acm

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

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

CRAIG GENTRY WINS ACM AWARD FOR MAJOR INNOVATION IN ENCRYPTION TECHNOLOGY

Doctoral Candidate Developed Scheme that Could Spur Advances in Cloud Computing, Search Engine Queries, and E-Commerce

NEW YORK, June 16, 2010 – Craig Gentry has won the 2009 Doctoral Dissertation Award http://awards.acm.org/doctoral_dissertation/ from ACM (the Association for Computing Machinery) for his breakthrough scheme that solves a central problem in cryptography—enabling computer systems to perform calculations on encrypted data without decrypting it. His dissertation, entitled "A Fully Homomorphic Encryption Scheme," adds a crucial layer of safety and privacy to the online world in settings ranging from banking and healthcare to networks and cloud computing. This approach allows users to outsource the processing of data without giving away access to the data. Gentry, who was nominated by Stanford University, is a research staff member in the Cryptography group at IBM T.J. Watson Research Center. He will receive the Doctoral Dissertation Award and its $20,000 prize at the annual ACM Awards Banquet on June 26, in San Francisco, CA. Financial sponsorship of the award is provided by Google Inc.

Using Gentry's technique, computer vendors who store the confidential electronic data of others would be able to fully analyze data on their clients' behalf without expensive interaction with the client, and without seeing any of the private data, providing a boost to cloud computing. Users could submit an encrypted query to a search engine, and the search engine would compute a succinct encrypted answer without ever looking at the query directly.

The idea of homomorphic encryption was first proposed by Ronald Rivest, Leonard Adleman and Michael Dertouzos more than 30 years ago. This development occurred shortly after Rivest, Adi Shamir, and Adleman invented the RSA encryption scheme that earned them the 2002 ACM A.M. Turing Award **http://awards.acm.org/turing.** But until Gentry's breakthrough, it was unclear whether fully homomorphic encryption was even possible.

Gentry's elegant solution to this epic cryptographic problem starts with a "somewhat homomorphic" encryption scheme using mathematical systems known as "ideal lattices." By modifying this scheme

slightly, it becomes "bootstrappable," or homomorphic enough to handle its own decryption function, leading to a fully homomorphic encryption scheme. In further research, Gentry and his coauthors from IBM and the Massachusetts Institute of Technology have been able to achieve this result using simple integers rather than ideal lattices.

Currently, Gentry's scheme is computationally expensive, requiring more theoretical work to make it more efficient. In the case of a search engine query, for instance, it is estimated that performing the process with encrypted keywords would multiply the necessary computing effort by about one trillion. Recently, two teams of researchers, including Gentry and Shai Halevi at IBM, demonstrated progress by performing the entire bootstrapping procedure in a few minutes.

A mathematics major at Duke University, Gentry received a law degree from Harvard University and specialized in intellectual property at a New York law firm. Returning to his math background, he worked as a senior research engineer at DoCoMo USA Labs on the security and cryptography project from 2000 to 2005, and then enrolled in the computer science Ph.D. program at Stanford University. At a three-month summer internship at IBM in 2008, he discovered the crucial bootstrapping step, and earned his Ph.D from Stanford in 2009.

Three researchers will share an Honorable Mention for the 2009 ACM Doctoral Dissertation Award, which carries a $10,000 prize, with financial sponsorship provided by Google. They are:

- Haryadi Gunawi, nominated by the University of Wisconsin – Madison for his dissertation "Towards Reliable Storage Systems." He is a post-doctoral scholar at the University of California, Berkeley.
- André Platzer, nominated by the University of Oldenburg, Germany, for his dissertation "Differential Dynamic Logics: Automated Theorem Proving for Hybrid Systems." He is an assistant professor at Carnegie Mellon University
- Noah Snavely, nominated by the University of Washington for his dissertation "Scene Reconstruction and Visualization from Internet Photo Collections." He is an assistant professor at Cornell University.

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.*

# # #