arXiv:2603.02078v1 [quant-ph] 2 Mar 2026

在玻色任意变化信道上进行数据传输时传递相关性

Janis N¨otzel，Florian Seitz

2026年3月3日

摘要

共享随机性是保护可对称化通信系统免受任意变化干扰者侵害的核心要素。然而，考虑到干扰者的存在，如何分发这一宝贵资源便成为一个问题。已有多项研究探讨了利用外部源完成这一任务。本文基于最标准的光通信模型，展示了发送方和接收方如何利用由发送方制备并传输的经典相关热光或纠缠双模压缩态，在分发阶段抵御能量受限干扰者的干扰攻击。在我们的模型中，发送方和接收方都只能使用零差探测，并且发送方还必须遵守功率限制。

1 引言

任意变化信道（AVC）在 [7]中被提出，并发展成为受干扰影响的通信系统的标准信息论模型。一个AVC的容量 C 是否为正这一问题被证明是非平凡的 [16, 1, 14]: 一旦发送方与接收方之间可用的共享随机性数量随码长¯多项式增长，系统的容量 C 便由一个类似于香农容量公式的信息论量来描述。为了描述 C，AVC的可对称化性这一概念得以确立 [16, 14] （另见 [5]）。可对称化AVC的容量为零，而不可对称化AVC的容量公式等于同一AVC在发送方与接收方之间具有共享随机性时的容量公式。

信号处理中对任意变化信道的研究始于 [15], ，其中接收信号被建模为 $y = s + x + z$， s 为干扰信号， x 为发送信号， z为加性白高斯噪声（$s, x, z \in \mathbb{C}$）。模型 [15] 在量子信号处理中的对应形式由相干态 $|s\rangle, |x\rangle$ 在透射率为η的分束器上干涉给出，接收信号$|\sqrt{\eta}s + \sqrt{1-\eta}x + z\rangle$ 受到经典高斯噪声 z[20]的扰动。 ——

AVC 展现出超激活 [11]和 C [10, 9]的不连续性。可对称化性条件无法计算 [13], ，但可以高效地计算近似解 [23]。只要存在任意与干扰者独立 的相关双体源¯，就 C [3, 8]足以保证系统运行。人们研究了有色高斯噪声 [21]和原生量子任务 [2, 12], 下不同类型干扰的容量，并观察到类似的结果。在某些情况下，共享随机性所需的精确阈值也已为人所知 [6]。

这些结果表明，共享（公共）随机性是干扰环境下通信的关键要素，而且极少量的共享随机性就足以实现随机容量 C。

然而，以下核心问题此前尚未被提出：假设一个可对称化 *AVC*，且不存在预共享相关随机性，发送方和接收方如何开始通信？例如，他们如何建立共享随机性的来源？

在本研究中，我们首次解决了这一高度矛盾的情形。我们证明，在每次传输均受能量限制的条件下，无论是特定的经典相关（非纠缠）量子态所产生的关联，还是纯量子资源，即共享纠缠态，都可用于实现正容量。最重要的是，这些相关态由发送方制备，并在干扰者攻击下与接收方共享。

为了模拟发送方不制备并共享相关分布的情形，我们让发送方和干扰者在传输中使用任意位移热态 $S_N(\alpha)$，并分别对发送方施加 $N+|\alpha|^2 < E$、对干扰者施加 $N+|\beta|^2 < P$ 的限制。为方便起见，两路信号在 50:50分束器处混合；这是一种标准的量子光通信模型 [17, 18]。对于 $P \geq E$ 的情形，我们证明该信道的容量为零。

由于通过直接发送位移热态 $S_N(\alpha)$，并借助 $|\alpha|^2 + N \leq P$ 来创建任何有助于数据传输的共享资源，都将意味着 $C > 0$，因此任何此类尝试都必然失败。

然而，如果我们赋予发射器生成双部态 ρ_{RS} 的能力，使得每个约化态 ρ_R 都满足 $\rho_R = S_N(\alpha)$，其中某个 $(\alpha,\ N)$ 满足 $|\alpha|^2 + N \leq E \leq P$，则可以证明相应的容量为正。我们的约束所允许的态类 ρ_{RS} 既包括双模压缩真空态（TMSV）态（它们是纠缠态），也包括特定的双模热态（它们仅具有经典相关性）。为了利用相关态进行数据传输，发送方在传输 R 系统的同时，存储 ρ_{SR} 的 S 系统。随后，发送方和接收方均进行零差测量，并利用所得结果生成一个相关随机变量。之后，他们可以按照 [3] 中概述的思路，利用该变量获得正容量。

2 系统模型与结果

系统模型

定义 1（确定性码（DC））。一个 $(n,\ \lambda)$ *DC* $\mathcal{C}$ 仅允许发送方使用 $\mathcal{S} = \{S_N(\alpha):\ N+|\alpha|^2 \leq E\}$，以及干扰者处的 $\mathcal{J} = \{S_N(\beta):\ N+|\beta|^2 \leq P\}$。它由函数 $f\colon\ [M] \to \mathcal{S}^n$ 以及两两不相交的译码集合 $D_m \subset \mathbb{R}^n$、$m = 1$、.....、M 组成，使得

$$\mathrm{succ}(\mathcal{C}) := \min_{\mathbf{j}^n \in \mathcal{J}^n} \frac{1}{M} \sum_{m=1}^{M} \int_{D_m} \left[\prod_{i=1}^{n} \mathrm{Tr} |\hat{x}\rangle\langle\hat{x}| \mathcal{N}\left(S(\mathbf{j}^n) \otimes S(f(m))\right) \right] dx^n \geq 1-\lambda. \tag{1}$$

非负数 R 称为以 DCs 可达，当且仅当存在一列 DCs，使得 下极限 $_{n\to\infty}\ \frac{1}{n}$ 对数 $M_n \geq R$。相应的容量 C 定义为所有可达数 R 的上确界。

定义 2（公共随机性辅助码（CRAC））。一个（n, M, λ） *CRAC* $\mathcal{C}$ 由一个（$n, \lambda^{(\gamma)}$） *DC* 集合 $\{\mathcal{C}^{\gamma}\}_{\gamma=1}^{\Gamma}$ 组成，其中 $\Gamma \in \mathbb{N}$。*CRAC* 的成功概率定义为

$$\mathrm{succ} = \min_{\mathbf{j}^n \in \mathcal{J}^n} \frac{1}{M \cdot \Gamma} \sum_{m,\gamma=1}^{M,\Gamma} \int_{D_m^{\gamma}} \left[\prod_{i=1}^{n} \mathrm{Tr} |\hat{x}\rangle\langle\hat{x}| \mathcal{N}\left(S(\mathbf{j}^n) \otimes S(f^{\gamma}(m))\right) \right] dx^n \geq 1 - \lambda. \tag{2}$$

若存在一个 $CRACs$序列，使得$\mathrm{liminf}_{n\to\infty} \frac{1}{n} \log\, M_n \geq R$，则称非负数 R 在 $CRACs$ 下可达。相应的容量 $\bar{C}$ 是所有可由 *CRAC* 达到的数 R 的上确界。

注 1. 定义 *2* 中提到的数 $\lambda^{(n)})$ 是为了符合定义 *1*，但这些数本身与定义 *2* 无关。

定义 3（相关码（CC））。一个（n, M, λ）*CC* $\mathcal{C}$ 使用扩展发送方字母表$\mathcal{Q} = \{\rho_{SR} \colon\ \rho_R \in \mathcal{S}\}$，其中同样有 $\mathcal{S} = \{S_N\ (\alpha) \colon\ N + |\alpha|^2 \leq E\}$。此外，它允许发送方对系统的 S 部分进行零差测量，并根据测量结果改变系统上的码参数。因此，一个（因果）编码由一组函数 f_i: $[M] \times R^i \to \mathcal{Q}$ 描述，其中 $i = 0$、.....、$n-1$，以及两两不相交的译码集合$D_m \subset \mathbb{R}^n$、 $m = 1$、.....、M。*CC* 的成功概率定义为

$$\mathrm{succ} = \min_{\mathbf{j}^n \in \mathcal{J}^n} \frac{1}{M} \sum_{m=1}^{M} \int_{D_m} \int_{r^n} \prod_{i=1}^{n} p(x_i, r_i | m, r^{i-1}) dr^n dx^n \tag{3}$$

其中条件概率密度定义为

$$p(x_i, r_i | m, r^{i-1}) = \mathrm{Tr}(H_{x_i} \mathcal{N}([(\mathbb{1} \otimes H_{r_i}) S(f(m, r^{i-1}))(\mathbb{1} \otimes H_{r_i})] \otimes S(\mathbf{j}_i))). \tag{4}$$

非负数 R 称为关于 CCs 可达，如果存在一个 CCs 序列，使得 $\mathrm{liminf}_{n\to\infty} \frac{1}{n} \log\, M_n \geq R$。相应的容量 C_Q 是所有可达数 R的上确界。

注 2. 每个函数 $f_i^{(m)}$ 都使发送方能够根据先前的 i 测量结果，决定接下来创建哪种状态，以传输消息 m。

注 3. 状态 $S_N(\alpha)$ 的一种重要推广是双模压缩真空态

$$|TMSV\rangle = \cosh(2r)^{-1/2} \sum_{n=0}^{\infty} \tanh(r)^n |n\rangle_A |n\rangle_B, \tag{5}$$

其中 r是压缩参数，且 $\mathrm{tr}_B(|TMSV\rangle\langle TMSV|) = S_{\cosh(r)^2-1}(0)$。这些状态是纠缠态。另一个重要例子是热态 S_{2N} 经过 50 :50分束器混合后，得到的状态为

$$S_N^{(2)} = \tfrac{1}{\pi \cdot 2N} \int \exp(-|\alpha|^2/2N) |\tfrac{\alpha}{\sqrt{2}}\rangle\langle\tfrac{\alpha}{\sqrt{2}}| \otimes |\tfrac{\alpha}{\sqrt{2}}\rangle\langle\tfrac{\alpha}{\sqrt{2}}| d\alpha. \tag{6}$$

同样，该状态的边缘分布等于 $S_N(0)$。第二类状态具有经典相关性，但两个模式 A 和 B 并未纠缠。

基于此定义，我们可以陈述主要定理。

定理 1。 以下结论成立：

1. 若 $P \geq E$，则 $C = 0$*2.* 若 $E < P$，则 $C > 0$*3.* 对所有 E、$P > 0$，我们有 $C > 0$*4.* 对所有 E、$P > 0$，我们有 $C_Q > 0$。

注 4。 我们基于双模压缩真空态 (5)中的关联证明性质 *4*。不过我们注意到，对于(6)中的 $S_N^{(2)}$ 这类状态，完全相同的证明策略同样适用。因此，经典关联完全足以证明 $C_Q > 0$，尽管 $\mathcal{Q}$ 的不同成员显然会导致关于 C_Q的不同下界。

注 5。 由于我们的 *CC* 定义并未明确发送端同相测量的确切时刻，如果发送端测量在传输之前进行，原则上可能违反峰值功率约束。另一方面，可靠且有意地制备高能态的能力，与利用这类状态偶尔出现的能力并不相同，因此我们的结果仍可能有助于阐明关联在数据传输中的潜在用途。

性质 (1) 的证明：我们沿用 [15] 中的论证。假设 $P \geq E$。对于每个具有信号 $\mathbf{s}^n = (\alpha_m^n, N_m^n)$ 的 (n, λ) DC$\mathcal{C}$，我们考虑相应的干扰序列 $\mathbf{j}^n = \mathbf{s}^n$。那么，对于任意解码器，我们有

$$\mathrm{err}(\mathcal{C}) = \max_{\mathbf{j}^n} \frac{1}{M} \sum_m \mathrm{Tr}((\mathbb{1} - D_m)\mathcal{N}(\mathbf{j}^n, \mathbf{s}_m^n)) \tag{7}$$

$$\geq \frac{1}{M^2} \sum_{l,m=1}^{M} \mathrm{Tr}((\mathbb{1} - D_m)\mathcal{N}(\mathbf{j}_l^n, \mathbf{s}_m^n)) \tag{8}$$

$$= \frac{1}{M^2} \sum_{l,m=1}^{M} \mathrm{Tr}((\mathbb{1} - D_m)\mathcal{N}(\mathbf{s}_m^n, \mathbf{j}_l^n)), \tag{9}$$

其中我们将最大干扰错误切换为平均干扰错误，然后利用了50:50分束器的对称性。我们继续进行，将每一项 $\mathbb{1} - D_m$ 替换为 D_l，对于一个 $l \neq m$:

$$\mathrm{err}(\mathcal{C}) \geq \frac{1}{M^2} \sum_{l \neq m=1}^{M} \mathrm{Tr}(D_l \mathcal{N}(\mathbf{s}_m^n, \mathbf{j}_l^n)) + \frac{1}{M^2} \sum_{l=1}^{M} \mathrm{Tr}((\mathbb{1} - D_l)\mathcal{N}(\mathbf{s}_l^n, \mathbf{j}_l^n)) \tag{10}$$

$$\geq \frac{1}{M^2} \sum_{l \neq m=1}^{M} \mathrm{Tr}(D_l \mathcal{N}(\mathbf{s}_m^n, \mathbf{j}_l^n)) \tag{11}$$

$$= \frac{1}{M^2} \sum_{l,m=1}^{M} \mathrm{Tr}(D_l \mathcal{N}(\mathbf{s}_m^n, \mathbf{j}_l^n)) - \frac{1}{M^2} \sum_{l=1}^{M} \mathrm{Tr}(D_l \mathcal{N}(\mathbf{s}_l^n, \mathbf{j}_l^n)) \tag{12}$$

$$\geq \min_{\mathbf{s}^n \in \mathcal{J}^n} \frac{1}{M} \sum_{l=1}^{M} \mathrm{Tr}(D_l \mathcal{N}(\mathbf{s}^n, \mathbf{j}_l^n)) - \frac{1}{M} \tag{13}$$

$$= 1 - \text{错误}(\mathcal{C}) - \tfrac{1}{M}, \tag{14}$$

这意味着（对所有 $M \geq 2$）

$$\mathrm{err}(\mathcal{C}) \geq \tfrac{1}{2} - \tfrac{1}{2M} \geq \tfrac{1}{4}. \tag{15}$$

因此， $P \geq E$ 意味着只有当 $|M_n| \to 1$ 渐近成立时，才能满足 $\mathrm{err}(\mathcal{C}_n) \to 0$ ，这意味着甚至无法传输单个比特， $C = 0$ 因此式（1）得证。 □

性质 (2) 的证明。 假设发射器发送相干态 $|\alpha\rangle$ ，而干扰者发送热态 S_N（β）。这两者可用一阶矩和二阶矩表示为

$$(\alpha, \tfrac{1}{2}\mathbb{1}), \qquad (\beta, (N + \tfrac{1}{2})\mathbb{1}). \tag{16}$$

将两者输入 50:50 分束器混合并对环境取偏迹后，可得接收方处状态的一阶矩和二阶矩

$$\left((\alpha + \mathbb{i}\beta)/\sqrt{2}, (N + 1)\mathbb{1}\right). \tag{17}$$

如果接收方现在使用零差探测器，则不失一般性，测得结果 $x \in \mathbb{R}$ 的概率为

$$p(x) = \tfrac{1}{\sqrt{\pi(N+1)}} \exp(-\tfrac{(x-(\alpha-\beta))^2}{N+1}), \tag{18}$$

对于满足 $|\beta|^2 + N \leq P$的实数（β， N），令 $\alpha = \sqrt{E}$，则该约束保证

$$\begin{aligned} \alpha - \beta &= \sqrt{E} - \beta && (19)\\ &\geq \sqrt{E} - \sqrt{P} && (20)\\ &> 0. && (21) \end{aligned}$$

由此可知，无论干扰者选择何种高斯态，

$$\begin{aligned} \mathbb{P}(x > 0|\alpha, \mathbf{j}) &= \tfrac{1}{2}(1 + \mathrm{erf}\big(\tfrac{\alpha-\beta}{\sqrt{N+1}}\big)) && (22)\\ &\geq \tfrac{1}{2}(1 + \min_{N' \leq P} \mathrm{erf}\big(\tfrac{\sqrt{E}-\sqrt{P-N'}}{\sqrt{N'+1}}\big)) && (23)\\ &= \tfrac{1}{2}(1 + \mathrm{erf}\big(\min_{N' \leq P} \tfrac{\sqrt{E}-\sqrt{P-N'}}{\sqrt{N'+1}}\big)) && (24)\\ &\geq \tfrac{1}{2}(1 + \mathrm{erf}\big(\tfrac{\sqrt{E}-\sqrt{P}}{\sqrt{P+1}}\big)) && (25)\\ &\geq \tfrac{1}{2} + \tfrac{1}{4}\mathrm{erf}\big(\tfrac{\sqrt{E}-\sqrt{P}}{\sqrt{P+1}}\big). && (26) \end{aligned}$$

如果发送方传输 $-\alpha$，同样的推理也适用于 $p(x < 0| - \alpha, \mathbf{j})$。在连续使用信道 n 次的过程中，发送方和接收方实际上是在一系列二元信道上进行传输，这些信道的转移概率为 $w_{\mathbf{j}_1}(y|x) \ldots, w_{\mathbf{j}_n}(y|x)$ (x, $y \in \{-1, 1\}$)，并具有如下性质

$$w_{\mathbf{j}_i}(x|x) \geq \tfrac{1}{2} + \nu(E, P) \qquad x \in \{-1, 1\} \tag{27}$$

其中 $\nu(E,\ P) := \frac{1}{4}\mathrm{erf}\big((\sqrt{E} - \sqrt{P})/\sqrt{P+1}\big)$ 对所有 $i = 1,\ \ldots\ldots,\ n$ 均一致成立。由于该信道的输入系统和输出系统均为二元的，因此适用 [4] 的定理 1，且 $\mathcal{N}$ 的容量下界为

$$\bar{C} \geq \max_{p} \min_{v \in \Xi} I(p; v) \tag{28}$$

其中 I 为互信息，而 Ξ 定义为由所有合法干扰者攻击所诱导的信道构成的凸包：

$$\Xi := \mathrm{conv}(\{w_{(\beta,N)}\}_{|\beta|^2+N\leq P}). \tag{29}$$

假设信号 α 和 α 服从对称分布 $\pi(-1) = \pi(1)$，通过Pinsker不等式和引理1可得

$$\begin{aligned}
\bar{C} &\geq \min_{v\in\Xi} I(\pi, v) && (30)\\
&\geq \min_{v\in\Xi} \tfrac{1}{2}\|v_\pi - \pi\otimes v(\pi)\|_1^2 && (31)\\
&\geq \min_{v\in\Xi} \tfrac{1}{2}|v(-1|-1)v(1|1) - v(-1|1)v(1|-1)| && (32)\\
&\geq \min_{v\in\Xi} \tfrac{1}{2}|v(-1|-1)v(1|1) - (1-v(1|1))(1-v(-1|-1))| && (33)\\
&= \min_{v\in\Xi} \tfrac{1}{2}|1 - v(-1|-1) - v(1|1)| && (34)\\
&= \min_{v\in\Xi} \tfrac{1}{2}(v(-1|-1) + v(1|1) - 1) && (35)\\
&\geq \nu(E,P) && (36)\\
&> 0. && (37)
\end{aligned}$$

□

性质(3)的证明。 我们通过假设在 n 次传输中有 n 比特的公共随机性（CR）可用来处理这个问题。在这种情况下，发送方和接收方可以对发送方和接收方的符号进行置换，该置换可由酉算子 $U = \exp(-\mathbb{i}\hat{}a^\dagger\hat{}a)$实现。于是，对于发送方的每个输入态 α和干扰者状态 $\sigma = (\beta, (N+\frac{1}{2})\mathbb{1})$，旋转后的状态为 $\sigma' = (-\beta, (N+\frac{1}{2})\mathbb{1})$，并且

$$\rho = \tfrac{1}{2}(\sigma + \sigma') \tag{38}$$

描述了干扰者的有效攻击：

$$\begin{aligned}
\mathcal{N}'(\alpha,\sigma) &= \tfrac{1}{2}(\mathcal{N}'(\alpha,\sigma) + \mathcal{N}'(-\alpha,\sigma)) && (39)\\
&= \mathcal{N}'(\alpha,\rho). && (40)
\end{aligned}$$

在接收方进行零差测量后，对于每个信号$\mathbf{s} = (\alpha, 0)$和干扰信号$\mathbf{j} = (\beta, N)$，由线性性可得

$$p(x|\mathbf{s},\mathbf{j}) = \tfrac{1}{\sqrt{\pi(N+1)}}\exp(-\tfrac{(x+\alpha)^2+\beta^2}{N+1})\cosh(\tfrac{2\beta(x+\alpha)}{N+1}). \tag{41}$$

该高斯混合由参数 α 平移，且与 β的符号无关。对于这种

分布，当$\mathbf{s}=(\sqrt{E},0)$且$\mathbf{j}=(\beta,\overline{N})$为任意值时，成立

$$\mathbb{P}(X>0|\mathbf{s},\mathbf{j}) = \left(2+\operatorname{erf}(\tfrac{\sqrt{E}+\beta}{\sqrt{1+N}})+\operatorname{erf}(\tfrac{\sqrt{E}-\beta}{\sqrt{1+N}})\right)/4 \tag{42}$$

$$= \left(2+\tfrac{2}{\sqrt{\pi}}\int_0^{a+b} e^{-t^2}dt+\int_0^{a-b} e^{-t^2}dt\right)/4 \tag{43}$$

$$= \left(2+\tfrac{2}{\sqrt{\pi}}\int_{b-a}^{b+a} e^{-t^2}dt\right)/4 \tag{44}$$

$$\geq \left(2+\tfrac{2}{\sqrt{\pi}}\int_{b-a}^{b+a} e^{-(b+a)^2}dt\right)/4 \tag{45}$$

$$= \left(2+\tfrac{4a}{\sqrt{\pi}}e^{-(b+a)^2}\right)/4 \tag{46}$$

其中我们使用了 $a:=\sqrt{E/(1+N)}$ 和 $b:=\beta/\sqrt{1+N_\circ}$ 为了得到关于数值 E, P 的下界，我们改回使用这些术语:

$$\min_{\mathbf{j}\in\mathcal{J}}\mathbb{P}(X>0|\mathbf{s},\mathbf{j}) = \left(2+\tfrac{4\sqrt{E}}{\sqrt{\pi(1+N)}}\exp(-\big(\tfrac{\sqrt{E}-\beta}{\sqrt{1+N}}\big)^2)\right)/4 \tag{47}$$

$$\geq \left(2+\tfrac{4\sqrt{E}}{\sqrt{\pi(1+P)}}\exp(-(\sqrt{E}-\sqrt{P})^2)\right)/4. \tag{48}$$

这里，我们分别对指数项前的因子和指数项本身进行了最大化，并使用了 $\mathcal{J}$ 的定义。使用

$$\epsilon(E,P):=\tfrac{\sqrt{E}}{\sqrt{\pi(1+P)}}\exp(-(\sqrt{E}-\sqrt{P})^2) \tag{49}$$

并注意到，当发送信号为 $\mathbf{s}'=(-\sqrt{E},\ 0)$ 时，同样的估计

$$\min_{\mathbf{j}\in\mathcal{J}}\mathbb{P}(X<0|\mathbf{s}',\mathbf{j})\geq\tfrac{1}{2}+\epsilon(E,P) \tag{50}$$

对另一个信号也成立。此外，分布 (41) 关于 x 的联合反射是对称的，且 $\mathbf{j}$ 在原点处的一阶矩为:

$$p(x|(\alpha,0),\mathbf{j}) = \tfrac{1}{\sqrt{\pi(N+1)}}\exp(-\tfrac{(x+\alpha)^2+\beta^2}{N+1})\cosh(\tfrac{2\beta(x+\alpha)}{N+1}) \tag{51}$$

$$= \tfrac{1}{\sqrt{\pi(N+1)}}\exp(-\tfrac{(-x-\alpha)^2+\beta^2}{N+1})\cosh(\tfrac{2\beta(-x-\alpha)}{N+1}) \tag{52}$$

$$= p(-x|(-\alpha,0),\mathbf{j}). \tag{53}$$

因此，我们接下来采用阈值解码器：如果测得的值 x 满足 $x>0$，就判定发送的是 $b=0$。正确接收该比特的概率严格大于 $1/2$（不过，具体数值取决于 P 和 E，且非常接近 $1/2$）。同样的估计表明，正确解码 $b=1$ 的概率严格大于 $1/2$。根据 $p(x|\mathbf{s},\ \mathbf{j})$ 的对称性，我们知道，对于干扰者的任意选择 $\mathbf{j}$，从 b 到阈值解码器解码所得值的信道都是二元对称信道。由 [4, 定理 1] 可知，任意变化二元对称信道的容量下界为 $1-h(\epsilon)$，其中 ϵ 是允许的最小比特翻转概率。因此，我们已经证明

$$\bar{C}\geq 1-h(\tfrac{1}{2}+\epsilon(E,P))>0. \tag{54}$$

□

性质 (4) 的证明。 我们采用由压缩参数 r 表征的双模压缩真空态，其一阶矩为零，二阶矩为

$$V_S = \frac{1}{2}\begin{pmatrix} \cosh(2r)\mathbb{1} & \sinh(2r)\mathbb{Z} \\ \sinh(2r)\mathbb{Z} & \cosh(2r)\mathbb{1} \end{pmatrix} \tag{55}$$

$$\mathbb{Z} = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \qquad \mathbb{1} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}. \tag{56}$$

描述干扰攻击与双模压缩真空态的联合系统为 $S_N(\beta) \otimes |TMSV\rangle\langle TMSV|$，其一阶矩和二阶矩为

$$b \oplus 0 \oplus 0, \quad \begin{pmatrix} (N+\frac{1}{2})\mathbb{1} & 0 & 0 \\ 0 & \cosh(2r)\mathbb{1} & \sinh(2r)\mathbb{Z} \\ 0 & \sinh(2r)\mathbb{Z} & \cosh(2r)\mathbb{1} \end{pmatrix}, \tag{57}$$

其中 $b = \sqrt{2}(\Re(\beta)\ \Im(\beta))^T$。作用于前两个模块的 50:50分束器建模为 $B \oplus \mathbb{1}$ [24]，其中

$$B = \frac{1}{\sqrt{2}}\begin{pmatrix} \mathbb{1} & \mathbb{1} \\ -\mathbb{1} & \mathbb{1} \end{pmatrix}. \tag{58}$$

它将一阶矩变为 $(\Re(\beta)\ \Im(\beta)\ -\Re(\beta)\ \Im(\beta),\ 0,\ 0)^T$，并将联合协方差矩阵变为

$$\begin{pmatrix} (A+B)\cdot\mathbb{1} & (A-B)\cdot\mathbb{1} & C\cdot\mathbb{Z} \\ (A-B)\cdot\mathbb{1} & (A+B)\cdot\mathbb{1} & -C\cdot\mathbb{Z} \\ C\cdot\mathbb{Z} & -C\cdot\mathbb{Z} & 2B\cdot\mathbb{1} \end{pmatrix}, \tag{59}$$

其中 $A = (N+\frac{1}{2})/2$, $B = \cosh(2r)/4$ 以及 $C = \sinh(2r)/4$。对第一和第三个模式的 $\hat{}x$ 正交分量进行零差测量后，测量结果的分布 $(x_1,\ x_3)$ 为高斯分布 [24, 式（5.128）]，其协方差矩阵和逆协方差矩阵为

$$V_G = \begin{pmatrix} A+B & C \\ C & 2B \end{pmatrix}, \qquad V_G^{-1} = \frac{1}{\det(V_G)}\begin{pmatrix} 2B & -C \\ -C & A+B \end{pmatrix}. \tag{60}$$

$(X_1,\ X_3)$ 的相关性为

$$\mathrm{Corr}(X_1, X_3) := \frac{\mathrm{Cov}(X_1, X_3)}{\sqrt{\mathrm{Var}(X_1)\mathrm{Var}(X_3)}} \tag{61}$$

$$= \frac{C}{\sqrt{(A+B)2B}} \tag{62}$$

均值为 $\Re(\beta)$。为简便起见且不失一般性，我们假设其等于 β 本身。定义新的随机变量后

$$(b_A, b_B) = \mathrm{dec}(X_1, X_3) \tag{63}$$

其中 $\mathrm{dec}(x_1, x_3) = ((-1)^{\mathrm{sgn}(x_1)}, (-1)^{\mathrm{sgn}(x_3)})$ 二元检测事件 (b_A, b_B) 的概率 $\in \{-1, 1\}^2$ 转换为概率

$$\mathbb{P}(\square.), \tag{64}$$

其中，$\square_{\nearrow}$、$\square_{\nwarrow}$、$\square_{\searrow}$ 和 $\square_{\swarrow}$ 分别表示复平面 $\mathbb{C}$的右上、左上、右下和左下象限。这些概率具有特定的几何结构，我们利用二元正态累积分布函数将其提取出来

$$\Phi_2(h,k,\rho) := \int_{-\infty}^{h}\int_{-\infty}^{k}\left[\exp\left(-\frac{x^2-2\rho xy+y^2}{2(1-\rho^2)}\right)/2\pi\sqrt{1-\rho^2}\right]dxdy. \tag{65}$$

定义新的随机变量 $X_A = (X_1-\beta)/\sqrt{A+B}$ 和 $X_B = \overline{X_3/\sqrt{2}}B$ 后，我们得到

$$\mathbb{P}(\square_{\swarrow}) = \int_{-\infty}^{0}\int_{-\infty}^{0}\frac{1}{2\pi\sqrt{\det(V_G)}}\exp\left(-\frac{2B(x_1-\beta)^2-2C(x_1-\beta)x_3+(A+B)x_3^2}{2\det(V_G)}\right)dx_1dx_3 \tag{66}$$

$$= \int_{-\infty}^{0}\int_{-\infty}^{-\frac{\beta}{\sqrt{A+B}}}\frac{\sqrt{2B(A+B)}}{2\pi\sqrt{\det(V_G)}}\exp\left(-\frac{(x_A^2+x_B)^2-x_Ax_B2C/\sqrt{2B(A+B)}}{2\det(V_G)/(2B(A+B))}\right)dx_Adx_B \tag{67}$$

其中 $\det(V_G) = (A+B)2B-C^2$。令

$$\rho = C/\sqrt{2B(A+B)} \tag{68}$$

我们得到

$$\sqrt{1-\rho^2} = \sqrt{1-C^2/(2B(A+B))} \tag{69}$$

$$= \frac{1}{\sqrt{2B(A+B)}}\sqrt{2B(A+B)-C^2} \tag{70}$$

$$= \frac{1}{\sqrt{2B(A+B)}}\sqrt{\det(V_G)} \tag{71}$$

因此可以将上述积分简化为

$$\mathbb{P}(\square_{\swarrow}) = \int_{-\infty}^{0}\int_{-\infty}^{-\frac{\beta}{\sqrt{A+B}}}\frac{1}{2\pi\sqrt{1-\rho^2}}\exp\left(-\frac{(x_A^2+x_B)^2-x_Ax_B2\rho}{2(1-\rho^2)}\right)dx_Adx_B \tag{72}$$

$$= \Phi_2(-\tfrac{\beta}{\sqrt{a}},0,\rho). \tag{73}$$

采用相同的方法，并且由于 (72) 中概率密度的每个边缘分布都是方差为一的零均值正态分布，因此还可以得到

$$\mathbb{P}(\square_{\nwarrow}) = \mathbb{P}(X_B<0)-\mathbb{P}(\square_{\swarrow}) \tag{74}$$

$$= \phi(-\tfrac{\beta}{\sqrt{a}})-\Phi_2(-\tfrac{\beta}{\sqrt{a}},0,\tfrac{C}{\sqrt{2(A+B)B}}) \tag{75}$$

$$= \phi(-\tfrac{\beta}{\sqrt{a}})-\mathbb{P}(\square_{\swarrow}), \tag{76}$$

其中

$$\phi(x) := (2\pi)^{-1/2}\int_{-\infty}^{x}\exp(-t^2/2)dt \tag{77}$$

是标准正态累积分布函数。进一步，我们得到

$$\mathbb{P}(\square_{\searrow}) = \mathbb{P}(X_A < 0) - \mathbb{P}(\square_{\swarrow}) \tag{78}$$
$$= \phi(0) - \Phi_2(-\tfrac{\beta}{\sqrt{a}}, 0, \tfrac{C}{\sqrt{2(A+B)B}}) \tag{79}$$
$$= \tfrac{1}{2} - \mathbb{P}(\square_{\swarrow}) \tag{80}$$

并且，由于归一化，

$$\mathbb{P}(\square_{\nearrow}) = 1 - \mathbb{P}(\square_{\swarrow}) - \mathbb{P}(\square_{\nwarrow}) - \mathbb{P}(\square_{\searrow}) \tag{81}$$
$$= 1 - \mathbb{P}(\square_{\swarrow}) - \mathbb{P}(\square_{\nwarrow}) - \mathbb{P}(\square_{\searrow}) \tag{82}$$
$$= 1 - \phi(-\tfrac{\beta}{\sqrt{a}}) - \mathbb{P}(\square_{\searrow}) \tag{83}$$
$$= \tfrac{1}{2} + \mathbb{P}(\square_{\swarrow}) - \phi(-\tfrac{\beta}{\sqrt{a}}). \tag{84}$$

然而，

$$\Phi_2(-x, 0, \rho) = \mathbb{P}(X_A < -x, X_B < 0) \tag{85}$$
$$\leq \mathbb{P}(X_B < 0) \tag{86}$$
$$\leq \tfrac{1}{2}. \tag{87}$$

因此，对于 $|\rho| \neq 1$，我们有 $\mathbb{P}(\square_{\searrow}) < \frac{1}{2}$。此外，由式 (85) 可知，$x \to \Phi_2(-x, 0, \rho)$ 是连续且单调递增的。因此，对于任意 $P \geq 0$，可知对所有 $|\rho| < 1$，都存在一个 $\delta > 0$，使得 $\Phi_2(-x, 0, \rho) < \frac{1}{2} - \delta$。因此，合理的假设是，对于每个干扰信号 $\mathbf{j} \in \mathcal{J}$，分布 1 仍保持相关。发送方和接收方处测量结果的确切几何性质将在下一段“几何性质”中讨论，其对信道的影响则将在“有效信道”一段中讨论。

几何性质 我们将 Θ 定义为式 (63) 中定义的 $(B_A, B_B) = \mathrm{dec}(X_A, X_B)$ 的所有分布构成的集合，其中 (β, N) 的取值任意且无界；并令 $\Theta(P)$ 为 Θ 的子集，其中干扰者的每符号干扰能量至多为 P。我们进一步将分布 q_c、q_{-1} 和 q_1 定义为

$$q_c(u, v) := \tfrac{1}{2}\delta(u, v) \tag{88}$$
$$q_{-1} := \delta_{-1} \otimes \pi \tag{89}$$
$$q_1 := \delta_1 \otimes \pi, \tag{90}$$

集合 $\Delta := \mathrm{conv}(\{q_c, q_{-1}, q_1\})$ 和集合 $\Delta_\delta := \mathrm{conv}(\{q_c, \tilde{q}_{-1}, \tilde{q}_1\})$，其中 $\tilde{q}_i := (1-\delta)q_i + \delta q_c$。干扰者的能量限制 P 限制了其位移 β，并通过 N限制干扰者对协方差矩阵的影响，因此对于每个 $P > 0$ 以及所有满足 $|\beta|^2 + N \leq P$ 的 (β, N)，都存在一个 $\delta(E, P) > 0$，使得 $\Theta(P) \subset \Delta_{\delta(E,P)}$。

证明。 我们首先证明 $\Theta \subset \Delta$。Θ 中的每个成员 q 均由公式 (66)、(74) 和 (78) 给出。为了清楚地指出从信号分布到比特分布的转换步骤，我们明确写出

$$q(-1, -1) = \mathbb{P}(\square_{\swarrow}) =: q \tag{91}$$
$$q(-1, 1) = \mathbb{P}(\square_{\nwarrow}) = s - q \tag{92}$$
$$q(1, -1) = \mathbb{P}(\square_{\searrow}) = \tfrac{1}{2} - q \tag{93}$$
$$q(1, 1) = \mathbb{P}(\square_{\nearrow}) = \tfrac{1}{2} - s + q, \tag{94}$$

其中 $s = \phi(-\frac{\beta}{\sqrt{a}})$。接着，我们将 $\mathcal{P}(\{-1,1\})$ 嵌入其中，从而通过将任意分布 r 映射为 $r(-1,-1)e_0 + r(-1,\ 1)e_1 + r(1,\ -1)e_2$，将 Δ 嵌入 $\mathbb{R}^3$。然后

$$q_c = (\tfrac{1}{2}, 0, 0)^T \tag{95}$$
$$q_{-1} = (\tfrac{1}{2}, \tfrac{1}{2}, 0)^T \tag{96}$$
$$q_1 = (0, 0, \tfrac{1}{2})^T. \tag{97}$$

Δ 的一个法向量为 $\mathbf{n} = (1,\ 1,\ 0)^T$：

$$\langle q_c - q_c, \mathbf{n}\rangle = 0 \tag{98}$$
$$\langle q_c - q_{-1}, \mathbf{n}\rangle = \langle (0, -\tfrac{1}{2}, 0)^T, (1,0,1)^T\rangle = 0 \tag{99}$$
$$\langle q_c - q_1, \mathbf{n}\rangle = \langle (\tfrac{1}{2}, 0, -\tfrac{1}{2}), (1,0,1)^T\rangle = 0. \tag{100}$$

每个分布 q 都是 Θ的子集。为此，我们取一个分布 q，并计算

$$\langle q - q_c, \mathbf{n}\rangle = (q - \tfrac{1}{2}) + (\tfrac{1}{2} - q) = 0. \tag{101}$$

因此，$\Theta \subset \Delta$。为推导出更明确的值 $\delta(E,\ P)$，我们再次应用引理1：对于每个乘积分布 $v \otimes w \in \mathcal{P}(\{-1,1\})$，有

$$\|q - v\otimes w\|_1 \geq |\det(q)| \tag{102}$$
$$= |q\cdot(\tfrac{1}{2} - s + q) - (s-q)\cdot(\tfrac{1}{2} - q)| \tag{103}$$
$$= |\tfrac{1}{2}q - qs + q^2 - \tfrac{1}{2}s + sq + \tfrac{1}{2}q - q^2| \tag{104}$$
$$= |q - \tfrac{1}{2}s| \tag{105}$$
$$= |\phi_2(-\tfrac{\beta}{\sqrt{A+B}}, 0, \rho) - \phi_2(-\tfrac{\beta}{\sqrt{a}}, 0, 0)| \tag{106}$$
$$\geq \min_{\mathbf{j}\in\mathcal{J}} |\rho| \tfrac{1}{2\pi} \exp(-\tfrac{|\beta|^2}{2(A+B)(1-\rho^2)}) \tag{107}$$

根据引理 2，由式 (68) 可知，值 ρ是干扰信号 $\mathbf{j}$ 的函数，A和 B也一样。接下来，我们用如下粗略下界：对于所有 $\mathbf{j} = (\beta,\ N) \in \mathcal{J}$，以下三个不等式成立：

$$|\rho| = \frac{|\sinh(2r)|}{\sqrt{\frac{1}{2}\cosh(2r)(\frac{1}{2}N + \frac{1}{4}\cosh(2r) + \frac{1}{4})}} \tag{108}$$
$$\geq \frac{|\sinh(2r)|}{\sqrt{\cosh(2r)(P + \cosh(2r) + 1)}} \tag{109}$$
$$A + B = \tfrac{1}{2}N + \tfrac{1}{4}(\cosh(2r) + 1) \tag{110}$$
$$\leq \tfrac{1}{2}P + \tfrac{1}{4}(\cosh(2r) + 1) \tag{111}$$
$$|\beta|^2 \leq P. \tag{112}$$

注意到 $\cosh(2r) = 1 + 2E$，并且（由于等式 $\cosh(2r)^2 = 1 - \sinh(2r)^2$ 成立）还有 $|\sinh(2r)| = 2\sqrt{E(E+2)}$，我们证明了存在 $\delta(E,\ P)$，使得

$$\|q - v\otimes w\|_1 \geq \delta(E, P) \tag{113}$$

对于所有乘积分布 $v \otimes w$ 以及干扰者的任意选择。在表示式

$$q = \lambda_c q_c + \lambda_{-1} q_{-1} + \lambda_1 q_1 \tag{114}$$

这意味着对于所有的 $\mathbf{j} \in \mathcal{J}$，我们都有

$$\lambda_c \geq \delta(E, P). \tag{115}$$

□

有效信道 考虑任意一个由条件概率分布$w(y|x)$建模的信道，其中 $x, y \in \{-1, 1\}$。假设发送方和接收方共享完全相关的均匀随机比特，他们可以将 w 转换为 w_c，如下所示:

$$w_c(y|x) := \tfrac{1}{2} \sum_u w(y \oplus u | x \oplus u). \tag{116}$$

在这种情况下，我们有

$$w_c(-1|-1) = \tfrac{1}{2} \sum_u w(-1 \oplus u | -1 \oplus u) \tag{117}$$

$$= \tfrac{1}{2} \sum_u w(1 \oplus u | 1 \oplus u) \tag{118}$$

$$= w_c(1|1) \tag{119}$$

因此， w_c 是一个二元对称信道（二元对称信道）。如果发送方和接收方改为使用模二相加结果相同的任意非相关分布 $v \otimes \pi$，那么对于每个 x, y，我们得到

$$w_u(y|x) = \sum_{x'} v(x') \sum_{y'} \tfrac{1}{2} w(y \oplus y' | x \oplus x') \tag{120}$$

$$= w_u(y \oplus 1 | x). \tag{121}$$

因此， w_u 再次是一个二元对称信道，但这次其交叉概率为 $1/2$。用于证明$C_Q > 0$ 的编码现在很简单：在 $2n$ 次传输期间，发送方和接收方在前 n 次传输中发送一个双模压缩真空态，从而得到一系列联合分布 $q_1, \ldots, q_n \in \Theta$。在接下来的 n 次传输中，他们如定理 1 的性质 (3) 的证明中那样，使用二进制相移键控字母表 $\{|-\sqrt{E}\rangle, |\sqrt{E}\rangle\}$ 进行传输，从而得到一系列信道$w_i(y|x)$。随后，他们再次按照定理 1 的性质 (3) 的证明，利用其分布 q_i 将每个 w_i 转换为一个二元对称信道:

$$\tilde{w}_i(y|x) := \textstyle\sum_{x',y'} w_i(y \oplus y' | x \oplus x') q(x', y') \tag{122}$$

$$= \lambda_{c,i} \textstyle\sum_{x'} \frac{w_i(y \oplus y' | x \oplus x')}{2} + \sum_{y'} [\lambda_{-1,i} \frac{w_i(y \oplus y' | x \oplus -1)}{2} + \lambda_{1,i} \frac{w_i(y \oplus y' | x \oplus 1)}{2}] \tag{123}$$

$$= \lambda_{c,i} \cdot b_{p_i}(y|x) + (1 - \lambda_{c,i}) \cdot b_{1/2}(y|x). \tag{124}$$

由定理 1 的性质 (3) 的证明可知，对于某个 $0 \leq \epsilon(E, P) < \frac{1}{2}$， $p_i \leq \epsilon(E, P)$ 在 $i = 1, \ldots, n$ 上一致成立。此外，对于任意两个二元对称信道， $\lambda \in [0, 1]$ 和 x, y，我们有如下性质

$$\lambda \cdot b_{p_1}(y|x) + (1 - \lambda) \cdot b_{p_2}(y|x) = b_{\lambda p_1 + (1-\lambda) p_2}(y|x). \tag{125}$$

因此，每个有效信道都是交叉概率为.....的二元对称信道

$$\lambda_{c,i} \cdot p_i + (1 - \lambda_{c,i}) \cdot \tfrac{1}{2} \leq \lambda_{c,i} \cdot \epsilon(E, P) + (1 - \lambda_{c,i}) \cdot \tfrac{1}{2} < \tfrac{1}{2}, \tag{126}$$

其中最后一个不等式由 (115) 的一致上界 $\lambda_{c,i} > \delta(E, P)$ 得出。

如前在性质 2 的证明中，应用 [4, 定理 1] 表明这蕴含$C_Q > 0$。

□

3 附录

以下两个引理在我们的推导中很重要:

引理1. 设 $p, q \in \mathcal{P}(\{-1,1\}^2)$，其中 p 为乘积分布，分解为 $p(i,j) = v(i) \cdot w(j)$，对某些 $v, w \in \mathcal{P}(\{-1,1\})$。则

$$\|p - q\|_1 \geq |q(1,1)q(-1,-1) - q(1,-1)q(-1,1)|. \tag{127}$$

证明. 令 $\det(p) := p(1,1)p(-1,-1) - p(1,-1)p(-1,1)$，并以同样方式定义 $\det(q)$。则

$$\begin{aligned}
\det(p) - \det(q) &= p(1,1)p(-1,-1) - p(1,-1)p(-1,1) && (128)\\
&\quad - q(1,1)q(-1,-1) - q(1,-1)q(-1,1) && (129)\\
&= p(1,1)p(-1,-1) - p(1,-1)p(-1,1) - q(1,1)q(-1,-1) && (130)\\
&\quad - q(1,-1)q(-1,1) + p(-1,1)q(1,-1) - p(-1,1)q(1,-1) && (131)\\
&= p(-1,-1)[p(1,1) - q(1,1)] + q(1,1)[p(-1,-1) - q(-1,-1)] && (132)\\
&\quad + p(-1,1)[q(1,-1) - p(1,-1)] + q(1,-1)[q(-1,1) - p(-1,1)] && (133)\\
&\leq \sum_{i,j} |p(i,j) - q(i,j)| && (134)\\
&= \|p - q\|_1 && (135)
\end{aligned}$$

由于 $\det(v \otimes w) = 0$，引理得证。 □

我们需要的第二个论据是以下引理

引理 2。 设 ϕ_2 为二元正态累积分布函数 (65)，ϕ为标准正态累积分布函数 (77)。那么对于所有 $t \in \mathbb{R}$ 和 $\rho \in [-1,1]$，有

$$|\phi_2(t, 0, \rho) - \tfrac{1}{2}\phi(t)| \geq |\rho| \tfrac{1}{2\pi} \exp(-\tfrac{t^2}{2(1-\rho^2)}). \tag{136}$$

引理 *2* 的证明。我们首先指出，根据普拉克特公式 [22]（有关我们在此使用的确切表述，请参见 [19, 式（10）]），我们有

$$\partial_\rho \phi_2(t, 0, \rho) = \tfrac{1}{2\pi\sqrt{1-\rho^2}} \exp\left(-\frac{t^2}{2(1-\rho^2)}\right). \tag{137}$$

因此我们有

$$\phi_2(t,0,\rho) - \tfrac{1}{2}\phi(t) = \phi_2(t,0,\rho) - \phi_2(t,0,0) \tag{138}$$

$$= \int_0^\rho \partial_\rho \phi_2(t,0,\rho) d\rho \tag{139}$$

$$= \int_0^\rho \tfrac{1}{2\pi\sqrt{1-\rho^2}} \exp\left(-\frac{t^2}{2(1-\rho^2)}\right) d\rho. \tag{140}$$

因此，我们可以推导出下界

$$|\phi_2(t,0,\rho) - \tfrac{1}{2}\phi(t)| \geq |\rho| \min_{0\leq\nu\leq\rho} \tfrac{1}{2\pi\sqrt{1-\nu^2}} \exp(-\tfrac{t^2}{2(1-\nu^2)}) \tag{141}$$

$$\geq |\rho| \min_{0\leq\nu\leq\rho} \tfrac{1}{2\pi} \exp(-\tfrac{t^2}{2(1-\rho^2)}) \tag{142}$$

$$\geq |\rho| \tfrac{1}{2\pi} \exp(-\tfrac{t^2}{2(1-\rho^2)}). \tag{143}$$

□

致谢

本研究部分得到德国科学基金会埃米·诺特计划（资助编号1129/2-1）的支持，部分得到联邦研究、技术和航天部（资助编号16KISQ039、16KISR026、16KIS1598K、16KISQ093、16KISQ077和16KIS2604）的支持，部分得到德国联邦研究、技术和航天部通过“Souver¨an. Digital. Vernetzt.”联合项目6G-life（项目识别号16KISK002）的支持。衷心感谢巴伐利亚州通过6GQT项目提供的慷慨支持。本研究是慕尼黑量子谷的一部分，该项目由巴伐利亚州政府利用巴伐利亚高科技议程Plus的资金予以支持。

参考文献

[1] R. Ahlswede. 任意变化信道随机码中的相关性消除。《概率论及相关领域》，44:159 – 175，1978。[2] R. Ahlswede、I. Bjelakovic、H. Boche 和 J. N¨otzel。对抗性量子噪声下的量子容量：任意变化量子信道。《数学物理通讯》，317:103 – 156，2013。[3] R. Ahlswede 和蔡宁。相关信源有助于通过任意变化信道进行传输。*IEEE*信息论汇刊，43(4):1254–1255，1997。[4] R. Ahlswede 和 J. Wolfowitz。具有任意变化信道概率函数和二元输出字母表的信道容量。《概率论 ¨及相关领域》，15:186 –194，1970。[5] Rudolf Ahlswede 和 Vladimir Blinovsky。经典-量子任意变化信道的经典容量。*IEEE*信息论汇刊，53(2):526–533，2007。

[6] Sagnik Bhattacharya、Amitalok J. Budkuley 和 Sidharth Jaggi。任意变化信道中的共享随机性。载于*2019 IEEE*信息理论国际研讨会（*ISIT*），第627–631页，2019。[7] D. Blackwell、L. Breiman 和 A. J. Thomasian。随机编码下若干信道类别的容量。《数学统计年刊》，31(3):558–567，1960。[8] H. Boche 和 J. N¨otzel。任意变化量子信道中的任意小量相关性。《数学物理学杂志》，54(11):112202，2013年11月。[9] H. Boche 和 J. N¨otzel。任意变化量子信道的正性、不连续性、有限资源与非零错误。《数学物理学杂志》，55(12):122201，2014年12月。[10] Holger Boche、Minglai Cai、Christian Deppe 和 Janis N¨otzel。经典-量子任意变化窃听信道：公共随机性辅助编码与连续性。《量子信息处理》，16(1)，2016年12月。[11] Holger Boche、Minglai Cai、Christian Deppe 和 Janis N¨otzel。经典-量子任意变化窃听信道：干扰攻击下的秘密消息传输。《数学物理学杂志》，58(10):102203，2017年10月。[12] Holger Boche、Christian Deppe、Janis N¨otzel 和 Andreas Winter。完全量子任意变化信道：随机编码容量与容量二分性。载于*2018 IEEE*信息理论国际研讨会（*ISIT*）。IEEE，2018年6月。[13] Holger Boche、Rafael F Schaefer 和 H. Vincent Poor。通信系统中拒绝服务攻击的可检测性。载于*ICASSP 2019 - 2019 IEEE*声学、语音与信号处理国际会议（*ICASSP*），第2532–2536页，2019。[14] I. Csiszar 和 P. Narayan。重新审视任意变化信道的容量：正性与约束。*IEEE*信息论汇刊，34(2):181–193，1988。[15] I. Csiszar 和 P. Narayan。高斯任意变化信道的容量。*IEEE*信息论汇刊，37(1):18–26，1991。[16] T. Ericson。任意变化信道随机码的指数误差界。*IEEE*信息论汇刊，31(1):42–48，1985。[17] Saikat Guha 和 Jeffrey H. Shapiro。玻色广播信道的经典信息容量。载于*2007 IEEE*信息理论国际研讨会，第1896–1900页，2007。[18] Saikat Guha、Jeffrey H. Shapiro 和 Baris I. Erkmen。玻色广播通信的经典容量与最小输出熵猜想。《物理评论*A*》，76:032303，2007年9月。[19] Janez Komelj。通过Owen函数和修正欧拉反正切级数计算二元正态积分。《美国计算数学杂志》，13(04):476–504，2023。

[20] Janis N¨otzel. 经典噪声下玻色信道上的数据传输。载于*2024*年*IEEE*国际信息论研讨会（*ISIT*），第 1227–1232 页，2024 年。[21] Uzi Pereg 和 Yossef Steinberg。有色高斯噪声下的任意变化信道。*IEEE*信息论汇刊，67(6):3781–3817，2021 年。[22] Robin L Plackett. 正态多重积分的约化公式。*Biometrika*，41(3/4):351–360，1954 年。[23] Florian Seitz 和 Janis N¨otzel. 物理系统中的可对称化性检测，2025 年。[24] Alessio Serafini. 量子连续变量：理论方法入门。CRC出版社，2017 年。