Chuanqi Zhang

https://chuanqizhang.com

Education

University of Technology Sydney — Sydney, Australia
Doctor of Philosophy — *Nov. 2021 – Present*
Supervisors: Prof. Youming Qiao, Prof. Mingsheng Ying and Prof. Troy Lee

University of Wisconsin-Madison — Madison, United States
Master of Arts in Mathematics — *Sep. 2018*[1] *– May. 2020*
Mentors: Prof. Sam Stechmann and Prof. Reed Ogrosky

Wuhan University — Wuhan, China
Bachelor of Science in Mathematics and Applied Mathematics — *Sep. 2015 – June. 2019*
Thesis Advisor: Prof. Huijiang Zhao

Research Interests

I have broad interests in mathematics and theoretical computer science. Specifically, I have been working on different algebraic structures, studying their connections and isomorphism problems with implications to quantum information theory, and designing corresponding algorithms and protocols for application in post-quantum cryptography.

Publications

Conference Proceedings

(C3) **Diffie–Hellman key exchange from commutativity to group laws** — ePrint: 2025/1677
with Dung Hoang Duong, and Youming Qiao
Accepted to *The 17th Innovations in Theoretical Computer Science (ITCS)*, 2026

(C2) **Faster isomorphism testing of p-Groups of Frattini class-2**
with Gábor Ivanyos, Euan Mendoza, Youming Qiao, and Xiaorui Sun
Published in *The 65th IEEE Annual Symposium on Foundations of Computer Science (FOCS)*, 2024

(C1) **On the complexity of isomorphism problems for tensors, groups, and polynomials III: actions by classical groups** — arXiv: 2306.03135
with Zhili Chen, Joshua A. Grochow, Youming Qiao, and Gang Tang
Published in *The 15th Innovations in Theoretical Computer Science (ITCS)*, 2024

Journal Articles

(J3) **Faster isomorphism testing of p-Groups of Frattini class-2**
with Gábor Ivanyos, Euan Mendoza, Youming Qiao, and Xiaorui Sun
Accepted to *SIAM Journal on Computing*, 2025

[1] I was admitted to a '3+2' accelerated program, which allows students to pursue their bachelor's degree and master's degree simultaneously after three years of undergraduate study.

(J2) **On linear-algebraic notions of expansion** arXiv: 2212.13154
with Yinan Li, Youming Qiao, Avi Wigderson, and Yuval Wigderson
Published in *Theory of Computing*, 2025

(J1) **Connections between graphs and matrix spaces** arXiv: 2206.04815
with Yinan Li, Youming Qiao, Avi Wigderson, and Yuval Wigderson
Published in *Israel Journal of Mathematics*, 2023

Preprints

(P2) **Schnorr Blind Signatures and Signed ElGamal KEM in Algebraic Group Action Model**
with Dung Hoang Duong, and Willy Susilo
Submitted.

(P1) **Blind signatures from cryptographic group actions** ePrint: 2025/397
with Dung Hoang Duong, Xuan Thanh Khuc, Youming Qiao, and Willy Susilo
Submitted.

Academic Visits

1. Institute of Cybersecurity and Cryptology (IC^2), University of Wollongong, hosted by Dr. Dung Hoang Duong, Dec. 19, 2025.
2. Department of Computer Sciences, University of Wisconsin-Madison, hosted by Prof. Sandeep Silwal, Nov. 1, 2024.
3. Department of Mathematics, University of Wisconsin-Madison, hosted by Prof. Tonghai Yang, Oct. 31, 2024.
4. School of Mathematics and Statistics, Wuhan University, hosted by Prof. Yinan Li, Jan. 12, 2024.
5. QuSoft, Centrum Wiskunde & Informatica, hosted by Dr. Jop Briët, Jan. 26-27, 2023.

Presentations[2]

1. Contributed talk at the 69th Annual Meeting of the Australian Mathematical Society, Melbourne, Dec. 9, 2025.
2. Invited talk at the 1st international workshop of Cryptography for Real-World Assets (affiliated with Asiacrypt 2025), Melbourne, Dec. 8, 2025.
3. Invited talk at the Theory of Computing Seminar, University of Wisconsin-Madison, Madison, Nov. 1, 2024.
4. Invited talk at the joint Number Theory/Representation Theory and Applied Algebra Seminar, University of Wisconsin-Madison, Madison, Oct. 31, 2024.
5. Invited talk at the SIAM Student Chapter Seminar, University of Wisconsin-Madison, Madison, Oct. 31, 2024.
6. Contributed talk at the 65th IEEE Annual Symposium on Foundations of Computer Science (FOCS), Chicago, Oct. 29, 2024.

7. Contributed talk at the 19th Theory of Quantum Computation, Communication and Cryptography (TQC), Okinawa, Sep. 10, 2024.
8. Invited talk at the Groups Analysis Geometry Seminar, University of Technology Sydney, Sydney, Apr. 18, 2024.
9. Contributed talk at the 45th Australasian Combinatorics Conference, Perth, Dec. 13, 2023.
10. Contributed talk at the 67th Annual Meeting of the Australian Mathematical Society, Brisbane, Dec. 6, 2023.
11. Poster presentation at the 18th Theory of Quantum Computation, Communication and Cryptography (TQC), online, Jul. 28, 2023.
12. Poster presentation at the 1st Quantum Australia Conference, Sydney, Feb. 22, 2023.
13. Invited talk at QuSoft Seminar, Centrum Wiskunde & Informatica, Amsterdam, Jan. 27, 2023.
14. Contributed talk at the 34th ACM-SIAM Symposium on Discrete Algorithms (SODA), Florence, Jan. 24, 2023.
15. Contributed talk at the 44th Australasian Combinatorics Conference, online, Dec. 12, 2022.

Honors and Awards

Distinguished Talk Award *2025*
Selective award at the Asiacrypt-affiliated workshop of Cryptography for Real-World Assets

SQA Supplementary Scholarship *2023 – 2025*
Top-up scholarship supported by Sydney Quantum Academy

AMSI Scholarship *2022*
Tuition waiver for summer school supported by Australian Mathematical Sciences Institute

ARC Discovery Project Scholarship *2021 – 2025*
Tax-free stipend supported by Australian Research Council

International Research Scholarship *2021 – 2025*
Tuition waiver supported by University of Technology Sydney

Special Scholarship for Studying Abroad *2018 & 2019*
One-off scholarship supported by Wuhan University

3rd/2nd Academic Excellence Award *2016 & 2017*
Annual academic excellence award in Mathematics Base Class at Wuhan University

3rd/2nd Provincial Mathematical Olympiad Prize *2014 & 2015*
29th/30th Chinese Mathematical Olympiad in Senior (Jilin Division)

[2] Some of the conference talks were delivered by co-authors.

Professional Services

Teaching Assistant *Session 2, 2024*
Theory of Computing Science (41080)
School of Computer Science, University of Technology Sydney

Teaching Assistant *Session 1, 2024*
Discrete Mathematics (37181)
School of Mathematical and Physical Sciences, University of Technology Sydney

Teaching Assistant *Session 1, 2024*
Mathematics 1 (33130)
School of Mathematical and Physical Sciences, University of Technology Sydney

Teaching Assistant *Session 2, 2023*
Theory of Computing Science (41080)
School of Computer Science, University of Technology Sydney

Teaching Assistant *Session 2, 2022*
Theory of Computing Science (41080)
School of Computer Science, University of Technology Sydney

Assignment Tutor & Grader *Spring 2020*
Methods of Applied Math II (Math 704)
Department of Mathematics, University of Wisconsin-Madison

Assignment Tutor & Grader *Fall 2019*
Analysis I (Math 521)
Department of Mathematics, University of Wisconsin-Madison

Conference Reviewer

❑ The 30th Australasian Conference on Information Security and Privacy (ACISP 2025)

❑ The 44th IARCS Annual Conference on Foundations of Software Technology and Theoretical Computer Science (FSTTCS 2024)

❑ The 35th ACM-SIAM Symposium on Discrete Algorithms (SODA 2024)

Undergraduate Research Mentor

❖ Honours student: Antonius Gunawan (2025), co-supervised under Prof. Youming Qiao

❖ Honours student: Euan Mendoza (2024), co-supervised under Prof. Youming Qiao

Research and Teaching Referees

Prof. Youming Qiao
Associate Professor
Centre for Quantum Software and Information
University of Technology Sydney
Youming.Qiao@uts.edu.au

Dr. Dung Hoang Duong
Senior Lecturer
School of Computing and Information Technology
University of Wollongong
hduong@uow.edu.au