黄军浩.个人简历

• (+86)18626423381 • *jhhuang_nuaa@126.com*
https://junhaohuang.github.io

教育背景

- **北师香港浸会大学　密码工程方向　香港浸会大学博士　2021 年 ~ 2025 年**
- **南京航空航天大学　网络空间安全　硕士　2018 年 ~ 2021 年**
- **南京航空航天大学　计算机科学与技术　学士　2014 年 ~ 2018 年**

访问经历

- **香港城市大学　指导老师：张泽松　2023 年 7 月 ~ 2023 年 12 月**
- **武汉大学　指导老师：何德彪　2019 年 7 月 ~ 2019 年 12 月**

研究方向

- 密码工程，后量子密码算法，格基密码算法，模算术，隐私保护技术

项目经历

量子安全的格密码系统软硬件协同计算平台的研究，国家自然科学基金　2021 ~2023

主要参与人　负责 *Kyber* 和 *NTTRU* 格基密码算法在 *ARM Cortex-M4* 平台上的快速优化实现

- 创新性地提出了改进的 Plantard 模乘算法，使其具有比最优的 Montgomery 模乘更快、更优异的性质；
- 在 Cortex-M4 上利用改进的 Plantard 模乘算法替换 Montgomery 算法，加速 NTT/INTT 计算 16%~25%。
- 相关论文发表于密码工程顶会 IACR CHES 2022，代码合并到 pqm4。

格密码系统的高效及轻量级多平台实现研究，CCF-之江实验室联合创新基金　2023 ~2024

主要参与人　负责 *Keccak*、*Kyber* 和 *Dilithium* 在 *ARMv7-M* 和 *RISC-V* 等平台上的快速、轻量级优化实现

- 进一步扩展 Plantard 模乘算法的输入范围 2.14 倍，提出其在 32 位平台 M3 和 RISC-V 上的优化实现方案；
- 在 ARMv7-M 上进一步加速 Keccak、Dilithium，Kyber 和 Dilithium 的整体方案效率提升 13% 以上；
- 相关论文发表于安全顶刊 IEEE TIFS 2024 和密码工程顶会 IACR CHES 2024，代码合并到 pqm4。

抗量子格基隐私计算系统的异构多平台关键技术研究，广东省自然科学基金-面上项目　2024 ~2026

主要参与人　负责基于全同态加密的隐私计算系统研究

- 研究基于全同态加密在决策树推理上的隐私保护技术；
- 相关论文发表于 CCF-B 类会议 ACM SIGMETRICS 2025。

学术论文（累积合作发表 15 篇，代表作如下:）

- **Junhao Huang**, Alexandre Adomnicăi, Jipeng Zhang, Wangchen Dai, Yao Liu, Ray C. C. Cheung, Çetin Kaya Koç, Donglong Chen*. Revisiting Keccak and Dilithium Implementations on ARMv7-M. IACR CHES 2024. **CCF-B 会议 & 密码工程顶会**
- **Junhao Huang**, Haosong Zhao, Jipeng Zhang, Wangchen Dai, Lu Zhou, Çetin Kaya Koç, Ray C.C. Cheung, Donglong Chen*. Yet another Improvement of Plantard Arithmetic for Faster Kyber on Low-end 32-bit IoT Devices. IEEE TIFS 2024. **CCF-A 期刊 & 安全顶刊 & & SCI 一区**
- **Junhao Huang**, Jipeng Zhang, Haosong Zhao, Zhe Liu, Ray C. C. Cheung, Çetin Kaya Koç, Donglong Chen*. Improved Plantard Arithmetic for Lattice-based Cryptography. IACR CHES 2022. **CCF-B 会议 & 密码工程顶会**
- **Junhao Huang**, Zhe Liu*, Zhi Hu, Johann Großschädl. Parallel Implementation of SM2 Elliptic Curve on Intel Processor with AVX2. ACISP 2018. **CCF-C 会议**
- Jipeng Zhang, **Junhao Huang**, Lirui Zhao, Donglong Chen, Çetin Kaya Koç*. ENG25519: Faster TLS 1.3 handshake using optimized X25519 and Ed25519. Usenix Security 2024. **安全四大顶会 & 杰出论文奖**
- Jipeng Zhang, Yuxing Yan, **Junhao Huang**, Çetin Kaya Koç*. Optimized Software Implementation of Keccak, Kyber, and Dilithium on RV{32,64}IM{B}{V}. IACR CHES 2025. **CCF-B 会议 & 密码工程顶会**
- Haosong Zhao, **Junhao Huang**, Zihang Chen, Kunxiong Zhu, Donglong Chen, Zhuoran Ji, Hongyuan Liu*, VESTA: A Secure and Efficient FHE-based Three-Party Vectorized Evaluation System for Tree Aggregation Models[C]. *ACM SIGMETRICS, 2025* **CCF-B 会议**
- Zewen Ye, **Junhao Huang**, Tianshun Huang, Yudan Bai, Jinze Li, Hao Zhang, Guangyan Li, Donglong Chen, Ray CC Cheung, Kejie Huang*, PQNTRU: Acceleration of NTRU-based Schemes via Customized Post-Quantum Processor[J]. *IEEE Transactions on Computers, 2025* **CCF-A 期刊 & SCI 二区**
- Jipeng Zhang, **Junhao Huang**, Zhe Liu*, Sujoy Sinha Roy. Time-memory Trade-offs for Saber on Memory-constrained RISC-V. IEEE TC 2022. **CCF-A 期刊 & SCI 二区**

- Xinyi Ji, Jiankuo Dong, **Junhao Huang**, Zhijian Yuan, Wangchen Dai, Fu Xiao, Jingqiang Lin. ECO-CRYSTALS: Efficient Cryptography CRYSTALS on Standard RISC-V ISA. IEEE TC 2024. **CCF-A 期刊 & SCI 二区**

荣誉奖项

- 2024 年广东省计算机学会优秀论文奖 **一等奖** **2024 年 12 月**
- Usenix Security 2024 **杰出论文奖** **2024 年 8 月**
- 2023 年广东网络空间安全优秀论文奖 **三等奖** **2023 年 5 月**

学术推荐人

- 陈东龙（副教授，副系主任，导师），北师香港浸会大学，donglongchen@uic.edu.cn
- 张泽松（教授，副校长，访问学者导师），香港城市大学，r.cheung@cityu.edu.hk
- Çetin Kaya Koç（教授，IEEE Life Fellow，CHES 发起人之一），加州大学圣巴巴拉分校，cetinkoc@ucsb.edu