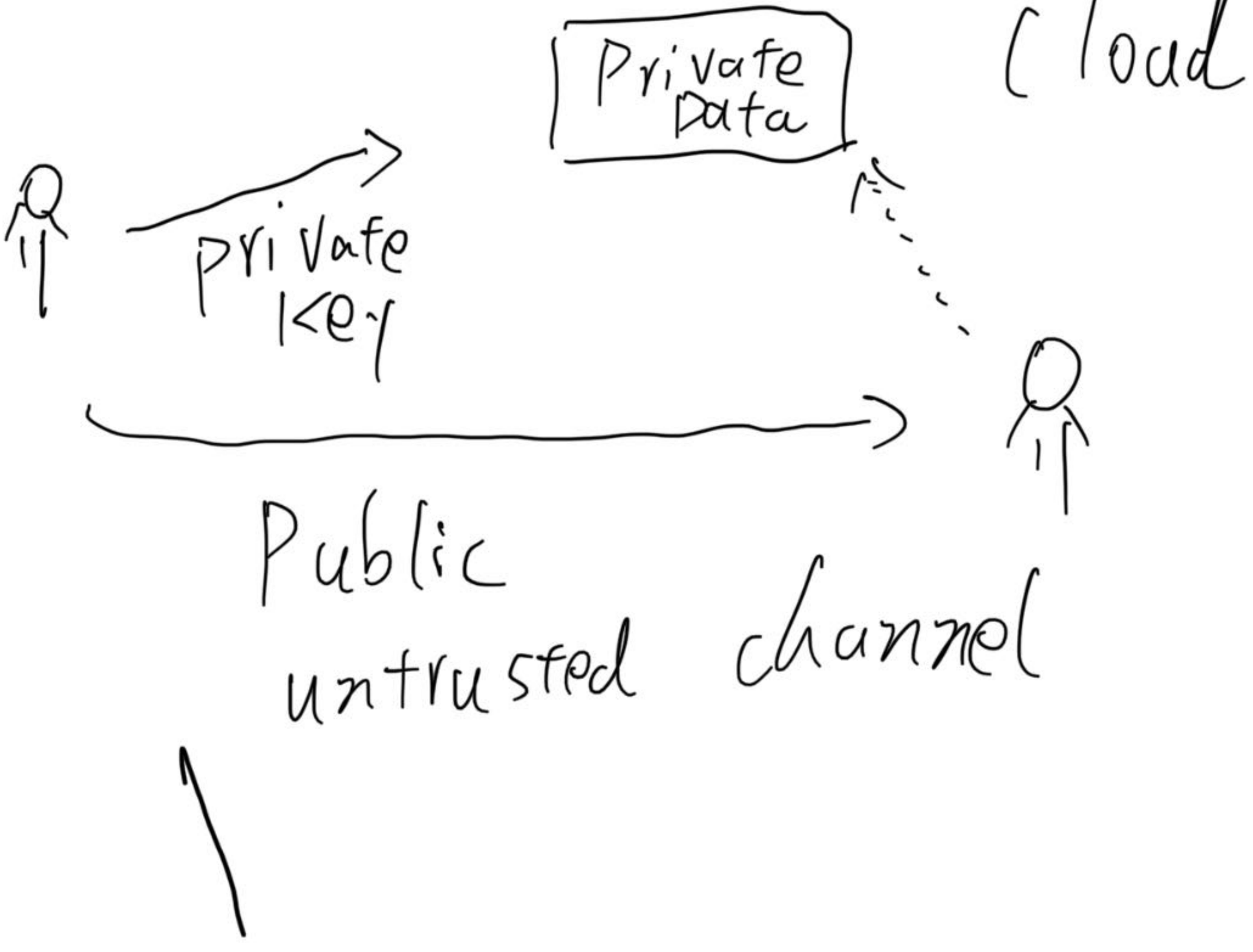
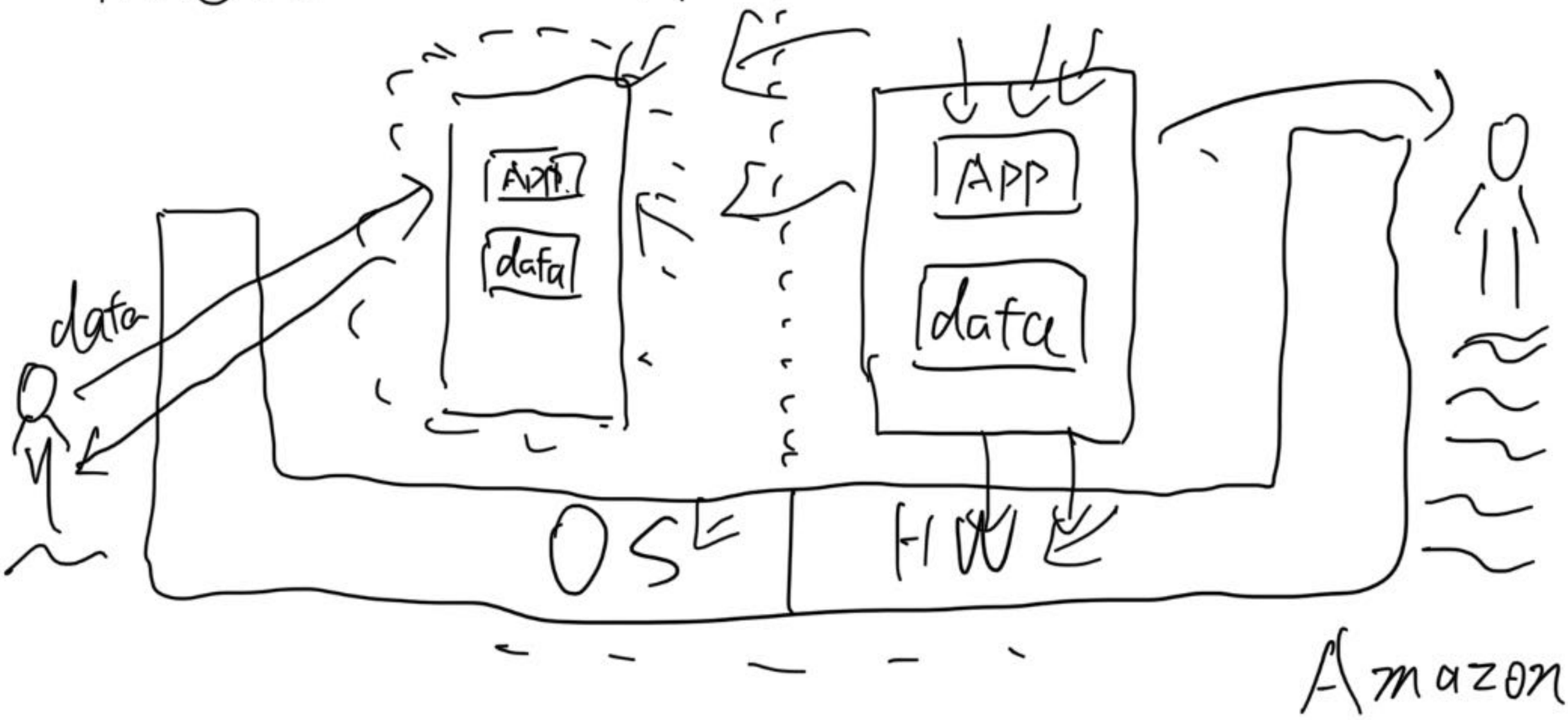
2020 Summer



Threat Model:



① Attacker

cloud vendor

other users

② capability

everything

limited access ?

side channel

everything

③ goal

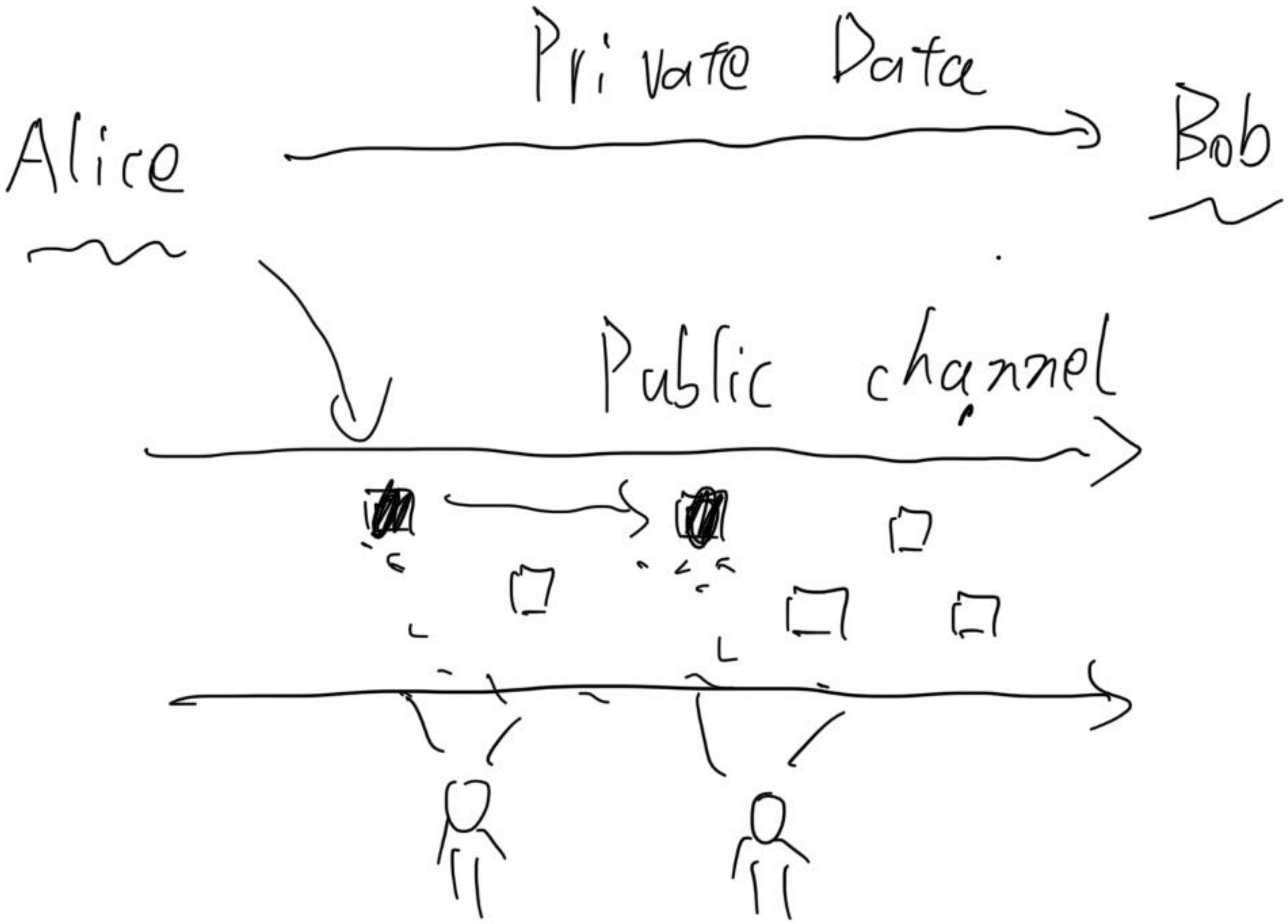
data crack

data

data

OS

network



A → B

cipher system:

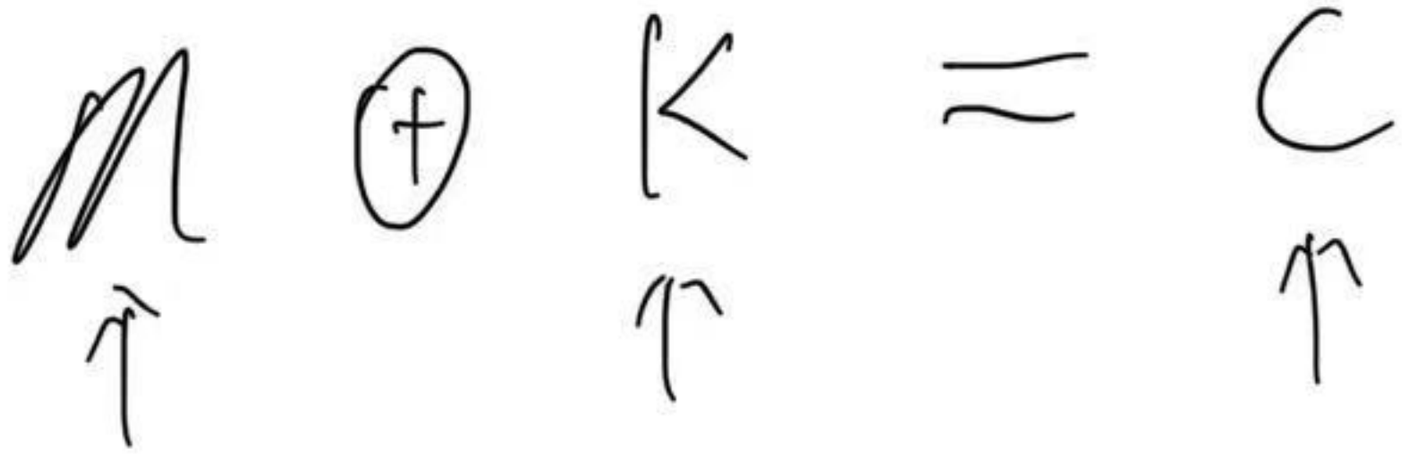
public

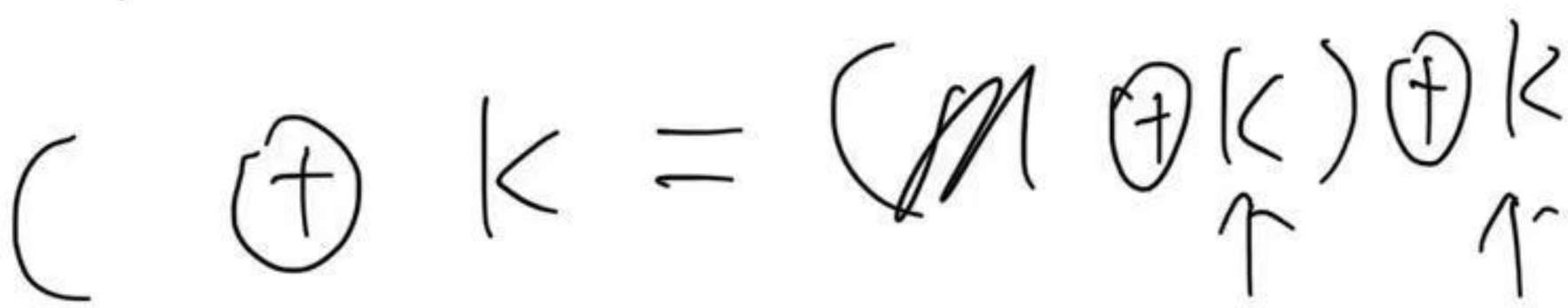
$$\begin{cases} ciphertext = Enc(plaintext, key) \\ plaintext = Dec(ciphertext, key) \end{cases}$$

ciphertext ↛ plaintext

cipher + key ⟶ plaintext

OTP: K <"real random">





uniformly random

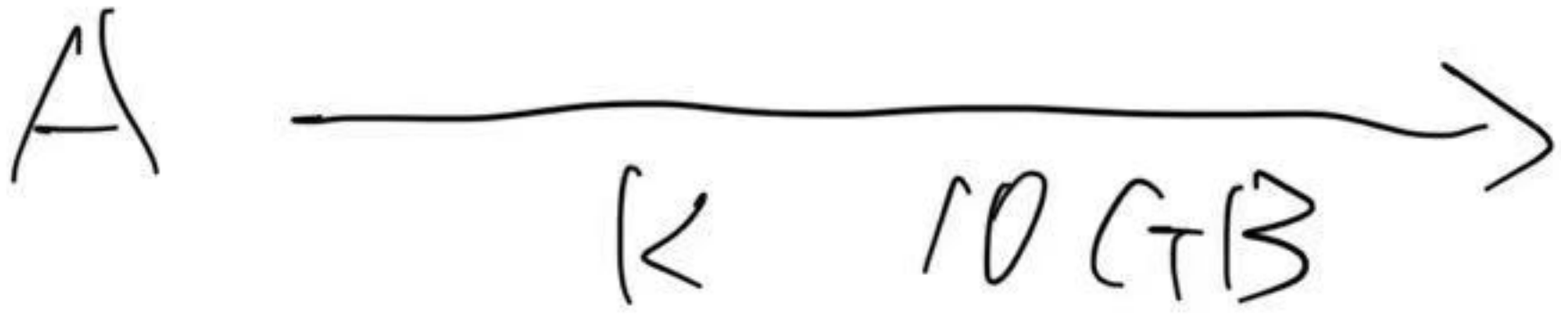
$P_1 \oplus K = C_1$

$P_2 \oplus K = C_2$

$C_1 \oplus C_2 = P_1 \oplus K \oplus P_2 \oplus K$

$= P_1 \oplus P_2$

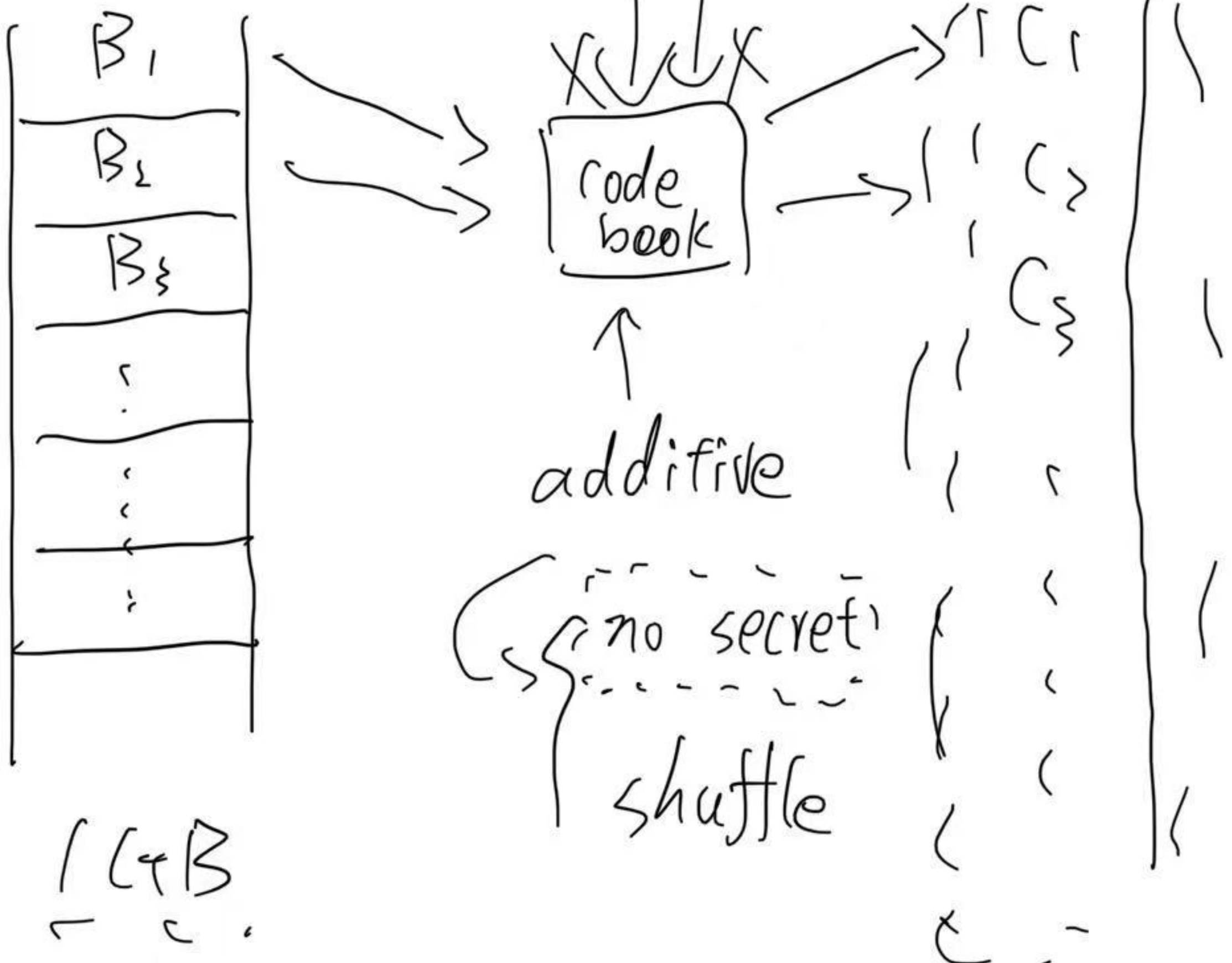
10GB 10GB key



codebook

cipher

additive



$|C| \leq |B|$

$B_1 = B_{10}$ $\quad B_1 = B_{10}$

$C_1 = C_{10}$ $\quad C_1 \neq C_{10}$