arXiv:2603.09577v1 [cs.IT] 10 Mar 2026

随机分布式函数计算（RDFC）：面向隐私的超高效语义通信应用

Onur G¨unl¨u[1,2]

[1]通信技术系，多特蒙德工业大学 ，
德国。[2]信息编码部，瑞典林雪平大学。

通讯作者：Onur G¨unl¨u，onur.guenlue@tu-dortmund.de。

摘要

我们建立了随机化分布式函数计算（RDFC）框架，在该框架中，发送方仅传输足以让接收方对输入数据生成随机化函数的信息。我们将 RDFC 描述为一种语义通信形式，本质上可视为广义的远程源编码问题，并表明安全和隐私约束天然适用于这一模型，因为它们通常需要一个随机化步骤。借助强协调度量指标，我们确保对每个输入序列都满足（局部差分）隐私，并证明即使发送方和接收方之间没有共享公共随机性，也能实现此类保证。

本文给出了 Wyner 公共信息（WCI）的下界；在不存在公共随机性的情况下，WCI 即为通信成本。本文还提出了数值技术，用于评估在具有无限共享随机性的连续字母表随机变量情形下 RDFC 速率区域的另一个角点。实验表明，与 WCI 点相比，充足的公共随机性可将语义通信速率降低多达两个数量级；而即使完全没有共享随机性，RDFC 的表现仍远胜无损传输。有限码长分析进一步证实，渐近与非渐近 RDFC 方法之间的隐私参数差距会随输入长度增加而呈指数速度缩小。我们的研究结果表明，RDFC 是一种适用于隐私感知分布式计算系统的节能语义通信策略。

关键词：随机化分布式函数计算（RDFC）、超高效语义通信、强协调、节能型分布式隐私计算。

1 引言

与其传输消息的原始比特，不如传输其预期含义；这一需求催生了语义通信框架 [1, 2]。在这一框架中，重构信号的评价依据是与其语义相关的质量度量 [3]。与对内容毫不关心的传统物理层方案不同，语义通信只传输相关信息。传输图像中的物体及其相对位置，而非完整的像素图，就是语义通信的一个例子 [3]。由于发送方处的语义描述可视为数据的一个函数，因此语义通信可以自然地建模为远程（隐藏）信源编码问题：传输的不是数据本身，而是数据的一个函数，且发送方并不知道这个函数 [4–6]。这种表述推广了有损信源编码问题，使保真度度量能够根据语义相关性进行定制。

我们研究一种更广泛的远程信源编码场景，其中数据的随机化函数用于分布式函数计算。因此，接收方计算一个函数，其输入是发送方观测的随机化版本，从而建立随机分布式函数计算（*RDFC*）框架与语义通信。由于安全与隐私方法通常需要随机化，此类约束是RDFC [7–9]的自然应用场景。具体而言，我们研究受隐私约束的RDFC问题，其中发送方希望让接收方远程模拟一个序列，使得输入与输出序列遵循给定的、可保护隐私的目标联合分布。最小化此类远程模拟所需的通信负载在文献中被称为协调问题，也称为分布式信道合成或模拟 [10–14]。与近期工作往往针对机器学习与神经压缩任务中的经验（弱）协调 [15–18]，不同，我们聚焦于强协调度量 [10]来设计RDFC 方法。因此，RDFC通过对每个计算实例而非平均行为施加联合典型性约束来提供协调保证，这对于稳健的安全与隐私至关重要，以免催生新的攻击。

1.1 贡献概要

与确定性函数计算任务不同，当发送方和接收方共享公共随机性时，随机化函数计算问题所需的通信负载会显著降低 [19]。在点对点场景中，协调随机性速率区域有两个角点。没有公共随机性时，最低通信速率对应于信道输入 X 与输出 Y [20]之间的Wyner 公共信息（WCI） $C(X;Y) = \inf_{U:\tilde{X}-U-Y} I(X,Y;U)$。有足够的公共随机性时，最低通信速率会降至互信息 $I(X;Y)$。基于这一观察，本文的主要贡献如下：

- 我们将 RDFC 框架引入并形式化为一种用于隐私约束分布式计算的语义通信模型，它是远程信源编码问题的扩展。在强协调设定下，我们将隐私机制解释为给定输入序列的随机化函数，这与

现有的随机化隐私机制不同，并确定了此类隐私问题的协调随机性速率区域的两个角点工作状态。

- 我们分析一种连续字母表 RDFC 场景，其中随机化输出必须满足局部差分隐私（LDP）约束。对于裁剪高斯输入和高斯（ϵ, δ）-LDP机制，我们施加对称性以推导 WCI 的下界，并设计一种数值方法来计算互信息 $\tilde{I}(X;X)$。由此得到的比较结果量化了在 LDP 约束下公共随机性所能带来的通信速率节省，并揭示了新 WCI 下界优于通用下界的参数范围。我们还考虑了一些参数集合，在这些集合中可以识别 LDP 参数 ϵ 的独立影响。

- 我们研究一种离散 RDFC 场景，该场景基于对称随机响应机制，可有效结合多个随机化比特响应。对于一类二元对称信道（BSC）混合模型，我们利用对称性和 Witsenhausen 型技术推导 WCI 的下界，并将其与互信息 $\tilde{I}(X;X)$进行比较；该互信息本身也是 WCI 的下界。所得示例表明，公共随机性能够大幅降低语义通信速率，而不使用任何共享随机性的 RDFC 在通信负载方面仍显著优于无损传输。这些通信速率增益表明能效得到显著提升。

这些结果中的一部分已在本工作的会议版本中报告[21]。此外，在本工作中，我们提出了以下贡献：

- 我们针对 LDP 约束下的 RDFC 建立了有限码长分析。具体而言，对于协调随机性速率区域内部的任意速率 $R > I(X;Y)$，我们给出了随机编码器-解码器对的 RDFC 性能的显式界。这项基本结果以错误指数分析的形式给出，表明可实现的局部差分隐私参数（ϵ，δ_n）能够以关于码长 n 的指数速率达到 $\delta_n \to \delta$，这说明具有充足公共随机性的非渐近 RDFC 编码器-解码器对能够以指数衰减的损失逼近渐近隐私保证。

这些结果表明，与先引入随机性、再压缩随机化输出相比，使用 RDFC 编码器-解码器对能够为设计隐私感知分布式计算系统提供一种有原则的方法，并显著降低通信负载，从而大幅节省能源。

1.2 论文结构

本文结构如下。第2 节介绍 RDFC 框架，该框架给出逐实例函数计算保证以及离散随机变量的局部差分隐私度量。第3节建立了 WCI 的下界以及一种数值计算程序，用于计算互信息 $I(X;Y)$，此时连续值随机变量受到 LDP 约束。第4节针对给定的目标局部差分隐私参数，给出有限长度 RDFC 编码器–解码器对可实现的局部差分隐私参数。第5 节考虑随机响应机制，并推导出下

界，适用于一类离散对称信道的 WCI。第6 节总结全文。

1.3 符号说明

随机变量用大写字母 X 表示，其取值用小写字母 x表示。随机变量 X 服从概率质量函数（pmf）P_X，其支撑集为 supp(P_X)，或者具有概率密度函数（pdf） p_X。集合用花体字母 $\mathcal{X}$ 表示，其基数记为 $|\mathcal{X}|$。长度为 n 的序列表示为 $X^n = (X_1, X_2, \ldots\ldots, X_i, \ldots\ldots, X_n)$。

两个分布 P_Y 和 P_X 之间的全变差（TV）距离定义为

$$\|P_Y - P_X\|_{\mathrm{TV}} \triangleq \frac{1}{2}\sum_{b\in\mathcal{B}} |P_Y(b) - P_X(b)|. \tag{1}$$

定义信息密度

$$\imath_{\widetilde{X};Y}(\widetilde{x}, y) = \log \frac{\mathrm{d}P_{\widetilde{X}Y}}{\mathrm{d}P_{\widetilde{X}}P_Y} \tag{2}$$

其中，~~$\mathrm{d}P_{XY}\mathrm{d}P_{\widetilde{X}}P_Y$~~是 $P_{\widetilde{X}Y}$相对于 $P_{\widetilde{X}}P_Y$的拉东-尼科迪姆导数。类似地，对任意 $\alpha > 1$，定义 α-互信息，

$$I_\alpha(\widetilde{X};Y) = \frac{\alpha}{\alpha-1}\log \mathbb{E}\Big[\mathbb{E}^{\frac{1}{\alpha}}\Big[e^{\alpha\imath_{\widetilde{X};Y}(\widetilde{X},\widetilde{Y})}\,\Big|\,\widetilde{Y}\Big]\Big] \tag{3}$$

~ ~其中 $(X, Y) \sim P_{\widetilde{X}}P_Y$。

2 预备知识

2.1 随机分布式函数计算（RDFC）：通过强协调实现语义通信

RDFC 框架利用强协调方法，旨在通过信道协调多个节点的序列，同时仅传输最低限度的必要信息。由于协调是通过在这些局部序列中呈现联合行为来建立的，而该行为由给定的目标联合概率分布概括，并取决于各节点的目标以及计算和通信资源，因此无需向其他节点可靠地传输原始局部序列。我们指出，RDFC 方法也可以通过使用低复杂度自编码器作为编码器-解码器对来实现 [22]。

考虑图中所示的双用户 RDFC 模型。1观察到序列 $\sim X^n = \widetilde{x}^n$后，发送方将 $\widetilde{x}^n$ 与公共随机性$C \in \{1, 2, \ldots, 2^{nR_0}\}$联合编码。该公共随机性由发送方和接收方共享，并可通过使用物理不可克隆函数获得 [23]。此编码生成索引 $S \in$

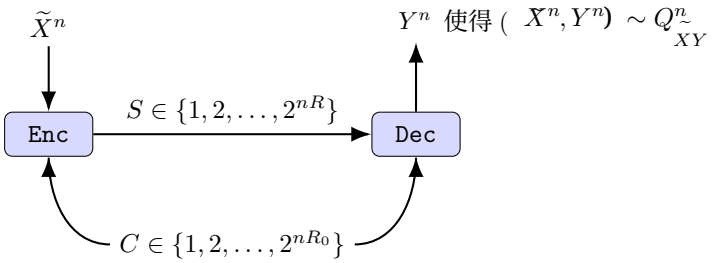

图 1：一个双节点 RDFC 模型，其中两个节点可以共享公共随机性 C。在强协调框架中，接收方使用传输索引 S 和 C 生成序列 Y^n。该过程确保每一对 $(\widetilde{x}^n, y^n)$ 都服从下文式 $(Q^n_{\widetilde{X}Y}$ 中给出的任意目标联合分布 4)，从而实现一种有利于两个节点的协作策略。设计目标是尽量降低信道速率 R，以减少函数计算时延和能耗。

$\{1, 2, \ldots, 2^{nR}\}$；发送方通过无噪声链路将 S 发送给接收方，接收方使用 S 和 C 合成序列 $Y^n = y^n$，使得 $(\widetilde{x}^n,\ y^n) \sim Q^n_{\widetilde{X}Y}$。接下来，我们定义图中所示双用户 RDFC 模型的协调-随机性区域，1其中考虑离散随机变量。

定义 1 速率对 (R, R_0) 称为 $Q_{\widetilde{X}Y}$的 *achievable*，如果对于任意 $\epsilon_n > 0$，都存在一个码长 $n \geq 1$ 以及相匹配的编码器-解码器对，使得

$$\lim_{n\to\infty} \left\| P_{\widetilde{X}^n Y^n}(\widetilde{x}^n, y^n) - \prod_{i=1}^{n} Q_{\widetilde{X}Y}(\widetilde{x}_i, y_i) \right\|_{\mathrm{TV}} = 0 \tag{4}$$

其中 $P_{\widetilde{X}^n Y^n}$ 表示由该编码器-解码器对所诱导的分布。

该 *coordination–randomness region* $\mathcal{R}_{\mathrm{RDFC}}$ 是图 R中 R_0所示双用户RDFC模型所有可达（1）元组的闭包。 ◊

接下来我们给出协调-随机性区域 $\mathcal{R}_{\mathrm{RDFC}}$。

定理 1 ([10,定理 II.1]) *The coordination-randomness region* $\mathcal{R}_{RDFC}$ *is the union over all* $P_{\widetilde{X}UY} = P_U P_{\widetilde{X}|U} P_{Y|U}$ *of the rate pairs* (R, R_0) *satisfying*

$$R \geq I(\widetilde{X}; U), \tag{5}$$

$$R + R_0 \geq I(\widetilde{X}, Y; U), \tag{6}$$

$$\sum_{u\in\mathcal{U}} P_{\widetilde{X}UY} = Q_{\widetilde{X}Y}. \tag{7}$$

*Remark 1*随机变量 U在（5）和（6）中是满足以下条件的任意辅助随机变量 $P_{\widetilde{X}UY} = P_U P_{\widetilde{X}|U} P_{Y|U}$和（7）。对于每个这样的辅助随机变量 U，都可以计算下界（5）和（6），从而得到一个有效的工作元组（R，R_0）。因此，考虑所有有效的辅助随机变量所得到的所有可达工作元组的并集，构成了协调-随机性区域 $\mathcal{R}_{\mathrm{RDFC}}$。

定理 1 对于下文分析的连续值随机变量，仍然适用于描述协调-随机性区域。标准的离散化论证 [24, 备注3。8] 可将可达性证明推广到性质良好的连续字母表，包括本文所考虑的（截断）高斯分布；另见 [10,第七节]。

在协调-随机性区域内，定理1 确定了两个角点。

首先，考虑 $R_0 = 0$的情况，即发送方和接收方不共享任何公共随机性。结合（5）和（6）可得第一个角点

$$R \geq C(\widetilde{X};Y) = \inf_{U:\ \widetilde{X}-U-Y} I(\widetilde{X},Y;U) \tag{8}$$

~ ~其中， $C(X;Y)$ 表示 X 与 Y [20]之间的 WCI。请注意，在许多多用户信息论结果中，人们会对满足马尔可夫链（如 $V-X-Y$）的辅助随机变量 V 进行优化，并且已有多种方法可以解决这一问题。然而，~此处的辅助随机变量 U 构成马尔可夫链 $X-U-Y$，使得对 $P_{\widetilde{X}UY}$ 的优化难度显著增加 [25]。我们针对具有实际意义的对称分布，推导了$\sim C(X;Y)$ 的下界。

其次，考虑相反的极端情况，即两个终端拥有足够的公共随机性 C。在此假设下，（5）和（6）可得第二个角点

$$R \geq I(\widetilde{X};Y) \tag{9}$$

~ ~由于数据处理不等式蕴含 $I(X;\ U) \geq I(X;\ Y)$。可以通过 $R_0 \geq H(Y|X)$ 达到式 (9) 中的角点，尽管 [26] 表明，有些情形所需的公共随机性甚至更少。式 (9) 中的界还推导出了反向香农定理[12], ，该定理表明，无限量的公共随机性和无噪信道足以模拟有噪信道。这与香农开创性著作中的信道编码定理所描述的操作方向相反 [27]。

根据 [20]，我们可以得到以下不等式链

$$I(\widetilde{X};Y) \leq C(\widetilde{X};Y) \leq \min\{H(\widetilde{X}),\ H(Y)\} \tag{10}$$

这凸显了 RDFC 在通信速率方面的显著节省。即使没有公共随机性，RDFC 方法也能优于两种标准~ ~基线方案：(i) 以 $H(X)$ 的速率无损传输序列 X^n，并让接收方计算随机函数输出 Y^n；(ii) 在发送方计算 Y^n，然后以 $H(Y)$ 的速率无损传输。

2.2 局部差分隐私

LDP（我们认为它可以保障个人用户隐私）自然构成一个 RDFC 问题，因为隐私保障源于对输入计算随机函数。

接下来，我们将 (ϵ, δ)–LDP 定义为 $\delta \neq 0$，通常称为近似 LDP。设 $\mathcal{M}(\cdot)$~为一种随机化机制，它将每个 $\widetilde{x} \in \mathcal{X}$ 映射到一个概率分布$\mathcal{M}(\cdot|\widetilde{x}) \in \mathcal{P}(\mathcal{Y})$。

~**定义 2** ([28–30]) 机制 $\mathcal{M}: \mathcal{X} \to \mathcal{P}(\mathcal{Y})$ 对于 ϵ, δ-LDP，若满足 $\epsilon \geq 0$ 和 $\delta \in [0, 1]$，则称其为

$$\sup_{\widetilde{x}, \widetilde{x}' \in \widetilde{\mathcal{X}}} \sup_{Y \subseteq \mathcal{Y}} \left(\mathcal{M}(Y|\widetilde{x}) - e^{\epsilon} \mathcal{M}(Y|\widetilde{x}') \right) \leq \delta. \tag{11}$$

◊

在第3节中，我们提出了一个 RDFC问题，用于综合设计高斯局部差分隐私机制 $\mathcal{M}(\cdot)$。通过添加独立的高斯噪声， $\mathcal{M}(\cdot)$ 可满足所需的 (ϵ, δ)–LDP 保证。由于复杂度较低，高斯机制常作为经验风险最小化方法中的隐私层，这些方法会运行随机梯度下降或 Adam优化器等优化流程 [31]。

3 采用加性高斯噪声实现局部差分隐私的 RDFC

接下来，我们考虑连续值随机变量。假设独立同分布高斯随机变量 $X^n \sim \mathcal{N}^n(0, \sigma_x^2)$ 被裁剪到范围 $[-C, C]$，其中 $C > 0$。对于 $a \in R$，定义

$$\beta = \frac{C}{\sigma_X}, \tag{12}$$

$$\mathrm{erf}(a) = \frac{2}{\sqrt{\pi}} \int_0^a e^{-t^2} dt, \tag{13}$$

$$\phi(a) = \frac{1}{\sqrt{2\pi}} e^{-a^2/2}, \tag{14}$$

$$\gamma(a) = \frac{a\phi(a)}{\mathrm{erf}\left(\frac{a}{\sqrt{2}}\right)}. \tag{15}$$

~裁剪后的输出 X^n 是一个均值为零、方差为以下数值的独立同分布截断高斯随机变量

$$\sigma_{\widetilde{X}}^2 = \sigma_X^2 \Big(1 - 2\gamma(\beta) \Big). \tag{16}$$

~发送方将裁剪序列 X^n 作为输入，并通过考虑高斯局部差分隐私机制 [32], , 旨在实现 (ϵ, δ)-LDP，使得接收方观测到的机制~ ~ ~ ~输出 Y^n 等于 $X^n + Z^n$，其中 X^n 和 Z^n 相互独立，并且有

$$\{(Y^n - \widetilde{X}^n)|\widetilde{X}^n\} := \{\widetilde{Z}^n|\widetilde{X}^n\} = \widetilde{Z}^n \sim \mathcal{N}^n(0, \sigma_{\widetilde{Z}}^2). \tag{17}$$

若有

$$\sigma_{\widetilde{Z}}^2 = \frac{8C^2}{\epsilon^2}\log\left(\frac{1.25}{\delta}\right), \tag{18}$$

那么，ϵ， δ)-LDP 约束对所有 $0 \le \epsilon \le 1$ [32, 33]均成立，这是因为~裁剪输入的 ℓ_2-敏感度 X 为 $2C$。我们还得到

$$\sigma_Y^2 = \sigma_{\widetilde{X}}^2 + \sigma_{\widetilde{Z}}^2 \tag{19}$$

~ ~这是因为 X^n 和 Z^n 相互独立。

接下来，考虑上述 (ϵ， δ)-LDP 问题的协调随机性速率区域的两个角点，它们由（8）和（9）给出。注意，这两个角点~ ~ ~，即 $C(X;Y)$ 和 $I(X;Y)$，均不受 X 和 Y 的均值影响。对 $a \in R$，定义

$$\{a\}^+ = \max\{a, 0\}, \tag{20}$$

$$\Phi(a) = 0.5\Big(1 + \mathrm{erf}(\frac{a}{\sqrt{2}})\Big), \tag{21}$$

$$\bar{\beta} = \frac{C}{\sigma_{\widetilde{X}}^2}, \tag{22}$$

$$m(a) = \frac{a}{\sigma_Y}. \tag{23}$$

~现在，我们给出 $C(X;Y)$ 的一个下界，以及计算 $I(X;Y)$ 的数值计算方法~。

定理 2 *Suppose an RDFC model with a clipped Gaussian input in the range $[-C, C]$under an (ϵ， δ)-LDP constraint, imposed via $Q_{\widetilde{X}Y}$, satisfied by using a Gaussian LDP mechanism. We obtain the following lower bound on $C(\widetilde{X};\ Y)$:*

$$C(\widetilde{X};Y) \ge \left\{0.5\log\left(1 + \frac{2\sigma_{\widetilde{X}}}{\sigma_Y - \sigma_{\widetilde{X}}}\right) + \log\left(\frac{\mathrm{erf}\left(\frac{\beta}{\sqrt{2}}\right)}{\sqrt{1 - 2\gamma(\beta)}}\right) - \gamma(\beta)\right\}^+. \tag{24}$$

~*Furthermore, $I(X;Y)$ can be computed numerically as*

$$I(\widetilde{X};Y) = -\mathbb{E}_{p_Y}[\log(p_Y(Y))] - 0.5\log(2\pi e\sigma_{\widetilde{Z}}^2) \tag{25}$$

where we have the pdf, for $y \in$ $(-\infty, \infty)$,

$$p_Y(y) = \frac{\phi(m(y))\left[\Phi\left(\frac{\bar{\beta}\sigma_Y^2 - \sigma_{\widetilde{X}}y}{\sigma_{\widetilde{Z}}\sigma_Y}\right) - \Phi\left(-\frac{\bar{\beta}\sigma_Y^2 + \sigma_{\widetilde{X}}y}{\sigma_{\widetilde{Z}}\sigma_Y}\right)\right]}{\mathrm{erf}\left(\frac{\bar{\beta}}{\sqrt{2}}\right)\sigma_Y}. \tag{26}$$

Proof Sketch: WCI 的下界源自 [34, 定理 1], 确立了以下下界

$$C(\widetilde{X};Y) \geq \left\{C(\widetilde{X}_g;Y_g) + h(\widetilde{X},Y) - h(\widetilde{X}_g,Y_g)\right\}^+ \tag{27}$$

其中，我们有 $(X_g,Y_g) \sim \mathcal{N}(0,K_{\widetilde{X}Y})$，且联合概率密度函数 $p_{\widetilde{X},Y}$ 满足交叉协方差矩阵约束 $K_{\widetilde{X}Y}$。由于 $(\widetilde{X}_g,Y_g)$ 服从联合高斯分布，因此可得 [20]

$$C(\widetilde{X}_g;Y_g) = \frac{1}{2}\log\left(\frac{1+|\rho_{\widetilde{X}Y}|}{1-|\rho_{\widetilde{X}Y}|}\right) \tag{28}$$

其中，我们有

$$\rho_{\widetilde{X}Y} = \frac{\sigma_{\widetilde{X}}}{\sigma_Y} = \frac{\sigma_{\widetilde{X}}}{\sqrt{\sigma_{\widetilde{X}}^2+\sigma_{\widetilde{Z}}^2}} \tag{29}$$

作为 $\widetilde{X}$ 与 Y 之间的相关系数。此外，我们得到

$$h(\widetilde{X}_g,Y_g) = \log(2\pi e\sigma_{\widetilde{X}}\sigma_{\widetilde{Z}}) = \log(2\pi e\sigma_X\sqrt{1-2\gamma(\beta)}\sigma_{\widetilde{Z}}) \tag{30}$$

由（16）可得。类似地，我们有

$$h(\widetilde{X},Y) = h(\widetilde{X}) + h(\widetilde{Z}) = \log\left(2\pi e\sigma_X \operatorname{erf}\left(\frac{\beta}{\sqrt{2}}\right)\sigma_{\widetilde{Z}}\right) - \gamma(\beta) \tag{31}$$

这可由截断高斯随机变量 $\widetilde{X}$ 的性质推出。

接下来，考虑互信息

$$I(\widetilde{X};Y) = h(Y) - h(\widetilde{Z}) = h(Y) - \log(\sqrt{2\pi e}\sigma_{\widetilde{Z}}) \tag{32}$$

可根据概率密度函数进行数值计算 p_Y 该概率密度函数见式（26），下文将对此进行说明。我们有 $Y^n = \widetilde{X}^n + \widetilde{Z}^n$，其中 $\widetilde{X}^n$ 是独立同分布的截断高斯变量，$\widetilde{Z}^n$ 是独立同分布的高斯变量，而 $\widetilde{X}^n$ 和 $\widetilde{Z}^n$ 相互独立。因此，根据 [35, 引理31]，我们可以得到独立高斯随机变量与截断高斯随机变量之和的概率密度函数。□

请注意，式（24）可能比式（10）中的一般不等式更紧，即，WCI $C(X;Y)$ 与式（24）之间的误差可能小于 WCI $C(X;Y)$ 与 $I(X;Y)$ 之间的误差。通过随机搜索扫描，我们确定了式（24）优于式（10）的参数范围。表1列出了此类示例，其中 $I(X;Y)$ 通过式（25）进行数值计算。

表 1 说明，借助 RDFC 框架中的语义通信方法，公共随机性可显著降低计算随机函数输出的通信成本，从而满足 (ϵ,δ)–LDP 约束，降幅最高可达 *214* 倍。表 1 还揭示了一种规律：更严格的 LDP（即更小的 ϵ）和更小的输入方差（即更小的 σ_X）会放大这一增益，使比值的下界 $C(X;Y)/I(X;Y)$进一步提高。

4 使用非渐近 RDFC 方法可实现的 LDP 参数

本节研究固定通信速率下 RDFC 的有限码长行为。具体而言，我们考虑任意严格位于

σ_X	ϵ	δ	WCI界（24）	$I(\widetilde{X};\ Y)$（25）	（24）/（25）
0.4938	0.8918	0.0097	0.0324	0.0019	17.05
0.4451	0.7917	0.0058	0.0307	0.0012	25.58
0.6112	0.9256	0.0016	0.0029	0.0019	1.53
0.2064	0.6399	0.0023	0.0186	0.0003	62.00
0.3839	0.3637	0.0061	0.0127	0.0002	63.50
0.4947	0.9884	0.0019	0.0298	0.0018	16.56
0.3280	0.4663	0.0032	0.0197	0.0002	98.50
0.3280	0.1266	0.0032	0.0038	1.8×10^{-5}	214.19

表1：由（24）计算得到的WCI下界、对 $I(X;\ Y)$ 的数值计算结果（来自25），以及针对随机搜索扫描所确定参数的比率，其中（24）优于（10）。这些结果说明了公共随机性为所施加的（ϵ，δ）-LDP约束带来的通信成本收益。

协调-随机性区域内部且公共随机性充足的速率。在 RDFC 框架中，如第 3 节所示，通过选择目标联合分布 $Q_{\widetilde{X}Y}$ 来施加 (ϵ,δ)-LDP 约束。然而，在非渐近情形下，也就是说，当 n 有限时，用于 RDFC 的编码器-解码器对无法精确逼近 $Q_{\widetilde{X}Y}$。本节旨在量化 RDFC 编码器-解码器对所诱导的联合分布以多快的速度在全变差意义下收敛到目标分布，以及有效 LDP 参数以多快的速度随 n 增大而收敛到期望的 (ϵ,δ)。因此，接下来我们将建立可达的 LDP 参数：对于给定的、合成 (ϵ,δ)-LDP 的目标联合分布，在公共随机性充足、足以使通信速率最小化时，使用 RDFC 编码器-解码器对即可实现这些参数。

定义

$$\rho^\star := \arg\max_{0<\rho\le\frac{1}{2}} \rho(R - I_{\frac{1}{1-\rho}}(\widetilde{X};Y)). \tag{33}$$

定理 3 *Let $Q_{\widetilde{X}Y}$ be a target joint law synthesizing (ϵ,δ)-LDP. Assume that a given rate $R > I(\widetilde{X};Y)$ satisfies $R > I(\widetilde{X};Y)$ and the moment generating function of the information density $\imath_{\widetilde{X}Y}(\widetilde{x},y)$ is finite in the neighborhood of origin. For every $n \ge 1$ there exists an RDFC $(\cdot,\cdot)$ encoder-decoder pair such that, for any $a > 1$, we obtain*

$$\begin{aligned} &\|P_{\widetilde{X}^n Y^n}(\widetilde{x}^n, y^n) - \prod_{i=1}^n Q_{\widetilde{X}Y}(\widetilde{x}_i, y_i)\|_{\mathrm{TV}} \\ &\quad\le a\Delta_n := aK \begin{cases} e^{-\frac{n}{2}(R - I_2(\widetilde{X};Y))}, & \text{if } \rho^\star = \frac{1}{2}, \\ n^{-\frac{1-\rho^\star}{2}} e^{-n\rho^\star\left(R - I_{\frac{1}{1-\rho^\star}}(\widetilde{X};Y)\right)}, & \text{if } \rho^\star < \frac{1}{2} \end{cases} \end{aligned} \tag{34}$$

where $K > 0$ is some constant. Consequently, the induced joint law $P_{\widetilde{X}^n Y^n}$ synthesizes $(\epsilon,\ \delta_n)$-LDP with

$$\delta_n = \delta + 2(e^{\epsilon} + 1)a\Delta_n. \tag{35}$$

Remark 2 定理 3 应在固定速率、大偏差意义下理解。对于任意˜速率 $R > I(X;Y)$（位于协调-随机性区域的内部），我们证明，对于每个码长 n，都存在一个速率为 R 的随机 RDFC 编码器-解码器对，其诱导的联合分布满足式 (34) 中的全变差界。量 Δ_n 随 n呈指数衰减，因此合成机制是 (ϵ, δ_n)-LDP，其中 δ_n 由式 (35) 给出，因此 $\delta_n \to \delta$ 呈指数级变化。特别地，速率 R 本身不依赖于 n，因为我们的非渐近分析控制了总变差近似质量对 n的依赖（因而也控制了 δ_n）。

注意，定理3 的结果可用于推导第 3 节所考虑的 RDFC 模型的可达 LDP 参数。

Proof Sketch: 考虑以独立同分布方式构造的似然编码器-解码器对，与 [36, 第 III] 节中的构造类似。利用 [37, 定理， 3]（该定理是针对离散随机变量的软覆盖引理的推广） [10, 引理 IV.1], ，可得

$$\mathbb{E}\Big[\big\|P_{\widetilde{X}^n Y^n}(\widetilde{x}^n, y^n) - \prod_{i=1}^{n} Q_{\widetilde{X}Y}(\widetilde{x}_i, y_i)\big\|_{\mathrm{TV}}\Big] \ \le\ \Delta_n. \tag{36}$$

此外，根据马尔可夫不等式，对于任意 $a > 1$，均存在满足（34）的似然编码器-解码器对。

˜记 X 的概率密度函数为 $p_{\widetilde{X}}$，并令

$$m_{\widetilde{X}} := \operatorname*{ess\,inf}_{\widetilde{x}\in\mathrm{supp}(P_{\widetilde{X}})} p_{\widetilde{X}}(\widetilde{x}) > 0 \tag{37}$$

其中，ess inf 表示本质下确界。由于全变差距离在可测映射 [38,（式（9）],）下具有非扩张性，将该对（$\widetilde{X}^n$， Y^n）投影到第一坐标可得

$$\big\|P_{\widetilde{X}Y}(\widetilde{x}^n, y^n) - Q_{\widetilde{X}Y}(\widetilde{x}_i, y_i)\big\|_{\mathrm{TV}} \ \le\ \big\|P_{\widetilde{X}^n Y^n}(\widetilde{x}^n, y^n) - \prod_{i=1}^{n} Q_{\widetilde{X}Y}(\widetilde{x}_i, y_i)\big\|_{\mathrm{TV}} \overset{(a)}{\le} a\Delta_n \tag{38}$$

其中，（a）由（34）可得。对于任意 $\widetilde{x} \in \mathrm{supp}(P_{\widetilde{X}})$ 以及可测集 $S \subseteq \mathcal{Y}$，有

$$\begin{aligned}\big|P_{Y|\widetilde{X}=\widetilde{x}}(S) - Q_{Y|\widetilde{X}=\widetilde{x}}(S)\big| &= \frac{1}{p_{\widetilde{X}}(\widetilde{x})}\Big|\int_S (p_{\widetilde{X}Y}(\widetilde{x}, y) - q_{\widetilde{X}Y}(\widetilde{x}, y))\, dy\Big| \\ &\le \frac{2}{m_{\widetilde{X}}}\,\big\|P_{\widetilde{X}Y} - Q_{\widetilde{X}Y}\big\|_{\mathrm{TV}}.\end{aligned} \tag{39}$$

结合（38）和（39）可得

$$\big|P_{Y|\widetilde{X}=\widetilde{x}}(S) - Q_{Y|\widetilde{X}=\widetilde{x}}(S)\big| \ \le\ \frac{2a\Delta_n}{m_{\widetilde{X}}}. \tag{40}$$

对于任意 $\widetilde{x}$， $\widetilde{x}' \in \mathrm{supp}(P_{\widetilde{X}})$，对于 $\widetilde{x} \neq \widetilde{x}'$ 和可测集 $S \subseteq \mathcal{Y}$，两次使用（40）以及 $Q_{Y|\widetilde{X}}$ 提供（ε， δ）-LDP 这一事实，可得

$$P_{Y|\widetilde{X}=\widetilde{x}}(S) \le Q_{Y|\widetilde{X}=\widetilde{x}}(S) + \frac{2a\Delta_n}{m_{\widetilde{X}}} \tag{41}$$

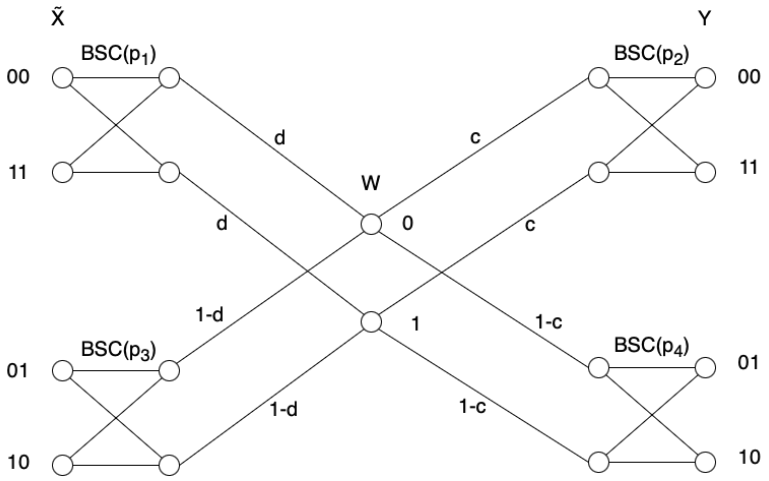

图 2：一个示例随机响应场景，其中联合分布 $Q_{\widetilde{X}Y}$ 可表示为二元对称信道的混合。为简便起见，假设 W 服从均匀分布。

$$\leq e^{\varepsilon} Q_{Y|\widetilde{X}=\widetilde{x}'}(S) + \delta + \frac{2a\Delta_n}{m_{\widetilde{X}}} \tag{42}$$

$$\leq e^{\varepsilon} \left[P_{Y|\widetilde{X}=\widetilde{x}'}(S) + \frac{2a\Delta_n}{m_{\widetilde{X}}} \right] + \delta + \frac{2a\Delta_n}{m_{\widetilde{X}}} \tag{43}$$

$$= e^{\varepsilon} P_{Y|\widetilde{X}=\widetilde{x}'}(S) + \delta + \frac{2\left(e^{\varepsilon}+1\right)a\Delta_n}{m_{\widetilde{X}}}. \tag{44}$$

将 $1/m_{\widetilde{X}}$ 并入常数 K 可得（35），因此合成机制是（ε，δ_n）-LDP。□

我们指出，定理3 是一个存在性的、非构造性的结果，因为（34）中的界刻画了逼近误差的指数衰减，但并不对应于某个特定的码族。因此，除了收敛到目标联合分布（以及（ϵ, δ）-LDP）可以呈指数快速这一基本洞见之外，要获得实用的有限码长性能曲线，还需要显式的RDFC码构造及其数值评估，我们将其视为未来工作中一个有趣的方向。

5 对称随机响应的RDFC

接下来，我们考虑一种离散随机响应场景，它可用作~一种LDP机制 [39]，其中发送方观测 X^n，而接收方必须~生成随机响应 Y^n，使得（X^n，Y^n）服从概率质量函数 $Q^n_{\widetilde{X}Y}$，其可表示为图2。为简单起见，图2 给出了2比特输出情形。中间的二元随机变量 W 假定服从均匀分布，并驱动两个信道 $P_{\widetilde{X}|W}$和 $P_{Y|W}$，且每个信道都可写为二元对称信道（二元对称信道）的混合，从而使整体概率质量函数对称。

令 $\widetilde{X}=(\widetilde{X}_1,\ \widetilde{X}_2)$ 和 $\widetilde{Y}=(\widetilde{Y}_1,\ \widetilde{Y}_2)$。图2中的随机响应模型则具有如下表示

$$\begin{bmatrix}\widetilde{X}_1\\ \widetilde{X}_2\\ \widetilde{Y}_1\\ \widetilde{Y}_2\end{bmatrix}=W\begin{bmatrix}1\\1\\1\\1\end{bmatrix}\oplus\begin{bmatrix}B_1\\B_2\\B_3\\B_4\end{bmatrix} \tag{45}$$

其中 $\oplus$ 表示模 2 加法。噪声比特 B_1–B_4 彼此相依，但仍与 W独立。由于 W 是均匀的，对称性

$$P_{\widetilde{X}_1\widetilde{X}_2\widetilde{Y}_1\widetilde{Y}_2}(\widetilde{x}_1,\widetilde{x}_2,y_1,y_2)=P_{\widetilde{X}_1\widetilde{X}_2\widetilde{Y}_1\widetilde{Y}_2}(\bar{\widetilde{x}}_1,\bar{\widetilde{x}}_2,\bar{y}_1,\bar{y}_2) \tag{46}$$

成立，其中 $\bar{y}=1-y$。

定义

$$q_{Y_1Y_2}=P_{Y_1Y_2|W}(y_1,y_2|0), \tag{47}$$

因此子信道概率为

$$c=q_{00}+q_{11}, \tag{48}$$
$$1-c=q_{01}+q_{10}, \tag{49}$$

其中二元对称信道的交叉概率给定为

$$p_2=q_{11}/c, \tag{50}$$
$$p_4=q_{10}/(1-c). \tag{51}$$

可以为 $P_{\widetilde{X}|W}$定义类似的量。同样的构造可推广至可分解为两个以上二元对称信道的联合概率质量函数 [40]。当给定的概率质量函数 $Q_{\widetilde{X}\widetilde{Y}}$满足（46）中的对称条件时，计算 $C(X;\ Y)$ 的下界会变得相当简单，如下文所示。

我们首先总结文献 [41] 中的定理 4 和定理 5，给出 WCI $C(X;Y)$ 的一个下界。定义

$$\alpha=\sqrt{\frac{kx-1}{k-1}}, \tag{52}$$
$$x_k^*=\frac{k^2-3k+3}{k(k-1)}, \tag{53}$$
$$f_1(x)=-\frac{2}{k}\big[(1+(k-1)\alpha)\log(1+(k-1)\alpha) + (k-1)(1-\alpha)\log(1-\alpha)\big]+2\log k, \tag{54}$$
$$f_2(x)=2\log k-2(k-1)\frac{\log(k-1)}{k-2}\left(x-\frac{1}{k}\right). \tag{55}$$

考虑一个 $k \times k$ 联合概率分布矩阵 $\mathbf{Q}_{\tilde{X}Y}$，其元素为 $Q_{i,j}$，表示概率质量函数 $Q_{\tilde{X}Y}$。例如，对于图 所示的分布，我们有 2。注意，只需考虑方阵 $\mathbf{Q}_{\tilde{X}Y}$，因为添加或删除全零的行或列不会影响 WCI 的计算 [41]。

将迹运算记为 tr(·)，并将最大迹运算定义为

$$\operatorname{maxtr}(\mathbf{Q}) = \max_{\pi \in \mathcal{S}_k} \sum_{i=1}^{k} Q_{i,\pi(i)} \tag{56}$$

其中， $\mathcal{S}_k$ 是指标 $\{1, 2, \ldots, k\}$ 的所有排列的集合。

定理 4 *Let $k > 2$ and $1/k \leq x \leq 1$, and*

- 若 $x_k^* \leq x \leq 1$，则考虑

$$f(x) := f_1(x) \tag{57}$$

- 并且，在其他情况下，若 $1/n \leq x \leq x_k^*$，则考虑

$$f(x) := f_2(x). \tag{58}$$

~Given a probability distribution matrix $\boldsymbol{Q}_{\tilde{X}Y}$, we obtain the following lower bound on $C(X;Y)$

$$C(\widetilde{X};Y) \geq H(\widetilde{X},Y) - f(\operatorname{maxtr}(\boldsymbol{Q}_{\widetilde{X}Y})). \tag{59}$$

某些对称分布在59）中满足等号 [41]。我们将讨论范围限定为符合图 $Q_{\tilde{X}Y}$ 中的二元对称信道混合模型以及式2 和（45）的联合概率质量函数，并评估定理4 给出的下界，再将其与互信息~I（X； Y）进行比较。随机搜索扫描揭示了若干参数范围，在这些范围内，式（59）比式（10）中的一般不等式更紧；表2列出了若干典型示例。

表2 显示，引入公共随机性可以显著降低合成随机函数输出所需的通信负载。此外，~互信息 $I(X;Y)$越小，这一收益就越大；也就是说，~~比值 $C(X;Y)/I(X;Y)$的下界相应增大。即使没有任何公共随机性，RDFC 方法仍能大幅节省通信成本，因为 WCI 下界最多比无损通信速率 $H(X)$和 $H(Y)$低 116.55 倍。因此，我们的结果表明，在 RDFC 中采用语义通信方法（无论是否使用公共随机性），相较于经典函数计算方法都能带来显著收益，并大幅提升能效。

这些结果促使人们进一步研究诸如在固定公共随机性数量下可实现的最小通信负载等问题。这一点非常重要，因为对于存储空间有限的设备而言，公共随机性是一种真正的资源。

$(p_1, p_2, p_3, p_4, c, d)$	~WCI（59		$\frac{(59)}{I(X;\ Y)}$	~$H($		$\frac{\min\{H(\ \tilde{X})\ H(Y)\}}{(59)}$
(0。05，0。45，0。5，0。25，0。45，0。4)	0.0977	0.0238	4.10	1.3662	1.3813	13.984
(0。05，0。1，0。2，0。4，0。45，0。3)	0.0998	0.0822	1.21	1.3040	1.3813	13.069
(0.15,0.25,0, 0.05,0.45,0.4)	0.3276	0.2570	1.27	1.3662	1.3813	4.170
(0.25, 0.4, 0.1, 0.25,0.5,0.25)	0.0967	0.0403	2.40	1.2555	1.3863	12.980
(0.45,0.4, 0.3, 0.1,0.45,0.3)	0.1315	0.0216	6.09	1.3040	1.3813	9.916
(0.3,0.5,0.3, 0,0.5,0.4)	0.1364	0.0411	3.32	1.3662	1.3863	10.010
(0.1, 0.05,0.1, 0, 0.1, 0.05)	0.5325	0.3601	1.48	0.8917	1.0182	1.675
(0.5, 0, 0.45, 0.3,0.4, 0.45)	0.0117	0.0014	8.36	1.3813	1.3662	116.550

~**表 2**：WCI 下界计算来自（59），I（X；Y）的精确计算来自 ~$Q_{\tilde{X}Y}$，其比率、无损信源编码率 H（X）和 H（Y），分别用于传输 X^n 和 Y^n，以及比率 $\min\{H(\tilde{X})\ H(Y)\}/$（59）。这些值针对随机选取的参数计算，对于这些参数，（59）给出了有效的下界。

6 结论

我们将随机化分布式函数计算（RDFC）框架引入为一种语义通信方法，使发送方仅传递足够的信息，让接收方能够合成输入数据的某个（保护隐私的）随机化函数。通过将高斯局部差分隐私和对称随机响应等隐私机制置于强协调模型中，我们证明，与无损压缩方法相比，RDFC 可将所需通信速率降低最多两个数量级。需要注意的是，无论是否使用公共随机性，通信速率取得如此显著的提升都会带来能效的大幅提高。我们进一步通过新的界和数值示例展示了，充足的公共随机性如何转化为超高效的语义通信速率；同时，有限码长分析证实，随着序列长度增加，所得到的隐私保证以指数速度收紧。这些发现表明，RDFC 是未来分布式计算系统实现隐私感知和高能效通信的一条实用途径。作为一个有趣的未来研究方向，近期关于 WCI[42] 的变分表述可以适配到 RDFC 场景中，从而为 WCI 提供变分上界，与本文发展的下界相互补充。

声明

数据和材料的可用性

数据共享不适用于本文，因为在当前研究中未生成或分析任何数据集。

竞争利益

作者声明不存在任何竞争利益。

资助
本研究部分获得了ZENITH研究与领导力职业发展基金、瑞典战略研究基金会（SSF）和欧盟 COST 行动 6G-PHYSEC的支持。

作者贡献
OG 是唯一作者，负责准备、阅读并批准最终稿。

致谢
OG 感谢本研究会议版本的匿名审稿人 [21]提出的深刻意见，其中包括仅改变表1中一个参数的建议。该建议带来了显著的通信负载增益，达到 214 倍，具体见表1的最后一行。

作者信息
OG于2011年在土耳其比尔肯特大学获得电气与电子工程理学学士学位（最高荣誉）；随后于2013年和2018年分别在德国慕尼黑工业大学（TUM）获得通信工程理学硕士学位（最高荣誉）和工学博士学位（相当于哲学博士）。2012年11月至2013年3月期间，他在德国慕尼黑的英特尔移动通信公司（IMC）通信系统部门担任工作学生；该公司现为苹果公司。2014年2月至2019年5月期间，Onur在慕尼黑工业大学通信工程教席（LNT）担任研究与教学助理。在担任访问研究员期间，他曾于2018年2月至2018年3月访问荷兰埃因霍温理工大学；此前后，他还在二十多所顶尖大学与企业开展了研究访问。2022年2月至2022年3月期间，Onur在美国亚特兰大的佐治亚理工学院担任访问研究组组长。2023年2月至2023年3月期间，他还在德国德累斯顿工业大学担任客座教授。在慕尼黑工业大学、柏林工业大学和锡根大学担任研究助理及研究组组长后，他于2022年10月加入林雪平大学，担任ELLIIT助理教授，并于2024年8月获得终身教职，晋升为副教授，负责信息论与安全实验室（ITSL）。2023年12月，他获得信息论瑞典副教授资格（特许博士）；2024年7月，他成为IEEE高级会员。自2025年9月起，Onur一直担任德国多特蒙德工业大学（TUDO）通信工程教席（通信工程研究所）的终身正教授并负责该教席，同时担任瑞典林雪平大学客座教授。

他曾获2025年IEEE信息论学会乔伊·托马斯最佳教程论文奖、2023年ZENITH研究与职业发展奖、2021年《IEEE通信汇刊》杰出审稿人奖，以及备受瞩目的VDE信息技术学会（ITG）2021年约翰·菲利普·赖斯奖。他的研究兴趣包括分布式函数计算、信息论隐私与安全、编码理论、一体化感知与通信，以及隐私

学习。他的出版物包括著作基于物理不可克隆函数和生物特征标识符的密钥协商 （Dr. Hut 出版社，2019年）。

他担任 IEEE JOURNAL ON SELECTEDAREAS IN COMMUNICATIONS、IEEE TRANSACTIONS ON COMMU-NICATIONS和 ENTROPY Journal 的副编辑，最近还担任
EURASIP JOURNAL ON WIRELESS COMMUNICATIONS AND NET-WORKING 的副编辑以及 IEEE JOURNAL ON SELECTED AREAS
IN INFORMATION THEORY的客座编辑。他还担任 IEEE 瑞典 VT/COM/IT 联合分会的董事会成员兼秘书，以及欧盟 COST 行动 6G-PHYSEC 的工作组组长。

参考文献

[1] Q. Lan 等，《什么是语义通信？机器智能时代传达意义的观点》。《通信与信息网络杂志》（JCIN）**6(4)**, 336–371（2021）[2]D. G¨und¨uz 等，《超越比特传输：语境、语义与面向任务的通信》。《IEEE通信领域选刊》（JSAC）**41(1)**, 5–41（2022）[3] D. G¨und¨uz 等，《6G中的及时海量通信：语用学、学习与推理》。《IEEE BITS信息论杂志》**3(1)**, 27–40（2023）[4] R. Dobrushin、B. Tsybakov，《存在附加噪声时的信息传输》。《IRE信息论汇刊》（T-IT）**8(5)**, 293–304（1962）[5] T. Berger，《率失真理论》。《威利电信百科全书》（2003）[6] I. Csisz´ar、J. K¨orner，《信息论：离散无记忆系统的编码定理》（剑桥大学出版社，2011）[7] M. Bloch 等，《信息论安全与隐私概述：度量、极限与应用》。《IEEE信息论领域选刊》（JSAIT）**2(1)**, 5–22（2021）[8] D. Data、G.R. Kurri、J. Ravi、V.M. Prabhakaran，《交互式安全函数计算》。《IEEE信息论汇刊》（T-IT）**66(9)**, 5492–5521（2020）[9] G. ˚Ahlgren、O. G¨unl¨u，《信道上的安全率失真感知权衡：随机分布式函数计算（*RDFC*）应用》，载于*IEEE*国际信息论研讨会（*ISIT*）（2025）

[10] *P. Cuff*, 《分布式信道合成》。《*IEEE*信息论汇刊》（*T-IT*）*59(11), 7071–7096*（*2013*）[11] *O. G¨unl¨u*、*M. Skorski*、*H.V. Poor*, 《低时延率失真感知权衡：随机分布式函数计算应用》，载于*EuCNC*与*6G*峰会（*2025*）[12] *C. Bennett*、*P. Shor*、*J. Smolin*、*A. Thapliyal*, 《量子信道的纠缠辅助容量与反向香农定理》。《*IEEE*信息论汇刊》（*T-IT*）*48(10), 2637–2655*（*2002*）[13] *P. Harsha*、*R. Jain*、*D. McAllester*、*J. Radhakrishnan*, 《相关性的通信复杂度》。《*IEEE*信息论汇刊》（*T-IT*）*56(1), 438–449*（*2010*）[14] *G. Kramer*、*S.A. Savari*, 《传递概率分布》。《*IEEE*信息论汇刊》（*T-IT*）*53(2), 518–525*（*2007*）[15] *M. Havasi*、*R. Peharz*、*J.M. Hern´andez-Lobato*, 《最小随机码学习：从压缩模型参数中取回比特》，载于国际学习表征会议（*ICLR*）（*2019*）[16] *A. Shah*、*W.N. Chen*、*J. Balle*、*P. Kairouz*、*L. Theis*, 《本地差分隐私机制的最优压缩》，载于国际人工智能与统计会议（*AISTATS*）（*2022*），第*7680–7723*页[17] *B. Phan*、*A. Khisti*、*C. Louizos*, 《含边信息有损压缩的重要性匹配引理》，载于国际人工智能与统计会议（*AISTATS*）（*2024*），第*1387–1395*页[18] *B. Isik*、*F. Pase*、*D. G¨und¨uz*、*S. Koyejo*、*T. Weissman*、*M. Zorzi*, 《利用边信息实现联邦学习中的自适应压缩》，载于国际人工智能与统计会议（*AISTATS*）（*2024*），第*487–495*页[19] *G.R. Kurri*、*V. Ramachandran*、*S.R.B. Pillai*、*V.M. Prabhakaran*, 《多址信道仿真》，载于*IEEE*国际信息论研讨会（*ISIT*）（*2021*），第*2411–2416*页[20] *A. Wyner*, 《两个相依随机变量的公共信息》。《*IEEE*信息论汇刊》（*T-IT*）*21(2), 163–179*（*1975*）[21] *O. G¨unl¨u*, 《语义通信中的随机分布式函数计算：隐私应用》，载于*IEEE*信息取证与安全国际研讨会（*WIFS*）（*2024*），第*1–6*页[22] *D. Bergstr¨om*、*O. G¨unl¨u*, 《深度随机分布式函数计算（*DeepRDFC*）：神经分布式信道仿真》，载于*IEEE*国际

信息论研讨会（*ISIT*）（2025）

[23] O. G¨unl¨u, O. I.scan, V. Sidorenko, G. Kramer, 采用变换编码的物理不可克隆函数可靠密钥绑定，载于 *IEEE*全球信号与信息处理会议 *(GLOBALSIP)* (2016)，第 986–991 页[24] A.E. Gamal, Y.H. Kim，网络信息论（英国剑桥：剑桥大学出版社，2011）[25] S.L. Huang, X. Xu, L. Zheng, G.W. Wornell，*Wyner*共同信息的局部刻画，载于 *IEEE*国际信息论研讨会 *(ISIT)* (2020)，第 2252–2257 页[26] P.W. Cuff, H.H. Permuter, T.M. Cover，协调容量。IEEE信息论汇刊 (T-IT) **56**(9), 4181–4206 (2010)[27]C.E. Shannon，通信的数学理论。贝尔系统技术期刊 **27**(3), 379–423 (1948)[28] S. Asoodeh, M. Aliakbarpour, F.P. Calmon，局部差分隐私等价于某种 f-散度的收缩，载于 *IEEE*国际信息论研讨会 *(ISIT)* (2021)，第 545–550 页[29] A. Evfimievski, J. Gehrke, R. Srikant，限制隐私保护数据挖掘中的隐私泄露，载于 *ACM*数据库系统原理研讨会 *(PODS)* (2003)，第 211–222 页[30] S.P. Kasiviswanathan, H.K. Lee, K. Nissim, S. Raskhodnikova, A. Smith，我们能私下学到什么？，载于*IEEE*计算机科学基础研讨会 *(FOCS)* (2008)，第 531–540 页[31] R. Bassily, A. Smith, A. Thakurta，私有经验风险最小化：高效算法与紧确误差界，载于*IEEE*计算机科学基础研讨会 *(FOCS)* (2014)，第 464–473 页[32] C. Dwork, A. Roth 等，差分隐私的算法基础。理论计算机科学前沿® **9**(3–4), 211–407 (2014) [33] M. Seif, R. Tandon, M. Li，具有局部差分隐私的无线联邦学习，载于*IEEE*国际信息论研讨会 *(ISIT)* (2020)，第 2604–2609 页[34] E. Sula, M. Gastpar，松弛的 *Wyner*共同信息下界，载于*IEEE*国际信息论研讨会 *(ISIT)* (2021)，第 1510–1515 页

[35] E. Drysdale，采用数据切割进行精确选择后推断的参数分布。预印本 arXiv:2305.12581 (2023)[36] E.C. Song, P. Cuff, H.V. Poor，有损压缩的似然编码器。IEEE信息论汇刊 (T-IT) **62**(4), 1836–1849(2016)[37] M.H. Yassaee，通过大偏差分析软覆盖引理的近乎精确分析，载于*IEEE*国际信息论研讨会 *(ISIT)* (2019)，第 1387–1391 页[38] H. Tyagi，讲座 2。技术报告，印度科学研究所 (IISc) (2019)。网址https://ece.iisc.ac.in/~htyagi/courses/E2209/lectures/lecture2-scribe.pdf。课程 E2 209 讲义[39] B. Bebensee，局部差分隐私：教程。预印本 arXiv:1907.11908 (2019)[40] O. G¨unl¨u, G. Kramer，针对标识符的多次含噪测量实现隐私、保密性与存储。IEEE信息取证与安全汇刊 (TIFS) **13**(11), 2872–2883 (2018)[41] H.S. Witsenhausen，两个离散随机变量公共信息的取值与界。SIAM应用数学杂志 (SIAP) **31**(2), 313–333 (1976)[42] T.H. Huang, H. El Gamal，Wyner共同信息的高效求解器及其在多模态聚类中的应用。IEEE信息论汇刊 (T-IT) **71**(3), 2054–2074 (2025)