[CLWW16]

- KeyGen(1^λ) ;
  - output $sk \xleftarrow{\$} K$, where K : key space.
- Enc(sk, m) ;
  - let $m = b_1 b_2 \cdots b_n$ be the binary representation
  - for each $1 \le i \le n$, $b_1 \cdots b_{i-1}$ 비트의 개별적 합산. (같은 경우에만 같은 값) $\{1, 2, \cdots, n\}_k$.

$$u_i = F(sk, (i, b_1 \cdots b_{i-1} \| 0^{n-i})) + b_i \bmod M \quad \text{where } F: K \times (\{n\} \times \{0,1\}^{n-1}) \to \mathbb{Z}_M \ (M \ge 3).$$

  - output the tuple $c = (u_1, u_2, \cdots, u_n)$
- CMP(c_1, c_2) ;
  - let $c_1 = (u_1, u_2, \cdots, u_n)$ and $c_2 = (u_1', u_2', \cdots, u_n')$.
  - Find the smallest i s.t. $u_i \neq u_i'$. → reveals the first different bit.
  - If no such index exists, output 0.
  - If exists, output 1 if $u_i' = u_i + 1 \bmod M$
    output 0 otherwise.

10진수 비교와 같은 동작.

Note. [DDC16] "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.

Think thing