acm
Association for Computing Machinery
Advancing Computing as a Science & Profession

Contact: Virginia Gold
212-626-0505
vgold@acm.org

GOLDWASSER AND MICALI RECEIVE ACM TURING AWARD FOR ADVANCES THAT REVOLUTIONIZED THE SCIENCE OF CRYPTOGRAPHY

MIT Researchers' Innovations Became Gold Standard for Enabling Secure Internet Transactions

NEW YORK, March 13, 2013– ACM, the Association for Computing Machinery, today named Shafi Goldwasser http://amturing.acm.org/goldwasser of the Massachusetts Institute of Technology (MIT) and the Weizmann Institute of Science and Silvio Micali http://amturing.acm.org/micali of MIT as the recipients of the 2012 ACM A.M. Turing Award. Working together, they 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.

The ACM Turing Award, widely considered the "Nobel Prize in Computing," carries a $250,000 prize, with financial support provided by Intel Corporation and Google Inc.

ACM President Vint Cerf said the practical impact of the ideas promulgated by 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."

"The work of Goldwasser and Micali has expanded the cryptography field beyond confidentiality concerns," said Limor Fix, Director of the University Collaborative Research Group, Intel Labs. "Their innovations also led to techniques for message integrity checking and sender/receiver identity authentication as well as digital signatures used for software distribution, financial transactions, and other cases where it is important to detect forgery or tampering. They have added immeasurably to our ability to conduct communication and commerce over the Internet."

Alfred Spector, Vice President of Research and Special Initiatives at Google Inc., said 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."

Probabilistic Encryption

Goldwasser and Micali produced one of the most influential papers in computer science, "Probabilistic Encryption," as graduate students in 1983, by introducing the question "What is a secret?" Their standards were very high: an adversary (third party) should not be able to gain any partial information about a secret. Their definition of the security of encryption as a "game" involving adversaries has become a trademark of modern cryptography. Their approach, known as the simulation paradigm, bypassed the traditional enumeration of desired properties that marked the definition of security, and led to the construction of a secure encryption scheme. This method provided a robust defense against malicious attempts to make these schemes deviate from their prescribed functionality.

They introduced two notions of encryption security – semantic security and indistinguishability of encrypted messages from each other – thus capturing the important aspects of the subject. They argued that these measures must be met for schemes to provide security across the wide range of cryptography applications. In contrast with prevailing trends in the field, 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.

Interactive Proof Systems

One of the most significant contributions of Goldwasser and Micali is their 1985 paper with Charles Rackoff, titled "The Knowledge Complexity of Interactive Proof Systems." It introduced knowledge complexity, a concept that deals with hiding information from an adversary, and is a quantifiable measure of how much "useful information" could be extracted. The paper initiated the idea of "zero-knowledge" proofs, in which interaction (the ability of provers and verifiers to send each other messages back and forth) and probabilism (the ability to toss coins to decide which messages to send) enable the establishment of a fact via a statistical argument without providing any additional information as to why it is true.

Zero-knowledge proofs were a striking new philosophical idea that provided the essential language for speaking about security of cryptographic protocols by controlling the leakage of knowledge. Subsequent works by Oded Goldreich, Micali, and Avi Wigderson and by Michael Ben-Or, Goldwasser, and Wigderson showed that every multiparty computation can be carried out securely, revealing to the players no more knowledge than prescribed by the desired outcome. These papers exhibited the power and utility of zero-knowledge protocols, and demonstrated their ubiquitous and omnipotent character.

The paper identified interactive proofs as a new method to verify correctness in the exchange of information. Going beyond cryptography, interactive proofs can be much faster to verify than classical proofs, and can be used in practice to guarantee correctness in a variety of applications.

Background

Shafi Goldwasser is the RSA Professor of Electrical Engineering and Computer Science at MIT, and Principal Investigator at the MIT Computer Science and Artificial Intelligence Lab (CSAIL), as well as a professor of Computer Science and Applied Mathematics at the Weizmann Institute of Science in Israel. A 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. 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.

A graduate of Carnegie Mellon University with a B.A. degree in mathematics, she received 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 Computer Science and Artificial Intelligence Lab (CSAIL), is a recipient of the Gödel Prize from ACM SIGACT and EATCS. A Fellow of the American Academy of Arts and Sciences, the National Academy of Sciences and 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. Micali is the editor (with Franco Preparata, Paris Kanellakis, Christoff Hoffmann, and Robert Hawkins) of a five-volume series of textbooks, *Advances in Computing Research*, and has published more than 100 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.

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

About the ACM A.M. Turing Award

The A.M. Turing Award **http://amturing.acm.org/** was named for Alan M. Turing, the British mathematician who articulated the mathematical foundation and limits of computing, and who was a key contributor to the Allied cryptanalysis of the German Enigma cipher and the German "Tunny" encoding machine in World War II. Since its inception in 1966, the Turing Award has honored the computer scientists and engineers who created the systems and underlying theoretical foundations that have propelled the information technology industry.

About ACM

ACM, the Association for Computing Machinery **www.acm.org,** is the world's largest educational and scientific computing society, uniting computing educators, researchers and professionals to inspire dialogue, share resources and address the field's challenges. ACM strengthens the computing profession's collective voice through strong leadership, promotion of the highest standards, and recognition of technical excellence. ACM supports the professional growth of its members by providing opportunities for life-long learning, career development, and professional networking.

# # #