Computer Science Colloquium

Thursday, March 19, 2015 **Nguyen Engineering 4201**

9:30 am-10:30 am

Omkant Pandey

Computing on Unbounded Private Data

Today, a large amount of private data resides in the cloud in an encrypted form. There are tremendous benefits of performing computations on this data to extract useful information. Yet, security of encryption seems inimical to this goal.

This raises the following fundamental question: Can the cloud perform general computations on encrypted datasets of unbounded size (without knowing the decryption key)?

My research provides the first positive resolution of this question. In this talk I will describe these new results, and discuss their interplay with other broad questions in cryptography.

Biography

Omkant Pandey is a postdoctoral researcher at the University of Illinois at Urbana Champaign (UIUC). He is interested in the broad areas of secure computation and next-generation encryption systems. He received his Ph.D. from UCLA, and has published over 20 original research papers at venues such as CRYPTO, EUROCRYPT, TCC, and ACM CCS, including an influential work on Attribute Based Encryption with over 1600 citations.