On testing for randomness of a bitstream and applications to cryptography

Rajeeva L. Karandikar

Cranes Software International Limited

We consider one of the simplest testing of hypothesis problem: Is a given bitstream statistically indistinguishable from output of a long sequence of Bernoulli trials (with p=0.5)? The catch here is that we can have a very large sample size - over a million. This situation is common in cryptography and we will discuss a test known as Maurer's test and its applications in cryptography.

`List of invited speakers` `Schedule for December 12`