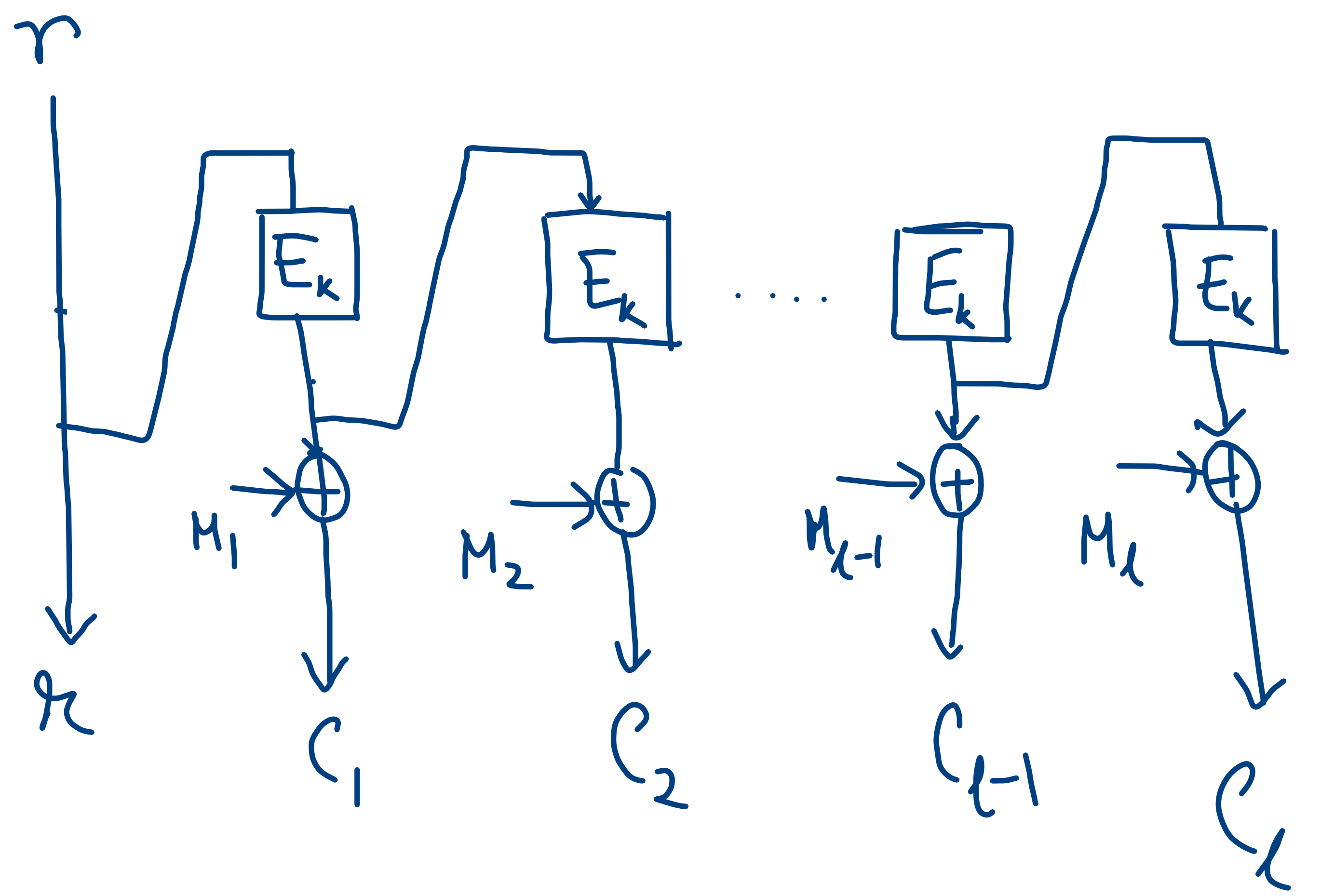
Modes of Operations

- ECB
- CBC
- OFB
- CTR

OFB (Output Feedback Mode)



$$\frac{Enc_k(M = M_1 \| M_2 \| \cdots \| \cdots M_\ell)}{r \xleftarrow{\$} \{0,1\}^n}$$

$$C_1 = E_k(r) \oplus M_1$$

$$C_2 = E_k(E_k(r)) \oplus M_2$$

$$= E_k(C_1 \oplus M_1) \oplus M_2$$

$$\vdots$$

$$C_i = E_k(C_{i-1} \oplus M_{i-1}) \oplus M_i$$

$$C \leftarrow r \| C_1 \| \cdots \| C_\ell$$

Output Feed-back Mode

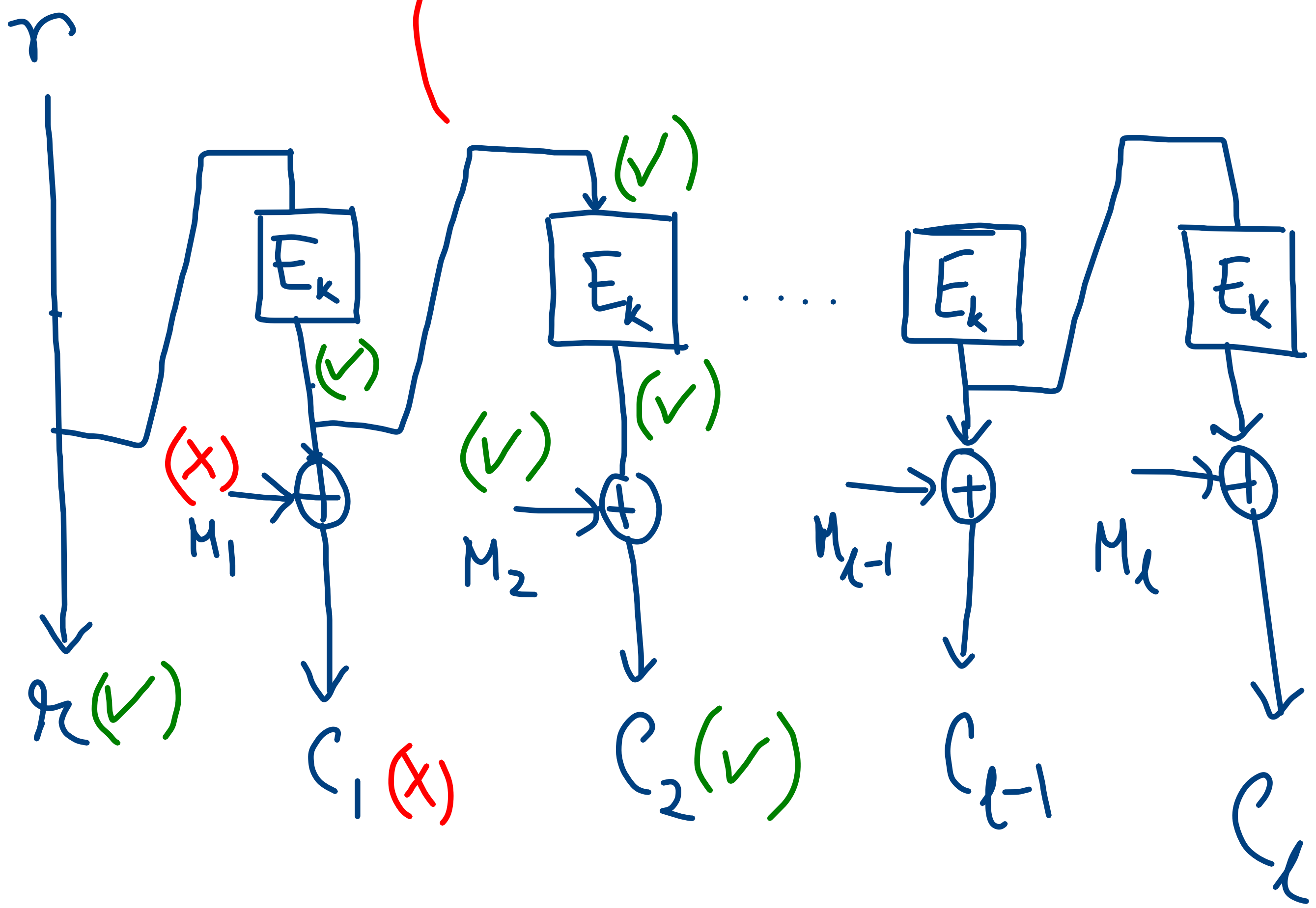
- Inverse-free
- Not Parallel
- Error at i^{th} ciphertext
  $\downarrow$
  Only changes i^{th} plaintext.

$E_K \rightarrow PRF$

$\Downarrow$

$OFB \rightarrow$ IND-CPA

Output is feeded back to the next block-cipher



$Dec_K(C_0 \| C_1 \| \cdots \| C_\ell)$

$$M_2 = C_2 \oplus E_K(C_1 \oplus M_1)$$

$\vdots$

$$M_i = C_i \oplus E_K(C_{i-1} \oplus M_{i-1})$$

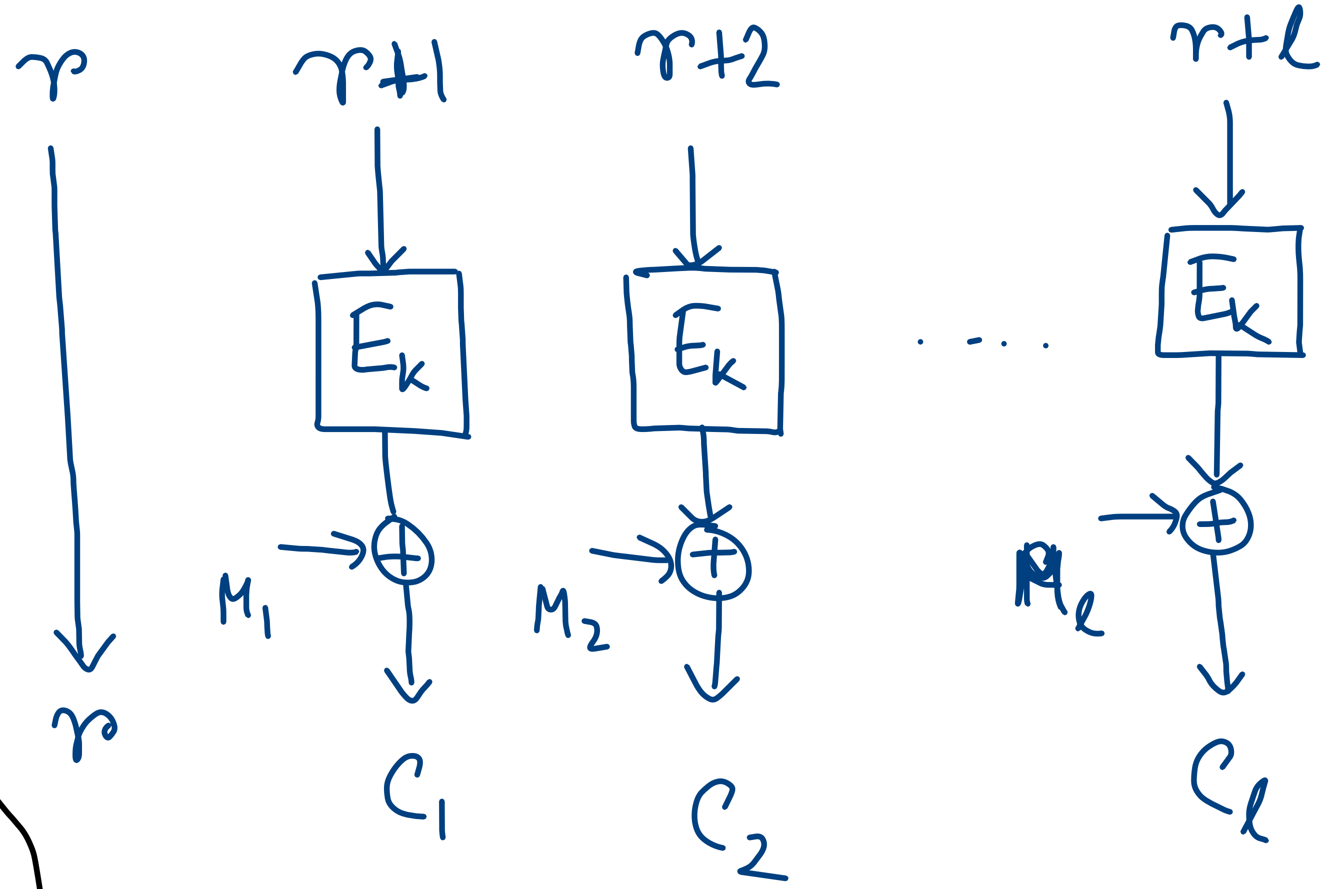
$C_1' \rightarrow M_1'$

$C_1 \oplus M_1 = C_1' \oplus M_1'$ ✓

$$M_2 = C_2 \oplus E_K(C_1 \oplus M_1)$$
$$= C_2 \oplus E_K(C_1' \oplus M_1')$$ ✓

Counter Mode

$+ \rightarrow$ integer addition modulo 2^n



$\underline{r = 4}$

$r = 00 \cdots 0100$

$\underline{\underline{r+2}} = 6$

$\Downarrow$

$r+2 = 00 \cdots 0110$

$r+i \equiv (r+i) \bmod 2^n$

- Parallel
- Inverse-free
- Error at i^{th} block (CT) $\Rightarrow$ Error at i^{th} block in message

$\underline{Enc_K(M = M_1 \| \cdots \| M_\ell)}$

$r \xleftarrow{\$} \{0,1\}^n$

for $i = 1(1)\ell$

$C_i = E_K(r+i) \oplus M_i$

return $C = r \| C_1 \| \cdots \| C_\ell$

$Dec_K(C = C_0 \| C_1 \| \cdots \| C_\ell)$

for $i = 1(1)\ell$

$M_i = E_K(r+i) \oplus C_i$

return $M = M_1 \| \cdots \| M_\ell$

Th^m If E_K is PRF then CTR mode achieves IND-CPA.

$C_i = E_K(r+i) \oplus M_i$

$i = 1(1)\ell$

E_K / f		$\mathcal{D}_{E_K/f} / Ch_{CTR}$		A_{CTR}
		$r^i \xleftarrow{\$} \{0,1\}^n$	$\longleftarrow$	$M^i = M_1^i \,\|\, M_2^i \,\|\, \dots \,\|\, M_{\ell_i}^i$
Q1	$\xleftarrow{r^i+1}$			
	$\xrightarrow{y_1^i}$			
	$\vdots$			
	$\xleftarrow{r^i+\ell_i}$			
	$\xrightarrow{y_{\ell_i}^i}$		$\xrightarrow{c^i = (r_i \,\|\, y_1^i \oplus M_1^i \,\|\, \dots \,\|\, y_{\ell_i}^i \oplus M_{\ell_i}^i)}$	
				$\lvert M_0 \rvert = \lvert M_1 \rvert = \ell$
Ch		$b \xleftarrow{\$} \{0,1\}$, $r \xleftarrow{\$} \{0,1\}^n$	$\longleftarrow$	$(M0, M1)$
	$\xleftarrow{r+1}$			
	$\xrightarrow{y_1}$			
	$\vdots$			
	$\xleftarrow{r+\ell}$			
Q2	$\xrightarrow{y_\ell}$		$\xrightarrow{(r \,\|\, y_1 \oplus M_{b,1} \,\|\, \dots \,\|\, y_\ell \oplus M_{b,\ell})}$	C_b
	$\longleftarrow (\hat{b} = b)\,?\, 1 : 0$		$\longleftarrow$	$\hat{b}$

$$\Pr\left[\mathcal{D}^{E_k(\cdot)} = 1\right] = \Pr\left[\mathrm{PrivK}^{\text{IND-CPA}}_{\text{CTR}} = 1\right]$$

$$\Downarrow$$

Playing the IND-CPA game with CTR mode & guessing the correct one

$\widetilde{\Pi} \to$ CTR mode with each E_k replaced by f

$$\Pr\left[\mathcal{D}^{f(\cdot)} = 1\right] = \Pr\left[\mathrm{PrivK}^{\text{IND-CPA}}_{\widetilde{\Pi}} = 1\right]$$

$$\leq \Pr[\text{BAD}] + \Pr\left[\mathrm{PrivK}^{\text{IND-CPA}}_{\widetilde{\Pi}} = 1 \wedge \overline{\text{BAD}}\right]$$

$$\leq \frac{q(n)\,\ell_{max}^2}{2^n} + \frac{1}{2}$$

$$\Pr\left[\mathrm{PrivK}^{\text{IND-CPA}}_{\text{CTR}} = 1\right] \leq \frac{1}{2} + \frac{q(n)\,\ell_{max}^2}{2^n} + negl(n)$$

$\max\{\ell_1, \ell_2, \ldots, \ell_{q(n)}, \ell\}$

$\hookrightarrow \ell_{max}$

BAD

$\llcorner\ \exists\, r^i$ s.t. $r^i \in \{r, r+1, \ldots, r+\ell\}$

$\vdots$

$r^i + \ell_i \notin \{r, r+1, \ldots, r+\ell\}$

$\exists\, i, j, j'$:

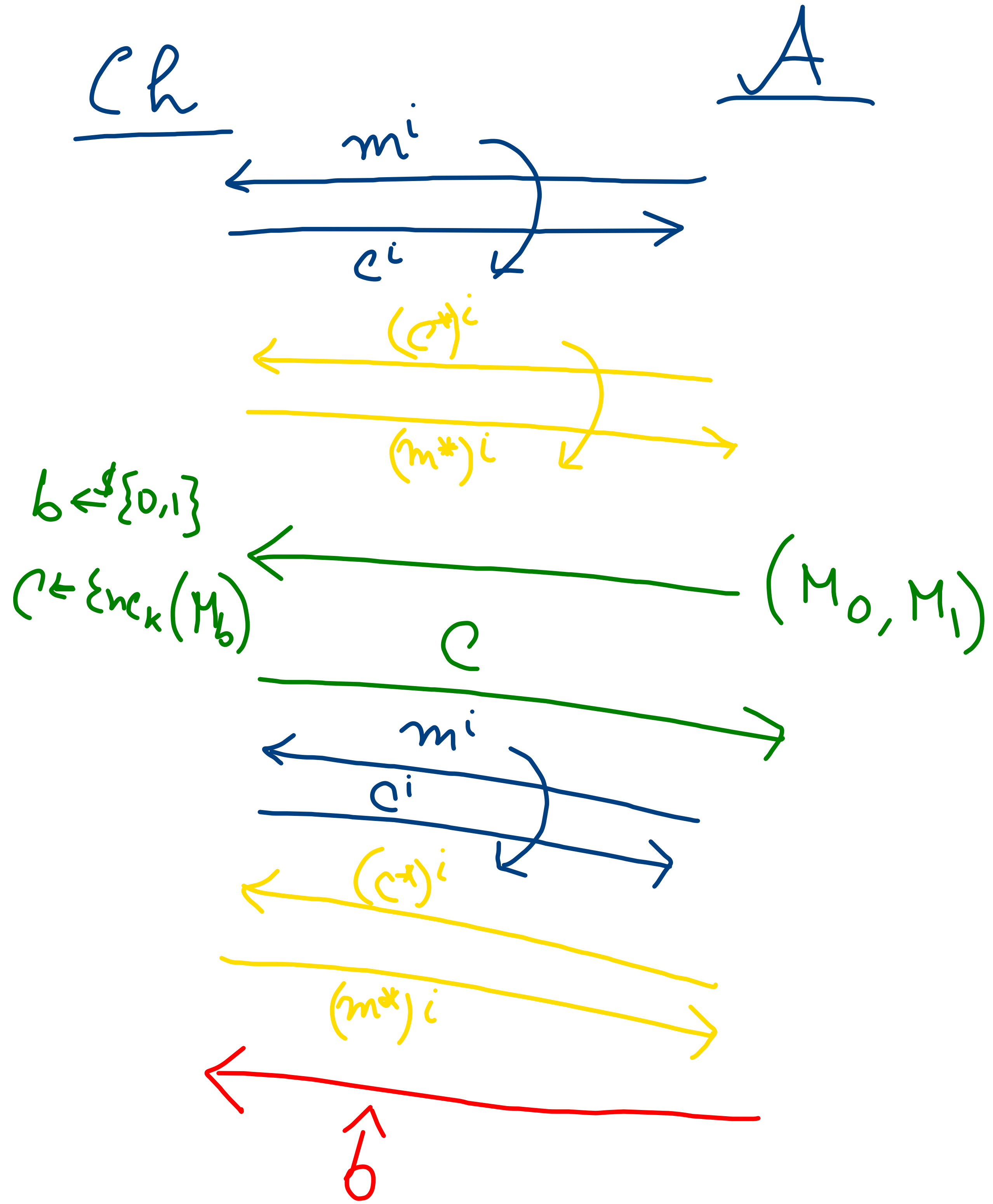
$r^i + j = r + j'$

- $j = \{0, \ldots, \ell_i\}$
- $j' = \{0, \ldots, \ell\}$

$$\Pr[\text{BAD}] \leq \sum_{i=1}^{q(n)} \frac{\ell_i \cdot \ell}{2^n} \leq \frac{q(n) \cdot \ell_{max}^2}{2^n}$$

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

Stronger Notion: IND-CCA



$$\Pr[\mathrm{PrivK}_{\Pi}^{\text{IND-CCA}} = 1]$$

$$= \Pr[b = \hat{b}]$$

All Modes of Operations

↳ IND-CCA Insecure

$\Downarrow$

Authenticated Encryption

↳ IND-CCA (ciphertexts may be invalid)