Goldwasser and Micali Awarded Turing Prize

SHAFI GOLDWASSER of the Massachusetts Institute of Technology (MIT) and the Weizmann Institute of Science and SILVIO MICALI of MIT have received the 2012 A. M. Turing Award of the Association for Computing Machinery (ACM). The award, considered the "Nobel Prize in Computing", carries a cash award of US$250,000.

Shafi Goldwasser

Silvio Micali

The prize citation reads in part: "Working together, [Goldwasser and Micali] pioneered the field of provable security, which laid the mathematical foundations that made modern cryptography possible. By formalizing the concept that cryptographic security had to be computational rather than absolute, they created mathematical structures that turned cryptography from an art into a science. Their work addresses important practical problems such as the protection of data from being viewed or modified, providing a secure means of communications and transactions over the Internet. Their advances led to the notion of interactive and probabilistic proofs and had a profound impact on computational complexity, an area that focuses on classifying computational problems according to their inherent difficulty."

Their 1983 paper "Probabilistic encryption" defined the security of encryption as a "game" involving adversaries; this definition has become a trademark of modern cryptography. Their simulation paradigm approach led to the construction of a secure encryption scheme. They observed that to satisfy their security definition, encryption schemes must be randomized rather than deterministic, with many possible encrypted texts corresponding to each message. This development revolutionized the study of cryptography and laid the foundation for the theory of cryptographic security that was developed throughout much of the 1980s.

Their introduction of the idea of zero-knowledge proofs provided the essential language for speaking about security of cryptographic protocols by controlling the leakage of knowledge.

DOI: http://dx.doi.org/10.1090/noti1021

Shafi Goldwasser is the RSA Professor of Electrical Engineering and Computer Science at MIT, principal investigator at the MIT Computer Science and Artificial Intelligence Lab (CSAIL), and professor of computer science and applied mathematics at the Weizmann Institute of Science in Israel. She is the recipient of a National Science Foundation Presidential Young Investigator Award and of the ACM Grace Murray Hopper Award for outstanding young computer professional. She has twice won the Gödel Prize presented jointly by the ACM Special Interest Group on Algorithms and Computation Theory (SIGACT) and the European Association for Theoretical Computer Science (EATCS). She was elected to the American Academy of Arts and Sciences, the National Academy of Sciences, and the National Academy of Engineering. She was recognized by the ACM Council on Women in Computing (ACM-W) as the Athena Lecturer and received the IEEE Piore Award and the Franklin Institute's Benjamin Franklin Medal in Computer and Cognitive Science. She received her B.A. degree in mathematics from Carnegie Mellon University and her M.S. and Ph.D. degrees in computer science from the University of California Berkeley.

Silvio Micali, the Ford Professor of Engineering at MIT and a principal investigator at the MIT CSAIL, has received the Gödel Prize from ACM SIGACT and EATCS. A fellow of the American Academy of Arts and Sciences, the National Academy of Sciences, and the National Academy of Engineering, he is the recipient of the RSA Mathematics Award, the Berkeley Distinguished Alumnus of the Year Award, and the ISE (Information Security Executive) New England Rising Star Award. He is coeditor of a five-volume series of textbooks, *Advances in Computing Research*, and has published more than one hundred scientific papers. A graduate of Sapienza, University of Rome, with a degree in mathematics, he earned a Ph.D. degree in computer science from the University of California Berkeley.

The A. M. Turing Award was instituted in 1966 to honor the computer scientists and engineers who created the systems and underlying theoretical foundations that have propelled the information technology industry. Financial support for the Turing Award is provided by the Intel Corporation and Google Inc.

—From an ACM announcement