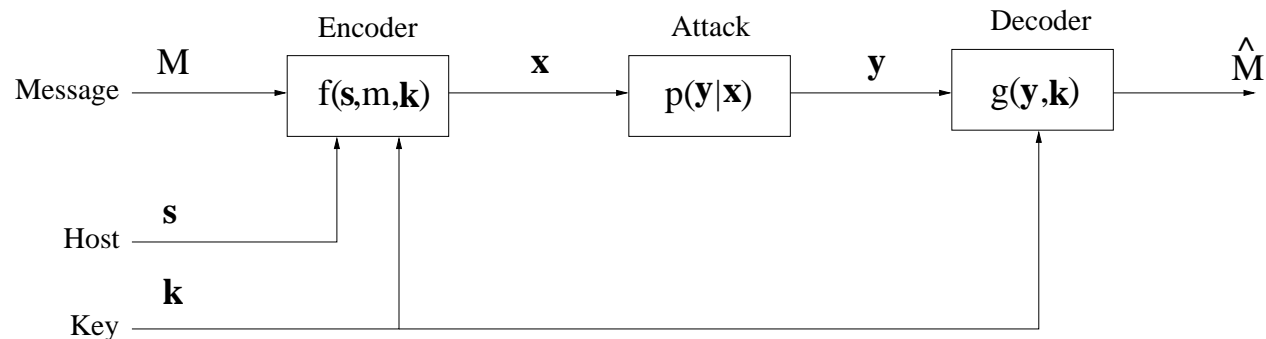


SESSION 5. PERFORMANCE ANALYSIS: CAPACITY

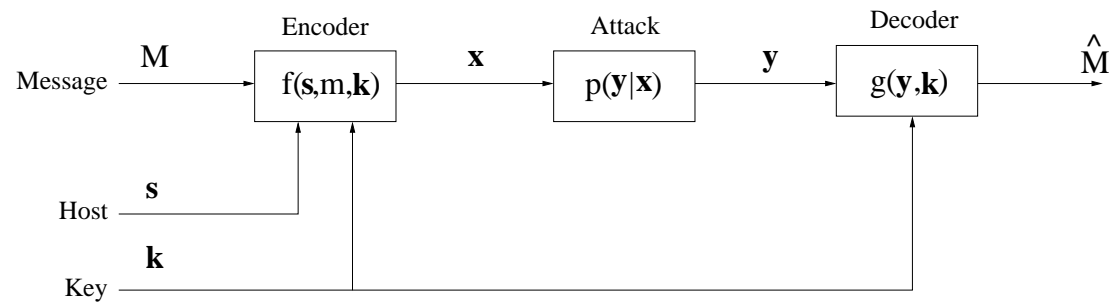
- Communication Model
- Data-Hiding Capacity
- Gaussian and Parallel-Gaussian Sources
- Capacity of Constrained Systems

1. Communication Model



- Probability of error $P_{e,N} = Pr[\hat{M} \neq M]$
- Message M uniform over $\{1, \dots, 2^{NR}\}$
- Probability mass function $p_{SK}(s, k)$ (i.i.d. symbols)
- Additive distortion function $d^N(\mathbf{S}, \mathbf{X}) = \frac{1}{N} \sum_{i=1}^N d(S_i, X_i)$
- Constraint on encoder: $d^N(\mathbf{S}, \mathbf{X}) \leq D_1$
- Constraint on attacker : $d^N(\mathbf{X}, \mathbf{Y}) \leq D_2$

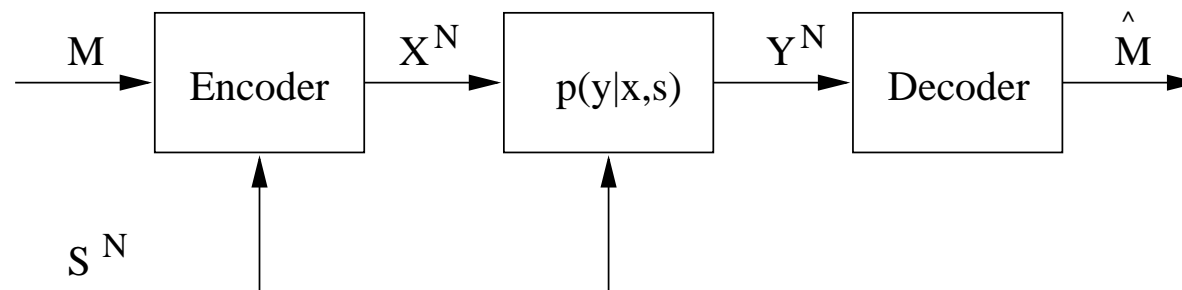
2. Data-Hiding Capacity



- **Goal:** make $P_{e,N} \rightarrow 0$ as $N \rightarrow \infty$
- Highest rate R such that this is possible is data-hiding capacity C
- Coding problem with side information (Gel'fand-Pinsker type)

Gel'fand-Pinsker Communication Problem (1980)

- Discrete Memoryless Channel $p(y|x, s)$ with random state s
- S available to encoder but not to decoder

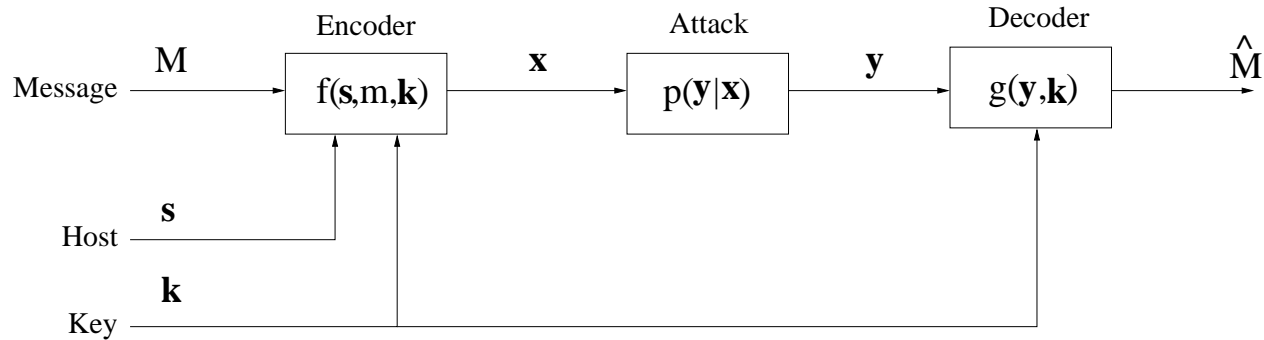


$$C = \max_{Q(x,u|s)} [I(U; Y) - I(U; S)]$$

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

- Capacity can be achieved by random binning

Data-Hiding Capacity

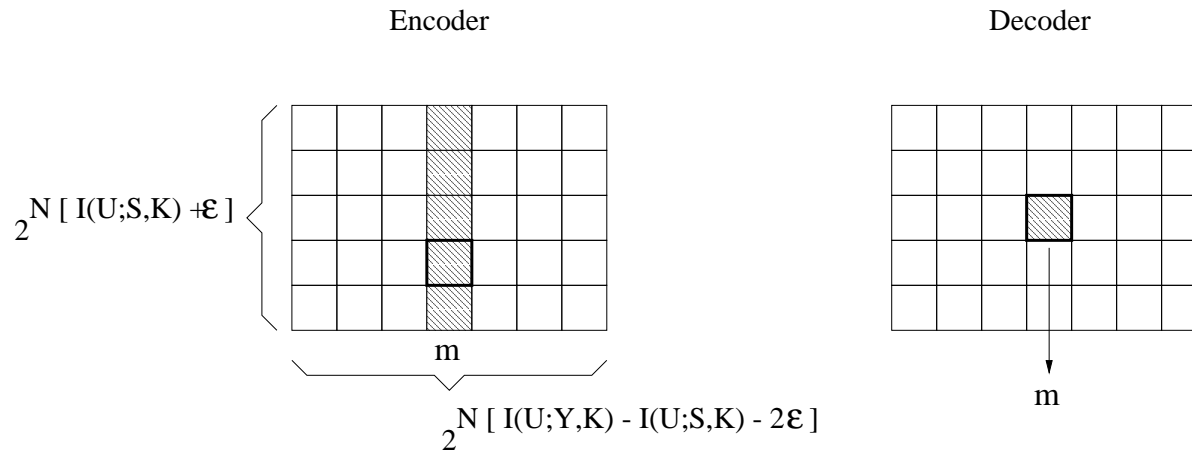


- Assume momentarily that $p(\mathbf{y}|\mathbf{x})$ is an unknown DMC satisfying expected distortion constraint $\mathbb{E} [d^N(\mathbf{X}, \mathbf{Y})] \leq D_2$
- Capacity is given by

$$C = \sup_U \max_{p_{XU|SK} \in \mathcal{P}_{XU|SK}(D_1)} \min_{p_{Y|X} \in \mathcal{P}_{Y|X}(D_2)} [I(U; YK) - I(U; SK)]$$

and is achievable by random binning

Random Binning Technique

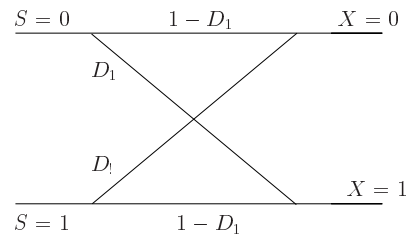


- Select large alphabet \mathcal{U}
- Construct array of codewords sampled from distribution $p(\mathbf{u})$
- Given $(\mathbf{s}, m, \mathbf{k})$, encoder selects codeword \mathbf{u} that is *jointly typical* with (\mathbf{s}, \mathbf{k}) ; then selects $x_i = f(s_i, u_i, k_i) \quad \forall i.$
- Decoder selects codeword that is jointly typical with (\mathbf{y}, \mathbf{k}) — typical w.r.t. the worst attack channel $p_{Y|X}$

Example: Bernoulli-Hamming

- $S \sim \text{Bernoulli}(\frac{1}{2})$, Hamming distortion measure, no attack ($D_2 = 0$)
- Capacity-achieving distribution: $U = X$,

$$p(X = 1|S = 0) = p(X = 0|S = 1) = D_1$$

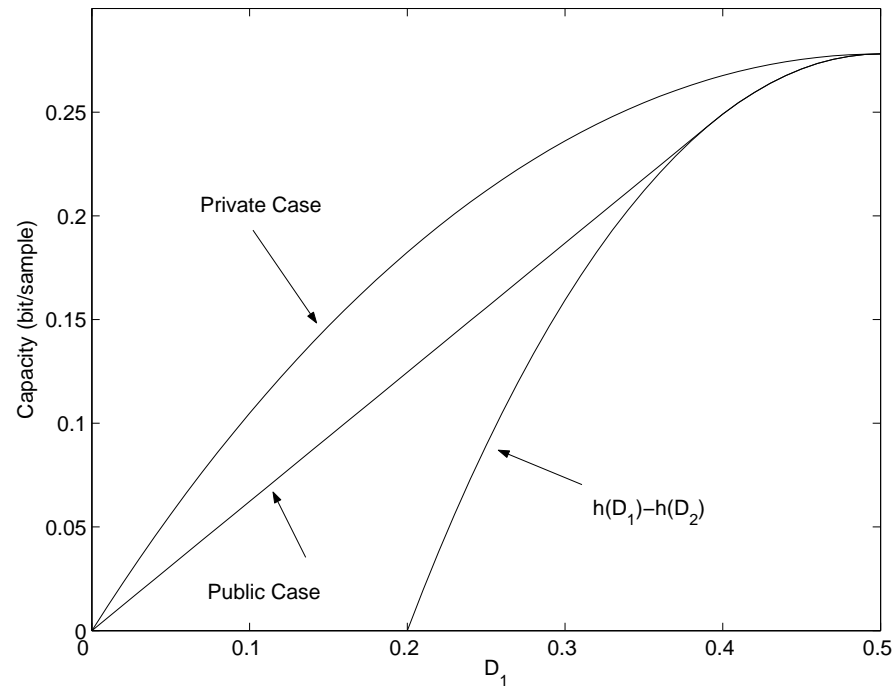


- Jointly typical sequences for $D_1 = \frac{1}{4}$:

$$\begin{aligned}
 S &= 1001110100101110 \\
 U = X &= 1000100100110110
 \end{aligned}$$

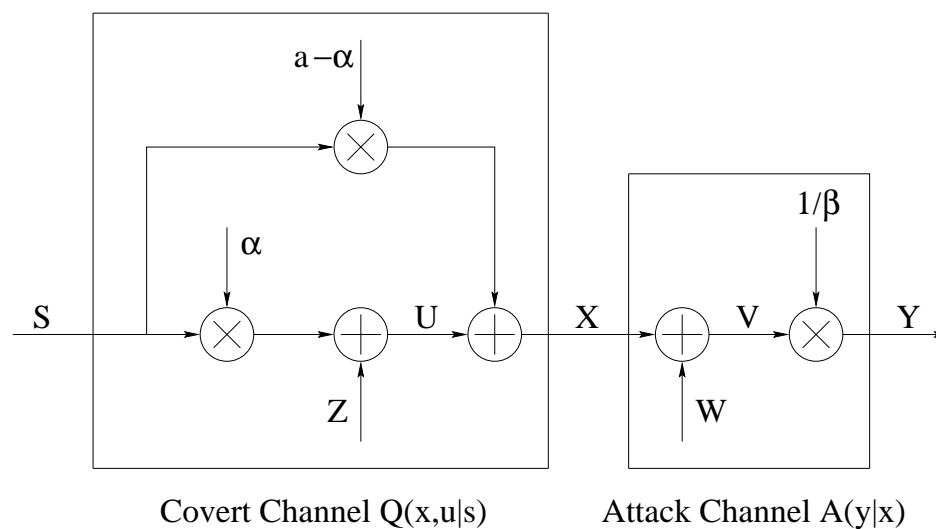
Capacity *vs.* D_1 when $D_2 = 0.2$

- Compare blind and nonblind cases; there is a cost for not knowing \mathbf{S} at receiver
- Time-sharing regime for $D_1 < D_{1,crit}$ in blind case



3. Gaussian Channels

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



where a, α, β are constants depending on D_1, D_2, σ_s^2 .

Strong Host: $\sigma_s^2 \gg D_1, D_2$

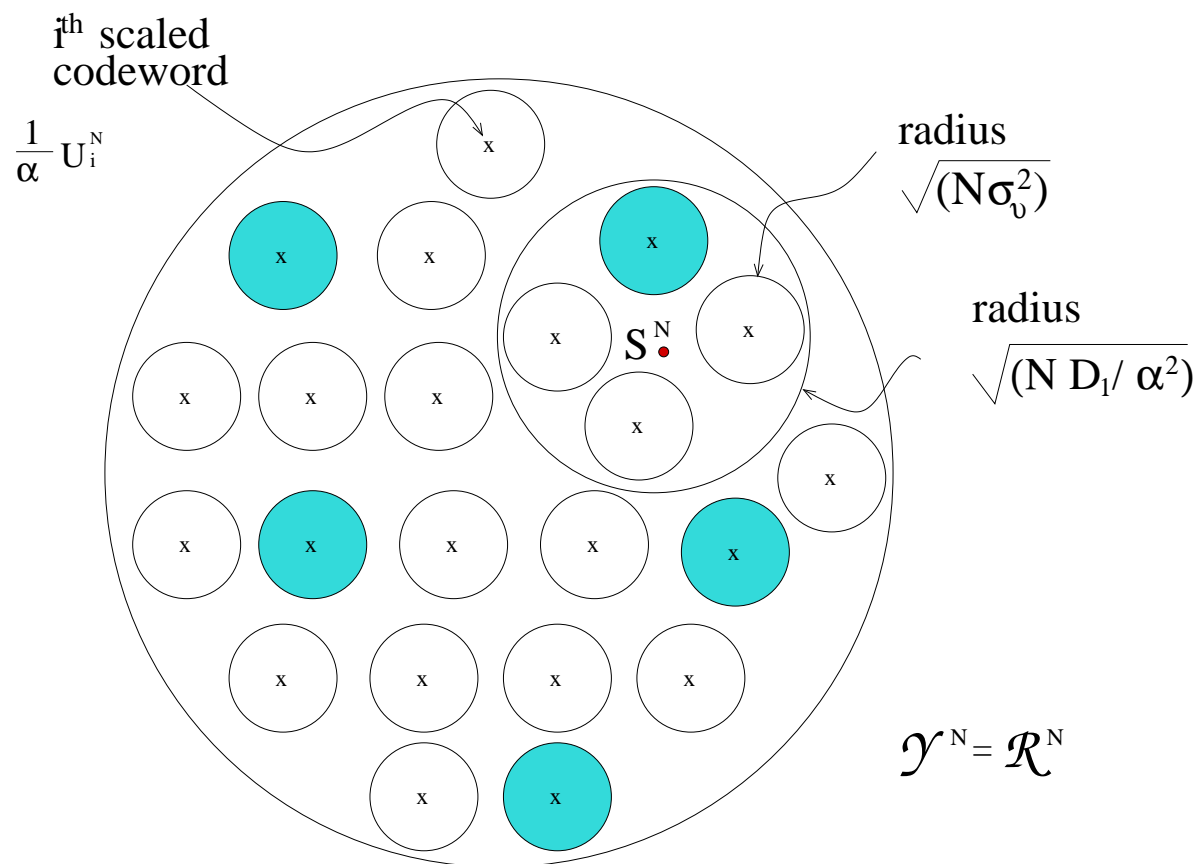
- Simpler solutions in this case : $a \sim 1, \beta \sim 1,$

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

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

- Same C as in private watermarking!
- Relates to Costa's 1983 result on capacity of Gaussian channel with Gaussian interference known to encoder
- Optimal covert channel: $U = Z + \alpha S$, where $\alpha \sim \frac{WNR}{1+WNR}$
- Same asymptotic capacity result holds if S is non-Gaussian

Sphere Packing View

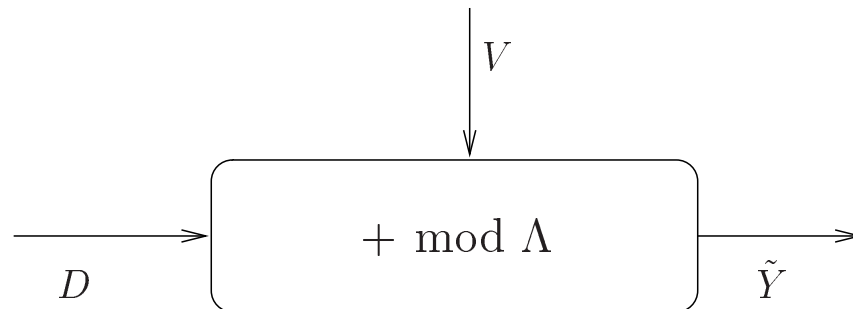


Attack Channels with Arbitrary Memory

- Almost-sure distortion constraint $d^N(\mathbf{X}, \mathbf{Y}) \leq D_2$
- See Cohen and Lapidot (2002) in Euclidean case and Somekh-Baruch and Merhav (2003) in finite-alphabet case
- Finite-alphabets: use conditionally-constant composition codes
- Randomize codes so that \mathbf{X} is uniformly distributed within type classes \Rightarrow attacker's memory is not an advantage
- Same capacity as in memoryless case
- Maximum Mutual Information type Decoder

4. Capacity of Constrained Systems

- First consider scalar QIM systems
- Transmission of codewords $\mathbf{d}_m, m \in \mathcal{M}$ over MAN channel:

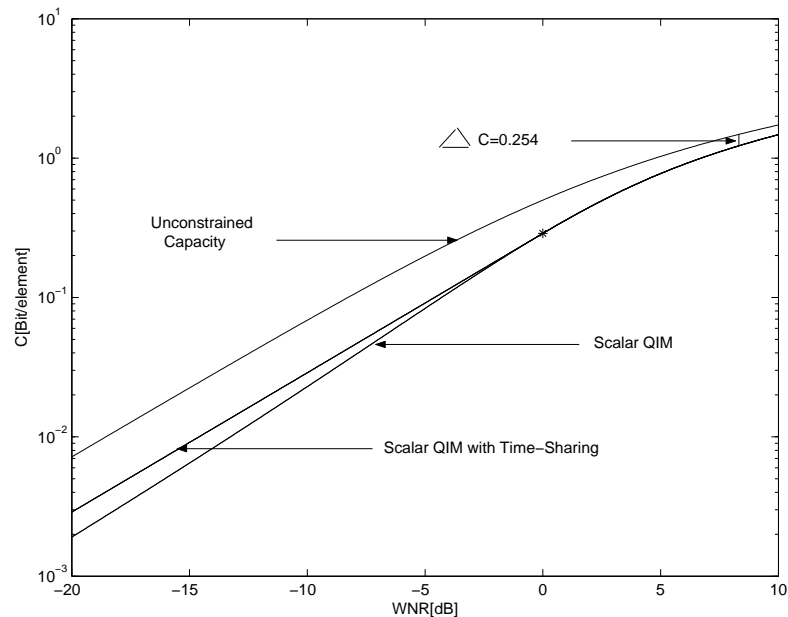


- Maximum rate of reliable transmission:

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

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

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



- Capacity gap ~ 2 dB 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 $\rightarrow 0$ 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 τ , 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 $WNR < WNR^*$.