Private DB: Big-size searching from (many) small-size MPC instances

Vlad Kolesnikov, Georgia Tech

In this talk, I will briefly discuss Blind Seer, a private database system, at whose core is secure evaluation of many small-size MPC instances. I will briefly discuss the Blind Seer approach. I will spend most of the time discussing related and supporting topics, such as: relevant security models and trade offs, improving performance of corresponding MPC protocols, and Blind Seer relationship to SSE (symmetric searchable encryption).

This is joint work with Ben Fisch, Vasilis Pappas, Fernando Krell, Binh Vo, Abishek Kumarasubramanian, Tal Malkin, Seung Geol Choi, Wesley George, Angelos D. Keromytis, and Steven M. Bellovin