

MU CHANGRUI

✉ changrui.mu@u.nus.edu

🌐 [personal website](#)

🌐 [linkedin.com/in/ChangruiMu](https://www.linkedin.com/in/ChangruiMu)

🌐 github.com/Ch40gRv1-Mu

Education

National University of Singapore

Bachelor of Computing (Information Security), Highest Distinction

August 2020 – December 2023

Singapore

Publications

Instance-Hiding Interactive Proof

Changrui Mu, Prashant Nalini Vasudevan

[\[ECCC\]](#), [\[IACR\]](#)

2024

TCC2024

Strong Batching for Non-Interactive Statistical Zero-Knowledge

Changrui Mu, Shafik Nassar, Ron D. Rothblum, Prashant Nalini Vasudevan

[\[ECCC\]](#), [\[IACR\]](#)

2024

Eurocrypt 2024

Research Experience

Interactive Proof Research

August 2022 – Present

Student; Research Assistant, supervised by Dr. Prashant Nalini Vasudevan (NUS)

Singapore

- Explored the power of instance-hiding interactive proof. Broaden understanding about this class. We also researched the connection between such scheme and the influential concept of Randomized Encodings.
- Explored on minimum assumption for instantiating Fiat-Shamir and Correlation-Intractable Hash Functions.

Zero Knowledge Proof Research

May 2023 – August 2023

Visiting Student Researcher, supervised by Dr. Ron Rothblum (Technion)

Haifa, Israel

- Explored the power and limit of statistical witness indistinguishability.
- Contribute to the construction of a strong batching for Non-Interactive Statistical Zero-Knowledge Proof (NISZK-batching).

Research on the Mechanisms in Fear Memory Consolidation

May 2022 – August 2022

Participant, Supervised by Dr. Cora Sau Wan Lai (HKU)

Hong Kong (Remote)

- Publication as third author: Selective Modulation Of Fear Memory In Non-Rapid Eye Movement Sleep on Advanced Science
- Applied a modified pool adjacent violators algorithm (PAVA) to conduct isotonic regression, improving the accuracy of the data analysis.
- Designed a labeling process that utilized deconvolution and filtered out “partial spikes” signals to improve the accuracy of spiking event detection.
- Based on the experimental design, proposed possible assumptions and classified neuronal ensembles into multiple groups for statistical tests to identify correlations between neuron activities and behavior test results.

Teaching Experience

Lead Teaching Assistant

August 2023 – Present

CS4236: Cryptography Theory and Practice, by Dr. Prashant Nalini Vasudevan (NUS)

Singapore

- Assisted in designing and setting up problem sets for students.
- Conducted Q&A sessions and tutorials to deepen students’ understanding.
- Participated in grading assignments, ensuring timely and accurate feedback.

Lead Teaching Assistant

August 2023 – Present

CS3235: Computer Security, instructed by Dr. Reza Shokri (NUS)

Singapore

- Collaborated in creating and setting up problem sets.
- Facilitated Q&A sessions and tutorials to enhance learning outcomes.
- Aided in the grading of assignments, maintaining a high standard of evaluation.

Working Experience

Binance

August 2022 – August 2023

Smart Contract Security Engineer (Part-time Intern)

Singapore (Remote)

- Conducted comprehensive reviews of newly disclosed vulnerabilities in smart contracts, summarizing the underlying causes of each exploit.
- Performed meticulous security audits on both internal and external smart contracts, generating high-quality analytical reports.
- Employed specialized scanning tools to identify vulnerabilities in deployed smart contracts and issued timely risk warnings.

TikTok, ByteDance

May 2022 – August 2022

Backend Engineer Intern (Trust and Safety)

Singapore

- Migrated and refactored GIF logic in direct messages on TikTok.
- Provided support for private message-related safety inquiries on TikTok.
- Conducted dry runs of new models in different regions.
- Assisted with business account message auto-reply logic.

Invited Talks

IEEE East Asian School of Information Theory (EASIT2024)

July 2024

Title: Strong Batching for Non-Interactive Statistical Zero-Knowledge, Poster Presentation

Shonan Village Center, Japan

Eurocrypt2024 Main Session

May 2024

Title: Strong Batching for Non-Interactive Statistical Zero-Knowledge

ETH

Eurocrypt2024 Rump Session

May 2024

Title: If Verifier Also Wants Privacy

ETH

NUS AlgoTheory Seminar

April 2024

Title: Strong Batching for Non-Interactive Statistical Zero-Knowledge

NUS

NTU Cryptography Seminar

March 2024

Title: Batch Verification for Statistical Zero-Knowledge Proofs

Nanyang Technological University

IJTCS2023 Undergraduate Forum

August 2023

Title: Non-Interactive Statistical Zero Knowledge Proof

University of Macau

Certificate & Reward

CS198.2x: Blockchain Technology, UC Berkeley

Issuer: edX (UC Berkeley)

2nd Place Enthusiast, Singapore Blockchain Innovation Challenge

Issuer: NUS, SBIP

Top Student in Computer Security

Issuer: NUS, SOC

Technical Skills

Dean's List

Issuer: NUS, SOC

IEEE EASIT2024 Outstanding Poster Presentation Award

Issuer: IEEE East Asian School of Information Theory

Cryptography I, Dan Boneh

Coursera (Stanford)

Languages: Solidity, Go, Java, C++/C, Python, JavaScript/HTML/CSS, SQL, Rust.

Developer Tools: Ganache, Tableau, Looker, VS Code, IntelliJ IDEA, Vim, Fiddler, Wireshark, Kali Linux, VMware.

Technologies: Natural Language Processing (NLP), Spring Boot, MySQL, Cryptography, Scrapy, Blockchain, Redis, Time Series Database (TS-Database), Message Queue (MQ).