Foundations and Trends® in
Theoretical Computer Science
Vol. 7, Nos. 1–3 (2011) 1–336

DOI: 10.1561/0400000010

now
the essence of knowledge

Pseudorandomness

By Salil P. Vadhan

Contents

Foundations and Trends® in
Theoretical Computer Science
Vol. 7, Nos. 1–3 (2011) 1–336

DOI: 10.1561/0400000010

now
the essence of knowledge

Pseudorandomness

Salil P. Vadhan

School of Engineering and Applied Sciences, Harvard University, Cambridge, MA, 02138, USA, salil@seas.harvard.edu

Abstract

This is a survey of *pseudorandomness*, the theory of efficiently generating objects that "look random" despite being constructed using little or no randomness. This theory has significance for a number of areas in computer science and mathematics, including computational complexity, algorithms, cryptography, combinatorics, communications, and additive number theory. Our treatment places particular emphasis on the intimate connections that have been discovered between a variety of fundamental "pseudorandom objects" that at first seem very different in nature: expander graphs, randomness extractors, list-decodable error-correcting codes, samplers, and pseudorandom generators. The structure of the presentation is meant to be suitable for teaching in a graduate-level course, with exercises accompanying each section.