The Generation of Cryptographically Strong Pseudo-Random Sequences

Adi Shamir
The Weitzman Institute

A Pseudo-random sequence is cryptographically strong if knowledge of some of its elements does not help to compute other elements. There are many heuristic methods for generating such sequences, but their strength cannot be proved. In this talk I'll present a new method for which a formal proof exists.