

Jiabin Guan

Applied Cryptographer, Zellic

(650) 796-1302 • jiabin@guan.io • www.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, Functional Encryption, Coding Theory, Time-Space Lower Bounds, Complexity, Meta-Complexity, Other Areas of Cryptography and Theoretical Computer Science in General

Publications

1. Jiabin Guan and Daniel Wichs, "**Streaming One-Time Programs in the Bounded Storage Model**", In Preparation
2. Marshall Ball and Jiabin Guan, "**A Complexity Theoretic Approach to Proofs of Space**", In Preparation
3. Pratish Datta, Jiabin Guan, Alexis Korb, and Amit Sahai, "**(Multi-Input) FE for Randomized Functionalities, Revisited**", TCC 2025
4. Pratish Datta, Jiabin Guan, Alexis Korb, and Amit Sahai, "**Adaptively Secure Streaming Functional Encryption**", TCC 2025
5. Yevgeniy Dodis, Jiabin Guan, Peter Hall, and Alison Lin, "**HELP: Everlasting Privacy through Server-Aided Randomness**", IACR CiC Volume 1 (2024), Issue 4
6. Jiabin Guan and Hart Montgomery, "**On Sequential Functions and Fine-Grained Cryptography**", CRYPTO 2024
7. Jiabin Guan, Daniel Wichs, and Mark Zhandry, "**Multi-Instance Randomness Extraction and Security against Bounded-Storage Mass Surveillance**", TCC 2023
8. Jiabin Guan, Alexis Korb, and Amit Sahai, "**Streaming Functional Encryption**", CRYPTO 2023
9. Dan Boneh, Jiabin Guan, and Mark Zhandry, "**A Lower Bound on the Length of Signatures based on Group Actions and Generic Isogenies**", EUROCRYPT 2023
10. Jiabin Guan, Daniel Wichs, and Mark Zhandry, "**Incompressible Cryptography**", EUROCRYPT 2022

11. Jiaxin Guan and Mark Zhandry, "**Iterated Inhomogeneous Polynomials**", CFail 2021
 12. Jiaxin Guan and Mark Zhandry, "**Disappearing Cryptography in the Bounded Storage Model**", TCC 2021
 13. Jiaxin Guan and Mark Zhandry, "**Simple Schemes in the Bounded Storage Model**", EUROCRYPT 2019
 14. James Bartusek, Jiaxin Guan, Fermi Ma, and Mark Zhandry, "**Return of GGH15: Provable Security Against Zeroizing Attacks**", TCC 2018
-

Talks

1. Space Jammed: Cryptography against Space-Bounded Adversaries
 - National University of Singapore (March 2025)
 - New Jersey Institute of Technology (March 2025)
 - Queens College Q4C Colloquium (December 2024)
2. On Sequential Functions and Fine-Grained Cryptography
 - CRYPTO 2024 Conference Talk (August 2024)
3. 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)
4. 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)
5. 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)
6. Disappearing Cryptography and Incompressible Cryptography
 - NYU Crypto Reading Group (January 2022)
 - TCC 2021 In-Person Workshop Talk (November 2021)
7. Disappearing Cryptography in the Bounded Storage Model
 - TCC 2021 Conference Talk (November 2021)
8. Iterated Inhomogeneous Polynomials
 - CFail 2021 Workshop, a CRYPTO 2021 Affiliated Event (August 2021)
9. Simple Schemes in the Bounded Storage Model

- EUROCRYPT 2019 Conference Talk (May 2019)
 - Princeton General Exam (May 2019)
-

Professional Activities

Program Committee:

CRYPTO 25, IACR CiC 25

Conference Reviews:

CRYPTO 18, EUROCRYPT 22, 23, TCC 21, 22, 23, 24, 25 ASIACRYPT 19, 20, 25
STOC 22, ITCS 21, 25, CCC 24, RANDOM 25

Teaching Experience

New York University:

- Instructor: CSCI-UA.0310-005, Basic Algorithms, Spring 2025
- Instructor: CSCI-UA.0310-007, Basic Algorithms, Fall 2024
- Instructor: CSCI-UA.0310-005, Basic Algorithms, Spring 2024
- Instructor: CSCI-UA.0310-007, Basic Algorithms, Fall 2023

Princeton University:

- Assistant in Instruction: COS 533, Advanced Cryptography, Spring 2021
- Assistant in Instruction: COS 433, Cryptography, Spring 2020
- Assistant in Instruction: COS 445, Economics and Computation, Spring 2019
- Assistant in Instruction: COS 432, Information Security, Fall 2018

Stanford University:

- Teacher's Assistant: CS 155, Computer and Network Security, Spring 2017
 - Senior Section Leader: CS 106B, Programming Abstractions, Winter 2016
 - Senior Section Leader: CS 106X, Programming Abstractions (Accelerated), Fall 2015
 - Senior Section Leader: CS 106B, Programming Abstractions, Spring 2015
 - Senior Section Leader: CS 106X, Programming Abstractions (Accelerated), Winter 2015
 - Senior Section Leader: CS 106X, Programming Abstractions (Accelerated), Fall 2014
 - Section Leader: CS 106B, Programming Abstractions, Spring 2014
 - Section Leader: CS 106A, Programming Methodology, Winter 2013
-

Work Experience

- **Zellic** **New York, NY**
Applied Cryptographer *06/25 – Present*
 - Audit and research cutting-edge cryptographic protocols and blockchain systems.
 - **New York University** **New York, NY**
Assistant Professor / Faculty Fellow *09/23 – 06/25*
 - Taught the undergraduate algorithms course and conducted 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.
 - **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, Python, Rust, JavaScript (Node.js, React), TypeScript, HTML, CSS, Java, SQL