A Review of Database Reconstruction

Brice Minaud, Inria and ENS

A growing number of articles show how the contents of a database may be inferred from the leakage of searchable encryption schemes. This has been especially the case for schemes supporting range queries, and other query types that display a similar "range-like" behavior. These attacks often require orthogonal assumptions, and exploit different underlying tools. In this talk, I will attempt to provide a coherent view of these attacks, the relationships that exist between them, and their implications. I will conclude with some open problems.