




# Keng-Yu Chen

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

**(Double Major) Bachelor of Science in Mathematics** Sep. 2018 – Jun. 2022

*Department of Mathematics, National Taiwan University*

## 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 such as Elliptic Curve Cryptography and NTRU Prime key encapsulation mechanism

**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

## HONORS AND AWARDS

---

<b>Champion — Innovation Application Competition of Digital Twins for Smart Farming</b> <i>Council of Agriculture, Executive Yuan, Taiwan</i>	Oct. 2022
<b>Academic Achievement Award</b> <i>Department of Computer Science &amp; Information Engineering, National Taiwan University</i>	Apr. 2019

## COURSEWORK

---

<b>Relevant Courses</b>	Sep. 2018 – Present
* Introduction to Cryptography (A)	
* Post-quantum Cryptography (A+)	
* Theoretical Aspects of Modern Cryptography (A)	
* Quantum Information and Computation (A+)	

## WORKING EXPERIENCE

---

<b>Teaching Assistant</b> <i>Calculus (1)(2)</i> <i>Teacher: Ya-Ju Tsai</i>	Sep. 2020 – Jan. 2021
---	-----------------------

## OTHER EXPERIENCE

---

<b>Attendee — Asiacrypt 2022</b> <i>Taipei, Taiwan</i>	Dec. 2022
<b>Attendee — Postquantum Crypto Minischool</b> <i>Academia Sinica, Taiwan</i>	Jul. 2022

## EXTRACURRICULAR ACTIVITY

---

<b>Public Address (PA) Team</b>	Sep. 2019 – Jun. 2021
* Student Activity Center, National Taiwan University	
* Operating audio and lighting systems for stage performances at the school's auditorium, including microphones, audio mixers, speakers, and lighting consoles	
<b>Equipment Team</b>	Feb. 2019 – Jun. 2021
* Tainan Alumni Association, National Taiwan University	
* Coping with all the work behind the scenes for stage performances, including stage lighting, audio systems, photography, and videography	

## SKILLS

---

**Programming:** C/C++, Python, Verilog, Makefile, MATLAB, R  
**Tools:** Git/GitHub, ChipWhisperer, L<sup>A</sup>T<sub>E</sub>X  
**Languages:** English (IELTS Score: 7.5), Chinese (Native)