11/17/2016
Thursday

Similarity between G-P and Wiretap

G-P

- $C = \max_{P_{UX|S}} I(U;Y) - I(U;S)$

  rate of padding

  padding to make code correlated with the state of the channel

- $M \perp\!\!\!\perp S^n$ ← setting

  Decode M ← objective

- $\begin{pmatrix} M \perp\!\!\!\perp M_g \\ M_g \sim \text{Unif} \end{pmatrix}$ Ideal dist.

Wiretap

- $C_s = \max_{P_{UX}} I(U;Y) - I(U;Z)$

  rate of padding

  padding to hide the message from user receiving Z.

- $I(M;Z^n) \approx 0$ (secrecy)

  Decode M (reliability)

  $\Big\}$ objectives

- $M \perp\!\!\!\perp M_g$ $M_g \sim$ uniform

Recall G-P Proof (Achievability):

(Converse will be HW, similar to Wiretap converse proof)

S^n iid, you won't need maximize over V as in wiretap channel

Induced distribution: $P_M \bar{P}_{S^n} \underbrace{P_{M_g U^n|M S^n}}_{\text{encoder}} \underbrace{\bar{P}_{X^n|U^n S^n} \bar{P}_{Y^n|X^n S^n}}_{\text{memoryless channel}} P_{\hat{M}|Y^n}$

likelihood encoder and look-up

Note:

($\bar{P}_{S^n} = P_{S^n}$ because of our choice of $\bar{P}$)

(Chosen $\bar{P}_{UXSY} = P_S \bar{P}_{UX|S} P_{Y|XS} \Rightarrow$ marginalize $\bar{P}_S = P_S$)

Ideal: $P_M Q_{S^n M_g U^n|M} \bar{P}_{X^n|U^n S^n} \bar{P}_{Y^n|X^n S^n} P_{\hat{M}|Y^n}$

where $Q_{S^n M_g U^n|M} = \underset{\text{unif}}{Q_{M_g}} \underset{\text{look-up}}{Q_{U^n|M M_g}} \bar{P}_{S^n|U^n}$

Magic is Bayes rule gives you Likelihood encoder.

Likelihood Encoder

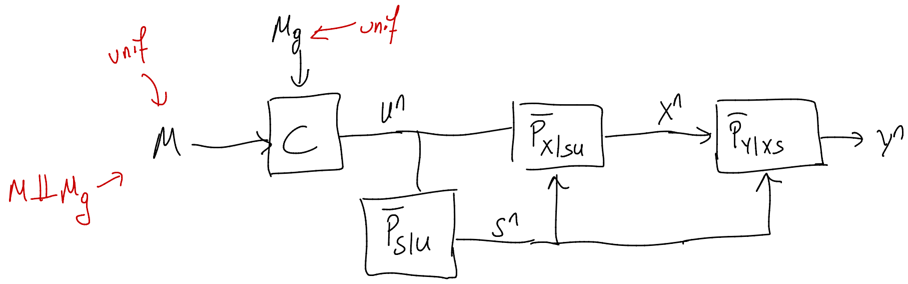
Notice $P_{M_g|S^n M} = Q_{M_g|S^n M}$ ← Bayes rule

and $P_{U^n|M M_g} = Q_{U^n|M M_g}$ ← look-up

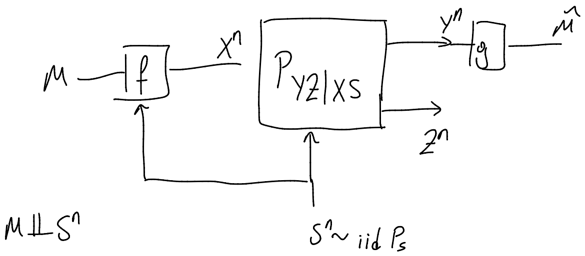
$\Rightarrow \|P-Q\|_{TV} = \frac{1}{|M|}\sum_m \|P_{S^n|M=m} - Q_{S^n|M=m}\|_{TV}$

$\bar{P}_{S^n}$

Ideal:



Combined Problem: G-P and Wiretap.



Objectives: $I(M; Z^n) \approx 0$
$\mathbb{P}[M \neq \hat{M}] \approx 0$

In this case:

$R_g > I(U;S)$ ← needed for distr. approximation

$R_g > I(U;Z)$ ← needed for secrecy

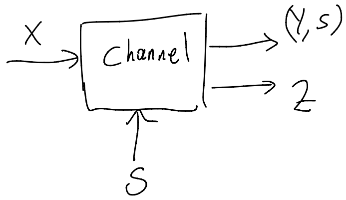
$$\Rightarrow \quad C_s \geq \max_{P_{UX|S}} I(U;Y) - \max\{I(U;S), I(U;Z)\} \quad (*)$$

Refer to [Chen-Han Vinck 2006]

→ ∇ $(*)$ is known to be suboptimal !!!

[Chia - El Gamal, 2012]:

Consider Special Case where S is known to decoder.



Equivalently: $H(S|Y) = 0$

where Y is channel output.

↘

Idea: Extract Secret Key from state ← (use random binning)

Use one-time-pad.

They achieve:

$$C_S \geq \max_{P_{UX|S}} \min \left\{ \begin{array}{l} I(U;Y|S), \\ H(S|Z,U) \end{array} \right\}$$

G-P rate $I(U;Y,S) - I(U;S)$

key rate

You can actually do a little bit better:

Better: Combine Key Extraction with Wiretap Code:

Thm (See Chia - El Gamal)

$$C_S \geq \max_{P_{UX|S}} \min \left\{ \begin{array}{l} I(U;Y|S), \\ H(S|Z,U) + \left[I(U;Y,S) - I(U;Z) \right]_+ \end{array} \right\}$$

Summary: In some cases Chia - El Gamal > Chen - Han Vinck

Chia - El Gamal is not general though! (Channel outputs the state to Y)

[Goldfeld - Cuff - Permuter 2016]

$$C_S \geq \max_{\substack{P_{UVX|S}: \\ I(U;S) \leq I(U;Y)}} \min \left\{ \begin{array}{l} I(U,V;Y) - I(U,V;S), \\ I(V;Y|U) - I(V;Z|U) \end{array} \right\}$$

↳ Choose $U = \emptyset$ to get Chen - Han Vinck

Choose $V=S$ to extract key (Chia - El Gamal)

$$C_s \geq \max_{\substack{P_{UVX|S}: \\ I(U;S) \leq I(U;Y)}} \min \left\{ \begin{array}{l} I(U,V;Y,S) - I(U,V;S), \\ I(V;Y,S|U) - I(V;Z|U) \end{array} \right\}$$

$\rightarrow I(U,\cancel{X};Y|S)$ with $V=S$

$\rightarrow I(S;Y,S|U) - I(S;Z|U)$

$H(S|U) - I(S;Z|U)$

$= H(S|Z,U)$

recovers Chia - El Gamal (first one!)

Feature of this above general solution: This scheme does not explicitly extract key as in El Gamal

Just super position code!

Encoder: 2 paddings

M_u' at rate R_u' and M_v' at rate R_v'

Codebook: $C_u = \{u^n(m_u')\} \sim \bar{P}_{U^n}$ ← Chosen from theorem

For each m_u': $C_v(m_u') = \{v^n(m, m_v')\} \sim \bar{P}_{V^n|U^n=u^n(m_u')}$

Encoder: Chose (M_u', M_v') with LE

$$P_{M_u' M_v'|S^n} \propto \bar{P}_{S^n|U^n V^n}(s^n | u^n(m_u'), v^n(m, m_v', m_u'))$$

Vary in denominator

Need Soft Covering Lemma for Super position codes.