מכון ויצמן למדע
WEIZMANN INSTITUTE OF SCIENCE

Faculty of Mathematics and Computer Science
The Weizmann Institute of Science

Distinguished Lecturer Series

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

Professor Michael O. Rabin

Harvard University & Hebrew University of Jerusalem

will speak on

Practically efficient zero knowledge proofs of correctness of computations, and financial cryptography

Abstract: We present a highly efficient method for proving correctness of computations while preserving secrecy of all input and intermediate values.This is done in an Evaluator-Prover model which can also be realized by a secure processor. Applications to secure auctions will be presented.

Joint work with Rocco Servedio and Chris Thorpe.

The lecture will take place in the Schmidt Lecture Hall
on Sunday, May 11, 2008
at 11:00