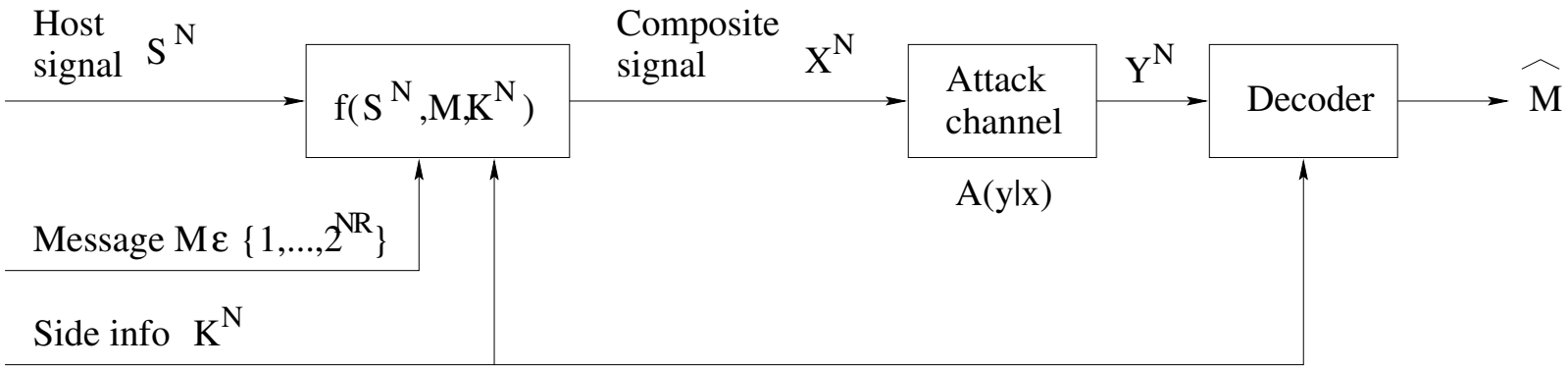
# SESSION 4. PERFORMANCE ANALYSIS: CAPACITY

- Communication Model
- Role of Side Information
- Data-Hiding Capacity
- Gaussian Sources
- Capacity of Constrained Systems
- Parallel Gaussian Sources

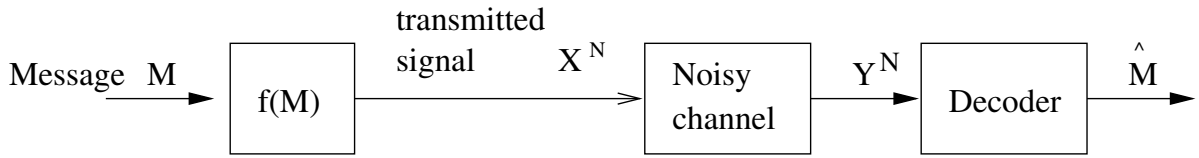
# 1. Communication Model




- Probability of error $P_{e,N} = Pr[\hat{M} \neq M]$
- Probability mass function $p(s,k)$ (iid symbols)
- Distortion function $d^N(S^N, X^N) = \frac{1}{N}\sum_{i=1}^{N} d(S_i, X_i)$
- Constraint on encoder: $E[d^N(S^N, X^N)] \leq D_1$
- Constraint on attacker : $E[d^N(S^N, Y^N)] \leq D_2$

- Goal: make $P_{e,N} \to 0$ as $N \to \infty$
- Maximum rate $R$ such that this is possible is *data-hiding capacity* $C$
- Hoes does this relate to classical communication problems?

# Problem #1: Shannon's Communication Problem




Shannon's channel coding theorem gives

$$C = \max_{p(x)} I(X;Y)$$

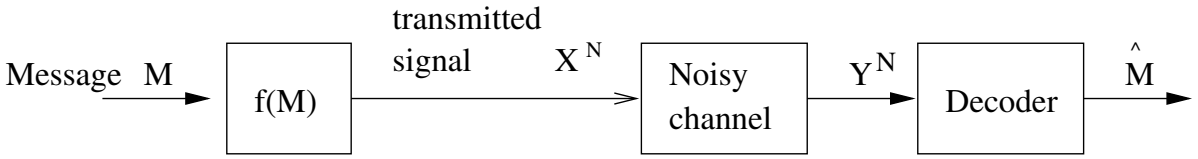
where $I(X;Y) = \sum_x \sum_y p(x,y) \log_2 \frac{p(x,y)}{p(x)p(y)}$

Capacity bound can be achieved by random coding

## 2. Role of Side Information

### Problem #2: Communication With Side Information at Encoder and Decoder

- Let $Z$ = side information shared by encoder and decoder

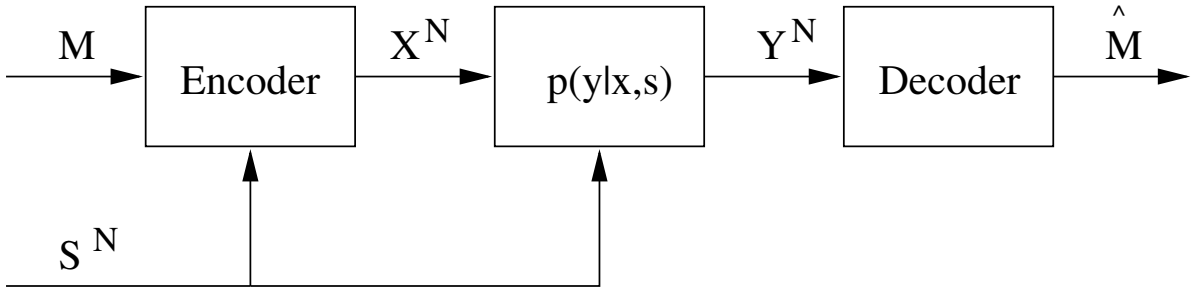



- For private data hiding, $Z = (S, K)$

$$C = \max_{p(x|z)} I(X;Y|Z)$$

# Problem #3: Communication With Side Information at Encoder Only

- Problem studied by Gel'fand and Pinsker (1980)
- Let $S$ = side info. available to encoder but not to decoder




$$C = \max_{Q(x,u|s)} [I(U;Y) - I(U;S)]$$

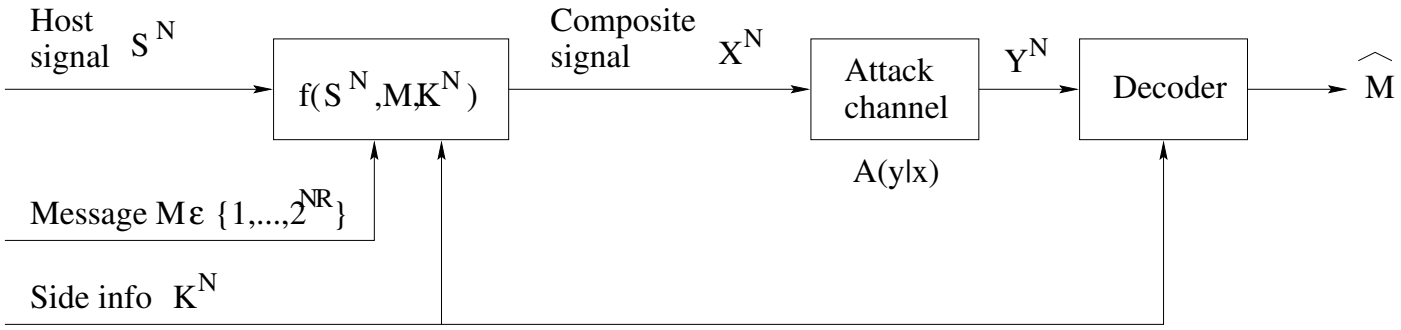
where $U$ is an auxiliary random variable, and $(U, S) \rightarrow X \rightarrow Y$ forms a Markov chain

- Capacity can be achieved by random coding

## Applications

- Communication over channels with random parameters $s$
- Communication with known interference
- Example: *Writing on Dirty Paper*

# 3. Data-Hiding Capacity

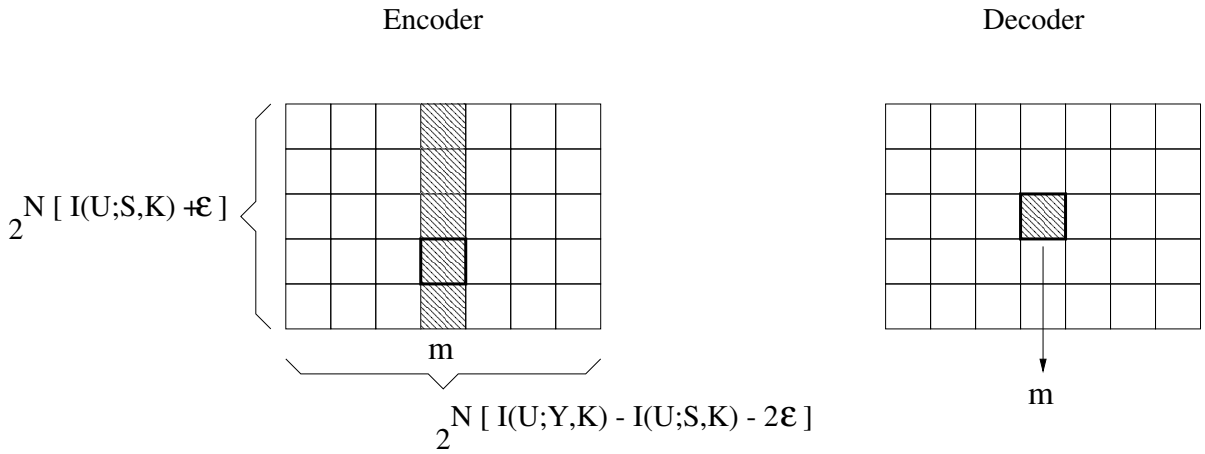



- For fixed attack channel, capacity is given by

$$C(D_1, A) = \max_{Q(x,u|s,k)} \underbrace{[I(U;Y|K) - I(U;S|K)]}_{J(Q,A)}$$

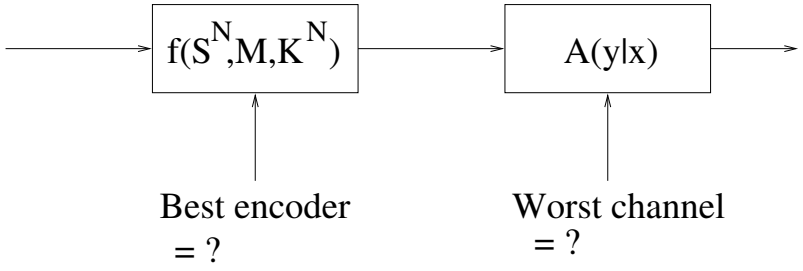
- $Q$ = covert channel
- Host signal $S^N$ is known at the encoder and should not be treated as unknown interference (as is often done in WM literature)

# Random Bin Coding Technique




- Construct array of codewords sampled from distribution $p(u^N)$
- Given message $m$, encoder selects codeword $u^N$ that is *jointly typical* with $(s^N, k^N)$; then selects $x^N = f(s^N, u^N, k^N)$
- Decoder selects codeword that is jointly typical with $(y^N, k^N)$

# The Data Hiding Game




- Who knows what?
- Assume information hider does not know attack channel $A$
- Assume attacker knows IH code $f$ but not secret key $k^N$
- Assume decoder knows IH code $f$ and attack channel $A$
- Hiding capacity for this game is

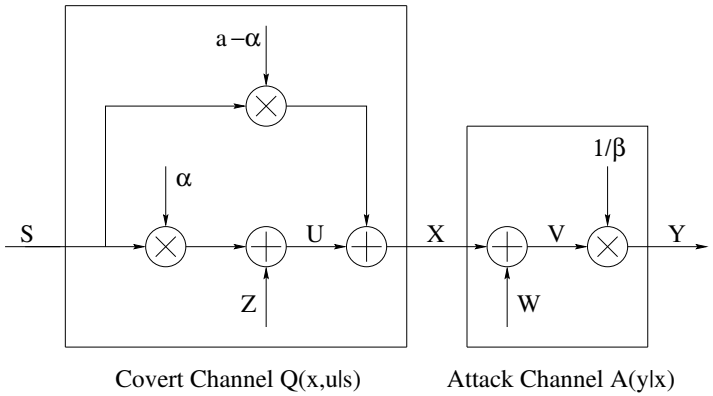
$$C(D_1, D_2) = \max_{Q} \min_{A} \underbrace{[I(U;Y|K) - I(U;S|K)]}_{J(Q,A)}$$

## Comments

- Capacity may be hard to evaluate
- In practice, require (capacity-approaching) structured codebooks instead of unmanageable random codebooks
- Optimal decoder = ML decoder

# 4. Gaussian Channels

- $S \sim$ i.i.d. $\mathcal{N}(0, \sigma^2)$, $\quad d(S, X) = (S - X)^2$
- Assume host signal is unavailable at decoder
- Capacity-achieving distributions are Gaussian:




- where $a$, $\alpha$, $\beta$ are constants depending on $D_1, D_2, \sigma_s^2$.

## Strong Host: $\sigma_s^2 >> D_1, D_2$

- Simpler solutions in this case

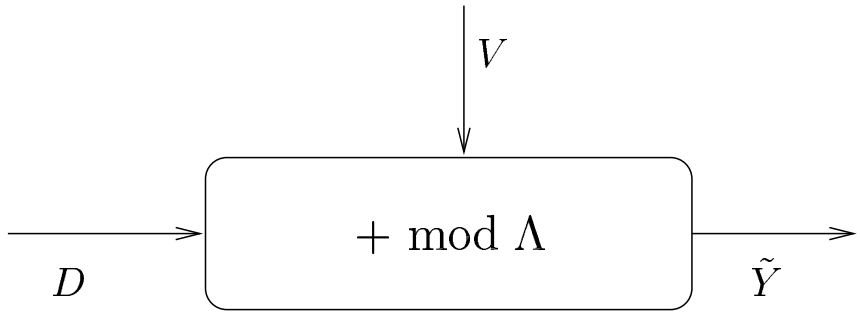
$$C \sim \tfrac{1}{2} \log (1 + WNR)$$

  where $WNR = \frac{D_1}{D_2}$

- Optimal covert channel: $U = Z + \alpha S$, where $\alpha \sim \frac{WNR}{1+WNR}$
- Same asymptotic capacity result holds if $S$ is non-Gaussian

# 5. Capacity of Constrained Systems

- First consider scalar QIM systems
- Transmission of codewords $d_m^N, m \in \mathcal{M}$ over MAN channel:

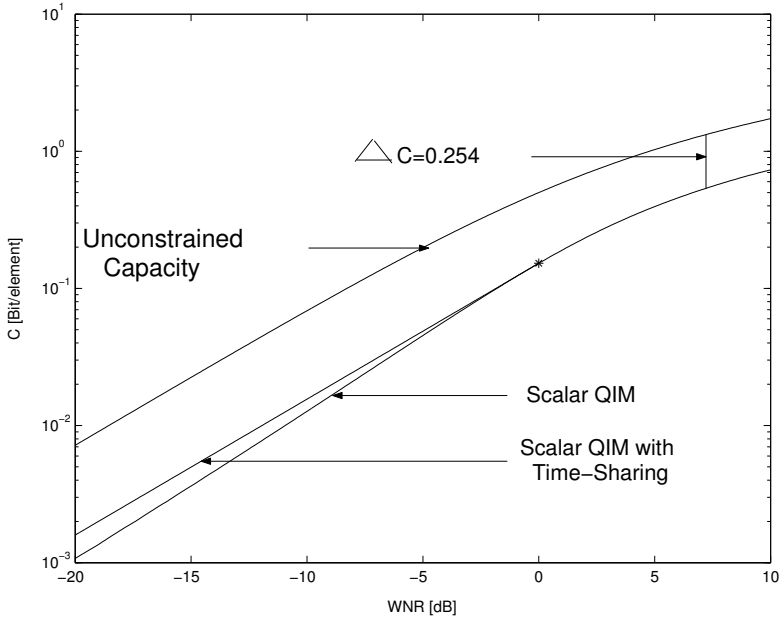



- Maximum rate of reliable transmission:

$$R_\alpha^{\mathrm{S-QIM}} = \max_{p_D} I(D; \tilde{Y})$$

- $\alpha_{\mathrm{opt}} \approx \sqrt{\frac{WNR}{WNR+2.71}}$, numerical approximation.

- Can enlarge input alphabet to $[0, \Delta]$
- Capacity curves:




- Capacity gap $\sim$ 2dB at $R = 0.5$ bit/sample
- Capacity gap $= \frac{1}{2}\log_2 \frac{2\pi e}{12} \approx 0.254$ bit at high WNR's
- Improvements can be obtained using lattice quantizers
- Capacity gap $\to 0$ using high-dimensional lattices

## Capacity of Sparse QIM Systems

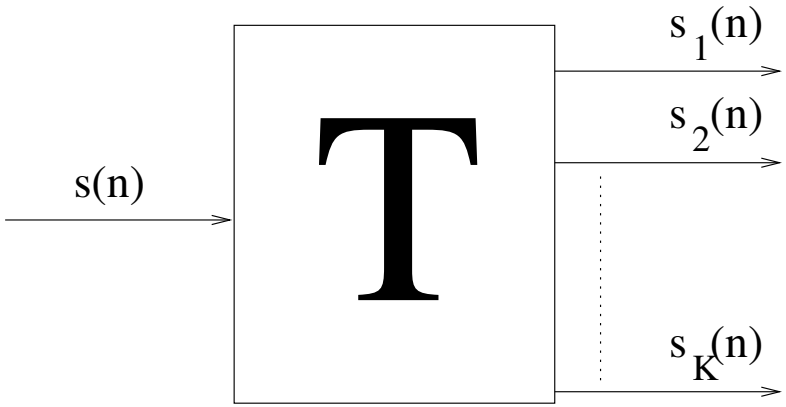
- Can easily obtain rates of reliable transmission:

$$C_{\tau}^{\text{sparse}}(WNR) = \tau\, C^{\text{S-QIM}}(WNR/\tau)$$

- Maximizing over sparsity factor $\tau$, we obtain $C^{\text{sparse}}(WNR)$ as the *upper convex envelope* of $C^{\text{S-QIM}}(WNR)$.
- Straight line for $0 \leq WNR \leq WNR^*$,
  same as $C^{\text{S-QIM}}(WNR)$ for $WNR < WNR^*$.

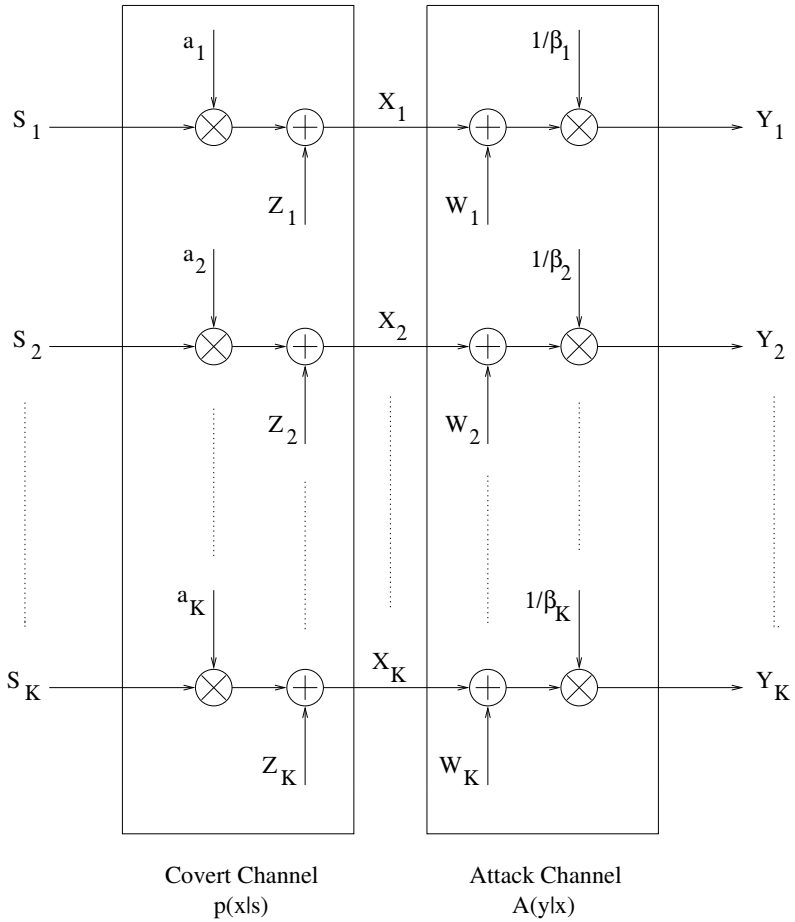
# 6. Parallel Gaussian Channels

Apply to wavelets, DCT signal models




- $K$ channel signals $S_k(n) \sim$ i.i.d. $\mathcal{N}\left(0, \sigma_k^2\right)$
- $N_k$ samples in channel $k$, $\sum_{k=1}^{K} N_k = N$, rates $r_k = N_k/N$
- Distortion measure : MSE

# Capacity-achieving distributions




$\{Z_i, W_i\}$ mutually independent; $\{d_{1i}, d_{2,i}\}$ = power allocations

- Power allocation problem

$$C = \max_{\{d_{1k}\}} \min_{\{d_{2k}\}} \sum_k r_k \qquad \underbrace{C_G(\sigma_k^2, d_{1k}, d_{2k})}_{\text{capacity of Gaussian channel } k}$$

where

$d_{1k}$ = distortion by info. hider in channel $k$

$d_{2k}$ = distortion by attacker in channel $k$

$r_k$ = rate of channel $k$

- Same capacity for blind & nonblind cases