汪楷星

主页: https://wangkaixing.github.io
Github: https://github.com/Wangkaixing

邮箱: ucaswkx@gmail.com
电话: +86-151-6677-2838

教育背景

- **中国科学院大学** 北京
  电子信息，工程硕士; *GPA: 3.86, 均分: 88.69(排名:2/17)* *2022.9 - 至今*
  课程：密码分析学 *(93)*、数据科学导论 *(96)*、公钥密码学 *(96)*、计算复杂性理论 *(91)*、格密码学、应用密码学、计算机网络与系统安全等

- **厦门大学** 厦门
  计算机科学与技术，工学学士; *GPA: 3.39, 均分* *2018.9 - 2022.6*
  课程：操作系统、算法分析、计算机网络、模式识别、计算机组成原理、概率论与数理统计、微积分、离散数学、金融学等

论文

- Binwu Xiang, Jiang Zhang, **Kaixing Wang**, Yi Deng, Dengguo Feng, "NTRU-based Bootstrapping for MK-FHEs without using Overstretched Parameters." **Asiacrypt 2024**.
- **Kaixing Wang**, Binwu Xiang, Jiang Zhang, "Improved FHE Bootstrapping and Its Applications in Privacy Preserving Inference of Discretized Neural Networks." (CHES 在投)

项目背景

- **密码科学技术全国重点实验室 (SKLC)** 北京
  访问学生 *2023.7 - 至今*
  - **同态加密理论与实现研究**: 参与国家级重点实验室的加密算法研究，专注于高效同态加密算法的开发与实现，目标是提升现有算法的性能和适用性。期间作为第一作者撰写了一篇论文在投（CCF B），另一篇合著论文已被 2024 年亚密接收，完成多个同态加密算法复现。
    - 基于 C++ 语言使用 OpenFHE 开源库开发并优化同态加密算法，提出了一种基于 NTRU 假设的新型自举算法，显著减少了密钥大小并加速了自举过程。
    - 设计并实现了改进的盲旋转算法，优化后的算法密钥切换大小从 $\tilde{O}(n^2)$ 降至 $\tilde{O}(n)$，提升了算法的整体效率。
    - 基于 MNIST 数据集和简单的逻辑回归模型，实施实验验证，评估算法在隐私保护的离散神经网络推理中的性能。
    - 成果超越了 2023 年密码学顶会 Xiang 等人提出的最先进方法，在 128 位安全性下仅需 9 毫秒完成自举，密钥大小减少 30 倍，自举速度提高 1.5 倍，显著提升了同态加密算法在实际应用中的可行性与效率。

- **空间感知与计算实验室 (ASC)** 厦门
  毕业设计 *2021.11 - 2022.7*
  - **基于城市空间大数据的医疗需求研究**: 开发并实现了一个系统，基于厦门核酸检测点的数据，致力于构建一个能够合理预测检测点未来医疗需求的系统，以优化公共卫生资源分配。
    - 使用 Python 研究并比较了不同的统计模型 (ARIMA、HMM) 和机器学习、深度学习模型 (GBRT、DeepST、DCRNN)，结合时间和空间维度，采用多步预测策略，精确预测医疗需求。
    - 实现了对核酸检测点未来几个小时拥挤程度的连续预测，有效辅助资源调配。
    - 使用 Apache ECharts 框架，通过网页展示每个检测点的拥堵情况、地理位置等基本信息，方便决策和管理。

荣誉和奖励

- **荣誉**
  - 中国科学院大学“三好学生”荣誉称号，2022-2023
  - 中国科学院大学正元密码学优秀学生奖三等奖，2023
- **奖学金**
  - 厦门大学本科生优秀学生奖学金二等奖，2020-2021
  - 厦门大学本科生优秀学生奖学金二等奖，2019-2020
- **竞赛**
  - 山东省高中数学竞赛一等奖，2017
  - 全国中学生英语能力竞赛全国一等奖，2017

专利

- 2024 年 7 月，“同态解密方法、非易失性存储介质以及电子设备”发明专利，国内申请号：2024109626264，PCT 申请号：PCT/CN2024/106013，位次 1/4。
- 2023 年 11 月，“多密钥同态加密方法、计算方法、存储介质及计算机设备”发明专利，国内申请号：2023115251904，PCT 申请号：PCT/CN2023/131857，位次 3/5。
- 2021 年 3 月，“Android 恶意 APP 检测软件”计算机软件著作权证书，证书号：软著登字第 7168634 号，位次：2/6。

技术能力

- 熟悉 C/C++, Python, Sage, Matlab, LaTeX
- 熟悉 Linux 脚本
- 熟悉 git 版本控制，进行代码管理