损耗玻色复合窃听信道的容量公式

Florian Seitz, Janis Nötzel, *Member, IEEE*
Emmy-Noether Group Theoretical Quantum Systems Design,
Technical University of Munich, Munich, Germany,
{flo.seitz,janis.noetzel}@tum.de

摘要—我们考虑玻色复合窃听信道。一对有损信道将发送者与一个（合法）接收者及一个窃听者连接起来。发送者和接收者仅对实际的信道状态具有部分信息。在这种情况下，他们的任务是在保证向窃听者泄露的信息量（渐近地）可忽略的前提下，通过无限次使用信道来传输最大数量的消息。我们证明了当发送者和接收者具有相同系统信息的情况下的容量公式以及发送者具有信道状态信息情况下的容量公式。

I. 介绍

复合窃听信道中的通信要求在各种信道条件下正确传输到接收端，这些条件可以在预定义的集合中取任意值。在实际场景中，当发送端对信道状态了解较少且必须确保低延迟数据传输时，这样的情况就显得尤为重要。此时，排除了通过发送导频符号让接收端学习信道然后将信息传回给发送者的策略。由于越来越多的服务实现了数字化，数据安全成为一个越来越重要的主题，这在物理层通信系统研究中通过引入窃听者得以体现。必须假设对于连接发送者与窃听者的信道状态信息的缺乏也是存在的，这增加了不仅确保准确的数据传输到合法接收端，而且还减少向窃听者的信息泄露的挑战。

相应的经典系统在所有信道参数完全已知的情况下，如 [14] 所示的研究中进行了探讨，并且在 [3], [8] 中对复合窃听信道进行了研究。有限维希尔伯特空间量子信道的秘密容量在 [5] 和独立地在 [4] 中被证明。玻色系统的私密容量进一步在 [7], [9], [10] 中进行了探讨。

This work was financed by the DFG via grant NO 1129/2-1 and by the BMBF via grants 16KISQ039 and 16KISQ077. The authors acknowledge the financial support by the Federal Ministry of Education and Research of Germany in the programme of “Souverän. Digital. Vernetzt.” . Joint project 6G-life, project identification number: 16KISK002. Further, this work was supported by the state of Bavaria via the 6GQT project.

II. 符号表示和系统模型

Fock 空间表示为 $\mathcal{H}$，其上所有密度算子的集合是 $\mathcal{P}(\mathcal{H})$。冯-诺伊曼熵表示为 S，热态的熵具有平均值 E 个热光子是 $g(E)$，其中 $g(x)=(x+1)\log(x+1)-x\log(x)$ 是 Gordon 函数 [6]。二进制熵是 $h:[0,1]\to[0,1]; x\mapsto -x\log x-(1-x)\log(1-x)$。在整个过程中，对数以 2 为底。集合 $\{p_i,\rho_i\}_i$ 的 Holevo 数量是 $\chi(\{p_i,\rho_i\}_i)$。在这项工作中，我们关注无噪声玻色经典-量子信道，这些信道由一个参数 $\tau\in[0,1]$ 定义，其中 τ^2 被称为透射率，$1-\tau^2$ 是损耗。接收到输入 $\alpha\in\mathbb{C}$ 后，信道输出由 $\mathcal{N}_\tau(\alpha)=|\tau\alpha\rangle\langle\tau\alpha|$ 给出。我们约定希腊字母表示相干态，因此 $|\tau\alpha\rangle = e^{-|\tau\alpha|^2/2}\sum_n \frac{(\tau\alpha)^n}{\sqrt{n!}}|n\rangle$ 是一个相干态，而 $|n\rangle$ 是所谓的*光子数态*，它们构成了 $\mathcal{H}$ 的正交基。一个无噪声的玻色复合线窃听信道由一组信道 $\mathcal{N}=\{\mathcal{N}_\tau,\mathcal{N}_\eta\}_{(\tau,\eta)\in\boldsymbol{S}}$ 给出，其中 $\boldsymbol{S}$ 是 $[0,1]\times[0,1]$ 的一个子集，τ 量化了合法方之间传输链路的透射率，而 η 量化了从合法发送者到窃听者的链路的透射率。在整个过程中，$\mathcal{X}$ 是一个集合，X 表示其上的一个随机变量。$\mathbb{E}_X$ 表示关于 X 的期望值。对于实数 r，如果 $(r)_+=r$ 则 $r>0$，否则 $(r)_+=0$。

定义 1 ((n,M_n,λ,μ) 代码): 一组信号集合 $\{x_{s,m}\}_{m\in[M_n],s\in\boldsymbol{S}}$，其中每个 $x_{s,m}$ 都是 $\mathbb{C}^n$ 的一个元素和一个 Positive Operator Valued Measurement (POVM) $\{D_m\}_{m=1}^{M_n}$ 被称为具有发送端状态信息的 (n,M_n,λ,μ) 编码 $\mathcal{C}$，如果对于所有成对的 $s=(\tau,\eta)\in\boldsymbol{S}$，成功概率

$$p_{\mathrm{suc},s}(\mathcal{C}):=\frac{1}{M_n}\sum_{m=1}^{M_n}\mathrm{Tr}\big[D_m\mathcal{N}_\tau^{\otimes n}(x_{s,m})\big] \tag{II.1}$$

满足 $p_{\mathrm{suc},s}(\mathcal{C})\geq 1-\lambda$，且向窃听者泄露的信息满足

$$\chi(\{M_n^{-1},\mathcal{N}_\eta^{\otimes n}(x_{s,m})\}_{x_m=1}^{M_n})<\mu. \tag{II.2}$$

。如果信号 $\{x_m\}_{m\in[M_n]}$ 不依赖于 s，并且对于所有 $s=(\tau,\eta)\in\boldsymbol{S}$ 都成立 $p_{\mathrm{suc},s}(\mathcal{C})\geq 1-\lambda$ 和

$$\chi(\{M_n^{-1},\mathcal{N}_\eta^{\otimes n}(x_m)\}_{x_m=1}^{M_n})<\mu \tag{II.3}$$

，该编码被称为没有发送端状态信息的 (n,M_n,λ,μ) 编码 $\mathcal{C}$。

定义 2 (可达速率，容量): 速率 $R\geq 0$ 被称为在发射机具有/不具有状态信息的情况下，在状态约束 $\mathcal{R}$ 下经典-量子复合搭线信道 $\mathcal{N}$ 中可实现的，如果存在一个序列 $(\mathcal{C}_n)_{n\in\mathbb{N}}$ 的 (n,M_n,λ_n,μ_n) 编码，该编码具有/不具有发射机的状态信息，并遵守状态约束 $\mathcal{R}$，使得 $\lambda_n\to 0$ 和 $\mu_n\to 0$ 以及 $\liminf_{n\to\infty}\frac{1}{n}\log M_n\geq R$。带有（不带）发送器状态信息的 $\mathcal{N}$ 的秘密消息传输容量被定义为所有可实现于 $\mathcal{N}$ 带有（不带）状态信息的速率的上确界，并表示为 C_{CSI}（C_{noCSI}）。

III. 预备知识

引理 3 (覆盖引理 [11, Chapter 17]): 设 $\mathcal{X}$ 是一个集合，$p_X(x)$ 是在 $\mathcal{X}$ 上的概率分布。然后 $\{p_X(x),\rho_x\}_{x\in\mathcal{X}}$，其中 $\{\rho_x\}_{x\in\mathcal{X}}\subset\mathcal{P}(\mathcal{H})$ 对于某些 $\mathcal{H}$，被称为真实集成。令 $\mathcal{L}$ 是一个集合，并为每个 $l\in\mathcal{L}$ 根据 $p_X(x)$ 随机选择一个码字 X_l，则 $\left\{\frac{1}{|\mathcal{L}|},\rho_{X_l}\right\}_{l\in\mathcal{L}}$ 被称为伪组合。设有一个码空间投影器 Π，它是一个满足

$$\mathrm{Tr}\left[\rho_x\Pi\right]\geq 1-\varepsilon,\qquad \mathrm{Tr}\left[\Pi\right]\leq D, \tag{III.1}$$

的正交投影器，以及一组具有性质

$$\mathrm{Tr}\left[\rho_x\Pi_x\right]\geq 1-\varepsilon,\qquad \Pi_x\rho_x\Pi_x\leq\frac{1}{d}\Pi_x, \tag{III.2}$$

的码字投影器 $\{\Pi_x\}_{x\in\mathcal{X}}$，其中 $\varepsilon>0$ 和 $0<d<D$。令 $\bar{\rho}=\sum_{x\in\mathcal{X}}p_X(x)\rho_x$ 为真实集合的平均状态，令 $\bar{\rho}_{\mathcal{L}}=\frac{1}{|\mathcal{L}|}\sum_{l\in\mathcal{L}}\rho_s$ 为虚假集合的平均状态。则

$$\Pr\left\{||\bar{\rho}-\bar{\rho}_{\mathcal{L}}||_1\leq 30\varepsilon^{\frac{1}{4}}\right\}\geq 1-2De^{-\frac{\varepsilon^3|\mathcal{L}|d}{4D}}, \tag{III.3}$$

给定 ε 较小且 $|\mathcal{L}|\gg\frac{\varepsilon^3 d}{D}$。概率是相对于随机代码簿选择而言的。注意原始界限紧一些。

我们还广泛使用了量子典型性和强经典典型性的概念。关键属性如下所述；完整讨论请参见 [11]。

定义 4 (强典型性): 令 $\mathcal{X}$ 为一个有限集，$x^n=(x_1,\ldots,x_n)$ 为一个序列，$x_1,\ldots,x_n\in\mathcal{X}$ 和 $N(x|x^n)$ 是符号 x 在 x^n 中出现的次数。令 $p_X(x)$ 为随机变量 X 的概率分布。对于 $\delta>0$，δ-强典型集 $T_\delta^{X^n}$ 包含所有 x^n 其中

$$\forall x\in\mathcal{X},\begin{cases}\left|\frac{1}{n}N(x|x^n)-p_X(x)\right|\leq\delta & \text{if } p_X(x)>0,\\ \frac{1}{n}N(x|x^n)=0 & \text{else}\end{cases}.$$

对于 $\varepsilon,\delta>0$，足够大的 n 和一个正常数 c，$T_\delta^{X^n}$ 具有性质

$$\Pr\{X^n\in T_\delta^{X^n}\}\geq 1-(2n)^{-|\boldsymbol{X}|}2^{-n\varepsilon^2\log(2)/2} \tag{III.4}$$

$$(2n)^{-|\boldsymbol{X}|}2^{n(H(X)-c\delta)}\leq|T_\delta^{X^n}|\leq 2^{n(H(X)+c\delta)}, \tag{III.5}$$

其中 $H(X)=\sum_{x\in\mathcal{X}}p_X(x)\log(p_X(x))$ 是熵。

定义 5 (典型子空间): 令 $\rho\in\mathcal{P}(\mathcal{H})$ 是一个具有谱分解 $\rho=\sum_{x\in\mathcal{X}}p_X(x)\left|x\right\rangle\!\left\langle x\right|$ 的密度算子。对于每个 $n\in\mathbb{N}$，投射到 $\rho^{\otimes n}$ 的典型子空间上的投影定义为

$$\Pi_{\rho,\delta}^n=\sum_{x^n\in T_\delta^{X^n}}\left|x^n\right\rangle\!\left\langle x^n\right|, \tag{III.6}$$

其中 $T_\delta^{X^n}$ 是 $p_{X^n}(x^n)=p_X(x_1)\ldots p_X(x_n)$ 长度为 n 的典型序列的集合。它具有以下性质，对于足够大的 n 和任意的 $\epsilon,\delta>0$：

$$\mathrm{Tr}\left[\Pi_{\rho,\delta}^n\right]\leq 2^{n(S(\rho)+\delta)}, \tag{III.7}$$

$$\mathrm{Tr}\left[\Pi_{\rho,\delta}^n\rho^{\otimes n}\right]\geq 1-\epsilon, \tag{III.8}$$

$$2^{-n\delta}\Pi_{\rho,\delta}^n\leq 2^{nS(\rho)}\Pi_{\rho,\delta}^n\rho^{\otimes n}\Pi_{\rho,\delta}^n\leq 2^{n\delta}\Pi_{\rho,\delta}^n. \tag{III.9}$$

空间 $\mathrm{span}\left\{\left|x^n\right\rangle\right\}_{x^n\in T_\delta^{X^n}}$ 被称为典型子空间。

引理 6 (相干态近似): 令 $\left|\alpha\right\rangle$ 为一个凝聚态，$P_N=\sum_{n=0}^N\left|n\right\rangle\!\left\langle n\right|$ 其中 $\left|n\right\rangle$ 是光子数态，是截断在 N 的 Fock 空间的投影算子。则对于所有 $N>8e|\alpha|^2$，有

$$\mathrm{Tr}\left[P_N\left|\alpha\right\rangle\!\left\langle\alpha\right|\right]\geq 1-\frac{1}{2}2^{-N} \tag{III.10}$$

显然相同的界限适用于状态 $\rho=\sum_{\alpha\in A}p(\alpha)\left|\alpha\right\rangle\!\left\langle\alpha\right|$，只要 $N>8e|\alpha|^2\ \forall\alpha\in A$。

引理 6 可由斯特林公式及以下观察得出：对于每一个 $c>0$，当 N 足够大时，我们有 $(c/N)^N<2^{-N}$。

引理 7: 令 $\mathcal{X}$ 是一个有限集，$\mathcal{H}$ 是一个希尔伯特空间，并且 $\mathcal{N}=\{\mathcal{N}_s\}_{s\in\boldsymbol{S}}\subset C(\mathcal{X},\mathcal{H})$ 是一个经典-量子复合信道，其中 $\boldsymbol{S}$ 是一组有限的信道状态。令 $\{|e_x\rangle\}_{x\in\mathcal{X}}$ 为复希尔伯特空间 $\mathbb{C}^{|\mathcal{X}|}$ 的一个标准正交基，且令 $p(x)$

对于 $x \in \mathcal{X}$ 是定义在 $\mathcal{X}$ 上的一个概率分布。此外，我们定义“修剪”分布 $p'_{X'^n}$ 为

$$p'_{X'^n}(x^n) = \frac{1}{\Delta_\delta^n} p_{X^n}(x^n) \mathbb{1}_{T_\delta^{X^n}}(x^n) \tag{III.11}$$

其中 $\Delta_\delta^n = \sum_{x^n \in T_\delta^{X^n}} p_{X^n}(x^n)$。对于块长度 $n \in \mathbb{N}$，在 $\mathbb{C}^{|\mathcal{X}|} \otimes \mathcal{H}$ 上定义以下状态：

$$\rho_n = \frac{1}{|\boldsymbol{S}|} \sum_{s \in \boldsymbol{S}} \sum_{x^n \in \boldsymbol{X}^n} p_n(x^n) \left|e_{x^n}\right\rangle\!\left\langle e_{x^n}\right| \otimes \mathcal{N}_s^{\otimes n}(x^n), \tag{III.12}$$

$$\tau_n = \left(\sum_{x^n \in \boldsymbol{X}^n} p_n(x^n) \left|e_{x^n}\right\rangle\!\left\langle e_{x^n}\right| \right) \otimes \frac{1}{|\boldsymbol{S}|} \sum_{s \in \boldsymbol{S}} \left(\sum_{x^n \in \boldsymbol{X}^n} p_n(x^n) \mathcal{N}_s^{\otimes n}(x^n) \right). \tag{III.13}$$

令 $\mathcal{C}^n = \{C_m^n\}_{m=1}^{K_n}$ 是一个随机码，其中每个元素 C_m^n 都是根据 $p'_n(x)$ 从 $\mathcal{X}^n$ 中独立随机选取的。然后如果对于某些 $\lambda \in [0,1]$ 和 $a > 0$ 存在一个投影器 P_n 使得

$$\operatorname{Tr}[P_n \rho_n] \geq 1 - \lambda \qquad \text{and} \qquad \operatorname{Tr}[P_n \tau_n] \leq 2^{-na}, \tag{III.14}$$

对于任意的 γ 满足 $0 < \gamma \leq a$ 和 $K_n = \lfloor 2^{n(a-\gamma)} \rfloor$，则存在一个解码 POVM $\{D_{C_m^n}^n\}_{m=1}^{K_n}$ 使得

$$\mathbb{P}(\min_{s \in \boldsymbol{S}} p_{err}(\mathcal{C}) < \xi^{\frac{1}{2}}) \geq 1 - \xi^{\frac{1}{2}} \tag{III.15}$$

其中

$$p_{err} = 1 - \frac{1}{K_n} \sum_{m=1}^{K_n} \operatorname{Tr}\left[\mathcal{N}_s^{\otimes n}(C_m^n) D_{C_m}^n\right], \text{ and} \tag{III.16}$$

$$\xi = |\boldsymbol{S}|(2\lambda + 2(1 - \Delta_\delta^n) + \frac{4}{(\Delta_\delta^n)^2} 2^{-n\gamma}) \tag{III.17}$$

本引理是来自 [2] 的引理 1 的改编版，其中还包含

引理 8 ([2, Lemma 5]): 对于每一个 $\delta > 0$，有限的复合 cq-信道 $\mathcal{N} = \{\mathcal{N}_s\}_{s \in \boldsymbol{S}} \subset C(\mathcal{X}, \mathcal{H})$ 和定义在 $\mathcal{X}$ 上的概率分布 p，存在一个常数 $\tilde{c}$，使得对于足够大的 $n \in \mathbb{N}$，存在一个投影器 $P_{n,\delta} \in \mathcal{B}\left((\mathbb{C}^{|\mathcal{X}|})^{\otimes l} \otimes \mathcal{H}^{\otimes l}\right)$，其具有以下性质

$$\operatorname{Tr}\left[P_{n,\delta} \rho_n\right] \geq 1 - |\boldsymbol{S}| \, 2^{-n\tilde{c}}, \tag{III.18}$$

$$\operatorname{Tr}\left[P_{n,\delta} \tau_n\right] \leq 2^{-n(a-\delta)}, \tag{III.19}$$

其中 $a := \min_{s \in \boldsymbol{S}} D(\rho_s \| \hat{p} \otimes \sigma_s)$ 的状态为

$$\hat{p} := \sum_{x \in \boldsymbol{X}} p(x) \left|e_x\right\rangle\!\left\langle e_x\right|, \quad \sigma_s := \sum_{x \in \boldsymbol{X}} p(x) \mathcal{N}_s(x), \tag{III.20}$$

$$\rho_s := \sum_{x \in \boldsymbol{X}} p(x) \left|e_x\right\rangle\!\left\langle e_x\right| \otimes \mathcal{N}_s(x). \tag{III.21}$$

$D(\cdot \| \cdot)$ 是量子相对熵，而 ρ_n,τ_n 根据 (III.12),(III.13) 定义。

我们注意到，8 引理的证明在某些情况下也有效，即对于某个 $t > 0$ 存在 $|\boldsymbol{S}| = \mathcal{O}(n^t)$，如 [2, equation (74)] 中明确所示。

引理 9 (有限支撑近似):
设 $0 \leq \rho, \sigma, \Lambda \leq \mathbb{1}$。那么

$$\operatorname{Tr}[\Lambda \rho] \leq \operatorname{Tr}[\Lambda \sigma] + \|\rho - \sigma\|_1. \tag{III.22}$$

证明见 [12]。

引理 10 (冯 · 诺伊曼熵连续性界): 令 $\hat{N}$ 表示光子数算符，并考虑无穷维可分希尔伯特空间 $\mathcal{H}$ 上的两个量子态 ρ 和 σ。假设这些状态满足条件

$$\max\{\operatorname{Tr}\left[\hat{N}\rho\right], \operatorname{Tr}\left[\hat{N}\sigma\right]\} \leq E \leq \infty, \text{ and } \frac{1}{2}\|\rho - \sigma\|_1 \leq \varepsilon,$$

其中 $0 \leq \varepsilon \leq \frac{E}{1+E}$。在这些条件下，von Neumann 熵 ρ 和 σ 满足连续性边界

$$|S(\rho) - S(\sigma)| \leq h(\varepsilon) + E \cdot h\left(\frac{\varepsilon}{E}\right). \tag{III.23}$$

该版本来自 [1]，基于 [13]。

IV. 结果

定理 11: 对于由满足 $(\tau, \eta) \in \boldsymbol{S} \implies \tau > \eta$ 的状态集 $\boldsymbol{S}$ 定义的复合窃听信道，并且具有平均功率约束，要求每个块长度为 n 和每个长度为 M_n 的码字均需满足 $\sum_{i=1}^{M_n} |x_i|^2 \leq nE$，发送方在有 Channel State Information (CSI) 时的秘密消息传输容量是

$$C_{\text{CSI}} = \inf_{s \in \boldsymbol{S}} \left(g(\tau E) - g(\eta E)\right), \tag{IV.1}$$

而没有 CSI 时则是

$$C_{\text{noCSI}} = \left(\inf_{s \in \boldsymbol{S}} g(\tau E) - \sup_{s \in \boldsymbol{S}} g(\eta E)\right)_+. \tag{IV.2}$$

V. 证明

逆命题：两个反向结果都来自于玻色子窃听通道 [10, Theorem 27] 的反向结果。在状态信息的情况下，所有 $(\tau,\eta)\in\boldsymbol{S}$ 中最坏情况的选择决定了性能。如果没有提供这样的状态信息，则正确传输（a）和安全传输（b）的数据要求解耦，并且 [10, Theorem 27] 再次提供了反向结果。

直接部分：我们首先考虑一个有限的信道状态集 $\boldsymbol{S}_n$，让其依赖于块长 n 作为 $|\boldsymbol{S}_n|=\mathcal{O}(n^t)$ 对于某些 $t\geq 0$ 和一个有限的 $\mathcal{X}\subset\mathbb{C}$，并将结果扩展到连续集合。令 $(\tau,\eta)=s\in\boldsymbol{S}_n$，其中 τ 是信道到接收者的透传率，η 是到窃听者的透传率。考虑序列 $x^n=x_1,\ldots,x_n$，其中每个 x_i 取值于 $\mathcal{X}$。然后经过 n 次信道使用后，接收方获得状态 $\rho^s_{x^n}=\rho^s_{x_1}\otimes\cdots\otimes\rho^s_{x_n}$，窃听者获得 $\tilde{\rho}^s_{x^n}=\tilde{\rho}^s_{x_1}\otimes\cdots\otimes\tilde{\rho}^s_{x_n}$，其中 $\rho^s_x=|\tau x\rangle\langle\tau x|$ 和 $\tilde{\rho}^s_x=|\eta x\rangle\langle\eta x|$。

设 X^n 是一个具有 n 重概率分布 $p_{X^n}(x^n)=p_X(x_1)\ldots p_X(x_n)$ 的随机变量，并且令 $p'_{X'^n}$ 是如在 III.11 中定义的相应的“修剪”分布。我们使用引理 9 和 6 来考虑传输状态的有限维近似。对于状态 ρ，我们设定 $\rho'=\lambda\cdot P_N\rho P_N$，其中 $\lambda>0$ 确保归一化。根据此定义和引理 6，我们得到 $\|\rho-\rho'\|_1\leq 2^{-N}$ 对于足够大的 N。对于 n 模态状态，我们必须将这个界限乘以 n，这意味着为了在大的 n 下得到一个消失的误差，我们需要 $N\sim\log(n)$，也就是说我们的 n 模态近似状态具有 $\sim\log(n)^n$ 维。如果我们设例如 $N=2\log(n)$，则对于足够大的 n，一个 n 模式状态的最大近似误差被上限为 $\frac{1}{n}$。对于容量和保密部分，我们首先证明良好的代码存在于近似的状态中，然后论证相同的代码和算子在原始状态下表现几乎同样好。

令 $\bar{\rho}'^s=\mathbb{E}_X\rho'^s_X=\sum_{x\in\mathcal{X}}p_X(x)\rho'^s_x$ 为接收器处的有限近似单模平均状态。设 $a=\inf_{s\in\boldsymbol{S}_n}S(\bar{\rho}'^s)$，取一个 γ 并使用 $0<\gamma\leq a$ 定义 $K_n=\lfloor 2^{n(a-\gamma)}\rfloor$。然后引理 7 和 8 表明，对于足够大的 n，存在一个随机码 $\mathcal{C}^n=\{C^n_m\}_{m=1}^{K_n}$，其中每个元素 C^n_m 都是根据 $p'_n(x)$ 从 $\mathcal{X}^n$ 中独立随机选取的，对应的 POVM $\{D^n_{C^n_m}\}_{m=1}^{K_n}$ 和相关的常数 $\tilde{c}$ 满足

$$\begin{aligned}&\mathbb{E}_{\mathcal{C}^n}\min_{s\in\boldsymbol{S}_n}\frac{1}{K_n}\sum_{m=1}^{K_n}\mathrm{Tr}\big[\rho'^s_{C^n_m}D^n_{C^n_m}\big]\\&\geq 1-|\boldsymbol{S}_n|(2|\boldsymbol{S}_n|2^{-n\tilde{c}}+2(1-\Delta^n_\delta)+\frac{4}{(\Delta^n_\delta)^2}2^{-n\gamma}),\end{aligned}\tag{V.1}$$

因此，借助引理 9，当 n 足够大时使得 $(\Delta^n_\delta)^2>1/2$

$$\begin{aligned}&\mathbb{E}_{\mathcal{C}^n}\min_{s\in\boldsymbol{S}_n}\frac{1}{K_n}\sum_{m=1}^{K_n}\mathrm{Tr}\big[\rho^s_{C^n_m}D^n_{C^n_m}\big]\\&\geq 1-|\boldsymbol{S}_n|(2|\boldsymbol{S}_n|2^{-n\tilde{c}}+2(1-\Delta^n_\delta)+8\cdot 2^{-n\gamma})-\tfrac{1}{n}.\end{aligned}\tag{V.2}$$

因此这样的随机码对于 $n\to\infty$ 具有消失的错误概率。如前所述，在充分大的 n 下，我们有 $\|\bar{\rho}'^s-\bar{\rho}^s\|_1\leq\frac{1}{n}$，其中 $\bar{\rho}^s=\mathbb{E}_X\rho^s_X$。因此通过引理 10，我们得到 $S(\bar{\rho}'^s)\geq S(\bar{\rho}^s)-h\left(\frac{1}{n}\right)-E\cdot h\left(\frac{1}{E\cdot n}\right)$，这意味着

$$\lim_{n\to\infty}S(\bar{\rho}'^s)=S(\bar{\rho}^s).\tag{V.3}$$

在下一部分中，我们使用覆盖引理（引理 3）来证明如果我们将代码划分成合适的“虚假”集合，则相同的随机码可以实现保密性。因此，我们构造了一组投影器 $\tilde{\Pi}^n$ 和 $\tilde{\Pi}^n_{x^n}$，其具有性质

$$\mathrm{Tr}\left[\tilde{\Pi}^n\tilde{\rho}'^s_{x^n}\right]\geq 1-\tilde{\varepsilon},\tag{V.4}$$

$$\mathrm{Tr}\left[\tilde{\Pi}^n_{x^n}\tilde{\rho}'^s_{x^n}\right]\geq 1-\tilde{\varepsilon},\tag{V.5}$$

$$\mathrm{Tr}\left[\tilde{\Pi}^n\right]\leq\tilde{D},\tag{V.6}$$

$$\tilde{\Pi}^n_{x^n}\tilde{\rho}'^s_{x^n}\tilde{\Pi}^n_{x^n}\leq\tfrac{1}{\tilde{d}}\tilde{\Pi}^n_{x^n},\tag{V.7}$$

对于某些 $0<\tilde{d}<\tilde{D}$ 和 $0<\tilde{\varepsilon}<1$。代码词投影仪很简单，我们利用我们的状态是纯态这一事实，因此它们本身就是秩一投影仪，并且我们可以设置 $\tilde{\Pi}^n_{x^n}=\tilde{\rho}^s_{x^n},\tilde{d}=1$，满足属性 (V.5) 和 (V.7)。对于代码空间投影仪，我们使用与平均状态 $\tilde{\sigma}^s=\sum_{x\in\mathcal{X}}p_X(x)\tilde{\rho}'^s_x$ 对应的强典型子空间投影仪，并设置 $\tilde{\Pi}^n=\Pi^n_{\tilde{\sigma}^s,\delta}$。此定义使我们能够直接应用来自 [11] 的属性 15.2.7，确保 (V.4) 得到满足。为了满足 (V.6)，我们设定 $\tilde{D}=2^{n(S(\tilde{\sigma}^s)+\delta)}$，由于典型子空间投影器的性质。

我们已经看到，对于足够大的 n，我们有 $\|\tilde{\sigma}^\eta-\tilde{\rho}^\eta\|_1\leq\frac{1}{n}$，其中 $\tilde{\rho}^\eta=\mathbb{E}_X\tilde{\rho}^\eta_X$ 是无限维度下的单模平均状态。通过引理 10 和输入能量约束 E，我们可以看到近似态的熵趋近于原始态的熵：

$$S(\tilde{\sigma}^\eta)\geq S(\tilde{\rho}^\eta)-h\left(\tfrac{1}{n}\right)-E\cdot h\left(\tfrac{1}{E\cdot n}\right).\tag{V.8}$$

现在令 $\mathcal{M}$ 为一组消息，并令 $\mathcal{L}$ 为一个具有 $|\mathcal{M}||\mathcal{L}|\leq K_n$ 的索引集。我们将之前的随机码稍作重新标记，通过根据 $p'_{X^n}(X^n_{m,l})$ 从 X^n 中选择 $|\mathcal{L}|$ 个随机变量 $X^n_{m,l}$，针对每个消息 $m\in\mathcal{M}$，得到了

$\mathcal{C}_n = \left\{X^n_{m,l}\right\}_{m\in\mathcal{M},l\in\mathcal{L}}$。特定代码中窃听者的平均近似状态是

$$\tilde{\rho}'^s_{\mathcal{C}} = \frac{1}{|\mathcal{M}||\mathcal{L}|}\sum_{m\in\mathcal{M},l\in\mathcal{L}} \tilde{\rho}'^s_{X^n_{m,l}}, \tag{V.9}$$

由消息 m 定义的集合的平均状态是

$$\tilde{\rho}'^s_{\mathcal{C},m} = \frac{1}{|\mathcal{L}|}\sum_{l\in\mathcal{L}} \tilde{\rho}'^s_{X^n_{m,l}}. \tag{V.10}$$

然后由于引理 3，我们有

$$\Pr\left\{\|\tilde{\rho}'^s_{\mathcal{C}} - \tilde{\rho}'^s_{\mathcal{C},m}\|_1 \le 30\tilde{\varepsilon}^{\frac{1}{4}}\right\} \ge 1 - 2\tilde{D}2^{-\frac{\varepsilon^3|\mathcal{L}|\tilde{d}}{4\tilde{D}}}, \tag{V.11}$$

给定 ε 很小且 $|\mathcal{L}| \gg \frac{\tilde{\varepsilon}^3\tilde{d}}{\tilde{D}}$。然后对于非近似状态

$$\tilde{\rho}^s_{\mathcal{C}} = \frac{1}{|\mathcal{M}||\mathcal{L}|}\sum_{m\in\mathcal{M},l\in\mathcal{L}} \tilde{\rho}^s_{X^n_{m,l}}, \tag{V.12}$$

$$\tilde{\rho}^s_{\mathcal{C},m} = \frac{1}{|\mathcal{L}|}\sum_{l\in\mathcal{L}} \tilde{\rho}^s_{X^n_{m,l}}, \tag{V.13}$$

我们有 $\tilde{\varepsilon} = 1/n^4$

$$\Pr\left\{\|\tilde{\rho}^s_{\mathcal{C}} - \tilde{\rho}^s_{\mathcal{C},m}\|_1 \le \tfrac{32}{n}\right\} \ge 1 - 2\tilde{D}2^{-\frac{n^{-12}|\mathcal{L}|\tilde{d}}{4\tilde{D}}}. \tag{V.14}$$

与 (V.8) 一起，这确保了对于足够大的 n，窃听者 (II.2) 的信息泄露可以任意小，如果 $|\mathcal{L}| > 2^{nS(\tilde{\rho}^s)}$ 成立的话。为了保证所有 $s \in \boldsymbol{S}_n$ 的信息泄露消失，合法方因此选择 $|\mathcal{L}| > \sup_{s\in\boldsymbol{S}_n} 2^{nS(\tilde{\rho}^s)}$。对所有 $s \in \boldsymbol{S}_n$ 应用联合界（union bound）得到了期望的结果。

我们已经证明，我们的随机码在数据传输和信息泄漏中具有实现低错误概率的特性，并且上限趋近于 0，当 n 趋向无穷大时。由于联合界，至少一个码将同时实现这两点，并且对于每一个 ε' 和足够大的 n 我们得到界

$$|\mathcal{M}| > \inf_{s\in\boldsymbol{S}_n} 2^{n(S(\bar{\rho})-S(\tilde{\rho}^s)-\varepsilon')}. \tag{V.15}$$

因为 ε' 是任意的，这意味着

$$C_{\text{noCSI}} \ge \lim_{n\to\infty}\inf_{s\in\boldsymbol{S}_n} S(\bar{\rho}^s) - \sup_{s\in\boldsymbol{S}_n} S(\tilde{\rho}^s). \tag{V.16}$$

在发送端有信道状态信息的情况下，传输被分割成两个长度为 $n_1 = \sqrt{n}$ 和 $n_2 = n - n_1$ 的块。在第一块中，发送者添加了一个衰减通道，使得实际信道的透射率为 $\tau_{\min} := (\tau_{\min}, \eta') \in \boldsymbol{S}_n : \tau_{\min} \le \tau\forall(\tau,\eta) \in \boldsymbol{S}_n$。发送方和接收方然后使用一个传输率为 $\tau^2_{\min}$、容量为 $C'' > 0$ 的纯损耗信道的数据传输码，以传输 $M_1 := 2^{\sqrt{n}C''}$ 位的信道状态信息，从而描述具有属性 $\tau_a \le \tau \le \tau_b$ 和 $\eta_a \le \eta \le \eta_b$ 以及 $|\tau_a - \tau_b| \le 2^{-M_1}$ 和 $|\eta_a - \eta_b| \le 2^{-M_1}$ 的两个集合 $(\tau_a, \tau_b]$ 和 $(\eta_a, \eta_b]$。之后他们使用一个不含 CSI 的代码来处理状态集为 $\boldsymbol{S}'_n := (\tau_a, \tau_b] \times (\eta_a, \eta_b]$ 的复合信道，从而建立

$$C_{\text{CSI}} \ge \lim_{n\to\infty}\inf_{s\in\boldsymbol{S}'_n} (S(\bar{\rho}^s) - S(\tilde{\rho}^s)) - \varepsilon' \tag{V.17}$$

其中 ε' 可以尽可能小。在能量约束 $\mathrm{Tr}\left[\hat{N}\int_{u\in\mathbb{C}} p(u)\mathcal{N}_\tau(u)du\right] \le E$ 下，使状态 $\int_{u\in\mathbb{C}} p(u)\mathcal{N}_\tau(u)du$ 的熵最大化的概率分布 $p(u)$ 是复高斯分布 $p(u) = \frac{1}{\pi E}2^{-|u|^2/E}$，其熵为

$$S\Big(\int_{u\in\mathbb{C}} p(u)\mathcal{N}_\tau(u)du\Big) = g(\tau^2 E). \tag{V.18}$$

。我们使用该分布的离散化形式来证明定理 11，如下所述：我们考虑集合 $\mathcal{E}_\Delta = \left\{|x\rangle\langle x|, p^{\hat{\Delta}}_X(x)\right\}_{x\in\mathcal{X}_\Delta}$，其中对于 $\Delta > 0$，$\mathcal{X}_\Delta$ 是一个有限集，它以以下方式逼近复高斯分布

$$\max_{0\le\gamma\le1}\left\|\frac{1}{\pi E}\int_{\mathbb{C}} 2^{-|x|^2/E}\mathcal{N}_\gamma(x)dx - \nu^\gamma_\Delta\right\|_1 \le \Delta \tag{V.19}$$

其中对于所有 γ 都有 $\nu^\gamma_\Delta = \sum_{x\in\mathcal{X}_\Delta} p^{\hat{\Delta}}_X(x)\mathcal{N}_\gamma(x)$ 和 $\mathrm{Tr}\left[\hat{N}\nu^\gamma_\Delta\right] \le E$。详情见附录。然后引理 10 暗示了

$$\lim_{\Delta\to0} S(\nu^1_\Delta) = S\left(\int_{u\in\mathbb{C}} p(u)\mathcal{N}_1(u)du\right). \tag{V.20}$$

由于 (V.18)，我们已经证明了

$$C_{\text{CSI}} = \lim_{n\to\infty}\inf_{s\in\boldsymbol{S}_n}\big(g(\tau^2E) - g(\eta^2E)\big) \tag{V.21}$$

$$C_{\text{noCSI}} = \lim_{n\to\infty}\big(\inf_{s\in\boldsymbol{S}_n} g(\tau^2E) - \sup_{s\in\boldsymbol{S}_n} g(\eta^2E)\big)_+. \tag{V.22}$$

最后我们指定了 $\boldsymbol{S}_n$。对于任何 $\boldsymbol{S} \subset [0,1]\times[0,1]$，都存在一个 $\boldsymbol{S}'_{\mu^{-1/2}} \subset \boldsymbol{S}$，使得 $\forall(\tau,\eta) \in \boldsymbol{S}\ \exists(\tau',\eta') \in \boldsymbol{S}'_{\mu^{-1/2}} : |\tau'-\tau| \le \mu, |\eta'-\eta| \le \mu$ 和 $\left|\boldsymbol{S}'_{\mu^{-1/2}}\right| \le \frac{1}{\mu^2}$。我们可以通过认识到在离散化 $\mathcal{X}_\Delta$ 中存在能量截止值 $\hat{E}_\Delta = \max_{x\in\mathcal{X}_\Delta}|x|^2$ 来简化论证。进一步，两个相干态的迹距离可以明确地表示为 $\||\alpha\rangle\langle\alpha| - |\beta\rangle\langle\beta|\|_1 = 2\cdot\sqrt{1-e^{-|\alpha-\beta|^2}}$，这表明对于每一个 $x^n \in \mathcal{X}^n_\Delta$ 和 $s \in \boldsymbol{S}$ 都存在一个 $s' \in \boldsymbol{S}'_{\mu^{-1/2}}$ 使得 $\left\|\rho^{s'}_{x^n} - \rho^s_{x^n}\right\|_1 \le 2\sqrt{1-e^{-n\mu\hat{E}_\Delta}}$。通过 $\mu = \frac{1}{n^2}$ 和引理 9，我们发现对于每一个 $\mathbb{1} \ge X \ge 0$

$$\mathrm{Tr}\left[\mathcal{N}^{\otimes n}_{s'}(x^n)X\right] \ge \mathrm{Tr}\left[\mathcal{N}^{\otimes n}_s(x^n)X\right] - 4\sqrt{\hat{E}/n}. \tag{V.23}$$

由于 $|\boldsymbol{S}'_n| = \mathcal{O}(n^4)$ 和 $\boldsymbol{S}'_n \subset \boldsymbol{S}$，定理 11 得证。

附录

高斯离散化

我们希望离散化一个高斯相干态集 $\left\{\frac{1}{\pi E}e^{-|x|^2/E}, |x\rangle\langle x|\right\}_{x\in\mathbb{C}}$，其平均状态为 $\bar{\rho} = \int_{x\in\mathbb{C}} \frac{1}{\pi E}e^{-|x|^2/E}\,|x\rangle\langle x|\,dx$，使得我们得到一个集合 $\{p_X(x), |x\rangle\langle x|\}_{x\in\mathcal{X}}$，其中 $\mathcal{X}$ 是一个有限集，p_X 是一个概率分布，其平均状态 $\bar{\rho}' = \sum_{x\in\mathcal{X}} p_X(x)\,|x\rangle\langle x|$ 接近原始的并具有有界能量：

$$\|\bar{\rho}' - \bar{\rho}\| \le \varepsilon, \qquad \mathrm{Tr}[\hat{N}\bar{\rho}'] \le \mathrm{Tr}[\hat{N}\bar{\rho}], \tag{V.24}$$

对于某些 $\varepsilon > 0$，其中 $\hat{N}$ 是光子数算符。

我们将复平面划分为有限数量的区域，并为每个区域分配一个复数 x 和一个概率 $p_X(x)$。分配给区域 $T_x \subset \mathbb{C}$ 的概率是 $p_X(x) = \int_{z\in T_x} \frac{1}{\pi E}e^{-|z|^2/E}dz$，我们选择相应的 x 使得 $x \in P_x$ 和 $|x|^2 = \mathrm{Tr}\left[\hat{N}\left(\int_{z\in T_x} \frac{1}{\pi E}e^{-|z|^2/E}\,|z\rangle\langle z|\,dz\right)\right]$。这并不能完全定义 x，但可以确保离散化集合的平均能量不超过连续集合的平均能量，并且对于我们的目的来说是足够的。我们首先考虑原点周围半径为 R 的圆内的所有内容。对于任意 $0 < r \le R$，可以通过使用 $c\left(\frac{R}{r}\right)^2$ 块，将复平面的这部分划分成若干部分，使得每个块都包含在一个半径为 r 的圆盘内，其中常数为 c。这表明对于任意的 $x' \in P_x, |x - x'| \le 2r$，因此 $\||x'\rangle\langle x'| - |x\rangle\langle x|\|_1 \le 2\sqrt{1 - e^{-4r^2}}$。相同的界限适用于任何补片的平均状态：

$$\left\||x\rangle\langle x| - \int_{z\in T_x} \frac{1}{\pi E}e^{-|z|^2/E}\,|z\rangle\langle z|\,dz\right\|_1 \tag{V.25}$$

$$\le \int_{z\in T_x} \frac{1}{\pi E}e^{-|z|^2/E}\,\||z\rangle\langle z| - |x\rangle\langle x|\|_1\,dz \tag{V.26}$$

$$\le \int_{z\in T_x} \frac{1}{\pi E}e^{-|z|^2/E} 2\sqrt{1 - e^{-4r^2}}dz \tag{V.27}$$

$$= 2p_X(x)\sqrt{1 - e^{-4r^2}}. \tag{V.28}$$

在半径为 R 的圆盘外剩余的复平面上，我们简单地赋值零：$p_X(0) = \int_{|x|>R} \frac{1}{\pi E}e^{-|x|^2/E}dx = e^{-R^2/E}$，或者如果已经分配了正概率给零，我们将它们相加。然后

$$\|\bar{\rho} - \bar{\rho}'\|_1 \le 2(1 - e^{-R^2/E})\sqrt{1 - e^{-4r^2}} + 2e^{-R^2/E} \tag{V.29}$$

通过选择合适的 r 和 R，我们得到了期望的结果。

编码引理修改

引理 7 是对引理 1 在 [2] 中的修改版本。证明使用了状态 ρ_n 和 τ_n。为了证明这个版本，我们定义稍有不同的状态

$$\rho'_n = \frac{1}{|\boldsymbol{S}_n|}\sum_{s\in\boldsymbol{S}_n}\sum_{x^n\in\boldsymbol{X}^n} p'_n(x^n)\delta_{x^n}\otimes\mathcal{N}_s^{\otimes n}(x^n), \tag{V.30}$$

$$\tau'_n = \sum_{x^n\in\boldsymbol{X}^n} p'_n(x^n)\delta_{x^n}\otimes\frac{1}{|\boldsymbol{S}_n|}\sum_{s\in\boldsymbol{S}_n}\sum_{x^n\in\boldsymbol{X}^n} p'_n(x^n)\mathcal{N}_s^{\otimes n}(x^n)$$

其中 $\delta_{x^n} := |e_{x^n}\rangle\langle e_{x^n}|$、$|e_{x^n}\rangle := \otimes_{i=1}^n |e_{x_i}\rangle$ 和 $|e_{x_i}\rangle$ 形成 $\mathbb{C}^{|\boldsymbol{X}|}$ 的正交基。然后按照 [2] 中的步骤进行，稍作修改。我们观察到 $\|\rho_n - \rho'_n\|_1 = 2(1 - \Delta_\delta^n)$。然后根据引理 9 我们有

$$\mathrm{Tr}\left[P_n\rho'_n\right] \ge 1 - \lambda - 2(1 - \Delta_\delta^n), \tag{V.31}$$

对于第二个性质，$\mathrm{Tr}\left[P_n\tau_n\right] \le 2^{-na}$，考虑如果我们用 $\Delta_\delta^n p'_n(x^n)$ 替换 τ'_n 定义中的 $p'_n(x^n)$，则与 τ_n 的唯一区别是去除了正项，因此 $\tau'_n \le \frac{1}{(\Delta_\delta^n)^2}\tau_n$。这表明

$$\mathrm{Tr}\left[P_n\tau'_n\right] \le \frac{1}{(\Delta_\delta^n)^2}\mathrm{Tr}\left[P_n\tau_n\right] \le \frac{1}{(\Delta_\delta^n)^2}2^{-na}. \tag{V.32}$$

其余的证明等同于在 [2] 中的证明。

参考文献

[1] Simon Becker, Nilanjana Datta, and Michael G. Jabbour. From classical to quantum: Uniform continuity bounds on entropies in infinite dimensions. *IEEE Transactions on Information Theory*, 69:4128–4144, 2021.

[2] Igor Bjelaković, Holger Boche, Gisbert Janßen, and Janis Nötzel. *Arbitrarily varying and compound classical-quantum channels and a note on quantum zero-error capacities*, page 247 – 283. Springer-Verlag, Berlin, Heidelberg, 2013.

[3] I. Bjelaković, H. Boche, and J. Sommerfeld. Secrecy results for compound wiretap channels. *Probl Inf Transm*, 49:73–98, 2013.

[4] Ning Cai, Andreas J. Winter, and Raymond W. Yeung. Quantum privacy and quantum wiretap channels. *Problems of Information Transmission*, 40:318–336, 2004.

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

[6] Alexander S. Holevo. *Quantum Systems, Channels, Information*. DE GRUYTER, Berlin, Boston, jan 2012.

[7] Kabgyun Jeong. Upper bounds on the private capacity for bosonic gaussian channels. *Physics Letters A*, 384(27):126730, 2020.

[8] Yingbin Liang, Gerhard Kramer, H. Vincent Poor, and Shlomo Shamai (Shitz). Compound wiretap channels. *J Wireless Com Network*, 2009.

[9] Stefano Pirandola, Samuel L Braunstein, Riccardo Laurenza, Carlo Ottaviani, Thomas P W Cope, Gaetana Spedalieri, and Leonardo Banchi. Theory of channel simulation and bounds for private communication. *Quantum Science and Technology*, 3(3):035009, may 2018.

[10] Kunal Sharma, Mark M Wilde, Sushovit Adhikari, and Masahiro Takeoka. Bounding the energy-constrained quantum and private capacities of phase-insensitive bosonic gaussian channels. *New Journal of Physics*, 20(6):063025, June 2018.

[11] Mark M. Wilde. *From Classical to Quantum Shannon Theory*. Cambridge University Press, Feb 2017.

[12] Mark M. Wilde, Saikat Guha, Si-Hui Tan, and Seth Lloyd. Explicit capacity-achieving receivers for optical communication and quantum reading. In *2012 IEEE International Symposium on Information Theory Proceedings*. IEEE, jul 2012.

[13] Andreas J. Winter. Tight uniform continuity bounds for quantum entropies: Conditional entropy, relative entropy distance and energy constraints. *Communications in Mathematical Physics*, 347:291–313, 2015.

[14] A. Wyner. The wiretap channel. *Bell Syst Tech. J.*, 54:1355–1387, 1975.