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：轻量级密码算法设计与分析、密码算法软硬件优化实现、密码算法侧信道攻击与防御等。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

◆ 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 (计算机技术)

教育背景

◆ 2017年9月-2021年6月，长沙学院，本科。

◆ 2023年9月-至今，衡阳师范学院，硕士，电子信息，导师：李浪教授，进行密码算法设计与优化实现。

科研成果

1.论文

(1) **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)

(2) **Jiahao Xiang**, Lang Li*. Thread-Adaptive: Optimized Parallel Architectures of SLH-DSA on GPUs[J]. *IEEE Computer Architecture Letters,2025-10*.https://doi.org/10.1109/LCA.2025.3622588.

(3) **Jiahao Xiang**, Lang Li*. Low-Latency Implementation of Bitsliced SPN-Cipher on IoT Processors. (*IEEE Transactions on Computers*, CCF-A, 二审小修已返稿)

(4) Lianrui Deng, Lang Li*, **Jiahao Xiang**. KD-SCA: Improving Lightweight CNN Model Profiling Side-Channel Analysis with Knowledge Distillation[J]. *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems,2025-10*.https://doi.org/10.1109/TCAD.2025.3626459. (CCF-A)

(5) Lianrui Deng, Lang 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.

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

(7) Shencheng Xia, Lang Li*, Yu Ou, **Jiahao Xiang**. Optimizing label correlation in deep learning-based side-channel analysis[J]. *Microelectronics Journal*, 2025: 106721.

获奖情况

◆ 2025年第十六届“挑战杯”湖南省课外学术科技作品竞赛二等奖.

◆ 2024年湖南省大学生创新大赛高教主赛道研究生创意组三等奖.

◆ 2024年湖南省第十七届研究生创新论坛优秀论文二等奖.

◆ 2023年衡阳师范学院“挑战杯”课外学术科技作品竞赛特等奖.

◆ 2023年度硕士研究生奖学金二等奖.

◆ 2023-2024年度硕士研究生奖学金二等奖.

主持项目

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