Eshan Chattopadhyay

Contact

Department of Computer Science
Cornell University
319 Gates Hall,
Ithaca, NY 14853, USA

Email: eshan@cs.cornell.edu
Homepage: https://www.cs.cornell.edu/eshan
Phone: (607) 216-9496

Research Interest

Computational Complexity Theory, Randomness in Computation, Cryptography.

Personal Information

Year of Birth: 1989
Citizenship: Indian

Appointments

2018-Present Assistant Professor at Cornell University, Ithaca
2017 Summer Consulting Researcher at Microsoft Research, India
2017 Spring Microsoft Research Fellow at the Simons Institute, UC Berkeley
2016 Fall, 2017-18 Postdoctoral Researcher at the Institute for Advanced Study, Princeton

Education

August 2011-May 2016 Ph.D. in Computer Science,
University of Texas, Austin
Advisor: Prof. David Zuckerman
Thesis: Explicit Two-Source Extractors and More
Received the Bert Kay Dissertation Award (best thesis)

June 2007-June 2011 B.Tech in Computer Science,
Indian Institute of Technology, Kanpur
Bachelor’s Thesis advisor: Prof. Manindra Agrawal
Best academic performance and Best Bachelor’s Thesis

Honors

2024 National Academy of Sciences Held Prize
2023 Alfred P. Sloan Research Fellow
2021 NSF CAREER Award
2019 NSF CRII Award
2017 Simons-Berkeley Research Fellowship
2016 Bert Kay Dissertation Award, UT Austin
2016 STOC Best Paper Award
2016 Dissertation Writing Fellowship, UT Austin
2015 US Junior Oberwolfach Fellow
2011 MCD Fellowship, UT Austin

Students

Current PhD Students

Jyun-Jie Liao (2018-2024 (expected))
Mohit Gurumukhani (2021-)
Noam Ringach (2022-)
Yunya Zhao (2023-)

Former PhD Student(s):
Jesse Goodman, PhD 2023. (Currently Postdoctoral Fellow at UT Austin.)

Invited Survey Article

A Recipe for Constructing Two-Source Extractors
Eshan Chattopadhyay
ACM SIGACT News Complexity Theory Column, June 2020 issue

Conference/Journal Publications

Extractors for Polynomial Sources over $\mathbb{F}_2$
Eshan Chattopadhyay, Jesse Goodman, Mohit Gurumukhani
15th Innovations in Theoretical Computer Science (ITCS), 2024

Recursive Error Reduction for Regular Branching Programs
Eshan Chattopadhyay, Jyun-Jie Liao
15th Innovations in Theoretical Computer Science (ITCS), 2024

Hardness against Linear Branching Programs and More
Eshan Chattopadhyay, Jyun-Jie Liao
38th Computational Complexity Conference (CCC), 2023
Low-Degree Polynomials Extract from Local Sources
Omar Alrabiah, Eshan Chattopadhyay, Jesse Goodman, Xin Li, João Ribeiro
49th EATCS International Colloquium on Automata, Languages and Programming (ICALP), 2022

Extractors for Sum of Two Sources
Eshan Chattopadhyay, Jyun-Jie Liao
54th Annual ACM Symposium on Theory of Computing (STOC), 2022

The Space Complexity of Sampling
Eshan Chattopadhyay, Jesse Goodman, David Zuckerman
13th Innovations in Theoretical Computer Science (ITCS) conference, 2022

Affine Extractors for Almost Logarithmic Entropy
Eshan Chattopadhyay, Jesse Goodman, Jyun-Jie Liao
62nd Annual IEEE Symposium on Foundations of Computer Science (FOCS), 2021

Improved Extractors for Small-Space Sources
Eshan Chattopadhyay, Jesse Goodman
62nd Annual IEEE Symposium on Foundations of Computer Science (FOCS), 2021

Fractional Pseudorandom Generators from Any Fourier Level
Eshan Chattopadhyay, Jason Gaitonde, Chin Ho Lee, Shachar Lovett, Abhishek Shetty
36th Computational Complexity Conference (CCC), 2021

Non-Malleable Codes, Extractors and Secret Sharing for Interleaved Tampering and Composition of Tampering
Eshan Chattopadhyay, Xin Li
18th Theory of Cryptography Conference (TCC) 2020

Extractors and Secret-Sharing against Bounded Collusion Protocols
Eshan Chattopadhyay, Jesse Goodman, Vipul Goyal, Ashutosh Kumar, Xin Li, Raghu Meka, David Zuckerman
61st Annual IEEE Symposium on Foundations of Computer Science (FOCS), 2020

Optimal Error Pseudodistributions for Read-Once Branching Programs
Eshan Chattopadhyay, Jyun-Jie Liao
35th Computational Complexity Conference (CCC), 2020

Non-Malleability against Polynomial Tampering
Marshall Ball, Eshan Chattopadhyay, Jyun-Jie Liao, Tal Malkin, Li-Yang Tan
40th Annual International Cryptology Conference (CRYPTO), 2020

XOR Lemmas for Resilient Functions Against Polynomials
Eshan Chattopadhyay, Pooya Hatami, Kaave Hosseini, Shachar Lovett, David Zuckerman
52nd Annual ACM Symposium on Theory of Computing (STOC), 2020
Extractors for Adversarial Sources via Extremal Hypergraphs
Eshan Chattopadhyay, Jesse Goodman, Vipul Goyal, Xin Li
52nd Annual ACM Symposium on Theory of Computing (STOC), 2020

Simple and efficient pseudorandom generators from Gaussian processes
Eshan Chattopadhyay, Anindya De, Rocco A. Servedio
34th Computational Complexity Conference (CCC), 2019.

Pseudorandom generators from the second Fourier level and applications to AC0 with parity gates
Eshan Chattopadhyay, Pooya Hatami, Shachar Lovett, Avishay Tal
10th Innovations in Theoretical Computer Science (ITCS) conference, 2019

Privacy Amplification from Non-Malleable Codes
Eshan Chattopadhyay, Bhavana Kanukurthi, Sai Lakshmi Bhavana Obbattu, Sruthi Sekar
20th International Conference on Cryptology in India (Indocrypt), 2019.

Pseudorandom Generators from Polarizing Random Walks
Eshan Chattopadhyay, Pooya Hatami, Kaave Hosseini, Shachar Lovett
Theory of Computing, 2019. Special Issue: 33rd Computational Complexity Conference (CCC), 2018

A New Approach for Constructing Low-Error, Two-Source Extractors
Avraham Ben-Aroya, Eshan Chattopadhyay, Dean Doron, Xin Li, Amnon Ta-Shma
33rd Computational Complexity Conference (CCC), 2018.

Improved Pseudorandomness for Unordered Branching Programs through Local Monotonicity
Eshan Chattopadhyay, Pooya Hatami, Omer Reingold, Avishay Tal
50th Annual ACM Symposium on Theory of Computing (STOC), 2018.

Non-Malleable Codes and Extractors for Small-Depth Circuits, and Affine Functions
Eshan Chattopadhyay, Xin Li
49th Annual ACM Symposium on Theory of Computing (STOC), 2017.

Explicit Non-Malleable Extractors, Multi-Source Extractors and Almost Optimal Privacy Amplification Protocols
Eshan Chattopadhyay, Xin Li
57th Annual IEEE Symposium on Foundations of Computer Science (FOCS) 2016.

Explicit Two-Source Extractors and Resilient Functions
Eshan Chattopadhyay, David Zuckerman
Annals of Mathematics 2019.
Preliminary version in the 48th Annual ACM Symposium on Theory of Computing (STOC), 2016. Won the Best Paper Award.

Extractors for Sumset Sources
Eshan Chattopadhyay, Xin Li
48th Annual ACM Symposium on Theory of Computing (STOC), 2016.
Non-Malleable Extractors and Codes, with their Many Tampered Versions
Eshan Chattopadhyay, Vipul Goyal, Xin Li
SIAM Journal on Computing (SICOMP) 2020. Preliminary version in the 48th Annual ACM Symposium on Theory of Computing (STOC), 2016.

New Extractors for Interleaved Sources
Eshan Chattopadhyay, David Zuckerman
31st Computational Complexity Conference (CCC), 2016.

Non-Malleable Codes against Constant-Split State Tampering
Eshan Chattopadhyay, David Zuckerman
55th Annual IEEE Symposium on Foundations of Computer Science (FOCS) 2014.

An Explicit VC-Theorem for Low-Degree Polynomials
Eshan Chattopadhyay, Adam Klivans, Pravesh Kothari
16th International Conference on Randomization and Computation (RANDOM) 2012.

Service

Co-organizer of the workshop Beyond the Boolean Cube in the program Analysis and TCS: New Frontiers at the Simons Institute, UC Berkeley, 2023

Presented a talk at the workshop: TCS Early Career Mentoring (at FOCS 2019); contributed a lecture in a collection of videos that aims to serve as a useful community resource as an online undergraduate course on Theory of computation (link).

Co-organizer of the workshop Cornell Junior Theorists' Workshop 2023, 2024.

Co-organizer of the workshop Randomness Extractors: Constructions and Applications at the 50th Annual ACM Symposium on Theory of Computing (STOC), 2018.

Served or will serve on the Program Committees for the:

37th Annual Conference on Foundations of Software Technology and Theoretical Computer Science (FSTTCS), 2017
59th Annual IEEE Symposium on Foundations of Computer Science (FOCS), 2018
24th International Conference on Randomization and Computation (RANDOM), 2020.
37th Computational Complexity Conference (CCC), 2022
3rd Information-Theoretic Cryptography (ITC) conference, 2022.
56th ACM Symposium on Theory of Computing (STOC 2024).
2025 ACM-SIAM Symposium on Discrete Algorithms (SODA 25).

Guest editor for the STOC 2024 special issue (in SICOMP).

Guest editor for the CCC 2022 special issue (in ToC).
Served on National Science Foundation (NSF) grant panel; reviewed proposals for NSF, European Research Council (ERC), Israel Science Foundation (ISF), and Natural Sciences and Engineering Research Council of Canada (NSERC).

Reviewer for many conferences and journals in areas of theoretical computer science and cryptography (such as FOCS, STOC, CCC, SODA, ITCS, ICALP, FSTTCS, RANDOM, ISIT, CRYPTO, INDOCRYPT, COLT, SICOMP, ToC, TOCT, JACM, etc).

Externally Funded Proposals

Alfred P. Sloan Research Fellowship. $75,000, 2023-25.

National Science Foundation (NSF) CAREER Award. $583,274, 2021-2026.

NSF Computer and Information Science and Engineering (CISE) Research Initiation Initiative (CRII) Award. $175,000, 2019-2021.

Teaching

CS 6810: Theory of Computing. Fall 2021, Fall 2023

CS 4820: Introduction to Analysis of Algorithms. Spring 2019 (co-taught with Prof. Robert Kleinberg), Spring 2022, Spring 2023 (co-taught with Katherine Van Koevering)

CS 6815: Pseudorandomness and Combinatorial Constructions. Fall 2018, Fall 2019, Fall 2022

CSMore (The Rising Sophomore Summer Program in Computer Science): Short introduction to Discrete Structures (pre-2800), co-taught with Prof. Éva Tardos. Summer 2020, Summer 2021.

CS 4814: Introduction to Computational Complexity. Spring 2020, Spring 2021

CS 6817: Analysis of Boolean Functions. Fall 2020.

Selected Invited Talks

Princeton University

Princeton NJ

Theory seminar

Stanford University

Stanford, CA

Theory seminar

Institute for Advanced Study
Princeton, NJ  
Computer Science & Discrete Math Seminar II  

University of Rochester  
Rochester, NY  
Computer Science Colloquium  

University of California, San Diego  
Online talk  
Theory seminar  

University of Texas at Austin  
Online talk  
Theory seminar  

Columbia University  
NYC, NY  
Theory seminar  

Texas A&M University  
College Station, Texas  
Randomness and Determinism in Compressive Data Acquisition (3 tutorial talks)  

Banff International Research Station  
Banff, Canada  
Algebraic Techniques in Computational Complexity  

7th Biennial Canadian Discrete and Algorithmic Mathematics Conference (CanaDAM)  
Vancouver, Canada  
Additive Combinatorics Minisymposia  

Cornell University  
Ithaca, NY  
Applied Math Colloquium  

CMO-BIRS  
Oaxaca, Mexico  
Analytic Techniques in Theoretical Computer Science
Simons Institute for the theory of computing
Berkeley, CA 2018
Pseudorandomness Reunion Workshop

Simons Algorithms and Geometry Meeting
New York City, NY 2017
Monthly meeting

Institute for Advanced Study, Princeton
Princeton, NJ 2017
Computer Science & Discrete Math Seminar II

University of Chicago
Chicago, IL 2017
Computer Science Seminar

Institute for Advanced Study
Princeton, NJ 2016
Computer Science & Discrete Math Seminar II

New York University
New York, NY 2016
Theory Seminar

Institute for Advanced Study
Princeton, NJ 2016
Mathematical Conversations

The Chinese University of Hong Kong
Hong Kong 2016
China Theory Week, 2016

Indian Institute of Science
Bangalore, India 2016
Theory Seminar

Infosys, Mysore
Mysore, India 2016
Mysore Park Workshop

*University of California, Los Angeles*

Los Angeles, CA
Theory Seminar 2016

*Microsoft Research, New England*

New England, MA
Theory Seminar 2016

*Oberwolfach*

Wolfach, Germany
Complexity Theory Workshop, specialized session 2015

*Stellenbosch Institute for Advanced Study*

Stellenbosch, South Africa
Workshop on Foundations of Randomness 2015

*Massachusetts Institute of Technology*

Boston, MA
Charles River Crypto Day 2015

*Institute for Advanced Study*

Princeton, NJ
Computer Science & Discrete Math Seminar II 2015

*Institute for Advanced Study*

Princeton, NJ
Computer Science & Discrete Math Seminar I 2015