

Chuanqi Zhang

<https://chuanqizhang.com>



EDUCATION

University of Technology Sydney

Doctor of Philosophy

Supervisors: Prof. Youming Qiao, Prof. Mingsheng Ying and Prof. Troy Lee

Sydney, Australia

Nov. 2021 – Nov. 2025

University of Wisconsin-Madison

Master of Arts in Mathematics

Mentors: Prof. Sam Stechmann and Prof. Reed Osgosky

Madison, United States

Sep. 2018¹ – May. 2020

Wuhan University

Bachelor of Science in Mathematics and Applied Mathematics

Thesis Advisor: Prof. Huijiang Zhao

Wuhan, China

Sep. 2015 – June. 2019

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

Published in *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

(J4) 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

Accepted to *Computational Complexity*, 2026

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.

(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

(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. Department of Computer Sciences, University of Wisconsin-Madison, hosted by Prof. Sandeep Silwal, Nov. 1, 2024.
2. Department of Mathematics, University of Wisconsin-Madison, hosted by Prof. Tonghai Yang, Oct. 31, 2024.
3. School of Mathematics and Statistics, Wuhan University, hosted by Prof. Yinan Li, Jan. 12, 2024.
4. QuSoft, Centrum Wiskunde & Informatica, hosted by Dr. Jop Briët, Jan. 26-27, 2023.

PRESENTATIONS²

1. Contributed talk at the 17th Innovations in Theoretical Computer Science Conference (ITCS), Milan, Jan. 30, 2026.
2. Contributed talk at the 69th Annual Meeting of the Australian Mathematical Society, Melbourne, Dec. 9, 2025.
3. Invited talk at the 1st international workshop of Cryptography for Real-World Assets (affiliated with Asiacrypt 2025), Melbourne, Dec. 8, 2025.
4. Invited talk at the Theory of Computing Seminar, University of Wisconsin-Madison, Madison, Nov. 1, 2024.
5. Invited talk at the joint Number Theory/Representation Theory and Applied Algebra Seminar, University of Wisconsin-Madison, Madison, Oct. 31, 2024.

6. Invited talk at the SIAM Student Chapter Seminar, University of Wisconsin-Madison, Madison, Oct. 31, 2024.
7. Contributed talk at the 65th IEEE Annual Symposium on Foundations of Computer Science (FOCS), Chicago, Oct. 29, 2024.
8. Contributed talk at the 19th Theory of Quantum Computation, Communication and Cryptography (TQC), Okinawa, Sep. 10, 2024.
9. Invited talk at the Groups Analysis Geometry Seminar, University of Technology Sydney, Sydney, Apr. 18, 2024.
10. Contributed talk at the 15th Innovations in Theoretical Computer Science Conference (ITCS), Berkeley, Feb. 2, 2024.
11. Contributed talk at the 45th Australasian Combinatorics Conference, Perth, Dec. 13, 2023.
12. Contributed talk at the 67th Annual Meeting of the Australian Mathematical Society, Brisbane, Dec. 6, 2023.
13. Poster presentation at the 18th Theory of Quantum Computation, Communication and Cryptography (TQC), online, Jul. 28, 2023.
14. Poster presentation at the 1st Quantum Australia Conference, Sydney, Feb. 22, 2023.
15. Invited talk at QuSoft Seminar, Centrum Wiskunde & Informatica, Amsterdam, Jan. 27, 2023.
16. Contributed talk at the 34th ACM-SIAM Symposium on Discrete Algorithms (SODA), Florence, Jan. 24, 2023.
17. 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
Ph.D. top-up scholarship supported by Sydney Quantum Academy	
AMSI Scholarship	2022
Summer school tuition waiver supported by Australian Mathematical Sciences Institute	
ARC Discovery Project Scholarship	2021 – 2025
Ph.D. tax-free stipend supported by Australian Research Council	
International Research Scholarship	2021 – 2025
Ph.D. 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	

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

PROFESSIONAL SERVICES

Teaching Assistant <i>Theory of Computing Science (41080)</i> School of Computer Science, University of Technology Sydney	Session 2, 2024
Teaching Assistant <i>Discrete Mathematics (37181)</i> School of Mathematical and Physical Sciences, University of Technology Sydney	Session 1, 2024
Teaching Assistant <i>Mathematics 1 (33130)</i> School of Mathematical and Physical Sciences, University of Technology Sydney	Session 1, 2024
Teaching Assistant <i>Theory of Computing Science (41080)</i> School of Computer Science, University of Technology Sydney	Session 2, 2023
Teaching Assistant <i>Theory of Computing Science (41080)</i> School of Computer Science, University of Technology Sydney	Session 2, 2022
Assignment Tutor & Grader <i>Methods of Applied Math II (Math 704)</i> Department of Mathematics, University of Wisconsin-Madison	Spring 2020
Assignment Tutor & Grader <i>Analysis I (Math 521)</i> Department of Mathematics, University of Wisconsin-Madison	Fall 2019
Conference Reviewer <input type="checkbox"/> The 30th Australasian Conference on Information Security and Privacy (ACISP 2025) <input type="checkbox"/> The 44th IARCS Annual Conference on Foundations of Software Technology and Theoretical Computer Science (FSTTCS 2024) <input type="checkbox"/> 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	