香港城市大學
City University of Hong Kong

# Lightweight Embedded Security Protection System under RISC-V Architecture

FYP by Charlie (Bofu Chang)

Bofu Chang, an Automation student from Harbin Institute of Technology, Shenzhen.
Interested in software coding and hardware application.

# Pre-FYP Progress

- Learning basic knowledge of RISC-V

**特权级别（Privileged Level）**

RISC-V：M → S → U　ISCAS NIST

X86：实模式 → 保护模式 → 长模式

只访问实际物理地址　MMU负责虚拟地址到实际地址转换

- **RISC-V 的 Privileged Specification 定义了三个特权级别（privilege level）**
- **Machine 级别是最高的级别，所有的实现都需要支持。**
- **可选的 Debug 级别**

| Level | Encoding | Name | Abbreviation |
|---|---|---|---|
| 0 | 00 | User/Application | U 用户态 |
| 1 | 01 | Supervisor | S 内核态 |
| 2 | 10 | *Reserved* | |
| 3 | 11 | Machine | M |

【参考 2】Table 1.1: RISC-V privilege levels.

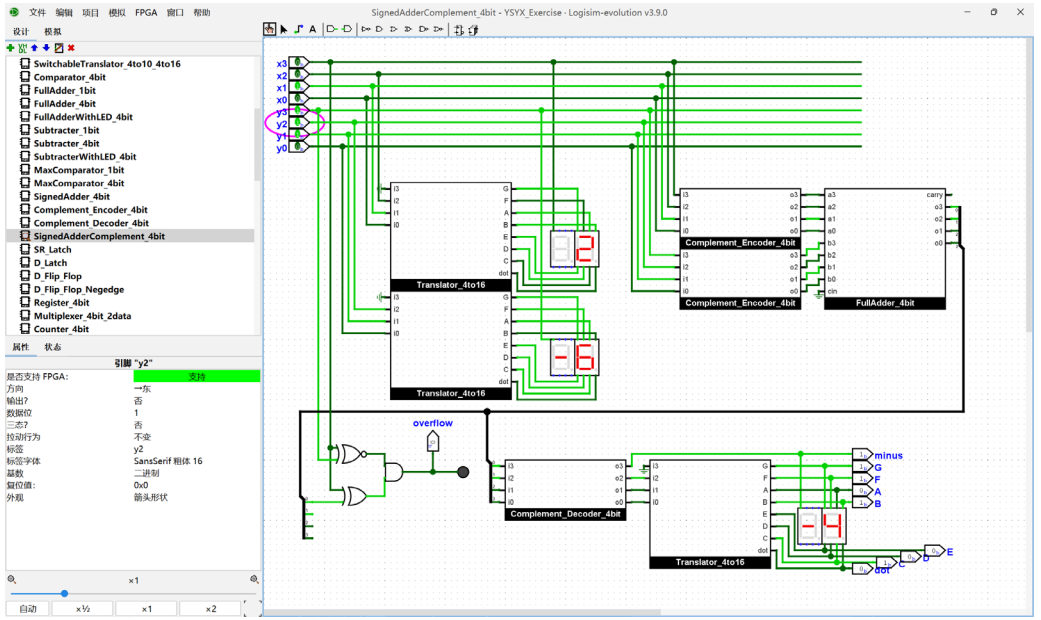
只有 Supervisor 有虚址虚存

| Number of levels | Supported Modes | Intended Usage |
|---|---|---|
| 1 | M | Simple embedded systems |
| 2 | M, U | Secure embedded systems |
| 3 | M, S, U | Systems running Unix-like operating systems |

不支持MMU，无虚拟地址

【参考 2】Table 1.2: Supported combinations of privilege modes.

- Following YSYX and reviewing DC knowledge




香港城市大學
City University of Hong Kong

# FYP Timeline

**Sept - Oct 2025**

- Literature research: security vulnerability cases, current protective plans
- Learn RISC-V privileged architecture and PMP module, simulate RISC-V core by QEMU
- Determine the requirements of the protection system

**Oct - Nov 2025**

- Design hardware encryption module: write logic of simplified AES-128 by Verilog
- Connect encryption module (Xilinx Artix-7) and RISC-V development board (GD32VF103)
- Hardware function verification using oscilloscope

**Nov - Jan 2025 - 2026**

- Permission isolation module: write PMP configuration code in M mode
- Encryption and verification module: write simplified SHA-256 by C++ and driver of AES module
- Integrate modules into RISC-V development board and debug the logic of inter-module calls

**Feb - Mar 2026**

- Attack simulation test: buffer overflow attacks and firmware tampering
- Performance optimization: reduce memory usage and increase speed of the encryption module
- Compatibility test: Verify system functionality on different RISC-V boards (like Nuclei N307)

**Mar - Apr 2026**

- Graduation thesis and thesis defense

香港城市大學
City University of Hong Kong

# Sept. – Oct. 2025 Progress

Literature research

# Determine the scope of the research

- Vulnerability type
  - Permission isolation failure
  - Firmware tampering
  - Side-channel attack
  - Interface abuse
- Protective technologies
  - PMP (Physical Memory Protection)
  - Privilege level mechanism
  - Hardware encryption
  - Secure boot
- Application scenarios
  - Resource-constrained embedded devices

# SoC Platform Security: Why RISC-V?

A Survey and Analysis on SoC Platform Security in ARM, Intel and RISC-V Architecture, Nicholas et al

## Proprietary Architectures

- ARM TrustZone
  - Vulnerable to cache-based side-channel attacks
- Intel SGX
  - Vulnerable to enclave malwares
  - Also vulnerable to cache-based side-channel attacks
- Main reason: lack of flexibility

## Open-source Architecture

- RISC-V
  - Different privilege modes
  - Sanctum Model
  - RISC-V MultiZone Security
  - Adding security features to the existing model
  - Anti Side-channel Attacks: implement different countermeasures in the existing framework
  - Facilitates the open community to participate in finding and fixing security vulnerabilities