Supporting less-than queries on encrypted data using multi-server secret sharing and practical order-revealing encryption

Nathan Chenette, Rose-Hulman Institute of Technology

We consider searchable encryption schemes where query responses are computed jointly by several connected servers. For a security model, we assume at most one of the servers is compromised at any time. Using secret sharing, an elegant technique can support some functionality quite naturally and with a high level of security; however, a less-than query is more challenging to implement securely. One possible solution involves using a practical order-revealing encryption (ORE) scheme to leak only an "acceptable" amount of information. The central question that we address is whether, by using a practical ORE, we can guarantee less information leakage than with a simpler, non-ORE solution.