

Kuo Zhao

Department of Software Systems and Cybersecurity
Faculty of Information Technology
Monash University

✉ raymond.zhao@monash.edu

📄 <https://raykzhao.github.io>

Academic Qualifications

- 02/2018–03/2022 **Doctor of Philosophy**,
Faculty of Information Technology,
Monash University, Clayton Campus.
PhD thesis: “Efficient Implementation Techniques for Lattice-based Cryptosystems”
Supervisors: Associate Professor Ron Steinfeld & Dr. Amin Sakzad
- 02/2016–12/2017 **Master of Networks and Security**,
Faculty of Information Technology,
Monash University, Caulfield Campus.
Masters thesis: “Efficient implementation techniques for lattice-based crypto”
- 09/2011–06/2015 **Bachelor of Engineering**,
College of Computer Science & Technology,
Zhejiang University, China.
Speciality: Computer Science & Technology

Scholarships and Awards

- 10/2021 Monash University Graduate Research Completion Award
- 10/2021 Faculty Graduate Research Completion Award
- 10/2021 Faculty of Information Technology International Postgraduate Research Scholarship
- 04/2018 Dux of Postgraduate (Master of Networks and Security), Cliff Bellamy Awards 2018, Monash University
- 2018 RTP Stipend, Monash University
- 2018 Monash International Tuition Scholarship (MITS), Monash University
- 02/2016 Information Technology International Merit Scholarship, Monash University

Academic Employment

- 08/2021–now **Research Assistant**,
Faculty of Information Technology, Monash University.

02/2018–now **Teaching Associate,**

Faculty of Information Technology, Monash University.

- Semester 1, 2022 FIT9137 Introduction to computer architecture and networks
- Semester 1, 2022 FIT2093 Introduction to cyber security (Admin Tutor)
- Semester 1, 2021 FIT9137 Introduction to computer architecture and networks
- Semester 1, 2021 FIT3173 Software security
- Semester 1, 2020 FIT9137 Introduction to computer architecture and networks
- Semester 1, 2020 FIT5163 Information and computer security
- Semester 1, 2020 FIT2093 Introduction to cyber security (Admin Tutor)
- Semester 2, 2019 FIT5124 Advanced topics in security (Admin Tutor)
- Semester 1, 2019 FIT2093 Introduction to cyber security (Admin Tutor)
- Semester 2, 2018 FIT5124 Advanced topics in security
- Semester 1, 2018 FIT2093 Introduction to cyber security

06/2017–11/2017 **Research Assistant,**

Faculty of Information Technology, Monash University.

Responsibilities:

- Undertaking research duties in the area of Lattice-based Cryptosystems and its Implementation, as directed by the supervisors, Dr Ron Steinfeld and Dr Amin Sakzad.
- Improving the efficiency of the Titanium, a new lattice-based cryptosystem proposed by the supervisors and their colleagues.
- Implementing an efficient and timing-attack resistant software implementation of the Titanium.

Professional Profile

- Highly developed research qualitative and analytical skills with a strong capacity to conduct independent research
- Proven ability to conceptualise problems and develop well-reasoned and integrated solutions, as demonstrated throughout research employment, Masters, and PhD research
- Strong programming skills in C and assembly. Working knowledge of Linux and \LaTeX
- Native speaker of Mandarin

Publications

Muhammed F. Esgin, Ron Steinfeld, and Raymond K. Zhao. Efficient verifiable partially-decryptable commitments from lattices and applications. In *Public Key Cryptography (1)*, volume 13177 of *Lecture Notes in Computer Science*, pages 317–348. Springer, 2022.

Muhammed F. Esgin, Ron Steinfeld, and Raymond K. Zhao. MatRiCT+: More efficient post-quantum private blockchain payments. In *IEEE Symposium on Security and Privacy*, pages 560–577. IEEE, 2022.

Muhammed F. Esgin, Raymond K. Zhao, Ron Steinfeld, Joseph K. Liu, and Dongxi Liu. MatRiCT: Efficient, scalable and post-quantum blockchain confidential transactions protocol. In *CCS*, pages 567–584. ACM, 2019.

Tasopoulos George, Jinhui Li, Apostolos P. Fournaris, Raymond K. Zhao, Amin Sakzad, and Ron Steinfeld. Performance evaluation of post-quantum tls 1.3 on embedded systems. *IACR Cryptol. ePrint Arch.*, 2021:1553, 2021.

Ron Steinfeld, Amin Sakzad, and Raymond K. Zhao. Practical MP-LWE-based encryption balancing security-risk versus efficiency. *Des. Codes Cryptogr.*, 87(12):2847–2884, 2019.

Raymond K. Zhao, Sarah McCarthy, Ron Steinfeld, Amin Sakzad, and Máire O’Neill. Quantum-safe HIBE: does it cost a latte? *IACR Cryptol. ePrint Arch.*, 2021:222, 2021.

Raymond K. Zhao, Ron Steinfeld, and Amin Sakzad. COSAC: compact and scalable arbitrary-centered discrete Gaussian sampling over integers. In *PQCrypto*, volume 12100 of *Lecture Notes in Computer Science*, pages 284–303. Springer, 2020.

Raymond K. Zhao, Ron Steinfeld, and Amin Sakzad. FACCT: fast, compact, and constant-time discrete Gaussian sampler over integers. *IEEE Trans. Computers*, 69(1):126–137, 2020.

Referees

Dr Ron Steinfeld
Associate Professor
Faculty of Information Technology
Monash University
Email: ron.steinfeld@monash.edu

Dr Amin Sakzad
Senior Lecturer
Faculty of Information Technology
Monash University
Email: amin.sakzad@monash.edu