




Keng-Yu Chen

 [kengyuchen](https://github.com/kengyuchen)  r11921066@ntu.edu.tw  kengyuchen.github.io

EDUCATION

Master's Student in Computer Science

Sep. 2022 – Present

Graduate Institute of Electrical Engineering, National Taiwan University

Thesis Advisor: Jiun-Peng Chen & Ho-Lin Chen

Current GPA: 4.12/4.3

Bachelor of Science in Computer Science & Information Engineering

Sep. 2018 – Jun. 2022

Department of Computer Science & Information Engineering, National Taiwan University

GPA: 3.89/4.3

Last 60 GPA: 4.11/4.3

Major GPA: 4.13/4.3

Bachelor of Science in Mathematics

Sep. 2018 – Jun. 2022

Department of Mathematics, National Taiwan University

Relevant Courses

Sep. 2018 – Present

- * Introduction to Cryptography (A)
- * Formal Languages and Automata Theory (A)
- * Computer Architecture (A+)
- * Post-quantum Cryptography (A+)
- * Advanced Digital Signal Processing (A+)
- * Introduction to Secure Coding (A+)
- * Theoretical Aspects of Modern Cryptography (A)
- * Advanced Algorithm (A)
- * Quantum Information and Computation (A+)

PUBLICATION

- Masking Floating-Point Number Multiplication and Addition of Falcon (Under Revision)

Keng-Yu Chen, Jiun-Peng Chen

IACR Transactions on Cryptographic Hardware and Embedded Systems, 2024

RESEARCH EXPERIENCE

Side-Channel Analysis Laboratory

Jun. 2020 – Present

- * Department of Electrical Engineering, National Taiwan University
- * Principal Investigator: Jiun-Peng Chen
- * Researching all topics of side-channel analysis on lattice-based post-quantum cryptography

Adjunct Research Assistant

Sep. 2020 – Present

- * Research Center for Information Technology Innovation, Academia Sinica
- * Principal Investigator: Jiun-Peng Chen

- * Studying and implementing side-channel analysis on concrete cryptographic schemes

Research Intern

Jul. 2023 – Aug. 2023

- * Institute of Information Science, Academia Sinica
- * Advisor: Kai-Min Chung
- * Surveying recent research in theoretical cryptography, mostly in instantiability of schemes in random oracle model, encrypt-then-sign paradigm, and quantum homomorphic encryption

Research Project – NTRU Prime

Oct. 2021 – Apr. 2022

- * Research Center for Information Technology Innovation, Academia Sinica
- * Principal Investigator: Jiun-Peng Chen
- * Implementing attacks and countermeasures on NTRU Prime key encapsulation mechanism

Research Project – Elliptic Curve Cryptography

Jan. 2021 – Jun. 2021

- * Research Center for Information Technology Innovation, Academia Sinica
- * Principal Investigator: Jiun-Peng Chen
- * Implementing attacks and countermeasures on curve P-256 with Jacobian coordinate systems

HONORS AND AWARDS

Champion — Innovation Application Competition of Digital Twins for Smart Farming

Oct. 2022

Council of Agriculture, Executive Yuan, Taiwan

Academic Achievement Award

Apr. 2019

Department of Computer Science & Information Engineering, National Taiwan University

WORKING EXPERIENCE

Teaching Assistant

Sep. 2020 – Jan. 2021

Calculus (1)(2)

Teacher: Ya-Ju Tsai

OTHER EXPERIENCE

Attendee — Asiacrypt 2022

Dec. 2022

Taipei, Taiwan

Attendee — Postquantum Crypto Minischool

Jul. 2022

Academia Sinica, Taiwan

SKILLS

Programming: C/C++, Python, Verilog, Makefile, MATLAB, R

Tools: Git/GitHub, ChipWhisperer, L^AT_EX

Languages: English (IELTS Score: 7.5), Chinese (Native)