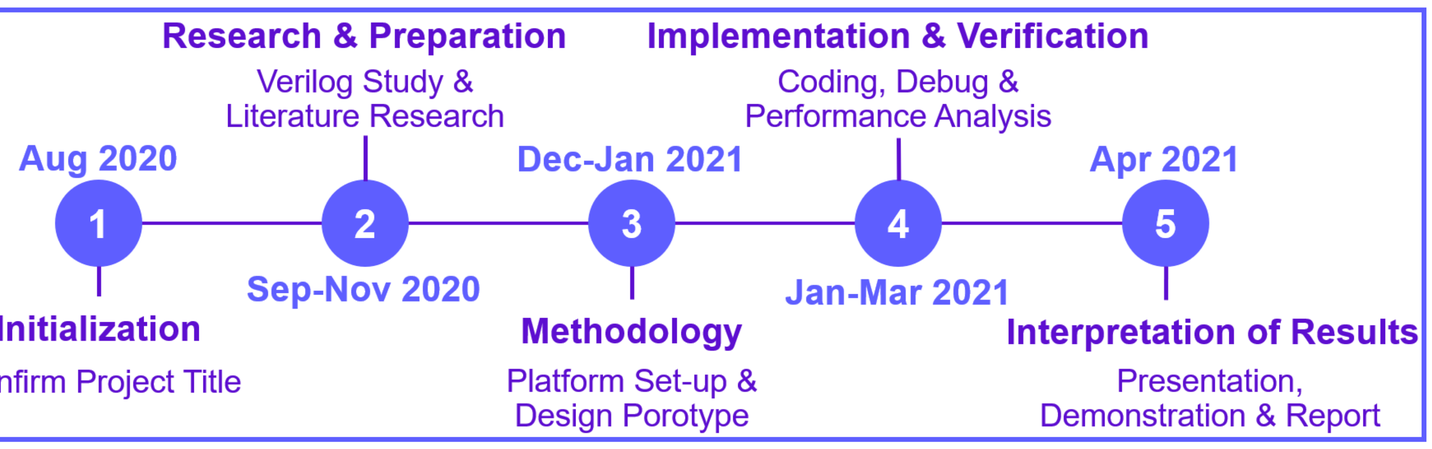
Cryptographic Hardware and Secure Processor Design

Department of Electrical Engineering
香港城市大學
City University of Hong Kong

Student: ZHAO Yifei

Supervisor: Dr. CHEUNG, Ray C C

Programme: BEngECE

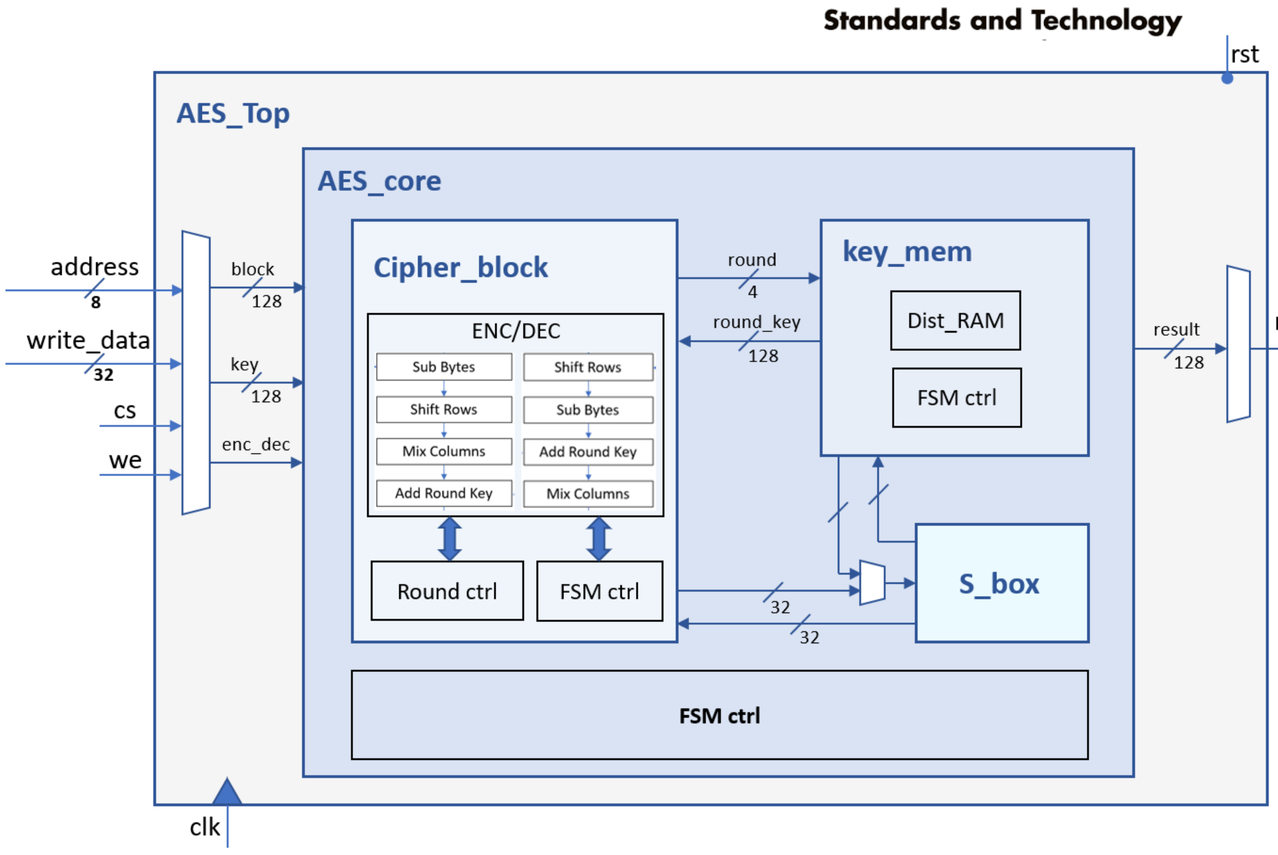


Objective/Background

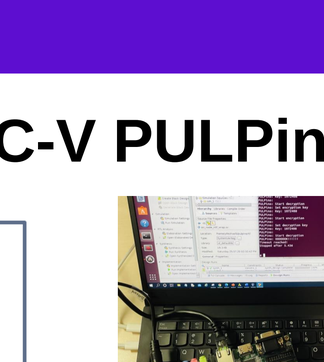
- **Design and Implement a hardware cryptographic AES module;**
- **Optimize the IP core to achieve lightweight requirement;**
- **Explore the application of this IP in lightweight RISC-V secure processor platform.**

Methodology

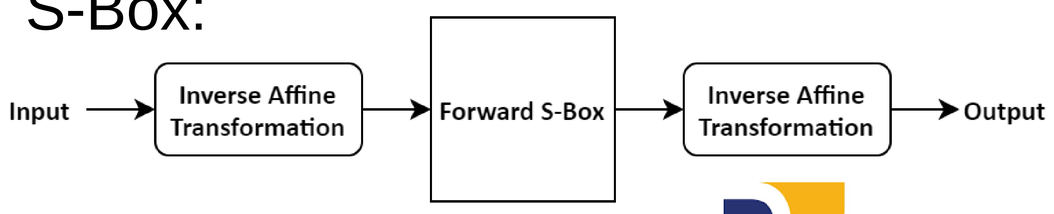
- **Top-Down Block Design**



- **RTL Implementation**
- **RTL Simulation Verification**
- **Optimization**
- Distributed RAM:



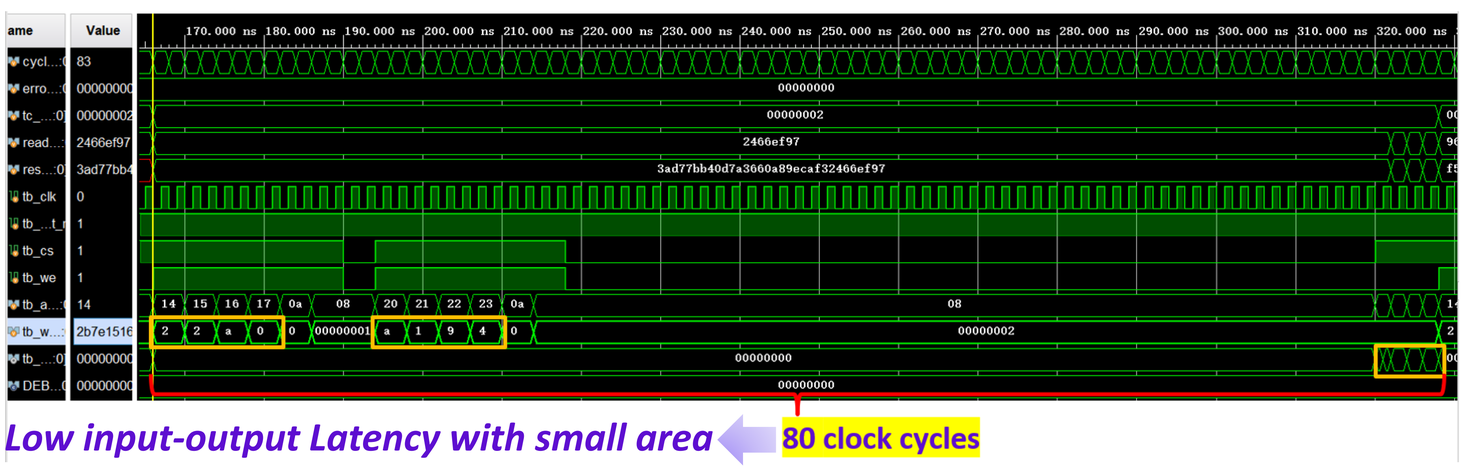
- S-Box:



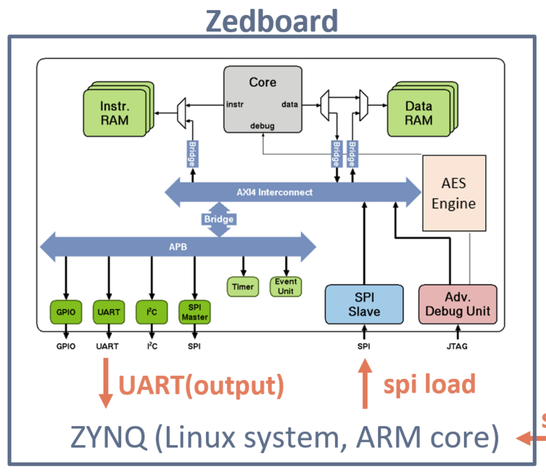
- **Set Up RISC-V PULPino platform**

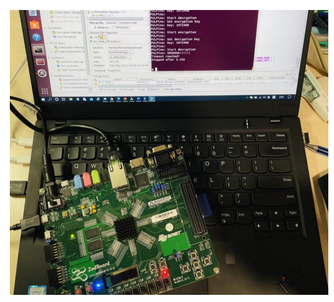
Results/Application

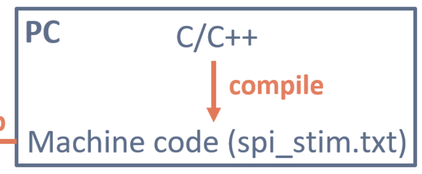
- **Functionality Verification**



- **Application in RISC-V PULPino**







- **Performance and Resource Utilization**

Name	Slice LUTs (53200)	Slice Registers (106400)	F7 Muxes (26600)	F8 Muxes (13300)	Slice (13300)	LUT as Logic (53200)	LUT as Memory (17400)
aes	1950	810	32	4	593	1862	88
core (aes_core)	1881	416	32	4	532	1793	88
cipher (cipher_block)	1126	137	30	4	416	1126	0
keymem (key_mem)	753	275	2	0	325	665	88
dist_ram (dist_mem	88	0	0	0	22	0	88
sbox (sbox)	32	0	0	0	32	32	0

- **ITF Project: Secure RISC-V Platform**