abstract

Computer Science/Discrete Mathematics Seminar I
Topic:

Speaker:

Affiliation:

Date:

Time/Room:

A trusted source of independent and uniform random bits is a basic resource in many computational tasks, such as cryptography, game theoretic protocols, algorithms and physical simulations. Implementing such a source presents an immediate challenge: how can one certify whether one has succeeded? i.e. suppose someone were to claim that a particular device outputs a uniformly random n-bit string; is there a feasible test to verify that claim? This seems like an impossible task: since the device must output each n-bit string with equal probability there is no basis on which to reject any particular output in favor of any other.

Ideas originating in the study of nonlocality in quantum mechanics suggest a remarkable solution to this conundrum: a random number generator whose output is certifiably random in the sense that if the output passes a simple statistical test, and a no-signaling condition is met between the two boxes in the randomness generating device, then even a quantum skeptic (viz Einstein's famous quote ``God does not play dice with the Universe''), would be convinced that the output is truly random.

Partially dropping the skeptic's hat, I will show how the same ideas can be used to obtain a protocol for key distribution whose security, although it relies on the correctness of quantum mechanics, does not require any assumption on the nature of the quantum mechanical devices used in the protocol. In particular, security of the generated key is guaranteed even if the devices are faulty or even have been handed over to the users by a malicious, computationally unbounded, adversary. These results suggest a powerful paradigm of "device independence" enabling previously impossible tasks under minimal assumptions.

Based on joint work with Umesh Vazirani.