11/10/2016
Thursday

# Secrecy Metric

induced — some distr.

$$\| P_{M,Z^n} - P_M Q_{Z^n} \|_{TV} < \varepsilon$$

secret message — eavesdropper observation

About $P_M Q_{Z^n}$: Message and observed $Z^n$ are independent
$Z^n$ is what eavesdropper observes.

→ "Strong secrecy" $I(M;Z^n) < \varepsilon$. Note that $I(M;Z^n) < \varepsilon \Rightarrow \| P_{M,Z^n} - P_M Q_{Z^n} \|_{TV} < \sqrt{\varepsilon/2}$

(by Pinskers ineq.)

⊛ If $|\mathcal{Z}| < \infty$ and $Q$ is i.i.d. and $P_M$ is uniform and $\varepsilon_n \searrow 0$ exponentially with $n$.

$D(P_{MZ^n} \| P_M Q_{Z^n}) \searrow 0$ exponentially fast (w/ some exponent, see last Tuesday's notes)

$D(P_{MZ^n} \| P_M P_{Z^n}) \leq D(P_{MZ^n} \| P_M Q_{Z^n}) \quad \forall Q$

proof: $D(P_{XY} \| P_X Q_Y) = \mathbb{E}_{P_{XY}} \log \frac{dP_{XY}}{dP_X Q_Y} = \mathbb{E}_{P_{XY}}\left[\log \frac{dP_{XY}}{dP_X P_Y}\right] + \mathbb{E}_{P_{XY}}\left[\log \frac{dP_Y}{dQ_Y}\right]$

So the two notions of secrecy are almost equivalent (in most cases assumptions in ⊛ hold!)

Weakness: "on average secret"

Assume message distribution! → weakness

$$\| P_{MZ^n} - P_M Q_{Z^n} \|_{TV} = \sum_m P_M(m) \| P_{Z^n|M=m} - Q_{Z^n} \|_{TV}$$

Similarly

$$I(M, Z^n) = D(P_{MZ^n} \| P_M P_{Z^n}) = \sum_m P_M(m) D(P_{Z^n|M=m} \| P_{Z^n})$$

You'll have a HW showing that this really is a weakness.

## Semantic Security (1982)

$\varepsilon$-SS ← semantic security if $\forall (m_0, m_1)$, $m_B$ is transmitted where $B \sim \mathrm{Bern}(1/2)$ then no ~~polinomial time~~ test can detect $B$ with error $\frac{1-\varepsilon}{2}$.

In information theory

$$\Leftrightarrow \| P_{Z^n|M=m_0} - P_{Z^n|M=m_1} \|_{TV} \leq \varepsilon \quad \forall (m_0, m_1) \text{ pairs.}$$

$$\Leftrightarrow \forall m \quad \| P_{Z^n|M=m} - \theta_{Z^n} \|_{TV} \leq \varepsilon'$$

## Bellare - Tessaro - Varde 2012:

$$\max_{P_M} I(M; Z^n) < \varepsilon \quad \text{is equivalent to S.S.}$$

## Wiretap Channel Secrecy Proof:

Choose $\bar{P}_X$ s.t. $R < I(X;Y) - I(X;Z)$ $\qquad \bar{P}_{X^n} = \prod \bar{P}_X$

Choose $R_g$: $R_g > I(X;Z)$ $\qquad \bar{P}_{XYZ} = \bar{P}_X P_{YZ|X}$

$R_g + R < I(X;Y)$ $\qquad \bar{P}_{Z^n} = \prod \bar{P}_Z$

Random Code book: $\{X^n(m, m_g)\} \sim \prod \bar{P}_X$

Reliability: $\mathbb{P}[(M, M_g) \neq (\hat{M}, \hat{M}_g)] \to 0$ as $n \to \infty$ proven for $\underbrace{\text{P2P channel}}_{\text{vanilla channel: } P_{Y|X}}$

Secrecy: $\forall m$: $\mathbb{E}_{\mathcal{C}} \| P_{Z^n|M=m} - \bar{P}_{Z^n} \|_{TV} \to 0$ by SCL. Averaged over $\mathcal{C}$.

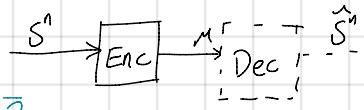
because $R_g > I_{\bar{P}}(X;Z)$

$$\Rightarrow \mathbb{E}_{\mathcal{C}} \| P_{MZ^n} - P_M \bar{P}_{Z^n} \|_{TV} \to 0 \quad \text{by linearity}$$

$\mathbb{E}_{\mathcal{C}}[A] + \mathbb{E}_{\mathcal{C}}(B) \to 0 \Rightarrow \mathbb{E}_{\mathcal{C}}[A+B] \to 0 \Rightarrow \exists \mathcal{C}$ s.t. both $A \to 0$, $B \to 0$.

# Likelihood Encoder:

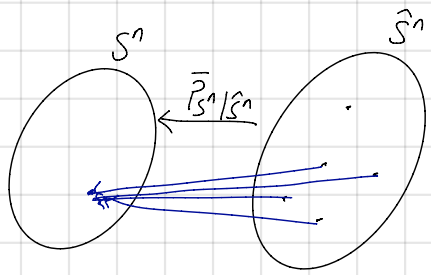
Encoder: $S^n \to M$




Given a codebook, $\{\hat{S}^n(m)\}$ and a "Test channel" $\overline{P}_{S\hat{S}} \Rightarrow \overline{P}_{S|\hat{S}}$

(no need for $\varepsilon$)

"Likelihood" (through the test channel) $\overline{P}_{S^n|\hat{S}^n}(s^n|\hat{s}^n(m))$




Likelihood Encoder (LE): Choose $M$ stoch. proportional to likelihood

$$P_{M|S^n}(m|s^n) = \frac{\overline{P}_{S^n|\hat{S}^n}(s^n|\hat{s}^n(m))}{\sum_{m'} \overline{P}_{S^n|\hat{S}^n}(s^n|\hat{s}^n(m'))}$$

<u>Two distributions:</u>

Induced:

$$\underbrace{P_{S^n}}_{\text{IID source}} \underbrace{P_{M|S^n}}_{\text{LE}} = P_{S^n,M}$$

Ideal:

$$Q_{S^nM} = \underbrace{Q_M}_{\text{uniform distr. on messages}} \underbrace{Q_{S^n|M}}_{\text{codebook look-up and test channel}}$$

$$Q_{S^nM}(s^n,m) = \frac{1}{|M|} \overline{P}_{S^n|\hat{S}^n}(s^n|\hat{s}(m))$$

apply bayes rule to see

Notice $\boxed{P_{M|S^n} = Q_{M|S^n}}$ $\longrightarrow$ Reason for Likelihood Encoder.

$$\Rightarrow \| P_{MS^n} - Q_{MS^n} \|_{TV} = \| \underbrace{P_{S^n}}_{\prod P_S \text{ does not depend on codebook}} - \underbrace{Q_{S^n}}_{\text{depends on codebook.}} \|_{TV}$$

use random codebook and $|M| = 2^{nR}$ w/ $R > I_{\overline{P}}(S,\hat{S})$ $(\sim \overline{P}_{S^n})$

$$\Rightarrow \mathbb{E}_{\mathcal{C}} \| P_{MS^n} - Q_{MS^n} \|_{TV} \longrightarrow 0 \quad \text{as } n \to \infty$$

$$\mathbb{E}_{\mathcal{C}}\left[\mathbb{E}_P\left[d(S^n, \hat{S}^n)\right]\right] \leq \mathbb{E}_{\mathcal{C}}\left[\mathbb{E}_Q\, d(S^n, \hat{S}^n) + d_{max} \| P - Q \|_{TV}\right]$$

$$= \underline{\mathbb{E}_{\mathbb{E}_{\mathcal{C}} Q}\, d(S^n, \hat{S}^n)} + d_{max}\, \underbrace{\mathbb{E}_{\mathcal{C}} \| P - Q \|_{TV}}_{\to 0}$$

$$\mathbb{E}_{\mathcal{C}} Q_{S^n \hat{S}^n}(s^n, \hat{s}^n) = \prod_{i=1}^{n} \bar{P}_{S\hat{S}}(s_i, \hat{s}_i)$$

Thus "ideal"

$\mathbb{E}_{\bar{P}}\, d(S, \hat{S})$

where $Q_{\hat{S}^n}|_M$ is a look up (deterministic)

Choose a $\bar{P}_{\hat{S}|S}$ s.t.

$\mathbb{E}_{\bar{P}}\left[d(S, \hat{S})\right] < D$

and $R < I_{\bar{P}}(S; \hat{S})$