Mu Changrui

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

Education

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

Research Experience

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

- One Paper in Submission: ITCS 2024
- Discovered a novel intuitive solution of Yao's Millionaire Problem in the physical world and made a protocol relying only on DDH, collision-resistant hash function with cheaper complexity in semi-honest settings.
- Researched the amortization theorem for the sum-check protocol, uncovered some interesting properties, and explored its potential applications.
- 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*

- One paper in Submission: Eurocrypt 2024
- Explored the power and limit of statistical witness indistinguishability.
- Contribute to strong NISZK batching protocol: EuroCrypt2024 on submission.
- Attended Workship: The Many Colors of Cryptography

Research on the Mechanisms in Fear Memory Consolidation **May 2022 – August 2023**
*Participant, Supervised by **Dr. Cora Sau Wan Lai (HKU)*** *Hong Kong(Remote)*

- Third Author: Nature Neuroscience on Submission
- 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 a paper on identity-based encryption (IBE) and analyzed the security of a new decentralized, non-interactive messaging system.
- Built a RN Bridge to wrap a new PC cryptography library for use with React Native (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.
- Researched the credibility algorithm of Weibo, specifically the Yang Guang credibility metric, analyzed its effectiveness and impact on user behavior, and related security problems.

Teaching Experience

Main 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.

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

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 cheapter trustworthy computation.
- Explored the potential development trend of blockchain and EVM, providing insights into the future of blockchain technology.

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.

Ethereum Risky Transaction Detection System **February 2022**

Independent Developer *Singapore*

- Developed an on-chain solidity bank that provided efficient 2-factor authentication for users.
- Created moderation policies that detected risky transactions on the Ethereum network, allowing for proactive risk management.

Certificate & Reward

CS198.2x: Blockchain Technology, UCBerkeley **February 2023**

Issuer: edX (UCBerkeley) ***Credential***

Dean's List **May 2022**

Issuer: NUS, SOC ***Credential***

Top Student in Computer Security **January 2022**

Issuer: NUS, SOC ***Credential***

Cryptography I, Dan Boneh **December 2021**

Issuer: Coursera(Stanford) ***Credential***

2nd Place Enthusiast, Singapore Blockchain Innovation Challenge **December 2021**

Issuer: SBIP ***Credential***

Orbital - Apollo 11 (Advanced) **August 2021**

Issuer: NUS, SOC ***Credential***

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)