段文星

男 24岁 全国 +86 17771122565 0x.WenxingDuan@gmail.com

教育背景

2023.09-2024.08 **The University of Edinburgh （硕士）** **网络安全，隐私与信任**

2019.09-2023.07 **The University of Edinburgh （本科）** **计算机科学**

成绩排名: 前30%

GPA: 4.0

实习经历

2023.06-2023.08 **基础计算机科学实验室（爱丁堡大学）** **初级研究助理**

公司行业: 教育/培训

- 在 Raul Garcia-Patron Sanchez 教授的指导下，以我之前的毕业论文为基础，进行了全面的量子计算分析。 这项工作旨在提供对源自Google的53位悬铃木量子计算机的实验数据的更深入见解。
- 在我之前的研究之上识别出了傅里叶权重输出中的的显着模式和异常，突出了大型量子位分析中的潜在差异，并为进一步研究指明了方向。
- 我随后的研究以这些异常为中心，旨在理解和阐明其根本原因及其影响。 这项研究工作包括严格的数据分析，得出对量子计算研究至关重要的富有洞察力的观察结果。
- 除了解决先前的发现之外，我还尝试从我的论文中改进分析方法。 特别关注的是建立量子系统动力学和特定参数之间的关系，增强我的研究成果的深度和适用性。

2022.06-2022.09 **Nethermind** **密码学 & 区块链研究实习生**

公司行业: 互联网/游戏/软件

- 参与了 Lido 项目下一阶段的协议研究：
- 研究并分析了当前主流的预言机协议，包括 DECO、Town Crier、Chainlink、Provable 等。
- 参与了去中心化身份（Decentralized Identity）的研究，并学习分析了链上身份的其他可行解决方案，包括 CanDID、灵魂绑定代币（soulbound token）、可验证凭证等。
- 学习了零知识证明相关知识，并参与了为 Lido 下一阶段制定无需信任验证框架方案的工作。
- 编写了一个智能合约，使用 Provable 预言机来衡量 ETH2.0 验证者的性能。
- 提高了对 Solidity 的熟练度；掌握了业界最先进的无需信任的预言机模型，加深了对零知识证明的理解，并了解了去中心化身份领域的最新动态。

2021.07-2021.09 **华中科技大学** **暑期研究实习生**

公司行业: 教育/培训

- 作为华中科技大学团队的一员参加了“中国软件杯”比赛
- 协调了4人团队完成了“危险农业害虫识别系统”的项目，该项目获得了全国二等奖
- 与副教授唐赫一起研究和探索细粒度识别的前沿研究学术文献
- 基于细粒度识别开发了一套有害农业害虫识别系统
- 负责后端开发和机器视觉开发
- 掌握了后端开发知识，提高了对 SQLite 数据库的了解，掌握了机器视觉的原理和应用
- 使用了 Python、TensorFlow、PyTorch、循环注意力卷积神经网络、SQLite 技术

2020.05-2020.08 **上海卓繁科技有限公司** **技术开发实习生**

公司行业: 互联网/游戏/软件

- 参与了襄阳市政务服务网的后端服务和系统维护工作
- 协助高级工程师开发和维护“湖北政务审批平台”项目
- 协助测试了包括自动查询网页生成、数据传输在内的多项新功能
- 通过使用 Python 脚本帮助高级工程师处理、分析和清理平台数据
- 参与了襄阳政府移动人员管理应用“鄂汇办”的数据库测试
- 加深了对常规软件厂商的生产和测试流程的理解，并掌握了多个网站后台的操作原理

学术经历

2024.05-2024.08

DECO预言机的分析和扩展 **承担人**

这是一个硕士毕业设计项目，由本人自己提案，在Markulf Kohlweiss教授指导下完成。该论文重点研究了一种基于密码学，TLS协议和零知识证明的区块链预言机协议——Decentralized Oracles（DECO）。项目详细分析了DECO的运行机制，指出了其不足之处和潜在的隐私风险。针对这些隐私问题，在不修改服务器端的TLS协议的情况下，本文基于对DECO，AES，HMAC，默克尔树和TLS的深度理解，对DECO进行了协议层面的修改，结合零知识证明技术，实现了更高程度的隐私性能。项目阐述了这些方法的运行原理和流程。对每种方法的优缺点进行了广泛的比较和分析，并通过代码验证证明了它们的有效性。此外，本文还正式定义了增强协议的安全属性，并对其隐私性进行了密码学安全性证明。

2022.09-2023.05

量子霸权假设的验证与测试 **承担人**

这是一个本科毕业论文项目，并被评为当年的Outstanding undergraduate projects。在我的论文中，我主要集中于分析谷歌的量子随机电路采样实验，目的是评估他们关于量子霸权的声明。我采用傅里叶分析方法来研究实验结果与量子比特数之间的关系，从而全面评估谷歌量子霸权声明的力度。在研究过程中，我遇到了一个有趣的现象。与预期相反，我的实验结果显示，谷歌的实验表现出的相关器值高于理论上无噪声理想电路的值。这一差异促使我进行了广泛的数据分析，以确定背后的原因，最终归因于样本数量不足。此外，发现系统中的噪声水平显著影响了不同样本大小的结果。因此，确定获得接近真实值的相关器所需的最佳样本大小，已成为一个值得进一步研究的重要研究问题。

2022.09-2022.12

基于IMU传感器和机器学习的物联网应用开发 **AI工程师，后端工程师**

在这个项目中，我负责设计和实现了一个基于穿戴式传感器的实时人体活动分类系统。我的主要工作包括人工智能算法的设计、后端的搭建以及模型的训练。通过利用惯性运动单元（IMU）传感器收集的数据，我们实现了对用户的活动进行分类，并将这些信息实时传输到安卓应用程序中。在项目过程中，我深入研究了时间序列传感器数据的预处理、特征提取和分类方法，并探索了这些方法在处理嘈杂传感器数据时的有效性。此外，我还体验了使用各种工具，如IoT开发板编译器、系统级模拟器和安卓移动应用开发环境。通过与另两位具有互补技能的队友合作，我们共同管理项目、并通过口头和书面报告展示我们的成果。这个项目不仅让我获得了从设计到实施一个典型的物联网系统的端到端经验，还增强了我在嵌入式编程、传感器数据分析和机器学习方法应用方面的技能，并在课程最后评分中获得A。

2022.06-2022.09

Lido 2.0项目提案 **密码学 & 区块链研究助理**

参与了大型研究项目Lido 2.0的协议提案。Lido 2.0是以太坊上的一个去中心化的质押解决方案，允许用户在多个区块链上质押其加密货币资产以赚取质押奖励，同时保持资产的流动性。Lido 2.0旨在进一步提升质押过程的去中心化和去信任化。我负责Lido 2.0的预言机部分的研究，撰写研究综述，比对当前市面上存在的预言机系统，分析其协议过程与信任基础。在此基础上，我深入研究并分析了当前主流的预言机协议，如DECO、Town Crier、Chainlink、Provable等，以及参与了去中心化身份（Decentralized Identity）的研究，并探讨了链上身份的其他可行解决方案，包括CanDID、灵魂绑定代币（soulbound token）、可验证凭证等。此外，我还学习了零知识证明的相关知识，并参与了为Lido 2.0下一阶段制定无需信任验证框架方案的工作，旨在通过技术创新进一步增强系统的安全性和去中心化程度，推动加密货币质押领域的发展。

2021.07-2021.09

“中国软件杯”竞赛项目“有害农业昆虫识别系统” **后端开发&机器视觉开发**

作为华中科技大学团队的一员，参加了“中国软件杯”并在项目“危险农业害虫识别系统”中担任4人团队的协调者，该项目荣获全国二等奖。在唐赫副教授的指导下，研究和探索了细粒度识别的前沿学术文献，并基于细粒度识别技术开发了一套有害农业害虫识别系统。我负责了后端开发和机器视觉开发工作，掌握了后端开发知识，提高了对SQLite数据库的理解，并深入了解了机器视觉的原理及其应用。在项目中，我使用了Python、TensorFlow、PyTorch、循环注意力卷积神经网络、SQLite等技术，表现出了杰出的技术能力和团队协作精神。

获奖经历

2023.07 **卓越毕业设计项目**

2021.09 **中国软件杯二等奖**

2019.03 **滑铁卢大学欧几里得数学竞赛top5%**

2019.03 **加拿大编程竞赛top5%**

2018.11 **澳大利亚数学竞赛一等奖**

技能/语言

Python：
熟练

Java :
熟练

C :
熟练

Haskell :
熟练

Solidity :
熟练

Cairo :
熟练

兴趣/特长

密码学 区块链 零知识证明 以太坊 EVM 量子计算