Oded Goldreich (Weizmann Institute of Science)

Title: **Probabilistic Proof Systems**

Abstract: The glory attached to the creativity involved in finding proofs makes us forget that it is the less glorified process of verification that gives proofs their value. Conceptually speaking, proofs are secondary to the verification process; whereas technically speaking, proof systems are defined in terms of their verification procedures.

The notion of a verification procedure presumes the notion of computation and furthermore the notion of efficient computation.
This implicit stipulation is made explicit in the definition of NP, where efficient computation is associated with deterministic polynomial-time algorithms. However, we can gain a lot if we are willing to take a somewhat non-traditional step and allow probabilistic verification procedures, which have a non-zero error probability. We stress that this error probability is explicitly bounded and can be reduced by successive applications of the proof system.

We shall review three types of probabilistic proof systems, called interactive proofs, zero-knowledge proofs, and probabilistic checkable proofs.
In each of these three cases, we shall present fascinating results that cannot be obtained when considering the analogous deterministic proof systems.