Abstract

Order Preserving Encryption (OPE) schemes have been examined to a great extent in the cryptography literature because of their prospective application to database design. OPE is an appealing method for database encryption as it permits to execute sort and range queries in an efficient manner without decrypting the data. Databases such as CryptDB are beginning to employ encryption to guard sensitive data. No existing OPE schemes that were proposed in the literature achieved IND-OCPA security except mutable Order-Preserving Encoding (mOPE) scheme, the first OPE scheme that satisfies IND-OCPA with respect to OPE encodings. However, mOPE scheme uses DET (deterministic encryption) to encrypt the plaintext values which leads to leakage of distribution of plaintext domain. This paper proposes a scheme called as Randomized Order Preserving Encryption (ROPE), a novel OPE scheme that leaks nothing beyond the order. ROPE follows the mOPE scheme by contributing randomness to it, so as to accomplish IND-OCPA security. The ROPE scheme implements insert, delete and query functions on an encrypted MySQL database. ROPE scheme permits various SQL queries to be employed instantly on encrypted data. The performance of ROPE scheme is compared with the existing DOPE scheme and observed that there is a query retrieval time overhead. Still, ROPE scheme renders more confidentiality and attains the IND-OCPA security for OPE when compared to the existing OPE schemes.
References

A New Randomized Order Preserving Encryption Scheme


Index Terms
  Computer Science
  Security

Keywords
  ROPE  treeencoding  AVL tree  IND-OCPA  Trusted Proxy and RND