The ISC Int'l Journal of Information Security
ISeCure

November 2023, Volume 15, Number 3 (pp. 19–34)
http://www.isecure-journal.org

Presented at the ISCISC'2023 in Tehran, Iran.

Quantum Multiple Access Wiretap Channel: On the One-Shot Achievable Secrecy Rate Regions **

Hadi Aghaee [1] and Bahareh Akhbari [*,1]
[1] *Faculty of Electrical Engineering, K. N. Toosi University of Technology, Tehran, Iran*

ARTICLE INFO.

Keywords:
Broadcast Channel, Multiple Access Channel, Mutual Information, Quantum Channel, Secrecy Capacity

Type:
Research Article

doi:
10.22042/isecure.2023.180848

ABSTRACT

In this paper, we want to investigate classical-quantum multiple access wiretap channels (CQ-MA-WTC) under one-shot setting. In this regard, we analyze the CQ-MA-WTC using a simultaneous position-based decoder for reliable decoding and using a newly introduced technique to decode securely. Also, for the sake of comparison, we analyze the CQ-MA-WTC using Sen's one-shot joint typicality lemma for reliable decoding. The simultaneous position-based decoder tends to a multiple hypothesis testing problem. Also, using convex splitting to analyze the privacy criteria in a simultaneous scenario becomes problematic. To overcome both problems, we first introduce a new channel that can be considered as a dual to the CQ-MA-WTC. This channel is called a point-to-point quantum wiretap channel with multiple messages (PP-QWTC). In the following, as a strategy to solve the problem, we also investigate and analyze quantum broadcast channels (QBC) in the one-shot regime.

© 2023 ISC. All rights reserved.

1 Introduction

Quantum Multiple Access Channel (QMAC) was first introduced by Winter [1], which takes two or more messages (classical or quantum) as inputs and produces one output.

Similar to the classical world, decoding messages over a QMAC is based on two main techniques: successive decoding and simultaneous decoding. In [1], the author employs the successive decoding technique. A quantum broadcast channel (QBC) has a sender and two or more receivers, in which the sender wishes to transmit two or more messages (classical or quantum) over the channel to the receivers. The QBC was first introduced by Yard *et al.* [2]. In [2], the authors derived an inner bound for QBC for i.i.d. (independent and identical) case, and in [3], the authors derived the same inner bound using a more straightforward method and more in the spirit of its classical analogous [4] than the method in [2].

In recent decades, with the development of quantum data processing and its applications, the necessity to study the security of quantum channels has increased. In this regard, the quantum wiretap channel (QWTC) was first introduced in [5], and [6]. Then, the secrecy constraints are extended to multi-user quantum channels such as quantum interference channel (QIC) [7, 8], and quantum multiple access channel

* Corresponding author.
**The ISCISC'2023 program committee effort is highly acknowledged for reviewing this paper.
Email addresses: Aghaee_Hadi@kntu.ac.ir, akhbari@eetd.kntu.ac.ir
ISSN: 2008-2045 © 2023 ISC. All rights reserved.

(QMAC) [9–13].

There are two bottlenecks in studying the security of quantum channels. The first is decoding three or more messages simultaneously (reliability), and the second is about how to securely decode two or more messages (security). The first bottleneck arises from the nonexistence of a general quantum joint typicality lemma. However, this problem has been solved in some cases, such as the min-entropy case and QMACs with commutative output [14]. Therefore, in i.i.d. case, successive decoding combined with time-sharing techniques should be used. In this setting, transmitters are allowed to transmit their messages using the channel only once. Sen proved a joint typicality lemma which helps to decode any number of messages simultaneously in the one-shot case [14]. Obtaining secrecy against the eavesdropper by Wyner's approach [15] of randomizing over a block becomes problematic in the quantum setting. Wyner's technique has been shown to work for point-to-point quantum channels by Devetak [6] and explained further in [16]. However, there are no easy generalizations to multiple senders for a quantum channel. This issue is discussed in detail in [16].

In this paper, we want to investigate the secrecy problem of quantum multiple access channel (QMAC) with classical inputs under one-shot setting. Also, we have investigated some bottlenecks connected to the decoding process for CQ-MA-WTC. The achievement of this paper is about analyzing bottlenecks in the decoding process and providing solutions to overcome them.

Also, we present two techniques for quantum multiple access wiretap channel with classical inputs(CQ-MA-WTC). The first approach is based on the method presented in [14], and another technique is the simultaneous position-based decoder. From [17], we know that the simultaneous position-based decoder tends to a multiple quantum hypothesis testing problem solvable in a special case. Also, from [18], we know that the convex split lemma could not be used to analyze the privacy of multiple messages in simultaneous decoding.

The paper is organized as follows: We have explained related works, and our motivations in Section 2, and Section 3, respectively. In Section 4, some seminal definitions are presented. In Section 5, the main channel and information processing tasks are presented. In Section 6, the results and main theorems are presented. In Section 7 we have compared our method and results with other methods. Section 8 is dedicated to discussion and future works.

2 Related Works

The security problem of QMACs has received a lot of attention in recent years, both in i.i.d. and one-shot regimes. The problem of secure communication over QMACs with classical inputs was first investigated by the authors in the i.i.d. regime using successive decoding [9]. After that, we studied the main channel under the one-shot setting [10] using Sen's one-shot joint typicality lemma [14] and convex splitting [19]. Also, the main channel under the one-shot setting and entanglement assistance is studied by the authors in [13] using the simultaneous position-based decoder. As we know from the quantum information theory and its computational bottlenecks, the study of the security problem of multipartite quantum channels faces some computational limits. Some papers are written in order to overcome or bypass these bottlenecks [8, 13, 16], which we will explain in the following sections. In [16], the authors suggested a new approach to securely decode C-QMA-WTC under the one-shot setting instead of using convex splitting. Also, the paper [20] studies a degraded version of C-QMA-WTC in the i.i.d. regime.

3 Motivation

Some papers are written to construct new decoding approaches, such as simultaneous position-based decoding [13, 17]. In this paper, we want to have a comprehensive study about C-QMA-WTC in i.i.d. and one-shot regimes. We also construct a new method based on introducing dual channels to bypass the multiple quantum hypothesis testing problem and the smoothing bottleneck of the multipartite convex split lemma.

4 Preliminaries

Let A (Alice), B (Bob) and C (Charlie) be three quantum systems. These quantum systems can be denoted by their corresponding Hilbert spaces as $\mathcal{H}^A$, $\mathcal{H}^B$ and $\mathcal{H}^C$. ρ^A, ρ^B and ρ^C are density operators of the above quantum systems, while ρ^{ABC} is the shared state (joint state) between Alice, Bob, and Charlie. A density operator is a positive semi-definite operator with a unit trace. Every quantum state can be defined by a partial trace operator over the shared state (joint state). The partial trace is used to model the lack of access to a quantum system. Thus, $\rho^A = Tr_{BC}\{\rho^{ABC}\}$ is Alice's density operator using partial trace. $|\psi\rangle^A$ denotes the pure state of system A. Also, $\psi^A = |\psi\rangle\langle\psi|^A$ is the corresponding density operator. $H(A)_\rho = -Tr\{\rho^A \log \rho^A\}$ is the von Neumann entropy of the state ρ^A. The quantum conditional entropy can be defined as $H(A|B)_\sigma = H(A,B)_\sigma - H(B)_\sigma$ for an arbitrary bipartite state

σ^{AB}. The quantum mutual information and the conditional quantum mutual information are defined as follows:

$$I(A;B)_\sigma = H(A)_\sigma + H(B)_\sigma - H(A,B)_\sigma$$

$$I(A;B|C)_\sigma = H(A|C)_\sigma + H(B|C)_\sigma - H(A,B|C)_\sigma$$

Quantum operations can be denoted by completely positive trace-preserving (CPTP) maps $\mathcal{N}^{A\to B}$. CPTP maps take state A as input and produce state B. The distance between two quantum states, such as A and B, is defined by trace distance. The trace distance between two arbitrary states, such as σ and ρ, is:

$$\|\sigma - \rho\|_1 = Tr|\sigma - \rho| \tag{1}$$

where $|\psi| = \sqrt{\psi^\dagger \psi}$. This quantity is zero for two perfectly distinguishable states.

For two arbitrary density operators such as (ρ, σ), *fidelity* and *purified distance* can be defined as $F(\rho,\sigma) = \left\|\sqrt{\rho}\sqrt{\sigma}\right\|_1^2$, and $P(\rho,\sigma) := \sqrt{1 - F(\rho,\sigma)^2}$, respectively. Most of the above definitions are given in [19].

Definition 4.1 (Hypothesis testing mutual information). Hypothesis testing mutual information is denoted by $I_H^\epsilon := D_H^\epsilon(\rho_{XY}\|\rho_X \otimes \rho_Y)$, $\epsilon \in (0,1)$ and is considered as *quantum hypothesis testing divergence* [17] where $D_H^\epsilon(.\|.)$ is *hypothesis testing relative entropy* [17]. ϵ is the smoothing variable, $\rho^{\mathcal{H}_X\mathcal{H}_Y}$ is the joint classical-quantum state of input and output over their Hilbert spaces $(\mathcal{H}_X, \mathcal{H}_Y)$, and it can be shown as ρ_{XY}:

$$\rho_{XY} = \sum_x p_X(x) \left|x\right\rangle \left\langle x\right|_X \otimes \rho_Y^x \tag{2}$$

where p_X is the input distribution.

Definition 4.2 (Quantum relative entropy [21]). Consider states $\rho_X, \sigma_X \in \mathcal{D}(\mathcal{H}_X)$. The quantum relative entropy is defined as:

$$D(\rho_X\|\sigma_X) := \begin{cases} Tr\{\rho_X[\log_2\rho_X - \log_2\sigma_X]\} & supp\,(\rho_X) \subseteq supp\,(\sigma_X) \\ +\infty & \text{otherwise} \end{cases}$$

where $supp\,(\sigma_X)$ refers to the *set-theoretic support* of σ. $supp\,(\sigma)$ is the subspace of $\mathcal{H}$ spanned by all eigenvectors of σ with non-zero eigenvalues.

Fact 4.1. The following relation exists between the quantum relative entropy and hypothesis testing relative entropy for $\epsilon \in (0,1)$ [17]:

$$D_H^\epsilon(\rho_X\|\sigma_X) \le \frac{1}{1-\epsilon}[D(\rho_X\|\sigma_X) + h_b(\epsilon)]$$

where $h_b(\epsilon) := -\epsilon\log_2\epsilon - (1-\epsilon)\log_2(1-\epsilon)$ is a binary entropy function.

Definition 4.3 (Max mutual information [22]). 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* [23] 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 4.4 (Quantum smooth max relative entropy [23]). Consider states $\rho_X, \sigma_X \in D(\mathcal{H}_X)$, and $\epsilon \in (0,1)$. The quantum smooth max relative entropy is defined as:

$$D_{max}^\epsilon := \inf_{\rho'_X \in \mathcal{B}^\epsilon(\rho_X)} D_{max}(\rho'_X\|\sigma_X)$$

where $\mathcal{B}^\epsilon(\rho_X) := \{\rho'_X \in \mathcal{D}(\mathcal{H}_X) : P(\rho'_X, \rho_X) \le \epsilon\}$ is *ϵ-ball* for ρ_{XY}.

Definition 4.5 (Quantum smooth max mutual information [22]). Consider $\rho_{XY} := \sum_{x\in\mathcal{X}} p_X(x) \left|x\right\rangle \left\langle x\right|_X \otimes \rho_Y^x$ as a classical-quantum state and a parameter $\epsilon \in (0,1)$. The smooth max mutual information between the systems X and Y can be defined as follows:

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

where $\mathcal{B}^\epsilon(\rho_{XY}) := \{\rho'_{XY} \in (\mathcal{H}_X \otimes \mathcal{H}_Y) : P(\rho'_{XY}, \rho_{XY}) \le \epsilon\}$ is *ϵ-ball* for ρ_{XY}.

Definition 4.6 (Conditional smooth hypothesis testing mutual information [24]). Consider $\rho_{XYZ} := \sum_{z\in\mathcal{Z}} p_Z(z) \left|z\right\rangle \left\langle z\right|_Z \otimes \rho_{XY}^z$ be a tripartite classical-quantum state and $\epsilon \in (0,1)$. We define,

$$I_H^\epsilon(X;Y|Z) := \max_{\rho'} \min_{z \in supp\,(\rho'_Z)} I_H^\epsilon(X;Y)_{\rho_{XY}^z}$$

where maximization is over all $\rho'_Z = \sum_{z\in\mathcal{Z}} p_Z(z) \left|z\right\rangle \left\langle z\right|_Z$ satisfying $P(\rho'_Z, \rho_Z) \le \epsilon$.

Fact 4.2. [25] Let $\rho_{XYZ} := \sum_{z\in\mathcal{Z}} p_Z(z) \left|z\right\rangle \left\langle z\right|_Z \otimes \rho_{XY}^z$ be a tripartite classical-quantum state and $\epsilon \in (0,1)$. The following relation holds,

$$\lim_{n\to\infty} \frac{1}{n} I_H^\epsilon\left(X^{\otimes n}; Y^{\otimes n}|Z^{\otimes n}\right)_{\rho^{\otimes n}} = I(X;Y|Z)_\rho$$

Definition 4.7 (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:

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

Fact 4.3 (Relation between two definitions of the smooth max mutual information [26]). Let $\epsilon \in (0,1)$ and $\gamma \in (0,\epsilon)$ For a bipartite state ρ_{XY}, it holds that:

$$\tilde{I}_{max}^\epsilon(Y;X)_\rho \le I_{max}^{\epsilon-\gamma}(X;Y)_\rho + \log\frac{3}{\gamma^2}$$

Definition 4.8 (Conditional smooth max mutual information [24]). Consider $\rho_{XYZ} := \sum_{z\in\mathcal{Z}} p_Z(z)\,|z\rangle\langle z|_Z \otimes \rho^z_{XY}$ be a tripartite classical-quantum state and $\epsilon \in (0,1)$. We define,

$$I^{\epsilon}_{max}(X;Y|Z) := \max_{\rho'} \min_{z\in supp\,(\rho'_Z)} I^{\epsilon}_{max}(X;Y)_{\rho^z_{XY}}$$

where maximization is over all $\rho'_Z = \sum_{z\in\mathcal{Z}} p_Z(z)\,|z\rangle\langle z|_Z$ satisfying $P(\rho'_Z,\rho_Z)\le\epsilon$.

Fact 4.4. [25] Let $\rho_{XYZ} := \sum_{z\in\mathcal{Z}} p_Z(z)\,|z\rangle\langle z|_Z \otimes \rho^z_{XY}$ be a tripartite classical-quantum state and $\epsilon \in (0,1)$. The following relation holds,

$$\lim_{n\to\infty}\frac{1}{n} I^{\epsilon}_{max}\left(X^{\otimes n};Y^{\otimes n}|Z^{\otimes n}\right)_{\rho^{\otimes n}} = I(X;Y|Z)_\rho$$

Definition 4.9 (Quantum Rényi relative entropy of order α [17]). The *quantum Rényi relative entropy of order* α for a state $\rho\in\mathcal{D}(\mathcal{H})$, a positive semi-definite operator σ, and $\alpha\in[0,1)\cup(1,+\infty)$ can be defined as follows:

$$D_\alpha(\rho\|\sigma) \equiv \frac{1}{\alpha-1}\log_2\left\{\rho^\alpha\sigma^{1-\alpha}\right\}$$

Also, *Rényi entropy of order* α can be defined as follows:

$$H_\alpha(A)_\rho \equiv \frac{1}{1-\alpha}\log_2 Tr\left\{\rho^\alpha_A\right\}$$

Definition 4.10 (One-shot inner bound of a classical-quantum multiple access channel [14]). A two-user C-QMAC under the one-shot setting is a triple $(\mathcal{X}_1\times\mathcal{X}_2, \mathcal{N}_{\mathcal{X}_1\mathcal{X}_2\to Y}(x_1,x_2)\equiv\rho^Y_{x_1x_2},\mathcal{H}_Y)$, where $\mathcal{X}_1$ and $\mathcal{X}_2$ are the alphabet sets of two classical inputs, and Y is the output system. $\rho^Y_{x_1x_2}$ is a quantum state. The CPTP of the channel is $\mathcal{N}_{\mathcal{X}_1\mathcal{X}_2\to Y}$. A one-shot inner bound of a C-QMAC is as follows:

$$\begin{aligned} R_1 &\le I^{\epsilon}_H(X_1:X_2Y)_\rho - 2 + \log\epsilon \\ R_2 &\le I^{\epsilon}_H(X_2:X_1Y)_\rho - 2 + \log\epsilon \\ R_1+R_2 &\le I^{\epsilon}_H(X_1X_2:Y)_\rho - 2 + \log\epsilon \end{aligned} \tag{3}$$

with decoding error at most $49\sqrt{\epsilon}$, where $I^{\epsilon}_H(.)$ is the hypothesis testing mutual information defined in Definition 4.1 with respect to the controlling state:

$$\rho^{QX_1X_2Y} := \sum_{qx_1x_2} p(q)p(x_1|q)p(x_2|q)\,|qx_1x_2\rangle\langle qx_1x_2|^{QX_1X_2}\otimes\rho^Y_{x_1x_2} \tag{4}$$

and Q is a time-sharing variable.

Note that $I^{\epsilon}_H(:)$ is the difference between a *Rényi entropy* of order two and a conditional quantum entropy.

Lemma 1. *[16] Given the control state in Equation 4 (without time-sharing variable), $\delta'>0$ and $0<\epsilon'<\delta'$, let $\{x_1,\dots,x_{K_1}\}$ and $\{y_1,\dots,y_{K_2}\}$ be i.i.d. samples from the distributions p_X and p_Y, respectively. Then, if*

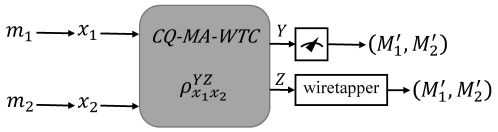

Figure 1. The CQ-MA-WTC model

$$\log|\mathcal{K}_1| \ge I^{\delta'-\epsilon'}_{max}(X:Z)_\rho + \log\frac{3}{\epsilon'^3} - \frac{1}{4}\log\delta'$$

$$\log|\mathcal{K}_2| \ge I^{\delta'-\epsilon'}_{max}(Y:ZX)_\rho + \log\frac{3}{\epsilon'^3} - \frac{1}{4}\log\delta' + \mathcal{O}(1)$$

the following holds,

$$\mathbb{E}_{\substack{X_1,\dots,X_{K_1}\sim P_X\\ Y_1,\dots,Y_{K_2}\sim P_Y}}\left\|\frac{1}{|\mathcal{K}_1|\,|\mathcal{K}_2|}\sum_{j=1}^{|\mathcal{K}_2|}\sum_{i=1}^{|\mathcal{K}_1|}\rho^Z_{x_iy_j} - \rho^Z\right\|_1 \le 20\,\delta'^{\frac{1}{8}}$$

Proof: see [16].

Lemma 2 (Convex split lemma)**.** *[19, 21] Let p_{XY} be an arbitrary state and suppose that $\tau_{X_1,\dots,X_kB}$ be the following state:*

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

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

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

then,

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

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

Proof: See [21].

Lemma 3 (Hayashi-Nagaoka inequality)**.** *[27] Suppose that $S,T\in\mathcal{P}(\mathcal{H}_X)$ such that $I-S\in\mathcal{P}(\mathcal{H}_X)$ are operators such that $T\ge0$ and $0\le S\le I$, then for all positive constant c, the following relation holds:*

$$I-(S+T)^{-\frac{1}{2}}S\,(S+T)^{-\frac{1}{2}} \le (1+c)(I-S)+(2+c+c^{-1})T$$

Proof: See [27].

5 Channel Model

A two-user CQ-MA-WTC is a triple $(\mathcal{X}_1\times\mathcal{X}_2, \mathcal{N}^{\mathcal{X}_1\mathcal{X}_2\to YZ}(x_1,x_2)\equiv\rho^{YZ}_{x_1x_2},\mathcal{H}^Y\otimes\mathcal{H}^Z)$, where $\mathcal{X}_i, i\in\{1,2\}$ denote the input alphabet sets and Y,Z denote the output systems (Y denotes the channel output at the legitimate receiver (Charlie), and Z is the channel output at the eavesdropper). $\rho^{YZ}_{x_1x_2}$ is the system output's quantum state. Both users want to transmit their messages as securely as possible over a CQ-MA-WTC to the receiver.

The main channel is illustrated in Figure 1.

Consider the main channel illustrated in Figure 1. Each user chooses its message $m_i; i \in \{1,2\}$ from its message set $\mathcal{M}_i = [1 : |\mathcal{M}_i| = 2^{R_i}]; i \in \{1,2\}$ (R_1 and R_2 are the transmitting rates corresponding to the first and the second messages, respectively) and send it over a CQ-MA-WTC. The users also use two junk variables $k_i; i \in \{1,2\}$ from two amplification sets $\mathcal{K}_i = [1 : |\mathcal{K}_i| = 2^{\hat{R}_i}]; i \in \{1,2\}$ for randomizing Eve's knowledge. We have two doubly indexed codebooks $x_1(m_1, k_1)$, and $x_2(m_2, k_2)$, for user-1 and user-2, respectively.

The above channel model is the same as what is described in [10, 11, 13], but here, we have considered the main channel with randomness-assisted codes.

6 Main Results

In this section, we present the main results.

Corollary 6.1 gives a one-shot achievable secrecy rate region for sending classical messages over a CQ-MA-WTC based on Sen's quantum joint typicality lemma [14]. The second theorem presents a novel approach to decode both messages over a CQ-MA-WTC reliably and confidentially (simultaneous position-based decoder). It should be noted that Corollary 6.1 and Theorem 1 use the same method to prove the security requirements. Also, we present a theorem that tries to overcome the bottlenecks connected to Theorem 1.

Corollary 6.1 (One-shot achievable rate region for CQ-MA-WTC). Consider a two-user CQ-MA-WTC that accepts X_1 and X_2 as inputs and Y, Z as outputs. $\rho^{YZ}_{x_1x_2}$ is the channel density operator. For any fixed $\epsilon \in (0,1), \epsilon' \in (0, \delta')$ and δ, δ' such that $\delta, \delta' > 0$, the rate pair $(R_1, R_2, 49\sqrt{\epsilon} + 20{\delta'}^{\frac{1}{8}})$ is achievable to satisfy the following inequalities:

$$\begin{aligned} R_1 \leq & I^{\epsilon}_H(X_1 : X_2Y|Q)_\rho - I^{\eta}_{max}(X_1 : Z|Q)_\rho \\ & + \log \epsilon - 2 - \log \frac{3}{\epsilon'^3} + \frac{1}{4}\log \delta' \end{aligned}$$

$$\begin{aligned} R_2 \leq & I^{\epsilon}_H(X_2 : X_1Y|Q)_\rho - I^{\eta}_{max}(X_2 : X_1Z|Q)_\rho \\ & + \log \epsilon - 2 - \log \frac{3}{\epsilon'^3} + \frac{1}{4}\log \delta' + \mathcal{O}(1) \end{aligned}$$

$$\begin{aligned} R_1 + R_2 \leq & I^{\epsilon}_H(X_1X_2 : Y|Q)_\rho - I^{\eta}_{max}(X_1 : Z|Q) \\ & - I^{\eta}_{max}(X_2 : ZX_1|Q)_\rho + \log \epsilon - 2 \\ & - 2\log \frac{3}{\epsilon'^3} + \frac{1}{2}\log \delta' + \mathcal{O}(1) \end{aligned}$$

where $\eta = \delta' - \epsilon'$ and the union is taken over input distribution $p_Q(q)p_{X_1|Q}(x_1|q)p_{X_2|Q}(x_1|q)$. Q is the time-sharing random variable, and all of the mutual information quantities are taken with respect to the following state:

$$\begin{aligned} \rho^{QX_1X_2YZ} \equiv & \sum_{q,x_1,x_2} p_Q(q)p_{X_1|Q}(x_1|q)p_{X_2|Q}(x_2|q) \\ & |q\rangle\langle q|^Q \otimes |x_1\rangle\langle x_1|^{X_1} \otimes |x_2\rangle\langle x_2|^{X_2} \\ & \otimes \rho^{YZ}_{x_1x_2} \end{aligned} \tag{5}$$

Proof: See Appendix 8.1.

Sketch of proof: The proof has two steps: 1- Reliable decoding based on Sen's quantum one-shot joint typicality (Definition 4.10). 2- Secure decoding based on Lemma 1.

Theorem 1 (One-shot lower bound for CQ–MA-WTC)**.** *For any fixed $\epsilon \in (0,1), \epsilon' \in (0,1)$, and δ, δ' such that $\delta \in (0, \epsilon), \delta' \in (0, \epsilon')$, there exists a one-shot code for the channel $\mathcal{N}^{X_1X_2 \to YZ}$, if rate pair $(R_1, R_2, \epsilon + 2\delta + 20{\delta'}^{\frac{1}{8}})$ satisfies the following bounds:*

$$\begin{aligned} R_1 \leq & I^{\epsilon}_H(X_1 : X_2Y|Q)_\rho - I^{\eta}_{max}(X_1 : Z|Q)_\rho \\ & + \log_2(\frac{4\epsilon}{\delta^2}) - \log \frac{3}{\epsilon'^3} + \frac{1}{4}\log \delta' \end{aligned}$$

$$\begin{aligned} R_2 \leq & I^{\epsilon}_H(X_2 : X_1Y|Q)_\rho - I^{\eta}_{max}(X_2 : X_1Z|Q)_\rho \\ & + \log_2(\frac{4\epsilon}{\delta^2}) - \log \frac{3}{\epsilon'^3} + \frac{1}{4}\log \delta' + \mathcal{O}(1) \end{aligned}$$

$$\begin{aligned} R_1 + R_2 \leq & I^{\epsilon}_H(X_1X_2 : Y|Q)_\rho - I^{\eta}_{max}(X_1 : Z|Q) \\ & - I^{\eta}_{max}(X_2 : ZX_1|Q)_\rho + \log_2(\frac{4\epsilon}{\delta^2}) \\ & - 2\log \frac{3}{\epsilon'^3} + \frac{1}{2}\log \delta' + \mathcal{O}(1) \end{aligned}$$

where $\eta = \delta' - \epsilon'$ and the union is taken over input distribution $p_Q(q)p_{X_1|Q}(x_1|q)p_{X_2|Q}(x_2|q)$. Q is the time-sharing random variable, and all mutual information quantities are taken with respect to the state Equation 5.

Proof: In Appendix 8.2.

Sketch of proof: The proof has two steps: 1- Reliable decoding based on the simultaneous position-based technique: for simplicity of analysis, we merge reliability and security criteria into a single criterion [21]. 2- Secure decoding based on the Lemma 1.

Remark 6.1. It should be noted that both of the above theorems tend to the same result if and only if $\delta = \epsilon$.

As mentioned before, the simultaneous position-based decoder tends to a multiple hypothesis testing problem, which is unsolvable in the general case. Also, the convex split lemma (Lemma 2) does not make sense in the simultaneous decoding, because

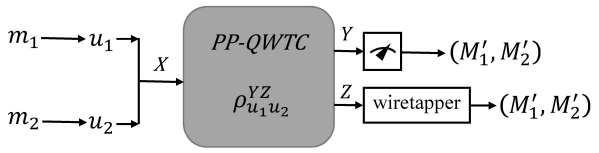

Figure 2. The PP-QWTC model

it runs to the famous smoothing bottleneck of quantum information theory. Now, consider the channel illustrated in Figure 2. This channel accepts two or more messages from one user. We call this channel a point-to-point quantum wiretap channel with multiple messages (PP-QWTC). Consider PP-QWTC with classical messages. This channel is studied in [28] under a different scenario wherein a sender wants to send classical and quantum messages simultaneously to a legitimate receiver.

Information processing task: Two classical messages, $(m_1, m_2) \in \mathcal{M}_1 \times \mathcal{M}_2$ are possessed by a sender (Alice) and are transmitted to a receiver (Bob) in the presence of a passive wiretapper over a point-to-point quantum channel under the one-shot scenario. Both of the messages should be kept as securely as possible from the wiretapper. The PP-QWTC is a triple $(\mathcal{X}, \mathcal{N}^{\mathcal{X}\to YZ}(u_1,u_2) \equiv \rho^{YZ}_{x(u_1,u_2)}, \mathcal{H}^Y \otimes \mathcal{H}^Z)$, where X denotes the input alphabet sets, and Y, Z denote the output systems (Y denotes the channel output at the legitimate receiver (Bob), and Z is the channel output at the eavesdropper). $\rho^{YZ}_{x(u_1,u_2)} \equiv \rho^{YZ}_{u_1u_2}$ is the system output's quantum state.

Alice chooses its message $m_i; i \in \{1,2\}$ from its message set $\mathcal{M}_i = [1 : |\mathcal{M}_i| = 2^{R_i}], i \in \{1,2\}$ and sends it over a PP-QWTC. Alice also uses two junk variables $k_i; i \in \{1,2\}$ from two amplification sets $\mathcal{K}_i = [1 : |\mathcal{K}_i| = 2^{\hat{R}_i}], i \in \{1,2\}$ for randomizing Eve's knowledge. We have two doubly indexed codebooks, $u_1(m_1, k_1)$, and $u_2(m_2, k_2)$.

Encoding: An encoding operation by Alice $E : M_1M_2 \to \mathcal{D}(\mathcal{H}_A)$

$$\forall\, m_1, m_2 \in M_1, M_2 \qquad \frac{1}{2}\left\|\rho_{M_1M_2Z} - \rho_{M_1M_2} \otimes \tilde{\rho}_Z\right\|_1 \le \epsilon_2 \quad (6)$$

where for each message $\rho_{M_1M_2Z}$ and $\rho_{M_1M_2}$ are appropriate marginal of the state $\rho_{M_1M_2YZ} = \frac{1}{|\mathcal{M}_1||\mathcal{M}_2|}\sum_{m_2=1}^{|\mathcal{M}_2|}\sum_{m_1=1}^{|\mathcal{M}_1|} |m_1\rangle\langle m_1| \otimes |m_2\rangle\langle m_2| \otimes \mathcal{N}(\mathcal{E}(m_1,m_2))$.

Also, $\tilde{\rho}_Z$ can be any arbitrary state.

Decoding: Decoding operation by Bob $\mathcal{D}(\mathcal{H}_B) \to \hat{M}_1\hat{M}_2$ such that:

$$pr\left((\hat{M}_1, \hat{M}_2) \neq (M_1, M_2)\right) \le \epsilon_1 \quad (7)$$

A rate pair (R_1, R_2) is (ϵ_1, ϵ_2)-achievable if, for such encoding and decoding maps $(\mathcal{E}, \mathcal{D})$, the conditions stated in Equation 6 and Equation 7 are satisfied.

As it can be understood from criterion (6), the reliability and security conditions are merged into a single criterion. This idea is used in [29] and [21] for the first time.

Theorem 2 (An inner bound on the one-shot capacity region of PP-QWTC)**.** *For any fixed* $\epsilon_1 \in (0,1)$, $\epsilon_2 \in (0,1)$ *and* δ_1, δ_2 *such that* $\delta_1 \in (0, \epsilon_1)$ *and* $\delta_2 \in (0, \epsilon_2)$*, there exists a one-shot code for the channel* $\mathcal{N}^{X\to YZ}$*, if rate pair* $(R_1, R_2, 3\epsilon_1 + 2(\sqrt{\epsilon_1} + \sqrt{\epsilon_2}), 2(\epsilon_1 + \sqrt{\epsilon_1}) + \sqrt{\epsilon_2})$ *satisfies the following bounds:*

$$R_1 \le I_H^{\epsilon_1-\delta_1}(U_1;Y|U_2)_\rho - \tilde{I}_{max}^{\sqrt{\epsilon_2}-\delta_2}(U_1;Z)_\rho - \log\frac{4\epsilon_1}{\delta_1^2} - 2\log\frac{1}{\delta_2}$$

$$R_2 \le I_H^{\epsilon_1-\delta_1}(U_2;Y|U_1)_\rho - \tilde{I}_{max}^{\sqrt{\epsilon_2}-\delta_2}(U_2;Z|U_1)_\rho - \log\frac{4\epsilon_1}{\delta_1^2} - 2\log\frac{1}{\delta_2}$$

with respect to state $\rho_{U_1U_2YZ} = \sum_{u_2=1}^{|\mathcal{U}_2|}\sum_{u_1=1}^{|\mathcal{U}_1|} p(u_1,u_2)\,|u_1\rangle\langle u_1| \otimes |u_2\rangle\langle u_2| \otimes \rho_{YZ}^{u_1u_2}$.

Proof: In Appendix 8.3.

Remark 6.2. The proof of Theorem 2 has two advantages over the proof of Theorem 1: The first is that the proof of Theorem 2 is based on solving a binary hypothesis testing problem against the proof of Theorem 1, which is based on solving a multiple hypothesis testing problem. The second is that in the privacy proof of Theorem 1, Lemma 1 is used. But, in the proof of Theorem 2, the convex split lemma (Lemma 2) can be used.

Remark 6.3. From comparing the results of Theorem 1 and Theorem 2, it can be understood that the proof of Theorem 2 does not give the sum rate $(R_1 + R_2)$. This is because of using the successive decoding technique. This issue should not cause doubts about whether PP-QWTC is a dual for CQ-MA-WTC. To solve this doubt, we propose the issue of quantum broadcast channels.

6.1 Quantum Broadcast Channels (QBCs)

The quantum broadcast channel accepts one user and two or more receivers. In the basic case, the sender (Alice) wishes to transmit three separate messages: m_1 is the personal message for the first receiver Y_1, m_2 is the personal message for the second receiver Y_2, and m_c is the common message for both of the receivers.

The basic QBC is illustrated in Figure 3. It should be noted that, for ease of analysis, we removed the security constraint from the problem.

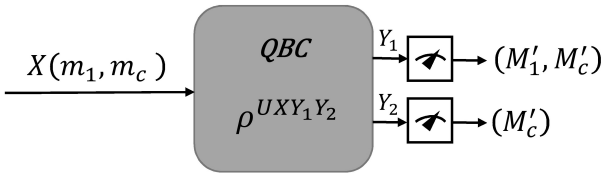

Figure 3. The QBC model

The problem of QBC is widely studied in the i.i.d. case in [2, 3] and in the one-shot case in [30]. In the following, we want to achieve a one-shot inner bound for QBC with classical messages. Suppose that Alice has not a personal message for the second receiver Y_2 ($m_2 = \emptyset \to R_2 = 0$).

The QBC under the one-shot setting is a triple $(\mathcal{X}, \mathcal{N}^{\mathcal{X}\to Y_1Y_2} \equiv \rho_x^{Y_1Y_2}, \mathcal{H}^{Y_1} \otimes \mathcal{H}^{Y_2})$, where X denotes the input alphabet set, and Y_1, Y_2 denote the output systems. $\rho_x^{Y_1Y_2}$ is the system output's quantum state.

Theorem 3. *Let U be an auxiliary random variable, $p = p_{X|U}(x|u)p_U(u)$ be the code probability function. The one-shot achievable rate consists of all rate pairs (R_1, R_c) such that:*

$$R_1 \le I_H^\epsilon(X;Y_1|U)_\rho - 2 + \log\epsilon$$
$$R_c \le I_H^\epsilon(U;Y_2)_\rho - 2 + \log\epsilon$$
$$R_1 + R_c \le I_H^\epsilon(X;Y_1)_\rho - 2 + \log\epsilon$$

is achievable, and all information quantities are taken with respect to the following state:

$$\rho_{UXY_1Y_2} = \sum_{u,x} p_U(u)\, p_{X|U}(x|u)\, |u\rangle\langle u|^U \otimes |x\rangle\langle x|^X \otimes \rho_x^{Y_1Y_2} \tag{8}$$

Proof: In Appendix 8.4.

Now, consider the extended version of the above theorem:

Corollary 6.2 (one-shot inner bound for QBC with three personal messages for the first receiver). Let U be an auxiliary random variable, $p = p_U(u)p_{X_1|U}(x_1|u)p_{X_2|UX_1}(x_2|ux_1)$ be the code probability function. The one-shot achievable rate region consists of all rate tuples (R_1, R_c, R_2) in order to sending (m_1, m_2, m_c) such that:

$$R_1 \le I_H^\epsilon(X_1;Y_1|U)_\rho - 2 + \log\epsilon$$
$$R_2 \le I_H^\epsilon(X_2;Y_1|UX_1)_\rho - 2 + \log\epsilon$$
$$R_c \le I_H^\epsilon(U;Y_2)_\rho - 2 + \log\epsilon$$
$$R_1 + R_2 \le I_H^\epsilon(X_1X_2;Y_1|U)_\rho - 2 + \log\epsilon$$
$$R_1 + R_c \le I_H^\epsilon(X_1;Y_1)_\rho - 2 + \log\epsilon$$
$$R_2 + R_c \le I_H^\epsilon(X_2;Y_1|X_1)_\rho - 2 + \log\epsilon$$

is achievable, and all information quantities are taken with respect to the following state:

$$\rho_{UX_1X_2Y_1Y_2} = \sum_{u,x_1,x_2} p_U(u)p_{X_1|U}(x_1|u)p_{X_2|UX_1}(x_2|ux_1)\, |u\rangle\langle u|^U \otimes |x_1\rangle\langle x_1|^{X_1} \otimes |x_2\rangle\langle x_2|^{X_2} \otimes \rho_{x_1x_2}^{Y_1Y_2}$$

Proof: The proof follows the extended version of Theorem 3's proof.

The channel described in Corollary 6.2 will be converted to the channel described in Theorem 2 (PP-QWTC) without secrecy constraint by choosing $m_c = \emptyset$. Set $R_c = 0$ in Corollary 6.2:

$$R_1 \le I_H^\epsilon(X_1;Y_1)_\rho - 2 + \log\epsilon$$
$$R_2 \le I_H^\epsilon(X_2;Y_1|X_1)_\rho - 2 + \log\epsilon$$
$$R_1 + R_2 \le I_H^\epsilon(X_1X_2;Y_1)_\rho - 2 + \log\epsilon$$
$$R_1 \le I_H^\epsilon(X_1;Y_1)_\rho - 2 + \log\epsilon$$
$$R_2 \le I_H^\epsilon(X_2;Y_1|X_1)_\rho - 2 + \log\epsilon$$

where the above last two rates are redundant. Then, we have the following region:

$$\begin{aligned} R_1 &\le I_H^\epsilon(X_1;Y_1)_\rho - 2 + \log\epsilon \\ R_2 &\le I_H^\epsilon(X_2;Y_1|X_1)_\rho - 2 + \log\epsilon \\ R_1 + R_2 &\le I_H^\epsilon(X_1X_2;Y_1)_\rho - 2 + \log\epsilon \end{aligned} \tag{9}$$

Consider the results of Theorem 2 without the leaked information terms. By choosing $\delta_2 = \epsilon_2$, we have:

$$\begin{aligned} R_1 &\le I_H^\epsilon(X_1;Y_1|X_2)_\rho - 2 + \log\epsilon_1 \\ R_2 &\le I_H^\epsilon(X_2;Y_1|X_1)_\rho - 2 + \log\epsilon_1 \end{aligned} \tag{10}$$

Comparing Equation 9, Equation 10, and Equation 46 the argument stated in Remark 6.3 is proved. Also, the region (9) is a near-optimal achievable rate region compared to Corollary 6.1. As it can be understood from a comparison between the results of Corollary 6.1, Theorem 2, and Corollary 6.2 by considering Equation 46, this idea can be proved that converting the CQ-MA-WTC to PP-QWTC can be a helpful approach to bypass the bottlenecks connected to the multiple hypothesis testing problem (Theorem 1) and the smoothing bottlenecks of quantum information theory (Corollary 6.1 and Theorem 1).

6.2 Asymptotic Analysis

In this subsection, we want to evaluate secrecy rate region presented in Theorem 2 in the asymptotic i.i.d. case (asymptotic limit of many uses of a memoryless channel). It should be noted that, all of the process can be repeated for asymptotic analysis of

Theorem 3 and Corollary 6.1. Consider PP-QWTC $\left(x(u_1,u_2)\to\rho_x^{YZ}\right)$. The capacity region of the channel can be expressed as follows:

$$\mathcal{C}_\infty(\mathcal{N}) := \lim_{\epsilon_1,\epsilon_2\to 0}\lim_{n\to\infty}\frac{1}{n}\mathcal{C}^{\epsilon_1,\epsilon_2}(\mathcal{N}^{\otimes n}) \tag{11}$$

where $\mathcal{C}^{\epsilon_1,\epsilon_2}(\mathcal{N}^{\otimes n}) \equiv \max_{p(u_1,u_2)}\mathcal{R}^{\epsilon_1,\epsilon_2}(\mathcal{N}^{\otimes n})$. Let $\mathcal{R}(\mathcal{N})$ be the set of the maximum rate pairs (R_1', R_2'),

$$\mathcal{R}(\mathcal{N}) = \begin{cases} R_1' \le I(U_1;Y|U_2)_\rho - I(U_1;Z)_\rho \\ R_2' \le I(U_2;Y|U_1)_\rho - I(U_2;Z|U_1)_\rho \end{cases} \tag{12}$$

Then, the capacity region $\mathcal{C}_\infty(\mathcal{N})$ is the union over n uses of the channel $\mathcal{N}$:

$$\mathcal{C}_\infty(\mathcal{N}) := \max_{p(u_1,u_2)}\frac{1}{n}\bigcup_{n=1}^{\infty}\mathcal{R}(\mathcal{N}^{\otimes n}) \tag{13}$$

we aim to prove the expression above. Consider both single rates. Applying Fact 4.2 (and its conditional version), we have,

$$R_1 \ge I_H^{\epsilon_1-\delta_1}(U_1;Y|U_2)_\rho - I_{max}^{\sqrt{\epsilon_2}-\delta_2-\gamma}(U_1;Z)_\rho - \log\frac{4\epsilon_1}{\delta_1^2} - 2\log\frac{1}{\delta_2} - \log\frac{3}{\gamma^2} \tag{14}$$

$$R_2 \ge I_H^{\epsilon_1-\delta_1}(U_2;Y|U_1)_\rho - I_{max}^{\sqrt{\epsilon_2}-\delta_2-\gamma}(U_2;Z|U_1)_\rho - \log\frac{4\epsilon_1}{\delta_1^2} - 2\log\frac{1}{\delta_2} - \log\frac{3}{\gamma^2} \tag{15}$$

To prove the achievability, consider the one-shot lower bounds presented in Theorem 2 and apply quantum AEP [31] for the conditional smooth hypothesis testing and max-mutual information. From Theorem 2, for r uses of the channel $\mathcal{N}$, the following lower bound $\mathcal{C}^{\epsilon_1,\epsilon_2}(\mathcal{N}^{\otimes n})$ can be obtained:

$$\bigcup_{n=1}^{r}\mathcal{R}(\mathcal{N}^{\otimes n}) \subseteq \mathcal{C}^{\epsilon_1,\epsilon_2}(\mathcal{N}^{\otimes r})$$

where $\mathcal{R}(\mathcal{N}^{\otimes n})$ is the set of all rate pairs (R_1', R_2') satisfying:

$$R_1' \le I_H^{\epsilon_1-\delta_1}(U_1^n;Y^{\otimes n}|U_2^n)_\rho - I_{max}^{\sqrt{\epsilon_2}-\delta_2-\gamma}(U_1^n;Z^{\otimes n})_\rho - \log\frac{4\epsilon_1}{\delta_1^2} - 2\log\frac{1}{\delta_2} - \log\frac{3}{\gamma^2} \tag{16}$$

$$R_2' \le I_H^{\epsilon_1-\delta_1}(U_2^n;Y^{\otimes n}|U_1^n)_\rho - I_{max}^{\sqrt{\epsilon_2}-\delta_2-\gamma}(U_2^n;Z^{\otimes n}|U_1^n)_\rho - \log\frac{4\epsilon_1}{\delta_1^2} - 2\log\frac{1}{\delta_2} - \log\frac{3}{\gamma^2} \tag{17}$$

We can assume that the sequences of the random variables are i.i.d. according to their distributions. This is due to the fact that the region above is a lower bound on the capacity region. This enable us to use of quantum AEP, as described below. From Fact 4.3, we have,

$$\lim_{\epsilon_1\to 0}\lim_{r\to\infty}\frac{1}{r}I_H^{\epsilon_1-\delta_1}\left(U_1^r;Y^{\otimes r}|U_2^r\right)_{\rho^{\otimes r}} = I\left(U_1;Y|U_2\right)_\rho \tag{18}$$

$$\lim_{\epsilon_1\to 0}\lim_{r\to\infty}\frac{1}{r}I_H^{\epsilon_1-\delta_1}\left(U_2^r;Y^{\otimes r}|U_1^r\right)_{\rho^{\otimes r}} = I\left(U_2;Y|U_1\right)_\rho \tag{19}$$

Also, using Fact 4.4, we have the following:

$$\lim_{\epsilon_2\to 0}\lim_{r\to\infty}\frac{1}{r}I_{max}^{\sqrt{\epsilon_2}-\delta_2-\gamma}\left(U_1^r;Z^{\otimes r}\right)_{\rho^{\otimes r}} = I\left(U_1;Z\right)_\rho \tag{20}$$

$$\lim_{\epsilon_2\to 0}\lim_{r\to\infty}\frac{1}{r}I_{max}^{\sqrt{\epsilon_2}-\delta_2-\gamma}\left(U_2^r;Z^{\otimes r}|U_1^r\right)_{\rho^{\otimes r}} = I\left(U_2;Z|U_1\right)_\rho \tag{21}$$

Putting Equation 18, Equation 19, Equation 20, and Equation 21 into Equation 16 and Equation 17 gives Equation 12:

$$\mathcal{R}(\mathcal{N}^{\otimes n}) \subseteq \lim_{\epsilon_1,\epsilon_2\to 0}\lim_{r\to\infty}\frac{1}{r}\mathcal{C}^{\epsilon_1,\epsilon_2}(\mathcal{N}^{\otimes r})$$

Given the argument above, using Equation 11 and Equation 13 completes the proof.

7 Comparison

In the following, we have compared the advantages of our method in comparison to the previously introduced methods. As mentioned before, the main novelty of this paper is introducing a new method that tries to investigate C-QMA-WTC using other channels (PP-CQ-WTC and Classical-Quantum Broadcast Wiretap Channel (CQ-B-WTC)). This method led us to achieve sub-optimal (Theorem 2) and near-optimal (Corollary 6.2) achievable rate regions. We have shown that we can bypass some of the quantum information theory bottlenecks using the simulation of a quantum channel by another quantum channel.

It should be mentioned that the previously investigated techniques suffer from quantum information theory bottlenecks. For example, the introduced method in the paper [13] suffers from the multiple quantum hypothesis testing limits, which tend to a lower bound on the secrecy capacity region of entanglement-assisted CQ-MA-WTC under the one-shot setting (in a special case in which output states are commutative). Also, the introduced method in the paper [10] suffers from the smoothing bottleneck of the tripartite convex split lemma.

Using the successive position-based decoder helps us to bypass the intractability of asymmetric multiple quantum hypothesis testing problem. Also, the successive position-based decoder enables us to use the convex split lemma, while the simultaneous position-based decoder does not have the capability to use it.

8 Conclusion

In this paper, we studied the problem of secure communication over a CQ-MA-WTC using three tech-

niques: 1- Sen's joint typicality lemma. 2-simultaneous position-based decoding and 3-successive position-based decoding. The first and the second decoding techniques use a newly introduced smooth technique [16] to analyze the privacy, while the third technique uses convex splitting [19]. We realized that the simultaneous position-based decoder tends to a multiple hypothesis testing problem, which is unsolvable in the general case. We introduced a new channel (PP-QWTC), which can be considered as a dual for CQ-MA-WTC. Also, this channel can be derived from the quantum broadcast channel. The results show that Theorem 2 has a sub-optimal achievable rate region to CQ-MA-WTC. Also, Corollary 6.2 validates our claim by providing a near-optimal achievable rate region.

References

[1] Andreas Winter. The capacity of the quantum multiple-access channel. *IEEE Transactions on Information Theory*, 47(7):3059–3065, 2001.

[2] Jon Yard, Patrick Hayden, and Igor Devetak. Quantum broadcast channels. *IEEE Transactions on Information Theory*, 57(10):7147–7162, 2011.

[3] Ivan Savov. Network information theory for classical-quantum channels. *arXiv preprint arXiv:1208.4188*, 2012.

[4] Abbas El Gamal and Young-Han Kim. Lecture notes on network information theory, 2010.

[5] Ning Cai, Andreas Winter, and Raymond W Yeung. Quantum privacy and quantum wiretap channels. *problems of information transmission*, 40(4):318–336, 2004.

[6] Igor Devetak. The private classical capacity and quantum capacity of a quantum channel. *IEEE Transactions on Information Theory*, 51(1):44–55, 2005.

[7] Omar Fawzi, Patrick Hayden, Ivan Savov, Pranab Sen, and Mark M Wilde. Classical communication over a quantum interference channel. *IEEE Transactions on Information Theory*, 58(6):3670–3691, 2012.

[8] Hadi Aghaee and Bahareh Akhbari. One-shot achievable secrecy rate regions for quantum interference wiretap channel. *The ISC International Journal of Information Security (ISeCure)*, 14(3):71–80, 2022.

[9] Hadi Aghaee and Bahareh Akhbari. Classical-quantum multiple access wiretap channel. In *2019 16th International ISC (Iranian Society of Cryptology) Conference on Information Security and Cryptology (ISCISC)*, pages 99–103. IEEE, 2019.

[10] Hadi Aghaee and Bahareh Akhbari. Private classical information over a quantum multiple access channel: One-shot secrecy rate region. In *2020 10th International Symposium onTelecommunications (IST)*, pages 222–226. IEEE, 2020.

[11] Hadi Aghaee and Bahareh Akhbari. Classical-quantum multiple access channel with secrecy constraint: One-shot rate region. *International Journal of Information and Communication Technology Research*, 12(2):1–10, 2020.

[12] Hadi Aghaee and Bahareh Akhbari. Classical-quantum multiple access wiretap channel with common message: one-shot rate region. In *2020 11th International Conference on Information and Knowledge Technology (IKT)*, pages 55–61. IEEE, 2020.

[13] Hadi Aghaee and Bahareh Akhbari. Entanglement-assisted classical-quantum multiple access wiretap channel: One-shot achievable rate region. In *2022 30th International Conference on Electrical Engineering (ICEE)*, pages 693–699. IEEE, 2022.

[14] Pranab Sen. Unions, intersections and a one-shot quantum joint typicality lemma. *Sādhanā*, 46(1):1–44, 2021.

[15] Aaron D Wyner. The wire-tap channel. *Bell system technical journal*, 54(8):1355–1387, 1975.

[16] Sayantan Chakraborty, Aditya Nema, and Pranab Sen. One-shot inner bounds for sending private classical information over a quantum mac. In *2021 IEEE Information Theory Workshop (ITW)*, pages 1–6. IEEE, 2021.

[17] Haoyu Qi, Qingle Wang, and Mark M Wilde. Applications of position-based coding to classical communication over quantum channels. *Journal of Physics A: Mathematical and Theoretical*, 51(44):444002, 2018.

[18] Anurag Anshu. *One-shot protocols for communication over quantum networks: Achievability and limitations*. PhD thesis, National University of Singapore (Singapore), 2018.

[19] Anurag Anshu, Rahul Jain, and Naqueeb Ahmad Warsi. A generalized quantum slepian–wolf. *IEEE Transactions on Information Theory*, 64(3):1436–1453, 2017.

[20] Rémi A Chou. Private classical communication over quantum multiple-access channels. *IEEE Transactions on Information Theory*, 68(3):1782–1794, 2021.

[21] Mark M Wilde. Position-based coding and convex splitting for private communication over quantum channels. *Quantum Information Processing*, 16(10):1–35, 2017.

[22] Ligong Wang and Renato Renner. One-shot classical-quantum capacity and hypothesis testing. *Physical Review Letters*, 108(20):200501, 2012.

[23] Hisaharu Umegaki. Conditional expectation in

an operator algebra, iv (entropy and information). In *Kodai Mathematical Seminar Reports*, volume 14, pages 59–85. Department of Mathematics, Tokyo Institute of Technology, 1962.

[24] Mario Berta, Matthias Christandl, and Renato Renner. The quantum reverse shannon theorem based on one-shot information theory. *Communications in Mathematical Physics*, 306(3):579–615, 2011.

[25] Farzin Salek, Anurag Anshu, Min-Hsiu Hsieh, Rahul Jain, and Javier Rodríguez Fonollosa. One-shot capacity bounds on the simultaneous transmission of classical and quantum information. *IEEE Transactions on Information Theory*, 66(4):2141–2164, 2019.

[26] Nikola Ciganović, Normand J Beaudry, and Renato Renner. Smooth max-information as one-shot generalization for mutual information. *IEEE Transactions on Information Theory*, 60(3):1573–1581, 2013.

[27] Masahito Hayashi and Hiroshi Nagaoka. General formulas for capacity of classical-quantum channels. *IEEE Transactions on Information Theory*, 49(7):1753–1768, 2003.

[28] Farzin Salek, Anurag Anshu, Min-Hsiu Hsieh, Rahul Jain, and Javier R Fonollosa. One-shot capacity bounds on the simultaneous transmission of public and private information over quantum channels. In *2018 IEEE International Symposium on Information Theory (ISIT)*, pages 296–300. IEEE, 2018.

[29] Mark M Wilde, Marco Tomamichel, and Mario Berta. Converse bounds for private communication over quantum channels. *IEEE Transactions on Information Theory*, 63(3):1792–1817, 2017.

[30] Pranab Sen. Inner bounds via simultaneous decoding in quantum network information theory. *Sādhanā*, 46(1):1–20, 2021.

[31] Mark M Wilde. *Quantum information theory*. Cambridge University Press, 2013.

[32] Ke Li. Discriminating quantum states: The multiple chernoff distance. *The Annals of Statistics*, 44(4):1661–1679, 2016.

[33] Mark M Wilde. Sequential decoding of a general classical-quantum channel. *Proceedings of the Royal Society A: Mathematical, Physical and Engineering Sciences*, 469(2157):20130259, 2013.

Appendix

Appendix 8.1 (Proof of Corollary 6.1). *Proof.* As mentioned, the proof has two steps: Reliable decoding and secure decoding. To these ends, consider two junk variables k_i; $i \in \{1,2\}$ for each user m_i; $i \in \{1,2\}$. These junk variables are used to make two doubly indexed codebooks $\{x_1(m_1,k_1)\}_{\substack{m_1\in\mathcal{M}_1\\k_1\in\mathcal{K}_1}}$ and $\{x_2(m_2,k_2)\}_{\substack{m_2\in\mathcal{M}_2\\k_2\in\mathcal{K}_2}}$. Bob should be able to detect the pair messages (m_1,m_2), and the junk variables k_1 and k_2 Using Definition 4.10 (Sen's inner bound for QMAC), we have the following relation:

$$R_{priv-CQ-MA-WTC} = R_{Sen} - R_{leaked}$$

with decoding error at most $49\sqrt{\epsilon}$, and privacy leakage at most $20\delta'^{\frac{1}{8}}$ (Lemma 1). Also, R_{Sen} refers to Sen's inner bound for QMAC (Definition 4.10), and R_{leaked} refers to the leaked information from senders to Eve.

From Lemma 1, we have the following:

$$R_{1-leaked} \leq I_{max}^{\delta'-\epsilon'}(X_1:Z)_\rho + \log\frac{3}{\epsilon'^3} - \frac{1}{4}\log\delta'$$

$$R_{2-leaked} \leq I_{max}^{\delta'-\epsilon'}(X_2:ZX_1)_\rho + \log\frac{3}{\epsilon'^3} - \frac{1}{4}\log\delta' + \mathcal{O}(1)$$

This completes the proof. □

Appendix 8.2 (Proof of Theorem 1). *Proof.* Both of the messages are uniformly distributed on their sets. The receiver has to be able to decode both messages with negligible error probability. Before communication begins, Alice (A) and Bob (B) share randomness with Charlie (C) and the wiretapper (Z). Let $\rho_{X_1X_1'X_1''}$ and $\sigma_{X_2X_2'X_2''}$ be shared-randomness between (A,C,Z) and shared-randomness between (B,C,Z), respectively:

$$\rho_{X_1X_1'X_1''} \equiv \sum_{x_1} p_{X_1}(x_1)\,|x_1\rangle\langle x_1|_{X_1} \otimes |x_1\rangle\langle x_1|_{X_1'} \otimes |x_1\rangle\langle x_1|_{X_1''} \quad (22)$$

$$\sigma_{X_2X_2'X_2''} \equiv \sum_{x_2} p_{X_2}(x_2)\,|x_2\rangle\langle x_2|_{X_2} \otimes |x_2\rangle\langle x_2|_{X_2'} \otimes |x_2\rangle\langle x_2|_{X_2''} \quad (23)$$

Alice has X_1' system, Bob has X_2' system, and Charlie has (X_1,X_2) system, and wiretapper has (X_1'',X_2'') system. Let $\rho_{X_1X_1''YZ}$ and $\sigma_{X_2X_2''YZ}$ denote the state resulting from sending X_1' and X_2' over the channel, respectively:

$$\rho_{X_1X_1''YZ} \equiv \sum_{x_1} p_{X_1}(x_1)\,|x_1\rangle\langle x_1|_{X_1} \otimes \rho_{x_1x_2}^{YZ} \otimes |x_1\rangle\langle x_1|_{X_1''} \quad (24)$$

$$\sigma_{X_2X_2''YZ} \equiv \sum_{x_2} p_{X_2}(x_2)\,|x_2\rangle\langle x_2|_{X_2} \otimes \rho_{x_1x_2}^{YZ} \otimes |x_2\rangle\langle x_2|_{X_2''} \quad (25)$$

Then, the overall controlling state of the channel is as follows:

$$\rho_{X_1X_2YZ} \equiv \mathcal{N}_{X_1'X_2'\to YZ}(\rho_{X_1X_1''YZ}\otimes\sigma_{X_2X_2''YZ}) = \sum_{x_1x_2} p_{X_1}(x_1)p_{X_2}(x_2)\,|x_1\rangle\langle x_1|_{X_1} \otimes |x_2\rangle\langle x_2|_{X_2}\otimes\rho^{YZ}_{x_1x_2} \quad (26)$$

Sketch of the coding scheme: For each of the messages $m_i; i\in\{1,2\}$, there exist local keys $k_i\in[1:|K_i|], i\in\{1,2\}$ as uniform randomness for randomizing Eve's knowledge about the sent messages. These local keys are not accessible to Charlie or Eve. Before the communication begins, assume that Alice, Charlie, and Eve share $|\mathcal{M}_1||\mathcal{K}_1|$ copies of the state (22) and Bob, Charlie, and Eve share $|\mathcal{M}_2||\mathcal{K}_2|$ copies of the state (23):

$$\rho_{X_1^{|\mathcal{M}_1||\mathcal{K}_1|}X_1'^{|\mathcal{M}_1||\mathcal{K}_1|}X_1''^{|\mathcal{M}_1||\mathcal{K}_1|}} = \rho_{X_1X_1'X_1''}^{\otimes|\mathcal{M}_1||\mathcal{K}_1|}$$

$$\sigma_{X_2^{|\mathcal{M}_2||\mathcal{K}_2|}X_2'^{|\mathcal{M}_2||\mathcal{K}_2|}X_2''^{|\mathcal{M}_2||\mathcal{K}_2|}} = \sigma_{X_2X_2'X_2''}^{\otimes|\mathcal{M}_2||\mathcal{K}_2|}$$

To send the pair messages m_1 and m_2, Alice and Bob pick $k_1\in[1:|\mathcal{K}_1|]$ and $k_2\in[1:|\mathcal{K}_2|]$, respectively, and uniformly at random. They send (m_1,k_1)-th system $X_1^{'}$ and (m_2,k_2)-th system $X_2^{'}$ through the channel $\mathcal{N}_{X_1'X_2'\to YZ}$.

There exists a simultaneous decoder for communication over a CQ-MA-WTC with the upper bound on the average error probability as follows:

$$\frac{1}{|\mathcal{M}_1||\mathcal{M}_2|}\sum_{m_2=1}^{|\mathcal{M}_2|}\sum_{m_1=1}^{|\mathcal{M}_1|} \frac{1}{2}\left\|\mathcal{D}_{Y\to\hat{M}_1\hat{M}_2}\left(\rho^{(m_1,k_1),(m_2,k_2)}_{(X_1X_1'')^{\otimes|\mathcal{M}_1||\mathcal{K}_1|}(X_2X_2'')^{\otimes|\mathcal{M}_2||\mathcal{K}_2|}YZ} - (|m_1\rangle\langle m_1|_{\hat{M}_1}\otimes|m_2\rangle\langle m_2|_{\hat{M}_2}) \otimes\hat{\rho}_{X_1''^{\otimes|\mathcal{M}_1||\mathcal{K}_1|}X_2''^{\otimes|\mathcal{M}_2||\mathcal{K}_2|}Z}\right)\right\|_1 \le \epsilon+2\delta+20\delta'^{\frac{1}{8}} \quad (27)$$

where,
$\hat{\rho}_{X_1''^{\otimes|\mathcal{M}_1||\mathcal{K}_1|}X_2''^{\otimes|\mathcal{M}_2||\mathcal{K}_2|}Z} := \rho^{(m_1,k_1),(m_2,k_2)}_{X_1''^{\otimes|\mathcal{M}_1||\mathcal{K}_1|}X_2''^{\otimes|\mathcal{M}_2||\mathcal{K}_2|}}\otimes\tilde{\rho}_Z$.

As it can be understood from Equation 27, the security criterion is merged into the reliability criterion [17]. The simultaneous position-based decoder can be constructed as follows:

$$\mathcal{D}_{Y\to\hat{M}_1\hat{M}_2}\left(\rho^{(m_1,k_1),(m_2,k_2)}_{X_1^{\otimes|\mathcal{M}_1||\mathcal{K}_1|}X_2^{\otimes|\mathcal{M}_2||\mathcal{K}_2|}YZ}\right) := \sum_{m_2=1}^{|\mathcal{M}_2|}\sum_{m_1=1}^{|\mathcal{M}_1|} p_{\hat{M}_1}(m_1)p_{\hat{M}_2}(m_2)\,|m_1\rangle\langle m_1|_{\hat{M}_1}\otimes|m_2\rangle\langle m_2|_{\hat{M}_2} = \sum_{m_2=1}^{|\mathcal{M}_2|}\sum_{m_1=1}^{|\mathcal{M}_1|} Tr\left\{\Lambda^{m_1m_2}_{X_1^{\otimes|\mathcal{M}_1||\mathcal{K}_1|}X_2^{\otimes|\mathcal{M}_2||\mathcal{K}_2|}Y}\,|m_1\rangle\langle m_1|_{\hat{M}_1}\otimes|m_2\rangle\langle m_2|_{\hat{M}_2}\right\} \quad (28)$$

where,

$$\Lambda^{m_1m_2}_{X_1^{\otimes|\mathcal{M}_1||\mathcal{K}_1|}X_2^{\otimes|\mathcal{M}_2||\mathcal{K}_2|}Y} = \sum_{k_2=1}^{|\mathcal{K}_2|}\sum_{k_1=1}^{|\mathcal{K}_1|}\Lambda^{(m_1k_1),(m_2k_2)}_{X_1^{\otimes|\mathcal{M}_1||\mathcal{K}_1|}X_2^{\otimes|\mathcal{M}_2||\mathcal{K}_2|}Y}$$

Now, we consider the error term. Charlie constructs her position-based decoder to decode m_1,m_2,k_1, and k_2. Let $\Lambda^{(m_1,k_1),(m_2,k_2)}_{X_1^{\otimes|\mathcal{M}_1||\mathcal{K}_1|}X_2^{\otimes|\mathcal{M}_2||\mathcal{K}_2|}Y}$ denotes the POVM:

$$Tr\left\{\left(I_{X_1^{|\mathcal{M}_1||\mathcal{K}_1|}X_2^{|\mathcal{M}_2||\mathcal{K}_2|}Y} - \Lambda^{(m_1,k_1),(m_2,k_2)}_{X_1^{\otimes|\mathcal{M}_1||\mathcal{K}_1|}X_2^{\otimes|\mathcal{M}_2||\mathcal{K}_2|}Y}\right)\rho^{m_1,m_2,k_1,k_2}_{X_1^{\otimes|\mathcal{M}_1||\mathcal{K}_1|}X_2^{\otimes|\mathcal{M}_2||\mathcal{K}_2|}Y}\right\} \le \epsilon$$

where $\Lambda^{(m_1,k_1),(m_2,k_2)}_{X_1^{\otimes|\mathcal{M}_1||\mathcal{K}_1|}X_2^{\otimes|\mathcal{M}_2||\mathcal{K}_2|}Y}$ can be expressed as follows:

$$\Lambda^{(m_1,k_1),(m_2,k_2)}_{X_1^{\otimes|\mathcal{M}_1||\mathcal{K}_1|}X_2^{\otimes|\mathcal{M}_2||\mathcal{K}_2|}Y} := \left(\sum_{m_2'}\sum_{m_1'}\sum_{k_2'}\sum_{k_1'}\Gamma^{m_1',k_1',m_2',k_2'}_{X_1^{|\mathcal{M}_1||\mathcal{K}_1|}X_2^{|\mathcal{M}_2||\mathcal{K}_2|}Y}\right)^{-\frac{1}{2}} \Gamma^{m_1,k_1,m_2,k_2}_{X_1^{|\mathcal{M}_1||\mathcal{K}_1|}X_2^{|\mathcal{M}_2||\mathcal{K}_2|}Y} \left(\sum_{m_2'}\sum_{m_1'}\sum_{k_2'}\sum_{k_1'}\Gamma^{m_1',k_1',m_2',k_2'}_{X_1^{|\mathcal{M}_1||\mathcal{K}_1|}X_2^{|\mathcal{M}_2||\mathcal{K}_2|}Y}\right)^{-\frac{1}{2}} \quad (29)$$

and for $m_i\in[1:|\mathcal{M}_i|]$ and $k_i\in[1:|\mathcal{K}_i|]; i\in\{1,2\}$, $\Gamma^{m_1,k_1,m_2,k_2}_{X_1^{|\mathcal{M}_1||\mathcal{K}_1|}X_2^{|\mathcal{M}_2||\mathcal{K}_2|}Y}$ is as follows:

$$\Gamma^{m_1,k_1,m_2,k_2}_{X_1^{|\mathcal{M}_1||\mathcal{K}_1|}X_2^{|\mathcal{M}_2||\mathcal{K}_2|}Y} := I^{(1,1),(1,1)}_{X_1X_2}\otimes\ldots\otimes I^{(1,1),(1,k_2)}_{X_1X_2}\otimes\ldots\otimes I^{(1,1),(m_2,k_2-1)}_{X_1X_2}\otimes\ldots\otimes I^{(1,k_1),(m_2,k_2)}_{X_1X_2}\otimes\ldots\otimes I^{(m_1,k_1-1),(m_2,k_2)}_{X_1X_2}\otimes T^{(m_1,k_1),(m_2,k_2)}_{X_1X_2Y}\otimes I^{(m_1,k_1),(m_2,k_2+1)}_{X_1X_2}\otimes\ldots\otimes I^{(|\mathcal{M}_1|,|\mathcal{K}_1|),(|\mathcal{M}_2|,|\mathcal{K}_2|)}_{X_1X_2} \quad (30)$$

in which $T^{(m_1,k_1,m_2,k_2)}_{X_1X_2Y}$ is a test operator used to discriminate between hypotheses $\rho_{X_1X_2Y}$, $\rho_{X_1X_2}\otimes\rho_Y$, $\rho_{X_1}\otimes\rho_{X_2Y}$, $\rho_{X_1}\otimes\rho_{X_2}\otimes\rho_Y$ with an error of

ϵ. Note that this hypothesis testing problem is equal to discriminating between hypotheses $\mathcal{N}_{X_1'X_2'\to YZ}\Big(\rho_{X_1X_2'}\otimes\sigma_{X_1X_2'}\Big)$, $\mathcal{N}_{X_1'X_2'\to YZ}\Big(\rho_{X_1X_2'}\otimes\sigma_{X_1}\otimes\sigma_{X_2'}\Big)$, $\mathcal{N}_{X_1'X_2'\to YZ}\Big(\rho_{X_1}\otimes\rho_{X_2'}\otimes\sigma_{X_1X_2'}\Big)$, $\mathcal{N}_{X_1'X_2'\to YZ}\Big(\rho_{X_1}\otimes\rho_{X_2'}\otimes\sigma_{X_1}\otimes\sigma_{X_2'}\Big)$. Therefore, if Charlie checks for message pair (m_1,m_2) when message pair (m_1,m_2) is actually transmitted, then the probability of incorrectly decoding is as follows:

$$\begin{aligned}&Tr\Big\{\Big(I-\Gamma^{m_1k_1m_2k_2}_{X_1^{|\mathcal{M}_1||\mathcal{K}_1|}X_2^{|\mathcal{M}_2||\mathcal{K}_2|}Y}\Big)\\&\qquad\qquad\rho^{m_1,m_2,k_1,k_2}_{X_1^{\otimes|\mathcal{M}_1||\mathcal{K}_1|}X_2^{\otimes|\mathcal{M}_2||\mathcal{K}_2|}Y}\Big\}\\&=Tr\Big\{\Big(I-T_{X_1X_2Y}\Big)\mathcal{N}_{X_1'X_2'\to YZ}\Big(\rho_{X_1X_2'}\otimes\sigma_{X_1X_2'}\Big)\Big\}\end{aligned}\tag{31}$$

Similarly, other kinds of error probabilities can be considered as follows:

- If Charlie checks for message pair (m_1,m_2) when message pair (m_1',m_2) is indeed transmitted, then the probability of incorrectly decoding is:

$$\begin{aligned}&Tr\Big\{\Big(\Gamma^{m_1',k_1,m_2,k_2}_{X_1^{|\mathcal{M}_1||\mathcal{K}_1|}X_2^{|\mathcal{M}_2||\mathcal{K}_2|}Y}\\&\qquad\rho^{m_1m_2k_1k_2}_{X_1^{\otimes|\mathcal{M}_1||\mathcal{K}_1|}X_2^{\otimes|\mathcal{M}_2||\mathcal{K}_2|}Y}\Big)\Big\}\\&=Tr\Big\{\Big(I-T_{X_1X_2Y}\Big)\\&\qquad\mathcal{N}_{X_1'X_2'\to YZ}\Big(\rho_{X_1}\otimes\rho_{X_2'}\otimes\sigma_{X_1X_2'}\Big)\Big\}\end{aligned}\tag{32}$$

- If Charlie checks for message pair (m_1,m_2) when message pair (m_1,m_2') is indeed transmitted, then the probability of incorrectly decoding is:

$$\begin{aligned}&Tr\Big\{\Big(\Gamma^{m_1,k_1,m_2',k_2}_{X_1^{|\mathcal{M}_1||\mathcal{K}_1|}X_2^{|\mathcal{M}_2||\mathcal{K}_2|}Y}\\&\qquad\rho^{m_1m_2k_1k_2}_{X_1^{\otimes|\mathcal{M}_1||\mathcal{K}_1|}X_2^{\otimes|\mathcal{M}_2||\mathcal{K}_2|}Y}\Big)\Big\}\\&=Tr\Big\{\Big(I-T_{X_1X_2Y}\Big)\\&\qquad\mathcal{N}_{X_1'X_2'\to YZ}\Big(\rho_{X_1X_2'}\otimes\sigma_{X_1}\otimes\sigma_{X_2'}\Big)\Big\}\end{aligned}\tag{33}$$

- If Charlie checks for message pair (m_1,m_2) when message pair (m_1',m_2') is indeed transmitted, then the probability of incorrectly decoding is:

$$\begin{aligned}&Tr\Big\{\Big(\Gamma^{m_1',k_1,m_2',k_2}_{X_1^{|\mathcal{M}_1||\mathcal{K}_1|}X_2^{|\mathcal{M}_2||\mathcal{K}_2|}Y}\\&\qquad\rho^{m_1m_2k_1k_2}_{X_1^{\otimes|\mathcal{M}_1||\mathcal{K}_1|}X_2^{\otimes|\mathcal{M}_2||\mathcal{K}_2|}Y}\Big)\Big\}\\&=Tr\Big\{\Big(I-T_{X_1X_2Y}\Big)\\&\qquad\mathcal{N}_{X_1'X_2'\to YZ}\Big(\rho_{X_1}\otimes\rho_{X_2'}\otimes\sigma_{X_1}\otimes\sigma_{X_2'}\Big)\Big\}\end{aligned}\tag{34}$$

Due to the code construction, the error probability under the position-based coding scheme is the same for each message pair (m_1,m_2):

$$\begin{aligned}&Pr\Big((\hat{M}_1,\hat{M}_2)\neq(M_1,M_2)\Big)=\\&\qquad Tr\Big\{\Big(I-\Lambda^{m_1',k_1,m_2',k_2}_{X_1^{\otimes|\mathcal{M}_1||\mathcal{K}_1|}X_2^{\otimes|\mathcal{M}_2||\mathcal{K}_2|}Y}\Big)\\&\qquad\rho^{m_1m_2k_1k_2}_{X_1^{\otimes|\mathcal{M}_1||\mathcal{K}_1|}X_2^{\otimes|\mathcal{M}_2||\mathcal{K}_2|}Y}\Big\}\end{aligned}$$

Applying Lemma 3 with $S=\Gamma^{m_1,k_1,m_2,k_2}_{X_1^{|\mathcal{M}_1||\mathcal{K}_1|}X_2^{|\mathcal{M}_2||\mathcal{K}_2|}Y}$ and $T=\sum_{m_2'\neq m_2}\sum_{m_1'\neq m_1}\sum_{k_2'\neq k_2}\sum_{k_1'\neq k_1}\Gamma^{m_1',k_1',m_2',k_2'}_{X_1^{|\mathcal{M}_1||\mathcal{K}_1|}X_2^{|\mathcal{M}_2||\mathcal{K}_2|}Y}$, and also using Equation 32-Equation 34, we have the following chain of equalities and inequalities:

$$\begin{aligned}&Pr\Big((\hat{M}_1,\hat{M}_2)\neq(M_1,M_2)\Big)\\&\leq(1+c)\,Tr\Big\{\Big(I-\Gamma^{m_1,k_1,m_2,k_2}_{X_1^{|\mathcal{M}_1||\mathcal{K}_1|}X_2^{|\mathcal{M}_2||\mathcal{K}_2|}Y}\Big)\\&\qquad\rho^{m_1m_2k_1k_2}_{X_1^{\otimes|\mathcal{M}_1||\mathcal{K}_1|}X_2^{\otimes|\mathcal{M}_2||\mathcal{K}_2|}Y}\Big\}\\&+(2+c+c^{-1})\sum_{m_2'\neq m_2}\sum_{m_1'\neq m_1}\sum_{k_2'\neq k_2}\sum_{k_1'\neq k_1}\\&\qquad Tr\Big\{\Gamma^{m_1',k_1',m_2',k_2'}_{X_1^{|\mathcal{M}_1||\mathcal{K}_1|}X_2^{|\mathcal{M}_2||\mathcal{K}_2|}Y}\\&\qquad\rho^{m_1m_2k_1k_2}_{X_1^{\otimes|\mathcal{M}_1||\mathcal{K}_1|}X_2^{\otimes|\mathcal{M}_2||\mathcal{K}_2|}Y}\Big\}\\&=(1+c)\,Tr\Big\{\Big(I-\Gamma^{m_1,k_1,m_2,k_2}_{X_1^{|\mathcal{M}_1||\mathcal{K}_1|}X_2^{|\mathcal{M}_2||\mathcal{K}_2|}Y}\Big)\\&\qquad\rho^{m_1m_2k_1k_2}_{X_1^{\otimes|\mathcal{M}_1||\mathcal{K}_1|}X_2^{\otimes|\mathcal{M}_2||\mathcal{K}_2|}Y}\Big\}\\&+(2+c+c^{-1})\sum_{m_1'\neq m_1}\sum_{k_1'\neq k_1}\\&\qquad Tr\Big\{\Gamma^{m_1',k_1',m_2,k_2}_{X_1^{|\mathcal{M}_1||\mathcal{K}_1|}X_2^{|\mathcal{M}_2||\mathcal{K}_2|}Y}\\&\qquad\rho^{m_1m_2k_1k_2}_{X_1^{\otimes|\mathcal{M}_1||\mathcal{K}_1|}X_2^{\otimes|\mathcal{M}_2||\mathcal{K}_2|}Y}\Big\}\\&+(2+c+c^{-1})\sum_{m_2'\neq m_2}\sum_{k_2'\neq k_2}\\&\qquad Tr\Big\{\Gamma^{m_1,k_1,m_2',k_2'}_{X_1^{|\mathcal{M}_1||\mathcal{K}_1|}X_2^{|\mathcal{M}_2||\mathcal{K}_2|}Y}\\&\qquad\rho^{m_1m_2k_1k_2}_{X_1^{\otimes|\mathcal{M}_1||\mathcal{K}_1|}X_2^{\otimes|\mathcal{M}_2||\mathcal{K}_2|}Y}\Big\}\\&+(2+c+c^{-1})\sum_{m_2'\neq m_2}\sum_{m_1'\neq m_1}\sum_{k_2'\neq k_2}\sum_{k_1'\neq k_1}\\&\qquad Tr\Big\{\Gamma^{m_1',k_1',m_2',k_2'}_{X_1^{|\mathcal{M}_1||\mathcal{K}_1|}X_2^{|\mathcal{M}_2||\mathcal{K}_2|}Y}\\&\qquad\rho^{m_1m_2k_1k_2}_{X_1^{\otimes|\mathcal{M}_1||\mathcal{K}_1|}X_2^{\otimes|\mathcal{M}_2||\mathcal{K}_2|}Y}\Big\}\end{aligned}$$

$$
\begin{aligned}
&= (1+c)\,Tr\Big\{\Big(I - T_{X_1X_2Y}\Big) \\
&\qquad \mathcal{N}_{X_1'X_2'\to YZ}\Big(\rho_{X_1X_2'}\otimes\sigma_{X_1X_2'}\Big)\Big\} \\
&+ (2+c+c^{-1})(|\mathcal{M}_1||\mathcal{K}_1|-1)\,Tr\Big\{\Big(I - T_{X_1X_2Y}\Big) \\
&\qquad \mathcal{N}_{X_1'X_2'\to YZ}\Big(\rho_{X_1}\otimes\rho_{X_2'}\otimes\sigma_{X_1X_2'}\Big)\Big\} \\
&+ (2+c+c^{-1})(|\mathcal{M}_2||\mathcal{K}_2|-1)\,Tr\Big\{\Big(I - T_{X_1X_2Y}\Big) \\
&\qquad \mathcal{N}_{X_1'X_2'\to YZ}\Big(\rho_{X_1X_2'}\otimes\sigma_{X_1}\otimes\sigma_{X_2'}\Big)\Big\} \\
&+ (2+c+c^{-1})(|\mathcal{M}_1||\mathcal{K}_1|-1)(|\mathcal{M}_2||\mathcal{K}_2|-1) \\
&\qquad Tr\Big\{\Big(I - T_{X_1X_2Y}\Big) \\
&\qquad\quad \mathcal{N}_{X_1'X_2'\to YZ}\Big(\rho_{X_1}\otimes\rho_{X_2'}\otimes\sigma_{X_1}\otimes\sigma_{X_2'}\Big)\Big\}
\end{aligned} \tag{35}
$$

Multiple quantum hypothesis testing: As mentioned several times, there is no a general simultaneous decoder for QMACs (more than two users) in the i.i.d. case. There is a helpful discussion about the multiple quantum hypothesis testing problem in [17]. In summary, the multiple quantum hypothesis testing problem is remained an open problem yet. There are two kinds of hypothesis testing: Symmetric and asymmetric. *Chernoff distance* from symmetric hypothesis testing gives a lower bound on the randomness-assisted error exponent [32]; on the opposite point, the asymmetric hypothesis testing tends to a lower bound on the one-shot randomness-assisted capacity (for QMAC with or without secrecy constraint) and in turn on the second-order coding rate for randomness-assisted communication.

In other words, from [7], we know that there exists a general simultaneous decoder if the output states be commutative, and from [17], we know that the multiple hypothesis testing problem can be solvable if the alternative composite hypothesis forms a commutative set of operators. This means that, for a test operator T, a finite set of positive semi-definite operators $\theta \equiv \{\theta_i : 1 \le i \le r\}$, for which $supp(\rho) \subseteq supp(\theta_i)$ and $\min_i D(\rho\|\theta_i) > 0$, there are two hypotheses, and we have:

$$Tr\{(1-T)\rho\} \le \epsilon \tag{36}$$

$$-\log_2 Tr\{T\theta_i\} \ge \Big[\min_i D(\rho\|\theta_i)\Big] - \delta \tag{37}$$

where δ is a positive integer. The last inequality holds when the set θ forms a commutative set of operators. More information can be found in [17]. With these explanations, we use asymmetric hypothesis testing for our problem. Note that we want to decode two messages simultaneously. Consider the upper bound on error probability in Equation 35. Then, we rewrite that as follows:

$$
\begin{aligned}
&Pr\Big((\hat{M}_1,\hat{M}_2)\neq(M_1,M_2)\Big) \\
&\qquad \le (1+c)\,Tr\{(1-T)\mu\} \\
&\qquad + (2+c+c^{-1})\,Tr\{(\theta_1,\theta_2,\theta_3)\}
\end{aligned}
$$

where,

$$
\begin{aligned}
\mu &= \mathcal{N}_{X_1'X_2'\to YZ}\Big(\rho_{X_1X_2'}\otimes\sigma_{X_1X_2'}\Big) \\
\theta_1 &= \mathcal{N}_{X_1'X_2'\to YZ}\Big(\rho_{X_1}\otimes\rho_{X_2'}\otimes\sigma_{X_1X_2'}\Big) \\
\theta_2 &= \mathcal{N}_{X_1'X_2'\to YZ}\Big(\rho_{X_1X_2'}\otimes\sigma_{X_1}\otimes\sigma_{X_2'}\Big) \\
\theta_3 &= \mathcal{N}_{X_1'X_2'\to YZ}\Big(\rho_{X_1}\otimes\rho_{X_2'}\otimes\sigma_{X_1}\otimes\sigma_{X_2'}\Big)
\end{aligned}
$$

This is called asymmetric hypothesis testing, which tries to minimize all other probabilities subject to a constraint on the error probability $Tr\{(1-T)\rho\} \le \epsilon$. Note that we consider all three hypotheses $(\theta_1+\theta_2+\theta_3)$ as a unique composite alternative hypothesis.

We can say for such a sequence of test operators, as stated in Equation 36 and Equation 37, the above multiple hypothesis testing problem can be solved as:

$$
\begin{aligned}
&Pr\Big((\hat{M}_1,\hat{M}_2)\neq(M_1,M_2)\Big) \\
&\quad \le (1+c)\,Tr\{(I-T)\mu\} \\
&\quad + (2+c+c^{-1})Tr\{T(\theta_1+\theta_2+\theta_3)\} \\
&\quad = (1+c)\epsilon \\
&\quad + (2+c+c^{-1})\Big\{|\mathcal{K}_1|2^{R_1-D_H^\epsilon(\mu\|\theta_1)} \\
&\quad + |\mathcal{K}_2|2^{R_2-D_H^\epsilon(\mu\|\theta_2)} \\
&\quad + |\mathcal{K}_1||\mathcal{K}_2|2^{R_1+R_2-D_H^\epsilon(\mu\|\theta_3)}\Big\} \\
&\quad = (1+c)\epsilon \\
&\quad + (2+c+c^{-1})\Big\{|\mathcal{K}_1|2^{R_1-I_H^\epsilon(X_1:X_2Y)} \\
&\quad + |\mathcal{K}_2|2^{R_2-I_H^\epsilon(X_2:X_1Y)} \\
&\quad + |\mathcal{K}_1||\mathcal{K}_2|2^{R_1+R_2-I_H^\epsilon(X_1X_2:Y)}\Big\}
\end{aligned}
$$

Let $|\mathcal{K}_1| = 2^{\hat{R}_1}$ and $|\mathcal{K}_2| = 2^{\hat{R}_2}$. Then, by setting the above term equal to ϵ, with a straightforward simplification, we have:

$$R_1+\hat{R}_1 = I_H^\epsilon(X_1:X_2Y) + \log_2\left(\frac{\epsilon-(1+c)\epsilon}{2+c+c^{-1}}\right)$$

$$R_2+\hat{R}_2 = I_H^\epsilon(X_2:X_1Y) + \log_2\left(\frac{\epsilon-(1+c)\epsilon}{2+c+c^{-1}}\right)$$

$$R_1+\hat{R}_1+R_2+\hat{R}_2 = I_H^\epsilon(X_1X_2:Y)+\log_2\left(\frac{\epsilon-(1+c)\epsilon}{2+c+c^{-1}}\right)$$

The global maximum of the above expression with respect to c occurs at $c = \frac{\delta}{\epsilon}$:

$$R_1+\hat{R}_1 = I_H^\epsilon(X_1:X_2Y) + \log_2\left(\frac{4\epsilon}{\delta^2}\right) \tag{38}$$

$$R_2+\hat{R}_2 = I_H^\epsilon(X_2:X_1Y) + \log_2\left(\frac{4\epsilon}{\delta^2}\right) \tag{39}$$

$$R_1+\hat{R}_1+R_2+\hat{R}_2 = I_H^{\epsilon}(X_1X_2:Y)+\log_2\left(\frac{4\epsilon}{\delta^2}\right) \quad (40)$$

and for such a c, we have:

$$Pr\Big((\hat{M}_1,\hat{M}_2)\neq(M_1,M_2)\Big)\leq \epsilon+2\delta \quad (41)$$

Now, we turn our attention to the secrecy criterion. Using Lemma 1, we have:

$$\hat{R}_1 \leq I_{max}^{\delta'-\epsilon'}(X_1:Z)_\rho+\log\frac{3}{\epsilon'^3}-\frac{1}{4}\log\delta' \quad (42)$$

$$\hat{R}_2 \leq I_{max}^{\delta'-\epsilon'}(X_2:ZX_1)_\rho+\log\frac{3}{\epsilon'^3}-\frac{1}{4}\log\delta'+\mathcal{O}(1) \quad (43)$$

Substituting Equation 42 and Equation 43 in Equation 38-Equation 40 completes the proof. □

Appendix 8.3 (Proof of Theorem 2). *Proof.* The proof uses two successive position-based decoders. The first decoder tries to decode the first message m_1, and the second decoder tries to decode the second message m_2, given the true decoded m_1. This means that if the first decoder fails, the second decoder fails, too. This decoding order can be shown as $m_1 \to m_2$.

Constructing the first position-based decoder is the same as that presented in [21]. To decode m_2, Bob performs his second position-based decoder conditioned on U_1, which works for all $u_1 \in \mathcal{U}_1$. It should be noted that the feeding state of the second decoder differs from the main state of the channel.

Alice, Bob, and Eve are allowed to pre-share some quantum state as randomness. Also, Alice has access to two sources of uniform junk randomness $k_i; i \in \{1,2\}$. The pre-shared randomness is as follows:

$$\rho_{U_1U_1'(AU_2U_2')^{\otimes|\mathcal{M}_2||\mathcal{K}_2|}}^{\otimes|\mathcal{M}_1||\mathcal{K}_1|} := \Bigg[\sum_{u_1} p_{U_1}(u_1)\,|u_1\rangle\langle u_1|_{U_1}\otimes|u_1\rangle\langle u_1|_{U_1'} \Bigg(\sum_{u_2} p_{U_2}(u_2)\,|u_2\rangle\langle u_2|_{U_2}\otimes|u_2\rangle\langle u_2|_{U_2'} \Bigg)^{\otimes|\mathcal{M}_1||\mathcal{K}_1|} \Bigg]^{\otimes|\mathcal{M}_2||\mathcal{K}_2|} \quad (44)$$

- The probability of error for decoding m_1:

$$p_{e_1} = p\{\hat{M}_1\neq M_1\} := \frac{1}{|\mathcal{M}_1|}\sum_{m_1=1}^{|\mathcal{M}_1|}\frac{1}{2}\Big\|\mathcal{D}_{YU_1\to\hat{M}_1}^{m_1}\Big(\rho_{U_1^{\otimes|\mathcal{M}_1||\mathcal{K}_1|}Y}^{(m_1,k_1),(m_2,k_2)}\Big) - |m_1\rangle\langle m_1|_{\hat{M}_1}\otimes\hat{\rho}_Z\Big\|_1 \leq \epsilon_1+\sqrt{\epsilon_2} \quad (45)$$

where $\mathcal{D}_{YU_1\to\hat{M}_1}^{m_1}\Big(\rho_{U_1^{\otimes|\mathcal{M}_1||\mathcal{K}_1|}Y}^{(m_1,k_1),(m_2,k_2)}\Big)$ is decoding map for m_1: The arguments connected to the decoding process for m_1 are listed as follows:

$$\mathcal{D}_{YU_1\to\hat{M}_1}^{m_1}\Big(\rho_{U_1^{\otimes|\mathcal{M}_1||\mathcal{K}_1|}Y}^{(m_1,k_1),(m_2,k_2)}\Big) := \sum_{k_1=1}^{|\mathcal{K}_1|}\sum_{m_1=1}^{|\mathcal{M}_1|} Tr\Big\{\Lambda_{U_1^{|\mathcal{M}_1||\mathcal{K}_1|}Y}^{m_1,k_1}\rho_{X_1^{\otimes|\mathcal{M}_1||\mathcal{K}_1|}Y}^{(m_1,k_1),(m_2,k_2)}\Big\} \otimes \frac{\sqrt{\Lambda_{U_1^{|\mathcal{M}_1||\mathcal{K}_1|}Y}^{m_1,k_1}}\,\rho_{U_1^{\otimes|\mathcal{M}_1||\mathcal{K}_1|}Y}^{(m_1,k_1),(m_2,k_2)}\sqrt{\Lambda_{U_1^{|\mathcal{M}_1||\mathcal{K}_1|}Y}^{m_1,k_1}}}{Tr\Big\{\Lambda_{U_1^{|\mathcal{M}_1||\mathcal{K}_1|}Y}^{m_1,k_1}\rho_{U_1^{\otimes|\mathcal{M}_1||\mathcal{K}_1|}Y}^{(m_1,k_1),(m_2,k_2)}\Big\}}$$

- $\Lambda_{U_1^{|\mathcal{M}_1||\mathcal{K}_1|}Y}^{m_1,k_1}$ is a pretty good measurement (POVM) for $m_1\in[1:|\mathcal{M}_1|]$:

$$\Lambda_{U_1^{|\mathcal{M}_1||\mathcal{K}_1|}Y}^{m_1,k_1} := \left(\sum_{k_1'=1}^{|\mathcal{K}_1|}\sum_{m_1'=1}^{|\mathcal{M}_1|}\Gamma_{U_1^{|\mathcal{M}_1||\mathcal{K}_1|}Y}^{m_1',k_1'}\right)^{-\frac{1}{2}}\Gamma_{U_1^{|\mathcal{M}_1||\mathcal{K}_1|}Y}^{m_1,k_1}\left(\sum_{k_1'=1}^{|\mathcal{K}_1|}\sum_{m_1'=1}^{|\mathcal{M}_1|}\Gamma_{U_1^{|\mathcal{M}_1||\mathcal{K}_1|}Y}^{m_1',k_1'}\right)^{-\frac{1}{2}}$$

where $\Gamma_{U_1^{|\mathcal{M}_1||\mathcal{K}_1|}Y}^{m_1,k_1}$ is the element of the first POVM:

$$\Gamma_{U_1^{|\mathcal{M}_1||\mathcal{K}_1|}Y}^{m_1,k_1} := I_{U_1}^{(1,1)}\otimes\ldots\otimes I_{U_1}^{(1,|\mathcal{K}_1|)}\otimes\ldots\otimes\tau_{U_1Y}^{m_1,k_1}\otimes\ldots\otimes I_{U_1}^{(|\mathcal{M}_1|,|\mathcal{K}_1|)}$$

and $\tau_{U_1Y}^{m_1,k_1}$ is a test operator to discriminate between two hypotheses ρ_{U_1Y}, and $\rho_{U_1}\otimes\rho_Y$. Also, it is obvious that to decode m_1, it does not matter for the second position-based decoder, which copy is selected by Alice among $|\mathcal{M}_1||\mathcal{K}_1|$ copies.

- We face a hypothesis testing problem. The null hypothesis is ρ_{U_1Y}, and the alternative hypothesis is $\rho_{U_1}\otimes\rho_Y$. Therefore, the probability of success in guessing null and alternative hypotheses are $Tr\{\tau_{U_1Y}\rho_{U_1Y}\}$ and $Tr\{(I_{U_1Y}-\tau_{U_1Y})(\rho_{U_1}\otimes\rho_Y)\}$.

The rest of the decoding process for m_1 is analogous to [21]. Therefore, we have:

$$R_1 \leq I_H^{\epsilon_1-\delta_1}(U_1;Y)_\rho-\tilde{I}_{max}^{\sqrt{\epsilon_2}-\delta_2}(U_1;Z)_\rho - \log\frac{4\epsilon_1}{\delta_1^2}-2\log\frac{1}{\delta_2} \quad (46)$$

Now, we turn our attention to decoding the second message. As mentioned before, the channel state changes after the first measurement. There is a detailed discussion in [33].

Let $\sigma_{U_1U_1'(U_2U_2')^{\otimes|\mathcal{M}_2||\mathcal{K}_2|YZ}}^{(m_1,k_1),(m_2,k_2)}$ denote the disturbed state after applying the first measurement (POVM):

$$\sigma^{(m_1,k_1),(m_2,k_2)}_{U_1U_1'(U_2U_2')^{\otimes|\mathcal{M}_2||\mathcal{K}_2|}YZ} := \sum_{u_1} p_{U_1}(u_1)\,|u_1\rangle\langle u_1|_{U_1}\,|u_1\rangle\langle u_1|_{U_1'} \otimes \sigma^{u_1(m_1,k_1)}_{U_2U_2'} \otimes \ldots \otimes \sigma^{u_1(m_1,k_1),(m_2,k_2)}_{U_2U_2'YZ} \otimes \ldots \otimes \sigma^{u_1(m_1,k_1),(|\mathcal{M}_2|,|\mathcal{K}_2|)}_{U_2U_2'}$$

Also, Bob's second POVM is as follows:

$$\Lambda^{m_2,k_2}_{U_1U_2^{|\mathcal{M}_2||\mathcal{K}_2|}Y} := \left(\sum_{k_2'=1}^{|\mathcal{K}_2|}\sum_{m_2'=1}^{|\mathcal{M}_2|}\lambda^{m_2',k_2'}_{U_1U_2^{|\mathcal{M}_2||\mathcal{K}_2|}Y}\right)^{-\frac{1}{2}} \lambda^{m_2,k_2}_{U_1U_2^{|\mathcal{M}_2||\mathcal{K}_2|}Y} \left(\sum_{k_2'=1}^{|\mathcal{K}_2|}\sum_{m_2'=1}^{|\mathcal{M}_2|}\lambda^{m_2',k_2'}_{U_1U_2^{|\mathcal{M}_2||\mathcal{K}_2|}Y}\right)^{-\frac{1}{2}}$$

$\lambda^{m_2,k_2}_{U_1X_2^{|\mathcal{M}_2||\mathcal{K}_2|}Y}$ is the element of the second POVM:

$$\lambda^{m_2,k_2}_{U_1U_2^{|\mathcal{M}_2||\mathcal{K}_2|}Y} := |u_1\rangle\langle u_1|_{U_1} \otimes I^{(1,1)}_{U_2} \otimes \ldots \otimes I^{(1,|\mathcal{K}_2|)}_{U_2} \otimes \ldots \otimes \theta^{m_2,k_2}_{U_2Y} \otimes \ldots \otimes I^{(|\mathcal{M}_2|,|\mathcal{K}_2|)}_{U_2}$$

$\theta^{m_2,k_2}_{U_2Y}$ is a binary test operator to discriminate between two hypotheses $\sigma^{u_1}_{U_2Y}$ and $\sigma^{u_1}_{U_2}\otimes\sigma^{u_1}_{Y}$ with an error of $\epsilon_1-\delta_1$; i.e.,

$$Tr\{\theta_{U_2Y}\sigma^{u_1}_{U_2Y}\} \geq 1-(\epsilon_1-\delta_1); \epsilon_1\in(0,1), \delta_1\in(0,\epsilon_1)$$

In other words, Bob has to be able to discriminate between the following states:

$$\sum_{u_1} p_{U_1}(u_1)\,|u_1\rangle\langle u_1|_{U_1}\otimes\sigma^{u_1}_{U_2Y}$$

$$\sum_{u_1} p_{U_1}(u_1)\,|u_1\rangle\langle u_1|_{U_1}\otimes\sigma^{u_1}_{U_2}\otimes\sigma^{u_1}_{Y}$$

Similar to what is mentioned in [21] and [28], we have the following rate:

$$R_2 \leq I_H^{\epsilon_1-\delta_1}(U_2;Y|U_1)_\rho - \tilde{I}_{max}^{\sqrt{\epsilon_1}-\delta_2}(U_2;Z|U_1)_\rho - \log\frac{4\epsilon_1}{\delta_1^2} - 2\log\frac{1}{\delta_2} \quad (47)$$

The probability of error for m_2 is as follows:

$$p_{e_2} = p\{\hat{M}_2\neq M_2\} := \frac{1}{|\mathcal{M}_2|}\sum_{m_2=1}^{|\mathcal{M}_2|}\frac{1}{2}\left\|\mathcal{D}^{m_1}_{\hat{M}_1YU_2\to\hat{M}_2}\left(\sigma^{(m_1,k_1),(m_2,k_2)}_{U_1U_1'(U_2U_2')^{\otimes|\mathcal{M}_2||\mathcal{K}_2|}YZ}\right)|m_2\rangle\langle m_2|_{\hat{M}_2}\otimes\hat{\sigma}_{U_1U_2'^{\otimes|\mathcal{M}_2||\mathcal{K}_2|}Z}\right\|_1 \leq 2(\epsilon_1+\sqrt{\epsilon_2})+\sqrt{\epsilon_1'} \quad (48)$$

Also, the error probability exponents stated in Equation 45 and Equation 48 are proved. See [21, 28].

This process can be repeated for another decoding order. In other words, we can first decode m_2 and then decode $m_1(m_2\to m_1)$. Then, taking the intersection of the regions resulting from both orders, we give:

$$R_1 \leq I_H^{\epsilon_1-\delta_1}(U_1;Y|U_2)_\rho - \tilde{I}_{max}^{\sqrt{\epsilon_2}-\delta_2}(U_1;Z)_\rho - \log\frac{4\epsilon_1}{\delta_1^2} - 2\log\frac{1}{\delta_2}$$

$$R_2 \leq I_H^{\epsilon_1-\delta_1}(U_2;Y|U_1)_\rho - \tilde{I}_{max}^{\sqrt{\epsilon_2}-\delta_2}(U_2;Z|U_1)_\rho - \log\frac{4\epsilon_1}{\delta_1^2} - 2\log\frac{1}{\delta_2}$$

This completes the proof. □

Appendix 8.4 (Proof of Theorem 3). *Proof.* The proof uses superposition coding. Assume that the first receiver, Y_1, has a better reception signal than the second receiver, Y_2. In this setting, Alice is able to encode a further message superimposed on top of the common message. Using successive decoding can be helpful.

Codebook generation: Randomly and independently generate 2^{R_c} sequence $u(m_c)$ according to the distribution $p_U(u)$. For each sequence $u(m_c)$, randomly and conditionally independently generate 2^{R_1} sequence $x(m_1,m_c)$ according to the distribution $p_{X|U}(x|u)$. The Y_1's state can be calculated by tracing out Y_2 from Equation 8:

$$\rho_{UXY} = \sum_{u,x} p_U(u)\,p_{X|U}(x|u)\,|u\rangle\langle u|^U\otimes|x\rangle\langle x|^X\otimes\rho_x^{Y_1}$$

Similar to what is mentioned in Theorem 2, we construct the POVM for the first receiver as:

$$\Lambda_{m_1,m_c} := \left(\sum_{m_c'=1}^{|\mathcal{M}_c|}\sum_{m_1'=1}^{|\mathcal{M}_1|}\Gamma_{m_1'm_c'}\right)^{-\frac{1}{2}}\Gamma_{m_1m_c}\left(\sum_{m_c'=1}^{|\mathcal{M}_c|}\sum_{m_1'=1}^{|\mathcal{M}_1|}\Gamma_{m_1'm_c'}\right)^{-\frac{1}{2}}$$

Also, the POVM for the second receiver can be constructed as follows:

$$\Lambda_{m_c} := \left(\sum_{m_c'=1}^{|\mathcal{M}_c|}\lambda_{m_c'}\right)^{-\frac{1}{2}}\lambda_{m_c}\left(\sum_{m_c'=1}^{|\mathcal{M}_c|}\lambda_{m_c'}\right)^{-\frac{1}{2}}$$

Consider the probability of error for m_1:

$$p_{e_1} = p\left\{(\hat{M}_1,\hat{M}_c)\neq(M_1,M_c)\right\} := \frac{1}{|\mathcal{M}_1||\mathcal{M}_c|}\sum_{m_c}\sum_{m_1}Tr\left\{(I-\Lambda_{m_1,m_c})\,\rho^{Y_1}_{x(m_1,m_c)}\right\}$$

and for m_c:

$$p_{e_2} = p\left\{\hat{M}_c \neq M_c\right\} := \frac{1}{|\mathcal{M}_c|}\sum_{m_c} Tr\left\{\left(I-\Lambda_{m_c}\right)\rho^{Y_2}_{x(m_1,m_c)}\right\}$$

By a straightforward calculation analogous to [3] for i.i.d. case and in [30] (to calculate one-shot Marton inner bound for QBC), the above error probability exponents can be calculated as follows:

$$\begin{aligned} p_{e_1}+p_{e_2} \leq\ & 2^{I^{\epsilon}_H(X;Y_1|U)_\rho - 2 + \log\epsilon} \\ & + 2^{I^{\epsilon}_H(U;Y_2)_\rho - 2 + \log\epsilon} \\ & + 2^{I^{\epsilon}_H(X;Y_1)_\rho - 2 + \log\epsilon} + \mathcal{O}(\epsilon) \end{aligned}$$

□

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.