

# MU CHANGRUI

✉ changrui.mu@u.nus.edu

🌐 personal website

🌐 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

---

### Strong Batching for Non-Interactive Statistical Zero-Knowledge

2024

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

*Accepted by Eurocrypt 2024*

[ECCC], [IACR]

### Instance-Hiding Interactive Proof

2024

*Changrui Mu, Prashant Nalini Vasudevan*

*Preprint, TCC2024 On Submission*

[ECCC], [IACR]

---

## 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.
- Explored on Search Delegation Scheme for All-Pairs Shortest Path (APSP) and Longest Common Subsequence (LCS).

### 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).
- Attended Workshop: The Many Colors of Cryptography: A Workshop in Honor of Ran Canetti.

### Research on the Mechanisms in Fear Memory Consolidation

May 2022 – August 2023

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

*Hong Kong (Remote)*

- 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.

### Development and Testing of Cryptography Library

February 2022 – May 2022

*Research Assistant at the Crystal Center, supervised by Dr. Prateek Saxena (NUS)*

*Singapore*

- Tested a new cryptography library and identified significant bugs. Successfully fixed the bugs I discovered.
- Reviewed papers on identity-based encryption (IBE) and analyzed the security of a new decentralized, non-interactive messaging system.
- Built a React Native (RN) Bridge to wrap a new pair-based cryptography (PBC) library for use with RN.

### Data Crawling and Analysis

February 2021 – December 2021

*Student Researcher, Supervised by Dr. Chen Nan (NUS)*

*Singapore*

- Exploited vulnerabilities in Weibo’s mobile API to build a highly efficient concurrent crawler that collected hundreds of millions of Weibo data points.
- Developed a crawler that bypassed the protections in place for WeChat public accounts and collected article data.

---

## 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.

## Projects and Work

---

### **OverPass: MVP of Applying Interactive Proof to Make EVM Cheaper**

**December 2022**

*Main Contributor*

*Singapore*

- Developed OverPass, a Minimum Viable Product (MVP) that applied interactive proof to optimize smart contracts and provide cheaper gas consumption for complex computation on the Ethereum Virtual Machine (EVM).
- Designed a new blockchain ecosystem model that involved untrusted “advisors” to provide cheaper trustworthy computation.

### **Rare Resources Trading System with Blockchain**

**February 2022**

*Co-Developer*

*Singapore*

- Developed an ERC721 token for trading rare resources, such as  $CO_2$  emissions, on a blockchain network.
- Built a React frontend for trading the tokens, providing a user-friendly interface for traders to interact with the blockchain network.

## Certificate & Reward

---

### **CS198.2x: Blockchain Technology, UC Berkeley**

Issuer: edX (UC Berkeley)

### **Top Student in Computer Security**

Issuer: NUS, SOC

### **Orbital - Apollo 11 (Advanced)**

Issuer: NUS, SOC

### **Technical Skills**

---

**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).

### **Dean's List**

Issuer: NUS, SOC

### **Cryptography I, Dan Boneh**

Issuer: Coursera (Stanford)

### **2nd Place Enthusiast, Singapore Blockchain Innovation Challenge**

Issuer: NUS, SBIP