Parameter-Hiding Order Revealing Encryption

Cong Zhang, Rutgers University

Order-revealing encryption (ORE) is a popular primitive for outsourcing encrypted databases, as it allows for efficiently performing range queries over encrypted data. Unfortunately, a series of works, starting with Naveed et al. (CCS 2015), have shown that when the adversary has a good estimate of the distribution of the data, ORE provides little protection. In this work, we consider the case that the database entries are drawn identically and independently from a distribution of known shape, but for which the mean and variance are not (and thus the attacks of Naveed et al. do not apply). We dene a new notion of security for ORE, called parameter-hiding ORE, which maintains the secrecy of these parameters. We give a construction of ORE satisfying our new definition from bilinear maps.