THE UNIVERSITY OF TEXAS AT DALLAS
ERIK JONSSON SCHOOL OF ENGINEERING & COMPUTER SCIENCE

UTD

about undergraduate graduate research people industry relations news & events contact

DEPARTMENT OF COMPUTER SCIENCE
THE ERIK JONSSON SCHOOL
OF ENGINEERING & COMPUTER SCIENCE
AT THE UNIVERSITY OF TEXAS AT DALLAS

CS COLLOQUIUM

Computer Science Home

Fri., Nov. 4, 2011

2 p.m.

ECSS 2.212

Refreshments will be served at 1:45 p.m.

"A Homomorphic Encryption System"

Professor Mahadevan Gomathisankaran, University of North Texas

Abstract

Homomorphic encryption has been studied for a long time. A homomorphic encryption system allows one to perform the computations on encrypted data thus enabling delegations of computations to an untrusted entity without the loss of privacy. The recent paradigm of cloud computing, which aggregates the computing, storage and network resources, makes such an encryption system all the more necessary to preserve privacy on the cloud. Rivest, Adleman, and Dertouzos introduced this notion and recently Gentry proposed a homomorphic encryption system. While Gentry's scheme is semantically

secure but it is not practical. In this presentation, we propose a practical homomorphic encryption system which overcomes the drawbacks of Gentry's scheme.

Bio

Professor Mahadevan Gomathisankaran is an Assistant Professor in Computer Science and Engineering at the University of North Texas. He received his Ph.D. degree in Computer Engineering from Iowa State University. He is the recipient of IBM Ph.D. Fellowship award for the academic years 2004 and 2005. Professor Mahadevan is interested in building secure computing systems. Towards that goal he has designed various cryptographic functions that achieve the required security with minimal circuit complexity, proposed new secure processor architecture that root the security in the hardware, and designed a testing framework that can test the security of the systems.

Updated: October 25, 2011