

尊敬的导师：

您好！我想申请读博，申请主要方向：轻量级密码算法设计与分析、密码侧信道攻击与防御、密码工程和物联网安全等，以下是个人信息与科研情况，迫切想通过读博进一步提升自己，希望老师给予机会，非常感谢您！

个人信息

姓名：向嘉豪 性别：男 出生年份：2000.11
邮箱：jiahaoxiang2000@gmail.com 手机：(+86)13087286239
主页：<https://github.com/jiahaoxiang2000>

教育经历

衡阳师范学院 | 电子信息，计算机学院 | 硕士研究生 | 师从李浪教授 2023.09—至今
长沙学院 | 机械设计制造及其自动化，机电工程学院 | 工学学士 2017.09—2021.06

技术能力

- 语言：常用 C, Python, LaTeX；熟悉 Verilog, Assembly, Rust；了解 C++, Java, TypeScript。
- 工作流：Linux, Shell, Vim, VsCode, Git, GitHub。

论文发表¹

Efficient implementations of CRAFT cipher for Internet of Things | *Computers and Electrical Engineering*, 2024

- 该论文为 CRAFT 对称加密算法，提供高性能、高性价比和低成本硬件实现方案。

Low-Latency Implementation of Bitsliced SPN-Cipher on IoT Processors | *IEEE Transactions on Computers* (一审中, CCF-A), 2025

- 该论文为 SPN 类结构对称加密算法，提供精简指令集上低延迟软件实现方案。

Thread-Adaptive: Optimized Parallel Architectures of SLH-DSA on GPUs | *IEEE Transactions on Circuits and Systems II: Express Briefs* (已完初稿, 拟投), 2025

- 该论文为 SLH-DSA 后量子数字签名算法，提供高吞吐量异构实现方案。

项目经历

主持湖南省研究生科研创新项目“轻量级分组密码的软硬件优化研究与实现” | 项目编号：CX20240977
2024—至今

¹ 本人一作，修改：2025 年 4 月 18 日