

Quang Dao

Pittsburgh, PA

✉ qvd@andrew.cmu.edu

🌐 <https://quangvdao.github.io/>

🔗 [Google Scholar](#)

Last updated: June 2025

Education

- 2022–Present **Carnegie Mellon University, Pittsburgh, PA**
PhD in Computer Science. *Advisors:* Aayush Jain and Riad Wahby.
- 2020–2022 **University of Michigan, Ann Arbor, MI**
MA in Mathematics. *Advisor:* Paul Grubbs
- 2016–2020 **Columbia University, New York, NY**
BA in Mathematics and Computer Science

Research Interests

I work at the intersection of **cryptography** and **formal verification**. My goal is to build new verification tools for advanced cryptographic primitives, such as **succinct zero-knowledge proofs**, and to use these tools to verify the security of existing constructions. I also work on **post-quantum cryptography**, with a focus on building new primitives from code-based assumptions.

Publications

7. Carl Kwan, **Quang Dao**, Justin Thaler. Verifying Jolt zkVM Lookup Semantics. *Financial Cryptography 2025*.
6. **Quang Dao**, Aayush Jain. Lossy Cryptography from Code-Based Assumptions. *CRYPTO 2024. Best Paper from Early Career Researchers*.
5. **Quang Dao**, Aayush Jain, Zhengzhong Jin. Non-Interactive Zero-Knowledge from LPN and MQ. *CRYPTO 2024*.
4. **Quang Dao**, Yuval Ishai, Aayush Jain, Huijia Lin. Multi-party Homomorphic Secret Sharing and Sublinear MPC from Sparse LPN. *CRYPTO 2023*.
3. **Quang Dao**, Jim Miller, Opal Wright, Paul Grubbs. Weak Fiat-Shamir Attacks on Modern Proof Systems. *IEEE S&P 2023. Distinguished Paper Award*.
2. **Quang Dao**, Paul Grubbs. Spartan and Bulletproofs are simulation-extractable (for free!). *EUROCRYPT 2023*.
1. **Quang Dao**, Julian Wellman, Calvin Yost-Wolff, Sylvester W. Zhang. Rowmotion Orbits of Trapezoid Posets. *The Electronic Journal of Combinatorics*, P2-29, 2022.

Preprints

3. Suyash Bagad, **Quang Dao**, Yuval Domb, Justin Thaler. Speeding-Up Sum-Check Proving. *In submission*.
2. **Quang Dao**, Justin Thaler. Constraint-Packing and the Sum-Check Protocol over Binary Tower Fields. *ePrint 2024*.

1. **Quang Dao**, Christina Meng, Julian Wellman, Zixuan Xu, Calvin Yost-Wolff, Teresa Yu. Extended Nestohedra and their Face Numbers. *arXiv 2019*.

Grants & Fellowships

- 2025 **Ethereum Foundation Grant**
Grant for the formalization of the Binius Polynomial Commitment Scheme
Amount: \$24,000
- 2025 **Ethereum Foundation Grant**
Grant for the development of ArkLib, a Lean library for formally verifying SNARKs
Amount: \$100,000
- 2024-2025 **Quad Fellowship**
One-year fellowship for US-based PhD students in STEM fields
Amount: \$40,000
- 2024-2025 **CyLab Fellowship**
One-year fellowship from CyLab at Carnegie Mellon University
Amount: \$50,000

Honors & Awards

- 2024 **Best Paper from Early Career Researchers**
Awarded to the best paper from early career researchers at CRYPTO 2024
- 2023 **Distinguished Paper Award**
Awarded to top 6% of accepted papers at IEEE Security & Privacy 2023
- 2020 **Russell C. Mills Award**
Awarded to 2 seniors for excellence in computer science at Columbia
- 2017 - 2019 **Van Amringe Math Prize**
Awarded annually to the top 3 non-senior students in math at Columbia
- 2016, 2018 **Putnam Math Competition**. Honorable Mention (top 50)
- 2016 **International Math Olympiad**. Silver Medal

Internships & Visiting Positions

- Summer 2025 Part-Time Contractor with a16z crypto.
- Summer 2024 Research Intern at a16z crypto.

Talks

- 8. ArkLib: Compositional Verification of SNARKs
 - University of Luxembourg Crypto Seminar (July 2025)
 - CRYPTO Day, Telecom Paris (June 2025)
 - EPFL Crypto Seminar (June 2025)
 - CMU Formal Cookies (Oct 2024)

7. Lossy Cryptography from Code-Based Assumptions
 - MIT CIS Seminar (Nov 2024)
 - BUSEC Seminar (Nov 2024)
 - NYU Crypto Reading Group (Nov 2024)
 - CMU CyLab Crypto Seminar (Sep 2024)
 - UCLA Crypto Reading Group (Apr 2024)
 - UToronto Theory Seminar (Mar 2024)
6. Non-Interactive Zero-Knowledge from LPN and MQ
 - CMU CyLab Crypto Seminar (Sep 2024)
5. Advanced Security for SNARKs: A Survey
 - a16z Crypto Research Seminar (Jun 2024)
4. Multi-party Homomorphic Secret Sharing and Sublinear MPC from Sparse LPN
 - JP Morgan AlgoCRYPT Seminar (Dec 2023)
 - CMU Crypto Seminar (Nov 2023)
 - NTT Research Seminar (Oct 2023)
 - CyLab Partners Conference (Oct 2023)
 - Vietnam Mathematical Congress (Aug 2023)
3. Weak Fiat-Shamir Attacks on Modern Proof Systems
 - Real World Crypto (Mar 2024)
 - CMU CyLab Security Seminar (Nov 2023)
 - Cornell Security Seminar (Sep 2023)
 - NYU Crypto Reading Group (Sep 2023)
 - Workshop on Attacks in Cryptography (Aug 2023)
2. Spartan and Bulletproofs are simulation-extractable (for free!)
 - Stanford Crypto Reading Group (May 2023)
 - Telecom Paris Seminar (May 2023)
 - Lattices Meet Hashes Workshop, EPFL (May 2023)
 - CMU Crypto Seminar (April 2023)

Service

Co-Organizer 2022-2025: CMU Crypto Seminar
 External 2025: EUROCRYPT, IEEE S&P, CRYPTO, RANDOM
 Reviewer 2024: STOC, EUROCRYPT, TCC
 2023: ASIACRYPT, TCC, FOCS
 2022: CRYPTO, EUROCRYPT

Teaching

2023-2025 **Western Pennsylvania ARML Team**, *Assistant Coach*, CMU
 Fall 2023 **Undergraduate Quantum Computation**, *Teaching Assistant*, CMU
 2020–2021 **Calculus I**, *Lead Instructor*, University of Michigan
 2017, 2021 **Math & Science Summer Program (MASSP)**, *Mentor*, Vietnam

Mentorship

Summer 2025 **Undergraduate**, *Ian Martin*
 Spring 2025 **Undergraduate**, *Liam Schilling, Jack Zhu, Christian Ang*

———— Miscellaneous

Languages English (fluent), Vietnamese (native), French (elementary), Malayalam (elementary)