Xinyu Zhang

Education

May 2021– (Expected) Jan 2025 **Ph.D. Candidate**, *Monash University & CSIRO Data61*.

- **Supervised By** *Prof. Joseph Liu*, A/Prof. Ron Steinfeld, Dr. Muhammed Esgin, Dr. Dongxi Liu
  - Primarily focused on designing post-quantum advanced signature schemes, including aggregate and ring signatures, using only symmetric key primitives.
  - Engaged in side projects such as developing new consensus mechanisms and blockchain-based post-quantum applications.
- **Award**
  - Best Paper Award at ACISP'24

Feb 2018– Dec 2019 **Master of Information Technology**, *Monash University*.

- **Academic Result** GPA 3.813
- **Scholarship** Information Technology International Merit Scholarship
- **Awards**
  - 2018 Semester 2 Top Mark Certificate for FIT5163 Information and Computer Security
  - 2019 Semester 2 Top Mark Certificate for FIT5214 Blockchain
  - 2019 Semester 2 Receiving High Distinction in all units
- **Master Thesis** Revocable and Linkable Ring Signature
  - **Supervised by:** Joseph Liu, Ron Steinfeld, Veronika Kuchta, and Jiangshan Yu

Sep 2013– Jun 2017 **Bachelor of Management**, *Hainan Normal University*.

- **Academic Result** WAM 84.9
- **Awards**
  - Hainan Normal University Second-Class Scholarship Award
  - Hainan Normal University Excellent Intern Award

Publications

2019

- **Revocable and Linkable Ring Signature**
  - Conference: Information Security and Cryptology: 15th International Conference (Inscrypt 2019)
  - Authors: **Xinyu Zhang**, Joseph Liu, Ron Steinfeld, Veronika Kuchta, and Jiangshan Yu
  - Page: 3 – 27
  - Publisher: Springer International Publishing

(+61) 431194313 • xinyu.zhang1@moansh.edu
cryptome-xyz.github.io

2024 ○ **Loquat: A SNARK-Friendly Post-Quantum Signature based on the Legendre PRF with Applications in Ring and Aggregate Signatures**
- Conference: Annual International Cryptology Conference (Crypto 2024)
- Authors: **Xinyu Zhang**, Ron Steinfeld, Muhammed Esgin, Joseph Liu, Dongxi Liu, and Sushmita Ruj
- Page: 3 – 38
- Publisher: Springer Nature Switzerland

2024 ○ **DualRing-PRF: Post-Quantum (Linkable) Ring Signature from Legendre and Power Residue PRFs (Best Paper Award)**
- Conference: Australasian Conference on Information Security and Privacy (ACISP 2024)
- Authors: **Xinyu Zhang**, Ron Steinfeld, Joseph Liu, Muhammed Esgin, Dongxi Liu, and Sushmita Ruj
- Page: 124 – 143
- Publisher: Springer Nature Singapore

2024 ○ **Smooth Transition from PoW to PoS**
- Conference: The 6th ACM International Symposium on Blockchain and Secure Critical Infrastructure (BSCI 2024)
- Authors: **Xinyu Zhang**, Runchao Han, Tong Cao, Jiangshan Yu
- Accepted for Publication

2024 ○ **BDEC: Enhancing Learning Credibility via Post-Quantum Digital Credentials**
- Conference: The 18th International Conference on Provable and Practical Security (ProvSec 2024)
- Authors: Ziyi Li, **Xinyu Zhang**, Hui Cui, Jun Zhao, Xuan Chen
- Accepted for Publication

Working Experience

Mar 2022 – current **(Admin) Teaching Associate**, *Monash University*.
- ○ Admin TA of FIT5163 (Information and Computer Systems)
- ○ TA of FIT1047 (Introduction to computer systems, networks and security)

Jun 2022 – Dec 2022 **Research Assistant**, *Monash University*.
- ○ Focused on optimizing the transition process from Proof-of-Work to Proof-of-Stake blockchain systems.