# 具有状态和因果信道状态信息的多址信道强保密性研究

Yiqi Chen*†、Tobias Oechtering†、Mikael Skoglund†和Yuan Luo*
*中国上海，上海交通大学，{chenyiqi,yuanluo}@sjtu.edu.cn
†瑞典皇家理工学院，瑞典斯德哥尔摩 100 44，{oech,skoglund}@kth.se

arXiv:2305.01393v1 [cs.IT] 2 May 2023

**摘要—本文研究存在外部窃听者的离散无记忆状态依赖多址信道（SD-MAC）上的强保密通信。该信道由离散无记忆且独立同分布的信道状态决定，信道状态信息以因果方式提供给编码器。本文给出了容量的一个内界。为建立该内界，我们研究了结合窃听信道编码以及发送方与合法接收方之间密钥协商的编码方案，并探讨了两种分块马尔可夫编码方案。第一种采用反向译码和Wyner-Ziv编码，并根据对信道状态信息的有损重构构造密钥。另一种则是对已有的、适用于具有因果信道状态信息的点对点窃听信道的编码方案进行扩展。我们进一步研究了具有退化消息集的状态依赖多址窃听信道（SD-MAWC）的一些容量可达情形。结果表明，在这些情形下，两种编码方案均为最优。**

## I. 引言

离散无记忆信道（DMC）上的安全通信最早在 [1] 中得到研究：发送方通过主信道向合法接收方进行通信，同时存在一个通过主信道的退化版本进行窃听的外部窃听者。随后， [2]将该模型扩展到一种更一般的情形，称为带机密消息的广播信道。继这些里程碑式的论文之后，近年来陆续有研究报告了不同广义多址信道模型的保密容量结果 [3–5]。

文献 [6]研究了编码器具有因果信道状态信息（CSI）的点对点信道。文献 [6], 证明，最优编码方案——香农策略——对于状态依赖多址信道（SD-MACs）并非最优；在某些情况下，采用分块马尔可夫编码、Wyner-Ziv编码和反向译码可获得严格更大的可达区域 [7], 。文献 [8]研究了各发送方具有独立状态的状态依赖多址信道。

在 [9] 中研究了编码器具有非因果信道状态信息的窃听信道，并通过结合 Gel’fand-Pinsker（GP）编码 [10] 与窃听信道编码，给出了保密容量的下界和上界。在 [11] 中，研究者进一步探讨了该模型，并采用了更严格的保密约束。对于状态依赖信道，掌握信道状态信息有助于通过该信道进行安全传输，因为系统参与者

本研究部分得到了中国国家重点研发计划项目（资助编号：2022YFA1005000）、国家自然科学基金项目（资助编号：61871264）和中国国家留学基金管理委员会（CSC）的资助。

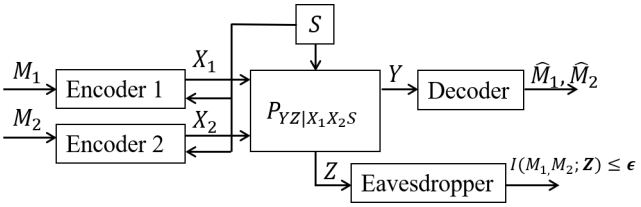


图 1：编码器具有因果信道状态信息的状态依赖多址窃听信道。

拥有一些额外资源，可用于构建密钥，并利用香农一次一密密码 [12]加密部分消息。窃听码与密钥协商的这种结合已用于近期有关状态依赖窃听信道（SD-WTCs）的研究。在 [13], 中，Chia 和 El Gamal 采用分块马尔可夫编码，研究了编码器和解码器均具有因果信道状态信息时，通过窃听信道进行安全通信的问题。在 [14] 和 [15] 中，研究了编码器具有因果信道状态信息的窃听信道。随后， [16] 利用软覆盖方法 [11]将研究结果进一步拓展至语义保密约束。

本文研究编码器具有因果信道状态信息、存在外部窃听者且满足强保密约束的状态依赖多址信道。我们设计了一种新的编码方案，将分块马尔可夫编码与 Wyner-Ziv编码、反向译码和密钥协商相结合 [17]。我们的内界涵盖了已有结果，并将现有针对其他模型的工作作为特殊情形纳入其中。

本文其余部分安排如下：第 II 节给出本文所考虑信道模型所需的符号和定义。第 III 节给出内界结果，该结果由三个不同的区域构成，分别对应不同的编码方案。前两种编码方案（分别称为编码方案 1 和编码方案2）将窃听信道编码与密钥协商相结合，而第三种编码方案仅使用窃听信道编码。第一种编码方案将在第 IV 节中介绍。第 V 节给出一些数值示例，以及一个编码方案 1 和 2 均达到最优的容量可达情形。第 VI 节总结全文。

## II. 符号与定义

本文中，随机变量和样本值分别用大写字母和小写字母表示，例如 $X$

以及 $x$。集合用花体字母表示。粗体大写和小写字母分别表示长度为 n 的随机变量序列和样本序列，例如 $\boldsymbol{X}=(X_1, X_2, \ldots\ldots, X_n)$ 以及$\boldsymbol{x}=(x_1, x_2, \ldots\ldots, x_n)$。令 $\mathrm{X}^n$ 表示 X 的 n重笛卡尔积，即所有可能的 $\boldsymbol{x}$所构成的集合。为表示子串，令 $X^b=(X_1, X_2, \ldots\ldots, X_b)$ 和 $X^{[b+1]}=(X_{b+1}, X_{b+2}, \ldots\ldots, X_n)$。我们用 $P_X$ 表示随机变量 $X$ 的概率质量函数（PMF），用 $P_{XY}$，$P_{X|Y}$ 分别表示联合概率质量函数和条件概率质量函数。给定集合 X 上所有 PMF 的集合记为 P (X)。对于根据某个分布 $P_X$ 独立同分布生成的序列 $\boldsymbol{x}$，我们记 $P_X^n(\boldsymbol{x})=\prod_{i=1}^n P_X(x)$。

**定义 1.** 带状态的离散无记忆多址窃听信道由随机转移矩阵$\mathcal{W}:\mathcal{X}_1\times\mathcal{X}_2\times\mathcal{S}\to\mathcal{Y}\times\mathcal{Z}$定义，其中$\mathcal{X}_1,\mathcal{X}_2$为有限输入字母表，$\mathcal{Y}$，$\mathcal{Z}$ 为有限输出字母表，$\mathcal{S}$ 为有限状态字母表。在给定状态序列 $\boldsymbol{s}$的情况下，从输入序列$(\boldsymbol{x}_1,\boldsymbol{x}_2)$ 到输出序列$(\boldsymbol{y},\boldsymbol{z})$ 的转移概率为

$$P_{YZ|X_1X_2S}(\boldsymbol{y},\boldsymbol{z}|\boldsymbol{x}_1,\boldsymbol{x}_2,\boldsymbol{s})=\prod_{i=1}^{n}P_{YZ|X_1X_2S}(y_i,z_i|x_{1i},x_{2i},s_i),$$

其中，$\boldsymbol{y}$ 是主信道的输出，$\boldsymbol{z}$ 是窃听信道的输出。信道状态序列由离散无记忆源生成，使得$P_S^n(\boldsymbol{s})=\prod_{i=1}^n P_S(s_i)$。

定义 *2.* 码 $(2^{nR_1},2^{nR_2},f_1^n,f_2^n,\phi)$由消息集合 $M_1=[1:2^{nR_1}]$，$M_2=[1:2^{nR_2}]$、编码器集合$f_{i,j}:M_i\times S^j\to X_i, i=1,2, j=1,\ldots,n$ 以及解码器$\phi:Y^n\to M_1\times M_2$组成。为传输消息 $M_i$，发送方发送码字 $\boldsymbol{X}_i$，其中每个分量 $X_{ij}$均按照 $f_{i,j}(M_i,\boldsymbol{S}^j)$生成。接收方接收 $\boldsymbol{Y}$，并通过解码器 $(\hat{M}_1,\hat{M}_2)=\phi(\boldsymbol{Y})$估计消息。码的平均译码错误率为

$$P_e=\frac{1}{|\mathcal{M}_1||\mathcal{M}_2|}\sum_{m_1\in\mathcal{M}_1}\sum_{m_2\in\mathcal{M}_2}Pr\{(M_1,M_2)\neq(\hat{M}_1,\hat{M}_2)|M_1=m_1,M_2=m_2\}.$$

码的信息泄漏定义为

$$I(M_1,M_2;\boldsymbol{Z}),$$

其中，$\boldsymbol{Z}$ 是窃听信道的输出。

**定义 3**。 如果对于任意 $\epsilon>0$，都存在一个 $n_0$，使得对于所有 $n>n_0$，都存在一个码（$2^{nR_1},2^{nR_2},f_1^n,f_2^n,\phi$），则称速率对（$R_1,R_2$）对于具有编码器因果信道状态信息的多址窃听信道是可达的，其中

$$P_e\leq\epsilon, I(M_1,M_2;\boldsymbol{Z})\leq\epsilon.$$

多址窃听信道的保密容量是所有可实现速率对集合的闭包。

## III. 主要结果

给定 $P_S$ 和 $P_{YZ|X_1X_2S}$，将区域 $\mathrm{R}_{1i}(P_{VUU_1U_2X_1X_2|S})$，$i=1,2,3$ 定义为由实数对 $(R_1,R_2)$ 组成的集合，使得

$$\mathcal{R}_{11}(P_{VUU_1U_2X_1X_2|S})=\begin{cases}R_1\leq\min\{I(U_1;Y|V,U,U_2)-I(U_1;Z|S,U)+R_{11}, I(U_1;Y|V,U,U_2)\};\\ R_2\leq\min\{I(U_2;Y|V,U,U_1)-I(U_2;Z|S,U)+R_{21}, I(U_2;Y|V,U,U_1)\};\\ R_1+R_2\leq\min\{R_{SUM}, R_{SUM}-I(U_1,U_2;Z|S,U)+R_{11}+R_{21}\};\\ R_{11}+R_{21}\leq I(V;Y)-I(V;U,Z).\end{cases}$$

$$\mathrm{R}_{12}(P_{VUU_1U_2X_1X_2|S})=\begin{cases}R_1\leq\min\{I(U_1;Y|V,U,U_2),R_{11}\};\\ R_2\leq\min\{I(U_2;Y|V,U,U_1)-I(U_2;Z|S,U,U_1)+R_{21}, I(U_2;Y|V,U,U_1)\};\\ R_1+R_2\leq\min\{R_{SUM}, R_{SUM}-I(U_2;Z|S,U,U_1)+R_{21}, I(U_2;Y|V,U,U_1)-I(U_2;Z|S,U,U_1)+R_{11}+R_{21}\};\\ R_{11}+R_{21}\leq I(V;Y)-I(V;Z,U,U_1),\end{cases}$$

$$\mathrm{R}_{13}(P_{VUU_1U_2X_1X_2|S})=\begin{cases}R_1\leq\min\{I(U_1;Y|V,U,U_2)-I(U_1;Z|S,U,U_2)+R_{11}, I(U_1;Y|V,U,U_2)\};\\ R_2\leq\min\{I(U_2;Y|V,U,U_1),R_{21}\};\\ R_1+R_2\leq\min\{R_{SUM}, R_{SUM}-I(U_1;Z|S,U,U_2)+R_{11}, I(U_1;Y|V,U,U_2)-I(U_1;Z|S,U,U_2)+R_{11}+R_{21}\};\\ R_{11}+R_{21}\leq I(V;Y)-I(V;Z,U,U_2),\end{cases}$$

其中 $R_{SUM}=\min\{I(U_1,U_2;Y|V,U),I(V,U,U_1,U_2;Y)-I(V;S)\}$，且联合分布满足

$$P_SP_{VUU_1U_2X_1X_2YZ|S}=P_SP_{V|S}P_UP_{U_1|U}P_{U_2|U}P_{X_1|UU_1S}P_{X_2|UU_2S}P_{YZ|X_1X_2S}。$$

令 $\mathrm{R}_1$ 为以下集合的凸包

$$\bigcup_{\substack{P_{V|S}P_UP_{U_1|U}P_{U_2|U}\\P_{X_1|UU_1S}P_{X_2|UU_2S}}}\bigcup_{i=1}^{3}\mathcal{R}_{1i}(P_{VUU_1U_2X_1X_2|S}).$$

移除保密约束后，区域 $\mathrm{R}_1$ 简化为 [7,定理 3]。进一步定义 $\mathrm{R}_{2i}(P_{U_1U_2X_1X_2|S})$，$i=1,2,3$，为满足以下条件的实数对 $(R_1,R_2)$ 的集合：

$$\mathcal{R}_{21}(P_{U_1U_2X_1X_2|S})=\begin{cases}R_1\leq\min\{I(U_1;Y|U_2)-I(U_1;Z|S)+R_{11}, I(U_1;Y|U_2)-R_{12}\};\\ R_2\leq\min\{I(U_2;Y|U_1)-I(U_2;Z|S)+R_{21}, I(U_2;Y|U_1)-R_{22}\};\\ R_1+R_2\leq\min\{I(U_1,U_2;Y)-I(U_1,U_2;Z|S)+H(S|Z)-H(S|U_1U_2Y), I(U_1,U_2;Y)-H(S|U_1U_2Y)\};\\ R_{11}+R_{12}+R_{21}+R_{22}<H(S|Z);\\ R_{12}+R_{22}>H(S|Y,U_1,U_2).\end{cases}$$

$$\mathcal{R}_{22}(P_{U_1U_2X_1X_2|S}) =$$
$$\begin{cases} R_1 \le \min\{R_{11}, I(U_1;Y|U_2) - R_{12}\}; \\ R_2 \le \min\{I(U_2;Y|U_1) - I(U_2;Z|S,U_1) + R_{21}, \\ \qquad I(U_2;Y|U_1) - R_{22}\}; \\ R_1 + R_2 \le \min\{I(U_2;Y|U_1) - I(U_2;Z|S,U_1) + H(S|Z,U_1) \\ \qquad - H(S|U_1U_2Y), I(U_1,U_2;Y) - H(S|U_1U_2Y)\}; \\ R_{11} + R_{12} + R_{21} + R_{22} < H(S|Z); \\ R_{12} + R_{22} > H(S|Y,U_1,U_2). \end{cases}$$

$$\mathcal{R}_{23}(P_{U_1U_2X_1X_2|S}) =$$
$$\begin{cases} R_1 \le \min\{I(U_1;Y|U_2) - I(U_1;Z|S,U_2) + R_{11}, \\ \qquad I(U_1;Y|U_2) - R_{12}\}; \\ R_2 \le \min\{R_{21}, I(U_2;Y|U_1) - R_{22}\}; \\ R_1 + R_2 \le \min\{I(U_1;Y|U_2) - I(U_1;Z|S,U_2) + H(S|Z,U_2) \\ \qquad - H(S|U_1U_2Y), I(U_1,U_2;Y) - H(S|U_1U_2Y)\}; \\ R_{11} + R_{12} + R_{21} + R_{22} < H(S|Z); \\ R_{12} + R_{22} > H(S|Y,U_1,U_2), \end{cases}$$

其中联合分布为 $P_S P_{U_1U_2X_1X_2YZ|S} = P_S P_{U_1} P_{U_2} P_{X_1|U_1S} P_{X_2|U_2S} P_{YZ|X_1X_2S}$。类似地，令 $\mathrm{R}_2$为以下集合的凸包

$$\bigcup_{\substack{P_{U_1}P_{U_2} \\ P_{X_1|U_1S}P_{X_2|U_2S}}} \bigcup_{i=1}^{3} \mathcal{R}_{2i}(P_{U_1U_2X_1X_2|S}).$$

进一步定义区域 $\mathrm{R}_3$ ：令 $R_{11} = R_{21} = 0$ 属于 $\mathrm{R}_1$ ，并从 $\mathrm{R}_1$中与$Z$ ($I(U_1; Z|S, U)$, $I(U_1, U_2; Z|S, U)$, $etc$。)相关的所有减法项中去除 $S$ ，其联合分布为 $P_S P_{VUU_1U_2X_1X_2YZ|S} = P_S P_{V|S} P_U P_{U_1|U} P_{U_2|U} P_{X_1|UU_1S} P_{X_2|UU_2S} P_{YZ|X_1X_2S}$。

在全文中，我们将区域 $\mathrm{R}_1$ 的编码方案称为编码方案1，将区域 $\mathrm{R}_2$ 的编码方案称为编码方案2。

**定理 1**。令 $\mathcal{R}^{CSI}$ 为 $\mathcal{R}_1 \cup \mathcal{R}_2 \cup \mathcal{R}_3$的凸包。具有因果信道状态信息 $C^{CSI}$ 的多址窃听信道的保密容量满足

$$\mathcal{R}^{CSI} \subseteq C^{CSI}.$$

在区域 $\mathrm{R}_1$，中，辅助随机变量 $U$ 是发送方传输的公共消息，用于帮助解码器找到上一块状态的有损描述 $V$ ，因为双方都能观测到状态序列。辅助随机变量$V$ 还包含编码方案中所用密钥的信息。区域 $\mathrm{R}_1$ 的编码方案见第 IV 节。我们省略区域 $\mathrm{R}_2$ 和 $\mathrm{R}_3$ 的编码方案，因为区域 $\mathrm{R}_2$ 的编码方案是对 [15, 第 III 节 ] 中方案的扩展，方法是将 Slepian-Wolf 编码索引和密钥分别拆分为两个独立部分；而区域 $\mathrm{R}_3$ 的编码方案则可通过跳过 密钥消息码本生成，并在第 IV 节给出的编码方案 1 中设置 消息码本生成中的 $R_{11} = R_{21} = 0$ 得到。

## IV. 区域$\mathcal{R}_1$的编码方案

本节给出区域 $\mathrm{R}_1$ 的编码方案。对于保密性部分，下面的编码方案与 [15] 中方案的主要区别在于：我们不再直接根据状态序列构造密钥，而是根据状态序列的有损描述构造密钥。

采用反向译码的编码方案分为$B + 1$ 个块。在第 $2 \le b \le B + 1$块中，编码器观测上一块 $b - 1$中的信道状态序列 $s_{b-1}$ 后，找到状态序列 $v_{b-1}$的有损描述，并根据 $v_{b-1}$构造一个密钥。在第 1 块和第 $B+1$块中不传输有意义的消息。我们进一步假设，对于某个正数 $\mu$，$I(U_1, U_2; Y) > \mu > 0$，否则，如 [7, (73b)], 所示，两个发送方的速率均为零。从第 1 块到第 $B$ 块的码字长度为 $n$ ，而最后一块的长度为

$$\widetilde{n} = n\frac{R_0}{\mu}, \tag{1}$$

其中，$R_0 > 0$ 是一个正实数，$2^{nR_0}$是后文定义的辅助消息码本的大小。上一块仅用于传输信道状态序列 $s_B$ 的信息，而$\widetilde{n}$ 的设置使解码器能够正确解码该信息。假设 $I(V; Y) - I(V; Z) > \tau_1 > 0$，且满足马尔可夫链关系 $V - S - (Y, Z)$。否则，密钥速率为 0，所得可达区域为 $\mathrm{R}_3$。由于两个发送方都观测到相同的信道状态，因此他们相互协作，并发送一条公共消息来传递他们观测到的信道状态序列的有损描述。基于该信道状态的有损描述，解码器能够解码更多消息，从而获得更大的可达速率区域。

反向译码遵循 [7, 附录 G] 中的原则，并因密钥协商而增加了密钥解密步骤。解码器首先对块$B + 1$ 进行译码，以获取块$B$的信道状态有损描述索引。在随后的译码块中，解码器首先找到当前信道状态序列的有损描述，然后借助该有损描述执行联合典型解码，以解码公共消息和私有消息。

这里，我们对该编码方案中的密钥协商给出直观解释。为简单起见，我们只考虑发送方 1 的加密和解密操作。在每个块 $b, b \in [2 : B]$ 中，发送方观察到信道状态序列 $s_{b-1}$ 及其有损描述 $v_{b-1}$后，通过映射 $\kappa : \mathrm{T} \to \mathrm{K}_1$,生成密钥 $k_{1,b}$ ，其中 T 是 Wyner-Ziv 子码本中 $V$ 的索引集。该密钥用于加密消息 $m_{1,b}$ ，计算方式为$c_{1,b} = m_{1,b} \oplus k_{1,b}$。在反向解码步骤的块$b, b \in [1 : B]$中，解码器已知来自上一块 $b + 1$ 的 Wyner-Ziv 索引 $k_{0,b+1}$ 。现在可以找到 $v_b$，它是当前块中状态序列 $s_b$ 的有损描述。随后，解码器重现用于块 $b + 1$ 的密钥 $k_{1,b+1}$ ，并通过计算 $m_{1,b+1} = c_{1,b+1} \ominus k_{1,b+1}$ 解密消息 $m_{1,b+1}$ 。

~ ~给定 $P_S$ 和信道 $P_{YZ|X_1X_2S}$，令 $R_0, R_1, R_2, R_{10}, R_{11}, R_{20}, R_{21}, R_{K_1}$ 为满足以下约束的正实数

$$\begin{aligned} R_0 &\geq I(V;S) - I(V;Y), \\ \widetilde{R}_1 &\leq I(U_1;Y|V,U,U_2), \widetilde{R}_2 \leq I(U_2;Y|V,U,U_1), \\ \widetilde{R}_1 - R_{10} &> I(U_1;Z|S,U), \widetilde{R}_2 - R_{20} > I(U_2;Z|S,U), \\ \widetilde{R}_1 + \widetilde{R}_2 - R_{10} - R_{20} &> I(U_1,U_2;Z|S,U), \\ R_{K_1} = R_{11} + R_{21} &\leq I(V;Y) - I(V;Z), \\ R_1 = R_{10} + R_{11}, R_2 &= R_{20} + R_{21} \end{aligned}$$

在固定联合分布下

$$P_S P_{V|S} P_U P_{U_1|U} P_{U_2|U} P_{X_1|UU_1S} P_{X_2|UU_2S} P_{YZ|X_1X_2S}.$$

密钥消息码本生成：给定 $\tau > 0$ 和 $\delta > 0$，令 $R_K = I(V;S) + \tau$。在每个块 $2 \leq b \leq B+1$ 中，发送方生成一个码本 $\mathsf{C}_{K_b} = \{\boldsymbol{v}(l)\}_{l=1}^{2^{nR_K}}$，该码本由 $2^{nR_K}$ 个码字组成，每个码字均按照分布 $P_V$ 独立同分布地生成，使得对于任意 $v \in \mathcal{V}$，有 $P_V(v) = \sum_{s\in\mathcal{S}} P_S(s) P_{V|S}(v|s)$。将码本 $\mathsf{C}_{K_b}$ 划分为 $2^{nR_{K_0}}$ 个子码本 $\mathsf{C}_{K_b}(k_{0,b})$，其中 $k_{0,b} \in [1 : 2^{nR_{K_0}}]$，且 $R_{K_0} = I(V;S) - I(V;Y) + 2\tau$。令 $\mathcal{T}$ 为每个子码本 $\mathsf{C}_{K_b}(k_{0,b})$ 中码字的索引集，使得对于任意 $k_{0,b} \in [1 : 2^{nR_{K_0}}]$，有 $|\mathcal{T}| = |\mathsf{C}_{K_b}(k_{0,b})|$。对于每个码本 $\mathsf{C}_{K_b}$，构造密钥映射 $\kappa : \mathcal{T} \to [1 : 2^{nR_{K_1}}]$。将所得密钥记为 $K_{1,b}$。

辅助消息码本生成：对于每个块 $b$，根据分布 $P_U$ 独立同分布地生成辅助消息码本 $\mathsf{C}_b = \{\boldsymbol{u}(m_0)\}_{m_0=1}^{2^{nR_0}}$，其中 $R_0 = I(V;S) - I(V;Y) + 3\tau$。

消息码本生成：块 $b, b \in [1 : B]$：对于每个 $m_0$，生成码本 $\mathsf{C}_{1,b}(m_0) = \{\boldsymbol{u}_1(m_0, l)\}_{l=1}^{2^{nR_1}}$，其中包含 $2^{nR_1}$ 个码字，每个码字均根据分布 $P_{U_1|U}$ 独立同分布地生成。将每个 $\mathsf{C}_{1,b}(m_0)$ 划分为 $2^{nR_{10}}$ 个子码本 $\mathsf{C}_{1,b}(m_0, m_{10})$，其中 $m_{10} \in [1 : 2^{nR_{10}}]$。对于每个子码本 $\mathsf{C}_{1,b}(m_0, m_{10})$，将其划分为双层子码本 $\mathsf{C}_{1,b}(m_0, m_{10}, m_{11}) = \{\boldsymbol{u}_1(m_0, m_{10}, m_{11}, l_1)\}_{l_1=1}^{2^{nR_1'}}$，其中 $m_{11} \in [1 : 2^{nR_{11}}]$，$R_1' := \widetilde{R}_1 - R_{10} - R_{11}$。类似地，生成码本 $\mathsf{C}_{2,b} = \{\boldsymbol{u}_2(m_0, l)\}_{l=1}^{2^{nR_2}}$，其码字根据 $P_{U_2|U}$ 独立同分布地生成，然后将其划分为双层子码本 $\mathsf{C}_{2,b}(m_0, m_{20}, m_{21}) = \{\boldsymbol{u}_2(m_0, m_{20}, m_{21}, l_2)\}_{l_2=1}^{2^{nR_2'}}$，其中 $m_{20} \in [1 : 2^{nR_{20}}]$，$m_{21} \in [1 : 2^{nR_{21}}]$，$R_2' = \widetilde{R}_2 - R_{20} - R_{21}$。

区块 $B+1$：对于 $k = 1, 2$，按上述方式生成码本 $\mathsf{C}_{k,B+1}$，码字长度 $\tilde{n}$ 的定义与式 (1) 相同。

上述码本均以随机且相互独立的方式生成。将每个块 $b$ 中的随机码本集合记为 $\mathbf{C}_b$。

编码：区块 1：给定 $m_{0,1} = m_{10,1} = m_{20,1} = m_{11,1} = \cdots = m_{21,1} = 1$，编码器均匀随机地选取一个索引 $l_j \in [1 : 2^{nR_j'}]$，$j = 1, 2$。码字 $\boldsymbol{x}_j$ 按照 $\prod_{i=1}^{n} P_{X_j|UU_jS}(x_{ji}|u_i, u_{ji}, s_i)$，$j = 1, 2$ 根据 $(\boldsymbol{u}, \boldsymbol{u}_1, \boldsymbol{u}_j, 1, 1, l_j, \boldsymbol{s}) = P^n_{X_j|UU_jS}(\boldsymbol{x}_j|\boldsymbol{u}, \boldsymbol{u}_j, \boldsymbol{s})$，$(\cdot, \cdot, \cdot, \cdot, \cdot)$，$(\cdot, \cdot)$，$\cdot$，生成。这里省略码字的索引。

块 $b$，$b \in [2 : B]$：在观测到上一块中的状态序列 $\boldsymbol{s}_{b-1}$ 后，编码器找到一个序列 $\boldsymbol{v}_{b-1}$ 使得 $(\boldsymbol{s}_{b-1}, \boldsymbol{v}_{b-1}) \in T^n_{P_{SV}}$，$\delta$ 并设置 $m_{0,b} = k_{0,b}$，其中 $k_{0,b}$ 是包含 $\boldsymbol{v}_{b-1}$ 的子码本 $\mathsf{C}_{K_{b-1}}(k_{0,b})$ 的索引。若序列 $\boldsymbol{v}_{b-1}$ 是子码本 $\mathsf{C}_{K_{b-1}}(k_{0,b})$ 中的第 $t_b$ 个序列，我们也将其写作 $\boldsymbol{v}(k_{0,b}, t_b)$。生成密钥 $k_{1,b} = \kappa(t_b)$，然后将其分成两个独立部分 $(k_{11,b}, k_{21,b}) \in [1 : 2^{nR_{11}}] \times [1 : 2^{nR_{21}}]$。为传输消息 $m_{1,b}$，编码器 1 将其分成两个独立部分 $(m_{10,b}, m_{11,b})$，并计算 $c_{11,b} = m_{11,b} \oplus k_{11,b}$（模 $2^{nR_{11}}$）。编码器均匀随机地选择索引 $l_{1,b} \in [1 : 2^{nR_1'}]$，并通过 $P^n_{X_1|UU_1S}(\boldsymbol{x}_1|\boldsymbol{u}(k_{0,b}), \boldsymbol{u}_1(k_{0,b}, m_{10,b}, c_{11,b}, l_{1,b}), \boldsymbol{s})$ 生成码字 $\boldsymbol{x}_1$。类似地，发送方 2 的码字 $\boldsymbol{x}_2$ 由 $P^n_{X_2|UU_2S}(\boldsymbol{x}_2|\boldsymbol{u}(k_{0,b}), \boldsymbol{u}_2(k_{0,b}, m_{20,b}, c_{21,b}, l_{2,b}), \boldsymbol{s})$ 生成。

块 $B+1$：在观察到上一块中的状态序列 $\boldsymbol{s}_B$ 后，编码器找到一个序列 $\boldsymbol{v}(k_{0,B+1}, t_{B+1})$，使得 $(\boldsymbol{s}_B, \boldsymbol{v}(k_{0,B+1}, t_{B+1})) \in T^n_{P_{SV},\delta_0}$。然后，编码器设置 $m_{0,B+1} = m_{10,B+1} = m_{11,B+1} = m_{20,B+1} = m_{21,B+1} = 1$，并根据分布 $P^n_{X_1|UU_1S}(\boldsymbol{x}_1|\boldsymbol{u}(k_{0,B+1}), \boldsymbol{u}_1(k_{0,B+1}, 1, 1, 1), \boldsymbol{s})$ 和 $P^n_{X_2|UU_2S}(\boldsymbol{x}_2|\boldsymbol{u}(k_{0,B+1}), \boldsymbol{u}_2(k_{0,B+1}, 1, 1, 1), \boldsymbol{s})$ 生成码字 $\boldsymbol{x}_1$ 和 $\boldsymbol{x}_2$。

反向译码：块 $B+1$：解码器寻找唯一的 $k_{0,B+1}$ 使得 $(\boldsymbol{u}_1(\hat{k}_{0,B+1}, 1, 1, 1), \boldsymbol{u}_2(\hat{k}_{0,B+1}, 1, 1, 1), \boldsymbol{y}_{B+1}) \in T^n_{P_{U_1U_2Y},\delta_0}$。

块 $b$，$b \in [1 : B]$：解码器已从上一块获知关于 $\hat{k}_{0,b+1}$ 的信息。它尝试寻找一个唯一元组 $\boldsymbol{v}_b = \boldsymbol{v}(\hat{k}_{0,b+1}, \hat{t}_{b+1})$，使得 $(\boldsymbol{v}(\hat{k}_{0,b+1}, \hat{t}_{b+1}), \boldsymbol{y}_b) \in T^n_{P_{VY},\delta_0}$。利用 $(\hat{k}_{11,b+1}, \hat{k}_{21,b+1}) = \kappa(\hat{t}_{b+1})$，解码器现在计算 $\hat{m}_{11,b+1} = \hat{c}_{11,b+1} \ominus \hat{k}_{11,b+1}$（模 $2^{nR_{11}}$）以及 $\hat{m}_{21,b+1} = \hat{c}_{21,b+1} \ominus \hat{k}_{21,b+1}$（模 $2^{nR_{21}}$）。对于块 $b$，$b \in [2 : B]$，借助 $\boldsymbol{v}(\hat{k}_{0,b+1}, \hat{t}_{b+1})$，解码器寻找一个唯一元组 $(\hat{k}_{0,b}, \hat{m}_{10,b}, \hat{m}_{20,b}, \hat{c}_{11,b}, \hat{c}_{21,b}, \hat{l}_{1,b}, \hat{l}_{2,b})$，使得

$$\begin{aligned} &(\boldsymbol{v}_b, \boldsymbol{u}(\hat{k}_{0,b}), \boldsymbol{u}_1(\hat{k}_{0,b}, \hat{m}_{10,b}, \hat{c}_{11,b}, \hat{l}_{1,b}), \\ &\quad \boldsymbol{u}_2(\hat{k}_{0,b}, \hat{m}_{20,b}, \hat{c}_{21,b}, \hat{l}_{2,b}), \boldsymbol{y}_b) \in T^n_{P_{VUU_1U_2Y},\delta}. \end{aligned}$$

区块 1：无需解码，因为区块 1 中传输的消息是虚拟消息。

错误分析与 [7,定理 1] 类似，故此处省略。安全性分析见附录 A。令 $R_{10} = 0$ 并将 $Z$ 替换为 $(Z, U_1)$，即可得到区域 $\mathrm{R}_{12}$；区域 $\mathrm{R}_{13}$ 同理可得。

## V. 示例与应用

本节给出数值示例以及一个可达到容量的情形。以下示例表明，通常情况下，区域 $\mathrm{R}_1$ 和区域 $\mathrm{R}_2$ 互不包含。在某些情况下，区域 $\mathrm{R}_1$ 中的可达点不属于区域 $\mathrm{R}_2$，反之亦然。

**例 1.** 考虑一个多址窃听信道，其中 $\mathcal{X}_1 = \mathcal{X}_2 = \{0,1\}$，$\mathcal{Y} = \mathcal{S} = \{0, 1\}$，其信道模型描述如下：

$$Y = \begin{cases} X_1, & \text{if } S = 0, \\ X_2, & \text{if } S = 1, \end{cases} \qquad Z = X_2,$$

其中 $Pr\{S = 1\} = p$。在此信道模型中，编码方案 *1* 可实现速率对 $(\min\{1 - p, 1 - h(p)\}, 0)$

但当 $p$ 足够大时，编码方案2 无法实现。如果主信道由

$$Y = X_1 \oplus X_2 \oplus S,$$

那么，对于某些满足 $p$ 且$1 - h(p) \geq h(p)$ 的$p$，速率对 $(0, h(p))$ 可由编码方案2实现，但无法由编码方案 1 实现。

证明见附录 C。

具有退化消息集的状态依赖多址信道

这里我们考虑具有退化消息集的状态依赖多址信道，其中发送方 2 仅发送公共消息，而发送方 1 同时发送公共消息和私有消息。私有消息需要对窃听者保密。

$$\mathcal{R}_{D,11}^{CSI-E} = \bigcup_{P_{VUU_1U_2X_1X_2|S}} \begin{cases} R_1 \leq \min\{I(U_1;Y|U,U_2,V) - I(U_1;Z|U_2,U,S) \\ \qquad + R_{SK}, I(U_1;Y|U,U_2,V)\}; \\ R_0 + R_1 \leq \min\{I(V,U,U_1,U_2;Y) - I(V;S) \\ \qquad - I(U_1;Z|U_2,U,S) + R_{SK}, \\ \qquad I(V,U,U_1,U_2;Y) - I(V;S)\}, \end{cases}$$

以及满足 $P_S P_{VUU_1U_2X_1X_2|S} = P_{VS} P_{UU_1U_2} P_{X_1|UU_1S} P_{X_2|UU_2S}$ 的联合分布，其中 $R_{SK} = I(V;Y) - I(V;Z,U,U_2)$，并且

$$\mathcal{R}_{D,12}^{CSI-E} = \bigcup_{P_{VUU_1U_2X_1X_2|S}} \begin{cases} R_1 \leq \min\{R_{SK}, I(U_1;Y|U,U_2,V)\}; \\ R_0 + R_1 \leq I(V,U,U_1,U_2;Y) - I(V;S). \end{cases}$$

此情形下编码方案 2 的区域可简化为

$$\mathcal{R}_{D,21}^{CSI-E} = \bigcup_{P_{UU_1U_2X_1X_2|S}} \begin{cases} R_1 \leq \min\{I(U_1;Y|U,U_2) - I(U_1;Z|U_2,U,S) \\ \qquad - H(S|U,U_1,U_2,Y) + H(S|Z,U,U_2), \\ \qquad I(U_1;Y|U,U_2) - H(S|U,U_1,U_2,Y)\}; \\ R_0 + R_1 \leq \min\{I(U,U_1,U_2;Y) \\ \qquad - I(U_1;Z|U_2,U,S) \\ \qquad - H(S|U,U_1,U_2,Y) + H(S|Z,U,U_2), \\ \qquad I(U,U_1,U_2;Y) - H(S|U,U_1,U_2,Y)\} \end{cases}$$

以及联合分布，使得 $P_S P_{UU_1U_2X_1X_2|S} = P_S P_{UU_1U_2} P_{X_1|UU_1S} P_{X_2|UU_2S}$，并且

$$\mathcal{R}_{D,22}^{CSI-E} = \bigcup_{P_{UU_1U_2X_1X_2|S}} \begin{cases} R_1 \leq \min\{H(S|Z,U,U_2) \\ \qquad - H(S|U,U_1,U_2,Y), \\ \qquad I(U_1;Y|U,U_2) \\ \qquad - H(S|U,U_1,U_2,Y)\}; \\ R_0 + R_1 \leq I(U,U_1,U_2;Y) \\ \qquad - H(S|U,U_1,U_2,Y). \end{cases}$$

窃听码区域 $\mathrm{R}_{D\,3}^{CSI-E} = \mathrm{R}_0 \quad I\ U_1\ Z|U_2\ U\ S \quad I\ U_1\ Z|U_2\ U \quad R_{SK} = {}_1$，可通过在 R 中设置并将（；，，）替换为（；，）得到。令 $\mathrm{R}_D^{CSI-E}$ 为 $\mathrm{R}_D^{CSI-E}{}_{,11} \cup \mathrm{R}_D^{CSI-E}{}_{,12} \cup \mathrm{R}_D^{CSI-E}{}_{,21} \cup \mathrm{R}_D^{CSI-E}{}_{,22} \cup \mathrm{R}_{D\,3}^{CSI-E}{}_{,}$ 的凸闭包。

**定理 2**。对于具有退化消息集合且两个编码器均具有因果状态信息的多址窃听信道，有$\mathcal{R}_D^{CSI-E} \subseteq C_D^{CSI-E}$。

区域 $\mathrm{R}_{D\,11}^{CSI-E}$、和 $\mathrm{R}_{D\,12}^{CSI-E}$、可通过令 $R_{20} = R_{21} = 0$，并令 $\boldsymbol{U}$ 由 $k_{0、b}$ 和公共消息 $m_{0、b}$ 在第 IV 节的每个块中确定而得到。区域 $\mathrm{R}_{D\,21}^{CSI-E}$、和 $\mathrm{R}_{D\,22}^{CSI-E}$、可通过将发送方 2 的私有消息速率设为 0 而得到。由于篇幅所限，省略具体细节。

一个编码器处的因果信道状态信息，另一个处的严格因果信道状态信息：现在考虑因果信道状态信息仅在同时发送两条消息的发送方处可用，而另一方处具有严格因果信道状态信息的情形。通过在 $\mathrm{R}_D^{CSI-E}$ 中令 $U_2 = X_2$，定义区域 $\mathrm{R}^{CSI-SCSI}$。

**命题 1**。对于发送两条消息的发送方具有因果信道状态信息、另一方具有严格因果信道状态信息且消息集降级的状态依赖多址窃听信道，有$\mathcal{R}_D^{CSI-SCSI} \subseteq C_D^{CSI-SCSI}$ 成立。

证明与定理 2 的证明相同，唯一不同的是发送方 2 的输入与信道状态相互独立。若进一步假设窃听信道是主信道的退化版本，且合法接收方已知信道状态信息，则有如下结论：

**定理 3.** 退化多址窃听信道的容量，其中消息集合退化，一方具有因果信道状态信息，另一方具有严格因果信道状态信息，且*和也为已知 sender and decoder is*

$$C_D^{CSI-SCSI} = \bigcup_{P_U P_{X_1|US} P_{X_2|U}} \begin{cases} R_1 \leq \min\{I(X_1;Y|U,X_2,S) - I(X_1;Z|U,X_2,S) \\ \qquad + H(S|Z,U,X_2), I(X_1;Y|U,X_2,S)\}; \\ R_0 + R_1 \leq \min\{I(X_1,X_2;Y|S) - I(X_1;Z|U,X_2,S) \\ \qquad + H(S|Z,U,X_2), I(X_1,X_2;Y|S)\}. \end{cases}$$

对于此模型，编码方案 1 和 2 均为最优。证明见附录 D。

定理 3 中的容量区域是在将信道状态信息揭示给解码器时达到的，此时两种编码方案均为最优。直观而言，这可以如下理解。令 $V = S$，Wyner-Ziv 编码便简化为 Slepian-Wolf 编码。因此，两种编码方案的主要区别在于译码过程。然而，将信道状态信息揭示给解码器后，这一区别便消失了，因此两种编码方案都有可能达到最优。下面的数值示例是一个“状态再现”信道，其容量可以达到。

**例 2.** 考虑一个状态相关多址信道，其字母表为$\mathcal{X}_1 = \mathcal{X}_2 = \mathcal{S} = \mathcal{Z} = \mathcal{N} = \{0,1\}$，且 $\mathcal{Y} = \{0,1\} \times \{0,1\}$。主信道输出包含两个分量，即 $Y = (Y_1, Y_2)$。信道模型描述如下：

$$(Y_1, Y_2) = ((X_1 \odot X_2) \oplus S, X_1 \odot X_2), \quad Z = Y_2 \oplus N,$$

其中 $S \backsim Bernoulli(q)$、$N \backsim Bernoulli(p)$、$q$、$p \in [0, \frac{1}{2}]$,并且发送双方消息的发送方可获得因果信道状态信息。该信道的容量为

$$\bigcup_{\alpha \in [\frac{1}{2},1]} \begin{cases} R_1 \leq \min\{h(\alpha) + h(q) - h(p * \alpha) + h(p), h(\alpha)\}, \\ R_1 + R_2 \leq \min\{1 + h(q) - h(\alpha * p) + h(p), 1\}, \end{cases}$$

其中 $h(\cdot)$ 是二元熵函数，$h(a) = -a\log(a) - (1-a)\log(1-a)$。

证明见附录 E。

## 参考文献


[1] A. D. Wyner，“窃听信道”，贝尔系统技术期刊，第 54 卷，第 8 期，第 1355–1387 页，1975 年。[2] I. Csiszár 和 J. Körner，“含机密消息的广播信道”，*IEEE* 信息论汇刊，第 24 卷，第 3 期，第 339–348 页，1978 年。[3] Y. Liang 和 H. V. Poor，“含机密消息的多址信道”，*IEEE* 信息论汇刊，第 54 卷，第 3 期，第 976–1002 页，2008 年。[4] M. H. Yassaee 和 M. R. Aref，“具有强保密性的多址窃听信道”，载于*2010* 年 *IEEE* 信息论研讨会，第 1–5 页，IEEE，2010 年。[5] M. Wiese 和 H. Boche，“多址信道的强保密性”，载于信息论、组合学与搜索理论，第 71–122 页，Springer，2013 年。[6] C. E. Shannon，“发射机处具有辅助信息的信道”，*IBM* 研究与开发杂志，第 2 卷，第 4 期，第 289–293 页，1958 年。[7]A. Lapidoth 和 Y. Steinberg，“具有因果辅助信息的多址信道：公共状态”，*IEEE* 信息论汇刊，第 59 卷，第 1 期，第 32–50 页，2012 年。[8] A. Lapidoth 和 Y. Steinberg，“具有因果辅助信息的多址信道：双重状态”，*IEEE* 信息论汇刊，第 59 卷，第 3 期，第 1379–1393 页，2012 年。[9] Y. Chen 和 A. H. Vinck，“具有辅助信息的窃听信道”，*IEEE* 信息论汇刊，第 54 卷，第 1 期，第 395–402 页，2008 年。[10] S. Gel’Fand 和 M. Pinsker，“具有随机参数的信道编码”，控制与信息理论问题，第 9 卷，第 1 期，第 19–31 页，1980 年。[11] Z. Goldfeld、P. Cuff 和 H. Permuter，“编码器非因果可用随机状态的窃听信道”，*IEEE* 信息论汇刊，第 66 卷，第 3 期，第 1497–1519 页，2019 年。[12] C. E. Shannon，“保密系统的通信理论”，贝尔系统技术期刊，第 28 卷，第 4 期，第 656–715 页，1949 年。[13]Y.-K. Chia 和 A. El Gamal，“具有因果状态信息的窃听信道”，*IEEE* 信息论汇刊，第 58 卷，第 5 期，第 2838–2849 页，2012 年。[14] H. Fujita，“关于发射机处具有辅助信息的窃听信道的保密容量”，*IEEE Trans-*

信息取证与安全，第 11 卷，第 11 期，第 2441–2452 页，2016 年。[15] M. Sasaki 和 T. S. Han，“具有因果状态信息的窃听信道：强保密”，*IEEE* 信息论汇刊，第 65 卷，第 10 期，第 6750–6765 页，2019 年。[16] M. Sasaki 和 T. S. Han，“具有因果和非因果状态信息的窃听信道：再探讨”，*IEEE Trans-actions on Information Theory*，第 67 卷，第 9 期，第 6122–6139 页，2021 年。[17] I. Csiszár 和 P. Narayan，“辅助者参与的公共随机性与密钥生成”，*IEEE* 信息论汇刊，第 46 卷，第 2 期，第 344–366 页，2000 年。[18]N. Helal、M. Bloch 和 A. Nosratinia，“监听多址信道中的协作可解析性与保密性”，*IEEE* 信息论汇刊，第 66 卷，第 9 期，第 5429–5447 页，2020 年。[19] I. Csiszár 和 J. Körner，信息论：离散无记忆系统的编码定理。剑桥大学出版社，2011 年。[20] D. He 和 W. Guo，“一类窃听网络的强保密容量”，熵，第 18 卷，第 7 期，第 238 页，2016 年。[21] C. T. Li 和 A. El Gamal，“强函数表示引理及其在编码定理中的应用”，*IEEE* 信息论汇刊，第 64 卷，第 11 期，第 6967–6978 页，2018 年。[22] A. El Gamal 和 Y.-H. Kim，网络信息论。剑桥大学出版社，2011 年。[23] A. Wyner 和 J. Ziv，“关于某些二进制序列熵的定理及其应用（一）”，*IEEE* 信息论汇刊，第 19 卷，第 6 期，第 769–772 页，1973 年。

## 附录 A 第 IV 节的安全性分析

安全性证明依赖于以下两个引理。

**引理 1.** 对于每个块中满足 $R_1 - R_{10} > I(U_1; Z|U, S)$, $R_2 - R_{20} > I(U_2; Z|U, S)$, $R_1 + R_2 - R_{10} - R_{20} > I(U_1, U_2; Z|S, U)$ 的码本，可得

$$I(M_{10}, M_{20}; \boldsymbol{Z}, \boldsymbol{S}|\boldsymbol{C}) \le \epsilon.$$

这可利用信道可解析性 [18] 得证，此处省略。第二个引理用于密钥构造。

引理 2. 假设 $V - S - (YZ)$ 构成一个马尔可夫链。令 $\mathcal{C}_{\mathcal{V}} = \{v(i,j)\}_{i\in[1:2^{nR_1}],\, j\in[1:2^{nR_2}]}$ 为一个包含 $2^{n\tilde{R}}$ 个码字的码本，其中 $\tilde{R} = I(V;S) + \tau$, $R_1 = I(V;S) - I(V;Y) + 2\tau$, $R_2 = I(V;Y) - \tau$, $\tau > 0$。存在一个映射 $\kappa: [1:2^{nR_2}] \to \{1, \ldots, k\}$，其中 $k = I(V;Y) - I(V;Z)$，使得

$$\mathrm{S}(\kappa(J)|\boldsymbol{Z}, I) \le \epsilon$$

对于某个可以任意小的 $\epsilon > 0$，其中 $\mathrm{S}(K|Z) = \log|\mathcal{K}| - H(K|Z)$，$\mathcal{K}$是随机变量 $K$ 的取值范围。事实上，通过将码本大小设置如上，我们可以进一步在码本上构造一个划分，使得

$$\mathrm{S}(I|\boldsymbol{Z}) \le \epsilon.$$

将引理 2 应用于我们的模型时，$\boldsymbol{Z}$ 是窃听信道的输出，$I$ 和 $J$ 对上一块的状态序列 $\boldsymbol{S}_{b-1}$ 的有损描述 $\boldsymbol{V}(I, J)$ 进行索引，$\kappa$ 是在密钥消息码本生成中构造的密钥映射。证明见附录 B。为界定信息泄漏，令 $\bar{\mathbf{C}}^{B+1}$ 表示 $B+1$ 个块中使用的所有码本。由此可得

$$\begin{aligned}
&I(M_1^{B+1}, M_2^{B+1}; \boldsymbol{Z}^{B+1}|\bar{\mathbf{C}}^{B+1}) \\
&\le I(M_1^{B+1}, M_2^{B+1}; \boldsymbol{Z}^{B+1}, \boldsymbol{U}^{B+1}|\bar{\mathbf{C}}^{B+1}) \\
&= \sum_b I(M_{1,b}, M_{2,b}; \boldsymbol{Z}^{B+1}, \boldsymbol{U}^{B+1}|M_1^{[b+1]}, M_2^{[b+1]}, \bar{\mathbf{C}}^{B+1}) \\
&\overset{(a)}{\le} \sum_b I(M_{1,b}, M_{2,b}; \boldsymbol{Z}^{B+1}, \boldsymbol{U}^{B+1}|\boldsymbol{S}_b, M_1^{[b+1]}, M_2^{[b+1]}, \bar{\mathbf{C}}^{B+1}) \\
&\overset{(b)}{=} \sum_b I(M_{1,b}, M_{2,b}; \boldsymbol{Z}^{b}, \boldsymbol{U}^{b}|\boldsymbol{S}_b, \bar{\mathbf{C}}^{B+1}),
\end{aligned}$$

其中，$(a)$ 根据 $(M_{1,b}, M_{2,b})$ 与 $\boldsymbol{S}_b$ 相互独立这一性质得到；$(b)$ 根据在给定 $(\boldsymbol{Z}^b, \boldsymbol{U}^b, \boldsymbol{S}_b)$ 的条件下，$(M_{1,b}, M_{2,b})$ 与 $(M_1^{[b+1]}, M_2^{[b+1]}, \boldsymbol{Z}^{[b+1]}, \boldsymbol{U}^{[b+1]})$ 相互独立这一性质得到。为了界定 $I(M_{1,b}, M_{2,b}; \boldsymbol{Z}^b, \boldsymbol{U}^b|\boldsymbol{S}_b, \bar{\mathbf{C}}^{B+1})$，可得

$$\begin{aligned}
&I(M_{1,b}, M_{2,b}; \boldsymbol{Z}^b, \boldsymbol{U}^b|\boldsymbol{S}_b, \bar{\mathbf{C}}^{B+1}) \\
&= I(M_{1,b}, M_{2,b}; \boldsymbol{Z}^{b-1}, \boldsymbol{U}^{b-1}|\boldsymbol{S}_b, \bar{\mathbf{C}}^{B+1}) \\
&\quad + I(M_{1,b}, M_{2,b}; \boldsymbol{Z}_b, \boldsymbol{U}_b|\boldsymbol{Z}^{b-1}, \boldsymbol{U}^{b-1}, \boldsymbol{S}_b, \bar{\mathbf{C}}^{B+1}) \\
&= I(M_{1,b}, M_{2,b}; \boldsymbol{Z}_b, \boldsymbol{U}_b|\boldsymbol{Z}^{b-1}, \boldsymbol{U}^{b-1}, \boldsymbol{S}_b, \bar{\mathbf{C}}^{B+1}) \\
&= \underbrace{I(M_{10,b}, M_{20,b}; \boldsymbol{Z}_b, \boldsymbol{U}_b|\boldsymbol{Z}^{b-1}, \boldsymbol{U}^{b-1}, \boldsymbol{S}_b, \bar{\mathbf{C}}^{B+1})}_{=:I_1} \\
&\quad + \underbrace{I(M_{11,b}, M_{21,b}; \boldsymbol{Z}_b, \boldsymbol{U}_b|\boldsymbol{Z}^{b-1}, \boldsymbol{U}^{b-1}, \boldsymbol{S}_b, M_{10,b}, M_{20,b}, \bar{\mathbf{C}}^{B+1})}_{=:I_2},
\end{aligned}$$

其中 $I_1$ 满足

$$\begin{aligned}
I_1 &\le I(M_{10,b}, M_{20,b}, \boldsymbol{Z}^{b-1}, \boldsymbol{U}^{b-1}; \boldsymbol{Z}_b, \boldsymbol{U}_b|\boldsymbol{S}_b, \bar{\mathbf{C}}^{B+1}) \\
&= I(M_{10,b}, M_{20,b}; \boldsymbol{Z}_b, \boldsymbol{U}_b|\boldsymbol{S}_b, \bar{\mathbf{C}}^{B+1}) \\
&\quad + I(\boldsymbol{Z}^{b-1}, \boldsymbol{U}^{b-1}; \boldsymbol{Z}_b, \boldsymbol{U}_b|\boldsymbol{S}_b, M_{10,b}, M_{20,b}, \bar{\mathbf{C}}^{B+1}) \\
&\le I(M_{10,b}, M_{20,b}; \boldsymbol{Z}_b, \boldsymbol{U}_b|\boldsymbol{S}_b, \bar{\mathbf{C}}^{B+1}) \\
&\quad + I(\boldsymbol{Z}^{b-1}, \boldsymbol{U}^{b-1}; \boldsymbol{Z}_b, \boldsymbol{U}_b, \boldsymbol{S}_b, M_{10,b}, M_{20,b}, K_{1,b}|\bar{\mathbf{C}}^{B+1}) \\
&\overset{(a)}{=} \underbrace{I(M_{10,b}, M_{20,b}; \boldsymbol{Z}_b, \boldsymbol{U}_b|\boldsymbol{S}_b, \bar{\mathbf{C}}^{B+1})}_{=:I_{11}} \\
&\quad + \underbrace{I(\boldsymbol{Z}^{b-1}, \boldsymbol{U}^{b-1}; K_{1,b}, K_{0,b}|\bar{\mathbf{C}}^{B+1})}_{=:I_{12}}.
\end{aligned}$$

其中，$(a)$ 由马尔可夫链 $(\boldsymbol{Z}^{b-1}, \boldsymbol{U}^{b-1}) - (K_{0,b}, K_{1,b}, \bar{\mathbf{C}}^{B+1}) - (\boldsymbol{Z}_b, \boldsymbol{S}_b, M_{10,b}, M_{20,b})$ 得出。根据引理 1，我们有 $I_{11} \le \epsilon$。根据引理 2，我们有

$$\begin{aligned}
I(K_{1,b}; K_{0,b}|\bar{\mathbf{C}}^{B+1}) &\le I(K_{1,b}; \boldsymbol{Z}_{b-1}, \boldsymbol{U}_{b-1}, K_{0,b}|\bar{\mathbf{C}}^{B+1}) \\
&\le \mathrm{S}(K_{1,b}|\boldsymbol{Z}_{b-1}, \boldsymbol{U}_{b-1}, K_{0,b}) \le \epsilon, \\
I(K_{0,b}; \boldsymbol{Z}_{b-1}, \boldsymbol{U}_{b-1}|\bar{\mathbf{C}}^{B+1}) &\le \mathrm{S}(K_{0,b}|\boldsymbol{Z}_{b-1}, \boldsymbol{U}_{b-1}) \le \epsilon.
\end{aligned}$$

按照与 [15] 相同的递推论证可得

$$I(K_{0,b}, K_{1,b}; \boldsymbol{Z}^{b-1}, \boldsymbol{U}^{b-1}|\bar{\mathbf{C}}^{B+1}) \le 2(B+1)\epsilon$$

以及 $I_1 \le (2B+3)\epsilon$。为了界定 $I_2$，可得

$$\begin{aligned}
I_2 &= I(M_{11,b}, M_{21,b}; \boldsymbol{Z}_b, \boldsymbol{U}_b|\boldsymbol{Z}^{b-1}, \boldsymbol{U}^{b-1}, \boldsymbol{S}_b, M_{10,b}, M_{20,b}, \bar{\mathbf{C}}^{B+1}) \\
&\le I(M_{11,b}, M_{21,b}, \boldsymbol{Z}^{b-1}, \boldsymbol{U}^{b-1}; \boldsymbol{Z}_b, \boldsymbol{U}_b|\boldsymbol{S}_b, M_{10,b}, M_{20,b}, \bar{\mathbf{C}}^{B+1}) \\
&= I(M_{11,b}, M_{21,b}; \boldsymbol{Z}_b, \boldsymbol{U}_b|\boldsymbol{S}_b, M_{10,b}, M_{20,b}, \bar{\mathbf{C}}^{B+1}) \\
&\quad + I(\boldsymbol{Z}^{b-1}, \boldsymbol{U}^{b-1}; \boldsymbol{Z}_b, \boldsymbol{U}_b|\boldsymbol{S}_b, M_{10,b}, M_{20,b}, \bar{\mathbf{C}}^{B+1}, M_{11,b}, M_{21,b}) \\
&\le I(M_{11,b}, M_{21,b}; \boldsymbol{Z}_b, \boldsymbol{U}_b, C_{11,b}, C_{21,b}|\boldsymbol{S}_b, M_{10,b}, M_{20,b}, \bar{\mathbf{C}}^{B+1}) \\
&\quad + I(\boldsymbol{Z}^{b-1}, \boldsymbol{U}^{b-1}; \boldsymbol{Z}_b, \boldsymbol{U}_b|\boldsymbol{S}_b, M_{10,b}, M_{20,b}, \bar{\mathbf{C}}^{B+1}, M_{11,b}, M_{21,b}) \\
&= \underbrace{I(M_{11,b}, M_{21,b}; C_{11,b}, C_{21,b}|\boldsymbol{S}_b, M_{10,b}, M_{20,b}, \bar{\mathbf{C}}^{B+1})}_{=:I_{21}} \\
&\quad + \underbrace{I(M_{11,b}, M_{21,b}; \boldsymbol{Z}_b, \boldsymbol{U}_b|\boldsymbol{S}_b, M_{10,b}, M_{20,b}, \bar{\mathbf{C}}^{B+1}, C_{11,b}, C_{21,b})}_{=:I_{22}} \\
&\quad + \underbrace{I(\boldsymbol{Z}^{b-1}, \boldsymbol{U}^{b-1}; \boldsymbol{Z}_b, \boldsymbol{U}_b|\boldsymbol{S}_b, M_{10,b}, M_{20,b}, \bar{\mathbf{C}}^{B+1}, M_{11,b}, M_{21,b})}_{=:I_{23}}.
\end{aligned}$$

于是，可得

$$
\begin{aligned}
&I_{21}\\
&= I(M_{11,b}, M_{21,b}; C_{11,b}, C_{21,b}|\boldsymbol{S}_b, M_{10,b}, M_{20,b}, \bar{\mathbf{C}}^{B+1})\\
&= I(M_{11,b}, M_{21,b}; C_{11,b}, C_{21,b}|\bar{\mathbf{C}}^{B+1})\\
&= H(C_{11,b}, C_{21,b}|\bar{\mathbf{C}}^{B+1}) - H(C_{11,b}, C_{21,b}|\bar{\mathbf{C}}^{B+1}, M_{11,b}, M_{21,b})\\
&\overset{(a)}{\leq} H(C_{11,b}, C_{21,b}) - H(K_{11,b}, K_{21,b}|\bar{\mathbf{C}}^{B+1})\\
&\overset{(b)}{\leq} H(C_{11,b}, C_{21,b}) - H(K_{11,b}, K_{21,b}|K_{0,b})\\
&\overset{(c)}{=} D(P_{K_1|K_0}||P_C) \leq \mathrm{S}(K_{1,b}|\boldsymbol{Z}, K_{0,b}) \leq \epsilon,
\end{aligned}
$$

其中，$(a)$由以下事实可得：$C_{i1,b} = M_{i1,b} \oplus K_{i1,b}$,and$M_{i1,b}$与$K_{i1,b}, i = 1$相互独立；2，$(b)$由马尔可夫链$K_{1,b} - K_{0,b} - \bar{\mathbf{C}}^{B+1}$以及$K_{1,b} = (K_{11,b}, K_{21,b})$可得；$(c)$由以下事实可得：$(C_{11,b}, C_{21,b})$在 $[1:\ 2^{nR_{11}}] \times [1:\ 2^{nR_{21}}]$上均匀分布，且 $P_C$ 在 $[1:\ 2^{nR_{11}}] \times [1:\ 2^{nR_{21}}]$上均匀分布。 $I_{22}$ 和 $I_{23}$ 的界与单用户情形 [15]类似，这里略去证明。证明完毕。

## 附录 B 引理 2 的证明

本节证明引理 2。证明分为两个步骤。步骤 1 中，我们证明存在一个定义在 $\mathrm{C}_{\mathcal{V}} = \{\mathrm{C}_{\mathcal{V}}(k_0)\}_{k_0=1}^{k}$ 上的等分划，满足 Wyner-Ziv 定理的要求，使得 $I(K_0;\ \boldsymbol{Z}) \leq \epsilon$。步骤 2 中，我们基于步骤 1 构造的划分，进一步构造一个密钥映射，使得所构造的密钥 $K_1$ 满足

$$\mathrm{S}(K_1|\boldsymbol{Z}, K_0) \leq \epsilon.$$

步骤 *1*：划分和密钥的构造基于 Csiszár 和 Körner [19]提出的以下提取器引理。

**引理 3**（[19]中的引理 17.3）。设 $P$ 是有限集合 $\mathcal{V}$ 上的一个分布，且$\mathcal{F}$ 是$\mathcal{V}$ 的一个子集，满足$\mathcal{F} = \{v \in \mathcal{V}:\ P(v) \leq 1/d\}$。对于某个正数 $\epsilon$，若 $P(\mathcal{F}) \geq 1 - \epsilon$，则存在一个随机选取的映射 $G:\ \mathcal{V} \to \{1, \ldots, k\}$ 满足

$$\sum_{m=1}^{k} \left| P(G^{-1}(m)) - \frac{1}{k} \right| \leq 3\epsilon \tag{2}$$

其概率至少为 $1 - 2ke^{-\epsilon^2(1-\epsilon)d/2k(1+\epsilon}$.

此外，如果某个族$\mathcal{P}$ 中的每个 $P$ 都满足该假设，则公式(2)对所有 $P \in \mathcal{P}$均成立的概率至少为 $1 - 2k|\mathcal{P}|e^{-\epsilon^2(1-\epsilon)d/2k(1+\epsilon)}$。

因此，当 $k$对数 $k < \epsilon^2(1-\epsilon)d$对数$2\ 1+\epsilon$ $e$ ~~$-()$对数$\cdot 2|\mathcal{P}|-$~~ 时，所需的映射存在。此 $G$ 的实现记为 $g$。

这一步的证明采用了 [19] 中引理 17.5 和定理 17.21 证明里的技巧，其核心思想是构造集合 F 和分布族 P，使其满足引理 3 中的条件。我们将参数设置如下。

$$
\begin{aligned}
d = I(V;S) - I(V;Y), k = I(V;S) - I(V;Y) - \tau\\
\mathcal{P} = P_{V^n} \bigcup \{P_{V|z}^n : z \notin \mathcal{E}\},
\end{aligned}
\tag{3}
$$

其中，E 是 $\mathrm{Z}^n$ 的一个子集，其概率呈指数级小，稍后将对其进行定义； $P_{V^n}$ 是码本 $\mathrm{C}_{\mathcal{V}}$上的均匀分布。令 $\sigma$， $\delta$，$\zeta$为正实数，使得 $\zeta < \delta < \sigma$。定义集合

$$\mathcal{T}_1 = \{\boldsymbol{s} : T_{P_{SV},\delta}^n[\boldsymbol{s}] \neq \emptyset\}$$

并令 $f$ 为定义在 $\mathrm{T}_1$ 上的函数，使得 $(f(\boldsymbol{S}), \boldsymbol{S}) \in T_{P_{SV},\delta}, f(\boldsymbol{S}) \in \mathrm{C}_{\mathcal{V}}$。进一步将 $f$ 扩展为定义在 $\mathrm{S}^n$ 上的函数，令 $f(\boldsymbol{s})$ 为 $\mathrm{V}^n$ 中某个固定序列，其中 $\boldsymbol{s} \notin \mathrm{T}_1$。根据 [19,推论 17.9A], , 通过设定 $|\mathrm{C}_{\mathcal{V}}| = 2^{n(I(V;S)+\tau)}$ 的大小，始终可以得到这样的函数 $f$。定义集合

$$\mathcal{T}_2 = \{(\boldsymbol{s}, \boldsymbol{z}) : \boldsymbol{s} \in \mathcal{T}_1, (f(\boldsymbol{s}), \boldsymbol{s}, \boldsymbol{z}) \in T_{P_{VSZ},\sigma}^n\}$$

并令 $\chi$ 为集合 $\mathrm{T}_2$ 的示性函数。那么，$(\boldsymbol{v}, \boldsymbol{s}, \mu)$ 的联合分布为

$$
\begin{aligned}
P(\boldsymbol{v}, \boldsymbol{z}, \mu) &= Pr\{f(\boldsymbol{S}) = \boldsymbol{v}, \boldsymbol{Z} = \boldsymbol{z}, \chi(\boldsymbol{S}, \boldsymbol{Z}) = \mu\}\\
&= \sum_{\boldsymbol{s}: f(\boldsymbol{s}) = \boldsymbol{v}, \chi(\boldsymbol{s}, \boldsymbol{z}) = \mu} P_{SZ}^n(\boldsymbol{s}, \boldsymbol{z})
\end{aligned}
\tag{4}
$$

定义集合 $\mathrm{B}$ $= \boldsymbol{v}\ z\ 1\quad \boldsymbol{v} \in \mathcal{V}\ z \in T_{P_Z\ \zeta}^n\ T_{P_{VSZ}\ \sigma}^n[\boldsymbol{v}, \boldsymbol{z}] \neq \emptyset$ $P \geq P_{SZ\ \ 2}^n - P_{Z\ \ P_{Z\ \zeta}}^n\ {}^{c} \geq 1 - \eta^2$ {(,,) : C,,,,}。由此可知，(B) (T) ((.) )，其中某个数 $\eta$ 指数级小，并且

$$
\begin{aligned}
|\mathcal{B}| &\overset{(a)}{\leq} \sum_{\boldsymbol{z} \in T_{P_Z,\zeta}^n} \left| \{\boldsymbol{v} : \boldsymbol{v} \in T_{P_{VZ},\sigma|S|}^n[\boldsymbol{z}]\} \right|\\
&\leq 2^{n(H(Z)+\epsilon)} 2^{n(I(V;S)+\tau-I(V;Z)+\epsilon)},
\end{aligned}
$$

其中，$(a)$由 [19, 引理 2.10]得出。对于任意的$(\boldsymbol{v},\ \boldsymbol{z},\ 1) \in \mathrm{B}$，由式 (4) 和 $\mathrm{T}_2$ 的定义可得

$$
\begin{aligned}
P(\boldsymbol{v}, \boldsymbol{z}, 1) &\leq \sum_{\boldsymbol{s} \in T_{P_{VSZ},\sigma}^n[\boldsymbol{v}, \boldsymbol{z}]} P_{SZ}^n(\boldsymbol{s}, \boldsymbol{z})\\
&\leq 2^{n(H(S|VZ)+\epsilon)} 2^{-n(H(SZ)-\epsilon)} < \frac{1}{\alpha|\mathcal{B}|},
\end{aligned}
$$

其中 $\alpha = 2^{-n(5\epsilon+\tau)}$。定义 $\mathrm{B}_{\mathrm{z},\ 1} := \{\boldsymbol{v} : (\boldsymbol{v},\ \boldsymbol{z},\ 1) \in \mathrm{B}\}$。由 [19, 17 15 ] $z \in T_{P_Z\ \zeta}^n$ $T_{P_{VZ}\ \delta}^n[\boldsymbol{z}] \neq \emptyset$ $\boldsymbol{v} \in (.),\ ,$ 可 $T_{P_{VZ}\ \delta}^n[\boldsymbol{z}]$ $T_{P_{VSZ}\ \sigma}^n[\boldsymbol{v}, \boldsymbol{z}] \neq \emptyset$ 推出，，且，是，的充分条件。因此，$\mathrm{B}_{\mathrm{z},\ 1}$ 的大小可下界估计为

$$|\mathcal{B}_{\boldsymbol{z},1}| \geq \left| \{\boldsymbol{v} : \boldsymbol{v} \in T_{P_{VZ},\delta}^n[\boldsymbol{z}], \boldsymbol{v} \in C_{\mathcal{V}}\} \right| \geq 2^{n(I(V;S)-I(V;Z)+\tau-\epsilon)}.$$

现在定义 $\mathrm{D} := \{\boldsymbol{z}:\ P_Z^n(\boldsymbol{z}) \geq {}^{\alpha^2|}{}_{\mathcal{B}\ z\ 1|.\ \mathcal{B}}\}$，并令 $\mathrm{B}' := \mathrm{B} \cap \{\mathrm{C}_{\mathcal{V}} \times \mathrm{D}\}$。根据我们的假设，对于任意$(\boldsymbol{v},\ \boldsymbol{z},\ 1) \in \mathrm{B}'$，且 1 为示性函数 $\chi$的取值，

$$I(V;\ Y) - I(V;\ Z) > \tau_1 > 2\tau + 16\epsilon > 0,$$

$$P_{\boldsymbol{V}|\boldsymbol{Z},1}(\boldsymbol{v}|\boldsymbol{z}, 1) = \frac{P(\boldsymbol{v}, \boldsymbol{z}, 1)}{P_{\boldsymbol{Z},1}(\boldsymbol{z}, 1)} \leq \frac{1}{\alpha^3 \min|\mathcal{B}_{\boldsymbol{z},1}|} < \frac{1}{d}$$

and

$$P_{\boldsymbol{V}\boldsymbol{Z},1}(\mathcal{B}') \geq P_{\boldsymbol{V}\boldsymbol{Z},1}(\mathcal{B}) - P_{\boldsymbol{Z},1}(\mathcal{D}^c) \geq P_{\boldsymbol{V}\boldsymbol{Z},1}(\mathcal{B}) - \alpha^2 \geq 1 - \eta_1^2$$

对于指数级小的数量 $\eta_1$。现在对每个 $z$，记 $\mathrm{B}_{\mathrm{z},\ 1}'$ 为集合 $\{\boldsymbol{v} : (\boldsymbol{v},\ \boldsymbol{z},\ 1) \in \mathrm{B}'\}$，并令 $\mathrm{E} \triangleq \{(z,\ 1) : P_{\boldsymbol{V}|\boldsymbol{Z},\ 1}(\mathrm{B}_{\mathrm{z},\ 1}'|\boldsymbol{z},\ 1) \leq 1 - \eta_1\}$，则有 $P_{\mathrm{Z},\ 1}(\mathrm{E}) < \eta_1$。对于每个 $z \notin \mathrm{E}$，分布 $P_{\boldsymbol{V}|\boldsymbol{Z},\ 1}(\cdot|\boldsymbol{z},\ 1)$ 满足以下条件

引理 3，其中设定 $\mathrm{F} = \mathrm{B}_{z,1}'$（F 在引理 3 中定义），因此存在一个映射，使得对所有$P_{V|z,1}(\cdot|z, 1), (z, 1) \notin \mathrm{E}$，式 (2) 均成立。

对于均匀分布，我们定义集合 $\mathrm{F} = \mathrm{C}_{\mathcal{V}}$。由于对于任意 $v \in \mathrm{C}_{\mathcal{V}}$，$P_{\overline{V}}(v) = \frac{1}{|\mathcal{V}|} < \frac{1}{d}$ 且 $P_{\boldsymbol{V}}(\mathrm{C}_{\mathcal{V}}) = 1$，引理 3 中的条件也得到满足。所构造的映射满足

$$\sum_{m=1}^{k}\left|P_{\boldsymbol{V}}(g^{-1}(m)) - \frac{1}{k}\right| \le 3\varepsilon, \tag{5}$$

$$\sum_{m=1}^{k}\left|P_{\boldsymbol{V}|\boldsymbol{Z},1}(g^{-1}(m)|z, 1) - \frac{1}{k}\right| \le 3\varepsilon \text{ for } (z, 1) \notin \mathcal{E} \tag{6}$$

其中 $\varepsilon$ 是一个指数级小的数。根据式 (6) 和安全索引 S 的定义，可得

$$I(g(\boldsymbol{V}); \boldsymbol{Z}) \le \mathrm{S}(g(\boldsymbol{V})|\boldsymbol{Z}) \le \varepsilon' \tag{7}$$

其中 $\varepsilon'$ 是一个指数级小的数。码本的划分由映射 $g$ 得到。若码字 $v$ 满足 $g(v) = k$，则属于箱 $k$。注意，根据式 (5)，该划分不一定是等划分。现在，令 $g(\boldsymbol{V})$ 为定义在 $\mathrm{C}_{\mathcal{V}}$ 上的随机变量，其分布由映射 $g$ 定义，且近似均匀。

**引理 4**。 *[20,引理 4]对于任意给定的码本 $C$，若函数 $g: C \to [1: k]$ 满足式 (5)，则在 $C$ 上存在一个划分 $\{C_m\}_{m=1}^{k}$，使得*

*1) $|C_m| = \frac{|C|}{k}$ for all $m \in [1 : k]$,*
*2) $H(K_0|g(\boldsymbol{V})) < 4\sqrt{\epsilon}\log k$,*

其中 $K_0 = g^{equal}(\boldsymbol{V})$ 是包含 $\boldsymbol{V}$的箱的索引，而 $g^{equal}$ 是诱导等分划的新映射。

现在，根据 (7) 和上述引理，我们有

$$\begin{aligned} I(K_0; \boldsymbol{Z}) &\le I(K_0, g(\boldsymbol{V}); \boldsymbol{Z}) \\ &= I(g(\boldsymbol{V}); \boldsymbol{Z}) + I(K_0; \boldsymbol{Z}|g(\boldsymbol{V})) \\ &= I(g(\boldsymbol{V}); \boldsymbol{Z}) + H(K_0|g(\boldsymbol{V})) \\ &\le 3\varepsilon + 4\sqrt{\varepsilon}\log k. \end{aligned}$$

注意，$\varepsilon$ 是一个指数级小的数，因此信息泄漏也呈指数级小。

步骤 2：步骤 2 的证明与步骤 1 的证明几乎相同，实际上就是 [19]中定理 17.21 的直接部分证明。在这里，我们将步骤 1 中的函数 $f$ 替换为一对函数 $\phi_1 \times \phi_2 : \mathrm{S} \to \mathrm{K}_0 \times \mathrm{K}_1$ on $\mathrm{T}_1$，使得 $(\boldsymbol{V}(\phi_1(\boldsymbol{S}), \phi_2(\boldsymbol{S})), \boldsymbol{S}) \in T^n_{P_{VS},\delta}$，其中 $\phi_1(\boldsymbol{S}) = g^{equal}(f(\boldsymbol{S}))$，而 $g^{equal}$是我们在步骤 1 中构造的最终映射。$\phi_2$ 的结果是 $\boldsymbol{V}$ 在子箱 $\mathrm{C}_{\mathcal{V}}(\phi_1(\boldsymbol{S}))$中的索引。将集合 B 改写为 $\mathrm{B} = \{(k_0, k_1, z, 1): k_0 \in \mathrm{K}0, k_1 \in \mathrm{K}1, z \in T^n_{P_Z,\zeta}, T^n_{P_{VSZ},\sigma}[v(k_0, k_1), z] \neq \emptyset\}$，并将集合 $\mathrm{B}_{z,1}$ 设为 $\mathrm{B}_{k_0,z,1} = \{k_1: (k_0, k_1, z, 1) \in \mathrm{B}\}$，其余证明与步骤 1 相同，详见 [19，定理 17.21] 的证明。最终构造的映射 $\kappa$ 满足

$$\mathrm{S}(\kappa(\phi_2(\boldsymbol{S}))|\boldsymbol{Z}, \phi_1(\boldsymbol{S})) \le \epsilon$$

证明至此完成。

## 附录 C
## 例 1 的证明

设定 $p = Pr\{S = 1\}$。我们首先考虑区域 $\mathrm{R}_1$。变量设置如下，

$$V = S, U_2 = \emptyset, X_1 = U_1, X_2 = U$$

其中 $(U, U_1)$ 相互独立，且 $S$和 $U \backsim Bernoulli(1/2)$ 以及 $U_1 \backsim Bernoulli(1/2)$。由此可得 $I(U_1; Z|S, U) = I(U_1; Z|S, U, U_2) = I(U_1, U_2; Z|S, U) = 0$。此外，我们还有

$$\begin{aligned} &I(U_1; Y|V, U, U_2) = I(U_1; Y|S, U) = H(Y|S, U) \\ &= Pr\{S = 1\}H(Y|U, S = 1) = 1 - p, \\ &I(V, U, U_1, U_2; Y) - I(V; S) = H(Y) - H(S) = 1 - h(p), \end{aligned}$$

其中 $h(p) = -p\log p - (1-p)\log(1-p)$。注意，互信息项 $I(V; Y) = I(S; Y) \ge 0$。因此，满足 $R_1 = \min\{1-p, 1-h(p)\}$ 的速率对 $(R_1, 0)$ 是可达的。现在考虑区域 $\mathrm{R}_2$。对 $R_2 = 0$ 施加限制，并将所有密钥速率分配给发送方 1，可得

$$\begin{aligned} &I(U_1; Z|U_2, S) = I(U_1; X_2|U_2, S) = 0, \\ &H(S|Z) = H(S|Z, U_1) = H(S), \end{aligned}$$

发送方 1 能够达到的最大速率不会超过 $I(U_1; Y|U_2)$。因此，只需证明 $I(U_1; Y|U_2) < \min\{1-p, 1-h(p)\}$，其中 $I(U_1; Y|U_2)$ 实际上是采用香农策略、具有因果信道状态信息的多址信道可达速率区域中的约束。为此，注意到 $I(U_1; Y|U_2)$ 是条件分布 $P_{Y|U_1U_2}$ 的凸函数，其中 $P_{Y|U_1U_2}(y|u_1, u_2) = \sum_{x_1, x_2, s} P_{Y|X_1X_2S}(y|x_1, x_2, s)P_{X_1|U_1S}(x_1|u_1, s)$

$P_{X_2|U_2S}(x_2|u_2, s)P_S(s)$ 是 $P_{X_1|U_1S}$ 和 $P_{X_2|U_2S}$ 的线性函数。因此，它也是 $P_{X_1|U_1S}$ 和 $P_{X_2|U_2S}$ 的凸函数，其最大值在极点处取得。因此，将分布 $P_{X_1|U_1S}$ 和 $P_{X_2|U_2S}$ 分别替换为确定性函数 $x_1(u_1, s)$ 和 $x_2(u_2, s)$，不失一般性。例 4 在 [7] 中表明，当 $p$ 足够大时，$I(U_1; Y|U_2) < \min\{1-p, 1-h(p)\}$ 成立。

对于第二种信道模型，考虑 $R_1 = 0$ 的情况。对于编码方案 1，可得。

$$I(U_2; Z|U, S) = I(U_2; X_2|U, S) \overset{(a)}{=} I(U_2; X_2|U, S, U_1)$$

其中，$(a)$ 根据 $(U_2, X_2)$ 与$U_1$ 在给定 $U$的条件下相互独立这一事实得出。我们进一步有

$$\begin{aligned} I(U_2; Y|V, U, U_1) &= H(U_2|V, U, U_1) - H(U_2|V, U, U_1, Y) \\ &\overset{(a)}{\le} H(U_2|S, U, U_1) - H(U_2|V, U, U_1, Y, S) \\ &\overset{(b)}{=} H(U_2|S, U, U_1) - H(U_2|U, U_1, Y, S) \\ &\overset{(c)}{=} I(U_2; Y|S, U, U_1) \\ &= I(U_2; X_1 + X_2|S, U, U_1), \end{aligned}$$

其中，$(a)$ 是由以下事实得出的：给定 $U$ 时，$U_2$ 与 $S$ 相互独立，且条件会降低熵；$(b)$ 是由以下事实得出的：给定 $S$ 时，$V$ 与其他任何变量都相互独立；$(c)$ 是由

将信道模型代入互信息即可得到。应用互信息的链式法则可得

$$\begin{aligned}
&I(U_2; X_1 + X_2, X_2|S, U, U_1)\\
&= I(U_2; X_2|S, U, U_1) + I(U_2; X_1 + X_2|S, U, U_1, X_2)\\
&= I(U_2; X_2|S, U, U_1) + I(U_2; X_1|S, U, U_1, X_2)\\
&\overset{(a)}{=} I(U_2; X_2|S, U, U_1)\\
&= I(U_2; X_1 + X_2|S, U, U_1) + I(U_2; X_2|S, U, U_1, X_1 + X_2)
\end{aligned}$$

其中，$(a)$成立是因为在给定$(S,\ U,\ U_1,\ X_2)$的条件下，$U_2$ 与 $X_1$ 相互独立。由互信息的非负性可得 $I(U_2;\ Z|U,\ S)$ $= I(U_2;\ X_2|S,\ U,\ U_1) \geq I(U_2;\ X_1 + X_2|S,\ U,\ U_1) = I(U_2;Y|S,\ U,\ U_1)$。因此，区域 $\mathrm{R}_1$缩减为$\mathrm{R}_{13}$。现在将全部密钥速率分配给发送方 2。发送方 2 的可达速率满足

$$\begin{aligned}
R_2 &\leq I(V;Y) - I(V;Z,U,U_2)\\
&= I(V;Y) - I(V;X_2,U,U_2)\\
&\overset{(a)}{\leq} I(V;Y) \overset{(b)}{\leq} I(S;Y) = H(S) - H(S|Y) \overset{(c)}{\leq} h(p),
\end{aligned}$$

其中，$(a)$由互信息的非负性得出，$(b)$由数据处理不等式得出。当 $V = S$ 和 $S$ 可由 $Y$确定时，$(c)$中的等式成立，这意味着$X_1 + X_2$ 取某些固定值。现在考虑 $V = S$ 和 $X_1 + X_2$ 均为固定值的情况。不失一般性，假设 $X_1 + X_2 = 0$。编码方案 1 中对发送方 2 的第二个约束为

$$I(U_2;Y|S,U,U_1) = H(Y|S,U,U_1) - H(Y|S,U,U_1,U_2) \overset{(a)}{=} 0,$$

其中，$(a)$成立是因为当 $X_1 + X_2 = 0$固定时，$Y$由 $S$确定。因此，在这种情况下，发送方 2 的速率为 $R_2 = 0$ 。我们得出结论，对于该模型，使用编码方案 1 可以达到 $R_2 < h(p)$。

对于编码方案2，令 $X_1 = U_1, X_2 = U_2, U_1 \backsim Bernoulli(1/2)$和 $U_2 \backsim Bernoulli(1/2)$，发送方-2 的第一个约束为

$$\begin{aligned}
I(U_2;Y|U_1) &= I(X_2;Y|X_1) = H(Y|X_1) - H(Y|X_1,X_2)\\
&= 1 - h(p).
\end{aligned}$$

在这种情况下，发送方 2 的密钥速率为

$$H(S|Z,U_2) - H(S|Y,U_1,U_2) = H(S) - H(S|Y,X_1,X_2) = h(p).$$

当信道状态的分布满足 $1 - h(p) \geq h(1/2)$时，$(0,\ h(p))$可以通过编码方案2实现，但无法通过编码方案 1 实现。

## 附录 D 定理 3 的证明

为说明这一点，我们首先证明编码方案 1 的可达性。在区域 $\mathrm{R}_D^{CSI-SCSI}$中设置 $V = S$和 $Y = (Y,\ S)$后，编码方案 1 对 $R_1$ 的约束为

$$\begin{aligned}
R_1 &\leq I(U_1;Y,S|U,X_2,S) - I(U_1;Z|U,X_2,S) + H(S|Z,U,X_2)\\
&= I(U_1;Y|U,X_2,S) - I(U_1;Z|U,X_2,S) + H(S|Z,U,X_2)
\end{aligned}$$

以及 $R_1 \leq I(U_1;\ Y|U,\ X_2,\ S)$。现在，根据强函数表示引理，对于具有条件分布 $P_{X_1S|U}$的任意随机变量 $(X_1,\ S,\ U)$，可以构造一个随机变量 $U_1$ ，使得 $X_1$ 可以由确定性函数 $x_1(u,\ u_1,\ s)$表示，并且在给定 $U$的条件下，$U_1$ 与 $S$相互独立。结合 $S$ 与 $U$相互独立这一事实，我们有

$$I(U_1;Y|U,X_2,S) \overset{(a)}{=} I(U_1,X_1;Y|U,X_2,S) \overset{(b)}{=} I(X_1;Y|U,X_2,S),$$

其中，$(a)$由确定性函数 $x_1(u,u_1,s)$得出，而$(b)$由马尔可夫链$(U,U_1)$ $-(X_1,X_2,S)$ $-(Y,Z)$得出。项 $I(U_1;\ Z|U,X_2,S)$同理可得。和速率满足

$$\begin{aligned}
R_1 + R_2 &\leq I(S,U,U_1,X_2;Y,S) - I(S;S) - I(U_1;Z|U,X_2,S)\\
&\quad + H(S|Z,U,X_2)\\
&= I(U,U_1,X_2;Y|S) - I(U_1;Z|U,X_2,S) + H(S|Z,U,X_2).
\end{aligned}$$

再次应用强函数表示引理，即完成证明。对于编码方案2，我们有

$$\begin{aligned}
R_1 \leq& I(U_1;Y|U,X_2) - I(U_1;Z|X_2,U,S) - H(S|U,U_1,X_2,Y)\\
&\quad + H(S|Z,U,X_2)\\
&\overset{(a)}{=} I(U_1;Y,S|U,X_2) - I(U_1;S|U,X_2,Y)\\
&\quad - I(U_1;Z,S|X_2,U)\\
&\quad - H(S|U,U_1,X_2,Y) + H(S|Z,U,X_2)\\
&= I(U_1;Y|U,X_2,S) - I(U_1;Z|U,X_2,S) - H(S|U,X_2,Y)\\
&\quad + H(S|U,X_2,Z),\\
&= I(U_1,S;Y|U,X_2) - I(U_1,S;Z|U,X_2) \qquad (8)
\end{aligned}$$

其中，$(a)$ 由严格因果假设以及 $S$ 与 $(U,U_1,X_2)$ 相互独立这一事实得出。将 $Y$替换为 $(Y,S)$ 并应用函数表示引理（FRL）[22] ，即可得到所需的界。证明其余部分类似，故此处略去。为证明逆命题，可得

$$\begin{aligned}
nR_1 &= H(M_1)\\
&\leq I(M_1;\boldsymbol{Y},\boldsymbol{S}|M_0,\boldsymbol{X}_2) - I(M_1;\boldsymbol{Z}|M_0,\boldsymbol{X}_2) + \delta\\
&\overset{(a)}{=} I(M_1;\boldsymbol{Y},\boldsymbol{S}|\boldsymbol{Z},M_0,\boldsymbol{X}_2) + \delta\\
&\leq I(M_1,\boldsymbol{X}_1,\boldsymbol{S};\boldsymbol{Y},\boldsymbol{S}|\boldsymbol{Z},M_0,\boldsymbol{X}_2) + \delta\\
&= I(\boldsymbol{X}_1,\boldsymbol{S};\boldsymbol{Y},\boldsymbol{S}|\boldsymbol{Z},M_0,\boldsymbol{X}_2)\\
&\quad + I(M_1;\boldsymbol{Y},\boldsymbol{S}|\boldsymbol{Z},M_0,\boldsymbol{X}_2,\boldsymbol{X}_1,\boldsymbol{S}) + \delta\\
&\overset{(b)}{=} I(\boldsymbol{X}_1,\boldsymbol{S};\boldsymbol{Y},\boldsymbol{S}|\boldsymbol{Z},M_0,\boldsymbol{X}_2) + \delta\\
&= H(\boldsymbol{X}_1,\boldsymbol{S}|\boldsymbol{Z},M_0,\boldsymbol{X}_2) - H(\boldsymbol{X}_1,\boldsymbol{S}|\boldsymbol{Z},M_0,\boldsymbol{X}_2,\boldsymbol{Y},\boldsymbol{S}) + \delta\\
&\overset{(c)}{=} H(\boldsymbol{X}_1,\boldsymbol{S}|\boldsymbol{Z},M_0,\boldsymbol{X}_2) - H(\boldsymbol{X}_1,\boldsymbol{S}|M_0,\boldsymbol{X}_2,\boldsymbol{Y},\boldsymbol{S}) + \delta\\
&= I(\boldsymbol{X}_1,\boldsymbol{S};\boldsymbol{Y},\boldsymbol{S}|M_0,\boldsymbol{X}_2) - I(\boldsymbol{X}_1,\boldsymbol{S};\boldsymbol{Z}|M_0,\boldsymbol{X}_2) + \delta \qquad (9)
\end{aligned}$$

其中，$(a)$，$(c)$ 是由窃听信道的退化性得出的，$(b)$ 则由马尔可夫链 $(M_1,\ M_0)$ 得出 $-$

$(\boldsymbol{X}_1,\ \boldsymbol{X}_2,\ \boldsymbol{S})-(\boldsymbol{Y},\ \boldsymbol{Z})$。令 $U_i=(Y^{i-1},\ S^{i-1},\ \boldsymbol{X}_2,\ M_0)$，可得 $U_i$ 与 $S_i$相互独立。于是，我们有

$$
\begin{aligned}
&I(\boldsymbol{X}_1,\boldsymbol{S};\boldsymbol{Y},\boldsymbol{S}|M_0,\boldsymbol{X}_2)-I(\boldsymbol{X}_1,\boldsymbol{S};\boldsymbol{Z}|M_0,\boldsymbol{X}_2)\\
&=\sum_{i=1}^{n} I(\boldsymbol{X}_1,\boldsymbol{S};Y_i,S_i|Y^{i-1},S^{i-1},M_0,\boldsymbol{X}_2)\\
&\qquad -I(\boldsymbol{X}_1,\boldsymbol{S};Z_i|Z^{i-1},M_0,\boldsymbol{X}_2)\\
&=\sum_{i=1}^{n} H(Y_i,S_i|Y^{i-1},S^{i-1},M_0,\boldsymbol{X}_2)\\
&\qquad -H(Y_i,S_i|Y^{i-1},S^{i-1},M_0,\boldsymbol{X}_2,\boldsymbol{X}_1,\boldsymbol{S})\\
&\qquad -H(Z_i|Z^{i-1},M_0,\boldsymbol{X}_2)+H(Z_i|Z^{i-1},M_0,\boldsymbol{X}_2,\boldsymbol{X}_1,\boldsymbol{S})\\
&\overset{(a)}{\le}\sum_{i=1}^{n} H(Y_i,S_i|U_i,X_{2,i})-H(Y_i,S_i|U_i,X_{2,i},X_{1,i},S_i)\\
&\qquad -H(Z_i|Y^{i-1},S^{i-1},Z^{i-1},M_0,\boldsymbol{X}_2)\\
&\qquad +H(Z_i|Y^{i-1},S^{i-1},M_0,\boldsymbol{X}_2,X_{1,i},S_i)\\
&\overset{(b)}{=}\sum_{i=1}^{n} H(Y_i,S_i|U_i,X_{2,i})-H(Y_i,S_i|U_i,X_{2,i},X_{1,i},S_i)\\
&\qquad -H(Z_i|Y^{i-1},S^{i-1},M_0,\boldsymbol{X}_2)\\
&\qquad +H(Z_i|Y^{i-1},S^{i-1},M_0,\boldsymbol{X}_2,X_{1,i},S_i)\\
&=\sum_{i=1}^{n} I(X_{1,i},S_i;Y_i,S_i|U_i,X_{2,i})-I(X_{1,i},S_i;Z_i|U_i,X_{2,i})\\
&=n(I(X_1;Y,S|U,X_2\ S)-I(X_1;Z|U\ X_2\ S)+H(S|Z\ U\ X_2))
\end{aligned}
$$

其中，$(a)$ 和 $(b)$ 可由马尔可夫链 $(U_i,M_0)-$ 得出 $(X_{1,i},X_{2,i},S_i)-(Y_i,Z_i)$，以及窃听信道的退化性信道。关于 $R_1$ 的第二个约束可类似地得到，并且此处省略。对于和速率 ，可得

$$
\begin{aligned}
&n(R_0+R_1)\\
&=H(M_0)+nR_1\\
&\le I(M_0;\boldsymbol{Y},\boldsymbol{S})+nR_1+\delta\\
&\le\sum_{i=1}^{n} I(M_0;Y_i,S_i|Y^{i-1},S^{i-1})+I(X_{1,i},S_i;Y_i,S_i|U_i,X_{2,i})\\
&\qquad -I(X_{1,i},S_i;Z_i|U_i,X_{2,i})+\delta\\
&\le\sum_{i=1}^{n} I(M_0,Y^{i-1},S^{i-1},\boldsymbol{X}_2;Y_i,S_i)+I(X_{1,i},S_i;Y_i,S_i|U_i,X_{2,i})\\
&\qquad -I(X_{1,i},S_i;Z_i|U_i,X_{2,i})+\delta\\
&=\sum_{i=1}^{n} I(U_i,X_{1,i},X_{2,i},S_i;Y_i,S_i)-I(X_{1,i},S_i;Z_i|U_i,X_{2,i})+\delta\\
&=n(I(X_1,X_2;S)-I(X_1;Z|U,X_2,S)+H(S|Z,U,X_2)+\delta).
\end{aligned}
$$

和速率的第二个约束可类似地推出，此处省略。

## Appendix E
## Proof of example 2

逆向证明：根据附录 D，并将 $(Y,S)$ 替换为 $\boldsymbol{Y}$ 可得（为简便起见，我们省略 $\delta$。）

$$
\begin{aligned}
nR_1&\le I(\boldsymbol{X}_1,\boldsymbol{S};\boldsymbol{Y}|M_0,\boldsymbol{X}_2)-I(\boldsymbol{X}_1,\boldsymbol{S};\boldsymbol{Z}|M_0,\boldsymbol{X}_2)\\
&=(H(\boldsymbol{Y}|M_0,\boldsymbol{X}_2)-H(\boldsymbol{Y}|M_0,\boldsymbol{X}_2,\boldsymbol{X}_1,\boldsymbol{S}))-(H(\boldsymbol{Z}|M_0,\boldsymbol{X}_2)\\
&\qquad -H(\boldsymbol{Z}|M_0,\boldsymbol{X}_2,\boldsymbol{X}_1,\boldsymbol{S}))\\
&=(H(\boldsymbol{Y}_2|M_0,\boldsymbol{X}_2)+H(\boldsymbol{Y}_1|M_0,\boldsymbol{X}_2,\boldsymbol{Y}_2))\\
&\qquad -(H(\boldsymbol{Z}|M_0,\boldsymbol{X}_2)-nh(p))\\
&\overset{(a)}{\le} n+nh(q)-(H(\boldsymbol{Y}_2\oplus N|M_0,\boldsymbol{X}_2)-nh(p)),
\end{aligned}
$$

其中，$(a)$ 根据 $H(\boldsymbol{Y}_2|M_0,\boldsymbol{X}_2)\le\sum_{i=1}^{n}H(Y_i)\le n$ 得出。因此，存在某个 $\alpha\in[\frac{1}{2},1]$ 使得

$$nR_1\le nh(\alpha)+nh(q)-(H(\boldsymbol{Y}_2\oplus N|M_0,\boldsymbol{X}_2)-nh(p)).$$

为界定 $H(\boldsymbol{Y}_2\oplus N|M_0,\ \boldsymbol{X}_2)$，我们调用[3]（见 [23]中提出的引理 5 和引理 6）。

$$
\begin{aligned}
&H(\boldsymbol{Y}_2\oplus N|M_0,\boldsymbol{X}_2)\\
&=\mathbb{E}_{M_0,\boldsymbol{X}_2}[H(\boldsymbol{Y}_2\oplus N|M_0=m_0,\boldsymbol{X}_2=\boldsymbol{x}_2)]\\
&\overset{(a)}{\ge}\mathbb{E}_{M_0,\boldsymbol{X}_2}\left[nh\left(p*h^{-1}\left(\frac{H(\boldsymbol{Y}_2|M_0=m_0,\boldsymbol{X}_2=\boldsymbol{x}_2)}{n}\right)\right)\right]\\
&\overset{(b)}{\ge} nh\left(p*h^{-1}\left(\mathbb{E}_{M_0,\boldsymbol{X}_2}\left[\frac{H(\boldsymbol{Y}_2|M_0=m_0,\boldsymbol{X}_2=\boldsymbol{x}_2)}{n}\right]\right)\right)\\
&=nh\left(p*h^{-1}\left(\frac{H(\boldsymbol{Y}_2|M_0,\boldsymbol{X}_2)}{n}\right)\right)\\
&=nh\left(p*h^{-1}\left(\frac{nh(\alpha)}{n}\right)\right)=nh(p*\alpha).
\end{aligned}
$$

其中，$(a)$由 [3], 中的引理 6 得出，$(b)$由 [3]中的引理 5 得出。结合前述界可得

$$nR_1\le nh(\alpha)+nh(q)-nh(p*\alpha)+nh(p). \tag{10}$$

对于第二个约束，根据附录 D，我们有

$$
\begin{aligned}
nR_1&\le I(\boldsymbol{X}_1;\boldsymbol{Y}|M_0,\boldsymbol{X}_2,\boldsymbol{S})\\
&=I(\boldsymbol{X}_1,\boldsymbol{S};\boldsymbol{Y}|M_0,\boldsymbol{X}_2)-I(\boldsymbol{S};\boldsymbol{Y}|M_0,\boldsymbol{X}_2)\\
&\overset{(a)}{=}I(\boldsymbol{X}_1,\boldsymbol{S};\boldsymbol{Y}|M_0,\boldsymbol{X}_2)-H(\boldsymbol{S})\\
&=nh(\alpha)+nh(q)-nh(q)=nh(\alpha).
\end{aligned}
\tag{11}
$$

其中，$(a)$由以下事实得出：$\boldsymbol{S}$ 与$(M_0,\ \boldsymbol{X}_2)$相互独立，且接收方总能通过 $S_i=Y_{1,\,i}\ominus Y_{2,\,i}$恢复 $\boldsymbol{S}$。

对于和速率的第一个约束，根据附录 D，我们有

$$
\begin{aligned}
n(R_1+R_2)&\le I(M_0;\boldsymbol{Y})+nR_1\\
&\le I(M_0,\boldsymbol{X}_2;\boldsymbol{Y})+nR_1\\
&\le I(M_0,\boldsymbol{X}_1,\boldsymbol{X}_2,\boldsymbol{S};\boldsymbol{Y})-I(\boldsymbol{X}_1,\boldsymbol{S};\boldsymbol{Z}|M_0,\boldsymbol{X}_2)\\
&\le n+nh(q)-nh(\alpha*p)+nh(p).
\end{aligned}
\tag{12}
$$

第二个约束可类似地推出，故略去。

直接部分：可达区域可通过先将 FRL 直接应用于 (8) 得到；其他项可通过在区域 $\mathrm{R}_{D\ 21}^{CSI-E}$，中令 $U_2=X_2$ 并按 (8) 使用 FRL 类似地得到。然后，令 $Pr\{X_2=1\}=1$ 并定义 $X_1=U\oplus S\oplus X'$，其中 $Pr\{U=1\}=\frac{1}{2}$，$X'$ 是一个与 $(U,\ X_2,\ S,\ N)$ 相互独立的随机变量，且 $Pr\{X'=1\}=\beta$，使得 $q*\beta=\alpha$ 对某个 $\alpha\in[\frac{1}{2},1]$ 成立。证明完成。