



个人信息

姓名: 黄亦成 性别: 男 邮箱: huangyicheng@buaa.edu.cn
出生年月: 2001/02 学历: 硕士 电话: 18224036908



教育背景

北京航空航天大学(985)—集成电路科学与工程学院—硕士 2023年9月–2026年1月

- 主修专业: 集成电路科学与工程 | 数字集成电路设计(导师: 王雪岩 副教授)
- 研究方向: 基于FPGA的密码学加速器设计, 软硬件协同优化, 数字IC设计
- 主要荣誉: 全国大学生集成电路创新创业大赛全国二等奖(2023); 学业奖学金一等奖学金(2024)

西南交通大学(211)—信息科学与技术学院—学士 2019年9月–2023年6月

- 主修专业: 电子科学与技术 | 3.68/4.00 (前5%, 保研综合成绩专业第一)
- 主修课程: 数字逻辑与计算机组成原理、数字集成电路分析与设计基础、电子设计自动化(EDA)、SoC设计方法、模拟集成电路分析与设计基础、集成电路工艺、微波集成电路、数字信号处理A等
- 主要荣誉: 全国大学生集成电路创新创业大赛·平头哥杯赛道第一名(2021)、全国大学生嵌入式芯片与系统设计竞赛(芯片设计赛道)·本科生组第一名(2021)、全国大学生电子设计大赛·国家级二等奖(2021)

研究项目

面积优先的模乘设计 (CCF-蚂蚁科研基金-预计顺利结题)

2024年2月–至今

- 提出针对经典蒙哥马利模乘算法中截断乘法的误差修正方法, 并支持结合Karatsuba算法进行联合优化
- 面向模乘应用, 提出基于贪婪算法的Karatsuba分解的优化搜索算法, 支持在给定约束下实现设计空间探索
- 投稿第一作者期刊论文: “KD-Finder: A Karatsuba Decomposition Optimization Finder for NTT-Friendly Montgomery Modular Multiplication”, under reviewed by *IEEE Trans. Comput. Aided Des. Integr. Circuits Syst*(TCAD)(CCF-A类期刊)

全同态加密处理器 (北航-北京微芯区块链与边缘计算研究院)

2023年4月–2024年4月

- 负责全流水可变点数转置单元设计以及NTT IP在Vitis环境的集成与开发,并在DATE 2024进行海报展示
- 合作(第三作者)会议论文: “ESC-NTT: An elastic, seamless and compact architecture for multi-parameter ntt acceleration”, in *Design, Automation & Test in Europe Conference & Exhibition (DATE)*, 2024. (CCF-B类会议)

国密算法硬件加速IP设计 (北航-北京微芯区块链与边缘计算研究院)

2022年10月–2023年12月

- 设计ECC算法硬件IP,支持SM2、Secp256r1/k1曲线、FPGA平台下实现点乘(1.2万次/秒)/双点乘(9千次/秒)
- 面向V2V (Vehicle to Vehicle) 场景, 提出了一种针对椭圆曲线密码算法的专用指令集加速器架构
- 发表第一作者会议论文: “LLP-ECCA: A Low-Latency and Programmable Framework for Elliptic Curve Cryptography Accelerators”, in *International Test Conference in Asia (ITC-Asia)*, 2024. (CCF-C类会议, 最佳论文提名)

竞赛经历

全国大学生集成电路创新创业大赛(平头哥杯)-国家级二等奖

2023年3月–2023年8月

- 项目简介: 基于无剑100开源SoC平台构建双核TEE(Trusted Execution Environment)安全系统
- 主要工作: 搭建双核SoC并在FPGA上部署、实现MailBox、IOPMP、硬件密码加速IP, 支持安全启动机制

全国大学生嵌入式芯片与系统设计竞赛(芯片设计赛道)-国家级一等奖·本科生组唯一 2021年8月–2021年11月

- 项目简介: 实现神经网络硬件加速器并挂载在RISC-V SoC,以加速海洋生物声学分类, 并进行ASIC设计流程
- 主要工作: 设计FFT IP、在FPGA上部署SoC、实现RISC-V自定义指令并编写IP驱动、Spyglass语法检查

全国大学生集成电路创新创业大赛(平头哥杯)-国家级一等奖·赛道第一名

2021年3月–2021年8月

- 项目简介: 设计基于神经网络的SAR图像压缩加速器并挂载在开源wujian 100 SoC平台中完成加速任务
- 负责嵌入式开发: 完成wujian 100 SoC在FPGA上的部署, 为加速器IP编写C语言驱动, 搭建实物展示系统

技能特长

- 编程语言: Python, Verilog, C
- 工具软件: Altium Designer、Modelsim、VCS、Design compiler、formality、Vivado等