Modes of Operation

Recap

- PRF

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

$$\forall D \ \exists \text{ negl.},$$

$$\left| \Pr\left[D^{F_k(\cdot)} = 1\right] - \Pr\left[D^{f(\cdot)} = 1\right] \right| \leq \text{negl}(n)$$

$k \xleftarrow{\$} \mathcal{K}$; $f \xleftarrow{\$} \text{Func}(n,n)$

- If F is a PRF then $\langle r, F_k(r) \oplus m \rangle$ is IND-CPA,

$m \in \{0,1\}^n \Rightarrow c \in \{0,1\}^{2n}$ where $r \xleftarrow{\$} \{0,1\}^n$.

- PRP (Pseudo random permutation)

- $E: \{0,1\}^k \times \{0,1\}^n \to \{0,1\}^n$ to be **PRP** if

$\forall$ PPT $\mathcal{D}$, $\exists$ negligible func negl s.t.

$$\left| \Pr_{k \xleftarrow{\$} \{0,1\}^k}\left[\mathcal{D}^{E_k(\cdot)} = 1\right] - \Pr_{\pi \xleftarrow{\$} Perm(n)}\left[\mathcal{D}^{\pi(\cdot)} = 1\right] \right| \leq negl(n)$$

- We call E to be **SPRP** (Strong PRP) if

$\forall$ PPT $\mathcal{D}$, $\exists$ - - negl s.t.

$$\left| \Pr\left[\mathcal{D}^{E_k(\cdot), E_k^{-1}(\cdot)} = 1\right] - \Pr\left[\mathcal{D}^{\pi(\cdot), \pi^{-1}(\cdot)} = 1\right] \right| \leq negl(n)$$

Mode of Operations

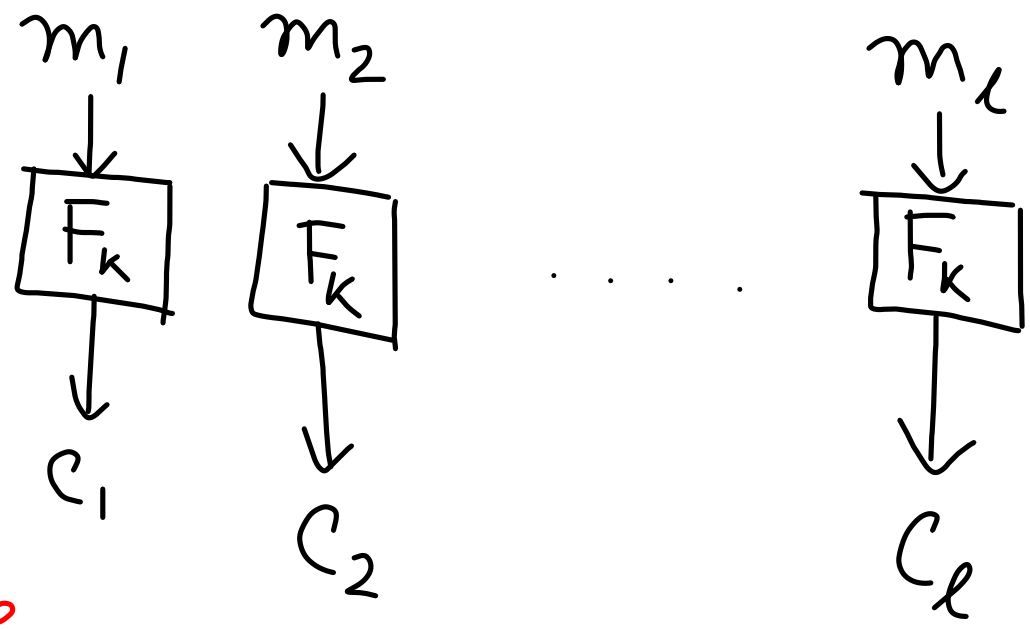
You have a length preserving PRF (or PRP) of say n-bits

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

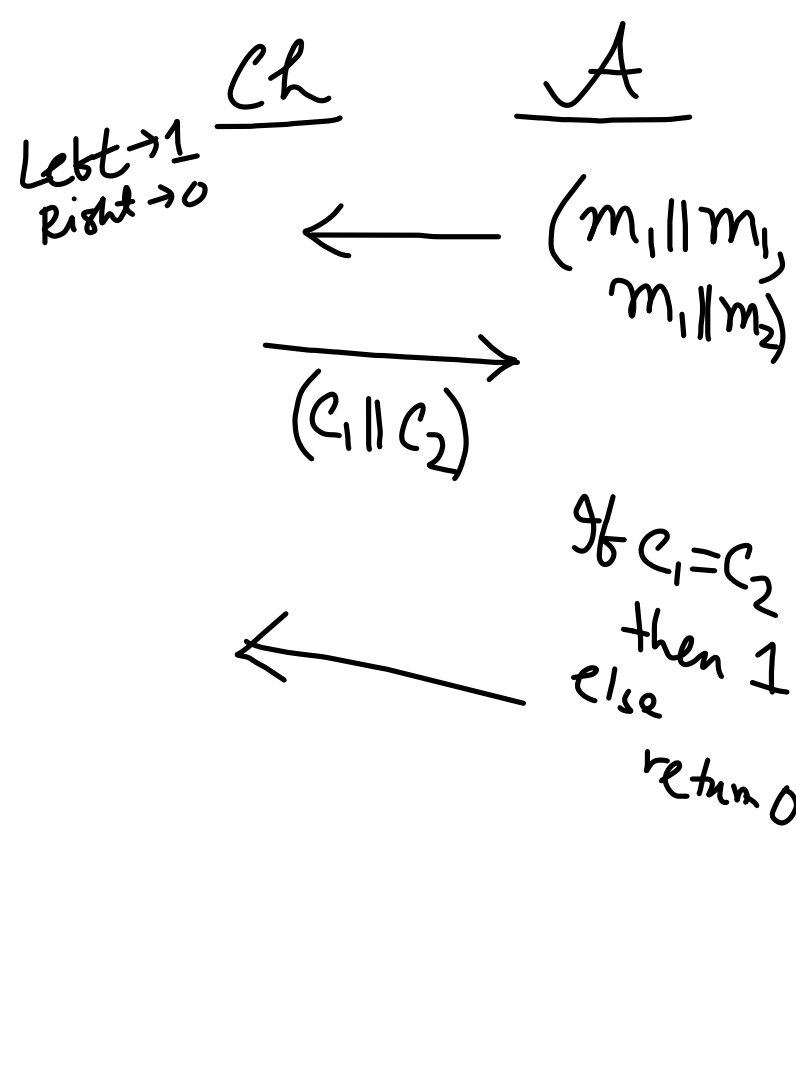
Modes of operation gives you a construction using F such that you can encrypt messages of arbitrary size.

ECB mode (Electronic code Book)

$F: \{0,1\}^k \times \{0,1\}^n \to \{0,1\}^n$ (PRF)



- Insecure
- Not Inverse-free (For decryption, you need F_k^{-1})
- Parallel
- Online ($c_i := f(m_1, \dots, m_i)$)



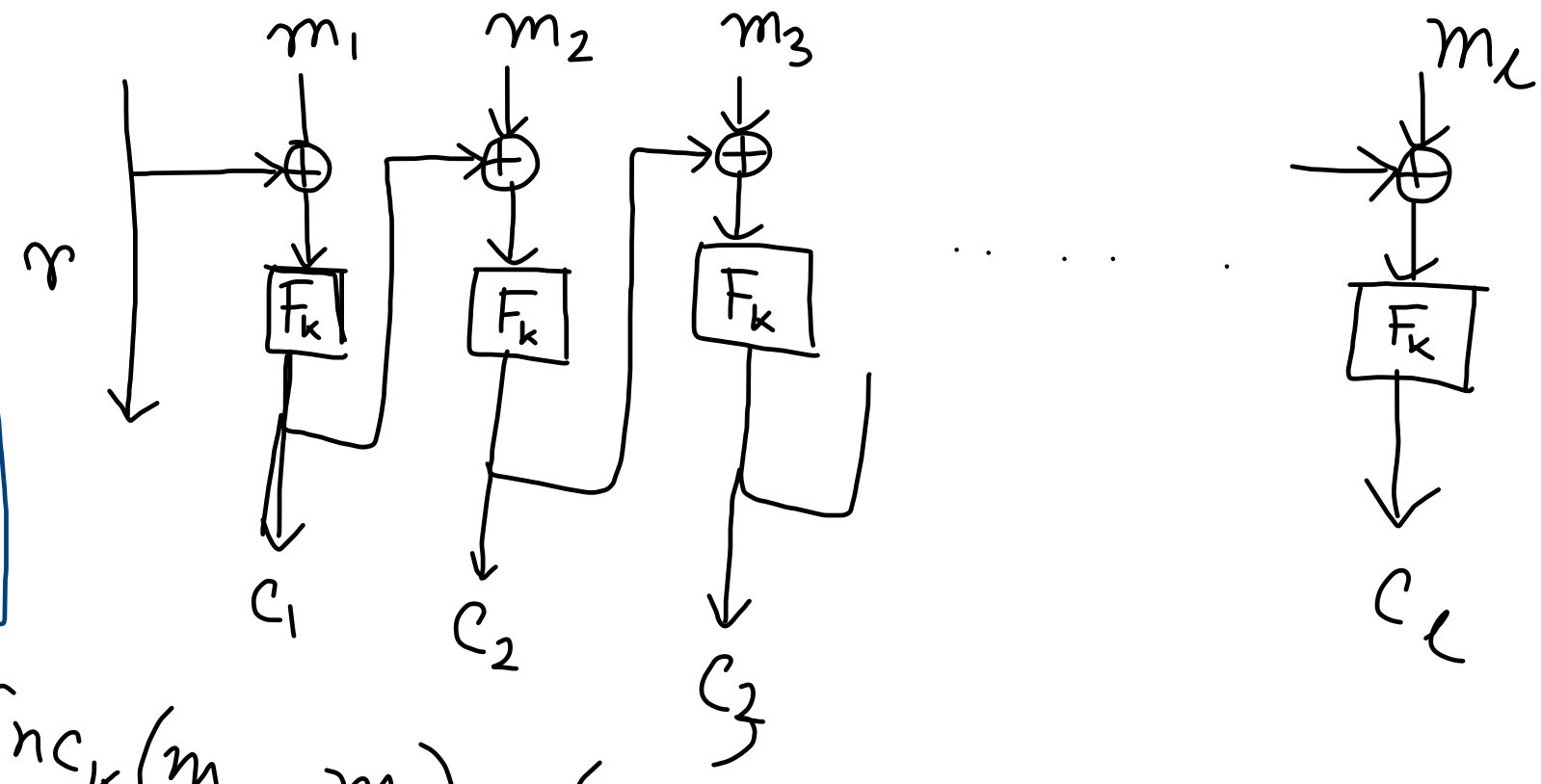
CBC Mode (Cipher Block Chaining)

$m_1 = F_k^{-1}(c_1) \oplus r$

$m_2 = F_k^{-1}(c_2) \oplus c_1$

$\vdots$

$m_i = F_k^{-1}(c_i) \oplus c_{i-1}$



$$\begin{cases} c_1 = F_k(r \oplus m_1) \\ c_2 = F_k(c_1 \oplus m_2) \\ \vdots \\ r = c_0 \end{cases}$$

$$c_i = F_k(c_{i-1} \oplus m_i)$$

$Enc_k(m_1 \dots m_\ell) := (r; c_1 c_2 \dots c_\ell)$, where $r \xleftarrow{\$} \{0,1\}^n$.

- Sequential
- Online
- Not Inverse-free

} If F is secure then CBC is secure.

☐ CBC with Nonce

$r \rightarrow$ distinct for each encryption.

$\begin{cases} r = 1 \\ r = 2 \\ \vdots \end{cases}$

$\leftarrow (m_1 \| m_2)$

$\rightarrow (r, c_1 \| c_2)$

$\leftarrow (m_1 \oplus 1 \oplus 2 \| m_2)$

$\rightarrow (2, c_1 \| c_2)$

$c_1 = F_k(m_1 \oplus 1)$

$c_1' = F_k(m_1' \oplus 2)$

$m_1' = (m_1 \oplus 1 \oplus 2)$

☐ Chained CBC

$(r, c_1 \cdots c_t) \leftarrow (m_1 \cdots m_t)$

$(c_t, c_1' \cdots c_{t'}') \leftarrow (m_1' \cdots m_{t'}')$

$\leftarrow (m_1 \| m_2)$

$\rightarrow (r, c_1 \| c_2)$

$\leftarrow (m_1 \oplus r \oplus c_2 \| m_2)$

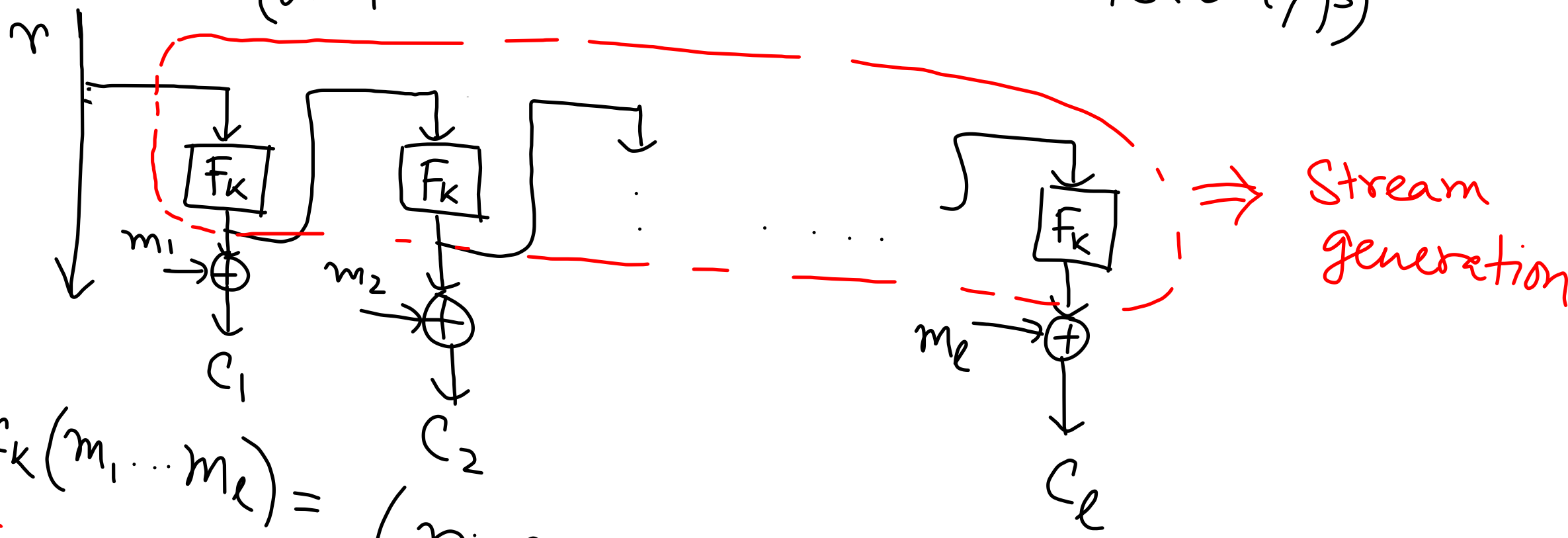
$\rightarrow (0, c_1 \| c_2)$

$c_1 = E_k(m_1 \oplus r)$

$c_1' = E_k(m_1' \oplus c_2)$

OFB (Output FeedBack)

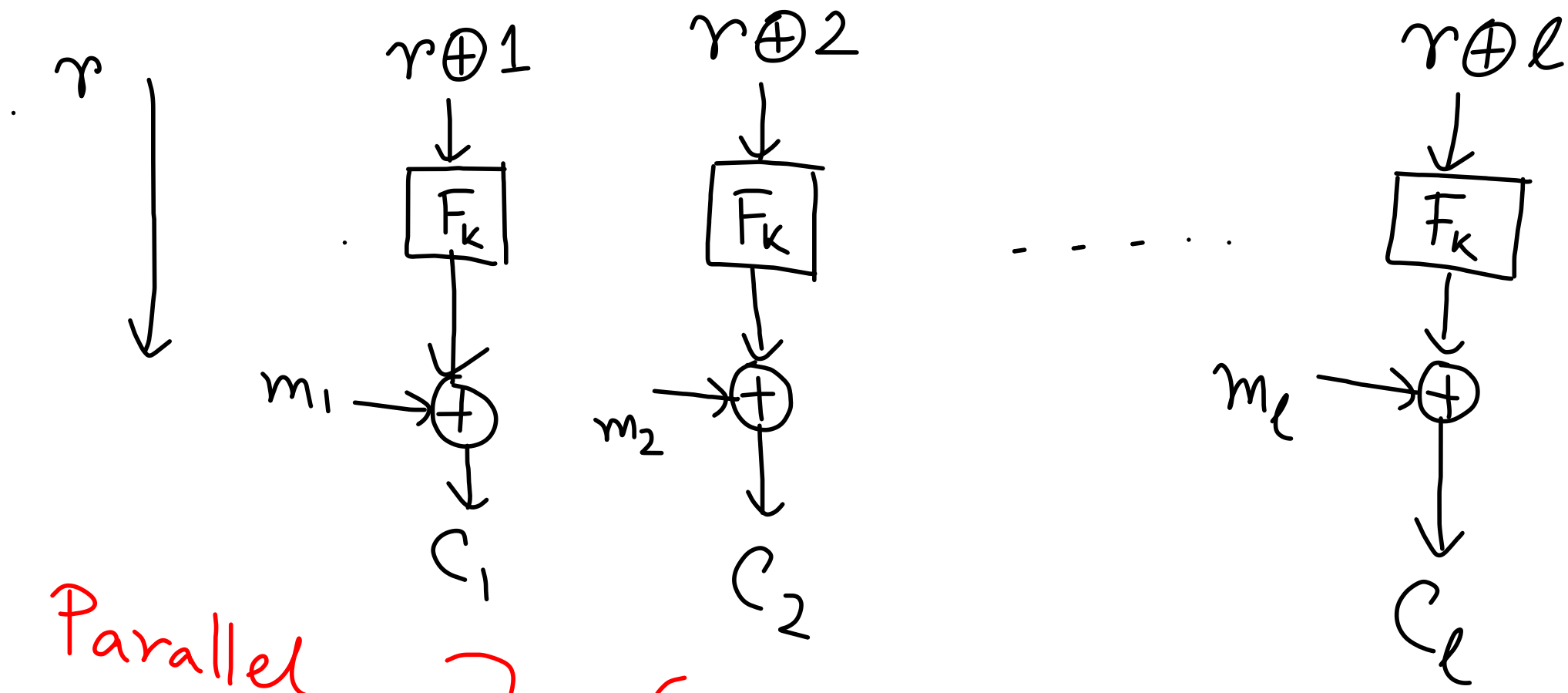
(output is feeded back to the next i/p)



$Enc_k(m_1 \cdots m_\ell) = (r, c_1 \cdots c_\ell)$

- Sequential
- Online
- Inverse-free

CTR (Counter Mode)

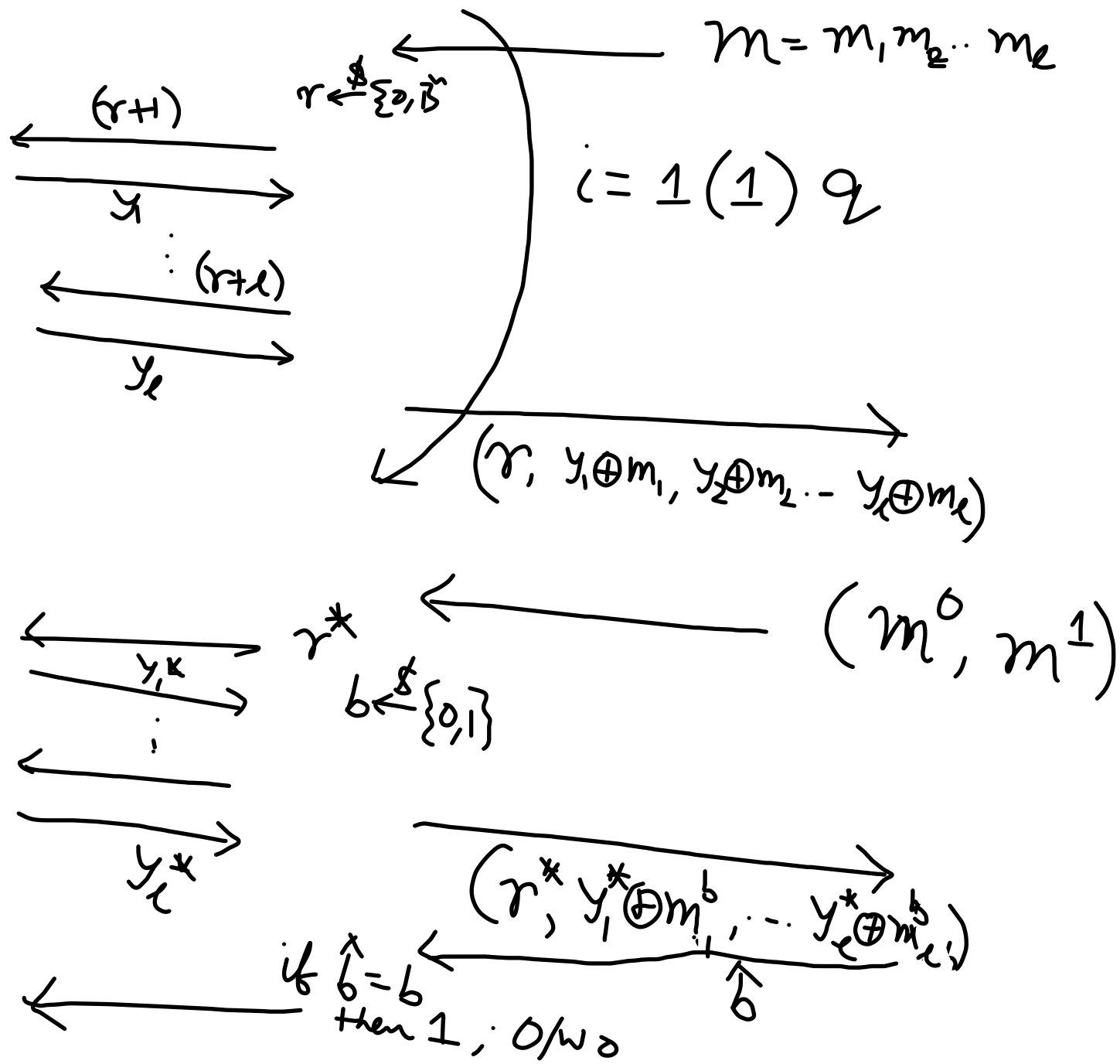


- Parallel
- Online
- Inverse-free

} If F is a PRF then Counter Mode of operation achieves IND-CPA

IND-CPA Security of CTR

$A \rightarrow$ breaks IND-CPA
then
$\mathcal{D} \rightarrow$ breaks PRF of F



$$\left| Pr[\mathcal{D}^F = 1] - Pr[\mathcal{D}^f = 1] \right| \leq negl(n)$$

$$\Downarrow \qquad \Downarrow$$

$$\left| Pr[Priv^{CPA}_{\mathcal{A},CTR} = 1] - \left(\frac{1}{2} + \frac{2l_2}{2^n}\right) \right| \leq negl(n)$$

$$\Rightarrow \boxed{Pr\left[Priv^{CPA}_{\mathcal{A},CTR} = 1\right] \leq \frac{1}{2} + \frac{2l_2}{2^n} + negl(n)}$$

$BAD_i := \{r_i \oplus 1, \ldots, r_i \oplus l\} \cap \{r^* \oplus 1, \ldots, r^* \oplus l\} \neq \emptyset$

$BAD := BAD_1 \cup \ldots \cup BAD_q$

$$Pr[BAD] \leq \sum_{i=1}^{q} Pr[BAD_i] \leq \frac{2l_2}{2^n}$$

i^{th} Query

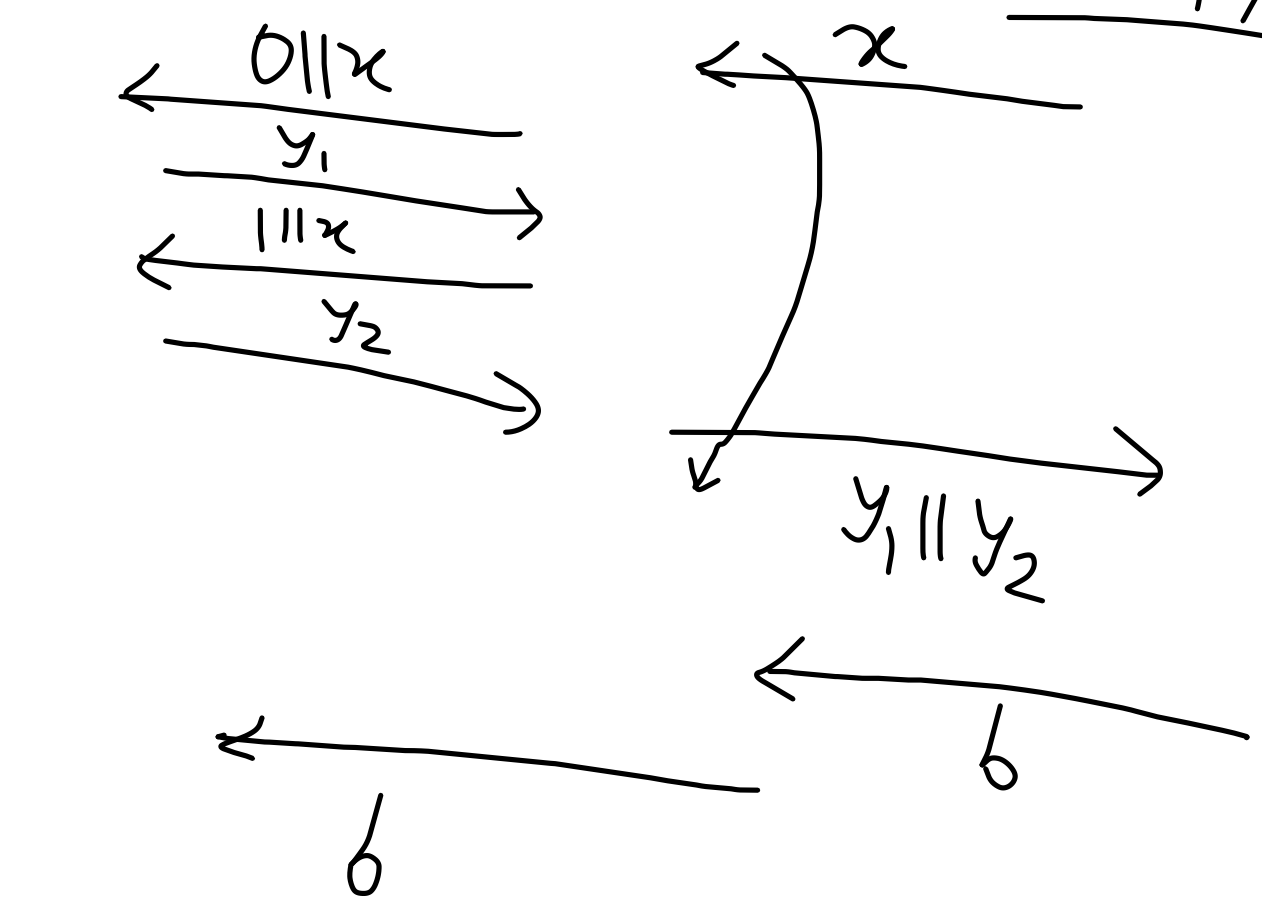
$f(r_i \oplus 1), f(r_i \oplus 2), \ldots f(r_i \oplus l)$

r^*

$f(r^*) \rightarrow f(r^* \oplus 1), \ldots, f(r^* \oplus l)$

Ex:

$$F' := F(0\|x) \,\|\, F(1\|x) \rightarrow PRF$$



$$\left| Pr\left[\mathcal{D}^F = 1\right] - Pr\left[\mathcal{D}^f = 1\right] \right|$$

$$\Downarrow$$

$$\left| Pr\left[\mathcal{A}^{F'} = 1\right] - Pr\left[\mathcal{A}^{f'} = 1\right] \right|$$

$$\begin{cases} f(0\|x_1),\ f(1\|x_1) \\ f(0\|x_2),\ f(1\|x_2) \\ \vdots \\ f(0\|x_t),\ f(1\|x_t) \end{cases}$$