Uppsala Abstracts

Abstracts of Papers Presented in Uppsala, Sweden, 13–18 August 1990

2nd World Congress of the
Bernoulli Society for Mathematical Statistics and Probability

53rd Annual Meeting of the Institute of Mathematical Statistics

Edited by George P. H. STYAN, McGill University

Composition by Rachel Victoria Hutton and Tracy Fairchild Bevell
with the assistance of Lachmi Ganeru Connell and Julie Bérubé

TABLE OF CONTENTS

Much of the material in this book, as well as shorter versions of many of the abstracts, were originally published in *The IMS Bulletin*, Vol.19, No.3, 1990; the article on Linnaeus and Celsius appeared originally in *The IMS Bulletin*, Vol.18, No.3, 1989, page 326. Printed by Capital City Press, Inc., P.O. Box 546, Montpelier, Vermont 05602-8903, USA, from camera-ready copy prepared in the editorial offices of *The IMS Bulletin* in the Dept. of Mathematics and Statistics, McGill University, 805 ouest, rue Sherbrooke Street West, Montréal, Québec, Canada H3A 2K6.

Copyright © 1990 by the Institute of Mathematical Statistics
and the Bernoulli Society for Mathematical Statistics and Probability

Printed in the United States of America

IP36-1. PSEUDO-RANDOM GENERATORS FROM ONE-WAY FUNCTIONS

Michael LUBY*, *International Computer Science Institute, Berkeley, California*,
Johan HÅSTAD, *Kungliga Tekniska Högskolan, Stockholm*,
Russell IMPAGLIAZZO, *University of Toronto*,
and Leonid LEVIN, *Boston University*.

One of the basic primitives in cryptography and other areas of computer science is a pseudo-random generator. The usefulness of a pseudo-random generator is demonstrated by the fact that it can be used to construct a private key cryptosystem that is secure even against chosen plain-text attack. A pseudo-random generator can also be used to conserve random bits and allows reproducibility of results in Monte Carlo simulation experiments. Intuitively, a *pseudo-random generator* is a polynomial time computable function g that stretches a short random string x into a much longer string $g(x)$ that "looks" just like a random string to *any* polynomial time adversary that is allowed to examine $g(x)$. [This should be contrasted with the classical definition of a pseudo-random generator. A classical pseudo-random generator is required to pass a particular set of statistical tests, but does not necessarily satisfy the more general requirement that it pass all polynomial-time tests. This is a particularly important distinction in the context of cryptography, where the adversary must be assumed to be as malicious as possible, with the only restriction on tests being computation time.]

It follows then that a pseudo-random number generator can be used to efficiently convert a small amount of true randomness into a much longer string that is indistinguishable from a truly random string of the same length to any polynomial time adversary. On the other hand, there seem to be a variety of natural examples of another basic primitive; the one-way function. Intuitively, a function f is one-way if: (1) given any x, $f(x)$ can be computed in polynomial time; (2) given $f(x)$ for a randomly chosen x, it is not possible on average to find an inverse x' such that $f(x') = f(x)$ in polynomial time. It has not been proven that there are any one-way functions, but there are a number of problems from number theory, coding theory, graph theory, and combinatorial theory that are candidates for problems that might eventually be proven to be one-way functions. We show how to construct a pseudo-random generator from *any* one-way function. [Received: 15 March 1990.]

IP36-2. KOLMOGOROV COMPLEXITY AND ALGORITHMIC RANDOMNESS: RECENT DEVELOPMENTS

A. Kh. SHEN', *Institute for Information Transmission, Moscow*.

(1) Connections between frequency and complexity approaches to randomness. (2) Algorithmic definition of randomness as a tool for analysing classical results in probability theory. (3) Some mathematical questions and philosophical speculations about algorithmic complexity and information theory. [Received: 26 April 1990.]