量子干扰窃听信道的单次可达保密率区域

Hadi Aghaee 电气工程学院 K. N. Toosi University of Technology 伊朗德黑兰 邮箱: Aghaee_Hadi@email.kntu.ac.ir

Bahareh Akhbari 电气工程学院 K. N. Toosi University of Technology 伊朗德黑兰 邮箱: akhbari@

摘要——本文旨在单次设定下，推导具有经典输入的量子干扰信道的可达保密速率区域。为此，我们的主要思路是将叠加与速率分割相结合来设计编码方案，并构造一种基于同时解码的译码方案。

关键词——量子信道；互信息；保密容量；多址信道

I. 引言

物理层安全最早由 Shannon 提出 [1] 。随后，Wyner 提出了窃听信道，在该信道中，发送方在被动窃听者存在的情况下，将其消息传输给合法接收方[2] 。此外，Csiszár 和 Körner 提出了带机密消息的广播信道 [3] 。

然而，鉴于其重要性及其在实际系统中的应用，物理层安全问题已扩展到多终端信道，例如多址信道（MAC）、干扰信道（IC）、中继信道等[4-10] 。

近几十年来，随着量子数据处理的发展及其应用，人们开始投入大量精力，利用量子力学的自然特性来改进通信。其中一些特性如下：纠缠、不确定性、不可克隆定理、叠加等 [11] 。这些自然特性有助于使通信更加快速和安全。

此外，安全问题在量子通信中发挥着至关重要的作用，并成为研究的重要组成部分。在这方面，量子窃听信道（QWTC）最早在 [12] 和 [13] 中被提出。

随后，保密约束被扩展到多用户量子信道，例如量子干扰信道（QIC）[14] 和量子多址信道（QMAC）[15-18] 。干扰现象是通信系统面临的主要问题之一。

本文推导了具有经典输入的量子干扰信道的一些可达保密速率区域。

量子信息论中的一个重大未解问题，与具有三个或更多发送方的量子信道的同时解码器（即联合典型译码器）有关。不过，这个问题在某些情形下已经得到解决，例如最小熵情形，以及输出系统可交换的量子多址信道（QMAC）情形 [19] 。因此，在独立同分布（i.i.d.）情形下，我们必须将逐次解码与时分复用结合使用。相比之下，在单次情形下，我们必须使用同时解码器。Sen 证明了一个联合典型性引理，有助于在单次情形下同时解码任意数量的消息 [19] 。

本文旨在研究单次设定下经典-量子干扰窃听信道（C-QI-WTC）上的安全通信。据我们所知，这是首次研究这种信道。即使在经典情形下，干扰信道的安全问题也曾在一种称为带机密消息的干扰信道的不同场景中得到研究。我们的问题还有另一个特点：信道是在单次设定下考虑的。之所以作此选择，是因为在渐近独立同分布情形下，对于一般量子信道（即发送方数量不限的量子信道），尚无经过证明的联合典型性引理。因此，本文所得的所有结果都是新的，所提出的策略也可应用于经典干扰信道。

本文结构安排如下：第二节介绍一些开创性的定义。第三节介绍主要信道和信息处理任务。第四节介绍研究结果和主要定理。第五节讨论未来工作。

II. 预备知识

设 A（爱丽丝）和 B（鲍勃）是两个量子系统。这些量子系统可用相应的希尔伯特空间表示为 H^{A}，H^{B}。上述量子系统的状态分别表示为密度算符 ρ^{A} 和 ρ^{B}，而爱丽丝与鲍勃之间的共享态表示为 ρ^{AB}。密度算符是具有单位迹的半正定算符。爱丽丝或鲍勃的状态可通过对共享态施加偏迹算符来定义。偏迹用于模拟无法访问某个量子系统的情形。因此，使用偏迹得到的爱丽丝的密度算符为 $\rho^{A}=Tr_{B}\{\rho^{AB}\}$，鲍勃的密度算符为 $\rho^{B}=Tr_{A}\{\rho^{AB}\}$。我们用 $|\psi^{A}$ 表示系统 A 的纯态。相应的密度算符为 $\psi^{A}=|\psi\psi|^{A}$。状态 ρ^{A} 的冯·诺依曼熵定义为 $H(A)_{\rho}=-Tr\{\rho^{A}\log\rho^{A}\}$。对于诸如 σ^{AB} 这样的任意状态，量子条件熵定义为 $H(A|B)_{\sigma}=H(A,B)_{\sigma}-H(B)_{\sigma}$。量子互信息定义为 $I(A;B)_{\sigma}=H(A)_{\sigma}+H(B)_{\sigma}-H(A,B)_{\sigma}$，条件量子互信息定义为：

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

量子操作可表示为完全正迹保持（CPTP）映射 $^{A\to B}$。CPTP 映射接收 A 中的输入态，并输出 B 中的输出态。两个量子态（如 A 和 B）之间的距离用迹距离定义。诸如 σ 和 ρ 这样的任意两个状态之间的迹距离为：

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

其中 $|\Psi| = \sqrt{\Psi^\dagger \Psi}$。对于两个相似且可完美区分的状态，该量为零。

保真度定义为“$(\rho,\sigma) = ()\rho\sqrt{\sigma}(_1^2$，而净化距离是 $\mathcal{D}$(H) 上的一个度量，定义为 $,(\rho,\sigma) := 1 - '(\rho,\sigma)^2$。上述大多数定义均由[20] 给出。

定义1：（假设检验互信息）假设检验互信息记为 I_H^ϵ $(1;2) := D_H^\epsilon(\rho_{XY}\|\rho_X \otimes \rho_Y)$，$\epsilon \in (0,1)$，并被视为量子假设检验散度 [21] ，其中 $D_H^\epsilon(.\|.)$ 是假设检验相对熵 [21] 。$\rho^{\mathcal{H}_X}$ $_{\mathrm{H}^Y}$ 是输入和输出在其希尔伯特空间上的联合态（H_X, H_Y），且可表示为 ρ_{XY}：

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

其中，$?_X$ 是输入分布。

定义2：（量子相对熵 *[22]* ）：考虑状态 ρ_X、$\sigma_X \in \mathcal{D}$（H_X）。量子相对熵定义为：

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

其中，EF??(σ_X)表示σ的集合论支撑。EF??(σ)是由σ的所有非零特征值对应的特征向量张成的H的子空间。

事实：对于$\epsilon \in (0,1)$ [21] ，量子相对熵与假设检验相对熵之间存在以下关系：

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

其中，$\mathrm{h}_b(8) := -\epsilon\log_2\epsilon - (1-\epsilon)\log_2(1-\epsilon)$是二元熵函数。

定义3：（最大互信息 *[23]* ）考虑一个双部态 ρ_{XY} 和参数$\epsilon \in (0,1)$。最大互信息可定义如下：

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

其中，ρ 表示状态ρ_{XY} ，而$D_{max}(\|)$是$\rho_X, \sigma_X \in \mathrm{H}_X$的最大相对熵 [24] ：

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

定义4：（量子平滑最大相对熵*[24]* ）给定状态ρ_X，$\sigma_X \in \mathcal{D}(\mathrm{H}_X)$和$\epsilon \in (0,1)$。量子平滑最大相对熵定义如下：

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

其中 $\mathrm{B}^\epsilon(\rho_X) := \{\rho'_X \in \mathcal{D}(\mathrm{H}_X): ,(\rho'_X,\rho_X) \le \epsilon\}$ 是 ρ_{XY} 的 8-球。

定义 5：（量子平滑最大互信息*[23]* ）设 $\rho_{XY} := \sum$，$_{x\in\mathcal{X}}$ $_X$ $|$ $|_X \otimes \rho_Y^x$ (@) @@ 是一个经典-量子态，参数 $\epsilon \in (0,1)$。系统 1 和系统 2 之间的平滑最大互信息可定义如下：

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

其中 $\mathrm{B}^\epsilon(\rho_{XY}) := \{\rho'_{XY} \in \mathcal{D}(\mathrm{H}_X \otimes \mathrm{H}_Y): ,(\rho'_{XY},\rho_{XY}) \le \epsilon\}$ 是 ρ_{XY} 的 8- 球。

定义 6：（条件平滑假设检验互信息*[25]* ）设ρ_{XYZ} $:= \sum_z(\mathrm{d})|$ $\mathrm{dd}|_{Z\,z\in\mathcal{Z}} \otimes \rho_{XY}^z$ 为一个三方经典-量子态，且 $\epsilon \in (0,1)$。我们定义：

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

其中，最大值取遍所有满足 $,(\rho'_Z,\rho_Z) \le \epsilon$的 $\rho'_Z = \sum ?_Z(\mathrm{d})|$

定义 7：（条件平滑最大互信息*[25]* ）设 $\rho_{XYZ} := \sum_z(\mathrm{d})|$:

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

其中，最大化遍历所有满足 $,(\rho'_Z,\rho_Z) \le \epsilon$ 的 $\rho'_Z = \sum ?_Z($

定义 8：（r*[21]* 阶量子 Rényi 相对熵）对于状态

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

此外，r 阶 Rényi 熵可定义如下：

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

定义 9：（经典-量子多址信道的一次性内界）[19] 单次设定下的双用户 C-QMAC 是一个三元组 $(\mathrm{b}_1 \times \mathrm{b}_2, {}_{x_1x_2\to Y}$ $(\mathrm{z}_1,\mathrm{z}_2) \equiv {}_{\rho_Y}{}_{x_1x_2}, \mathrm{H}_Y)$，其中 b_1 和 b_2 是两个经典输入的字母表集合，2 是输出系统。$\rho_{x_1x_2Y}$ 是一个量子态，且该信道具有一个完全正迹保持映射（CPTP）$_{x_1x_2\to Y}$。

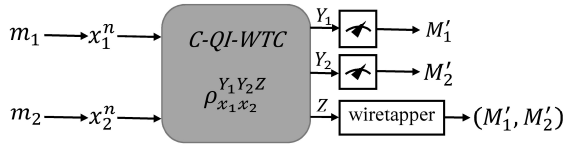

图1。C-QI-WTC 模型

考虑到[推论 4, 19], 中引入的联合典型性引理, C-QMAC 的一次性内界如下:

$$R_1 \le I_H^{\epsilon}(X_1{:}\,X_2Y)_\rho - 2 + \log\epsilon$$

$$R_2 \le I_H^{\epsilon}(X_2{:}\,X_1Y)_\rho - 2 + \log\epsilon$$

$$R_1 + R_2 \le I_H^{\epsilon}(X_1X_2{:}\,Y)_\rho - 2 + \log\epsilon$$

其中， $I_H^{\epsilon}(.)$ 是定义1中针对控制态定义的假设检验互信息:

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

且 Q 是一个时分变量。

注意， $I_H^{\epsilon}(:)$ 是二阶 Rényi 熵与条件量子熵之差。

III. 信道模型

双用户 C-QI-WTC 是一个三元组 $(\mathrm{b}_1 \times \mathrm{b}_2, x_1x_2 \to Y_1Y_2Z(z_1, z_2) \equiv \rho_{x_1x_2}^{Y_1Y_2Z}, \mathrm{H}^{Y_1} \otimes \mathrm{H}^{Y_2} \otimes \mathrm{H}^{Z})$,
其中 b_i、$\mathrm{N} \in \{1,2\}$ 表示输入字母表集合，而 Y_1、 Y_2、g 表示输出系统（Y_1、 Y_2 表示两个合法接收方处的信道输出，g 表示窃听者处的信道输出）。$\rho_{x_1x_2}^{Y_1Y_2Z}$ 是系统输出的量子态。每个用户都希望通过 C-QI-WTC，尽可能安全地将其消息传输给指定的接收方。

主信道（独立同分布情形）如图1所示。

考虑图1所示的主信道在单次设定下的情形。每个用户从其消息集合 $\mathrm{M}_i = \mathrm{C1}{:}\,|\,\mathrm{M}_i| = 2^{R_i}\mathrm{D}$ 中选择其消息 m_i; $\mathrm{N} \in \{1,2\}$，并通过 C-QI-WTC 发送该消息。用户还使用来自两个扩增集合 $\dagger_i =$的两个无用变量 ...i; $\mathrm{N} \in \{1,2\}$ ‡1: $|\dagger_{\mathrm{I}} = 2^{R\text{-}i}$‰; $\mathrm{N} \in \{1,2\}$ 用于随机化窃听者所掌握的信息。

我们为用户 1 和用户 2 分别准备了两个双重索引码本 $@_1(m_1, \ldots_1)$ 和 $@_2(m_2,\ldots_2)$。上述信道可分为两个子经典 - 量子多访问窃听信道（一个从两个用户到 (Y_1,g)，另一个从两个用户到 (Y_2, g)）。

IV. 主要结果

本节介绍主要结果。

定理 1: （C-QI-WTC 的单次可达速率区域）考虑一个接受 X_1 andX_2 作为输入、Y_1、 Y_2 和 g 作为输出的双用户 C-QI-WTC。$\rho_{x_1x_2}^{Y_1Y_2Z}$ 是信道密度算子。对于任意固定的 $\epsilon \in (0,1)$、 $\epsilon' \in (0, \check{\mathrm{S}}')$ 和 Š，以及满足 Š、Š′ 的 $\check{\mathrm{S}}' > 0$，速率对 $\{_i = \mathrm{\OE Ig}|\,\mathrm{M}_i| + \check{\mathrm{S}},\mathrm{N} \in \{1,2\}$ 可达，并满足以下不等式:

$$R_1 \le \min\{I_H^{\epsilon}(X_1{:}\,X_2Y_1|Q)_\rho, I_H^{\epsilon}(X_1{:}\,X_2Y_2|Q)_\rho\} - I_{max}^{\eta}(X_1{:}\,Z|Q)_\rho + \log\epsilon - 1 - \log\frac{3}{\epsilon'^3} + \frac{1}{4}\log\delta$$

$$R_2 \le \min\{I_H^{\epsilon}(X_2{:}\,X_1Y_1|Q)_\rho, I_H^{\epsilon}(X_2{:}\,X_1Y_2|Q)_\rho\} - I_{max}^{\eta}(X_2{:}\,ZX_1|Q)_\rho + \log\epsilon - 1 - \log\frac{3}{\epsilon'^3} + \frac{1}{4}\log\delta$$

$$R_1 + R_2 \le \min\{I_H^{\epsilon}(X_1X_2{:}\,Y_1|Q)_\rho, I_H^{\epsilon}(X_1X_2{:}\,Y_2|Q)_\rho\} - I_{max}^{\eta}(X_1{:}\,Z|Q)_\rho - I_{max}^{\eta}(X_2{:}\,ZX_1|Q)_\rho + \log\epsilon - 1 - 2\log\frac{3}{\epsilon'^3} + \frac{1}{2}\log\delta + \mathcal{O}(1)$$

其中 $\eta = \delta' - \epsilon'$ ，并集取遍输入分布 $?_Q(\})?_{X_1|Q}(@_1|\ \})?_{X_2|Q}(@_2|\ \})$。Q 是时分随机变量，所有互信息量均根据以下状态计算:

$$\rho^{QX_1X_2Y_1Y_2Z} \equiv \sum_{q,x_1,x_2} p_Q p(q) p_{X_1|Q}(x_1|q) p_{X_2|Q}(x_2|q) |q\rangle\langle q|^Q \otimes |x_1\rangle\langle x_1|^{X_1} \otimes |x_2\rangle\langle x_2|^{X_2} \otimes \rho_{x_1x_2}^{Y_1Y_2Z} \quad (4)$$

证明：见附录 A。

证明思路：该信道可以分解为两个具有经典输入的子 C-Q MA-WTC。一个信道从 (X_1, X_2) 到 (Y_1, g)，另一个从 (X_1, X_2) 到 (Y_2, g)。采用 El-Gamal 和 H. Kim [26] 提出的方法有助于证明该定理。

定理 1 给出了单次设定下 C-QI-WTC 最简单的可达速率区域。在不考虑保密约束的情况下，Han 和 Kobayashi 通过速率分割，将消息分为公共消息和私有消息，从而得到了干扰信道（独立同分布设置）的最佳可达速率区域。该技术经扩展后可用于量子情形，但存在一些限制 [14] 。采用 Han-Kobayashi 技术，消息 X_i 被分为 X_{i0} （公共部分）和X_{ii} （私有部分），其中 $\mathrm{N} \in \{1,2\}$。

Han-Kobayashi 设定下 C-QI-WTC 的结构如图 2 所示。以下信道可划分为两个彼此独立的三用户经典-量子多址窃听信道：一个从 (X_{10}, X_{11}, X_{20}) 到 (Y_1, g)，另一个从 (X_{20}, X_{22}, X_{10}) 到 (Y_2, g)。

如前所述，目前尚无能够一般性地解码三个或更多消息的量子同时译码器，其存在性仍是一个猜想（输出态的对易版本和最小熵等情况除外[14] ）。

$$\left\{I_{max}^{\eta}(m_{10}m_{11}m_{20}m_{22}:Z)_{\rho}\leq\varepsilon_3\middle|I_{max}^{\eta}(m_{10}m_{11}m_{20}:Z)_{\rho}\leq\varepsilon_1,I_{max}^{\eta}(m_{10}m_{20}m_{22}:Z)_{\rho}\leq\varepsilon_2\right\} \tag{5}$$

where $\varepsilon_1,\varepsilon_2$ and ε_3 are arbitrary small numbers.

$$R_1\leq I_H^{\epsilon}(X_{10}X_{11}:Y_1X_{20})_{\rho}-I_{max}^{\delta'-\epsilon'}(X_{10}:Z)_{\rho}-I_{max}^{\delta'-\epsilon'}(X_{11}:ZX_{10}X_{20})_{\rho}-2\log\frac{3}{\epsilon'^3}+\frac{1}{2}\log\delta'+\log\epsilon-2+\mathcal{O}(1) \tag{6}$$

$$R_1\leq I_H^{\epsilon}(X_{11}:Y_1X_{10}X_{20})_{\rho}+I_H^{\epsilon}(X_{10}:Y_2X_{20}X_{22})_{\rho}-I_{max}^{\delta'-\epsilon'}(X_{10}:Z)_{\rho}-I_{max}^{\delta'-\epsilon'}(X_{11}:ZX_{10}X_{20})_{\rho}-2\log\frac{3}{\epsilon'^3}+\frac{1}{2}\log\delta'+2\log\epsilon-4+\mathcal{O}(1) \tag{7}$$

$$R_2\leq I_H^{\epsilon}(X_{20}X_{22}:Y_2X_{10})_{\rho}-I_{max}^{\delta'-\epsilon'}(X_{20}:ZX_{10})_{\rho}-I_{max}^{\delta'-\epsilon'}(X_{22}:ZX_{10}X_{11}X_{20})_{\rho}-2\log\frac{3}{\epsilon'^3}+\frac{1}{2}\log\delta'+\log\epsilon-2+\mathcal{O}(1) \tag{8}$$

$$R_2\leq I_H^{\epsilon}(X_{20}:Y_1X_{10}X_{11})_{\rho}+I_H^{\epsilon}(X_{22}:Y_2X_{10}X_{20})_{\rho}-I_{max}^{\delta'-\epsilon'}(X_{20}:ZX_{10})_{\rho}-I_{max}^{\delta'-\epsilon'}(X_{22}:ZX_{10}X_{11}X_{20})_{\rho}-2\log\frac{3}{\epsilon'^3}+\frac{1}{2}\log\delta'+2\log\epsilon-4+\mathcal{O}(1) \tag{9}$$

$$R_1+R_2\leq I_H^{\epsilon}(X_{11}:Y_2X_{10}X_{20})_{\rho}+I_H^{\epsilon}(X_{10}X_{11}X_{20}:Y_2)_{\rho}-I_{max}^{\delta'-\epsilon'}(X_{10}:Z)_{\rho}-I_{max}^{\delta'-\epsilon'}(X_{11}:ZX_{10}X_{20})_{\rho}-I_{max}^{\delta'-\epsilon'}(X_{20}:ZX_{10})_{\rho}-I_{max}^{\delta'-\epsilon'}(X_{22}:ZX_{10}X_{11}X_{20})_{\rho}-4\log\frac{3}{\epsilon'^3}+\log\delta'+2\log\epsilon-4+\mathcal{O}(1) \tag{10}$$

$$R_1+R_2\leq I_H^{\epsilon}(X_{11}:Y_1X_{20}X_{10})_{\rho}+I_H^{\epsilon}(X_{22}X_{20}X_{10}:Y_2)_{\rho}-I_{max}^{\delta'-\epsilon'}(X_{10}:Z)_{\rho}-I_{max}^{\delta'-\epsilon'}(X_{11}:ZX_{10}X_{20})_{\rho}-I_{max}^{\delta'-\epsilon'}(X_{20}:ZX_{10})_{\rho}-I_{max}^{\delta'-\epsilon'}(X_{22}:ZX_{10}X_{11}X_{20})_{\rho}-4\log\frac{3}{\epsilon'^3}+\log\delta'+2\log\epsilon-4+\mathcal{O}(1) \tag{11}$$

$$\{_1+\{_2\leq I_H^{\epsilon}(X_{11}X_{20}:\ Y_1X_{10})_{\rho}+I_H^{\epsilon}(X_{22}X_{10}:\ Y_2X_{20})_{\rho}-I_{max-\epsilon'}^{\delta'}(X_{10}:\mathrm{g})_{\rho}-I_{max-\epsilon'}^{\delta'}(X_{11}:\mathrm{g}X_{10}X_{20})_{\rho}-I_{max}^{\delta'-\epsilon'}(X_{20}:ZX_{10})_{\rho}-I_{max}^{\delta'-\epsilon'}(X_{22}:ZX_{10}X_{11}X_{20})_{\rho}-4\log\frac{3}{\epsilon'^3}+\log\delta'+2\log\epsilon-4+\mathcal{O}(1) \tag{12}$$

$$\begin{aligned}2R_1+R_2\leq{}&I_H^{\epsilon}(X_{11}:Y_1X_{10}X_{20})_{\rho}+I_H^{\epsilon}(X_{10}X_{22}:Y_2X_{20})_{\rho}+I_H^{\epsilon}(X_{11}X_{10}X_{20}:Y_2)_{\rho}-2I_{max}^{\delta'-\epsilon'}(X_{10}:Z)_{\rho}\\&-2I_{max}^{\delta'-\epsilon'}(X_{11}:ZX_{10}X_{20})_{\rho}-I_{max}^{\delta'-\epsilon'}(X_{20}:ZX_{10})_{\rho}-I_{max}^{\delta'-\epsilon'}(X_{22}:ZX_{10}X_{11}X_{20})_{\rho}-6\log\frac{3}{\epsilon'^3}\\&+\frac{3}{2}\log\delta'+3\log\epsilon-6+\mathcal{O}(1)\end{aligned} \tag{13}$$

$$\begin{aligned}R_1+2R_2\leq{}&I_H^{\epsilon}(X_{11}X_{20}:Y_1X_{10})_{\rho}+I_H^{\epsilon}(X_{22}:Y_2X_{10}X_{20})_{\rho}+I_H^{\epsilon}(X_{22}X_{20}X_{10}:Y_1)_{\rho}-I_{max}^{\delta'-\epsilon'}(X_{10}:Z)_{\rho}\\&-I_{max}^{\delta'-\epsilon'}(X_{11}:ZX_{10}X_{20})_{\rho}-2I_{max}^{\delta'-\epsilon'}(X_{20}:ZX_{10})_{\rho}-2I_{max}^{\delta'-\epsilon'}(X_{22}:ZX_{10}X_{11}X_{20})_{\rho}-6\log\frac{3}{\epsilon'^3}\\&+\frac{3}{2}\log\delta'+3\log\epsilon-6+\mathcal{O}(1)\end{aligned} \tag{14}$$

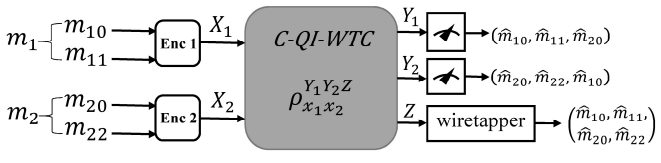

图 2. Han-Kobayashi 设置下 C-QI-WTC 的结构。

注 1：请注意，为了求定理 1 中提出的两个三发送方多址信道的私有区域的交集，我们采用了 [26] 的方法。另一种方法是使用 Fùrier-Motzkin 消元法 [附录 D，26] 该方法可得出与 Han-Kobayashi 表达式类似的可达速率区域。

注 2：Han-Kobashi 技术基于速率分割。需要注意的是，分割消息彼此并不独立。因此，在这种情况下，利用 Wyner 随机化技术来实现对窃听者的保密会变得棘手。换言之，我们无法在每个码块上独立地进行随机化。例如，m_1 应使用两个无用变量的乘积进行随机化（...10. ...11）。

猜想： （C-QI-WTC 一次性保密容量区域的一个内界）考虑以下区域：

$$\mathcal{R}(N)=\bigcup_{\pi}\{(R_1,R_2)\in R^2|Eqns.(6)-(14)\ hold\}$$

证明：见附录 B。

证明概要：我们考虑两个子经典-量子多访问窃听信道。因此，从第一个接收方（Y_1）的角度来看，有三个消息（Y_1、、）（，g），

而对于第二个接收方，有三个消息（m_{20}、m_{22}、m_{10}）→（Y_2，g）。该论文 [27] 介绍了相同的设置，但考虑了诸如 $m_{10} \to m_{20} \to m_{11}$ 的随机顺序。对于第一个 C-QMA-WTC，爱丽丝应在大小为（...10。...11）的总码块上进行随机化。对于第二个 C-QMA-WTC，鲍勃应在大小为（...20。...22）的总码块上进行随机化。然后，我们可以分析两个子信道。

备注3：上述猜想成立当且仅当条件 (5) 成立。因为对两个三发送方经典-量子多访问信道的私有区域取交集，并不足以得到整个 C-QI-WTC 的私有区域。

为了解决上述问题，我们应当改变编码过程，由此得到以下定理。

定理 2：（C-QI-WTC 一次性保密容量区域的内界）考虑以下区域：

$$\mathcal{R}(N) = \bigcup_{\pi}\{(R_1, R_2) \in R^2 | Eqns.(15) - (28)\ hold\}$$

证明：见附录 C。

证明思路：证明的整体思路与上述猜想相同，只有一处不同：假设两个接收方都想解码无干扰消息。此外，这种设置与定理 1 类似。解码各自的消息（包括目标消息和干扰消息）可能有助于接收方。换言之，X_{10} 和X_{20} 可以用作辅助信息。因此，第一个子信道可以建模为 $(X_{10}X_{11}X_2) \to (Y_1, \mathrm{g})$。所有步骤（例如编码和解码）都与上述猜想相同。

保密准则：信道的保密准则可定义如下：

$$I(M_1, M_2 : Z) \le \vartheta \qquad \text{For Theorem 1}$$

$$I(M_{10}, M_{11}, M_{20}, M_{22} : Z) \le \vartheta \qquad \text{For Conjecture and Theorem 2}$$

这意味着，发送消息与窃听者之间的互信息应被限制在任意小的数值以内。

V. 讨论与未来工作

本文研究了量子干扰信道上的安全通信问题。解码发送消息的主要方法是同时解码（单次量子联合典型性引理）[19] 。此外，我们采用了[27] 方法来随机化窃听者掌握的信息，并计算泄露信息。上述猜想给出了 C-QI-WTC 的单次可达速率区域，其形式为 Han-Kobayashi 速率区域。不过，我们仍不清楚如何根据子 C-QMA-WTC 的保密准则，推导出该信道的保密要求。然而，定理 2 通过一种新编码解决了这一问题。

附录

附录 A：（定理 1 的证明）

图1中的信道可以拆分为两个具有经典输入的子 QMA-WTC。一个连接两个用户与 (Y_1, g)，另一个连接两个用户与 (Y_2, g)。最后，可以计算出整体的可达保密速率区域：

$$\mathrm{R}_{C-QI-WTC} \le \min\check{Z}\mathrm{R}_{C-QMA-WTC_1}, \mathrm{R}_{C-QMA-WTC_2}\}$$

考虑第一个子信道。根据 Sen 的联合典型解码器 [19] 和 [引理 3. 2, 27]，，显然：

$$R_1 \le I_H^{\epsilon}(X_1 : X_2 Y_1 | Q)_\rho - I_{max}^{\eta}(X_1 : Z|Q)_\rho + \log\epsilon - 1 - \log\frac{3}{\epsilon'^3} + \frac{1}{4}\log\delta$$

$$R_2 \le I_H^{\epsilon}(X_2 : X_1 Y_1 | Q)_\rho - I_{max}^{\eta}(X_1 : ZX_2|Q)_\rho + \log\epsilon - 1 - \log\frac{3}{\epsilon'^3} + \frac{1}{4}\log\delta$$

$$R_1 + R_2 \le I_H^{\epsilon}(X_1X_2 : Y_1|Q)_\rho - I_{max}^{\eta}(X_1 : Z|Q)_\rho - I_{max}^{\eta}(X_1 : ZX_2|Q)_\rho + \log\epsilon - 1 - 2\log\frac{3}{\epsilon'^3} + \frac{1}{2}\log\delta + \mathcal{O}(1)$$

第二个子信道也有类似的速率。取两个子信道所得区域的交集，即完成证明。

保密准则：保密约束要求窃听者只能解码到可忽略的信息：

$$I_{max}^{\eta}(M_1M_2 : Z)_\rho \le \vartheta$$

显然，[引理 3.2, 27] 保证了保密准则。

附录 B：（猜想的证明）

为绕过注 1 中提出的问题，并恢复保密速率区域中的非角点，我们采用速率分割。我们采用如下设置：

我们考虑两个子经典-量子多访问窃听信道。因此，从第一个接收方 (Y_1) 的角度来看，有三条消息 $(m_{10}, m_{11}, m_{20}) \to (Y_1, \mathrm{g})$；而对于第二个接收方，有三条消息 $(m_{20}, m_{22}, m_{10}) \to (Y_2, \mathrm{g})$。论文 [27] 介绍了相同的设定，但采用了诸如 $m_{10} \to m_{20} \to m_{11}$ 这样的随机顺序。此顺序不会影响消息的解码，但有助于计算泄露信息。此外，需要注意的是，在单次情形下，我们不使用连续解码器，因为时分策略只能给出有限个可达速率对。相反，我们对两个子信道都使用单次联合典型解码器 [19] 。

对于第一个 C-QMA-WTC，爱丽丝应对大小为（...10. ...11）的总码块进行随机化。这是因为分割消息之间存在依赖关系。[28] 中对此有详细讨论。

对于 C-QI-WTC，控制态如下　　流：

$$\{_1 \leq \min\check{Z}I_H^{\epsilon}(X_{10}X_{11}\colon Y_1X_2)_\rho, I_H^{\epsilon}(X_1\colon Y_2X_{20}X_{22})_\rho\} - I_{max}^{\delta'-\epsilon'}(X_{10}\colon \mathrm{g})_\rho - I_{max}^{\delta'-\epsilon'}(X_{11}\colon \mathrm{g}X_{10}X_{20})_\rho - 2\,\text{对数}\frac{3}{\epsilon'^3} + \frac{1}{2}\log\delta' + \log\epsilon - 2 + \mathcal{O}(1) \tag{15}$$

$$R_1 \leq \left\{I_H^{\epsilon}(X_{11}\colon Y_1X_{10}X_2)_\rho + I_H^{\epsilon}(X_{10}\colon Y_1X_{11}X_2)_\rho, I_H^{\epsilon}(X_1X_{20}\colon Y_2X_{22})_\rho, I_H^{\epsilon}(X_1X_{22}\colon Y_2X_{20})_\rho\right\} - I_{max}^{\delta'-\epsilon'}(X_{10}\colon Z)_\rho - I_{max}^{\delta'-\epsilon'}(X_{11}\colon ZX_{10}X_{20})_\rho - 2\log\frac{3}{\epsilon'^3} + \frac{1}{2}\log\delta' + \log\epsilon - 2 + \mathcal{O}(1) \tag{16-17}$$

$$R_2 \leq \min\left\{I_H^{\epsilon}(X_{20}X_{22}\colon Y_2X_1)_\rho, I_H^{\epsilon}(X_2\colon Y_1X_{10}X_{11})_\rho\right\} - I_H^{\epsilon}(X_{20}X_{22}\colon Y_2X_{10})_\rho - I_{max}^{\delta'-\epsilon'}(X_{20}\colon ZX_{10})_\rho - I_{max}^{\delta'-\epsilon'}(X_{22}\colon ZX_{10}X_{11}X_{20})_\rho - 2\log\frac{3}{\epsilon'^3} + \frac{1}{2}\log\delta' + \log\epsilon - 2 + \mathcal{O}(1) \tag{18}$$

$$R_2 \leq \left\{I_H^{\epsilon}(X_{22}\colon Y_2X_{20}X_1)_\rho + I_H^{\epsilon}(X_{20}\colon Y_2X_{22}X_1)_\rho, I_H^{\epsilon}(X_2X_{10}\colon Y_1X_{11})_\rho, I_H^{\epsilon}(X_2X_{11}\colon Y_1X_{10})_\rho\right\} - I_{max}^{\delta'-\epsilon'}(X_{20}\colon ZX_{10})_\rho - I_{max}^{\delta'-\epsilon'}(X_{22}\colon ZX_{10}X_{11}X_{20})_\rho - 2\log\frac{3}{\epsilon'^3} + \frac{1}{2}\log\delta' + 2\log\epsilon - 4 + \mathcal{O}(1) \tag{19-21}$$

$$R_1 + R_2 \leq \min\left\{I_H^{\epsilon}(X_{11}X_{10}X_2\colon Y_1)_\rho, I_H^{\epsilon}(X_{22}X_{20}X_1\colon Y_2)_\rho\right\} - I_{max}^{\delta'-\epsilon'}(X_{10}\colon Z)_\rho - I_{max}^{\delta'-\epsilon'}(X_{11}\colon ZX_{10}X_2)_\rho - I_{max}^{\delta'-\epsilon'}(X_{20}\colon ZX_{10})_\rho - I_{max}^{\delta'-\epsilon'}(X_{22}\colon ZX_1X_{20})_\rho - 4\log\frac{3}{\epsilon'^3} + \log\delta' + 2\log\epsilon - 4 + \mathcal{O}(1) \tag{22}$$

$$\begin{aligned} R_1 + R_2 \leq \{&I_H^{\epsilon}(X_{11}\colon Y_1X_{10}X_2)_\rho + I_H^{\epsilon}(X_{10}X_{20}\colon Y_1X_{11})_\rho, I_H^{\epsilon}(X_{22}\colon Y_2X_{20}X_1)_\rho + I_H^{\epsilon}(X_{20}X_{10}\colon Y_1X_{11})_\rho, I_H^{\epsilon}(X_{22}X_1\colon Y_2X_{20})_\rho \\ &+ I_H^{\epsilon}(X_{20}\colon X_{22}X_1Y_2)_\rho, I_H^{\epsilon}(X_{11}X_2\colon Y_1X_{10})_\rho + I_H^{\epsilon}(X_{10}\colon X_{11}X_2Y_1)_\rho\} - I_{max}^{\delta'-\epsilon'}(X_{10}\colon Z)_\rho \\ &- I_{max}^{\delta'-\epsilon'}(X_{11}\colon ZX_{20}X_{10})_\rho - I_{max}^{\delta'-\epsilon'}(X_{20}\colon ZX_{10})_\rho - I_{max}^{\delta'-\epsilon'}(X_{22}\colon ZX_{10}X_{11}X_{20})_\rho - 4\log\frac{3}{\epsilon'^3} + \log\delta' \\ &+ 2\log\epsilon - 4 + \mathcal{O}(1) \end{aligned} \tag{23-26}$$

$$2R_1 + R_2 \leq I_H^{\epsilon}(X_{20}X_1\colon Y_2X_{22})_\rho + I_H^{\epsilon}(X_1X_{22}\colon Y_2X_{20})_\rho - 2I_{max}^{\delta'-\epsilon'}(X_{10}\colon Z)_\rho - 2I_{max}^{\delta'-\epsilon'}(X_{11}\colon ZX_{10}X_{20})_\rho - I_{max}^{\delta'-\epsilon'}(X_{20}\colon ZX_{10})_\rho - I_{max}^{\delta'-\epsilon'}(X_{22}\colon ZX_{10}X_{11}X_{20})_\rho - 6\log\frac{3}{\epsilon'^3} + \frac{3}{2}\log\delta' + 2\log\epsilon - 4 + \mathcal{O}(1) \tag{27}$$

$$\begin{aligned} R_1 + 2R_2 \leq\ & I_H^{\epsilon}(X_{10}X_2\colon Y_1X_{11})_\rho + I_H^{\epsilon}(X_2X_{11}\colon Y_1X_{10})_\rho - I_{max}^{\delta'-\epsilon'}(X_{10}\colon Z)_\rho - I_{max}^{\delta'-\epsilon'}(X_{11}\colon ZX_{10}X_2)_\rho \\ &- 2I_{max}^{\delta'-\epsilon'}(X_{20}\colon ZX_{10})_\rho - 2I_{max}^{\delta'-\epsilon'}(X_{22}\colon ZX_{10}X_{11}X_{20})_\rho - 6\log\frac{3}{\epsilon'^3} + \frac{3}{2}\log\delta' + +2\log\epsilon - 4 \\ &+ \mathcal{O}(1) \end{aligned} \tag{28}$$

$$\begin{aligned} &\rho^{X_{10}X_{11}X_{20}X_{22}Y_1Z} \\ &\coloneqq \sum_{\substack{X_{10},X_{11}\in\mathcal{X}_1 \\ X_{20},X_{22}\in\mathcal{X}_2}} P_{X_{10}}(x_{10})P_{X_{20}}(x_{20})P_{X_{11}}(x_{11})P_{X_{22}}(x_{22}) \\ &|x_{10}\rangle\langle x_{10}|_{X_{10}} \otimes |x_{11}\rangle\langle x_{11}|_{X_{11}} \otimes |x_{20}\rangle\langle x_{20}|_{X_{20}} \\ &\otimes |x_{22}\rangle\langle x_{22}|_{X_{22}} \otimes \rho_{Y_1Y_2Z}^{x_{01}x_{11}x_{20}x_{22}} \end{aligned} \tag{29}$$

为简化分析，我们首先移除问题中的安全约束。根据 Sen 的单次联合典型解码器 [19]，，第一个 C-QMAC 的速率区域如下：

$$\begin{aligned} R'_{10} &\leq I_H^{\epsilon}(X_{10}\colon Y_1X_{11}X_{20})_\rho + \log\epsilon - 2 \\ R'_{11} &\leq I_H^{\epsilon}(X_{11}\colon Y_1X_{10}X_{20})_\rho + \log\epsilon - 2 \\ R'_{20} &\leq I_H^{\epsilon}(X_{20}\colon Y_1X_{10}X_{11})_\rho + \log\epsilon - 2 \\ R'_{10} + R'_{11} &\leq I_H^{\epsilon}(X_{10}X_{11}\colon Y_1X_{20})_\rho + \log\epsilon - 2 \\ R'_{10} + R'_{20} &\leq I_H^{\epsilon}(X_{10}X_{20}\colon Y_1X_{11})_\rho + \log\epsilon - 2 \\ R'_{11} + R'_{20} &\leq I_H^{\epsilon}(X_{11}X_{20}\colon Y_1X_{10})_\rho + \log\epsilon - 2 \\ R'_{10} + R'_{11} + R'_{20} &\leq I_H^{\epsilon}(X_{10}X_{11}X_{20}\colon Y_1)_\rho + \log\epsilon - 2 \end{aligned}$$

此外，第二个 C-QMAC 也有类似的速率。需要注意的是 $\{_1 = \{_{10} + \{_{11}$ 和 $\{_2 = \{_{20} + \{_{22}$。消去冗余速率并使用傅里叶-莫茨金消元后，我们得到：

$$\mathcal{R}_{C-QIC} = \bigcup_{\pi\colon P_{X_{10}}(x_{10})P_{X_{11}}(x_{11})P_{X_{20}}(x_{20})P_{X_{22}}(x_{22})}$$

$$\begin{aligned} R'_1 &\leq I_H^{\epsilon}(X_{10}X_{11}\colon Y_1X_{20})_\rho + \log\epsilon - 2 \\ \{'_1 &\leq I_H^{\epsilon}(X_{11}\colon Y_1X_{10}X_{20})_\rho + I_H^{\epsilon}(X_{10}\colon Y_2X_{20}X_{22})_\rho + 2\,\text{对数}\ \epsilon - 4 \\ R'_2 &\leq I_H^{\epsilon}(X_{20}X_{22}\colon Y_2X_{10})_\rho + \log\epsilon - 2 \\ \{'_2 &\leq I_H^{\epsilon}(X_{20}\colon Y_1X_{10}X_{11})_\rho + I_H^{\epsilon}(X_{22}\colon Y_2X_{10}X_{20})_\rho + 2\,\text{对数}\ \epsilon - 4 \\ R'_1 + R'_2 &\leq I_H^{\epsilon}(X_{11}\colon Y_2X_{10}X_{20})_\rho + I_H^{\epsilon}(X_{10}X_{11}X_{20}\colon Y_2)_\rho + 2\log\epsilon - 4 \\ R'_1 + R'_2 &\leq I_H^{\epsilon}(X_{11}X_{20}\colon Y_1X_{10})_\rho + I_H^{\epsilon}(X_{22}X_{10}\colon Y_2X_{20})_\rho + 2\log\epsilon - 4 \end{aligned}$$

$$R_1 \le I_H^{\epsilon}(X_{10}X_{11}\colon Y_1X_2)_\rho - I_{max}^{\delta'-\epsilon'}(X_{10}\colon Z)_\rho - I_{max}^{\delta'-\epsilon'}(X_{11}\colon ZX_{10}X_2)_\rho - 2\log\frac{3}{\epsilon'^3} + \frac{1}{2}\log\delta' + \log\epsilon - 2 + \mathcal{O}(1) \tag{30}$$

$$R_1 \le I_H^{\epsilon}(X_{11}\colon Y_1X_{10}X_2)_\rho + I_H^{\epsilon}(X_{10}\colon Y_1X_{11}X_2)_\rho - I_{max}^{\delta'-\epsilon'}(X_{10}\colon Z)_\rho - I_{max}^{\delta'-\epsilon'}(X_{11}\colon ZX_{10}X_2)_\rho - 2\log\frac{3}{\epsilon'^3} + \frac{1}{2}\log\delta' + 2\log\epsilon - 4 + \mathcal{O}(1) \tag{31}$$

$$R_2 \le I_H^{\epsilon}(X_2\colon Y_1X_{10}X_{11})_\rho - I_{max}^{\delta'-\epsilon'}(X_{20}\colon ZX_{10})_\rho - I_{max}^{\delta'-\epsilon'}(X_{22}\colon ZX_{10}X_{11}X_{20})_\rho - 2\log\frac{3}{\epsilon'^3} + \frac{1}{2}\log\delta' + \log\epsilon - 2 + \mathcal{O}(1) \tag{32}$$

$$R_2 \le I_H^{\epsilon}(X_2X_{10}\colon Y_1X_{11})_\rho - I_{max}^{\delta'-\epsilon'}(X_{20}\colon ZX_{10})_\rho - I_{max}^{\delta'-\epsilon'}(X_{22}\colon ZX_{10}X_{11}X_{20})_\rho - 2\log\frac{3}{\epsilon'^3} + \frac{1}{2}\log\delta' + \log\epsilon - 2 + \mathcal{O}(1) \tag{33}$$

$$R_2 \le I_H^{\epsilon}(X_2X_{11}\colon Y_1X_{10})_\rho - I_{max}^{\delta'-\epsilon'}(X_{20}\colon ZX_{10})_\rho - I_{max}^{\delta'-\epsilon'}(X_{22}\colon ZX_{10}X_{11}X_{20})_\rho - 2\log\frac{3}{\epsilon'^3} + \frac{1}{2}\log\delta' + \log\epsilon - 2 + \mathcal{O}(1) \tag{34}$$

$$R_1 + R_2 \le I_H^{\epsilon}(X_{11}\colon Y_1X_{10}X_2)_\rho + I_H^{\epsilon}(X_{10}X_{20}\colon Y_1X_{11})_\rho - I_{max}^{\delta'-\epsilon'}(X_{10}\colon Z)_\rho - I_{max}^{\delta'-\epsilon'}(X_{11}\colon ZX_{10}X_2)_\rho - I_{max}^{\delta'-\epsilon'}(X_{20}\colon ZX_{10})_\rho - I_{max}^{\delta'-\epsilon'}(X_{22}\colon ZX_{10}X_{11}X_{20})_\rho - 4\log\frac{3}{\epsilon'^3} + \log\delta' + 2\log\epsilon - 4 + \mathcal{O}(1) \tag{35}$$

$$R_1 + R_2 \le I_H^{\epsilon}(X_{11}X_2\colon Y_1X_{10})_\rho + I_H^{\epsilon}(X_{10}\colon X_{11}X_2Y_1)_\rho - I_{max}^{\delta'-\epsilon'}(X_{10}\colon Z)_\rho - I_{max}^{\delta'-\epsilon'}(X_{11}\colon ZX_{10}X_2)_\rho - I_{max}^{\delta'-\epsilon'}(X_{20}\colon ZX_{10})_\rho - I_{max}^{\delta'-\epsilon'}(X_{22}\colon ZX_{10}X_{11}X_{20})_\rho - 4\log\frac{3}{\epsilon'^3} + \log\delta' + 2\log\epsilon - 4 + \mathcal{O}(1) \tag{36}$$

$$R_1 + R_2 \le I_H^{\epsilon}(X_{11}X_{10}X_2\colon Y_1)_\rho - I_{max}^{\delta'-\epsilon'}(X_{10}\colon Z)_\rho - I_{max}^{\delta'-\epsilon'}(X_{11}\colon ZX_{10}X_2)_\rho - I_{max}^{\delta'-\epsilon'}(X_{20}\colon ZX_{10})_\rho - I_{max}^{\delta'-\epsilon'}(X_{22}\colon ZX_{10}X_{11}X_{20})_\rho - 4\log\frac{3}{\epsilon'^3} + \log\delta' + \log\epsilon - 2 + \mathcal{O}(1) \tag{37}$$

$$R_1 + 2R_2 \le I_H^{\epsilon}(X_{10}X_2\colon Y_1X_{11})_\rho + I_H^{\epsilon}(X_2X_{11}\colon Y_1X_{10})_\rho - I_{max}^{\delta'-\epsilon'}(X_{10}\colon Z)_\rho - I_{max}^{\delta'-\epsilon'}(X_{11}\colon ZX_{10}X_2)_\rho - 2I_{max}^{\delta'-\epsilon'}(X_{20}\colon ZX_{10})_\rho - 2I_{max}^{\delta'-\epsilon'}(X_{22}\colon ZX_{10}X_{11}X_{20})_\rho - 6\log\frac{3}{\epsilon'^3} + \frac{3}{2}\log\delta' + +2\log\epsilon - 4 + \mathcal{O}(1) \tag{38}$$

$$R_1' + R_2' \le I_H^{\epsilon}(X_{11}\colon Y_1X_{20}X_{10})_\rho + I_H^{\epsilon}(X_{22}X_{20}X_{10}\colon Y_2)_\rho + 2\log\epsilon - 4$$

$$2R_1' + R_2' \le I_H^{\epsilon}(X_{11}\colon Y_1X_{10}X_{20})_\rho + I_H^{\epsilon}(X_{10}X_{22}\colon Y_2X_{20})_\rho + I_H^{\epsilon}(X_{11}X_{10}X_{20}\colon Y_2)_\rho + 3\log\epsilon - 6$$

$$R_1' + 2R_2' \le I_H^{\epsilon}(X_{11}X_{20}\colon Y_1X_{10})_\rho + I_H^{\epsilon}(X_{22}\colon Y_2X_{10}X_{20})_\rho + I_H^{\epsilon}(X_{22}X_{20}X_{10}\colon Y_1)_\rho + 3\log\epsilon - 6$$

该区域称为 C-QIC 的量子单次 Han-Kobayashi 速率区域，这是 Sen 在 [30] 中针对特殊情形计算得到的。他考虑了这样一种干扰信道情形：发送方 1 与其预期接收方之间，以及发送方 2 与其预期接收方之间，分别具有独立先验纠缠。需要注意的是，C-QIC 在独立同分布情形下的量子 Han-Kobayashi 速率区域已在 [14] 中被猜想。

注意，上述所有速率均对应于不带保密约束的 C-QMAC。现在我们希望考虑该问题的保密要求。

对于 C-QMA-WTC，我们需要三方凸分裂引理的平滑版本 [20] 。这会遇到量子信息论中的平滑瓶颈。在 [27], 中，作者提出了一个新颖的引理，用平滑最大互信息给出了随机化码块的大小。

引理 1：给定式 (29) 中的控制态以及解码顺序，例如 $m_{10} \to m_{20} \to m_{11} \to m_{22}$、Š′ > 0 和 0 ≪ϵ′ < Š′，令 $\{@_{10}^{(1)}, \dots, @_{10}^{(K_{10})}2$、$\{@_{11}^{(1)}, \dots, @_{11}^{(K_{11})}2$ 和 $\{@_{2}^{(1)}, \dots, @_{2}^{(K_{2})}2$ 为分别服从分布 $,_{X_{10}}, ,_{X_{11}}$ 和 $,_{X_2}$ 的独立同分布样本。那么，若

$$\log|\mathcal{K}_{10}| \ge I_{max}^{\delta'-\epsilon'}(X_{10}\colon Z)_\rho + \log\frac{3}{\epsilon'^3} - \frac{1}{4}\log\delta'$$

$$\log|\mathcal{K}_{20}| \ge I_{max}^{\delta'-\epsilon'}(X_{20}\colon ZX_{10})_\rho + \log\frac{3}{\epsilon'^3} - \frac{1}{4}\log\delta' + \mathcal{O}(1)$$

$$\log|\mathcal{K}_{11}| \ge I_{max}^{\delta'-\epsilon'}(X_{11}\colon ZX_{10}X_{20})_\rho + \log\frac{3}{\epsilon'^3} - \frac{1}{4}\log\delta' + \mathcal{O}(1)$$

$$\log|\mathcal{K}_{22}| \geq I_{max}^{\delta'-\epsilon'}(X_{22}:ZX_{10}X_{11}X_{20})_\rho + \log\frac{3}{\epsilon'^3} - \frac{1}{4}\log\delta' + \mathcal{O}(1)$$

满足以下条件，

$$\mathbb{E}_{\substack{\mathcal{X}_{10}\sim P_{X_{10}}\\ \mathcal{X}_{11}\sim P_{X_{11}}\\ \mathcal{X}_{20}\sim P_{X_{20}}\\ \mathcal{X}_{22}\sim P_{X_{22}}}} \left\| \frac{1}{|\mathcal{K}_1||\mathcal{K}_2|} \sum_{k=1}^{|\mathcal{K}_{22}|} \sum_{l=1}^{|\mathcal{K}_{11}|} \sum_{j=1}^{|\mathcal{K}_{20}|} \sum_{i=1}^{|\mathcal{K}_{10}|} \rho^{Z}_{x_{10}^i x_{20}^j x_{11}^l x_{22}^k} - \rho^Z \right\|_1 \leq 60\delta'^{\frac{1}{8}}$$

证明：该证明与[27] 中所述的双用户情形类似。

如前所述，令 …$_1$ = …$_{10}$. …$_{11}$ 和 …$_2$ = …$_{20}$. …$_{22}$. 注意，{ $_1$ = {$'_1$ − log …$_1$, {$_2$ = {$'_2$ − log …$_2$. 利用上述引理即可完成证明。

附录 C：（定理 2 的证明）如附录 A 所述，保密约束要求窃听者只能解码到可忽略的信息：

$$I_{max}^{\eta}(m_{10}m_{11}m_{20}m_{22}:Z)_\rho \leq \vartheta \qquad (39)$$

编码：假设两个接收方都希望解码非干扰消息。这种设置与定理 1 类似。对接收方而言，解码其消息（包括目标消息和干扰消息）可能会有所帮助。换言之，X_{10} 和X_{20} 可用作辅助信息。因此，第一个子信道可建模为 $(X_{10}X_{11}X_2) \to (Y_1, \mathrm{g})$。

考虑第一个 C-QMA-WTC $(X_{10}X_{11}X_2) \to (Y_1, \mathrm{g})$。根据 [27]，，可按 (30)-(38) 所述计算可达速率区域。

对于第二个 C-QMA-WTC $(X_1X_{20}X_{22}) \to (Y_2, \mathrm{g})$，也存在类似的可达速率。两个子信道的保密区域的交集可按式 (15)-(28) 所述计算。与猜想相对，引理 1 保证了该问题 (39) 的保密约束成立。至此，证明完成。

参考文献

[1] C. Shannon, 《保密系统通信理论》, 《贝尔系统技术期刊》, 第 28 卷第 4 期, 第 656–715 页, 1949 年。[2] A. D. Wyner, 《窃听信道》, 《贝尔系统技术期刊》, 第 54 卷第 8 期, 第 2–10 页, 1975 年 10 月。[3] I. Csiszar 和 J. Korner, 《带机密消息的广播信道》, 《IEEE 信息论汇刊》, 第 24 卷第 3 期, 第 339–348 页, 1978 年 5 月。[4] E. Ekrem 和 S. Ulukus, 《多址窃听信道的保密性》, 载于第 46 届 Allerton 通信、控制与计算年会论文集, 美国伊利诺伊州厄巴纳 - 香槟, 2009 年 3 月。[5] E. [illegible] 《IEEE 信息论汇刊》, 第 54 卷第 12 期, 第 5747–5755 页, 2008 年 12 月。[6] E. Tekin 和 A. [illegible] 可达速率与协作干扰》, 《IEEE 信息论汇刊》, 第 54 卷第 6 期, 第 2735–2751 页, 2008 年 6 月。[7] Y. Liang、H. V. Poor, 《带机密消息的多址信道》, 《IEEE 信息论汇刊》, 第 54 卷第 3 期, 第 976–1002 页, 2008 年。

[8] X. Tang、R. Liu、P. Spasojevi´ c、H. V. Poor, 《带广义反馈和机密消息的多址信道》, 载于信息论研讨会论文集, 美国加利福尼亚州太浩湖（2007 年 9 月）. 第 608–613 页。[9] B. Dai 和 Z. Ma, 《多址窃[illegible]些新结[illegible]93–4712 页，2014 年。[10] R. Liu、I. Mari´ c、R. Yates、P. Spasojevi´ c, 《带机密消息的离散无记忆多址信道》, 载于国际信息论研讨会论文集, 美国西雅图（2006 年 7 月）. 第 957–961 页。[11] L. Gyongyosi、S. Imre、H. V. Nguyen, [illegible] 《IEEE通信调查与教程》, 第 20 卷[illegible]1205 页，2018 年。[12] N. Cai、A. Winter 和 R. W. Yeung, 《量子隐私与量子窃听信道》, 《信息传输问题》, 第 40 卷第 4 期, 第 318–336 页，2004 年。[13] I. Devetak, 《量子信道的私有经典容量与量子容量》, 《IEEE 信息论汇刊》, 第 51 卷第 1 期, 第 44–55 页，2005 年 1 月。[14] O. Fawzi、P. Hayden、I. Savov、P. Sen 和 M. M. Wilde, 《通过量子干扰信道进行经典通信》, 《IEEE 信息论汇[illegible]58 卷第 6 期，第 3670–3691 页，2012 年 6 月。[15] H. Aghaee、B. Akhbari. 《经典-量子多址窃听信道[illegible] *16th* 国际ISC信息安全与密码学会议（ISCISC 19）论文集，伊朗马什哈德，2019 年 8 月。[16] H. A[illegible] 《通过量子多址信道传[illegible]（IS[illegible]）论文集，伊朗，2020 年。[17] H. Aghaee、B. Akhbari, 《带保密约束的经典-量子多址信道：单次速率区域》, 《国际信息与通信技[illegible]》（IWCMC）. 第 13 卷第 2 期，第 1–10 页，2020 年春季。[18] H. Aghaee、B. Akhbari, 《带公共消息的经典-量子多址窃听信道：单次速率区域》, 载于11th信息与知识技[illegible]论文集，伊朗，2020 年。[19] [illegible] 《[illegible]型性引理》, 《Sadhana》, 46(1):1–44，2021 年。[20] A. Anshu、R. Jain 和 N. A. Warsi, 《广义量子 Slepian–Wolf 定理》, 载于《IEEE [illegible]》, doi: 10.1109/TIT.2017.2786348。[21] H. Qi、Q. Wang、M. M. Wilde, 《将基于位置的编码应用于通过量子信道进行经典通信》, 《Journal of Physics A: Mathematical and Theoretical》, 51(44), 2018 年 9 月。[22] M. M. Wilde, 《基于位置的编码与凸分裂：通过量子信道进行私有通信》, 《量子信息处理》, 16(10):264，2017 年 10 月。arXiv:1703.01733。[23] L. Wang 和 R. Renner, 《单次经典-量子容量与假设检验》, 《物理评论快报》, 第 108 卷第 20 期，文章编号 200501，2012 年。[24] H. Umegaki, 《算子代数中的条件期望 IV（熵与信息）》, 《Kodai 数学研讨会报告》, 第 14 卷，第 59–85 页，1962 年。[25] M. Berta、M. Christandl 和 R. Renner, 《基于单次信息论的量子反向香农定理》, 《Communications in Mathematical Physics》, 第 306 卷第 3 期，第 579–615 页，2011 年。[26] A. El Gamal、Y.H. Kim, 《网络信息论》, 剑桥大学出版社，2012 年。[27] S. Chakraborty、A. Nema、P. Sen, 《通过量子多址信道发送私有经典信息的单次内界》, arXiv:2105.06100。[28] O. Fawzi、I. Savov, 《存在多个接收方时的速率分割》, ArXiv abs/1207.0543 (2012)：无页码。[29] N. Datta, 《最小-最大相对熵与一种新的纠缠单调量》, 《IEEE 信息论汇刊》, 第 59 卷，第 2816–2816 页，2009 年。[30] P. Sen, 《通过同时解码获得量子网络信息论的内界》, arXiv 预印本，文章编号 arXiv:1806.07276，2018 年 6 月。