Speaker: Zvika Brakerski, Weizmann Institute of Science

Title: 5 years of FHE

Fully Homomorphic Encryption (FHE) allows to transform Enc(x) into Enc(f(x)) for any efficient function f, using only public information. This notion was introduced in 1978 by Rivest, Adleman and Dertouzos, yet a first candidate has only been introduced in 2009 by Gentry. In the 5 years since Gentry's breakthrough, there has been great progress in research on FHE, ranging from improving the security and efficiency, to utilizing FHE towards additional applications. In my talk I will survey some of this progress and try to outline some directions for future study.