DEX: an Encrypted Relational Database

Zheguang Zhao, Brown University

End-to-end encrypted databases (EDBs) has been long studied in the context of relational database management systems. Previous schemes based on quantization or property-preserving encryption (PPE) reveal nontrivial information about the data such as membership, equality and order. Structured encryption (STE) is a less leaky scheme, but designing STE-based relational EDBs remains challenging. In fact, it has been the main open problem in the area of encrypted search for over a decade. Kamara and Moataz recently showed, for the first time, that STE-based relational EDBs could be constructed in their scheme SPX. However, SPX is constructed around encrypted multi-maps and does not have trivial adaptation to relational databases.

On the other hand, one major obstacle to wide adoption of end-to-end encrypted systems is that end-to-end encryption breaks many of the applications and services including cloud computing, data analytics and search.

In this work, we bridge the gap by describing an emulation technique that adapts SPX to existing relational databases without modification. Our technique is only based on relational algebra or SQL and thereby does not break existing applications and services such as PostgreSQL or SparkSQL. We discuss query optimization, storage trade-offs, and other techniques towards making structured encrypted relational databases more practical.