Private Data Access via Function Secret Sharing

Elette Boyle, IDC Herzliya

We propose an avenue toward practical private manipulation of remotely held databases, via the cryptographic tool of Function Secret Sharing (FSS) (Boyle et al. Eurocrypt'15). Our solutions apply when the database is held by a small number of non-colluding servers.

An FSS scheme is an ""additive secret sharing"" of functions, enabling one to split functions f from a given class F into functions f_i that individually hide f, and which support a simple additive per-input reconstruction. FSS for appropriate function classes yields private database queries/updates of various complexities. Paired with recent advances in FSS constructions, this provides a promising direction for efficient solutions within the multi-server domain.

This talk will present the connection between FSS and private database manipulation, and survey the state of the art in FSS.