AMERICAN COMMITTEE FOR THE WEIZMANN INSTITUTE OF SCIENCE

SCIENCE FOR THE BENEFIT OF HUMANITY

CONTACT: Jeffrey J. Sussman
212.895.7951
jeffrey@acwis.org

TURING AWARD TO THE WEIZMANN INSTITUTE'S SHAFI GOLDWASSER FOR ADVANCES THAT REVOLUTIONIZED THE SCIENCE OF CRYPTOGRAPHY

The Award was given for innovations that became the gold standard for enabling secure Internet transactions

Goldwasser is the third member of the Weizmann Institute of Science faculty to receive the Turing Award. The others are Profs. Amir Pnueli (1996) and Adi Shamir (2002)

REHOVOT, ISRAEL—March 13, 2013—The Association for Computing Machinery (ACM) today announced that Prof. Shafrira (Shafi) Goldwasser of the Weizmann Institute's Department of Computer Science and Applied Mathematics and the Massachusetts Institute of Technology's (MIT's) Computer Science and Artificial Intelligence Lab, will receive the ACM A.M. Turing Award. She receives the Award together with Prof. Silvio Micali of MIT "for transformative work that laid the complexity-theoretic foundations for the science of cryptography, and in the process pioneered new methods for efficient verification of mathematical proofs in complexity theory."

The Turing Award, widely considered the world's highest prize in the field of computing (there is no Nobel Prize in the field), carries a $250,000 prize, with financial support provided by Intel Corporation and Google Inc.

Probabilistic Encryption

In their 1982 paper on "Probabilistic Encryption," Profs. Goldwasser and Micali laid the rigorous foundations for modern cryptography. The work is universally credited in changing cryptography from an "art" to a "science."

This paper pioneered several themes which are today considered basic to the field. These include the introduction of formal security definitions that are now the gold

standard for security; the introduction of randomized methods for encryption which can satisfy stringent security requirements that could not be satisfied by previous deterministic encryption schemes; and the methodology of "reductionist proofs," which shows how to translate the slightest attack on security into a fast algorithm for solving such hard classical mathematical problems as factoring integers. These proofs are a double-edged sword, in that they show that one of two things must be true: Either we have a super-secure encryption scheme, or we have new algorithms for factoring integers.

The 1982 paper also introduced the "simulation paradigm," in which the security of a system is established by showing that an enemy could have simulated, on his own, any information he obtained during the employment of a cryptographic system, and thus this cryptographic system represents no risk. The simulation paradigm has become the most general method for proving security in cryptography, going beyond privacy to define and prove security of authentication methods, security of software protection schemes, and security of cryptographic protocols that involve many participants, such as electronic elections and auctions.

Zero-Knowledge Interactive Proofs

In another influential paper, published in 1985 with Prof. Charles Rackoff, Profs. Goldwasser and Micali introduced the concept of "zero-knowledge interactive proofs."

An example of a zero-knowledge interactive proof would be an ATM machine that would not need you to enter your PIN number, but would only need to verify that you yourself know it. Zero-knowledge proofs can also enable users working on the Internet who may not trust each other to compute joint functions on their secret data.

In contrast to classical mathematical proofs, which can always be written down, an interactive proof is a sort of conversation. One side – the "prover" – tries to convince the other – the "verifier" – that he knows the proof of a mathematical statement. The verifier must ask the prover a series of questions, which are randomly chosen depending on the prover's previous answers and the mathematical statement to be proved. If the prover does not know the proof, the overwhelming probability is that the verifier will be

able to catch him out by his mistakes. Because the verifier can be convinced that the proof exists, without learning the proof itself, such proofs are truly "zero-knowledge proofs."

When Profs. Goldwasser, Micali, and Rackoff published their paper, its relevance to cryptography was immediately apparent. For example, it suggested an identification system that can be used safely over the Internet. The idea is that an individual user will know a proof for her own special theorem, which will be her password. To identify herself, the user can interact with a verifier (an ATM machine, for example) to give that verifier a zero-knowledge proof of her special theorem.

Interactive proofs are not only a cryptographic tool; they have had a major impact on complexity theory. What seemed to be obvious for cryptographic purposes – that randomization and interaction must be used – has turned out to be widely applicable to complexity theory in general. It enables faster verification of proofs than classical mathematics and even gives mathematicians the ability to prove that some mathematical statements are *no*t correct, by proving "non-existence" of classical proofs.

In a further series of works by Profs. Goldwasser, Micali, and others, interactive proofs were extended to include interactions between a verifier and multiple provers, which ultimately led to surprising new ways to prove NP-completeness results for approximation problems. (In computational complexity theory, NP stands for nondeterministic polynomial time.) This is an active area of research today.

Practical Impact

ACM President Vint Cerf said the practical impact of the ideas put forward by Profs. Goldwasser and Micali is tangible. "The encryption schemes running in today's browsers meet their notions of security. The method of encrypting credit card numbers when shopping on the Internet also meets their test. We are indebted to these recipients for their innovative approaches to ensuring security in the digital age."

Alfred Spector, Vice President of Research and Special Initiatives at Google Inc., said Profs. Goldwasser and Micali developed cryptographic algorithms that are designed

around computational hardness assumptions, making such algorithms hard to break in practice. “In the computer era, these advances in cryptography have transcended the cryptography of Alan Turing’s code-breaking era. They now have applications for ATM cards, computer passwords, and electronic commerce, as well as preserving the secrecy of participant data, such as electronic voting. These are monumental achievements that have changed how we live and work.”

The Third Woman to Receive a Turing Award

Prof. Shafi Goldwasser is recipient of the National Science Foundation Presidential Young Investigator Award. She also won 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 Science, the National Academy of Sciences, and the National Academy of Engineering. Prof. Goldwasser 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.

A graduate of Carnegie Mellon University with a BA degree in mathematics, Prof. Goldwasser received MS and PhD degrees in computer science from the University of California, Berkeley. She joined the Weizmann Institute in 1993 as a full professor. She is the third woman to receive a Turing Award since their inception in 1966.

ACM will present the 2012 A.M. Turing Award at its annual Awards Banquet, to be held on June 15, 2013 in San Francisco, CA.

Prof. Shafrira Goldwasser’s research is supported by Walmart.

# # #

Weizmann
5-5-5-5-5

The Weizmann Institute of Science in Rehovot, Israel, is one of the world's top-ranking multidisciplinary research institutions. The Institute's 2,700-strong scientific community engages in research addressing crucial problems in medicine and health, energy, technology, agriculture, and the environment. Outstanding young scientists from around the world pursue advanced degrees at the Weizmann Institute's Feinberg Graduate School. The discoveries and theories of Weizmann Institute scientists have had a major impact on the wider scientific community, as well as on the quality of life of millions of people worldwide.