Semantic Security using a Stronger Soft-Covering Lemma

Paul Cuff (Princeton University),
Ziv Goldfeld, and Haim Permuter

Soft Covering

$R > I(U;V)$

Randomly select a codeword

Pass through a memoryless channel

Output is i.i.d.

Output Distribution

Desired output distribution:

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

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

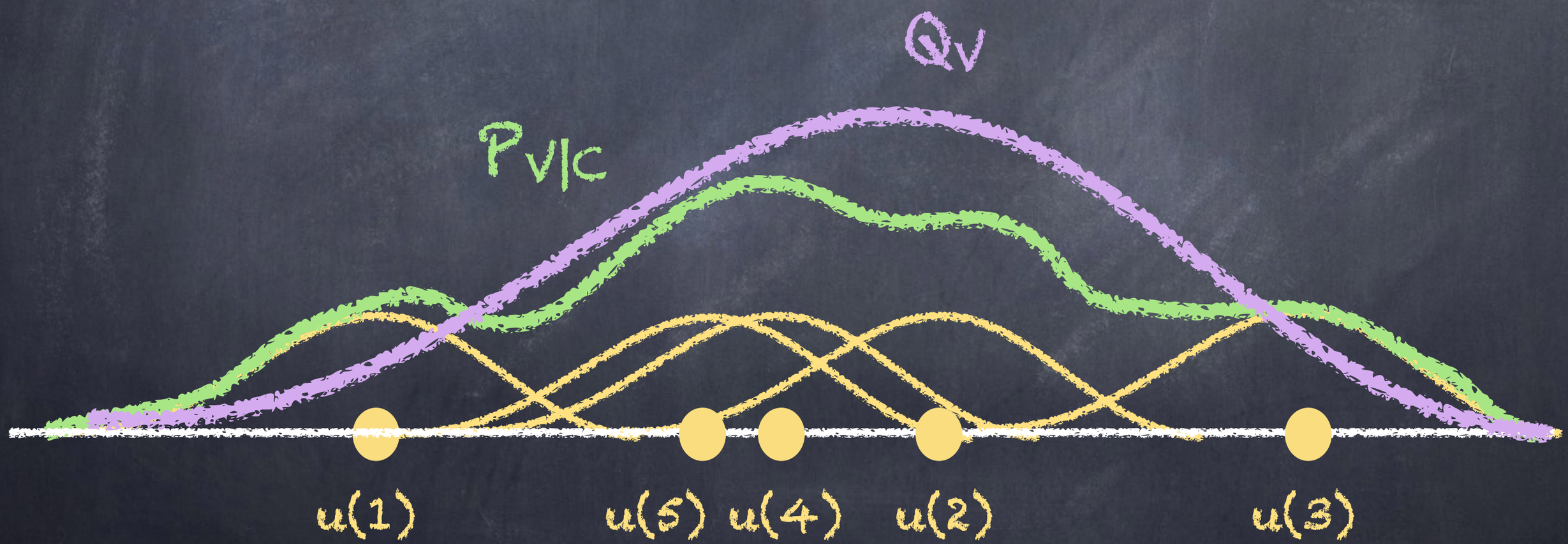
$$Q_{U^n} = \prod Q_U$$

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

Induced output distribution:

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

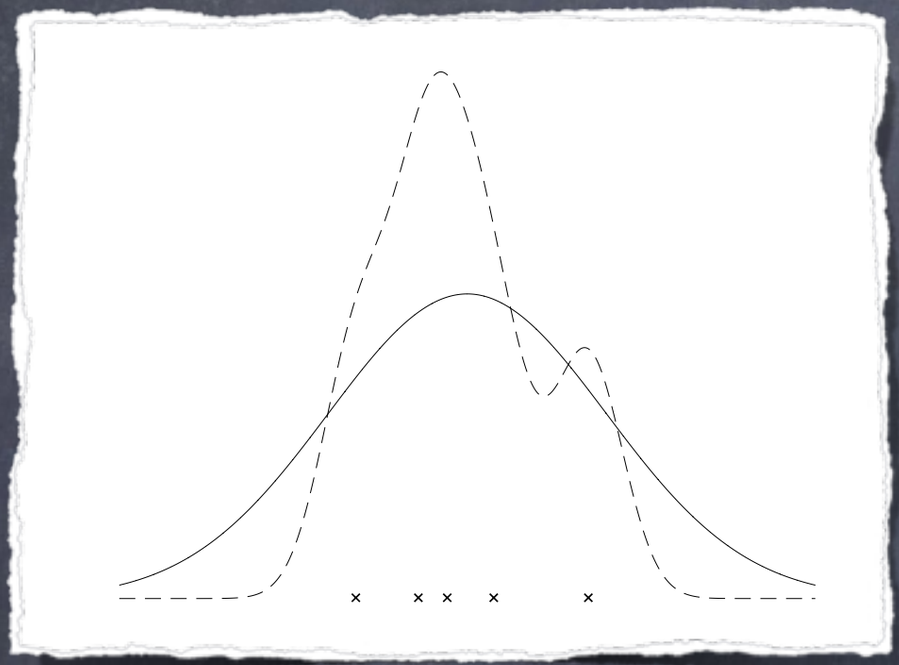
Output Distribution

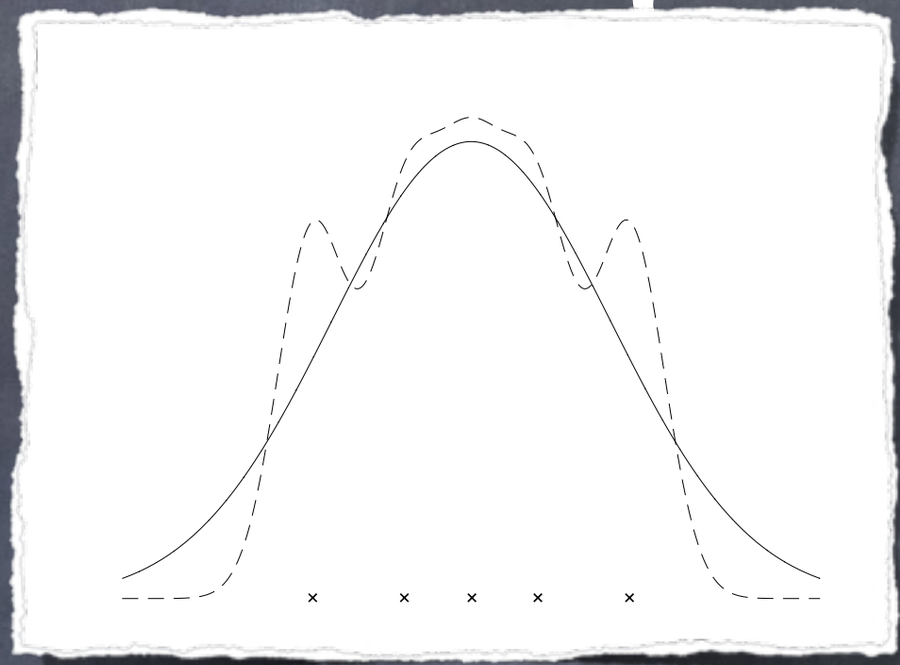


Soft Covering Lemma

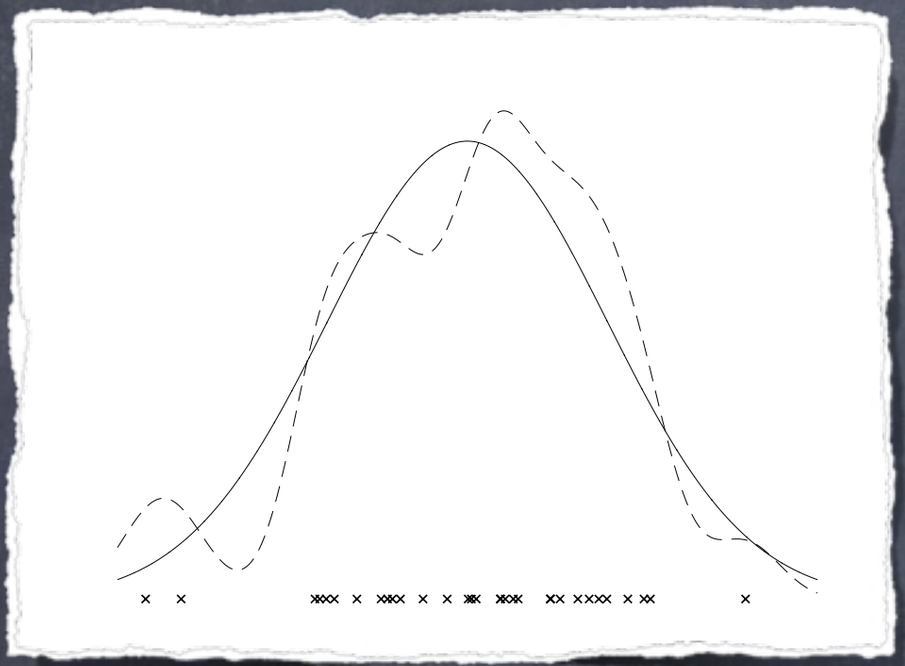
- Codebook size: $R > I(U;V)$
- Codebook generation: $U^n(m) \sim Q_U$ i.i.d.
- Success: $P_{V^n|\mathcal{C}} \approx Q_{V^n}$

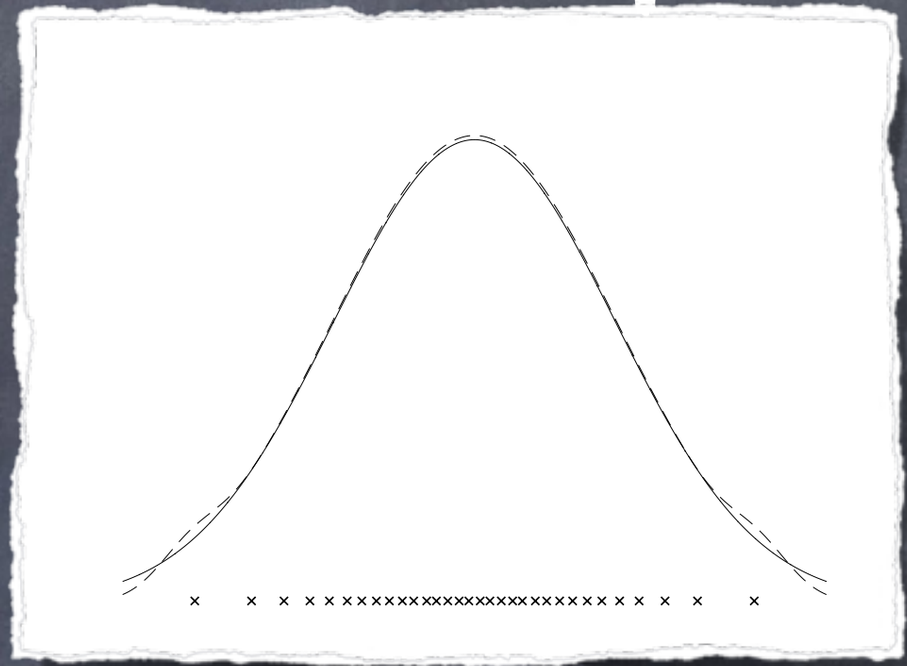
Gaussian Example

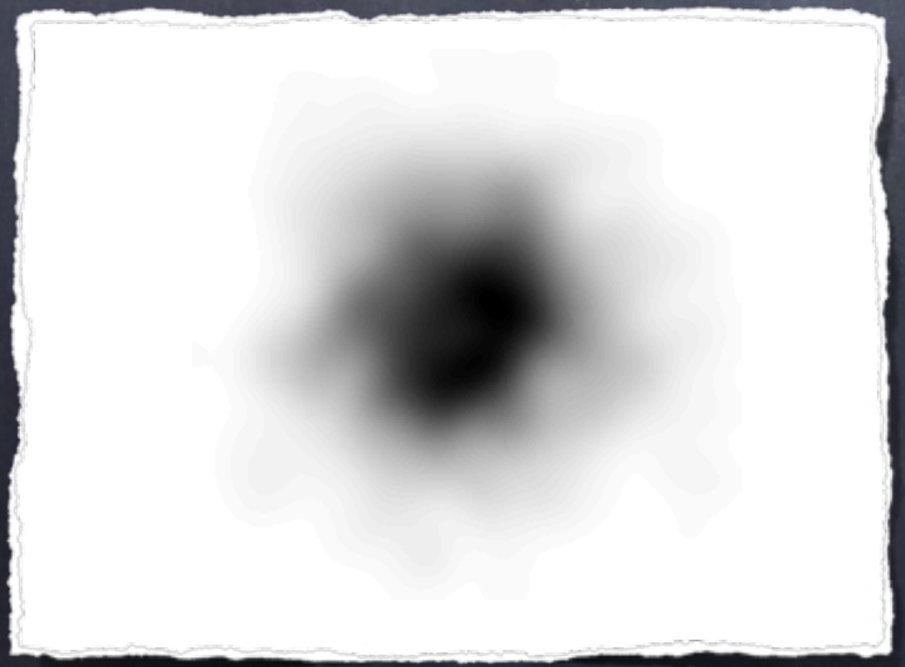




Gaussian Example

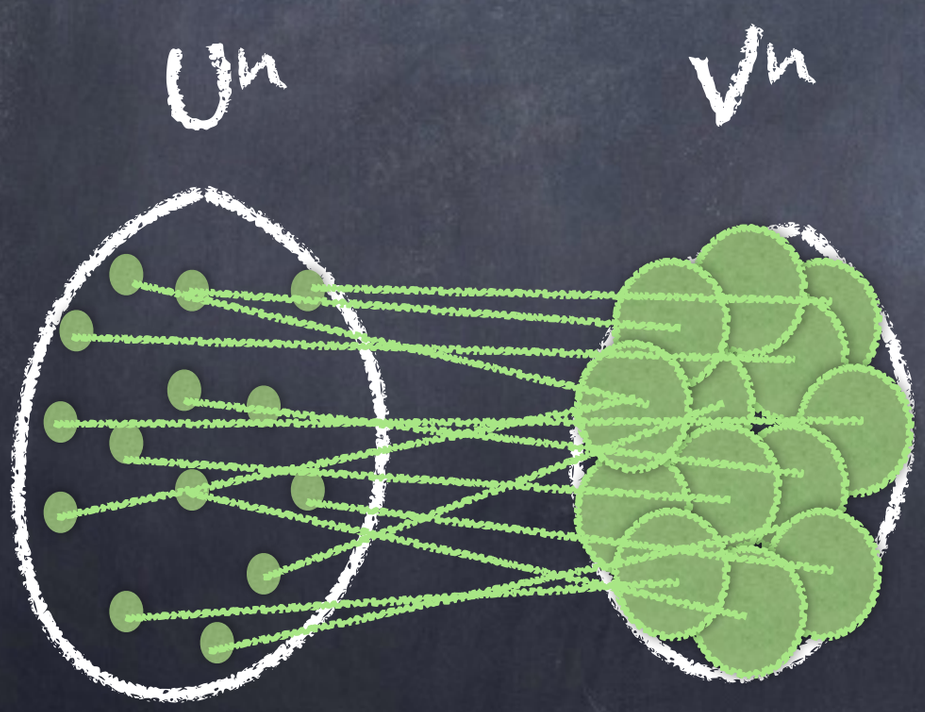




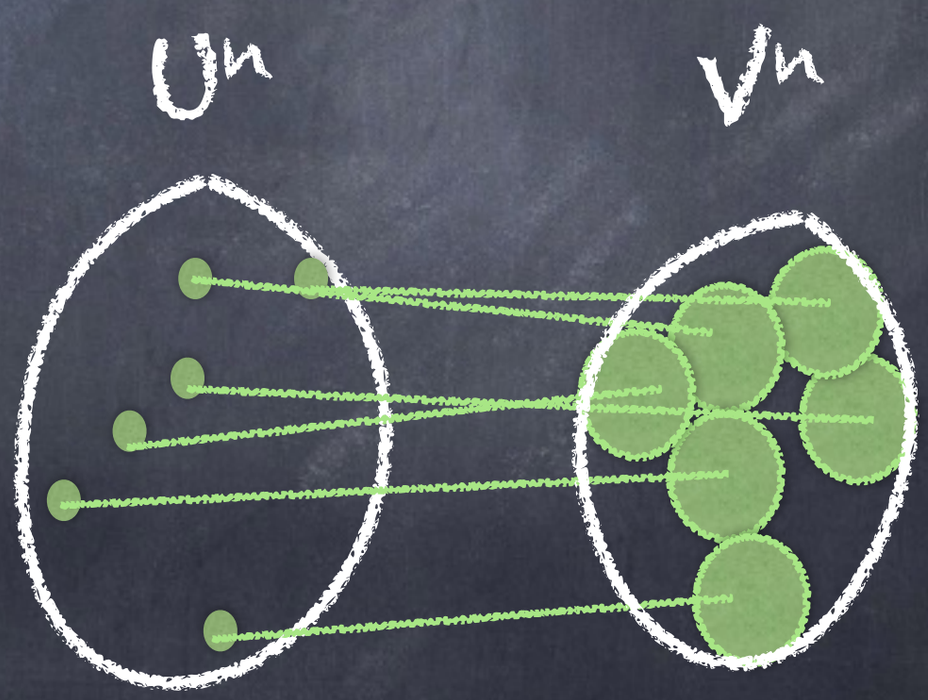


Covering and Packing

Covering (compression)



Packing (transmission)



Covering

Hard covering:

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

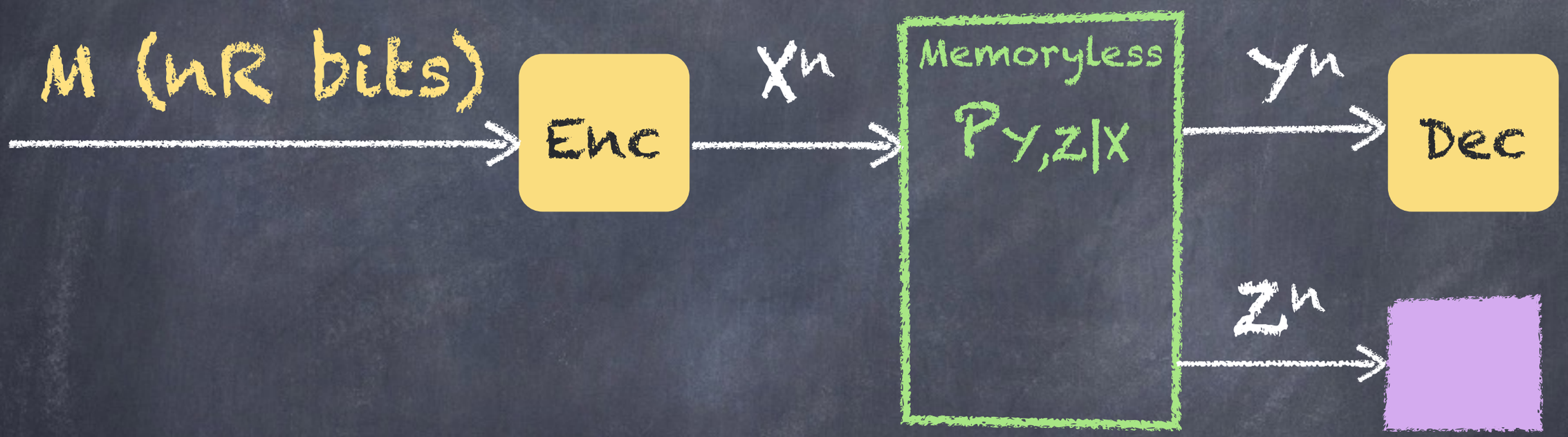
Soft covering:

$$\frac{1}{2^{nR}} \sum_{u^n(m)\in\mathcal{C}} Q_{V^n|U^n=u^n(m)} \approx Q_{V^n}$$

Aaron Wyner: 1975

- Common Information
  - Soft covering: Theorem 6.3
- Wiretap Channel

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

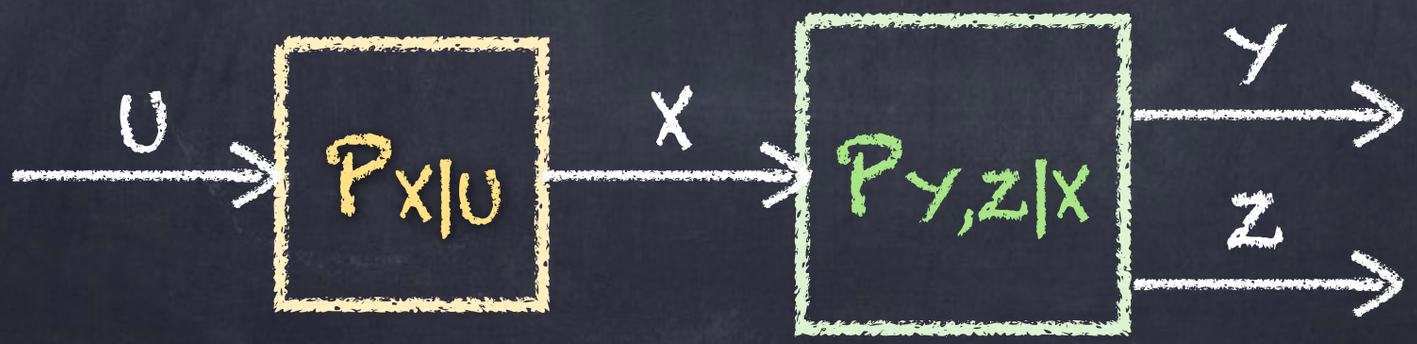
Solution

Degraded:

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

General:

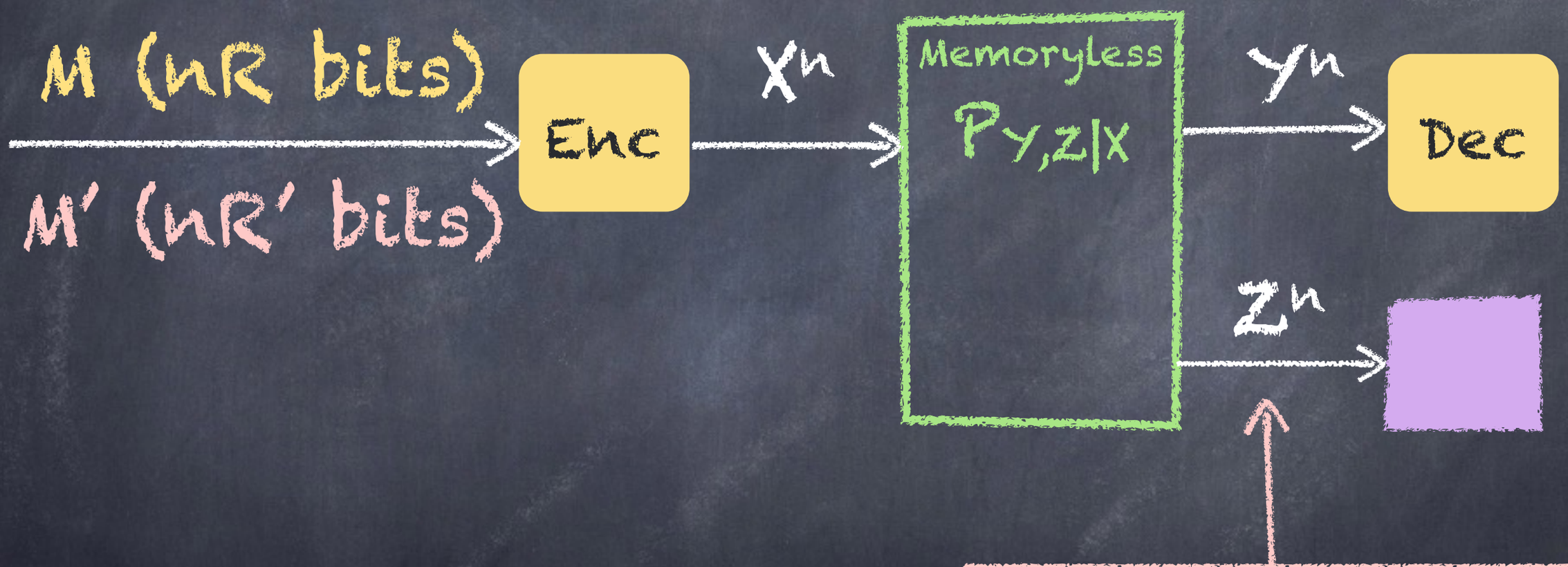
$$C_s = \max_{P_{XU}} I(U;Y) - I(U;Z)$$



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 Concept



$R' \approx I(X;Z) \implies$

Stronger Soft Covering Lemma

Claims

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

Conditions:

- R > I(U;V)
- V has finite cardinality

2. $$\mathbb{P}\left(\|P_{Y^n|\mathcal{C}} - Q_{Y^n}\|_{TV} > \varepsilon\right) < e^{-n^d}$$

Conditions:

- $$R_n = I(X;Y) + \frac{1}{\sqrt{n}}\mathcal{Q}^{-1}(\varepsilon)\sqrt{V} + c\frac{\log n}{n}$$
- V and U have finite cardinality

Proof Concept

Typical part close to 1 for all v^n

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

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

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:
  - $P(e_{1,n}>\varepsilon \text{ OR } e_{1,n}>\varepsilon \ldots) \leq P(e_{1,n}>\varepsilon) + P(e_{1,n}>\varepsilon) \ldots$

Semantic Security

- Goldwasser-Micali 1982
- Bellare-Tessaro-Vardy 2012

  - 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

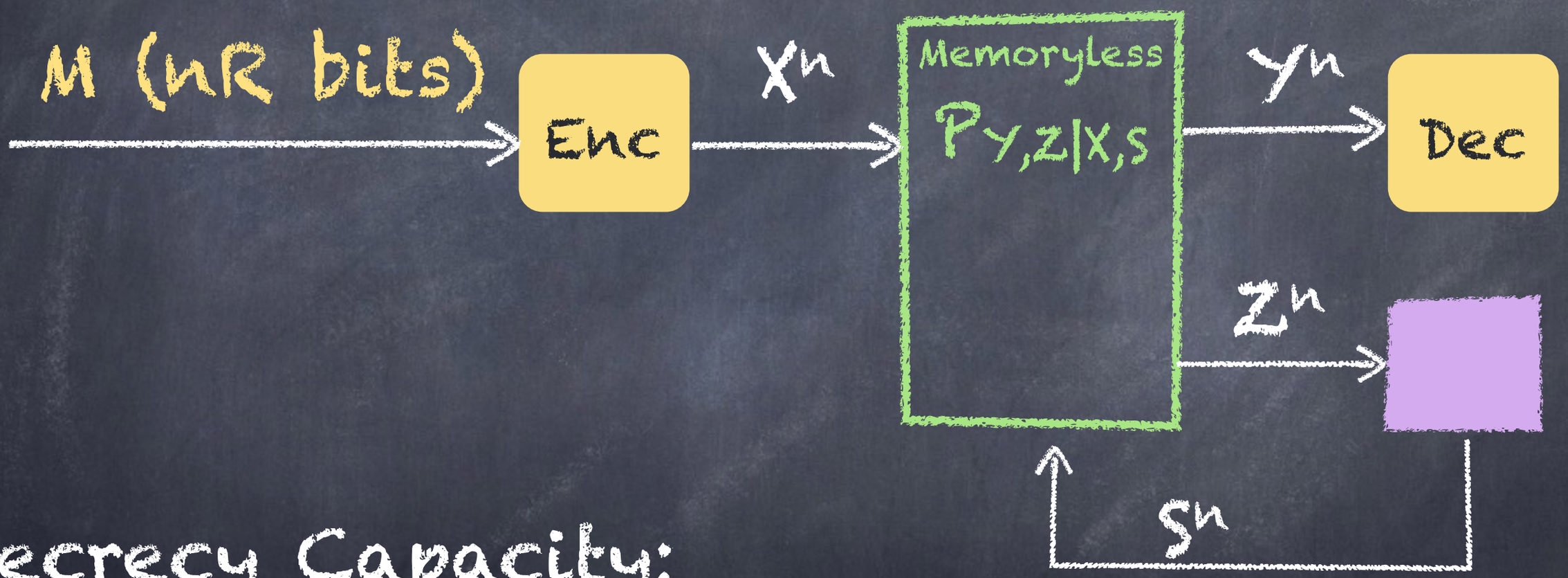
Strong is Too Weak

- 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

Arbitrarily Varying Wiretap Channel



Secrecy Capacity:

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

Result

- Goldfeld-Cuff-Permuter 2016
  - Solved under type constraint
  - Achieve wiretap channel secrecy capacity in general
  - Semantic security capacity is the same