1035-68-1 **Avi Wigderson*** (avi@ias.edu), Institute for Advance Study, Department of Mathematics, Princeton, NJ 08540. *Randomness—A computational complexity view.*

Man has grappled with the meaning and utility of randomness for centuries. Research in the Theory of Computation in the last thirty years has enriched this study considerably. I'll describe two main aspects of this research on randomness, demonstrating its power and weakness respectively.

-Randomness is paramount to computational efficiency:

The use of randomness can dramatically enhance computation (and do other wonders) for a variety of problems and settings. In particular, examples will be given of probabilistic algorithms (with tiny error) for natural tasks in different areas of mathematics, which are exponentially faster than their (best known) deterministic counterparts.

-Computational efficiency is paramount to understanding randomness:

I will explain the computationally-motivated definition of ”pseudorandom” distributions, namely ones which cannot be distinguished from the uniform distribution by efficient procedure from a given class. We then show how such pseudorandomness may be generated deterministically, from (appropriate) computationally difficult problems. Consequently, randomness is probably not as powerful as it seems above.

I'll conclude with the power of randomness in other computational settings, primarily probabilistic proof systems. We discuss the remarkable properties of Zero-Knowledge proofs and of Probabilistically Checkable proofs. (Received September 13, 2007)