SHAFI GOLDWASSER

Shafi Goldwasser is an American-Israeli computer scientist. She has made a few contributions to cryptography, computational complexity, computational number theory and probabilistic algorithms. These are included in creating the theoretical foundations of modern cryptography, the introduction of zero-knowledge interactive proofs, the introduction of multi-prover proofs.

Shafrira GoldWasser was born in 1959 in NewYork City. She studied grade school in Tel Aviv in Israel.After her schooling, she went U.S. and became an undergraduate(B.S) in the mathematics department at Carnegie Mellon University. Later she completed her M.S and PhD in computer science from the University of California, Berkeley under the guidance of Manuel Blum.

After graduation, she joined MIT in 1983 first as a postdoc and then as a faculty. She became the RSA Professor of Electrical Engineering and Computer Science in 1997. She also started teaching as a Professor of Computer Science and Applied Mathematics at the Weizmann Institute of Science in Israel.

When Shafi came to M.I.T she joined a group with similar research interests: Micali ,Benny Chor, Oded Goldreich, Ron Rivest and Mike Sipser were there. With Goldreich and Micali , Shafi researched whether the notion of a pseudorandom number generator could be generalized . This definition was so important, and it is the main foundation for a blockcipher such as AES to be secure. Next Shafi and Joe Kilian proved that when a prime number is chosen for a cryptographic algorithm such as RSA, one can be absolutely certain that the number really is prime.

Goldwasser has twice won the Gödel Prize in theoretical computer science: first in 1993 for The knowledge complexity of interactive proof systems, and again in 2001 for Interactive Proofs and the Hardness of Approximating Cliques. She received the IEEE Emanuel R. Piore Award in 2011.Later she was awarded

the 2012 Turing Award along with Silvio Micali for their work in the field of cryptography.