

# Keng-Yu Chen

📧 [kengyuchen](mailto:kengyuchen) ✉ [r11921066@ntu.edu.tw](mailto:r11921066@ntu.edu.tw)

## EDUCATION

---

### Master's Student in National Taiwan University

Sep. 2022 – Present

*Graduate Institute of Electrical Engineering, majoring Computer Science*

Current GPA: 4.12/4.3

*Thesis Advisor: Jiun-Peng Chen / Ho-Lin Chen*

### Bachelor of Science in National Taiwan University

Sep. 2018 – Jun. 2022

*Major: Computer Science & Information Engineering*

GPA: 3.89/4.3

*Double Major: Mathematics*

### Relevant Courses

Sep. 2018 – Present

- \* Data Structure and Algorithm
- \* Introduction to Cryptography
- \* Formal Languages and Automata Theory
- \* Computer Architecture
- \* Post-quantum Cryptography
- \* Introduction to Secure Coding
- \* Theoretical Aspects of Modern Cryptography
- \* Advanced Algorithm
- \* Quantum Information and Computation

GPA: 4.0/4.3

GPA: 4.0/4.3

GPA: 4.0/4.3

GPA: 4.3/4.3

GPA: 4.3/4.3

GPA: 4.3/4.3

GPA: 4.0/4.3

GPA: 4.0/4.3

GPA: 4.3/4.3

## 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 Project – Elliptic Curve Cryptography

Jan. 2021 – Apr. 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

### Research Project – NTRU Prime

Jan. 2021 – Apr. 2021

- \* Research Center for Information Technology Innovation, Academia Sinica
- \* Principal Investigator: Jiun-Peng Chen
- \* Implementing attacks and countermeasures on NTRU Prime Key Encapsulation Mechanism

### Summer Intern

Jun. 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

## 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*

### Champion — Innovation Application Competition of

Oct. 2022

### Digital Twins for Smart Farming

*Council of Agriculture, Executive Yuan, Taiwan*

## SKILLS

---

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

**Tools:** Git/GitHub, ChipWhisperer, L<sup>A</sup>T<sub>E</sub>X