Q&A with Turing Award winner Prof. Shafi Goldwasser

Prof. Goldwasser holds a joint appointment in the Department of Computer Science and Applied Mathematics at the Weizmann Institute and at MIT, was awarded the Turing Award, with her MIT colleague Prof. Silvio Micali. The Turing Award is the highest prize in the field of computing, and they were cited for laying the foundation for the science of cryptography, which is the basis for secure Internet transactions—enabling safe banking, commerce, and other transactions over the Internet. See more

What does the winning of the Turing Award mean to you?
Mostly, that the ideas behind what we call the “foundations of cryptography” that I have worked on for the last 30-plus years have been widely accepted and understood. Concepts such as “computational indistinguishability,” “probabilistic proofs,” and “simulations as proofs of security” no longer hold novelty, and that’s a good thing!

Why is the Weizmann Institute the best kind of environment to do computer science research?
The Weizmann Institute has consistently hired incredibly strong researchers, and not only in the narrower sense of technical excellence. Institute scientists in my field of theory of computation have all, without exception, managed, at one time or another, to re-direct their entire research community to focus on the problems they chose. Thus, they have led rather than been led and ultimately have made a real impact on our discipline. Having such colleagues is what makes the environment what it is.

What’s next on the horizon for you?
There are several themes that recur throughout my work and in the theory of computing more largely in the last few decades. These concern using randomization, interaction, and locality in computation. I am interested in showing that these ingredients are fundamentally necessary.