Goldwasser and Micali win Turing Award

Massachusetts Institute of Technology

MIT professors Shafi Goldwasser and Silvio Micali have won the Association for Computing Machinery's (ACM) A.M. Turing Award [1] for their pioneering work in the fields of cryptography and complexity theory. The two developed new mechanisms for how information is encrypted and secured, work that is widely applicable today in communications protocols, Internet transactions and cloud computing. They also made fundamental advances in the theory of computational complexity, an area that focuses on classifying computational problems according to their inherent difficulty.

Goldwasser and Micali were credited for "revolutionizing the science of cryptography" and developing the gold standard for enabling secure Internet transactions. The Turing Award, which is presented annually by the ACM, is often described as the "Nobel Prize in computing" and comes with a $250,000 prize.

"For three decades Shafi and Silvio have been leading the field of cryptography by asking fundamental questions about how we share and receive information. I am thrilled that they have been honored for their pioneering work, and particularly excited that they have been recognized for their achievements as a team," says Professor Daniela Rus, director of MIT's Computer Science and Artificial Intelligence Lab (CSAIL). "We are honored and privileged to have this tremendous duo here at CSAIL."

Goldwasser is the RSA Professor of Electrical Engineering and Computer Science at MIT and a professor of computer science and applied mathematics at the Weizmann Institute of Science in Israel. She leads the Theory of Computation Group at CSAIL. Micali is the Ford Professor of Engineering at MIT and leads the Information and Computer Security Group at CSAIL, along with Goldwasser and Professor Ronald L. Rivest.

"I am delighted that Professors Shafi Goldwasser and Silvio Micali have been recognized and honored with the prestigious ACM Turing Award for their fundamental contributions to the field of provable security. Their work has had a major impact on a broad spectrum of applications touching everyday lives and has opened exciting new research opportunities," says Anantha Chandrakasan, head of MIT's Department of Electrical Engineering and Computer Science (EECS). "This is a tremendous honor for the EECS department and inspiring for the large number of students and faculty who have benefited from interactions with Shafi and Silvio."

Goldwasser and Micali began collaborating as graduate students at the University of California at Berkeley in 1980. While toying around with the idea of how to securely play a game of poker over the phone, they devised a scheme for encrypting and ensuring the security of single bits of data. From there, Goldwasser and Micali proved that their scheme could be scaled up to tackle much more complex problems, such as communications protocols and Internet transactions.

Based on their work, Goldwasser and Micali published a paper in 1982, titled "Probabilistic Encryption," which laid the framework for modern cryptography. In the paper they introduced formal security definitions, which remain the gold standard for security to this day, and pioneered randomized methods for encryption. Goldwasser and Micali proved that encryption schemes must be randomized rather than deterministic, with many possible encrypted texts corresponding to each message, a development that revolutionized the study of cryptography and laid the foundation for the theory of cryptographic security.

They also introduced the simulation paradigm, which demonstrates a system's security by showing that an enemy could have simulated all the information he obtained during the employment of a cryptographic system, proving that the cryptographic system poses no risk. The simulation paradigm has become the most widely used method for enabling security in cryptography, going beyond privacy to address problems in authentication and integrity of data, software protection and protocols that involve many participants, such as electronic elections and auctions.

One of Goldwasser and Micali's most significant contributions 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 Benor, Goldwasser and Wigderson, showed that every multiparty computation could 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. Beyond cryptography, interactive proofs can be verified much faster than classical proofs, and can be used in practice to guarantee correctness in a variety of applications such as cloud computing. In a series of works by Goldwasser, Micali and other collaborators, interactive proofs have been extended in several new directions. One direction was to include interactions between a single verifier and multiple provers, which has led to a new way to define and prove NP completeness for approximation problems (an area of active research). Another led to the development of computationally sound proofs, which can be easily compacted and verified, allowing for expedient accuracy checks.

"I am very proud to have won the Turing Award," Goldwasser says. "Our work was

very unconventional at the time. We were graduate students and let our imagination run free, from using randomized methods to encrypt single bits to enlarging the classical definition of a proof to allow a small error to setting new goals for security. Winning the award is further testimony to the fact that the cryptographic and complexity theoretic community embraced these ideas in the last 30 years."

"I am honored by this recognition and thankful to the computer science community," Micali adds. "As graduate students, we took some serious risks and faced a few rejections, but also received precious encouragement from exceptional mentors. I am also proud to see how far others have advanced our initial work."

Past recipients of the Turing Award from MIT have included Barbara Liskov, Ronald L. Rivest, Butler Lampson, Fernando Corbato and Marvin Minsky.

The Turing Award is given annually by the ACM and is named for British mathematician Alan M. Turing, who invented the idea of the computer and who helped the Allies crack the Nazi Enigma cipher during World War II. Goldwasser and Micali will formally receive the award during the ACM's annual Awards Banquet on June 15 in San Francisco.

Links:
[1] http://www.acm.org/press-room/news-releases/2013/turing-award-12/