Last Updated on October 24th, 2023

Keng-Yu Chen

kengyuchen ✉ r11921066@ntu.edu.tw

Education

Master's Student in National Taiwan University Sep. 2022 – Present

Graduate Institute of Electrical Engineering, majoring Computer Science
Thesis Advisor: Jiun-Peng Chen / Ho-Lin Chen
Current GPA: 4.12/4.3

Bachelor of Science in National Taiwan University Sep. 2018 – Jun. 2022

Major: Computer Science & Information Engineering
Double Major: Mathematics
GPA: 3.89/4.3

Relevant Courses Sep. 2018 – Present

∗ Data Structure and Algorithm	GPA: 4.0/4.3
∗ Introduction to Cryptography	GPA: 4.0/4.3
∗ Formal Languages and Automata Theory	GPA: 4.0/4.3
∗ Computer Architecture	GPA: 4.3/4.3
∗ Post-quantum Cryptography	GPA: 4.3/4.3
∗ Introduction to Secure Coding	GPA: 4.3/4.3
∗ Theoretical Aspects of Modern Cryptography	GPA: 4.0/4.3
∗ Advanced Algorithm	GPA: 4.0/4.3
∗ Quantum Information and Computation	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 Techonology Innovation, Acamedia Sinica
- Principal Investigator: Jiun-Peng Chen
- Studying and implementing side-channel analysis on concrete cryptographic schemes

Summer Intern Jun. 2023 – Aug. 2023

- Institute of Information Science, Acamedia 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 Techonology Innovation, Acamedia 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 Techonology Innovation, Acamedia Sinica
- Principal Investigator: Jiun-Peng Chen
- Implementing attacks and countermeasures on curve P-256 with Jacobian coordinate systems

Working Experience

Teaching Assistant Sep. 2020 – Jan. 2021
Calculus (1)(2)
Teacher: Ya-Ju Tsai

Other Experience

Attendee — Asiacrypt 2022 Dec. 2022
Taipei, Taiwan

Champion — Innovation Application Competition of Digital Twins for Smart Farming Oct. 2022
Council of Agriculture, Executive Yuan, Taiwan

Attendee — Postquantum Crypto MiniSchool Jul. 2022
Academia Sinica, Taiwan

Skills

Programming: C/C++, Python, Verilog, Makefile, MATLAB, R
Tools: Git/GitHub, ChipWhisperer, LaTeX