Xinrui Wang

Nanjing University, Nanjing, Jiangsu Province, China
(+86) 18306009145 ⋄ xc123n@gmail.com

EDUCATION

Chongqing University *Sep 2018 - Jun 2022*
School of Microelectronics and Communication Engineering
B.E. of Communication Engineering *GPA: 3.73/4.00*

Nanjing University *Sep 2022 - Jun 2025 (Expected)*
School of Electronic Science and Engineering
M.E. of Integrated Circuits
Supervisor: Lang Feng and Zhongfeng Wang, IEEE Fellow

RESEARCH INTERESTS

side-channel attack, hardware-assisted security, trust execution environment (TEE)

PUBLICATIONS

[1] **ProMiSE: A High Performance Programmable Hardware Monitor for High Security Enforcement of Software Execution**
Xinrui Wang, Lang Feng, Zhongfeng Wang. *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems (TCAD), 2023.*

[2] **RISC-V Custom Instructions of Elementary Functions for IoT Endpoint Devices**
Yuxing Chen, Xinrui Wang, Suwen Song, Lang Feng, Zhongfeng Wang. *IEEE Transactions on Computers (TC), 2024.*

[3] **PreSIT: Predict Cryptography Computations in SGX-style Integrity Trees**
Xinrui Wang, Lang Feng, Zhongfeng Wang. *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems (TCAD), 2024.*

ACADEMIC PROJECTS

1. Rowhammer Exploration in 3D/HBM Memory, leader *Undergraduate Stage*
Motivation: Can Rowhammer occur not only within a layer but also across different layers? Can electrons leak to another layer through Through Silicon Via (TSV), leading to Rowhammer in other layers?
Experiments: I designed an experiment on an Intel FPGA platform with HBM memory. By writing Verilog to control the HBM controller to repeatedly read lines in a certain layer, we then measured the memory values of adjacent layers.
Conclusion: We did not observe Rowhammer in adjacent layers, suggesting that TSV may not support electron leakage from one layer to another.

2. A Programmable Hardware-assisted Security Monitor, leader *Jun 2022 - Mar 2023*
Motivation: Current security monitors are inefficient and inflexible in detecting software runtime attacks.
Contributions: 1) We abstracted and summarized the common requirements for conducting security monitoring into a monitor instruction set. 2) With this monitor instruction set and security-assisting designs, users can efficiently program the monitor to perform a variety of monitoring tasks.
Evaluations: We demonstrated our design on an open-source RISC-V platform (Rocket-Chip) on FPGA. We implemented five security monitoring tasks: shadow stack, whitelist, lightweight DIFT, control-flow integrity, and data-flow integrity. The performance overhead varied from 0% to approximately 23%.

3. Acceleration for Transcendental Functions in IoT, collaborator *Mar 2023 - Nov 2023*
Motivation: Software-based transcendental functions consume considerable time to compute in IoT devices.
Contributions: We proposed a configurable "Cordic" module along with custom instructions in a RISC-V core to perform transcendental computations such as sin, cos, and arctan.
Evaluations: We demonstrated our design on an open-source RISC-V platform (PULP). Compared to software-based computation, the configurable module with custom instructions achieved a speedup of 3.3x to 18x.

4. Performance Improvement of SGX-style Integrity Trees, leader *Apr 2023 - Feb 2024*
Motivation: The hash computation contributes significantly to the performance overhead in the SGX-style integrity tree (SIT) system.
Contributions: 1) We conducted a detailed analysis to identify the performance overhead bottleneck in SIT, focusing on data hash computation and encryption. 2) We proposed a predictive design to prefetch data in memory by leveraging the memory controller's spare time interval. The data hash and encryption were precomputed and recorded in on-chip secure memory. 3) Future computations could refer to the recorded results rather than computing them again.
Evaluations: We implemented our design on a simulator (GEM5). According to the evaluations on benchmarks, the performance overhead was reduced by 5.1% on average (up to 21.6%) compared with SIT without prediction.

5. Side-channel Attack in Chiplet and Corresponding Defense, leader *Mar 2024 - Nov 2024*
Motivation: Chiplets integrate chips from untrusted vendors, leading to security threats.
Contributions: 1) We performed a detailed analysis of this timing side-channel attack. 2) Based on the analysis, we proposed a design to defend against this attack. (**More details are reserved due to paper reviewing.**)
Evaluations: The defense design was implemented on GEM5 simulators, and real-world application evaluations demonstrated the efficiency of our design.

SKILLS

Technical: C, CPP, Verilog, Chisel, Python

Language: IELTS 7.0

AWARDS & SCHOLARSHIPS

National Inspiration Scholarship (3-5%), China Government *Oct 2020*

The 3rd Prize of Intel Cup Undergraduate Electronic Deisgn Contest, Intel Corporation *Oct 2020*

The First Prize Scholarship of Graduate Student (20%), Nanjing University *Sep 2022 and Sep 2023*

Xiaomi Special Scholarship (top 10 of Nanjing University), Xiaomi Corporation *Sep 2023*