

Kuo Zhao

ExeQuantum
✉ raykzhao@gmail.com
🌐 raykzhao.gitlab.io



Qualifications

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

Selected Projects:

○ 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.

○ Post-quantum Privacy Preserving Protocols

- I investigated the implementation aspects for post-quantum privacy preserving protocol primitives, in *ongoing* research collaborations with researchers in Monash University. These protocols are crucial for cryptocurrencies such as Monero and 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 CSIRO and / or Monash University.

02/2016– **Master of Networks and Security,**
12/2017 *Faculty of Information Technology, Monash University*

Awards:

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

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

Employments

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

11/2022– **Postdoctoral Fellow,**
06/2025 *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).

Selected Projects:

- **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).
- **GPU-accelerated FN-DSA Digital Signature Scheme**
 - I created *new* techniques to solve the unique challenges of efficiently implementing the **FN-DSA** post-quantum digital signature scheme, a **pending standard** by NIST, on a GPU. My techniques increase the throughput of a crucial algorithm in FN-DSA by *ten times* on a GPU.
 - We developed *first* GPU-accelerated FN-DSA implementation with *high throughput*.
 - Monash University has released a **media article**.

08/2021– **Research Assistant,**

10/2022 *Faculty of Information Technology, Monash University*

Selected Projects:

- **LATTE Hierarchical Identity-based Encryption**
 - I developed *first* complete optimised practical implementation of LATTE, a post-quantum Hierarchical Identity-based Encryption scheme endorsed by **ETSI**.
 - I created *new* optimisation 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 ETSI.
 - Monash University has released a **LinkedIn blog**.
- **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.

02/2018– **Teaching Associate,**

10/2022 *Faculty of Information Technology, Monash University*

06/2017– **Research Assistant,**

11/2017 *Faculty of Information Technology, Monash University*

Selected Projects:

- **Titanium Key Encapsulation Mechanism**
 - I developed an *efficient* and *secure* software implementation of Titanium, a new post-quantum Key Encapsulation Mechanism designed by 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 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