Kuo Zhao

ExeQuantum
✉ *raykzhao@gmail.com*
🌐 *https://raykzhao.github.io*

Qualifications

02/2018–03/2022 **Doctor of Philosophy**,
Faculty of Information Technology, Monash University
PhD thesis: Efficient Implementation Techniques for Lattice-based Cryptosystems
Supervisors: Associate Professor Ron Steinfeld and Associate Professor Amin Sakzad

Selected Projects:

- **Discrete Gaussian Sampling Algorithms**
  - I created *two new* discrete Gaussian sampling algorithms. Discrete Gaussian sampling is a crucial algorithm used by the post-quantum cryptography.
  - My algorithms are *faster*, consuming *less* memory, and/or supporting a *wider* range of discrete Gaussian distributions, compared to previous techniques.
  - My techniques have been employed by the Falcon post-quantum digital signature scheme, a pending standard by the NIST.
- **Post-quantum Privacy Preserving Protocols**
  - I investigated the implementation aspects for post-quantum privacy preserving protocol primitives, in *ongoing* research collaborations with researchers in the Monash University. These protocols are crucial for cryptocurrencies such as the Monero and the Algorand.
  - I developed *efficient* techniques and/or implementations for these cryptography primitives. My techniques are *faster* than previous post-quantum solutions for the same protocol.
  - Four media articles (1, 2, 3, 4) have been released by the CSIRO and/or the Monash University.

02/2016–12/2017 **Master of Networks and Security**,
Faculty of Information Technology, Monash University
Minor thesis: Efficient implementation techniques for lattice-based crypto
Achievements:

- Dux of Postgraduate (Master of Networks and Security), Cliff Bellamy Awards 2018, Monash University.

09/2011–06/2015 **Bachelor of Engineering**,
College of Computer Science & Technology, Zhejiang University, China

Employments

07/2025– **Co-founder, Chief Technology Officer**,
ExeQuantum

11/2022–06/2025 **Postdoctoral Fellow**,
Data61 Cybersecurity and Quantum Systems Group, CSIRO

Awards:

- SCS Biannual Award May 2023 (Engineering and Technology Award).
- SCS Biannual Award May 2024 (Early Career in Engineering Award).
- iAwards 25 ACT Finalist.

Program Committee: Asiacrypt 2023, ACM CCS 2024 Artifact Evaluation, ICISC 2024, TCCS 2024.

PhD Supervisions:

- Mert Yassı (Jul 2023–present, co-supervisor)
- Meghali Nandi (Sep 2024–present, co-supervisor)

Selected Projects:

- **MIKA: A Minimalist Approach to Hybrid Key Exchange**
  - I worked with researchers in CSIRO's Data61 and the Australian company Penten to develop a new framework for hybrid key exchange protocols. The framework achieves *minimal* modifications to the core codebase and the state machine of the protocol compared to existing solutions.
  - I developed and tested a proof-of-concept implementation of MIKA in the IPSec software strongSwan.
  - Our project is one of the iAwards 25 ACT Finalists.
- **GPU-accelerated Falcon Digital Signature Scheme**
  - I *initiated* a research collaboration with researchers from South Korea.
  - I created *new* techniques to solve the unique challenges of efficiently implementing the Falcon post-quantum digital signature scheme, a pending standard by the NIST, on a GPU. My techniques increase the throughput of a crucial algorithm in Falcon by *ten times* on a GPU.
  - We developed the *first* GPU-accelerated Falcon implementation with *high throughput*.
  - A media article has been released by the Monash University.

08/2021–10/2022 **Research Assistant**,
Faculty of Information Technology, Monash University

Selected Projects:

- **Latte Hierarchical Identity-based Encryption**
  - I *initiated* a research collaboration with researchers from Canada and the United Kingdom.
  - I developed the *first* complete optimized practical implementation of Latte, a post-quantum Hierarchical Identity-based Encryption scheme endorsed by the ETSI.
  - I created *new* optimization techniques for the algorithms in Latte. My techniques significantly *accelerate* the algorithms and *reduce* the communication costs. With my techniques, a crucial algorithm in Latte now only takes *less than a second* computational time on a desktop computer, significantly *faster* than the order of minutes previously estimated by the ETSI.
  - A LinkedIn blog has been released by the Monash University.

- **Implementation of Post-Quantum Algorithms for Bouncy Castle Library**
  - I was a Chief Investigator for the project of post-quantum cryptography integration in the Bouncy Castle, an *Australian sovereign* software cryptography library.
  - I was part of the supervision team, providing cryptographic engineering insights and guidance to four student research assistants.
  - My name has been listed on the Contributors of the Bouncy Castle.

02/2018–10/2022 **Teaching Associate**,
Faculty of Information Technology, Monash University

Teaching:

- Semester 2, 2022: FIT9137 Introduction to computer architecture and networks
- 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

Selected Projects:

- **Titanium Key Encapsulation Mechanism**
  - I developed an *efficient* and *secure* software implementation of the Titanium, a new post-quantum Key Encapsulation Mechanism designed by the Monash University.
  - I created *new* techniques to significantly *accelerate* its arithmetic computations.
  - My implementation has been submitted to the Post-Quantum Cryptography Standardization Process by the NIST.

Referees

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

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

Dr Dongxi Liu
Principal Research Scientist
Data61
CSIRO
Email:
dongxi.liu@data61.csiro.au