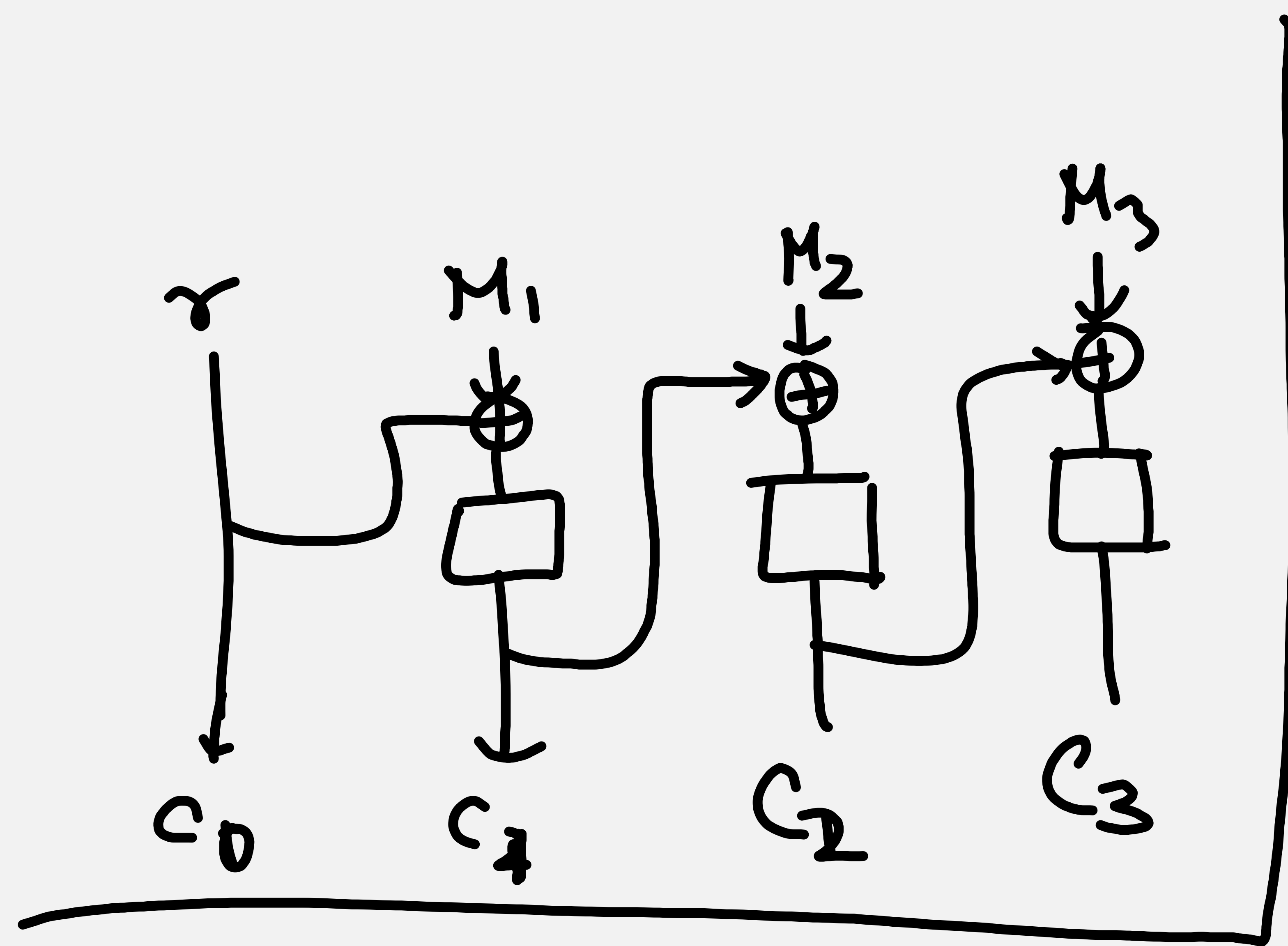


Modes of Operation

Given $F: \{0,1\}^k \times \{0,1\}^n \rightarrow \{0,1\}^n$, how to define encryption for message length $\ell \cdot n$ ($\ell \geq 1$).
↳ bits

How to extend it for arbitrary length (not multiple of n)?

- Chop / Truncate the last ciphertext-block. (Additional No. C/T expansion)
- Pad the message to make it full block & then perform encryption. (Use Injective Padding) (Introduce additional C/T expansion up to n -bits)



$$M_1 = 0^n \parallel 0^n \parallel 0^{n-1} 1 \Rightarrow \text{Pad}(M_1) = 0^{3n-1} \parallel 1$$

$$M'_1 = 0^n \parallel 0^n \parallel 0^{n-1} \Rightarrow \text{Pad}(M'_1) = 0^{3n-1} \parallel 1$$

(if I do not pad 10^* for full block)

$$\text{Pad}(M_1) = M_1 \parallel 10^*$$

$$\text{Pad}(M_2) = M_2 \parallel 10^*$$

Claim: if $M_1 \neq M_2$
 $\text{Pad}(M_1) \neq \text{Pad}(M_2)$

$\Rightarrow$ Pad function needs to be Injective.

$$M = M_1 \parallel M_2 \parallel M_3^*$$

$$|M_1| = |M_2| = n$$

$$|M_3^*| = (n-10)$$

$$\bar{M} = M_1 \parallel M_2 \parallel M_3$$

$$\Rightarrow c_0 \parallel c_1 \parallel c_2 \parallel c_3 \leftarrow \text{CBC}(\bar{M})$$

During Decryption: The last block is $M_3 = \underline{M_3^*} \parallel 10^*$
 Then return (M_1, M_2, M_3^*)

- Suppose I use 0^* padding
- How about 10^* padding?
 (Add the padding even if message is full block).

Significance of Provable Security Results

96 $F: \{0,1\}^k \times \{0,1\}^n \rightarrow \{0,1\}^n$ is PRF, then

— CTR[F] mode achieves IND-CPA Security with

$$\text{advantage} = \frac{2q l_{\max}}{2^n} + \text{negl}(n)$$

Suppose, I have an application where the messages can be $2^{n/4}$ - bit long
then the CTR mode provides security under same-key until

$$q \ll 2^{3n/4}$$

$n=128$ $\Rightarrow$ message length $\leq 2^{32}$, CTR mode provides guarantee until $q \ll 2^{96}$.

Error Propagation in Modes of Operation

- Suppose some ciphertext blocks are missing/corrupted.

How many message blocks does it affect?

└ If less, then it is good in terms of error-propagation
└ o/w, it is not.

In this respect

- CTR, OFB are good choices $\Rightarrow i^{\text{th}}$ C/T block corrupt $\Rightarrow i^{\text{th}}$ P/T block corrupt
- CBC is not a good choice $\Rightarrow i^{\text{th}}$ C/T block corrupt $\Rightarrow i, i+1, \dots$, all successive P/T blocks corrupt.

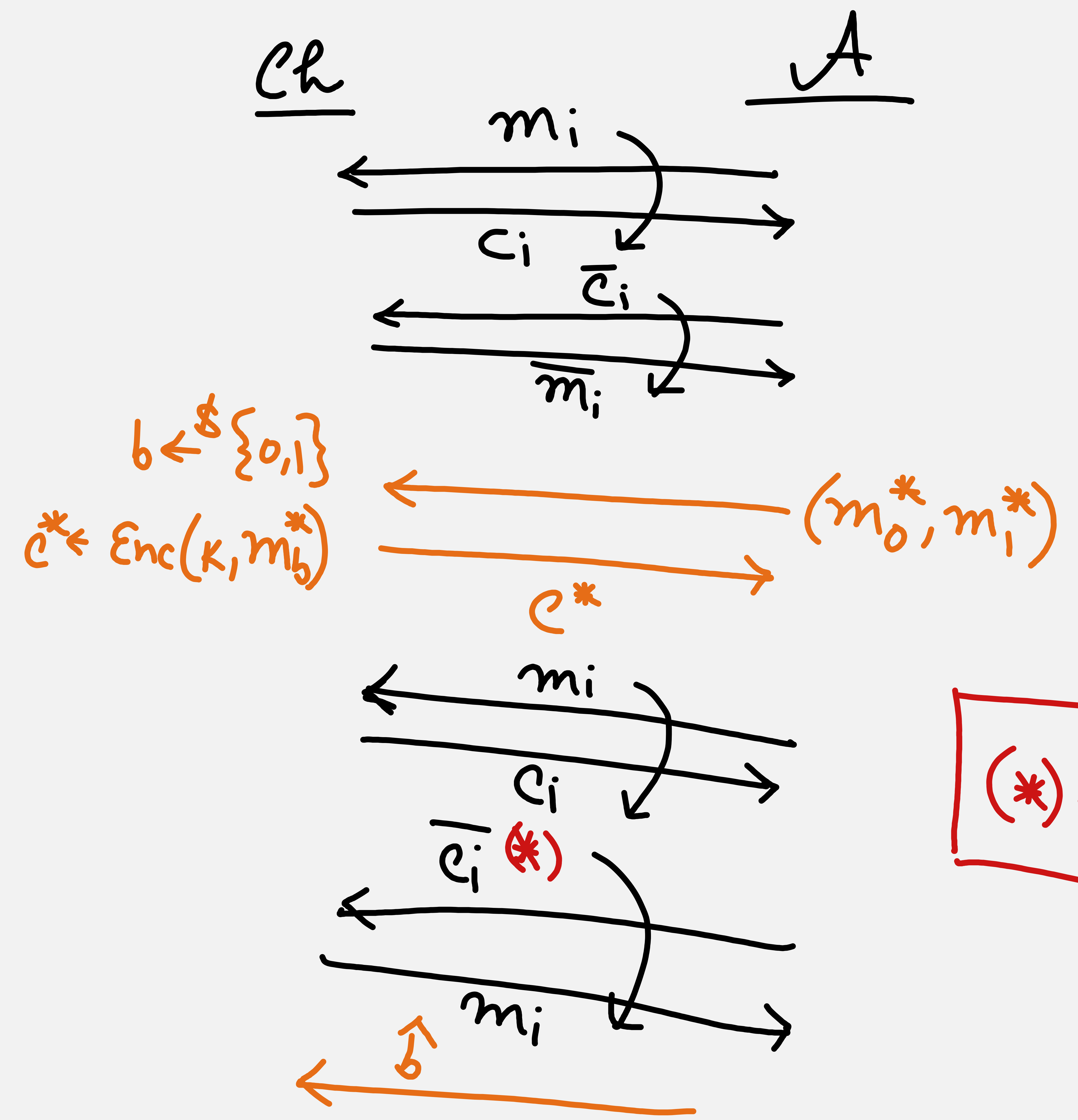
$$\Pi = (KG, Enc, Dec)$$

IND-CCA Notion

Π is IND-CCA Secure if

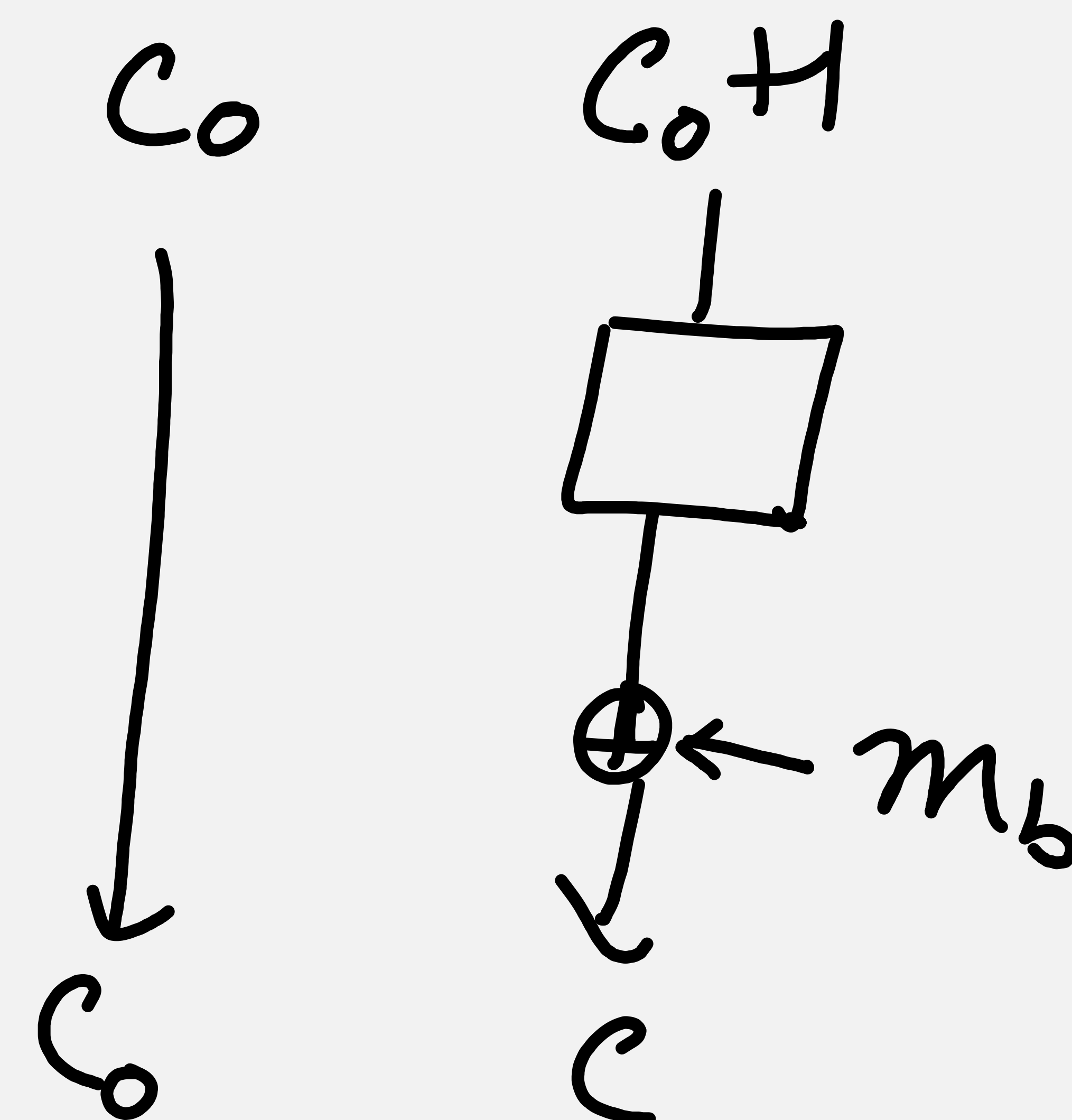
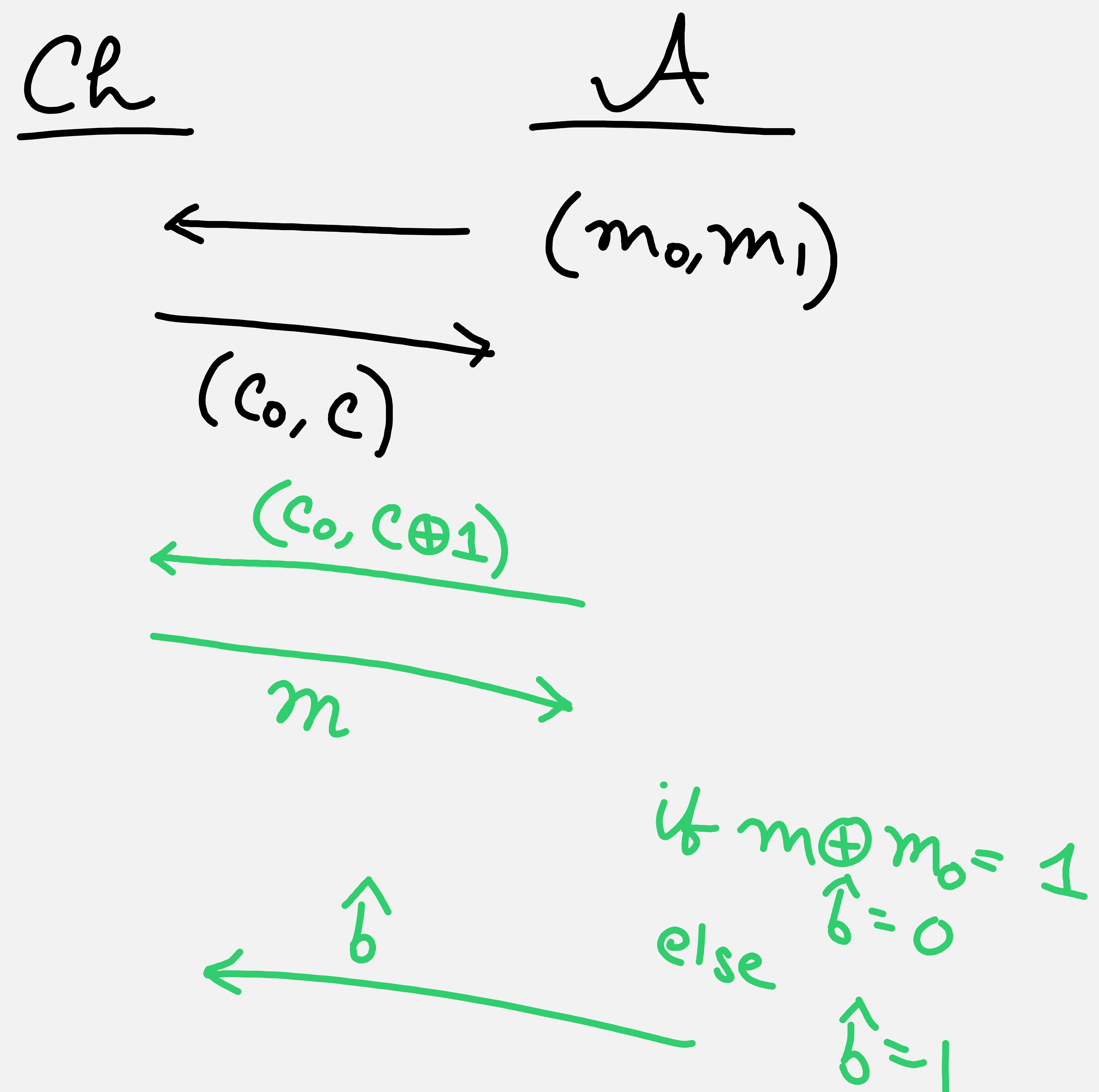
$$\Pr[PrivK_{\Pi, A}^{IND-CCA} = 1] = \Pr[b = \hat{b}] \leq \frac{1}{2} + \text{negl}(n)$$

$$Adv_{\Pi}^{IND-CCA}(A) = \left| \frac{1}{2} - \Pr[b = \hat{b}] \right| \leq \text{negl}(n)$$



H/W: CTR, OFB, CBC all can be broken in IND-CCA attack

CCA Attack on CTR



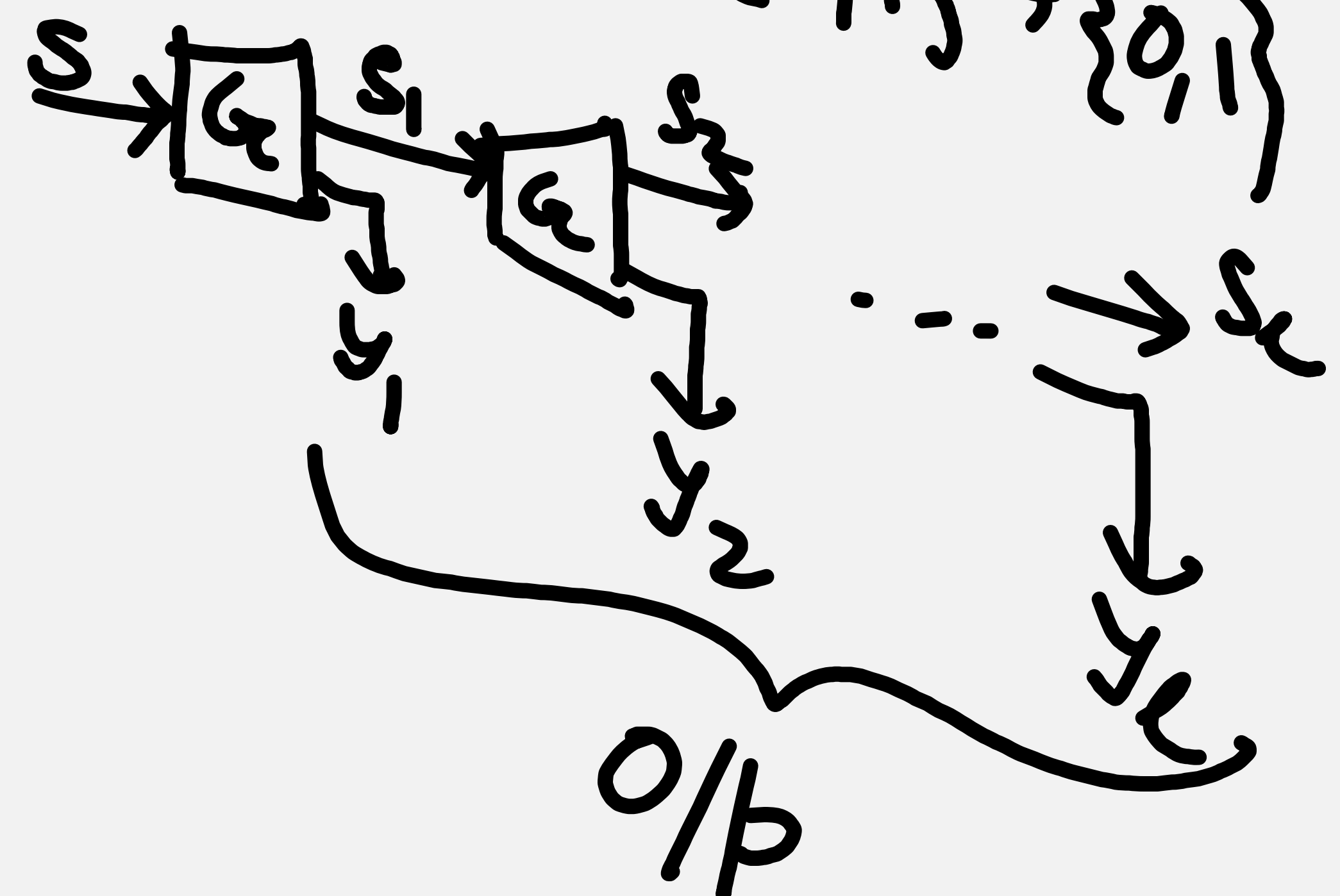
Stream Cipher

PRG

$$G: \{0,1\}^n \rightarrow \{0,1\}^{l(n)}$$

- $l(n)$ is fixed
- Output released at one-shot

Suppose you are given $G: \{0,1\}^n \rightarrow \{0,1\}^{n+1}$



$\left\{ \begin{array}{l} IV \rightarrow \text{Initialization vector} \\ \rightarrow \text{Optional} \end{array} \right.$

→ Flexible extension of PRG that has

- variable-length output
- output released as required.

$SC(\text{Init}, \text{Next})$

Init(s, IV)

return st.

Next(st)

return (st', y)
 ↓ ↓
 updated state O/p

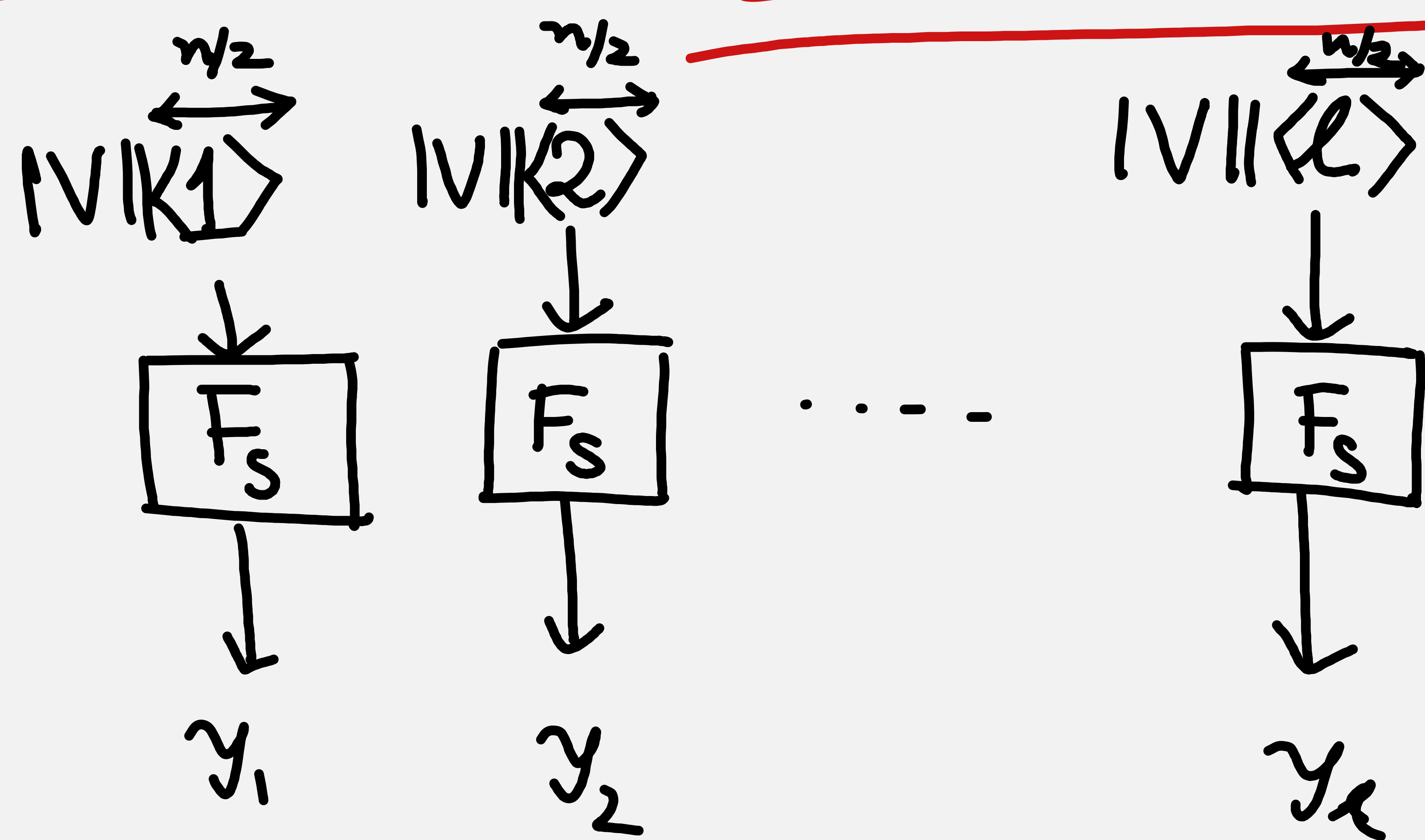
$SC(s, IV, 1^l)$

$st_0 \leftarrow \text{Init}(s, IV)$
 For $i \leftarrow 1(1)l$
 $(st_i, y_i) \leftarrow \text{Next}(st_{i-1})$
 return $(y_1, \dots, y_l)$

$Enc(s, IV, m)$
 $y \leftarrow SC(s, IV, |m|)$
 $c \leftarrow m \oplus y$

Example:

Block-cipher based Stream Cipher



$$F: \{0,1\}^k \times \{0,1\}^n \rightarrow \{0,1\}^n$$

$$l < 2^{n/2}$$

$$|IV| = \frac{n}{2}$$

$\langle i \rangle \rightarrow$ binary representation of
integer i in $\frac{n}{2}$ -bits

INIT(IV, s, l)

$$St = (IV, s, 1)$$

Next(IV, s, c)

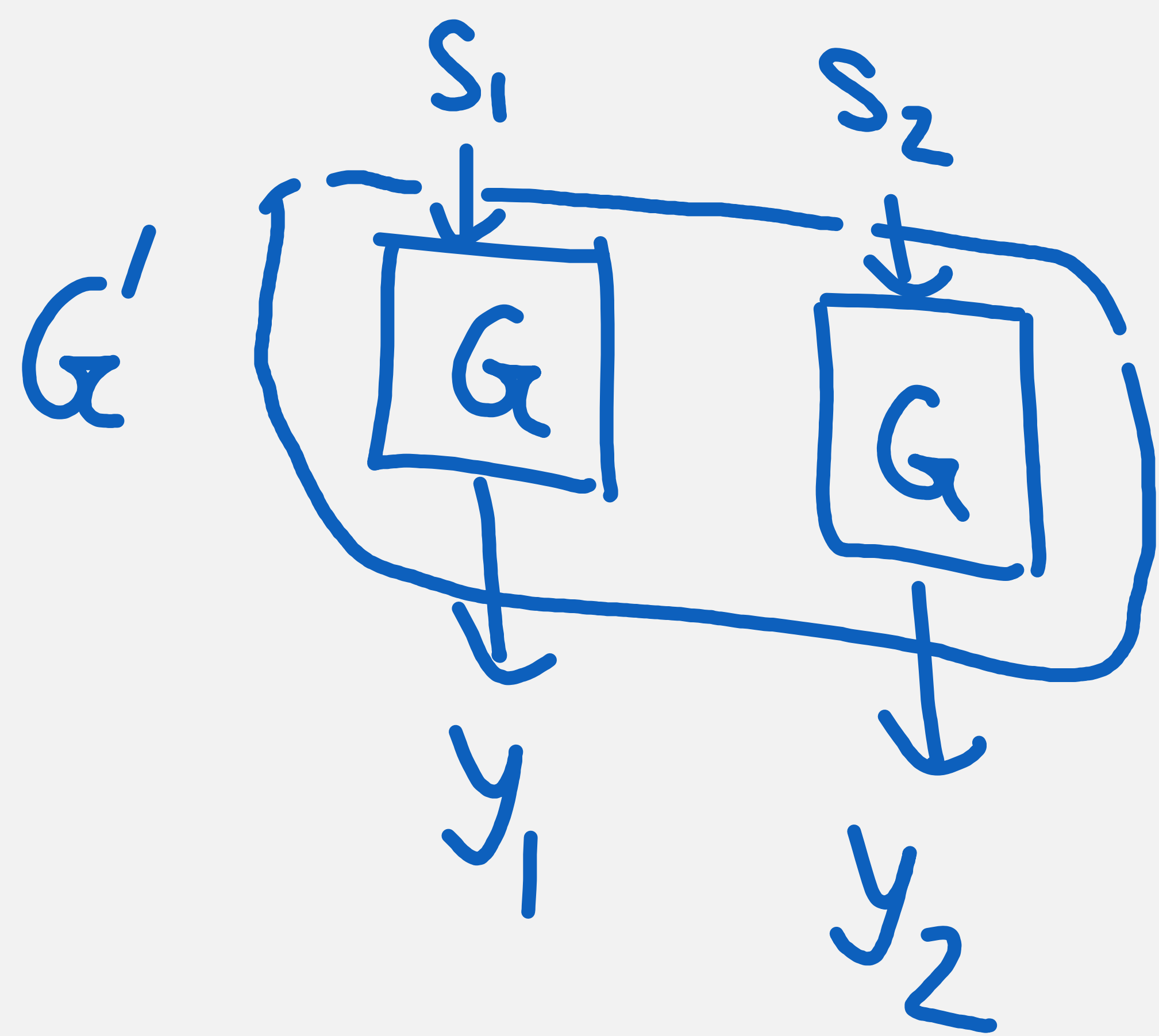
$$y \leftarrow F_s(IV || c)$$

$$St' \leftarrow (IV, s, c+1)$$

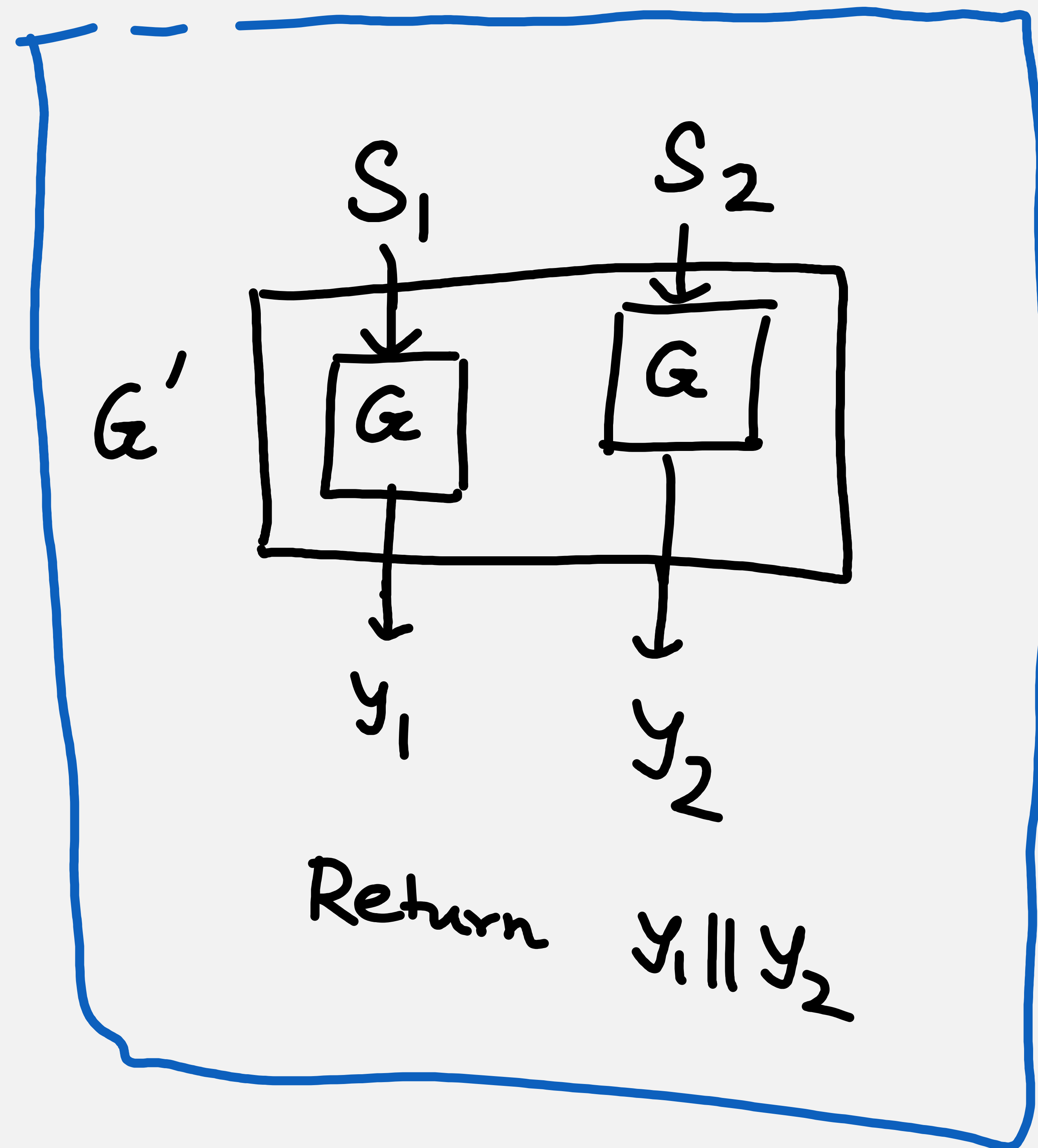
Parallel Composition of PRGs

$$G: \{0,1\}^n \rightarrow \{0,1\}^{2n}$$

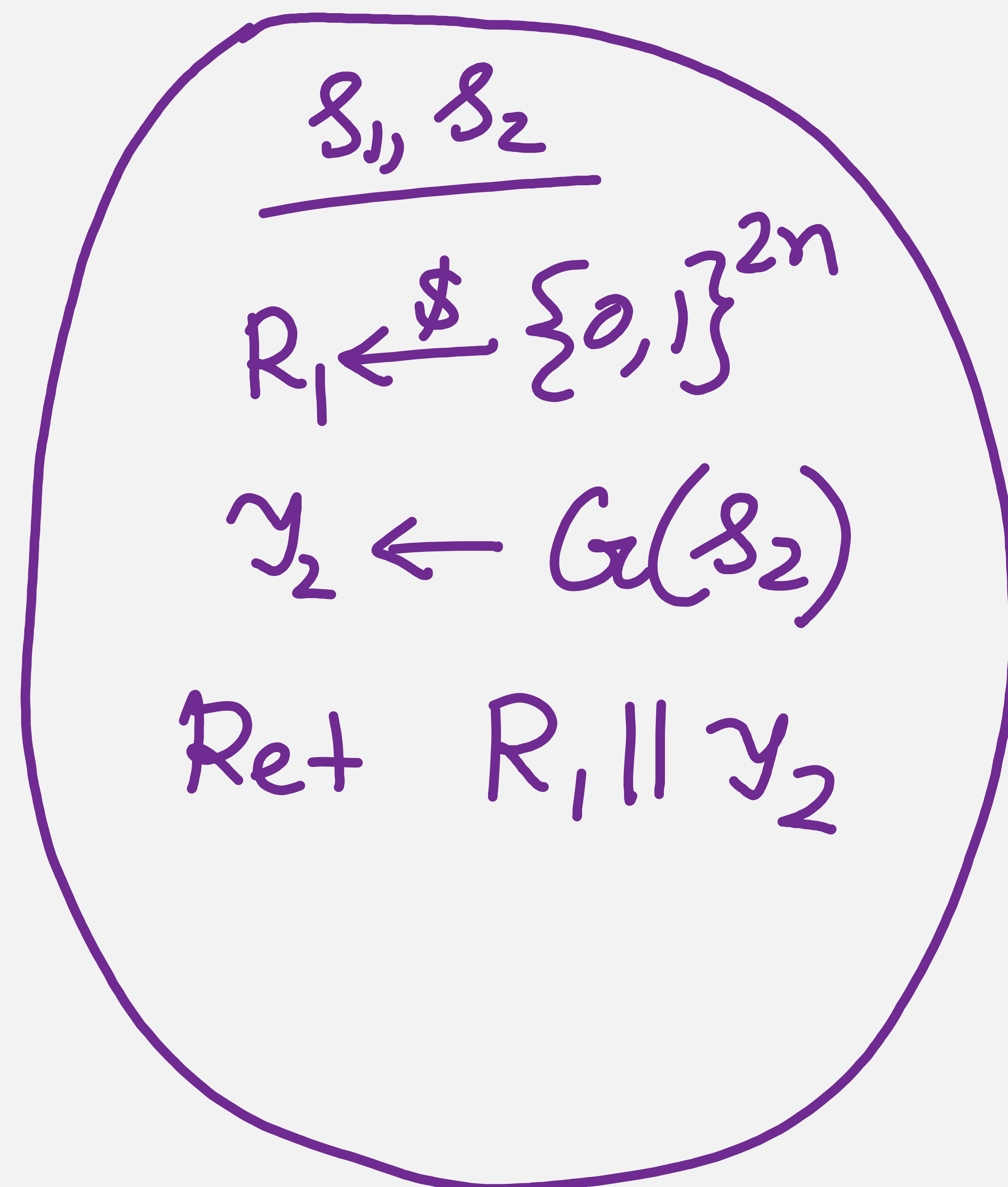
$$G': \{0,1\}^{2n} \rightarrow \{0,1\}^{4n}$$



↑ If G is ϵ -PRG
↓ then G' is 2ϵ -PRG

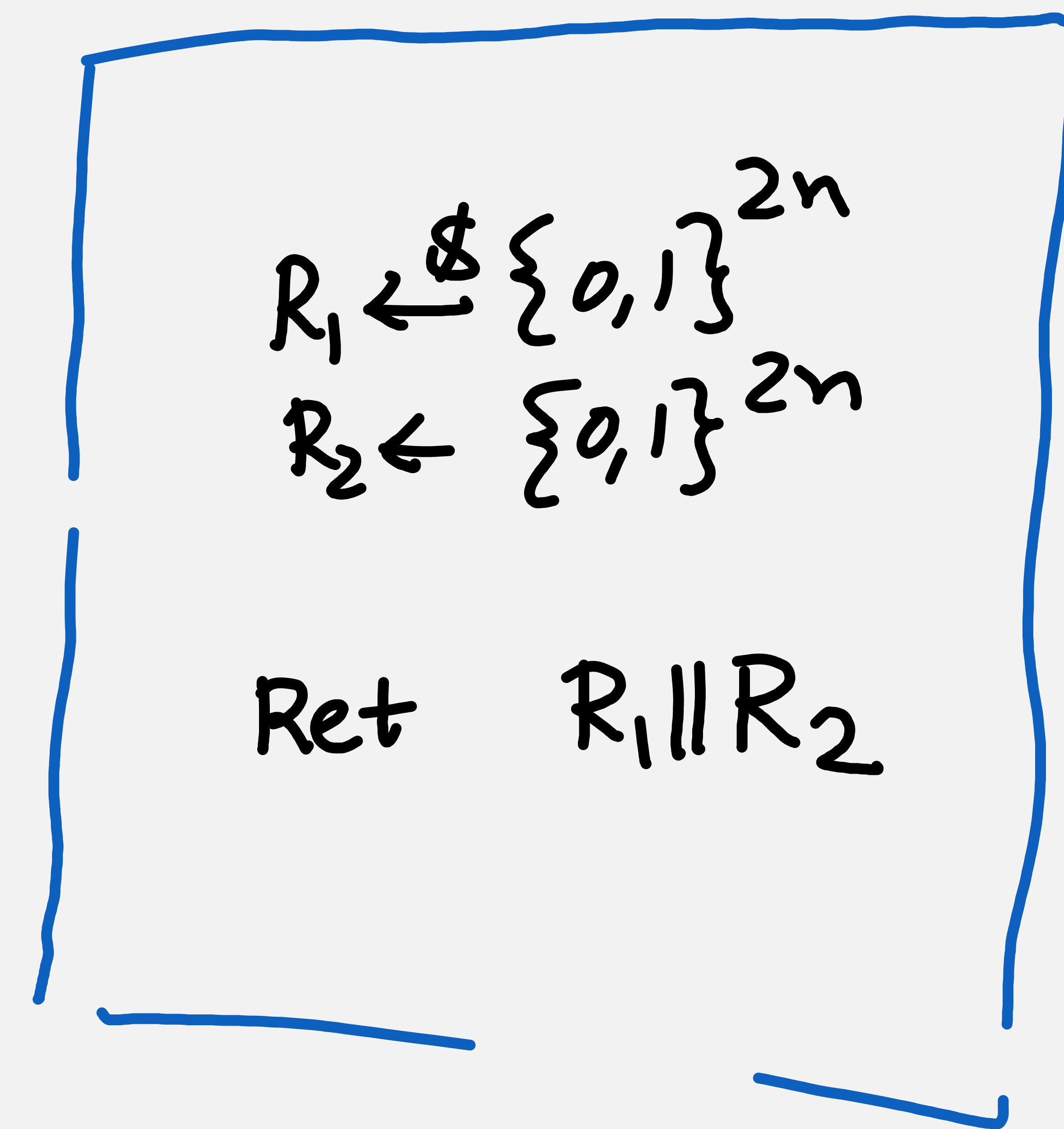


$$\Pr[\mathcal{D}(G'(s_1, s_2)) = 1] = p_0$$



Hybrid Game

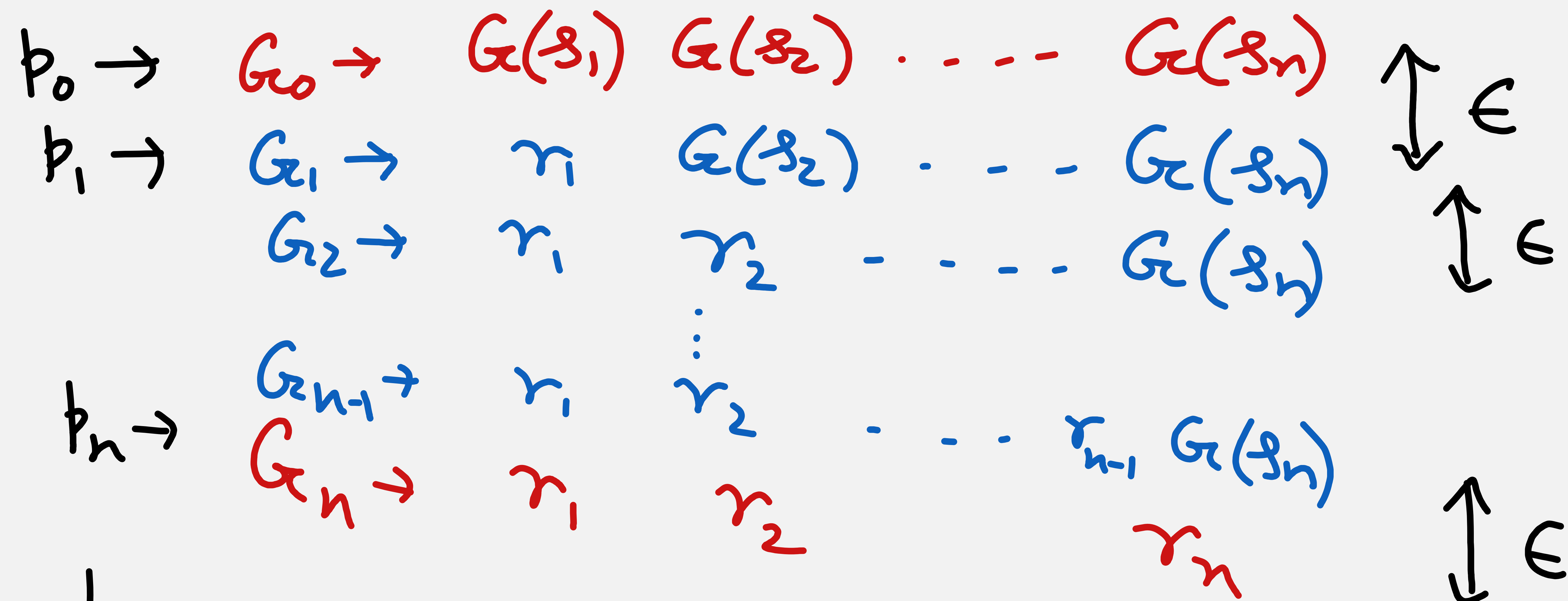
$$\Pr[\mathcal{D}(R_1 || y_2) = 1] = p_1$$



$$\Pr[\mathcal{D}(R_1 || R_2) = 1] = p_2$$

$$\begin{aligned}
 |p_0 - p_2| &= |p_0 - p_1 + p_1 - p_2| \\
 &\leq |p_0 - p_1| + |p_1 - p_2| \\
 &= \epsilon + \epsilon \\
 &= 2\epsilon.
 \end{aligned}$$

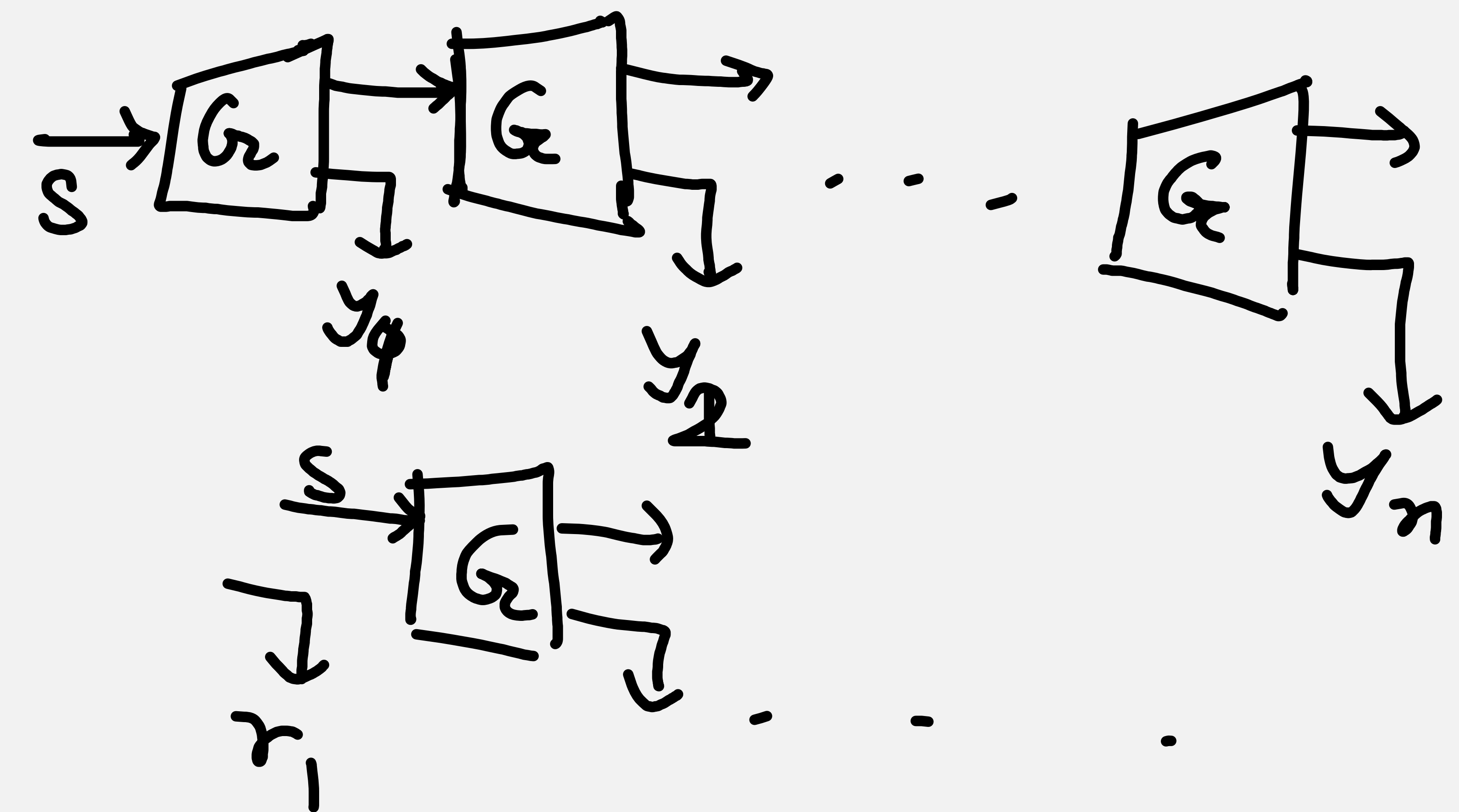
n -Composition



$$|p_n - p_0| \leq |p_n - p_{n-1}| + \dots + |p_2 - p_1| + |p_1 - p_0|$$

$$= n \cdot \epsilon.$$

Sequential Composition



$$G \rightarrow \epsilon\text{-PRG}$$

$$G' \rightarrow n\epsilon\text{-PRG}$$