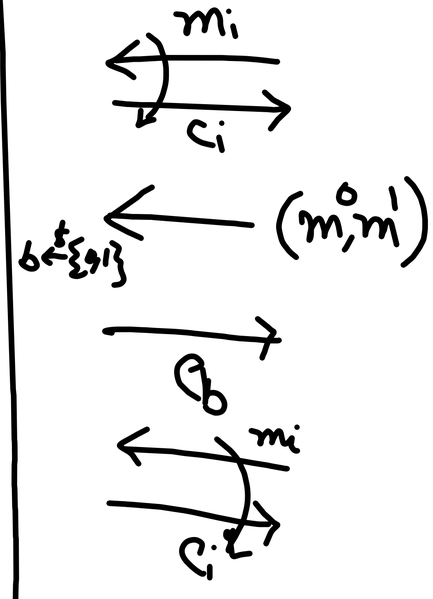
CPA Secure Encryption Scheme

Recap

- Perfect Secrecy
- Computational Indist (CI)
- PRG → Scheme that achieves CI
- CI not sufficient
  - CPA power (X)
  - Multiple enc (X)
- IND-CPA (✓)
- PRF

IND-CPA



PRF

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

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

(*) $Enc(k, m) = \left(r, F_k(r) \oplus m\right)$

— IND-CPA

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

$KG(1^n)$

$k \xleftarrow{\$} \mathcal{K}$

$Enc(m, k)$

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

return $(r, F_k(r) \oplus m)$

$Dec((c_1, c_2), k)$

return $c_2 \oplus F_k(c_1)$

Thm: If F is a PRF, then Π is IND-CPA secure.

$O = F/f$ | $\mathcal{D}_O / Ch_\Pi$ | A_Π

Query Phase 1

A_Π: m_i

$\mathcal{D}_O/Ch_\Pi$: $r_i \xleftarrow{\$} \{0,1\}^n$

r_i

$y_i = O(r_i)$

$(r_i, y_i \oplus m_i)$

Challenge Phase

A_Π: (m^0, m^1)

$\mathcal{D}_O/Ch_\Pi$: $b \xleftarrow{\$} \{0,1\}$, $r \xleftarrow{\$} \{0,1\}$

r

$y = O(r)$

$(r, y \oplus m^b)$

Query Phase 2

i

$(\hat{b} = b)\ ?\ 1 : 0$

$\hat{b}$

Observation

$$\Pr\left[\mathcal{D}^{F_k(\cdot)} = 1\right] = \mathrm{PrivK}^{cpa}_{\pi}(\,)$$

Observation

$\tilde{\Pi}$: Same as Π except we use f instead of F_k

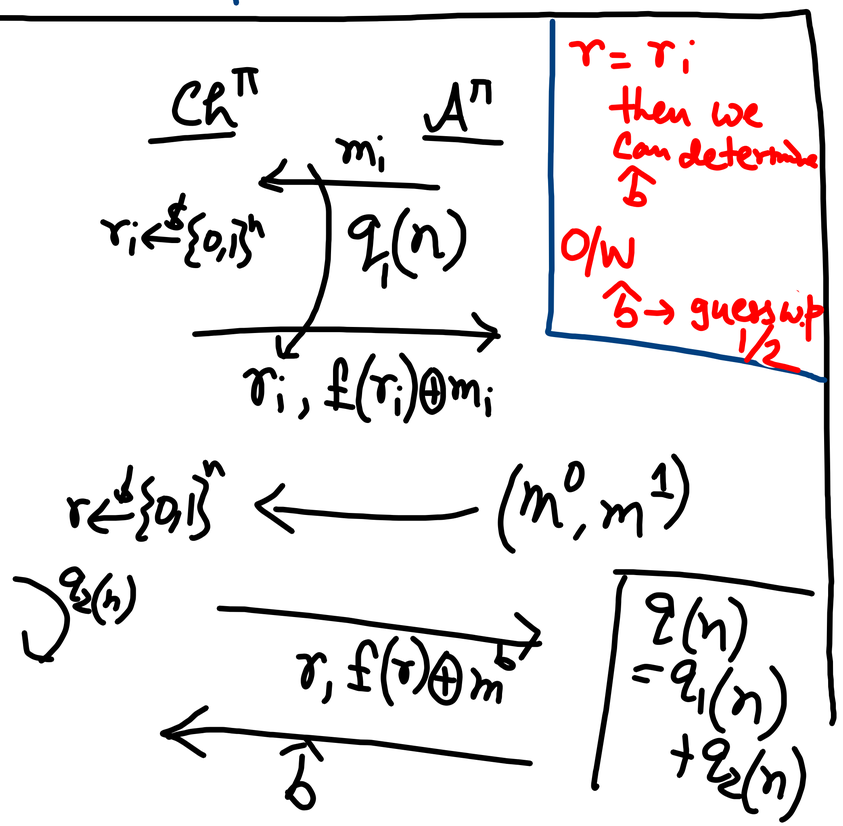
$$\Pr\left[\mathcal{D}^{F_k(\cdot)} = 1\right] = \Pr\left[\mathrm{PrivK}^{cpa}_{\Pi}(\mathcal{A}_\Pi) = 1\right]$$

$$\Pr\left[\mathcal{D}^{f(\cdot)} = 1\right] = \Pr\left[\mathrm{PrivK}^{cpa}_{\tilde{\Pi}}(\mathcal{A}_{\tilde{\Pi}}) = 1\right]$$

$$= \Pr\left[\mathrm{PrivK}^{cpa}_{\tilde{\Pi}}(\mathcal{A}_{\tilde{\Pi}}) = 1 \wedge BAD\right] + \Pr\left[\mathrm{PrivK}^{cpa}_{\tilde{\Pi}}(\mathcal{A}_{\tilde{\Pi}}) = 1 \wedge \overline{BAD}\right]$$

$$\leq \Pr[BAD] + \Pr\left[\mathrm{PrivK}^{cpa}_{\tilde{\Pi}}(\mathcal{A}_{\tilde{\Pi}}) = 1 \wedge \overline{BAD}\right]$$

$$= \left(\frac{q(n)}{2^n} + \frac{1}{2}\right)$$



BAD: $\exists i$ s.t. $r = r_i$

$\circledast$

$$\Pr[A] = \Pr[A \wedge B] + \Pr[A \wedge \overline{B}]$$

Observation

$\tilde{\Pi}$: Same as Π except we use f instead of F_k

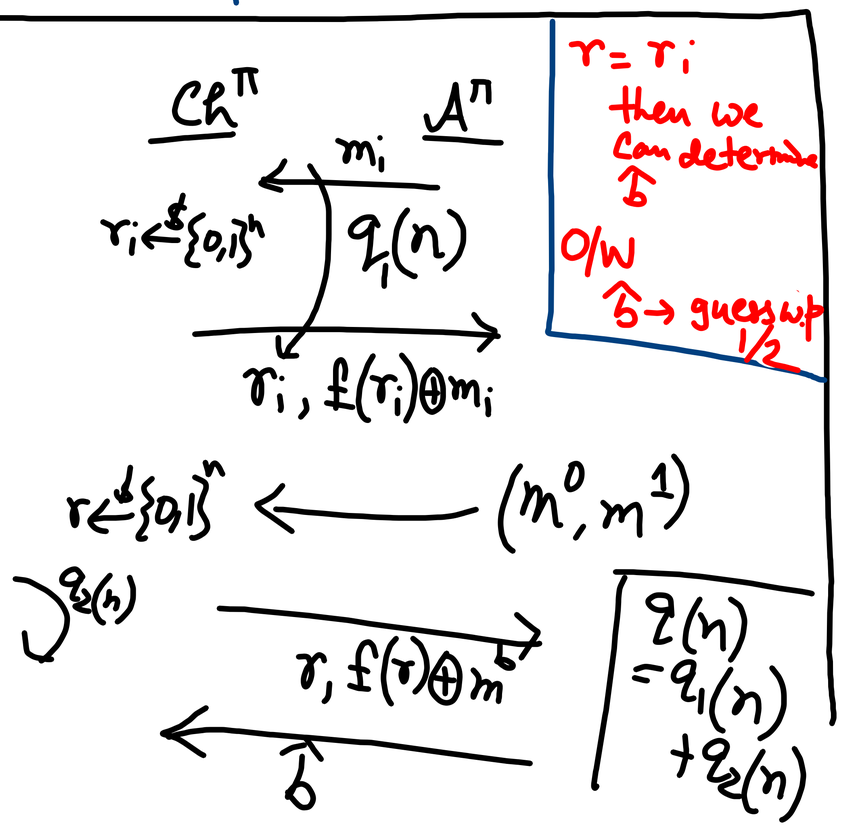
$$\Pr\left[\mathcal{D}^{F_k(\cdot)} = 1\right] = \Pr\left[\mathrm{PrivK}^{cpa}_{\Pi}(\mathcal{A}_\Pi) = 1\right]$$

$$\Pr\left[\mathcal{D}^{f(\cdot)} = 1\right] = \Pr\left[\mathrm{PrivK}^{cpa}_{\tilde{\Pi}}(\mathcal{A}_{\tilde{\Pi}}) = 1\right]$$

$$= \Pr\left[\mathrm{PrivK}^{cpa}_{\tilde{\Pi}}(\mathcal{A}_{\tilde{\Pi}}) = 1 \wedge BAD\right] + \Pr\left[\mathrm{PrivK}^{cpa}_{\tilde{\Pi}}(\mathcal{A}_{\tilde{\Pi}}) = 1 \wedge \overline{BAD}\right]$$

$$\leq \Pr[BAD] + \Pr\left[\mathrm{PrivK}^{cpa}_{\tilde{\Pi}}(\mathcal{A}_{\tilde{\Pi}}) = 1 \wedge \overline{BAD}\right]$$

$$\leq \left(\frac{q(n)}{2^n} + \frac{1}{2}\right)$$



BAD: $\exists i$ s.t. $r = r_i$ ⊛

$$\Pr[A] = \Pr[A \wedge B] + \Pr[A \wedge \overline{B}]$$

$$\Pr[BAD] \leq \frac{q(n)}{2^n}$$

If F is a PRF

$\forall$ PPT $\mathcal{D}$

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

$$\Rightarrow \quad Pr\left[\mathcal{D}^{F_k(\cdot)}(1^n) = 1\right] \leq \left(\frac{1}{2} + \frac{q(n)}{2^n} + negl(n)\right)$$

$\Pi \rightarrow$ IND-CPA $\quad Pr\left[PrivK^{cpa}_{\Pi}(1^n) = 1\right] \leq \frac{1}{2} + negl(n)$

Other Security Notions

PRP (Pseudo random Permutation)

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

$F_k : \{0,1\}^n \to \{0,1\}^n$

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

Fix k

$F_k(x) \neq F_k(y)$ iff $x \neq y$

Permutation

Other Security Notions

PRP (Pseudo random Permutation)

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

$F_k : \{0,1\}^n \to \{0,1\}^n$

$$\left| \Pr_k\left[\mathcal{A}^{F_k(\cdot)}(1^n) = 1\right] - \Pr_{\pi \leftarrow^{\$} Perm(\{0,1\}^n)}\left[\mathcal{A}^{\pi(\cdot)}(1^n) = 1\right] \right| \leq negl(n)$$

Fix k

$F_k(x) \neq F_k(y)$ iff $x \neq y$

Permutation

$O = F_k / \pi$

Other Security Notions

Strong SPRP (Pseudo random Permutation)

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

$F_k : \{0,1\}^n \to \{0,1\}^n$

$$\left| Pr\left[\mathcal{A}^{F_k(\cdot), F_k^{-1}(\cdot)}(1^n) = 1 \right]_{k} - Pr\left[\mathcal{A}^{\pi(\cdot), \pi^{-1}(\cdot)}(1^n) = 1 \right]_{\pi \leftarrow^{\$} Perm(\{0,1\}^n)} \right| \leq negl(n)$$

$O_1 = F_k / \pi$

$O_2 = F_k^{-1} / \pi^{-1}$

Fix k

$F_k(x) \neq F_k(y)$ iff $x \neq y$

Permutation

Block-Cipher

$n = 128 / 64$

Block → n-bit string.

(b is a block if $b \in \{0,1\}^n$.)

A keyed function (permutation):

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

If Perm

$\forall k \in K$, $E_k: \{0,1\}^n \to \{0,1\}^n$ is a permutation.

Block Cipher Modes of Operations

Given $E: \{0,1\}^k \times \{0,1\}^n \to \{0,1\}^n$, a block-cipher,

how can you encrypt a message of any length $[m \in \{0,1\}^*]$

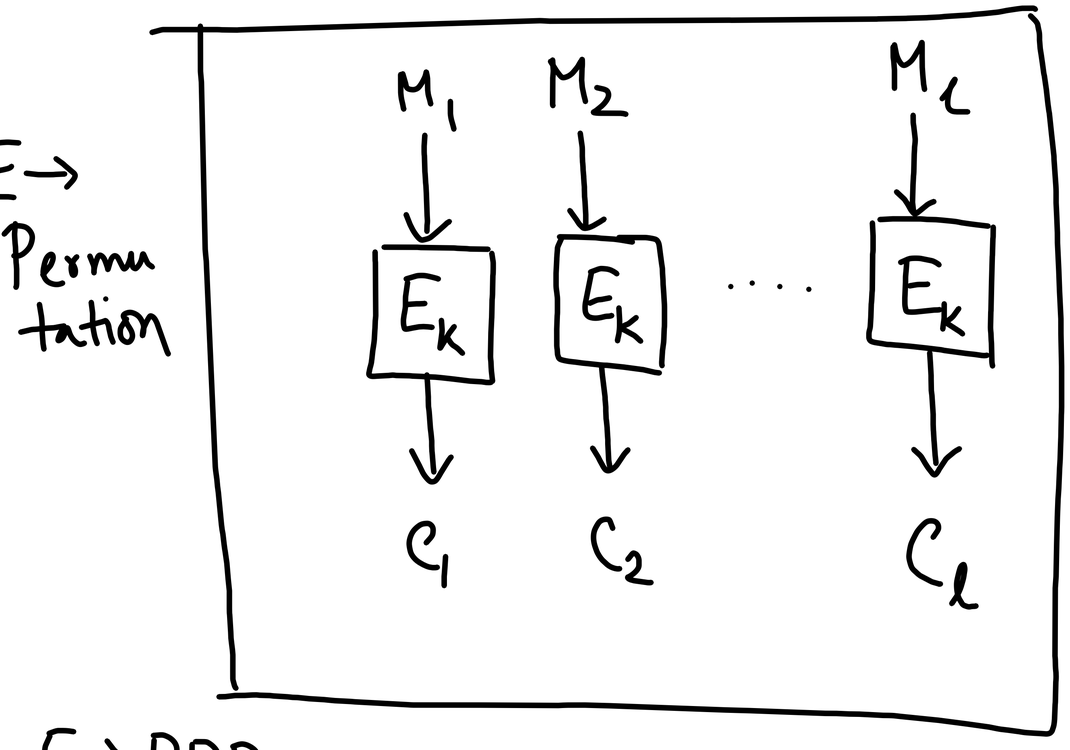
- ECB
- CBC
- OFB
- CTR

ECB (Electronic Code Book Mode)

$E \rightarrow$ Block cipher

$M \in (\{0,1\}^n)^*$

$M = M_1 \| M_2 \| \cdots \| M_\ell \;,\; |M_i| = n$



$E \rightarrow$ PRP secure.

$\underline{Enc(k,\ M = M_1 \| \cdots \| M_\ell)}$

For $i = 1(1)\ \ell$

$C_i = E_k(M_i)$

return $C = (C_1 \| C_2 \| \cdots \| C_\ell)$

$\underline{Dec(k,\ C = C_1 \| C_2 \| \cdots \| C_\ell)}$

For $i = 1(1)\ \ell$

$M_i = E_k^{-1}(C_i)$

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

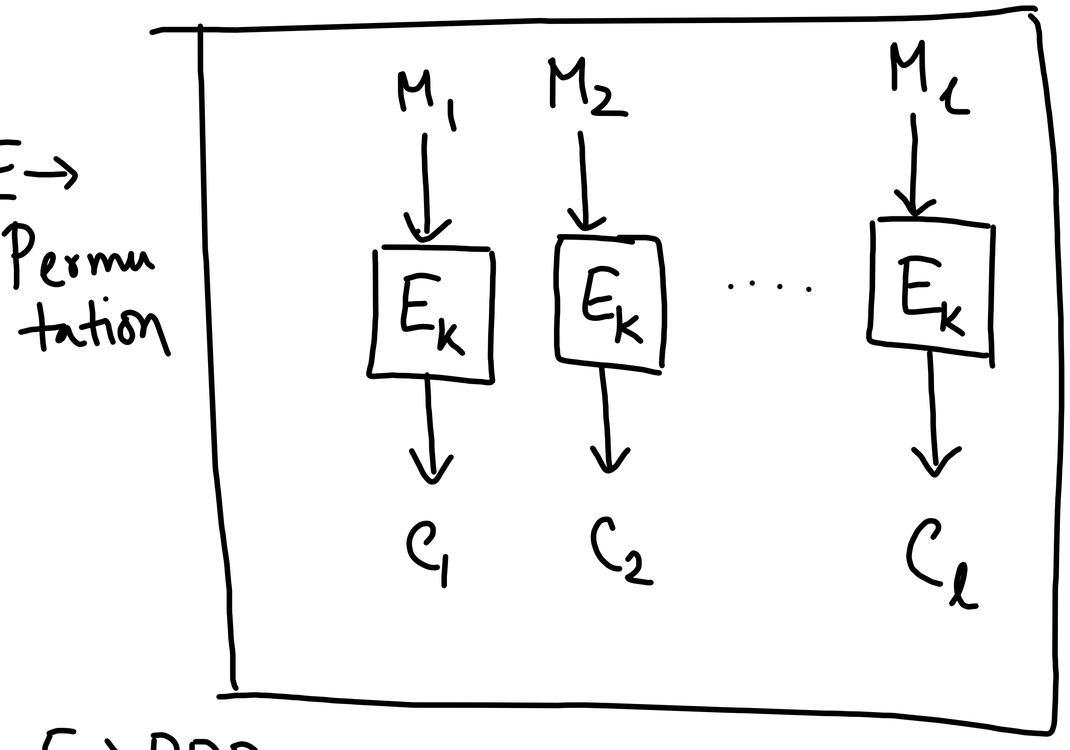
- Parallel
- Not Inverse-free
- Error Propagation
  - Error at i^{th} ciphertext block implies error at i^{th} plaintext block

ECB (Electronic Code Book Mode)

$E \rightarrow$ Block cipher

$M \in (\{0,1\}^n)^*$

$M = M_1 \| M_2 \| \cdots \| M_\ell \;,\; |M_i| = n$



$E \rightarrow$ PRP secure.

- Parallel
- Not Inverse-free
- Error Propagation
  - Error at i^{th} ciphertext block implies error at i^{th} plaintext block

$\underline{Enc(k, M = M_1 \| \cdots \| M_\ell)}$

For $i = 1(1)\ell$

$C_i = E_k(M_i)$

return $C = (C_1 \| C_2 \| \cdots \| C_\ell)$

$\underline{Dec(k, C = C_1 \| C_2 \| \cdots \| C_\ell)}$

For $i = 1(1)\ell$

$M_i = E_k^{-1}(C_i)$

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

ECB

A

$M^0 = M_1 \| M_1$

$M^1 = M_1 \| M_2$

$\leftarrow$ (M^0, M^1)

b

$\rightarrow$

$C^b = (C_1 \| C_2)$

If $C_1 = C_2$ then $b = 0$

else $b = 1$

ECB is NOT IND-CPA Secure

ECB

$\mathcal{A}$

$M^0 = M_1 \| M_1$

$M^1 = M_1 \| M_2$

$\longleftarrow$ (M^0, M^1)

b

$\longrightarrow$

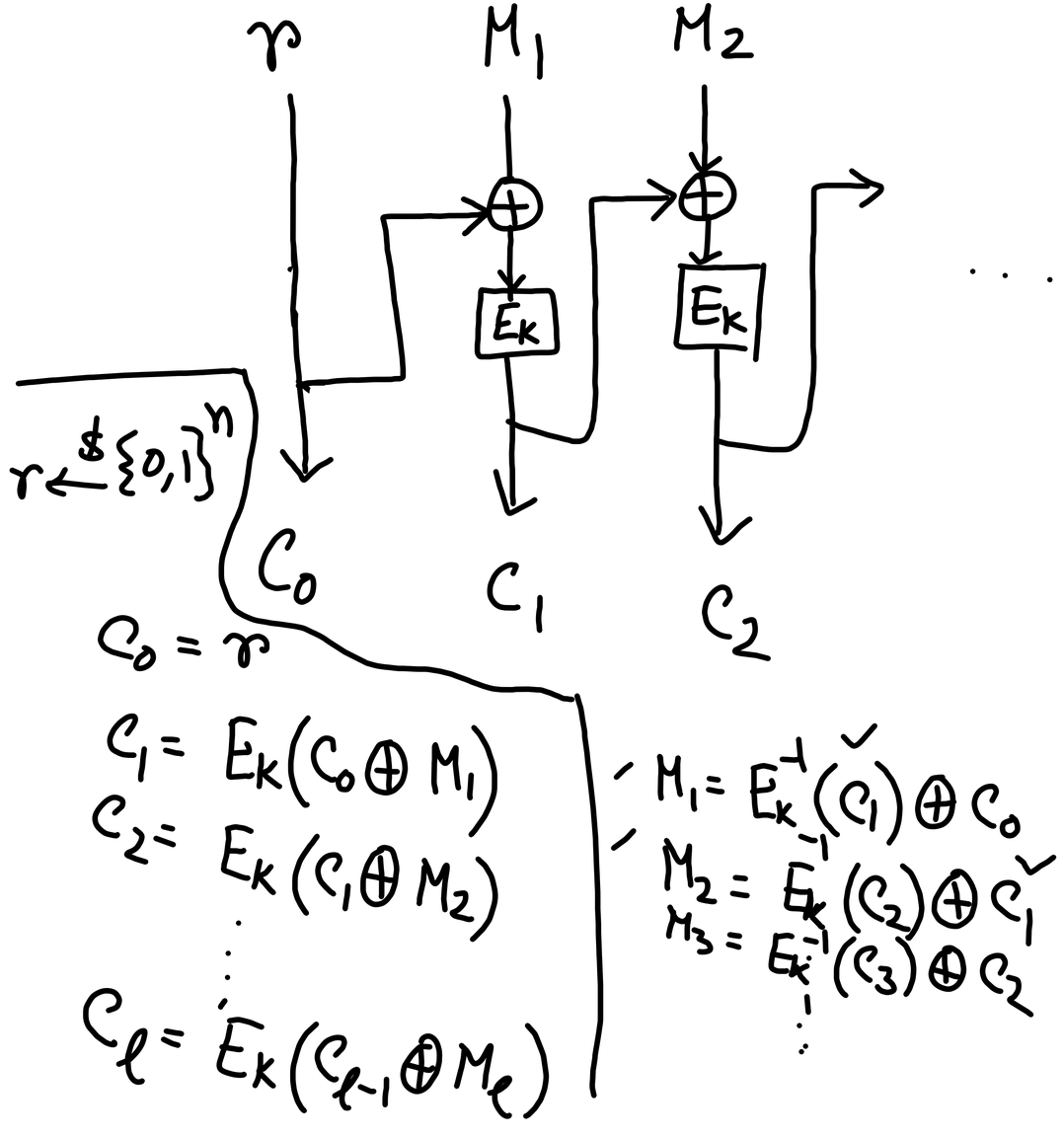
$C^b = (c_1 \| c_2)$

If $c_1 = c_2$ then $b = 0$

else $b = 1$

ECB is NOT IND-CPA Secure

CBC (Cipher Block Chaining)



$C_0 = r$

$C_1 = E_k(C_0 \oplus M_1)$

$C_2 = E_k(C_1 \oplus M_2)$

$\vdots$

$C_\ell = E_k(C_{\ell-1} \oplus M_\ell)$

$M_1 = E_k^{-1}(C_1) \oplus C_0$

$M_2 = E_k^{-1}(C_2) \oplus C_1$

$M_3 = E_k^{-1}(C_3) \oplus C_2$

$\vdots$

$C_1^* C_2 C_3 \cdots C_\ell$

$\downarrow$

$M_1^* M_2^* M_3 \cdots M_\ell$

$r \rightarrow$ distinct (but not random)

Can you construct IND-CPA attack on CBC?

If E is PRP Secure then

CBC is IND-CPA Secure

- Sequential
- Not Inverse-free
- Error propagation
  - two block error