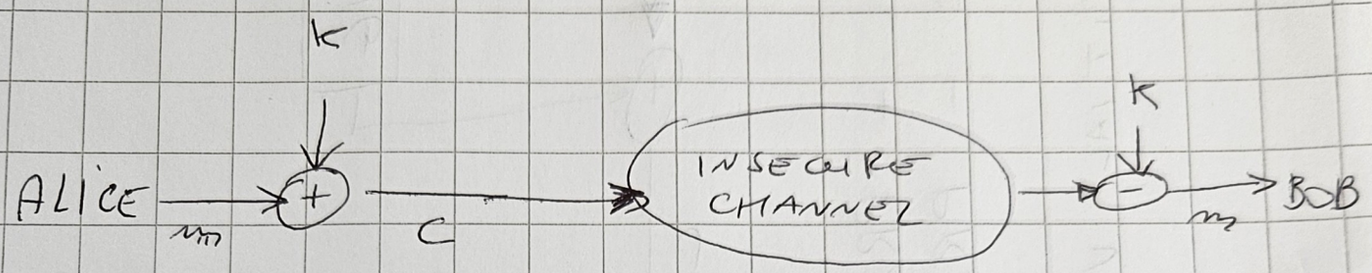
ONE-TIME PAD

Assumption : Key size = Plaintext size

$\Rightarrow k, m \in \mathbb{Z}_q^n$



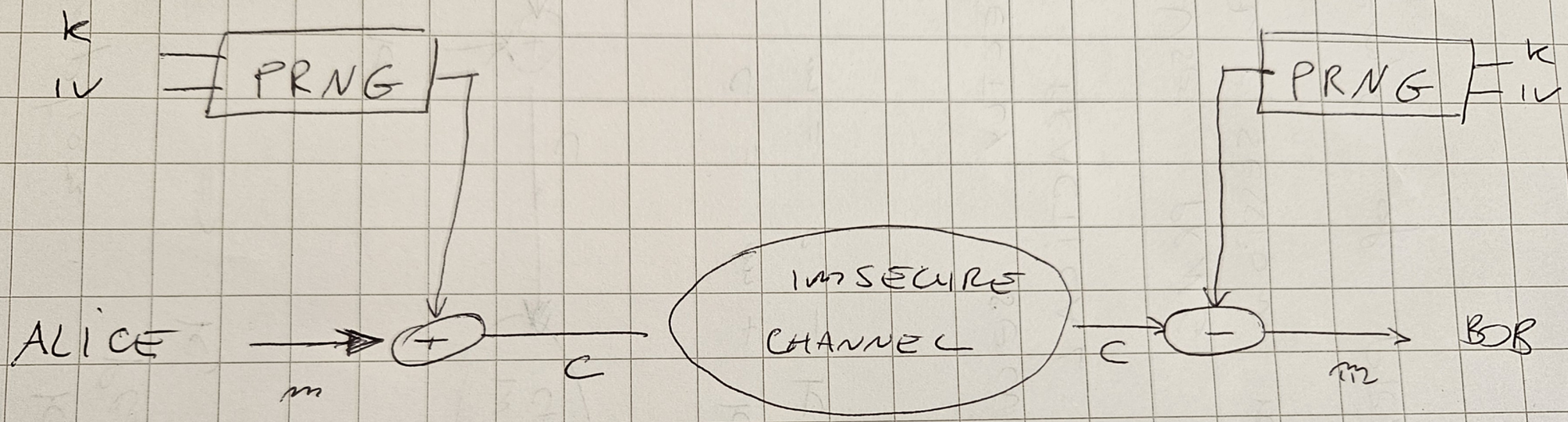
$c = m + k$

$m = c - k$

- PERFECTLY SECURE, but
- NOT PRACTICAL !!

$\Rightarrow$ USE PRNG to generate a SESSION KEY

(Example of PRNG : LFSR !)



$$c = m + PRNG(k, IV)$$

$$m = c - PRNG(k, IV)$$

IV ≡ INITIAL VALUE