acm
Association for Computing Machinery
Advancing Computing as a Science & Profession

Contacts:
Paul Beame
ACM SIGACT Chair
206-543-5114
beame@cs.washington.edu

Virginia Gold
ACM
212-626-0505
vgold@acm.org

ACM SIGACT, IEEE-CS AWARD KNUTH PRIZE TO CO-DISCOVERER OF NP-COMPLETENESS

Boston University's Levin Cited for Innovations in Computational Complexity and Cryptography

NEW YORK, August 22, 2012 – The ACM Special Interest Group on Algorithms and Computation Theory (SIGACT) **http://sigact.acm.org** and the IEEE Computer Society Technical Committee on the Mathematical Foundations of Computing (TCMF) will jointly present the 2012 Knuth Prize to Leonid Levin for his visionary research in complexity, cryptography, and information theory, including the discovery of NP-completeness. Working in the Soviet Union at the same time as Stephen Cook in the United States, Levin made his discovery of NP-completeness, the core concept of computational complexity. This discovery best explains why many computational problems require prohibitively slow brute-force solutions. Levin also developed the theory of "average-case NP-completeness," for problems considered intractable on average.

The Knuth Prize is named in honor of Donald Knuth of Stanford University who has been called the "father" of the analysis of algorithms. It will be presented at the Symposium on Foundations of Computer Science (FOCS 2012), sponsored by the IEEE Computer Society TCMF, in New Brunswick, NJ, October 21-23, where Levin will give the Knuth Prize Lecture.

With co-authors Laszlo Babai, Lance Fortnow, and Mario Szegedy, Levin also provided a key step in the proof of the celebrated PCP Theorem, the cornerstone of the theory of computational hardness of approximation. It investigates the inherent difficulty in designing efficient approximation algorithms for various optimization problems. Together, this team proposed the notion of "holographic proofs," whose correctness can be checked efficiently by a program that samples only a small fraction of the bits.

In cryptography theory, Levin co-authored the "Goldreich-Levin hardcore bit" with Oded Goldreich, which has become an essential ingredient in many subsequent key results to establish improved security. He also changed the landscape of Kolmogorov complexity, a modern notion of randomness dealing with the quantity of information in individual objects. Andrey Kolmogorov, a

Russian mathematician, was Levin's doctoral advisor at Moscow University. Levin's advances have become essential tools in the research area of algorithmic information.

A professor of Computer Science at Boston University, Levin earned a Master's degree and a Ph.D. equivalent at Moscow University. He was awarded a Ph.D. from the Massachusetts Institute of Technology.

The Knuth Prize, previously presented every 18 months, will now be given annually by ACM SIGACT and the IEEE Computer Society TCMF and includes a $5,000 award.

About ACM

ACM, the Association for Computing Machinery www.acm.org is the world's largest educational and scientific computing society, uniting computing educators, researchers and professionals to inspire dialogue, share resources and address the field's challenges. ACM strengthens the computing profession's collective voice through strong leadership, promotion of the highest standards, and recognition of technical excellence. ACM supports the professional growth of its members by providing opportunities for life-long learning, career development, and professional networking.

About SIGACT

The ACM Special Interest Group on Algorithms and Computation Theory http://sigact.acm.org fosters and promotes the discovery and dissemination of high quality research in the domain of theoretical computer science. The field includes algorithms, data structures, complexity theory, distributed computation, parallel computation, VLSI, machine learning, computational biology, computational geometry, information theory, cryptography, quantum computation, computational number theory and algebra, program semantics and verification, automata theory, and the study of randomness. Work in this field is often distinguished by its emphasis on mathematical technique and rigor.

# # #