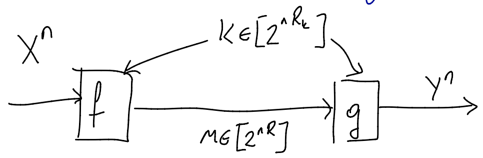
12/13/2016
Tuesday

Distributed Channel Synthesis



$\boxed{\text{Desired } Q_{Y|X}}$

$\| P_{Y^n X^n} - P_X^n Q_{Y|X}^n \|_{TV} < \varepsilon$ ← objective

$X^n \perp\!\!\!\perp K$ → from block diagram
$X^n - (M,K) - Y^n$

For $R_k = 0$, $\quad R > C_W(X,Y) = \min\limits_{X-U-Y} I(X,Y;U)$

↑ necessary and sufficient.

$C_W(X;Y) \in [I(X;Y), \min\{H(X), H(Y)\}]$

↑ let $U=X$ or $U=Y$

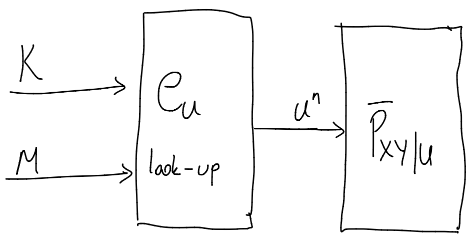
Recall:

$C_{GK}(X,Y) = \max\limits_{\substack{U-X-Y \\ X-Y-U}} I(X,Y;U)$

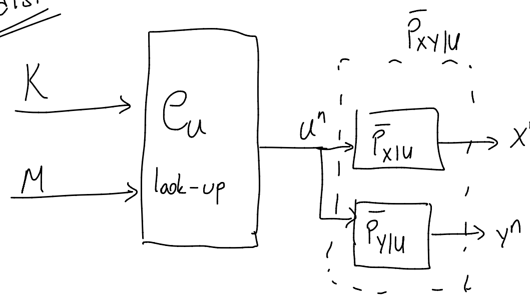
$C_{GK}(X;Y) \in [0, I(X;Y)]$

They look like dual

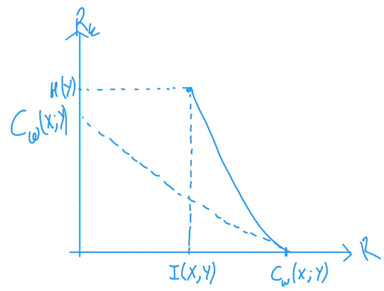
Note $C_{GK} = I(X;Y) \Leftrightarrow C_W(X;Y) = I(X;Y)$



ideal distr



Choose $\bar{P}_{XYU}$ s.t.
$X - U - Y$
and $\bar{P}_{XY} = P_X Q_{Y|X}$



$R_k + R > I(U;X,Y)$ (soft covering)

What's missing: $P_{X^n|K} = P_{X^n}$

$R_k + R > I(U;X,Y)$ (soft covering)

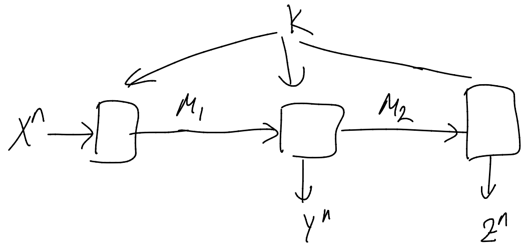
$R > I(U;X)$

Secure DCS

Objective: $\| P_{X^nY^nM} - P_X^n Q_{Y|X}^n P_M \|_{TV}$ Given M, X^nY^n look iid and ind. of M

Thm: $R_k > I(U;X,Y)$
$R > I(U;X)$ for some U: $X-U-Y$

Aside:



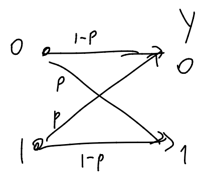
Desired: $Q_{YZ|X}$

Sai Satpathy solved secure version

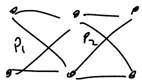
Example

$X \sim Ber(1/2)$

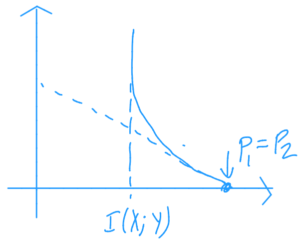
$Y|X \sim BSC(p)$



Optimal U:



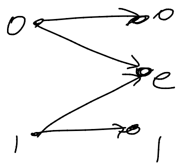
$P_1 \cdot P_2 = p$

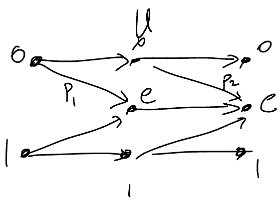


example:

$X \sim Ber(1/2)$

$Y|X \sim BEC(p)$

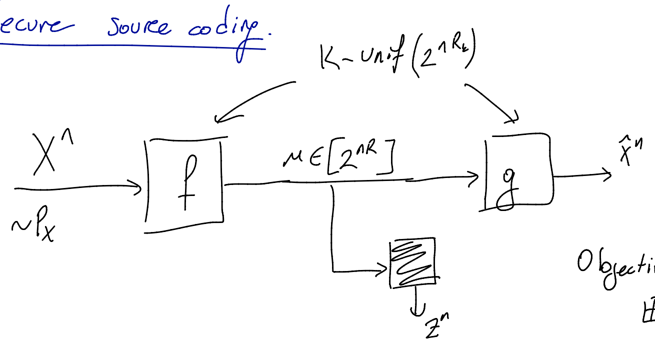




$P_1 + (1-P_1)P_2 = p$

$P_1 + P_2 - P_1P_2 = p$

Secure source coding.



Objective

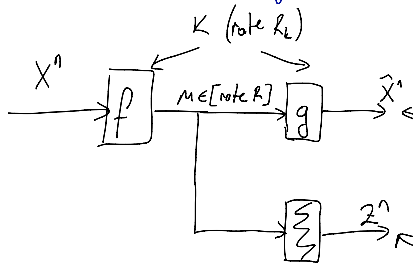
$$\mathbb{E}[d_1(X^n, \hat{X}^n)] < D_1$$

$$\min_{Z^n = f(M)} \mathbb{E}[d_2(X^n, Z^n)] > D_2$$

$\{(R, R_k, D_1, D_2)\}$ achievable ones.

12/15/2016
Thursday

Rate Distortion Theory for Secrecy Systems:



Distortion Measured by $d_1(x, \hat{x})$

Distortion measured by $d_2(x, \hat{x})$

$X^n \perp\!\!\!\perp K$

Let $d_i(x^n, \hat{x}^n) = \frac{1}{n} \sum_{i=1}^{n} d_i(x_i, \hat{x}_i)$

Performance: $\mathbb{E}[d_1(X^n, \hat{X}^n)] \leq D_1$

$$\min_{Z(\cdot)} \mathbb{E}[d_2(X^n, Z^n(M))] \geq D_2 \qquad \underbrace{\left(= \frac{1}{n} \sum_{i=1}^{n} \min_{Z_i} \mathbb{E}[d_2(X_i, Z_i(M))] \right)}_{}$$

$R_k = \infty$

because M is indep. of X_i when $R_k = \infty$

Theorem:

Closure of achievable region $= \left\{ (R, R_k, D_1, D_2) : \exists P_{\hat{X}|X} \text{ s.t. } \mathbb{E}[d_1(X, \hat{X})] \leq D_1, \ \mathbb{E}[d_2(X, \hat{X})] \geq D_2, \ I(X; \hat{X}) \leq R, \ \cancel{R_k \geq 0} \right.$

rate distortion theory

(already satisfied)

↳ because this is the closure

(we actually need $R_k > 0$)

How?