Yunce Zhang

yunce.zhang.sec@gmail.com https://zhangyc0.github.io/ linkedin.com/in/yunce-zhang-b806b0214/

Education

Zhejiang University **Hangzhou,China**

Bachelor of Information Security GPA:3.25/4 *Sep.2020 - Jul.2024*

- **Selected Course:** Computer System I II III, Cryptography, Introduction to Hardware Security, Network Security Theory and Practice, System Security(Overall 89+)
- **Awards:** Academic improvement award, Public service award, Innovation and Entrepreneurship award
- **Student society:** ZJU electronic volunteer association, ZJU MTB team
- **Volunteer service hours:** 400h+
  Research Assistant Jul.2024 - May.2025

Experience

School of Cybersecurity, College of Computer Science and Technology, ZJU **Hangzhou,China**

Research Assistant. Advisor: Prof. Fan Zhang *Feb.2022 - Now*

- Linear change analysis of the mix column section of AES encrypted by IPM
  For the MixColumn coefficient property part in AES, study the impact of its linear transformation on the security performance of IPM. Finally, No correlation was found between its secure performance and coefficient selection.
- Secure Implementation and security performance analysis of SM4 encrypted by IPM encryption
  Refer to the AES encryption scheme and design the SM4 IPM scheme based on the similar algorithm properties of AES and SM4.
- A pragmatic evaluation on Code-based masking
  Conducted basic CPA attacks against DES and AES, etc., and learned the use of Chipwhisperer attacks and Side Channel Attack methods and principles.

Hangzhou Data Resources Management Bureau **Hangzhou,China**

Data Governance Intern *Jun.2022 - Sep.2022*

- Survey on residents' COVID prevention and control measures about QR code
- Bridge inspection equipment Internet of Things online project
- Urban residents' livelihood digital twin project

Publications

Secure evaluation and efficient implementation of inner product masking for SM4 **2024**

- Accepted by Chinese Cryptology Transactions,CCF-A Transcations
- Developed an efficient implementation of the inner product masking technique in the SM4 algorithm by integrating slicing technology.
- Conducted a side-channel security evaluation of the efficient SM4 implementation on a 32-bit platform.
- Optimized the SM4 algorithm implementation based on the evaluation results to achieve an efficient side-channel attack-resistant inner product masking implementation.
- The initial version of this paper was my undergraduate thesis, which received the school's Outstanding Thesis Award

Projects

Five stage pipeline CPU design on RISC-V **Sep.2021 - Jun.2022**

- According to the course requirements, design a 5-State pipeline CPU based on RISC-V by Verilog
- Implemented the CSR register and some privileged instructions, and used forward delivery to solve all conflicts that can be solved by forward delivery
- Implemented D-Cache and I-Cache, and can run a simple version of the kernel (My own Toy-OS)

Toy-OS **Feb.2022 - May.2022**

- Refer to Course requirements, implemented a Toy-operating system kernel built-in RISC-V instructions and C language
- Implemented dynamic memory allocation and page fault exception handling, and implemented mmap series system calls
- Implemented simple ELF Loader and exec and other system calls, and implemented software and hardware interaction

Secure implementation and security evaluation of IPM **Apr.2022 - Jun.2023**

- Refer to IPM [Cheng et al. CHES'21] design, supplement safety performance evaluation, with N=3 T-probing model test.
- First-order and second-order CPA attacks were carried out, and the trace collection range was the first two SBox in the first round
- There is no correlation between the degree of share leakage and the difficulty of CPA attacks. The minimum number of traces required for a successful attack is not accurate enough as an indicator of the difficulty of CPA attacks.

TCP connection design **Sep.2022 - Dec.2022**

- Refer to Stanford-CS144 framework to achieve implementation of the full TCP protocols with C++.
- A TCP finite state machine(FSM) is implemented by combining TCPReceiver and TCPSender to realize communication between different sockets.

Deep Learning Supply Chain Construction and Analysis **Apr.2023 - Jun.2023**

- Conduct supply chain analysis for AI systems, count and analyze CVE and CWE vulnerabilities.
- Build a supply chain network through dependencies in Github, and perform vulnerability checks on the code through CodeQL, the code analysis engine developed by GitHub

Implementation of SM4 encrypted by IPM encryption **Apr.2023 - Aug.2023**

- CISCN'16 National Honor Award(Top 10%).
- Referring to the method of IPM processing of AES in China, based on the interoperability between SM4 and AES (Sbox, block cipher, linear transformation), the IPM scheme of SM4 is designed.

Technical Skills

Languages: C, C++, Python, Verilog, Chisel
Developer Tools: Jetbrains IDE, Vivado, Docker, Jupyter Notebook, Git
Hobbies: Mountain biking, LEGO, Racing car simulator Games