Luowen Qian

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

Education

Sep 2019 - **Boston University**
Ph.D. student in Computer Science
Advisor: Ran Canetti

Sep 2015 - Jun 2019 **Nanjing University**, China
Bachelor of Science in Computer Science

Publications

W. Kretschmer, L. Qian, M. Sinha, A. Tal. Quantum Cryptography in Algorithmica.
STOC 2023.

Z. Brakerski, R. Canetti, L. Qian. On the computational hardness needed for quantum cryptography.
ITCS 2023.

P. Ananth, KM. Chung, X. Fan, L. Qian. Collusion-Resistant Functional Encryption for RAMs.
ASIACRYPT 2022.

J. Liu, Q. Liu, L. Qian, M. Zhandry. Collusion-Resistant Copy-Protection for Watermarkable Functionalities.
TCC 2022.

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

Quantum Cryptography in Algorithmica
STOC 2023 (June 23, 2023); A special crypto day in honor of Ran Canetti on the occasion of his 60th birthday (May 12, 2023)

Quantum pseudorandomness in Algorithmica, and its implications to cryptography and complexity
Minimal Complexity Assumptions for Cryptography workshop @ Simons Institute (May 5, 2023)

Cryptography from Quantum Pseudorandomness
IQC Math and CS Seminar (March 9, 2023)

On the computational hardness needed for quantum cryptography
ITCS 2023 (January 12, 2023); QCW 2022; Invited to Third Kyoto Workshop on Quantum Information, Computation, and Foundations (October 18, 2022); MIT Cryptography and Information Security seminar (September 30, 2022); CRYPTO 2022 Rump Session (August 16, 2022)

Collusion Resistant Copy-Protection for Watermarkable Functionalities
QCrypt 2022 (joint poster)

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

Beating Classical Impossibility of Position Verification
QIP 2022 contributed talk (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)

Teaching

Three guest lectures for GRS PY 896 (Spring 2023): Special Topics Seminar in Theoretical Physics.
Quantum cryptography: from encryption to black hole paradoxes
CAS CS 538: Fundamentals of Cryptography (Spring 2023), Teaching Fellow
→ Two lectures on pseudorandom generators
BU CS 538: Fundamentals of Cryptography (Spring 2022), Teaching Fellow
→ Guest lecture on quantum & cryptography
BU CS 332: Theory of Computation (Fall 2020), Teaching Fellow

Honors & Awards

2024 - "An efficient quantum parallel repetition theorem and applications"
Selected as a Short Plenary Talk at QIP 2024
- "Unitary Complexity and the Uhlmann Transformation Problem"
Selected as a Long Plenary Talk at QIP 2024

2023 - "Quantum Cryptography in Algorithmica"
Invited to QCrypt 2023
- "Pseudorandom Quantum States, Revisited: New Properties, Variants, Constructions and Cryptographic Applications"
Selected as a Short Plenary Talk at QIP 2023

2022 - Funded by BU Hariri Institute Focused Research Program
- 2024 "Quantum Convergence" beginning 2022

2021 - "Tight Quantum Time-Space Tradeoffs for Function Inversion"
Invited Keynote at TQC 2021
- Google Security Rewards ($2,000) for reporting a Moderate severity vulnerability via a bug report and proof of concept (CVE-2021-0980)

2016 - Honorable Mention in *Mathematical Contest in Modeling*