

Ziyi Guan

ziyi.guan@epfl.ch • ziyiguan.github.io

EDUCATION

Ph.D. in Computer Science, EPFL

Advisor: Alessandro Chiesa, Mika Göös

2021 – present

B.S. in Computer Science, Carnegie Mellon University

University Honors

2017 – 2020

B.S. in Mathematical Sciences, Carnegie Mellon University

University Honors

2017 – 2020

PUBLICATIONS

Authors are listed alphabetically (theoretical CS convention). My name is in **bold**.

Conference Publications

- [BCGM26] Sarah Bordage, Alessandro Chiesa, **Ziyi Guan**, and Ignacio Manzur. “All Polynomial Generators Preserve Distance with Mutual Correlated Agreement”. In: *Proceedings of the 41st Annual IEEE Conference on Computational Complexity*. CCC ’26. 2026.
- [CGKY26] Alessandro Chiesa, **Ziyi Guan**, Christian Knabenhans, and Zihan Yu. “On the Fiat–Shamir Security of Succinct Arguments from Functional Commitments”. In: *Proceedings of the 46th Annual International Cryptology Conference*. CRYPTO ’26. 2026.
- [Ale+25] Yaroslav Alekseev, Mika Göös, **Ziyi Guan**, Gilbert Maystre, Artur Riazanov, Weiqiang Yuan, and Dmitry Sokolov. “Generalised Linial-Nisan Conjecture is False for DNFs”. In: *Proceedings of the 40th Annual IEEE Conference on Computational Complexity*. CCC ’25. 2025.
- [BCG25] Annalisa Barbara, Alessandro Chiesa, and **Ziyi Guan**. “Relativized Succinct Arguments in the ROM Do Not Exist”. In: *Proceedings of the 23rd Theory of Cryptography Conference*. TCC ’25. 2025.
- [Chi+25] Alessandro Chiesa, Marcel Dall’Agnol, Zijing Di, **Ziyi Guan**, and Nicholas Spooner. “Quantum Rewinding for IOP-Based Succinct Arguments”. In: *Proceedings of the 23rd Theory of Cryptography Conference*. TCC ’25. 2025.
- [GRY25] **Ziyi Guan**, Artur Riazanov, and Weiqiang Yuan. “Breaking Verifiable Delay Functions in the Random Oracle Model”. In: *Proceedings of the 45th Annual International Cryptology Conference*. CRYPTO ’25. 2025.
- [Chi+24] Alessandro Chiesa, Marcel Dall’Agnol, **Ziyi Guan**, Nicholas Spooner, and Eylon Yogev. “On the Security of Succinct Interactive Arguments from Vector Commitments”. In: *Proceedings of the 22nd Theory of Cryptography Conference*. TCC ’24. 2024.
- [CGSY24] Alessandro Chiesa, **Ziyi Guan**, Shahar Samocha, and Eylon Yogev. “Security Bounds for Proof-Carrying Data from Straightline Extractors”. In: *Proceedings of the 22nd Theory of Cryptography Conference*. TCC ’24. 2024.
- [CGY24] Alessandro Chiesa, **Ziyi Guan**, and Burcu Yildiz. “On Parallel Repetition of PCPs”. In: *Proceedings of the 15th Innovations in Theoretical Computer Science Conference*. ITCS ’24. 2024, 34:1–34:14.
- [GHYY24] **Ziyi Guan**, Yunqi Huang, Penghui Yao, and Zekun Ye. “Quantum and Classical Communication Complexity of Permutation-Invariant Functions”. In: *Proceedings of the 41st Symposium on Theoretical Aspects of Computer Science*. STACS ’24. 2024, 39:1–39:19.

- [GGM23] Mika Göös, **Ziyi Guan**, and Tiberiu Mosnoi. “Depth-3 Circuits for Inner Product”. In: *Proceedings of the 48th International Symposium on Mathematical Foundations of Computer Science*. MFCS ’23. 2023.

Manuscripts & Preprints

- [Woo+26] David P. Woodruff et al. *Accelerating Scientific Research with Gemini: Case Studies and Common Techniques*. 2026. arXiv: [2602.03837](https://arxiv.org/abs/2602.03837) [cs.CL]. URL: <https://arxiv.org/abs/2602.03837>.
- [GY25] **Ziyi Guan** and Eylon Yogev. *SNARGs for NP via Fiat–Shamir in the Plain Model*. Cryptology ePrint Archive, Paper 2025/2328. 2025.
- [CDGS23] Alessandro Chiesa, Marcel Dall’Agnol, **Ziyi Guan**, and Nicholas Spooner. *On the Security of Succinct Interactive Arguments from Vector Commitments*. IACR Cryptology ePrint Archive, Report 2023/1646. 2023.
- [BCGL22] Jonathan Bootle, Alessandro Chiesa, **Ziyi Guan**, and Siqi Liu. *Linear-Time Probabilistic Proofs with Sublinear Verification for Algebraic Automata Over Every Field*. IACR Cryptology ePrint Archive, Report 2022/1056. 2022.

INVITED TALKS

On the Security of Succinct Arguments from Probabilistic Proofs

- Workshop on Zero-Knowledge, Succinct Proofs and Symmetric Cryptography, TU Vienna Feb 2026
- Security Seminar, Boston University Sep 2025
- CyLab Crypto Seminar, Carnegie Mellon University Aug 2025
- Aarhus University Jun 2025
- ETH Zurich May 2025

Relativized Succinct Arguments in the ROM Do Not Exist

- TCC 2025, Aarhus Dec 2025
- Swiss Crypto Day, EPFL Oct 2025
- ZKProof 7, Sofia Mar 2025

Breaking Verifiable Delay Functions in the Random Oracle Model

- Crypto & Security Seminar, New York University Sep 2025
- Cryptography and Information Security Seminar, MIT Sep 2025
- Theory Seminar, Cornell University Aug 2025
- Crypto 2025, UCSB Aug 2025
- NordiCrypt Summer 2025, Aarhus University Jun 2025

Quantum Rewinding for IOP-Based Succinct Arguments

- Paris ZK Day, ENS Jun 2025
- Workshop on the Mathematics of Post-Quantum Cryptography, University of Zurich Jun 2025
- Bocconi University May 2025

Untangling the Security of Kilian’s Protocol: Upper and Lower Bounds

- TCC 2024, Bocconi University Dec 2024

Security Bounds for Proof-Carrying Data from Straightline Extractors

- ZKProof 7, Sofia Mar 2025
- TCC 2024, Bocconi University Dec 2024

– Swiss Crypto Day 2024, University of St. Gallen	Sep 2024
– CrossFyre 2024 (affiliated event of Eurocrypt 2024), ETH Zurich	May 2024
– Crypto Seminar, Carnegie Mellon University	Mar 2024
<i>On the Security of Succinct Interactive Arguments from Vector Commitments</i>	
– Crypto Reading Group, New York University	Feb 2024
– CYS Research Seminar, King’s College London	Feb 2024
– Crypto Seminar, Bar-Ilan University	Jan 2024
<i>On Parallel Repetition of PCPs</i>	
– Algorithms and Complexity Seminar, University of Cambridge	Feb 2024
– Bocconi Seminar, Bocconi University	Jan 2024
– Theory Seminar, Nanjing University	Nov 2023
<i>Depth-3 Circuits for Inner Product</i>	
– MFCS 2023, Bordeaux INP	Aug 2023

TEACHING

EPFL

Co-instructor • Theory of Computation	Spring 2026
Head Teaching Assistant • Theory of Computation	Spring 2025
Head Teaching Assistant • Theory of Computation	Spring 2024
Teaching Assistant • Theory of Computation	Spring 2023
Teaching Assistant • Foundations of Probabilistic Proofs	Fall 2023
Teaching Assistant • Foundations of Probabilistic Proofs	Fall 2022
Teaching Assistant • Foundations of Probabilistic Proofs	Spring 2022

SLMath (formerly MSRI)

Teaching Assistant • Foundations and Frontiers of Probabilistic Proofs	Summer 2023
--	-------------

Carnegie Mellon University

Teaching Assistant • Great Ideas in Theoretical Computer Science	Fall 2020
Tutor • Great Ideas in Theoretical Computer Science	Spring 2020
Teaching Assistant • Continuous Time Finance	Spring 2020
Teaching Assistant • Discrete Time Finance	Fall 2019
Teaching Assistant • Integration and Approximation	Spring 2019

PROFESSIONAL SERVICE

Program Committee

Asiacrypt 2026

External Reviewer

Crypto 2026, Eurocrypt 2026, STOC 2026, LATINCRYPT 2025, TCC 2025, Crypto 2025, ICALP 2025, Eurocrypt 2025, QIP 2025, Eurocrypt 2024, TCC 2023, CCC 2023