Kuo Zhao

ExeQuantum
✉ raykzhao@gmail.com
raykzhao.phd

Qualifications

02/2018–03/2022 **Doctor of Philosophy**,
Faculty of Information Technology, Monash University.
PhD thesis: *Efficient Implementation Techniques for Lattice-based Cryptosystems*

02/2016–12/2017 **Master of Networks and Security**,
Faculty of Information Technology, Monash University.
Awards:
- 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– **Chief Technology Officer, Co-founder**,
ExeQuantum.

11/2022–06/2025 **Postdoctoral Fellow**,
Data61 Cybersecurity and Quantum Systems Group, CSIRO.
Awards:
- iAwards 25 ACT Winner (Government & Public Sector).
- SCS Biannual Award, May 2024 (Early Career in Engineering Award).
- SCS Biannual Award, May 2023 (Engineering and Technology Award).

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

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

06/2017–11/2017 **Research Assistant**,
Faculty of Information Technology, Monash University.

Selected Works

Discrete Gaussian Sampling Algorithms

- I created *two new* discrete Gaussian sampling algorithms. Discrete Gaussian sampling is a crucial algorithm used in post-quantum cryptography.
- My algorithms are *faster*, consume *less* memory, and / or support a *wider* range of discrete Gaussian distributions, compared to previous techniques.
- My techniques have been used by the FN-DSA post-quantum digital signature scheme, a pending standard by NIST. The adopted technique is likely to become part of the NIST standard.

MIKA: A Minimalist Approach to Hybrid Key Exchange

- I worked with 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 work **won** the iAwards 25 ACT (Government & Public Sector).

Implementation of Post-Quantum Algorithms for Bouncy Castle Library

- I was a Chief Investigator for the project of post-quantum cryptography integration in Bouncy Castle, an *Australian sovereign* software cryptography library.
- I was part of the supervision team, providing cryptographic engineering insights and guidance to four research assistants.
- I have been recognised as Contributor of Bouncy Castle.