

吴华伟

+86 15860043535

wuhuawei1996@gmail.com

中国福建省莆田市

教育 & 学术背景

巴黎第八大学 | 博士后研究员

2024.03 - 2025.03

- 合作导师: Sihem Mesnager 教授
- 研究方向: 具有良好密码学性质的密码函数
- 研究成果: 完成三篇论文, 两篇已发表在领域核心期刊

清华大学 | 博士

2018.09 - 2024.06

- 专业: 数学
- 研究方向: 前期为代数几何与数论, 后转入编码学、密码学与组合设计
- 研究成果: 完成四篇论文, 三篇已发表在领域核心期刊

华中科技大学 | 学士

2014.09 - 2018.06

- 专业: 信息与计算科学 (数学与统计学院)
- 相关课程: 概率论, 随机过程, C++, 数据结构
- 绩点: 4.0 (专业第二)

研究描述

- 对称密码学
 - 研究内容: S-盒为对称密码体制安全性的核心。我的研究聚焦于通过优化设计与关键参数评估, 构造兼具多种优良密码学性质的 S-盒, 旨在增强密码系统的抗攻击能力。
 - 研究方法: 编写多进程程序 (基于 Python 的 SageMath 框架) 获取大量数值结果, 从中识别规律并提出猜想, 最终完成严格的数学证明。
 - 研究成果: 运用代数几何及数论工具, 确定了数类经典密码函数的重要密码学参数, 证实或证伪了领域内的若干猜想 (论文 [4, 5, 7])。
- 编码学
 - 研究内容: 聚焦于为经典及新兴信道 (如 DNA 存储) 构造兼具强纠错能力与高效率的编码方案。
 - 研究方法: 针对信道特性, 运用代数学、组合数学、图论等工具, 确定所设计编码方案的参数或推导其理论界限。
 - 研究成果: 确定了两类基于 PN 函数的线性码的重量分布, 克服了以往研究对函数具体形式的依赖 (论文 [1]); 运用图论工具证明了 DNA 纠错码具备良好纠错能力的充要条件, 将此前的相关成果推广至一般情形 (论文 [6])。
- 组合设计
 - 研究内容: 组合设计主要研究从集合中选择子集族并安排它们的结构, 以满足某些组合性质, 其在算法设计、实验设计等领域有广泛应用。我的研究聚焦于构造各类新型的组合设计对象, 或证明其不存在性。
 - 研究成果: 构造了一大类由著名组合学家 Stinson 提出的新组合对象: 循环外差族 (其在秘密共享中有重要应用), 并证明了强循环外差族的不存在性定理 (论文 [2]); 利用某些对称多项式构造了新的 3-设计的无穷族 (论文 [3])。

项目经历

- Realized Volatility Prediction
 - 目标: 基于高频订单簿与交易数据预测股价已实现波动率。
 - 核心流程:
 - 特征工程: 使用 NumPy、Pandas 处理高频数据, 构建量价因子、时间窗聚合特征, 并应用近邻算法生成上下文特征。
 - 混合建模: 主力模型采用 LightGBM, 同时基于 PyTorch 构建 MLP 与 1D CNN。应用时间序列交叉验证, 最终通过加权平均集成预测结果。
 - 技术栈: NumPy, Pandas, Scikit-learn, LightGBM, PyTorch, Joblib。
 - 成果与评估: 通过该项目熟悉了高频数据处理、高级特征构建及多模型集成策略。模型在 RMSPE (均方根百分比误差) 指标上可达到 0.22 的水平。

- Reputation Interplay in Supply Chains: How Partners' Environmental Risks Shape Firms' Disclosure Strategies
 - 担任数据处理分析工作，微调了 FinBERT 模型及指令微调 Qwen 2.5 模型，将其用于中国上市公司年报的文本分类任务，从而衡量企业的气候风险披露程度。
 - 论文已投递至管理学领域顶刊 Production and Operations Management (UTD-24)。

技能与兴趣

- 语言: Python, JavaScript, Rust
- 技能: 数据分析, 机器学习, 深度学习, 桌面应用开发
- 工具: GIT, Jupyter Notebook, Visual Studio Code, SageMath
- 兴趣: 音乐 (唱歌 & 弹琴), 编程, 旅行

荣誉与奖项

学术类奖项

- 中国科学院信息工程研究所“密码与数学”暑期学校竞赛第 1 名, 2023
 - 核心任务: 两周内尝试解决一个开放性密码学问题。
 - 创新性地运用编程工具辅助数学证明。
 - 作为唯一完整解答该问题的参赛者, 还将研究结果推广至更一般情形。
- 第八届全国大学生数学竞赛 (数学类高年级组) 决赛二等奖 (第 16 名), 2017
 - 湖北省该年仅一人入围该组别全国决赛。
 - 创下本系学生在该赛事全国决赛中的首次获奖记录。

国家级荣誉

- 国家奖学金 (8,000 元), 2 次
- 国家励志奖学金 (5,000 元), 2015

省级荣誉

- 武汉市优秀毕业生, 2018

校级荣誉

- 清华大学综合奖学金, 2022
- 华中科技大学三好学生, 3 次

学生工作

- | | |
|---------------------------|-------------------|
| • 组织创办华中科技大学推理协会并担任副会长 | 2017.09 - 2018.06 |
| • 担任华中科技大学数学与统计学院学生会副主席 | 2016.10 - 2017.10 |
| • 担任华中科技大学数学与统计学院科学技术协会主席 | 2016.10 - 2017.10 |

论文发表

- [1] **Wu, H.***, Yang, J. and Feng, K., 2023. The Weight Distributions of Two Classes of Linear Codes from Perfect Nonlinear Functions. IEEE Transactions on Information Theory, vol. 70, no. 6, pp. 4102-4109.
- [2] **Wu, H.***, Yang, J. and Feng, K., 2024. Circular External Difference Families: Construction and Non-Existence. Designs, Codes and Cryptography, pp.1-14.
- [3] Xu, G., Cao, X., Luo, G.* and **Wu, H.**, 2024. Infinite Families of 3-Designs from Special Symmetric Polynomials. Designs, Codes and Cryptography, pp.1-23.
- [4] Mesnager, S. and **Wu, H.***, 2025. On the Differential and Walsh Spectra of x^{2q+1} over \mathbb{F}_{q^2} . Finite Fields and Their Applications, 103, p.102576.
- [5] Mesnager, S. and **Wu, H.***, 2025. The Differential and Boomerang Properties of a Class of Binomials. IEEE Transactions on Information Theory, vol. 71, no. 6, pp. 4854-4871.
- [6] **Wu, H.***, 2023. DNA-Correcting Codes in DNA Storage Systems. arXiv preprint arXiv:2311.09910.
- [7] Mesnager, S. and **Wu, H.***, 2025. An In-Depth Study of the Power Function x^{q+2} over the Finite Field \mathbb{F}_{q^2} : the Differential, Boomerang and Walsh Spectra, with an Application to Coding Theory. arXiv preprint arXiv:2407.07710.

注: 在数学领域的国际合作中, 论文作者按名字首字母排序; 打 * 号的表示为通讯作者; 除 [3] 外, 均为第一核心贡献者。