# Mu Changrui

✉ changrui.mu@u.nus.edu personal website linkedin.com/in/ChangruiMu github.com/Ch40gRv1-Mu

## Education

**National University of Singapore** **August 2020 – December 2023**
*Bachelor of Computting (Information Security), Highest Distinction* *Singapore*

## Publications

**Instance-Hiding Interactive Proofs** **2024**
*Changrui Mu, Prashant Nalini Vasudevan* *TCC2024, Invited to the Journal of Cryptology*
[ECCC], [IACR]

**Strong Batching for Non-Interactive Statistical Zero-Knowledge** **2024**
*Changrui Mu, Shafik Nassar, Ron D. Rothblum, Prashant Nalini Vasudevan* *Eurocrypt2024*
[ECCC], [IACR]

**Selective Modulation of Fear Memory in Non-Rapid Eye Movement Sleep** **2024**
*Qiyu Zheng, Yuhua Huang, Changrui Mu, Xiaoqing Hu, Cora Sau Wan Lai* *Advanced Science2024*
[Advanced Science]

## Research Experience

**Interactive Proof Research** **August 2022 – Present**
*Student; Research Assistant, supervised by* ***Dr. Prashant Nalini Vasudevan (NUS)*** *Singapore*

- Conducted a systematic study of instance-hiding interactive proof (IHIP).
  - ∗ Showed that any language with an IHIP is contained in $NP/Poly \cap CoNP/Poly$.
  - ∗ Demonstrated that if an average-case hard language has a constant-round IHIP, then infinitely-often One-Way Functions exist.
  - ∗ Proved the existence of an oracle with respect to which there is a language that has an IHIP but not an SZK proof.
  - ∗ Established that IHIPs are closed under composition with any efficiently computable function.
- Additionally explored a stronger version of IHIP, called *Simulatable IHIP*, yielding even stronger results:
  - ∗ Any language with a Simulatable IHIP is contained in $AM \cap coAM$.
  - ∗ Demonstrated that if a *worst-case* hard language has a Simulatable IHIP, then One-Way Functions exist.
- 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.
- Contributed to advancing the state-of-the-art in batching verification for non-interactive statistical zero-knowledge proofs (NISZK). The research showed that any problem with an NISZK proof has a batching protocol with polylogarithmic communication in the number of instances.
- Working closely with Prof. Ron D. Rothblum during my research internship at Technion equiped me with important techniques, and taught me how to approach problem in clarity, enabling meaningful progress.
- Inspired by Prof. Ron Rothblum's clear communication style, this experience also reinforced the importance of clear communication in scientific research and inspired me to aspire to contribute to both theory and its effective dissemination.

## Teaching Experience

**Lead Teaching Assistant** **August 2023 – December 2023**
*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 – December 2023**
*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.

## Invited Talks

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

- Eurocrypt2024 Main Session
- IEEE East Asian School of Information Theory (EASIT2024)
- NUS AlgoTheory Seminar 2024
- NTU Cryptography Seminar 2024
- IJTCS2023 Undergraduate Forum

**Instance-Hiding Interactive Proofs:**

- Eurocrypt2024 Rump Session
- TCC2024
- NUS AlgoTheory Seminar 2024
- CUHK AlgoThoery Seminar 2024

## Certificate & Award

**CS198.2x: Blockchain Technology, UCBerkeley**
Issuer: edX (UCBerkeley)

**2nd Place Enthusiast, Singapore Blockchain Innovation Challenge**
Issuer: NUS, SBIP

**Top Student in Computer Security**
Issuer: NUS, SOC

**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)

## Additional Research and 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.

**Research on the Mechanisms in Fear Memory Consolidation** — **May 2022 – August 2022**
*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.

**Development and Testing of Cryptography Library** — **February 2022 – May 2022**
*Research Assistant at the Crystal Center, supervised by* ***Dr. Prateek Saxena (NUS)*** — *Singapore*

- 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*

- Data collection and analysis on Weibo Credit System Data.

## 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).