

Cody Freitag

Postdoctoral Researcher
codyrfreitag@gmail.com

Research Interests

My research primarily focuses on cryptography with an emphasis on cryptographic proofs and their applications to distributed computing.

Postdoctoral Appointments

Hebrew University of Jerusalem	Sep. 2025 – Present
• Host: Ilan Komargodski	
Northeastern University	Sep. 2023 – Present
• Host: Daniel Wichs	
Boston University	June 2023 – Aug. 2023
• Host: Ran Canetti	

Education

Cornell University	Aug. 2017 – May 2023
• PhD in Computer Science	
• MS in Computer Science	
• Dissertation: <i>How to Provably Leverage Time in Cryptography</i>	
• Advisor: Rafael Pass	
The University of Texas at Austin	Aug. 2013 – May 2017
• BS in Computer Science, Turing Scholars Honors	
• BS in Mathematics, Dean's Scholars Honors	
• Thesis: <i>Testing and Searching Pattern Avoiding Sequences</i>	
• Advisor: Eric Price	

Research Internships

NTT Research	Fall 2021 – Spring 2022
• Host: Ilan Komargodski	
Rutgers University, DIMACS REU	Summer 2016
• Host: Muthu Muthukrishnan	
University of Maryland, REU CAAR	Summer 2015
• Host: Jonathan Katz	

Industry Experience

Consultant	2016 – 2018
<ul style="list-style-type: none">• Consulted for Yeletech Security and Bolt Labs focusing on blockchain technologies• Developed software for attribute-based encryption technology for Zeutro	
Bloomberg LP, Software R&D Intern	Summer 2014
L-3 Communications, Software Engineering Intern	Summer 2013

Honors and Awards

• Khoury College Distinguished Postdoctoral Fellowship	Sep. 2023 – Aug. 2025
• NSF Graduate Research Fellowship	June 2019 – May 2021, June 2022 – May 2023
• Cornell University Fellowship	Fall 2017 – Spring 2018
• UT Computer Science Best Undergraduate Thesis Award	Spring 2017
• UT Unrestricted Endowed Presidential Scholarship	Fall 2016 – Spring 2017
• UT CNS Distinguished College Scholar	Fall 2014 – Spring 2017

Teaching

Teaching Assistant, Cornell	
• Networks and Markets (Rafael Pass)	Sp 19, F 19, F 20, Sp 21
Undergraduate Teaching Assistant, UT Austin	
• Algorithms and Complexity (Vijaya Ramachandran)	Spring 2016
• Discrete Mathematics (William Bulko)	Spring 2016
• Honors Discrete Mathematics (İşıl Dillig)	Fall 2015
• Computer Fluency (Nathan Clement)	Fall 2014, Spring 2015

Service

• Program committee member for Crypto 2024, TCC 2025, TCC 2026	
• Subreviewer for various conferences including STOC, FOCS, SODA, Crypto, Eurocrypt, TCC, Asiacrypt, ITCS, ICALP, PKC, SCN, DISC, SOSA	
• TA for New Horizons in TCS online summer school	2021
• Section leader for Stanford's online Code In Place course	2020
• Co-organizer of Cornell Cryptography Seminar	2018 – 2021
• Cornell CS PhD admissions committee	2020
• Volunteer for Cornell CS PhD admissions committee	2018, 2019
• Cornell CS visit day leader	2019

Publications

Conference Papers

- **Crypto 2026** *Unique SNARGs with Adaptive Security: Constructions and Black-Box Separations*
Cody Freitag, Daniel Wichs
- **ITCS 2026** *Improved Rate for Non-Malleable Codes and Time-Lock Puzzles*
Cody Freitag, Manu Kondapaneni, Ilan Komargodski, Jad Silbak
- **TCC 2025** *Seedless Condensers for Efficiently Samplable Sources*
Cody Freitag, Jad Silbak, Daniel Wichs
- **STOC 2025** *Unambiguous SNARGs for P from LWE with Applications to $PPAD$ Hardness*
Liyen Chen, Cody Freitag, Zhengzhong Jin, Daniel Wichs
- **Eurocrypt 2024** *Public-Coin, Complexity-Preserving, Succinct Arguments of Knowledge for NP from Collision-Resistance*
Cody Freitag, Omer Paneth, Rafael Pass
- **CCS 2023** *Riggs: Decentralized Sealed-Bid Auctions*
Nirvan Tyagi, Arasu Arun, Cody Freitag, Riad Wahby, Joseph Bonneau, David Mazières
- **Crypto 2023** *How to Use (Plain) Witness Encryption: Registered ABE, Flexible Broadcast, and More*
Cody Freitag, Brent Waters, David J. Wu
- **ITC 2023** *The Cost of Statistical Security in Proofs for Repeated Squaring*
Cody Freitag, Ilan Komargodski
- **Eurocrypt 2023** *Optimal Security for Keyed Hash Functions: Avoiding Time-Space Tradeoffs*
Cody Freitag, Ashrujit Ghoshal, Ilan Komargodski
- **TCC 2022** *Parallelizable Delegation from LWE*
Cody Freitag, Rafael Pass, Naomi Sirkin
- **TCC 2022** *Cosmic Security: Security Relative to Stateful Natures*
Benjamin Chan, Cody Freitag, Rafael Pass
- **Crypto 2022** *Time-Space Tradeoffs for Sponge Hashing: Attacks and Limitations for Short Collisions*
Cody Freitag, Ashrujit Ghoshal, Ilan Komargodski
- **TCC 2021** *Non-Malleable Time-Lock Puzzles and Applications*
Cody Freitag, Ilan Komargodski, Rafael Pass, Naomi Sirkin
- **SCN 2020** *Impossibility of Strong KDM Security with Auxiliary Input*
Cody Freitag, Ilan Komargodski, Rafael Pass
- **Eurocrypt 2020** *SPARKs: Succinct Parallelizable Arguments of Knowledge*
Cody Freitag, Ilan Komargodski, Rafael Pass, Naomi Sirkin
- **Eurocrypt 2020** *Continuous Verifiable Delay Functions*

Cody Freitag, Ilan Komargodski, Rafael Pass, Naomi Sirkin

- **Crypto 2019** *Non-uniformly Sound Certificates with Applications to Concurrent Zero-Knowledge*
Cody Freitag, Ilan Komargodski, Rafael Pass
- **AISTATS 2019** *Test without Trust: Optimal Locally Private Distribution Testing*
Jayadev Acharya, Clément L. Canonne, Cody Freitag, Himanshu Tyagi
- **RANDOM 2017** *Testing Hereditary Properties of Sequences*
Cody Freitag, Eric Price, and William Swartheworth
- **ACNS 2017** *Signature Schemes with Randomized Verification*
Cody Freitag, Rishab Goyal, Susan Hohenberger, Venkata Koppula, Eysa Lee, Tatsuaki Okamoto, Jordan Tran, and Brent Waters
- **CSCML 2017** *Symmetric-Key Broadcast Encryption: The Multi-Sender Case*
Cody Freitag, Nathan Klein, and Jonathan Katz

Journal Papers

- **Journal of Cryptology 2025** *Time-Space Tradeoffs for Sponge Hashing: Attacks and Limitations for Short Collisions*
Cody Freitag, Ashrujit Ghoshal, Ilan Komargodski
- **Journal of the ACM 2022** *SPARKs: Succinct Parallelizable Arguments of Knowledge*
Cody Freitag, Ilan Komargodski, Rafael Pass, Naomi Sirkin
- **IEEE Journal on Special Areas in Information Theory: Privacy and Security of Information Systems 2021** *Inference under Information Constraints III: Local Privacy Constraints*
Jayadev Acharya, Clément L. Canonne, Cody Freitag, Ziteng Sun, Himanshu Tyagi
- **Polyhedron 2014** *Modeling of Late 3d Transition Metal Metathesis of tert-Butoxide Complexes with Amines*
Cody Freitag, Francisco Birk, William Ou, and Thomas Cundari
- **Journal of the American Chemical Society 2012** *Variable Pathways for Oxygen Atom Insertion into Metal-Carbon Bonds: The Case of $Cp^*W(O)_2(CH_2SiMe_3)$*
Jiajun Mei, Kurtis Carsch, Cody Freitag, T. Brent Gunnoe, and Thomas Cundari

Other Manuscripts

- **PhD Dissertation 2023** *How to Provably Leverage Time in Cryptography*
Cody Freitag (advised by Rafael Pass)
- **Undergraduate Thesis 2017** *Testing and Searching Pattern Avoiding Sequences*
Cody Freitag (advised by Eric Price)

Presentations

Improved Rate for Non-Malleable Codes and Time-Lock Puzzles

- Talk at ITCS 2026 Conference Jan. 2026

Seedless Condensers for Efficiently Samplable Sources

- Talk at TCC 2025 Conference Dec. 2025

Unambiguous SNARGs for P from LWE with Applications to $PPAD$ Hardness

- Talk at Charles River Crypto Day Apr. 2025
- Talk at University of Washington Cryptography Reading Group Feb. 2025

Public-Coin, Complexity-Preserving, Succinct Arguments for NP from Collision-Resistance

- Talk at Eurocrypt 2024 Conference May 2024
- Talk at MIT Cryptography and Information Seminar Dec. 2023

How to Use (Plain) Witness Encryption: Registered ABE, Flexible Broadcast, and More

- Talk at Crypto 2023 Conference Aug. 2023
- Talk at Boston University Security Seminar June 2023

How to Provably Leverage Time in Cryptography

- PhD Thesis Defense Apr. 2023

Cosmic Security: Universal Reductions Relative to a Stateful Oracle

- Talk at Boston University Security Seminar Dec. 2022

Parallelizable Delegation from LWE

- Talk at TCC 2022 Conference Nov. 2022

The Cost of Statistical Security in Proofs for Repeated Squaring

- Talk at ITC 2023 Conference June 2023
- Talk at UT Austin Crypto Reading Group Oct. 2022
- Talk at MIT Cryptography and Information Seminar Sept. 2022
- Talk at Cornell Theory Seminar Sept. 2022
- Talk at NYU Crypto Reading Group Sept. 2022

SPARKs: Succinct Parallelizable Arguments of Knowledge

- Talk at Eurocrypt 2020 Conference May 2020
- Talk at Bar Ilan University Cyber Center Colloquium May 2020
- Talk at Boston University Security Seminar May 2020

Non-Uniformly Sound Certificates with Applications to Concurrent Zero-Knowledge

- Talk at Crypto 2019 Conference Aug. 2019
- Talk at Cornell Cryptography Seminar at Cornell Tech Sept. 2019

Test without Trust: Optimal Locally Private Distribution Testing

- Poster at TPDP 2018 Workshop as part of CCS 2018 Oct. 2018

• Talk at Cornell Cryptography Seminar at Cornell Tech	Oct. 2018
<i>Testing and Searching Pattern Avoiding Sequences</i>	
• Talk at Cornell Theory Tea at Cornell	Mar. 2018
• Undergraduate Thesis Defense at UT Austin	May 2017
<i>Pan-Private Graph/Geometric Streaming Algorithms</i>	
• Talk at DIMACS REU at Rutgers University	July 2016
<i>Symmetric-Key Broadcast Encryption: The Multi-Sender Case</i>	
• Talk at TSSA Undergraduate Research Talks at UT Austin	Nov. 2015
• Talk at DS ResULTS at UT Austin	Sept. 2015
• Talk at REU CAAR at UMD	Aug. 2015