Speaker: Seny Kamara, Microsoft Research, Redmont

Title: Structured Encryption and Leakage Suppression

This work studies the leakage of structured and searchable encryption. We propose a new model for describing and understanding leakage in these increasingly important primitives with the aim of providing a foundation for the design of new and efficient techniques to suppress it.
We show that structured encryption provides a powerful abstraction that captures, not only searchable symmetric encryption (SSE), but also oblivious RAMs (ORAM). From this new, more general, perspective we describe a general transformation based on Goldreich and Ostrovsky's Square-Root ORAM solution that can suppress the query equality leakage (also known as the query or search pattern) of a large class of structured and searchable encryption schemes \emph{without the overhead of an ORAM simulation}. We apply this transformation to a new SSE construction to obtain the first practical SSE scheme that does not leak the access and search patterns. This solves a long-standing open problem in the area of encrypted search.

Joint work with Olya Ohrimenko