CORR 2000-12

A Comparison of Two Approaches to Pseudorandomness

Yongge Wang

Abstract The concept of pseudorandomness plays an important role in cryptography. In this note we contrast the notions of complexity-theoretic pseudorandom strings (from algorithmic information theory) and pseudorandom strings (from cryptography). For example, we show that we can easily distinguish a complexity-theoretic pseudorandom ensemble from the uniform ensemble. Both notions of pseudorandom stings are uniformly unpredictable; in contrast with pseudorandom strings, complexity-theoretic pseudorandom strings are not polynomial-time unpredictable.

Keywords pseudorandom generators, Kolmogorov complexity, unpredictability.