LI-JIE JIAN (Lip-kiat Kan)

⌂ No.27, Ln. 332, Hushan Rd., Caotun Township, Nantou City 542, R.O.C(Taiwan)

☎(+886)-985-710-306 ✉jcuyo613@gmail.com • leejay0389@citi.sinica.edu.tw

---

EDUCATION

B.S. in Program of Electrical Engineering and Computer Science Sep. 2019 – Jun. 2023

National Central University, Taiwan

Double Major: Computer Science and Network Engineering

GPA / Honors: 4.15/4.30, Academic Excellence Award, Academia Sinica Scholarship

PUBLICATION

Jumping for Berstein-Yang Inversion 2024

The 29th Australasian Conference on Information Security and Privacy (ACISP 2024)

Li-Jie Jian, Ting-Yuan Wang, Bo-Yin Yang, Ming-Shing Chen

EXPERIENCE

Research Assistant Jul. 2023 – Present

Academia Sinica, Research Center for Information Technology Innovation, Taiwan

Advised by Professor Bo-Yin Yang

- Implemented the NTRU Prime key encapsulation mechanism on ARMv8, optimizing low-complexity polynomial multiplications and modular reciprocal algorithms.
- Achieved over 30x performance improvement for the sntrup761 algorithm and actively pursued its application for OpenSSH.
- Conducted formal verification using the Cryptoline tool on the Bernstein-Yang algorithm and polynomial multiplications.

Undergraduate Research Assistant Aug. 2021 – Jun. 2023

Academia Sinica, Research Center for Information Technology Innovation, Taiwan

Co-advised by Professor Bo-Yin Yang and Professor Tung Chou

- Developed, Optimized, and Benchmarked Fast Fourier Transform (FFT) and modular multiplication implementations on ARM Cortex-A53.
- Explored pipeline cycle information and ordering policies on Cortex-A53, analyzing instruction latencies to optimize the efficiency of polynomial multiplications
- Implemented post-quantum cryptography algorithms, especially in code-based and lattice-based cryptography and systems, to speed up polynomial multiplication and to save data space in the whole system.

Undergraduate Research Assistant Aug. 2021 – Jun. 2023

Advanced Defense Lab, National Central University, Taiwan

Advised by Professor Fu-Hau Hsu

- Published work on Hacks In Taiwan Conference (HITCON ZeroDay).
- Achieved First Place in National Central University 2022 CTF Competition.
- Conducted a vulnerability assessment of current commercial cybersecurity for food ordering websites to mitigate information leakage risks, focusing on packet encryption, database maintenance, and related security enhancements.

Co-founder & Software Engineer   Dec. 2020 – Jul. 2021

FalCo Multimedia Company

Advised by Professor Po-Chyi Su

- Led and presented a project focused on overcoming challenges in hair modeling and facial vectorization, resulting in Silver Award in the National Central University Innovation & Incubation Center Startup Competition 2020.
- Designed experiments with mathematical models and wrote code to enhance the accuracy of hair flow and color simulations.
- Cooperated with Smartist Technology Company to design a communication App for customer service at exhibitions during COVID-19.

Software Engineer & Developer   Sep. 2020 – Sep. 2022

National Central University Computer Center, Taiwan

Co-advised by Research Staff Maggie Wu and Research Engineer Huei-Long Chiou

- Led a project servicing classroom reservation for university users.
- Designed and updated school MVC system to reduce data breach risk 99%.
- Built database management systems to save more than 20% overall management time.
- Contributed to three service systems authenticated by the government.

AWARDS AND HONORS

Academia Sinica Scholarship   2021, 2022, 2023

Awarded by Academia Sinica, Taiwan

Undergraduate Research Scholarship   2021, 2022, 2023

Awarded by National Central University, Taiwan

Academic Excellence Award   2019, 2020

Awarded by National Central University, Taiwan

Startup Competition Silver Award   2020

Awarded by National Central University Innovation & Incubation Center, Taiwan

Certificate of Completion   2020

Awarded by Qiskit Hackathon Taiwan, IBM-Q Hub at National Taiwan University, Taiwan

CONFERENCES

Australasian Conference on Information Security and Privacy (ACISP 2024)

University of Technology Sydney, NSW, Australia

Theory of Cryptography Conference (TCC 2023)

International Association for Cryptologic Research (IACR)

Cryptographic Hardware and Embedded Systems (CHES 2023)

International Association for Cryptologic Research (IACR)

Asiacrypt 2022

International Association for Cryptologic Research (IACR)

TECHNICAL SKILLS

Languages: C/C++, Python, ARM-ASM, x86-ASM, SageMath, JavaScript, SQL, Java, Rust

Software Tools: LATEX, Git, Linux Pref, CryptoLine, Docker, AWS