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

Research Interest

Computational Complexity Theory, Randomness in Computation, Cryptography.

Personal Information

Born: September 23, 1989
Citizenship: Indian

Appointments

2023 Summer	Visiting Scientist at the Simons Institute, UC Berkeley
2018 July-Present	Assistant Professor at Cornell University, Ithaca
2017 Sep-2018 June	Postdoctoral Researcher at Institute for Advanced Study, Princeton
2017 Summer	Postdoctoral Researcher at Microsoft Research, India
2017 Spring	Microsoft Research Fellow at the Simons Institute, UC Berkeley
2016 Fall	Postdoctoral Researcher at Institute for Advanced Study, Princeton
2015 Summer, 2016 Summer	Research Intern at Microsoft Research, India
2011-2016	Teaching Assistant and Research Assistant at University of Texas, Austin
2010 Summer	Research Intern at ETH Zurich, Switzerland

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.
June 2007-June 2011	B.Tech in Computer Science, Indian Institute of Technology, Kanpur

Honors/Awards

Alfred P. Sloan Research Fellowship, 2023.

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

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

Microsoft Research Fellow at Simons Institute, Spring 2017.

Bert Kay Dissertation Award 2016, given for the best doctoral thesis in computer science at UT Austin.

Best Paper Award in 48th Annual ACM Symposium on Theory of Computing (STOC), 2016.

Dissertation Writing Fellowship awarded by University of Texas at Austin Graduate School for Spring 2016.

US Junior Oberwolfach Fellow, 2015.

Microelectronics and Computer Development (MCD) Fellowship 2011-14 awarded by University of Texas at Austin.

General Proficiency Medal for Best Academic Performance in B. Tech in Computer Science 2007-11, Indian Institute of Technology (IIT) Kanpur.

Best Bachelor's Thesis Award in Computer Science, IIT Kanpur for the year 2011. (Thesis title: Pseudorandom generators for polynomials, advised by Prof. Manindra Agrawal.)

PhD Students

Jesse Goodman (2018-2023 (expected)), Jyun-Jie Liao (in progress, 2018-), Mohit Gurumukhani (in progress, 2021-).

Invited Survey Article

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

Conference/Journal Publications

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
35th 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
34th Computational Complexity Confererence (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
33rd Computational Complexity Confererence (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: 32nd Computational Complexity Confererence (CCC), 2018

A New Approach for Constructing Low-Error, Two-Source Extractors
Avraham Ben-Aroya, Eshan Chattopadhyay, Dean Doron, Xin Li, Amnon Ta-Shma
32nd Computational Complexity Confererence (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
30th Computational Complexity Confererence (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 workshop *Beyond the Boolean Cube* in the program *Analysis and TCS: New Frontiers* at the Simons Institute, UC Berkeley (to be held in Summer, 2023)

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

Served 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.
- 36th Computational Complexity Conference (CCC), 2022
- 3rd Information-Theoretic Cryptography (ITC) conference, 2022.

Guest editor for CCC '22 special issue.

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, FSTTCS, RANDOM, ISIT, CRYPTO, INDOCRYPT, COLT, SICOMP, ToC, TOCT, JACM, etc).

Teaching

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

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

CS 6810: Theory of Computing. Fall 2021

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

Institute for Advanced Study

Princeton, NJ 2023
Computer Science & Discrete Math Seminar II

University of Rochester

Rochester, NY 2021
Computer Science Colloquium

University of California, San Diego

Online talk 2021
Theory seminar

University of Texas at Austin

Online talk 2020
Theory seminar

Columbia University

NYC, NY 2019
Theory seminar

Texas A&M University

College Station, Texas 2019
Randomness and Determinism in Compressive Data Acquisition (3 tutorial talks)

Banff International Research Station

Banff, Canada 2019
Algebraic Techniques in Computational Complexity

7th Biennial Canadian Discrete and Algorithmic Mathematics Conference (CanaDAM)

Vancouver, Canada 2019

Additive Combinatorics Minisymposia

Cornell University

Ithaca, NY 2018
Applied Math Colloquium

CMO-BIRS

Oaxaca, Mexico 2018
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 2016
Theory Seminar

Microsoft Research, New England

New England, MA 2016
Theory Seminar

Oberwolfach

Wolfach, Germany 2015
Complexity Theory Workshop, specialized session

Stellenbosch Institute for Advanced Study

Stellenbosch, South Africa 2015
Workshop on Foundations of Randomness

Massachusetts Institute of Technology

Boston, MA 2015
Charles River Crypto Day

Institute for Advanced Study

Princeton, NJ 2015
Computer Science & Discrete Math Seminar II

Institute for Advanced Study

Princeton, NJ 2015
Computer Science & Discrete Math Seminar I