl} \left( \bigcup_{l=1}^{\infty} \prod_{p=1}^{l} C^{(1)}(W,p,l) \right). \tag{14}
\]
(V(m), D_{B,m}, D_{E,m_0})_{m \in M} with M := [M_0] \times [M_c], where (D_{B,m})_{m \in M} and (D_{E,m_0})_{m_0 \in [M_0]} are POVMs on \mathcal{H}_{B}^{\otimes n} resp. \mathcal{H}_{E}^{\otimes n} and V(m) is a state on \mathcal{H}_{A}^{\otimes n} for each m.

The average transmission errors for the receivers B, and E with channel \mathcal{N} : \mathcal{L}(\mathcal{H}_A) \rightarrow \mathcal{L}(\mathcal{H}_B \otimes \mathcal{H}_E) and \((n, M_0, M_c)\)-code \mathcal{C} are defined by

\[ \bar{e}_B(\mathcal{C}, \mathcal{N}^{\otimes n}) := \frac{1}{|M|} \sum_{m \in M} \text{tr} D^c_{B,m} N^{\otimes n}(V(m)), \]
and

\[ \bar{e}_E(\mathcal{C}, \mathcal{N}^{\otimes n}) := \frac{1}{|M|} \sum_{m \in M} \text{tr} D^c_{E,m_0} N^{\otimes n}(V(m)). \]

By replacing the code and errors the definitions of achievable rate pairs can be directly guessed from Definition 2 (the notational ambiguity should cause no misunderstandings since the set \mathcal{J} determines whether the classical-quantum or quantum broadcast channel scenario are considered.) We denote the corresponding BCC capacity region by \( C_{BCC} [\mathcal{J}] \). We moreover define \( \hat{C}^{(1)}(\mathcal{J}, p, l, (\rho_p)_{p \in \mathbb{Y}}) \) the set of all points in \( \mathbb{R}^2 \) which fulfill the inequalities

\[ 0 \leq R_0 \leq \inf \min_{s \in S} \{ I( U; B, \omega_s), I( U; E, \omega_s) \} \]
and

\[ 0 \leq R_c \leq \inf \min_{s \in S} \{ I( Y; B U, \omega_s) - \inf I( Y; E U, \omega_s) \} \]

where we understand the entropic quantities above as being evaluated on the cqq state \( \omega_s := \omega(\mathcal{N}_s, p, l) := \sum_{u \in \mathcal{U}, y \in \mathcal{Y}} p(u, y) |u, y\rangle \langle u, y| \otimes N^S_l (\rho_p) \) for each \( s \in S \).

**Theorem 9.** It holds

\[ C_{BCC} [\mathcal{J}] = \text{cl} \left( \bigcup_{l=1}^{\infty} \bigcup_{p \in \mathbb{P}} \hat{C}^{(1)}(\mathcal{J}, p, l) \right) \]

The second union is taken over all \( p_{U|XY} \in \mathcal{P}(\mathcal{U} \times \mathcal{Y} \times \mathcal{X}^l) \) such that random variable \( U - Y - X \) distributed accordingly, form a Markov chain and alphabets \( \mathcal{U} \) and \( \mathcal{Y} \) are finite.

**V. Conclusion**

To construct private codes for the broadcast channel, we first generated suitable random message transmission codes for the broadcast channel without imposing privacy constraints (Lemma 14 [13]). This was done by establishing suitable bounds for random universal "superposition codes". With subsequent application of a covering principle, these codes were transformed to fulfill the security criterion.

As a possible alternative technique to generate such codes, we mention the rather recent 'position decoding' and 'convex split' techniques [5], [6]. This approach proved to be powerful yet elegant and was successfully applied to determine "one-shot capacities" or "second order rates" in several scenarios. However, these techniques need still to be further developed, to also be suitable when dealing with channel uncertainties as in the scenarios considered in the present paper. A partial result in that directions is [7], where near-optimal universal codes for entanglement message transmission over compound quantum channels with finitely many channel states are constructed. Recently, convex split and position- decoding have been applied in [20] to determine the second-order capacity of a cqq compound wiretap channel under the restriction, that the channel state does not vary for the legitimate receiver. For establishing this result, only the "convex split" part has to be universal, while "position- decoding" is applied on a channel with fixed state. As a future research goal, it is desirable to close the gap and establish a fully universal version of these protocol steps.

As mentioned in the introduction, a strong converse cannot be established for the message transmission capacity of the compound cq channel under average error criterion, even when considering \(|S| = 2\). When considering a fixed non-vanishing upper bound on the average of decoding error, calculation of capacity for the compound channel is further problematic as there are examples where the optimistic definition of the \( \epsilon \)-capacity yields a strictly larger number than the one yielded by its pessimistic definition (see [11] Remark 13). This implies that in general there is no second rate capacity theorem possible. The implications of these negative statements are highly interesting in practice, as channel coding in all existing communication systems (such as wireless cellular and WiMax systems), is done given a fixed error probability. It is therefore important to design channel codes corresponding to \( \epsilon \)-capacity of the compound channel, that is in general larger than its message transmission capacity.

Security of the protocols considered in this work, as opposed to those obtained by cryptographic methods, does not rely on potential computational limitations of illegal receivers. Instead, the information theoretic security considered here, is implemented on "physical layer service integration" schemes (see [17] for more discussions on information theoretic security). Further discussions on our results from a quantum network perspective can be found in [8].

**Acknowledgment**

H. Boche is partly supported by the Deutsche Forschungsgemeinschaft (DFG, German Research Foundation), under Germany’s Excellence Strategy EXC-2111-390814868. G. Jänsch is partly supported by the Gottfried Wilhelm Leibniz program of the DFG under Grant BO 1734/20-1 and by the national research initiative on quantum technologies of Bundesministerium für Bildung und Forschung (German Federal Ministry of Education and Research), within the project Q-Link.X 16KIS05858. S. Saeedinaeieni is partly supported by the national research initiative on quantum technologies of Bundesministerium für Bildung und Forschung (German Federal Ministry of Education and Research), within the project QuaDiQua 16KIS0948.
References

[1] R. Ahlswede. Certain results in coding theory for compound channels. Proceedings of Colloquium on Information Theory, Debrecen, 1967, J. Bolyai Mathematical Society, Budapest, Hungary vol.1, 35-60 (1968).

[2] R. Ahlswede. The Structure of Capacity Functions for Compound Channels. Proceedings of the International Symposium on Probability and Information Theory at McMaster University, Canada 12-54, (1969).

[3] R. Ahlswede. Elimination of correlation in random codes for arbitrarily varying channels. Z.f. Wahrscheinlichkeitstheorie und verwandte Gebiete 44, 159-175(1978).

[4] R. Ahlswede. Transmitting and gaining data:Rudolf Ahlswede's Lectures on Information Theory 2. R. Ahlswede, I. Althofer, C. Deppe and U. Tamm, Eds. New York, Springer (2015).

[5] A. Anshu, V. K. Devabathini. Quantum communication using coherent rejection sampling. Phys. Rev. Lett. 199(12) 120506 (2017).

[6] A. Anshu, R. Jain, N. A. Warsi. One shot entanglement assisted classical and quantum communication over noisy quantum channels: A hypothesis testing and convex split approach. IEEE Trans. Inf. Theory vol. 65, pp. 1287-1306 (2019).

[7] A. Anshu, R. Jain, N. A. Warsi. A hypothesis testing approach for communication over entanglement-assisted compound quantum channel. IEEE Trans. Inf. Theory vol. 65, pp. 2623-2636 (2019).

[8] R. Bassoli, H. Boche, C. Deppe, R. Ferrera, F.H.P. Fitzek, G. Janßen, S. Saeedinaeeni. Quantum communication networks. Springer Nature (2020).

[9] I. Bjelaković, H. Boche, G. Janßen, J. Nötzel. Arbitrarily varying and compound classical-quantum channels and a note on quantum zero-error capacities. Aydinian, H., Cicalerse, F., Deppe, C. (eds.) Information Theory, Combinatorics, and Search Theory, in Memory of Rudolf Ahlswede vol. 7777, pp. 247-283 (2012).

[10] H. Boche, M. Cai, C. Deppe. Secrecy capacities of compound wiretap channels and applications. Phys.Rev A (2014).

[11] H. Boche, R. F. Schaefer, H. V. Poor. Analytical Properties of Shannon's Capacity of Arbitrarily Varying Channels under List Decoding: Super-Additivity and Discontinuity Behavior problems of Information Transmission vol 54, 3, pp. 199-228 (2018).

[12] H. Boche, G. Janßen, S. Saeedinaeeni. Simultaneous transmission of classical and quantum information under channel uncertainty and jamming attacks. J. Math. Phys. 60, 022204 (2019).

[13] H. Boche, G. Janßen, S. Saeedinaeeni. Universal superposition codes: capacity regions of compound quantum broadcast channel with confidential messages. Journal of Mathematical Physics 61, 042204 (2020).

[14] M. Mosonyi. Coding theorems for compound problems via quantum Rényi divergences. IEEE Trans. Inf. Theory vol. 61, pp. 2997-3012 (2015).

[15] F. Salek, A. Anshu, M.Hsieh, R. Jain, J.R. Fonollosa. One-shot capacity bounds on the simultaneous transmission of public and private information over quantum channels. IEEE International Symposium for Information Theory pp. 296-300 (2018).

[16] R.F Schaefer, H. Boche. Robust Broadcasting of Common and Confidential Messages Over Compound Channels: Strong Secrecy and Decoding Performance. IEEE Transactions on Information Forensics and Security vol. 9, Issue 10, pp. 1720-1732 (2014).

[17] R.F Schaefer, H. Boche. Physical layer service integration in wireless networks. IEEE Signal Processing vol. 31, Issue 3, pp. 147-156 (2014).

[18] M. M. Wilde, M.-H. Hsieh. Public and private communication with a quantum channel and secret key. Physical Review A 80, 022306 (2009).

[19] M. M. Wilde, M.-H. Hsieh. Public and private resource trade-offs for a quantum channel. Quantum Inf. Process. 11, pp. 1465–1501 (2012).

[20] M. M. Wilde, S. Khatri, E. Kaur, S. Guha. Second-order coding rates for key distillation in quantum key distribution. Preprint: arXiv:1910.03993 (2019).