# Luowen Qian

Website: https://cs-people.bu.edu/luowenq

## Research Interests

I am broadly interested in quantum computation and cryptography, as well as their connections to other fields in theoretical computer science in general.

## Publications

P. Ananth, A. Gulati, L. Qian, H. Yuen. Pseudorandom (Function-Like) Quantum State Generators: New Definitions and Applications.
To appear in TCC 2022.

P. Ananth, L. Qian, H. Yuen. Cryptography from Pseudorandom Quantum States.
CRYPTO 2022.

J. Liu, Q. Liu, L. Qian. Beating Classical Impossibility of Position Verification.
ITCS 2022.

KM. Chung, S. Guo, Q. Liu, L. Qian. Tight Quantum Time-Space Tradeoffs for Function Inversion.
FOCS 2020.

KM. Chung, TN. Liao, L. Qian. Lower Bounds for Function Inversion with Quantum Advice.
ITC 2020.

KM. Chung, L. Qian. Adaptively Secure Garbling Schemes for Parallel Computations.
TCC 2019.

## Talks & Posters

On the computational hardness needed for quantum cryptography
Invited to Third Kyoto Workshop on Quantum Information, Computation, and Foundations (October 2022); MIT Cryptography and Information Security seminar (September 30, 2022); CRYPTO 2022 Rump Session (August 16, 2022)

Cryptography from Pseudorandom Quantum States
QCrypt 2022 (August 29, 2022); CRYPTO 2022 (August 15, 2022); UC Berkeley Theory CS Seminar (January 11, 2022)

Beating Classical Impossibility of Position Verification
QIP 2022 (March 10, 2022); Ottawa QUASAR seminar (March 4, 2022); ITCS 2022 (February 2, 2022); Charles River Crypto Day (November 19, 2021); BUsec Seminar (September 29, 2021)

Tight Quantum Time-Space Tradeoffs for Function Inversion
BU Algorithms and Theory Seminar (April 5, 2021)

Lower Bounds for Function Inversion with Quantum Advice
ITC 2020 (June 17, 2020), QIP 2020 (poster)

Adaptively Secure Garbling Schemes for Parallel Computations
TCC 2019 (December 4, 2019), NY CryptoDay (October 18, 2019)

## Honors & Awards

| | |
|---|---|
| Jan 2016 | Honorable Mention in Mathematical Contest in Modeling |
| Oct 2021 | Google Security Rewards ($2,000) for reporting a Moderate severity vulnerability via a bug report and proof of concept (CVE-2021-0980) Fixed in Android 13 via FGS Task Manager |

## Education

| | |
|---|---|
| Sep 2019 | **Boston University** |
| - | Ph.D. student in Computer Science |
| | Advisor: Ran Canetti |
| Sep 2015 | **Nanjing University**, China |
| - Jun 2019 | Bachelor of Science in Computer Science |
| | GPA: 4.31/5 |

## Teaching

BU CS 538: Fundamentals of Cryptography (Spring 2022), Teaching Fellow
BU CS 332: Theory of Computation (Fall 2020), Teaching Fellow