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
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:

\[ C_s = \max_{P_{X,U}} I(U;Y) - I(U;Z) \]
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 $I(X;Z)$
Given $M$, can decode $M'$.

\[ R' \approx I(X;Z) \]
Wyner's security argument

\[ I(M,M';Z^n) = I(M;Z^n) + I(M';Z^n|M) \]

\[ I(X^n;Z^n) \approx nI(X;Z) \]

\[ H(M') = nR' \]

Decodable if \( R' < I(X;Z) \)
Secrecy Metric

Secrecy capacity asks for perfect secrecy

Lossless compression \rightarrow near-lossless

as

Perfect secrecy \rightarrow near-perfect
Weak Secrecy

- Wyner’s proof establishes “weak” perfect secrecy

\[ I(M;Z^n) \text{ can be made arbitrarily small compared to } n \]
Strong Secrecy

- Recent proofs focus on “strong” perfect secrecy.

\[ I(M;Z^n) \text{ can be made arbitrarily small} \]

**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:

\[ u^n(M) \]

\[ \mathcal{V} \]

\[ \mathcal{Q} \mid \mathcal{U} \]

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

Desired output distribution:

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

Induced output distribution:

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

\[
\begin{align*}
Q_{V^n} & = \prod Q_V \\
Q_{U^n} & = \prod Q_U \\
Q_{V^n|U^n} & = \prod Q_{V|U}
\end{align*}
\]
Output Distribution

\[ \begin{align*}
Q & \\
V & \\
P & \\
1 \quad u(1) & 2 \quad u(2) & 3 \quad u(3) & 4 \quad u(4) & 5 \quad u(5)
\end{align*} \]
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)

\[ U^n \quad V^n \]

Packing (transmission)

\[ U^n \quad V^n \]
Covering

Hard covering:

$$\bigcup_{u^n(m)} T_{c}(u^n(m)) \approx \mathcal{V}^n \quad \text{in probability}$$

Soft covering:

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

\[ C(X;Y) = \min_{X \rightarrow U \rightarrow Y} I(X,Y;U) \]

\[ M \text{ (nR bits)} \]

\[ X^n \]

\[ Y^n \]
Wyner's Application

\[ C(X;Y) = \min_{X-U-Y} I(X,Y;U) \]
Soft Covering Metrics

- Wyner:
  \[ \mathbb{E} \frac{1}{n} D (P_{V^n|C} \| Q_{V^n}) \to 0 \]

- Han-Verdú “resolvability” (1993):
  \[ \mathbb{E} \| P_{V^n|C} - Q_{V^n} \|_{TV} \to 0 \]

- Many other proofs and uses:
  \[ \mathbb{E} D (P_{V^n|C} \| Q_{V^n}) \to 0 \]
Back to Wiretap Channel

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

\[ \begin{align*}
M & \text{(nR bits)} \\
\rightarrow & \text{Enc} \\
\rightarrow M' & \text{ (nR' bits)} \\
\end{align*} \]

\[ X^n \]

\[ \text{Memoryless } \]

\[ P_{Y,Z|X} \]

\[ \rightarrow \]

\[ Y^n \]

\[ Z^n \]

\[ \rightarrow \]

\[ \text{Dec} \]

\[ R' \approx I(X;Z) \Rightarrow \]

\[ \text{Given } M, \text{ distribution } \approx \Pi P_z \]
Stronger Soft Covering Lemma
Claim

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

Conditions:

- $R > I(U;V)$
- For some $\gamma_1$ and $\gamma_2$ 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:
  - $E[e_{1,n} + e_{1,n} ...] = E[e_{1,n}] + E[e_{1,n}] ... \leq \varepsilon$

- Probability of a good codebook:
  - $P(e_{1,n} > \varepsilon \text{ OR } e_{1,n} > \varepsilon ... ) \leq P(e_{1,n} > \varepsilon) + P(e_{1,n} > \varepsilon) ...$
Proof Definitions

\[ \Delta_c(v^n) \triangleq \frac{dP_{V^n|c}}{dQ_{V^n}}(v^n). \]

\[ D(P_{V^n|c}||Q_{V^n}) = \int dP_{V^n|c} \log \Delta_c. \]
Typical Set

"Weak" typical set

$$A_\epsilon \triangleq \left\{ (u^n, v^n) : \frac{1}{n} \log \frac{dQ_{V^n|U^n=u^n}}{dQ_{V^n}}(v^n) \leq I_Q(U; V) + \epsilon \right\}.$$ 

Split induced distribution

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

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

Split $\Delta c$

$$\Delta c = \Delta c,1 + \Delta c,2$$

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

$$\Delta c,2(v^n) \triangleq \frac{dP_{C,2}}{dQ_{V^n}}(v^n)$$
Output Distribution

$P_{\text{V1c}}$ $Q_V$

$u(1)$ $u(2)$ $u(3)$ $u(4)$ $u(5)$
A Decomposition

\[ D(P_{V^n} | c \| Q_{V^n}) \leq h \left( \int dP_{c,1} \right) \ldots \]

\[ + \int dP_{c,1} \log \Delta c_{1} + \int dP_{c,2} \log \Delta c_{2} \]

very close to 1

small
Bound $P_{c,2}$

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

Chernoff Bound:
- Expected value exponentially small
- i.i.d. average
- Each term bounded by 1
- Exponential number of terms
Bound \( \Delta_{c,1} \)

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

Chernoff Bound:
- Expected value \( \leq 1 \)
- i.i.d. average
- Each term bounded by \( 2^{n(I(U;V) + \epsilon)} \)
- Exponential number of terms \( 2^{nR} \)
Semantic Security

- Goldwasser-Micali 1982

- No test can distinguish between a random selection from any two messages ($P_{\text{error}} \approx 1/2$)

- $\|P_{\text{mi}} - P_{\text{mk}}\|_{TV} \approx 0$ for all $i,k$
Strong is Too Weak

Message is assumed to be uniformly distributed

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

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

0 0 1 0 1 0

Eavesdropper
Solution

- Achieve secrecy capacity of wiretap channel
- No noise
- Erasure probability to the eavesdropper \((1-\alpha)\)
- 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

\[ M \text{ (nR bits)} \rightarrow \text{Enc} \rightarrow X^n \rightarrow \text{Memoryless} \rightarrow Y^n \rightarrow \text{Dec} \]

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
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