Hayden-Howard Lecture

Inaugurated in the spring semester of 2001 by a generous contribution to the University of Kentucky Department of Mathematics, the Hayden-Howard Lecture series was established to honor mathematics professors Thomas Hayden and Henry Howard. This new series endows an annual lecture by a research mathematician of international stature. For more information about giving to the UK College of Arts and Sciences, contact (859) 257-5455 or www.uky.edu/ArtsSciences.

Previous Hayden-Howard Lecturers:

Professor Richard Stanley (MIT), 2000-01
Professor Craig Evans (Berkeley), 2001-02
Professor Craig Huneke (University of Kansas), 2002-03
Professor Doron Zeilberger (Rutgers University), 2003-04
Professor Gang Tian (Princeton University and MIT), 2004-05
Professor FangHua Lin (New York University), 2005-06
Professor John Neuberger (University of No. Texas), 2006-07

Hayden-Howard Lecture 2008

Three Challenges of Claude Shannon

Dr. Joachim Rosenthal
Mathematics Institute
University of Zürich, Switzerland

4 p.m. Wednesday, April 2, 2008
Student Center, Room 230
University of Kentucky

About the Speaker

Joachim Rosenthal is a Professor of Applied Mathematics in the Department of Mathematics at the University of Zürich and Adjunct Professor at the University of Notre Dame. He received his diploma in Mathematics from the University of Basel in 1986 and the Ph.D. in Mathematics from Arizona State University in 1990.

From 1990 until 2006 he was with the Department of Mathematics at the University of Notre Dame, where he was last the Notre Dame Professor in Applied Mathematics and Concurrent Professor of Electrical Engineering. In the academic year 1994/1995 he spent a sabbatical year at CWI, the Center for Mathematics and Computer Science in Amsterdam, The Netherlands.

His current research interests are in coding theory and cryptography. In coding theory he is interested in convolutional codes, LDPC codes and more general codes on graphs. In cryptography his main interest lies in the construction of new one-way trapdoor functions.

About the Topic

"Three Challenges of Claude Shannon"

ABSTRACT: In 1948/1949 Claude Shannon wrote two papers [Sha48, Sha49] which became the foundation of modern information theory. The papers showed that information can be compressed up to the `entropy', that data can be transmitted error free at a rate below the capacity and that there exist provable secure cryptographic systems. These were all fundamental theoretical result. The challenge remained to build practical systems which came close to the theoretical optimal systems predicted by Shannon.

In this overview talk we will explain how the first two challenges concerning coding theory have resulted in practical solutions which are very close to optimal. Then we explain why the gap between the practical implementation of cryptographic protocols with the theoretical result of Shannon is largest.

The talk will be tutorial in nature and should be accessible to advanced undergraduate students.

[Sha48] C.E. Shannon, A mathematical theory of communication, Bell Syst. Tech. J. (1948), 379-423 and 623-656.

[Sha49] C.E. Shannon, Communication theory of secrecy systems, Bell System Tech. J. (1949), 656-715.