量子多址窃听信道：论一次性可达保密速率区域

Hadi Aghaee，电气工程学院，K. N. Toosi University of Technology，伊朗德黑兰。电子邮箱：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。电子邮箱：akhb

摘要——本文拟研究一次性设置下的经典—量子多址窃听信道（CQ-MA-WTC）。为此，我们使用同时位置型解码器分析 CQ-MA-WTC，以实现可靠解码；并采用一种新近提出的技术进行安全解码。此外，为作比较，我们使用 Sen 的一次性联合典型性引理分析 CQ-MA-WTC，以实现可靠解码。同时位置型解码器会引出一个多重假设检验问题。此外，在同时场景中使用凸分裂分析隐私准则会遇到困难。为解决这两个问题，我们首先引入一种新信道，可将其视为 CQ-MA-WTC 的对偶信道。该信道称为多消息点对点量子窃听信道（PP-QWTC）。随后，作为解决问题的一种策略，我们还研究并分析一次性设置下的量子广播信道（QBC）。

关键词——量子信道；互信息；保密容量；多址信道

I. 引言

量子多址信道（QMAC）最早由 Winter [1] 提出。QMAC 可以接收两个或更多消息（经典或量子）作为输入，并产生一个输出。

与经典领域类似，QMAC 上的消息解码主要基于两种技术：连续消除解码和同时解码。在 [1]， 中，作者采用了连续消除解码技术。

量子广播信道（QBC）是一种具有一个发送方和两个或更多接收方的信道。发送方希望通过该信道向接收方传送两个或更多消息（经典或量子）。QBC 最早由 Yard 等人[2] 提出。在 [2]， 中，作者针对 i.i.d.（独立同分布）情形推导出了 QBC 的一个内界；在 [3]， 中，作者采用一种更直接且更符合其经典对应形式的方法，推导出了相同的内界[4] ，而非采用 [2] 中的方法。

近几十年来，随着量子数据处理及其应用的发展，研究量子信道安全性的必要性日益增加。在这方面，量子窃听信道（QWTC）最早由[5] 和[6] 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）[7,8]，和量子多址信道（QMAC）[9-13] 。

研究量子信道安全性时有两个瓶颈。第一个是同时解码三条或更多消息（可靠性），第二个则是如何安全地解码两条或更多消息（保密性）。第一个瓶颈源于一般量子联合典型性引理的缺失。不过，在一些情形下，这个问题已得到解决，例如最小熵情形以及具有交换输出的 QMAC [14] 。因此，在独立同分布（i.i.d.）情形下，应采用连续解码并结合时分复用技术。在这种设置中，发送方可以仅通过一次使用信道来发送消息。Sen 证明了一个联合典型性引理，有助于在一次性情形下同时解码任意数量的消息 [14] 。在量子设置中，通过 Wyner技术 [15] 对一个数据块进行随机化以抵御窃听者并实现保密，会变得棘手。Devetak [6] 已证明 Wyner技术适用于点对点量子信道，并在 [16] 中作了进一步阐释。然而，对于量子信道而言，并没有简单的方法将其推广到多个发送方。这一问题已在 [16] 中作了详细讨论。

本文旨在研究一次性设置下具有经典输入的量子多址信道（QMAC）的保密问题。此外，我们还研究了与CQ-MA-WTC的解码过程相关的一些瓶颈。本文的工作主要包括分析解码过程中的瓶颈，并提出克服这些瓶颈的解决方案。

此外，我们为具有经典输入的量子多址窃听信道（CQMA-WTC）介绍了两种技术。第一种方法基于[14]，中提出的方法，另一种技术是同时位置型解码器。由 [17]，可知，同时位置型解码器趋于一个多重量子假设检验问题，该问题在特殊情况下是可解的。此外，由[18]，可知，凸分裂引理不能用于分析同时解码中多条消息的隐私性。

本文结构安排如下：第二节介绍一些重要的定义。第三节介绍主信道和信息处理任务。第四节介绍研究结果和主要定理。第五节用于讨论。

II. 预备知识

设 A（Alice）、B（Bob）和 C（Charlie）为三个量子系统。这些量子系统可分别用对应的希尔伯特空间 H^{A}，H^{B} 和 H^{C}表示。上述量子系统的状态分别表示为密度算子 ρ^{A}, ρ^{B} 和 ρ^{C}，而 Alice、Bob 与 Charlie 之间的共享态记为 ρ^{ABC}。密度

算子是迹为单位的半正定算子。Alice、Bob 或 Charlie 的状态可通过对共享态应用偏迹算子来定义。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 Alice 的密度算子为 $\rho^A = Tr_{BC}\{\rho^{ABC}\}$。$|\psi^A$ 表示系统 A 的纯态。对应的密度算子为 $\psi^A = |\psi\psi|^A$。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：

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

量子操作可以用完全正迹保持映射（CPTP）$!^{A\to B}$表示。CPTP 映射接收 A 中的输入状态，并输出 B 中的状态。两个量子态（例如 A 和 B）之间的距离由迹距离定义。两个任意状态（例如 σ 和 ρ ）之间的迹距离为：

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

其中 $|\Psi| = \sqrt{\Psi^\dagger \Psi}$。对于两个相同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 ,(H) 上的一种度量，定义为 $-(\rho,\sigma) := 1 - ((\rho,\sigma)^2$。上述大部分定义见 [19] 。

定义 1：（假设检验互信息）假设检验互信息记为 I_H^ϵ $(2;3) := D_H^\epsilon(\rho_{XY}\|\rho_X \otimes \rho_Y)$，$\epsilon \in (0,1)$，并被视为量子假设检验散度 [17] ，其中 $D_H^\epsilon(.\|.)$ 是假设检验相对熵 [17] 。9 是平滑变量，$\rho^{\mathcal{H}_X H^Y}$ 是输入和输出在其希尔伯特空间上的联合经典-量子态（H_X, H_Y），并可表示为 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 *[20]* ）：考虑状态 ρ_X, $\sigma_X \in$, (H_X)。量子相对熵定义如下：

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

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

事实 1：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 $h_b(9) := -\epsilon \log_2 \epsilon - (1-\epsilon)\log_2(1-\epsilon)$ 是二元熵函数。

定义 3：（最大互信息 *[21]* ）考虑双方态 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 $\rho_X, \sigma_X \in H_X$ 的最大相对熵 [22] ：

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

定义 4：（量子平滑最大相对熵 *[22]* ）设 $\rho_X, \sigma_X \in$, (H_X) 为状态，且 $\epsilon \in (0,1)$。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，$B^\epsilon(\rho_X) := \{\rho'_X \in ,(H_X): -(\rho'_X, \rho_X) \le \epsilon\}$ 是 ρ_{XY} 的 9-球。

定义 5：（量子平滑最大互信息*[21]* ）设 $\rho_{XY} := \sum$ - $_{x\in\mathcal{X}}$ $_X$ | $|_X \otimes \rho_Y^x$ (A) AA} 为经典-量子态，且参数 $\epsilon \in (0,1)$。系统 2 和 3 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，$B^\epsilon(\rho_{XY}) := \{\rho'_{XY} \in ,(H_X \otimes H_Y): -(\rho'_{XY}, \rho_{XY}) \le \epsilon\}$ 是针对 ρ_{XY} 的 9-球。

定义 6：（条件平滑假设检验互信息*[23]* ）设 ρ_{XYZ} $:= \sum @_Z(e)|$ ee$|_Z$ $_{z\in\mathcal{Z}} \otimes \rho_{XY}^z$ 是一个三方经典-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，最大化遍历所有满足 $-(\rho'_Z, \rho_Z) \le \epsilon$ 的 $\rho'_Z = \sum @_Z$

事实 2：[24] 设 $\rho_{XYZ} := \sum @_Z(e)|$ ee$|_Z$ $_{z\in\mathcal{Z}} \otimes \rho_{XY}^z$ 是一个三方经典-量子态，且 $\epsilon \in (0,1)$，则以下关系成立：

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

定义7：（交替平滑最大互信息）考虑一个双方态 ρ_{XY} 以及一个参数 $\epsilon \in (0,1)$。系统 2 和 3 之间的平滑最大互信息的另一种定义如下：

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

事实 3：（平滑最大互信息两种定义之间的关系）[25]：令 $\epsilon \in (0,1)$ 且 Y $\in (0, 9)$。对于双方态 ρ_{XY}，有：

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

定义 8：（条件平滑最大互信息[23]）设 $\rho_{XYZ} := \sum$ @z(

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

其中，最大化遍历所有满足 -(ρ′Z, ρZ) ≤ ϵ 的 $\rho'_Z = \sum$ @z

事实 4： [24] $\rho_{XYZ} := \sum$ @z(e)| ee|Z z∈Z ⊗ ρ^z_{XY} 是一个三方经典-量子态，且 ϵ ∈(0,1) 时，以下关系成立：

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

定义9：（阶数为 z[17] 的量子 Rényi 相对熵）对于

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

A此外，阶数为 z 的 Rényi 熵可以定义为 如下：

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

定义10：（经典-量子多址信道的单次内界）[14] 单次设置下的双用户经典-量子多址信道（经典-量子多址信道）是一个三元组 (c1 × c2, !$x_1x_2\to Y$(x1, x2) ≡$\rho_{x_1x_2Y}$, HY)，其中 c1 和 c2 是两个经典输入的字母表集合，3 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）!$x_1x_2\to Y$。

考虑到[推论4, 14], 中引入的联合典型性引理, QMAC 的单次内界如下：

$$R_1 \leq I^{\epsilon}_H(X_1{:}X_2Y)_{\rho} - 2 + \log\epsilon$$

$$R_2 \leq I^{\epsilon}_H(X_2{:}X_1Y)_{\rho} - 2 + \log\epsilon$$

$$R_1 + R_2 \leq I^{\epsilon}_H(X_1X_2{:}Y)_{\rho} - 2 + \log\epsilon$$

解码错误至多为 49$\sqrt{\epsilon}$，其中 $I^{\epsilon}_H(.)$ 是定义 1 中相对于控制态定义的假设检验互信息：

$$\rho^{QX_1X_2Y} := \sum_{qx_1x_2} p(q)p(x_1|q)p(x_2|q)|qx_1x_2\rangle\langle qx_1x_2|^{QX_1X_2} \otimes \rho^Y_{x_1x_2} \quad (2)$$

且 ˆ 是一个时分变量。

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

引理1：[16] 给定式（2）中的控制状态（不含时分复用变量），‰′ > 0 和0 < ϵ′ < ‰′，令 ŒA1, ... , A_{K_1}} 和 Œy_1, ..., y_{K_2}} 为分别取自分布 -χ 和 -Y 的独立同分布样本。那么，如果

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

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

以下结论成立，

$$\mathbb{E}_{\substack{x_1,\dots,x_{K_1}\sim P_X \\ y_1,\dots,y_{K_2}\sim P_Y}} \left\| \frac{1}{|\mathcal{K}_1||\mathcal{K}_2|}\sum_{j=1}^{|\mathcal{K}_2|}\sum_{i=1}^{|\mathcal{K}_1|} \rho^Z_{x_iy_j} - \rho^Z \right\|_1 \leq 20\delta'^{\frac{1}{8}}$$

证明：见 [16] 。

引理 2：（凸分裂引理）[19,20] 设 ρ_{XY} 为任意状态，并假设 ¢$_{X_1\dots 6k_B}$ 是如下状态：

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

设 ϵ ∈ (0,1) 且 ‰ ∈ o0,$\sqrt{\epsilon}$], 若

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

那么，

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

对于某个状态 ρ«Y ，满足 -(ρY, ρ«Y) ≤ $\sqrt{\epsilon}$ − ‰。

证明：见 [20] 。

引理 3：（Hayashi-Nagaoka不等式 *[26]* ）设$S,T \in \mathcal{P}$ (Hx)，且 $(I-S) \in \mathcal{P}$(Hx) 为满足 $T \geq 0$ 和 $0 \leq S \leq I$ 的算子，则对所有正数常量 ®，以下关系成立：

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

证明：见 [26] 。

III. 信道模型

双用户 CQ-MA-WTC 是一个三元组 (c1 ×c2, !$^{x_1x_{2\to Y}}$ z(x1, x2) ≡ $\rho_{x_1x_2YZ}$, $H^Y \otimes H^Z$)，其中 cı,O ∈{1,2} 表示输入字母表集合，3 和 h 表示输出系统（3 表示合法接收方（Charlie）处的信道输出，h 表示窃听者处的信道输出）。$\rho_{x_1x_2YZ}$ 是系统输出的量子态。两个用户都希望通过 CQ-MA-WTC 尽可能安全地向接收方传输其消息。

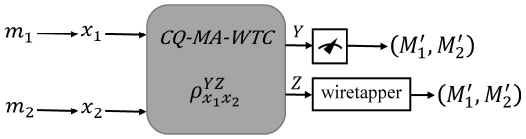


图 1. CQ-MA-WTC模型

主信道如图 1 所示。

考虑图 1 所示的主信道。每个用户从其消息集 $M_i = D1:|M_i| = 2^{R_i}E$ 中选择其消息 m_i; O $\in\{1,2\}$（,₁ 和 ,₂ 分别是对应于第一条和第二条消息的传输速率），并通过 CQ-MA-WTC 发送该消息。用户还分别从两个放大集 $'_i = 31:|'_i| = 2^{\hat{R}_i}]$; O $\in\{1,2\}$ 中选取两个辅助变量 2ᵢ; O $\in\{1,2\}$，以随机化 Eve 所掌握的信息。对于用户 1 和用户 2，我们分别有两个双重索引码本 $A_1(m_1, 2_1)$ 和 $A_2(m_2, 2_2)$。

IV. 主要结果

本节将介绍主要结果。

推论1基于Sen量子联合典型性引理 [14]，给出了通过 CQ-MA-WTC 发送经典消息的单次可达保密速率区域。第二个定理提出了一种新颖的方法，可通过 CQ-MA-WTC 可靠且保密地译出两条消息（同时位置译码器）。值得注意的是，推论1和定理 1 使用相同的方法来证明安全要求。此外，我们还提出了一个定理，尝试克服与定理 1 相关的瓶颈。

推论1：（CQ-MA-WTC 的单次可达速率区域）考虑一个双用户 CQ-MA-WTC，其输入为 X_1 andX_2，输出为 3 和 h。$\rho_{x_1x_2YZ}$ 是信道密度算子。对于任意固定的 $\epsilon \in (0,1)$、$\epsilon' \in (0, \text{‰}')$ 和 ‰、‰′₁，满足 $\text{‰}' > 0$ 时，速率对 μ,₁, ,₂, $49\sqrt{\epsilon} + 20\text{‰}'^{8\cdot}$ 可达到以下不等式：

$$R_1 \le I_H^{\epsilon}(X_1{:}X_2Y|Q)_\rho - I_{max}^{\eta}(X_1{:}Z|Q)_\rho + \log\epsilon - 2 - \log\frac{3}{\epsilon'^3} + \frac{1}{4}\log\delta'$$

$$R_2 \le I_H^{\epsilon}(X_2{:}X_1Y|Q)_\rho - I_{max}^{\eta}(X_2{:}ZX_1|Q)_\rho + \log\epsilon - 2 - \log\frac{3}{\epsilon'^3} + \frac{1}{4}\log\delta' + \mathcal{O}(1)$$

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

其中 1 $= \text{‰}' - \epsilon'$ 并集取遍输入分布 @Q(†)@$_{x_1|}$…(A₁| †)@$_{x_2|}$…(A₂| †)。Q 是时间共享随机变量，所有互信息量均相对于以下状态而言：

$$\rho^{QX_1X_2YZ} \equiv \sum_{q,x_1,x_2} p_Q p(q) p_{X_1|Q}(x_1|q) p_{X_2|Q}(x_2|q) |q\rangle\langle q|^Q \otimes |x_1\rangle\langle x_1|^{X_1} \otimes |x_2\rangle\langle x_2|^{X_2} \otimes \rho^{YZ}_{x_1x_2} \quad (3)$$

证明：见附录A。

证明概要：证明分为两步：1- 基于 Sen 的量子单次联合典型性（定义9）进行可靠解码。2- 基于引理1进行安全解码。

定理 1：（CQ-MA-WTC 的单次下界）对于任意固定的 $\epsilon \in (0,1)$、$\epsilon' \in (0,1)$ 和 ‰，‰′ 使得 $\text{‰} \in (0, 9)$，且 $\text{‰}' \in (0, \epsilon')$，存在一个用于信道₁!$_{x_1x_2\to YZ}$的单次使用码，若速率对 μ,₁，,₂, $\epsilon + 2\text{‰} + 20\text{‰}'^{8\cdot}$ 满足以下界：

$$R_1 \le I_H^{\epsilon}(X_1{:}X_2Y|Q)_\rho - I_{max}^{\eta}(X_1{:}Z|Q)_\rho - \log_2\left(\frac{4\epsilon}{\delta^2}\right) - \log\frac{3}{\epsilon'^3} + \frac{1}{4}\log\delta'$$

$$R_2 \le I_H^{\epsilon}(X_2{:}X_1Y|Q)_\rho - I_{max}^{\eta}(X_2{:}ZX_1|Q)_\rho - \log_2\left(\frac{4\epsilon}{\delta^2}\right) - \log\frac{3}{\epsilon'^3} + \frac{1}{4}\log\delta' + \mathcal{O}(1)$$

$$R_1 + R_2 \le I_H^{\epsilon}(X_1X_2{:}Y|Q)_\rho - I_{max}^{\eta}(X_1{:}Z|Q)_\rho - I_{max}^{\eta}(X_2{:}ZX_1|Q)_\rho - \log_2\left(\frac{4\epsilon}{\delta^2}\right) - 2\log\frac{3}{\epsilon'^3} + \frac{1}{2}\log\delta' + \mathcal{O}(1)$$

其中 1 $= \text{‰}' - \epsilon'$，并且并集取遍输入分布 @Q(†)@$_{x_1|}$…(A₁| †)@$_{x_2|}$…(A₂| †)。Q 是时间共享随机变量，所有互信息量均是相对于状态 (3) 取值的。

证明：见附录 B。

证明概要：证明分为两步：1- 基于同步位置编码技术进行可靠解码：为简化分析，我们将可靠性和保密性判据合并为单一判据 [20]。2- 基于引理1进行安全解码。

注 1：需要注意的是，当且仅当 ‰ $= \epsilon$ 时，上述两个定理趋于相同的结果。

如前所述，同时位置型解码器会转化为一个一般情况下无解的多重假设检验问题。此外，凸分裂引理（引理 2）在同时解码中并无意义，因为它会遇到量子信息论中著名的平滑瓶颈。

现在，考虑图 2 所示的信道。

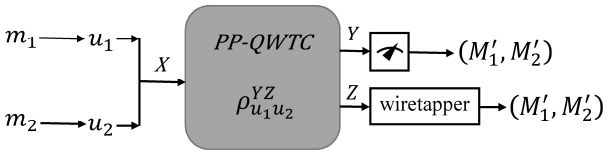


图 2. PP-QWTC 模型。

该信道接受来自一位用户的两条或更多消息。我们将这种信道称为多消息点对点量子窃听信道（PP-QWTC）。

考虑具有经典消息的 PP-QWTC。[27] 在另一种场景下研究了该信道：发送方希望同时向合法接收方发送经典消息和量子消息。

信息处理任务：发送方（Alice）持有两条经典消息 $(m_1, m_2) \in \mathrm{M}_1 \times \mathrm{M}_2$ ，并要在一次性场景下通过点对点量子信道将其发送给接收方（Bob），同时存在一名被动窃听者。这两条消息都应尽可能对窃听者保密。PP-QWTC 是一个三元组 (c, $!^{X\to YZ}$(G1, G2) ≡ $\rho_{x(u_1,\,u2)YZ}$, $\mathrm{H}^Y \otimes \mathrm{H}^Z$)，其中 c 表示输入字母表集合，而 3、h 表示输出系统（3 表示合法接收方（Bob）处的信道输出，h 表示窃听者处的信道输出）。$\rho_{x(u_1,\,u2)YZ} \equiv \rho_{u_1u2YZ}$ 是系统输出的量子态。

Alice 从消息集 M_i = D1: $|\mathrm{M}_i| = 2^{R_i}$E; O ∈{1,2} 中选择消息 m_i; O ∈{1,2}，并通过 PP-QWTC 将其发送出去。Alice 还使用来自两个放大集 $'_i = 31: |'_i| = 2^{\hat{R}_i}]$; O ∈{ 1,2} 的两个辅助变量 2i; O ∈{1,2}，以随机化 Eve 所掌握的信息。我们有两个双重索引码本 G1(m_1, 21) 和 G2(m_2, 22)。

编码：Alice 的编码操作 E: »1»2 →(HA)

$$\forall m_1, m_2 \in M_1, M_2 \quad \frac{1}{2}\left\|\rho_{M_1M_2Z} - \rho_{M_1M_2} \otimes \tilde{\rho}_Z\right\|_1 \le \epsilon_2 \qquad (4)$$

其中，对于每条消息 m_1, m_2, $\rho_{M_1\prime2_2Z}$，以及 $\rho_{M_1\prime2_2}$，它们是状态 $\rho_{M_1\prime2_2YZ}$ =1 | M1|| M2| $\sum \sum_1 |m_1$ $\frac{|\ _1|}{}$ $m_1| \otimes |m_2\ \ m_2| \otimes$ M R Ÿ$ | M2| m2=1!oE(m_1, m_2) q 的适当边缘态。此外，ρ«$_Z$ 可以是任意状态。

解码：Bob 的解码操作 ,: ,(HB) → »3⁄41»3⁄42，使得：

$$pr\left(\left(\hat{M}_1, \hat{M}_2\right) \neq (M_1, M_2)\right) \le \epsilon_1 \qquad (5)$$

如果编码映射和解码映射 (E, ,) 满足 (4) 和 (5) 中所述的条件，则速率对 (,1, ,2) 是 (ϵ_1, ϵ_2)-可达的。

从判据 (4) 可以看出，可靠性和保密性条件被合并为单一判据。这一思想首次用于 [28] 和 [20] 。

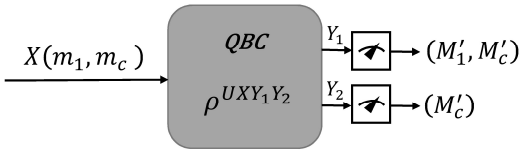


图3。量子广播信道模型。

定理 2：（PP-QWTC 单次使用容量区域的一个内界）对于任意固定的 $\epsilon_1 \in (0,1)$、 $\epsilon_2 \in (0,1)$ 以及 %o01、%o02 ，满足 %o0$_1 \in (0, \epsilon_1)$ 和 %o0$_2 \in (0, \epsilon_2)$，如果速率对 (,1、,2、$3\epsilon_1 + 2\sqrt{\epsilon_1} + 2\sqrt{\epsilon_2}$、$2(\epsilon_1 + \sqrt{\epsilon_1}) + \sqrt{\epsilon_2}$) 满足以下界限，则信道 $!^{X\to YZ}$ 存在一个单次使用码：

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

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

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

Proof: In Appendix C.

注2：定理 2 的证明相比定理 1 的证明有两个优点：首先，定理 2 的证明基于求解一个二元假设检验问题，而定理 1 的证明则基于求解一个多重假设检验问题。其次，在定理 1 的隐私证明中使用了引理 1 [16] 。然而，在定理 2 的证明中可以使用凸分裂引理（引理 2）。

备注 3：比较定理 1 和定理 2 的结果可以看出，定理 3 的证明未能给出和速率 (,1 + ,2)。这是因为使用了逐次解码技术。这个问题不应使人怀疑 PP-QWTC 是否是 CQ-MA-WTC 的对偶。为消除这一疑虑，我们提出量子广播信道这一问题。

量子广播信道

量子广播信道（QBC）接收一个用户和两个或更多接收方。在基本情况下，发送方（Alice）希望传输三条独立的消息：m_1 是发送给第一接收方Y_1的个人消息，m_2 是发送给第二接收方Y_2的个人消息，而m_c 是发送给两位接收方的公共消息。

基本的量子广播信道如图3所示。需要注意的是，为便于计算，我们从问题中移除了安全约束。

$$\rho_{X_1X_1'X_1''} \equiv \sum_{x_1} p_{X_1}(x_1)|x_1\rangle\langle x_1|_{X_1} \otimes |x_1\rangle\langle x_1|_{X_1'} \otimes |x_1\rangle\langle x_1|_{X_1''} \tag{6}$$

$$\sigma_{X_2X_2'X_2''} \equiv \sum_{x_2} p_{X_2}(x_2)|x_2\rangle\langle x_2|_{X_2} \otimes |x_2\rangle\langle x_2|_{X_2'} \otimes |x_2\rangle\langle x_2|_{X_2''} \tag{7}$$

$$\rho_{X_1X_1''YZ} \equiv \sum_{x_1} p_{X_1}(x_1)|x_1\rangle\langle x_1|_{X_1} \otimes \rho_{YZ}^{x_1x_2} \otimes |x_1\rangle\langle x_1|_{X_1''} \tag{8}$$

$$\sigma_{X_2X_2''YZ} \equiv \sum_{x_2} p_{X_2}(x_2)|x_2\rangle\langle x_2|_{X_2} \otimes \rho_{YZ}^{x_1x_2} \otimes |x_2\rangle\langle x_2|_{X_2''} \tag{9}$$

$$\rho_{X_1x_2\epsilon 7\mathrm{d}} \equiv \mathcal{N}_{X_1'X_2'\to YZ}\mu\rho_{X_1X_1''YZ} \otimes \sigma_{X_2X_2''YZ} \cdot = ? \quad \underset{\mathrm{B}_1\mathrm{B}\epsilon}{p_{X_1}(x_1)p_{X_2}(x_2)}\,|x_1\rangle\langle x_1|_{X_1} \otimes |x_2\rangle\langle x_2|_{X_2} \otimes \rho_{YZ}^{\mathrm{B}_1\mathrm{B}\epsilon} \tag{10}$$

$$\frac{1}{|\mathcal{M}_1||\mathcal{M}_2|}\sum_{m_2=1}^{|\mathcal{M}_2|}\sum_{m_1=1}^{|\mathcal{M}_1|}\frac{1}{2}\left\|\mathcal{D}_{Y\to\hat{M}_1\hat{M}_2}\left(\rho_{(X_1X_1'')^{\otimes|\mathcal{M}_1||\mathcal{K}_1|}(X_2X_2'')^{\otimes|\mathcal{M}_2||\mathcal{K}_2|}YZ}^{(m_1,k_1),(m_2,k_2)} - \left(|m_1\rangle\langle m_1|_{\hat{M}_1} \otimes |m_2\rangle\langle m_2|_{\hat{M}_2}\right)\right.\right.$$
$$\left.\left. \otimes \hat{\rho}_{X_1''^{\otimes|\mathcal{M}_1||\mathcal{K}_1|}X_2''^{\otimes|\mathcal{M}_2||\mathcal{K}_2|}Z}\right)\right\|_1 \leq \epsilon + 2\delta + 20\delta'^{\frac{1}{8}} \tag{11}$$

其中 $\rho Æ_{X_1''^{\otimes|\mathcal{M}_1||\mathcal{K}_1|}X_{2,,\otimes|\,\mathrm{M}\epsilon||\,\mathcal{K}2|\,Z} \coloneqq \rho_{X_1''^{\otimes|}{}_{\mathrm{M}_1||\,\mathcal{K}_1|}{}_{X^2,,\otimes|\,\mathrm{M}\epsilon||\,\mathcal{K}2|}}$

$_{(m_1,k_1),(m2,k2)} \otimes \rho\text{«}_Z$。

$$\mathcal{D}_{Y\to\hat{M}_1\hat{M}_2}\left(\rho_{X_1^{\otimes|\mathcal{M}_1||\mathcal{K}_1|}X_2^{\otimes|\mathcal{M}_2||\mathcal{K}_2|}Y}^{(m_1,k_1),(m_2,k_2)}\right) \coloneqq \sum_{m_2=1}^{|\mathcal{M}_2|}\sum_{m_1=1}^{|\mathcal{M}_1|} p_{\hat{M}_1}(m_1)p_{\hat{M}_1}(m_1)|m_1\rangle\langle m_1|_{\hat{M}_1} \otimes |m_2\rangle\langle m_2|_{\hat{M}_2}$$
$$= \sum_{m_2=1}^{|\mathcal{M}_2|}\sum_{m_1=1}^{|\mathcal{M}_1|} Tr\left\{\Lambda_{X_1^{\otimes|\mathcal{M}_1||\mathcal{K}_1|}X_2^{\otimes|\mathcal{M}_2||\mathcal{K}_2|}Y}^{m_1m_2}\rho_{X_1^{\otimes|\mathcal{M}_1||\mathcal{K}_1|}X_2^{\otimes|\mathcal{M}_2||\mathcal{K}_2|}Y}^{m_1m_2k_1k_2}\right\}|m_1\rangle\langle m_1|_{\hat{M}_1} \otimes |m_2\rangle\langle m_2|_{\hat{M}_2} \tag{12}$$

QBC 的问题在独立同分布情形下于[2-3] 中得到了广泛研究，在一次性情形下则于 [29] 中进行了研究。下面，我们希望为带有经典消息的 QBC 实现一个单次内界。假设 Alice 没有要发送给第二接收方的个人消息 Y_2 $(m_2 = \emptyset \to ,_2 = 0)$。

一次性设置下的 QBC 是一个三元组（c，$!^{\mathcal{X}\to Y_1Y_2}$ $\equiv \rho_x^{Y_1Y_2}$，$\mathrm{H}^{Y_1} \otimes \mathrm{H}^{Y_2}$），其中 c 表示输入字母表集合，而 Y_1、Y_2 表示输出系统。$\rho_x^{Y_1Y_2}$ 是系统输出的量子态。

定理 3：（QBC 的单次内界）设 À 为辅助随机变量，@ = @$_{X|U}$(A| G)@$_U$(G) 为码概率函数。单次可达速率由所有满足以下条件的速率对（,1，,$_c$）组成：

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

是可达的，并且所有信息量均取自以下状态：

$$\rho_{UXY_1Y_2} = \sum_{u,x} p_U(u)p_{X|U}(x|u)\,|u\rangle\langle u|_U \otimes |x\rangle\langle x|_X \otimes \rho_x^{Y_1Y_2} \tag{13}$$

证明：见附录D。

现在，考虑上述定理的扩展版本：

推论 2：（第一接收方具有三个私人消息的 QBC 的单次内界）设 À 为辅助随机变量，@ = @$_U$(G)@$_{X_1|\,U}$(A$_1$| G)@$_{X_2|\,UX_1}$(A$_2$| GA$_1$) 为码概率函数。单次可达速率区域由所有速率元组（,1，,$_c$，,$_2$）组成，用于发送（m_1，m_2，m_c），且满足：

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

是可实现的，且所有信息量均是针对以下状态而言：

$$\rho_{UX_1X_2Y_1Y_2} = \sum_{u,x} p_U(u)p_{X_1|U}(x_1|u)\,p_{X_2|UX_1}(x_2|ux_1)|u\rangle\langle u|_U$$
$$\otimes |x_1\rangle\langle x_1|_{X_1} \otimes |x_2\rangle\langle x_2|_{X_2} \otimes \rho_{X_1X_2}^{Y_1Y_2}$$

$\Lambda_{X_1^{\otimes|\mathcal{M}_1||\mathcal{K}_1|}X_{€^{\otimes|}\,\mathrm{M}€||\,'€|_Y}(\mathrm{R}_1,§_1),}$

$(\mathrm{R}€,§€)$

$$\coloneqq \left(\sum_{m_2'}\sum_{m_1'}\sum_{k_2'}\sum_{k_1'}\Gamma^{\mathrm{R}_1',§_1',m_2',k_2'}_{X_1^{|\mathrm{M}_1||\,'_1|}\,X_2^{|\mathrm{M}€||\,'€|}\,Y}\right)^{-\frac{1}{2}}\Gamma^{\mathrm{R}_1,§_1,\mathrm{R}€,§€}_{X_1^{|\mathrm{M}_1||\,'_1|}\,X_2^{|\mathrm{M}€||\,'€|}\,Y}\left(\sum_{m_2'}\sum_{m_1'}\sum_{k_2'}\sum_{k_1'}\Gamma^{\mathrm{R}_1',§_1',m_2',k_2'}_{X_1^{|\mathrm{M}_1||\,'_1|}\,X_2^{|\mathrm{M}€||\,'€|}\,Y}\right)^{-\frac{1}{2}} \tag{14}$$

$\Gamma^{\mathrm{R}_1,\ §_1,\ \mathrm{R}€,\ §\ 2}_{X_1^{|\,\mathrm{M}_1||\,'_1|}\,X_2^{|\mathcal{M}_2||\mathcal{K}_2|}Y}$

$$\begin{aligned}&\coloneqq I_{X_1X_2}^{(1,1),(1,1)}\otimes\ldots\otimes I_{X_1X_2}^{(1,1),(1,k_2)}\otimes\ldots\otimes I_{X_1X_2}^{(1,1),(m_2,k_2-1)}\otimes\ldots\otimes I_{X_1X_2}^{(1,k_1),(m_2,k_2)}\otimes\ldots\otimes I_{X_1X_2}^{(m_1,k_1-1),(m_2,k_2)}\\&\otimes T_{X_1X_2Y}^{(m_1,k_1),(m_2,k_2)}\otimes I_{X_1X_2}^{(m_1,k_1),(m_2,k_2+1)}\otimes\ldots\otimes I_{X_1X_2}^{(|\mathcal{M}_1|,|\mathcal{K}_1|),(|\mathcal{M}_2|,|\mathcal{K}_2|)}\end{aligned} \tag{15}$$

$$Tr\left\{\left(I-\Gamma^{m_1,k_1,m_2,k_2}_{X_1^{|\mathcal{M}_1||\mathcal{K}_1|}X_2^{|\mathcal{M}_2||\mathcal{K}_2|}Y}\right)\rho^{m_1m_2k_1k_2}_{X_1^{\otimes|\mathcal{M}_1||\mathcal{K}_1|}X_2^{\otimes|\mathcal{M}_2||\mathcal{K}_2|}Y}\right\}=Tr\left\{\left(I-T_{X_1X_2Y}\right)\mathcal{N}_{X_1'X_2'\to YZ}\left(\rho_{X_1X_2'}\otimes\sigma_{X_1X_2'}\right)\right\} \tag{16}$$

$$\begin{aligned}&Pr\left(\left(\widehat{M}_1,\widehat{M}_2\right)\neq(M_1,M_2)\right)\\&\leq(1+c)Tr\left\{\left(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}\right)\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}\right\}\\&+(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}Tr\left\{\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}\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}\right\}\\&=(1+c)Tr\left\{\left(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}\right)\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}\right\}\\&+(2+c+c^{-1})\sum_{m_1'\neq m_1}\sum_{k_1'\neq k_1}Tr\left\{\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}\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}\right\}\\&+(2+c+c^{-1})\sum_{m_2'\neq m_2}\sum_{k_2'\neq k_2}Tr\left\{\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}\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}\right\}\\&+(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}Tr\left\{\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}\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}\right\}\\&=(1+c)Tr\left\{\left(I-T_{X_1X_2Y}\right)\mathcal{N}_{X_1'X_2'\to YZ}\left(\rho_{X_1X_2'}\otimes\sigma_{X_1X_2'}\right)\right\}\\&+(2+c+c^{-1})(|\mathcal{M}_1||\mathcal{K}_1|-1)Tr\left\{\left(I-T_{X_1X_2Y}\right)\mathcal{N}_{X_1'X_2'\to YZ}\left(\rho_{X_1}\otimes\rho_{X_2'}\otimes\sigma_{X_1X_2'}\right)\right\}\\&+(2+c+c^{-1})(|\mathcal{M}_2||\mathcal{K}_2|-1)Tr\left\{\left(I-T_{X_1X_2Y}\right)\mathcal{N}_{X_1'X_2'\to YZ}\left(\rho_{X_1X_2'}\otimes\sigma_{X_1}\otimes\sigma_{X_2'}\right)\right\}\\&+(2+c+c^{-1})(|\mathcal{M}_1||\mathcal{K}_1|-1)(|\mathcal{M}_2||\mathcal{K}_2|\\&-1)Tr\left\{\left(I-T_{X_1X_2Y}\right)\mathcal{N}_{X_1'X_2'\to YZ}\left(\rho_{X_1}\otimes\rho_{X_2'}\otimes\sigma_{X_1}\otimes\sigma_{X_2'}\right)\right\}\end{aligned} \tag{17}$$

证明：证明过程沿用定理 3 证明的扩展版本。

通过选择 $m_c=\emptyset$，推论 2 中描述的信道将转换为定理 2 （PP-QWTC）中描述的不带保密约束的信道。在推论 2 中设置 $,_c=0$ ：

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

其中，上述最后两个速率是冗余的。因此，我们得到以下区域：

$$R_1\leq I_H^{\epsilon}(X_1;Y_1)_{\rho}-2+\log\epsilon$$

$$\begin{aligned}R_2&\leq I_H^{\epsilon}(X_2;Y_1|X_1)_{\rho}-2+\log\epsilon\\R_1+R_2&\leq I_H^{\epsilon}(X_1X_2;Y_1)_{\rho}-2+\log\epsilon\end{aligned} \tag{18}$$

考虑不含泄露信息项的定理 2 结果。通过选择 $\%o_2=\epsilon_2$，我们有：

$$\begin{aligned}R_1&\leq I_H^{\epsilon}(X_1;Y_1|X_2)_{\rho}-2+\log\epsilon_1\\R_2&\leq I_H^{\epsilon}(X_2;Y_1|X_1)_{\rho}-2+\log\epsilon_1\end{aligned} \tag{19}$$

通过比较 (18)、(19) 和 (33)，备注 3 中陈述的论证得以证明。此外，与推论1相比，区域 (18) 是一个近乎最优的可达速率区域。通过考虑 (31) 并比较推论1、定理 2 和推论 2 的结果可以看出，将 CQ-MA-WTC 转换为 PP-QWTC 可能是一种有用的方法，能够绕过与多重假设检验问题（定理 1）以及量子信息论中的平滑瓶颈（推论1和定理 1）相关的瓶颈。

渐近分析

在本小节中，我们希望评估渐近独立同分布情形下的保密速率区域（即多次使用无记忆信道时的渐近极限）。考虑 PP-QWTC ($A(G_1,G_2)\to\rho_x^{YZ}$)。该信道的容量区域可表示如下：

$$\mathcal{C}_\infty(\mathcal{N}) \coloneqq \lim_{\epsilon_1,\epsilon_2\to 0}\lim_{n\to\infty}\frac{1}{n}\mathcal{C}^{\epsilon_1,\epsilon_2}(\mathcal{N}^{\otimes n}) \tag{20}$$

其中 $\mathcal{C}^{\epsilon_1,1\epsilon}(\mathcal{N}^{\otimes n})\equiv$ 最大 $\mathrm{R}^{\epsilon_1,1\epsilon}(\mathcal{N}^{\otimes n})$。n(m1,mϵ)

令 R(!) 表示最大速率对 (,′1, ,′2) 的集合，

$$\mathcal{R}(\mathcal{N}) = \begin{cases} R_1' \le I(U_1;Y|U_2)_\rho - I(U_1;Z)_\rho \\ R_2' \le I(U_2;Y|U_1)_\rho - I(U_2;Z|U_1)_\rho \end{cases} \tag{21}$$

那么，容量区域 Ò∝(!) 是对信道 ! 使用 u 次所得结果的并集：

$$\mathcal{C}_\infty(\mathcal{N}) \coloneqq \max_{p(u_1,u_2)}\frac{1}{n}\bigcup_{n=1}^{\infty}\mathcal{R}(\mathcal{N}^{\otimes n}) \tag{22}$$

我们的目标是证明上述表达式。考虑两个单独的速率。应用事实 2（及其条件版本），可得，

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

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

为证明可达性，考虑定理 2 中给出的单次下界，并应用条件平滑假设检验和最大互信息的量子渐近等分性质 [30] 。根据定理 2，对于信道 ! 的 r 次使用，可以得到以下下界 Ò$^{\epsilon_1,\epsilon_2}$(! $^{\otimes n}$)：

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

其中，R(!$^{\otimes n}$) 是满足以下条件的所有速率对 (,′1, ,′2) 的集合：

$$R_1' \le I_H^{\epsilon_1-\delta_1}(U_1^n;Y^{\otimes n}|U_2^n)_\rho - I_{max}^{\sqrt{\epsilon_2}-\delta_2-\gamma}(U_1^n;Z^{\otimes n})_\rho - \log\frac{4\epsilon_1}{\delta_1^2} - 2\log\frac{1}{\delta_2} - \log\frac{3}{\gamma^2} \tag{23}$$

$$R_2' \le I_H^{\epsilon_1-\delta_1}(U_2^n;Y^{\otimes n}|U_1^n)_\rho - I_{max}^{\sqrt{\epsilon_2}-\delta_2-\gamma}(U_2^n;Z^{\otimes n}|U_1^n)_\rho - \log\frac{4\epsilon_1}{\delta_1^2} - 2\log\frac{1}{\delta_2} - \log\frac{3}{\gamma^2} \tag{24}$$

我们可以假设这些随机变量的序列是按照其分布以独立同分布的方式生成的。这是因为上述区域基本上是容量区域的一个下界。这使我们能够运用下文所述的量子渐近等分性质。根据事实 3，我们有：

$$\lim_{\epsilon_1\to 0}\lim_{r\to\infty}\frac{1}{r}I_H^{\epsilon_1-\delta_1}(U_1^r;Y^{\otimes r}|U_2^r)_{\rho^{\otimes r}} = I(U_1;Y|U_2)_\rho \tag{25}$$

$$\lim_{\epsilon_1\to 0}\lim_{r\to\infty}\frac{1}{r}I_H^{\epsilon_1-\delta_1}(U_2^r;Y^{\otimes r}|U_1^r)_{\rho^{\otimes r}} = I(U_2;Y|U_1)_\rho \tag{26}$$

此外，根据事实 4，我们有：

$$\lim_{\epsilon_2\to 0}\lim_{r\to\infty}\frac{1}{r}I_{max}^{\sqrt{\epsilon_2}-\delta_2-\gamma}(U_1^r;Z^{\otimes r})_{\rho^{\otimes r}} = I(U_1;Z|U_2)_\rho \tag{27}$$

$$\lim_{\epsilon_2\to 0}\lim_{r\to\infty}\frac{1}{r}I_{max}^{\sqrt{\epsilon_2}-\delta_2-\gamma}(U_2^r;Z^{\otimes r}|U_1^r)_{\rho^{\otimes r}} = I(U_2;Z|U_1)_\rho \tag{28}$$

将 (25)、(26)、(27) 和 (28) 代入 (23) 和 (24)，即可得到 (21)：

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

结合上述论证并利用 (20) 和 (22)，即可完成证明。

V. 讨论

本文研究了在 CQ-MA-WTC 上进行安全通信的问题，并采用了三种技术：1-Sen 联合典型性引理；2-同时位置型解码；3-逐次位置型解码。前两种解码技术采用一种新引入的平滑技术 [16] 来分析隐私，而第三种技术则采用凸分裂 [19] 。我们发现，同时位置型译码器会转化为一个在一般情况下无解的多重假设检验问题。我们引入了一种新的信道（PP-QWTC），可将其视为 CQ-MA-WTC 的对偶。此外，这种信道也可以由量子广播信道导出。结果表明，PP-QWTC 的可达速率区域与 CQ-MA-WTC 的可达速率区域近乎最优。

附录

附录A：（推论1的证明）

如前所述，证明分为两个步骤：可靠解码和安全解码。为此，考虑两个辅助变量

2_i; O $\in\{1,2\}$，针对每个用户 m, O $\in\{1,2\}$。这些辅助变量用于构造两个双重索引码本 $\{A_1(m,2_1)\}_{m_1\in M_1,k_1\in\mathcal{K}_1}$ 和 $\{A_2(m_2,2_2)\}_{m2\in M_2,k2\in\mathcal{K}_2}$。Bob 应能以较高概率检测出消息对 (m, m_2) 以及辅助变量 2_1 和 2_2 。

根据定义10（Sen 的量子多址信道内界），有如下关系：

$$\mathcal{R}_{priv-QMA-WTC} = \mathcal{R}_{Sen} - \mathcal{R}_{leaked}$$

解码错误至多为 $49\sqrt{\epsilon}$，隐私泄露至多为120‰′8 （引理1）。此外，R_{Sen} 表示 Sen 的量子多址信道内界（定义9），而 R_{leaked} 表示发送方泄露给 Eve 的信息。

由引理1可得：

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

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

证明至此完成。

附录 B：（定理 1 的证明）

两条消息均在各自的集合上服从均匀分布。接收方必须能够以可忽略的错误概率解码两条消息。通信开始前，Alice (A) 和 Bob (B) 与 Charlie (C) 以及窃听者 (Z) 共享随机性。设 $\rho_{X_1X_1'X_1''}$ (6) 和 $\sigma_{X_2X_2'X_{2''}}$ (7) 分别表示 (A,C,Z) 之间的共享随机性以及 (B,C,Z) 之间的共享随机性。Alice 持有 X_1' system，Bob 持有 X_2' system，Charlie 持有 (X_1, X_2) system，窃听者持有 (X_1'', X_2'') system。令 $\rho_{X_1X_1''YZ}$ (8) 和 $\sigma_{X_2X_2''YZ}$ (9) 分别表示将 X_1' 和 X_2' 通过信道发送后得到的状态。那么，该信道的整体控制态如式 (10) 所示。

编码方案概述：对于每条消息 (m_i)，O ∈{1,2}，均存在本地密钥 2_i ∈D1: | ‘$_i$| E，O ∈{1,2}，作为均匀随机性，用于随机化 Eve 对已发送消息的了解。这些本地密钥 Charlie 和 Eve 均无法获取。在通信开始前，假设 Alice、Charlie 和 Eve 共享 | M_1|| ‘$_1$| 份状态 (6)，而 Bob、Charlie 和 Eve 共享 | M_2|| ‘$_2$| 份状态 (7)：

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

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

为发送消息对 m_1 和 m_2，Alice 和 Bob 分别随机且均匀地选取 2_1∈D1: | ‘$_1$| E 和 2_2 ∈D1: | ‘$_2$| E。他们分别通过信道 $!x_1'x_2'\to_{YZ}$ 发送第 $(m_1, 2_1)$- 个系统 $2_{1'}$ 和第 $(m_2, 2_2)$ 个系统 $X_{2'}$。

存在一种用于 CQ-MA-WTC 通信的同时解码器，其平均错误概率上界如式 (11) 所示。从式 (11) 可以看出，安全性准则已并入可靠性准则 [20] 。同时位置型解码器可按式 (12) 所述构造，其中，

$$\Lambda_{X_1^{\otimes|\mathcal{M}_1||\mathcal{K}_1|}X_2^{\otimes|\mathcal{M}_2||\mathcal{K}_2|}Y}^{m_1m_2} = \sum_{k_2=1}^{|\mathcal{K}_2|}\sum_{k_1=1}^{|\mathcal{K}_1|}\Lambda_{X_1^{\otimes|\mathcal{M}_1||\mathcal{K}_1|}X_2^{\otimes|\mathcal{M}_2||\mathcal{K}_2|}Y}^{(m_1,k_1),(m_2,k_2)}$$

现在，我们来考虑误差项。Charlie 构造她的位置型解码器，以解码 m_1, m_2, 2_1 和 2_2。令 $\Lambda_{X_1^{\otimes|\mathcal{M}_1||\mathcal{K}_1|}X_{2^{\otimes|}\mathrm{M}\epsilon||\mathcal{K}_2|_Y}^{(m_1,k_1),(m_2,k_2)}$ 表示如下正算子值测度：

$$Tr\left\{\left(I_{X_1^{|\mathcal{M}_1||\mathcal{K}_1|}X_2^{|\mathcal{M}_2||\mathcal{K}_2|}Y} - \Lambda_{X_1^{\otimes|\mathcal{M}_1||\mathcal{K}_1|}X_2^{\otimes|\mathcal{M}_2||\mathcal{K}_2|}Y}^{(m_1,k_1),(m_2,k_2)}\right)\rho_{X_1^{\otimes|\mathcal{M}_1||\mathcal{K}_1|}X_2^{\otimes|\mathcal{M}_2||\mathcal{K}_2|}Y}^{m_1m_2k_1k_2}\right\} \leq \epsilon$$

其中，$\Lambda_{X_1^{\otimes|\mathcal{M}_1||\mathcal{K}_1|}X\epsilon_{\otimes|}\mathrm{M}\epsilon||\,`\epsilon|_Y}(\mathrm{R}_1,\S_1),(\mathrm{R}\epsilon,\S\epsilon)$ 在式 (14) 中给出；对于 m_i ∈ D1: | M_i| E 和 2_i ∈ D1: | ‘$_i$| E，$\Gamma_{X_1^{|\mathcal{M}_1||\mathcal{K}_1|}X\epsilon|}^{m_1,k_1,m_2,k_2}$ M€|| ‘€|$_Y$R$_1$,§$_1$,R€,§€ 在式 (15) 中给出，其中 $T_{X_1X\epsilon Y}(\mathrm{R}_1,\S_1,\mathrm{R}\epsilon,\S\epsilon)$ 是一个检验算子，用于以 9 的误差区分假设 $\rho_{X_1X\epsilon Y}$, $\rho_{X_1X\epsilon}\otimes\rho_Y, \rho_{X_1}\otimes\rho_{X_2Y}$ 和 $\rho_{X_1}\otimes\rho_{X_2}\otimes\rho_Y$ 。注意，这个假设检验问题等价于区分假设 $!x_1'x\epsilon'\to_Y d\mu\rho_{X_1X\epsilon}\otimes\sigma_{X_1X\epsilon}$, $!x_1'x\epsilon'\to_Y d\mu\rho_{X_1X\epsilon}\otimes\sigma_{X_1}\otimes\sigma_{X_2'}$, $!x_1'x\epsilon'\to_Y d\mu\rho_{X_1}\otimes\rho_{X_2'}\otimes\sigma_{X_1X\epsilon}$ 和 $!x_1'x\epsilon'\to_Y d\mu\rho_{X_1}\otimes\rho_{X_2'}\otimes\sigma_{X_1}\otimes\sigma_{X_2'}$。因此，如果实际发送的是消息对 (m_1, m_2)，而 Charlie 检查消息对 (m_1, m_2)，那么错误解码概率如式 (16) 所述。

类似地，还可以考虑其他类型的错误概率：

- 如果 Charlie 在消息对 (m_1', m_2) 确实已传输时，检查消息对 (m_1, m_2)，那么错误解码概率为：

$$Tr\left\{\left(I - \Gamma_{X_1^{|\mathcal{M}_1||\mathcal{K}_1|}X_2^{|\mathcal{M}_2||\mathcal{K}_2|}Y}^{m_1',k_1,m_2,k_2}\right)\rho_{X_1^{\otimes|\mathcal{M}_1||\mathcal{K}_1|}X_2^{\otimes|\mathcal{M}_2||\mathcal{K}_2|}Y}^{m_1m_2k_1k_2}\right\} = Tr\left\{\left(I - T_{X_1X_2Y}\right)\mathcal{N}_{X_1'X_2'\to YZ}\left(\rho_{X_1}\otimes\rho_{X_2'}\otimes\sigma_{X_1X_2'}\right)\right\} \quad (29)$$

- 如果 Charlie 在消息对 (m_1, m_2') 确实已传输时，检查消息对 (m_1, m_2)，那么错误解码概率为：

$$Tr\left\{\left(I - \Gamma_{X_1^{|\mathcal{M}_1||\mathcal{K}_1|}X_2^{|\mathcal{M}_2||\mathcal{K}_2|}Y}^{m_1,k_1,m_2',k_2}\right)\rho_{X_1^{\otimes|\mathcal{M}_1||\mathcal{K}_1|}X_2^{\otimes|\mathcal{M}_2||\mathcal{K}_2|}Y}^{m_1m_2k_1k_2}\right\} = Tr\left\{\left(I - T_{X_1X_2Y}\right)\mathcal{N}_{X_1'X_2'\to YZ}\left(\rho_{X_1X_2'}\otimes\sigma_{X_1}\otimes\sigma_{X_2'}\right)\right\} \quad (30)$$

- 如果 Charlie 在消息对 (m_1', m_2') 确实已传输时，检查消息对 (m_1, m_2)，那么错误解码概率为：

$$Tr\left\{\left(I - \Gamma_{X_1^{|\mathcal{M}_1||\mathcal{K}_1|}X_2^{|\mathcal{M}_2||\mathcal{K}_2|}Y}^{m_1',k_1,m_2',k_2}\right)\rho_{X_1^{\otimes|\mathcal{M}_1||\mathcal{K}_1|}X_2^{\otimes|\mathcal{M}_2||\mathcal{K}_2|}Y}^{m_1m_2k_1k_2}\right\} = Tr\left\{\left(I - T_{X_1X_2Y}\right)\mathcal{N}_{X_1'X_2'\to YZ}\left(\rho_{X_1}\otimes\rho_{X_2'}\otimes\sigma_{X_1}\otimes\sigma_{X_2'}\right)\right\} \quad (31)$$

由于编码构造，在基于位置的编码方案下，每个消息对 (m_1, m_2) 的错误概率都相同：

$$Pr\left(\left(\widehat{M}_1, \widehat{M}_2\right) \neq (M_1, M_2)\right) = Tr\left\{\left(I - \Lambda_{X_1^{\otimes|\mathcal{M}_1||\mathcal{K}_1|}X_2^{\otimes|\mathcal{M}_2||\mathcal{K}_2|}Y}^{(m_1,k_1),(m_2,k_2)}\right)\rho_{X_1^{\otimes|\mathcal{M}_1||\mathcal{K}_1|}X_2^{\otimes|\mathcal{M}_2||\mathcal{K}_2|}Y}^{m_1m_2k_1k_2}\right\}$$

Applying Lemma 3 with $S = \Gamma_{X_1^{|\mathcal{M}_1||\mathcal{K}_1|}X_2^{|\mathcal{M}_2||\mathcal{K}_2|}Y}^{m_1,k_1,m_2,k_2}$ and $T = \sum_{m_2'\neq m_2}\sum_{m_1'\neq m_1}\sum_{k_2'\neq k_2}\sum_{k_1'\neq k_1}\Gamma_{X_1^{|\mathcal{M}_1||\mathcal{K}_1|}X_2^{|\mathcal{M}_2||\mathcal{K}_2|}Y}^{m_1',k_1',m_2',k_2'}$, we have a

如式 (17) 所示的一系列等式和不等式。注意，我们使用了 (29)-(31)。

多重量子假设检验：如前所述，在独立同分布情形下，针对一般 QMAC（用户数超过两个）是否存在同时解码器，仍是一个悬而未决的问题。在 [17]，中，作者对多重量子假设检验及其与量子多址信道的关系进行了有益的讨论。总而言之，多重假设检验问题同样尚未解决。假设检验有两种可能的方案：对称和非对称。对称假设检验中的切尔诺夫距离给出了随机辅助误差指数 [31] 的下界；相比之下，应用非对称假设检验的结果，可以得到一次性随机辅助容量（针对不带保密约束的 QMAC）的下界，进而得到随机辅助通信二阶编码率的下界。

换言之，由 [7]，可知，在输出的可交换版本情形下，存在一个一般的同时解码器，能够同时译码两个以上的消息；由 [17]，可知，如果复合备择假设构成一个可交换算子集，则多重假设检验问题可以得到解决。这意味着，对于检验算子 T，一个由半正定算子构成的有限集合 à ≡{à$_i$: $1 \le$ O $\le r$}，其中 FG@@(ρ) ⊆ FG@@(à$_i$) 且 min$_i$ D(ρ‖ à$_i$)> 0，存在两个假设，并且有：

$$Tr\{(I-T)\rho\} \le \epsilon \tag{32}$$

$$-\log_2 Tr\{T\theta_i\} \ge \left[\min_i D(\rho\|\theta_i)\right] - \delta \tag{33}$$

其中 ‰ 为正整数。

当集合 à 构成一个可交换算子集时，最后一个不等式成立。更多信息请参见 [17] 。

基于上述说明，我们对该问题采用非对称假设检验。注意，我们希望同时解码两条消息。考虑式 (17) 中错误概率的上界。于是，我们将其改写如下：

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

其中，

$$\mu = \mathcal{N}_{X_1'X_2'\to YZ}\left(\rho_{X_1X_2'} \otimes \sigma_{X_1X_2'}\right)$$

$$\theta_1 = \mathcal{N}_{X_1'X_2'\to YZ}\left(\rho_{X_1} \otimes \rho_{X_2'} \otimes \sigma_{X_1X_2'}\right)$$

$$\theta_2 = \mathcal{N}_{X_1'X_2'\to YZ}\left(\rho_{X_1X_2'} \otimes \sigma_{X_1} \otimes \sigma_{X_2'}\right)$$

$$\theta_3 = \mathcal{N}_{X_1'X_2'\to YZ}\left(\rho_{X_1} \otimes \rho_{X_2'} \otimes \sigma_{X_1} \otimes \sigma_{X_2'}\right)$$

这称为非对称假设检验，其目标是在满足对错误概率 $Tr\{(I-T)$ã$\}$ 的约束下，最小化所有其他概率。请注意，我们将这三个假设（à$_1$ + à$_2$ + à$_3$）视为一个唯一的复合备择假设。

如式 (32) 和 (33) 所述，对于这样一组检验算子，我们可以将上述多重假设检验问题表示为：

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

令 |‘$_1$| = $2^{\hat{R}_1}$ 和 |‘$_2$| = $2^{\hat{R}_2}$。然后，将上述项设为 9，并经过简单化简，可得：

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

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

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

上述表达式关于 ® 的全局最大值在 ® $= \frac{\delta}{\epsilon}$ 处取得：

$$R_1 + \hat{R}_1 = I_H^\epsilon(X_1:X_2Y) - \log_2\left(\frac{4\epsilon}{\delta^2}\right) \tag{34}$$

$$R_2 + \hat{R}_2 = I_H^\epsilon(X_2:X_1Y) - \log_2\left(\frac{4\epsilon}{\delta^2}\right) \tag{35}$$

$$R_1 + \hat{R}_1 + R_2 + \hat{R}_2 = I_H^\epsilon(X_1X_2:Y) - \log_2\left(\frac{4\epsilon}{\delta^2}\right) \tag{36}$$

对于这样的 ®，有：

$$Pr\left((\widehat{M}_1,\widehat{M}_2) \neq (M_1,M_2)\right) \le \epsilon + 2\delta \tag{37}$$

现在，我们转而关注保密性判据。利用引理1，可得：

$$\hat{R}_1 \le I_{max}^{\delta'-\epsilon'}(X_1:Z)_\rho + \log\frac{3}{\epsilon'^3} - \frac{1}{4}\log\delta' \tag{38}$$

$$\hat{R}_2 \le I_{max}^{\delta'-\epsilon'}(X_2:ZX_1)_\rho + \log\frac{3}{\epsilon'^3} - \frac{1}{4}\log\delta' + \mathcal{O}(1) \tag{39}$$

将 (38) 和 (39) 代入 (34)-(36)，即可完成证明。

附录 C：（定理 2 的证明）

该证明使用两个连续的基于位置的译码器。第一解码器尝试解码第一条消息 m_1，而

第二解码器尝试在已正确解码 m_1 的条件下解码第二条消息 m_2 。这意味着，如果第一解码器解码失败，第二解码器也会失败。该解码顺序可表示为 $m_1 \to m_2$。

第一个位置型解码器的构造方式与 [20] 中所述的相同。为了对 m_2 进行解码，Bob 在 À₁ 条件下执行他的第二个位置型解码器，该解码器对所有 $G_1 \in$Â₁ 均有效。需要注意的是，第二解码器的输入状态不同于信道的主状态。

Alice、Bob 和 Eve 可以预先共享某个量子态作为随机性。此外，Alice 还可以使用两个来源的均匀无用随机性 $2i$;O $\in \{1,2\}$。预共享随机性如下：

$$\rho_{X_1X_1'(AX_2X_2')^{\otimes|\mathcal{M}_2||\mathcal{K}_2|}}^{\otimes|\mathcal{M}_1||\mathcal{K}_1|} \coloneqq \left[\sum_{x_1} p(x_1)|x_1\rangle\langle x_1|_{X_1} \otimes |x_1\rangle\langle x_1|_{X_1'} \left(\sum_{x_2} p(x_2)|x_2\rangle\langle x_2|_{X_2} \otimes |x_2\rangle\langle x_2|_{X_2'}\right)^{\otimes|\mathcal{M}_2||\mathcal{K}_2|}\right]^{\otimes|\mathcal{M}_1||\mathcal{K}_1|} \tag{40}$$

与 m_1 的解码过程相关的论证如下：

- 对 m_1 进行解码时的错误概率：

$$p_{e_1} = p\{\widehat{M}_1 \neq M_1\} \coloneqq \frac{1}{|\mathcal{M}_1|}\sum_{m_1=1}^{|\mathcal{M}_1|}\frac{1}{2}\left\|\mathcal{D}_{YX_1\to\widehat{M}_1}^{m_1}\left(\rho_{X_1^{\otimes|\mathcal{M}_1||\mathcal{K}_1|}Y}^{(m_1,k_1),(m_2,k_2)}\right) - |m_1\rangle\langle m_1|_{\widehat{M}_1}\otimes\hat{\rho}_Z\right\|_1 \leq \epsilon_1 + \sqrt{\epsilon_2} \tag{41}$$

其中，$_{YX_1\text{-}4/234_1m^1}$ $\mu\rho_{X_1^{\otimes|\mathcal{M}_1||\mathcal{K}_1|}Y}^{(m_1,k_1),(m2,k2)}$· 是针对 m_1 的解码映射：

$$\mathcal{D}_{YX_1\to\widehat{M}_1}^{m_1}\left(\rho_{X_1^{\otimes|\mathcal{M}_1||\mathcal{K}_1|}Y}^{(m_1,k_1),(m_2,k_2)}\right) \coloneqq \sum_{k_1=1}^{|\mathcal{K}_1|}\sum_{m_1=1}^{|\mathcal{M}_1|} Tr\left\{\Lambda_{X_1^{|\mathcal{M}_1||\mathcal{K}_1|}Y}^{m_1,k_1}\rho_{X_1^{\otimes|\mathcal{M}_1||\mathcal{K}_1|}Y}^{(m_1,k_1),(m_2,k_2)}\right\} \otimes \frac{\sqrt{\Lambda_{X_1^{|\mathcal{M}_1||\mathcal{K}_1|}Y}^{m_1,k_1}}\rho_{X_1^{\otimes|\mathcal{M}_1||\mathcal{K}_1|}Y}^{(m_1,k_1),(m_2,k_2)}\sqrt{\Lambda_{X_1^{|\mathcal{M}_1||\mathcal{K}_1|}Y}^{m_1,k_1}}}{Tr\left\{\Lambda_{X_1^{|\mathcal{M}_1||\mathcal{K}_1|}Y}^{m_1,k_1}\rho_{X_1^{\otimes|\mathcal{M}_1||\mathcal{K}_1|}Y}^{(m_1,k_1),(m_2,k_2)}\right\}}$$

- $\Lambda_{X_1^{|\mathcal{M}_1||\mathcal{K}_1|}Y_{m_1,k^1}}$ 是针对$m_1 \in$ D1: | M_1| E:的近似优正算子值测度（POVM）：

$$\Lambda_{X_1^{|\mathcal{M}_1||\mathcal{K}_1|}Y}^{m_1,k_1} \coloneqq \left(\sum_{k_1'=1}^{|\mathcal{K}_1|}\sum_{m_1'=1}^{|\mathcal{M}_1|}\Gamma_{X_1^{|\mathcal{M}_1||\mathcal{K}_1|}Y}^{m_1',k_1'}\right)^{-1/2}\Gamma_{X_1^{|\mathcal{M}_1||\mathcal{K}_1|}Y}^{m_1,k_1}\left(\sum_{k_1'=1}^{|\mathcal{K}_1|}\sum_{m_1'=1}^{|\mathcal{M}_1|}\Gamma_{X_1^{|\mathcal{M}_1||\mathcal{K}_1|}Y}^{m_1',k_1'}\right)^{-1/2}$$

其中，$\Gamma_{X_1^{|\mathcal{M}_1||\mathcal{K}_1|}Y}{}^{m_1,k^1}$ 是第一个正算子值测度的元素：

$$\Gamma_{X_1^{|\mathcal{M}_1||\mathcal{K}_1|}Y}^{m_1,k_1} \coloneqq I_{X_1}^{(1,1)}\otimes\ldots\otimes I_{X_1}^{(1,|\mathcal{K}_1|)}\otimes\ldots\otimes\tau_{X_1Y}^{m_1,k_1}\otimes\ldots \otimes I_{X_1}^{(|\mathcal{M}_1|,|\mathcal{K}_1|)}$$

并且 $¢_{X_1Y_{m_1,k^1}}$ 是一个用于区分两个假设 ρ_{X_1Y} 和 $\rho_{X_1}\otimes\rho_Y$ 的检验算子。此外，显然，为了对 m_1 进行译码，对于第二个位置型解码器而言，Alice 从 | M_2|| ‘$_2$| 个副本中选择哪一个并不重要。

- 我们面对一个假设检验问题。零假设是ρ_{X_1Y} ，备择假设是 $\rho_{X_1}\otimes\rho_Y$。因此，猜中零假设和备择假设的成功概率分别为 $Tr\text{Œ}¢_{X_1Y}\,\rho_{X_1Y}\}$ 和 $Tr\text{Œ}oI_{X_1Y}$ –¢$_{X_1Y}$q o$\rho_{X_1}\otimes\rho_Y$q}。

m_1 的其余解码过程与 [20] 类似。因此，我们有：

$$R_1 \leq I_H^{\epsilon_1-\delta_1}(U_1;Y)_\rho - \tilde{I}_{max}^{\sqrt{\epsilon_2}-\delta_2}(U_1;Z)_\rho - \log\frac{4\epsilon_1}{\delta_1^2} - 2\log\frac{1}{\delta_2} \tag{42}$$

现在，我们来关注第二条消息的解码。如前所述，第一次测量后信道状态会发生变化。[32] 中有详细讨论。

令 $\sigma_{X_1X_1'(X_2X_2')^{\otimes|\mathcal{M}_2||\mathcal{K}_2|}YZ}$d $(m_1,\ 21)$，$(m_2,\ 2^2)$ 表示应用第一次测量（正算子值测度）后得到的扰动态：

$$\sigma_{X_1X_1'(X_2X_2')^{\otimes|\mathcal{M}_2||\mathcal{K}_2|}YZ}^{(m_1,k_1),(m_2,k_2)} \coloneqq \sum_{x_1} p_{X_1}(x_1)|x_1\rangle\langle x_1|_{X_1}\otimes|x_1\rangle\langle x_1|_{X_1'} \otimes\sigma_{X_2X_2'}^{x_1(m_1,k_1)}\otimes\ldots\otimes\sigma_{X_2X_2'YZ}^{x_1(m_1,k_1),(m_2,k_2)}\otimes\ldots \otimes\sigma_{X_2X_2'}^{x_1(m_1,k_1),(|\mathcal{M}_2|,|\mathcal{K}_2|)}$$

此外，Bob 的第二个正算子值测度如下：

$$\Lambda_{X_1X_2^{|\mathcal{M}_2||\mathcal{K}_2|}Y}^{m_2,k_2} \coloneqq \left(\sum_{k_2'=1}^{|\mathcal{K}_2|}\sum_{m_2'=1}^{|\mathcal{M}_2|}\lambda_{X_1X_2^{|\mathcal{M}_2||\mathcal{K}_2|}Y}^{m_2',k_2'}\right)^{-1/2}\lambda_{X_1X_2^{|\mathcal{M}_2||\mathcal{K}_2|}Y}^{m_2,k_2}\left(\sum_{k_2'=1}^{|\mathcal{K}_2|}\sum_{m_2'=1}^{|\mathcal{M}_2|}\lambda_{X_1X_2^{|\mathcal{M}_2||\mathcal{K}_2|}Y}^{m_2',k_2'}\right)^{-1/2}$$

$\lambda_{X_1X_2^{|\mathcal{M}_2||\mathcal{K}_2|}Y_{m_2,k^2}}$ 是第二个正算子值测度的元素：

$$\lambda_{X_1X_2^{|\mathcal{M}_2||\mathcal{K}_2|}Y}^{m_2,k_2} \coloneqq |x_1\rangle\langle x_1|_{X_1}\otimes I_{X_2}^{(1,1)}\otimes\ldots\otimes I_{X_2}^{(1,|\mathcal{K}_2|)}\otimes\ldots\otimes\theta_{X_2Y}^{m_2,k_2} \otimes\ldots\otimes I_{X_2}^{(|\mathcal{M}_2|,|\mathcal{K}_2|)}$$

à$_{X_2Y m_2,k^2}$ 是一个二元测试算子，用于区分两个假设$\sigma_{X_2Y x^1}$ 和 σ_{X_2} $_{x^1} \otimes \sigma_Y^{x_1}$ ，误差为 ϵ_1 –‰01；即，

$$Tr\{\theta_{X_2Y}\sigma_{X_2Y}^{x_1}\} \geq 1-(\epsilon_1-\delta_1) \quad \epsilon_1 \in (0,1), \qquad \delta_1 \in (0,\epsilon_1)$$

换言之，Bob 必须能够区分以下状态：

$$\sum_{x_1} p_{X_1}(x_1)|x_1\rangle\langle x_1|_{X_1} \otimes \sigma_{X_2Y}^{x_1}$$

$$\sum_{x_1} p_{X_1}(x_1)|x_1\rangle\langle x_1|_{X_1} \otimes \sigma_{X_2}^{x_1} \otimes \sigma_Y^{x_1}$$

与 [20]，和 [27]，中提到的情况类似，我们有以下速率：

$$R_2 \leq I_H^{\epsilon_1-\delta_1}(U_2;Y|U_1)_\rho - \tilde{I}_{max}^{\sqrt{\epsilon_2}-\delta_2}(U_2;Z|U_1)_\rho - \log\frac{4\epsilon_1}{\delta_1^2} - 2\log\frac{1}{\delta_2} \tag{43}$$

m_2 的错误概率如下：

$$p_{e_2} = p\{\widehat{M}_2 \neq M_2\}$$
$$\coloneqq \frac{1}{|\mathcal{M}_2|}\sum_{m_2=1}^{|\mathcal{M}_2|}\frac{1}{2}\left\|\mathcal{D}_{\widehat{M}_1Y X_2\to\widehat{M}_2}^{m_1}\left(\sigma_{X_1X_1'(X_2X_2')^{\otimes|\mathcal{M}_2||\mathcal{K}_2|}YZ}^{(m_1,k_1),(m_2,k_2)}\right)|m_2\rangle\langle m_2|_{\widehat{M}_2}\right.$$
$$\left.\otimes\,\hat{\sigma}_{X_1'X_2'^{\otimes|\mathcal{M}_2||\mathcal{K}_2|}Z}\right\|_1 \leq 2(\epsilon_1+\sqrt{\epsilon_2})+\sqrt{\epsilon_1'} \tag{44}$$

(41) 和 (44) 中给出的错误概率指数已得到证明。见 [20, 27] 。

这一过程可以针对另一种解码顺序重复。换言之，我们可以先解码 m_2，再解码 m_1($m_2 \to m_1$)。然后取两种顺序所得到区域的交集，得到：

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

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

证明至此完成。

附录D：（定理 3 的证明）

该证明采用叠加编码。假设第一接收方 Y_1 的接收信号优于第二接收方Y_2。在这种情况下，Alice 能够在公共消息之上叠加编码另一条消息。采用连续解码会有所帮助。

码本生成：根据分布 @$_U$(G)，随机且独立地生成 2^{R_c} 序列 G(m_c)。对于每个序列 G(m_c)，根据分布 @$_{X|U}$ oAòG(m_c)q，随机且有条件地独立生成 2^{R_1} 序列 A(m_1, m_c)。通过对 (13) 中的Y_2 进行偏迹，可以计算出 Y_1 的状态：

$$\rho_{UXY_1} = \sum_{u,x} p_U(u)p_{X|U}(x|u)\,|u\rangle\langle u|_U \otimes |x\rangle\langle x|_X \otimes \rho_x^{Y_1}$$

与定理 2 中所述类似，我们将第一接收方的正算子值测度构造为：

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

此外，第二接收方的正算子值测度可构造如下：

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

考虑 m_1的错误概率：

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

以及 m_c的错误概率：

$$p_{e_2} = p\{\widehat{M}_c \neq M_c\} \coloneqq \frac{1}{|\mathcal{M}_c|}\sum_{m_c} Tr\left\{(I-\Lambda_{m_c})\rho_{x(m_c)}^{Y_2}\right\}$$

通过与 [3] 中的独立同分布情形以及[29] 中的计算（用于求出量子广播信道的单次 Marton 内界）类似的直接计算，可得上述错误概率指数如下：

$$p_{e_1}+p_{e_2} \leq 2^{-I_H^\epsilon(X;Y_1|U)_\rho-2+\log\epsilon} + 2^{-I_H^\epsilon(U;Y_2)_\rho-2+\log\epsilon} + 2^{-I_H^\epsilon(X;Y_1)_\rho-2+\log\epsilon} + \mathcal{O}(\epsilon)$$

证明至此完成。

参考文献

[1] A. Winter，《量子多址信道的容量》，IEEE 信息论汇刊，第47卷，第7期，第3059–3065页，2001年7月。[2] J. Yard、P. Hayden 和 I. Devetak，《量子广播信道》，《IEEE信息论汇刊》，第57卷，第10期，第7147–7162页，2011年10月。[3] I. Savov，《经典-量子信道的网络信息论》，博士学位论文，麦吉尔大学，蒙特利尔，2012年。[4] A. El Gamal 和 Y.-H. Kim，《网络信息论讲义》，2010年1月，在线网址：http://arxiv.org/abs/1001.3404[5] 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。[6] 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。[7] 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信息论汇刊》，第58卷，第6期，[illegible]–3691页，2012年6月。[8] H. Aghaee, B. Akh[illegible]，《量子干扰窃听信道的一次性可达保密速率区域》，《ISC国际信息安全期刊》（IseCure），第14卷，第3期，第71–80页，2022年。

[9] H. Aghaee、B. Akhbari，《经典-量子多址窃听信道》，载于 *16th* 国际信息安全与密码学IS
哈德 。[10] H. Aghaee、B. Akhbari，《量子多址信道上的私有经典信息：单次保密速率区域》，载于 国际电信研讨会论文集（IST'2020），伊朗，2020年。[11] H. Aghaee、B. Akhbari，《带保密约束的经典-量子多址信道：单次速率区域》，《国际信息与通信技术研究杂志》（IJICTR），第12卷，第2期，第1–10页，2020年春季。
[12] 信道：单次速率区域》，载于11th信息与知识技术会议论文集（IKT'2020），伊朗，2020年。[13] H. Aghaee、B. Akhbari，《纠缠辅助经典-量子多址窃听信道：单次可达速率区域》，载于 20th 国际电气工程会议
集（ 2022），伊朗，2022年。[14] P. Sen，《并集、交集与单次量子联合典型性引理》，Sadhana，46(1):1–44，2021年。[15] A. D. Wyner，《窃听信道》，《贝尔系统技术杂志》，第54卷，第8期，第2–10页，1975年 [16] 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》，2021年IEEE信息论研讨会（ITW），第1–6页，2021年。[17] H. Qi、Q. Wang 和 M. M. Wilde，《基于位置的编码在通过量子信道进行经典通信中的应用》，https://arxiv.org/abs/1704.01361，2017年。[18] A. Anshu，《量子网络通信的单次协议：可达性与局限性》，博士论文，新加坡国立大学（新加坡），2018年。[19] A. Anshu、R. Jain 和 N. A. Warsi，《广义量子 Slepian–Wolf》，载于《IEEE信息论汇刊》，第64卷，第3期，第1436–1453页，2018年3月。[20] M. M. Wilde，《基于位置的编码与凸分裂在量子信道私密通信中的应用》，《量子信息处理》，16(10):264，2017年10月。[21] 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，第200501页，2012年。[22] 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。[23] M. Berta、M. Christandl 和 R. Renner，《基于单次信息论的量子反向香农定理》，《数学物理通讯》，第306卷，第3期，第579–615页，2011年。[24] F. Salek、A. Anshu、M. -H. Hsieh、R. Jain 和 J. R. Fonollosa，《同时传输经典信息与量子信息的单次容量界》，《IEEE信息论汇刊》，第66卷，第4期，第2141–2164页，2020年4月。[25] N. Ciganovi´ c、N. J. Beaudry 和 R. Renner，《平滑最大信息作为互信息的单次推广》，IEEE 信息论汇刊，第60卷，第1537–1581页，2014年3月。[26] M. Hayashi、H. Nagaoka，《经典-量子信道容量的一般公式》，IEEE 信息论汇刊，第49卷，第1753–1768页，2003年7月。[27] F. Salek、A. Anshu、M. -H. Hsieh、R. Jain 和 J. R. Fonollosa，《量子信道上同时传输公有信息与私有信息的单次容量界》，2018年IEEE国际信息论研讨会（ISIT），2018年，第296–300页。[28] M. M. Wilde、M. Tomamichel 和 M. Berta，《量子信道私密通信的逆向界》，载于《IEEE信息论汇刊》，第63卷，第3期，第1792–1817页，2017年3月。[29] P. Sen，《通过同时解码得到的量子网络信息论内界》，Sādhanā 46, 18（2021）。https://doi.org/10.1007/s12046-020-01517-9[30] M. Wilde，《量子信息论》，剑桥大学出版社，2013年。
[31] K. Li，“区分量子态：多重切尔诺夫距离”，《统计年鉴》，44(4):1661{1679，2016年8月。arXiv:1508.06624。[32] M. M. Wilde，“一般经典-量子信道的序贯译码”，《英国皇家学会会刊A辑：数学、物理与工程科学》，469(2157)，2013年。20130259。