HORNS: A Novel Homomorphic Encryption System and its Application

Gomathisankaran Mahadevan, Univ. of North Texas

Apr 23 Tuesday, 12:30 to 1:30pm

Venue – CS 209

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 a 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 paper we propose a practical homomorphic encryption system which overcomes the drawbacks of Gentry's scheme.

Brief Bio – 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. 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.