Functional Encryption

* Motivation

- encryption is a method to send a message or data to a single entity holding sk.
- access to the encrypted data is all or nothing. i) can decrypt and read the entire message.

  ii) can learn nothing at all about message.

*Goal: want to "only" give access to a function of the message. e.g, decrypt the target face from the encrypted image.

Def. A functional encryption (FE) for a functionality F defined over $(\overset{\text{key space}}{K}, \underset{\text{plaintext space.}}{X})$ is a tuple of 4 algorithms:

- $\text{Setup}(1^\lambda) \to (pp, msk)$
- $\text{KeyGen}(mk, k) \to sk$ for $k \in K$.
- $\text{Enc}(pp, x) \to c$ for $x \in X$. one FE only supports the specific function.
- $\text{Dec}(sk, c) \to y$ where $y = F(k, x)$ with probability 1.

e.g, Searchable Encryption (SE): allows encryption while still enabling search for keywords

Order - Preserving Encryption (OPE): ciphertexts that preserve the order of plaintexts.

$$m_1 < m_2 \text{ iff } ct_1 < ct_2$$

Order - Revealing Encryption (ORE): generalized notion of OPE.

$$m_1 < m_2 \text{ iff } \text{CMP}(ct_1, ct_2) = 1.$$

Inner - Product Encryption (IPE). etc.

→ allows for efficient range queries, sorting and threshold filtering on encrypted data.