基于RISC-V架构的轻量级嵌入式安全保护系统

报告人：常伯符

指导老师：熊昊

哈爾濱工業大學(深圳)

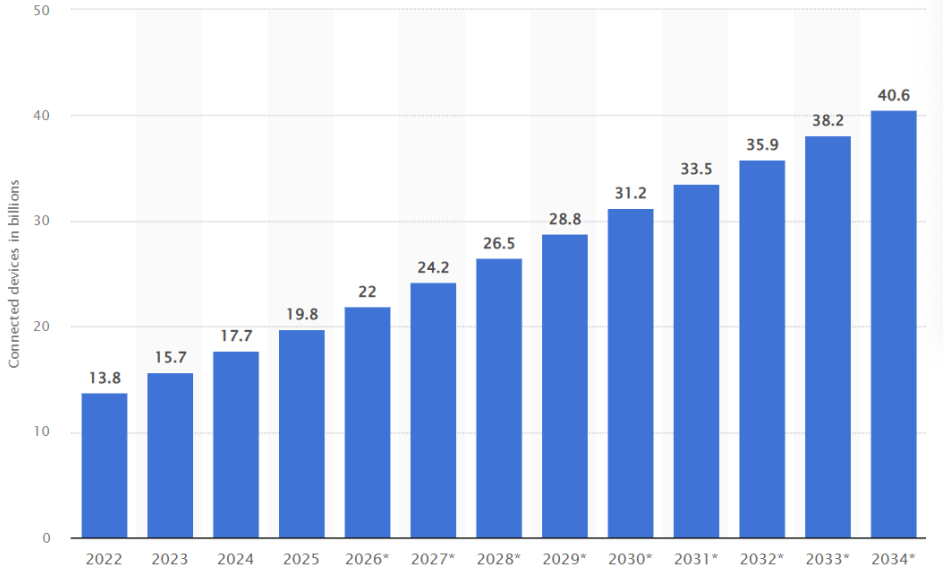
HARBIN INSTITUTE OF TECHNOLOGY, SHENZHEN

目录

课题背景及研究的目的和意义

课题背景

- 物联网时代
  - 超过198亿台IoT设备入网
  - 大量资源受限设备暴露在复杂环境中
- RISC-V
  - 开源性、模块化、轻量级、免版税
  - 多种安全特性
- 面临挑战
  - PMP配置错误
  - 固件篡改
  - 侧信道攻击
  - 中低端MCU实证研究匮乏



哈爾濱工業大學(深圳)
HARBIN INSTITUTE OF TECHNOLOGY, SHENZHEN

研究的目的与意义

研究动机

- 研究重点在高性能处理器，适于IoT设备的中低端MCU平台的研究较少
- 安全与性能的平衡问题：软件实现与硬件优化
- 新型威胁：侧信道、量子电脑等

研究意义

- 填补中低端MCU安防研究的空白
- 促进自主可控物联网安全生态发展
- 理论-实践闭环，提升个人能力

研究现状及分析

研究现状及分析

RISC-V安全特性

- 特权体系结构与隔离机制
- PMP（物理内存保护）

密码学算法与硬件加密

- AES
- Crypto扩展
- Ascon

侧信道攻击与防护技术

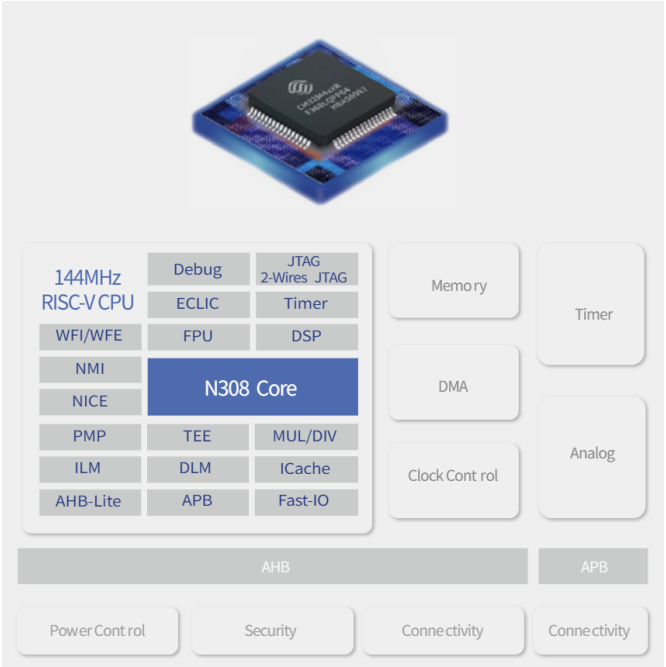
- RISC-V助力现代处理器侧信道防护的研究
- 掩码技术破坏统计学特征
- 通用的常规侧信道漏洞检测方案

后量子密码学

- 传统公钥密码学的弱点
- SLH-DSA（无状态散列数字签名算法）

主要研究内容及研究方案

开发板选择



最终选择：中移CM32M433R-START开发板

- 采用芯来科技Nuclei N308内核
  - 144MHz
  - RISC-V架构
  - 支持M/U特权模式、PMP
- 内置密码算法硬件加速引擎（SAC）
  - 支持AES、SHA、MD5、SM4等算法
- 内置真随机数发生器（TRNG）
- 开源的技术文档、工具链、示例项目代码

哈爾濱工業大學(深圳)
HARBIN INSTITUTE OF TECHNOLOGY, SHENZHEN

研究内容与研究方案

对称加密算法研究与技术对比

- 基于SAC实现硬件AES-128
- 基于tiny-AES-c库实现软件AES-128
- 基于ascon-c库和DMA优化实现Ascon-128a
- 量化对比三种实现的性能指标

后量子签名技术应用与固件完整性校验

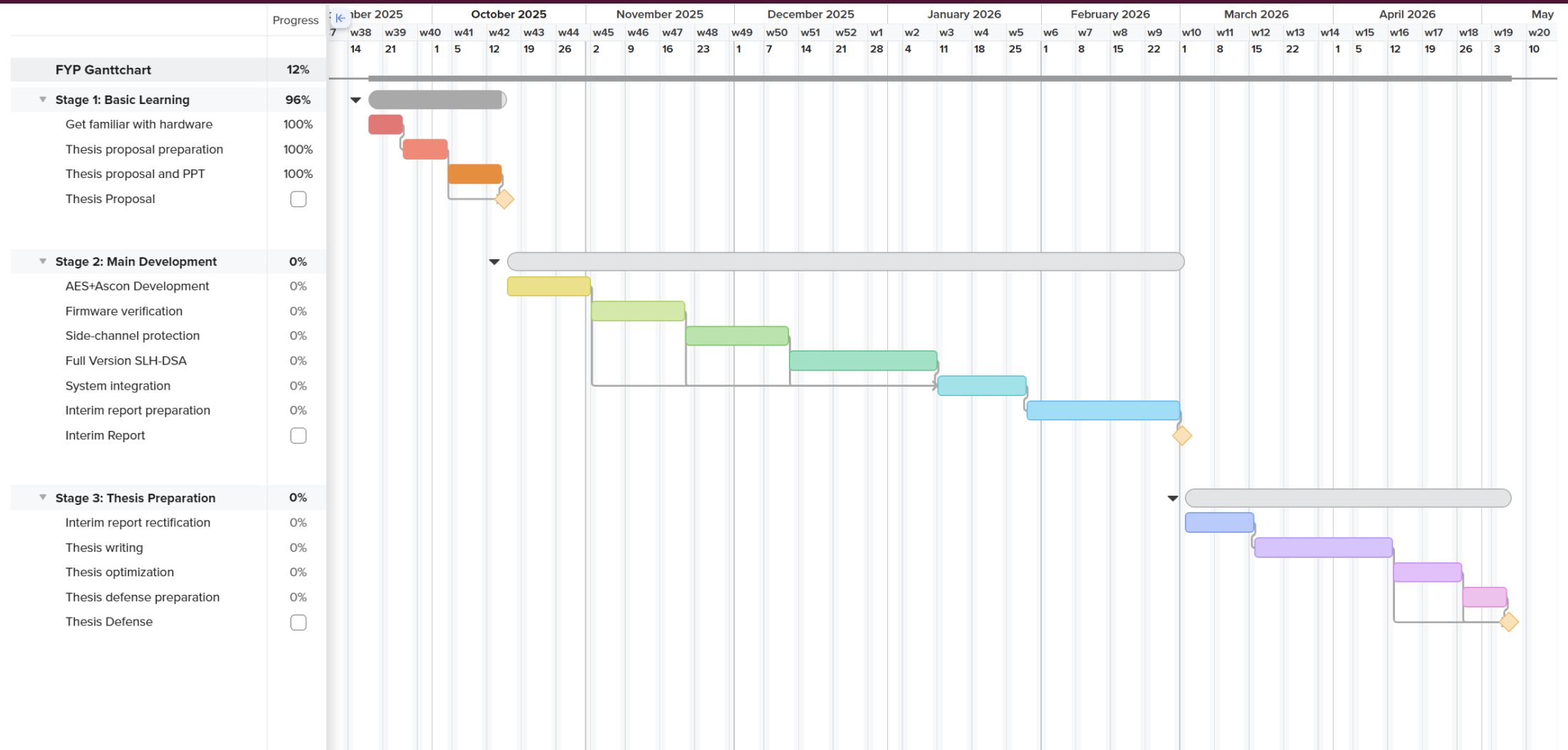
- 基于SLH-DSA的C语言开源库实现
- 利用SAC实现硬件哈希加速
- Bootloader：安全启动流程验证
- 引入SLH-DSA作为数字签名验证算法

侧信道防护优化

- 使能TRNG产生随机数
- 将掩码与AES明文、密钥、Ascon寄存器在传递前后异或
- 使用掩码盲化SLH-DSA的私钥种子
- 使用TVLA对功耗做测试验证防护成果

进度安排及预期目标

项目甘特图


Progress
October 2025
November 2025
December 2025
January 2026
February 2026
March 2026
April 2026
May
FYP Ganttchart 12%
Stage 1: Basic Learning 96%
Get familiar with hardware 100%
Thesis proposal preparation 100%
Thesis proposal and PPT 100%
Thesis Proposal
Stage 2: Main Development 0%
AES+Ascon Development 0%
Firmware verification 0%
Side-channel protection 0%
Full Version SLH-DSA 0%
System integration 0%
Interim report preparation 0%
Interim Report
Stage 3: Thesis Preparation 0%
Interim report rectification 0%
Thesis writing 0%
Thesis optimization 0%
Thesis defense preparation 0%
Thesis Defense

已具备和所需的条件和经费

已具备和所需的条件和经费

实验室条件和经费保障

- 设备：直流电源、数字万用表、数字示波器、焊台等
- 已具备的条件：CM32M433R开发板一块、杜邦线若干
- 香港城市大学青岛研究院承诺提供经费保障

所需条件和经费

- 目前暂无急需的条件或经费
- 可能需要：低阻分流电阻、差分电流探头、备用的CM32M433R开发板

预计困难及解决方案

哈爾濱工業大學(深圳)
HARBIN INSTITUTE OF TECHNOLOGY, SHENZHEN

预计困难及解决方案

- 官方文档缺失
  - 充分利用SDK文件
  - 替换官方设置
- SAC模块配置复杂
  - 分步调试
  - 监视寄存器状态
- 硬件资源受限
  - 充分利用DMA
  - 降低加密算法的性能
- 指标测定方法理想化
  - 先确保各模块功能正确
  - 条件不允许则转为定性分析
- SLH-DSA性能低
  - 优化哈希计算、DMA缓解CPU压力
  - 无法进一步优化则换为简单的SHA签名/认证
- 系统集成潜在困难
  - 严格对照寄存器地址
  - 无法解决则放弃集成，先确保子模块成功

感谢！

电话：+86 13976246251

邮箱：citcra@foxmail.com

哈爾濱工業大學(深圳)

HARBIN INSTITUTE OF TECHNOLOGY, SHENZHEN