

## Computer Science Seminar Series

### National Capital Region

## Order-Preserving Encryption

**Speaker: Prof. Adam O'Neill**

Georgetown University

**Friday, September 18, 2015**

**1:00PM- 2:00PM, NVC 325**

### Abstract

Order-preserving encryption is a type of symmetric-key encryption that encrypts larger plaintexts to larger ciphertexts. It was originally proposed in the database community in 2004 due to its attractive properties for allowing range queries on encrypted data. In this talk, I will overview my work that put order-preserving encryption on a rigorous cryptographic foundation. I will first discuss possibilities for defining the security of order-preserving encryption, showing along the way that, perhaps surprisingly, straightforward attempts yield definitions that are unachievable. The definition we end up targeting has some curious properties as well: it does not really tell us what security properties such a scheme ensures, just that they are in some sense “as strong as possible.” We construct a highly efficient scheme under this definition based on a blockcipher and black-box sampling of the hypergeometric distribution on large domains. We then return to the question of what security properties such a scheme ensures, and provide a combinatorial analysis showing that the lower-half the plaintext bits are hidden.

### Biography



Adam O'Neill is an Assistant Professor in the Computer Science Department at Georgetown University. He also holds a guest faculty appointment at NIST. He received his Ph.D. from the Georgia Institute of Technology and previously held postdoctoral research position at the University of Texas at Austin and Boston University. His main research interest is cryptography.