



**Association for  
Computing Machinery**

*Advancing Computing as a Science & Profession*

**Contact:**

Virginia Gold  
ACM  
212-626-0505  
v\_gold@acm.org

**CRYPTOGRAPHY EXPERT WINS ACM DOCTORAL DISSERTATION AWARD**

**Microsoft Researcher Honored for Advances in Privacy Protection for Information Retrieval**

**NEW YORK**, May 22, 2008 – Sergey Yekhanin, a researcher at Microsoft Research Silicon Valley Lab, has won the [2007 Doctoral Dissertation Award](#) from ACM (the Association for Computing Machinery) for developing a novel approach to protecting the privacy of users' queries when they are accessing a public database. His dissertation is titled "Locally Decodable Codes and Private Information Retrieval Schemes." Yekhanin, nominated by Massachusetts Institute of Technology (MIT), will receive the Doctoral Dissertation Award and its \$20,000 prize at the annual ACM Awards Banquet on June 21, in San Francisco, CA. Financial sponsorship of this award is provided by Google Inc.

The issue of preserving individual privacy and anonymity without impairing the user's ability to access various web resources is an important component in making cyber-infrastructure secure and more usable. Private information retrieval (PIR) schemes allow a user to retrieve an item from a server that hosts a database without revealing which item the user is retrieving. PIRs are closely related to a special kind of error-correcting code known as locally decodable codes (LDCs). They are used to ensure reliable transmission of information over noisy channels, and to provide reliable storage information on a medium that is subject to corruption and reading errors.

Yekhanin's research provides a fresh algebraic look at the theory of PIR schemes and LDCs, and creates new families of PIRs and LDCs that have much better parameters than those previously constructed. For PIRs, these parameters include communication complexity, which counts the number of bits exchanged between the

user and the servers, and the number of servers involved in a protocol. For LDCs, these parameters include codeword length, which measures the amount of redundancy that is introduced into the message by the encoder; and query complexity, which counts the number of bits that need to be read from the codeword in order to recover a single bit of message.

Yekhanin's results have also yielded progress in the areas of protection for data storage, secure multi-party computation, and computational complexity.

A graduate of Moscow State University in Russia, Yekhanin received his Ph.D. degree in computer science from MIT. Before joining Microsoft Research, he was a member of the School of Mathematics at the Institute for Advanced Study in Princeton, NJ.

Three recipients received Honorable Mention for the 2007 ACM Doctoral Dissertation Award, which carries a \$10,000 prize, with financial sponsored provided by Google. They are:

- Benny Applebaum, a post doctoral candidate at Princeton University, for his dissertation “Cryptography in Constant Parallel Time,” nominated by Technion – Israel Institute of Technology
- Yan Liu, a Research Staff Member at IBM Research, for her dissertation “Conditional Graphical Models for Protein Structure Prediction,” nominated by Carnegie Mellon University
- Vincent Conitzer, Assistant Professor of Computer Science and Economics at Duke University, for his dissertation “Computational Aspects of Preference Aggregation,” nominated by Carnegie Mellon University.

#### **About ACM**

*ACM, the Association for Computing Machinery [www.acm.org](http://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.*

###