



**Association for
Computing Machinery**

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

**AVI WIGDERSON RECEIVES ACM A.M. TURING AWARD FOR
GROUNDBREAKING INSIGHTS ON RANDOMNESS**

Leading Theoretical Computer Scientist Cited for Field-Defining Contributions

New York, NY, April 10, 2024 – ACM, the Association for Computing Machinery, today named Avi Wigderson as recipient of the 2023 ACM A.M. Turing Award for foundational contributions to the theory of computation, including reshaping our understanding of the role of randomness in computation, and for his decades of intellectual leadership in theoretical computer science.

Wigderson is the Herbert H. Maass Professor in the School of Mathematics at the Institute for Advanced Study in Princeton, New Jersey. He has been a leading figure in areas including computational complexity theory, algorithms and optimization, randomness and cryptography, parallel and distributed computation, combinatorics, and graph theory, as well as connections between theoretical computer science and mathematics and science.

The ACM A.M. Turing Award, often referred to as the “Nobel Prize of Computing,” carries a \$1 million prize with financial support provided by Google, Inc. The award is named for Alan M. Turing, the British mathematician who articulated the mathematical foundations of computing.

What is Theoretical Computer Science?

Theoretical computer science is concerned with the mathematical underpinnings of the field. It poses questions such as “Is this problem solvable through computation?” or “If this problem is solvable through computation, how much time and other resources will be required?”

Theoretical computer science also explores the design of efficient algorithms. Every computing technology that touches our lives is made possible by algorithms. Understanding the principles that make for powerful and efficient algorithms deepens our understanding not only of computer science, but also the laws of nature. While theoretical computer science is known as a field that presents exciting intellectual challenges and is often not directly concerned with improving the practical applications of computing, research breakthroughs in this discipline have led to advances in almost every area of the

field—from cryptography and computational biology to network design, machine learning, and quantum computing.

Why is Randomness Important?

Fundamentally, computers are *deterministic* systems; the set of instructions of an algorithm applied to any given input uniquely determines its computation and, in particular, its output. In other words, the deterministic algorithm is following a predictable pattern. *Randomness*, by contrast, lacks a well-defined pattern, or predictability in events or outcomes. Because the world we live in seems full of random events (weather systems, biological and quantum phenomena, etc.), computer scientists have enriched algorithms by allowing them to make random choices in the course of their computation, in the hope of improving their efficiency. And indeed, many problems for which no efficient deterministic algorithm was known have been solved efficiently by probabilistic algorithms, albeit with some small probability of error (that can be efficiently reduced). But is randomness essential, or can it be removed? And what is the quality of randomness needed for the success of probabilistic algorithms?

These, and many other fundamental questions lie at the heart of understanding randomness and pseudorandomness in computation. An improved understanding of the dynamics of randomness in computation can lead us to develop better algorithms as well as deepen our understanding of the nature of computation itself.

Wigderson's Contributions

A leader in theoretical computer science research for four decades, Wigderson has made foundational contributions to the understanding of the role of randomness and pseudorandomness in computation.

Computer scientists have discovered a remarkable connection between randomness and computational difficulty (i.e., identifying natural problems that have no efficient algorithms). Working with colleagues, Wigderson authored a highly influential series of works on trading hardness for randomness. They proved that, under standard and widely believed computational assumptions, every probabilistic polynomial time algorithm can be efficiently derandomized (namely, made fully deterministic). In other words, randomness is not necessary for efficient computation. This sequence of works revolutionized our understanding of the role of randomness in computation, and the way we think about randomness. This series of influential papers include the following three:

- [“Hardness vs. Randomness”](#) (co-authored with Noam Nisan)
Among other findings, this paper introduced a new type of pseudorandom generator, and proved that efficient deterministic simulation of randomized algorithms is possible under much weaker assumptions than previously known.
- [“BPP Has Subexponential Time Simulations Unless EXPTIME has Publishable Proofs”](#) (co-authored with László Babai, Lance Fortnow, and Noam Nisan)
This paper used ‘hardness amplification’ to demonstrate that bounded-error probabilistic

polynomial time (BPP) can be simulated in subexponential time for infinitely many input lengths under weaker assumptions.

- [“P = BPP if E Requires Exponential Circuits: Derandomizing the XOR Lemma”](#) (co-authored with Russell Impagliazzo)
This paper introduces a stronger pseudo-random generator with essentially optimal hardness vs randomness trade-offs.

Importantly, the impact of these three papers by Wigderson goes far beyond the areas of randomness and derandomization. Ideas from these papers were subsequently used in many areas of theoretical computer science and led to impactful papers by several leading figures in the field.

Still working within the broad area of randomness in computation, in [papers](#) with Omer Reingold, Salil Vadhan, and Michael Capalbo, Wigderson gave the first efficient combinatorial constructions of expander graphs, which are sparse graphs that have strong connectivity properties. They have many important applications in both mathematics and theoretical computer science.

Outside of his work in randomness, Wigderson has been an intellectual leader in several other areas of theoretical computer science, including multi-prover interactive proofs, cryptography, and circuit complexity.

Mentoring

In addition to his groundbreaking technical contributions, Wigderson is recognized as an esteemed mentor and colleague who has advised countless young researchers. His vast knowledge and unrivaled technical proficiency—coupled with his friendliness, enthusiasm, and generosity—have attracted many of the best young minds to pursue careers in theoretical computer science.

“It’s important to point out that Avi Wigderson also received the Abel Prize, which is considered the most important honor for lifetime achievements in the field of mathematics,” explained ACM President Yannis Ioannidis. “Being selected for the ACM A.M. Turing Award is a fitting follow-up—as mathematics is foundational to computer science and Wigderson’s work has connected a wide range of mathematical sub-areas to theoretical computer science. Wigderson is a towering intellectual force in theoretical computer science, an exciting discipline that attracts some of the most promising young researchers to work on the most difficult challenges. This year’s Turing Award recognizes Wigderson’s specific work on randomness, as well as the indirect but substantial impact he has had on the entire field of theoretical computer science.”

"Avi Wigderson’s work on randomness and other topics has set the agenda in theoretical computer science for the past three decades,” explained Jeff Dean, Senior Vice President, Google. “From the earliest days of computer science, researchers have recognized that incorporating randomness was a way to design faster algorithms for a wide range of applications. Efforts to better understand randomness continue to yield important benefits to our field, and Wigderson has opened new horizons

in this area. Google also salutes Wigderson’s role as a mentor. His colleagues credit him with generating great ideas and research directions, and then motivating a new generation of smart young researchers to work on them. We congratulate Avi Wigderson on receiving the ACM A.M. Turing Award— computing’s highest honor.”

Biographical Background

Since 1999, Avi Wigderson has been the Herbert H. Maass Professor in the School of Mathematics at the Institute for Advanced Study in Princeton, New Jersey. Earlier, he was a Professor at the Hebrew University of Jerusalem and held visiting appointments at Princeton University, the University of California at Berkeley, IBM, and other institutions.

A graduate of The Technion – Israel Institute of Technology, Wigderson earned MA, MSE, and PhD degrees in Computer Science from Princeton University. Wigderson’s honors include the Abel Prize, the IMU Abacus Medal (previously known as the Nevanlinna Prize), the Donald E. Knuth Prize, the Edsger W. Dijkstra Prize in Distributed Computing, and the Gödel Prize. He is an ACM Fellow and a member of the U.S. National Academy of Sciences and the American Academy of Arts and Sciences.

Read more about Avi Wigderson receiving the ACM A.M. Turing Award in [Communications of the ACM](#).

About the ACM A.M. Turing Award

[The A.M. Turing Award](#) is named for Alan M. Turing, the British mathematician who articulated the mathematical foundations of computing, and who was a key contributor to the Allied cryptanalysis of the Enigma cipher during World War II. Since its inception in 1966, the Turing Award has honored the computer scientists and engineers who created the systems and their underlying theoretical foundations that have propelled the information technology industry.

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.

###