Quang Dao

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

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

Publications

3. **Quang Dao**, Jim Miller, Opal Wright, Paul Grubbs. Weak Fiat-Shamir Attacks on Modern Proof Systems. *IEEE S&P 2023*.
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

May 2023	Stanford Reading Group
May 2023	Telecom Paris Seminar
May 2023	Lattices Meet Hashes Workshop, EPFL
April 2023	CMU Crypto Seminar

Service

External Reviewer FOCS 2023, CRYPTO 2022, EUROCRYPT 2022

Teaching

2020–2021 **Math 115**, *University of Michigan*, Ann Arbor, MI.

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)