NEWS RELEASE

Contact: Jim Ormond
212-626-0505
ormond@hq.acm.org

Recent UCLA Computer Grad Constructs "Crown Jewel of Cryptography"

Aayush Jain Receives ACM Doctoral Dissertation Award for Dissertation on the Feasibility of Mathematical Software Obfuscation

New York, NY, May 24, 2022 – ACM, the Association for Computing Machinery, today announced that **Aayush Jain** receives the **2022 ACM Doctoral Dissertation Award** for his dissertation "Indistinguishability Obfuscation From Well-Studied Assumptions," which established the feasibility of mathematically rigorous software obfuscation from well-studied hardness conjectures.

The central goal of software obfuscation is to transform source code to make it unintelligible without altering what it computes. Additional conditions may be added, such as requiring the transformed code to perform similarly, or even indistinguishably, from the original. As a software security mechanism, it is essential that software obfuscation have a firm mathematical foundation.

The mathematical object that Jain's thesis constructs, indistinguishability obfuscation, is considered a theoretical "master tool" in the context of cryptography—not only in helping achieve long-desired cryptographic goals such as functional encryption, but also in expanding the scope of the field of cryptography itself. For example, indistinguishability obfuscation aids in goals related to software security that were previously entirely in the domain of software engineering.

Jain's dissertation was awarded the Best Paper Award at the ACM Symposium on Theory of Computing (ACM STOC 2021) and was the subject of an article in *Quanta Magazine* titled "Scientists Achieve Crown Jewel of Cryptography."

Jain is an Assistant Professor at Carnegie Mellon University. He is interested in theoretical and applied cryptography and its connections with related areas of theoretical computer science. Jain received a BTech in Electrical Engineering, and an MTech in Information and Communication Technology from the Indian Institute of Technology, Delhi. He received a PhD in Computer Science from the University of California, Los Angeles.

Honorable Mentions

Honorable Mentions for the 2022 ACM Doctoral Dissertation Award go to **Alane Suhr** whose PhD was earned at Cornell University, and **Conrad Watt,** who earned his PhD at the University of Cambridge.

Suhr's dissertation, "Reasoning and Learning in Interactive Natural Language Systems," was recognized for formulating and designing algorithms for continual language learning in collaborative interactions, and designing methods to reason about context-dependent language meaning. Suhr's dissertation made transformative contributions in several areas of Natural Language Processing (NLP).

Suhr is an Assistant Professor at the University of California, Berkeley. Suhr's research is focused on natural language processing, machine learning, and computer vision. Suhr received a BS in Computer Science and Engineering from Ohio State University, as well as a PhD in Computer Science from Cornell University.

Watt's dissertation, "Mechanising and Evolving the Formal Semantics of WebAssembly: The Web's New Low-Level Language," establishes a mechanized semantics for WebAssembly and defines its concurrency model. The model will underpin current and future web engineering. His dissertation is considered a stand-out example of developing and using fully rigorous mechanized semantics to directly affect and improve the designs of major pieces of our industrial computational infrastructure.

Watt is a Research Fellow (postdoctoral) at the University of Cambridge, where he focuses on mechanized formal verification, concurrency, and the WebAssembly language. He received a MEng in Computer Science from Imperial College London and a PhD in Computer Science from the University of Cambridge.

About the ACM Doctoral Dissertation Award

Presented annually to the author(s) of the best doctoral dissertation(s) in computer science and engineering. The Doctoral Dissertation Award is accompanied by a prize of $20,000, and the Honorable Mention Award is accompanied by a prize totaling $10,000. Winning dissertations will be published in the ACM Digital Library as part of the ACM Books Series.

About ACM

ACM, the Association for Computing Machinery is the world's largest educational and scientific computing society, uniting computing educators, researchers and professionals to inspire dialogue, share resources and address the field's challenges. ACM strengthens the computing profession's collective voice through strong leadership, promotion of the highest standards, and recognition of technical excellence. ACM supports the professional growth of its members by providing opportunities for life-long learning, career development, and professional networking.

###