# 荣大中 / Dazhong Rong

✉ rdz98@zju.edu.cn ☎ +86 15927237774
🎓 https://scholar.google.com/citations?user=C29smY4AAAAJ

## 教育经历

2020 – 2025 **直博, 浙江大学** 计算机科学与技术
荣誉: 优秀研究生/三好研究生

2016 – 2020 **本科, 武汉大学** 网络空间安全
荣誉: 优秀毕业生/推荐免试攻读研究生/三好学生

## 实习经历

2022.11 – 2023.05 **算法工程师,** 蚂蚁集团-大安全-机器智能, 支付宝（杭州）信息技术有限公司.
- 隐私计算技术在金融风控领域的应用
- 针对 AI 模型的后门攻击和防御技术

2019.04 – 2019.07 **后端研发.** 技术工程事业群, 腾讯科技（深圳）有限公司.
- 内部运维系统的前后端开发
- CDN 流量统计和预测算法

2018 – 2019 **信息学竞赛老师.** 武汉深学网络技术有限公司.
- 中学生信息学竞赛（NOIP、CCF CSP）辅导
- 腾讯课堂视频课程录制（购课学生人数超 500 人）

## 科研成果 主要方向: 数据挖掘, 联邦学习, AI 安全

### 会议论文

1. **Dazhong Rong**, S. Ye, R. Zhao, H. N. Yuen, J. Chen, and Q. He, “Fedrecattack: Model poisoning attack to federated recommendation,” in *38th IEEE International Conference on Data Engineering, ICDE 2022, Kuala Lumpur, Malaysia, May 9-12, 2022*, IEEE, 2022, pp. 2643–2655. DOI: 10.1109/ICDE53745.2022.00243.

2. **Dazhong Rong**, Q. He, and J. Chen, “Poisoning deep learning based recommender model in federated learning scenarios,” in *Proceedings of the Thirty-First International Joint Conference on Artificial Intelligence, IJCAI 2022, Vienna, Austria, 23-29 July 2022*, L. D. Raedt, Ed., ijcai.org, 2022, pp. 2204–2210. DOI: 10.24963/IJCAI.2022/306.

3. H. Hu, **Dazhong Rong**, J. Chen, Q. He, and Z. Liu, “Cometa: Enhancing meta embeddings with collaborative information in cold-start problem of recommendation,” in ***(best paper candidate)*** *Knowledge Science, Engineering and Management - 16th International Conference, KSEM 2023, Guangzhou, China, August 16-18, 2023, Proceedings, Part III*, Z. Jin, Y. Jiang, R. A. Buchmann, Y. Bi, A. Ghiran, and W. Ma, Eds., ser. Lecture Notes in Computer Science, vol. 14119, Springer, 2023, pp. 213–225. DOI: 10.1007/978-3-031-40289-0_17.

4. J. Zhang, H. Li, **Dazhong Rong**, Y. Zhao, K. Chen, and L. Shou, "Preventing the popular item embedding based attack in federated recommendations," in *40th IEEE International Conference on Data Engineering, ICDE 2024, Utrecht, The Netherlands, May 13-16, 2024*, IEEE, 2024, pp. 2179–2191. 🔗 DOI: 10.1109/ICDE60146.2024.00173.
5. **Dazhong Rong**, G. Yu, S. Shen, *et al.*, "Clean-image backdoor attacks," in *Artificial Neural Networks and Machine Learning - ICANN 2024 - 33rd International Conference on Artificial Neural Networks, Lugano, Switzerland, September 17-20, 2024, Proceedings, Part X*, M. Wand, K. Malinovská, J. Schmidhuber, and I. V. Tetko, Eds., ser. Lecture Notes in Computer Science, vol. 15025, Springer, 2024, pp. 187–202. 🔗 DOI: 10.1007/978-3-031-72359-9_14.
6. J. Wei*, **Dazhong Rong* (co-first)**, X. Zhu, Q. He, and Y. Wang, "Speed-enhanced subdomain alignment for long-term stable neural decoding in brain-computer interfaces," in *IEEE International Conference on Bioinformatics and Biomedicine, BIBM 2024, Lisbon, Portugal, December 3-6, 2024*, IEEE, 2024. 🔗 URL: https://arxiv.org/pdf/2407.17758.

### 发明专利

1. 陈建海，**荣大中**，沈睿，何钦铭, "基于带权贝叶斯个性化排序的强时序性项目推荐方法及系统," CN202011072547.4, 授权日期: 2022-05-03.
2. 陈建海，杨楠，沈睿，何钦铭，**荣大中**, "一种基于题意文本的同知识点试题分组系统和方法," CN202011083837.9, 授权日期: 2022-05-03.
3. 陈建海，周骏丰，沈睿，**荣大中**，何钦铭, "一种融合局部协同与特征交叉的推荐方法及系统," CN202110097853.1, 授权日期: 2022-07-15.

## 科研项目

| | |
|---|---|
| 国家重点研发计划 | 区块链生态安全监管关键技术研究 (2021YFB2700500). |
| 教育部高校体系建设研究 | 基于评测大数据的程序设计能力画像和智能导练推荐 |

## 其他经历

### 竞赛获奖

| | |
|---|---|
| 2017 | **银奖**, CCPC 第三届中国大学生程序设计竞赛. |
| | **银奖**, ACM-ICPC 国际大学生程序设计竞赛亚洲区域赛. |
| | **铜奖**, ACM-ICPC EC-Final 东亚洲大陆总决赛. |
| 2018 | **二等奖**, 第十一届全国大学生信息安全竞赛. |

### 奖学金

| | |
|---|---|
| 2022 | **华为基础研究奖学金**. |