Kuo Zhao

CSIRO's Data61
✉ *raymond.zhao@data61.csiro.au*
🌐 *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 Dr. Amin Sakzad
Key Projects and Achievements:
Discrete Gaussian Sampling Algorithms [1, 2]

- 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 [3, 4, 5, 6, 7]

- 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

11/2022–now **Postdoctoral Fellow**,
Data61 Cybersecurity and Quantum Systems Group, CSIRO
Key Projects:
GPU-accelerated Falcon Digital Signature Scheme [8]

- 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.

eMLE-Sig 2.0 Digital Signature Scheme

- I developed an *efficient* software implementation of the eMLE-Sig 2.0, a new post-quantum digital signature scheme designed by the CSIRO. For the same cryptography security level, my implementation is *faster* than the NIST-approved post-quantum digital signature algorithms.
- I created *new* techniques to significantly *accelerate* its arithmetic computations.
- My implementation has been submitted to the Call for Additional Digital Signature Schemes for the Post-Quantum Cryptography Standardization Process by the NIST.

Awards:

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

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

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

Key Projects and Achievements:

Latte Hierarchical Identity-based Encryption [9]

- 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.

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

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

Key Projects and Achievements:

Titanium Key Encapsulation Mechanism [10]

- 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

Publications

[1] Zhao, Raymond K. ; Steinfeld, Ron ; Sakzad, Amin: FACCT: FAst, Compact, and Constant-Time Discrete Gaussian Sampler over Integers. In: *IEEE Trans. Computers* 69 (2020), Nr. 1, S. 126–137

[2] Zhao, Raymond K. ; Steinfeld, Ron ; Sakzad, Amin: COSAC: COmpact and Scalable Arbitrary-Centered Discrete Gaussian Sampling over Integers. In: *PQCrypto* Bd. 12100, Springer, 2020 (Lecture Notes in Computer Science), S. 284–303

[3] Esgin, Muhammed F. ; Zhao, Raymond K. ; Steinfeld, Ron ; Liu, Joseph K. ; Liu, Dongxi: MatRiCT: Efficient, Scalable and Post-Quantum Blockchain Confidential Transactions Protocol. In: *CCS*, ACM, 2019, S. 567–584

[4] Esgin, Muhammed F. ; Steinfeld, Ron ; Zhao, Raymond K.: Efficient Verifiable Partially-Decryptable Commitments from Lattices and Applications. In: *Public Key Cryptography (1)* Bd. 13177, Springer, 2022 (Lecture Notes in Computer Science), S. 317–348

[5] Esgin, Muhammed F. ; Steinfeld, Ron ; Zhao, Raymond K.: MatRiCT+: More Efficient Post-Quantum Private Blockchain Payments. In: *IEEE Symposium on Security and Privacy*, IEEE, 2022, S. 560–577

[6] Esgin, Muhammed F. ; Ersoy, Oguzhan ; Kuchta, Veronika ; Loss, Julian ; Sakzad, Amin ; Steinfeld, Ron ; Yang, Xiangwen ; Zhao, Raymond K.: A New Look at Blockchain Leader Election: Simple, Efficient, Sustainable and Post-Quantum. In: *AsiaCCS*, ACM, 2023, S. 623–637

[7] Steinfeld, Ron ; Sakzad, Amin ; Esgin, Muhammed F. ; Kuchta, Veronika ; Yassi, Mert ; Zhao, Raymond K.: *LUNA: Quasi-Optimally Succinct Designated-Verifier Zero-Knowledge Arguments from Lattices*. Cryptology ePrint Archive, Paper 2022/1690. https://eprint.iacr.org/2022/1690. Version: 2022. – https://eprint.iacr.org/2022/1690

[8] Lee, Wai-Kong ; Zhao, Raymond K. ; Steinfeld, Ron ; Sakzad, Amin ; Hwang, Seong O.: High Throughput Lattice-Based Signatures on GPUs: Comparing Falcon and Mitaka. In: *IEEE Trans. Parallel Distributed Syst.* 35 (2024), Nr. 4, S. 675–692

[9] Zhao, Raymond K. ; McCarthy, Sarah ; Steinfeld, Ron ; Sakzad, Amin ; O'Neill, Máire: Quantum-Safe HIBE: Does It Cost a Latte? In: *IEEE Trans. Inf. Forensics Secur.* 19 (2024), S. 2680–2695

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

[11] Tasopoulos, George ; Li, Jinhui ; Fournaris, Apostolos P. ; Zhao, Raymond K. ; Sakzad, Amin ; Steinfeld, Ron: Performance Evaluation of Post-Quantum TLS 1.3 on Resource-Constrained Embedded Systems. In: *ISPEC* Bd. 13620, Springer, 2022 (Lecture Notes in Computer Science), S. 432–451

[12] Tasopoulos, George ; Dimopoulos, Charis ; Fournaris, Apostolos P. ; Zhao, Raymond K. ; Sakzad, Amin ; Steinfeld, Ron: Energy Consumption Evaluation of Post-Quantum TLS 1.3 for Resource-Constrained Embedded Devices. In: *CF*, ACM, 2023, S. 366–374