

Coen: שם המערכת

Perfect ind \Leftrightarrow Shannon Secrecy

אנליזה: ניתוח המסר על ידי הצד השני

אנליזה: ניתוח המסר על ידי הצד השני

$$\Pr[E_K(M)=c] > 0$$

כל $m \in P$ ייתכן

$$\Pr[M=m | E_K(M)=c] \quad : \text{SIC}$$

$$= \frac{\Pr[E_K(M)=c | M=m] \cdot \Pr[M=m]}{\Pr[E_K(M)=c]}$$

↓
סימטריה

$$\Pr[E_K(M)=c]$$

$$= \frac{\Pr[E_K(m)=c] \cdot \Pr[M=m]}{\Pr[E_K(M)=c]}$$

↓
סימטריה K, M

$$\Pr[E_K(M)=c]$$

Perfect indistinguishability \Rightarrow Shannon Secrecy: $\Pr[E_K(M)=c] = \Pr[M=c]$

$C \subseteq P \subseteq \mathcal{M}$ ויכחוש M ויהי

$$\Pr[E_K(M)=c] > 0$$

יהי m ויהי

$$M=m \mid E_K(M)=c$$

$$\Pr[E_K(M)=c \mid M=m] = \frac{\Pr[E_K(m)=c]}{\Pr[E_K(M)=c]} \cdot \Pr[M=m]$$

↓
 יהי c ויהי m ויהי

יהי c

$$\Pr[E_K(M)=c] = \sum_{m' \in P} \Pr[E_K(M)=c \mid M=m'] \cdot \Pr[M=m']$$

$$\sum_{m' \in P} \Pr[E_K(m')=c] \cdot \Pr[M=m']$$

$$\stackrel{\text{perfect ind}}{\leftarrow} = \sum_{m' \in P} \Pr[E_K(m')=c] \cdot \Pr[M=m']$$

$$= \Pr[E_K(m)=c] \cdot \left(\sum_{m' \in P} \Pr[M=m'] \right)$$

1

Shannon Secrecy \Rightarrow Perfect ind

SK | PL

$$M = \begin{cases} \frac{1}{2} \rightarrow m_1 \\ \frac{1}{2} \rightarrow m_2 \end{cases}$$

$m_1, m_2 \in P$

$$\Pr[E_K(m_1) = c] = \Pr[E_K(m_2) = c] \quad \text{c.s.} \quad \text{S.3}$$

$$\Pr[E_K(m_1) = c] = 0 \quad \text{sk} \quad \Pr[E_K(M) = c] = 0 \quad \text{okc} \quad \text{z.s.} \quad \text{ok}$$

$$\Pr[E_K(m_2) = c] = 0$$

$\Pr[E_K(M) = c] > 0 \quad \text{p} \quad \text{c} - 2 \quad \text{z.s.} \quad \text{p}$

$$\frac{1}{2} = \Pr[M = m_1] = \Pr[M = m_1 | E_K(M) = c]$$

Shannon
Secrecy

$$= \frac{\Pr[E_K(m_1) = c] \cdot \Pr[M = m_1]}{\Pr[E_K(M) = c]}$$

$$\Pr[E_K(M) = c] = \Pr[E_K(m_1) = c]$$

$$\Pr[E_K(M) = c] = \Pr[E_K(m_2) = c]$$

pli
p.k. z.s. z.d
S.R.N