Pittsburgh, PA
✉ *qvd@andrew.cmu.edu*
https://quangvdao.github.io/
Last updated: October 2023

Quang Dao

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 am interested in theoretical and applied cryptography, with a focus on **post-quantum cryptography**, **secure computation**, and **zero-knowledge proof systems**.

Publications

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.

Talks

4. Multi-party Homomorphic Secret Sharing and Sublinear MPC from Sparse LPN
   - 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
   - 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	2022-2023: CMU Crypto Seminar
External Reviewer	2023: ASIACRYPT, TCC, FOCS 2022: CRYPTO, EUROCRYPT

Teaching

Fall 2023	**Undergraduate Quantum Computation**, *Teaching Assistant*, CMU.
2020–2021	**Calculus I**, *Lead Instructor*, University of Michigan.

Honors & Awards

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	**International Math Olympiad**. Silver Medal

Miscellaneous

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