尊敬的博士生导师：

您好！我申请审核制攻读博士学位，申请主要研究方向：密码算法软硬件优化实现、密码算法侧信道攻击与防御、轻量级密码算法设计与分析等。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，望老师给予机会，非常感谢！

个人信息

|  |
| --- |
| /Users/xiangjiahao/Desktop/image.jpgimage◆ 姓 名： 向嘉豪  ◆ 出生年月： 2000.11  ◆ 手 机： 13087286239  ◆ 邮 箱： simple.xjh@qq.com  ◆ 专 业： 电子信息  教育背景**:**  ◆ 2017年 9月- 2021年 6月，长沙学院，本科，机械设计制造及其自动化。  ◆ 2023年 9月-至今，衡阳师范学院，硕士，电子信息，导师：李浪教授，进行密码算法软硬件优化实现等研究。 |
| 科研成果**:** |

1.论文

◆ **Jiahao Xiang**, Lang Li\*. Efficient implementations of CRAFT cipher for Internet of Things[J]. *Computers and Electrical Engineering*, 2024, 116: 109168. (中科院 3 区, IF=4.0).

◆ **Jiahao Xiang**, Lang Li\*. Low-Latency Implementation of Bitsliced SPN-Cipher on IoT Processors. (*IEEE Transactions on Computers*, CCF-A, 一审).

◆ **Jiahao Xiang**, Lang Li\*. Thread-Adaptive: Optimized Parallel Architectures of SLH-DSA on GPUs. (拟投 *IEEE Transactions on Circuits and Systems II: Express Briefs*, 已完初稿).

◆ Lianrui Deng, Liang Li\*, Yu Ou, **Jiahao Xiang**. Tripm: a multi-label deep learning SCA model for multi-byte attacks[J]. *International Journal of Machine Learning and Cybernetics*, 2025: 1-16.

◆ Xingqi Yue, Liang Li\*, Quiping Li, **Jiahao Xiang**, Zhiwen Hu. QLW: a lightweight block cipher with high diffusion[J]. *The Journal of Supercomputing*, 2025, 81(1): 224.

主持项目情况

◆ 轻量级分组密码的软硬件优化研究与实现，2024年湖省省研究生科研创新项目(No. CX20240977).