Order-Revealing Encryption: Definitions, Constructions, and Challenges

David Wu, University of Virginia

An order-revealing encryption (ORE) scheme is an encryption scheme where there is a public function that can be used to compare ciphertexts. Because ORE enables comparisons over encrypted data, they are a natural cryptographic primitive for building systems that support searching over encrypted data.

In this talk, I will provide a general survey of the definitions, constructions, and security of ORE. I will conclude by discussing some of the challenges in leveraging ORE for building encrypted databases.