Cybersecurity Lab
Faculty of Information Technology
Monash University
✉ *raymond.zhao@monash.edu*
raykzhao.github.io

Raymond K. Zhao

Academic Qualifications

2018–2022 **Doctor of Philosophy**,
Faculty of Information Technology,
Monash University, Clayton Campus.
Supervisors: Ron Steinfeld & 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

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

02/2018–now **Teaching Associate**,
Faculty of Information Technology, Monash University.
Semester 1, 2018 FIT2093 Introduction to cyber security
Semester 2, 2018 FIT5124 Advanced topics in security

06/2017–11/2017 **Casual Academic Research Assistant to Dr Amin Sakzad and Dr Ron Steinfeld**,
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.
- 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 and Masters research
- Strong programming skills in C and assembly. Working knowledge of Linux and LaTeX
- Native speaker of Mandarin

Publications

Ron Steinfeld, Amin Sakzad, and Raymond K. Zhao. Titanium: Post-quantum public-key encryption and KEM algorithms, 2017. Submitted to the NIST Post-Quantum Competition.

Raymond K. Zhao, Ron Steinfeld, and Amin Sakzad. FACCT: fast, compact, and constant-time discrete gaussian sampler over integers. *IACR Cryptology ePrint Archive*, 2018:1234, 2018.

Extra Curricular Activities – Volunteering

07/2016–09/2016 **ASK Me Volunteer**,
Monash Student Association (MSA), Monash University.

09/2016 **Support Crew, Monash MS 24 Hour Mega Swim**,
Monash Sport, Monash University.

07/2016 **2016 Monash Games Court Operations Volunteer (Fustal)**,
Monash Sport, Monash University.

Interests

Board games, Card games, Japanese culture

Referees

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

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