* Order-Revealing Encryption (ORE)

Goal Given the ciphertexts, determine the order of messages being encrypted.

⇒ allows for efficient range queries
sorting.
threshold filtering.

- introduced by Boneh et al. @ Eurocrypt'15. [BLR+15]
- cf. OPE. - the ciphertexts are no longer numerical
  - ORE provides another public (keyless) algorithm that compares the ciphertext.

ORE

- KeyGen(1^λ) → sk
- Enc(sk, m) → c
- CMP(c_1, c_2) → b where $b = \begin{cases} 1 & \text{if } c_1 \geq c_2 \\ 0 & \text{if } c_1 < c_2. \end{cases}$

Security of ORE → "the most" challenge problem.

i) Provable Secure : should reveal no more than ordering of plaintexts

ii) short in ctxt size : should be about the same as the size of the plaintext

iii) Stateless and Non-Interactive : encryption should be able to compute in parallel and independently of one another.

iv) practical : should rely on simple, realizable and efficient cryptographic primitives.

Related Works

- [BLR+15] : based on multilinear maps (@ Eurocrypt'15)
- [CLWW16] : the first "bit" that differs is revealed. (@ FSE'16)
- [LW16] : the first "block" that differs is revealed. (@ ccs'16)