以可靠性换取安全性：超可靠低时延通信中机器类通信的泄漏-失败概率最小化

朱尧，袁晓鹏，胡玉林*，Rafael F. Schaefer，Anke Schmeink

arXiv:2303.03880v2 [cs.IT] 8 Mar 2023

摘要——如何在满足超高可靠性和低时延要求的同时提供信息安全，是实现下一代超可靠低时延通信服务（增强型超可靠低时延通信）的主要关注点之一，尤其是在机器类通信中。本文通过定义泄漏失效概率来研究可靠性-安全性权衡，该指标能够联合表征短数据包传输的可靠性和安全性能。我们发现，对于采用有限码长（FBL）码的传输，反直觉地分配较少资源反而能够提升系统性能。为解决联合资源分配的相应优化问题，我们提出了一种优化框架，该框架利用有限码长体制下译码错误概率的下界近似。我们刻画了重构问题的凸性，并建立了一种高效的迭代搜索方法，其收敛性得到了保证。为展示该框架的可扩展性，我们进一步讨论了满足实际可靠安全性能要求的块长分配方案，以及采用统计信道状态信息（信道状态信息）的传输。数值结果验证了所提方法的准确性，并展示了各种设置下的可靠性-安全性权衡。

索引词——有限块长机制、物理层安全、机器类通信、超可靠低时延通信

I. 引言

未来无线网络预计将支持超可靠低时延通信（URLLC），这是许多新兴应用的关键推动因素，例如车对车/车对基础设施通信、增强现实/虚拟现实以及工厂自动化 [1], [2]。这些应用的共同特征之一是时延敏感和任务关键型。鉴于此，超可靠低时延通信中的传输通过有限码长（FBL）编码进行，这类通信也常被称为短数据包通信 [3], [4]。与无限码长这一假设的根本区别在于，在有限码长体制下，即使传输速率低于信道容量，传输错误也不再能够忽略。因此，在超可靠低时延通信的设计框架中，应仔细考虑有限码长编码对可靠性的影响；这要求采用一种与当前无线通信系统中根本不同的方法 [4]。为解决这一问题，文献 [5] 推导了有限码长体制下最大可达传输速率的界限，在此基础上，大量研究致力于提供有限码长设计，例如考虑协作中继网络 [6], 、非正交多址接入（NOMA）方案 [7], 、无线能量传输 [8] 以及绿色通信 [9]。

另一方面，无线媒介的广播特性使信息安全成为未来无线通信系统设计中的另一项关键问题 [10]。当我们将关注重点从以人为中心的通信转向机器类通信时，这一问题变得更加严峻。例如，在物联网（IoT）中，窃听者可能并非外部监听者，而是其他会窃听机密信息的内部物联网设备 [11], [12]。为了解决这一问题，人们已投入大量精力提升安全性能。特别是，与传统的上层加密相比，物理层安全（PLS）凭借实现复杂度低、系统设计灵活等优势，已成为适用于大规模设备机器类通信的一种有前景的解决方案 [13]。事实上，针对非超可靠低时延通信网络的物理层安全已在多种场景中得到广泛研究 [14], , 例如无人机辅助网络 [15], 、认知无线电网络 [16],和可见光通信 [17]。

近年来，面向机器类通信的超可靠低时延通信中的物理层安全也受到了广泛关注。具体而言，作为广泛采用的Wyner保密容量的更一般表达式， [18] 中的作者推导出了有限码长体制下可达保密传输速率的紧界，该界同时考虑了有限码长码和信息泄漏的影响。在采用该界的基础上，研究者提出了各种性能指标。例如， [19] 中的作者采用人工噪声技术，同时实现隐蔽性和安全性。保密传输速率被直接用作待最大化的度量，并提出了一种获得全局最优解的解析方法和一种获得次优解的高效方法。

本研究部分得到中国国家重点研发计划项目（项目编号：2021YFB2900301）的资助；部分得到德国研究联合会（DFG）基础研究项目（项目编号：DFG SCHM 2643/17）的资助；部分得到德国联邦教育与研究部“主权化。数字化。互联化。”计划的资助，包括项目编号为16KISK028的6G-RIC联合项目、项目编号为16KISK001K的6G-Life项目，以及项目编号为16KISK097和16KISK103的6G-ANNA项目。

X.Yuan, Y. Hu 任职于中国武汉大学电子信息学院（中国武汉 430072）以及德国亚琛工业大学信息论与数据分析教席（德国亚琛 52074）。（电子邮箱：$yuan|zhu|hu$@inda.rwth-aachen.de）。R. F. Schaefer 任职于德国德累斯顿工业大学信息论与机器学习教席（德国德累斯顿 01062）（电子邮箱：rafael.schaefer@tu-dresden.de）。A. Schmeink 任职于德国亚琛工业大学信息论与数据分析教席（德国亚琛 52074）（电子邮箱：schmeink@inda.rwth-aachen.de）。*Y. Hu 为通信作者。

在 [20], 中，研究者提出了基于错误概率且给定信息泄漏时的平均可达保密吞吐量，将其作为一种安全度量，并在单天线和多天人物联网场景中将其最小化。 [21],采用并扩展了该度量，将其应用于无人机辅助网络，其中对无人机的轨迹和发射功率进行了优化。另一方面， [22] 中的作者在考虑自干扰和同信道干扰的情况下，推导了全双工多用户系统中的保密吞吐量表达式。此外， [23] 中的作者分析了有限码长体制下安全传输的中断概率，并在此基础上提供了旨在最大化有效吞吐量的优化框架。

然而，上述研究可能忽视了可靠性与安全性之间的相互作用，尤其是在下一代超可靠低时延通信（xURLLC）中的机器类通信场景下，因为可靠性和安全性都是 xURLLC 的关键性能指标。具体而言，采用有限码长编码时，从发射机到合法接收机和窃听者的传输可靠性取决于分配给传输的资源，例如块长或发射功率。如果我们有意减少分配的资源，这意味着合法接收机的可靠性会下降，但信息泄漏概率，即窃听者正确解码保密信息的概率，也会降低。换言之，只要对窃听者造成的损害（即安全性提高）大于对合法接收机造成的损害（即可靠性降低），整体可靠安全性能就能得到改善。因此，我们可以通过反直觉地分配较少资源，以牺牲可靠性来换取安全性。文献 [18]首次探讨了有限码长体制下的安全性与可靠性权衡，以推导可实现的保密传输速率。然而，据我们所知，尚未有研究通过概率度量来表示可靠安全性能，并着重关注机器类通信。具体而言，与以人为中心的通信不同，机器类通信中仅在偶发情况下才会传输固定数量的信息。因此，平均保密速率 [19] 不适合表征这些场景下的系统性能。另一方面，在固定传输错误概率 [23] 下的中断概率，以及在固定信息泄漏概率 [20] 下的有效吞吐量，可能无法充分反映有限码长体制下可靠性与安全性之间的动态关系。

基于上述观察，本文引入一种新颖的度量指标——泄漏失效概率（LFP），用于表示信息未能被合法接收机解码或被窃听者成功解码的可能性。为最小化LFP，我们在经典的三节点场景中构建了一个优化问题，以解决可靠性与安全性之间的基本权衡，其中Eve正在窃听Alice与Bob之间的通信。针对该问题的非凸性，我们提出了一个受主化-最小化 [24] 和逐次凸近似 [25] 算法启发的优化框架来求解该问题。具体而言，我们的贡献可总结如下：

- 为揭示可靠性-安全性权衡下的整体系统性能，我们引入泄漏失效概率，并刻画其在每次传输中的表达式。同时，我们还分析了所提出度量指标与其他众所周知的度量指标之间的关系。
- 我们从分析角度阐述了可靠性与安全性之间的权衡。为解决这一权衡问题，我们构建了一个通用优化问题，通过联合分配块长和发射功率，最小化泄漏失败概率。
- 我们提出了一种优化框架，通过解耦有限块长（FBL）误差概率的乘积并求出其下界近似，来求解所构建的问题。为解决非凸性问题，我们为有限块长（FBL）误差概率提出了一种新颖的近似方法，并刻画了其凸性；与我们先前工作中的结果相比，这是一个更具普适性的结果，见 [26, 定理。 1]。随后，我们提出了一种采用逐次近似的迭代搜索算法，以求解改写后的问题。此外，我们从分析角度保证了该算法的收敛性以及近似的紧致性。随后，我们提出了一种采用逐次近似的迭代搜索算法，以求解改写后的问题。此外，我们从分析角度保证了该算法的收敛性。
- 为展示所提优化框架的可扩展性，我们进一步讨论了在高可靠安全阈值要求下，以及基于统计信道状态信息（CSI）时，块长分配方案的低复杂度求解方法。
- 通过数值仿真，我们验证了分析结果，并评估了所提出方法的性能。该方法能够获得近乎最优的解。为了进一步深入了解资源分配，我们还展示了信道增益、Eve 数量以及分组大小的影响。特别是，我们观察了不同配置下的可靠性-安全性权衡及其潜在应用，这些发现可为机器类型通信中物理层安全的系统设计提供指导。

本文其余部分安排如下。第二节讨论系统模型并刻画相关指标。随后，第三节提出旨在最小化泄漏失效概率的优化框架。接着，第四节探讨其可扩展性。第五节评估所提出的设计，第六节总结全文。

II. 系统模型与泄漏失效概率

A. 系统模型

考虑一个典型的三节点传输系统，其中 Alice 向合法接收机（Bob）传输机密信息，而窃听者（Eve）试图窃听来自 Alice 的合法用户消息。然而，不同于以人为中心的场景，我们考虑机器类通信场景，其中传输仅

偶发地发生，所传递的信息有限但很重要。具体而言，在每个通信轮次（信息到达时）中，Alice 的传输采用有限码长码进行，分组大小固定为 d [比特]，块长为 m [信道使用次数]，其中传输速率$r = \frac{d}{m}$ 的上限为 d [比特/信道使用次数]。不失一般性，假设 Alice 与 Bob 或 Eve 之间的信道经历准静态瑞利衰落，即信道在每次传输持续期间保持不变，并在下一次传输时变化。因此，从 Alice 到 Bob 和 Eve 的信道系数分别表示为 $h_b = \sqrt{\xi_b}\hat{}\, h_b$ 和$h_e = \sqrt{\xi_e}\hat{}\, h_e$，其中 $\sqrt{\xi_b}$ 和 $\sqrt{\xi_e}$ 表示大尺度路径损耗。此外，$\hat{}\, h_b \sim \mathcal{N}(0, 1)$ 和 $\hat{}\, h_e \sim \mathcal{N}(0, 1)$ 表示小尺度衰落，假设它们独立同分布。我们假设设备均配备单天线，且 Alice 可获得 Bob 和 Eve 的完美信道状态信息*。随后，在给定发射功率 p 时，Bob 和 Eve 接收到的信号如下：

$$y_b = \sqrt{p} h_b s + a_b, \tag{1}$$

$$y_e = \sqrt{p} h_e s + a_e, \tag{2}$$

其中，s是发射信号，$a_b \sim \mathcal{CN}(0, \sigma_b^2)$和 $a_e \sim \mathcal{CN}(0, \sigma_e^2)$分别是Bob和Eve处的加性白高斯噪声。因此，信噪比可表示为：

$$\gamma_b = \frac{p|h_b|^2}{\sigma_b^2}, \tag{3}$$

$$\gamma_e = \frac{p|h_e|^2}{\sigma_e^2}. \tag{4}$$

B. 泄漏失效概率（LFP）的表征

由于每个通信轮次传输的数据量有限，保密传输速率或保密中断概率等传统指标，可能无法充分反映所考虑场景下物理层安全的性能。主要原因在于，这些指标侧重于刻画由多个数据包连续传输时的性能。鉴于此，我们引入一种新指标——泄漏失效概率（LFP）ε_{LF}，用于表示单次传输的可靠安全性能。它表示这样一个事件发生的概率：Y 传输的数据包被 Eve 成功译码（即发生泄漏），或被 Bob 错误译码（即合法传输失败）。令 X_b 和 X_e 分别表示 Bob 和 Eve 正确译码的事件。我们有$\varepsilon_{LF} = \mathcal{P}(Y = 1) = \mathcal{P}(X_b = 0 \cup X_e = 1)$。所有可能事件组合的详细情况列于表 I。回顾一下，传输采用块长 m。由于有限块长影响，即使编码速率低于 Bob 和 Eve 各自的香农容量，传输仍可能出错。在 [5], 中，推导出了最大可达传输速率的一个紧界

*我们的系统模型也可以扩展到Alice配备多根天线的情形，此时所提出的框架仍然适用。随后，我们还将讨论Eve配备多根天线且无法获得Eve的完美信道状态信息的情形。

在 AWGN 信道中，给定目标译码错误概率 $\bar{\varepsilon}$ 时：

$$r^* \approx \mathcal{C}(\gamma) - \sqrt{\frac{V(\gamma)}{m}} Q^{-1}(\bar{\varepsilon}), \tag{5}$$

其中，$\mathcal{C}(\gamma) = \log_2(1+\gamma)$是香农容量，$V(\gamma)$是信道色散 [27]。在复AWGN信道中，$V(\gamma) = 1 - (1+\gamma)^{-2}$。此外，$Q^{-1}(x)$是Q函数的逆函数，其中Q函数定义为 $Q(x) = \int_x^\infty \frac{1}{\sqrt{2\pi}} e^{-\frac{t}{2}} dt$。另外，对于任意给定的数据大小，根据式（5），单次传输的（块）错误概率为：

$$\varepsilon = \mathcal{P}(\gamma, \tfrac{d}{m}, m) \approx Q\left(\sqrt{\tfrac{m}{V(\gamma)}}(\mathcal{C}(\gamma) - r)\ln 2\right), \tag{6}$$

其中，$r = \frac{d}{m}$ 为传输速率。因此，Bob 和 Eve 对数据包进行解码时的错误概率分别表示为 $\varepsilon_b = \mathcal{P}(X_b = 0) = Q\left(\sqrt{\frac{m}{V(\gamma_b)}}(\mathcal{C}(\gamma_b) - \frac{d}{m})\ln 2\right)$和 $\varepsilon_e = \mathcal{P}(X_e = 0) = Q\left(\sqrt{\frac{m}{V(\gamma_e)}}(\mathcal{C}(\gamma_e) - \frac{d}{m})\ln 2\right)$。因此，LFP 为：

$$\begin{aligned} \varepsilon_{LF}(\varepsilon_e, \varepsilon_b) &= 1 - \mathcal{P}(Y = 1) = \mathcal{P}(X_b = 0 \cup X_e = 1) \\ &= 1 - (1 - \varepsilon_b)\varepsilon_e = \varepsilon_b \varepsilon_e + (1 - \varepsilon_e). \end{aligned} \tag{7}$$

上述等号链成立，是因为 X_b 和 X_e 是两个独立事件。

C. 泄漏失效概率与其他指标之间的关系

事实上，已有多种指标被提出，用于表征物理层安全（PLS）的可靠安全性能。具体而言，最常见的一些指标如下：

- 保密容量：$\mathcal{C}_s = \mathcal{C}_b - \mathcal{C}_e$ [28], 这是基于块长无穷大这一假设的传统指标。在有限码长体制下，该指标并不准确。
- 最大可达保密速率：$r_s^* = \mathcal{C}_s - \sqrt{\frac{V\gamma_b}{m}} Q^{-1}(\bar{\varepsilon}_b) - \sqrt{\frac{V\gamma_e}{m}} Q^{-1}(\bar{\delta})$ [18], 在给定 Bob 的错误概率和给定的信息泄漏概率 $\bar{\varepsilon}_b$ – $\delta = 1 - \bar{\varepsilon}_e$的情况下，可达保密速率的上界，其中 $\bar{\varepsilon}_e$ 是经典三节点场景中给定的 Eve 错误概率。然而，这可能无法充分体现机器类通信中的信息安全性，因为在这种通信中只有一次传输，且分组大小固定。
- 中断概率：$\mathcal{P}\text{out} = \mathcal{P}(r_s^* \le \frac{r}{m} | \bar{\varepsilon}_b, \bar{\varepsilon}_e)$ [23], 传输速率为 r_s^* 时，违反给定可靠性约束 $\varepsilon_b \ge \bar{\varepsilon}_b$ 或给定安全性约束 $\varepsilon_e \le \bar{\varepsilon}_e$的概率。它刻画了固定约束下的性能，因此无法揭示可靠性与安全性之间的权衡。
- 在给定泄漏约束下的错误概率：$\varepsilon_s = Q\left(\sqrt{\frac{m}{V\gamma_b}}\mathcal{C}_s - \sqrt{\frac{V\gamma_e}{m}} Q^{-1}(1 - \bar{\varepsilon}_e) - \frac{d}{m}\ln 2\right)$ [20], 以及在给定阈值$\bar{\varepsilon}_e$（针对 Eve 的错误概率）时 Bob 的译码错误概率。由于该阈值是给定且固定的，因此泄漏不受块长影响，这一指标可能无法准确地联合表征安全可靠性能。

	$X_e=0$	$X_e=1$
$X_b=1$	安全且可靠	不安全但可靠
$X_b=0$	安全但不可靠	不安全且不可靠

表 I: X_b 和 X_e的事件组合所有可能结果的定义。红色表示非优选结果，其可能性被视为所提出的指标，即泄漏失效概率 ε_{LF}。

与现有指标相比，我们提出的 LFP 考虑了有限块长影响，同时联合表征可靠性和安全性方面的系统性能。此外，它关注单次传输。因此，LFP 适合体现机器类通信的特征，因为这类通信中的传输是间歇性发生的。

请注意，传输的数据包大小 d 是固定的。LFP 也可以解释为传输恰好达到 $r_s^*=\frac{d}{m}$的保密传输速率的可能性。特别地，对于实现 ε_{LF}的 ε_e 和 ε_b 的任意组合，有

$$\begin{aligned}&r_s^*(\varepsilon_b,\varepsilon_e|\varepsilon_{LF})\\=&r_b^*(\varepsilon_b)-r_e^*(\varepsilon_e)\\=&\mathcal{C}(\gamma_b)-\sqrt{\frac{V(\gamma_b)}{m}}Q^{-1}(\varepsilon_b)-\mathcal{C}(\gamma_e)+\sqrt{\frac{V(\gamma_e)}{m}}Q^{-1}(\varepsilon_e)\\=&\mathcal{C}(\gamma_b)-\mathcal{C}(\gamma_e)-\sqrt{\frac{V(\gamma_b)}{m}}Q^{-1}(\varepsilon_b)-\sqrt{\frac{V(\gamma_e)}{m}}Q^{-1}(1-\varepsilon_e)\\=&\mathcal{C}_s-\sqrt{\frac{V(\gamma_b)}{m}}Q^{-1}(\varepsilon_b)-\sqrt{\frac{V(\gamma_e)}{m}}Q^{-1}(\delta).\end{aligned}\tag{8}$$

有趣的是，(8) 与 [18, 式（106）]中的指标——保密传输速率——一致。换言之，尽管二者之间的直接转换似乎难以实现，但 LFP ε_{LF} 与保密传输速率 r_s^* 存在隐式关联。为了更直观地区分这两个指标，我们讨论以下示例：

示例：假设 Alice 与 Bob 之间的信道极佳，$\mathcal{C}(\gamma_b)\to\infty$；而 Alice 与 Eve 之间的信道则受到限制，使得 $\mathcal{C}(\gamma_e)=($ $\mu+1)$，其中 $\frac{1}{m}\leq\mu\leq 1$。在每个通信轮次中，仅需传输一个数据大小为 $d=1$ 比特的数据包，且可用块长足够长，即 $m\to\infty$。因此，我们可以根据 (6) 推导出 Bob 和 Eve 处的错误概率，即 $\varepsilon_b=\varepsilon_e=0$。显然，安全容量为无穷大，且 $\mathcal{C}_s=\mathcal{C}(\gamma_b)-\mathcal{C}(\gamma_e)=\infty$。此外，保密传输速率也为无穷大，即 $r_s^*=\mathcal{C}(\gamma_b)-\mathcal{C}(\gamma_e)$ $\sqrt{\frac{V\ \gamma_b}{m}}Q^{-1}\ \varepsilon_b\ -\sqrt{\frac{V\ \gamma_e}{m}}Q^{-1}\ \delta\ =\infty$ $-$ $()$ $()$。于是，中断概率为零，即 $\mathcal{P}_{out}=\mathcal{P}(r_s^*\leq\frac{d}{m}|\varepsilon_b,\varepsilon_e)=0$。根据中断概率可知，该传输是安全的。对于给定的泄漏约束 $\delta>0$，错误概率也可得出类似结论，即 $\varepsilon_s=Q(\infty)=0$。与此相反，LFP 可表示为 $\varepsilon_{LF}=1-(1-0)\cdot 0=1$，这表明该传输极不安全。事实上，在这种情况下，尽管 Bob 成功解码了信息，Eve 也能获取该信息。换言之，该传输完全不安全。

一方面，这个例子指出了以人为中心的通信与机器类通信在物理层安全性方面的关键区别：在以人为中心的通信中，中断概率的表现反映了安全性的表现；然而，在机器类通信中，由于传输分组大小是固定的，信息安全性已无法再由最大可达传输速率的大小充分体现。

另一方面，我们可以用可靠性换取安全性，因为相对于资源（例如发射功率 p 或块长 m），可靠性和安全性呈相反的相关性。具体而言，以下引理对此给出了分析上的说明。

引理1. ε_b 随块长 m 和发射功率 p单调递减，而 δ 则单调递增。

证明。见附录A。 ■

这表明，即使有足够多的可用资源，反直觉地分配较少的资源也能提升安全性。这是因为较少的资源确实会降低 Bob 处的可靠性，但也会降低 Eve 处的可靠性，从而增强安全性。只要 Bob 处可靠性的降幅小于 Eve 处可靠性的降幅，可靠安全性能就会得到提升。因此，需要仔细研究资源分配，以在可靠性与安全性之间取得平衡，从而提升整体安全可靠性能。

D. 问题表述

鉴于此，我们提出新的指标——泄漏失效概率 ε_{LF}，并研究相应的优化框架，以刻画可靠性与安全性之间的基本权衡。具体而言，我们旨在通过优化分配块长 m 和发射功率 p，最大化安全可靠性。为重点解决可靠性-安全性权衡问题，我们考虑一个最简配置，其中 m 和 p无界，且对可靠性和安全性†的要求不受约束。因此，优化问题可写为：

$$\begin{aligned}\underset{m,p}{\text{minimize}}\quad&\varepsilon_{LF}&\text{(9a)}\\\text{subject to}\quad&p\geq 0,&\text{(9b)}\\&m\in\mathbb{N}_+.&\text{(9c)}\end{aligned}$$

显然，问题（9）是一个整数非凸优化问题，可以通过穷举搜索求解。然而，由于计算复杂度很高，这种方法在实际应用中可能并不实用。因此，在下一节中，我们将提出一种高效的优化框架来求解该优化问题。

†在后续章节中，我们还将研究一种更实际场景下的优化问题，其中资源设有上界，且对可靠性和安全性的个别要求均有限制。

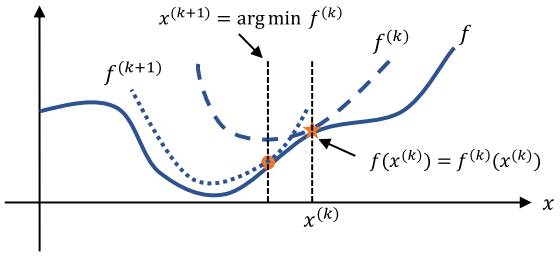

图1：一般函数 $f(x)$的优化框架示例。

III. 优化框架

为求解问题（9），本节提出一种优化框架。该框架的一般思路如下：考虑一个优化问题，目标是在其可行集 $x \in \mathcal{X}$（但不一定是凸集）中最小化一般函数 $f(x)$。在第 k 轮迭代中，我们构造一个有下界的近似函数 $f^{(k)}(x) \geq f(x)$，它关于 x 是凸的。在局部点 $x^{(k)}$ 处两者相等，即 $f^{(k)}(x^{(k)}) = f(x^{(k)})$。我们通过 $x^{(k+1)} = \arg\min f^{(k)}(k)$ 求得 $f_{(k)}$ 的最小值，该点即为下一轮迭代的局部点。随后，在第（$k+1$）轮迭代中，我们构造另一个有下界且为凸的近似函数 $f^{(k+1)}(x) \geq f(x)$，此时满足 $f_{(k+1)}(x^{(k+1)}) = f(x^{(k+1)})$。这一过程不断重复，直至结果收敛。其收敛性由以下不等式链保证：

$$\begin{aligned} f(x^{(k)}) &= f^{(k)}(x^{(k)}) \geq f^{(k)}(x^{(k+1)}) \geq f(x^{(k+1)}) \\ &= f^{(k+1)}(x^{(k+1)}) \geq f^{(k+1)}(x^{(k+2)}) \geq \cdots \end{aligned} \tag{10}$$

图1展示了优化框架的示意图。

A. 有限块长（FBL）误差概率的界

由于 ε_{LF} 涉及 $\varepsilon_b\varepsilon_e$的乘积，这使得进一步进行凸性分析变得困难，因此我们给出以下引理将其解耦：

引理2. 对于任意函数 $f_i(\boldsymbol{x}) > 0, \forall i \in \{1,\ldots,N\}$，其乘积 $\prod_{i=1}^N f_i(\boldsymbol{x})$可由常数 $f_i, \forall i \in \{1,\ldots,N\}$上界，即

$$\prod_{i=1}^N f_i(\boldsymbol{x}) \leq \frac{1}{\prod_{i=1}^N \hat{F}_i} \left(\frac{\sum_{i=1}^N \hat{F}_i f_i(\boldsymbol{x})}{N} \right)^N, \tag{11}$$

^其中 $\hat{F}_i = \frac{f_1}{f_i}, \forall i \in \{1,\ldots,N\}$。

^证明。首先，我们引入 $\hat{F}_i = \frac{f_1}{f_i}$ 来重新整理乘积，即：

$$\prod_{i=1}^N f_i(\boldsymbol{x}) = \frac{\prod_{i=1}^N \hat{F}_i}{\prod_{i=1}^N \hat{F}_i} \prod_{i=1}^N f_i(\boldsymbol{x}) = \frac{1}{\prod_{i=1}^N \hat{F}_i} \prod_{i=1}^N \hat{F}_i f_i(\boldsymbol{x}), \tag{12}$$

其中，$\hat{F}_i f_i(\boldsymbol{x}) \geq 0$ 成立。然后，我们可以针对 $\hat{F}_i f_i(\boldsymbol{x})$ 构造算术平均数与几何平均数不等式：

$$\begin{aligned} &\sqrt[N]{\prod_{i=1}^N \hat{F}_i f_i(\boldsymbol{x})} \leq \frac{\sum_{i=1}^N \hat{F}_i f_i(\boldsymbol{x})}{N} \\ \iff &\prod_{i=1}^N \hat{F}_i f_i(\boldsymbol{x}) \leq \left(\frac{\sum_{i=1}^N \hat{F}_i f_i(\boldsymbol{x})}{N} \right)^N \\ \iff &\frac{1}{\prod_{i=1}^N \hat{F}_i} \prod_{i=1}^N \hat{F}_i f_i(\boldsymbol{x}) \leq \frac{1}{\prod_{i=1}^N \hat{F}_i} \left(\frac{\sum_{i=1}^N \hat{F}_i f_i(\boldsymbol{x})}{N} \right)^N \\ \iff &\prod_{i=1}^N f_i(\boldsymbol{x}) \leq \frac{1}{\prod_{i=1}^N \hat{F}_i} \left(\frac{\sum_{i=1}^N \hat{F}_i f_i(\boldsymbol{x})}{N} \right)^N, \end{aligned} \tag{13}$$

证毕。 ■

^注：当 $f_i(\boldsymbol{x}) = f_i$，即 $\hat{F}_i f_i(\boldsymbol{x}) = F_j f_j(\boldsymbol{x}), \forall i \neq j$ 时，等号成立。该引理可直观地解释如下：对于任意由非负项组成的函数乘积，我们可以将其近似为在给定局部点处取相同项之和，并且在该点处可保证近似精度。

根据引理2，对于给定的资源分配 $(\hat{m}, \hat{p})$，有

$$\begin{aligned} \varepsilon_{LF}(m,p) \leq \frac{\varepsilon_e(\hat{m},\hat{p})}{4\varepsilon_b(\hat{m},\hat{p})} \left(\varepsilon_b(m,p) + \frac{\varepsilon_b(\hat{m},\hat{p})}{\varepsilon_e(\hat{m},\hat{p})} \varepsilon_e(m,p) \right)^2 \\ + (1 - \varepsilon_e(m,p)). \end{aligned} \tag{14}$$

然而，这种近似仍不足以将问题（9）重新表述为凸问题，因为 ε_e 和 ε_b 均为非凸且非凹。为解决这一问题，我们进一步着手重构 Q函数 $Q(\omega)$，其中 $\omega(m,p) = \sqrt{V_{\gamma}^{m}()}(C(\gamma) - \frac{d}{m}) \ln 2$ 是辅助函数。具体而言，我们分别为 Bob 和 Eve 定义 $\omega_e = \sqrt{V_{\gamma_e}^{m}((p))}(C(\gamma_e(p)) - \frac{d}{m}) \ln 2$ 和 $\omega_b = \sqrt{V_{\gamma_b}^{m}((p))}(C(\gamma_b(p)) - \frac{d}{m}) \ln 2$。随后，我们可以建立以下引理：

引理3. 对于给定的 $\hat{\omega} \in \mathcal{R}$，Q函数 $Q(\omega = \int_{\omega}^{\infty} \frac{1}{\sqrt{2\pi}} e^{-\frac{\omega^2}{2}} d\omega$) 有如下界

$$1 - b(-\hat{\omega}) e^{-a(-\hat{\omega})\omega} - c(-\hat{\omega}) \leq Q(\omega) \leq b(\hat{\omega}) e^{-a(\hat{\omega})\omega} + c(\hat{\omega}), \tag{15}$$

其中

$$a(\hat{\omega}) = \max\{ \frac{e^{-\frac{(\hat{\omega})^2}{2}}}{\sqrt{2\pi} Q(\hat{\omega})}, \hat{\omega} \} > 0, \tag{16}$$

$$b(\hat{\omega}) = \frac{1}{\sqrt{2\pi}\hat{a}} e^{\hat{a}\hat{\omega} - \frac{(\hat{\omega})^2}{2}} > 0, \tag{17}$$

$$c(\hat{\omega}) = Q(\hat{\omega}) - \hat{b} e^{-\hat{a}\hat{\omega}}. \tag{18}$$

特别地，当 $\omega = \hat{\omega}$ 时，等号成立。

Proof. See Appendix B. ■

请注意，有限码长 $\varepsilon(m,p)$ 中任意单次传输的译码错误概率是函数的复合

$Q(\omega)$ 和 $\omega(m,p)$，即 $\varepsilon(m,p) = Q(\omega(m,p))$。例如，我们有 $\varepsilon_b = Q(\omega_b(m,p))$ 和 $\varepsilon_e = Q(\omega_e(m,p))$。因此，假设存在一个具有局部点 $(\hat{m},\hat{p})$ 的预定义资源分配，根据引理2和引理3以及 ε_b 和 ε_e 的近似，我们可以推导出 ε_{LF} 的以下近似：

$$\begin{aligned}&\varepsilon_{LF}(m,p)\\ \lesssim&\frac{\varepsilon_e(\hat{m},\hat{p})}{4\varepsilon_b(\hat{m},\hat{p})}\left(\hat{\varepsilon}_b(m,p)+\frac{\varepsilon_b(\hat{m},\hat{p})}{\varepsilon_e(\hat{m},\hat{p})}\hat{\varepsilon}_e(m,p)\right)^2+\hat{\delta}(m,p)\\ \triangleq&\hat{\varepsilon}_{LF}(m,p|\hat{m},\hat{p}),\end{aligned} \tag{19}$$

其中

$$\hat{\varepsilon}_b = b(\hat{\omega})e^{-a(\hat{\omega})\omega_b}+c(\hat{\omega}), \tag{20}$$

$$\hat{\varepsilon}_e = b(\hat{\omega})e^{-a(\hat{\omega})\omega_e}+c(\hat{\omega}), \tag{21}$$

$$\hat{\delta} = b(-\hat{\omega})e^{a(-\hat{\omega})\omega_e}+c(-\hat{\omega}). \tag{22}$$

根据（19），当 $(m_0,p_0) = (\hat{m},\hat{p})$ 时，有 $\varepsilon = \hat{\varepsilon}(m_0,p_0|\hat{m},\hat{p})$；当 $(m_0,p_0) \neq (\hat{m},\hat{p})$ 时，有 $\varepsilon < \hat{\varepsilon}(m_0,p_0|\hat{m},\hat{p})$。换言之，该近似具有下界，且在局部点 $(\hat{m},\hat{p})$ 处取等。

B. 问题重构与凸性刻画

根据引理2和引理3，给定局部点 $(\hat{m},\hat{p})$ 后，问题（9）可重构为：

$$\begin{aligned}\underset{m,p}{\text{minimize}}\quad & \hat{\varepsilon}_{LF}(m,p|\hat{m},\hat{p}) && \text{(23a)}\\ \text{subject to}\quad & p\geq 0, && \text{(23b)}\\ & m\geq 0, && \text{(23c)}\\ & \hat{\varepsilon}_e\leq 1,\ \hat{\varepsilon}_b\leq 1, && \text{(23d)}\end{aligned}$$

其中，附加约束（23d）确保该近似可行，因为错误概率不能超过1。此外，块长 m 从 $m\in\mathbb{N}+$ 放宽为 $m\geq 0$。然后，我们给出以下引理来刻画凸性：

引理4. $\omega(m,p) = \sqrt{V\frac{m}{\gamma^2((p))}}(\mathcal{C}(\gamma(p))-\frac{d}{m})\ln 2$ 关于块长 m 和发射功率 p 是联合凹的，条件是满足以下条件：

$$r\geq\frac{-\Delta_b+\sqrt{\Delta_b^2-4\Delta_a\Delta_c}}{2\Delta_a}, \tag{24}$$

其中

$$\Delta_a = \frac{8+9t}{4t^2}, \tag{25}$$

$$\Delta_b = \frac{t(6t+8)-(3t+8)\mathcal{C}(\gamma)\ln 2}{4t^2\ln 2}, \tag{26}$$

$$\Delta_c = \frac{t\mathcal{C}\ln 2(4-3\ln 2)+t^2(\mathcal{C}\ln 2-1)-4\mathcal{C}^2(\ln 2)^2}{4t^2(\ln 2)^2}, \tag{27}$$

其中 $t=\gamma^2+2\gamma$。

证明。见附录 C。 ■

注释2：尽管类似的分析结果已在 *[26]* 中给出，引理4对联合凸性作出了更一般的刻画，其中 $\gamma\geq 1$ 在 *[26]* 中的条件不再是必要的。这显著提高了其在超可靠低时延通信机器类通信中的适用性，因为无线环境具有动态性，传输的信噪比可能并不总是足够好。此外，尽管条件（24）的表达式直观，但它实际上揭示了传输速率与信噪比之间满足凹性所需的关系。换言之，对于给定的信噪比，可以找到一个凸的传输速率可行范围。从数值上看，当 $r\geq 0.023$ *[比特/信道使用]* 时，该条件成立。事实上，（6）的准确性要求传输速率足够高 *[29]*。在本文余下部分中，我们假设，对于研究区域内的大多数实际有限码长应用，条件（24）都隐含成立。

根据引理4，可以通过复合规则 [30] 直接刻画问题（23）的凸性，如下所示：

推论1. 问题（23）是凸的。

证明. 目标函数 $\hat{\varepsilon}_{LF}$ 是关于 ω_b 和 ω_e 的指数函数之和，且满足 $a\geq 0$。因此，根据（20）、（21）和（22），$\hat{\varepsilon}_{LF}(\omega_b,\omega_e)$ 关于 $\omega_b(m,p)$ 和 $\omega_e(m,p)$ 是凸且递减的，而它们关于变量 m 和 p 均为联合凹，即，$\hat{\varepsilon}_{LF}(\omega_b(m,p)\ \omega_e(m,p))$ 关于 m 和 p 是联合凸的。显然，所有约束均为仿射或凸。因此，问题（23）是凸的。■

因此，可以使用标准凸优化工具高效求解问题（23）。回想一下，$\hat{\varepsilon}_{LF}$ 是实际目标函数 ε_{LF} 的下界近似，其精度仅在 $\omega=\hat{\omega}$ 处得到保证。仅求解一次问题（23）不足以得到原问题（9）的解。

C. 逐次近似迭代搜索

鉴于此，我们提出一种迭代搜索方法，在每次迭代中依次近似目标函数。具体而言，我们首先为第1次迭代初始化参数对 $(m^{(0)},p^{(0)}) = (m_{init},p_{init})$，其中 $m_{init}>0$ 和 $p_{init}>0$。请注意，这些初始参数对也必须满足问题（23）的可行性要求，否则可能会影响收敛速度。然后，在第 k 次迭代中，我们在第 k 个局部点 $(\hat{m},\hat{p}) = (m^{(k)},p^{(k)})$ 处构造问题（23），并据此定义相应的近似 LFP：$\hat{\varepsilon}_{LF}^{(k)}(m,p) = \hat{\varepsilon}_{LF}(m,p|m^{(k)},p^{(k)})$。根据引理4，该问题可以得到最优解。我们将解记为 $(m^{(k)}\text{ opt }p^{(k)}\text{ opt})$，并将其代入（7），得到第 k 次迭代的结果，即 $\varepsilon_{LF}^{(k)}(m^{(k)}\text{ opt }p^{(k)}\text{ opt})$。接下来，我们将 $(m^{(k)}\text{ opt }p^{(k)}\text{ opt})$ 设为下一次迭代的局部点，即 $(m^{(k+1)},p^{(k+1)}) = (m^{(k)}\text{ opt }p^{(k)}\text{ opt})$。重复此过程，直到两次迭代之间的差小于阈值 μ_{th}，且满足 $|\varepsilon_{LF}^{(k)}(m^{(k)}\text{ opt }p^{(k)}\text{ opt}) - \varepsilon_{LF}^{(k+1)}(m^{(k+1)}\text{ opt }p^{(k+1)}\text{ opt})| \leq \mu_{\text{th}}$。然后，我们得到松弛解 $(m_{\mathcal{R}}^*,p^*) = (m^{(k)}\text{ opt }\ m^{(p)}\text{ opt})$。最后，

算法1 求解问题（9）的算法

1：初始化一个可行对（$m^{(0)}$，$p^{(0)}$）和 $k=1$。
2：根据（20）、（21）和（22）构造 $\varepsilon^{(k)}$。
3：根据引理4求解（23），得到（$m^{(k)}$ opt，$m^{(k)}$ opt）。
4: 如果 $|\varepsilon_{LF}^{(k)}(m^{(k)}\text{ opt}\ p^{(k)}\text{ opt})-\varepsilon_{LF}^{(k+1)}(m^{(k+1)}\text{ opt}\ p^{(k+1)}\text{ opt})|\le\mu_{\text{th}}$ 则
5: $(m_{\mathcal{R}}^*, p^*)=(m^{(k)}\text{ opt}\ m^{(k)}\text{ opt})$
6: 否则
7: $(m^{(k+1)}\ p^{(k+1)})=(m^{(k)}_{\text{最优}}\ \ ^{(k)}_{\text{最优}})$ 和 $r=r+1$。
8: 返回步骤 2。
9: 结束 if
10: 获取 $\underset{\text{取最大值}}{\text{the}}$ 整数解 via $m^*=\underset{m\in\{\lfloor m_{\mathcal{R}}^*\rfloor,\lceil m_{\mathcal{R}}^*\rceil\}}{\varepsilon_{LF}(m,p^*)}$

我们通过比较块长 $m^*=\text{argmax}\,\varepsilon_{LF}(m,p^*)$，$m\in\{\lfloor m_{\mathcal{R}}^*\rfloor,\lceil m_{\mathcal{R}}^*\rceil\}$ 的整数邻点来重构解

其中，$\lfloor\cdot\rfloor$ 和 $\lceil\cdot\rceil$ 分别为向下取整函数和向上取整函数。需要强调的是，停止准则基于实际的 LFP，而非其近似。此外，迭代的收敛性可由以下不等式链保证：

$$\begin{aligned}&\varepsilon_{LF}(m^{(k)},p^{(k)})=\hat{\varepsilon}_{LF}^{(k)}(m^{(k)},p^{(k)})\ge\hat{\varepsilon}_{LF}^{(k)}(m_{\text{opt}}^{(k)},p_{\text{opt}}^{(k)})\\ \ge&\varepsilon_{LF}(m^{(k+1)},p^{(k+1)})=\hat{\varepsilon}_{LF}^{(k+1)}(m^{(k+1)},p^{(k+1)})\\ \ge&\hat{\varepsilon}_{LF}^{(k+1)}(m_{\text{opt}}^{(k+1)},p_{\text{opt}}^{(k+1)})\ge\dots\end{aligned}\tag{28}$$

换言之，目标函数值可在迭代过程中不断降低，直至最终收敛到一个次优解。回想一下，ε_{LF} 的近似在局部点处是紧的。因此，由于我们提出的算法总是收敛的，该近似在次优解处的紧性也得到了保证。所得解与全局最优解之间的差距也将在第五节中进行研究。此外，上述算法的伪代码见算法1。由于算法1在每次迭代中求解一个凸优化问题，其复杂度可表示为 $\mathcal{O}(\theta(L)^4)$，其中 θ 为迭代次数，L 为变量数量。

D. 特殊情况：多个 Eve 窃听者

在机器类通信中，Alice 不太可能只向一个目的地发送信息。相反，可能存在多个设备，其中一个设备是合法用户（Bob），其余设备则是潜在的窃听者（Eve 窃听者）。具体而言，考虑一个多节点场景，其中有 N Eve 窃听者，其信道增益为$h_{e,n}$, $\forall n\in\{1,\dots,N\}$。我们研究两类 Eve，即被动 Eve 窃听者和超级 Eve 窃听者。

被动Eve窃听者：在 Alice 与 Bob 进行传输期间，Bob 附近还有其他接收器同时接收广播信号。它们不一定怀有恶意，但仍能窃听机密消息，即作为被动窃听者 [31]。由于有限码长码的影响，每个被动 Eve n 都有可能无法正确解码数据包，该事件$X_{e,n}$ 与其他接收器发生的事件相互独立。令$\varepsilon_{e,n}$ 表示其错误概率，则存在被动Eve窃听者时的 LFP 可改写为：

$$\begin{aligned}\varepsilon_{LF,P}&=1-\mathcal{P}(X_b=1\bigcup_{n=1}^{N}X_{e,n}=1)=1-(1-\varepsilon_b)\prod_{n=1}^{N}\varepsilon_{e,n}\\&=\varepsilon_b\prod_{n=1}^{N}\varepsilon_{e,n}+(1-\prod_{n=1}^{N}\varepsilon_{e,n}),\end{aligned}\tag{29}$$

其中 ε_e $\overline{\gamma_{e\,n}}$ $\gamma_{e\,n}$ $-$ $\gamma_{e\,n}=$，$_n=\mathcal{Q}\left(\sqrt{\frac{p|h_e}{V}}^{m}(,)(\mathcal{C}(,)-\frac{d}{m})\ln 2\right)$ 根据 (6) 得到，$,_{,n}|^2/\sigma_e^2$。由于每个 Eve 窃听者的错误概率相乘后带有负号，即$1-\prod_{n=1}^{N}\varepsilon_{e,n}$，引理2不适用于存在被动 Eve 窃听者时的 LFP，因此无法直接应用上述优化框架。具体而言，引理2要求每个函数 $f_i(\boldsymbol{x})$均为非负数。为解决这一问题，我们通过以下变换对其进行重新表述：

$$\begin{aligned}1-\prod_{n=1}^{N}\varepsilon_{e,n}=&1+(1-\varepsilon_{e,1})\prod_{n=2}^{N}\varepsilon_{e,n}-\prod_{n=2}^{N}\varepsilon_{e,n}\\=&1+(1-\varepsilon_{e,1})\prod_{n=2}^{N}\varepsilon_{e,n}\\&+(1-\varepsilon_{e,2})\prod_{n=3}^{N}\varepsilon_{e,n}-\prod_{n=2}^{N}\varepsilon_{e,n}\\&\dots\\=&\sum_{n=1}^{N}(1-\varepsilon_{e,n})\prod_{i=n+1}^{N+1}\varepsilon_{e,i}.\end{aligned}\tag{30}$$

特别地，为简化符号，我们定义$\varepsilon_{e,N+1}=1$。显然，式（30）中的所有项均为非负，因为始终有$0\le\varepsilon_{e,n}\le 1$，$\forall n\in\{1,\dots,N+1\}$。然后，根据引理2和引理3，我们可以得到以下近似：

$$\varepsilon_{LF,P}\lesssim\hat{\varepsilon}_b\sum_{n=1}^{N}\hat{\varepsilon}_{e,n}+\sum_{n=1}^{N}\hat{\delta}_n\sum_{i=n+1}^{N+1}\hat{\varepsilon}_{e,i},\tag{31}$$

其中 $\hat{}$ $\varepsilon_{e\,n}=b\,\omega\,e^{-a(\hat{\omega})\omega_{e\,n}}+c\,\omega$，$\delta_n=$，$b\,-\omega\,e^{a(-\hat{\omega})\omega_{e\,n}}+c\,-\omega\quad\forall n$ (ˆ), (ˆ) 和 ˆ (ˆ), (ˆ), 。然后，我们采用第三 III-C 节中的方法，将优化问题中的式（14）替换为式（31），以求解存在被动Eve窃听者时的优化问题。为避免重复，这里省略具体细节。

超级窃听者：然而，如果其中一些接收器是恶意的，例如内部攻击者，它们可能会彼此串谋。考虑最坏情况：每个 Eve 都能完美共享其接收信号，因此可以应用最大比合并（MRC） [19], [32]。那么，所有信道增益为 $z_{e,n}$ 的 N串谋窃听者都可以视为一个合并后的超级窃听者，其信道增益为 $z_{e,super}=\sum_{n=1}^{N}z_{e,n}$。因此，可以直接应用第三节中的优化框架。然而，需要强调的是，尽管解析模型简单，与被动

Eve 相比，超级窃听者要难以应对得多；这一点将在第五节中观察并讨论。

IV. 满足可靠安全要求的块长分配

在第二节和第三节中，我们研究了优化问题中的一种最简设置，以揭示可靠性-安全性权衡的基本原理。例如，假设传输的可靠性和安全性不受约束，并且信道状态信息完美。此外，在实际的URLLC系统中，由于电路简单，Alice可能无法进行功率控制，而块长分配则是我们关注的重点。因此，本节重点研究满足可靠安全要求的块长分配，并讨论不同信道状态信息对系统的影响。

A. 问题重构与最优解

考虑与第三节类似的场景：Alice向Bob发送消息，Eve是窃听者。我们的目标仍是通过分配块长 m来最小化 LFP ε_{LF} 。此外，我们还考虑传输具有特定的可靠性和安全性要求：1）传输速率大于Eve的香农容量，从而使URLLC中的信息泄漏概率足够低，即 $\delta \le \delta_{\max} \le 0.5$，其中 $\delta_{\max}$是可容忍的泄漏量；2）传输速率小于Bob的香农容量，从而使URLLC中的可靠性足够高，即$\varepsilon_b \le \varepsilon_{b,\max} \le 0.5$，其中$\varepsilon_{e,\min}$ 是给定的错误概率阈值。于是，优化问题（9）可重写为：

$$\begin{aligned} \underset{m}{\text{minimize}} \quad & \varepsilon_{LF} && \text{(32a)}\\ \text{subject to} \quad & \delta \le \delta_{\max}, && \text{(32b)}\\ & \varepsilon_b \le \varepsilon_{b,\max}, && \text{(32c)}\\ & m \in \mathbb{N}_+. && \text{(32d)} \end{aligned}$$

尽管上一节提出的优化框架也可用于求解问题（32），但本节针对这一特殊情况提出一种复杂度更低的方法。具体而言，我们同样将块长放宽为实数值，即 $m \in \mathbb{N}_+ \to m \in \mathbb{R}_+$。随后，我们不再近似 ε_{LF}，而是基于引理4直接得出以下推论：

引理5. 将块长放宽为 $m \in \mathbb{R}_+$后，问题（32）是凸的。

证明。首先，我们分析 ε_b 和ε_e的凸性/凹性。注意，$\varepsilon_b \le \varepsilon_{b,\max}$ 表示 $\mathcal{C}_b \ge d/m = r$。根据式（57）和凸性复合规则，$\varepsilon_b$ 关于m是凸的，这可证明如下：

$$\frac{\partial^2 \varepsilon_b}{\partial m^2} = \underbrace{\frac{\partial^2 \varepsilon_b}{\partial \omega_b^2}}_{\ge 0}\left(\frac{\partial \omega_b}{\partial m}\right)^2 + \underbrace{\frac{\partial \varepsilon_b}{\partial \omega_b}}_{\le 0}\underbrace{\frac{\partial^2 \omega_b}{\partial m^2}}_{\le 0} \ge 0. \tag{33}$$

这与 [26]中的结果一致。此外，我们可以推导出约束(32c)也是凸的。另一方面，$\varepsilon_b \le \varepsilon_{b,\max}$ 意味着 $\mathcal{C}_b \le d/m = r$。因此，复合规则不能应用于 ε_e。具体而言，其二阶导数为

$$\begin{aligned} \frac{\partial^2 \varepsilon_e}{\partial m^2} =& \frac{\partial^2 \varepsilon_e}{\partial \omega_e^2}\left(\frac{\partial \omega_e}{\partial m}\right)^2 + \frac{\partial \varepsilon_e}{\partial \omega_e}\frac{\partial^2 \omega_e}{\partial m^2}\\ =& \frac{1}{4\sqrt{V_e m^3}}\left((\mathcal{C}_e + r)^2 \omega_e + (\mathcal{C}_e + 3r)\right)\\ \overset{V_e \le 1}{\le}& \frac{1}{4\sqrt{V_e m^3}}\left((\mathcal{C}_e + r)^2\sqrt{m}\underbrace{(\mathcal{C}_e - r)}_{\le 0} + (\mathcal{C}_e + 3r)\right)\\ =& \frac{1}{4\sqrt{V_e m^3}}\underbrace{-r^3 - \mathcal{C}_e r^2 + \left(\frac{3}{m^5} + \mathcal{C}_e^2\right) + \frac{\mathcal{C}_e}{\sqrt{m}} + \mathcal{C}_e^3}_{g(r)}, \end{aligned} \tag{34}$$

其中，$\mathcal{C}_e = \mathcal{C}(\gamma_e)$和 $V_e = V(\gamma_e) = 1 - (1+\gamma_e)^{-2} \le 1$。我们通过求导证明，$h(r)$是关于 $r \ge 0$ 的单调递减函数：

$$\frac{\partial h(r)}{\partial r} = \left(\frac{3}{\sqrt{m^5}} + \mathcal{C}_e^2\right) - 2\mathcal{C}_e r - 3r^2, \tag{35}$$

这是一个开口向下且没有实根的二次多项式函数，因为有 $(2\mathcal{C}_e)^2 - 4\cdot 3\left(\frac{3}{\sqrt{m^5}} + \mathcal{C}_e^2\right) \le 0$。回想一下，$0 \le \mathcal{C}_e \le r$。换言之，如果 $r = 0$，则必然也有 $\mathcal{C}_e = 0$。于是，我们有 $h(r) \le h(0) \le 0$。这意味着

$$\frac{\partial^2 \varepsilon_e}{\partial m^2} = \frac{1}{4\sqrt{V_e m^3}} h(r) \le 0, \tag{36}$$

这意味着 ε_e 在 m 中是凹函数，且约束（32b）是凸的。因此，通过证明下式，我们可以得出目标函数ε_{LF}在 m 中是凸的

$$\begin{aligned} \frac{\partial^2 \varepsilon_{LF}}{\partial m^2} =& \underbrace{\frac{\partial^2 \varepsilon_b}{\partial m^2}}_{\ge 0}\varepsilon_e + \underbrace{\frac{\partial \varepsilon_b}{\partial m}}_{\le 0}\underbrace{\frac{\partial \varepsilon_e}{\partial m}}_{\le 0} + \underbrace{(\varepsilon_b - 1)}_{\le 0}\underbrace{\frac{\partial^2 \varepsilon_e}{\partial m^2}}_{\le 0}\\ \ge& 0. \end{aligned} \tag{37}$$

因此，目标函数和所有约束都是凸的，也就是说，问题（32）是凸的。■

根据引理5，我们可以使用标准凸优化工具高效地求解问题（32）。与算法1相比，该凸问题只需求解一次，既不需要近似，也不需要迭代。此外，所得解可保证为全局最优解。然而，我们应强调，引理5仅适用于具有可靠安全要求的块长分配，其适用范围不如第三节所考虑的问题广泛。

此外，还值得一提的是，这些分析结果可应用于其他目标函数。例如，我们还可以最大化保密有效吞吐量，其定义为 $\tau_{LF} = \frac{d}{m}(1 - \varepsilon_{LF})$‡。那么，我们有如下

‡需要强调的是，保密有效吞吐量与 [23]，中基于中断概率的保密有效吞吐量不同，也与 [20]，中基于固定泄漏概率的保密有效吞吐量不同。

以下修改后的问题:

$$\begin{aligned} \underset{m}{\text{maximize}} \quad & \tau_{LF} \\ \text{subject to} \quad & \text{(32b), (32c) and (32d).} \end{aligned} \tag{38a}$$

我们有如下推论来对其进行表征:

推论2。问题（38）是准凹的。

证明。我们已在引理5中证明， ε_{LF} 是一个凸函数。此外，显然 $1/m$ 为正且为凸函数。这意味着 $\tau_{LF} = d\frac{1-\varepsilon_{LF}}{m}$可视为一个凹函数除以一个正的凸函数，因此是准凹的 [30]。 ■

因此，问题（38）存在唯一的局部最优解，该解也就是全局最优解。这意味着问题（38）可以高效求解，例如采用贪心搜索。对于多次传输的情况，也可以得出类似结论。对于总计T 次传输，有效保密吞吐量为$\tau = \frac{1}{T}\sum_{t=1}^{T} d_{(t)}\, m_{(t)}\,(1-\varepsilon(t))$，其中 $d(t)$是第 t次传输时的数据包大小， $\forall t \in \{1,\ldots,\cancel{T}\}$。换言之，由于每次传输彼此独立， τ_{LF} 可以近似为下界凹函数$\hat{}\tau_{LF}$之和。

B. Eve 的统计信道状态信息讨论

在前面的章节中，我们假设已知 Eve 的完美信道状态信息。然而，在实际应用中，我们可能只知道统计信道状态信息。具体而言，令 $z_e = |h_e|^2$ 表示 Eve 的信道增益， $f_Z(z_e)$ 表示相应的概率密度函数（PDF），则基于统计信道状态信息的（期望）泄漏失败概率 $\mathbb{E}_z[\varepsilon_{LF}]$ 可改写为:

$$\mathbb{E}_z[\varepsilon_{LF}] = \int_0^{\infty} \varepsilon_{LF}(m,p|z_e) f_Z(z_e) dz_e. \tag{39}$$

类似地，Eve 的错误概率为 $\mathbb{E}_z[\varepsilon_e] = \int_0^{\infty} \varepsilon_e(m,p|z_e) f_Z(z_e)\, dz_e$。2.4-3 积分形式不会影响第三节中问题 (9) 的优化框架的有效性，因为式 (19) 中近似 LFP $\hat{}\varepsilon_{LF}$ 的凸性与 z_e 无关。于是，$\mathbb{E}_z[\hat{}\varepsilon_{LF}]$ 可视为凸函数的连续和，因此，对于任意给定的常数 ($\hat{}m, \hat{}p$)，我们仍可用 $\mathbb{E}_z[\hat{}\varepsilon_{LF}]$ 近似 $\mathbb{E}_z[\varepsilon_{LF}]$，而不影响其凸性。然而，需要重新审视引理 5 的有效性，因为 ε_e 的凸性/凹性仅在 z_e 的某个可行范围内成立。这是由于式 (6) 中的 Q函数 $Q(\omega)$ 是一个函数，其凸凹性会随 ω 而变化，先凸后凹。为解决这一问题，我们沿用先前工作的思路 [26]，通过以下推论建立基于统计信道状态信息的 $\mathbb{E}_z[\varepsilon_{LF}]$ 的凸性:

推论3. $\mathbb{E}_z[\varepsilon_{LF}]$ 关于块长度 m 的凸性在 Eve 的统计信道状态信息下成立。

证明. $\mathbb{E}_z[\varepsilon_{LF}]$ 的二阶导数为

$$\frac{\partial^2 \mathbb{E}_z[\varepsilon_{LF}]}{\partial m^2} = \underbrace{\frac{\partial^2 \varepsilon_b}{\partial m^2}}_{\geq 0} \mathbb{E}_z[\varepsilon_e] + \underbrace{\frac{\partial \varepsilon_b}{\partial m}}_{\leq 0} \underbrace{\frac{\partial \mathbb{E}_z[\varepsilon_e]}{\partial m}}_{\leq 0} + \underbrace{(\varepsilon_b - 1)}_{\leq 0} \frac{\partial^2 \mathbb{E}_z[\varepsilon_e]}{\partial m^2} \tag{40}$$

显然可以证明， $\mathbb{E}_z[\varepsilon_e]$ 关于m单调递减，即 $\frac{\partial \mathbb{E}_z[\varepsilon_e]}{\partial m} \leq 0$，因为无论$z_e$如何， ε_e 都关于 m 递减。因此，我们重点确定 $\mathbb{E}_z[\varepsilon_e]$ 关于 m是否仍为凹函数。具体而言，令 $\bar{z}_e$ 表示 Eve 的平均信道增益， $\bar{z}_{\text{th}}$ 为一个阈值，使得传输速率恰好高于瞬时香农容量。回顾可知，存在一个约束，使得 $\mathbb{E}_z[\varepsilon_e] \geq \varepsilon_{e,\min} \geq 0.5$。必须满足 $\bar{z}_e \leq \bar{z}_{\text{th}}$。否则，该约束将无法满足。因此，我们有

$$\begin{aligned} \frac{\partial^2 \mathbb{E}[\varepsilon_e]}{\partial m^2} = & \underbrace{\int_0^{\bar{z}_e} \frac{\partial^2 \varepsilon}{\partial x^2} f_Z(z_e) dz_e}_{\leq 0} + \underbrace{\int_{\bar{z}_e}^{\bar{z}_{\text{th}}} \frac{\partial^2 \varepsilon}{\partial x^2} f_Z(z_e) dz_e}_{\leq 0} \\ & + \underbrace{\int_{\bar{z}_{\text{th}}}^{\infty} \frac{\partial^2 \varepsilon_e}{\partial x^2} f_Z(z_e) dz}_{\geq 0}. \end{aligned} \tag{41}$$

此外，由于 $\bar{z}_e$ 是平均信道增益，累积分布函数（CDF）可以分解如下

$$\begin{aligned} \int_0^{\bar{z}_{\text{th}}} f_Z(z_e) dz_e \geq \int_0^{\bar{z}_e} f_Z(z_e) dz_e = \int_{\bar{z}_e}^{\infty} f_Z(z_e) dz_e = \frac{1}{2} \\ \geq \int_{\bar{z}_{\text{th}}}^{\infty} f_Z(z_e) dz_e. \end{aligned} \tag{42}$$

因此，我们有

$$\begin{aligned} & \left| \int_0^{\bar{z}_{\text{th}}} \frac{\partial^2 \varepsilon_e}{\partial m^2} dz_e \right| \geq \left| \int_{\bar{z}_{\text{th}}}^{\infty} \frac{\partial^2 \varepsilon_e}{\partial m^2} dz_e \right| \\ \iff & \left| \int_0^{\bar{z}_{\text{th}}} \frac{\partial^2 \varepsilon_e}{\partial m^2} f_Z(z_e) dz_e \right| \geq \left| \int_{\bar{z}_{\text{th}}}^{\infty} \frac{\partial^2 \varepsilon_e}{\partial m^2} f_Z(z_e) dz_e \right|, \end{aligned} \tag{43}$$

这意味着 $\frac{\partial^2 \mathbb{E}[\varepsilon_e]}{\partial m^2} \leq 0$。因此， $\mathbb{E}[\varepsilon_e]$ 关于 m确实是凹函数，即 $\mathbb{E}[\varepsilon_{LF}]$ 关于 m是凸函数。 ■

根据推论3，具有 Eve 的统计信道状态信息的 问题（32）是凸的。需要注意的是，推论3的有效性不取决于 z_e 的分布，即只要 z_e 的平均值低于阈值 $\bar{z}_e$， $f_Z(z_e)$ 即可。因此，推论3也适用于 Eve 配备多根天线的情况。在这种情况下，只有 z_e 的分布会发生变化，并且它服从伽马分布 [23]。对于不完美信道状态信息，也可以得出相同的结论。此外，虽然本文重点关注单次传输的性能，但推论3实际上表明，我们可以将系统模型扩展到具有固定分组大小 d 的多次传输。具体而言，设 $t = \{1,\ldots,T\}$ 为总共 T 次传输的索引。由于满足时分共享条件 [33], [34]，因此有 $\mathbb{E}_t[\varepsilon_{LF}] = \mathbb{E}_z[\varepsilon_{LF}]$。由此可得，无论信道状态信息如何，也无论传输次数多少，我们此前的所有分析结果仍然成立。

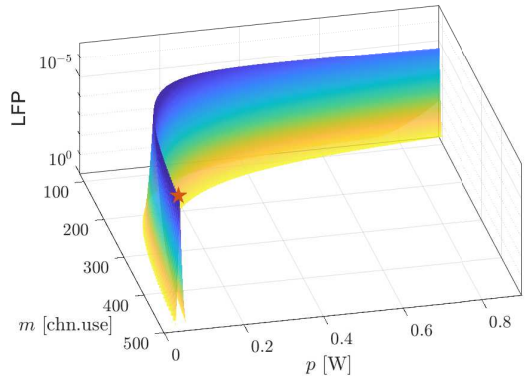

图2：LFP ε_{LF} 随块长 m 和发射功率 p的变化。为清晰起见，省略了 $\varepsilon_{LF} \geq 0.5$ 的点。标记表示 ε_{LF}的最小值。此外，z轴方向反转。

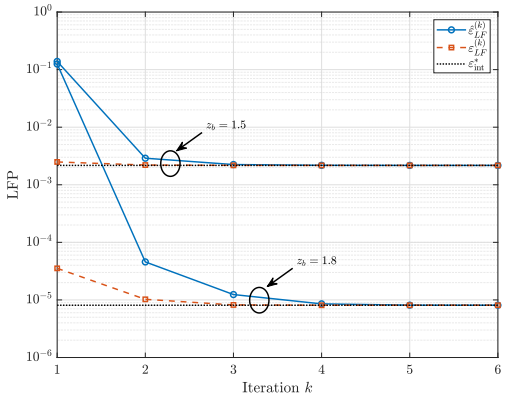

图3：在 Bob 的不同信噪比 $z_b = \{1.5, 1.8\}$ 下，实际 LFP $\varepsilon_{LF}^{(k)}$ 和根据算法1得到的近似值$\hat{\varepsilon}_{LF}^{(k)}$ 随迭代次数 k 的变化。此外，还展示了通过整数规划得到的全局最优结果ε_{int}^{*}作为基准。

V. 仿真结果

本节通过数值仿真验证分析结果，并研究所考虑场景下的系统性能。除非另有说明，仿真采用以下设置：我们考虑一个归一化场景，其中 Bob 的信道增益设为 $z_b = |h_b|^2 = 1.5$，Eve 的信道增益设为 $z_e = |h_e|^2 = 1$。噪声功率水平设为 $\sigma_e^2 = \sigma_b^2 = 0.1$。传输分组大小 d 为 320 比特。此外，可用块长和发射功率分别设为足够大的 3000 次信道使用和 10 W。求解问题（9）的整数规划结果作为基准，该结果给出了全局最优解。

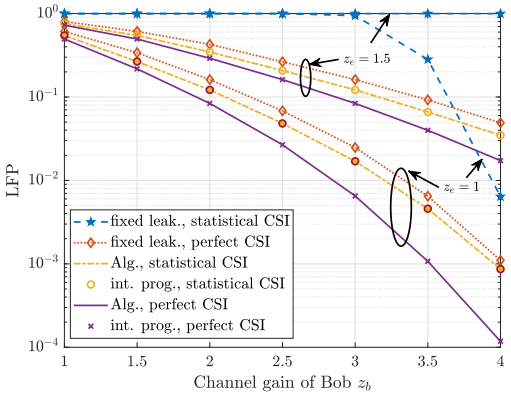

图4：在 Eve 的不同信道增益 z_e下，最小化的 LFP ε_{LF}^{*} 随 Bob 的信道增益 z_b 的变化。图中展示了完美信道状态信息和不完美信道状态信息两种情况。线条表示通过我们提出的算法1得到的解，标记则表示通过整数规划得到的解。此外，还展示了泄漏阈值固定为 $\delta \leq 0.001$ 时的 LFP 性能作为基准。

首先，我们在图2中展示LFP与其变量之间的关系。具体而言，我们以对数刻度绘制LFP ε_{LF} 的取值，并反向显示，同时给出相应的发射功率 p 和块长 m。为清晰起见，我们省略了 $\varepsilon_{LF} \geq 0.5$的点。事实上，根据（7），如果 $\varepsilon_{LF} \geq 0.5$，则意味着Bob的译码错误概率 $\varepsilon_b \geq 0.5$ 或Eve的错误概率 $\varepsilon_e \leq 0.5$，也就是说，传输要么不可靠，要么不安全。正如预期的那样， ε_{LF} 是非凸的。这意味着标准凸方法不足以求解涉及 ε_{LF}的优化问题。这促使我们研究更高效的优化框架。另一方面，在实际的泄漏与错误概率阈值下（对应问题（32）），ε_{LF} 关于块长 m确实是部分凸的。这一现象证实了引理5中的分析结果。然而，需要指出的是，这一结论不能直接推广到对 m 和 p的联合优化。这是因为满足 $\varepsilon_b \leq \varepsilon_{b,\max}$ 和 $\varepsilon_e \leq \varepsilon_{e,\min}$的可行集（这些正是我们在第四节A部分讨论的可靠安全要求）实际上是非凸的。因此，有必要考察我们所提出优化框架的效率，以及与最优解相比的性能差距；图3中以红色标出了最优解。

在图 3 中，我们展示了每次第 k 次迭代所得的 LFP。为了说明所提出的优化框架的收敛性能，我们绘制了通过求解凸问题（23）得到的近似 LFP $\hat{\varepsilon}_{LF}^{(k)}$，以及基于（7）得到的实际 LFP $\varepsilon_{LF}^{(k)}$。此外，我们还展示了通过整数规划得到的最优值 ε_{int}^{*}，作为基准。可以观察到，初始几轮中的 $\hat{\varepsilon}_{LF}^{(k)}$ 与实际最优值相差甚远，因为它必须保证是实际 LFP 的下界。然而，我们提出的优化框架以次线性速率快速收敛。此外，在收敛点处可确保近似值的紧致性，而 $\varepsilon_{LF}^{(k)}$ 则达到全局最优结果ε_{int}^{*}。需要指出的是，收敛性和最优性不受配置影响。例如，将 Bob 的信道增益 z_b 从 1.5 调整为 1.8，尽管 LFP 的取值有所不同，但两种迭代都几乎在相同轮次收敛，并得到（近乎）最优解。

接下来，我们进一步验证所提方法在不同设置下的性能。图4绘出了最小化后的LFP ε_{LF}^{*} Bob的信道增益 z_b 在不同

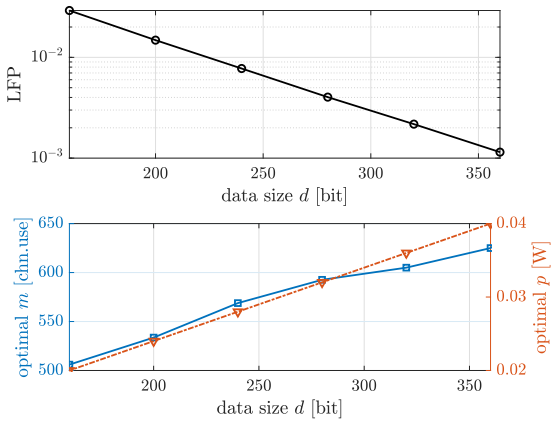

图5：最小化的LFP ε_{LF}^{*} 与数据大小 d 的关系，同时展示块长 m^{*} 和发射功率 p^{*} 的最优解。

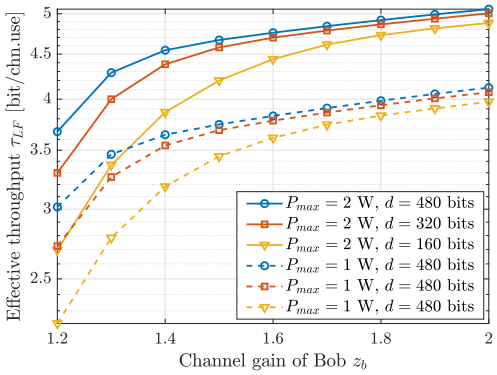

图6：在不同最大发射功率 $P_{\max}=\{1,2\}$ W以及数据大小 $d=\{480,320,160\}$ 比特条件下，有效吞吐量 τ_{LF}^{*} 与Bob的信道增益 z_b 的关系。

Eve的信道增益下的表现，其中展示了完美信道状态信息和统计信道状态信息两种情况下的性能，信道实现次数设为5000。此外，还展示了通过整数规划（标记为 int. prog.）以及固定泄漏阈值 $\delta \leq 0.001$ （标记为 fixed leak.）得到的最小化LFP，作为性能基准。需要指出的是，固定泄漏阈值来最小化LFP，等价于最小化Bob的错误概率。因此，与算法1相比，根据引理4可以更高效地求解该优化问题。不过，其与最优结果之间的性能差距也相当显著。显然，随着 z_b增加，ε_{LF}^{*} 会降低。这不仅是因为 z_b 与 z_e 之间更大的差距会带来更高的保密容量$\mathcal{C}_s = \mathcal{C}(z_b) - \mathcal{C}(z_e)$，也得益于可靠性与安全性之间更显著的权衡。换言之，通过减少分配给传输的各项资源，我们可以更大幅度地提高 ε_e ，即增强安全性，而 ε_b仅略有下降，即可靠性损失较小。这一观察结果表明，我们应据此谨慎分配可用资源。更重要的是，无论信道状态信息设置如何，与前一幅图中的结果相似，所提算法的性能都接近整数规划的性能。这些结果也证实了第四节B中的分析结论，即无论信道知识如何，优化框架和LFP的部分凸性均成立。因此，为清晰起见，后续图中我们仅展示所提算法得到的结果。

根据 (6)， ε_e 和 ε_b 也会受到传输 d 分组大小的显著影响，且变化趋势相似。在图 5 中，我们绘制最小化 LFP 随数据大小 d的变化曲线，以展示 d 对系统性能的影响。为了进一步了解资源分配方案，我们还绘制了达到最小化 LFP 时的块长 m 和发射功率 p 。有趣的是，图中显示，增大数据大小 d 实际上可以改善系统的可靠安全性能。尽管这一现象似乎有违直觉，但实际上符合我们在本文中强调的以可靠性换取安全性这一理念——性。具体而言，当 Bob 的信道增益优于 Eve 的信道增益，即 $z_b \geq z_e$时，如图 5 下方子图所示，如果可用资源充足，则可以通过分配更多无线资源来弥补对译码错误概率的不利影响。然而，由于 Eve 的信道增益较差，这种补偿对 Eve 的作用较小。因此，较大的 d需要更多补偿，进而导致 Bob 与 Eve 在译码错误概率方面的性能差距扩大。因此，增大 d会使最小化的 ε_{LF} 下降。需要指出的是，这一现象应视为数值观察结果，而非为实际资源分配方案提供指导。首先，机器类通信中的分组大小是固定的，因为信息量是确定的。一种可能的解决方案是结合其他技术，但这会增加实现复杂度，例如采用先进的编码方案或重传方案来提高冗余度。此外，在实际系统中，可用资源有限。要获得最优解，更大的分组大小需要更多资源，这可能不可行。

接下来，我们以有效吞吐量 τ_{LF} 为指标，研究系统性能。在图6中，我们绘制了最大化有效吞吐量 τ_{LF}^{*}随 Bob 的信道增益 z_b变化的曲线。为了展示可用资源对 τ_{LF}^{*} 的影响与其对 LFPε_{LF}^{*}的影响有何不同，我们还改变了最大可用发射功率$P_{\max}=\{1,2\}$ W 和分组大小 $d=\{480,320,160\}$ 比特。与 LFP 性能类似，增加 z_b 也能提升 τ_{LF}^{*}。然而，当 z_b 足够好时，这种提升就不那么显著了。这是因为，当（$1-\varepsilon_{LF}$）趋近于 1 时，进一步提升 z_b 对 $\tau_{LF}^{*} = d/m\,(1-\varepsilon_{LF})$ 的增量贡献很小，因为此时它受 d/m 主导。因此，为了提高 τ_{LF}，系统倾向于选择更高的发射功率 p 和更短的块长 m。比较 τ_{LF}^{*} 与 $P_{\max}=1$ W 和 $P_{\max}=2$ W 的结果可以验证这一点。这也意味着，与 z_e相比，当 z_b 足够好时，系统对分组大小 d 变化的敏感度也较低。在这种情况下，系统总能以可靠性换取安全性，即 Bob 侧的损失较小，而 Eve 侧的损失较大。

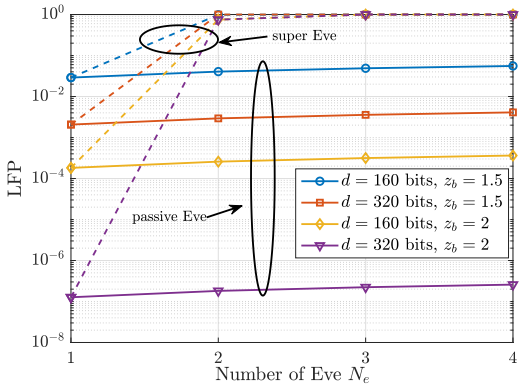

图 7：最小化的 LFP ε_{LF}^* 与网络中的 Eve 数量N的关系，$d = \{160, 320\}$ [比特], 数据大小不同，且 Bob 的信道增益为 $z_b = \{1.5, 2\}$。同时考虑被动窃听者和超级窃听者。

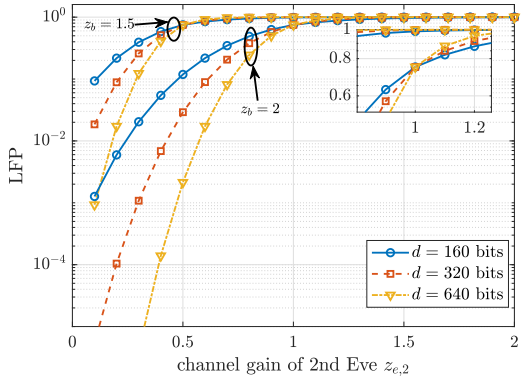

图 8：两个超级窃听者情况下最小化的 LFP ε_{LF}与第二个 Eve 的信道增益 $z_{e,\ 2}$ 的关系，其中第一个 Eve 的信道增益 $z_{e,\ 1}$=1 保持固定。此外，还改变 Bob 的信道增益 $z_b = \{1.5, 2\}$以及分组大小 $d = \{160, 320, 640\}$ 比特。

在图7中，我们通过绘制不同设置下最小化的 LFP ε_{LF}^* 随网络中 Eve 的数量 N 变化的曲线，展示不同类型的 Eve 对系统的影响，其中设置包括 d ={160, 320} 比特和 $z_b = \{1.5, 2\}$。具体而言，我们设定 $z_{e,\ 1} = \ldots = z_{e,\ N} = 1$。尽管 N 增加会导致两种类型的 Eve 对应的 ε_{LF}^* 都增加，但它们对系统性能的影响截然不同。一方面，对于被动窃听者，我们可以用 Bob 的损失换取每个 Eve 的损失；其中，各 Eve 的损失影响与 $\prod_{n=1}^{N} \varepsilon_{e,\ n}$呈乘法关系。因此，当 $\varepsilon_{e,\ n}^*$ 趋近于 1 时， N 的作用就不那么显著了。换言之，存在被动窃听者时，系统性能由信道增益更好的 Eve 主导，而 N 的不利影响可以通过牺牲少量可靠性性能来抵消。因此，可容忍的 N 取决于信道增益最佳的 Eve。另一方面，对于超级窃听者，系统中每增加一个 Eve，超级窃听者的信道增益就会以加和的方式提高。可靠性-安全性权衡无法应对这一点，因为当 N较高时，超级窃听者的损失甚至可能小于 Bob 的损失。事实上，可容忍的 N 很大程度上取决于 Bob 的信道增益 z_b 与 Eve 的信道增益之和 $\sum_{n=1}^{N} z_{e,\ n}$之间的实际差距。

为了研究超级窃听者场景下的系统性能，我们考虑一个包含两名 Eve 的一般场景，其中一名 Eve 的信道增益固定为 $z_{e,\ 1} = 1$ 而第二名 Eve 的信道增益 $z_{e,\ 2}$ 则会变化。图 8 展示了在此场景下，针对不同分组大小设置 $d = \{160, 320, 640\}$ 比特和 Bob 的信道增益 $z_b = \{1.5, 2\}$，最小化后的 LFP ε_{LF}^*。正如预期的那样，无论采用何种设置，$z_{e,\ 2}$ 的增加都会导致性能显著下降，即 ε_{LF}^* 升高。与图 5 类似，我们可以观察到，通常增大 d 有利于传输，但代价是消耗更多资源。当 z_b 升高时，这一优势会更加明显。不过，这一结论是在 z_b 足够好、使得 $z_b \geq \sum_{n=1}^{N} z_{e,\ n}$ 的条件下得出的。若不满足这一条件，该优势便会转为劣势，此时可靠性-安全性权衡不再有利于 Bob（如图 8 的局部放大图所示）。在这些情况下，增大 d 意味着可靠安全性能的损失。因此，系统抵御超级窃听者的鲁棒性下界为 z_b；对于机器类型通信中的广播信道而言，这一下界通常难以提升。这一观察也表明，其他信号增强技术（例如波束成形技术或非正交多址方案）十分重要。

VI. 结论

在本研究中，我们探讨了如何通过有限码块长度区间内的资源分配方案，提升机器类通信的可靠安全性能。为更准确地刻画以可靠性换取安全性的概念，我们定义了泄漏失效概率这一指标，用以综合考虑信息泄漏概率和译码错误概率。我们展示了该指标与传统保密传输速率之间的关系。有趣的是，我们发现，反直觉地为短分组传输分配较少资源，反而能够提升可靠安全性能。基于这一发现，我们构建了相应的优化问题，并提出了优化框架。具体而言，我们针对有限码长编码的译码错误概率提出了下界近似。随后，我们证明了这些近似关于块长和发射功率具有联合凸性，而且这一结论也适用于原始错误概率表达式。基于这些分析结果，我们提出了一种迭代搜索算法来求解该优化问题，结果表明该算法能够获得近乎最优的解。为强调该优化框架的可扩展性，我们进一步讨论了其在其他实际场景中的应用，包括存在多个窃听者的网络，以及在假设可靠安全阈值较高时进行的块长分配。通过数值仿真，我们验证了所提方法的性能，展示了可靠性与安全性之间的权衡，并说明了信道增益、数据大小和窃听者数量对系统的影响。

最后，我们希望强调以可靠性换取安全性这一概念以及所提出的泄漏失效概率具有普适性。尽管我们是在经典的三节点设置下讨论这一概念，但它同样适用于其他设置，包括多天线、多址接入以及多功能网络。通过采用相应的设置并结合其他实际约束（例如资源预算、对可靠性或安全性的个体要求），泄漏失效概率也可用于刻画可靠安全性能。

附录A 引理1的证明

证明。定义辅助函数 ω，其中 $\omega(m,p) = \sqrt{V^{m}}\gamma()(\mathcal{C}($ $= \int_{\omega}^{\infty} \frac{1}{\sqrt{2\pi}} e^{-\frac{t^2}{2}} dt$ $\omega \quad \frac{\partial\varepsilon}{\partial\omega} \leq 0)-\frac{d}{m})$

$\ln 2$。显然可知，$Q(\,)$ 关于 单调递减，即 。然后，关于 m的单调性显而易见，可通过导数检验证明，即

$$\frac{\partial\varepsilon}{\partial m} = \frac{\partial\varepsilon}{\partial\omega}\frac{\ln 2}{2} m^{-\frac{1}{2}} V^{-\frac{1}{2}} (\mathcal{C} + m^{-1} d) \leq 0, \tag{44}$$

ε 关于p 的偏导数为

$$\begin{aligned}\frac{\partial\varepsilon}{\partial p} =& \frac{\partial\varepsilon}{\partial\omega}\frac{\partial\omega}{\partial\gamma}\frac{\partial\gamma}{\partial p} \\ =& \underbrace{|h|^2 \frac{m^{\frac{1}{2}} V^{-\frac{1}{2}}}{\sigma^2 (\gamma^2+2\gamma)(\gamma+1)}}_{\geq 0} \underbrace{\left(\gamma^2 + 2\gamma - \ln(\gamma+1)\right)}_{\Delta_1} \\ &+ \underbrace{m^{-\frac{1}{2}} V^{-\frac{3}{2}} d \ln 2 \frac{1}{(1+\gamma)^3}}_{\geq 0},\end{aligned} \tag{45}$$

其中，$\Delta_1(\gamma) = \gamma^2 + 2\gamma - \ln(\gamma+1)$ 是关于 γ的辅助函数。根据(45)，若 Δ_1 非负，则有 $\frac{\partial w}{\partial\gamma} \geq 0$。这可通过证明 Δ_1 关于 $\gamma > 0$ $\frac{\partial\Delta_1}{\partial\gamma} = 2\gamma + 2 - \frac{1}{\gamma+1} \geq$ 单调 0 递增来得出，即

$$\Delta_1(\gamma) \geq \Delta_1(0) = 0. \tag{46}$$

因此，ε 也随 p单调递减。由此可知，$\delta = 1 - \varepsilon$ 的单调性相反，即其随 m 和 p递增。■

附录B 引理3的证明

证明。我们首先定义函数 $g(\omega)$和 $h(\omega)$:

$$g(\omega) = Q(\omega) - b(\hat{\omega}) e^{-a(\hat{\omega})\omega} - c(\hat{\omega}), \tag{47}$$

$$h(\omega) = Q(\omega) - 1 + b(-\hat{\omega}) e^{-a(-\hat{\omega})\omega} + c(-\hat{\omega}). \tag{48}$$

回顾一下，$\hat{}\omega$是一个常数，而$\omega(m,P) = \sqrt{V^{m}}\gamma()(\mathcal{C}(\gamma) - \frac{d}{m})$ $\ln 2$是关于块长 m和发射功率 p的辅助函数。因此，只需证明 $g(\omega) \leq 0$ 和 $h(\omega) \leq 0$ 成立，即可证明引理3。

对于任意 m 和 p，即任意 ω。特别地，$g(\omega)$关于 ω 的导数为

$$\begin{aligned}\frac{\partial g}{\partial\omega} &= -\frac{1}{\sqrt{2\pi}} e^{-\frac{\omega^2}{2}} + abe^{-a\omega} \\ &= \frac{1}{\sqrt{2\pi}} \left(e^{a\hat{\omega} - \frac{\hat{\omega}^2}{2} - a\omega} - e^{-\frac{\omega^2}{2}} \right).\end{aligned} \tag{49}$$

容易证明，指数函数 e^x 关于 x是单调递增函数。因此，由于$\frac{\partial g}{\partial\omega}$ 是两个指数函数之和，有

$$\text{sign}(\frac{\partial g}{\partial\omega}) = \text{sign}(g_{\text{sgn}}(\omega)), \tag{50}$$

其中，$g_{\text{sgn}}(\omega) = \frac{\omega^2}{2} - a\omega + (a\hat{}\omega - \cdot\frac{\omega^2}{2})$，且sign(·)为符号函数，其

$$\text{sign}(x) = \begin{cases} 1, & \text{if } x > 0, \\ 0, & \text{if } x = 0, \\ -1, & \text{if } x < 0. \end{cases} \tag{51}$$

由于$g_{\text{sgn}}(\omega)$关于 ω 是二次多项式函数，且 $a(\omega) \geq 0$，因此存在两个根，可写为 $\omega_1 = \hat{}\omega$和 $\omega_2 = 2(a - \hat{}\omega)$，使得根据式(16)有 $\omega_2 - \omega_1 = 2a - 2\hat{}\omega \geq 0$。因此，这两个根始终为实数，且

$$\begin{aligned}\text{sign}(\frac{\partial g}{\partial\omega}) =& \text{sign}(g_{\text{sgn}}(\omega)) \\ & \begin{cases} < 0, & \text{if } \omega \in (\omega_1, \omega_2), \\ \geq 0, & \text{if } \omega \in (-\infty, \omega_1] \cup [\omega_2, \infty). \end{cases}\end{aligned} \tag{52}$$

换言之，$g(\omega)$ 随 $\omega \in (-\infty, \omega_1]$ 递增，随 $\omega \in (\omega_1, \omega_2)$ 递减，然后又随 $\omega \in [\omega_2, \infty$ 递增，即 $g(\omega)$ 在 $\omega = \omega_1 = \hat{}\omega$ 或 $\omega \to \infty$ 处取得最大值。显然，我们有 $g(\hat{}\omega) = 0$。此外，根据 (16) 和 (18)，有

$$\begin{aligned}\lim_{\omega\to\infty} g(\omega) =& Q(\infty) - be^{-a\cdot\infty} - c \\ =& 1 - 1\frac{1}{\sqrt{2\pi}a(\hat{\omega})} - Q(\hat{\omega}) < 0.\end{aligned} \tag{53}$$

因此，我们可以推导出

$$g(\omega) \leq \max\{g(\hat{\omega}), \lim_{\omega\to\infty} g(\omega)\} \leq 0, \ \forall\omega \in \mathbb{R}. \tag{54}$$

类似地，我们可以证明 $h(\omega) \leq$max{$h(-\hat{}\omega)$,lim$_{\omega\to-\infty}$ $h(\omega)$ } $\leq$ 0, $\forall\omega \in \mathbb{R}$，其中 $Q(x) = 1 - Q(-x)$，并将 $\hat{}\omega$ 替换为 $-\hat{}\omega$。证明的其余部分沿用上述方法。为避免重复，细节从略。■

附录 C 引理4的证明

证明。注意，信噪比 $\gamma = \frac{p|h|^2}{\sigma^2}$ 与发射功率 p呈线性关系。因此，ω 关于 γ 的凹性/凸性等价于其关于p的凹性/凸性。为简化符号，下面研究 ω 关于 m 和 γ的联合凹性。具体而言，根据西尔维斯特判据 [30]，若海森矩阵 H 的第一个顺序主子式（即二阶导数 $\frac{\partial^2\omega}{\partial m^2}$）非负，则可证明 ω 为凹函数

且海森矩阵的行列式 det H 也非负，其中

$$\mathbf{H} = \begin{pmatrix} \frac{\partial^2 \omega}{\partial m^2} & \frac{\partial^2 \omega}{\partial m \partial \gamma} \\ \frac{\partial^2 \omega}{\partial \gamma \partial m} & \frac{\partial^2 w}{\partial \gamma^2} \end{pmatrix} \tag{55}$$

and

$$\det(\mathbf{H}) = \frac{\partial^2 w}{\partial m^2}\frac{\partial^2 \omega}{\partial \gamma^2} - \left(\frac{\partial^2 \omega}{\partial m \partial \gamma}\right)^2. \tag{56}$$

随后，我们考察矩阵 H 中的各个分量。一方面，对于 w 关于 m 的偏导数，有

$$\begin{aligned} \frac{\partial w}{\partial m} &= \frac{\ln 2}{2} m^{-\frac{1}{2}} V^{-\frac{1}{2}} (\mathcal{C} + m^{-1} d) \geq 0, \\ \frac{\partial^2 w}{\partial m^2} &= -\frac{\ln 2}{4} m^{-\frac{3}{2}} V^{-\frac{1}{2}} (\mathcal{C} + 3m^{-1} d) \leq 0, \end{aligned} \tag{57}$$

这表明 ω 关于 m 单调递增且为凹函数。接下来，我们考察二阶导数，其可写为

$$\begin{aligned} \frac{\partial^2 w}{\partial \gamma^2} &= \frac{m^{\frac{1}{2}}}{(\gamma(\gamma+2))^{\frac{5}{2}}} \\ &\cdot \Big(\underbrace{-(\gamma+1)^3 + \frac{1}{\gamma+1} + 3(\gamma+1)\ln(\gamma+1)}_{\Delta_2} - \underbrace{3\ln 2 (\gamma+1)\frac{d}{m}}_{\leq 0} \Big), \end{aligned} \tag{58}$$

其中， $\Delta_2(\gamma)$ 是一个单调递减函数，这可由下式证明

$$\begin{aligned} \frac{\partial \Delta_2(\gamma)}{\partial \gamma} &= -3(\gamma+1)^2 - \frac{1}{(\gamma+1)^2} + 3 + 3\ln(\gamma+1) \\ &\leq -3(\gamma+1)^2 - \frac{1}{(\gamma+1)^2} + 3 + 3\gamma \\ &= -3(\gamma+1)\gamma - \frac{1}{(\gamma+1)^2} \leq 0. \end{aligned} \tag{59}$$

因此，成立 $\Delta_2(\gamma) \leq \Delta_2(0) = 0$，即

$$\frac{\partial^2 \omega}{\partial \gamma^2} \leq \frac{m^{\frac{1}{2}}}{(\gamma(\gamma+2))^{\frac{5}{2}}} \left(0 - 3\ln 2(\gamma+1)\frac{d}{m}\right) \leq 0. \tag{60}$$

因此， ω 关于 γ 单调递增且为凹函数。最后，我们推导 H 中最后两个元素的表达式，其可写为

$$\frac{\partial^2 w}{\partial m \partial \gamma} = \frac{\partial^2 w}{\partial \gamma \partial m} = \frac{m^{-\frac{1}{2}} \ln 2}{2\gamma^{\frac{1}{2}}(\gamma+2)^{\frac{1}{2}}} \left(-\frac{\mathcal{C}(\gamma) + r}{\gamma^2 + 2\gamma} + \frac{1}{\ln 2}\right). \tag{61}$$

结合（57）、（58）和（61），通过按 $r = \frac{d}{m}$ 分组，我们将 det H 改写为（62）所示形式，其中h（r）$= \Delta_a r^2 + \Delta_b r + \Delta_c$ 是关于 r的二次多项式。显然，有 sign(det H) = sign(h（r）)。由于 $\gamma \geq 0$，因此可以直接确定 $\Delta_a \geq 0$和 $\Delta_b \geq 0$。这意味着 h（r）最多只有一个正实根，也可能没有实根，而负根可被舍弃，因为 $r \geq 0$。因此，当满足$r \geq \frac{-\Delta_b + \sqrt{\Delta_b^2 - 4\Delta_a\Delta_c}}{2\Delta_a}$时，det H 非负。由此， ω 关于 m和 p是联合凹的。■

参考文献

[1] M. Bennis、M. Debbah 和 H. V. Poor，“超可靠低时延无线通信：尾部、风险与规模”，《IEEE会刊》，第 106 卷第 10 期，第 1834–1853 页，2018 年。[2] C. She、C. Sun、Z. Gu、Y. Li、C. Yang、H. V. Poor 和 B. Vucetic，“6G 中超可靠低时延通信教程：将领域知识融入深度学习”，《IEEE会刊》，第 109 卷第 3 期，第 204–246 页，2021 年。[3] C. She、C. Yang 和 T. Q. S. Quek，“超可靠低时延通信的无线电资源管理”，IEEE Communica- tions Magazine，第 55 卷第 6 期，第 72–78 页，2017 年。[4] G. Durisi、T. Koch 和 P. Popovski，“借助短数据包实现大规模、超可靠和低时延无线通信”，《IEEE会刊》，第 104 卷第 9 期，第 1711–1726 页，2016 年。[5] Y. Polyanskiy、H. V. Poor 和 S. Verdu，“有限码块长度区间中的信道编码速率”，IEEE Trans. Inf. Theory，第 56 卷第 5 期，第 2307–2359 页，2010 年。[6] Y. Hu、J. Gross 和 A. Schmeink，“有限码长下中继通信的容量”，IEEE Transactions on Vehicular Technology，第 65 卷第 3 期，第 1790–1794 页，2016 年。[7] Z. Xiang、W. Yang、Y. Cai、Z. Ding、Y. Song 和 Y. Zou，“物联网中的非正交多址辅助安全短数据包通信”，IEEE Wireless Communications，第 27 卷第 4 期，第 8–15 页，2020 年。[8] O. L. Alcaraz Lopez、E. M. G. Fernandez、R. D. Souza 和 H. Alves，“有限电池和有限码长下的无线供能通信”，IEEE Transactions on Communications，第 66 卷第 4 期，第 1803–1816 页，2018 年。[9] K. Singh、M.-L. Ku 和 M. F. Flanagan，“采用有限码长码的下行多用户多输入单输出网络能效预编码设计”，IEEE Transactions on Green Communications and Networking，第 5 卷第 1 期，第 160–173 页，2021 年。[10] M. Wang、T. Zhu、T. Zhang、J. Zhang、S. Yu 和 W. Zhou，“6G网络中的安全与隐私：新领域与新挑战”，《数字通信与网络》，第 6 卷第 3 期，第 281–291 页，2020 年。[11] J. Granjal、E. Monteiro 和 J. Sá Silva，“物联网安全：现有协议与开放研究问题综述”，《IEEE通信调查与教程》，第 17 卷第 3 期，第 1294–1312 页，2015 年。[12] V. Hassija、V. Chamola、V. Saxena、D. Jain、P. Goyal 和 B. Sikdar，“物联网安全综述：应用领域、安全威胁与解决方案架构”，《IEEE开放期刊》，第 7 卷，第 82 721–82 743 页，2019 年。[13] Y. Wu、A. Khisti、C. Xiao、G. Caire、K.-K. Wong 和 X. Gao，“5G无线网络物理层安全技术综述及未来挑战”，《IEEE通信领域精选期刊》，第 36 卷第 4 期，第 679–695 页，2018 年。[14] H. V. Poor 和 R. F. Schaefer，“无线物理层安全”，《美国国家科学院院刊》，第 114 卷第 1 期，第 19–26 页，2017 年。[在线]。可访问：https://www.pnas.org/doi/abs/ 10 1073 1618130114 。/pnas。[15] X. Sun、D. W. K. Ng、Z. Ding、Y. Xu 和 Z. Zhong，“无人机系统中的物理层安全：挑战与机遇”，IEEE Wireless Communications，第 26 卷第 5 期，第 40–47 页，2019 年。[16] Z. Xiang、W. Yang、G. Pan、Y. Cai 和 Y. Song，“认知无线电启发的非正交多址网络中的物理层安全”，《IEEE信号处理精选主题期刊》，第 13 卷第 3 期，第 700–714 页，2019 年。[17] M. A. Arfaoui、M. D. Soltani、I. Tavakkolnia、A. Ghrayeb、M. Safari、C. M. Assi 和 H. Haas，“可见光通信系统的物理层安全：综述”，《IEEE通信调查与教程》，第 22 卷第 3 期，第 1887–1908 页，2020 年。[18] W. Yang、R. F. Schaefer 和 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。[19] C. Wang、Z. Li、H. Zhang、D. W. K. Ng 和 N. Al-Dhahir，“有限码长下广播信道中的隐蔽性与安全性实现”，IEEE Transactions on Wireless Communications，第 21 卷第 9 期，第 7624–7640 页，2022 年。[20] H.-M. Wang、Q. Yang、Z. Ding 和 H. V. Poor，“任务关键型物联网应用的安全短数据包通信”，IEEE Transactions on Wireless Communications，第 18 卷第 5 期，第 2565–2578 页，2019 年。[21] Y. Wang、X. Zhou、Z. Zhuang、L. Sun、Y. Qian、J. Lu 和 F. Shu，“有限码长下的无人机赋能的安全通信”，IEEE Transactions on Vehicular Technology，第 69 卷第 12 期，第 16 309–16 313 页

$$
\begin{aligned}
\det \mathbf{H} = & \underbrace{\frac{m^{-1}(\ln 2)^2}{\gamma^2+2\gamma}}_{\geq 0} \Bigg(\underbrace{\frac{(\gamma^2+2\gamma)C\ln 2(4-3\ln 2)+(\gamma^2+2\gamma)^2(C\ln 2-1)-4C^2(\ln 2)^2}{4(\gamma^2+2\gamma)^2(\ln 2)^2}}_{\Delta_c} \\
& + \underbrace{\left(\frac{(\gamma^2+2\gamma)(6(\gamma^2+2\gamma)+8)-(3(\gamma^2+2\gamma)+8)C\ln 2}{4(\gamma^2+2\gamma)^2\ln 2}\right)}_{\Delta_b \geq 0} r + \underbrace{\left(\frac{8+9(\gamma^2+2\gamma)}{4(\gamma^2+2\gamma)^2}\right)}_{\Delta_a \geq 0} r^2 \Bigg) \\
= & \frac{m^{-1}(\ln 2)^2}{\gamma^2+2\gamma} h(r),
\end{aligned} \tag{62}
$$

[22] L. Wei、Y. Yang 和 B. Jiao，“全双工多用户 MIMO 短包通信中的保密吞吐量”，IEEE 无线通信汇刊，卷 10，第 6 期，第 1339–1343 页，2021 年。[23] C. Feng、H.-M. Wang 和 H. V. Poor，“可靠安全的短包通信”，IEEE 无线通信汇刊，卷 21，第 3 期，第 1913–1926 页，2022 年。[24] Y. Sun、P. Babu 和 D. P. Palomar，“信号处理、通信和机器学习中的主化-最小化算法”，IEEE 信号处理汇刊，卷 65，第 3 期，第 794–816 页，2017 年。[25] G. Scutari、F. Facchinei、P. Song、D. P. Palomar 和 J.-S. Pang，“部分线性化分解：多智能体系统的并行优化”，IEEE 信号处理汇刊，卷 62，第 3 期，第 641–656 页，2014 年。[26] Y. Zhu、Y. Hu、X. Yuan、M. C. Gursoy、H. V. Poor 和 A. Sch meink，“有限码块长度区间中错误概率关于块长和发射功率的联合凸性”，IEEE 无线通信汇刊，2022 年，提前发表。[27] Y. Polyanskiy、H. V. Poor 和 S. Verdu，“高斯信道的色散”，载于 2009 年 IEEE 国际信息论研讨会，2009 年，第 2204–2208 页。[28] A. D. Wyner，“窃听信道”，贝尔系统技术期刊，卷 54，第 8 期，第 1355–1387 页，1975 年。[29] A. Lancho、J. Ostman、G. Durisi、T. Koch 和 G. Vazquez-Vilar，“短包无线通信的鞍点近似”，IEEE 无线通信汇刊，卷 19，第 7 期，第 4831–4846 页，2020 年。[30] S. Boyd 和 L. Vandenberghe，《凸优化》。剑桥大学出版社，2004 年。[31] D. Kapetanovic、G. Zheng 和 F. Rusek，“大规模 MIMO 的物理层安全：被动窃听和主动攻击综述”，IEEE 通信杂志，卷 53，第 6 期，第 21–27 页，2015 年。[32] K. S. Ahn 和 R. W. Heath，“存在同信道干扰时采用不完美信道估计的最大比合并性能分析”，IEEE 无线通信汇刊，卷 8，第 3 期，第 1080–1085 页，2009 年。[33] W. Yu 和 R. Lui，“多载波系统非凸频谱优化的对偶方法”，IEEE 通信汇刊，卷 54，第 7 期，第 1310–1322 页，2006 年。[34] Y. Zhu、X. Yuan、Y. Hu、T. Wang、M. Cenk Gursoy 和 A. Schmeink，“低时延混合 NOMA-TDMA：QoS 驱动的设计框架”，IEEE 无线通信汇刊，第 1–1 页，2022 年。