Weakly Randomized Encryption

Charles Wright, Portland State University

Efficiently searchable and easily deployable encryption schemes enable an untrusted, legacy service such as a relational database engine to perform searches over encrypted data. The ease with which such schemes can be deployed on top of existing services makes them especially appealing in operational environments where encryption is needed but it is not feasible to replace core infrastructure components like databases. Unfortunately all previously known approaches for efficiently searchable and easily deployable encryption are vulnerable to inference attacks where an adversary can use knowledge of the data distribution to recover the plaintext with high probability.

We present a new efficiently searchable, easily deployable database encryption scheme that is provably secure against offline inference attacks. Experimental results on a Haskell prototype with databases of up to 10 million records show that our construction achieves a reasonable balance of security, deployability and performance.