Functional Encryption

- 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
  - one can decrypt and read the entire message
  - one can learn nothing at all almost message

<u>Goal</u> want to *only* give access to a function of the message

- e.g., decrypt the target face from the encrypted images

Def. A functional encryption (FE) for a functionality F defined over $(\mathcal{K}, \mathcal{X})$:

- $\mathsf{Setup}(1^\lambda) \to (pp, msk)$
- $\mathsf{KeyGen}(msk, k) \to sk$ for $k \in \mathcal{K}$
- $\mathsf{Enc}(pp, x) \to c$ for $x \in \mathcal{X}$
- $\mathsf{Dec}(sk, c) \to y$ where $y = F(k, x)$ with probability 1

Note that one functional encryption only supports *the specific* function

Example.

- Searchable Encryption (SE)
  - allows encryption while still enabling search for keywords
- Order-Preserving Encryption (OPR)
  - ciphertexts that preserve the order of plaintexts

$$m_1 < m_2 \text{ if and only if } c_1 < c_2$$

- Order-Revealing Encryption (ORE)
  - the cipher texts are no longer numerical
  - provides another public (keyless) algorithm that compoares the ciphertexts
- Inner-Product Encryption (IPE), etc.

Order-Revealing Encryption

introduced by Boneh et al. [BLR+15] @ Eurocrypt'15

<u>Goal</u> given the ciphertexts, determine the order of messages being encrypted

- allows for efficient range queries, sorting, threshold filtering

Def. An order-revealing encryption (ORE) is defined by:

- $\mathsf{KeyGen}(1^\lambda) \to sk$
- $\mathsf{Enc}(sk, m) \to c$
- $\mathsf{CMP}(c_1, c_2) \to b \in \{0, 1\}$
  - $b = 1$ if $c_1 < c_2$
  - $b = 0$ if $c_1 \geq c_2$

Security of ORE

- Provable Secure
  - should reveal no more than ordering of plaintexts
- Short Ciphertext Size
  - should be about the same as the size of the plaintexts
- Stateless and Non-Interactive
  - encryption should be able to compute in parallel and independently of one another
- Practical
  - should rely on simple, reliable and efficient cryptographic primitives

Recent Works

- [BLR+15] @ Eurocrypt'15
  - based on multilinear maps which is a impractical cryptographic primitive
- [CLWW16] @ FSE'16
  - the first different *bit* is revealed
- [LW16] @ CCS'16
  - the first different *block* is revealed

Construction of [CLWW16]

Let $\mathcal{K}$ be the key space and $[n] = \{1, 2, \ldots, n\}$.

Define a secure PRF $F : \mathcal{K} \times ([n] \times \{0, 1\}^{n-1}) \to \mathbb{Z}_M$ with $M \geq 3$.

- $\mathsf{KeyGen}(1^\lambda)$;
  - Output $sk \leftarrow \mathcal{K}$
- $\mathsf{Enc}(sk, m)$;
  - Let $b_1 b_2 \cdots b_n$ be the binary representation of m
  - For each $1 \leq i \leq n$,

$$u_i = F(sk, (i, b_1 \cdots b_{i-1} || 0^{n-i})) + b_i \bmod M$$

  - Output the tuple $c = (u_1, u_2, \ldots, u_n)$

- CMP(c_1, c_2);
    - Let $c_1 = (u_1, \ldots, u_n)$ and $c_2 = (u'_1, \ldots, u'_n)$
    - Find the smallest index i such that $u_i \neq u'_i$
    - If no such index exists, output 0
    - If exists,
        - output 1 if $u'_i = u_1 + 1 \bmod M$
        - output 0 otherwise

Remark.

[DCC16] "What Else is Revealed by Order-Revealing Encryption?" @ CCS'16

- almost *half bits* of a plaintext are revealed
- leakage of concrete ORE schemes on *non-uniform* data leads to more accurate plaintext recovery than suggested