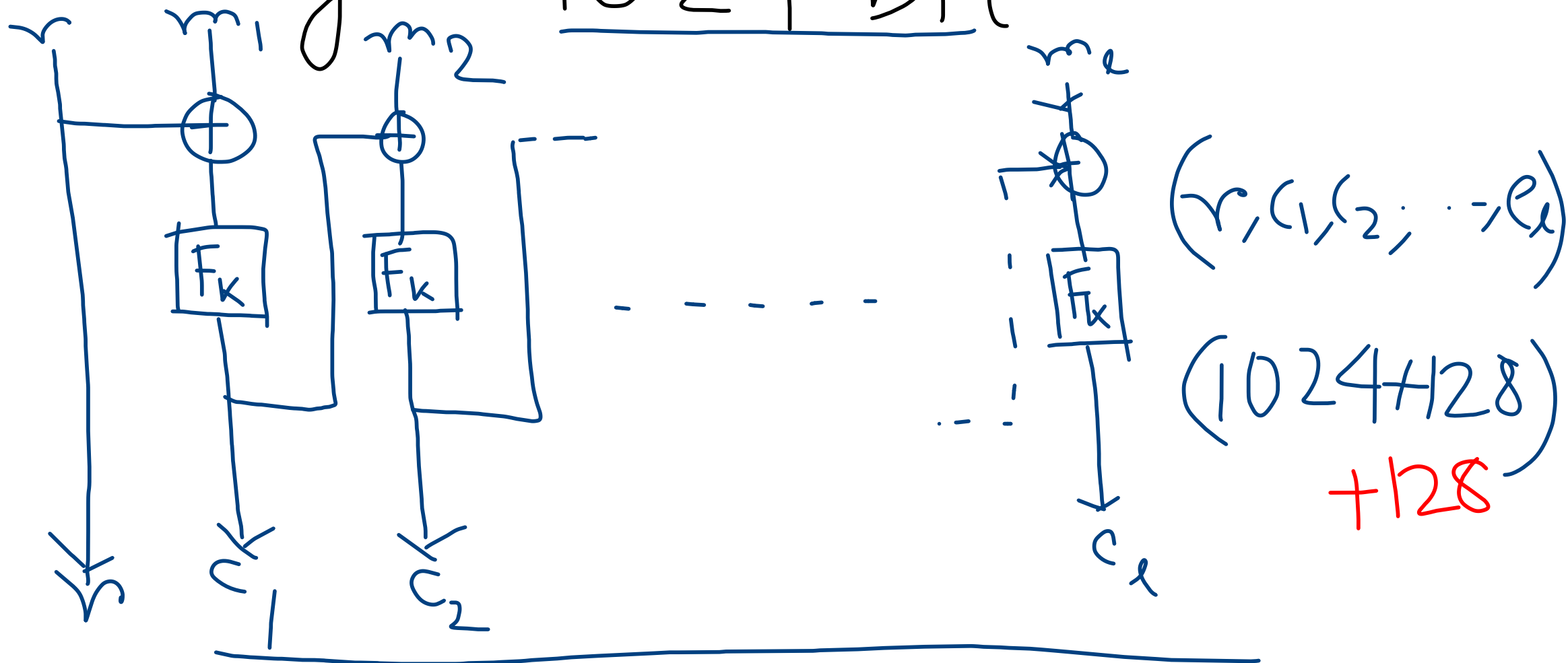


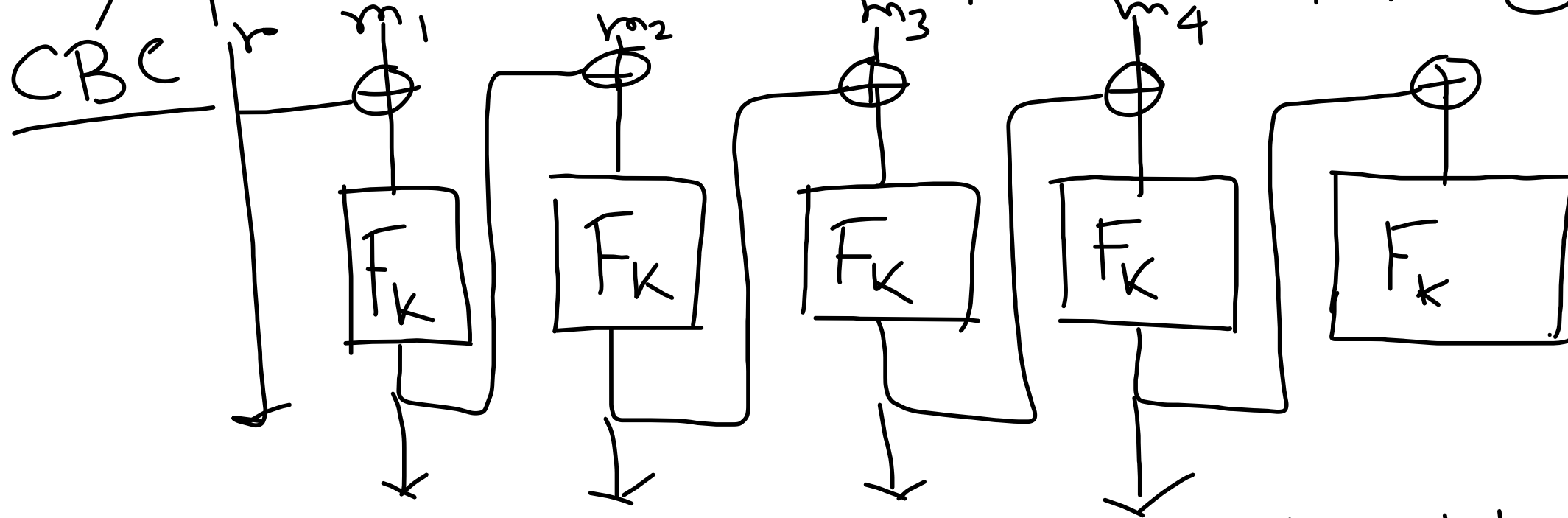
Problem Set-2

1) PRF: 128 bit (256 bit Key)

message: 1024 bit



2) $|m| = 520 = 128 \times 4 + 8$



$f^8(m) \rightarrow 128$
 $f(m) \rightarrow m^*$

001011 $\rightarrow C$
001011 $\rightarrow C$

10* padding

10111100

5/2

510

000 . . . 010

000 . . . 0101010 ————— 0

10* padding

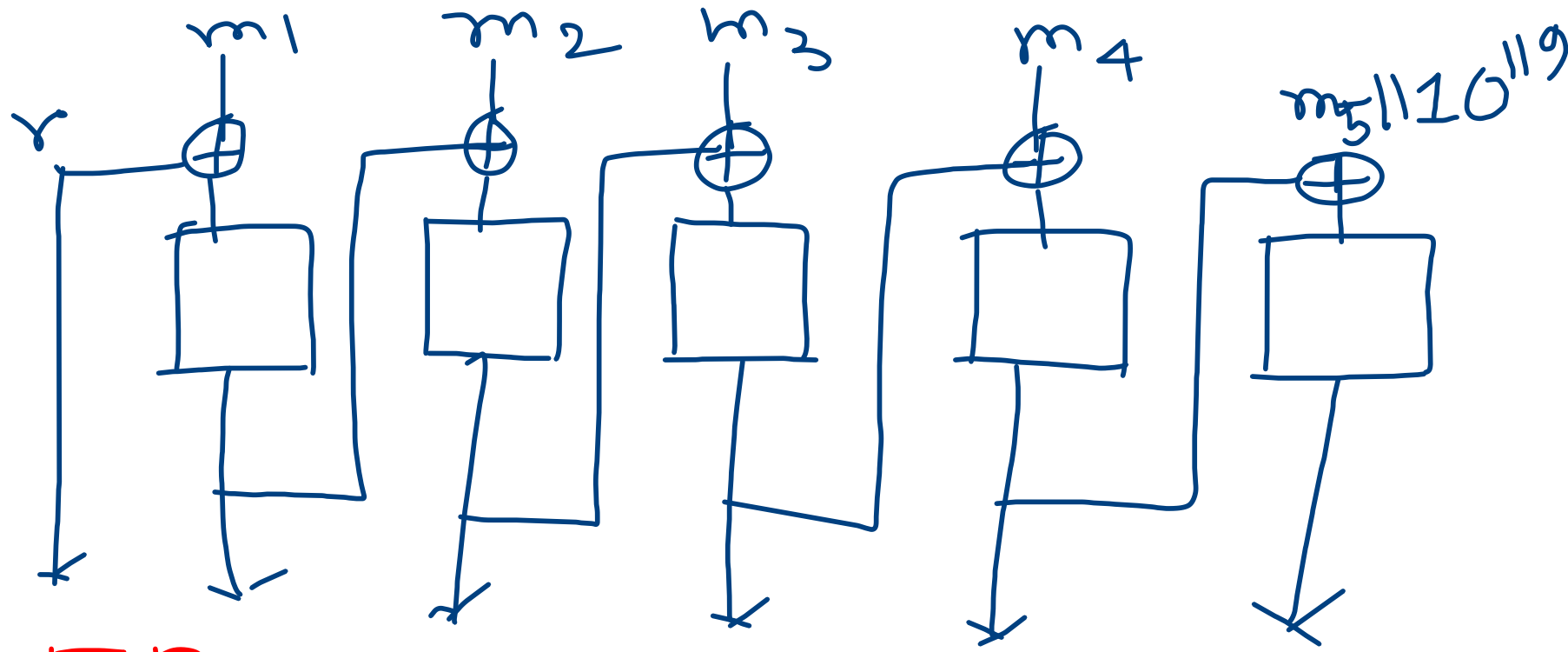
10111100

5/2

510

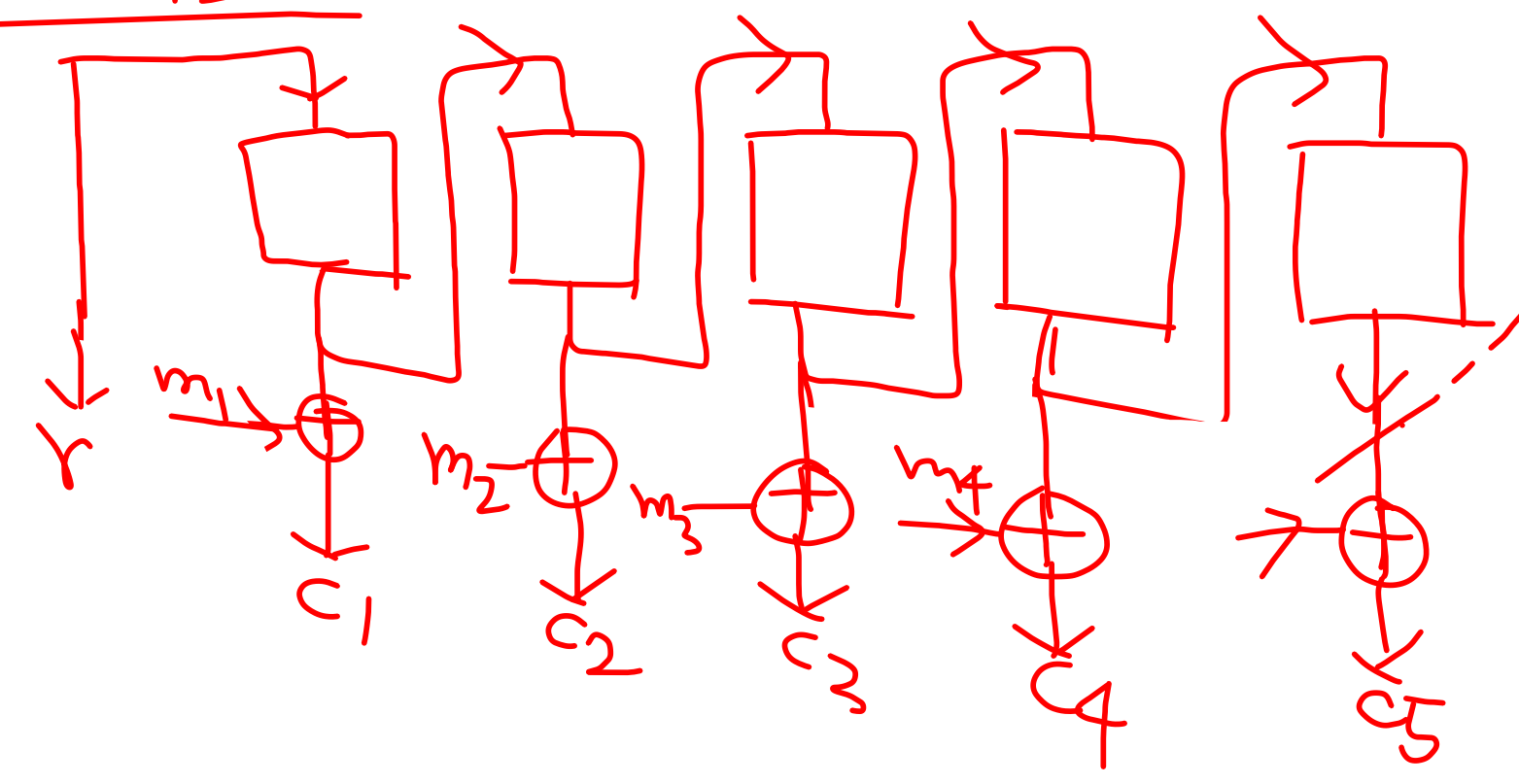
000 . . . 010

000 . . . 0101010 ————— 0



PRF 6 bit
last block 4 bit

OFB



101110
1111

100001
11110

1111

3) a) $G_k(\underline{x}, y) = F_k(x) \oplus F_k(y)$

Ch_{G_k} A_{G_k}

$k \leftarrow \text{random}$
 $b \leftarrow \{0, 1\}$ $\leftarrow 1^n$

$b = 1$
 $O = G_{k,b}$

$b = 0$
 $O = g$

$g \leftarrow \text{Func}(2n, n)$

(x, x)
 $O(x, x)$

if $O(x, x) = O^n$ return 1
 else $\rightarrow$ return 0



$$Pr_k [g^{G_k^{(1)}}(1^n) = 1] - Pr_g [g^{g^{(1)}}(1^n) = 1]$$

$$= 1 - \frac{1}{2^n}$$

3)(b)

$$\frac{Ch_G}{\mathcal{D}_G}$$

$$g(1^n, 1) \rightarrow \frac{2^n}{\log 2^n}$$

$$\frac{b=1}{g_k} \quad \frac{b=0}{g}$$

$$\left. \begin{array}{l} \overleftarrow{x} \\ \overrightarrow{O(x)} \\ \overleftarrow{x \oplus 1^n} \\ \overrightarrow{O(x \oplus 1^n)} \end{array} \right\}$$

$$F_k(x) \oplus F_k(x \oplus 1^n)$$

$$F_k(x \oplus 1^n) \oplus F_k(x \oplus 1^n \oplus 1^n)$$

$$\frac{2^n}{2^n} \cdot \frac{1}{2^n} = \frac{1}{2^n}.$$

(4) (a)

$$G'(s) = G(s_1 s_2 \dots s_{n/2}) \quad \frac{H}{W}$$

$\underbrace{\text{Ch}_G}_{\omega} \quad \underbrace{\text{D}_G} \quad \underbrace{\text{D}_{G'}}$

/

$$4) \textcircled{b} \quad G'(s) = G(0^{|s|} \parallel s)$$

$$\underline{G''(s) = G(0^{|s|})}$$

$\text{Ch}_{G''}$

$\mathcal{D}_{G''}$

$$\begin{array}{c} s \leftarrow \{0,1\}^n \\ \hline b=1 \\ \omega = G''(s) \end{array} \quad \xleftarrow{1^n}$$

$$\begin{array}{c} b=0 \\ \hline s \leftarrow \{0,1\}^{r(k)} \end{array}$$

$$\xrightarrow{\omega} \omega = G(0^n)$$

$$\begin{array}{c} G(s) \\ \downarrow \\ G'(0^{|s|} \parallel s) \\ \downarrow \\ G''(0^{|s|}) \end{array}$$

$$4) \textcircled{b} \quad G'(s) = G(0^{|s|} \parallel s)$$

$$\underline{G''(s) = G(0^{|s|})}$$

$\text{Ch}_{G''}$

$\mathcal{D}_{G''}$

$$\begin{array}{c} s \leftarrow \{0,1\}^n \\ \hline b=1 \\ \omega = G''(s) \end{array} \quad \xleftarrow{1^n}$$

$$\begin{array}{c} b=0 \\ \hline s \leftarrow \{0,1\}^{r(k)} \end{array}$$

$$\xrightarrow{\omega} \omega = G(0^n)$$

$$\begin{array}{c} G(s) \\ \downarrow \\ G'(0^{|s|} \parallel s) \\ \downarrow \\ G''(0^{|s|}) \end{array}$$

$$4) \textcircled{b} \quad G'(s) = G(0^{|s|} \parallel s)$$

$$\underline{G''(s) = G(0^{|s|})}$$

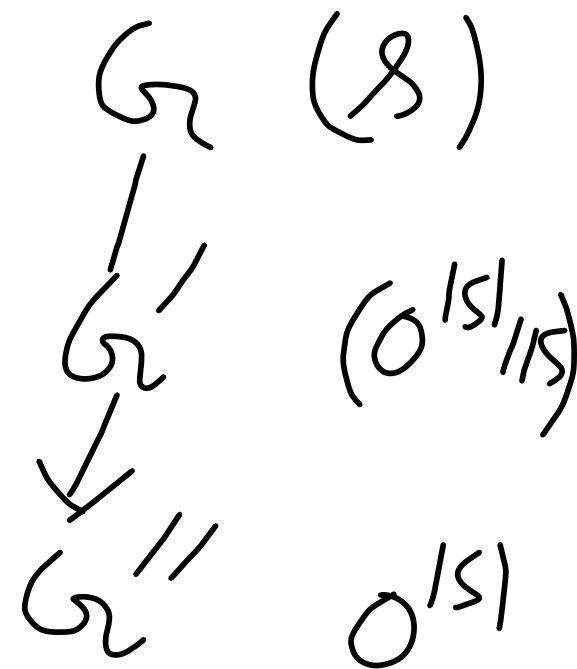
$\text{Ch}_{G''}$

$\mathcal{D}_{G''}$

$$\begin{array}{c} s \leftarrow \{0,1\}^n \\ \hline b=1 \\ \omega = G''(s) \end{array} \quad \xleftarrow{1^n}$$

$$\begin{array}{c} b=0 \\ \hline s \leftarrow \{0,1\}^{r(n)} \end{array}$$

$$\xrightarrow{\omega} \omega = G(0^n)$$



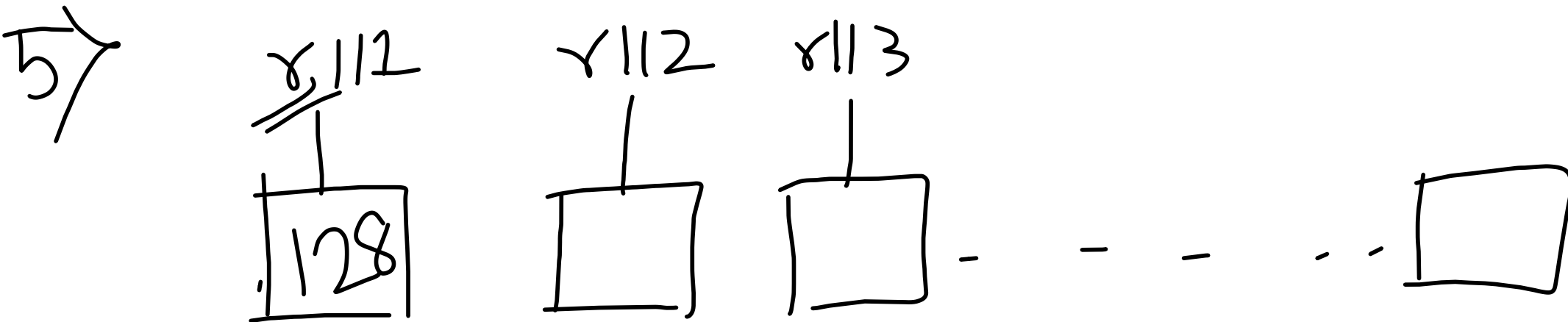
4c) G_0

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

$$b = \sum_{i=1}^{2n} s_i s_{n+i} \pmod{2}$$

$$G(s) = F(s_1 \dots s_n) s_{n+1} \dots s_{2n} \underline{\underline{b}}$$

00 01 10 11
1 1 1 1



1 $\rightarrow$ bin₆₄

2 $\rightarrow$ bin₆₄

$0-2^{64}-1$

$$128 \times (2^{64} - 1)$$

$\underbrace{00 \dots 010}_{126}$

$$\frac{2^2}{2^{181}}$$