**Leakage Suppression and Structured Encryption**

Tarik Moataz, Brown University

Structured encryption (STE) schemes encrypt data structures in such a way that they can be privately queried. One aspect of STE that is still poorly understood is its leakage. This talk will walk through leakage suppression-- a new research direction that focused on designing "low-leakage" schemes.

In the first part of this talk, we will describe a general framework to design STE schemes that do not leak the query/search pattern. We show that our framework produces STE schemes with query complexity that is asymptotically better than ORAM simulation in certain (natural) settings. We use our framework to design a new STE scheme that is "almost" zero-leakage in the sense that it reveals an, intuitively-speaking, small amount of information. We also show how the scheme can be used to achieve zero-leakage queries when one can tolerate a probabilistic guarantee of correctness.

In the second part of this talk, we will go over new techniques to suppress other types of leakage patterns. Specifically, we focus on the design of volume-hiding encrypted multi-maps; that is, of encrypted multi-maps that hide the response length to computationally-bounded adversaries. We describe the first two volume-hiding STE schemes that do not rely on naive padding and have efficient query complexity and/or storage. Beyond the fundamental interest of suppressing leakage, this new generation of schemes can help thwart most (if not all) existing single-keyword or range attacks.