Toyota Technological Institute at Chicago
Distinguished Lecture

PRESENTS:

Shafi Goldwasser
MIT

Title: Pseudo Deterministic Algorithms and Proofs

Abstract: Probabilistic algorithms for both decision and search problems can offer significant complexity improvements over deterministic algorithms. One major difference, however, is that they may output different solutions for different choices of randomness. This is less than desirable in settings where uniqueness of output is important such as in the generation of system-wide cryptographic parameters or in a distributed setting where different sources of randomness are used. Pseudo-deterministic algorithms are a class of randomized search algorithms, which output a unique answer with high probability. Intuitively, they are indistinguishable from deterministic algorithms by a polynomial time observer of their input/output behavior. In this talk I will describe what is known about pseudo-deterministic algorithms in the sequential, sub-linear and parallel setting. I will also describe an extension of pseudo-deterministic algorithms to interactive proofs for search problems where the verifier is guaranteed with high probability to deliver the same output on different executions, regardless of the prover strategies.

Bio: Shafi Goldwasser is Director of the Simons Institute for the Theory of Computing, and Professor of Electrical Engineering and Computer Science at the University of California Berkeley. Goldwasser is also Professor of Electrical Engineering and Computer Science at MIT and Professor of Computer Science and Applied Mathematics at the Weizmann Institute of Science, Israel. Goldwasser holds a B.S. Applied Mathematics from Carnegie Mellon University (1979), and M.S. and Ph.D. in Computer Science from the University of California Berkeley (1984).

Goldwasser's pioneering contributions include the introduction of probabilistic encryption, interactive zero knowledge protocols, elliptic curve primality testings, hardness of approximation proofs for combinatorial problems, and combinatorial property testing.

Goldwasser was the recipient of the ACM Turing Award in 2012, the Gödel Prize in 1993 and in 2001, the ACM Grace Murray Hopper Award in 1996, the RSA Award in Mathematics in 1998, the ACM Athena Award for Women in Computer Science in 2008, the Benjamin Franklin Medal in 2010, the IEEE Emanuel R. Piore Award in 2011, the Simons Foundation Investigator Award in 2012, and the BBVA Foundation Frontiers of Knowledge Award in 2018. Goldwasser is a member of the NAS, NAE, AAAS, the Russian Academy of Science, the Israeli Academy of Science, and the London Royal Mathematical Society. Goldwasser holds honorary degrees from Ben Gurion University, Bar Ilan University, Haifa University, and the University of Oxford, and has received the UC Berkeley Distinguished Alumnus Award and the Barnard College Medal of Distinction. **Host:** Avrim Blum

Friday, November 8, 10:30 – 11:30 am
TTIC Rm 526