Certifiable Quantum Dice
Umesh Vazirani
U.C. Berkeley

Is it possible to certify that the n-bit output of a random number generator is "really random"? A possible approach to this question is via the theory of algorithmic randomness due to Kolmogorov, Chaitin and Solomonoff, which identifies randomness with uncompressibility by any Turing Machine. Unfortunately this definition does not result in an efficient test for randomness. Indeed, in the classical World it seems impossible to provide such a test.

Quantum mechanics allows for a remarkable random number generator: its output is certifiably random in the sense that if the output passes a simple statistical test, and there is no information communicated between the two boxes in the randomness generating device (based, say, on the speed of light limit imposed by special relativity), then the output is certifiably random. Moreover, the proof that the output is truly random does not even depend upon the correctness of quantum mechanics!

Based on joint work with Thomas Vidick.

http://theory.cs.cmu.edu/seminars/