KOU ZILI

zkou@connect.ust.hk · (+86) 15651723602 · KOU_Zili

EDUCATION

Hong Kong University of Science and Technology, Hong Kong SAR, China 2019.08 – Now

PhD Candidate, Electronic & Computer Eng., Supervised by Prof. ZHANG Wei

Alibaba DAMO Academy, Computing Technology Lab, *Research Intern* 2022.06 – 2022.11

Southeast University, Nanjing, China 2015.08 – 2019.06

Bachelor, Electronics Sci. & Eng., GPA 3.94/4.0

FIRST-AUTHORED RESEARCH

GPU Framework for Hybrid and Efficient Fully Homomorphic Encryption 2022.06 – 2023.01

- CUDA-Accelerate the hybrid FHE scheme that supports both linear and nonlinear operations
- Achieve hundreds times of speed-up, making FHE practical
- Under double-blind reviewing

Cache Attacks and Defenses of the Sliding Window Algorithm in TEEs 2021.12 – 2022.05

- Scrutinize implementations of the sliding window algorithm in RSA
- Reveal a new vulnerability in the latest Mbed TLS design
- Assigned CVE-2022-46392 as the public identifier
- Accepted by DATE 2023

Attack Directories on ARM big.LITTLE Processors 2021.02 – 2021.11

- Reverse engineer the Snoop Filter (SF) built in Arm CCI-5XX.
- Comprehensive methodology to exploit the SF as a new side channel
- Best Paper Award
- Accepted by ICCAD 2022

Precise Framework for Side-channel Attacks on Arm TrustZone 2020.03 – 2021.01

- Single profiling trace attack on RSA, breaching the exponent blinding defense.
- Target on reference implementation TF-A + OPTEE + Mbed TLS
- Assigned CVE-2021-36647 as the public identifier
- Accepted by DAC 2021

SKILLS

- Programming Languages: C/C++, CUDA, Python, Verilog
- Engineering Scope: Linux Kernel, ARMv8 ISA, Gem5, FHE
- Research Focus: System Security, Side-Channel Attack, Post-quantum Cryptography

HONORS AND AWARDS

William J. McCalla ICCAD Best Paper Award 2022

HKUST RedBird Academic Excellence Award 2022 & 2023

Baowu Steel Excellent Student Award (4 undergraduate students per year) 2019

National Scholarship, President Scholarship (Top 1%) 2018

ACTIVITIES

- Sub-Reviewer: TCAD, TRETS, TVLSI, TECS, FCCM, FPL, CASES, ASPDAC, etc.
- Student Helper: FPT 2022, EDAthon 2020