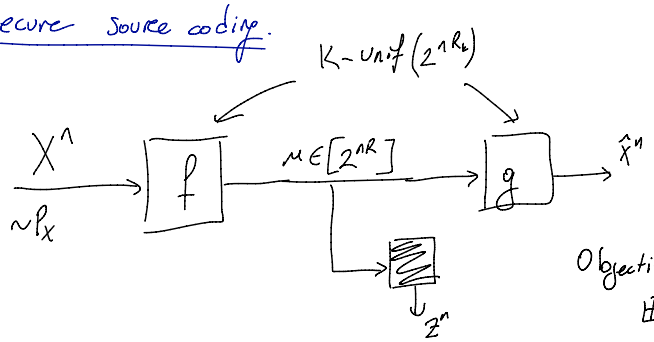
Secure source coding.



Objective

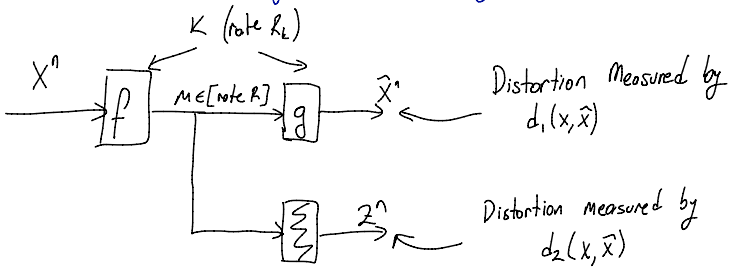
$\mathbb{E}[d_1(X^n, \hat{X}^n)] \le D_1$

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

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

12/15/2016
Thursday

Rate Distortion Theory for Secrecy Systems:



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

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

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

$\min_{Z(\cdot)} \mathbb{E}[d_2(X^n, Z^n(M))] \ge D_2$

$\left(= \frac{1}{n} \sum_{i=1}^{n} \min_{Z_i} \mathbb{E}[d_2(X_i, Z_i(M))] \right.$

$R_K = 0$ ← because M is indep. of X_i when $R_K = 0$

Theorem:

Closure of achievable region $= \{(R, R_K, D_1, D_2) :$

- $\exists P_{\hat{X}|X}$ s.t.
- $\mathbb{E}[d_1(X, \hat{X})] \le D_1$
- $\mathbb{E}[d_2(X, \hat{X})] \ge D_2$
- $I(X, \hat{X}) \le R$
- ~~$R_K \ge 0$~~ (already satisfied)
  - ↳ because this is the closure (we actually need $R_K > 0$)

rate distortion theory

How?

Example: $X \sim \text{Bern}(1/2)$

Lossless at intended receiver: $(D_1 = 0)$

d_2 = Hamming distance

Let $R = 1$ bit/symbol

$R_k = \frac{1 \text{ bit}}{n \text{ symbols}}$

Encoder using 1 bit of Key Total for any n.

Xor Key with entire source

If $K=0$ $M = X^n$ $\quad \mathbb{E}[d_2(X^n, Z^n(M))] = 1/2$

$K=1$ $M = \bar{X}^n$

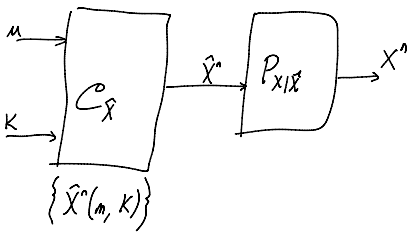
→ But this secrecy (although best we can hope for) is very fragile because if Z gets a tiny side information and get 1-bit of X^n, then Z^n knows X^n !!!

In general, construct different random codebook for each key value

If R_k is big enough, effectively one-time pad

↳ Not our case!!

With LE, consequence is obvious!



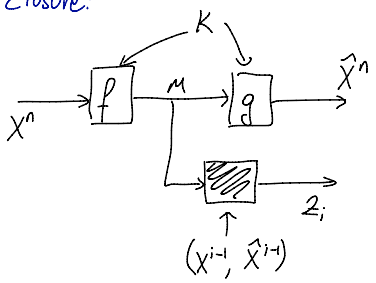
$K \perp\!\!\!\perp X^n \Rightarrow I(X;\hat{X}) \le R$

and

$P_{X_i|M} \simeq P_X \quad \forall i$

→ Eavesdropper cares about $P_{X_i|M}$

Causal Disclosure:



$Z_i(M, X^{i-1}, \hat{X}^{i-1})$ for each i

extra information.

→ "Real-time" pessimistic assumption.

→ Applies to repeated game

→ Has nice special case

* Solution: Sanitize past output (using secure DCS)

Thm: Rate region:

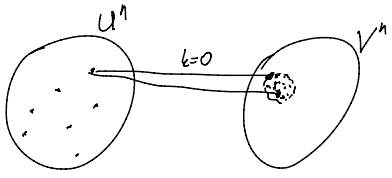
$$\left\{(R_1, R_k, D_1, D_2) : \exists\, P_{UV\hat{X}} \text{ s.t. } \begin{array}{l} X-(UV)-\hat{X} \\ R \geq I(X;UV) \\ R_k \geq I(X,\hat{X};V|U) \\ D_1 \geq \mathbb{E}[d_1(X,\hat{X})] \\ D_2 \leq \min_z \mathbb{E}[d_2(X, z(U))] \end{array}\right\}$$

Intuition: Split description into two parts. Send U in the clear. Secure V.

Achievability: Superposition code:

U is base layer

V layer indexed by key (diff for each key)



Ignore U for the moment $U=\emptyset$, use secure DCS

$$P_{X^n\hat{X}^n|M} = \pi^n P_{X\hat{X}}$$

Special case when you have log-loss dist. func.

Secrecy performance:

$$\min_{Z_i(M, X^{i-1})} \mathbb{E}\left[\frac{1}{n}\sum d_2(X_i, Z(M, X^{i-1}))\right]$$

$$\frac{1}{n}\sum_{i=1} H(X_i \mid M, X^{i-1}) = \frac{1}{n} H(X^n \mid M)$$