# 通过噪声信道与非信号关联实现网络不经意传输的（不）可能性

Hadi Aghaee†、Christian Deppe†、Holger Boche*
†通信技术研究所，布伦瑞克工业大学，德国布伦瑞克

*理论信息技术教席，慕尼黑工业大学，德国慕尼黑电子邮箱：
(hadi.aghaee, christian.deppe)@tu-bs.de，boche@tum.de

arXiv:2602.03421v1 [cs.IT] 3 Feb 2026

**摘要**

本文研究了在诚实但好奇参与方之间，通过噪声多址接入信道和广播信道实现网络不经意传输的基本极限，其中参与方可以访问一般的三方无信号关联。通过将共享资源建模为任意三方无信号盒，我们对信道行为及其产生的关联给出了统一的观点。我们的主要结果表明，完美不经意传输是不可能实现的。在渐近情形下，我们进一步证明，即使是可忽略的泄漏也无法实现，因为反复使用该资源会增强接收方区分非其预期接收消息的能力。相比之下，接收方自身的隐私并不存在普遍的不可能性限制。

## 一、引言

不经意传输（OT）最早由拉宾提出 [1], ，他考虑了一种通信场景：爱丽丝向 Bob 发送一条消息，Bob 成功接收该消息的概率为二分之一，而爱丽丝并不知道传输是否成功。从香农的信息论视角来看，这种机制等价于擦除概率为二分之一的擦除信道。这一概念后来启发了 Even、Goldreich 和 Lempel 的开创性工作 [2], ，他们对 OT 进行了形式化，并确立了其作为一种基础密码学原语的地位。

众所周知，无法仅凭基于不可区分性假设的密码学技术从零构造 OT。这一不可能性结果还适用于各种交互式原语，包括比特承诺、零知识、秘密共享和安全两方计算，即使攻击者的计算能力受到限制也是如此。Dodis 等人 [3] 进一步证明，无法利用任何不完美随机性源实现 OT，其中包括偏差任意小的 Santha–Vazirani（SV）源 [4]。关键的是，这一不可能性是无条件的，不依赖于计算假设，也不要求限制攻击者的行为。更一般地说，只要可用的只有 SV 型熵源，任何要求隐私的密码学功能都无法实现。因此，信息论表明，噪声通信信道是熵的一种合理且可行的来源。

利用噪声信道可以实现丰富多样的信息论密码学协议。这一研究方向由早期奠基性工作开创，并随着时间推移得到深入发展 [1, 5–12], 。在对称私有信息检索（SPIR）的背景下，相关研究通常以 OT 这一术语来描述：参与方之间通过噪声信道实现信息论安全性，例如 [13–15]。相比之下，共享噪声信道——即多个用户通过共同媒介通信并观测到相关的噪声实现值——受到的关注相对有限。相关初步研究直到最近才出现 [16–20]。与相互独立的点对点噪声链路不同，共享信道使参与方能够利用噪声关联，实现协同编码与解码、降低通信开销并增强隐私保障。这些特性对于这样一些场景尤为重要：多个接收方从单一信息源获取信息，同时不泄露各自的选择。因此，

系统性地理解共享噪声信道，是将 OT 从成对通信扩展至更一般网络模型（包括广播信道（BC）和多址信道（MAC））的关键一步。

与此同时，在6G系统背景下，一条新兴研究路线旨在借助量子资源增强经典通信网络，有望改善吞吐量、安全性与时延 [21]。尽管点对点量子通信已取得实质性进展[22, 23] ，并且在诸如经典多址信道等相对简单的多用户场景中 [24–29] 以及广播信道 [30,31], ，更为复杂的网络配置在很大程度上仍有待探索。文献 [32] 研究了由纠缠发送方所带来的速率分割优势，并引入了一个受CHSH游戏启发的干扰信道（IC） [33] ，并采用了波佩斯库–罗尔利希盒（PR 盒）型超量子关联 [34]。后续研究 [35–37] 分析了两个发送方与两个接收方共享纠缠的干扰信道，表明由非经典关联引起的量子优势并不局限于多址信道，也会扩展至干扰信道模型。

受这些进展的启发，我们研究在三方无信号关联（NS盒）辅助下、具有两个发送方的离散无记忆多址信道（DM-MAC）上的不经意传输。Fawzi等人 [29]表明，此类NS盒可以严格扩大经典DM-MAC的容量区域。本文所探讨的核心问题是，对于DM-MAC的不经意传输容量[17], ，尤其是对于二进制加法信道这一特例 [38]，是否也能获得类似的增益。

本文结构安排如下：在第II节中，我们根据概率分布和互信息量给出三方无信号盒子的定义，并介绍离散无记忆多址信道和离散无记忆广播信道上的不经意传输定义。在第III节中，我们给出通过噪声信道实现网络不经意传输的主要不可能性结果。我们还讨论了通过二方无信号关联辅助的离散无记忆点对点噪声信道（离散无记忆信道）实现不经意传输的可行性，并证明，如果双方都包含在无信号关联中，则无法通过任何无信号关联辅助的噪声离散无记忆信道在两方之间实现不经意传输。在第IV节中，我们详细讨论了在发送方之间或接收方之间仅共享二方无信号相关性的情况下，在离散无记忆多址信道和离散无记忆广播信道上实现网络不经意传输的可行性。

符号说明：我们采用信息论中的标准记法，并约定如下。令 $\mathbb{N}$ 为自然数集， $\mathbb{R}$ 为实数集。对于任意 $x$、$y \in \mathbb{R}$，定义 $[x:\ y] \triangleq [\lfloor x \rfloor, \lceil y \rceil] \cap \mathbb{N}$ 以及 $[x] \triangleq [1:\ x]$。花体字母（如 $\mathcal{X}$）表示有限集合。大写字母（如 $X$）表示经典随机变量（RV），小写字母（如 $x$）表示其实现值。对于 $n \in \mathbb{N}$，我们将 $x^n = (x_i)_{i\in[n]}$ 记作取值于 $\mathcal{X}$、长度为 $n$ 的序列。离散随机变量 $X$ 的分布用概率质量函数（PMF） $p_X(x)$表示，其定义在有限字母表 $\mathcal{X}$上。令 $p_X$和 $q_X$为有限集合$\mathcal{X}$上的概率质量函数。 $p_X$与 $q_X$之间的全变差距离定义为 $\mathbb{V}(p_X, q_X) \triangleq \frac{1}{2}\sum_{x\in\mathcal{X}} |p_X(x) - q_X(x)|$。我们用 $A \triangleq A \oplus 1$ 表示比特 $A \in \{0,1\}$的二进制补，其中 $\oplus$ 表示模二加法。为将此概念推广到非二进制字母表，令 $\mathcal{I}$ 为有限指标集，且 $|\mathcal{I}| = 2$。定义双射 $f:\ \mathcal{I} \to \mathcal{I}$，使得对于所有 $i \in \mathcal{I}$，均有 $f(f(i)) = i$。我们将 $i \triangleq f(i)$记为 $i$，并称其为 $i$的补。因此， $i = i$，而映射 $f$ 仅交换 $\mathcal{I}$中的两个元素。例如，若$i \in \{1,2\}$，则当 $i = 2$时， $i = 1$ 。

## II. 系统模型

本节介绍本文中使用的系统模型和形式化定义。我们描述了有无无信号辅助时，在多址信道和广播信道上的网络不经意传输，并说明相关的正确性和安全性标准。

### *A.* 基于离散无记忆多址信道的网络不经意传输

我们介绍两个发送方和一个接收方通过离散无记忆多址信道进行网络不经意传输的系统模型。我们的目标是形式化描述如何在共享信道场景中实现不经意传输：在存在噪声和公开交互的情况下，多个发送方与公共接收方进行通信。

我们首先介绍一种三方NS关联，它可以由两个发送方和接收方共享。这种抽象使我们能够以统一的方式对经典信道行为以及额外的关联资源进行建模；后者可能源于量子机制或超量子机制。接着，我们定义离散无记忆多址信道的不经意传输协议、安全要求和可达速率概念，并分别讨论有无非信号辅助的情形。

这些定义确立了本文分析多址信道场景下网络不经意传输（不）可能性的基本框架。

定义 1（二方无信号相关性）。 设 $\mathcal{I}_1, \mathcal{I}_2, \mathcal{X}_1, \mathcal{X}_2$ 为有限集合。由 Alice-1 和 Alice-2 共享的二方 NS 盒由一个条件概率分布指定

$$P(x_1, x_2 \mid \imath_1, \imath_2), \tag{1}$$

其中， $I_1 \in \mathcal{I}_1$ 和 $I_2 \in \mathcal{I}_2$ 分别为输入， $X_1 \in \mathcal{X}_1$ 和 $X_2 \in \mathcal{X}_2$ 分别为输出。如果对于每个联合输入分布 $P_{I_1 I_2}$，其诱导的随机变量 $(I_1, I_2, X_1, X_2)$ 满足以下条件，则称该盒为非信号传递的

$$I(I_1; X_2 \mid I_2) = 0, \tag{2}$$
$$I(I_2; X_1 \mid I_1) = 0. \tag{3}$$

等价地，条件分布满足以下边缘约束

$$\sum_{x_1} P(x_1, x_2 \mid \imath_1, \imath_2) = \sum_{x_1} P(x_1, x_2 \mid \imath_1', \imath_2), \quad \forall \imath_1, \imath_1', \imath_2, x_2, \tag{4}$$
$$\sum_{x_2} P(x_1, x_2 \mid \imath_1, \imath_2) = \sum_{x_2} P(x_1, x_2 \mid \imath_1, \imath_2'), \quad \forall \imath_1, \imath_2, \imath_2', x_1. \tag{5}$$

定义 2（三方 NS 关联辅助的离散无记忆多址信道 [29]）。 两个发送方在离散无记忆多址信道上使用的三方 NS 盒由一个联合条件概率分布描述

$$P(x_1 x_2 (\jmath_1 \jmath_2) \mid \imath_1 \imath_2 y), \tag{6}$$

其中， $x_1, x_2$ 表示发送方的输出，$(\jmath_1, \jmath_2)$ 表示接收方的输出，而 $(\imath_1, \imath_2, y)$ 分别表示输入。无信号性质要求任意两方对应的边缘分布均与第三方的输入无关。也就是说，对于所有 $x_1, x_2, \jmath_1, \jmath_2, \imath_1, \imath_2, y, \imath_1', \imath_2', y'$，以下条件成立：

$$\sum_{x_1} P(x_1 x_2 (\jmath_1 \jmath_2) \mid \imath_1 \imath_2 y) = \sum_{x_1} P(x_1 x_2 (\jmath_1 \jmath_2) \mid \imath_1' \imath_2 y), \tag{7}$$

$$\sum_{x_2} P(x_1 x_2 (\jmath_1 \jmath_2) \mid \imath_1 \imath_2 y) = \sum_{x_2} P(x_1 x_2 (\jmath_1 \jmath_2) \mid \imath_1 \imath_2' y), \tag{8}$$

$$\sum_{\jmath_1, \jmath_2} P(x_1 x_2 (\jmath_1 \jmath_2) \mid \imath_1 \imath_2 y) = \sum_{\jmath_1, \jmath_2} P(x_1 x_2 (\jmath_1 \jmath_2) \mid \imath_1 \imath_2 y'). \tag{9}$$

方程（7）–（9）表明，任何一方都无法通过共享无信号资源向其他参与方传递关于其输入的信息。方程（7）-（9）可用互信息量表示如下：

$$I(I_1; X_2, J \mid I_2, Y) = 0, \tag{10}$$
$$I(I_2; X_1, J \mid I_1, Y) = 0, \tag{11}$$
$$I(Y; X_1, X_2 \mid I_1, I_2) = 0. \tag{12}$$

例如，三方 NS 条件确保边缘分布 $P(x_1 x_2 \mid \imath_1 \imath_2)$ 与接收方的输入 $y$ 无关，并且 $P(x_1 \mid \imath_1)$ 与 $\imath_2$ 和 $y$ 均无关。因此，在

我们的编码框架中，为发送方和接收方提供非信号辅助，相当于允许他们访问一个由联合条件分布 $P$ 描述的共享三方非信号盒。

首先请注意， $P$ 作为NS盒的性质完全独立于 $W$；特别地，变量 $y$ 在将 $P$ 定义为NS盒时无需满足任何特定分布。唯一剩下的微妙之处在于表面上需要同时进行编码和解码。然而，由于 $P$ 是非信号传递的，因此无需同时进行这两项操作。事实上，根据无信号性质，我们有

$$\forall y, \quad P(x_1x_2 \mid \imath_1\imath_2) = P(x_1x_2 \mid \imath_1\imath_2 y).$$

因此，输出 $x_1, x_2$ 可由输入 $\imath_1, \imath_2$ 得到，而无需知道 $y$，因为 $x_1, x_2$ 的分布不受其影响。随后，变量 $y$ 遵循由 $W$确定的分布，并以 $x_1, x_2$为条件。最后，在可访问 $y$的情况下，解码过程描述如下:

$$P((\jmath_1\jmath_2) \mid \imath_1\imath_2 y x_1 x_2) = \frac{P(x_1x_2(\jmath_1\jmath_2) \mid \imath_1\imath_2 y)}{P(x_1x_2 \mid \imath_1\imath_2 y)} = \frac{P(x_1x_2(\jmath_1\jmath_2) \mid \imath_1\imath_2 y)}{P(x_1x_2 \mid \imath_1\imath_2)}. \tag{13}$$

因此，我们全局地恢复了 $P((\jmath_1\jmath_2) \mid \imath_1\imath_2 y x_1 x_2) \times P(x_1x_2 \mid \imath_1\imath_2) = P(x_1x_2(\jmath_1\jmath_2) \mid \imath_1\imath_2 y)$,这对应于所规定的条件概率。NS条件保证可以将与各方相关联的条件概率独立处理。这一观察阐明了如何利用三方共享的NS盒一致地进行消息的编码与解码。总之，存在如下因果单向关系:

$$(\imath_1, \imath_2) \xrightarrow{\text{NS-box}} (x_1, x_2) \xrightarrow[\text{DM-MAC}]{} y \xrightarrow[\text{with } (\imath_1, \imath_2)]{\text{NS-box}} (\jmath_1, \jmath_2).$$

定义 3（非平凡非定域信号盒多址信道形式）。若存在至少两个不同的输入对 $(\imath_1\imath_2)$ 和 $(\imath_1', \imath_2')$，以及某个 $y$ ，则称三方非信号盒 $P(x_1x_2(\jmath_1\jmath_2) \mid \imath_1\imath_2 y)$ 为非平凡的：

$$P((\jmath_1\jmath_2) \mid \imath_1\imath_2 y) \neq P((\jmath_1\jmath_2) \mid \imath_1', \imath_2', y). \tag{14}$$

等价地说，Bob 的输出边缘分布取决于发送方的联合输入。若不满足此条件，即

$$P((\jmath_1\jmath_2) \mid \imath_1\imath_2 y) = P((\jmath_1\jmath_2) \mid \imath_1', \imath_2', y) \quad \text{for all } (\imath_1\imath_2), (\imath_1', \imath_2'), y,$$

则称该盒子为平凡的。平凡非定域信号盒是指 Bob 的边缘输出分布独立于发送方输入的盒子。此类盒子虽然满足非信号约束，但除独立局部随机性外不提供任何相关性。特别地，对于平凡盒子，全局分布可分解为

$$P(x_1x_2(\jmath_1\jmath_2) \mid \imath_1\imath_2 y) = P(x_1 \mid \imath_1)\, P(x_2 \mid \imath_2)\, P((\jmath_1\jmath_2) \mid y),$$

因此，三方的输出在不同位置上统计独立。故平凡非定域信号盒无法提高多址信道的可达速率区域，因为接收方输出独立于发送方的信道输入。换言之，当且仅当 $I\big(I_1, I_2; J \mid Y\big) > 0$ 时，称该盒子为非平凡的 。等价地，当且仅当 $I\big(I_1, I_2;\ J \mid Y\big) = 0$ 时，该盒子为平凡的 ，此时 Bob 的边缘输出分布独立于发送方的联合输入。

定义4（基于离散无记忆多址信道的 OT 设置，图1-($a$)）。令 $n,\ k_1,\ k_2 \in \mathbb{N}$。一个（$n,\ k_1,\ k_2$）协议涉及 Alice-1、Alice-2 和 Bob 之间的交互。在每个时间步 $l = 1,\ 2,\ \ldots\ldots,\ n$，Alice-$i$ 通过多址信道发送一位$X_{i,\ l}$ 。用户在每次传输之前以及在 $l = n$ 处最后一次传输之后，均通过无噪声公共信道以多轮交替交换消息。轮次数可以变化，但必定有限。每个用户的传输由一个函数决定，该函数取决于其输入、私有随机性，以及此前观察到的所有消息、信道输入或信道输出。一个正的速率对

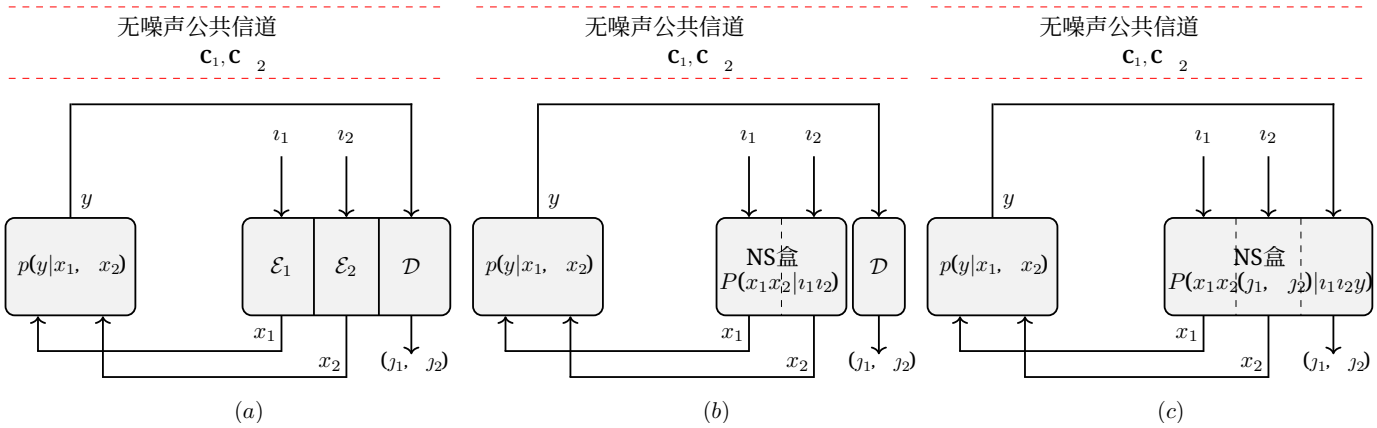



**图 1：** $(a)$ 具有两个编码器和一个译码器的双用户噪声离散无记忆多址信道上的不经意传输系统模型。$(b)$ 二方无信号相关性辅助的噪声离散无记忆多址信道上的不经意传输系统模型。$(c)$ 三方NS关联辅助的噪声离散无记忆多址信道上的不经意传输系统模型。

（$R_1$， $R_2$）称为该离散无记忆多址信道的可实现 OT 速率对，若对于 $n \to \infty$ 存在（$n$， $k_1$，$k_2$）协议满足 $\frac{k_i}{n} \to R_i$，使得对于互不串通的参与方，渐近条件（15）–（17）成立：

$$\lim_{n\to\infty} \Pr\left[(\hat{M}_{1Z_1}, \hat{M}_{2Z_2}) \neq (M_{1Z_1}, M_{2Z_2})\right] = 0, \tag{15}$$

$$\lim_{n\to\infty} I(M_{1\overline{Z}_1}, M_{2\overline{Z}_2}; V) = 0, \tag{16}$$

$$\lim_{n\to\infty} I(Z_i; U_i)_{i\in\{1,2\}} = 0, \tag{17}$$

其中，爱丽丝-$i$ 和Bob的最终视图分别为 $U_i = (M_{i0}, M_{i1}, R_{A_i}, X_i^n, \mathrm{C})$和 $V = (Z_1, Z_2, R_B, Y^n, \mathrm{C})$，并且C $\triangleq$ ($\mathrm{C}_1$,$\mathrm{C}_2$)。条件(15)-(17)分别表示正确性、对爱丽丝的安全性-$i$ (SfA-$i$)以及对Bob的安全性(SfB)。

定义 5（通过三方无信号相关性辅助离散无记忆多址信道实现的网络 OT 设置，图 1-($c$)）。考虑一个有两名发送方 Alice-1 和 Alice-2，以及一名接收方 Bob 的离散无记忆多址信道。各方还获得一个共享的三方无信号资源，其特征由 (6) 中定义的条件分布描述，并具有 (7)-(9) 中所述的性质。在该离散无记忆多址信道上，$(n, k_1, k_2)$ NS 辅助不经意传输协议定义为一种 $(n, k_1, k_2)$ OT 协议，其中各方还可以使用上述共享无信号资源。在每个时间步 $l = 1, \ldots, n$，Alice-$i$ 根据其对协议的局部视图以及无信号盒先前的输出，生成信道输入 $X_{i,l}$，并可能生成无信号盒输入 $\imath_{i,l}$。Bob 也可以向无信号盒输入一个变量 $y_l$，并获得相应的输出 $(\jmath_{1,l}, \jmath_{2,l})$，这些输出可用于后续的信道或局部计算。若对于 $n \to \infty$，存在满足条件 (15)- (17) 的 $(n, k_1, k_2)$ 非信号辅助协议，则称速率对 $(R_1, R_2)$ 在非信号辅助下可实现，其中 $U_i = (M_{i0}, M_{i1}, R_{A_i}, X_i^n, \mathrm{C})$ 表示 Alice-$i$ 的最终视图，而 $V = (Z_1, Z_2, R_B, Y^n, \mathrm{C})$ 表示 Bob 的最终视图。这里，$R_{A_i}$ 和 $R_B$ 表示本地随机性，C 表示公开通信，并且这些随机变量可能依赖于多址信道和无信号盒。

所有满足条件的可达速率对的闭包$(R_1, R_2)$ （满足（15）–（17））称为*NS*辅助*OT*容量区域，适用于参与方不合谋的多址信道。

定义 6（基于 NS 盒的完美安全准则）。固定分组长度 $n$。对于 $i \in \{1, 2\}$，记作$U_i = \left(M_{i0}, M_{i1}, R_{A_i}, X_i^n, A_i^n, \mathrm{C}\right)$，表示协议结束时爱丽丝的完整局部视图：她的两个文件、本地随机性 $R_{A_i}$、信道输入 $X_i^n$（或 NS 输入 $\imath_i^n$）、她的本地 NS 盒输出 $A_i^n$（即 $a_{i,t}$ 的序列），以及公开通信记录 C。Bob 的选择比特为 $Z =$ （$Z_1, Z_2$），其完整视图为

$V = (Z, Y^n, J, R_B, \mathbf{C})$，与之前相同。

$$P(U_i = u_i \mid M = m, Z = z) = P(U_i = u_i \mid M = m, Z = z') \quad \text{for all } u_i \tag{18}$$

$$P\big(V = v \mid \imath_1\imath_2, Z = z\big) = P\big(V = v \mid \imath_1'\imath_2', Z = z\big) \quad \text{for all } v. \tag{19}$$

*B.* 基于离散无记忆广播信道的网络不经意传输

现在考虑离散无记忆广播信道的对偶网络设定，其中单个发送方与多个接收方进行通信。在此模型中，发送方持有多个消息对，而每个接收方私下选择一条消息进行传送，同时不向发送方或另一名接收方透露其选择。

与多址信道的情形一样，我们允许各方共享一个三方非信号关联，该关联可以在遵守非信号约束的同时影响编码、解码和信道交互。我们首先定义广播场景中此类非信号关联的结构，然后形式化相应的不经意传输、正确性和安全性概念。

由此得到的框架能够直接比较多址信道和广播信道设定，并构成第 III 节中所确立的不可能性结果的基础。

定义 7（离散无记忆广播信道上的三方非信号盒）。 具有两个接收方的离散无记忆广播信道上的三方非信号盒由联合条件概率分布描述

$$P(x\jmath_1\jmath_2 \mid \imath y_1 y_2), \tag{20}$$

其中，$x$ 表示发送方的输出，$\jmath_i$ 表示接收方-$i$的输出，而（$\imath$、$y_1$、$y_2$）分别表示各方的输入。无信号性质要求，任意两方所对应的边缘分布均与第三方的输入无关。也就是说，对于所有 $x$、$\jmath_1$、$\jmath_2$、$\imath$、$y_1$、$y_2$、$\imath'$、$y_1'$、$y_2'$，以下条件成立：

$$\sum_x P(x\jmath_1\jmath_2 \mid \imath y_1 y_2) = \sum_x P(x\jmath_1\jmath_2 \mid \imath' y_1 y_2), \tag{21}$$

$$\sum_{\jmath_1} P(x\jmath_1\jmath_2 \mid \imath y_1 y_2) = \sum_{\jmath_1} P(x\jmath_1\jmath_2 \mid \imath y_1' y_2), \tag{22}$$

$$\sum_{\jmath_2} P(x\jmath_1\jmath_2 \mid \imath y_1 y_2) = \sum_{\jmath_2} P(x\jmath_1\jmath_2 \mid \imath y_1 y_2'). \tag{23}$$

上述 NS 条件意味着，任意两方的边缘分布都与第三方的输入无关。特别是，对于所有 $(y_1,\ y_2)$，发送端输出无需获知接收方的输入即可生成，

$$P(x \mid \imath) = P(x \mid \imath y_1 y_2).$$

因此，编码和解码无需同时进行。在操作层面，这会形成如下单向因果结构：

$$\imath \xrightarrow{\text{NS-box}} x \xrightarrow[\text{DM-BC}]{} (y_1, y_2) \xrightarrow[\text{with } \imath]{\text{NS-box}} (j_1, j_2).$$

也就是说，发送端输出 $x$仅由发送方的输入 $\imath$生成，广播信道产生接收端观测 $(y_1,\ y_2)$，最后，接收端无信号盒输出 $(j_1,\ j_2)$ 根据 $(\imath,\ y_1,\ y_2)$ 生成，并与联合条件分布保持一致。这种因果分离保证了在遵守 NS 约束的同时，实现指定的无信号盒分布。

方程（21）–（23）表示，任何一方都不能通过共享无信号资源向其他方传递有关其输入的信息。方程（21）-（23）可用互信息量表示如下：

$$I(I; J_1, J_2 \mid Y_1, Y_2) = 0, \tag{24}$$

$$I(Y_1; X, J_2 \mid I, Y_2) = 0, \tag{25}$$

$$I(Y_2; X, J_1 \mid I, Y_1) = 0. \tag{26}$$

定义 8（非平凡NS盒-广播信道形式）。我们考虑一个条件分布为$p(y_1, y_2 \mid x)$的广播信道，以及一个由条件分布 $P(xj_1j_2 \mid \imath y_1y_2)$指定的三方非信号盒，其中 $I$表示发送方输入到NS盒的输入，$(Y_1, Y_2)$为边信息输入， $X$ 为输入到广播信道的输出，而$(J_1, J_2)$为接收方的输出。由此产生的联合分布为

$$P(\imath, x, y_1, y_2, j_1, j_2) = P(\imath)\, P(x, j_1, j_2 \mid \imath, y_1, y_2)\, p(y_1, y_2 \mid x).$$

当三方非信号盒满足以下条件时，称其为平凡的

$$P(x, j_1, j_2 \mid \imath, y_1, y_2) = P(x, j_1, j_2 \mid y_1, y_2), \quad \forall\, \imath, y_1, y_2. \tag{27}$$

如果存在 $\imath \neq \imath'$和 $y_1$、 $y_2$、 $x$、 $j_1$、 $j_2$使得，则称三方非信号盒为非平凡的

$$P(x, j_1, j_2 \mid \imath, y_1, y_2) \neq P(x, j_1, j_2 \mid \imath', y_1, y_2). \tag{28}$$

换言之，当且仅当满足以下条件时，三方非信号盒是平凡的

$$I(I\,;\, X, J_1, J_2 \mid Y_1, Y_2) = 0. \tag{29}$$

等价地，

$$H(X, J_1, J_2 \mid Y_1, Y_2) = H(X, J_1, J_2 \mid I, Y_1, Y_2).$$

定义 9. 设 $n$、 $k_1$、 $k_2 \in \mathbb{N}$。$(n,\ k_1,\ k_2)$ 协议是爱丽丝、鲍勃-1 和鲍勃-2 之间的交互通信。在 $n$ 个时间步内，爱丽丝在每个时间 $l = 1$、.....、 $n$ 通过广播信道传输一个单比特 $X_l$ 。此外，各方可以在每次传输之前以及最终传输之后，通过无噪声公共信道进行有限轮次的消息交换。某方发送的每条消息都可以取决于其输入、私有随机性，以及此前观察到的所有消息、信道输入和信道输出。若对于不经意传输在离散无记忆广播信道上的情况，当 $n \to \infty$时，存在满足 $\frac{k_i}{n} \to R_i$ 的 $(n,\ k_1,\ k_2)$ 协议，使得渐近非共谋条件 (30)–(32) 得到满足，则称速率对 $(\overline{R}_1,\ R_2)$ 是可实现的。

$$\lim_{n\to\infty} \Pr\left[(\hat{M}_{iZ_i}) \neq (M_{iZ_i})\right]_{i\in\{1,2\}} = 0, \tag{30}$$

$$\lim_{n\to\infty} I(M_{i\overline{Z}_i}; V_i)_{i\in\{1,2\}} = 0, \tag{31}$$

$$\lim_{n\to\infty} I(Z_1, Z_2; U) = 0, \tag{32}$$

其中 $V_i = (Z_i, R_{B_i}, Y_i^n, \mathsf{C}_i)$ $U = (M_{i0}, M_{i1}, R_A, X^n, \mathsf{C})$ $i \in \{1, 2\}$ 且 $\mathsf{C} \triangleq (\mathsf{C}_1, \mathsf{C}_2)$。条件 (30)-(32) 分别为正确性、对爱丽丝的安全性 (SfA) 以及对Bob的安全性-$i$ (SfB-$i$)。

定义 10（通过三方 NS 辅助离散无记忆广播信道实现的网络OT设置——图 2——($b$)）。考虑一个有两个接收方的离散无记忆广播信道。各方还获得一个共享三方NS资源，其特征由式 (20) 中定义的条件分布描述，并具有式 (21)–(23) 所述的性质。离散无记忆广播信道上的一个 $(n, k_1, k_2)$ NS辅助不经意传输协议，定义为一个 $(n, k_1, k_2)$ 不经意传输协议，其中各方还可以使用上述共享无信号资源。在每个时间步 $l = 1, \ldots, n$，爱丽丝根据协议的局部视图以及此前的NS盒输出，生成一个信道输入 $X_l$，并可能生成一个NS盒输入 $\imath_l$。Bob-$i$ 也可以向NS盒输入变量 $y_{i,l}$，并获得相应的输出 $\jmath_{i,l}$，这些输出可用于后续的信道计算或局部计算。如果对于 $n \to \infty$，存在满足条件 (30)–(32) 的 $(n, k_1, k_2)$ 个NS辅助协议，则称速率对 $(R_1, R_2)$ 在NS辅助下可达；其中 $U = (M_{10}, M_{11}, M_{20}, M_{21}, R_A, X^n, \mathsf{C})$ 表示爱丽丝的最终视图，而 $V_i = (Z_i, R_{B_i}, Y_i^n, \mathsf{C})$ 表示Bob-$i$的最终视图。这里， $R_A$ 和$R_{B_i}$ 表示本地随机性，C表示公开通信，且随机变量可能同时依赖于离散无记忆广播信道和NS盒。满足条件 (30)–(32) 的所有可达速率对 $(R_1, R_2)$ 的闭包，称为非合谋参与方在多址信道上的NS辅助不经意传输容量区域。

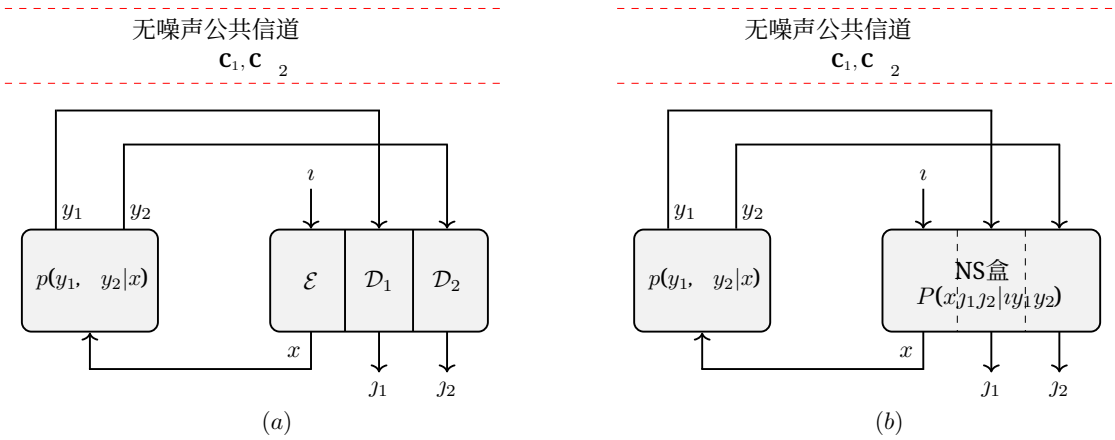



**图 2：** (a) 使用两个译码器的有噪离散无记忆广播信道上的 OT 系统模型。(b) 使用 NS盒的有噪离散无记忆广播信道上的 OT 系统模型。

## III. 主要结果与证明

### *A.* 在非平凡三方无信号盒辅助下通过离散无记忆多址信道实现完美不经意传输

我们首先研究在所有参与方均得到共享三方NS关联辅助的情况下，双发送方离散无记忆多址信道上完美不经意传输的可行性。本小节旨在探究这种强大的关联资源能否绕过共享噪声信道上不经意传输的经典不可能性。

我们考虑最强的辅助情形：NS盒由两个发送方和接收方共享，且可以是任意非平凡的，而编码器是发送方文件的确定性函数。在这些假设下，我们证明无法实现完美不经意传输：任何能够正确译码所选消息的协议，都必然会侵犯至少一方发送方的隐私。

以下定理将这一不可能性结果形式化。

**定理*1.*** *考虑一个双发送方离散无记忆多址信道：* $W\colon \mathcal{X}_1 \times \mathcal{X}_2 \to \mathcal{Y}$*。分别令非信号盒输入为确定性函数*[1] $\imath_1 = f_1(M_{10}, M_{11}) \in \{0,1\}^n, \imath_2 = f_2(M_{20}, M_{21}) \in \{0,1\}^n$*，且 Bob 观察到信道输出* $y \in \mathcal{Y}$*。假设三方共享一个三方NS关联* $P(x_1, x_2, (\jmath_1\jmath_2) \mid \imath_1, \imath_2, y)$*，并满足标准NS约束 (7)-(9)，则在这种非信号辅助下，不经意传输是不可能实现的。*

证明。 根据NS盒的定义，Bob的译码律由条件（13）给出：

$$P((\jmath_1\jmath_2) \mid \imath_1\imath_2 y x_1 x_2) = \frac{P(x_1x_2(\jmath_1\jmath_2) \mid \imath_1\imath_2 y)}{P(x_1x_2 \mid \imath_1\imath_2)}.$$

此外，我们有：

$$P(x_1x_2(\jmath_1\jmath_2)\, y \mid \imath_1\imath_2) = P(x_1x_2(\jmath_1\jmath_2) \mid \imath_1\imath_2 y)\, W(y \mid x_1, x_2). \tag{33}$$

根据条件概率和边缘化的定义，

$$\begin{aligned} P(y \mid \imath_1\imath_2) &= \sum_{x_1x_2\jmath_1\jmath_2} P\big(x_1x_2(\jmath_1\jmath_2) y \mid \imath_1\imath_2\big) \\ &= \sum_{x_1x_2\jmath_1\jmath_2} P\big(x_1x_2(\jmath_1\jmath_2) \mid \imath_1\imath_2\, y\big)\, W(y \mid x_1, x_2). \end{aligned} \tag{34}$$

[1]请注意， $f_i$ 并不是在 NS 盒之上额外添加的编码器。它们只是描述双方如何根据各自的消息，将盒子的输入 $\imath_i$， $i \in \{1,2\}$ 作为确定性函数来选择。

这个条件律通常同时依赖于两个输入 $\imath_1$ 和 $\imath_2$，因为 NS 条件只保证对一方的输出进行边缘化后具有不变性。

然而，在安全不经意传输协议中，隐私约束要求 Bob 的视图中的信道输出与每个未被选择的发送方的消息相互独立：

$$P(y \mid \imath_1, \imath_2) = P(y \mid \imath_1', \imath_2), \quad \forall \imath_1, \imath_1', \imath_2, \tag{35}$$

$$P(y \mid \imath_1, \imath_2) = P(y \mid \imath_1, \imath_2'), \quad \forall \imath_2, \imath_2', \imath_1. \tag{36}$$

但根据一般结　　构，在 NS关联辅助多址信道中，存在 $(\imath_1\imath_2, \imath_1', \imath_2', y)$ 使得　　at

$$P(y \mid \imath_1, \imath_2) \neq P(y \mid \imath_1', \imath_2),$$

因为译码律通过比值 $P(x_1x_2(\jmath_1\jmath_2) \mid \imath_1\imath_2 y)/P(x_1x_2 \mid \imath_1\imath_2)$ 共同依赖于 $(\imath_1, \imath_2)$。这意味着 Bob 的译码输出同时与两个发送方的输入在统计上相关。因此，接收方可以推断出两个发送方消息的信息，从而违反不经意传输隐私条件 (35)–(36)。这一矛盾表明，即使各方之间存在三方NS关联，也没有任何协议能在多址信道上实现不经意传输。如前所述，对于 $i \in \{1,2\}$爱丽丝-$i$ 有两个文件 $M_{i0}, M_{i1}$。Bob 选择选择比特 $z = (z_1, z_2) \in \{0,1\}^2$。每个发送方使用一个（确定性）编码器 $\imath_i = f_i(M_{i0}, M_{i1})$，即他们输入到 NS盒的输入（或多址编码索引）。令 $V$ 表示 Bob 的整个最终视图（其中可能包括多址信道输出 $Y$、NS盒输出$J = (\jmath_1, \jmath_2)$、公开通信记录 C 以及 Bob 的本地随机性）。对于单轮次，我们将 Bob 从 NS辅助多址信道得到的可观测量记为 $v = (y, j)$；在 $n$ 轮次的情形中，记为 $V = (Y^n, J, Z, \mathrm{C})$。

对于不经意传输保密性，我们要求：对于每个发送方 $i$ 以及每个固定的选择比特 $Z_1$, $Z_2$，当已选文件 $M_{iZ_i}$ 固定时，Bob 的视图与未选文件 $M_{i\overline{Z}_i}$ 相互独立。形式化地，对于每个 $i \in \{1,2\}$、每个选择比特向量 $z = (z_1, z_2)$，以及任意两个消息元组

$$m = (m_{10}, m_{11}, m_{20}, m_{21}), \qquad m' = (m'_{10}, m'_{11}, m'_{20}, m'_{21}),$$

使得

$$M_{iz_i} = m_{iz_i}, \quad \text{(the chosen file for Alice-}i\text{ is equal)}$$

and

$$m_{k\ell} = m'_{k\ell} \quad \text{for all } (k,\ell) \neq (i, \overline{Z}_i) \quad \text{(all other files equal)},$$

发送方保密性（19）要求

$$P\big(V = v \mid M = m,\ Z = z\big) \;=\; P\big(V = v \mid M = m',\ Z = z\big) \quad \text{for all } v. \tag{37}$$

这意味着，当所选文件及所有其他文件均相同时，改变未选文件不得影响 Bob 的视图。由于编码器是确定性的，$\imath_i = f_i(M_{i0},\ M_{i1})$，条件（37）等价于对 Bob 的可观测量所诱导的条件分布施加以下约束：对于每个 $z$ 以及每一对编码器输入 $(\imath_1\imath_2)$ 和 $(\imath_1',\ \imath_2')$，它们由满足上述同一性条件（所选文件相同，所有其他文件均相同）的消息元组 $m,\ m'$产生时，必须有

$$P\big(V = v \mid \imath_1\imath_2, Z = z\big) \;=\; P\big(V = v \mid \imath_1'\imath_2', Z = z\big) \quad \text{for all } v. \tag{38}$$

左侧可以通过无信号盒子与多址信道复合显式写出；例如，对于一轮，其中多址信道定律为 $W(y \mid x_1,\ x_2)$，无信号核为 $P(x_1x_2(\jmath_1\jmath_2) \mid \imath_1\imath_2 y)$，

对于固定的发送方输入 $(\imath_1\imath_2)$，无信号盒子与多址信道的联合行为为

$$P(x_1x_2(\jmath_1\jmath_2), y \mid \imath_1\imath_2) = P(x_1x_2(\jmath_1\jmath_2) \mid \imath_1\imath_2 y)\, W(y \mid x_1, x_2). \tag{39}$$

因此，Bob 在可观测量对 $(y,(\jmath_1\jmath_2))$ 上的边缘分布为

$$P(y, (\jmath_1\jmath_2) \mid \imath_1\imath_2) = \sum_{x_1,x_2} P(x_1x_2(\jmath_1\jmath_2) \mid \imath_1\imath_2 y)\, W(y \mid x_1, x_2). \tag{40}$$

因此，纳入其选择 $z$ 及可能的公开通信记录$\mathbf{C}$后，Bob 完整视图的整体分布为

$$\begin{aligned} P(V=v \mid \imath_1\imath_2) &= \delta_{Z=z}\, P(\mathbf{C}=c \mid \imath_1\imath_2, z)\, P(y,(\jmath_1\jmath_2) \mid \imath_1\imath_2) \\ &= \delta_{Z=z}\, P(\mathbf{C}=c \mid \imath_1\imath_2, z) \sum_{x_1,x_2} P(x_1x_2(\jmath_1\jmath_2) \mid \imath_1\imath_2 y)\, W(y \mid x_1,x_2), \end{aligned} \tag{41}$$

其中 $\delta_{Z=z}$ 只是将 Bob 的视图中的选择比特固定为所选值。根据 NS盒的非平凡性（定义 3），这违反了爱丽丝的保密性（38）。 □

我们有如下命题，指出只有平凡的 NS盒才不会通过 DM-MAC 违反不经意传输保密性。

命题 2。 设 $P(x_1x_2(\jmath_1\jmath_2) \mid \imath_1\imath_2 y)$ 为一个三方 NS核，且多址信道为 $W(y \mid x_1,x_2)$。考虑在编码器输入 $(\imath_1\imath_2)$ 和 Bob 的选择 $Z=z$ 条件下 Bob 的视图 $V=(Z,Y,(\jmath_1\jmath_2),\mathbf{C})$ 的诱导分布。若满足以下通用编码器级保密性:

$$\forall\ \imath_1,\imath_2,\imath_1',\imath_2',\ \forall v, \qquad P(V=v \mid \imath_1\imath_2, Z=z) = P(V=v \mid \imath_1'\imath_2', Z=z), \tag{42}$$

那么 Bob 的边缘分布与发送方的输入无关；等价地，无信号辅助多址信道资源是 平凡的。反之，若无信号辅助多址信道是非平凡的，则（42）不成立。

证明。 假设（42）成立。对可观测部分进行边缘化（或仅限于可观测部分），我们得到，对所有$\imath_1$， $\imath_2$，$\imath_1'$， $\imath_2'$ 以及对每一个 $y$， $(\jmath_1\jmath_2)$，

$$P(y,(\jmath_1\jmath_2) \mid \imath_1\imath_2, Z=z) = P(y,(\jmath_1\jmath_2) \mid \imath_1',\imath_2', Z=z).$$

去掉对 $Z=z$ 的无关条件化（它在等式中是固定的），我们写成

$$P(y,(\jmath_1\jmath_2) \mid \imath_1\imath_2) = P(y,(\jmath_1\jmath_2) \mid \imath_1',\imath_2').$$

因此，Bob 的可观测量（$Y$， $(\jmath_1\jmath_2)$）的边缘分布对每一个编码器输入对都相同；即

$$P(y,(\jmath_1\jmath_2) \mid \imath_1\imath_2) \equiv Q(y,(\jmath_1\jmath_2)) \quad \text{(independent of } \imath_1\imath_2). \tag{43}$$

利用 NS核与多址信道的复合（分解），

$$P(x_1,x_2,(\jmath_1\jmath_2),y \mid \imath_1\imath_2) = P(x_1,x_2,(\jmath_1\jmath_2) \mid \imath_1\imath_2 y)\, W(y \mid x_1,x_2),$$

并对 $x_1$， $x_2$ 进行边缘化，我们得到

$$Q(y,(\jmath_1\jmath_2)) = \sum_{x_1,x_2} P(x_1,x_2,(\jmath_1\jmath_2) \mid \imath_1\imath_2 y)\, W(y \mid x_1,x_2), \tag{44}$$

对每一个 $(\imath_1\imath_2)$。

现在，44表明右侧不依赖于 $(\imath_1\imath_2)$。特别是，给定 $Y$ 时，$(\imath_1\imath_2)$的边缘分布独立于$(\imath_1\imath_2)$:

$$P(Y=y \mid \imath_1\imath_2) = \sum_{\jmath_1,\jmath_2} Q(y,(\jmath_1\jmath_2)) \quad \text{(independent of } \imath).$$

因此，Bob 的边缘分布 $P(Y \mid \imath_1\imath_2)$关于 $(\imath_1\imath_2)$是常数。类似地， $P((\jmath_1\jmath_2) \mid \imath_1\imath_2 y)$必须满足，使得总和（44）独立于 $(\imath_1\imath_2)$。

这正是我们语境中平凡 资源的定义：Bob 的分布不依赖于发送方的输入，因此，无信号辅助多址信道不提供任何可用于区分不同编码器输入的依赖/相关性。反过来，如果无信号辅助多址信道是非平凡的——也就是说，存在 $(\imath_1\imath_2) \neq (\imath_1',\ \imath_2')$，使得

$$P(y,(\jmath_1\jmath_2) \mid \imath_1\imath_2) \neq P(y,(\jmath_1\jmath_2) \mid \imath_1'\imath_2'),$$

那么，(42) 不成立。 □

注记 1. 命题 2 刻画了 Bob 的整个视图何时独立于发送方的编码器输入，即当 NS辅助MAC资源为平凡时。然而，该条件严格强于不经意传输的保密性要求。在 OT 协议中，保密性是就可靠性而言有条件的：Bob 不得获得关于未选择的消息的信息，同时仍能可靠地解码所选消息。相比之下，通用编码器级保密性（42）要求 Bob 的视图独立于所有编码器输入，从而排除任何可靠通信。因此，若无信号辅助多址信道是平凡的，则正确性不成立，且不经意传输不可能。若无信号辅助多址信道是非平凡的，则（42）必然不成立，这意味着 Bob 能够区分某些编码器输入，从而违反完美 SfA。因此，无论三方NS辅助是平凡还是非平凡，完美不经意传输都不可能。命题 2 因此应被理解为对平凡性的刻画，而非不经意传输的可达性结果。

命题3. 考虑一个双发送方离散无记忆多址信道 $W$：$\mathcal{X}_1\times\mathcal{X}_2\to\mathcal{Y}$。设非信号盒输入分别为确定性函数$\imath_1 = f_1(M_{10}, M_{11}) \in \{0,1\}^n$和 $\imath_2 = f_2(M_{20}, M_{21}) \in \{0,1\}^n$，且 Bob 观察到信道输出 $y \in \mathcal{Y}$。假设三方共享一个非平凡/平凡的三方NS关联$P(x_1, x_2, (\jmath_1\jmath_2) \mid \imath_1, \imath_2, y)$，并满足标准NS约束 (10)-(12)，则在这种非信号辅助下，不经意传输是不可能的。

证明. 考虑 (16)：

$$\begin{aligned} I(M_{1\overline{Z}_1}, M_{2\overline{Z}_2}; V) &= I(M_{1\overline{Z}_1}, M_{2\overline{Z}_2}; Z, Y, J, \mathbf{C}) \\ &= I(M_{1\overline{Z}_1}; Z, Y, J, \mathbf{C}) + I(M_{2\overline{Z}_2}; Z, Y, J, \mathbf{C} | M_{1\overline{Z}_1}) \\ &\overset{(a)}{=} I(M_{1\overline{Z}_1}; Z, Y, J, \mathbf{C}) + I(M_{2\overline{Z}_2}; Z, Y, J, \mathbf{C}, M_{1\overline{Z}_1}) \\ &\overset{(b)}{=} I(M_{1\overline{Z}_1}; Z, Y, J, \mathbf{C}) + I(M_{2\overline{Z}_2}; Z, Y, J, \mathbf{C}) \\ &= I(M_{1\overline{Z}_1}; V) + I(M_{2\overline{Z}_2}; V) \\ &= 0, \end{aligned} \tag{45}$$

其中 $(a)$ 是由于 $M_{1Z_1}$ 与 $M_{2Z_2}$ 相互独立，而 $(b)$ 是由于马尔可夫链 $M_{2Z_2}$ –$(Z, Y, J,\mathbf{C})$ – $M_{1Z_1}$。于是，$I(M_{1Z_1}; V) = 0$。

由于 NS 关联不会对公共信道传输产生任何影响，因此我们忽略 $\mathbf{C}$，将其视为完整的公共传输记录。考虑第一个 NS盒判据（10），$I(I_1; X_2, J|I_2, Y) = 0$：

$$\begin{aligned} I(I_1; X_2, J|I_2, Y) &= I(I_1; J|I_2, Y) \\ &\quad + I(I_1; X_2|I_2, Y, J) \\ &= 0. \end{aligned} \tag{46}$$

已知 $V = (J, Z, Y^n)$，我们有：

$$\begin{aligned} I(I_1; V|I_2, Y) &= I(I_1; J, Z, Y|I_2, Y) \\ &= I(I_1; J|I_2, Y) \\ &\quad + I(I_1; Z|I_2, Y, J) \\ &\quad + I(I_1; Y|I_2, Y, J, Z) \\ &= 0, \end{aligned} \tag{47}$$

其中，最后一个等号由（46）以及最后两项均为零这一事实得出。非信号传递和确定性编码的数据处理过程形成如下马尔可夫链：$(M_{1Z_1}, M_{1Z_1})$–$I_1 - I_2, Y - V$。由于 $I_1$ 是$(M_{1Z_1}, M_{1Z_1})$的确定性函数，NS条件意味着

$$I(M_{1Z_1}, M_{1\overline{Z}_1}; V \mid I_2, Y) = 0,$$

或用熵形式表示

$$H(M_{1Z_1}, M_{1\overline{Z}_1} \mid I_2, Y) = H(M_{1Z_1}, M_{1\overline{Z}_1} \mid V, I_2, Y). \tag{48}$$

链式法则展开（48）：

$$H(M_{1Z_1} \mid I_2, Y) + H(M_{1\overline{Z}_1} \mid M_{1Z_1}, I_2, Y) = H(M_{1Z_1} \mid V, I_2, Y) + H(M_{1\overline{Z}_1} \mid M_{1Z_1}, V, I_2, Y). \tag{49}$$

（*i*）零差错传输：正确性意味着 $H(M_{1Z_1} \mid V, I_2, Y) = 0$。于是，（49）蕴含：

$$\begin{aligned} H(M_{1Z_1} \mid I_2, Y) + H(M_{1\overline{Z}_1} \mid M_{1Z_1}, I_2, Y) &= H(M_{1\overline{Z}_1} \mid M_{1Z_1}, V, I_2, Y) \\ &\leq H(M_{1\overline{Z}_1} \mid M_{1Z_1}, I_2, Y), \end{aligned} \tag{50}$$

因此

$$H(M_{1Z_1} \mid I_2, Y) = 0. \tag{51}$$

这表明所选消息 $M_{1Z_1}$ 已由（$I_2$, $Y$）确定，从而与非平凡的 Alice-1 安全性相矛盾，除非消息是退化的。

若 $H(M_{1Z_1} \mid I_2, Y) = 0$，则非平凡的 Alice-1 保密性

$$I(M_{1\overline{Z}_1}; V) = 0,$$

被违反，除非在未选消息熵为零（即确定性）的退化情形中。考虑（49）：

$$H(M_{1Z_1} \mid I_2, Y) + H(M_{1\overline{Z}_1} \mid M_{1Z_1}, I_2, Y) = H(M_{1Z_1} \mid V, I_2, Y) + H(M_{1\overline{Z}_1} \mid M_{1Z_1}, V, I_2, Y).$$

由于 $H(M_{1Z_1} \mid V, I_2, Y) = 0$，我们得到：

$$H(M_{1Z_1} \mid I_2, Y) + H(M_{1\overline{Z}_1} \mid M_{1Z_1}, I_2, Y) = H(M_{1\overline{Z}_1} \mid M_{1Z_1}, V, I_2, Y). \tag{52}$$

由（51）可得 $H(M_{1Z_1} \mid I_2, Y) = 0$，于是：

$$H(M_{1\overline{Z}_1} \mid M_{1Z_1}, I_2, Y) = H(M_{1\overline{Z}_1} \mid M_{1Z_1}, V, I_2, Y). \tag{53}$$

另一方面，条件化不会增加熵，

$$H(M_{1\overline{Z}_1} \mid M_{1Z_1}, V, I_2, Y) \leq H(M_{1\overline{Z}_1} \mid M_{1Z_1}, I_2, Y),$$

因此，（53）迫使这种单调性取等号。条件熵单调性取等意味着 $V$（等价地说，$V$ 中超出（$I_2$, $Y$, $M_{1Z_1}$）的部分）不包含关于 $M_{1Z_1}$ 的额外信息。由于 $Y \in V$，直接可得：每当（$I_2$, $Y$）确定 $M_{1\overline{Z}_1}$ 时（根据（51），确实如此），给定（$I_2$, $Y$）后 $M_{1Z_1}$ 的剩余不确定性等于给定（$I_2$, $Y$, $V$）后的剩余不确定性。另一方面，NS盒的非平凡性意味着 $I(I_1, I_2; J|Y) > 0$ 和 $I_i = f_i(M_{i0}, M_{i1})$ $i \in \{1, 2\}$。考察 $V = (J, Z, Y^n)$，我们有：

$$\begin{aligned} I(I_1, I_2; J|Y) &= I(I_1; J|Y) + I(I_1; J|I_2, Y) \\ &\overset{(a)}{=} I(I_1; J|Y) \\ &\overset{(b)}{\leq} I(I_1; V|Y) \qquad (54) \\ &> 0, \qquad (55) \end{aligned}$$

其中 $(a)$ 由（10）推出，且 $(b)$ 由数据处理不等式推出。考虑（54）：

$$\begin{aligned} I(I_1; V|Y) &\overset{(a)}{=} I(M_{1Z_1}, M_{1\overline{Z}_1}; V|Y) \\ &= H(M_{1Z_1}, M_{1\overline{Z}_1}|Y) - H(M_{1Z_1}, M_{1\overline{Z}_1}|V, Y) \\ &= H(M_{1Z_1}|Y) + H(M_{1\overline{Z}_1}|M_{1Z_1}, Y) - H(M_{1Z_1}|V, Y) - H(M_{1\overline{Z}_1}|M_{1Z_1}, V, Y) \\ &> 0, \end{aligned} \tag{56}$$

其中（$a$）源于这样一个事实： $I_1$ 是 $M_{10}$、$M_{11}$的确定性函数。由于条件化不会增加熵， $H(M_{1Z_1}|M_{1Z_1}, Y)$ $\geq H(M_{1Z_1}|M_{1Z_1}, V, Y)$；结合（56），我们有$H(M_{1Z_1}|M_{1Z_1}, Y) > H(M_{1Z_1}|M_{1Z_1}, V, Y)$。然而，这与（53）矛盾，这意味着对$V$进行条件化会泄露有关爱丽丝未选消息的信息，从而违反 Alice-1 安全性。

（*ii*）渐近正确性：考虑（15）。应用 Fano 不等式可得：

$$H(M_{1Z_1}, M_{2Z_2}|V) \leq h(\varepsilon_n) + \varepsilon_n \log_2 |\mathcal{M}|, \tag{57}$$

其中 $M \triangleq (M_{1Z_1}, M_{2Z_2}) \in \{0,1\}^{k_1+k_2}$，并且 $\log_2 |\mathcal{M}| = \log_2 2^{k_1+k_2} = k_1 + k_2$。于是，（57）可写为：

$$H(M_{1Z_1}, M_{2Z_2}|V) \leq \eta_n, \tag{58}$$

其中 $\eta_n \triangleq h(\varepsilon_n) + \varepsilon_n(k_1 + k_2)$。将（58）代入（49），得到：

$$H(M_{1Z_1} \mid I_2, Y) + H(M_{1\overline{Z}_1} \mid M_{1Z_1}, I_2, Y) \leq H(M_{1\overline{Z}_1} \mid M_{1Z_1}, V, I_2, Y) + \eta_n. \tag{59}$$

另一方面， $H(M_{1Z_1} \mid M_{1Z_1}, V, I_2, Y) \leq H(M_{1Z_1} \mid M_{1\overline{Z}_1}, I_2, Y)$。如果此单调性取等号（即满足 SfA-1 条件），那么 $H(M_{1Z_1} \mid I_2, Y_1) \leq \eta_n$，其中 $\eta_n \to 0$ as $n \to \infty$。这违反了不经意传输的因果性[2] 。如果不等式为严格不等式，则爱丽丝-1 的完美保密性遭到破坏。爱丽丝-2 的论证类似。证明完毕。

□

*B.* 非平凡三方无信号盒下离散无记忆多址信道上的渐近不经意传输

虽然上一小节的不可能性结果排除了完美不经意传输，但我们仍可能希望通过增大分组长度，实现误差和泄漏渐近趋于零的不经意传输。具体而言，一个自然的问题是：重复使用非平凡三方无信号辅助多址信道，能否实现信息泄漏可忽略的渐近不经意传输?

本小节将证明，情况并非如此。即使只要求可靠性渐近满足，且协议可以在许多次独立信道使用中运行，任何非平凡三方无信号盒都会导致编码器输入之间出现可区分性，并且这种可区分性会在重复使用时放大。因此，接收方渐近地能够获知有关未选消息的信息。

本小节的主要结果表明，在这些条件下，渐近不经意传输是不可能实现的。

**定理4**（非平凡三方无信号盒下渐近不经意传输的不可能性）。假设各方共享一个三方非信号盒 $P(x_1x_2(j_1j_2) \mid i_1, i_2, y)$，且该盒按上述意义是非平凡的；编码器 $i_i = f_i(M_{i0}, M_{i1})$ 是发送方文件的确定性函数，并且各方独立重复使用同一个单次使用核（各轮次间取乘积形式）。那么，不存在任何协议序列能够同时渐近满足可靠性和发送方安全性。

证明。假设存在一列 $(n, k_1, k_2)$-协议，它们满足可靠性和 Alice 安全性（16）。我们将构造两个消息元组 $m$, $m'$，它们仅在一个未选文件上不同，并证明 Bob 能以趋于 1 的概率区分它们，从而与 Alice 安全性矛盾。

由非平凡性可知，存在输入 $(i_1^*, i_2^*) \neq (\tilde{i}_1, \tilde{i}_2)$ 以及 $y^*$，使得 Bob 的单轮次输出分布在（全变差距离）上有所不同。

$$\varepsilon := \mathbb{V}\big(P_{J|i_1^*,i_2^*,y^*},\ P_{J|\tilde{i}_1,\tilde{i}_2,y^*}\big) > 0.$$

（此处 $J$ 表示单轮中 Bob 的视图；如果 Bob 还观测到 MAC 输出 $Y$，我们将其纳入 $J$，或按照模型将条件化置于 $y^*$ 上；通过将 $Y$ 纳入可观测量，表述保持不变。）

[2]不经意传输是一种因果密码学原语，其含义是接收方获得一条由本地生成的选择变量所决定的消息。因此，接收方的最终重构消息依赖于这一选择，而这种因果性体现在传递的消息 $M_{iZ_i}$、$i \in \{1,2\}$
中。这种因果依赖出现在最终解码的层面：重构消息是接收方视图及其选择的函数。从熵的角度来看，这意味着 $H(M_{iZ_i} \mid V_i,\ Z_i) = 0$，而对于诸如 NS 盒输出 $J_i$ 之类的中间变量，并不存在类似的恒等式。

由于编码器是确定性映射 $\imath_i = f_i(M_{i0},\ M_{i1})$，发送方可以选择消息元组，使其映射到其取值范围内所需的任意一对编码器输入。特别地，选取两个消息元组

$$m = (m_{10}, m_{11}, m_{20}, m_{21}), \qquad m' = (m'_{10}, m'_{11}, m'_{20}, m'_{21}),$$

使得

$$f_1(m_{10}, m_{11}) = \imath_1^*, \quad f_2(m_{20}, m_{21}) = \imath_2^*,$$

and

$$f_1(m'_{10}, m'_{11}) = \tilde{\imath}_1, \quad f_2(m'_{20}, m'_{21}) = \tilde{\imath}_2.$$

（如果编码器值域不包含所需的输入，则可以从可实现输入中选取非平凡的一对；该论证只要求存在两个可实现输入对，使盒子能够区分它们。）

此外，我们选择 $m,\ m'$ 使得对于某个固定选择 $z$，它们在所有已选文件上的取值相同，但在某个未选文件上的取值不同，因此不经意传输保密性要求 Bob 无法区分它们。具体而言，选取 $z$，并假设 $m,\ m'$ 仅在 $M_{1z_1}$（或 $M_{2z_2}$）上不同；两种情况的论证完全相同。根据构造，在消息 $m$ 和 $m'$ 下，输入 NS盒 的编码器输入分别为 $(\imath_1^*,\ \imath_2^*)$ 和 $(\tilde{\imath}_1,\ \tilde{\imath}_2)$，因此 Bob 的单轮可观测分布在全变差距离上相差 $\varepsilon$：

$$\mathbb{V}\big(P_{J|m}, P_{J|m'}\big) \ = \ \varepsilon.$$

由于协议采用独立重复（各轮之间为乘积结构），$n$ 轮分布 $P_{J^n|m}$ 和 $P_{J^n|m'}$ 是单轮分布的 $n$ 重乘积分布（或者至少，它们在 $J$ 分量上的边缘分布以类似方式因子化）。对于乘积分布，全变差距离满足张量化性质：

$$\mathbb{V}\big(P^{\otimes n}, Q^{\otimes n}\big) \ = \ 1 - (1 - \mathbb{V}(P, Q))^n.$$

因此，

$$\mathbb{V}\big(P_{J^n|m}, P_{J^n|m'}\big) = 1 - (1 - \varepsilon)^n.$$

特别地，$\mathbb{V}(\cdot) \to 1$ 以指数速度趋于零，当 $n \to \infty$。

考虑如下二元假设检验问题：Bob 必须根据观测到的 $J^n$，判断使用的是两个消息元组 $m$ 还是 $m'$。若 $m$ 和 $m'$ 的先验概率相等，则最小错误概率 $P_{(n)e}$ 为

$$P_e^{(n)} \ = \ \frac{1}{2}\big(1 - \mathbb{V}(P_{J^n|m}, P_{J^n|m'})\big).$$

等价地，最大正确决策概率为

$$p_{\text{corr}}^{(n)} \ = \ 1 - P_e^{(n)} \ = \ \frac{1}{2}\big(1 + \mathbb{V}(P_{J^n|m}, P_{J^n|m'})\big) = 1 - \tfrac{1}{2}(1 - \varepsilon)^n.$$

因此，当 $n \to \infty$ 时，$p_{\text{corr}}^{(n)} \to 1$，且 $P_e^{(n)} \to 0$。

定义二元随机变量 $B$：若消息元组是 $m$，则其取值为 0；若是 $m'$，则取值为 1，且先验概率相等，为 $1/2$。根据等概率二元 $B$ 及观测 $J^n$ 的二元假设检验错误与互信息之间的标准关系，

$$I(B; J^n) = H(B) - H(B \mid J^n) = 1 - H_2(P_e^{(n)}),$$

其中，$H_2(\cdot)$ 是以比特为单位的二元熵，且 $H(B) = 1$ 比特。由于 $P_{(n)e} \to 0$，我们有 $H_2(P_e^{(n)}) \to 0$，因此

$$\lim_{n\to\infty} I(B; J^n) = 1.$$

由于 $B$ 是未选文件的确定性函数（我们选择了 $m,\ m'$，因此它们仅在一个未选文件上不同），我们得到数据处理下界

$$I\big(M_{1\overline{Z}_1}, M_{2\overline{Z}_2}; J^n\big) \ \geq \ I(B; J^n) \xrightarrow[n\to\infty]{} 1.$$

因此，未选文件与 Bob 的 $n$ 轮次视图之间的互信息有一个正的常数下界（事实上至少趋近于 1 比特），这与 Alice 安全性要求相矛盾，因为

$$\lim_{n\to\infty} I\big(M_{1\overline{Z}_1}, M_{2\overline{Z}_2}; V^{(n)}\big) = 0.$$

（此处 $V^{(n)}$ 包括 Bob 可以获得的 $J^n$ 以及可能更多的信息，因此 $I(\cdot; J^n) \le I(\cdot; V^{(n)})$；所以对于 $V^{(n)}$，同样的矛盾更加明显。）

任何非平凡三方无信号盒都能使某些编码器输入之间在单轮中具有可区分性 $\varepsilon > 0$；由于编码器以确定性方式将消息映射为输入，因此可以安排两个仅在未选文件上有所不同的消息元组，使其产生可区分的鲍勃的分布；重复操作会放大这种可区分性，使 Bob 渐近地以趋近于一的概率获知未选文件。因此，Alice 安全性（泄漏渐近消失）是不可能实现的。至此，证明完成。 □

### *C.* 存在三方无信号盒时 *Bob* 的安全性

上述不可能性结果着重于发送方安全性的破坏。这自然引出了一个互补的问题：在存在三方非信号辅助的情况下，SfB 是否也普遍不可能实现。

与发送方安全性相反，我们表明，对于鲍勃的安全性不存在这样的普遍限制。根据协议中如何使用公开通信和 NS盒输出，Bob 的选择比特可能会泄露，也可能不会泄露。因此，SfB 是一种取决于协议的性质，而不是 NS辅助信道模型所固有的限制。

下面的定理说明了这一差异。

**定理5**（关于 Bob 安全性不存在普遍不可能性）。 在存在非平凡三方无信号盒的情况下，不经意传输方案中的 *Bob* 安全性不存在普遍不可能性结果：对于某些协议，*Bob* 安全性可以成立，而对于其他协议则可能失败。

证明。 考虑以下设置：

1）所有公开通信记录消息 $\mathbf{C}$ 均仅由发送方的本地随机性和消息（以及先前的公开消息）生成，但不 由 $Z$ 或任何 Bob 信息生成；2）编码器 $\imath_i^n = f_i^{(n)}(M_{i0},\ M_{i1})$ 仅是发送方文件的确定性函数，且从不依赖于 $Z$ （即发送方从不根据 Bob 的信息进行自适应）；3）不存在额外的侧信道（不使用依赖于 $Z$的、由发送方自适应使用的消息认证码反馈）。

对于 $n$ 轮协议，将给定消息 $M = m$ 和 Bob 的选择 $Z = z$ 时的全局条件分布记为

$$P_{\text{global}}(x_1^n, x_2^n, j^n, y^n, c \mid M = m, Z = z) = \left[\prod_{t=1}^{n} P\big(x_{1t}, x_{2t}, (\jmath_{1t}\jmath_{2t}) \mid \imath_{1t}, \imath_{2t}, y_t\big)\, W(y_t \mid x_{1t}, x_{2t})\right] P(\mathbf{C} = c \mid \text{protocol inputs}), \tag{60}$$

其中 $\mathbf{C}$表示公开通信记录随机变量，而 $\imath_i^n = f_{(n)\,i}(M_{i0}, M_{i1})$ 是确定性编码器输入。爱丽丝在 $n$ 轮内的局部视图为 $U_i^{(n)} = (M_{i0}, M_{i1}, \imath_i^n, X_i^n, \mathbf{C})$，其中 $X_i^n = (x_{i1}, \ldots, x_{in})$ 是她的多址信道输入序列。

要得到在给定 $(M,\ Z)$ 条件下爱丽丝-$i$ 视图的边缘分布，我们必须对她无法观察到的所有变量求和。这些变量恰好是另一位发送方 Bob 的变量以及信道输出，也就是隐藏变量：$x_i^n$，$j^n$，$y^n$。

因此，爱丽丝-$i$ 的条件边缘分布的完整表达式如下：

$$P(U_i^{(n)} = u_i \mid M = m, Z = z) = \sum_{x_{\overline{i}}^n, j^n, y^n} \left[ \prod_{t=1}^{n} P\big(x_{1t}, x_{2t}, (j_{1t} j_{2t}) \mid \imath_{1t}, \imath_{2t}, y_t\big) W(y_t \mid x_{1t}, x_{2t}) \right] P(\mathbf{C} = c \mid M = m, Z = z, x_1^n, x_2^n, j^n, y^n). \tag{61}$$

如果通信记录生成律 $P(\mathbf{C} \mid \cdot)$ 与 $Z$ 无关，且对于 $P$满足无信号边缘分布等式，那么（61）右侧与 $z$无关，这意味着对爱丽丝-$i$的 ***Bob*** 安全性，$i \in \{1, 2\}$。

接下来，令该协议与前一个协议完全相同，不同之处在于：在第 1 轮中，Bob 收到自己的本地非信号输出（$j_1$，$j_2$）（或计算出 $y$ 的某个确定性函数）后，会广播一个单比特，例如

$$B = g(j_1, j_2, y, Z),$$

其中，$g$ 的选择使得 $B$ 取决于 $Z$ （例如 $B = Z_1$，或者 $B$ 是一个哈希函数，会泄露 $Z$的一部分）。这显然违反了鲍勃的安全性。 □

*D.* 非平凡三方无信号盒辅助下离散无记忆广播信道上的完美不经意传输

现在我们转向离散无记忆广播信道设置，探究在存在三方无信号关联时，网络不经意传输在离散无记忆广播信道上是否也存在类似的不可能性结果。

定理 *6.* 考虑一个离散无记忆广播信道，$W: \mathcal{X} \to \mathcal{Y}_1 \times \mathcal{Y}_2$。令非信号盒输入为确定性函数$\imath = f(M_{10}, M_{11}, M_{20}, M_{21}) \in \{0,1\}^n$，且 ***Bob-****i* 观察到信道输出 $y_i \in \mathcal{Y}_i, i \in \{1, 2\}$。假设三方共享一个三方非平凡 / 平凡非信号关联 $P(x, j_1, j_2 \mid \imath, y_1, y_2)$，满足标准***NS***约束 ***(24)-(26)***，那么在这种非信号辅助下，不经意传输（定义 ***10***）是不可能实现的。

证明。 考虑式（24）中所表达的从爱丽丝到两个接收方的非信号传递：

$$\begin{aligned} I(I; J_1, J_2 \mid Y_1, Y_2) &= I(I; J_1 \mid Y_1, Y_2) + I(I; J_2 \mid J_1, Y_1, Y_2) \\ &= 0. \end{aligned} \tag{62}$$

于是 $I(I; J_1 \mid Y_1, Y_2) = 0$。接下来，我们有以下等式链：

$$\begin{aligned} I(I; V_1 | Y_1, Y_2) &= I(I; J_1, Z_1, Y_1 | Y_1, Y_2) \\ &= I(I; J_1 | Y_1, Y_2) + I(I; Z_1 | Y_1, Y_2, J_1) + I(I; Y_1 | Y_1, Y_2, J_1, Z_1) \\ &= 0, \end{aligned} \tag{63}$$

其中，最后一个等式显然成立，因为 $Z_1 \perp\!\!\!\perp (I, Y_1, Y_2, J_1)$，这意味着鲍勃-1 的选择比特是本地生成的，且独立于爱丽丝的消息（$I - (Y_1, Y_2, J_1) - Z_1$）。

由于 $I$ 是所有消息的确定性函数，我们有：

$$\begin{aligned} I(I; V_1 | Y_1, Y_2) &= I(M_{10}, M_{11}, M_{20}, M_{21}; V_1 | Y_1, Y_2) \\ &= I(M_{1Z_1}, M_{1\overline{Z}_1}, M_{2Z_2}, M_{2\overline{Z}_2}; V_1 | Y_1, Y_2) \\ &= I(M_{1Z_1}, M_{1\overline{Z}_1}; V_1 | Y_1, Y_2) + I(M_{2Z_2}, M_{2\overline{Z}_2}; V_1 | Y_1, Y_2, M_{1Z_1}, M_{1\overline{Z}_1}) \\ &= 0. \end{aligned} \tag{64}$$

于是，$I(M_{1Z_1}, M_{\overline{1}Z_1}; V_1 | Y_1, Y_2) = 0$，并且有：

$$H(M_{1Z_1}, M_{1\overline{Z}_1} | Y_1, Y_2) = H(M_{1Z_1}, M_{1\overline{Z}_1} | Y_1, Y_2, V_1). \tag{65}$$

展开两边可得：

$$H(M_{1Z_1} | Y_1, Y_2) + H(M_{1\overline{Z}_1} | Y_1, Y_2, M_{1Z_1}) = H(M_{1Z_1} | Y_1, Y_2, V_1) + H(M_{1\overline{Z}_1} | Y_1, Y_2, V_1, M_{1Z_1}). \tag{66}$$

不经意传输的正确性（零差错传输）要求 $H(M_{1Z_1}|V_1) = 0$。然后，由于条件化不会增加熵，因此 $H(M_{1Z_1}|Y_1, Y_2, V_1) = 0$。接下来：

$$H(M_{1Z_1}|Y_1, Y_2) + H(M_{1\overline{Z}_1}|Y_1, Y_2, M_{1Z_1}) = H(M_{1\overline{Z}_1}|Y_1, Y_2, V_1, M_{1Z_1}). \tag{67}$$

另一方面 $H(M_{1Z_1}|Y_1, Y_2, V_1, M_{1Z_1}) \leq H(M_{1Z_1}|Y_1, Y_2, M_{1Z_1})$。如果该单调性中的等式成立（满足 SfA），则 (67) 要求 $H(M_{1Z_1}|Y_1, Y_2) = 0$，这意味着鲍勃-1 选择的消息完全由广播信道输出决定，且独立于他的最终视图 $V_1$，包括他的选择比特 $Z_1$。这与不经意传输的因果性相矛盾。如果单调性中的不等式成立，则违反 (67)。

在上述证明中，我们考虑了通过噪声广播信道进行零差错传输，这是一个非常严格的假设。˙现在，考虑渐近正确性约束 (30) $\lim_{n\to\infty}\Pr\{M_{1Z_1} \neq M_{1Z_1}\} = 0$。换一种形式˙$\Pr\{M_{1Z_1} \neq M_{1Z_1}\} = \varepsilon_n$，其中 $\varepsilon_n \to 0$ 当 $n \to \infty$ 时成立。于是，法诺不等式给出：

$$H(M_{1Z_1}|V_1) \leq h(\varepsilon_n) + \varepsilon_n \log_2 |\mathcal{M}_{1Z_1}|. \tag{68}$$

由于 $M_{1Z_1} \in \{0,1\}^{k_1}$ 和 $k_1$ 是消息长度，因此：

$$H(M_{1Z_1}|V_1) \leq \eta_n, \tag{69}$$

其中 $\eta_n \triangleq h(\varepsilon_n) + \varepsilon_n k_1$。现在，从 (66) 开始：

$$H(M_{1Z_1}|Y_1, Y_2) + H(M_{1\overline{Z}_1}|Y_1, Y_2, M_{1Z_1}) = H(M_{1Z_1}|Y_1, Y_2, V_1) + H(M_{1\overline{Z}_1}|Y_1, Y_2, V_1, M_{1Z_1}). \tag{70}$$

代入 (69)，得到：

$$H(M_{1Z_1}|Y_1, Y_2) + H(M_{1\overline{Z}_1}|Y_1, Y_2, M_{1Z_1}) \leq H(M_{1\overline{Z}_1}|Y_1, Y_2, V_1, M_{1Z_1}) + \eta_n. \tag{71}$$

另一方面 $H(M_{1Z_1}|Y_1, Y_2, V_1, M_{1Z_1}) \leq H(M_{1Z_1}|Y_1, Y_2, M_{1Z_1})$。如果该单调性中的等式成立（满足 SfA），那么 $H(M_{1Z_1}|Y_1, Y_2) \leq \eta_n$，且当 $n \to \infty$ 时，$\eta_n$ 消失。这与不经意传输的因果性相矛盾。如果不等式成立，则与爱丽丝的完美保密性相矛盾。关于鲍勃-2 的证明可直接得出。至此，证明完成。□

### *E. O*双部非信号辅助噪声点对点离散无记忆信道上的不经意传输不可能性

我们已经证明，在三部非信号辅助离散无记忆多址信道和三部非信号辅助离散无记忆广播信道上，不存在同时满足可靠性和 SfA 的不经意传输协议序列。这构成了一个强有力的不可能性结果，因为它完全不受底层信道的噪声行为和噪声类型影响。

此外，这一不可能性不仅在半诚实模型下成立，也适用于更严格的保密性概念，包括有界恶意方 [6] 和无界恶意方 [20]。从这个意义上说，我们的结果确立了一种严格强于现有计算不可能性结果的不可能性，因为即使存在强大的无信号关联，不经意传输仍然无法实现。

Fawzi 和 Ferm´e [29] 证明，二方无信号相关性既不能提高离散无记忆信道的容量，也不能提高离散无记忆多址信道的和容量。从技术上说，他们的结果适用于这样的情形：爱丽丝-1与 Bob 之间独立共享无信号辅助，其描述为 $P^1(x_1, y_1 \mid \imath_1, y)$；爱丽丝-2与 Bob 之间也独立共享无信号辅助，其描述为 $P^2(x_2, y_2 \mid \imath_2, y)$。我们将其称为独立 NS 辅助。从网络不经意传输的角度来看，我们的不可能性结果可以推广至二方 NS 辅助的噪声离散无记忆信道和独立 NS 辅助的离散无记忆多址信道。然而，在此类 NS 辅助下，较弱的交互式密码任务（例如比特承诺和秘密密钥协商）是否可行，仍是一个开放问题。

*F.* 关于双方无信号辅助的噪声离散无记忆多址信道上的不经意传输

迄今为止，我们考察了在三方 NS 关联辅助下，通过噪声信道实现网络不经意传输的可行性。我们已经证明，在这种情形下，完美不经意传输和不完美不经意传输均无法实现。具体而言，任何三方 NS 关联要么违反 SfA，要么向接收方泄露非预期信息，要么与不经意传输固有的因果结构相矛盾。

这就引出了一个自然而核心的问题：能否在由二方 NS 关联辅助的共享噪声信道上实现不经意传输，其中无信号资源仅在多址信道模型中的两个发送方之间共享（图 1-$(b)$），或者在广播信道模型中的两个接收方之间共享？在本工作中，我们将注意力限制在多址信道模型上，并研究两个发送方由二方 NS 关联辅助的情形。

**定理7.** *考虑一个噪声离散无记忆多址信道，* $W:\ \mathcal{X}_1 \times \mathcal{X}_2 \to \mathcal{Y}$。*假设爱丽丝-1 与爱丽丝-2 共享一个二方非信号传递（NS）盒子* $P_{X_1X_2|I_1I_2}$，*其满足 (2) 与 (3)，而接收方 Bob 无法访问该 NS 盒子。那么，无法推导出在该离散无记忆多址信道上实现完美不经意传输的普遍信息论不可能性。*

证明。令 $M_i = (M_{i0},\ M_{i1})$、$i \in \{1,2\}$ 在 $\{0,1\}^{k_i}$ 上独立且均匀分布，并令$Z = (Z_1,\ Z_2)$表示 Bob 的选择比特。令 $V = (Y^n,\ \mathbf{C}\ Z)$ 为 Bob 的完整视图。完美不经意传输的正确性／零误差传输意味着

$$H(M_{1Z_1}, M_{2Z_2} \mid V) = 0, \tag{72}$$

因此 $I(M_{1Z_1},\ M_{2Z_2}; Y^n \mid Z) = H(M_{1Z_1},\ M_{2Z_2})$。完美 SfA-$i$ 要求 $I(M_{i\bar{Z}_i};\ V) = 0,\ i = \{1,2\}$。

在三方无信号辅助情形下，由无信号约束可推出$I(I_i;\ Y^n,\ J \mid I_{\bar{i}}) = 0$，其中 $J$是 Bob 的无信号输出。然而，此处唯一的无信号约束是（2）和（3），且它们仅涉及发送端变量。由于 Bob 既无法观测 $(X_1,\ X_2)$，也无法观测任何 NS 盒输出，因此没有约束能够保证 $I(I_i;\ Y^n \mid I_{\bar{i}}) = 0$。因此，推导

$$H(M_{iZ_i} \mid Y^n, Z, I_{\bar{i}}) = 0, \tag{73}$$

无法由 SfA-$i$ 建立。

因此，命题 2 中用于迫使 $M_{i\bar{Z}_i}$ 泄漏的熵恒等式并不成立。然而，如果允许各方串通，那么每个发送方都可以向 Bob 泄露私有信息，从而使 OT 要求失效。

□

*G.* 无信号关联与 *OT* 中选择依赖因果性的消失

不经意传输本质上是一种因果性 密码学原语：接收方的最终重构消息实质上取决于本地生成的选择变量。具体而言，Bob-$i$ 将其估计值 $\hat{}M_{iZ_i}$ 作为其全部视图 $V_i$的确定性函数获得；该视图包括 NS盒的输出、$\hat{}\,\hat{}$ 公开通信记录，以及他的私人选择 $Z_i$。形式上，$H(M_{iZ_i} \mid V_i) = 0$，而 $M_{iZ_i}$无法从 $V_i \setminus \{Z_i\} \triangleq (J_i,\ \mathbf{C}Y_i^n)$重构。在渐近正确协议中，$\hat{}\ M_{iZ_i}$ 以趋近于零的差错概率与真实消息 $M_{iZ_i}$ 一致，因此 $H(M_{iZ_i} \mid V_i) \to 0$。因此，选择变量的因果作用体现在最终解码后的消息层面，而非 NS盒的原始输出中。

这一熵关系体现了 OT 因果性的一个基本方面：若不知道选择比特，就无法完全确定^接收方输出。换言之，$M_{iZ_i}$ 中的不确定性必然反映 $Z_i$中的不确定性，解码过程必须保留这种依赖关系。因此，任何有效的 OT 协议都必须确保接收方的最终输出在信息和因果层面上都与选择变量相关联。

NS 关联从根本上破坏了这种因果结构。非信号约束保证，在给定信道输出的条件下，接收方的整个视图（包括最终输出）都不会携带关于发送方私有输入的额外信息。因此，任何能够使接收方

恢复所选消息的信息都必须已包含在信道输出本身中。这迫使对 $M_{iZ_i}$ 的解码渐近地独立于选择变量 $Z_i$，从而消除了选择对最终输出的因果影响。

从熵视角来看，无信号约束有效地将系统推向这样一种状态：$H(M_{iZ_i} \mid Y_1,\ Y_2) \to 0$ (离散无记忆广播信道)，使得接收方输出渐近地由信道观测决定。在这种状态下，选择变量的熵贡献消失，违背了不经意传输的一项基本要求，即输出取决于选择。总之，非信号关联抹去了接收方的选择影响传递消息的因果路径。尽管非信号关联能够引入强非局域关联，但它们同时也施加了一种信息对称性，阻止了不经意传输所需的不对称、依赖选择的信息流。这种因果关系的坍塌正是本文所确立的不可能性结果的核心。

### *H.* 基于非局域原语的不经意传输与非信号辅助

Wolf和Wullschleger提出了一项密切相关且颇具影响力的结果 [39], ，他们研究了 PR 非局域盒的密码学能力。在他们的模型中，两方可以使用一种双边非信号原语：双方各输入一个单比特，并各自收到一个均匀随机的输出比特，且输出的异或等于输入的与。该工作的核心贡献在于证明了不经意传输与 PR 原语之间存在精确的信息论等价关系：使用一次 PR 盒即可实现一个完美安全的 1 取 2 OT 实例；反过来，使用一个不经意传输实例也可以模拟一个 PR 盒。这两种归约都是单份、完美（零错误）且信息论安全的，因此确立了 PR 盒是在非信号设定下实现不经意传输的完备原语。在他们基于 PR 的构造中，PR 盒被视为一种抽象的双边密码学原语，而不经意传输则通过双方之间的局部操作和经典消息交换直接归约得到。该模型未嵌入物理通信网络，也未施加任何编码器—信道—解码器结构。

乍看之下，我们的不可能性结果似乎与先前关于不经意传输与 PR 非局域性之间存在密码学等价性的研究相矛盾。该研究表明，单次使用 PR 原语便足以实现信息论安全的不经意传输；反过来，也可以利用不经意传输模拟 PR 关联。只需注意到这两种场景采用的资源模型和因果模型存在根本差异，这种表面上的矛盾便迎刃而解。在基于 PR 的构造中，PR 盒被视为一种抽象的双边密码学原语，直接利用其输入—输出关联来实现不经意传输功能；这种归约是独立的、单份的，并且是在其他方面均有无噪声公共信道的场景中完成的，不会将该原语嵌入物理通信网络。具体而言，PR 盒作为一种非局域原语，用来提供关键的密码学关联，不受任何中间噪声信道或操作性编码—解码结构的约束。与此相反，在我们的模型中，NS 关联仅作为辅助资源，用于帮助通过受物理条件约束的信道进行通信，例如离散无记忆多址信道或离散无记忆广播信道。所有实际信息流都必须经过噪声信道，而 NS 盒本身只能提供关联，不能传递信息。因此，协议必须严格遵循操作性的因果顺序——编码、信道传输和解码；而抽象的 PR 盒框架中并不存在这一顺序。我们的不可能性结果恰恰利用了这种操作因果性：在不经意传输中，接收方的选择必须在因果上影响解码后的消息；而无信号约束禁止这一选择对发送方视角产生任何反向影响。基于 PR 的归约中不存在这种矛盾，因为原语本身已经包含了所需的非局域依赖。因此，我们的结果并不与 PR–OT 等价性相矛盾，而是表明，当 NS 关联仅限于在具有因果顺序的通信协议中发挥辅助作用时，无法普遍保证不经意传输的安全性。这一区别凸显了作为独立密码学功能使用的非局域原语，与作为通信网络中辅助关联使用的 NS 资源之间的根本差异。

Short、Gisin 和 Popescu 在研究非局域关联的密码学能力时，指出了 NS 资源的其他密切相关的概念局限 [40] ， Buhrman 等人 [41], 则展示了如何利用非局域盒执行任意双方安全计算。在 [40], 作者研究了理想 OT 盒与 PR 非局域盒之间的操作性差异，并指出，复现相同的输入输出概率分布通常不足以复现某种原语的密码学功能。特别是，他们强调，除了匹配联合分布之外，还必须遵循理想功能输入与输出的时间和因果结构。对于 OT 盒，只有发送方输入其信息后，接收方的输出才有定义；而对于任何 NS 盒，尤其是 PR 盒，接收方都必须能够获得有效输出，无论另一方是否已经使用该盒。这一根本差异意味着，尽管可以在分布层面利用 PR 盒和经典通信模拟 OT 盒，但该模拟并未保留 OT 功能固有的因果顺序，因此不具备普遍可组合性。正如 Short、Gisin 和 Popescu 用口号所概括的那样：“无信号——无需在最后之前进行测量——无承诺”：无信号约束使协议无法强制要求某一方在协议较早阶段就已确定一个与因果相关的局部输入。我们的模型和结果恰恰体现了通信理论场景中的同一障碍。在本文考虑的 NS 辅助信道模型中，NS 盒仅作为辅助资源提供，所有信息都必须通过受物理条件约束的广播信道或多址信道传递。因此，协议必须明确遵循编码、信道传输和解码的操作顺序。由此，无信号约束意味着，辅助资源无法确保某一方的局部选择已在其他各方生成输出之前通过因果方式生效。因此，尽管 NS 关联可以复现某些输入—输出统计特性，但通常无法复现通信网络中实现 OT 所需的因果结构。从这个意义上说， [40]关于非局域模拟的研究从操作性和可组合性的角度，证实了我们在 NS 辅助信道模型中所确立的局限。

一旦明确因果性的作用，Wolf和Wullschleger的可能性结果与Short、Gisin和Popescu的不可能性结果之间表面上的矛盾便迎刃而解。Wolf和Wullschleger在输入—输出关联层面确立了不经意传输与PR 非局域性之间的功能等价性：PR 盒可以模拟不经意传输盒子的分布，反之亦然，且不对双方输入的时机施加任何操作约束。相比之下，Short、Gisin和Popescu表明，非信号关联无法实现承诺类原语所要求的时间绑定，因为NS条件要求一方的输出必须有明确定义，且不取决于另一方是否已经行动。在我们的模型中，不经意传输嵌入一个具有因果顺序的通信协议中——包括编码、物理信道传输和解码——因此隐含地要求私人选择与最终输出之间存在因果依赖。非信号辅助虽然能够生成关联，却无法施加这种因果顺序，因此无法普遍保证通过通信信道实现的OT安全性。从这一角度看，Wolf和Wullschleger的可能性结果与Short、Gisin和Popescu的不可能性结果完全相容：前者讨论的是在关联层面对理想功能的模拟，而后者以及我们的工作则揭示了无信号资源在操作受限的密码协议中实现因果不可逆性的根本局限。

NS 盒所施加的因果性与不经意传输内在的因果性密切相关，但从根本上说截然不同。NS 强制的是一种消极的结构性因果性概念，禁止一方的局部输出分布依赖于另一方的输入。相比之下，不经意传输要求的是一种积极的功能性因果性概念：接收方的私人选择必须在因果上决定重构消息。我们不可能性结果背后的关键观察是，NS 关联无法用于强制实现这种功能性因果性。若强制要求某项私人选择已被应用，另一方就能检测到这一事实，从而违反无信号性。因此，尽管 NS 资源可能复现 OT 盒的统计特性，但当它们嵌入具有因果顺序的通信协议时，无法施加不经意传输所要求的因果不可逆性。这种结构性因果性与功能性因果性之间的不匹配

既解释了基于抽象 OT 盒模拟的可能性结果，也解释了 NS 辅助通信模型的不可能性结果。

## IV. 讨论

我们研究了在无信号辅助噪声信道上实现网络不经意传输的可行性，重点关注多址信道和广播信道。我们的结果表明，存在三方无信号关联时，网络不经意传输是不可能实现的，无论这些关联是平凡的还是非平凡的。由于经典关联和量子关联都严格包含于无信号关联集合中，这一结果意味着，发送方与接收方之间共享的任何三方纠缠都必然导致信息泄漏，进而违反不经意传输的保密要求。

推动本研究的一个核心问题是：量子关联（纠缠），甚至 PR 盒等超量子关联，能否用于提升网络场景下共享噪声信道的不经意传输容量。我们的研究结果表明，在所考虑的系统模型中，三方无信号关联会从根本上损害不经意传输的安全性，因此无法用于提升不经意传输容量。

尽管如此，我们的分析表明，二方无信号关联——具体而言，即多址信道模型中发送方之间共享的关联，或广播信道模型中接收方之间共享的关联——在各方不允许串通时，仍可能满足不经意传输的安全性要求。本文针对多址信道模型考察了这一问题。这类二方无信号关联能否用于提升基础噪声信道的不经意传输容量，仍是一个开放问题。探讨这一问题是未来研究中一个自然且重要的方向。

## 致谢

作者感谢 Omar Fawzi 和 Matthieu Bloch 在本研究过程中进行的宝贵讨论。

## 参考文献

[1]M. O. Rabin，《如何通过不经意传输交换秘密》，Aiken 计算实验室，哈佛大学，马萨诸塞州剑桥，技术报告 TR-81，1981。[2] S. Even、O. Goldreich 和 A. Lempel，《用于签署合同的随机化协议》，《*ACM* 通讯》，第 28 卷，第 637–647 页，1985。[3] Y. Dodis、S. J. Ong、M. Prabhakaran 和 A. Sahai，《论不完美随机性下密码学的（不）可能性》，载于第 *45* 届 *IEEE* 计算机科学基础年会论文集（*FOCS*），2004 年，第 196–205 页。[4] M. Santha 和 U. V. Vazirani，《从半随机源生成拟随机序列》，《计算机与系统科学杂志》，第 33 卷，第 1 期，第 75–87 页，1986。[5] C. Cr´epeau 和 J. Kilian，《基于弱化的安全假设实现不经意传输》，载于第 *29* 届 *IEEE* 计算机科学基础研讨会论文集（*FOCS*），美国纽约州怀特普莱恩斯，1988 年，第 42–52 页。[6] A. C. A. Nascimento 和 A. Winter，《噪声资源的不经意传输容量》，*IEEE* 信息论汇刊，第 54 卷，第 6 期，第 2572–2581 页，2008 年 6 月。[7] ——，《噪声关联的不经意传输容量》，载于*IEEE* 国际信息论研讨会（*ISIT*）论文集，美国华盛顿州西雅图，2006 年，第 1871–1875 页。[8] R. Ahlswede 和 I. Csisz´ar，《论不经意传输容量》，载于*IEEE* 网络信息论研讨会（*ITW*）论文集，希腊沃洛斯，2009 年，第 1–3 页。[9] C. Cr´epeau、K. Morozov 和 S. Wolf，《几乎任意噪声信道上的高效无条件不经意传输》，载于*SCN* 论文集，《计算机科学讲义》系列，第 3352 卷。德国柏林：Springer-Verlag，2005 年，第 47–59 页。

[10] H. Imai、K. Morozov 和 A. C. A. Nascimento，《擦除信道的不经意传输容量》，载于 IEEE 国际信息论研讨会（ISIT）论文集，美国华盛顿州西雅图，2006 年，第 1428–1431 页。[11] S. Suda、S. Watanabe 和 H. Yamaguchi，《通过交互式擦除仿真改进不经意传输容量的下界》，载于 IEEE 国际信息论研讨会（ISIT）论文集，2024 年，第 1872–1877 页。[12] S. Suda 和 S. Watanabe，《利用极化与交互改进不经意传输容量的下界》，arXiv:2501.11883 [cs.IT], 2025。[13] A. Shekofteh 和 R. A. Chou，《噪声信道中存在串通且非复制服务器时的 SPIR》，载于第 60 届阿勒顿通信、控制与计算会议论文集，2024 年，第 1–6 页。[14] ——，《二进制擦除信道上的单服务器 SPIR：噪声旁信息的益处》，载于第 61 届阿勒顿通信、控制与计算会议论文集，2025 年，第 1–5 页。[15] ——，《改进二进制擦除信道上单服务器 SPIR 的可达速率》，载于第 61 届阿勒顿通信、控制与计算会议论文集。伊利诺伊州厄巴纳：阿勒顿通信、控制与计算会议，2025 年。[16] H. Aghaee 和 C. Deppe，《噪声多址信道的不经意传输容量》，载于 IEEE 国际信息论研讨会（ISIT）论文集，美国密歇根州安娜堡，2025 年，第 1–6 页。[17]H. Aghaee、B. Akhbari 和 C. Deppe，《网络不经意传输：极限与容量》，arXiv:2501.17021 [cs.IT], 2025。[18] H. Aghaee、C. Deppe 和 H. Boche，《通过噪声广播信道实现网络不经意传输》，arXiv:2510.25343v1 [cs.IT], 2025。[19] ——，《离散无记忆广播信道上的不经意传输》，载于 IEEE 国际通信会议（ICC2026）论文集，2026 年，即将刊出。[20] H. Aghaee、C. Deppe 和 B. Akhbari，《不经意传输的信息论极限》，载于 IEEE 全球通信会议（GLOBECOM）论文集，中国台湾台北，2025 年。[21] F. Granelli、R. Bassoli、J. N¨otzel、F. H. P. Fitzek、H. Boche、N. L. S. da Fonseca 和 A. Guerrieri，《面向未来经典-量子通信网络的新型架构》，《无线通信与移动计算》，第 2022 卷，文章编号 3770994，2022 年 1 月。[22] A. K. Ekert，《基于贝尔定理的量子密码学》，《物理评论快报》，第 67 卷，第 6 期，第 661–663 页，1991。[23] C. H. Bennett、P. W. Shor、J. A. Smolin 和 A. V. Thapliyal，《量子信道的纠缠辅助容量与反向香农定理》，IEEE 信息论汇刊，第 48 卷，第 10 期，第 2637–2655 页，2002。[24] M.-H. Hsieh、I. Devetak 和 A. Winter，《量子多址信道的纠缠辅助容量》，IEEE 信息论汇刊，第 54 卷，第 7 期，第 3078–3090 页，2008。[25] J. N¨otzel，《纠缠赋能通信》，IEEE 信息论精选领域期刊，第 1 卷，第 2 期，第 401–415 页，2020。[26] F. Leditzky、M. Alhejji、E. Levin 和 G. Smith，《利用多址信道进行博弈》，《自然通讯》，第 11 卷，第 1 期，文章编号 1497，2020 年 3 月。[27] A. Seshadri、F. Leditzky、V. Siddhu 和 G. Smith，《论多址信道相关性辅助和容量的分离》，IEEE 信息论汇刊，第 69 卷，第 9 期，第 5805–5844 页，2023 年 9 月。[28] U. Pereg、C. Deppe 和 H. Boche，《量子干扰信道：容量界与协议》，IEEE 信息论汇刊，第 69 卷，第 5 期，第 1–15 页，2023。[29] O. Fawzi 和 P. Ferm´e，《利用非信号关联进行多址信道编码》，IEEE 信息论汇刊，第 70 卷，第 1693–1719 页，2024。[30] J. Yard、P. Hayden 和 I. Devetak，《量子多址信道的容量定理》，IEEE

《信息论汇刊》，第57卷，第10期，第7147–7167页，2011年。[31] U. Pereg、C. Deppe 和 H. Boche，《量子广播信道：容量与协议》，《 IEEE 信息论汇刊》，第 67 卷，第 12 期，第 1–20页，2021年。[32] Y. Quek 和 P. W. Shor，《双发送方双接收方信道的量子与超量子增强》，《物理评论A》，第95卷，第5期，文章号052329，2017年5月。[33] J. F. Clauser、M. A. Horne、A. Shimony 和 R. A. Holt，《旨在检验局域隐变量理论的实验提案》，《物理评论快报》，第23卷，第15期，第880–884页，1969年10月。[34] S. Popescu 和 D. Rohrlich，《作为公理的量子非局域性》，《物理学基础》，第24卷，第3期，第379–385页，1994年3月。[35]J. Hawellek、A. Mohan、H. Aghaee 和 C. Deppe，《纠缠发送方的干扰信道》，arXiv 预印本 arXiv:2411。10067 [量子物理], 2024年11月。[36] ——，《纠缠发送方的干扰信道》，已被 IEEE 国际信息论研讨会（ISIT）2025 接收发表。[37] H. Aghaee 和 C. Deppe，《关于纠缠发送方的干扰信道》，载于《2025年 IEEE 信息论研讨会（ITW）》，2025年，第1–6页。[38] R. A. Chou，《成对不经意传输》，载于《2020年 IEEE 信息论研讨会（ITW）》，2021年，第1–5页。[39] S. Wolf 和 J. Wullschleger，《不经意传输与非局域性》，《IEEE 信息论汇刊》，第52卷，第6期，第2519–2528页，2006年。[40] A. J. Short、N. Gisin 和 S. Popescu，《无比特承诺的物理学：广义量子非局域性与不经意传输》，《量子信息处理》，第5卷，第2期，第131–143页，2006年。[41] H. Buhrman、M. Christandl、F. Unger、S. Wehner 和 A. Winter，《超强非局域性对密码学的影响》，英国皇家学会会刊A辑：数学、物理与工程科学，第462卷，第2071期，第1919–1932页，2006年2月。 [在线]。链接：https://doi.org/10.1098/rspa.2006.1663