Photo credit: Andrea Kane, Institute for Advanced Studies, Princeton, NJ, USA / Abel Prize

# A biography of Avi Wigderson

When Avi Wigderson began his academic career in the late 1970s, the theory of 'computational complexity' – which concerns itself with the speed and efficiency of algorithms – was in its infancy. Wigderson's contribution to enlarging and deepening the field is arguably greater than that of any single other person, and what was a young subject is now an established field of both mathematics and theoretical computer science. Computational complexity has also become unexpectedly important, providing the theoretical basis for internet security.

Wigderson was born in Haifa, Israel, in 1956. He entered the Technion, the Israeli Institute of Technology, in 1977, and graduated with a B.Sc. in Computer Science in 1980. He moved to Princeton for his graduate studies, receiving his PhD in 1983 for the thesis *Studies in Combinatorial Complexity*, for which Richard Lipton was his advisor. In 1986 Wigderson returned to Israel to take up a position at the Hebrew University in Jerusalem. He was given tenure the following year and made full professor in 1991.

In the 1970s, computer theoreticians framed certain fundamental ideas about the nature of computation, notably the notions of P and NP. P is the set of problems that computers can solve easily, say, in a few seconds, whereas NP also contains problems that computers find hard to solve, meaning that the known methods can only find the answer in, say, millions of years. The question of whether all these hard problems can be reduced to easy ones, that is, whether or not P = NP, is the foundational question of computational complexity. Indeed, it is now considered one of the most important unsolved questions in all of mathematics.

Wigderson made stunning advances in this area by investigating the role of randomness in aiding computation. Some hard problems can be made easy using algorithms in which the computer flips

coins during the computation. If an algorithm relies on coin-flipping, however, there is always a chance that an error can creep into the solution. Wigderson, first together with Noam Nisan, and later with Russell Impagliazzo, showed that for any fast algorithm that can solve a hard problem using coin-flipping, there exists an almost-as-fast algorithm that does not use coin-flipping, provided certain conditions are met.

Wigderson has conducted research into every major open problem in complexity theory. In many ways, the field has grown around him, not only because of his breadth of interests, but also because of his approachable personality and enthusiasm for collaborations. He has co-authored papers with well over 100 people, and has mentored a large number of young complexity theorists. “I consider myself unbelievably lucky to live in this age,” he says. “[Computational complexity] is a young field. It is a very democratic field. It is a very friendly field, it is a field that is very collaborative, that suits my nature. And definitely, it is bursting with intellectual problems and challenges.”

In 1999 Wigderson joined the Institute for Advanced Study (IAS) in Princeton where he has been ever since. At an event to celebrate Wigderson’s sixtieth birthday, in 2016, IAS director Robbert Dijkgraaf said that he had launched a golden age of theoretical computer science at the institute.

Wigderson is known for his ability to see links between apparently unrelated areas. He has deepened the connections between mathematics and computer science. One example is the ‘zig-zag graph product’, which he developed with Omer Reingold and Salil Vadhan, which links group theory, graph theory and complexity theory, and has surprising applications such as how best to get out of a maze.

The most important present-day application of complexity theory is to cryptography, which is used to secure information on the internet such as credit card numbers and passwords. People who design cryptosystems, for example, must make sure that the task of decoding their system is an NP problem, that is, one that would take computers millions of years to achieve. Early in his career Wigderson made fundamental contributions to a new concept in cryptography, the zero-knowledge proof, which more than 30 years later is now being used in blockchain technology. In a zero-knowledge proof, two people must prove a claim without revealing any knowledge beyond the validity of that claim, such as the example of the two millionaires who want to prove who is richer without either of them letting on how much money they have. Wigderson, together with Oded Goldreich and Silvio Micali, showed that zero-knowledge proofs can be used to prove, in secret, any public result about secret data. Just say, for example, that you want to prove to someone that you have proved a mathematical theorem, but you don’t want to reveal any details of how you did it, a zero-knowledge proof will allow you to do this.

In 1994, Wigderson won the Rolf Nevanlinna Prize for computer science, which is awarded by the International Mathematical Union every four years. Among his many other prizes is the 2009 Gödel Prize and the 2019 Knuth Prize.

Wigderson is married to Edna, whom he met at the Technion, and who works in the computer department of the Institute for Advanced Study. They have three children, and two grandchildren.

*Source for quote: Heidelberg Laureate Foundation Portraits, interview with Avi Wigderson, 2017.*