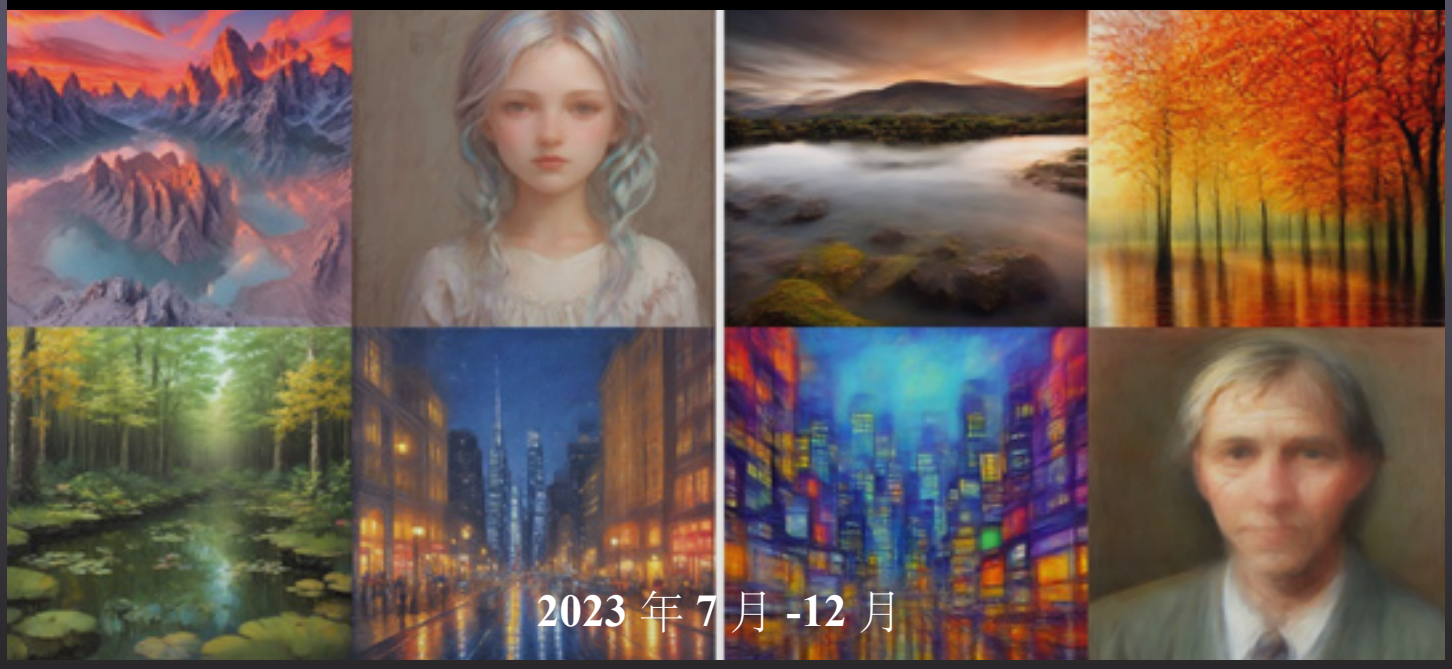
清華大學 交叉信息研究院
Institute for Interdisciplinary Information Sciences, Tsinghua University

# 学术科研简报

**IIIS Academic Newsletter**

Latent Consistency Models:
Synthesizing High-Resolution Images with Few-Step Inference



**2023 年 7 月 -12 月**

# 人工智能



# 量子信息

# 人工智能

# 一、机器学习

主要完成人：袁洋研究组、李建研究组、高阳研究组、吴翼研究组、张景昭研究组、许华哲研究组、弋力研究组、赵行研究组

## 大语言模型“累积推理”框架

大语言模型（LLMs）已取得显著进步，但面对高度复杂的推理任务时，它们仍难以提供稳定且准确的答案。为突破这一局限性，姚期智和袁洋领衔的研究团队提出了“累计推理（Cumulative Reasoning, CR）”框架，尝试对思维过程进行更一般性的建模。

“累计推理”框架利用三个不同的 LLMs 来解决复杂推理问题，包括提议者 (Proposer)、验证者 (Verifier) 和报告者 (Reporter)。其中，提议者基于现有前提 (premises) 和命题 (propositions) 提出一个或几个提案来启动该过程。随后，验证者评估该提案，确定该提案是否可以作为新的命题保留。最后，报告者决定是否是终止思考过程并提供最终答案的最佳时机。

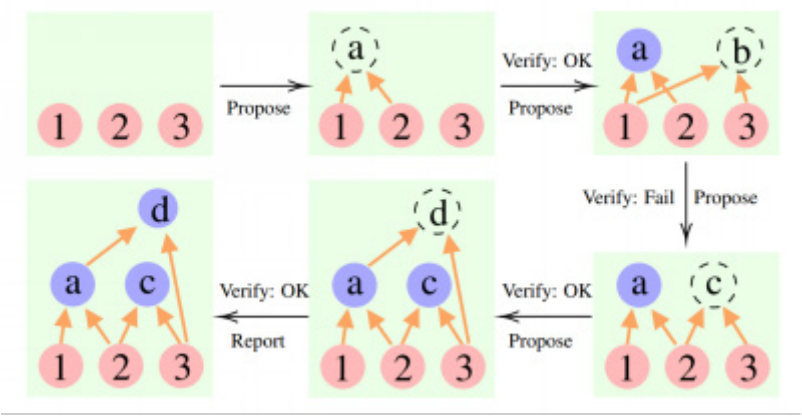



图 1：累积推理框架用于解决含三个前提的问题

研究组选择在 FOLIO wiki 和 AutoTNLI、24 点游戏、MATH 数据集上对“累积推理”框架进行检验。结果表明，在 FOLIO wiki 和 AutoTNLI 数据集上“累积推理”框架始终优于现有方法，显示出高达 9.3% 的提升。特别是在校对后的 FOLIO wiki curated 数据集上，CR 达到了 98.04% 的准确率。在围绕 24 点游戏的实验中，CR 达到了 98% 的准确率。值得注意的是，与先前的最先进的方法 ToT 相比，这一数字有着高达 24% 的显著提升。MATH 数据集的实验结果表明，CR 算法在两种不同的实验设定下，均达到了超出当前已有算法的正确率。其中 CR 总体正确率可达 58%，并在 Level 5 的难题中实现了 42% 的相对准确率提升，建立了 GPT-4 模型下的新 SOTA。

Table 2: Results for various reasoning approaches on FOLIO-wiki-curated dataset.

| Model | Method | Acc. ↑ (%) | Error ↓ (%) |
|---|---|---|---|
| - | [Random] | 33.33 | 66.67 |
| LLaMA-13B | Direct | 49.13 | 50.87 |
| | CoT | 52.17 (+3.04) | 47.83 (-3.04) |
| | CoT-SC ($k$ = 16) | 53.70 (+4.57) | 46.30 (-4.57) |
| | **CR (ours**, $n$ = 2) | **55.87** (+6.74) | **44.13** (-6.74) |
| LLaMA-65B | Direct | 74.78 | 25.22 |
| | CoT | 74.13 (-0.65) | 25.87 (-0.65) |
| | CoT-SC ($k$ = 16) | 79.13 (+4.35) | 20.87 (-4.35) |
| | **CR (ours**, $n$ = 2) | **79.57** (+4.79) | **20.43** (-4.79) |
| GPT-3.5-turbo | Direct | 69.57 | 30.43 |
| | CoT | 70.65 (+1.08) | 29.35 (-1.08) |
| | CoT-SC (k = 16) | 69.32 (-0.25) | 30.68 (+0.25) |
| | **CR (ours**, $n$ = 2) | **78.70** (+9.13) | **21.30** (-9.13) |
| GPT-4 | Direct | 89.57 | 10.43 |
| | CoT | 95.00 (+5.43) | 5.00 (-5.43) |
| | CoT-SC (k = 16) | 96.09 (+6.52) | 3.91 (-6.52) |
| | **CR (ours**, $n$ = 2) | **98.04** (+8.47) | **1.96** (-8.47) |

图 2:FOLIO wiki 数据集对比测试结果

Table 3: Results for various reasoning approaches on AutoTNLI dataset.

| Model | Method | Acc. ↑ (%) | Error ↓ (%) |
|---|---|---|---|
| - | [Random] | 50.00 | 50.00 |
| LLaMA-13B | Direct | 52.6 | 47.4 |
| | CoT | 54.1 (+1.5) | 45.9 (-1.5) |
| | CoT-SC (k = 16) | 52.1 (-0.5) | 47.9 (+0.5) |
| | **CR (ours**, $n$ = 4) | **57.0** (+5.4) | 43.0 (-5.4) |
| LLaMA-65B | Direct | 59.7 | 40.3 |
| | CoT | 63.2 (+3.5) | 36.8 (-3.5) |
| | CoT-SC (k = 16) | 61.7 (+2.0) | 38.3 (-2.0) |
| | **CR (ours**, $n$ = 4) | **72.5** (+12.8) | 27.5 (-12.8) |

图 3:AutoTNLI 数据集对比测试结果

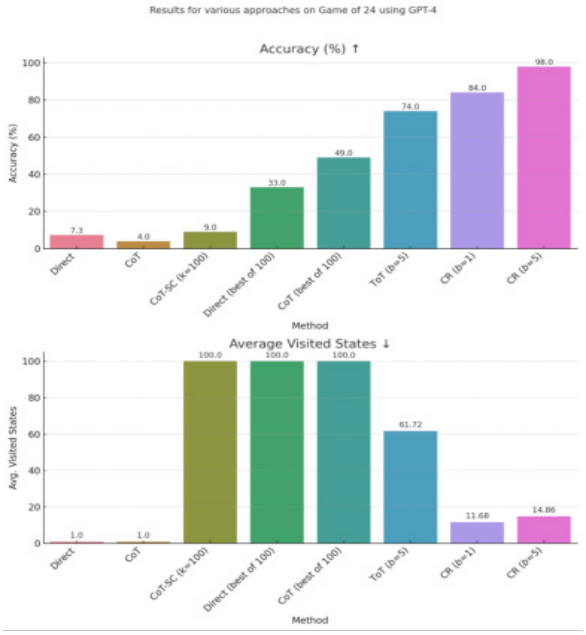



图 4: 24 点游戏对比测试结果

Table 5: Comparative performance on the MATH dataset using GPT-4. We adopted a default temperature setting of $t = 0.0$, consistent with prior research settings (greedy decoding). PHP denotes the application of the progressive-hint prompting. "Iters" represents the average number of LLM interactions, and **Overall** reflects the overall results across MATH subtopics.

| | w/ PHP | MATH Dataset (* denotes using 500 test examples subset following Lightman et al. (2023)) | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| | | InterAlgebra | Precalculus | Geometry | NumTheory | Probability | PreAlgebra | Algebra | **Overall** |
| CoT (OpenAI, 2023) | ✗ | - | - | - | - | - | - | - | 42.50 |
| Complex CoT, 8-shot (Zhang et al., 2023) | ✗ | 23.4 | 26.7 | 36.5 | 49.6 | 53.1 | 71.6 | 70.8 | 50.36 |
| | ✓ | 26.3 | 29.8 | 41.9 | 55.7 | 56.3 | 73.8 | 74.3 | 53.90 |
| | (Iters) | 3.2414 | 3.2435 | 3.2233 | 3.1740 | 2.8122 | 2.3226 | 2.4726 | 2.8494 |
| Complex CoT* (repro., 8-shot) | ✗ | 29.9 | 33.9 | 34.1 | 46.8 | 47.4 | 62.1 | 70.7 | 48.80 |
| | ✓ | 28.9 | 30.4 | 43.9 | 53.2 | 50.0 | 68.5 | 84.1 | 53.80 |
| | (Iters) | 2.7629 | 2.4643 | 2.7805 | 2.7581 | 2.4474 | 2.3780 | 2.5484 | 2.59 |
| **CR*** (ours, 4-shot) | ✗ | 28.9 (-1.0) | 30.4 (-3.5) | 39.0 (+4.9) | 54.8 (+8.0) | 57.9 (+10.5) | 71.8 (+9.7) | 79.3 (+8.6) | **54.20** (+5.40) |
| | ✓ | **32.0** (+3.1) | **35.7** (+5.3) | **43.9** (+0.0) | **59.7** (+6.5) | **63.2** (+13.2) | **71.8** (+3.3) | **86.6** (+2.5) | **58.00** (+4.20) |
| | (Iters) | 2.6598 | 2.4821 | 2.5122 | 2.2903 | 2.2105 | 2.2195 | 2.3548 | **2.40** (-0.19) |

Table 6: Comparative performance on the MATH dataset using GPT-4 for different difficulty levels.

| | w/ PHP | MATH Dataset (* denotes using 500 test examples subset) | | | | | |
|---|---|---|---|---|---|---|---|
| | | Level 5 | Level 4 | Level 3 | Level 2 | Level 1 | **Overall** |
| CoT (OpenAI, 2023) | ✗ | - | - | - | - | - | 42.50 |
| Complex CoT* (repro., 8-shot) | ✗ | 22.4 | 38.3 | 62.9 | 72.2 | 79.1 | 48.80 |
| | ✓ | 23.9 | 43.8 | 63.8 | 86.7 | 83.7 | 53.80 |
| **CR*** (ours, 4-shot) | ✗ | **32.1** (+9.7) | 43.0 (+4.7) | 62.9 (+0.0) | 78.9 (+6.7) | 83.7 (+4.6) | **54.20** (+5.40) |
| | ✓ | 27.3 (+3.4) | **50.0** (+6.2) | **70.9** (+7.1) | **86.7** (+0.0) | **90.7** (+7.0) | **58.00** (+4.20) |

图 5: MATH 数据集对比测试结果

“累积推理”框架不仅被证明可以在逻辑推理任务中实现更高的准确率，也为人工智能领域带来了新的启示和可能性。研究组表示，随着这种“步步为营”的方法不断完善，在解决复杂的数学与科学问题上，人类有望迎来能够独立完成研究的 AI Mathematician（人工智能数学家）。但研究者们承认，这样的远景目标仍面临“如何对大语言模型输出结果进行高效验证”、“如何增加思考上下文的长度，以处理更加复杂的问题”等挑战。

该成果研究论文：Yifan Zhang, Jingqin Yang, Yang Yuan, Andrew Chi-Chih Yao, "Cumulative Reasoning with Large Language Models", https://arxiv.org/abs/2308.04371.

# 基于替换的可解释性算法中有效性与一致性的权衡

在当前的深度学习可解释性背景中，大多数主流方法（如 SHAP 和 LIME）是通过模拟来忽视特定特征的各种场景，并采用基于替换的技术来评估单个特征的影响。然而这些方法主要强调在原始上下文中的有效性，通常会导致普遍的不一致性。袁洋研究组通过建立不可能三角定理，证明了这种不一致性是这些方法固有的内容，该定理认为可解释性、有效性和一致性无法同时保持。研究人员也认识到获得理想解释仍然是难以捉摸的，对此该研究组提出使用解释误差作为衡量有效性和一致性不足的指标；为此研究人员提出了两种基于标准多项式基的新算法，旨在最小化解释误差。实验表明，提出的方法在减少解释误差方面取得了显著成效，与其他技术相比，解释误差降低了多达 31.8 倍。

有效性指的是经过可解释性算法归因后，输入特征的贡献之和与网络输入值之间有恒等关系。不一致性（图 1）指的是，在解释算法对输入进行解释后，输入内容发生微小改变，此时再次使用解释算法解释改变后的输入，能够发现改变前和改变后的输入之间的相同部分的贡献值发生了大幅改变。这种不一致性将在特定的解释场景下给使用者带来很大困惑。

该研究组设计了 Harmonica 算法，利用了在布尔基上进行的傅里叶分解解决了解释算法的不一致性，并达到了更好的解释效果（图 2）。


图 1：可解释性中的不一致性。当删掉 very 后，可解释性算法对剩余单词上的贡献大幅改变

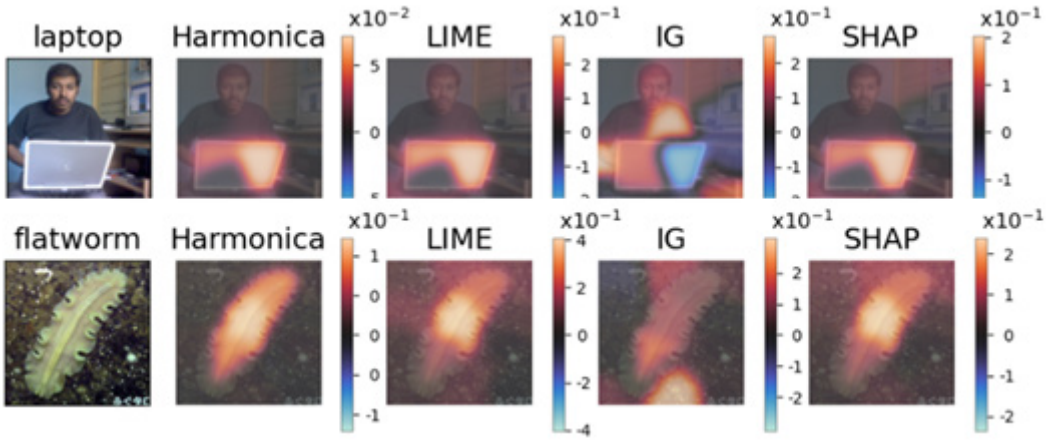



图 2：单体（上）与多体（下）情况下对真实实验体系的模拟结果

此外，该研究组进一步对输入空间切分开发了 Harmonica-anchor 算法。Harmonica-ancho 在减少解释误差方面取得了显著成效，与其他技术相比，解释误差降低了多达 31.8 倍（图 3）。

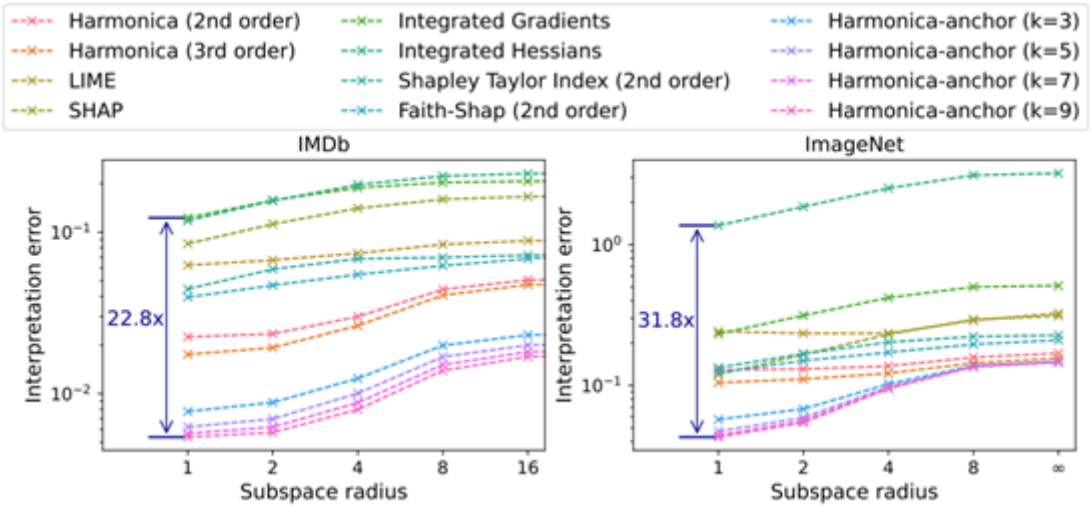



图 3：Harmonica、Harmonica-anchor 以及其他基线算法在自然语言任务上的解释误差。

该成果研究论文：Yifan Zhang, Haowei He, Zhiquan Tan, Yang Yuan, "Trade off Between Efficiency and Consistency for Removal-based Explanations", NeurIPS 2023.

# GLIME: 基于 LIME 的通用、稳定以及忠诚的解释方法

机器学习解释方法通过解释黑盒机器学习模型的行为帮助人们更好地理解机器学习模型的行为。在众多解释方法中，LIME 因其在图像分类任务中的应用而备受关注。然而，LIME 存在显著的不稳定性，其解释在不同的随机种子下产生明显差异，可能误导终端用户，同时也限制了模型错误和偏见的识别。此外，LIME 的局部准确性不佳，导致解释缺乏一致性，具体表现为对不同基准输入产生不同解释的情况（图 1）。

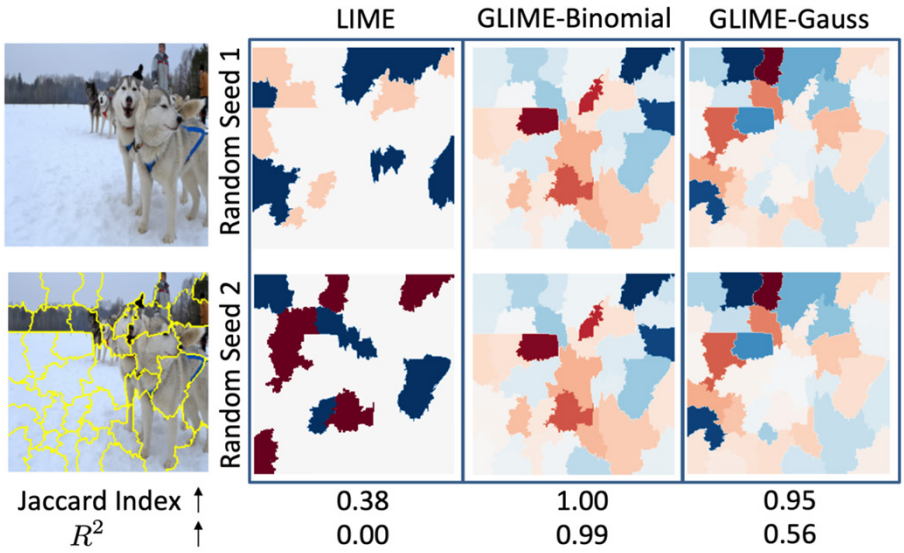



图 1: 在使用两个随机种子的小型 Swin-Transformer 上，对 ImageNet 图像进行 LIME 和 GLIME 解释。使用 σ=0.25 和样本大小为 16384。第二行下方呈现的数值代表两个解释图之间的 Jaccard 指数。

为解决这些问题，研究人员提出了 GLIME 框架，作为 LIME 的一种扩展。在 GLIME 中，研究人员通过引入灵活的采样分布设计，提高了解释的稳定性和局部准确性。具体而言，研究人员推导出一种和 LIME 在样本数量无穷大时等价的方法 GLIME-Binomial，将权重集成到采样分布中，加速了模型的收敛过程，从而提高了解释的稳定性。此外，GLIME 通过从本地分布中采样，独立于特定参考点，增强了局部准确性（图 2 右）和解释的一致性（图 2 左）。

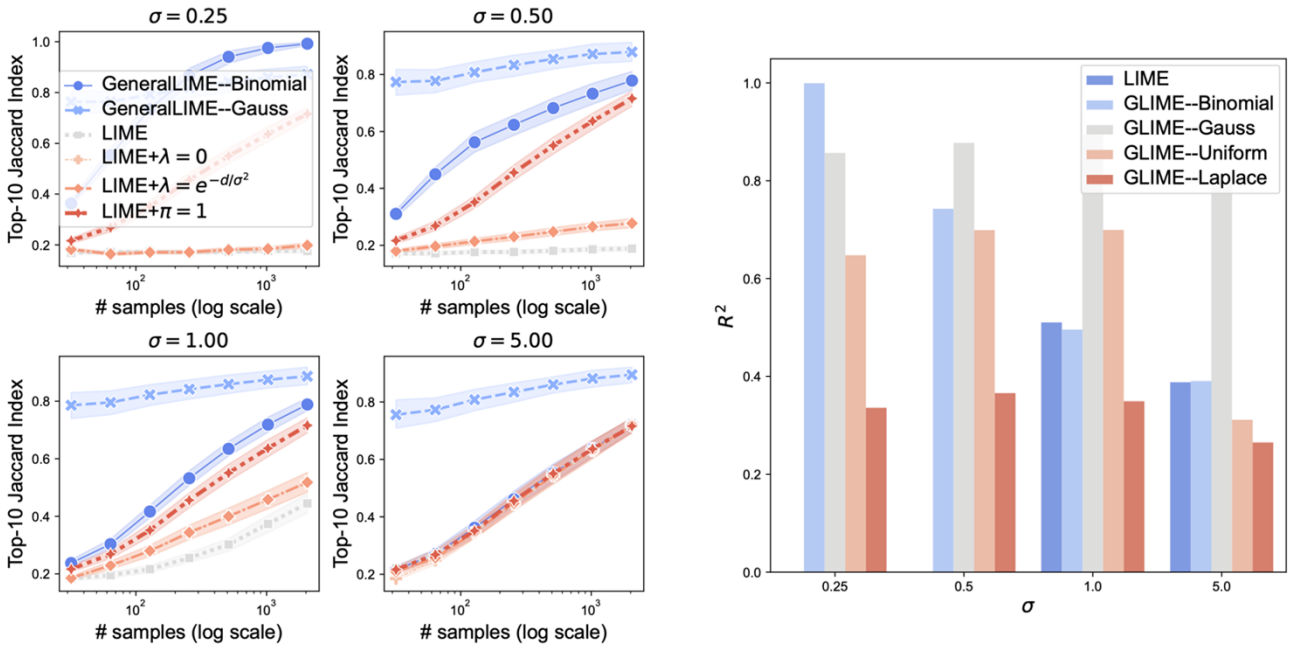



图 2:（左）各种方法的稳定性。当 σ 较小时，LIME 表现出不稳定性，而 GLIME 在不同的 σ 值下表现出增强的稳定性。在 σ 较大时，正则化和权重对 LIME 的稳定性影响较小。（右）LIME 与不同采样分布的各种 GLIME 方法的 R^2 比较。总体而言，LIME 的 $R^2$ 始终低于 GLIME 的 R^2，突显了 GLIME 在局部保真度方面的增强

此外，研究人员通过真人测试发现，GLIME 对于人类理解和选择模型更有帮助，GLIME 的打分明显超过 LIME（图 3）。

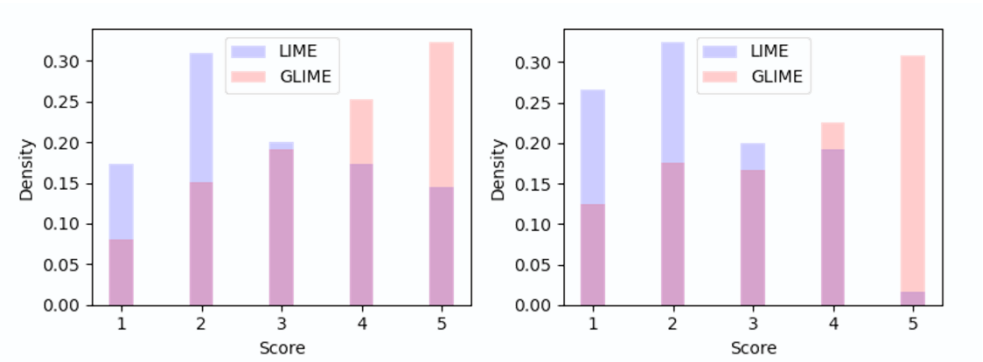


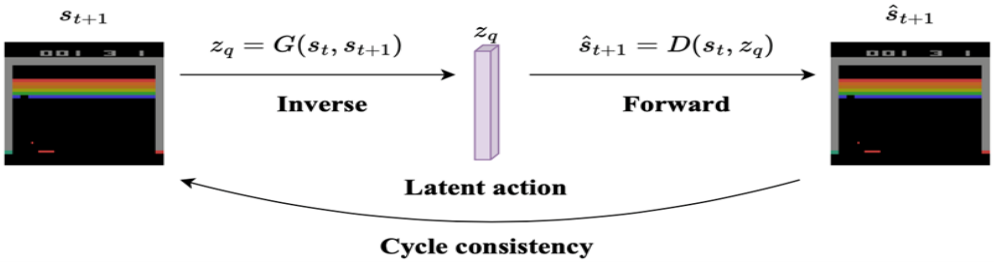

图 3: 人类实验结果。（左）参与者一致性地将 GLIME 的评分明显高于 LIME，表明 GLIME 作为一种更有效的工具，用于解释模型的预测。（右）参与者一致性地将 GLIME 的评分明显高于 LIME，表明 GLIME 在更有效地识别模型错误方面优于 LIME

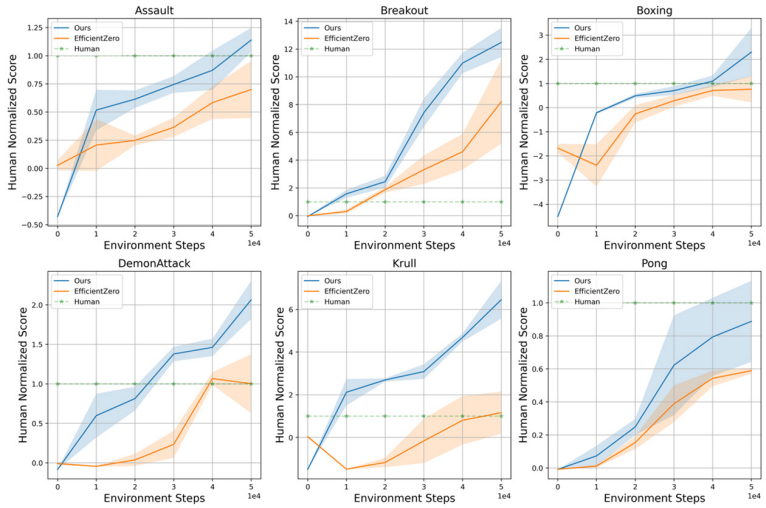
该成果研究论文：Zeren Tan, Yang Tian, and Jian Li, "GLIME: General, Stable and Local LIME Explanation", Thirty-seventh Conference on Neural Information Processing Systems. 2023.

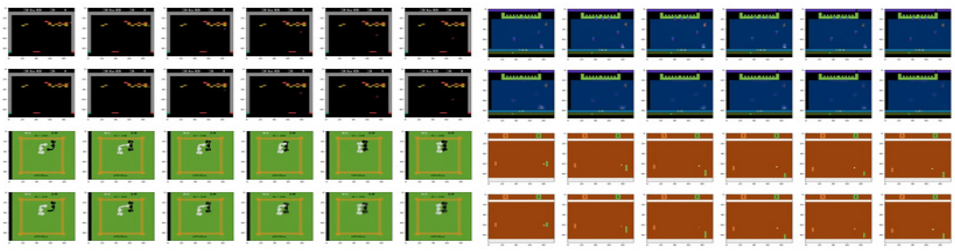
# 一种针对基于模型的强化学习算法的预训练方法

样本效率和泛化性向来是强化学习中最重要的研究问题之一。受启发于无监督预训练方法在计算机视觉和自然语言处理领域的成功，高阳研究组提出一种针对基于模型的强化学习算法的预训练方法。这种预训练方法利用向量量化的方式提取相邻两帧的隐式动作表达，然后通过一种新颖的前向 - 反向循环一致性损失函数（FICC）进行预训练。因此，它能够利用纯视频数据对强化学习算法模型进行预训练（包括特征模型和状态转移模型），而无需每一帧的动作标签。预训练后，对于给定的下游任务，在微调的时候，仅需使用统计方式得到对应的动作映射表，使得真实的动作能够映射到对应隐式动作表达。该研究组提出的预训练方法能够在 1 小时 Atari 游戏数据上超过原有算法 85.6% 的性能，样本效率得到较大提升；此外，此方法无需动作标签，能够对同一个模型进行多环境多任务的预训练，从而提升模型的泛化性。这也为基于模型的强化学习算法在真实场景中的落地提供了更大可能。

该成果研究论文：Weirui Ye, Yunsheng Zhang, Pieter Abbeel, Yang Gao, "Becoming A Proficient Player with Limited Data through Watching Pure Videos", FICC 2023.



# 对于应用在机器人控制的预训练视觉模型，并非所有策略学习方法都是平等的

在现代深度学习中，将预训练模型迁移到各种下游任务中是一个普遍模式。这种方法已经彻底改变了计算机视觉、自然语言处理等其他领域。越来越多的研究也专注于将这些预训练模型作为基于视觉运动控制的基石。由于这些模型通常是在大规模的视觉数据上进行训练，它们的特征拥有关于世界及其属性的语义的一般性知识，这对于通用控制来说极为宝贵。

然而，迄今为止的研究重点主要在于如何更好地进行预训练。为了学习下游控制策略，之前的工作通常在强化学习或模仿学习方法上做出权宜之计，导致下游控制策略对最终性能影响的理解不足。一个给定的预训练视觉模型是否能在不同的下游策略学习方法中保持一致的有效性？如果不行，人们能解释这种差异吗？考虑到多种可能的下游策略学习方法，人们应该如何评估预训练视觉模型？

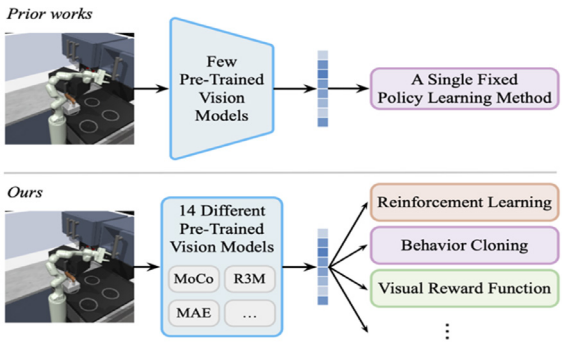
为了回答这些问题，高阳研究组对多种预训练视觉模型进行大规模的基准测试。研究人员一共考虑了三种策略学习算法：强化学习（RL），通过行为克隆进行的模仿学习（BC），使用视觉奖励函数的模仿学习（VRF）。一共测试了 14 种预训练视觉模型，涵盖了不同的架构和流行的预训练方法。为了进行公平和全面比较，研究人员在 3 种机器人操控环境中的 21 个模拟任务上进行了广泛实验，包括 Meta-World、Franka-Kitchen 和 Robosuite。论文中揭示了一些重要结果：

1. 缺乏始终如一的高性能模型。预训练视觉模型的有效性高度依赖于下游策略学习方法。

2. 指出可靠评估方法的方向。由于结果有很大方差，RL 不是一种稳健的评估方法。而 VRF 和 BC 的结果有很强的一致性，使它们成为对预训练视觉模型进行基准测试的可靠评估方法。

3. 在对视觉模型属性的深入探究中，获得了诸如线性损失和 k-NN 分类准确率等具有对模型表现有预测能力的指标。

该成果研究论文：Yingdong Hu, Renhao Wang, Li Erran Li, Yang Gao, "For Pre-Trained Vision Models in Motor Control, Not All Policy Learning Methods are Created Equal", arXiv:2304.04591.



# 利用隐空间扩散模型实现自然语言指导视频预测

通过当前环境观察分析预测并基于先验知识去预想未来的轨迹是机器人做出合理规划并成功实现目标的关键。 因此，文本条件视频预测是促进通用机器人策略学习的一项重要任务。具体来说，限制文本条件视频预测任务性能的问题主要有 3 个：

1) 对大规模标记文本视频数据集的要求和昂贵的计算成本：学习捕获两种不同模态之间的对应关系并非易事，需要大量有监督的文本视频和过多的训练计算开销 。

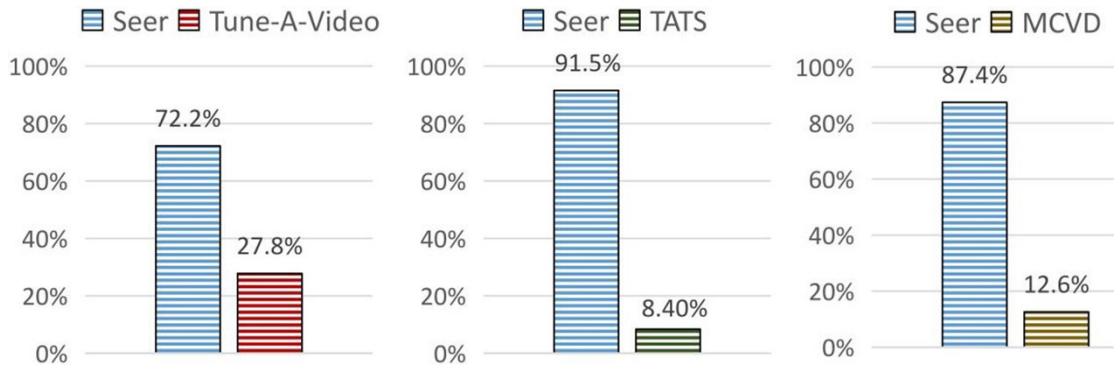
2) 生成帧的保真度低：模型生成的帧通常是独立随机的，无法清晰地显示参考帧中指定的背景和对象。

3) 任务级视频中的每一帧缺乏细粒度的指令：文本指令指定的目标通常描述任务级行为，这使得仅以全局文本嵌入为条件理解行为轨迹并在每个时间步生成相应的帧变得困难。

为了解决这一任务并赋予机器人预见未来的能力，研究人员提出了一个样本和计算高效的模型，名为 Seer，通过沿时间轴膨胀文本到图像的冻结预训练扩散模型。 研究组通过结合计算高效的时空注意力来增强 U 型网络结构和语言条件模型。 此外，研究人员引入了一种新颖的延帧的时间顺序分解语言指令的分解器模块，该模块将句子的全局指令分解为时间对齐的子指令，确保精确对齐到每个生成帧中。 该框架使得模型能够有效地利用跨领域的预训练文本到图像模型中获取通用的图像生成先验知识。

凭借上述适应性设计的架构，Seer 可以通过在少量数据上微调几个层来生成高保真、连贯且指令对齐的视频帧。并在标准人类以及机器行为的视频数据集上的实验结果表明，该方法在大约 480 个 GPU 小时的视频预测性能优于具有超过 12,480 个 GPU 小时的当前开源视频生成基准模型 CogVideo：与当前的最优模型相比，实现了 31% 的弗雷歇视频距离 (FVD) 指标的提升，并且人类观察评估中，该方法生成结果相比其他基准模型达到更高的 83.7% 的平均择优率。

该研究组提出方法 Seer 使用帧顺序文分解器设计了一个数据和计算高效的视频网络，以沿时间轴膨胀预训练的文本到图像稳定扩散模型。 凭借预训练文本图像生成模型包含的丰富先验知识和精心设计的架构，Seer 仅通过微调自回归空间时序注意力层和帧顺序文分解层实现生成了高质量视频，从而显著降低了数据和计算成本。




人类评估结果，单位为择优率百分比

| Method | Pre.-weight | Text | Resolution | SSv2 FVD↓ | SSv2 KVD↓ | Bridge FVD↓ | Bridge KVD↓ | Epic100 FVD↓ | Epic100 KVD↓ |
|---|---|---|---|---|---|---|---|---|---|
| TATS (Ge et al., 2022) | video | No | 128 × 128 | 428.1 | 2177 | 1253 | 6213 | 920.0 | 5065 |
| MCVD (Voleti et al., 2022) | No | No | 256 × 256 | 1407 | 3.80 | 1427 | 2.50 | 4804 | 5.17 |
| SimVP (Gao et al., 2022) | No | No | 64 × 64 | 537.2 | 0.61 | 681.6 | 0.73 | 1991 | 1.34 |
| MAGE (Hu et al., 2022b) | video | Yes | 128 × 128 | 1201.8 | 1.64 | 2605 | 3.19 | 1358 | 1.61 |
| PVDM (Yu et al., 2023) | No | No | 256 × 256 | 502.4 | 61.08 | 490.4 | 122.4 | 482.3 | 104.8 |
| VideoFusion (Luo et al., 2023) | txt-video | Yes | 256 × 256 | 163.2 | 0.20 | 501.2 | 1.45 | 349.9 | 1.79 |
| Tune-A-Video (Wu et al., 2022b) | txt-img | Yes | 256 × 256 | 291.4 | 0.91 | 515.7 | 2.01 | 365.0 | 1.98 |
| Seer (Ours) | txt-img | Yes | 256 × 256 | **112.9** | **0.12** | **246.3** | **0.55** | **271.4** | 1.40 |

文本条件视频预测在三个主流数据集的定量对比结果。 该结果以弗雷歇视频距离 (FVD) 和核视频距离 (KVD) 指标为判断标准

该成果研究论文 : Gu, Xianfan, Chuan Wen, Jiaming Song, and Yang Gao, "Seer: Language Instructed Video Prediction with Latent Diffusion Models", arXiv preprint arXiv:2303.14897 (2023).

# 针对机器人操控的通用“语义 - 几何表征”

机器人在感知和与世界交互时高度依赖传感器，尤其是 RGB 摄像头和深度摄像头。RGB 摄像头记录了具有丰富语义信息的 2D 图像，但缺失了精确的空间信息；另一方面，深度摄像头提供了关键的 3D 几何数据，但捕获的语义信息有限。因此，整合这两种模式对于机器人感知和控制的表征是至关重要的。

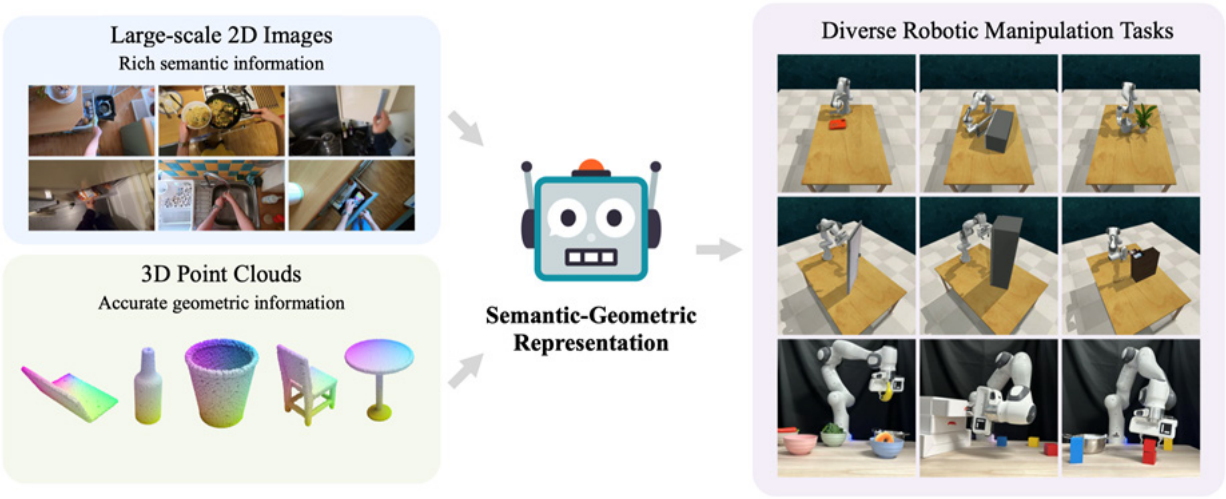



图 1：“语义 - 几何表征”：利用来自大量 2D 图像的语义信息和来自 3D 点云的几何信息，研究人员提出了“语义 - 几何表征”，其使机器人能够完成一系列仿真和现实世界的操控任务

然而，当前的研究主要集中在其中一种模式上，忽视了结合两者的好处。为了解决这个问题，高阳研究组提出了“语义 - 几何表征”（SGR，图 1），这是一个针对机器人的通用感知模块，它不仅充分利用了大规模预训练 2D 模型中的丰富语义信息，还结合了 3D 空间的推理优势。研究人员的实验结果显示，“语义 - 几何表征”使机器人能够出色地应对各类仿真与实际场景中的任务，无论是单任务还是多任务情境，其表现都超过 SOTA。值得一提的是，SGR 在处理新的语义属性上展现了出色的泛化能力，这一特性也使其显著区别于其他技术。

该成果研究论文：Zhang, Tong, Yingdong Hu, Hanchen Cui, Hang Zhao, and Yang Gao, "A Universal Semantic-Geometric Representation for Robotic Manipulation", In Conference on Robot Learning, pp. 3342-3363. PMLR 2023.

# 基于状态距离信息迭代式学习多样性策略

不同于监督学习，强化学习可能会在同一种任务上学习到不同的解决任务方式。发现多样化策略是深度强化学习研究中的一项根本问题，并且有重要的实践意义——设计鲁棒机器人步态、促进人类和 AI 的交互合作、发现新型分子和药物等等，都离不开强化学习得到的多样化策略。

吴翼和张景昭研究组合作总结并分析了先前学习多样化策略的工作，并针对设计算法的两个关键选择进行重点探讨。第一个关键点是如何选择“多样性”的测量方式。先前的工作大多基于智能体的动作或者状态分布来反映策略之间的多样性，然而，该论文通过举出反例，说明了这些方法可能会给相似的策略很高的多样性分数。内在的原因是，动作或策略分布仅仅隐式反映行为的不同，但是策略的相似性本质体现在状态之间的距离上。第二个关键点是如何选择发现多样性算法的计算框架。主流的框架包括基于种群学习（population-based training, PBT）和迭代式学习（iterative learning, ITR）。PBT 是精确的计算框架，但有较高的计算复杂度；ITR 复杂度低，但是不一定能得到精确解。该论文通过理论分析指出，ITR 在放松多样性约束的条件下能得到和 PBT 同样精确的解，这说明在实践上 ITR 更适合作为发现多样性算法的计算框架。

根据以上的分析，该论文结合了基于状态距离的多样性测量方式和迭代式学习，开发了一种新颖的多样性强化学习算法，并在高纬度机器人控制和复杂多智能体游戏中取得了优异表现。具体而言，该算法能够仅通过图片观察学习到不同的机器人步态，也能够在多智能体足球游戏中学习到和人类行为相符的复杂传球策略，这些行为都是变换随机种子或利用先前算法无法发现的。

该成果研究论文：Wei Fu, Weihua Du, Jingwei Li, Sunli Chen, Jingzhao Zhang, and Yi Wu, "Iteratively Learn Diverse Strategies with State Distance Information", NeurIPS 2023.

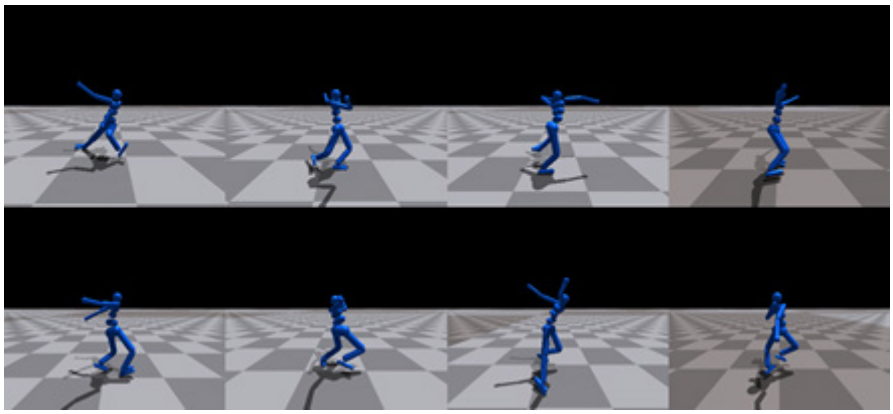


图 1：基于状态（上）和图片（下）输入学习到的多样化机器人前行步态

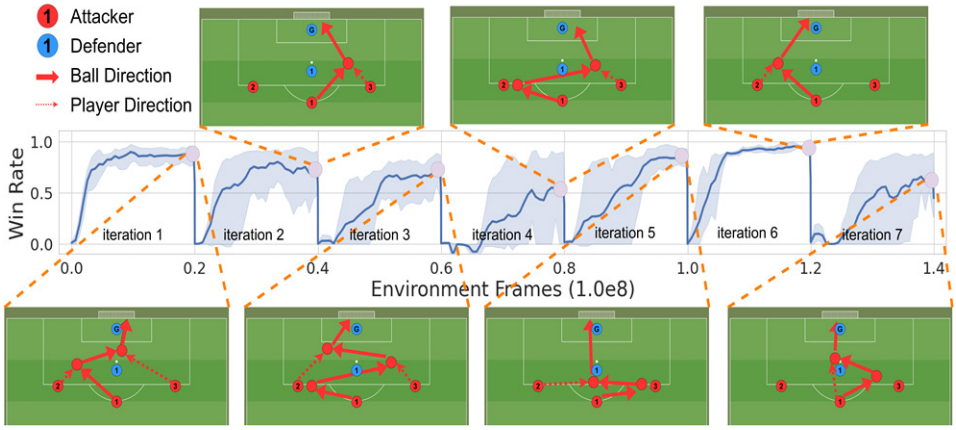


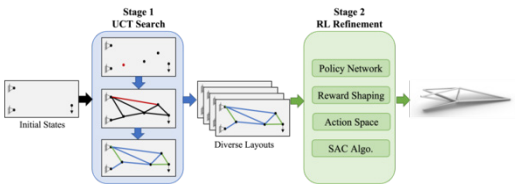

图 2：在多智能体足球环境中，前 7 次迭代中每次迭代学习到的不同传球和进攻方式

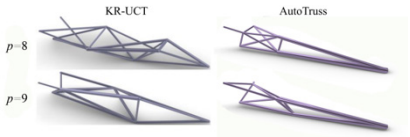
# 基于强化学习的自动桁架优化方法

桁架结构是一种常见的工程结构形式，广泛应用于各种建筑，由杆件按照一定的几何形式连接构成。桁架优化涉及节点位置、节点之间的拓扑和连接杆的横截面积的优化，是一个复杂的组合优化问题。由于解空间巨大，简单地用计算机进行穷举式搜索并不可行，需要耗费大量的时间和计算资源。强化学习可以进行桁架布局的优化，但存在奖励稀疏，训练困难的问题。

为解决这一问题，吴翼研究组创新性地提出了先搜索后精调的两阶段优化方法，先搜索出满足力学条件的基本解，然后在此基础上通过强化学习进行优化。在搜索阶段，使用应用于树的上置信界限法（Upper Confidence Bound applied to Trees，简称 UCT）搜索并找到多样化的有效桁架结构。在精细优化阶段，使用深度强化学习中的 Soft Actor-Critic 算法 ( 简称 SAC) 来进一步优化这些桁架结构。该方法能够有效避免现有优化方法中常见的陷入局部最优的问题，快速高效地生成轻量且符合物理约束的桁架结构，为建筑、汽车乃至航空航天等相关领域带来效益。

该成果研究论文：Weihua Du, Jinglun Zhao, Chao Yu, Xingcheng Yao, Zimeng Song, Siyang Wu, Ruifeng Luo, Zhiyuan Liu, Xianzhong Zhao and Yi Wu, "Automatic Truss Design with Reinforcement Learning", IJCAI 2023, to appear.

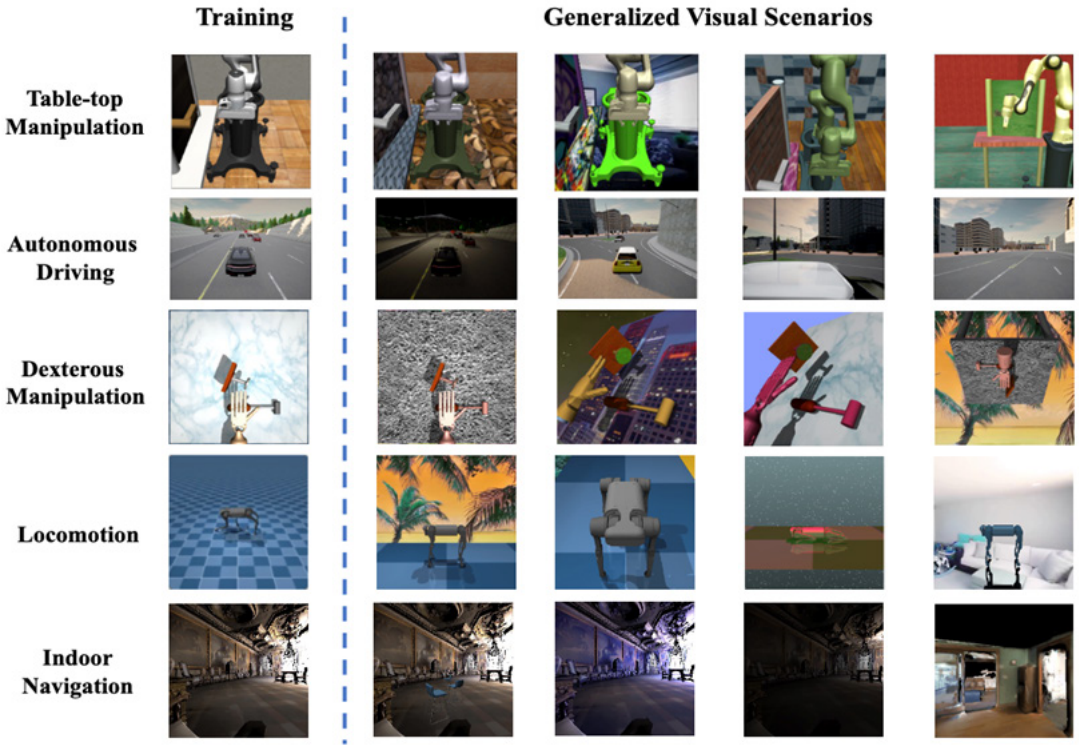


# RL-ViGen: 新型视觉强化学习测试基准

许华哲研究组提出了一种新型视觉泛化测试基准，解决了现有基准的不足之处，如：图像与真实世界输入之间的差距较大、任务类型单一和多样性差等问题，为开发真正具备全面视觉泛化能力的强化学习智能体打下坚实基础。该文的基准包括五种不同类型的泛化任务，并包含多样的泛化种类，可以从多个维度评估算法的泛化能力。此外，该文还在一个统一的运行框架下集成了各种算法，使得对各算法的有效性进行公平和合理的评估成为可能。

该成果研究论文：Zhecheng Yuan, Sizhe Yang, Pu Hua, Can Chang, Kaizhe Hu, Huazhe Xu, "RL-ViGen: A Reinforcement Learning Benchmark for Visual Generalization", arXiv:2307.10224。



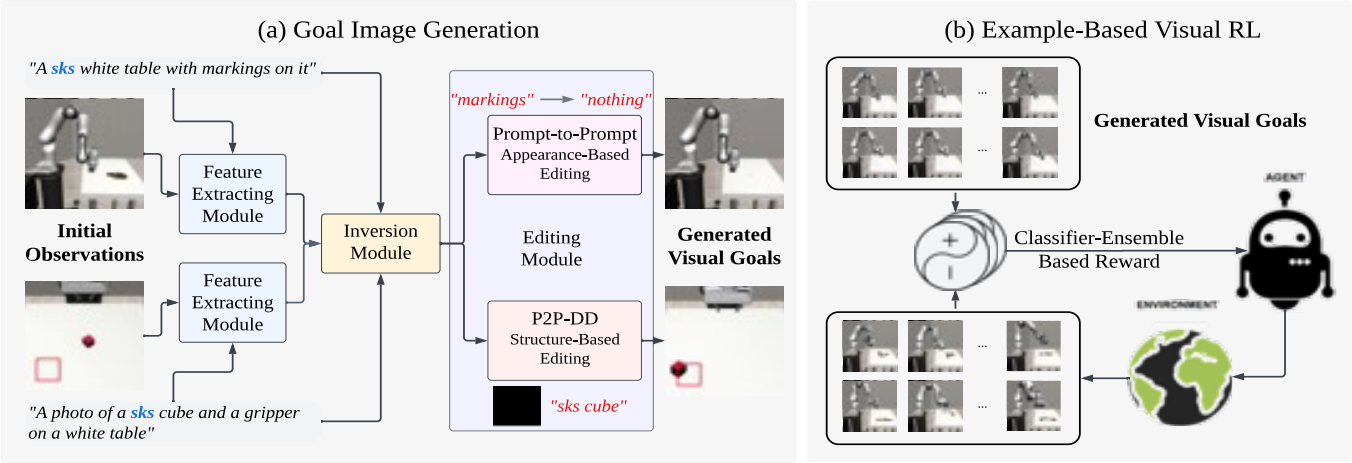
# 预训练图像生成模型能否为强化学习提供视觉目标?

预训练大模型中通常内嵌了关于世界的很多先验知识，如何将这些先验知识提取并为强化学习智能体所用，是值得研究的问题。

在该工作中，许华哲研究组研究利用基于文本转图片的扩散模型进行图像编辑得到目标图像，进而指导视觉强化学习智能体完成任务的范式。在第一阶段，研究人员提出的方法可以根据文本描述编辑当前图片，得到有意义的目标图像，如将有污渍的桌面擦干净等。研究人员添加了特别的方法来保证在编辑过程中保持背景和无关图像不改变。在第二阶段，研究人员训练区分编辑后图像和未编辑原始图像的分类器，并用其指导强化学习智能体完成任务。

该研究组的方法在多种模拟环境中取得了很好的效果，同时不需要任何的奖励函数设计或专家示例。同时，研究人员在真实环境中进行了图像编辑，并证明了分类器训练得到的奖励函数能够为强化学习智能体的训练提供有意义的指导。

该成果研究论文：Gao, J., Hu, K., Xu, G., & Xu, H., "Can Pre-Trained Text-to-Image Models Generate Visual Goals for Reinforcement Learning?", ArXiv, abs/2307.07837.

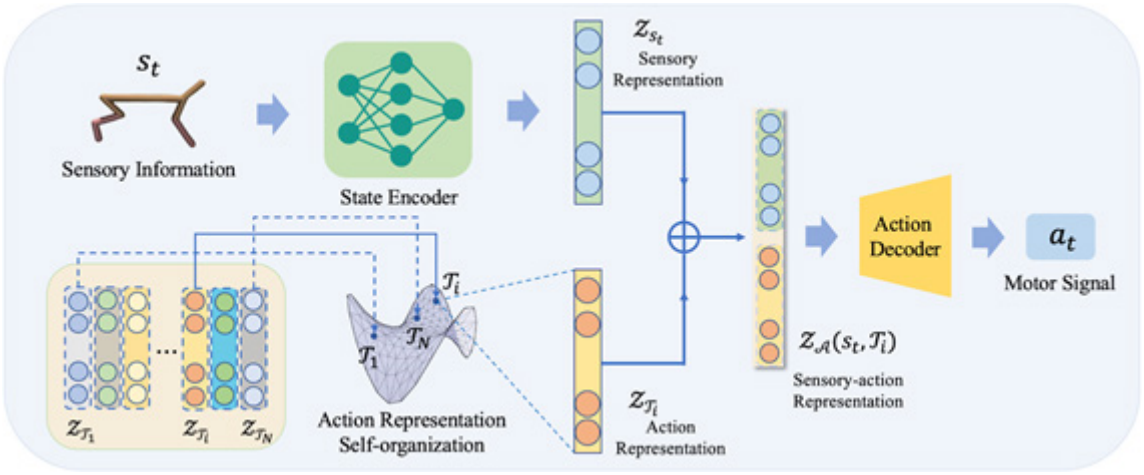


# 使用多任务强化学习得到自组织的动作表征空间

人类执行多项任务时，研究人员会自然地将底层的肌肉运动概括为顶层的、更抽象的“动作表征”，例如“拿起物体”或“向左转”，这些表征只需稍作修改即可在新的任务中重复使用。通过类比人类的这种能力，人们希望强化学习中的智能体也能拥有将底层的运动控制抽象为顶层的动作表征，然后它们可以通过重复使用、修改或组合这些动作表征来执行新任务。

为了解决以上问题，研究组提出在多任务学习的框架下使智能体学习到可泛化的动作表征，从而实现任务层面对新的未接触任务的泛化。在训练过程中，时变的感知信息与时不变的动作信息被解耦，而后两者拼接成为感知 - 动作表征并被策略网络转化为底层的动作控制信号。经过训练，智能体学习到了一个自组织的动作表征空间，在表征空间内对预训练的任务表征向量进行简单的插值、组合以及搜索都能够十分高效地获得新任务的动作表征。

该成果研究论文：Hua, Pu, Yubei Chen, and Huazhe Xu, "Simple Emergent Action Representations from Multi-Task Policy Training", arXiv preprint arXiv:2210.09566 (2022).



# 基于可扩展的仿真、专家演示和模仿学习人机交接问题

长期以来，具身智能研究一直以赋予机器人与人类互动、协作的目标为动力。在这一追求中，重要的方向之一是使机器人能够基于动态视觉观察可靠地接收由人类递交的几何形状各异、运动轨迹任意的物体。这种人对机器人（H2R）递交的能力使得机器人能够在包括烹饪、居室整理和家具组装等多样任务中与人类无缝协同合作。

为了实现这一目标，弋力研究组提出了 GenH2R，一个学习通用基于视觉的人机（Human to Robot，H2R）交接技能框架。该研究组的目标是使机器人能够可靠地接收人类以各种复杂轨迹递交的具有未知几何形状的物体。为了达到这个通用性，研究人员采用了一整套综合性解决框架，包括程序化地创建海量仿真环境，自动生成有效的专家演示和进行有效的模仿学习。该研究组充分利用大规模的 3D 模型库、熟练的抓取生成方法以及基于曲线的 3D 仿真动画，创建了一个名为 GenH2R-Sim 的 H2R 交接模拟环境，其场景数量超过现有模拟器的三个数量级。为了支持学习，研究人员还引入了一种适用于仿真的专家演示生成方法，该方法可以自动生成适用于学习的百万级别高质量专家演示。最后，弋力研究组提出了一种 4D 模仿学习方法，通过未来预测目标来将演示提炼成视觉 - 动作交接策略。如图 1 所示：

该研究组在现有的研究基础上，提出了大规模的训练集与测试集，以及提出了更适合通用人机交接场景的评测指标。研究人员在所有情况下都超过了最好的基线水平，取得了较大幅度的改进（至少 +10% 的成功率）。

该成果研究论文：Zifan Wang, Junyu Chen, Ziqing Chen, Pengwei Xie, Rui Chen, Li Yi，“GenH2R: Learning Generalizable Human-to-Robot Handover via Scalable Simulation, Demonstration, and Imitation”，https://arxiv.org/abs/2401.00929.

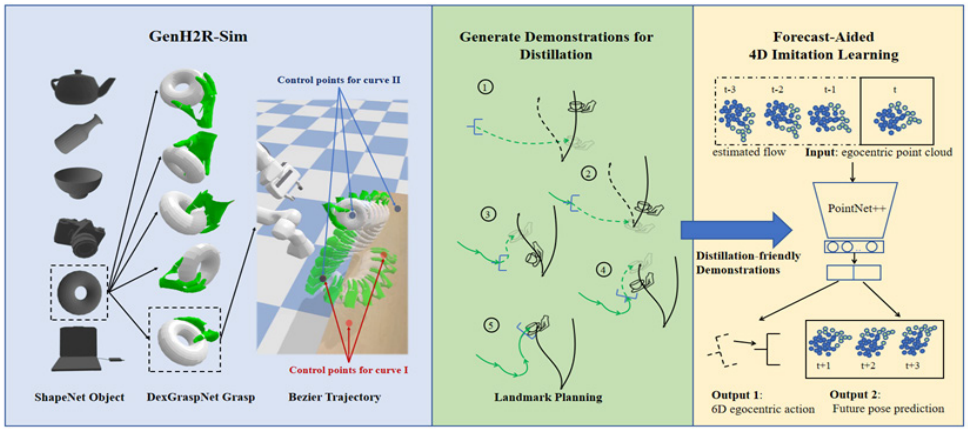


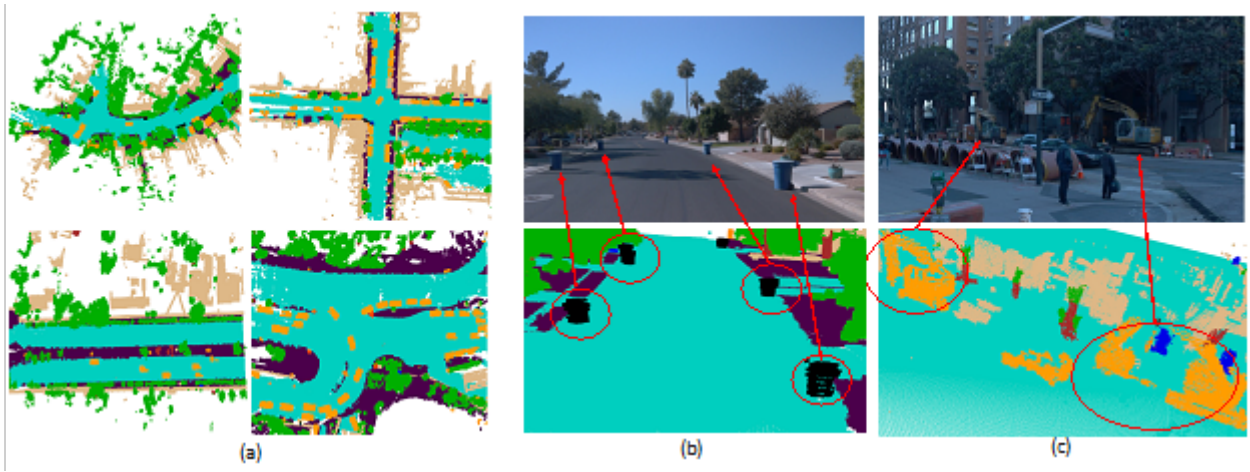

图 1：GenH2R-Sim 整体框架图，可以有效地生成百万级别人机交接场景，提供高质量的基于标志点规划的专家演示，以及进行基于未来预测的 4D 模仿学习

| | s0 (Sequential) | | s0 (Simultaneous) | | t0 | | t1 | |
|---|---|---|---|---|---|---|---|---|
| | S | AS | S | AS | S | AS | S | AS |
| Handover-Sim2real | 65.97 | 29.5 | 62.50 | 33.5 | 33.71 | 18.4 | 47.10 | 24.1 |
| Ours | **87.27** | **35.8** | **84.03** | **48.0** | **40.43** | **25.4** | **62.40** | **32.8** |

图 1：部分实验结果图，在所有的测试集上，该研究组的模型都能对基线模型取得大幅度的领先，其中 S 表示成功率 (Success)，AS 表示平均成功 (Average Success)

# 自动驾驶三维占用预测数据集 Occ3D

自动驾驶的感知系统需要准确地知道环境的三维几何和语义信息。现有的感知方法主要侧重于估计 3D 物体框，往往忽略了更为细致的几何结构，以及预设类别以外的物体，即通用障碍物。针对这些问题，借鉴机器人中的占用建图问题，赵行研究组定义了自动驾驶中的三维占用预测（3D Occupancy Prediction）任务和指标，即模型需要给出三维空间中每一个位置的占用状态和语义分类。基于此，研究组提出了高效的 Coarse-to-Fine Occupancy 网络模型用于解决该问题。与此同时，建立了基准数据集 Occ3D，该基准数据集被 CVPR2023 自动驾驶大赛所采纳，获得了来自全球一百多个团队的参赛和使用，在学术社区中产生了广泛影响。




图：Occ3D 数据集。（a）多样化的场景；（b）预设类别以外的物体，如垃圾桶；（c）异形障碍物，如吊车

该成果研究论文：Xiaoyu Tian, Tao Jiang, Longfei Yun, Yucheng Mao, Huitong Yang, Yue Wang, Yilun Wang, Hang Zhao, "Occ3D: A Large-Scale 3D Occupancy Prediction Benchmark for Autonomous Driving", NeurIPS 2023 Dataset Track.

# 超快速的生成模型 LCM

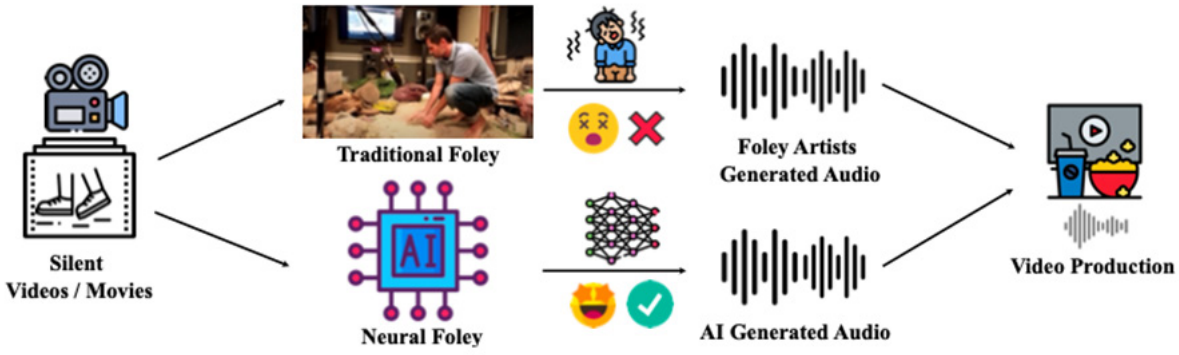
随着扩散模型的流行，文生图的质量有了大幅度的提升。然而扩散模型的最大不足在于其生成速度过慢，在推理时往往要迭代几十到上千步，大幅限制了其在工业界中的实际应用。基于领域的先驱工作一致性模型（Consistency Model），赵行研究组提出了潜在一致性模型 LCM（Latent Consistency Model），首次将扩散模型的推理达到 2-4 步，速度提升了 5-10 倍。LCM 的出现，让文生图问题进入了实时时代，并且使得推理成本大幅下降。LCM 发布后，登顶开源社区 HuggingFace，Replicate 的最热门应用，获得了百万点击量和数万的下载量，行业领头公司 Stable Diffusion 也跟进使用了 LCM。

基于 LCM，研究组联合 HuggingFace 发布了 LCM-LoRA，一种基于 LoRA 的可泛化的 LCM。具体来说，LCM-LoRA 可以在不需要领域数据微调的情况下，通过模型参数叠加的方式，直接加速各种风格数据的 LoRA 模型，大幅扩展了 LCM 的使用范围，让普通人都能用上 LCM。


该成果研究论文：Simian Luo, Yiqin Tan, Longbo Huang, Jian Li, Hang Zhao, "Latent Consistency Models: Synthesizing High-resolution Images with Few-step Inference", https://arxiv.org/abs/2310.04378.

# 视频配音 Diff-Foley

逼真的声音生成是一个重要的问题，也是影视行业长久以来的需求。在拍摄电影时，拟音师们往往会采用各种道具来模拟场景中的声音，例如打雷、下雨、海浪等。以往的声音生成模型质量不高，且无法和视频做到时序一致。赵行研究组提出了当前最逼真视频生成声音模型 Diff-Foley。具体来说，Diff-Foley 有预训练和扩散生成两个主要步骤：（1）利用视频和声音时序的一致性，进行大规模的对比预训练 CAVP（Contrastive Audio-Visual Pre-training），从而得到高质量的隐式特征；（2）训练一个以视频特征为条件的声音潜在扩散模型 Audio LDM，生成与视频时序一致的、高质量的声音。




图：传统的配音涉及到大量的人力劳动，Diff-Foley 用神经网络实现了基于视频的自动声音生成

该成果研究论文：Simian Luo, Chuanhao Yan, Chenxu Hu, Hang Zhao, "Diff-Foley: Synchronized Video-to-Audio Synthesis with Latent Diffusion Models", NeurIPS 2023.

# 二、计算机网络

主要完成人：房智轩研究组

## 带有 QoS 约束的去中心化在线资源分配

多人多臂赌博机（Decentralized multi-player multi-armed bandits，MP-MAB）模型是解决网络科学和运筹学中各类问题的一个有力框架，近年来引起了广泛关注。在这个框架中，有 N 个玩家在 T 轮内竞争拉动 K 个臂。玩家无法观察其他玩家的动作和获得的奖励，玩家间也不能进行显式的通信或协调。研究该框架的一个主要动机是分布式资源分配，因为在实际场景中以集中式的方式中协调大量用户是不可行的，当多个用户竞争相同资源时会出现冲突。MP-MAB 算法的目标是以分布式方式使得各玩家如何最优地分配这些资源。在这个目标下，已有文献主要关注的是玩家随时间累积的奖励总和。然而，在许多网络优化的场景中，该目标可能导致一些用户只被分配到较少的资源，即该目标没有个体收益或者服务质量 (QoS) 的保证。在许多应用中，每个用户都希望获得预期的 QoS，而最大化奖励总和的目标并不能实现这一点。

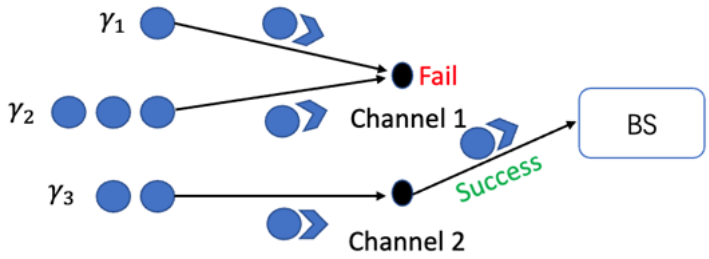



Figure 1: The online queuing model.

为了解决这一难点，房智轩研究组的研究目标是为保证每个玩家的 QoS 至少达到某个值的 MP-MAB 模型，且考虑臂产生的奖励对不同玩家不同的这种具有挑战性的设置。研究组利用随机匹配的方法开发了一种新颖的分布式 MP-MAB 算法来实现这一研究目标。研究组证明了研究人员的分布式算法能够确保所有玩家的 QoS 遗憾为 O(1)，还揭示了研究人员的 MP-MAB 模型与在线队列系统之间的关系，并说明研究人员的分布式算法可以保证该队列系统的稳定性。

该成果研究论文：Qingsong Liu and Zhixuan Fang, "Decentralized Scheduling with QoS Constraints: Achieving O(1) QoS regret of Multi-player Bandits", AAAI 2024.

# 带有 QoS 约束的信息采集中的在线调度

房智轩研究组考虑信息收集中的调度问题，其中多个传感器 / 信息源持续收集信息（例如，胎压、燃料剩余多少）并将观测数据传输给监视器。这调度问题在许多物联网（IoT）系统中很常见，如空中监视网络和自动化工业厂房。监视器需要调度多个信息源 ( 例如传感器 ) 来收集信息。在从信息源获取数据包时，监视器主要面临两个挑战。首先，来自不同信息源的数据可能为监视器带来不同的价值。但在许多实际情景中，监视器对不同信息源产生的数据信息价值没有先验的统计知识。其次，无线通信宽带通常有限且不稳定，信息源与监视器之间的无线信道的可靠性（丢包率）也是未知的。这些挑战促使监视器进行基于学习的调度，其中监视器学习信息源和信道的统计信息，并在调度过程中尽可能采集有价值的数据。除此之外，在许多实际情景中，监视器还需要满足每个信息源的一些服务质量（QoS）约束（即吞吐量或平均延迟），以确保及时有效的采样和制定决策。比如，对于自动驾驶汽车系统，障碍物 / 碰撞检测的数据应以较高频率地发送到处理器（监视器），而测量燃料剩余多少的传感器可以以较低的频率更新。

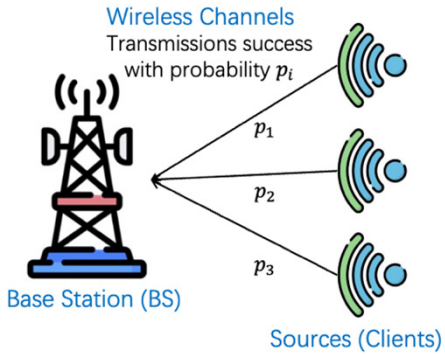



Fig. 1. The system model.

具体而言，该研究组遵循每个信息源生成的数据包的信息价值是独立（但不一定是相同分布）的随机变量的常见假设。然后，研究人员的调度问题可以被建模为受吞吐量约束的组合多臂老虎机问题，其中每个源可以被看作一个“臂”，而数据包的信息价值则是奖励。对于数据包信息价值服从独立且同分布的静态情况，研究人员提出了一种基于线性规划（LP）的高效在线调度策略。该研究组的证明该策略满足每个源的 QoS 约束，且仅产生对数遗憾。在无线信道丢包率已知的特殊情况下，该调度策略还能够进一步保证有界遗憾。此外，在非静态包值的情况下，研究人员将滑动窗口技术应用于该基于 LP 的调度策略，并证明它仍然在满足每个源的 QoS 要求的同时保证次线性遗憾。最后，研究组进行了数值模拟来支持研究人员的理论结果。

该成果研究论文：Qingsong Liu, Weihang Xu, and Zhixuan Fang, "Learning-based Scheduling for Information Gathering with QoS Constraints", INFOCOM 2024.

# 三、计算机系统结构

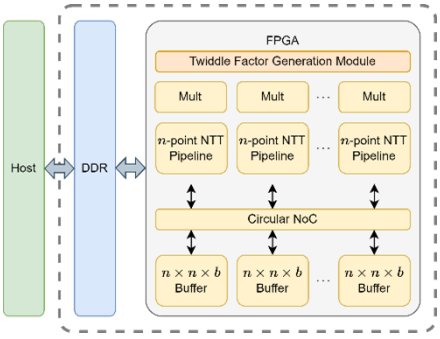
主要完成人：高鸣宇研究组、马恺声研究组

## 基于多维分解算法的快速数论变换专用硬件加速器

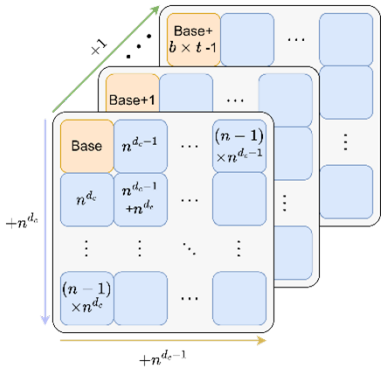
近年来，随着云服务、区块链、物联网技术的普及，计算机系统对数据安全的重视程度日益增加。在隐私保护计算领域，同态加密和零知识证明作为关键算法工具，引起了广泛的关注。然而，这些算法通常需要大量的计算资源，导致执行时间较长，阻碍了在实际场景中的部署。环上多项式乘法是这些算法中的常用操作。为了降低该操作的算法复杂度，最常用的优化方法是快速数论变换（NTT）。但由于不规律的内存访问等问题，NTT 仍然是耗时较长的模块，因此其一直是主流的专用硬件加速研究方向之一。

高鸣宇研究组观察到目前针对 NTT 的加速器往往为固定的算法参数而设计，然而，在同态加密与零知识证明中，不同协议的参数存在显著的差异。因此研究人员提出了一种名为 SAM 的加速器架构，基于 FPGA 平台实现。SAM 采用多维分解的算法，支持不同的多项式度数的任务。SAM 的片上使用有限且固定的资源，将大规模的 NTT 分解为与片上硬件相匹配的小规模任务，从而实现了高效的任务执行，并且可以灵活地应对不同规模的 NTT 计算。同时，研究人员提出了针对片上和片外数据传输以及片上计算架构的多种优化技术，并实现了片上计算吞吐量与片外内存带宽的平衡。实验结果表明，在大规模任务下，SAM 对比 CPU 性能提升可达 109 倍，对比之前基于 FPGA 的加速器性能提升超过 2 倍。

该研究成果论文：Cheng Wang and Mingyu Gao, "SAM: A Scalable Accelerator for Number Theoretic Transform Using Multi-Dimensional Decomposition", ICCAD 2023.




加速器架构




片上数据流

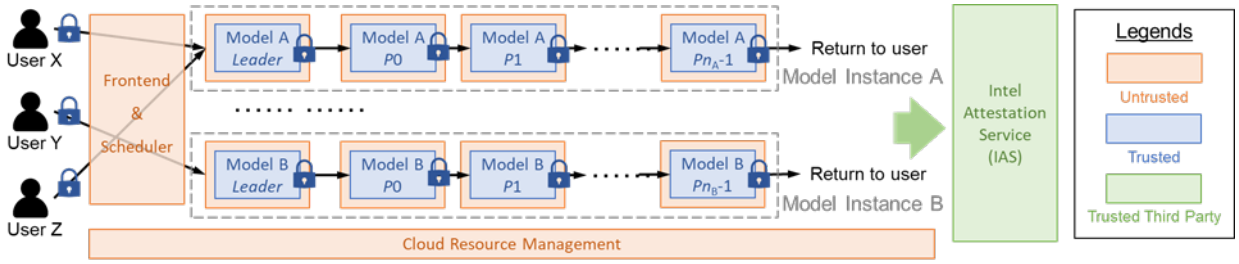
# 基于可信执行环境的可信机器学习即服务框架

近年来，深度学习大模型（LLM）的流行使得在本地部署和运行机器学习模型变得越来越困难和昂贵。因此，当前的机器学习模型通常被部署在云端，并外包给远程服务器进行计算。许多公司也开放了自己研发的机器学习模型API，供其他企业或个人用户免费或付费调用。虽然这些技术正在酝酿一场新的生产力革命，但这种推广模式也带来了更多对数据隐私性的关注。

硬件可信执行环境（TEE）为这个问题提供了实用的解决方案。TEE 使用硬件保护将敏感代码与其他应用程序隔离开来，可以为客户提供可靠的数据隐私保证。

高鸣宇研究组对当前的基于 TEE 的机器学习即服务（MLaaS）推理框架设计进行了深入分析，并确定了三个关键的性能低效问题：飞地（enclave）初始化、模型加载和有限的可信内存空间。为解决上述三个问题，研究人员提出了两种关键优化技术。一方面，通过启用跨用户的安全飞地重用，以消除飞地初始化和模型加载成本。另一方面，提出一种新的模型划分方法，以减轻在有限可信内存中安全换页的开销。同时，研究人员使用准确的延迟估计模型和轻量级的优化器，共同有效地平衡模型划分后各分区之间的计算和通信延迟。根据实验结果，上述优化可使推理延迟优于当前最先进设计 2.2 倍，吞吐量可达到 2.1 倍，相比最好的基于密码学的可信机器学习及服务设计性能提升 1607 倍。

该研究成果论文：Fabing Li, Xiang Li, Mingyu Gao, "Secure MLaaS with Temper: Trusted and Efficient Model Partitioning and Enclave Reuse", ACSAC 2023.



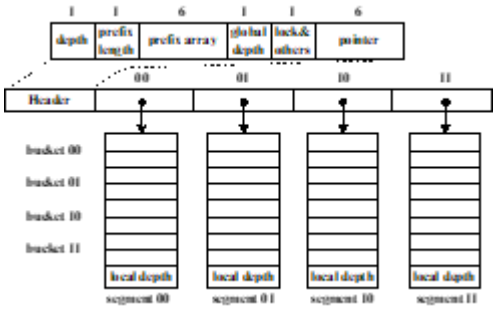

系统整体架构

# 面向持久内存的融合基数树与可扩展哈希的索引结构

现代数据密集型应用逐渐开始转向基于新型持久存储器件的内存系统，并通过将关键数据结构移植到持久内存上来持续保持其高性能。其中一个例子是用于支持高效数据查询和更新的索引结构。许多关于面向持久内存上索引结构的特定优化，主要研究重点均是减少持久数据的昂贵写入代价。高鸣宇研究组重新审视了之前的设计在真实的持久内存器件（英特尔傲腾，Intel Optane）上的表现，发现在基于树结构的索引中，以数据读取为主的树型结构遍历和树节点内搜索占据了整体延迟的主导地位。

因此，研究人员提出了一种针对持久内存特定优化的索引结构，名为“可扩展基数树”（Extendible Radix Tree，ERT）。该索引结构可以显著减少树的高度以最小化随机读取开销，同时仍然保持快速的节点内搜索速度。其关键思想是对基数树中的每个节点使用可扩展哈希，以允许研究人员增大基数树的分支扇出而减小树的高度，并且在节点内通过哈希结构实现常数时间的查找。使用可扩展哈希还允许在插入和更新期间对节点进行增量修改而不产生过多的写入。通过在每个节点的哈希表中保持键值之间的部分顺序，可以有效而稳健地处理范围查询请求，而不引入过多的哈希冲突。实验结果表明，该索引结构相对于当前最先进的持久内存索引结构可实现 2 至 4 倍的速度提升。

该研究成果论文：Ke Wang, Guanqun Yang, Yiwei Li, Huanchen Zhang, Mingyu Gao, "When Tree Meets Hash: Reducing Random Reads for Index Structures on Persistent Memories", SIGMOD 2023.




可扩展基数树节点结构


可扩展基数树

# 基于 2.5D 封装的可扩展异构 Chiplet NPU 加速器

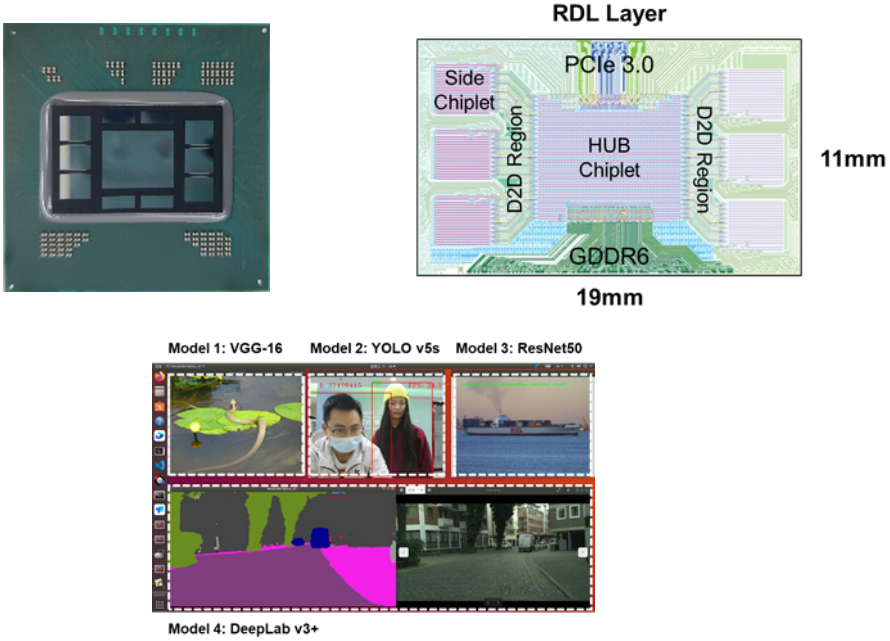
随着摩尔定律的放缓，专用计算的场景多样性以及应用算法的快速发展，高效的芯片设计需要模块化、灵活性和可扩展性。在这项研究中，马恺声研究组提出了一个基于芯片组的深度学习加速器原型，包括一个 HUB Chiplet 和六个扩展的 SIDE Chiplet，集成在 2.5D 封装的 RDL 层上。SIDE 和 HUB 分别包含一个和四个人工智能处理核心。

鉴于该研究组的芯片组系统通过可扩展连接的 SIDE Chiplet 面向多样化场景，研究组需要应对三个挑战：a）设计支持不同形状的灵活架构，b）寻找低片对片通信的工作负载映射，c）采用高带宽的片对片接口以保持有效的数据传输。

该研究组提出了一种灵活的神经核心（FNC），具有动态位宽计算和灵活并行性。接下来，研究人员使用基于层次的映射方案来分离不同并行级别，并帮助分析通信。引入了 12Gbps 的 D2D 接口，实现了每个片对片端口 192Gb/s 的带宽，比特效率为 1.04pJ/bit，55μm 焊球凸点（bump）间距。

研究人员提出的7-Chiplet加速器在 INT16/8/4 上实现了 10/20/40 TOPS 的峰值性能。当启用 0~6 个 SIDE Chiplet时，系统功耗范围从 4.5W 到 12W。FNC 的功耗效率为 2.02TOPS/W，整体系统的功耗效率为 1.67TOPS/W。

该成果研究论文 Zhanhong Tan, Yifu Wu, Yannian Zhang, Haobing Shi, Wuke Zhang, Kaisheng Ma, "A Scalable Multi-Chiplet Deep Learning Accelerator with Hub-Side 2.5D Heterogeneous Integration", Hot Chips 2023.



# 平铺加速器层间调度空间的定义和探索

深度神经网络（DNN）在图像识别、目标检测和自然语言处理等领域中得到了广泛应用。随着 DNN 的不断发展，网络结构变得更加复杂，因此需要大规模的加速器来加速推理过程。目前，采用瓦片式架构的大规模加速器已经成为主流，其中每个硬件瓦片（HW-tile）包括一个处理元素（PE）阵列和一个全局缓冲区，并由网络芯片（NoC）相互连接（图 1（b））。然而，单个大型 HW-tile 的利用率和能量效率较低，因此如何有效地利用这些计算和存储资源是一个开放性的挑战。解决这一挑战的关键在于调度，分为层内调度（图 1（c））和层间调度（图 1（c））两类。层内调度研究如何将单个层映射到一个或多个 HW-tile 上，而层间调度研究如何在加速器上调度所有层的计算顺序和资源分配。

尽管层间调度在保持瓦片式加速器高度利用和能量效率方面发挥着越来越重要的作用，但其研究存在显著的不足：大多数研究仍在优化现有的启发式模式，如 LP 和 LS，但没有提出新的模式，更没有清晰而系统地定义瓦片式加速器上层间调度的空间。缺乏层间调度空间的明确定义极大地限制了优化瓦片式加速器性能和能量效率的机会。此外，缺乏系统性定义也阻碍人们理解不同层间调度选择如何影响不同硬件行为以及这些行为如何进一步影响加速器的能量效率和性能。

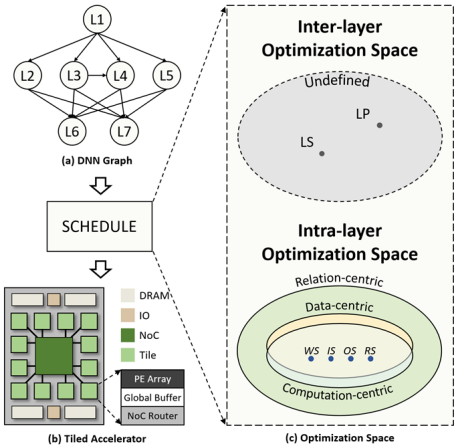



图 1. 在平铺加速器上的调度

马恺声研究组针对这一挑战而引入一种统一而系统的资源分配树符号来描述瓦片式加速器上具有不同结构的推理 DNN 的层间调度空间。该符号包括时间切割，将相同的 HW-tile 组和不同的计算时间间隔分配给每个子节点，以及空间切割，将不同的 HW-tile 组分配给每个子节点。每个 RA 树都是一个切割和叶节点（DNN 的层）的分层组织。然后，研究组详细阐述如何将树形结构解析为相应的资源分配方案和数据流动。

基于 RA 树符号，研究人员全面分析了不同的层间调度选择如何影响硬件行为以及这些行为如何影响加速器的能量效率和性能。此外，研究人员在符号中表示了现有的 LS 和 LP 模式并分析了其特征。结合上述内容，研究人员开发了一个端到端且高度可移植的调度框架 SET，用于自动探索瓦片式加速器上 DNN 的整个调度空间。为了有效地探索新定义的层间调度空间，研究人员将 SET 配备了一种基于模拟退火的算法，具有 6 个特别设计的操作。SET 可以轻松地移植到各种瓦片式加速器上，具有良好的可移植性。研究人员已经开发了一个端到端的 SET 部署流程用于测试芯片。该框架可在 https://github.com/SET-Scheduling-Project/SET-ISCA2023 上获取。

与 SOTA 开源框架 Tangram 相比，SET 平均可实现 1.78 倍的性能提升和 13.2% 的能量成本降低。此外，研究人员对不同的 DNN、批次大小和硬件平台进行了大量实验，以展示 SET 的通用性和探索新定义空间相对于现有 LS 和 LP 调度模式的效果。此外，研究人员利用 SET 分析了 LS 和 LP 的特性，并揭示了层间调度空间的特征。

该成果研究论文：Jingwei Cai, Yuchen Wei, Zuotong Wu, Sen Peng, and Kaisheng Ma, "Inter-layer Scheduling Space Definition and Exploration for Tiled Accelerators", International Symposium on Computer Architecture (2023).

# PHEP：高性能同态加密处理器

云计算可为大量新兴的信息应用提供可靠的高性能服务，但在计算过程中需要处理大量的个人和机构数据。Paillier 同态加密可以允许直接对密文进行计算，避免个人和机构的隐私数据泄露。在图 1 示出的 Paillier 同态加密方案中，客户端将其明文加密为密文，随后将密文发送至服务器，服务器执行同态求值并且向客户端返回加密结果。

目前 Paillier 同态加密算法在通用处理器 CPU 和图形处理器 GPU 上的性能较低。针对这一计算瓶颈，马恺声研究组在 28nm 工艺下设计并制造了面向 Paillier 同态加密的领域专用处理器 PHEP。该处理器 ( 图 2) 可以提供 192 ～ 480TOPS 算力，PHEP 与具有 192 核的 Intel 的台式 CPU Xeon 相比能到 1 个数量级的加速，为隐私保护云计算提供了高性能的解决方案。

该成果研究论文 : Guiming Shi, Yi Li, Xueqiang Wang, Zhanhong Tan, Dapeng Cao, Jingwei Cai, Yuchen Wei, Zehua Li, Wuke Zhang, Yifu Wu, Wei Xu, Kaisheng Ma, "PHEP: Paillier Homomorphic Encryption Processors for Privacy-Preserving Applications in Cloud Computing", IEEE Hot Chips 35 Symposium (HCS) 2023。

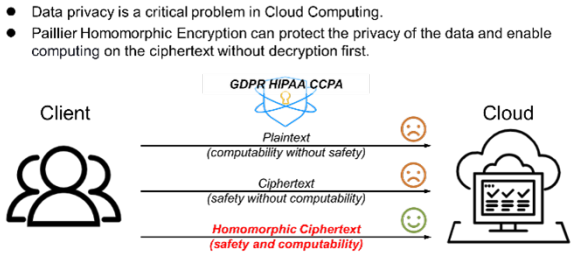



图 1

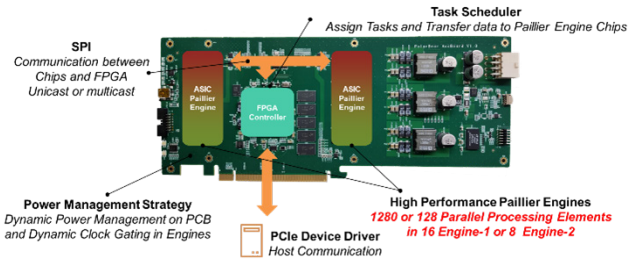



图 2

# 四、数据库系统

主要完成人：张焕晨研究组

## 基于机器学习的数据压缩算法

数据压缩在大数据处理中起到节省存储成本和加速查询等至关重要的作用。当今海量数据的产生与对查询极高的时间响应要求，让大数据压缩技术面临着全新的挑战。相对于传统的消除数据重复的思路，张焕晨研究组从一个全新的角度建模数据压缩问题，结合机器学习技术深度消除数据中的相似性冗余，获得突出的压缩率提升表现，同时加速解码过程以提升后续计算的效率。

在列存数据库的基础上提出解决方案 LeCo，用数据挖掘和模式识别技术将单列数据的分布信息凝缩在模型中，并存储错误修正码以实现无损压缩。在无损压缩领域，LeC 第一个提出用模型进行压缩，并且系统性探讨了该问题下优化压缩率的可能参数空间。LeCo 作为完整的数据压缩方案，自动化地进行模型选择，参数选择，基于分布检测的智能数据分段等。

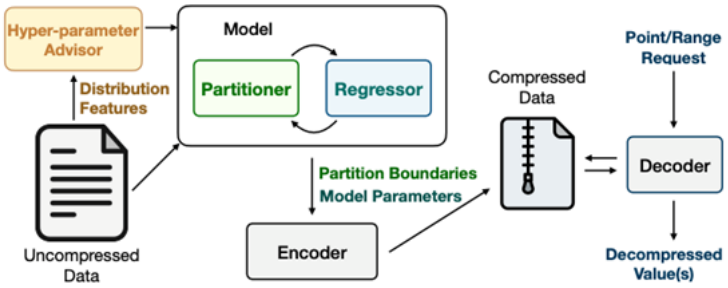



图 1 LeCo 系统的组成部分及压缩流程

在多个真实系统测试中，该压缩方案凭借突出的压缩率与轻量级解压操作提升查询速度、缓解内存瓶颈，在基于 Apache Arrow 和 Parquet 的列存执行引擎中，有着高至 5 倍的 SQL 查询速度提升，在 Rocksdb 系统中提升了 16% 以上的查询吞吐速率。

该成果研究论文：Yihao Liu, Xinyu Zeng, Huanchen Zhang, "LeCo: Lightweight Compression via Learning Serial Correlations", SIGMOD 2024.

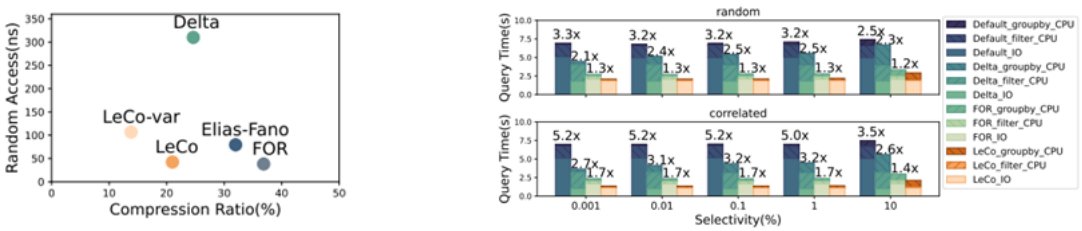



图 2 LeCo 与其他压缩方法的性能对比

# 列式存储格式的实证评估

列式存储是现代数据分析系统的核心组件之一。尽管许多数据库管理系统 (DBMS) 都有专有的存储格式，但大多数都对 Parquet 和 ORC 等开源存储格式提供广泛支持，以促进跨平台数据共享。但这些格式是十多年前（即 2010 年代初）为 Hadoop 生态系统开发的。从那时起，硬件和工作负载格局都发生了显著变化。

张焕晨研究组重新审视最广泛采用的开源列式存储格式（Parquet 和 ORC），并通过深入探讨其内部结构以及不同的组成模块，梳理总结了这两类最广泛的存储格式的技术分类方法以及相应的优缺点。研究组设计了一个基准来对不同工作负载配置下的格式性能和空间效率进行压力测试。通过对 Parquet 和 ORC 的综合评估，研究人员归纳了对现代硬件和实际数据分布有利的设计决策。其中包括默认使用字典编码、在整数编码算法中优先考虑解码速度而不是为了更高的压缩比而采用几种编码混合交替、使块压缩成为可选以及嵌入更细粒度的辅助数据结构。

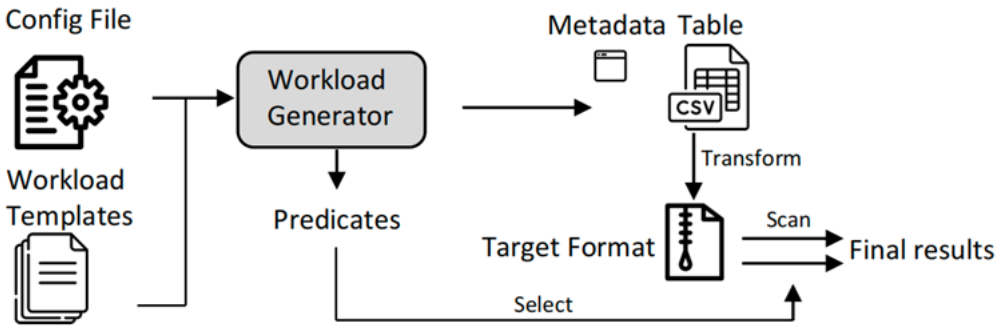



**Figure 4: Benchmark Procedure Overview**

图 2 QuerySplit 与其他查询优化技术的对比

除此之外，因为机器学习类型的负载在数据处理工作流程中的流行，研究组还对机器学习训练以及向量搜索过程中需要访问列式文件格式的相应操作进行了测试。最后，研究人员评估了在 GPU 上进行解码的性能，结果显示现有文件格式的设计在机器学习负载以及 GPU 上的解码操作存在缺陷，并有提出更有利的设计的空间。

该成果研究论文：Xinyu Zeng, Yulong Hui, Jiahong Shen, Andrew Pavlo, Wes McKinney, Huanchen Zhang. "EAn Empirical Evaluation of Columnar Storage Formats. Proc", Proc. VLDB Endow. 17(2): 148-161 (2023).

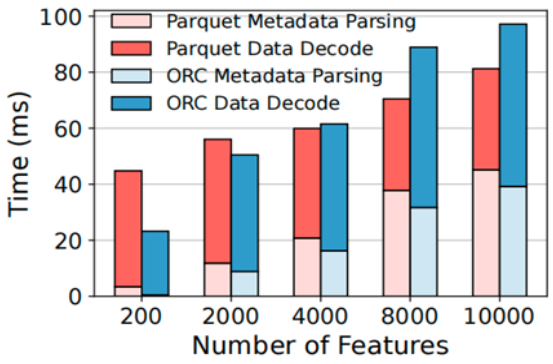
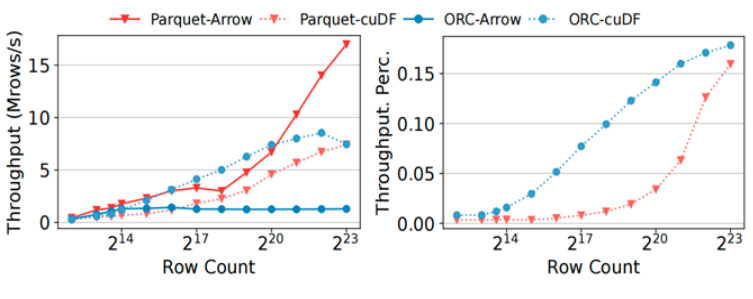



**Figure 11: Wide-Table Projection**




(a) core workload (b) Peak GPU Throughput Percentage

GPU Decoding

# 五、区块链

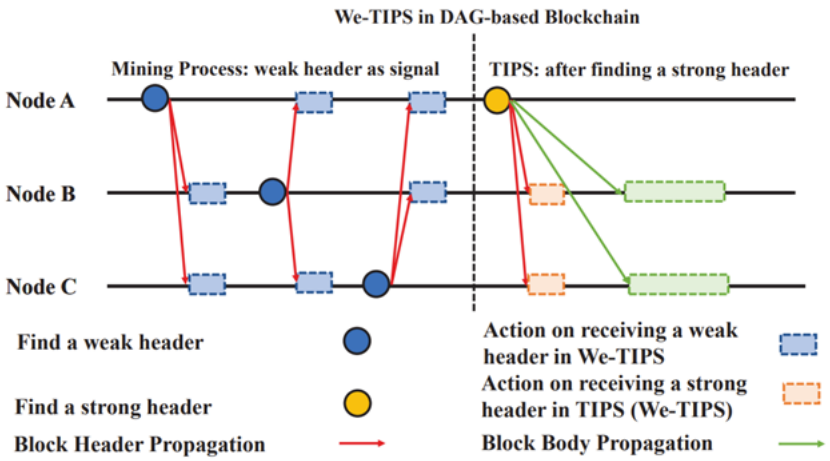
主要完成人：房智轩研究组

## 设计有向无环图的区块链系统中基于信号的交易包含协议 (TIPS)

传统的区块链如比特币系统采用了线性链式结构，同一时刻只有一个区块可以被添加到主链上。这一结构限制了线性区块链的系统吞吐量。而基于有向无环图的区块链系统采用了有向无环图的结构，同一时刻允许多个区块并发地添加到区块链系统中，这极大地提高了区块链系统性能。但并发的区块中可能会包含相同的交易，而这些冗余的交易碰撞会降低系统的利用率，甚至可能还会严重影响系统性能。

基于DAG的区块链由于高并发和网络延迟而面临交易包容的关键挑战，在该文中，房智轩研究组提出了“We-TIPS”，这是一种基于弱块的交易包含协议，利用弱区块头带有信号来解决这一关键挑战。在 We-TIPS 中，在挖矿过程中，矿工可以将其弱块头作为信号广播，该信号可以指示矿工当前的交易包含情况。通过信号的及时广播，矿工可以有效避免交易包含碰撞，从而大大提升系统性能。此外，在 We-TIPS 协议中研究了矿工之间的交易选择博弈，并证明该博弈是一个 Potential Game，并进一步设计了一种可以实现近似纳什均衡的去中心化算法。

该成果研究论文：Canhui Chen and Zhixuan Fang, "We-TIPS: Weak-Block-Based Transaction Inclusion Protocol with Signaling in DAG-based Blockchain", WiOpt 2023.



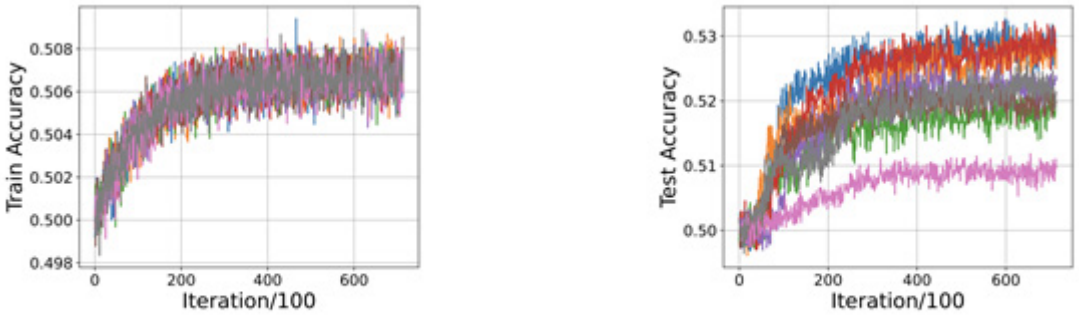
# 六、密码学

主要完成人：陈一镭研究组

## 用神经网络算法更快地破解密码学中的高噪声 LPN 问题

神经网络算法在近几年快速发展，在自然语言处理、图像处理等领域有突出的效果。但神经网络算法在密码学中还没有明显领先经典算法的例子。陈一镭研究组对使用神经网络解决密码学中常用的“带噪声学习奇偶性问题”（LPN）进行了系统的研究。该研究组的主要贡献是设计了一系列两层神经网络。研究人员考虑了三种 LPN 样本数量的设置：丰富、非常有限以及介于两者之间。 在每种设置中，研究人员都提供能够尽快解决 LPN 问题的神经网络模型。 对于某些设置，研究人员还能够提供解释模型设计原理的理论。实验表明研究人员的模型在高噪声、低维情况下的性能优于经典算法。

该成果研究论文：Haozhe Jiang, Kaiyue Wen, Yilei Chen, "Practically Solving LPN in High Noise Regimes Faster Using Neural Networks", https://eprint.iacr.org/2023/372.




(a) Training Accuracy　　(b) Test Accuracy

图为 LPN 破解实验的训练精度与测试精度的对比

# 关于 S|LWE> 问题的算法及复杂度证明

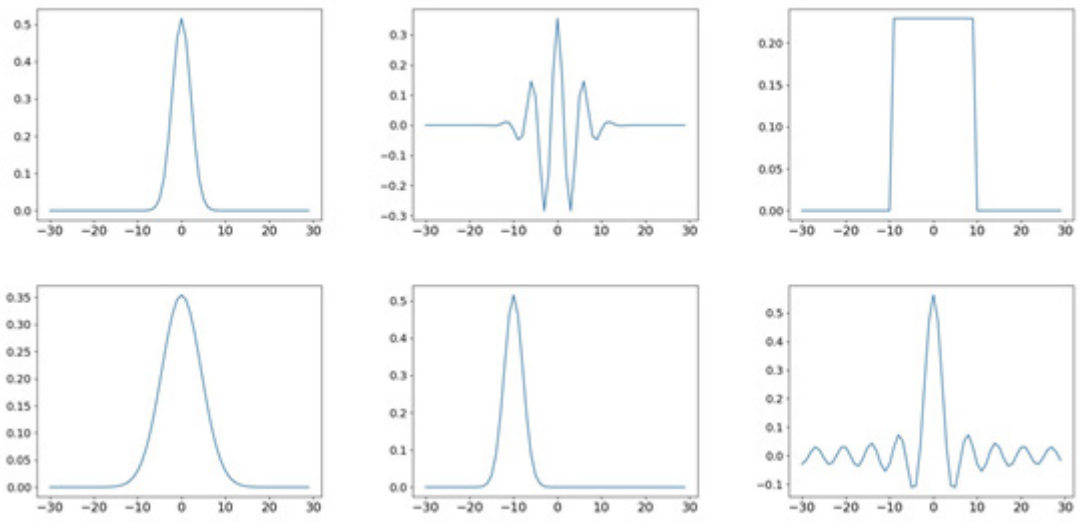
“带错误学习问题”（LWE）是后量子密码学最重要的构建模块之一。 为了更好地理解 LWE 对于量子计算机的困难度，探索 LWE 的量子变体、展示这些变体的量子算法或证明它们与标准 LWE 一样困难至关重要。研究人员深入研究了 Chen、Liu 和 Zhandry 在 [Eurocrypt 2022] 定义的一种 LWE 的量子变体——S|LWE> 问题。它将 LWE 样本的误差编码为量子幅度。在该文中，陈一镭研究组证明了新的 S|LWE> 困难度和算法。研究人员的主要结果：

1. 如果 S|LWE> 具有未知相位的高斯幅度，那么它就和传统的 LWE 问题一样难；

2. 如果 S|LWE> 具有已知相位的高斯幅度，那么 S|LWE> 就具有亚指数时间量子算法。

因此，如果研究组能进一步改进以上两个结论的“未知相位”与“已知相位”的差距，就有可能设计出对于传统 LWE 问题的亚指数时间量子算法。

该成果研究论文：Yilei Chen, Zihan Hu, Qipeng Liu, Han Luo, Yaxin Tu, "On the Hardness of S|LWE> with Gaussian and Other Amplitudes", https://eprint.iacr.org/2023/1498.



图为已知相位的高斯幅度、未知相位的高斯幅度、均匀随机幅度（上排从左到右）以及它们的傅立叶变换的图例（下排从左到右）

# 七、理论算法

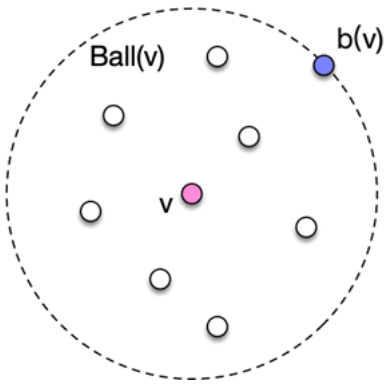
主要完成人：段然研究组

## 新的无向图单源最短路算法

最短路问题是图论领域最基础的问题之一，单源最短路问题需要找到从一点 s 到其他所有点的最短路。Dijkstra 算法（利用斐波那契堆）的时间复杂度为 O(m+n · log n)，因为 Dijkstra 算法的副产品是所有点对从 s 的距离排序，而比较模型下排序需要 (n · log n) 时间，所以要改进 Dijkstra 算法就要避免整体排序。在比较模型下，对于另一个图论基础问题——最小生成树，姚期智院士早在 1975 年就给出了比排序时间快的算法，而目前已有 O(m) 时间的随机算法。对于最短路问题人们也进行过很多尝试，包括整数边权无向图上的线性时间的算法 [Thorup 99] 以及整数边权有向图上 O(m+n · loglog min{n,W}) 时间的算法 [Thorup 03]。而在实数边权下（比较模型），[Pettie & Ramachandran 05] 给出了 O(m · (m,n)+min{n · log n, n · loglog r}) 时间的算法，这里 W 是最大整数边权，r 是最大 - 最小边权比值，是 inverse-Ackermann 函数。但是实数边权下的最短路问题一直没有真正突破排序时间的算法。

该论文给出了实数边权无向图上时间复杂度为 O(m\sqrt{\log n\log\log n}) 的单源最短路算法。这个时间复杂度也突破了 [Pettie & Ramachandran 05] 给出的关于“hierarchy-type”算法的 (m+min{n · log n, n · loglog r}) 的时间下界，因为研究人员的随机算法并不基于“hierarchy-type”方法，并且比之前的“hierarchy-type”的算法简单。

该成果研究论文：Ran Duan, Jiayi Mao, Xinkai Shu, Longhui Yin, "FA Randomized Algorithm for Single-Source Shortest Path on Undirected Real-Weighted Graphs", FOCS 2023.




```
d(s)←0, d(v)←+∞ for other vertices v;
initialize Fibonacci heap H with vertices in R;
while H is not empty do
  u ← H.ExtractMin();
  forall v such that u=b(v) do
    relax(v, d(u)+dist(u,v));
    forall y in Ball(v)∪{v} do
      relax(v, d(y)+dist(y,v));
      forall z in Neighbor(y) do
        relax(v, d(z)+w(z,y)+dist(y,v));
  forall x such that u=b(x) do
    forall y in Neighbor(x) do
      relax(y, d(x)+w(x,y));
      forall z in Ball(y) do
        relax(z, d(x)+w(x,y)+dist(y,z));
```

# 量子信息

# 一、离子阱量子模拟

主要完成人：段路明研究组、吴宇恺研究组

## 首次实现基于数百离子的可调耦合可单点分辨的二维量子模拟器

离子阱系统被认为是最有希望实现大规模量子模拟和量子计算的物理系统之一。目前为止，人们在 Paul 型离子阱的一维离子链上实现了数十离子的量子模拟实验，以及在 Penning 型离子阱的二维离子晶格上实现了约两百离子的量子模拟实验，然而后者因缺乏单点分辨探测的能力而不利于提取实验上的空间关联信息。

基于低温一体化 Paul 离子阱以及相关的一系列技术探索，段路明研究组首次在 512 离子的二维晶格上实现了稳定囚禁和基态冷却（图 1a）；并首次在 300 离子的二维晶格上，实现了可调耦合、可单点分辨探测的长程伊辛模型的量子模拟实验（图 1c）。该研究为中等规模带噪声量子（NISQ）时代的大规模离子阱量子模拟实验铺平了道路。

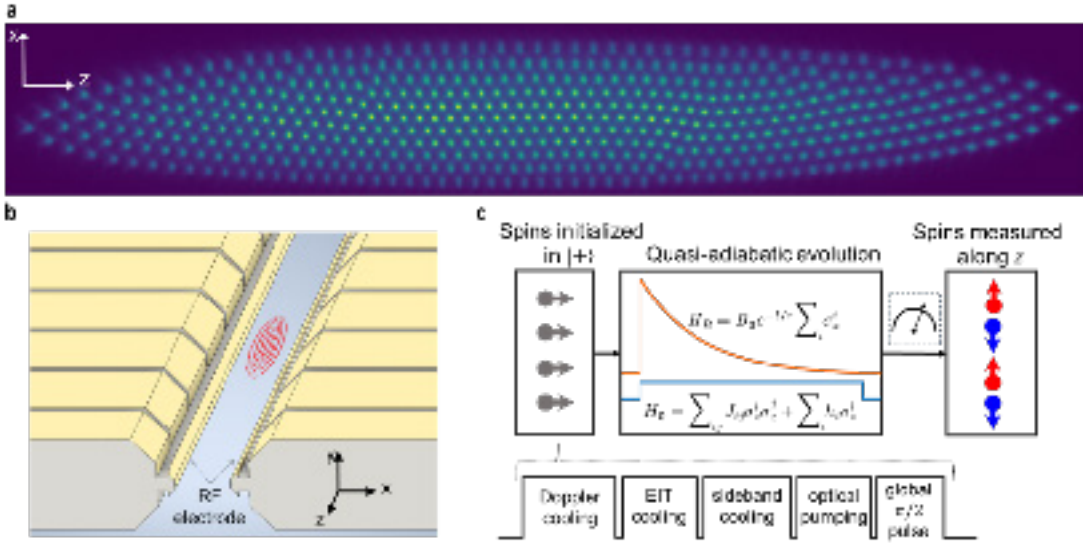



图 1. a. 512 离子的二维离子晶格图像；b. 一体化离子阱的三维模型示意图；
c. 制备长程伊辛模型基态的实验序列。

研究人员首先将量子系统准绝热地制备到长程伊辛模型哈密顿量的基态，利用单次测量中对每个量子比特的单点分辨能力，进而观察到了针对不同声子模式的丰富的空间关联图像（图 2 上：质心声子模式；图 2 下：第 4 个声子模式），得到了任意两对离子之间的关联矩阵（图 2 左列 a,d），展示了对 300 离子晶格的典型单次探测结果（图 2 中列 b,e），并将空间关联函数进行傅里叶变换至动量空间（图 2 右列 c,f）。

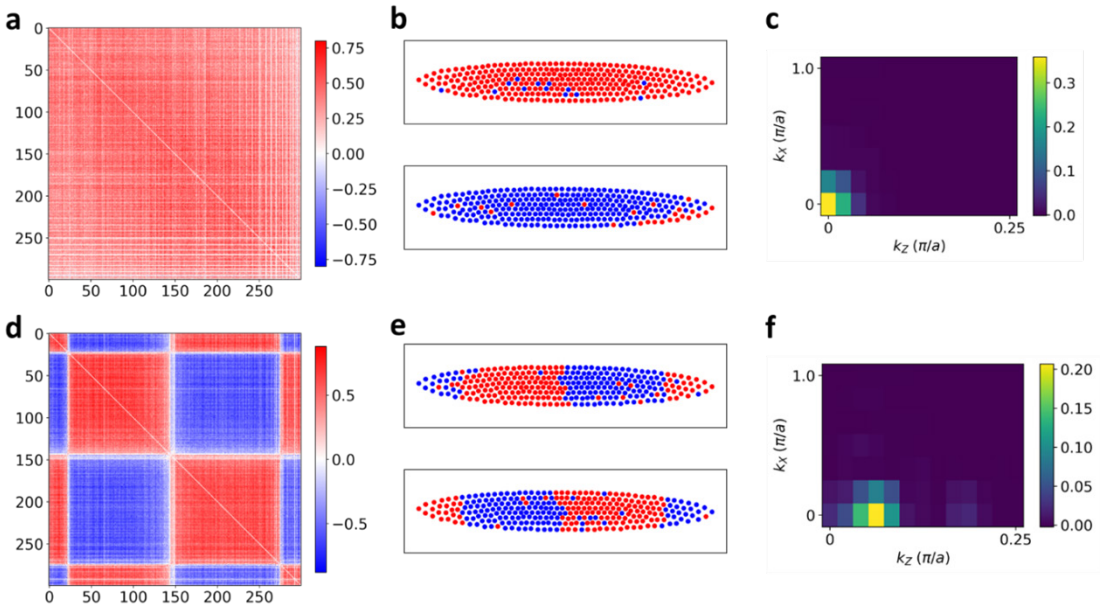



图 2. 对于不同模式准绝热制备到基态后的空间关联信息

这种空间分辨率使该研究组能够将实验上的典型单次探测结果与计算出的集体声子模式进行比较（图 3 a 和 b），进一步验证了量子模拟结果。由于该第 19 个声子模式在二维晶格的两个方向上均有震荡，因此如果仍简单地将离子沿长轴方向排列序号就无法充分反映该模式的信息（图 3d）；而如果将离子按照理论计算的声子模式矢量排序，就可以验证对应该模式的空间关联信息（图 3e）。

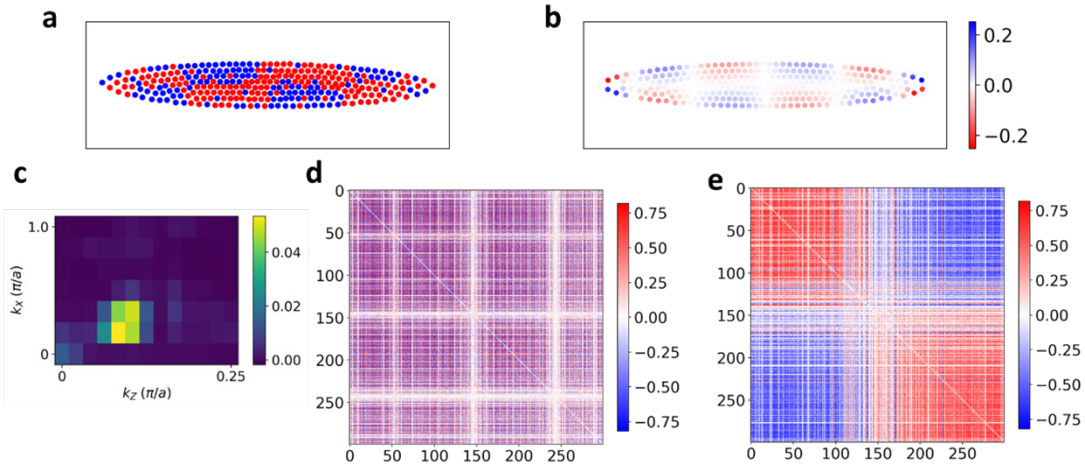



图 3. 对照理论计算的第 19 个声子模式验证量子模拟结果

为展现更复杂的哈密顿量、模拟更丰富的量子动力学现象，研究人员进一步给激光同时施加两组拍频，进而同时耦合两个声子模式。通过从左至右逐渐减少第 7 个模式的耦合强度、增加第 4 个模式的耦合强度比例（图 4 c-e），可以看出这两个耦合同时存在时的竞争关系：关联图像从被第 7 个模式主导，逐渐变化至被第 4 个模式主导。130, 16300

1 – Published 21 April 2023.

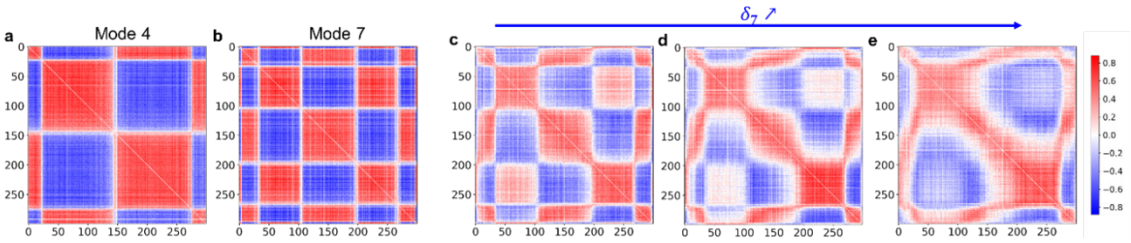



图 4. a-b. 只单独耦合第 4 个以及第 7 个模式的空间关联矩阵；c-e. 同时耦合两个声子模式

该成果研究论文：S.-A. Guo, Y.-K. Wu, J. Ye, L. Zhang, W.-Q. Lian, R. Yao, Y. Wang, R.-Y. Yan, Y.-J. Yi, Y.-L. Xu, B.-W. Li, Y.-H. Hou, Y.-Z. Xu, W.-X. Guo, C. Zhang, B.-X. Qi, Z.-C. Zhou, L. He, L.-M. Duan, "A site-resolved 2d quantum simulator with hundreds of trapped ions under tunable couplings", https://arxiv.org/abs/2311.17163.

# 二、量子通信

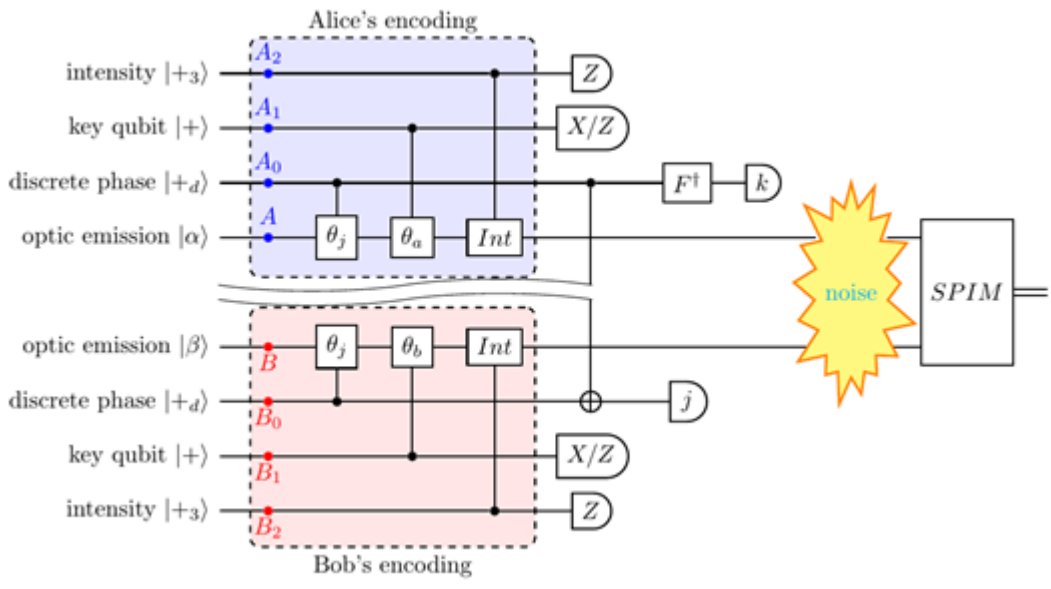
主要完成人：马雄峰研究组

## 相位匹配量子密钥分发协议的源替换模型及分束攻击的分析

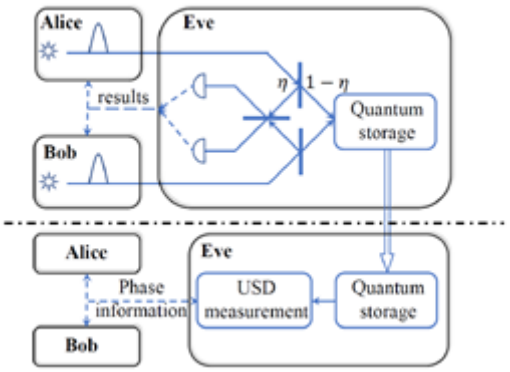
量子密钥分发（QKD）作为构建安全通信网络的一种很有前途的解决方案，D 允许远程通信双方通过利用量子力学原理建立安全密钥。QKD 安全性理论基于量子比特和相位纠错，通过纠正比特和相位误差，Alice 和 Bob 能够共享两个相同且私密的密钥字符串。最近的量子密钥分发协议之一，相位匹配协议，可以有二次密钥速率的改进。它的安全性最初是使用一种称为对称保护隐私的抽象方法建立的，与传统的基于互补性的安全性证明不同，它利用编码的对称性来确保安全，从而推导出相位误差率。这种方法的优势在于其独立于源和测量的具体细节，专注于编码操作，为安全性分析提供了简单的框架。然而，它的抽象性质也限制了对特定协议的安全分析，阻碍了对潜在窃听攻击的全面评估。

为了解决这一问题，马雄峰研究组通过源替代方法重新审视了相位匹配方案的安全性，该方法更易理解。研究人员引入了一个虚拟纠缠协议，其中用户使用 CNOT 门、量子傅立叶变换和光子数测量来构建伪 Fock 态，见图（a）。最终，基于原始定义，文章建立了光子数和相位错误之间的关联。该研究旨在通过源替代分析提供对相位匹配方案安全性的新视角，强调了协议的安全性，并深入了解了其基本机制。该文还介绍了一个可能对相位匹配方案构成威胁的分束攻击，见图（b），并在源替代框架内推导了相位误差率的下界，量化了攻击对协议的影响。模拟结果显示，安全性证明提供的相位错误率非常接近分束攻击引入的错误率，这表明安全性分析提供的相位错误率上界和因此导致的密钥速率的下界已经很紧凑，改进的余地很小。这一分析建立了攻击与量子相位误差率之间的直接联系，增强了对相位匹配方案安全性的理解。

(a)



(b)




该成果研究论文：Yizhi Huang, Zhenyu Du, Xiongfeng Ma, "Source-Replacement Model for Phase-Matching Quantum Key Distribution", [Adv. Quantum Technol. 2023, 2300275, https://doi.org/10.1002/qute.202300275].

# 基于测量互补性的设备无关量子密码协议安全性分析

测量互补性是量子力学的一个基本原理，对非对易观测量的同时测量结果的精确度给出了根本限制。在量子力学的发展过程中，人们注意到测量互补性与量子纠缠这一非定域量子态之间存在着紧密关系。特别地，量子纠缠的存在可以通过贝尔不等式违背一种超越经典力学的非定域关联统计—予以验证，且这一结论仅基于量子力学的正确性，不需要实验者对量子设备进行任何先验刻画或假设，因而也被称作是“设备无关”的。

测量互补性原理和量子非定域性在量子通信与密码中发挥了重要作用。基于测量互补性原理，可以实现等具有信息论安全性的量子密码协议。另一方面，量子非定域性启发了仅基于量子力学正确性的密码协议设计。上世纪 90 年代，姚期智院士等研究者提出了通过贝尔不等式违背，实现具有设备无关特性的量子密码协议。然而，不同于使用可信设备的量子密码协议安全性分析，在设备无关量子密码学的发展中，测量互补性的作用并未得到明确。

在新的研究工作中，马雄峰研究组与多伦多大学研究者合作，解决了设备无关量子密码协议中安全性的测量互补性来源这一开放性问题。如图 1 所示，该研究以设备无关量子密钥分发协议为例，定义了关于密钥生成观测量的互补测量，从而通过一个等价的量子纠错过程，通过相位错误数量反映实际协议中的隐私泄露，给出了紧致的解析估计。此外，通过推广经典信息论中的采样熵概念，并结合随机过程中的鞅论等技术，该研究设计了适用于非独立同分布统计的新型参数估计方法，从而给出了适用于最一般的相干攻击情形的完整安全性分析。基于对测量互补性原理作用的更好理解，新的安全性分析可以自然地与优势密钥提取等技术结合，并且显著降低了设备无关量子密码协议所需的数据量。通过重新分析基于离子阱平台实现的首个设备无关量子密钥分发实验演示的数据，新的分析方法可以将实验所需时间缩短至原先的三分之一。其中，针对冷原子、金刚石色心等平台的合理实验参数，新方法较先前最优的分析方法的提升甚至可达 2-3 个数量级，图 2 展示了相关模拟结果。这一结果对推进设备无关量子密码协议的实用化具有重要意义。

该成果研究论文：Xingjian Zhang, Pei Zeng, Tian Ye, Hoi-Kwong Lo, and Xiongfeng Ma, "Quantum Complementarity Approach to Device-Independent Security", Phys. Rev. Lett. 131, 140801 – Published 3 October 2023

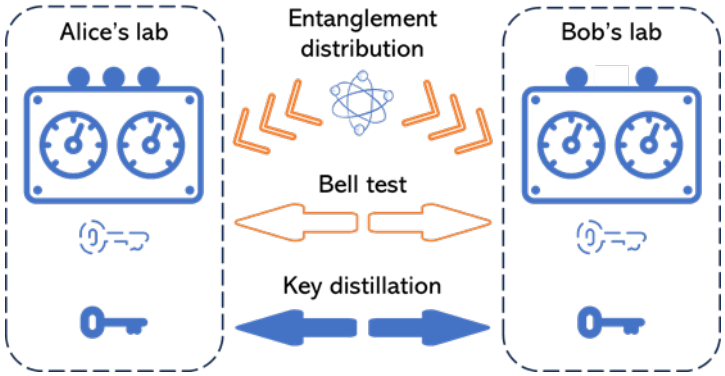



图 1 设备无关量子密钥分发流程示意图

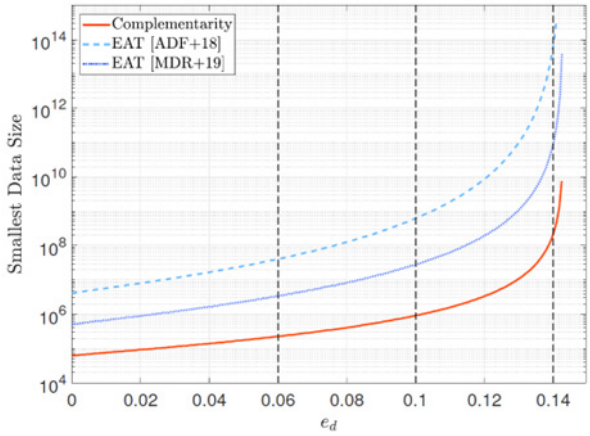



图 2 新分析方法（橙色实线）与先前分析方法（蓝色实线、虚线）最小数据量要求比较

# 实现基于器件无关量子随机数信标的零知识证明

零知识证明（ZKP）是一种基本的密码学工具，允许互不信任的通信双方之间，一方向另一方证明某个命题的有效性，同时不泄露任何额外信息。非交互式零知识证明（NIZKP）是 ZKP 的一种最重要的变体，其特点是通信双方无需多次信息交换。由于其简单易行并且互相通信次数少，NIZKP 广泛应用于数字签名、区块链和身份认证等领域。常用的 NIZKP 系统的安全性建立在生成可信的真随机数的假设之上，然而在实际应用中，由于真随机数生成器难以实现，通常会使用确定性的伪随机数算法来替代。此前已有研究指出，这种方法会产生潜在的安全隐患。

量子物理学的内禀随机性为解决这一安全隐患提供了全新方案。特别地，基于无漏洞贝尔不等式检验的器件无关量子随机数（DIQRNG）可以提供具有最高安全等级的真随机数，其安全性由量子力学基本原理保证，无需用户对量子设备进行任何先验表征或假设。图 3 展示了这一新方案的实现流程图。

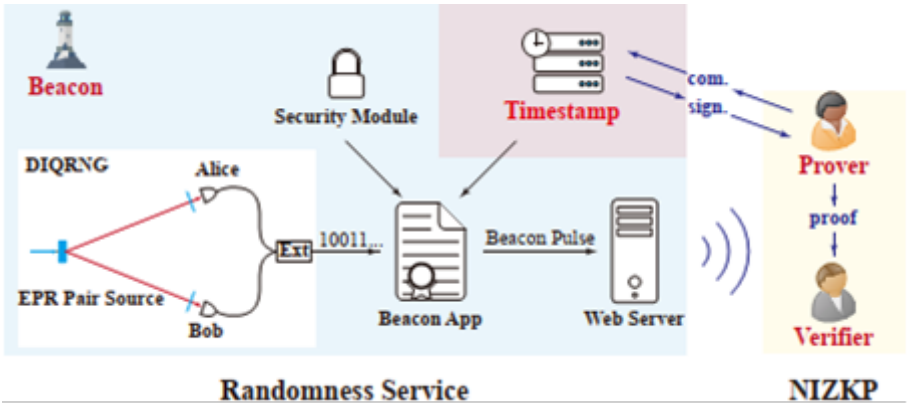



图 3 基于设备无关随机数信标服务的无交互零知识证明

马雄峰研究组与中科大实验团队合作，搭建了一个基于 DIQRNG 的信标公共服务系统，并利用该系统设计并实施了一种不依赖于真随机数假设的 NIZKP 方案。该随机数信标服务可以实时向公众广播生成的随机数。此外，为确保随机数在广播过程中的安全性，研究组采用了可以抵御量子攻击的量子安全签名算法。随后，研究组利用接收到的来自 DIQRNG 的随机数代替之前的伪随机数，构建并实验验证了更安全的 NIZKP 协议。该研究工作首次将量子非局域性、量子安全算法和零知识证明三个不同的领域结合起来，大幅提升了零知识证明的安全性，其中构建的面向公众的随机数服务在密码学、彩票业和社会公益等领域有着重要的潜在应用。

该成果研究论文：Cheng-Long Li, Kai-Yi Zhang, Xingjian Zhang, Kui-Xing Yang, Yu Han, Su-Yi Cheng, Hongrui Cui, Wen-Zhao Liu, Ming-Han Li, Yang Liu, Bing Bai, Hai-Hao Dong, Jun Zhang, Xiongfeng Ma, Yu Yu, Jingyun Fan, Qiang Zhang, Jian-Wei Pan, "Device-independent quantum randomness – enhancedzero-knowledge proof", Proc. Natl. Acad. Sci. U. S. A. 120(45), e2205463120. (2023). 2023 Nov 7.

# 在一般测量下对输出结果的内禀随机性进行刻画

随机数是重要的资源，量子力学中的不确定性原理提供了产生无法预测的真随机数的方法。典型的量子随机数发生器由源端与测量端构成。源发射出的彼此独立的态经过测量可以产生一系列测量结果，窃听者可以通过与设备之间的关联获得测量结果的相关信息，因此测量结果的随机性实际分为两部分：内禀随机性与外在随机性。用户需要分析测量结果中除去信息泄露部分的内禀随机性。通过层析，源发出的态由密度算子刻画，测量端由正算子测量（POVM）刻画。一个基本的问题是在给定态与测量的情况下对测量结果的内禀随机性进行刻画。

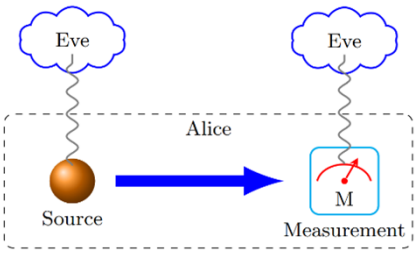



图 4 一类典型的量子随机数发生器

马雄峰研究组通过对量子测量进行广义 Naimark 延拓以及对输入态进行纯化，给出了相应的对抗模型。在该对抗模型中，窃听者可以通过与用户的随机数发生器产生纠缠推测用户可能得到的测量结果。此时，内禀随机性的量化可以写成一个优化问题，特别地，当测量是极测量时，这个优化问题可以准确求解。根据该结果，对于对称且信息完备的测量（SIC POVM），对所有的输入态，内禀随机性都会有一个仅与系统维度相关的下界。这给出了一种源无关的随机数产生方案。另外，由于内禀随机性与量子相干的紧密相关，随机性度量可以看成相干度量，基于该度量可以定义非相干态与非相干操作。

该成果研究论文：Hao Dai, Boyang Chen, Xingjian Zhang, and Xiongfeng Ma, "Intrinsic randomness under general quantum measurements", Physical Review Research 5, 033081 (2023).

# 三、超导量子计算

主要完成人：孙麓岩研究组、邓东灵研究组

## 实现量子纠错对逻辑量子比特的纠缠保护

纠缠是上个世纪物理学中最重要的概念之一，也是量子信息科学中最基本的资源之一。纠缠的探索不仅有助于量子力学的基础，还推动了量子信息技术的发展。纠缠使许多反直觉的事情成为可能，如用于传输未知量子态的量子隐形传态、用于纠缠非相互作用粒子的纠缠交换以及超越经典极限的精密测量。因此，纠缠成为应用中最重要的量子资源。然而，纠缠是非常脆弱的。尽管纠缠不能通过局部操作和经典通信生成，但它可以被局部的退相干效应摧毁。图 1a 所示，由于每个量子比特与环境相互作用，量子信息泄漏到环境中导致纠缠破坏。

在孙麓岩研究组的研究中，研究人员通过量子纠错（QEC）实现了纠缠的逻辑量子比特，并进一步保护了逻辑量子比特之间的纠缠。与二能级的物理量子比特相比，逻辑量子比特由高维量子系统的子空间编码而成，冗余的自由度允许检测和纠正潜在的错误。如图 1b 所示，通过将图 1a 中的物理量子比特替换为逻辑量子比特，系统与环境的相互作用将纠缠从 code-code 子空间转变为 code-error 或 error-error 子空间，而不是直接破坏它，逻辑量子比特之间的纠缠可以通过局域的量子纠错操作恢复。

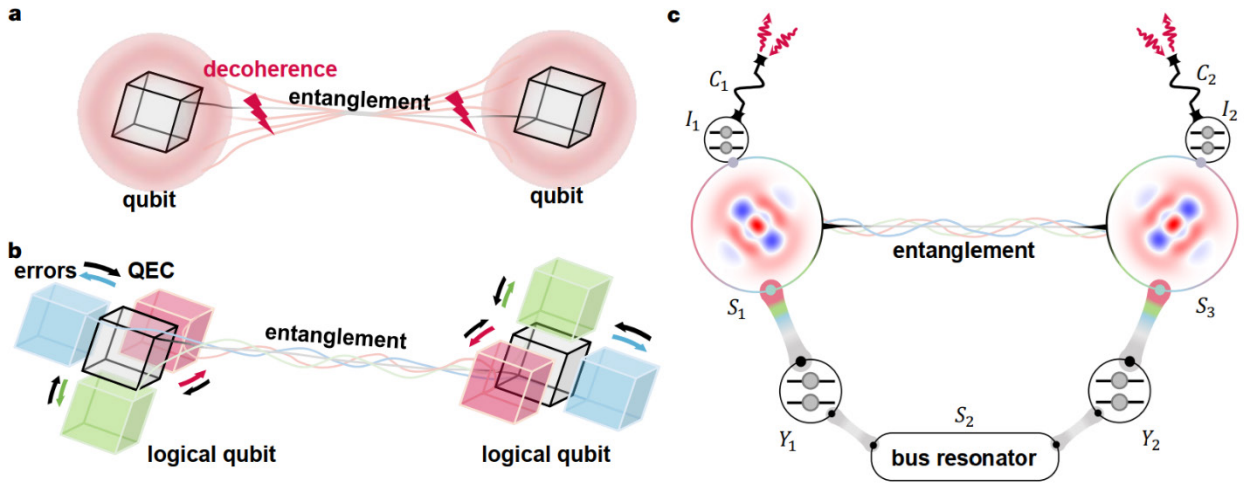



图 1 纠缠逻辑量子比特（ELQ）的原理和装置图

在孙麓岩研究组的实验中，研究人员首次通过量子纠错，成功保护了纠缠状态，相较于未受保护的 ELQ，ELQ 的相干时间提高了 45%，如图 2。此外，首次展示了逻辑量子位通过独立误差检测和每个逻辑量子位的后选择在测量贝尔信号 B = 2.250 ± 0.019 时违反贝尔不等式，超过了经典边界 13 个标准偏差，如图 3。受保护的 ELQ 有望在未来的量子基础研究和量子网络应用中发挥重要作用。

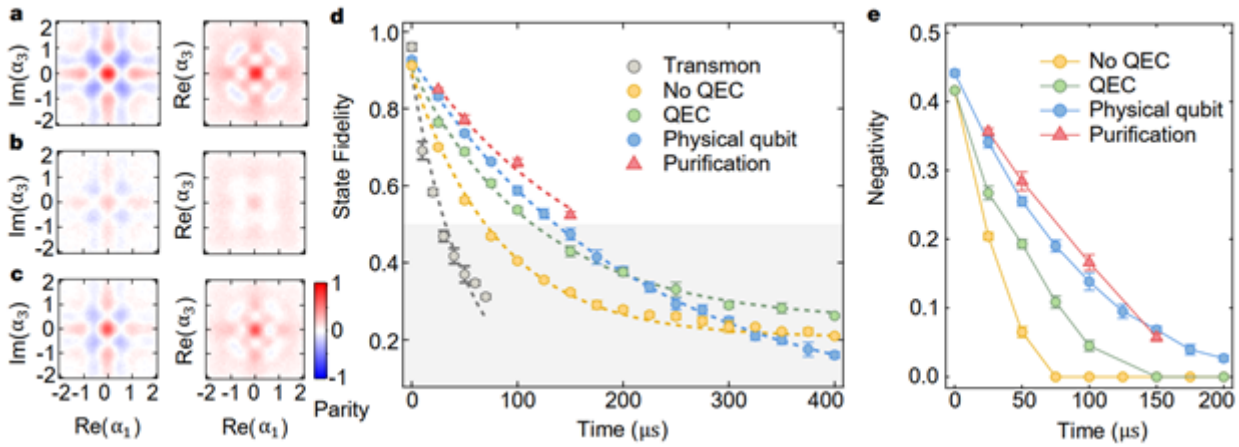



图 2 利用量子纠错实现对逻辑量子比特的纠缠保护

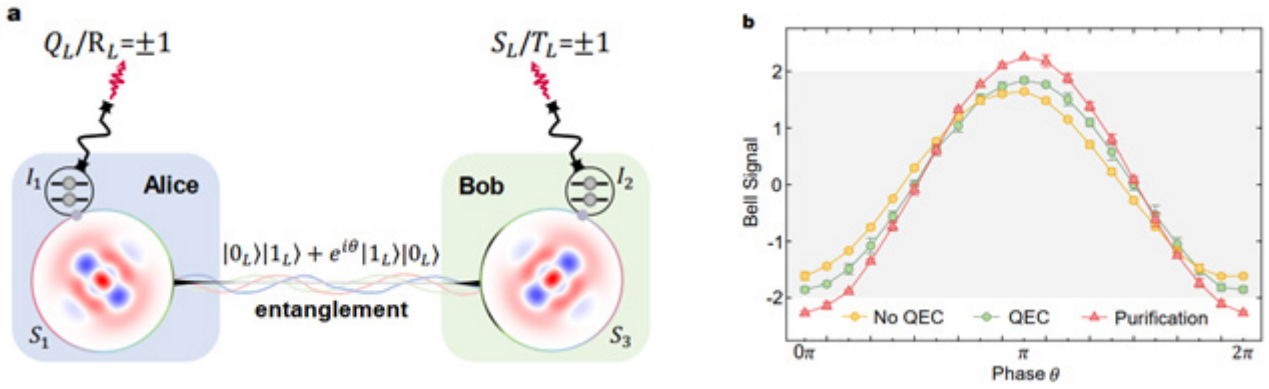



图 3 利用纠缠的逻辑量子比特演示贝尔不等式的违背

该成果研究论文：Weizhou Cai, Xianghao Mu, Weiting Wang, Jie Zhou, Yuwei Ma, Xiaoxuan Pan, Ziyue Hua, Xinyu Liu, Guangming Xue, Haifeng Yu, Haiyan Wang, Yipu Song, Chang-Ling Zou, Luyan Sun, "Protecting quantum entanglement between error-corrected logical qubits", arXiv preprint arXiv:2302.13027.

# 在超导量子系统中演示深度量子神经网络

近年来，经典机器学习已经在科学研究和商业应用中取得了显著的成就。特别是深度神经网络模型的快速发展，对解决一些具有挑战性的问题起到了关键作用。深度神经网络的多层结构被认为是从复杂数据中提取有效特征的关键，而反向传播训练算法则有效提升了深度神经网络的训练效率，推动了其快速发展和广泛应用。与此同时，量子机器学习领域也取得了重大进展。在理论上，已有研究证明在某些特定的分类任务中，量子机器学习模型相对于经典机器学习模型具有指数级的加速优势。在实验方面，随着量子器件的快速发展，一些量子机器学习模型，如量子卷积神经网络、量子对抗机器学习模型，已在实验平台上成功演示。

最近两年，有理论工作提出一种新型的深度量子神经网络结构和量子反向传播算法。然而，在当前带噪声的中等规模量子器件上演示深度量子神经网络的训练过程面临着很多困难。孙麓岩研究组与邓东灵研究组专注于该深度量子神经网络模型，并设计了一种可以在数字量子器件中实施的反向传播算法，并在平面超导量子系统上成功演示了该模型的训练有效性和泛化能力。在该模型中，量子比特被分层排布，从而形成深度量子神经网络的多层结构；作用在相邻层量子比特上的参数化量子线路构成层间感知器。在正向运行网络的过程中，量子信息会通过量子感知器，由输入层，经过多个隐藏层，最终逐层传递到输出层。在反向运行网络时，量子信息会逐层由输出层传递到输入层。当训练相邻层间的量子门参数时，研究人员需要分别正向和反向运行深度量子神经网络，并提取这相邻两层的局部量子信息，以计算层间各参数的梯度。

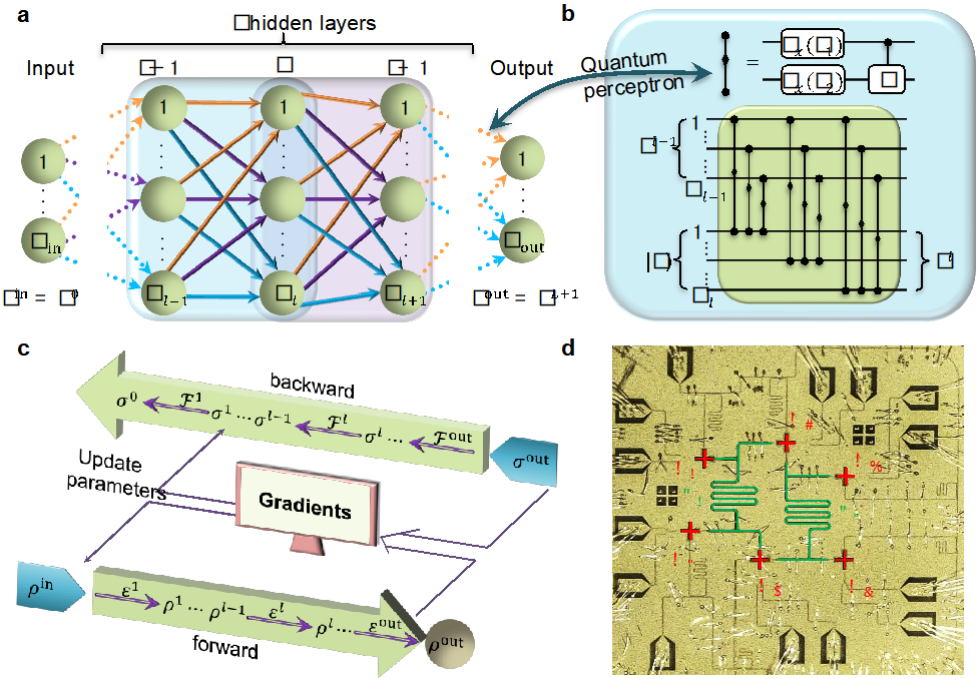



图 1：深度量子神经网络结构及量子反向传播算法示意图

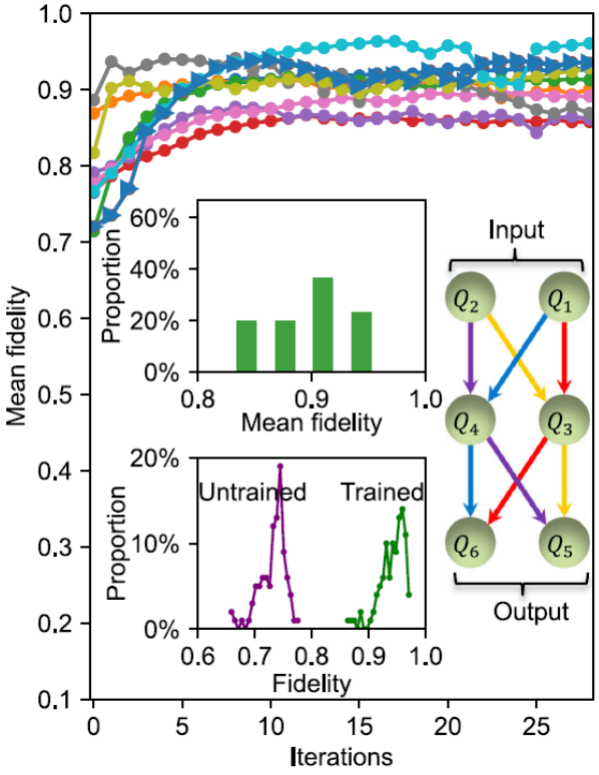



图 2：深度量子神经网络学习两比特量子通道的训练过程

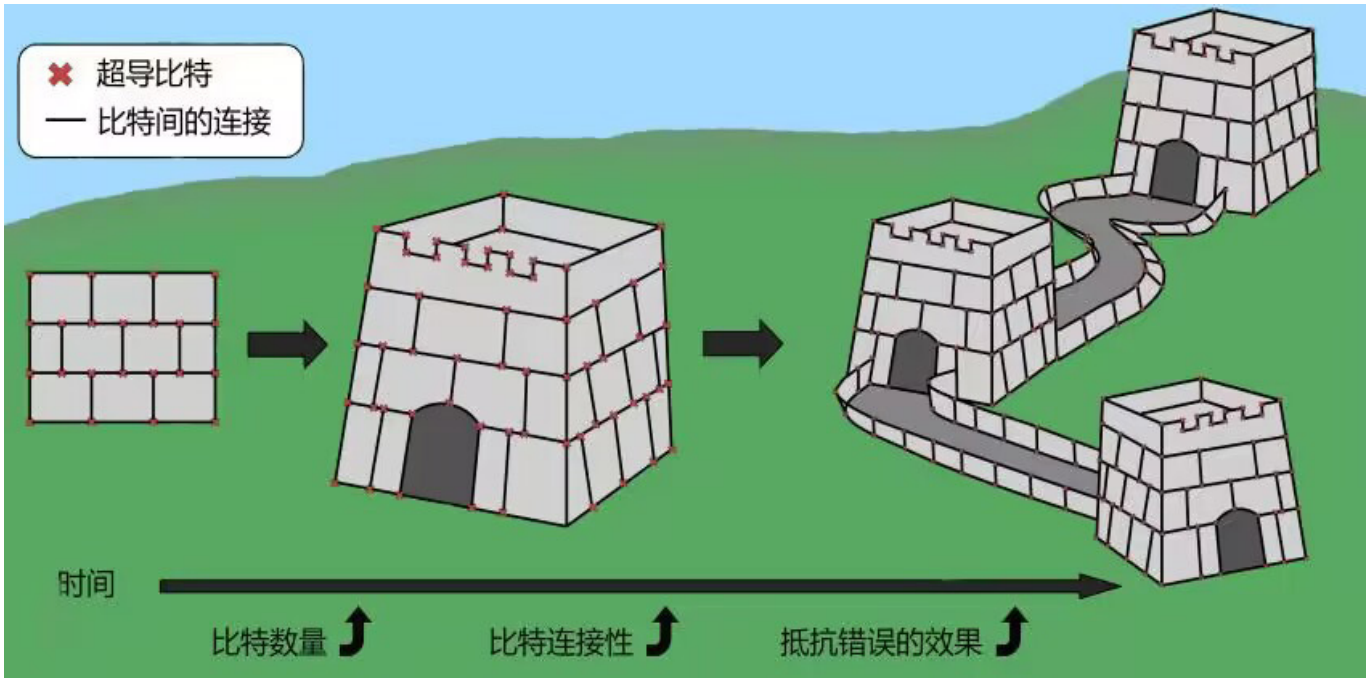
实验演示了深度量子神经网络学习量子通道的训练过程。实验通过反向传播算法优化网络的门参数，使得量子网络输出层的量子态与目标量子通道的输出态尽可能接近。在训练过程中，研究人员在量子芯片上正向运行了深度量子网络，并在经典计算机上模拟了网络的反向运行过程。实验通过量子态层析方法提取网络中每一层的量子态，并利用提取出的相邻层间的量子态信息计算得到相邻层间各参数的梯度，从而实现深度量子神经网络参数的迭代更新。

实验设计了深度为三层，每层宽度为两比特的 6 比特超导量子芯片，用于学习两比特量子通道。实验结果如图 2 所示。结果表明，在较短的迭代次数内，训练过程可以有效收敛，且平均保真度最高达到 96%。在泛化测试中，训练后的量子神经网络对于 43% 的随机输入态，输出态与目标量子信道输出态的保真度超过 95%。这些实验结果成功展示了深度量子神经网络的可训练性与泛化能力。当量子比特噪声水平进一步降低后，实验所用的训练方法可以直接扩展到具有更深层数和更大宽度的大规模量子网络上，从而进一步提升量子机器学习的实用价值。

该成果研究论文：Xiaoxuan Pan, Zhide Lu, Weiting Wang, Ziyue Hua, Yifang Xu, Weikang Li, Weizhou Cai, Xuegang Li, Haiyan Wang, Yi-Pu Song, Chang-Ling Zou, Dong-Ling Deng & Luyan Sun, "Deep quantum neural networks on a superconducting processor", Nature Communications volume 14, Article number: 4006 (2023).

# 超导量子计算系统中的容错技术

随着超导系统中的量子控制技术日益成熟，量子纠错技术也在不断发展。最近，已有一些平台实现了超越量子纠错盈亏平衡点的里程碑式突破。然而，要实现最终目标—容错量子计算，仍需要拓展系统的维度并进一步压制噪声。受《物理》杂志邀请，孙麓岩教授与中国科学技术大学邹长铃和陈子杰撰写了一篇综述文章，以超导量子系统为例，首先介绍了四种实现容错错误症状测量的思路；以此为基础，讨论了实现容错量子计算的三个关键阶段以及各阶段所面临的挑战，包括超越盈亏平衡点、达到容错阈值和实现完备逻辑门操作。为了实现这些目标，将按照连通性从低到高归纳三种可能的拓展系统规模的方案。此外，这篇文章还总结了实验上纠错技术的进展以及对连通性的探索，最后讨论当前关键的研究问题。

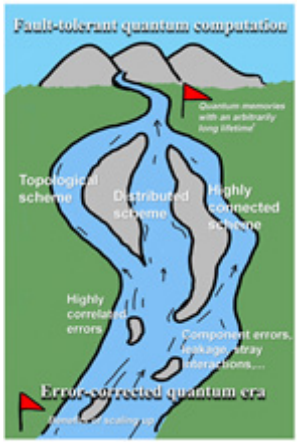



该成果研究论文：陈子杰，孙麓岩，邹长铃，“超导量子计算系统中的容错技术”，物理 52，751 （2023）。

# 进入量子纠错时代

量子计算机具有在某些问题上（比如大数因子分解和无序数据库搜索）远超经典计算机的运算能力，因此受到大家极大的关注。然而，量子计算面临一个巨大的挑战 -- 退相干，因为存储量子信息的物理系统跟外界环境之间的相互作用不能够完全可控。这就导致计算过程中会随机出错，从而使最终的计算结果不可靠。因此，一个通用量子计算机一定要由逻辑比特构造而成，通过量子纠错来对抗外界环境噪音的影响。所以，量子纠错是量子计算的最核心问题之一。

孙麓岩教授与南方科技大学、福州大学、中国科学技术大学和北京量子院合作，一方面提高了超导量子比特的相干时间，另一方面结合了最近发展的新操控技术，基于玻色二项式编码突破了量子纠错的盈亏平衡点，真正展示了量子纠错的优势。与此同时，美国耶鲁大学团队也在基于玻色模式的 GKP 编码中突破了量子纠错盈亏平衡点；谷歌量子团队基于表面编码演示了码距变大时逻辑比特的错误率得到进一步抑制，展示了表面编码扩展的有效性。受 Science Bulletin 杂志的邀请，孙麓岩教授与中国科学技术大学邹长铃和陈子杰撰写了评论文章，认为这些工作标志着量子计算已经进入了量子纠错时代。该文展望了实现最终容错量子计算所面临的各种挑战和可能的解决方法，总结了实现容错量子计算的三种不同技术方案，最后提出了该纠错时代中另一个标志性节点：进一步提高量子纠错的性能，实现量子纠错保护的逻辑比特寿命超过量子纠错盈亏平衡点 100 倍。




实现容错量子计算的挑战与展望

该成果研究论文：Z.-J. Chen, L. Sun, and C.-L. Zou, "Entering the error-corrected quantum era", Sci. Bul. 68, 961 (2023).

# 四、量子人工智能

主要完成人：邓东灵研究组

## 机器学习物质相：无法学到的部分

近年来，机器学习中的一些方法和技术被用来处理复杂的量子多体问题以应对希尔伯特空间维度指数增长带来的挑战。例如，一些监督和非监督学习方法已在识别系统所属的物质相以及判别对应的相变点上取得了显著进展。然而，不论是从理论还是实验的角度，这些方法的可靠性都受到了极大的关注：经典机器学习领域中的研究发现，如果数据的维度足够高，机器学习模型可能会对人为设计的微小扰动极其脆弱。考虑到物质相所表现出的稳定性，人们会考虑：通过机器学习方法训练的模型是否能真正学习到物质相分类的物理判据？在考虑实验噪声的情况下，机器学习方法带来的优势是否仍然存在？

通过分析两个具体例子的对抗样本与机器学习模型的推断过程，邓东灵研究组表明基于神经网络的分类器并未完全学习到物理系统中潜在的关键属性。第一个例子考虑二维经典铁磁伊辛模型（图 1）。通过分析分类器激活图，发现分类器虽然能以近乎完美的准确率判别系统所处的物质相，其并未捕捉到系统所具有的空间平移对称性。通过在激活图中违反对称性权重较大的位置施加扰动，对抗样本更容易产生，以此解释了对抗攻击在这个例子中的来源。

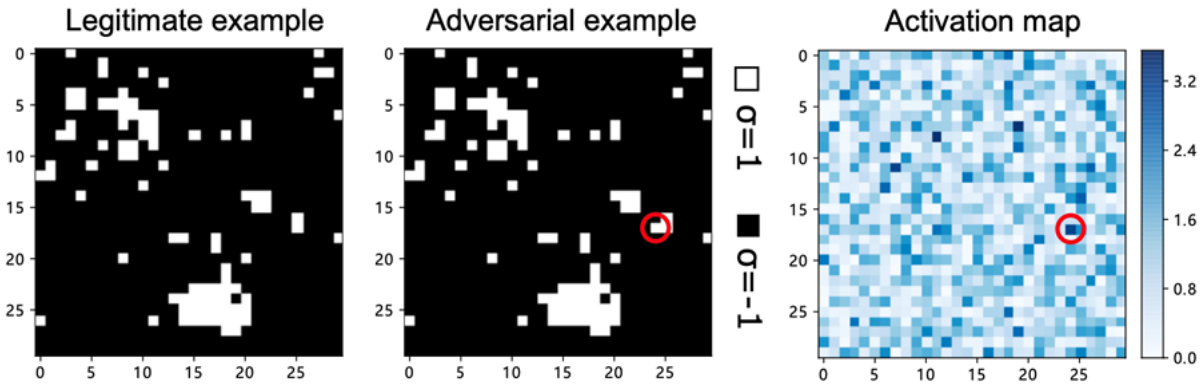



图 1: 经典铁磁伊辛模型分类任务中的原始样本、对抗样本和分类器的激活图

第二个例子考虑拓扑相。发现对原始样本进行少数局部的扰动会误导分类器做出错误的预测，这与描述该系统的拓扑不变量对局部扰动鲁棒的事实相悖。同时发现对抗样本在动量空间中的纹路没有发生显著变化（图 2 中），固定自旋朝向在动量空间的原相也仍然形成了闭合环路（图 2 右）。由此说明了分类器并未捕捉到系统的拓扑性质作为分类判据。

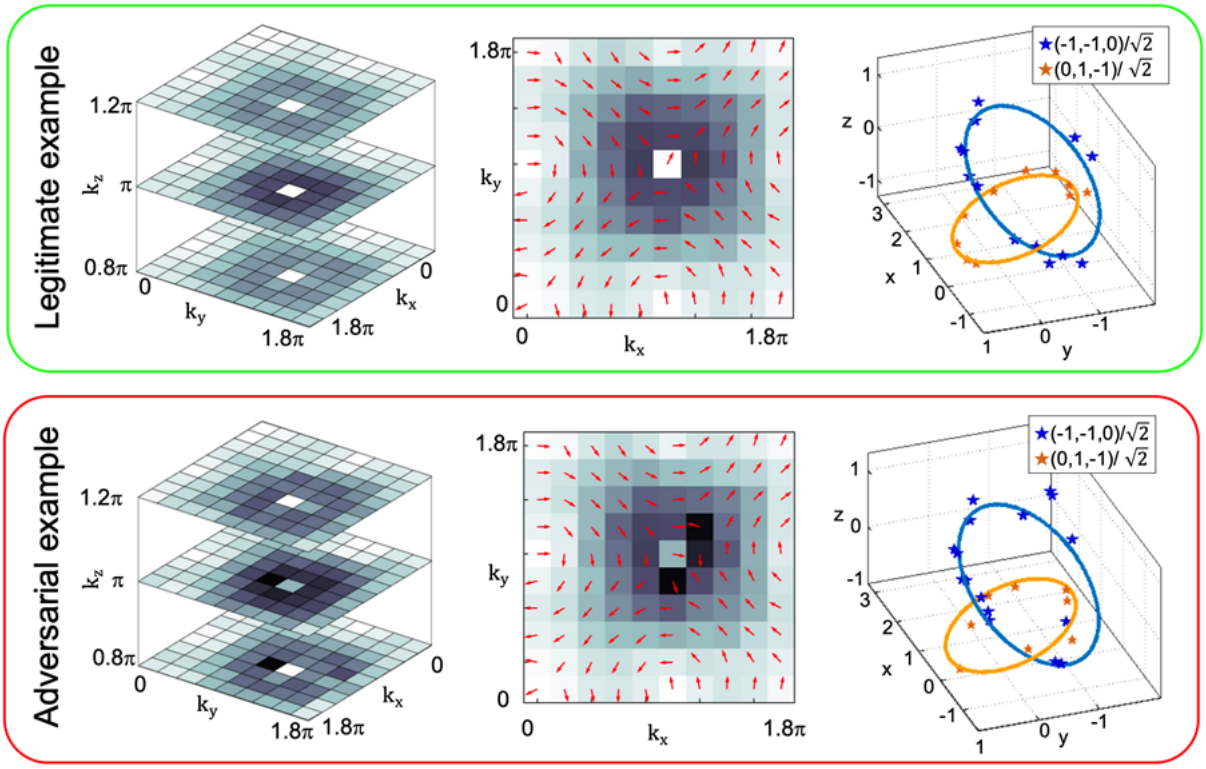



图 2: 拓扑相分类任务中的原始样本、对抗样本和对应的拓扑性质

此外，发现随着数据需求量的减少，实验随机噪声成为对抗扰动的的比例也在增加（图 3 左）。在接近相变点时，实验随机噪声更有可能表现为对抗性扰动（图 3 右）。 由此表明机器学习模型表现出的对数据量的优势在考虑实验噪声的情况下会被减弱，相变点的精确识别也变得更加困难。

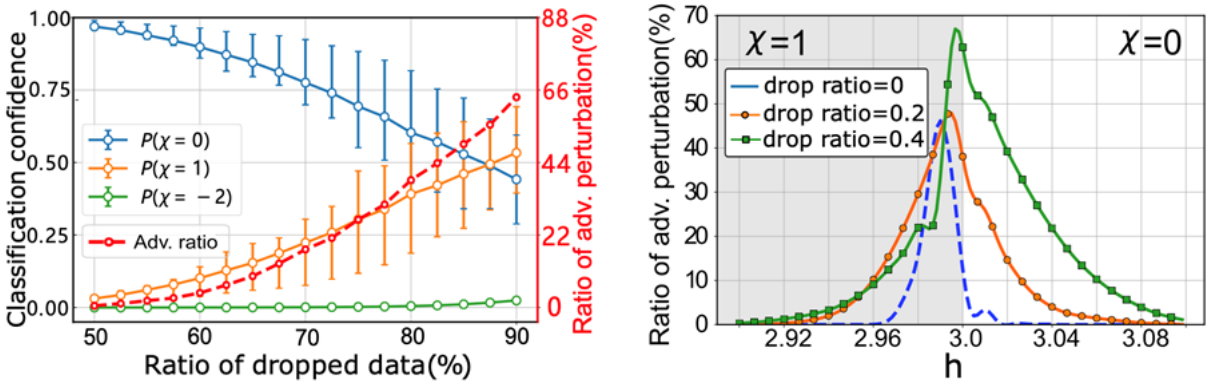



图 3: 不同数据需求量下实验随机噪声成为对抗扰动的的比例与相变点附近的表现

该成果研究论文：1. Huili Zhang, Si Jiang, Xin Wang, Wengang Zhang, Xianzhi Huang, Xiaolong Ouyang, Yefei Yu, Yanqing Liu, Dong-Ling Deng, L.-M. Duan, "Experimental demonstration of adversarial examples in learning topological phases", Nat Commun 13, 4993 (2022)； 2. Si Jiang, Sirui Lu, Dong-Ling Deng, "Adversarial Machine Learning Phases of Matter", Quantum Front 2, 15 (2023).

# 五、凝聚态物理学

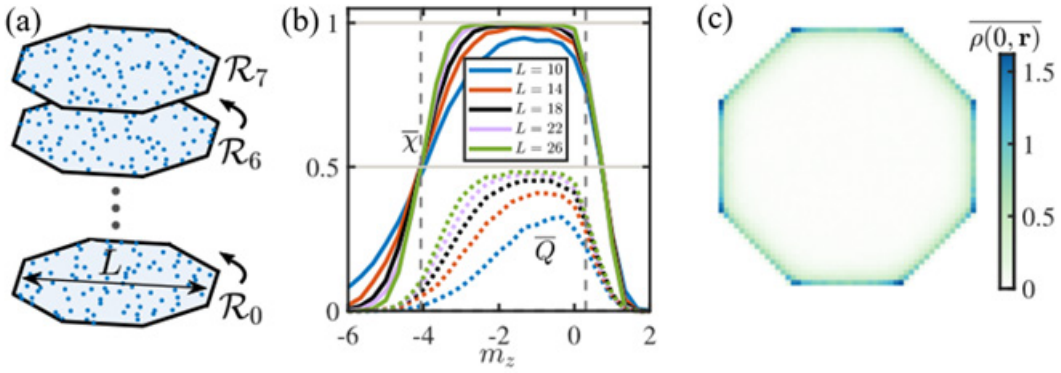
主要完成人：徐勇研究组

## 平均对称性保护的高阶非定形拓扑绝缘体

有关拓扑相的研究大多建立在有平移对称性的晶体系统上，而非晶体系中的拓扑相也逐渐引起了大家的兴趣，其中包括准晶和非定形晶格。不同于常规晶格中只允许存在二重、三重、四重或六重旋转对称性，准晶允许更加宽泛的旋转对称性，比如五重或八重旋转对称性，有趣的是这些新奇的旋转会保护一些新的高阶拓扑相。非定形体系作为另一种非晶体系，虽然对于单一样本它没有旋转对称性，但是对于大量样本的系综平均，非晶体系有平均旋转对称性。那么自然有一个问题：非定形体系的平均旋转对称性是否保护新的高阶拓扑相，而这种拓扑相并不存在于常规晶格?

徐勇研究组首次在理论上证明了二维非定形晶格中存在受平均对称性保护的高阶拓扑相，这些新的拓扑相并不存在于常规晶格中。研究组基于正八边形中的非定形晶格构造新的紧束缚模型，其哈密顿量满足一种结合了平均八重旋转对称性和镜面对称性的新对称性。在这一平均对称性下，系统是有八个零能拓扑角态的安德森绝缘体，这一新奇拓扑相没有常规晶格的对应。此外研究组提出两个拓扑不变量来描述这一拓扑相，其中一个是基于平均对称性定义的拓扑量，另一个是新提出的一般化四极矩。另外，课题组还在正十二边形的非定形晶格中发现了受平均对称性保护的高阶拓扑相，其拓扑表象是十二个零能角态。

此项工作发现了非定形晶格中的新的高阶拓扑相，并提出了两个新的拓扑不变量，为后续探索非定形晶格中的新奇拓扑相开辟了道路。




(a) 非定形晶格的示意图；(b) 两种拓扑不变量随参数变化图；(c) 非平庸角态的态密度图

该成果研究论文： Yu-Liang Tao, Jiong-Hao Wang and Yong Xu, "Average symmetry protected higher-order topological amorphous insulators", SciPost Phys. 15, 193 (2023).

# 六、冷原子量子网络

主要完成人：段路明研究组、濮云飞研究组

## 可实现 1000 个光量子比特随机存取的存储器

量子存储器是实现量子计算，量子网络，量子精密测量的关键部件。同时具备高保真度，长存储寿命，多存储模式，以及随机存取功能的光量子存储器是实现长距离量子中继和量子网络的必备条件。目前可以用来处理大规模光量子比特流的量子存储器尚未实现。

在该工作中，段路明、濮云飞研究组实验实现了具有 72 个光量子存储单元（规模同目前最大的量子计算机可比），存储时间 >500 微秒（光子在 100km 光纤中传输的时间），以及 1000 次光量子比特操作（对于一个 72 光量子比特的输入序列可产生 72! ≈ 10^104 种不同的输出序列），是之前的世界纪录 12 次的接近 100 倍。在此基础上，该工作首先展示了一个接近于经典计算机中的随机读写存储器（RAM）的光量子随机读写，在 1000 次读写中，存储的保真度为 93(5) %。

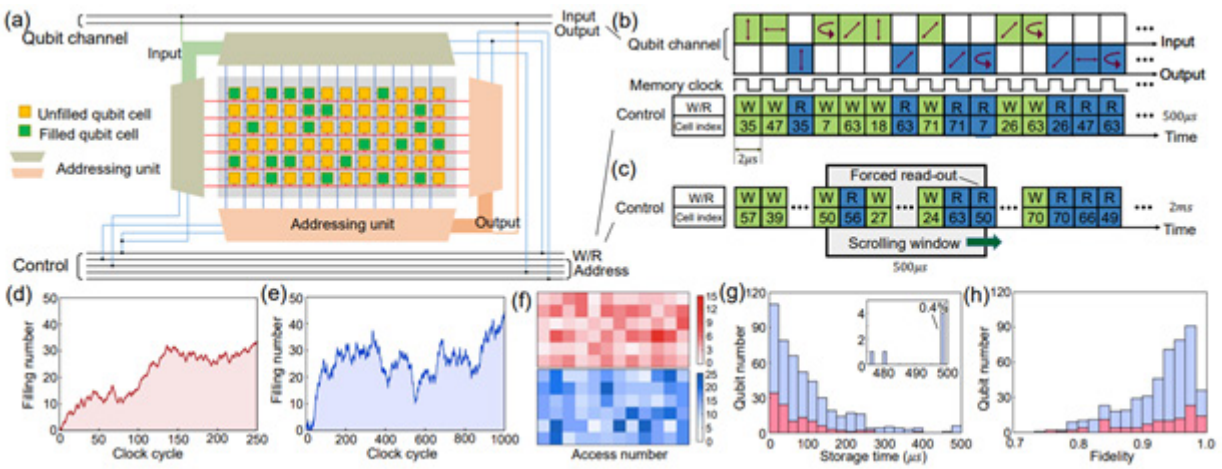



图 1：大规模量子随机读取存储器

此外，该工作也展示了几种在经典信息处理中的数据结构在量子系统中的实现。分别实现了量子队列，量子堆栈，和量子缓存器。这些实现对于拓宽量子存储的工具库以及对未来更大规模和更加复杂的量子体系，以及量子操作系统的实现有帮助。

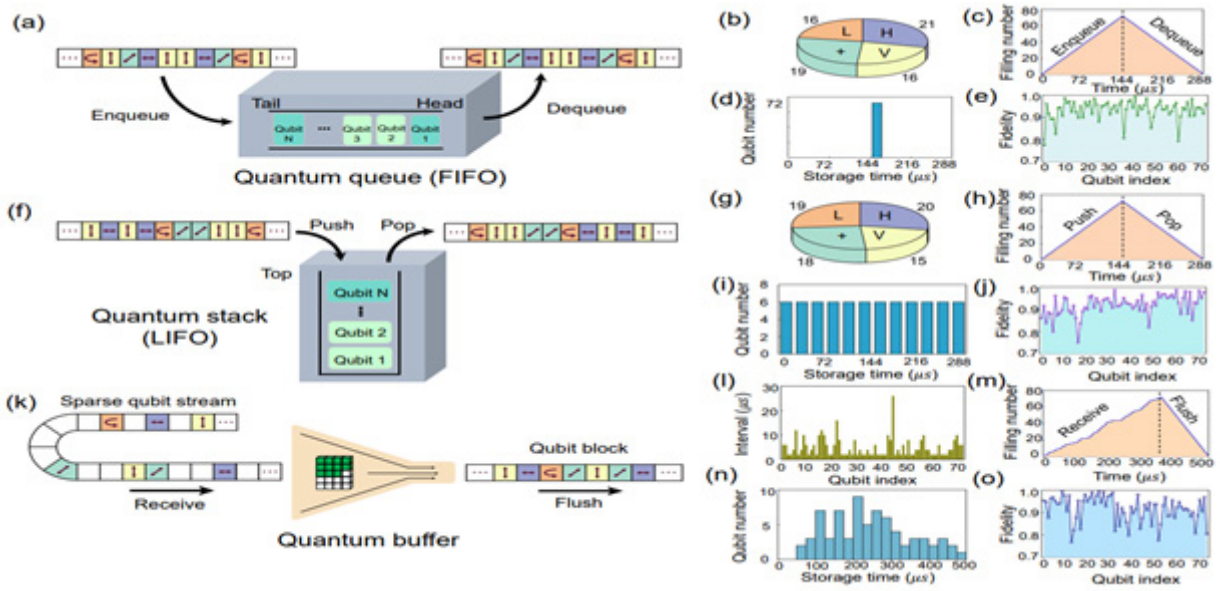



图 2：量子队列，堆栈，缓存器的实验实现

最后，该工作展示了连续 4 个随机产生的纠缠光子对的存储，同步，以及交换顺序的输出。这对于量子中继的实现至关重要。

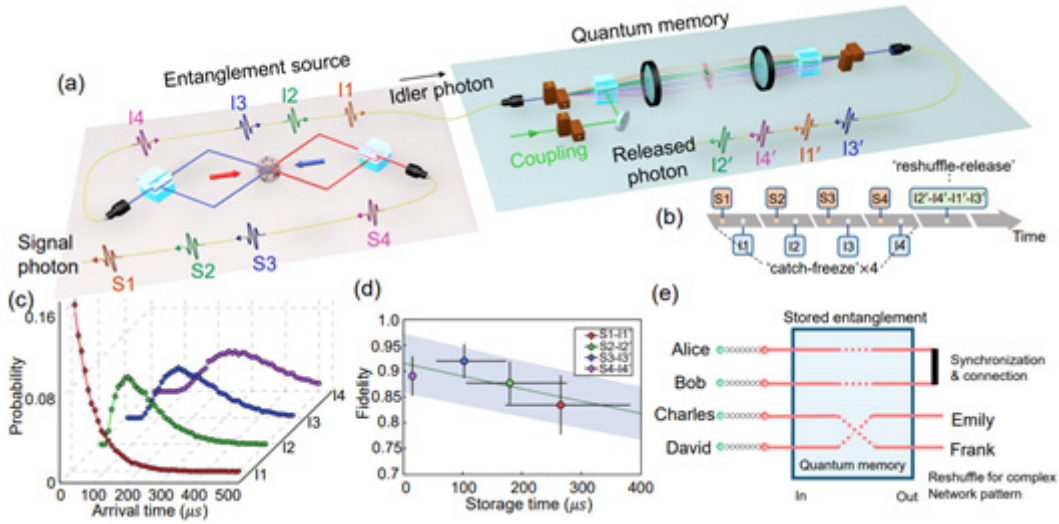



图 3：同步和交换四个纠缠光子对

该成果研究论文：Sheng Zhang, Jixuan Shi, Zhaibin Cui, Ye Wang, Yukai Wu, Luming Duan and Yunfei Pu, "Realization of a programmable multi-purpose photonic quantum memory with over-thousand qubit manipulations", arxiv:2311:10292.