

黄军浩. 个人简历

广东·珠海·☎(+86)18626423381 · ✉jhhuang_nuaa@126.com
🌐https://junhaohuang.github.io



🎓 教育背景

· 香港浸会大学	密码工程方向	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

🔍 项目经历

- 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 年 ~ 2024 年**
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;
 - 相关论文发表于密码顶会 IEEE TIFS 2024 和 IACR CHES 2024 上, 代码合并到 pqm4。
- 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 年 ~ 2023 年**
主要参与人 负责 Kyber 和 NTRU 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顶会 IACR CHES 2022 上, 代码合并到 pqm4。

📄 学术论文 (累积合作发表 13 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
- 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, 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
- 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 & 密码顶会
- 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

· Usenix Security 2024	杰出论文奖	2024 年 8 月
· 广东网络空间安全优秀论文奖	三等奖	2023 年 5 月
· 研究生学业奖学金	一等奖	2018 年 10 月

🛠 专业技能

- 编程语言: C/C++, x86-64, ARMv7-M 汇编, RISC-V 汇编, Intel AVX2 汇编, Python
- 英语能力: CET-4(597), CET-6(512), IELTS(7.0)

👥 学术推荐人

- 陈东龙副教授 (副主任, 导师), 北京师范大学-香港浸会大学联合国际学院, 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