

The Faculty of Mathematics and Computer Science
The Weizmann Institute of Science
announces the third

Amir Pnueli Memorial Lecture

to be delivered by

Professor Michael O. Rabin

Hebrew University, Harvard University SEAS

Sponsored by the Arthur and Rochelle Belfer Institute of Mathematics and Computer Science
at The Weizmann Institute of Science

The title:

Miracles of Cryptography and Secrecy Preserving Conduct of Secure Auctions

on Thursday, 20 December 2012, at 16:00
in the Dolfi and Lola [Ebner Auditorium](#), on campus

A reception in honor of Prof. Rabin will be held after the lecture

Abstract

Recently devised novel highly efficient Zero Knowledge Proofs (a surprising concept fully explained in the talk) demonstrate that an auctioneer can receive bids, determine winners and later prove correctness of announced auction results, without revealing any bids values. New work done with Silvio Micali, allows bidders to submit bids in an incoercible and deniable manner. In certain auctions this combined shield of complete secrecy frustrates collusions of bidders against the auctioneer/seller. The talk will be accessible to non-specialists.