衰落窃听信道中的无速率格码：有限长度保密性与退化会话的密钥容量

Hassan Khodaiemehr、Khadijeh Bagheri 和 Chen Feng

arXiv:2611.29177v1 [cs.IT] 22 Nov 2026

摘要——**在无速率传输中，发送方会持续发送，直到合法接收方（Bob）能够解码。在窃听信道中，这带来了一个有益的副作用：窃听者（Eve）看到的符号数量仅与 Bob 所需的数量相同，尽管发送方对两个信道都一无所知。我们研究了此情形下无速率格码的保密性。首先，利用公开抖动和隐私放大，我们证明了一个适用于每种信道实现的有限长度保密界，以全变差距离度量；即使 Eve 知道所有编码和种子，并合并所有数据包，该界仍然成立。其次，像混合自动重传请求那样，在 Bob 确认成功解码时停止传输，所付出的代价至多为可能反馈结果数量的对数个秘密比特。第三，对于采用基于状态的停止、且没有预共享密钥或其他公开讨论的退化会话，单次会话的密钥速率不会超过其累积的高斯保密容量；当 Eve 的信道状态在会话结束后公开时，采用整形无速率格码的自适应密钥生成可达到该上限的任意 $\epsilon > 0$ 范围内。若只知道这些状态的统计特性，则在会话结束后选择密钥长度，可保证预先设定的保密中断概率。最后，在块瑞利衰落信道中，采用基于循环冗余校验的确认和联合置信传播译码，且 Eve 的平均信道比 Bob 弱20 分贝时，对于8–20 分贝的 Bob 信噪比，该方案达到理想无限长度安全混合自动重传请求基准之中断加权吞吐量的59–69% 。**

索引词—**无速率编码、格编码、物理层安全、隐私放大、密钥协商、安全混合自动重传请求、分块衰落。**

I. 引言

IN 在无速率传输中，被动窃听者（Eve）观察到的符号数量由合法接收方（Bob）的信道决定：信道状况良好时，发射方（爱丽丝）会提前停止传输，此时 Eve 尚未积累太多信息，而且爱丽丝无需了解信道状况。由此产生两个问题。在混合自动重传请求中，Bob 在译码器成功时发送确认；因此，停止时间取决于消息本身，进而成为侧信道；文献 [1] 采用高斯分箱分析了长码块极限下的安全混合自动重传请求，而文献 [2],给出了固定长度窃听码的有限码长界限，但两者都未涵盖由基于译码的确认触发停止的实用无速率编码。此类方案每个会话能实现怎样的密钥速率？固定维数的格窃听码 [3]以及已知信道信息时的衰落保密容量 [4], [5]都无法回答这一问题。

我们研究由嵌套 Raptor 码通过构造 D 构建的无速率格：1）一种逐状态有限长度保密界：即使 Bob 在译码成功时发送确认，该界仍然有效，代价至多为反馈结果数量的 $\log_2$（定理 1）；2）退化会话的密钥容量：其逆定理（定理 2）及通过自适应密钥生成实现该容量的方案（推论1）；3）能够保证保密中断的密钥长度，以及扩频（直接序列扩频）层还能带来什么（命题 2）；4）通过置信传播（BP）解码经抖动的块瑞利衰落传输所得的结果。

作者来自加拿大不列颠哥伦比亚大学奥肯那根校区工程学院，地址为加拿大不列颠哥伦比亚省基洛纳（电子邮箱：has- san.khodaiemehr@ubc.ca、khadijeh.bagheri@ubc.ca、chen.feng@ubc.ca）。

II. 系统模型

无速率限制格。设 π_n 保留向量的前 n 个坐标。

定义 1 （无速率限制格 [6]）。 若满秩格序列 $(\Lambda_n)_{n\geq N}$ $\Lambda_n \subset \mathbb{R}^n$ 满足以下条件，则称其为 q元无速率格：(i)$q\mathbb{Z}^n \subseteq \Lambda_n \subseteq \mathbb{Z}^n$ 对每个 n均成立；(ii) $\pi_n(\Lambda_{n'}) = \Lambda_n$ 对所有$n' \geq n \geq N$均成立；(iii) 码本 $\mathcal{S}_n = \Lambda_n \cap \{0,\dots,q-1\}^n$的大小不依赖于 n。

整性使 $\mathcal{S}_n$ 成为 $\Lambda_n/q\mathbb{Z}^n$的一组代表元，因此 $|\mathcal{S}_n| = q^n/\mathrm{vol}(\Lambda_n)$；结合条件 (ii)–(iii)，它还使 $\pi_n : \mathcal{S}_{n'} \to \mathcal{S}_n$ 成为双射 [6]: 一条消息为每个$\mathcal{S}_n$选取一个点，而这些点是同一数据流的前缀。我们采用 [6]的 Raptor 格。设 $\mathcal{C}_{\mathrm{pre}} \subseteq \mathbb{F}_2^N$是一个维数为 K、校验矩阵为$\mathbf{H}_{\mathrm{pre}}$的预编码，并设 $\mathbf{s}_1, \mathbf{s}_2, \cdots \in \mathbb{F}_2^N$为 LT 阶段的各行。那么

$$\Lambda_n = \Big\{\mathbf{x} \in \mathbb{Z}^n : \ \mathbf{H}_{\mathrm{pre}}\mathbf{x}_{[1:N]} \equiv \mathbf{0} \pmod 2, \\ \mathbf{s}_t^{\mathsf{T}}\mathbf{x}_{[1:N]} + x_{N+t} \equiv 0 \pmod 4 \text{ for } t \leq n-N\Big\} \tag{1}$$

是一个整数 4 元无速率格，其 $\mathrm{vol}(\Lambda_n) = 2^{2n-k}$ 和$|\mathcal{S}_n| = 2^k$，$k = K + N$ [6,定理 1]。一个字 $\mathbf{u} = (\mathbf{m}_0, \mathbf{m}_1) \in \mathcal{C}_{\mathrm{pre}} \times \mathbb{F}_2^N$被编码为 $\boldsymbol{\xi} = \mathbf{m}_0 + 2\mathbf{m}_1$，随后为 $x_{N+t} = (-\mathbf{s}_t^{\mathsf{T}}\boldsymbol{\xi})$ 模 4，$t = 1, 2, \dots\dots$；我们将此数据流记为 $\mathbf{x_u}$。

信道。 一个符号 $a \in \{0,1,2,3\}$ 以中心化 4-PAM 振幅 $a - \frac{3}{2}$发送，其功率为 $P = \frac{5}{4}$；接收机已知的恒定平移不会影响距离或信息。Bob 和 Eve 分别观测到 $Y_{\mathrm{B},\,j} = X_j + \sigma_{\mathrm{B},\,j} Z_j$和 $Y_{\mathrm{E},\,j} = X_j + \sigma_{\mathrm{E},\,j} Z'_j$，其中噪声相互独立且为标准高斯噪声，$\sigma = \infty$ 表示擦除，信噪比为 $\mathrm{SNR}_{u,\,j} = P/\sigma^2_{u,\,j}$。这些状态 $\mathsf{S} = ((\sigma_{\mathrm{B},\,j}), (\sigma_{\mathrm{E},\,j}))$ 具有任意联合分布，且与消息、噪声和公开随机性相互独立，对爱丽丝而言未知。我们记 $W_\sigma(y|x)$ $\varphi_\sigma(y-x)$ $\bar{W}_\sigma = \frac{1}{4}\sum_{a=0}^{3} W_\sigma(\cdot|x)$ ( ) 和 ( )。

公开抖动。爱丽丝发送 $X_j = (x_{\mathbf{u},\,j} + D_j) \bmod 4$，并在每次会话中使用一个新的抖动 $\mathbf{D}$，它在 $\mathbb{Z}_4^n$ 上均匀分布，且 Bob 和 Eve 都知道。由于 $x \mapsto (x+d) \bmod 4$ 不是 PAM等距变换，该抖动会改变欧几里得码，而且通常会使 Bob 的错误概率 ($\{0,1\}$ 变为 $\{3,0\}$，其中 $d = 3$)。Bob 使用 $W_{\sigma_{\mathrm{B},\,j}}(y_j|(x_{\mathbf{u},\,j} + D_j) \bmod 4)$ 进行解码。我们采用的 [6] 可靠性结果是：对于每个与码集合和抖动相互独立的状态序列，均对码集合和抖动取平均；也就是说，这些保证适用于由公开种子抽取的编码，而非某个确定性编码对所有状态均适用 [6, 注 2]。

停止与反馈。符号按轮次发送，直至 $n_1 < n_2 < \cdots$，$L_r = n_r - n_{r-1}$。基于状态的规则设定$\tau = \bar{\tau}(\mathrm{S})$，例如，选取 Bob 的累积容量超过关卡大小的 $(1+\delta)$ 倍之后的第一轮。基于解码的规则设定 $\tau = \min(\tau_{\mathrm{dec}}, \bar{\tau})$，其中 τ_{dec} 是 Bob 的验证测试首次通过的轮次；其公开记录 T（否定确认、确认轮次、达到上限时的中止标志）取 $|\mathcal{T}| \le \bar{\tau}+1$个值，$\bar{\tau}$ 是以 $\bar{\tau}$ 结束的轮次数，且不得依赖哈希种子。c 比特的循环冗余校验是一种可实现的测试：它会消耗 c 比特的源熵，并且每次尝试接受错误码字的概率约为 2^{-c}。

隐私放大。对于密钥协商，爱丽丝发送均匀分布的 $\mathbf{U}$，双方在会话结束后计算 $\mathbf{M} = f_{\mathbf{h}}(\mathbf{U})$，使用二重通用哈希族 $f_{\mathbf{h}} : \mathbb{F}_2^k \to \mathbb{F}_2^{k_{\mathrm{s}}}$以及新的公开种子 $\mathbf{h}$，例如 $f_{\mathbf{h}}(\mathbf{u}) = \mathbf{u}_{[1:k_{\mathrm{s}}]} \oplus \mathbf{T}_{\mathbf{h}}\mathbf{u}_{[k_{\mathrm{s}}+1:k]}$；$k_{\mathrm{s}}$可以依赖于 τ以及已公开的状态。长度预先固定的秘密消息通过先求逆后编码 [8],发送，具体做法是从 $f^{-1}{}_{\mathbf{h}}(\mathbf{M})$ 中均匀抽取 $\mathbf{U}$。如果界给出的值为正，则长度取其向下取整；否则密钥为空。

*Eve*与保密性度量。Eve 观测 $\mathbf{Y}_{\mathrm{E}} = (Y_{\mathrm{E},\,j})_{j \le \tau}$、$T$、S、$\mathbf{h}$、$\mathbf{D}$ 以及所有编码参数；她的计算能力无限，并且可以合并所有轮次。给定 $\mathbf{V}_{\mathrm{E}} = (\mathbf{Y}_{\mathrm{E}},\ T,\ \mathbf{h},\ \mathbf{D})$ 以及与 $(\mathbf{h},\ \mathbf{D},\ \mathrm{S})$ 独立且均匀的 $\mathbf{M}$，$d_{\mathrm{TV}} = \frac{1}{2}\| P_{\mathbf{M}\mathbf{V}_{\mathrm{E}}|\mathrm{S}} - P_{\mathrm{unif}} \times P_{\mathbf{V}_{\mathrm{E}}|\mathrm{S}} \|_1$。它对公开随机性取平均：$d_{\mathrm{TV}} \le \varepsilon$ 对除比例 α 之外的所有种子和抖动，其距离至多为 ε/α。

III. 针对任意被动对手的泄漏界

对于 $\theta \in (0,1]$ 令

$$I_{1+\theta}(\sigma) = \frac{1}{\theta} \log\Big(\frac{1}{4} \sum_{x=0}^{3} \int W_\sigma(y|x)^{1+\theta} \bar{W}_\sigma(y)^{-\theta} dy \Big), \quad (2)$$

均匀 4-PAM 的阶-$1+\theta$ Rényi 信息，它随 $\theta \downarrow 0$ 趋近于其互信息 $C_{\mathrm{X}}(\sigma)$，并令$\mathcal{L}(\sigma) = \log \int \max_x W_\sigma(y|x) dy = \log(1 + 3\,\mathrm{erf}(\frac{1}{2\sqrt{2}\sigma}))$ 为最大泄漏 [9]。当 $\sigma = \infty$ 时二者均趋于零；对数以 2 为底，且 $A_n = \sum_{j \le n} I_{1+\theta}(\sigma_{\mathrm{E},\,j})$。

定理 1（无速率有限长度保密）。考虑任意一个具有 2^k 个等概率字 $\mathbf{u}$ 的编码，以及针对每个字的固定数据流$\mathbf{x}_{\mathbf{u}} \in \{0,1,2,3\}^\infty$、输出长度为 k_{s} 的隐私放大和一个基于状态的停止规则。固定 S。

(a) 使用公开抖动时，对每个 $\theta \in (0,1]$ 和 $\omega \ge 0$，

$$d_{\mathrm{TV}} \le \tfrac{1}{2}\, 2^{-\frac{1}{2}(k - k_{\mathrm{s}} - A_\tau - \omega)} + 2 \cdot 2^{-\theta\omega}. \quad (3)$$

(b) 不使用抖动时，$d_{\mathrm{TV}} \le \frac{1}{2}\, 2^{-\frac{1}{2}(k - k_{\mathrm{s}} - \sum_{j \le \tau} \mathcal{L}(\sigma_{\mathrm{E},\,j}))}$。*(c)* 使用基于解码的规则 $\tau = \min(\tau_{\mathrm{dec}}, \bar{\tau})$，其记录 T 与$\mathbf{h}$ 相互独立，且至多取 $|\mathcal{T}|$ 个值，则将 τ 替换为 $\bar{\tau}$、将 k 替换为$k - \log|\mathcal{T}|$ 后，*(a)* 和 *(b)* 仍成立。

此外 $I(\mathbf{M};\ \mathbf{V}_{\mathrm{E}}|\mathrm{S}) \le d_{\mathrm{TV}} k_{\mathrm{s}} + (1 + d_{\mathrm{TV}})\, h_{\mathrm{b}}\big(\frac{d_{\mathrm{TV}}}{1+d_{\mathrm{TV}}}\big)$，并且，如果 $\sigma_{\mathrm{E},\,j} \ge \sigma_{\min} > 0$，那么对每个 $\zeta > 0$，都存在 $\theta > 0$，使得长度为 $k_{\mathrm{s}} = k - \sum_{j \le \tau} C_{\mathrm{X}}(\sigma_{\mathrm{E},\,j}) - \zeta\tau - \theta^{-1} \log \frac{4}{\varepsilon} - 2 \log \frac{2}{\varepsilon}$ 的编码满足 $d_{\mathrm{TV}} \le \varepsilon$。

证明：由于 $\mathbf{h}$ 与源字独立，也与 Eve 除$\mathbf{h}$之外所看到的一切独立，因此只需对给定该视图 [10] 时$\mathbf{U}$ 的平滑平均最小熵给出下界，并应用剩余哈希引理：若一个通过移除质量为 $\varepsilon_{\mathrm{sm}}$ 的部分而得到的次归一化测度$\tilde{}$满足 $H_\infty \ge \lambda$，则距离至多为 $2\varepsilon_{\mathrm{sm}} + \frac{1}{2}\sqrt{2^{k_{\mathrm{s}} - \lambda}}$ [11]。

(a) 此处 $\tau = n$为固定值。将 (U, D, $\mathrm{Y_E}$) 的联合密度记为 $p(\mathbf{u}, \mathbf{d}, \mathbf{y}) = P_{\mathbf{D}}(\mathbf{d})\, 2^{-k} \prod_j W_{\sigma_{\mathrm{E}\,j}}(y_j | x_{\mathbf{u}\,j} + \mathbf{d}\,y)$，$(\mathbf{d}, \mathbf{y}) \mapsto (d_j)_{j \le n}$ 为 $(\mathbf{u}, \mathbf{d}, \mathbf{y})$ 的边缘密度，令 $\bar{W}^n = \prod_j W_{\sigma_{\mathrm{E},j}}$ 和 $\lambda = k - A_n - \omega$，并删除满足 $p > 2^{-\lambda} P_{\mathbf{D}}(\mathbf{d})\, \bar{W}^n(\mathbf{y})$ 的集合。在其余部分，$\sum_{\mathbf{d}} \max_{\mathbf{u}} p' \le 2^{-\lambda}$，即 $\tilde{H}_\infty(\mathrm{U}|\mathrm{D}, \mathrm{Y_E}) \ge \lambda$。对于每个固定的 $\mathbf{u}$，对 D 取平均会使 X 成为独立同分布的均匀变量；因此，$\bar{}$信息密度 $L_j = \log[W_{\sigma_{\mathrm{E},j}}(Y_{\mathrm{E},j}|X_j) / \bar{W}_{\sigma_{\mathrm{E},j}}(Y_{\mathrm{E},j})]$ 在满足 $\mathbb{E}[2^{\theta L_j}] = 2^{\theta I_{1+\theta}(\sigma_{\mathrm{E},j})}$ 的联合分布下相互独立，而马尔可夫不等式将删除部分的质量界定为 $2^{-\theta\omega}$。

(b) 无抖动时，$2^{-H_\infty(\mathbf{U}|\mathbf{Y_E})} \le 2^{-k} \int \max_{\mathbf{x}} \prod_j W_{\sigma_{\mathrm{E},\,j}}(y_j|x_j)\, d\mathbf{y} = 2^{-k} \prod_j 2^{\mathcal{L}(\sigma_{\mathrm{E},j})}$，因为不同变量函数乘积的最大值可以因式分解。

(c) 由于数据流 $\mathbf{x_u}$ 预先已固定，Eve 截至上限的潜在观测 $\mathrm{Y_E^{\bar{\tau}}}$ 是定义良好的，而她的实际视图是 ($\mathrm{Y_E^{\tau}}$、D T、h) 的函数；丢弃未使用的尾部不会降低保密性。在完整时域 $\bar{\tau}$上使用 (a) 中的删除操作一次，并取 $\lambda = k - A_{\bar{\tau}} - \omega$；被删除的质量至多为$2^{-\theta\omega}$。根据原始实验中的条件分布附加 T；于是 $p'(\mathbf{u}, \mathbf{d}, \mathbf{y}\ t) \le p'(\mathbf{u}, \mathbf{d}, \mathbf{y})$，对 $\mathbf{u}$ 的最大值在 t 的至多 $|\mathcal{T}|$ 个取值上求和，可得 $\tilde{H}_\infty(\mathrm{U}|\mathrm{D}, \mathrm{Y_E^{\bar{\tau}}}, T) \ge \lambda - \log|\mathcal{T}|$，无论$T$ 与消息及 Bob 的噪声具有什么依赖关系。由于 T 与 h 独立，剩余哈希引理适用；无需对轮次使用并集界。(b) 的对应结论也可由同样的论证得到。

互信息界是条件熵的连续性界 [12,引理 2]。对于密钥长度，$I_{1+\theta}$在紧集 $[\sigma_{\min}, \infty]$ 上连续，并在 $\theta \downarrow 0$时递减至 C_{X}；根据 Dini 定理，$I_{1+\theta} \le C_{\mathrm{X}} + \zeta$ 在某个 $\theta > 0$处成立；取 $\omega = \theta^{-1} \log \frac{4}{\varepsilon}$，可使式 (3) 中的每一项至多为 $\varepsilon/2$。

■

该界根据状态按会话评估；其在 θ 中的指数与 [13]的指数相同。根据 (c)，在相同的基于状态的上限下，基于译码的确认需要 $\log|\mathcal{T}| \le \log(\bar{\tau}+1)$ 比特（31 轮时为 5 比特）；使用 $A_{\bar{\tau}}$ 而非 A_τ 会额外耗费 $A_{\bar{\tau}} - A_\tau$ 比特，这是预先不知道 τ 所付出的代价。假设条件很重要：若某条规则将 $f_{\mathbf{h}}(\mathbf{U})$ 的一比特编码进轮次索引，那么无论 $k - k_{\mathrm{s}}$ 为何，它都会泄露该比特；每条额外的公开消息也必须计入 T。只有编码的大小和字母表以及 Eve 的信道会产生影响；知识

格、抖动和哈希的知识、不受限制的计算能力，以及对所有数据包进行联合解码，均已涵盖。抖动使泄漏率趋近于 $C_{\mathrm{X}}(\sigma_{\mathrm{E}})$：在 0 分贝时为 $\mathcal{L} = 1.03$ 比特，而 $C_{\mathrm{X}} = 0.49$ 和 $I_{1.05} = 0.51$。该保证是有限长度 ε全变差保密性；渐近强保密性需要 $\varepsilon_k \downarrow 0$ 和 $\varepsilon_k k_{\mathrm{s}} \to 0$，例如 $\varepsilon_k = k^{-2}$，代价为$O(\log k)$ 比特。

IV. 退化会话的密钥容量

定理 1(a)对任意抖动符号均匀分布的字母表均逐字成立，特别适用于 [6, Thm. 7],中的几何成形 p元无速率格编码，其前缀是缩放无速率格的平移副本中的点，且其 p 等概率点逼近高斯分布。令 $I_g(\sigma)$表示这种功率为 P的星座的互信息。由于 2^{k_s} 不能整除 p^{k_p}，没有平衡二进制哈希能够作用于所有字；我们使用一个固定子集 $\mathcal{U}_b$ of2^b 个字，即 $b = \lfloor k_p \log p \rfloor$，并以二进制字符串标记。在该子集上，全码译码器的平均出错次数至多是 $|\mathcal{U}_b| > p^{k_p}/2$的两倍。我们假设界限为$\sigma_{\mathrm{E},\,j} \geq \sigma_{\mathrm{E},\,j}$，这些界限在该会话之后发表，信噪比为 SNR$_{\mathrm{E},\,j} = P/\sigma^2_{\mathrm{E},\,j}$（保护区限制的是路径损耗，而非瑞利衰落；命题 1处理统计信息）。

推论1（自适应密钥生成）。在与U 在 $\mathcal{U}_b$ 上均匀分布时进行密钥协商，设 *Bob* 接收的信噪比至多为 信噪比$_{\max}$，令 $\sigma_{\mathrm{E},j}$ 位于$(0,\infty]$ 的一个紧子集中。令 *Bob* 在满足 $\sum_{j\leq\tau} I_g(\sigma_{\mathrm{B},j}) \geq (1+\delta)k_p \log p$ 的首个轮次结束时停止，并令停止轮次的长度 L_ι（其中 $\tau = n_\iota$）满足 $L_\iota \leq \ell_{k_p}$，且 $\ell_{k_p}/k_p \to 0$。对于每个 $\epsilon > 0$，均存在 p 及一个星座，使得当 δ 足够小且 k_p 足够大时，*Bob* 的系综平均错误概率趋于零，并且公钥长度满足

$$\frac{k_{\mathrm{s}}}{\tau} \;\geq\; \frac{1}{\tau}\sum_{j\leq\tau} \tfrac{1}{2}\log\frac{1+\mathrm{SNR}_{\mathrm{B},j}}{1+\overline{\mathrm{SNR}}_{\mathrm{E},j}} - \epsilon - \frac{L_\iota \log p + F_\varepsilon}{\tau} \qquad (4)$$

得到 $d_{\mathrm{TV}} \leq \varepsilon$，其中 $F_\varepsilon = \theta^{-1}\log\frac{4}{\varepsilon} + 2\log\frac{2}{\varepsilon} + 2$ 包含整数舍入；最后一项随 $k_p \to \infty$ 趋于零。

证明：在基于状态的时刻，可靠性由定理 7]保证（对每个固定状态序列的系综保证），并限制在 $\mathcal{U}_b$ 上。令 $B_n = \sum_{j\leq n} I_g(\sigma_{\mathrm{B},j})$。由 τ 的最小性可得 $B_{n_{\iota-1}} < (1+\delta)k_p \log p$，而停止轮次至多增加 $L_\iota \log p$，因此为 $k_p \log p > (B_\tau - L_\iota \log p)/(1+\delta)$；除非每轮只有一个符号，否则轮次长度项无法由 $\log p$ 界定。对该字母表应用定理 1(a)，在 σ_{E} 处取 $I_{1+\theta}$（由退化可知，它关于 σ 单调不增），并根据 Dini 定理选择θ，使其在紧范围上满足 $I_{1+\theta} \leq I_g + \zeta$，即可保证 $k_{\mathrm{s}} = \lfloor b - \sum_{j\leq\tau} I_g(\sigma_{\mathrm{E},j}) - \zeta\tau - \theta^{-1}\log\frac{4}{\varepsilon} - 2\log\frac{2}{\varepsilon}\rfloor \geq k_p \log p - \sum_{j\leq\tau} I_g(\sigma_{\mathrm{E},j}) - \zeta\tau - F_\varepsilon$ 比特，其中使用了 $b \geq k_p \log p - 1$。最后，$I_g/(1+\delta) \geq I_g - \delta\log p$，$I_g(\sigma_{\mathrm{B},j}) \geq \frac{1}{2}\log(1 + \text{信噪比}_{\mathrm{B},j}) - \epsilon/3$，由定理 7]得出；根据高斯最大熵界，$I_g(\sigma_{\mathrm{E},j}) \leq \frac{1}{2}\log(1 + \text{信噪比}_{\mathrm{E},j})$；取足够小的 ζ, δ 即得式 (4)。由于 $I_g \leq \log p$，$\tau \geq k_p$，且式 (4) 的最后一项趋于零。 ∎

推论1涉及自适应密钥生成；预先确定的秘密消息需要预先固定长度。

定理 *2*（逆定理）。考虑任意一种方案：该方案没有预共享密钥，也没有公开讨论，唯一例外是公布状态和基于状态的停止通知；其中，公开随机性 *Q*（种子、抖动、码选择）与 *(M, S)* 相互独立，给定 *Q* 后，爱丽丝的潜在数据流 (X_j) 与 *S* 相互独立，且 $\mathbb{E}[X_j^2] \leq P$。对于满足 $\hat{}\sigma_{\mathrm{E},j} \geq \sigma_{\mathrm{B},j}$ *for* $j \leq \tau$ 的 *S*，固定 *S*。若 *Bob* 对 *M* 的估计值 *M*(Y_{B}, *Q)* 满足 $\hat{}Pr\{M \neq M \,|\, S\} \leq \varepsilon_{\mathrm{B}}$ *and* $I(M; Y_{\mathrm{E}}, Q \,|\, S) \leq \ell$，且 *M* 均匀分布，则

$$(1-\varepsilon_{\mathrm{B}})\, k_{\mathrm{s}} \;\leq\; \sum_{j\leq\tau} \tfrac{1}{2}\log\frac{1+\mathrm{SNR}_{\mathrm{B},j}}{1+\mathrm{SNR}_{\mathrm{E},j}} + \ell + 1. \qquad (5)$$

使用 κ 比特的预共享密钥后，右侧加上 κ。

证明：对 S 进行条件化；此时 $n = \tau$ 固定。由 Fano 不等式，$(1-\varepsilon_{\mathrm{B}})k_{\mathrm{s}} \leq I(\mathrm{M}; \mathrm{Y_B}|\mathrm{Q}) + 1$。给定 Q，可靠性和保密性仅取决于两个边缘信道，因为不会根据 $\mathrm{Y_B}$ 计算任何记录；因此我们可以假设 $Y_{\mathrm{E},j} = Y_{\mathrm{B},j} + Z''_j$，且具有相互独立的 $Z''_j \sim \mathcal{N}_j(0, \sigma^2_{\mathrm{E}} - \sigma^2_{\mathrm{B}})$。给定 Q，马尔可夫链 M X Y Y 导出 $I(\mathrm{M}; \mathrm{Y_B}|\mathrm{Q}) \leq I(\mathrm{M}; \mathrm{Y_E}|\mathrm{Q}) + \sum_j I(X_j; Y_{\mathrm{B},j}|Y_{\mathrm{E},j}, \mathrm{Q})$，并且 $I(\mathrm{M}; \mathrm{Y_E}|\mathrm{Q}) \leq I(\mathrm{M}; \mathrm{Y_E}, \mathrm{Q}) \leq \ell$，因为 M 与 Q 独立。给定 Q = q 时，第 j 项至多为 $f_j(P_j(\mathrm{q}))$ [14],，其中 $P_j(\mathrm{q}) = \mathbb{E}[X_j^2|\mathrm{Q} = \mathrm{q}]$，且 $f_j(v) = \frac{1}{2}\log(1+v/\sigma^2_{\mathrm{B},j})$，对于 $\sigma_{\mathrm{E},j} \geq \sigma_{\mathrm{B},j}$ 是非递减且凹的。由 Jensen 不等式以及 $\mathbb{E}[P_j(\mathrm{Q})] \leq P$，可得 $\mathbb{E}[f_j(P_j(\mathrm{Q}))] \leq f_j(P)$。一个 κ 比特的密钥至多使 $I(\mathrm{M}; \mathrm{Y_B}|\mathrm{Q}) - I(\mathrm{M}; \mathrm{Y_E}|\mathrm{Q})$ 增加 κ。 ∎

在信噪比$_{\mathrm{E},\,j}$ =信噪比$_{\mathrm{E},\,j}$的紧确界和短轮次条件下，推论1和定理 2表明，在基于状态的停止机制下，无需额外资源，实际会话累积的高斯保密容量就是退化会话的密钥容量（$\sigma_{\mathrm{E},\,j} \geq \sigma_{\mathrm{B},\,j}$）。这些限制至关重要（预共享的一次一密在信道相同的情况下也能实现正速率），而基于译码的停止和非退化会话仍有待研究。非退化轮次并不少见：对于均值相差 G 的独立指数分布信噪比，Eve 在某一轮次中更强的概率为$1/(1+G)$，20 分贝时为0.99%，15 分贝时为3.07%。对于下面的4-PAM编码，$\sum_{j\leq\tau}[C_{\mathrm{X}}(\sigma_{\mathrm{B},\,j}) - C_{\mathrm{X}}(\sigma_{\mathrm{E},\,j})]$ 是均匀输入的对应形式。

V. 统计窃听者知识

在实际中，爱丽丝和 Bob 只知道 Eve 状态的分布。假设每轮内状态保持不变，$(\sigma_{\mathrm{B},\,j}, \sigma_{\mathrm{E},\,j}) = (\beta_r, \gamma_r)$ 对于 $n_{r-1} < j \leq n_r$ 成立，并且各轮之间的配对 (β_r, γ_r) 相互独立，且给定 β_r 时 γ_r 的条件分布已知；令 $\boldsymbol{\beta} = (\beta_1, \beta_2, \ldots)$。

命题 1 (具有保证中断的密钥长度)。在基于状态的 $\bar{\tau} = n_{\bar{r}}$ 密钥协商中，令 $\Lambda_\theta = \sum_{r\leq\bar{r}} L_r I_{1+\theta}(\gamma_r)$，并令 $q_{1-\eta}(\boldsymbol{\beta})$ 为给定 $\boldsymbol{\beta}$时其条件分布的一个上$1-\eta$分位数。密钥长度$k_{\mathrm{s}} = \max\{0, \lfloor k - q_{1-\eta}(\boldsymbol{\beta}) - \theta^{-1}\log\frac{4}{\varepsilon} - 2\log\frac{2}{\varepsilon}\rfloor\}$ 满足$\Pr\{d_{\mathrm{TV}} > \varepsilon \,|\, \boldsymbol{\beta}\} \leq \eta$，对任意 $\boldsymbol{\beta}$ 均成立。此外，

$$q_{1-\eta}(\boldsymbol{\beta}) \leq \sum_{r\leq\bar{r}} L_r\, \mathbb{E}[I_{1+\theta}(\gamma_r)|\beta_r] + \left(2\ln\tfrac{1}{\eta}\sum_{r\leq\bar{r}} L_r^2\right)^{1/2}. \qquad (6)$$

证明：给定 β，$\bar{r}$ 是固定的；由定理 1(a)，取 $\omega = \theta^{-1}\log\frac{4}{\varepsilon}$，可知当 $\Lambda_\theta \le q_{1-\eta}(\beta)$ 时，$d_{\mathrm{TV}} \le \varepsilon$ 成立；这是一个条件概率至少为 $1-\eta$ 的事件；空密钥的距离为 0。给定 β，各项 $L_r I_{1+\theta}(\gamma_r)$ 相互独立且取值于 $[0, 2L_r]$，因为 $W_\sigma(y|x)/W_\sigma(y) \le 4$；由 Hoeffding 不等式 [15] 得到式 (6)。 ∎

这是一项保密中断保证，而非保证每个会话都具备保密性：如果 $d(\mathsf{s}) \le \varepsilon$ 在概率为 η 的状态集合之外，则包括公开状态在内的距离为 $\mathbb{E}_{\mathsf{S}} d(\mathsf{S}) \le (1-\eta)\varepsilon + \eta$。在第七节的较长首轮中，(6) 较为宽松，我们通过蒙特卡洛估计分位数；由于原始百分位数可能低估该值，我们采用容差分位数：使用 m 个校准样本时，第 j 个次序统计量以置信度 $1-\alpha$ 成为上侧（$1-\eta$）分位数，若 $\Pr\{\mathrm{Bin}(m, 1-\eta) \ge j\} \le \alpha$。

六、扩频能带来什么，不能带来什么

我们之前的方案 [7] 将 DSSS 层建模为 Eve 处固定的信噪比惩罚。下一个命题将取代这一假设。

命题 2（DSSS 与保密性）。设每个符号 x_j 均以 $x_j \boldsymbol{\psi}_j$ 的形式在 $\mathfrak{s}$ 个码片上发送，$\boldsymbol{\psi}_j \in \{\pm 1\}^{\mathfrak{s}}$，且码片噪声为白高斯噪声，其方差为 $\varsigma^2_{\mathrm{B},\,j}$ 和 $\varsigma^2_{\mathrm{E},\,j}$。

(a) 如果 *Eve* 知道这些序列，则定理 *1* 对 $\sigma^2_{u,j} = \varsigma^2_{u,j}/\mathfrak{s}$，$u \in \{B, E\}$ 仍然成立；*DSSS* 不会改变 $\sigma_{\mathrm{E},j}/\sigma_{\mathrm{B},j}$。*(b)* 如果这些序列由一个与 *(U,h, D)* 相互独立的 κ 比特密钥 K_{sp} 生成，而 V 是 *Eve* 的 $\tilde{}$ 码片级观测，那么 $H_\infty(\mathbf{U}|\mathbf{V}, K_{\mathrm{sp}}) \le H_\infty(\mathbf{U}|\tilde{\mathbf{V}}) \le H_\infty(\mathbf{U}|\mathbf{V}, K_{\mathrm{sp}}) + \kappa$，且 $I(\mathbf{U};\mathbf{V},K_{\mathrm{sp}}) - I(\mathbf{U};\mathbf{V}) = I(\mathbf{U};K_{\mathrm{sp}}|\mathbf{V}) \le \kappa$。

证明：(a) 对 $\boldsymbol{\psi}_j/\sqrt{\mathfrak{s}}$ 进行投影，得到 $\sqrt{\mathfrak{s}}\,x_j$，其噪声方差为 $\varsigma^2_{u,\,j}$，这是一个充分统计量。(b) 条件化不会 $\tilde{}$ 增加平均最小熵，$H_\infty(\mathbf{U}|\mathbf{V},\,\mathbf{K}) \ge H_\infty(\mathbf{U}|\mathbf{V}) - \log|\mathcal{K}|$ [10, 引理 2.2]，而该恒等式即为链式法则。 ∎

带密钥的序列最多可将联合泄漏减少其密钥长度，而密钥长度是一种消耗的资源；Eve 的互信息按符号减少，并不意味着每个符号都需要密钥，因为多个观测可能冗余地描述同一组源比特。在 (a) 中，两台接收机的符号能量均增大 $\mathfrak{s}$ 倍；在符号能量固定时，不存在处理增益。

VII. 数值结果

设置。我们使用 [6] 的 Raptor 格，采用 $N = 684$，$K = 571$（设计 A，LT 配置 M，[6, 算法 1]），首轮为 684 维，后续各轮为 114 维，最多 31 轮，并采用块瑞利衰落，复增益为 $h_{\mathrm{E},\,r} = \varrho h_{\mathrm{B},\,r} + \sqrt{1-\varrho^2} w_r$，$h_{\mathrm{B},\,r},\ w_r \sim \mathcal{CN}(0, 1)$ 相互独立，信噪比为 $\gamma_{u,\,j} = |h_{u,\,r}|^2$ 信噪比 γ_u。每个会话都使用新的公开抖动，Bob 和 Eve 均对抖动符号进行解码。Bob 在基于状态的时刻停止，并采用多阶段（MSD）BP 和裕量为 δ 的层容量规则，或采用联合 $\mathbb{Z}_4$-BP [6]和规则 $\sum_{j\le\tau} C_{\mathrm{X}}(\sigma_{\mathrm{B},\,j}) \ge (1+\delta)k$（通过数值求积计算容量）；译码错误和容量上限失效均计为损失。Eve 的平均信噪比比 Bob 低 15 或 20 分贝（差距）；$\varrho = 0$除非另有说明。每个会话均根据定理 1(a) 进行评估

表 I 块瑞利衰落下的中断加权安全吞吐量（比特/维），抖动传输，$\varrho = 0$，$\varepsilon = 10^{-6}$，1000 个会话/点

gap	Bob 的信噪比（分贝）	8	11	14	17	20	23
20 分贝	理想安全 HARQ [1]	0.91	1.05	1.09	1.02	0.86	0.65
	联合 BP，互信息准则	0.64	0.77	0.84	0.80	0.67	0.52
	联合 BP，定理 1(a)	0.56	0.65	0.70	0.64	0.52	0.38
	联合 BP，CRC-ACK，定理 1(c)	0.61	0.70	0.75	0.68	0.51	0.32
	MSD 置信传播，定理 1(a)	0.36	0.50	0.57	0.54	0.41	0.26
	固定，联合准则，定理 1(a)	0.42	0.47	0.54	0.52	0.45	0.36
	固定，MSD 准则，定理 1(a)	0.25	0.35	0.43	0.46	0.39	0.25
15 分贝	理想安全 HARQ [1]	0.75	0.80	0.76	0.64	0.48	0.32
	联合 BP，互信息准则	0.51	0.56	0.57	0.48	0.34	0.23
	联合 BP，定理 1(a)	0.41	0.44	0.43	0.35	0.24	0.15
	联合 BP，CRC-ACK，定理 1(c)	0.44	0.47	0.44	0.32	0.20	0.10
	MSD BP，定理 1(a)	0.23	0.31	0.33	0.26	0.15	0.08
	固定，联合准则，定理 1(a)	0.29	0.31	0.32	0.27	0.22	0.15
	固定，MSD 准则，定理 1(a)	0.16	0.20	0.25	0.24	0.15	0.08

在 $\varepsilon = 10^{-6}$ 处，对 $\theta \in [0.01, 1]$ 的 12 个取值以及 ω 取最小值；如果在所选 k_{s} 下，该界超过 ε，则该会话发生保密中断。按中断概率加权的安全吞吐量为 $\mathrm{T_s} = k_{\mathrm{s}} \Pr\{\text{Bob 正确解码且未发生保密中断}\}/\mathbb{E}[\tau]$，并针对固定的 k_{s} 进行最大化；这并不意味着每个传输会话都安全。表 I 每个点采用 1000 个会话，其中δ针对 $\{0.25, 0.35, 0.45\}$（MSD）、$\{0.2, 0.3, 0.4\}$（联合）和 0.3（ACK）进行优化。在 ACK 各行中，Bob 在每轮后解码，最多持续至 $\bar{\tau}$，并在首次成功时停止；这一过程建模为理想的 16 位 CRC：我们计入 16 比特（$k \to k-16$），采用 $|\mathcal{T}| = \bar{r}+1$，并从 Bob 的成功概率中减去未检出错误界（$\bar{r}+1$）$2^{-16} < 5\times10^{-4}$。固定长度基准（采用相同编码和界，并对长度及 k_{s} 进行优化）不经解码，而是依据容量准则判定 Bob 是否成功，这对该基准更有利。理想安全 HARQ 参考方案 [1] 采用相同的有效载荷、轮次和 4-PAM 输入，在 $\sum_{j\le\tau} C_{\mathrm{X}}(\sigma_{\mathrm{B},\,j}) \ge k$ 时停止，并在 $\sum_{j\le\tau} C_{\mathrm{X}}(\sigma_{\mathrm{E},\,j}) \le k - k_{\mathrm{s}}$ 时判定保密（理想解码，渐近准则）。$\mathrm{T_s}$ 的自助法 95% 半宽至多为 0.028 比特/维。

仅靠编码并不能实现保密性。在 Eve 的置信传播恢复了所传输的格点的全部 8089 个模拟会话中，定理 1 保证没有秘密比特。当 Bob 的信噪比为 14 分贝、差距为 6 分贝时，Eve 在 12% 的会话中恢复了格点（图1(c)）。

无速率与定长。使用 MSD BP、$\delta = 0.35$ 和 20 分贝的差距时，无速率方案在 Bob 的信噪比分别为 8、11、14 和 17 分贝时达到 0.37、0.47、0.54 和 0.50 比特/维，而最佳定长传输分别为 0.25、0.31、0.40 和 0.43（图1(a)）。15–51%的增益来自泄漏自适应性：当 Bob 的信道状况良好时，爱丽丝会提前停止。在高信噪比下，两台接收机都趋近于 4-PAM 的 2 比特上限；整形码（推论1）可以消除这一限制，但缺乏实用的译码器。

联合解码、确认信息以及与理想值的差距。在 Bob 处采用联合 BP，相比 MSD BP，可将吞吐量提高 18–55%（差距为 20 分贝时）和 30–90%（差距为 15 分贝时）（表 I），因为它缩短了 $\mathbb{E}[\tau]$（在 8 分贝时从 2335 降至 1565 维度），而每节省一个维度，就意味着从 Eve 处扣留一个维度。采用联合 BP 时，无速率方案相比使用相同准则的固定长度方案高出 4–43%。相对于理想值，采用基于状态的停止的联合 BP 可达到理想值的 68–80%（互信息准则），

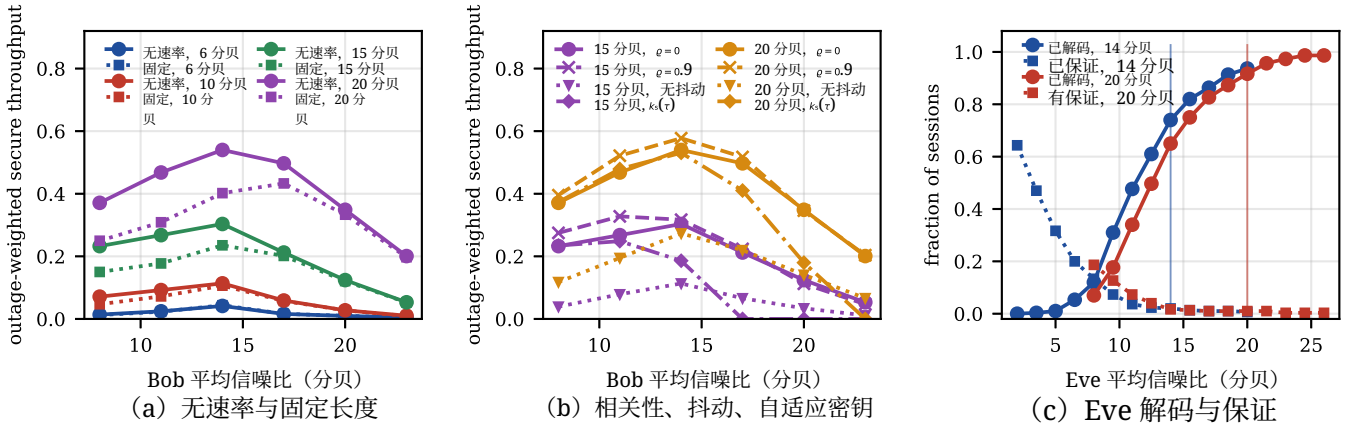

图 1. 块瑞利衰落下的中断加权安全吞吐量，采用抖动传输（$\varepsilon = 10^{-6}$，每个点 300 个会话）。(a) 基于状态的无速率传输（实线）与采用相同编码和界的最佳固定长度传输（虚线）。(b) 相关性 ϱ、无抖动（定理 1(b)），以及 5% 中断率下的密钥长度 $k_s(\tau)$。(c) Eve 的置信传播在所有符号上都恢复格点，且定理 1(a) 保证 256 比特的会话；竖线：Bob 的信噪比。

而有限长界还可进一步达到理想值的 65–87%。采用定理 1(c)的界时，基于 CRC 的确认可进一步缩短$\mathbb{L}[\tau]$（在 14 分贝时从 987 降至 911 维度），并在差距为 20 分贝时，将吞吐量提高 6–9%，最高可达到 17 分贝；在更高信噪比下，其开销（$\log|\mathcal{T}|$、CRC 以及达到上限的泄漏）占据主导地位。对于差距为 20 分贝且 Bob 的信噪比为 8–20 分贝的情况，两种停止规则中表现较好者可达到理想基准的 60–69%（在使用确认信息且信噪比最高为 17 分贝时为 66–69%），在 23 分贝时为 58%；对于差距为 15 分贝的情况，在信噪比最高为 17 分贝时为 54–59%。在最优点处，联合定理 1(a) 行的保密中断概率随信噪比增加而上升：差距为 20 分贝时从 4% 增至 33%，差距为 15 分贝时从 10% 增至 66%；这是因为此时更大的 k_s 值得付出更多的中断代价。

抖动、相关性与自适应密钥。与使用定理 1(b)评估的无抖动传输相比，公开抖动使吞吐量翻倍：在 14 分贝、差距为 20 分贝时，分别为 0.54 和 0.27 比特/维（图 1(b)）。Bob 与 Eve 之间较强的相关性会在中等信噪比下使其略有提升（在 11 分贝时，分别为 0.52 和 0.47），因为 Bob 提前停止的会话也正是 Eve 信道较强的会话。对于采用 $\eta = 5\%$ 和 $\varrho = 0$ 的命题 1（给定 β 后，Λ_θ 的分布仅取决于 $\bar{r}$），我们针对每个停止轮次使用 $m = 4000$ 个校准样本和 $j = 3840$，即在 31 个可能轮次上同时达到 95% 的置信度；在 300 个独立验证会话中，该方案在 8 至 14 分贝的信噪比范围内保持 0.37–0.53 比特/维的吞吐量，在 8 至 20 分贝范围内测得的中断率为 2.0–6.3%，与 5% 的目标相符（标准误差为 1.3 个百分点）。在独立瑞利衰落下，差距不超过 10 分贝时几乎无法保证保密性 [4]。

VIII. 结论

采用公开抖动和隐私放大的无速率格码，能够针对最强的被动对手实现逐状态的有限长度保密性；即使在译码成功时发送确认信息也同样如此，代价是时序延迟，其大小为反馈结果数量的对数。对于采用基于状态的停止策略的退化会话，采用成形无速率格码的自适应密钥生成能够达到累积高斯保密容量，而我们的逆定理证明了该容量就是极限。仿真结果表明，Bob 处的联合解码对于保密性和可靠性同样重要。非退化会话、基于解码的停止策略以及主动对手的逆定理仍有待研究。

参考文献

[1] X. Tang, R. Liu, P. Spasojevi´c, and H. V. Poor, 《高斯块衰落信道安全混合自动重传请求协议的吞吐量》, *IEEE* 信息论汇刊, 第 55 卷, 第 4 期, 第 1575–1591 页, 2009 年。[2] W. Yang, R. F. Schaefer, and H. V. Poor, 《窃听信道：非渐近基本极限》, *IEEE* 信息论汇刊, 第 65 卷, 第 7 期, 第 4069–4093 页, 2019 年。[3] C. Ling, L. Luzzi, J. C. Belfiore, and D. Stehl´e, 《高斯窃听信道的语义安全格编码》, *IEEE* 信息论汇刊, 第 60 卷, 第 10 期, 第 6399–6416 页, 2014 年。[4] M. Bloch, J. Barros, M. R. D. Rodrigues, and S. W. McLaughlin, 《无线信息论安全》, *IEEE* 信息论汇刊, 第 54 卷, 第 6 期, 第 2515–2534 页, 2008 年。[5] Y. Liang, H. V. Poor, and S. Shamai (Shitz), 《衰落信道上的安全通信》, *IEEE* 信息论汇刊, 第 54 卷, 第 6 期, 第 2470–2492 页, 2008 年。[6] P. Sharifi, H. Khodaiemehr, K. Bagheri, and C. Feng, 《无速率限制格：构造、编码定理与容量》, 2026 年, 已投稿至 IEEE 信息论汇刊。[7] ——, 《面向衰落与擦除信道上安全协作式 V2X 广播的无速率嵌套晶格码》, arXiv:2610.02605, 2026 年。[8] M. Bellare, S. Tessaro, and A. Vardy, 《窃听信道的语义安全》, 载于密码学进展 – *CRYPTO 2012*, LNCS 系列, 第 7417 卷, 2012 年, 第 294–311 页。[9] I. Issa, A. B. Wagner, and S. Kamath, 《信息泄漏的操作性方法》, *IEEE* 信息论汇刊, 第 66 卷, 第 3 期, 第 1625–1657 页, 2020 年。[10] Y. Dodis, R. Ostrovsky, L. Reyzin, and A. Smith, 《模糊提取器：如何从生物特征和其他噪声数据中生成强密钥》, *SIAM* 计算杂志, 第 38 卷, 第 1 期, 第 97–139 页, 2008 年。[11] M. Tomamichel, C. Schaffner, A. Smith, and R. Renner, 《针对量子旁信息的剩余哈希》, *IEEE* 信息论汇刊, 第 57 卷, 第 8 期, 第 5524–5535 页, 2011 年。[12] A. Winter, 《量子熵的紧致一致连续性界：条件熵、相对熵距离与能量约束》, 数学物理通讯, 第 347 卷, 第 1 期, 第 291–313 页, 2016 年。[13] M. Hayashi, 《通用随机隐私放大中泄漏信息的指数衰减率》, *IEEE* 信息论汇刊, 第 57 卷, 第 6 期, 第 3989–4001 页, 2011 年。[14] S. K. Leung-Yan-Cheong and M. E. Hellman, 《高斯窃听信道》, *IEEE* 信息论汇刊, 第 24 卷, 第 4 期, 第 451–456 页, 1978 年。[15] W. Hoeffding, 《有界随机变量之和的概率不等式》, 美国统计学会杂志, 第 58 卷, 第 301 期, 第 13–30 页, 1963 年。