IJICTR
International Journal of Information & Communication Technology Research

Volume 12- Number 2 – 2020 (1 -10)

Classical-Quantum Multiple Access Channel with Secrecy Constraint: One-shot Rate Region

Hadi Aghaee
Faculty of Electrical Engineering
K. N. Toosi University of Technology
Tehran, Iran
Email: Aghaee_Hadi@email.kntu.ac.ir

Bahareh Akhbari*
Faculty of Electrical Engineering
K. N. Toosi University of Technology
Tehran, Iran
Email: akhbari@eetd.kntu.ac.ir

Received: 6 October 2019 - Accepted: 12 January 2020

Abstract—**In this paper, we aim to study a *l*-user quantum multiple access wiretap channel with an arbitrary number of wiretappers under one-shot setting. In this regard, we first introduce the general quantum multiple access wiretap channel and the simplified proposed channel. Then, we calculate an achievable secrecy rate region for the main channel with two users. The encoding process uses the superposition and wiretap coding techniques, and the decoding technique is based on the simultaneous decoder. Also, Convex splitting is used to satisfy security requirements. At last, we extend the results to the *l*-user case.**

Keywords—Quantum Channel; Wiretap Channel; Hypothesis Testing Mutual Information; Secrecy Rate Region; Multiple Access Channel

I. INTRODUCTION

Information-theoretic security was first introduced by Shannon, which led to introducing of the Shannon cipher system [1]. After that, Wyner introduced the wiretap channel in his basic paper [2]. After Wyner's work, Csiszár and Körner extended the Wyner wiretap channel to a general case in which a transmitter wants to transmit its message over a discrete memoryless channel (DMC) to a legitimate receiver at the presence of a passive wiretapper [3]. In all of the above channels, the secrecy constraint can be considered as follows: the message should be transmitted reliably and confidentially as much as possible at the presence of a passive wiretapper. This criterion is also used to study the problem of physical layer security of multi-terminal channels such as interference channel (IC), multiple access channel (MAC) [4], etc., in the network information theory area.

The MACs are among important channels that have been the subject of many studies. These channels can be considered as building blocks of practical scenarios in 5G wireless communication. Therefore, the secrecy problem of MACs is an important issue.

The MAC as a type of multi-terminal channels has accept two or more messages as inputs and one receiver. The secrecy problem for the MACs is studied in many types of research [4-11].

The quantum wiretap channel was first discussed in [12] and [13]. In the quantum wiretap channel, a sender wants to transmit classical or quantum message to a legitimate receiver over a noisy quantum channel as secure as possible from Eve's attacks.

* Corresponding Author

The quantum multiple access channel (QMAC) and its secrecy problem were investigated in [14] and [15], respectively. In [15], the authors employed a successive decoder to decode the sent messages. In [16], the authors studied the private classical information transfer problem over a special quantum interference channel based on the QMAC. In [17], classical-quantum multiple access wiretap channel with a common message (C-QMA-WTC-CM) under one-shot setting is studied.

The usefulness of the quantum simultaneous decoder is proved just for decoding two messages, and it has remained as an unproven conjecture for the general case [18]. P. Sen [18] proved that the intersection argument is crucial in constructing a simultaneous decoder for the receiver. In the asymptotic independently and identically distributed (i.i.d) setting for MAC, employing simultaneous decoder instead of using successive decoder combined with time-sharing, is a better choice [19]. However, successive decoding gives a finite set of achievable rate pairs in the one-shot case. Thus, using the simultaneous decoder leads us to a continuous achievable rate region.

In the area of quantum network information theory, finding a general simultaneous decoder is an important problem that can pave the way for progress in this field of researches.

However, under the one-shot setting wherein users allowed to send their messages with only one use of the channel, the quantum simultaneous decoding scheme has no limit on decoding any number of message. A detailed discussion can be found in [18, 20-22].

In this paper, we aim to study private classical communication over a C-QMAC with an arbitrary number of wiretappers under the one-shot setting. In this regard, achievable rate regions for the main channel with two senders or more are calculated.

The paper is structured as follows:

In Section II, some notations and definitions are presented. The main channel and information processing task are presented in Section III, and in Section IV, the main results and proofs are presented.

II. Preliminaries

Throughout this paper, we assume that all random variables have finite alphabets, and dimensions of quantum systems are finite. Quantum and classical systems are denoted by uppercase letters X, Y etc.

Consider two quantum systems as X and Y. Alphabet sets of X and Y are denoted by calligraphic letters $\mathcal{X}$ and $\mathcal{Y}$, respectively. The state of system X which is presented as a density matrix ρ_X over X is determined by its diagonal elements that are indexed by elements $x \in \mathcal{X}$, i.e., $\rho_X = \sum_{x\in\mathcal{X}} P_X(x)|x\rangle\langle x|$ where P_X is a distribution over $\mathcal{X}$. The density operator ρ_X is a positive semidefinite operator with unit trace. The shared state between sender and receiver is denoted by $\rho_{XY} = \sum_{x\in\mathcal{X}} P_X(x)|x\rangle\langle x| \otimes \rho_Y^x$, where P_X is the probability distribution, $\{|x\rangle\}_x$ is an orthonormal basis, and $\{\rho_Y^x\}_x$ is a set of quantum states. Note that the state of Alice or Bob can be obtained by trace out uninvolved system. In other words, Alice and Bob's density operators can be obtained as $\rho_X = Tr_Y\{\rho_{XY}\}$ and $\rho_Y = Tr_X\{\rho_{XY}\}$, respectively. The pure state of system X is denoted by $|\psi\rangle^X$, while the corresponding density operator is $\psi^X = |\psi\rangle\langle\psi|^X$. The von Neumann entropy of the state ρ_x is denoted by $H(X)_\rho = -Tr\{\rho_x \log \rho_x\}$. Similar to the classical definition, the quantum conditional entropy is defined as difference between the von Neumann entropy of the joint system and the von Neumann entropy of the individual system for an arbitrary state such as σ_{XY} : $H(X|Y)_\sigma = H(X,Y)_\sigma - H(Y)_\sigma$. The quantum mutual information between two systems is defined as $I(X;Y)_\sigma = H(X)_\sigma + H(Y)_\sigma - H(X,Y)_\sigma$ and conditional quantum mutual information for arbitrary systems such as X, Y and Z is defined as $I(X;Y|Z)_\sigma = H(X|Z)_\sigma + H(Y|Z)_\sigma - H(X,Y|Z)_\sigma$.

Every quantum operation can be illustrated by completely positive trace-preserving (CPTP) map $\mathcal{N}^{X\to Y}$ where accepts input states in X and output states in Y. The trace distance gives the distance between two quantum states and is defined for two arbitrary states σ and ρ as follows:

$$\|\sigma - \rho\|_1 = Tr|\sigma - \rho| \quad (1)$$

where $|\mathcal{D}| = \sqrt{\mathcal{D}^\dagger \mathcal{D}}$.

In the following, we provide definitions that we use to derive and illustrate our main results.

Definition 1: *(Quantum smooth hypothesis testing mutual information)* Quantum smooth hypothesis testing mutual information is denoted by $I_H^\epsilon(X;Y) := D_H^\epsilon(\rho^{XY}\|\rho^X \otimes \rho^Y), \epsilon \in (0,1)$ [Proposition 1, 18] where $D_H^\epsilon(.\|.)$ is *quantum smooth hypothesis testing relative entropy* [Eq. (1), 22]. $\rho^{\mathcal{H}_X\mathcal{H}_Y}$ is the joint state of input and output over their Hilbert spaces $(\mathcal{H}_X, \mathcal{H}_Y)$, and it can be shown as ρ^{XY}:

$$\rho^{XY} = \sum_x P_X(x)|x\rangle\langle x|^X \otimes \rho_x^Y \quad (2)$$

where P_X is input distribution.

Definition 2*: (Max mutual information [23])* Consider a bipartite state ρ_{XY} and a parameter $\epsilon \in (0,1)$. The max mutual information can be defined as follows:

$$I_{max}(X;Y)_\rho := D_{max}(\rho_{XY}\|\rho_X\otimes\rho_Y)_\rho$$

where ρ refers to the state ρ_{XY} and D_{max} is the *max-relative entropy* [24] for $\rho_X, \sigma_X \in \mathcal{H}_X$:

$$D_{max}(\rho_X\|\sigma_X) := \inf\{\gamma \in \mathbb{R}: \rho_X \le 2^\gamma \sigma_X\}$$

Definition 3*: (Quantum smooth max Rényi divergence [23])* Consider $\rho^{XY} := \sum_{x\in\mathcal{X}} P_X(x)|x\rangle\langle x|^X \otimes \rho_x^Y$ as a CQ state and a parameter $\epsilon \in (0,1)$. The *smooth max mutual information* between the systems X and Y can be defined as follows:

$$I_{max}^{\epsilon}(X;Y) := \inf_{\rho'_{XY}\in\mathcal{B}^{\epsilon}(\rho_{XY})} D_{max}(\rho'_{XY} \| \rho_X \otimes \rho_Y) = \inf_{\rho'_{XY}\in\mathcal{B}^{\epsilon}(\rho_{XY})} I_{max}(X;Y)_{\rho'}$$

where $\mathcal{B}^{\epsilon}(\rho_{XY})$ is ϵ-*ball* for ρ_{XY} and is defined in [21].

***Definition 4**: (Alternate smooth max-mutual information)* Consider a bipartite state ρ^{XY} and a parameter $\epsilon \in (0,1)$. The *alternate* definition of the *smooth max-mutual information* between the systems X and Y can be defined as follows:

$$\tilde{I}_{max}^{\epsilon}(Y;X) := \inf_{\rho'_{XY}\in\mathcal{B}^{\epsilon}(\rho_{XY})} D_{max}(\rho'_{XY} \| \rho_X \otimes \rho'_Y)$$

***Definition 5**: (Conditional smooth hypothesis testing mutual information) Consider* $\rho_{XYZ} := \sum_{x\in\mathcal{X}} P_X(x)|x\rangle\langle x|^X \otimes \rho_x^{YZ}$ as a classical-quantum state and a positive parameter ϵ. Define

$$I_H^{\epsilon}(Y;Z|X)_{\rho} := \max_{\rho'} \min_{x\in supp(\rho'_X)} I_H^{\epsilon}(Y;Z)_{\rho_x^{YZ}}$$

where maximization is over all $\rho'_X = \sum_{x\in\mathcal{X}} P_X(x)|x\rangle\langle x|^X$ satisfying $P(\rho'_X,\theta_X) \leq \epsilon$ and, $P(.,.)$ is *purified distance* between two states [21]. $supp(f)$ refers to *set-theoretic support* of $\underset{X\to\mathbb{R}}{f(x)}$ and is defined as the set of points in set X where $f(x)$ is non-zero ($supp(f) = \{x\epsilon X | f(x) \neq 0\}$). In other words, given a quantum state ρ on Hilbert space $\mathcal{H}$, $supp(\rho)$ is the subspace of $\mathcal{H}$ spanned by all eigen-vectors of ρ with non-zero eigenvalues.

***Definition 6**: (One-shot lower bound of a classical-quantum multiple access channel)* [18] A two user C-QMAC under the one-shot setting is defined by a triple $(\mathcal{X}_1 \times \mathcal{X}_2, \mathcal{N}^{X_1X_2\to Y}(x_1,x_2) \equiv \rho_{x_1x_2}^{Y}, \mathcal{H}^Y)$, where $\mathcal{X}_1$ and $\mathcal{X}_2$ are the input alphabet sets, and Y is the output system. $\rho_{x_1x_2}^{Y}$ is output quantum state, and the channel is illustrated by $\mathcal{N}^{X_1X_2\to Y}$ as CPTP. Considering the joint typicality lemma introduced in [Corollary 4, 18], the one-shot lower bound of a C-QMAC is as follows:

$$R_1 \leq I_H^{\epsilon}(X_1;Y|X_2Q)_{\rho} - 2 - \log(1/\epsilon)$$

$$R_2 \leq I_H^{\epsilon}(X_2;Y|X_1Q)_{\rho} - 2 - \log(1/\epsilon)$$

$$R_1 + R_2 \leq I_H^{\epsilon}(X_1,X_2;Y|Q)_{\rho} - 2 - \log(1/\epsilon)$$

where $I_H^{\epsilon}(.)$ is the quantum smooth hypothesis testing mutual information defined in Definition 1 with respect to the following state:

$$\rho^{QX_1X_2Y} := \sum_{qx_1x_2} p(q)p(x_1|q)p(x_2|q)|qx_1x_2\rangle \langle qx_1x_2|^{QX_1X_2} \otimes \rho_{x_1x_2}^{Y}$$

and Q is a random variable used as time-sharing.

***Definition 7:** (Inner bound of a classical-quantum multiple access wiretap channel)* [15] A two-user C-QMA-WTC is defined by a triple $(\mathcal{X}_1 \times \mathcal{X}_2, \mathcal{N}^{X_1X_2\to YZ}(x_1,x_2) \equiv \rho_{x_1x_2}^{YZ}, \mathcal{H}^Y \otimes \mathcal{H}^Z)$, where $\mathcal{X}_1$ and $\mathcal{X}_2$ denote the input alphabet sets, and Y, Z denote the output systems.

The inner bound of a two-user C-QMA-WTC is as follows:

$$R_1 \leq I(X_1;Y|X_2Q) - I(X_1;Z|Q)$$
$$R_2 \leq I(X_2;Y|X_1Q) - I(X_2;Z|Q)$$
$$R_1 + R_2 \leq I(X_1X_2;Y|Q) - I(X_1X_2;Z|Q)$$

where Q is a random variable used as time-sharing.

***Definition 8**: (Pretty good measurement)* [26]: Consider an operator T. Then $T^{-1/2}$ is the inverse square root of operator T and is defined only on the $supp(T)$. That is, given a spectral decomposition of the operator T:

$$T = \sum_t t|t\rangle\langle t| \quad (3)$$

and

$$T^{-1/2} = \sum_t f(t)|t\rangle\langle t| \quad (4)$$

where

$$f(t) = \begin{cases} t^{-1/2} & , \quad t \neq 0 \\ 0 & , \quad t \neq 0 \end{cases} \quad (5)$$

The main concept of *square-root measurement* is based on the positive-operator valued measure (POVM) elements $\{\Lambda_m\}_{m=1}^{|\mathcal{M}|}$, that correspond to the sent messages and Λ_0, that corresponds to an error result.

$$\Lambda_m \equiv \left(\sum_{m'=1}^{|\mathcal{M}|} P_{m'}\right)^{-\frac{1}{2}} P_m \left(\sum_{m'=1}^{|\mathcal{M}|} P_{m'}\right)^{-\frac{1}{2}} \quad (6)$$

where

$$P_m = \Pi\Pi_m\Pi \quad (7)$$

and the operator P_m is a positive operator, and Π, Π_m are the code subspace projector and the codeword subspace projector, respectively.

More details can be found in [15.4.2, 26].

III. CHANNEL MODEL

In this section, we want to define the main channel.

A l-user C-QMA-WTC with d wiretappers is defined by a triple $(\mathcal{X}_1 \times \mathcal{X}_2 \ldots \times \mathcal{X}_l, \mathcal{N}^{X_1X_2\ldots X_l\to YZ_1Z_2\ldots Z_d}(x_1,x_2\ldots x_l) \equiv \rho_{x_1x_2\ldots x_l}^{YZ_1Z_2\ldots Z_d}, \mathcal{H}^Y \otimes \mathcal{H}^{Z_1} \otimes \ldots \otimes \mathcal{H}^{Z_d})$, where $\mathcal{X}_i, i \in \{1,2,\ldots,l\}$ denote the input alphabet sets and $\mathcal{Y}$, $Z_i, i \in \{1,2,\ldots,d\}$ denote the output systems at the legitimate receiver and d wiretappers, respectively.

A $(2^{nR_1}, 2^{nR_2}, \ldots, 2^{nR_l})$ code for C-QMA-WTC consists of the l independent messages $M_1, M_2 \ldots M_l$, each of them is selected from their message sets $M_i = \{1,\ldots,2^{nR_i}\}, i \in \{1,2,\ldots,l\}$. There are l stochastic encoders for each user: $\varepsilon_i: \mathcal{M}_i \to \mathcal{X}_i$ and l decoding POVMs.

The main channel model is illustrated in Fig. 1.

Remark 1: We should note that, in all of discussed cases in the paper, all channels assumed to be memoryless and all of the wiretappers have the same effect on the sent messages. In other words, the capability of all wiretappers assumed to be equal.

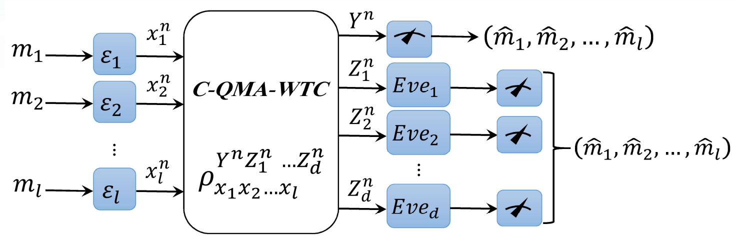

Figure. 1. The l-user classical-quantum multiple access wiretap channel with d wiretappers. (for one-shot setting set n=1).

IV. Main Results And Proofs

In this section, to provide our main results, we consider the two-user case without the one-shot setting at first. Then we generalize our results to the l-user case with one-shot setting.

Theorem 1: *(An inner bound -two user case) An achievable secrecy rate region for the C-QMA-WTC with an arbitrary number of wiretappers is the convex closure of all non-negative rates* (R_1, R_2)*:*

$$R_1 \leq I(X_1;Y|X_2Q) - \sum_{i=1}^{d} I(X_1;Z_i|Q)$$

$$R_2 \leq I(X_2;Y|X_1Q) - \sum_{i=1}^{d} I(X_2;Z_i|Q)$$

$$R_1 + R_2 \leq I(X_1X_2;Y|Q) - \sum_{i=1}^{d} I(X_1;Z_i|Q) - \sum_{i=1}^{d} I(X_2;Z_i|Q)$$

where Q *is an auxiliary random variable which is used as time-sharing,* d *is the number of wiretappers, and the probability density function is:*

$$\pi: p(q)p(x_1|q)p(x_2|q)p(yz_1 \ldots z_l|x_1x_2)$$

Proof: In Appendix A.

Remark 2: In the case of the channel with one wiretapper, if we assume that the leaked information of each user is independent from another user ($I(X_1X_2;Z|Q) = I(X_1;Z|Q) + I(X_2;Z|X_1Q) \overset{if}{=} I(X_1;Z|Q) + I(X_2;Z|Q)$), then the result of the Theorem 1 is reduced to the results in [15]. This assumption is due to the employment of the *successive cancellation decoder* in [15].

Conjecture: *(An inner bound-l-user case) An achievable secrecy rate region for the C-QMA-WTC with an arbitrary number of wiretappers is the convex closure of all non-negative rates* $(R_1, R_2, \ldots, R_l)$

$\forall J \subset [\mathcal{L}], \forall T \subset [\mathcal{D}]$

$$\sum_{s \in J} R_s \leq I\left(X_J;Y|X_{J^c}Q\right)_\rho - \sum_{J,T} I\left(X_J;Z_T|Q\right)_\rho$$

where $\mathcal{L} = \{1,2,\ldots,l\}$ *and* $\mathcal{D} = \{1,2,\ldots,d\}$*.* Q *is an auxiliary random variable that denotes time-sharing,* J *is an arbitrary subset of the set* $\mathcal{L}$ *denotes the set of users,* J^c *denotes the complementary of the subset* J *in the space of the set* $\mathcal{L}$*,* T *is a subset of the set* $\mathcal{D}$ *denotes the set of wiretappers, and the probability density function is:*

$$\pi: p(q)p(x_1|q)p(x_2|q) \ldots p(x_l|q)p(yz_1 \ldots z_d|x_1x_2 \ldots x_l)$$

with respect to the following state:

$$\rho^{QX_1X_2\ldots X_lYZ_1\ldots Z_d} := \sum_{qx_1x_2\ldots x_l} p(q)p(x_1|q)p(x_2|q)\ldots p(x_l|q)|qx_1x_2\ldots x_l\rangle\langle qx_1x_2\ldots x_l|^{QX_1X_2\ldots X_l} \otimes \rho_{x_1x_2\ldots x_l}^{YZ_1\ldots Z_d}$$

Proof: The proof is similar to the two-user case. The only difference is assuming that a proven simultaneous decoder exists. The proof of *secrecy constraint* is presented in Appendix B.

Remark 3*:* We should note that the proof of the above conjecture is based on simultaneous decoding. Therefore, according to the discussion presented in the first section, this technique leads us to a conjecture, not a theorem.

Remark 4*:* In contrast to the general case, the usefulness of the simultaneous decoder is proven for some special cases such as min-entropy case and the special case of QMAC where the induced channel to each receiver has average output states that commute (commutative version of output states) [27].

Now, we want to discuss about the main channel under the one-shot setting. As mentioned before, in the one-shot case there are fewer quantum computing limitations compared to the general case. Two of these benefits are availability of a proven simultaneous decoder and one-shot quantum joint typicality lemma.

The main results for the one-shot case is presented below.

Theorem 2: *(One shot inner bound- two user case) An achievable secrecy rate region for the C-QMA-WTC with an arbitrary number of wiretappers is the convex closure of all non-negative rates* (R_1, R_2)*:*

$$R_1 \leq I_H^\epsilon(X_1;Y|X_2Q)_\rho - \sum_{i=1}^{d} \tilde{I}_{max}^\epsilon(X_1;Z_i|Q)_\rho - 2 - (d+1)\log\left(\frac{1}{\epsilon}\right)$$

$$R_2 \leq I_H^\epsilon(X_2;Y|X_2Q)_\rho - \sum_{i=1}^{d} \tilde{I}_{max}^\epsilon(X_2;Z_i|Q)_\rho - 2 - (d+1)\log\left(\frac{1}{\epsilon}\right)$$

$$R_1 + R_2 \leq I_H^\epsilon(X_1,X_2;Y|Q)_\rho - \sum_{i=1}^{d} \tilde{I}_{max}^\epsilon(X_1;Z_i|Q)_\rho - \sum_{i=1}^{d} \tilde{I}_{max}^\epsilon(X_2;Z_i|Q)_\rho - 2 - (2d+1)\log\left(\frac{1}{\epsilon}\right)$$

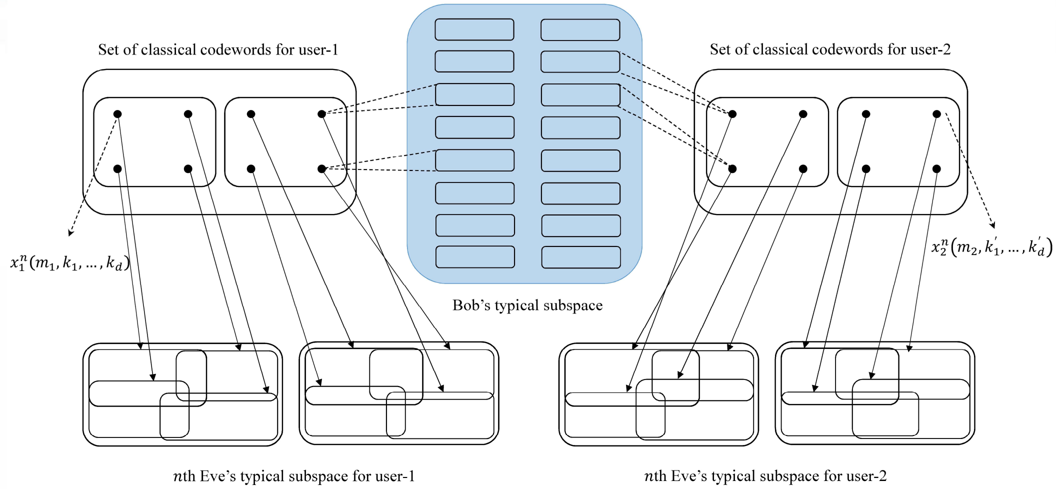

Figure. 2. The code structure for private classical information over QMAC (it is the same for the one-shot setting). For simplicity of illustration, we assumed $m_i \in \{1,2\};\ i \in \{1,2\}$ and $k_f, k_f' \in \{1,2,3,4\};\ f \in \{1,2,\dots,d\}$. We only show the typical subspace of nth Eve.

where Q is an auxiliary random variable that denotes time-sharing, d is the number of wiretappers, and the probability density function is:

$$\pi: p(q)p(x_1|q)p(x_2|q)p(yz_1 \dots z_d|x_1x_2)$$

Sketch of proof: The main concepts in the proof of the Theorem 2 are the same as Theorem 1. The only difference is that in the one-shot case, we use *convex split lemma* (instead of the covering lemma) for calculating the leaked information from senders to wiretappers. The detailed proof is presented in Appendix C.

Theorem 3: *(One-shot inner bound-general case) An achievable secrecy rate region for the l-user C-QMA-WTC with an arbitrary number of wiretappers is the convex closure of all non-negative rates $(R_1, R_2, \dots, R_l)$:*

$$\forall J \subset [\mathcal{L}], \forall T \subset [\mathcal{D}]$$

$$\sum_{s\in J} R_s \le I_H^\epsilon\left(X_J; Y \middle| X_{J^c}Q\right)_\rho - \sum_{J,T} \tilde{I}_{max}^\epsilon\left(X_J; Z_T \middle| Q\right)_\rho - 2 - (|JT| + 1)\log\left(\frac{1}{\epsilon}\right),$$

where $\mathcal{L} = \{1,2,\dots,l\}$ and $\mathcal{D} = \{1,2,\dots,d\}$. Q is an auxiliary random variable that denotes time-sharing, J is an arbitrary subset of the set $\mathcal{L}$ denotes the set of users, J^c denotes the complementary of the subset J in the space of the set $\mathcal{L}$, T is a subset of the set $\mathcal{D}$ denotes the set of wiretappers, and the probability density function is:

$$\pi: p(q)p(x_1|q)p(x_2|q)\dots p(x_l|q)p(yz_1 \dots z_d|x_1x_2 \dots x_l)$$

with respect to the following state:

$$\rho^{QX_1X_2\dots X_lYZ_1\dots Z_d} := \sum_{qx_1x_2\dots x_l} p(q)p(x_1|q)p(x_2|q)\dots p(x_l|q)|qx_1x_2 \dots x_l\rangle\langle qx_1x_2 \dots x_l|^{QX_1X_2\dots X_l} \otimes \rho_{x_1x_2\dots x_l}^{YZ_1\dots Z_d}$$

Proof: The proof is similar to the two-user case. The *leaked information* analysis is presented in Appendix D

V. Discussion And Future Works

In this paper, we studied the problem of private classical communication over a l-user quantum multiple access channel with an arbitrary number of wiretappers. We also studied the proposed channel under the one-shot setting. We constructed a simultaneous decoder in order to guarantee that Bob can decode the messages reliably and confidentially. We also used the convex split lemma [28] to ensure that the wiretappers are unable to determine which user's message is transmitted. This paper shows that convex splitting is an effective method to study multi-terminal quantum channels' privacy.

Appendix

Appendix A: *(Proof of Theorem 1)*

Outline of the proof: The sender's goal is to build two separate indexed codebooks $\{x_1^n(m_1, k_1, \dots, k_d)\}_{m_1\in\mathcal{M}_1, k_f\in\mathcal{K}_f, f=[1:d]}$ and $\{x_2^n(m_2, k_1', \dots, k_d')\}_{m_2\in\mathcal{M}_2, k_f'\in\mathcal{K}_f', f=[1:d]}$ so that Bob should be able to detect the pair messages (m_1, m_2) and the junk variables $(k_1, \dots, k_d, k_1', \dots, k_d')$ with high probability. The coding scheme has been illustrated in Fig. 2.

In this illustration, we have assumed $m_i \in \{1,2\};\ i \in \{1,2\}$ and $k_f, k_f' \in \{1,2,3,4\}, f \in \{1,\dots,d\}$. The users want to transmit one of the two messages separately, and they have variables $k_f, k_f', f \in \{1,\dots,d\}$ for randomizing Eve's state. Thus, we have $4d$ classical codewords ($2d$ codewords for user-1 and $2d$ codewords for the second user). Each of the codewords is mapped into a distinguishable subspace on Bob's typical subspace (for simplicity of illustration, we showed four mappings in Fig. 2). In other words, each of the $x_1^n(m_1, k_1, \dots, k_d)$ and $x_2^n(m_2, k_1', \dots, k_d')$ are grouped in a box. These boxes indicate the privacy amplification sets. Here we have four amplification sets. When randomizing the junk variables k_f and k_f' the codewords $\{x_1^n(1,k_1,\dots,k_d)\}$ and $\{x_1^n(2,k_1,\dots,k_d)\}$ uniformly cover Eve's typical subspace. Thus, that is nearly impossible for Eve to understand whether user-1 is sending the first codeword or the second. This scenario is the same for another user. From the packing lemma, we can understand that user-1 can reliably send about $2^{nI(X_1;Y|X_2)}$ and user-2 can reliably send distinguishable information about $2^{nI(X_2;Y|X_1)}$ and from the covering lemma, we can understand that the minimum size for each of the privacy amplification set is $2^{nI(X_i;Z_f)}$; $i\in\{1,2\}, f\in\{1,2,\dots,d\}$. For docoding, as mentioned before, the simultaneous decoding is employed to decode the messages.

Now, we provide analysis of the probability of error in detail.

Codebook construction: To generate codebooks, fix $p(q), p(x_1|q), p(x_2|q)$. Consider the c-q controlling state, which controls the performance of encoding and decoding schemes of the channel:

$$\rho^{QX_1X_2YZ_1\dots Z_d} := \sum_{qx_1x_2} p(q)p(x_1|q)p(x_2|q)|qx_1x_2\rangle \langle qx_1x_2|^{QX_1X_2} \otimes \rho_{x_1x_2}^{YZ_1\dots Z_d} \quad (8)$$

Randomly and independently generate 2^{nR_i}; $i\in\{1,2\}$ sequences $x_1^n(m_1,k_1,\dots,k_d)$ and $x_2^n(m_2,k_1',\dots,k_d')$ according to $\prod_{j=1}^n p_{X_1}(x_{1j},k_{1j},\dots,k_{fj})$ and $\prod_{j=1}^n p_{X_2}(x_{2j},k_{1j}',\dots,k_{fj}')$, respectively. Suppose that the receiver employs a decoding POVM $\{\Lambda_{\hat{m}_1,\hat{m}_2,k_1,\dots,k_d,k_1',\dots,k_d'}\}$. Based on the definition of the probability of error in [17], it is defined for our channel model as:

$$p_e(m_1,m_2) \equiv pr\{(M_1',M_2') \neq (m_1,m_2)\}$$
$$= Tr\{(I-\Lambda_{\hat{m}_1,\hat{m}_2,k_1,\dots,k_d,k_1',\dots,k_d'})\rho_{m_1,m_2,k_1,\dots,k_d,k_1',\dots,k_d'}^{Y^nZ_1^n\dots Z_d^n}\}$$

Also, we need the following lemma in our proof.

Lemma 1: (*Hayashi-Nagaoka inequality* [29]) *Suppose that S , $T\in\mathcal{P}(\mathcal{H}_X)$ such that $(I-S)\in\mathcal{P}(\mathcal{H}_X)$ are operators such that $T\geq 0$ and $0\leq S\leq I$. Then, the following relation holds:*

$$I-(S+T)^{-\frac{1}{2}}S\,(S+T)^{-\frac{1}{2}} \leq 2(I-S)+4T \quad (9)$$

where $\mathcal{P}(\mathcal{H}_X)$ is set of non-negative operators on $\mathcal{H}_X$.

Proof: see [29].

Now, consider that Bob uses the positive-operator valued measure (POVM) with $(\Pi')^{Y'}_{q,x_1(m_1),x_2(m_2),\delta}$. Let $S\equiv(\Pi')^{Y'}_{q,x_1(m_1),x_2(m_2),\delta}$ and $T\equiv\sum_{(\hat{m}_1,\hat{m}_2)\neq(m_1,m_2)}(\Pi')^{Y'}_{q,x_1(m_1),x_2(m_2),\delta}$. Then from the above lemma, we have:

$$P_e \leq 2Tr\left[\left(I-(\Pi')^{Y'}_{q,x_1(\hat{m}_1),x_2(\hat{m}_2),\delta}\right)(\rho')^{Y'}_{q,x_1(m_1),x_2(m_2)}\right] + 4\sum_{\substack{(\hat{m}_1,\hat{m}_2)\neq\\(m_1,m_2)}} Tr\left[(\Pi')^{Y'}_{q,x_1(\hat{m}_1),x_2(\hat{m}_2),\delta}(\rho')^{Y'}_{q,x_1(m_1),x_2(m_2)}\right]$$

Now, the last term of the above relation is split to three terms, each of them is corresponding to an error event. So,

$$\begin{aligned}P_e &\leq 2Tr\left[\left(I-(\Pi')^{Y'}_{q,x_1(\hat{m}_1),x_2(\hat{m}_2),\delta}\right)(\rho')^{Y'}_{q,x_1(m_1),x_2(m_2)}\right]\\
&+4\sum_{(\hat{m}_1)\neq(m_1)}\sum_{k_1}\dots\sum_{k_d} Tr\left[(\Pi')^{Y'}_{q,x_1(\hat{m}_1),x_2(m_2),\delta}(\rho')^{Y'}_{q,x_1(m_1),x_2(m_2)}\right]\\
&+4\sum_{(\hat{m}_2)\neq(m_2)}\sum_{k_1'}\dots\sum_{k_d'} Tr\left[(\Pi')^{Y'}_{q,x_1(m_1),x_2(\hat{m}_2),\delta}(\rho')^{Y'}_{q,x_1(m_1),x_2(m_2)}\right]\\
&+4\sum_{\substack{(\hat{m}_1,\hat{m}_2)\neq\\(m_1,m_2)}}\sum_{k_1}\dots\sum_{k_d}\sum_{k_1'}\dots\sum_{k_d'} Tr\left[(\Pi')^{Y'}_{q,x_1(\hat{m}_1),x_2(\hat{m}_2),\delta}(\rho')^{Y'}_{q,x_1(m_1),x_2(m_2)}\right]\end{aligned}$$

By applying the expectation over the codebook, we have:

$$\begin{aligned}&\mathbb{E}\left\{Tr\left[(I-\Lambda^{Y'}_{\hat{m}_1\hat{m}_2k_1k_2})(\rho')^{Y'}_{q,x_1(m_1),x_2(m_2)}\right]\right\}\\
&\leq \sum_{qx_1x_2} p(q)p(x_1|q)p(x_2|q)\ Tr\left[\left(I-(\Pi')^{Y'}_{q,x_1(\hat{m}_1),x_2(\hat{m}_2),\delta}\right)(\rho')^{Y'}_{q,x_1(m_1),x_2(m_2)}\right]\\
&+4(2^{n\tilde{R}_1}-1)\sum_{qx_1'x_2} p(q)p(x_1|q)p(x_1'|q)p(x_2|q)\,Tr[(\Pi')^{Y'}_{q,x_1(\hat{m}_1),x_2(m_2),\delta}(\rho')^{Y'}_{q,x_1(m_1),x_2(m_2)}]\\
&+4(2^{n\tilde{R}_2}-1)\sum_{qx_1x_2'} p(q)p(x_1|q)p(x_2|q)p(x_2'|q)\,Tr[(\Pi')^{Y'}_{q,x_1(m_1),x_2(\hat{m}_2),\delta}(\rho')^{Y'}_{q,x_1(m_1),x_2(m_2)}]\\
&+4(2^{n\tilde{R}_1}-1)(2^{n\tilde{R}_2}-1)\sum_{qx_1'x_2'} p(q)p(x_1|q)p(x_1'|q)p(x_2|q)p(x_2'|q)\ Tr\left[(\Pi')^{Y'}_{q,x_1(\hat{m}_1),x_2(\hat{m}_2),\delta}(\rho')^{Y'}_{q,x_1(m_1),x_2(m_2)}\right]\end{aligned}$$

After a straightforward calculation similar to what explained in [27], we have:

$$\bar{p}_e \leq \epsilon' + \prod_{f=1}^{d} |k_f| \, 2^{n\tilde{R}_1} 2^{-I(X_1:Y|X_2Q)_\rho} + \prod_{f=1}^{d} |k'_f| \, 2^{n\tilde{R}_2} 2^{-I(X_2:Y|X_1Q)_\rho} + \prod_{f=1}^{d} |k_f||k'_f| \, 2^{n\tilde{R}_1+n\tilde{R}_2} 2^{-I(X_1X_2:Y|Q)_\rho}$$

Then, we have:

$$\tilde{R}_1 \leq I(X_1:Y|X_2Q)_\rho$$
$$\tilde{R}_2 \leq I(X_2:Y|X_1Q)_\rho$$
$$\tilde{R}_1 + \tilde{R}_2 \leq I(X_1,X_2:Y|Q)_\rho$$

By setting $|k_f| = 2^{nI(X_1;Z_f)_\rho}$ and $|k'_f| = 2^{nI(X_1;Z'_f)_\rho}$, we have:

$$R_1 \leq I(X_1;Y|X_2Q) - \sum_{i=1}^{d} I(X_1;Z_i|Q)$$
$$R_2 \leq I(X_2;Y|X_1Q) - \sum_{i=1}^{d} I(X_2;Z_i|Q)$$
$$R_1 + R_2 \leq I(X_1X_2;Y|Q) - \sum_{i=1}^{d} I(X_1;Z_i|Q) - \sum_{i=1}^{d} I(X_2;Z_i|Q)$$

This completes the proof.

Appendix B: *(Proof of the secrecy constraint)*

In this section, we provide the proof of the secrecy constraint.

Secrecy constraint: (two-user case) The secrecy criterion for C-QMA-WTC can be defined as follows:

$$I(\mathcal{M}_1,\mathcal{M}_2;Z_1^n,\dots,Z_d^n) \leq \lambda \tag{10}$$

This relation tells us that the mutual information between Eve and the pair messages $(\mathcal{M}_1,\mathcal{M}_2)$ (leaked information) is smaller than an arbitrarily small positive number.

The senders select the junk variables k_f and $k'_f, f \in \{1,\dots,d\}$ uniformly at random in order to randomize each Eve's knowledge about the sent messages m_1, m_2. Then Eves' expected state can be defined as follows:

$$\theta_{m_1,m_2}^{Z_1^n\dots Z_d^n} = \frac{1}{|\mathcal{K}_1||\mathcal{K}_2|} \sum_{k_1\in\mathcal{K}_1} \sum_{k_2\in\mathcal{K}_2} P_{X_1}(x_1^n(m_1,k_1,\dots,k_d)) P_{X_2}(x_2^n(m_2,k'_1,\dots,k'_d)) \rho_{x_1^n x_2^n}^{Z_1^n\dots Z_d^n}$$

Let $\bar{\theta}^{Z_1^n,\dots,Z_d^n}$ denote Eves' state averaged over all possible messages:

$$\bar{\theta}^{Z_1^n,\dots,Z_d^n} = \frac{1}{|\mathcal{M}_1||\mathcal{M}_2|} \sum_{m_1\in\mathcal{M}_1} \sum_{m_2\in\mathcal{M}_2} \theta_{m_1,m_2}^{Z_1^n\dots Z_d^n} \tag{11}$$

If Eves' state be close to a constant state $(\theta^{Z_1^n\dots Z_d^n})$ the constraint of λ-privacy holds:

$$\left\|\bar{\theta}^{Z_1^n\dots Z_d^n} - \theta^{Z_1^n\dots Z_d^n}\right\|_1 \leq 2\lambda' < \frac{1}{e} \tag{12}$$

This constraint implies that Eves' information about the sent messages is small:

$$I(\mathcal{M}_1,\mathcal{M}_2;Z_1^n,\dots,Z_d^n) = H(Z_1^n,\dots,Z_d^n) - H(Z_1^n,\dots,Z_d^n|\mathcal{M}_1,\mathcal{M}_2)$$
$$= S(\bar{\theta}^{Z_1^n\dots Z_d^n}) - \frac{1}{|\mathcal{M}_1||\mathcal{M}_2|} \sum_{m_1\in\mathcal{M}_1} \sum_{m_2\in\mathcal{M}_2} S\left(\theta_{m_1,m_2}^{Z_1^n\dots Z_d^n}\right)$$
$$\leq S(\theta^{Z_1^n\dots Z_d^n}) - \frac{1}{|\mathcal{M}_1||\mathcal{M}_2|} \sum_{m_1\in\mathcal{M}_1} \sum_{m_2\in\mathcal{M}_2} S(\theta^{Z_1^n\dots Z_d^n}) + 2n\lambda' \log\dim\mathcal{H}^{Z_1\dots Z_d} - 2\lambda' \log 2\lambda'$$
$$= 2n\lambda' \log\dim\mathcal{H}^{Z_1\dots Z_d} - 2\lambda' \log 2\lambda' \tag{13}$$

The inequality follows from using *Fannes' inequality* [30] for both entropies. With choosing λ' arbitrarily small, for example $\lambda' = 2^{-n}$, equation (13) guarantees that the Eves knowledge about the sent messages exponentially vanishes.

The security proof for the l-user case can be concluded by a similar procedure.

Appendix C: *(Proof of the Theorem 2)*

In this section, we prove Theorem 2. Some steps are similar to those for Theorem 1. So, we only mention the differences.

Encoding and transmission: This step is the same as Theorem 1. The only difference is that under the one-shot setting, we can only use the channel once.

Decoding: In order to decode the messages and the junk variables, we use the simultaneous decoder and *convex split lemma* [28] which is employed as a useful tool in recent developments in quantum information theory and it also has been used to obtain the one-shot bounds for secure communications [25,31,32] over quantum channels.

***Lemma 2**: (Convex split lemma)* [28] *let ρ_{XY} be an arbitrary state and suppose that $\tau_{X_1\dots X_kB}$ be the following state:*

$$\tau_{X_1\dots X_kB} = \frac{1}{K} \sum_{k=1}^{K} \rho_{X_1} \otimes \dots \otimes \rho_{X_{k-1}} \otimes \rho_{X_kB} \otimes \rho_{X_{k+1}} \otimes \dots \rho_{X_k}$$

Let $\epsilon \in (0,1)$ and $\eta \in (0,\sqrt{\epsilon}]$, if

$$\log_2 K = \tilde{I}_{max}^{\sqrt{\epsilon}-\eta}(Y;X)_\rho + 2\log_2\left(\frac{1}{\eta}\right) \tag{14}$$

then,

$$P(\tau_{X_1\dots X_kB}, \rho_{X_1} \otimes \dots \otimes \rho_{X_k} \otimes \tilde{\rho}_Y) \leq \sqrt{\epsilon}$$

for some state $\tilde{\rho}_Y$ such that $P(\rho_Y,\tilde{\rho}_Y) \leq \sqrt{\epsilon} - \eta$.

Proof: see [25].

To generate codebooks, fix $p(q), p(x_1|q), p(x_2|q)$. Consider the following c-q state, which is employed to control the performance of encoding and decoding operations of the channel:

$$\rho^{QX_1X_2YZ_1\dots Z_d} := \sum_{qx_1x_2} p(q)p(x_1|q)p(x_2|q)|qx_1x_2\rangle\langle qx_1x_2|^{QX_1X_2} \otimes \rho^{YZ_1\dots Z_d}_{x_1x_2} \quad (15)$$

Generate 2^{R_i} codewords x_i with the probability $p(x_i|q) \to x_i(m_i), i \in \{1,2\}$.

According to the described setting in [18], we can consider new alphabets according to the Hilbert space $\mathcal{H}$: $\mathcal{Q}' = \mathcal{Q} \times \mathcal{H}$, $\mathcal{X}_1' = \mathcal{X}_1 \times \mathcal{H}$ and $\mathcal{X}_2' = \mathcal{X}_2 \times \mathcal{H}$. Now, the new codewords can be shown as: $(q, h_q) \equiv \tilde{q}$, $(x_1, h_{x_1}) \equiv \tilde{x}_1$, $(x_2, h_{x_2}) \equiv \tilde{x}_2$ and the new controlling state is $\rho^{QX_1X_2YZ_1\dots Z_d} \otimes |0\rangle\langle 0|^{\mathbb{C}^2} \otimes \frac{I^{\otimes \mathcal{H}^3}}{|\mathcal{H}|^3}$. These choices are due to the *tilting map* described in [18]. The new channel, named as *perturbed channel,* can be trivially obtained from the main channel.

Note that, the expected average decoding error for the main channel is the same as the perturbed channel. Now, the controlling state of the perturbed channel is as follows:

$$(\rho')^{Q'X_1'X_2'Y'Z_1'\dots Z_d'} := |\mathcal{H}|^{-3} \sum_{\tilde{q}\tilde{x}_1\tilde{x}_2} p(q)p(x_1|q)p(x_2|q)|\tilde{q}\rangle\langle\tilde{q}|^{Q'} \otimes |\tilde{x}_1\rangle\langle\tilde{x}_1|^{X_1'} \otimes |\tilde{x}_2\rangle\langle\tilde{x}_2|^{X_2'} \otimes (\rho')^{YZ}_{\tilde{q}\tilde{x}_1\tilde{x}_2\delta} \quad (16)$$

where $0 \le \delta < 1$.

For $m_1 = \{1, \dots, 2^{R_1}\}$, choose $(\tilde{x}_1)(m_1) \in \mathcal{X}_1 \times \mathcal{H}$, and for $m_2 = \{1, \dots, 2^{R_2}\}$ choose $(\tilde{x}_2)(m_2) \in \mathcal{X}_2 \times \mathcal{H}$.

Decoding: At first, we should analyze the error events. Bob uses $(\Pi')^{Y'}_{\tilde{q},\tilde{x}_1(m_1),\tilde{x}_2(m_2),\delta}$ to construct his POVM (see Definition 8). Let $\Lambda^{Y'}_{\hat{m}_1,\hat{m}_2,k_1,\dots,k_d,k_1',\dots,k_d'}$ be Bob's POVM for decoding the messages.

Consider the *Hayashi-Nagaoka inequality*. Let $S \equiv (\Pi')^{Y'}_{\tilde{q},\tilde{x}_1(m_1),\tilde{x}_2(m_2),\delta}$ and $T \equiv \sum_{(\hat{m}_1,\hat{m}_2)\neq(m_1,m_2)} (\Pi')^{Y'}_{\tilde{q},\tilde{x}_1(m_1),\tilde{x}_2(m_2),\delta}$. Then from the lemma 2, we have:

$$P_e \le 2Tr\left[\left(I - (\Pi')^{Y'}_{\tilde{q},\tilde{x}_1(\hat{m}_1),\tilde{x}_2(\hat{m}_2),\delta}\right)(\rho')^{Y'}_{\tilde{q},\tilde{x}_1(m_1),\tilde{x}_2(m_2)}\right] + 4\sum_{\substack{(\hat{m}_1,\hat{m}_2)\neq\\(m_1,m_2)}} Tr\left[(\Pi')^{Y'}_{(\tilde{q}),\tilde{x}_1(\hat{m}_1),\tilde{x}_2(\hat{m}_2),\delta}(\rho')^{Y'}_{\tilde{q},\tilde{x}_1(m_1),\tilde{x}_2(m_2)}\right]$$

$$= 2Tr\left[\left(I - (\Pi')^{Y'}_{\tilde{q},\tilde{x}_1(\hat{m}_1),\tilde{x}_2(\hat{m}_2),\delta}\right)(\rho')^{Y'}_{\tilde{q},\tilde{x}_1(m_1),\tilde{x}_2(m_2)}\right] + 4\sum_{(\hat{m}_1)\neq(m_1)}\sum_{k_1}\dots\sum_{k_d} Tr\left[(\Pi')^{Y'}_{\tilde{q},\tilde{x}_1(\hat{m}_1),\tilde{x}_2(m_2),\delta}(\rho')^{Y'}_{\tilde{q},\tilde{x}_1(m_1),\tilde{x}_2(m_2)}\right]$$
$$+4\sum_{(\hat{m}_2)\neq(m_2)}\sum_{k_1'}\dots\sum_{k_d'} Tr\left[(\Pi')^{Y'}_{\tilde{q},\tilde{x}_1(m_1),\tilde{x}_2(\hat{m}_2),\delta}(\rho')^{Y'}_{\tilde{q},\tilde{x}_1(m_1),\tilde{x}_2(m_2)}\right]$$
$$+4\sum_{\substack{(\hat{m}_1,\hat{m}_2)\neq\\(m_1,m_2)}}\sum_{k_1}\dots\sum_{k_d}\sum_{k_1'}\dots\sum_{k_d'} Tr\left[(\Pi')^{Y'}_{\tilde{q},\tilde{x}_1(\hat{m}_1),\tilde{x}_2(\hat{m}_2),\delta}(\rho')^{Y'}_{\tilde{q},\tilde{x}_1(m_1),\tilde{x}_2(m_2)}\right]$$

By applying the expectation over the codebook, we have:

$$\mathbb{E}\left\{Tr\left[(I - \Lambda^{Y'}_{\hat{m}_1\hat{m}_2k_1k_2})(\rho')^{Y'}_{\tilde{q},\tilde{x}_1(m_1),\tilde{x}_2(m_2)}\right]\right\}$$
$$\le 2|\mathcal{H}|^{-3}\sum_{\tilde{q}\tilde{x}_1\tilde{x}_2} p(q)p(x_1|q)p(x_2|q)\, Tr\left[\left(I - (\Pi')^{Y'}_{\tilde{q},\tilde{x}_1(\hat{m}_1),\tilde{x}_2(\hat{m}_2),\delta}\right)(\rho')^{Y'}_{\tilde{q},\tilde{x}_1(m_1),\tilde{x}_2(m_2)}\right]$$
$$+ 4(2^{\tilde{R}_1} - 1)|\mathcal{H}|^{-4}\sum_{\tilde{q}\tilde{x}_1'\tilde{x}_2} p(q)p(x_1|q)p(x_1'|q)p(x_2|q)\, Tr[(\Pi')^{Y'}_{\tilde{q},\tilde{x}_1'(\hat{m}_1),\tilde{x}_2(m_2),\delta}(\rho')^{Y'}_{\tilde{q},\tilde{x}_1(m_1),\tilde{x}_2(m_2)}]$$
$$+4(2^{\tilde{R}_2} - 1)|\mathcal{H}|^{-4}\sum_{\tilde{q}\tilde{x}_1\tilde{x}_2'} p(q)p(x_1|q)p(x_2|q)p(x_2'|q)\, Tr[(\Pi')^{Y'}_{\tilde{q},\tilde{x}_1(m_1),\tilde{x}_2'(\hat{m}_2),\delta}(\rho')^{Y'}_{\tilde{q},\tilde{x}_1(m_1),\tilde{x}_2(m_2)}]$$
$$+4(2^{\tilde{R}_1} - 1)(2^{\tilde{R}_2} - 1)|\mathcal{H}|^{-5}\sum_{\tilde{q}\tilde{x}_1'\tilde{x}_2'} p(q)p(x_1|q)p(x_1'|q)p(x_2|q)p(x_2'|q)\, Tr[(\Pi')^{Y'}_{\tilde{q},\tilde{x}_1'(\hat{m}_1),\tilde{x}_2'(\hat{m}_2),\delta}(\rho')^{Y'}_{\tilde{q},\tilde{x}_1(m_1),\tilde{x}_2(m_2)}]$$

At this step, using the quantum joint typicality lemma [Corollary 4, 18], we have:

$$\bar{p}_e \le \epsilon' + 2^{\tilde{R}_1+2}2^{-I_H^\epsilon(X_1;Y|X_2Q)_\rho} + 2^{\tilde{R}_2+2}2^{-I_H^\epsilon(X_1;Y|X_2Q)_\rho} + 2^{\tilde{R}_1+\tilde{R}_2+2}2^{-I_H^\epsilon(X_1,X_2;Y|Q)_\rho}$$

Then, we have:

$$\begin{aligned}\tilde{R}_1 &\le I_H^\epsilon(X_1;Y|X_2Q)_\rho - 2 - \log\left(\frac{1}{\epsilon}\right)\\ \tilde{R}_2 &\le I_H^\epsilon(X_2;Y|X_1Q)_\rho - 2 - \log\left(\frac{1}{\epsilon}\right)\\ \tilde{R}_1 + \tilde{R}_2 &\le I_H^\epsilon(X_1,X_2;Y|Q)_\rho - 2 - \log\left(\frac{1}{\epsilon}\right)\end{aligned} \quad (17)$$

Using the convex split lemma, we have:

$$\log_2 K_f = \tilde{I}_{max}^{\sqrt{\varepsilon_1}-\eta_1}(X_1;Z_f|Q)_\rho + 2\log_2\left(\frac{1}{\eta_1}\right) \quad (18)$$

$$\log_2 K_f' = \tilde{I}_{max}^{\sqrt{\varepsilon_2}-\eta_2}(X_2;Z_f'|Q)_\rho + 2\log_2\left(\frac{1}{\eta_2}\right) \quad (19)$$

Suppose $\eta_i = \sqrt{\epsilon}$, $i \in \{1,2\}$, then:

$$\log_2 K_f = \tilde{I}^{\epsilon}_{max}\left(X_1; Z_f|Q\right)_{\rho} + \log_2\left(\frac{1}{\epsilon}\right) \quad (20)$$

$$\log_2 K'_f = \tilde{I}^{\epsilon}_{max}\left(X_2; Z'_f|Q\right)_{\rho} + \log_2\left(\frac{1}{\epsilon}\right) \quad (21)$$

Combining (20), (21), and (17) with a straightforward simplification completes the proof.

Appendix D: (*Leaked information analysis*)

Secrecy criterion: In fact, the mutual information between sent messages and wiretappers, should be negligible. Actually, it should be smaller than an arbitrary small number:

$$I(M_1, M_2; Z_1 \dots Z_d) \leq \epsilon, \epsilon \in (0,1) \quad (22)$$

The leaked information from the ,user-i to Eve is $I(M_i; Z_f) \leq \epsilon_i, f \in \{1, \dots, d\}$. we just calculate the sum rate leakage $(R'_1 + R'_2)$.

Let $\rho^{X_1X_2Z_1\dots Z_d} := \sum_{\substack{m_1\in[2^{R_1}]\\ m_2\in[2^{R_2}]}} \frac{1}{2^{R_1+R_2}} |m_1\rangle\langle m_1|^{X_1} \otimes |m_2\rangle\langle m_2|^{X_2} \otimes \rho^{Y}_{x_1x_2}$ be the joint state of the senders and Eves $(X_1X_2Z_1 \dots Z_d)$. Then, we have:

$$\rho^{Z_1\dots Z_d}_{m_1m_2} = \frac{1}{R'_1 + R'_2} \sum_{k_f\in[2^{R'_1}], k'_f\in[2^{R'_2}], f=[1:d]} \rho^{Z_1\dots Z_d}_{x_1(m_1,k_1,\dots,k_d), x_2(m_2,k'_1,\dots,k'_d)} \quad (23)$$

where $\rho^{Z_1\dots Z_d}_{x_1(m_1,k_1,\dots,k_d),x_2(m_2,k'_1,\dots,k'_d)} := Tr_Y[\rho^{YZ_1\dots Z_d}_{x_1\,x_2}]$ and $\rho^{YZ_1\dots Z_d}_{x_1\,x_2} := \mathcal{N}^{X_1X_2\to YYZ_1\dots Z_d}(\rho^{X_1X_2}_{x_1\,x_2})$. Let $\tilde{\rho}^{Z_1\dots Z_d} := \frac{1}{R'_1+R'_2}\sum_{m_2=1}^{2^{R'_2}}\sum_{m_1=1}^{2^{R'_1}} \rho^{Z_1\dots Z_d}_{m_1m_2}$ and $\rho^{Z_1\dots Z_d} := \mathbb{E}_{x_1\,x_2}\{\rho^{Z_1\dots Z_d}_{x_1\,x_2}\}$.

Information leakage can be calculated as follows:

$$\left\| \sum_{m_2=1}^{2^{R'_2}}\sum_{m_1=1}^{2^{R'_1}} \frac{1}{R'_1 + R'_2} |m_1\rangle\langle m_1|^{x_1} \otimes |m_2\rangle\langle m_2|^{x_2} \otimes \rho^{Z_1\dots Z_d}_{m_1m_2} - \sum_{m_2=1}^{2^{R'_2}}\sum_{m_1=1}^{2^{R'_1}} \frac{1}{R'_1 + R'_2} |m_1\rangle\langle m_1|^{x_1} \otimes |m_2\rangle\langle m_2|^{x_2} \otimes \tilde{\rho}^{Z_1\dots Z_d} \right\|$$

$$\leq \sum_{m_2=1}^{2^{R'_2}}\sum_{m_1=1}^{2^{R'_1}} \frac{1}{2^{R'_1+R'_2}} \left\|\rho^{Z_1\dots Z_d}_{m_1m_2} - \tilde{\rho}^{Z_1\dots Z_d}\right\| \overset{(a)}{\leq} \sum_{m_2=1}^{2^{R'_2}}\sum_{m_1=1}^{2^{R'_1}} \frac{1}{2^{R'_1+R'_2}} \left\|\rho^{Z_1\dots Z_d}_{m_1m_2} - \rho^{Z_1\dots Z_d}\right\| + \left\|\rho^{Z_1\dots Z_d} - \tilde{\rho}^{Z_1\dots Z_d}\right\|$$

$$\leq 2\sum_{m_2=1}^{2^{R'_2}}\sum_{m_1=1}^{2^{R'_1}} \frac{1}{2^{R'_1+R'_2}} \left\|\rho^{Z_1\dots Z_d}_{m_1m_2} - \rho^{Z_1\dots Z_d}\right\| \overset{(b)}{\leq} 2\sum_{m_2=1}^{2^{R'_2}}\sum_{m_1=1}^{2^{R'_1}} \frac{1}{2^{R'_1+R'_2}} \mathbb{E}_C\left\|\rho^{Z_1\dots Z_d}_{m_1m_2} - \rho^{Z_1\dots Z_d}\right\| \overset{(c)}{\leq} \epsilon'$$

where (a) follows from triangle inequality [33], (b) follows from applying expectation over the random codebook and using the symmetry of the code construction and (c) follows from using the *Gentle operator lemma for ensembles* [26].

This relation tells us that the leaked information from both senders to Eve while they are communicating simultaneously with a legitimate receiver is smaller than an arbitrarily small number.

REFERENCES

[1] C. Shannon, "Communication Theory of Secrecy Systems," *Bell Syst. Tech. J.*, vol. 28(4), pp. 656–715, 1949.

[2] A. D. Wyner. "The wire-tap channel," *Bell Syst. Tech. J.*, vol. 54, no. 8, pp. 2–10, October 1975.

[3] I. Csiszar and J. Korner. "Broadcast channels with confidential messages," *IEEE Trans. Inf. Theory*, vol. 24, no. 3, pp. 339–348, May 1978.

[4] E. Ekrem and S. Ulukus. "On the secrecy of multiple access wiretap channel," *in proc. 46th Annual Allerton Conference on Communication, Control, and Computing*, Urbana-Champaign, IL, USA, March 2009.

[5] E. Tekin and A. Yener, "The Gaussian multiple access wiretap channel," *IEEE Trans. Inf. Theory*, vol.54, no.12, pp. 5747-5755, December 2008.

[6] E. Tekin and A. Yener, "The general Gaussian multiple access and two-way wire-tap channels: Achievable rates and cooperative jamming," *IEEE Trans. Inf. Theory*, vol.54, no. 6, pp. 2735–2751, June 2008.

[7] Y. Liang, H.V. Poor, "Multiple-access channels with confidential messages," *IEEE Trans. Inf. Theory*, vol. 54, no.3, pp. 976–1002, March 2008.

[8] X. Tang, R. Liu, P. Spasojevi´c, H.V. Poor, "Multiple acess channels with generalized feedback and confidential messages," *In: Proc. Inf. Theory Workshop*, Lake Tahoe, CA, USA (September 2007) 608–613.

[9] B. Dai and Z.Ma, "Some New Results on the Multiple-Access Wiretap Channel," *Entropy*, pp. 4693-4712, 2014.

[10] R. Liu, I. Mari´c, R. Yates, P. Spasojevi´c, "The discrete memoryless multiple access channel with confidential messages," *In: Proc. Int. Symp. Inf. Theory*, Seattle, USA (July 2006) 957–961.

[11] R. Liu, I. Maric, P. Spasojevic, R.D. Yates, "Discrete Memoryless Interference and Broadcast Channels With Confidential Messages: Secrecy Rate Regions," *IEEE Trans. Inf. Theory*, vol. 54, no. 6, June 2008, pp. 2493-2507.

[12] N. Cai, A. Winter, and R. W. Yeung. "Quantum Privacy and Quantum Wiretap Channels," *Problems of Information Transmission,* vol. 40, no. 4, pp. 318-336, 2004.

[13] I. Devetak, "The Private Classical Capacity and Quantum Capacity of a Quantum Channel," *IEEE Trans. Inf. Theory*, vol. 51, no. 1, pp. 44-55, January 2005.

[14] A. Winter, "The capacity of the quantum multiple-access channel," *IEEE Trans. Inf. Theory*, vol. 47, no. 7, pp. 3059–3065, July 2001.

[15] H. Aghaee, B. Akhbari, "Classical-quantum multiple access wiretap channel," *16th International ISC Conference on Information Security and Cryptology (ISCISC'19)*, Mashhad, Iran, August 2019.

[16] H. Aghaee, B. Akhbari, "Achievable secrecy rate regions for 3-User classical-quantum interference wiretap channels with a mixed strong-very strong interference," *10th Conference on Information and Knowledg Technology (IKT'19)*, Iran, 2019.

[17] H. Aghaee, B. Akhbari, "Classical-quantum multiple access wiretap channel with common message: one-shot rate region," *11th Conference on Information and Knowledge Technology (IKT'20)*, Iran, 2020.

[18] P. Sen, "A one-shot quantum joint typicality lemma," (2018), arXiv:1806.07278.

[19] A. El Gamal, Y.H Kim, "Network information theory" Cambridge University Press, January 2012.

[20] A. Anshu, R. Jain, N. Warsi, "On the near-optimality of one-shot classical communication over quantum channels," arXiv 1804.09644, 2018.

[21] A. Anshu, R. Jain, N. Warsi, "One-shot entanglement assisted classical and quantum communication over noisy quantum channels: A hypothesis testing and convex-split approach," arXiv 1702.01940, 2017."

[22] L. Wang and R. Renner "One-Shot Classical-Quantum Capacity and Hypothesis Testing". *Phys. Rev. Lett*., 108(20), May 2012.

[23] M. Berta, M. Christandl and R. Renner, "The quantum reverse Shannon theorem based on one-shot information theory," *Commun. Math. Phys.*, vol. 306, no. 3, pp. 579-615, 2011.

[24] N. Datta, "Min-max-relative entropies and a new entanglement monotone," *IEEE. Trans. Inf. Theory*, vol. 59, pp. 2816-2816, 2009.

[25] M. Wilde, "Position-based coding and convex splitting for private communication over quantum channels," *Quantum Information Processing*, 16(10):264, October 2017. arXiv:1703.01733.

[26] M. Wilde, Quantum Information Theory, *Cambridge Univ. Press, 2013.*

[27] O. Fawzi, P. Hayden, I. Savov, P. Sen, and M. M. Wilde, "Classical communication over a quantum interference channel," *IEEE Trans. on Inf. Theory*, vol. 58, no. 6, pp. 3670-3691, June 2012.

[28] A. Anshu, V. K. Devabathini, R. Jain, "Quantum message compression with applications,". arXiv:1410.3031, 2014.

[29] M. Hayashi, H. Nagaoka, "General formulas for capacity of classical-quantum channels," *IEEE Trans. Inf. Theory,* vol. 49, pp. 1753–1768, 2003.

[30] M. Fannes, "A Continuity Property of the Entropy Density for Spin Lattice Systems," *Comm. Math. Phys.*, vol. 31, pp. 291-294, 1973.

[31] H. Qi, K, Sharma, and M. Wilde, "Entanglement-assisted private communication over quantum broadcast channels," *Journal of Physics A: Mathematical and Theoretical*, 51(37):374001, August 2018. arXiv:1803.03976.

[32] F. Salek, A. Anshu, M.-H. Hsieh, R. Jain, J. R. Fonollosa, "One-shot Capacity Bounds on the Simultaneous Transmission of Public and Private Information Over Quantum Channels," *IEEE. Int. Symp. Inf. Theory,* CO, USA, 2018.

[33] M. Tomamichel, "A framework for non-asymptotic quantum information theory." *PhD Thesis*, ETH Zurich, http://arXiv,org/abs/1203.2142, 2012.

Hadi Aghaee received the B.Sc. degree in Electrical Engineering from Qom University of Technology, Qom, Iran, in 2015, and the M.Sc. degree in Telecommunication Engineering from Faculty of Electrical Engineering K. N. Toosi University of Technology (KNTU), Tehran, Iran, in 2018. His current research interests include quantum information theory, information theory and secure communication over quantum channels.

Bahareh Akhbari received the B.Sc. degree in 2003, the M.Sc. degree in 2005 and the Ph.D. degree in 2011 all in Electrical Engineering from Sharif University of Technology (SUT), Tehran, Iran. She was also a visiting Ph.D student at the University of Minnesota for one year, starting in 2010. Since 2012, she is an assistant professor of the Faculty of Electrical Engineering, K. N. Toosi University of Technology (KNTU), Tehran, Iran. Her research interests include information theory, cryptography and network security, communication theory and information-theoretic security.