Contact: Virginia Gold
212-626-0505
vgold@acm.org

INNOVATOR OF BREAKTHROUGH CRYPTOGRAPHY TECHNOLOGY WINS ACM DOCTORAL DISSERTATION AWARD

Garg Developed Technique to Protect Against Cyberattacks

NEW YORK, May 8, 2014 – Sanjam Garg has won the 2013 Doctoral Dissertation Award presented by ACM (the Association for Computing Machinery) for developing tools that enable the first secure solution to the problem of making computer program code "unintelligible" while preserving its functionality. This problem, known as software obfuscation, conceals the program's purpose or its logic in order to prevent tampering, deter reverse engineering, or as a challenge to readers of the source code. His approach makes it impossible to reverse-engineer the obfuscated software without solving mathematical problems that could take hundreds of years to work out on today's computers.

Garg, a Josef Raviv Memorial Postdoctoral Fellow at IBM T.J. Watson Research Center, completed his dissertation at the University of California, Los Angeles, which nominated him. A graduate of the Indian Institute of Technology, Delhi, he 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 the award is provided by Google Inc.

In his dissertation "Candidate Multilinear Maps," Garg described new mathematical tools that serve as key ingredients for transforming a program into a "jigsaw puzzle" of encrypted pieces. Corresponding to each input is a unique set of puzzle pieces that, when assembled, reveal the output of the program. Security of the obfuscated program hinges on the fact that illegitimate combinations of the puzzle pieces do not reveal anything.

Honorable Mention for the 2013 ACM Doctoral Dissertation Award went to Grey Ballard of Sandia National Laboratories and Shayan Oveis Gharan of the University of California, Berkeley. They will share a $10,000 prize, with financial sponsorship provided by Google Inc.

Grey Ballard's dissertation, "Avoiding Communication in Dense Linear Algebra," explores fundamental computations within dense linear algebra, and whether significant improvement of the current algorithms for these computations is possible given the communication they require and their performance in practice. He received B.S. and M.A. degrees from Wake Forest University, and a Ph.D. degree from the University of California, Berkeley. He is a Truman Fellow at Sandia National Laboratories.

Shayan Oveis Gharan's dissertation, "New Rounding Techniques for the Design and Analysis of Approximation Algorithms," develops new approximation algorithms for two classical optimization problems, the Traveling Salesman and Graph Partitioning. He introduces new techniques for rounding a solution of a successive relaxation of these problems into near optimal integral solutions.

A graduate of Sharif University of Technology in Tehran, Iran with a B.S. degree in Computer Engineering, he received a Ph.D. degree from Stanford University. He is a Postdoctoral Miller Fellow at the University of California, Berkeley and will join University of Washington's computer science department as an assistant professor in the winter of 2015.

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.

# # #