Jiaxin Guan

Assistant Professor / Faculty Fellow, New York University

251 Mercer Street • New York, NY 10012, USA
(650) 796-1302 • jiaxin@guan.io

Education

- **Princeton University** **Princeton, NJ**
  PhD in Computer Science *09/17 – 07/23*
  M.A. in Computer Science *09/17 – 09/19*
  - Research Area: Cryptography
  - Advisor: Mark Zhandry
- **Stanford University** **Stanford, CA**
  M.S. in Computer Science *01/16 – 06/17*
  B.S. with Honors in Computer Science (Theory Track) *09/13 – 06/17*

Academic Interests

Information-Theoretic Cryptography, Space-Bounded Cryptography, Post-Quantum Cryptography, Lower Bounds, Other Areas of Cryptography, and Theoretical Computer Science in General

Publications

1. Pratish Datta, Jiaxin Guan, Alexis Korb, and Amit Sahai, "**(Multi-Input) FE for Randomized Functionalities, Revisited**", Preprint
2. Jiaxin Guan and Hart Montgomery, "**On Sequential Functions and Fine-Grained Cryptography**", CRYPTO 2024
3. Yevgeniy Dodis, Jiaxin Guan, Peter Hall, and Allison Lin, "**HELP: Everlasting Privacy through Server-Aided Randomness**", Preprint
4. Pratish Datta, Jiaxin Guan, Alexis Korb, and Amit Sahai, "**Adaptively Secure Streaming Functional Encryption**", Preprint
5. Jiaxin Guan, Daniel Wichs, and Mark Zhandry, "**Somewhere Randomness Extraction and Security against Bounded-Storage Mass Surveillance**", TCC 2023
6. Jiaxin Guan, Alexis Korb, and Amit Sahai, "**Streaming Functional Encryption**", CRYPTO 2023
7. Dan Boneh, Jiaxin Guan, and Mark Zhandry, "**A Lower Bound on the Length of Signatures based on Group Actions and Generic Isogenies**", EUROCRYPT 2023
8. Jiaxin Guan, Daniel Wichs, and Mark Zhandry, "**Incompressible Cryptography**", EUROCRYPT 2022
9. Jiaxin Guan and Mark Zhandry, "**Iterated Inhomogeneous Polynomials**", CFail 2021
10. Jiaxin Guan and Mark Zhandry, "**Disappearing Cryptography in the Bounded Storage Model**", TCC 2021

11. Jiaxin Guan and Mark Zhandry, "**Simple Schemes in the Bounded Storage Model**", EUROCRYPT 2019
12. James Bartusek, Jiaxin Guan, Fermi Ma, and Mark Zhandry, "**Return of GGH15: Provable Security Against Zeroizing Attacks**", TCC 2018

Talks

1. On Sequential Functions and Fine-Grained Cryptography
   - CRYPTO 2024 Conference Talk (August 2024)
2. Multi-Instance Randomness Extraction and Security against Bounded-Storage Mass Surveillance
   - ITC 2024 Highlights Track (August 2024)
   - SJTU John Hopcroft Center Lecture Series (January 2024)
   - NYU Crypto Reading Group (December 2023)
   - TCC 2023 Conference Talk (December 2023)
3. A Lower Bound on the Length of Signatures based on Group Actions and Generic Isogenies
   - EUROCRYPT 2023 Conference Talk (April 2023)
   - CMU CyLab Crypto Seminar (April 2023)
   - Texas Crypto Day (April 2023)
4. Incompressible Cryptography
   - NTT Research (July 2022)
   - EUROCRYPT 2022 Conference Talk (May 2022)
   - UCLA Crypto Reading Group (April 2022)
   - CMU CyLab Crypto Seminar (April 2022)
   - Stanford Security Seminar (March 2022)
5. Disappearing Cryptography and Incompressible Cryptography
   - NYU Crypto Reading Group (January 2022)
   - TCC 2021 In-Person Workshop Talk (November 2021)
6. Disappearing Cryptography in the Bounded Storage Model
   - TCC 2021 Conference Talk (November 2021)
7. Iterated Inhomogeneous Polynomials
   - CFail 2021 Workshop, a CRYPTO 2021 Affiliated Event (August 2021)
8. Simple Schemes in the Bounded Storage Model
   - EUROCRYPT 2019 Conference Talk (May 2019)
   - Princeton General Exam (May 2019)

Professional Activities

Program Committee:

CRYPTO 25

Conference Reviews:

CRYPTO 18, **EUROCRYPT** 22, 23, **TCC** 21, 22, 23, 24, **ASIACRYPT** 19, 20
STOC 22, **ITCS** 21, 24, **CCC** 24

Teaching Experience

- Instructor: CSCI-UA.0310-005, Basic Algorithms, New York University, Spring 2025
- Instructor: CSCI-UA.0310-007, Basic Algorithms, New York University, Fall 2024
- Instructor: CSCI-UA.0310-005, Basic Algorithms, New York University, Spring 2024
- Instructor: CSCI-UA.0310-007, Basic Algorithms, New York University, Fall 2023
- Assistant in Instruction: COS 533, Advanced Cryptography, Princeton University, Spring 2021
- Assistant in Instruction: COS 433, Cryptography, Princeton University, Spring2020
- Assistant in Instruction: COS 445, Economics and Computation, Princeton University, Spring 2019
- Assistant in Instruction: COS 432, Information Security, Princeton University, Fall 2018
- Teacher's Assistant: CS 155, Computer and Network Security, Stanford University, Spring 2017

Work Experience

- **New York University** **New York, NY**
  Assistant Professor / Faculty Fellow *09/23 – Present*
  - Teaching the undergraduate algorithms course and conducting research on various areas of cryptography.
- **NTT Research, Inc.** **Sunnyvale, CA**
  Research Intern *10/19 – 05/20, 09/20 – 05/21*
  - Conducted research on Incompressible Cryptography and various topics of cryptography.
- **Fujitsu Laboratories of America, Inc.** **Sunnyvale, CA**
  Research Intern *05/20 – 08/20*
  - Conducted research on Memory Hard Functions.
- **Keybase Inc.** **San Francisco, CA**
  Software Engineering Intern *07/16 – 09/16*
  - Implemented a keyword search scheme for encrypted data on Keybase File System.
- **Computer Science Department, Stanford University** **Stanford, CA**
  Senior Section Leader *01/14 – 03/16*
  - Held weekly sections for 10-12 students learning intro programming in Java and C++.
  - Led 3-hr helper sessions twice a week to assist students with assignments.
  - Graded the assignments and exams, and provided feedbacks for students.

- **Google Inc.** **New York, NY**
  Software Engineering Intern *06/15 – 09/15*
  - Worked on the Technical Infrastructure team to provide user data protection.
  - Implemented tools to provide health analysis feedbacks for security policies.

Skills

Languages: Native in Mandarin, Fluent in English, Intermediate German, Cantonese and Sanskrit
Programming: C++, C, Go, Ruby, JavaScript, Java, HTML, CSS, Python, SQL