Semantic Security using a Stronger Soft-Covering Lemma

Paul Cuff (Princeton University)

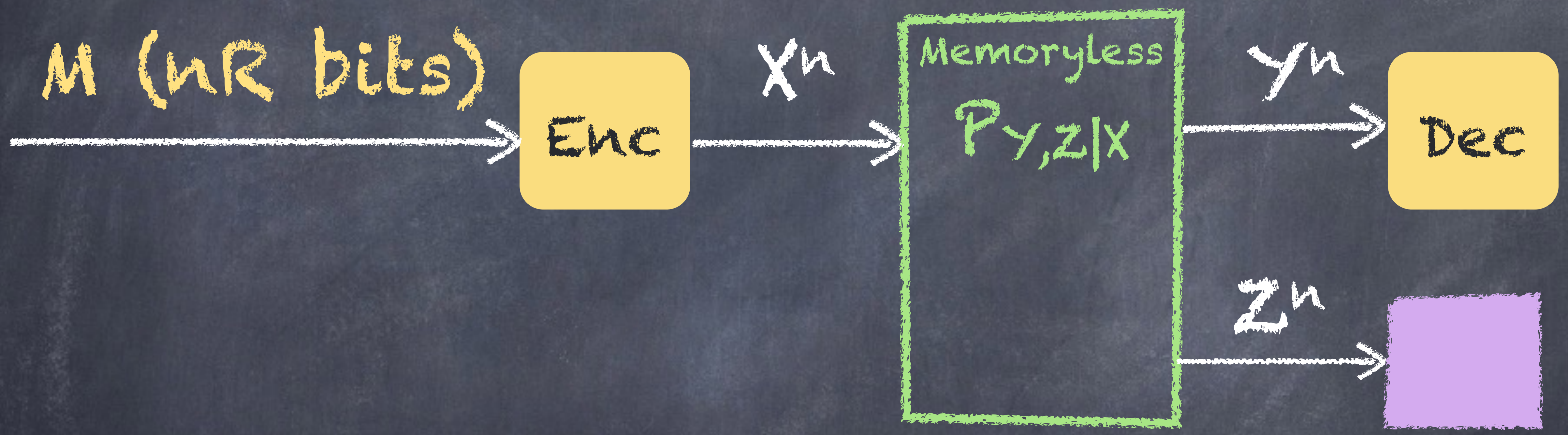
The Setting: 1975

- Wyner publishes five paper
- I will discuss two
  - Wiretap Channel
  - Common Information

Wiretap Channel

- Foundation of physical-layer security

Wiretap Channel



Secrecy Capacity:

- Reliable communication
- Z^n contains no information about M

Solutions

- Wyner gave solution for degraded channels
- Csiszár-Körner gave solution for all channels (1978)
    - Encoding requires pre-channel

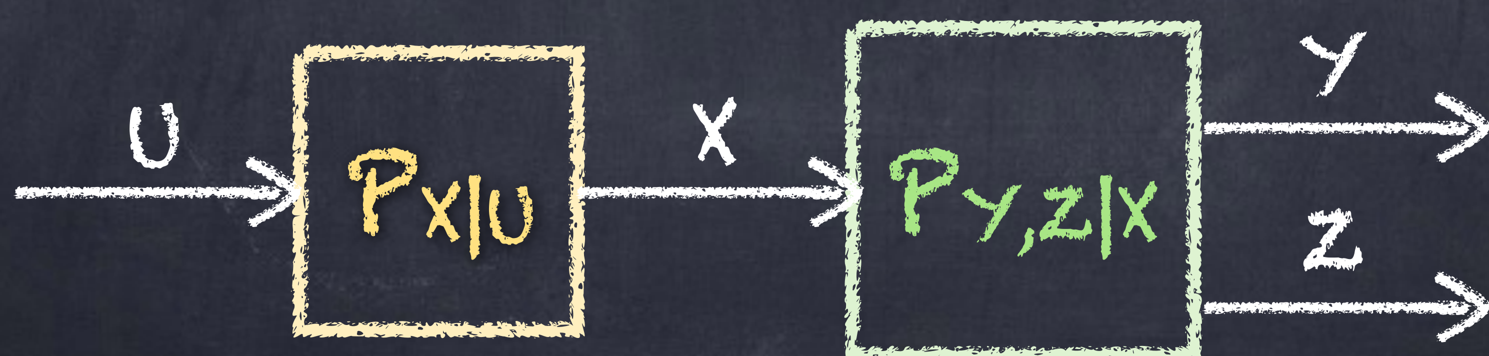
Solution

Degraded:

$$C_s = \max_{P_X} I(X;Y) - I(X;Z)$$

General:

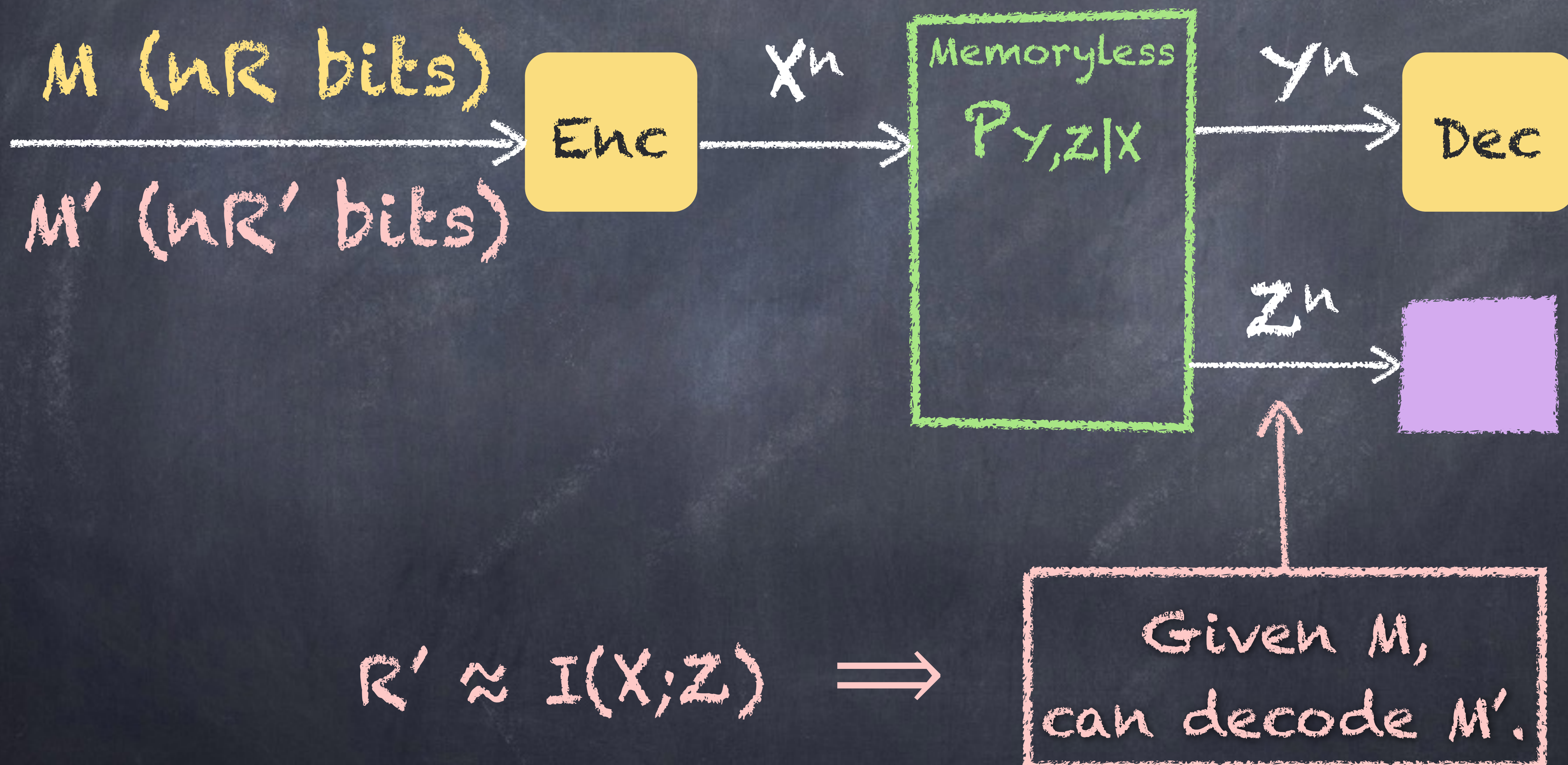
$$C_s = \max_{P_{XU}} I(U;Y) - I(U;Z)$$



Encoding

- Same construction as point-to-point
- Codebook generated according to P_X
- Send two messages, M and M'
  - M' is random garbage
  - The rate of M' is $I(X;Z)$

Encoding Diagram



Wyner's security argument

$$I(M,M';Z^n) = I(M;Z^n) + I(M';Z^n|M)$$

$I(X^n;Z^n) \approx nI(X;Z)$

$H(M') = nR'$

$\boxed{\text{Decodable if } R' < I(X;Z)}$

Secrecy Metric

- Secrecy capacity asks for perfect secrecy

Lossless compression $\longrightarrow$ near-lossless

as

Perfect secrecy $\longrightarrow$ near-perfect

Weak Secrecy

- Wyner's proof establishes "weak" perfect secrecy

$I(M;Z^n)$ can be made arbitrarily small compared to n

Strong Secrecy

- Recent proofs focus on "strong" perfect secrecy.

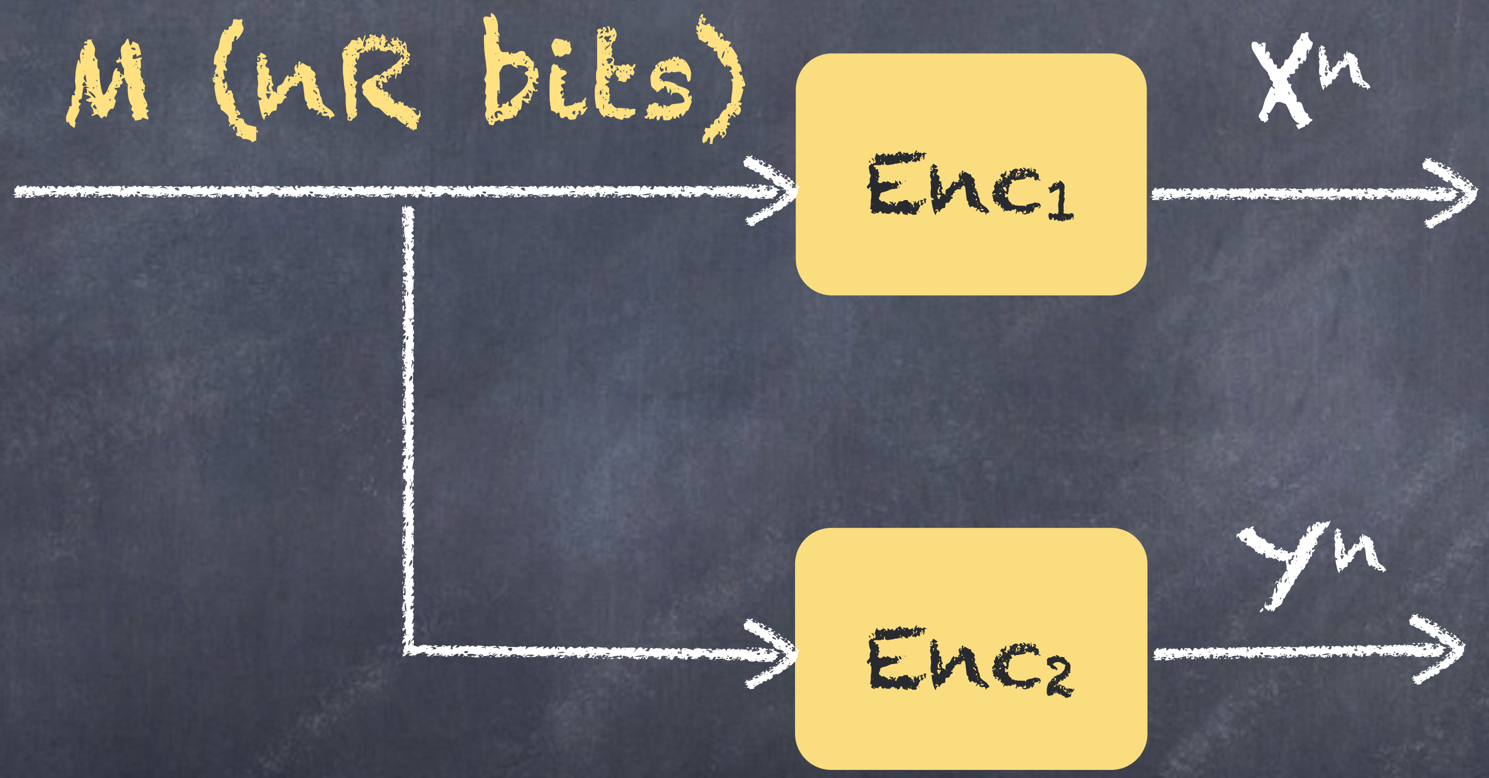
$I(M;Z^n)$ can be made arbitrarily small

Warning: Strong is not strong enough!

Modern Proof

- Use soft-covering principle from Wyner's other 1975 paper

Common Information



Produce i.i.d. pairs from desired $P_{X,Y}$

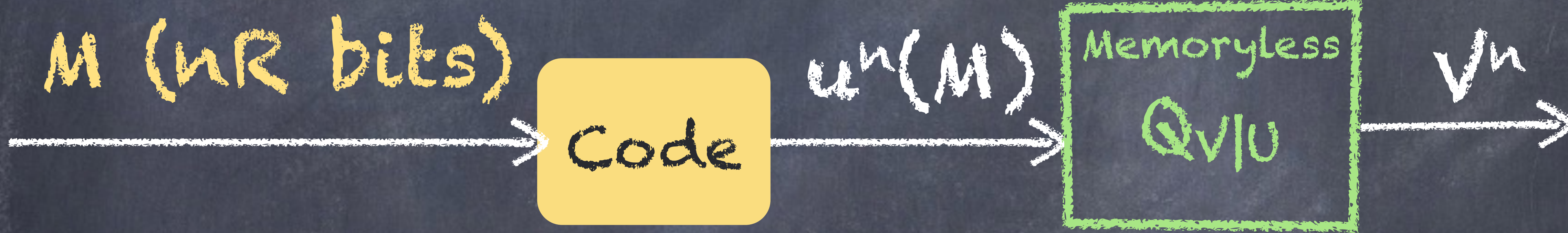
Common Information

- Minimum rate of common randomness needed:

$$C(X;Y) = \min_{X-U-Y} I(X,Y;U)$$

Soft Covering

- Theorem 6.3 of Wyner's C.I. paper:



Randomly select a codeword
Pass through a memoryless channel
Does induced output distribution match desired?

Output Distribution

Desired output distribution:

$$Q_V(v) = \sum_u Q_{V|U}(v|u) Q_U(u)$$

$$Q_{V^n} = \prod Q_V$$

$$Q_{U^n} = \prod Q_U$$

$$Q_{V^n|U^n} = \prod Q_{V|U}$$

Induced output distribution:

$$P_{V^n|\mathcal{C}} = 2^{-nR} \sum_{u^n(m) \in \mathcal{C}} Q_{V^n|U^n = u^n(m)}$$

Output Distribution

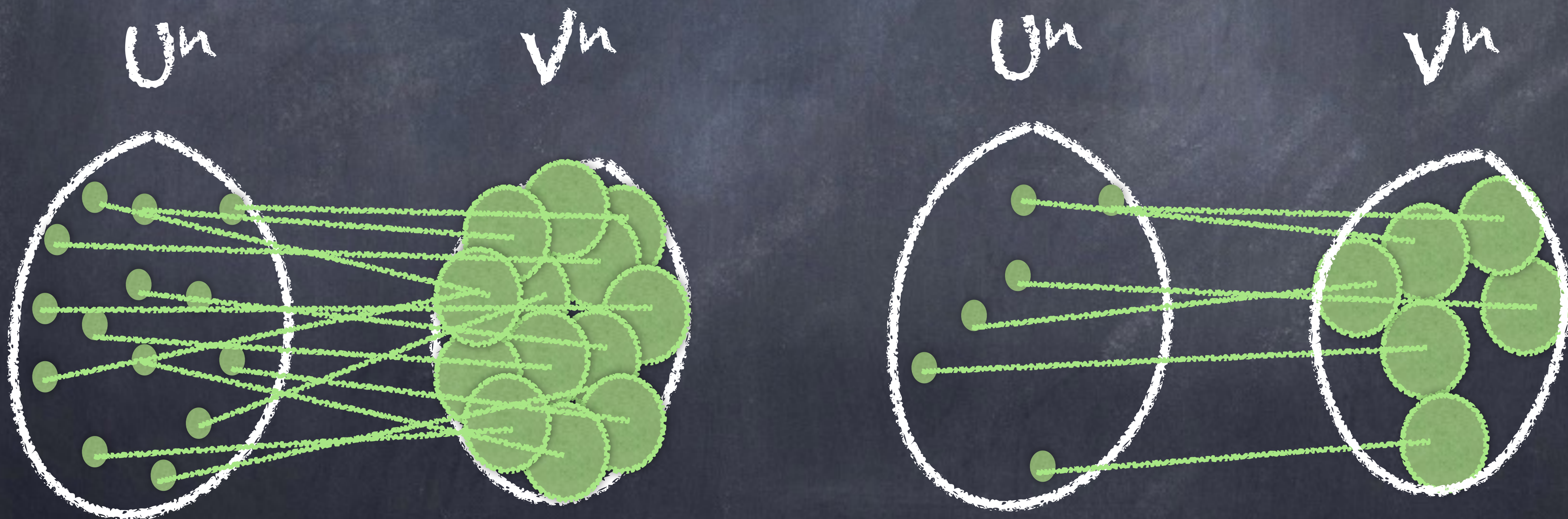
Soft Covering Lemma

- Codebook size: If $R > I(U;V)$
- Codebook generation: $U^n(m) \sim Q_U$ i.i.d.
- Success: $P_{V^n|C} \approx Q_{V^n}$

Covering and Packing

Covering (compression)

Packing (transmission)



Covering

Hard covering:

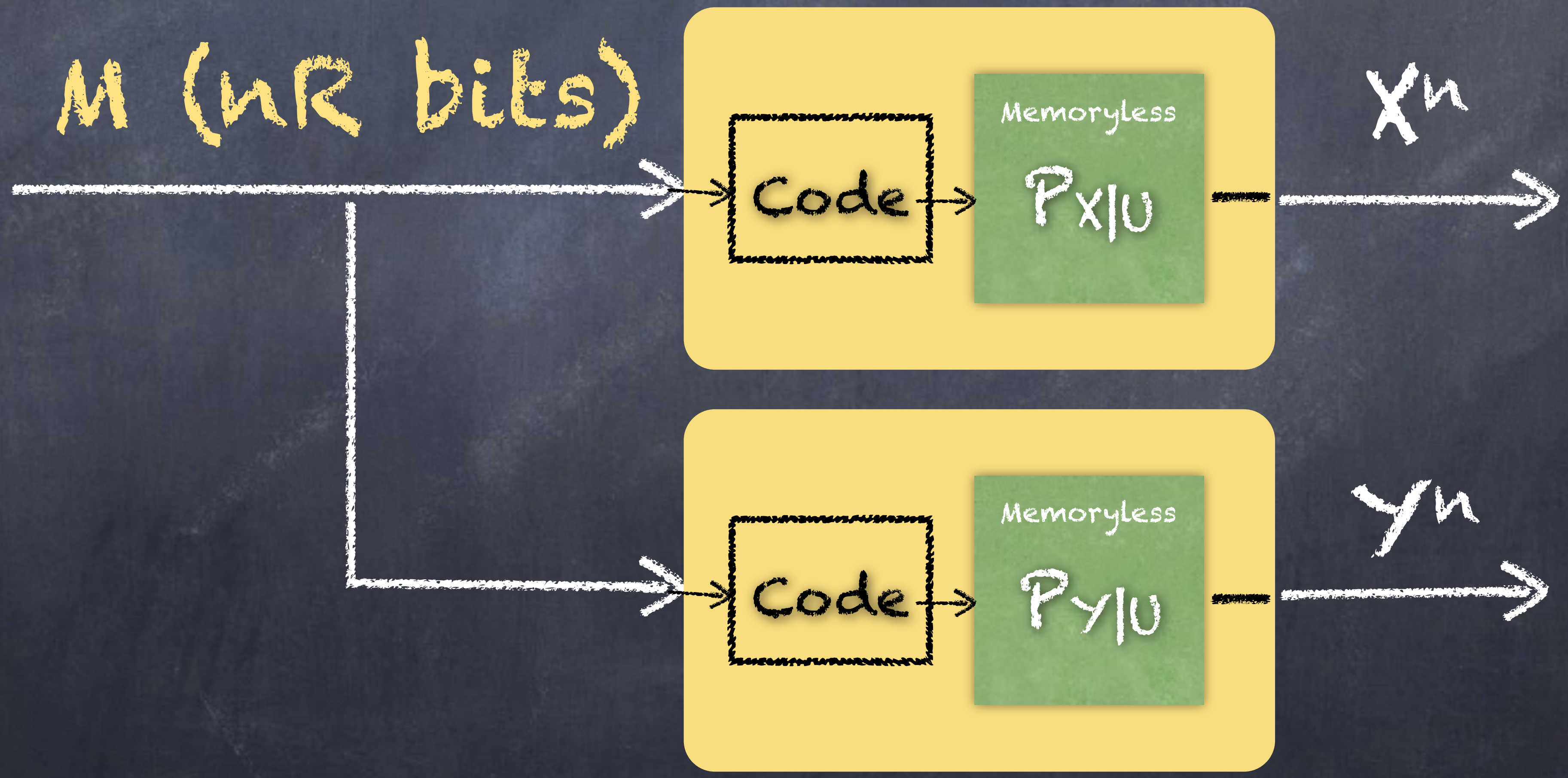
$$\bigcup_{u^n(m)} \mathcal{T}_\epsilon(u^n(m)) \approx \mathcal{V}^n \quad \text{in probability}$$

Soft covering:

$$\frac{1}{n} \sum_{u^n(m)} Q_{V^n|U^n=u^n(m)} \approx Q_{V^n}$$

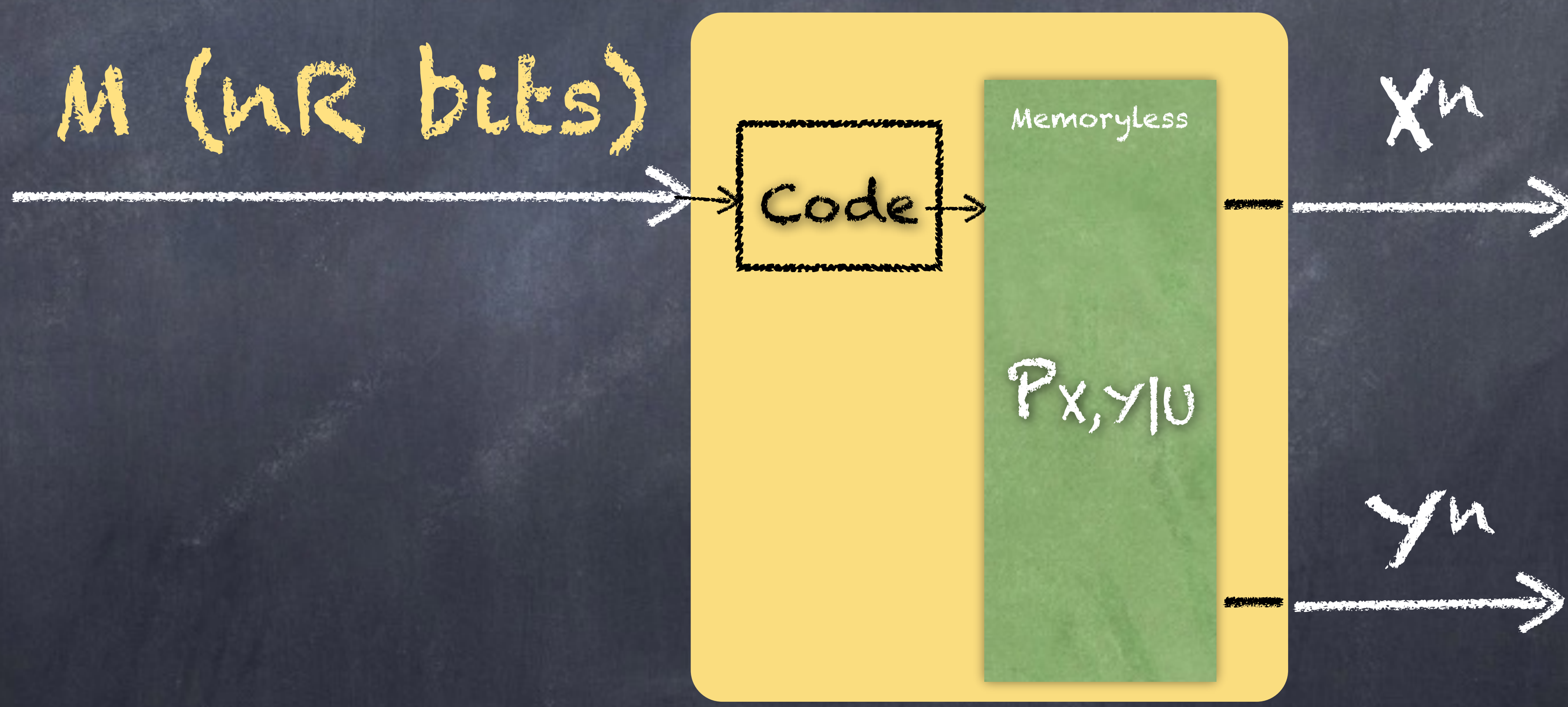
Wyner's Application

$$C(X;Y) = \min_{X-U-Y} I(X,Y;U)$$



Wyner's Application

$$C(X;Y) = \min_{X-U-Y} I(X,Y;U)$$



Soft Covering Metrics

- Wyner: $$\mathbb{E}\,\frac{1}{n} D\left(P_{V^n|\mathcal{C}} \| Q_{V^n}\right) \to 0$$
- Han-Verdú "resolvability" (1993):

$$\mathbb{E}\left\|P_{V^n|\mathcal{C}} - Q_{V^n}\right\|_{TV} \to 0$$

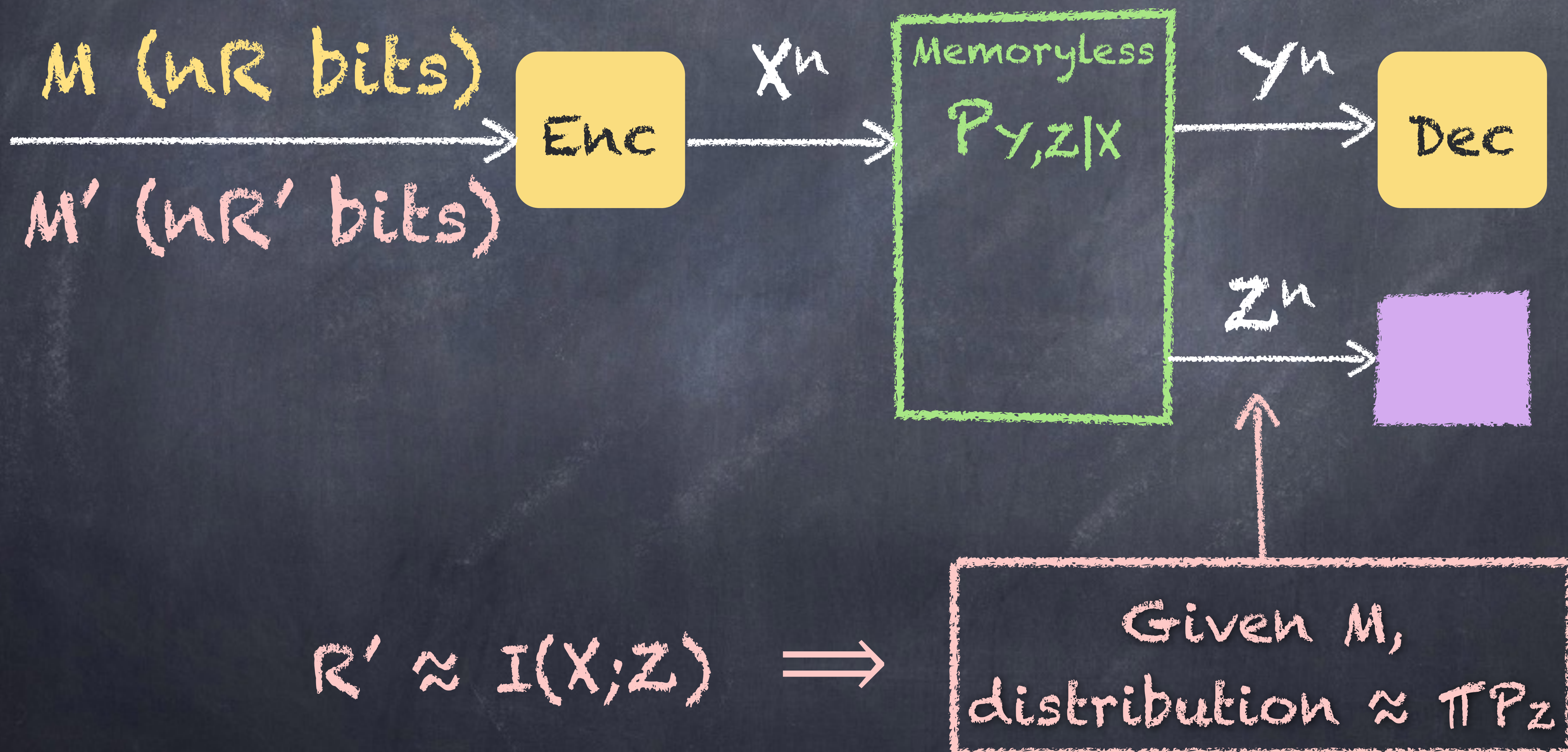
- Many other proofs and uses:

$$\mathbb{E}\,D\left(P_{V^n|\mathcal{C}} \| Q_{V^n}\right) \to 0$$

Back to Wiretap Channel

- Same encoding construction as previously
- Use soft covering to show secrecy

Encoding Concept



Stronger Soft Covering Lemma

Claim

$$\mathbb{P}\left(D(P_{V^n|\mathcal{C}} \| Q_{V^n}) > e^{-\gamma_1 n}\right) < e^{-e^{\gamma_2 n}}$$

Conditions:

- R > I(U;V)
- For some γ_1 and γ_2 and n large enough
- V has finite support

Existence argument

- Performance error metrics:
  - $e_{1,n}$, $e_{2,n}$, … must all go to zero
- Expected value over codebooks:
  - $E\,[e_{1,n}+e_{1,n}\ \ldots] = E[e_{1,n}] + E[e_{1,n}]\ \ldots \leq \varepsilon$
- Probability of a good codebook:
  - $P(e_{1,n}>\varepsilon \text{ OR } e_{1,n}>\varepsilon\ \ldots) \leq P(e_{1,n}>\varepsilon) + P(e_{1,n}>\varepsilon)\ \ldots$

Proof Definitions

$$\Delta_{\mathcal{C}}(v^n) \triangleq \frac{dP_{V^n|\mathcal{C}}}{dQ_{V^n}}(v^n).$$

$$D\left(P_{V^n|\mathcal{C}} \| Q_{V^n}\right) = \int dP_{V^n|\mathcal{C}} \log \Delta_{\mathcal{C}}.$$

Typical Set

"Weak" typical set $$\mathcal{A}_\epsilon \triangleq \left\{ (u^n, v^n) : \frac{1}{n} \log \frac{dQ_{V^n|U^n=u^n}}{dQ_{V^n}}(v^n) \leq I_Q(U;V) + \epsilon \right\}.$$

Split induced distribution

$$P_{\mathcal{C},1} \triangleq 2^{-nR} \sum_{u^n(m) \in \mathcal{C}} Q_{V^n|U^n=u^n(m)} \mathbf{1}_{(V^n, u^n(m)) \in \mathcal{A}_\epsilon}$$

$$P_{\mathcal{C},2} \triangleq 2^{-nR} \sum_{u^n(m) \in \mathcal{C}} Q_{V^n|U^n=u^n(m)} \mathbf{1}_{(V^n, u^n(m)) \notin \mathcal{A}_\epsilon}$$

Split $\Delta_\mathcal{C}$

$$\Delta_\mathcal{C} = \Delta_{\mathcal{C},1} + \Delta_{\mathcal{C},2}$$

$$\Delta_{\mathcal{C},1}(v^n) \triangleq \frac{dP_{\mathcal{C},1}}{dQ_{V^n}}(v^n)$$

$$\Delta_{\mathcal{C},2}(v^n) \triangleq \frac{dP_{\mathcal{C},2}}{dQ_{V^n}}(v^n)$$

Output Distribution

A Decomposition

$$D\left(P_{V^n|\mathcal{C}} \| Q_{V^n}\right) \leq h\left(\int dP_{\mathcal{C},1}\right) \ldots$$

$$+\int dP_{\mathcal{C},1} \log \Delta_{\mathcal{C},1} + \int dP_{\mathcal{C},2} \log \Delta_{\mathcal{C},2}$$

very close to 1

small

Bound $P_{\mathcal{C},2}$

$$\int dP_{\mathcal{C},2} = 2^{-nR} \sum_{u^n(m)\in\mathcal{C}} \mathbb{P}_Q\left(\overline{\mathcal{A}_\epsilon} \mid U^n = u^n(m,\mathcal{C})\right)$$

Chernoff Bound:

- Expected value exponentially small
- i.i.d. average
- Each term bounded by 1
- Exponential number of terms

Bound $\Delta_{C,1}$

$$\Delta_{\mathcal{C},1}(v^n) = 2^{-nR} \sum_{u^n(m)\in\mathcal{C}} \frac{dQ_{V^n|U^n=u^n(m)}}{dQ_{V^n}}(v^n)\mathbf{1}_{(v^n,u^n(m))\in\mathcal{A}_\epsilon}$$

Chernoff Bound:

- Expected value ≤ 1
- i.i.d. average
- Each term bounded by $2^{n(I(U;V)+\varepsilon)}$
- Exponential number of terms 2^{nR}

Semantic Security

- Goldwasser-Micali 1982
  - No test can distinguish between a random selection from any two messages ($P_{error} \approx 1/2$)
  - $\|P_{\cdot|M_i} - P_{\cdot|M_k}\|_{TV} \approx 0$ for all i,k

Strong is Too Weak

- Message is assumed to be uniformly distributed

$$I(M;Z^n) = 2^{-nR} \sum_{m} D\left(P_{Z^n|M=m} \| P_{Z^n}\right)$$

close on average

Example

- Encoding is in packets of 256 bits
- End user only needs to use 3/4 of the packet during each transmission
- By protocol, end user fills the end of the packet with 0's
- Can have no security and still strong perfect secrecy!

Uniform mutual information $\approx (3/4)^n$

Semantic Security as Mutual Information

- Bellare-Tessaro-Vardy 2012
- Equivalence:
  - Semantic security

$$\max_{P_M} I(M; Z^n) < \epsilon$$

Expurgation

- Semantic Security in Wiretap Channel
- Easy way:
  - Remove bad codewords
- Another easy way:
  - Use stronger soft-covering lemma

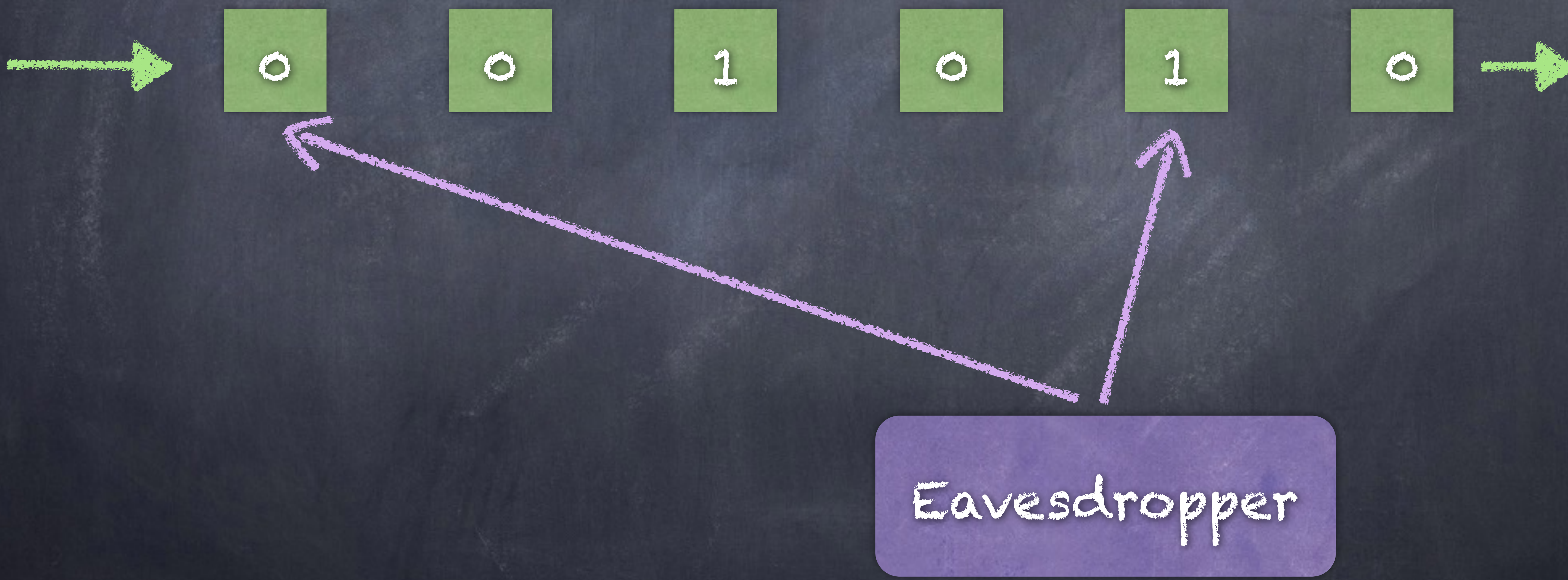
Demonstrate Strong Soft Covering on Wiretap Channels of Type II

Ziv Goldfeld and Haim Permuter

Type II Wiretap Channel

- Ozarow-Wyner 1984
- No noise
- Eavesdropper selects to αn packets to observe out of n transmitted

Type II Wiretap Channel



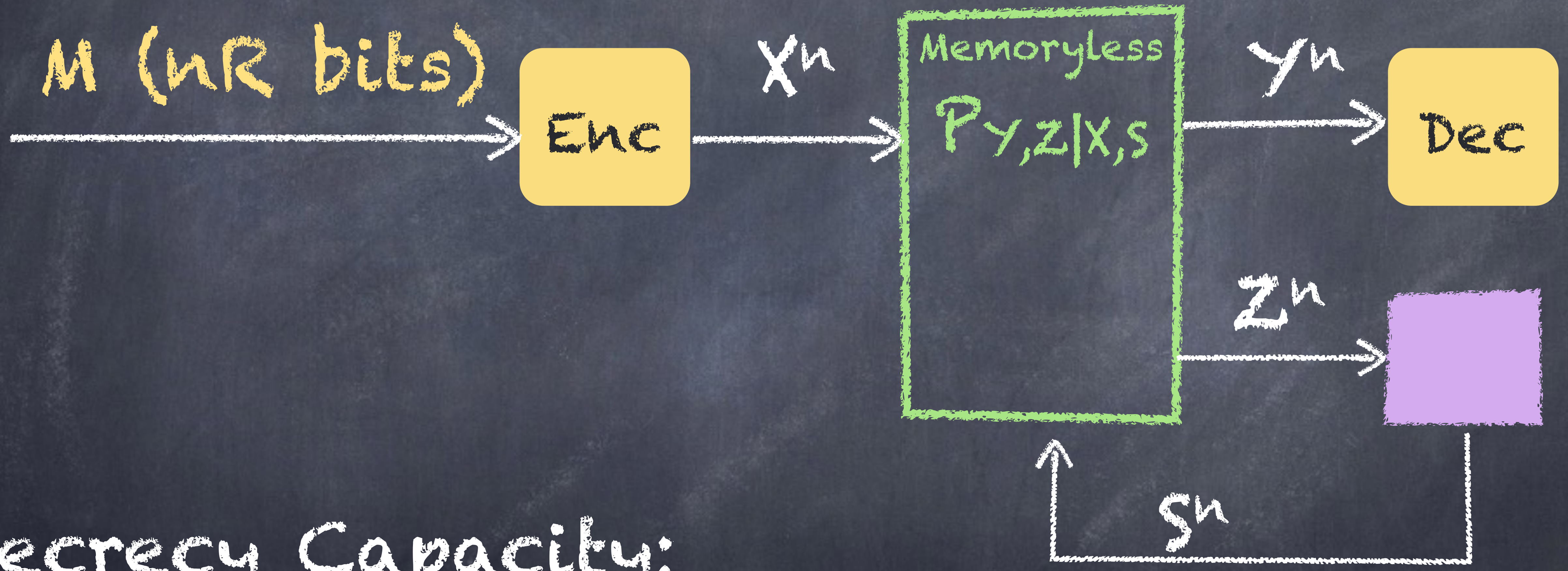
Solution

- Achieve secrecy capacity of wiretap channel
    - No noise
    - Erasure probability to the eavesdropper (1-α)
- Use coset codes

Noisy Main Channel

- Nafea-Yener 2015
  - Built on coset code construction
  - Not optimal in general
- Goldfeld-Cuff-Permuter 2015
  - Achieve wiretap channel secrecy capacity in general
  - Semantic security capacity is the same

Arbitrarily Varying Wiretap Channel



Secrecy Capacity:

- Reliable communication
- Z^n contains no information about M

Secrecy Proof

1. Analyze random codebook
2. Consider an arbitrary message and eavesdropper choice
   - Exponential number of these
3. Soft-covering lemma
4. Union bound $\square$

Channel Coding vs. Source Coding

Difference

- Channel coding
  - Packing - weak claims
- Source coding
  - Covering - strong claims
  - Strong soft covering
  - Exact hard covering (of typical set)
  - Doubly-exponential bounds

Secrecy Analysis Uses Covering