Arbitrarily Varying Wiretap Channels with Type Constrained States

Ziv Goldfeld, Paul Cuff and Haim Permuter

Ben-Gurion University and Princeton University

The 4th IEEE GlobeCom Workshop on Physical Layer Security

December 8th, 2016
Information Theoretic Security over Noisy Channels

Pros:
Motivation

Information Theoretic Security over Noisy Channels

Pros:
1. Security versus *computationally unlimited* eavesdropper.
Motivation

Information Theoretic Security over Noisy Channels

Pros:

1. Security versus *computationally unlimited* eavesdropper.
2. **No shared key** - Use intrinsic randomness of a noisy channel.
Motivation

Information Theoretic Security over Noisy Channels

Pros:

1. Security versus \textit{computationally unlimited} eavesdropper.
2. \textbf{No shared key} - Use intrinsic randomness of a noisy channel.

Cons:
Information Theoretic Security over Noisy Channels

Pros:
1. Security versus \textit{computationally unlimited} eavesdropper.
2. No shared key - Use intrinsic randomness of a noisy channel.

Cons:
1. Eve’s channel assumed to be \textit{fully known}. 

Z. Goldfeld, P. Cuff and H. Permuter
Ben-Gurion University and Princeton University
Motivation

Information Theoretic Security over Noisy Channels

Pros:

1. Security versus *computationally unlimited* eavesdropper.
2. No shared key - Use intrinsic randomness of a noisy channel.

Cons:

1. Eve’s channel assumed to be *fully known*.
2. Security metrics *insufficient for (some) applications*.
Information Theoretic Security over Noisy Channels

**Pros:**

1. Security versus *computationally unlimited* eavesdropper.
2. No shared key - Use intrinsic randomness of a noisy channel.

**Cons:**

1. Eve’s channel assumed to be *fully known*.
2. Security metrics *insufficient for (some) applications*.

**Our Goal:** Stronger metric and weaken “known channel” assumption.
Wiretap Channels - Security Metrics
Wiretap Channels and Security Metrics
Degraded [Wyner 1975], General [Csiszár-Körner 1978]

\[ U[1:2^{nR}] \sim M \rightarrow Alice \rightarrow X^n \rightarrow P_{Y,Z|X} \rightarrow Bob \rightarrow \hat{M} \]

\[ \rightarrow Eve \rightarrow Z^n \]

Z. Goldfeld, P. Cuff and H. Permuter
Ben-Gurion University and Princeton University
Arbitrarily Varying WTCs with Type Constrained States
Wiretap Channels and Security Metrics

Degraded [Wyner 1975], General [Csiszár-Körner 1978]

\[ U[1 : 2^{nR}] \sim M \]

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

\{C_n\}_{n \in \mathbb{N}} - a sequence of \((n, R)\)-codes
Wiretap Channels and Security Metrics
Degraded [Wyner 1975], General [Csiszár-Körner 1978]

\[ U[1 : 2^{nR}] \sim M \quad \text{Alice} \quad X^n \quad P_{Y,Z|X} \]

Bob \quad \hat{M}

Eve \quad \overline{M}

\[ Z^n \]

\( \{C_n\}_{n \in \mathbb{N}} \) - a sequence of \((n, R)\)-codes

- **Weak-Secrecy**: \( \frac{1}{n} I_{C_n}(M; Z^n) \xrightarrow{n \to \infty} 0 \).
Wiretap Channels and Security Metrics
Degraded [Wyner 1975], General [Csiszár-Körner 1978]

\[ U[1:2^{nR}] \sim M \]

\[ X^n \rightarrow P_{Y,Z|X} \]

\[ Y^n \rightarrow \text{Bob} \]

\[ Z^n \rightarrow \text{Eve} \]

\[ \hat{M} \]

\[ \{C_n\}_{n \in \mathbb{N}} \text{ - a sequence of }(n,R)\text{-codes} \]

- **Weak-Secrecy:** \[ \frac{1}{n} I_{C_n}(M;Z^n) \xrightarrow{n \to \infty} 0. \]

  Only leakage rate vanishes
Wiretap Channels and Security Metrics
Degraded [Wyner 1975], General [Csiszár-Körner 1978]

\[ U[1:2^{nR}] \sim M \rightarrow X^n \rightarrow P_{Y,Z|X} \rightarrow Y^n \rightarrow Bob \]
\[ Z^n \rightarrow Eve \]

\( \hat{M} \)

\( \{C_n\}_{n \in \mathbb{N}} \) - a sequence of \((n, R)\)-codes

- **Weak-Secrecy:** \( \frac{1}{n} I_{C_n}(M; Z^n) \xrightarrow[n \to \infty]{\text{ }} 0 \).
Wiretap Channels and Security Metrics
Degraded [Wyner 1975], General [Csiszár-Körner 1978]

\[ U[1 : 2^{nR}] \sim M \]

\( \{C_n\}_{n \in \mathbb{N}} \) - a sequence of \((n, R)\)-codes

- **Weak-Secrecy:** \( \frac{1}{n} I_{C_n}(M; Z^n) \xrightarrow{n \to \infty} 0 \).
- **Strong-Secrecy:** \( I_{C_n}(M; Z^n) \xrightarrow{n \to \infty} 0 \).
Wiretap Channels and Security Metrics
Degraded [Wyner 1975], General [Csiszár-Körner 1978]

\[ U[1 : 2^{nR}] \sim M \]

\[ X^n \]

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

\[ Z^n \]

\[ \hat{M} \]

\[ M \]

\{C_n\}_{n \in \mathbb{N}} - a sequence of \((n, R)\)-codes

- **Weak-Secrecy:** \( \frac{1}{n} I_{C_n}(M; Z^n) \xrightarrow{n \to \infty} 0. \)

- **Strong-Secrecy:** \( I_{C_n}(M; Z^n) \xrightarrow{n \to \infty} 0. \) Security only on average
Wiretap Channels and Security Metrics

Degraded [Wyner 1975], General [Csiszár-Körner 1978]

\[
U[1 : 2^{nR}] \sim M \\
\xrightarrow{P_{Y,Z|X}} \\
\xrightarrow{X^n} \\
\xrightarrow{Y^n} Bob \\
\xrightarrow{Z^n} Eve \\
\xrightarrow{\hat{M}}
\]

\[
\{C_n\}_{n \in \mathbb{N}} - a sequence of (n, R)-codes
\]

- **Weak-Secrecy:** \( \frac{1}{n} I_{C_n}(M; Z^n) \xrightarrow{n \to \infty} 0. \)
- **Strong-Secrecy:** \( I_{C_n}(M; Z^n) \xrightarrow{n \to \infty} 0. \)
Wiretap Channels and Security Metrics
Degraded [Wyner 1975], General [Csiszár-Körner 1978]

\[ U[1 : 2^{nR}] \sim M \rightarrow X^n \rightarrow P_{Y,Z|X} \rightarrow Y^n \rightarrow Bob \rightarrow \hat{M} \]

\[ Z^n \rightarrow Eve \rightarrow M \]

\[ \{C_n\}_{n\in\mathbb{N}} - a\ sequence\ of\ (n, R)\text{-codes} \]

- **Weak-Secrecy:** \( \frac{1}{n} I_{C_n}(M; Z^n) \xrightarrow[n\to\infty]{} 0. \)
- **Strong-Secrecy:** \( I_{C_n}(M; Z^n) \xrightarrow[n\to\infty]{} 0. \)
- **Semantic Security:**
Wiretap Channels and Security Metrics

Degraded [Wyner 1975], General [Csiszár-Körner 1978]

\[
U[1 : 2^{nR}] \sim M \xrightarrow{X^n} P_{Y,Z|X} \xrightarrow{Y^n, Z^n} \hat{M} \xrightarrow{\hat{M}} Bob
\]

\[
\{C_n\}_{n \in \mathbb{N}} - a sequence of (n, R)-codes
\]

- **Weak-Secrecy**: 
  \[
  \frac{1}{n} I_{C_n}(M; Z^n) \xrightarrow{n \to \infty} 0.
  \]

- **Strong-Secrecy**: 
  \[
  I_{C_n}(M; Z^n) \xrightarrow{n \to \infty} 0.
  \]

- **Semantic Security**: [Bellare-Tessaro-Vardy 2012]
  \[
  \max_{P_M} I_{C_n}(M; Z^n) \xrightarrow{n \to \infty} 0.
  \]
Wiretap Channels and Security Metrics

Degraded [Wyner 1975], General [Csiszár-Körner 1978]

\[ U[1:2^{nR}] \sim M \]

\[ X^n \rightarrow P_{Y,Z|X} \]

\[ Y^n \rightarrow Bob \]

\[ Z^n \rightarrow Eve \]

\[ \hat{M} \]

\[ \{C_n\}_{n \in \mathbb{N}} - a sequence of (n, R)-codes \]

- **Weak-Secrecy:** \[ \frac{1}{n} I_{C_n}(M; Z^n) \xrightarrow{n \rightarrow \infty} 0. \]

- **Strong-Secrecy:** \[ I_{C_n}(M; Z^n) \xrightarrow{n \rightarrow \infty} 0. \]

- **Semantic Security:** [Bellare-Tessaro-Vardy 2012]

\[ \max_{P_M} I_{C_n}(M; Z^n) \xrightarrow{n \rightarrow \infty} 0. \]

★ A single code that satisfied exponentially many secrecy constraints ★

Z. Goldfeld, P. Cuff and H. Permuter

Ben-Gurion University and Princeton University

Arbitrarily Varying WTCs with Type Constrained States
Strong Soft-Covering Lemma
Soft-Covering - Setup

\[ W \xrightarrow{\text{Unif}[1 : 2^{n\tilde{R}}]} \text{Codebook} \xrightarrow{U^n} Q_{V|U} \xrightarrow{} V^n \]
Soft-Covering - Setup

$$W \xrightarrow{\text{Unif}[1:2^{n\tilde{R}}]} \text{Codebook} \xrightarrow{U^n} Q_{V|U} \xrightarrow{V^n} \text{Resemble i.i.d.}$$
Soft-Covering - Setup

Random Codebook: \( C_n = \{ U^n(w) \}_{w} \overset{iid}{\sim} Q^n_U. \)
Random Codebook: $C_n = \{U^n(w)\}_{w} \overset{iid}{\sim} Q^n_U$. 

$W \xrightarrow{\text{Unif}[1:2^{n\tilde{R}}]} \text{Code } C_n \xrightarrow{U^n} Q_{V|U} \xrightarrow{V^n} \text{Resemble } i.i.d.$
Soft-Covering - Setup

- **Random Codebook:** $C_n = \{ U^n(w) \}_{w \sim Q_U}^{i.i.d.} Q^n_U$.

- **Induced Output Distribution:** Codebook $C_n \implies V^n \sim P^{(C_n)}_{V^n}$.
**Soft-Covering - Setup**

- **Random Codebook:** $C_n = \{U^n(w)\}_{w \sim Q^n_U}$.
- **Induced Output Distribution:** Codebook $C_n \implies V^n \sim P^{(C_n)}_{V^n}$.
- **Target IID Distribution:** $Q^n_V$ marginal of $Q^n_U Q^{n|U}$.

\[ W \xrightarrow{\text{Unif}[1 : 2^{n\tilde{R}}]} \text{Code } C_n \xrightarrow{U^n} Q^n_{V|U} \xrightarrow{V^n} \sim P^{(C_n)}_{V^n} \]
• **Random Codebook:** \( C_n = \{ U^n(w) \} \overset{\text{iid}}{\sim} Q^n_U. \)

• **Induced Output Distribution:** Codebook \( C_n \implies V^n \sim P^{(C_n)}_{V^n} \approx Q^n_V. \)

• **Target IID Distribution:** \( Q^n_V \) marginal of \( Q^n_U Q^n_{V|U}. \)
**Soft-Covering - Setup**

- **Random Codebook:** $C_n = \{U^n(w)\}_{w}^{iid} \sim Q^n_U$.

- **Induced Output Distribution:** Codebook $C_n \implies V^n \sim P^{(C_n)}_{V^n} \approx Q^n_V$.

- **Target IID Distribution:** $Q^n_V$ marginal of $Q^n_U Q^n_{V|U}$.

\[ \star \textbf{Goal:} \text{Choose } \tilde{R} \text{ (codebook size) s.t. } P^{(C_n)}_{V^n} \approx Q^n_V \star \]
Soft-Covering - Results

\[
\begin{align*}
\text{Unif}[1 : 2^n \tilde{R}] & \quad \xrightarrow{W} \quad \text{Code } C_n \\
\xrightarrow{U^n} & \quad Q_{V|U} \\
\xrightarrow{V^n \sim P_{V^n}^{(C_n)}} & \quad \approx Q^n_V
\end{align*}
\]

\[\tilde{R} > I_Q(U; V) \quad \Longrightarrow \quad P_{V^n}^{(C_n)} \approx Q^n_V\]
Soft-Covering - Results

\[
\begin{align*}
W & \xrightarrow{\text{Unif}[1:2^{n\tilde{R}}]} \text{Code } C_n & & & & & & & & & & & & \Rightarrow & & & & & & & & & & & & & & & & V^n \sim & P_{V^n}^{(C_n)} & \approx & Q^n_V \\
U^n & \xrightarrow{Q^n_U} & Q_V & \xrightarrow{P_{V^n}^{(C_n)}} & Q_V^n
\end{align*}
\]

\[\tilde{R} > I_Q(U;V) \implies P_{V^n}^{(C_n)} \approx Q^n_V\]

• **Wyner 1975:** \[
\mathbb{E}_{C_n} \frac{1}{n} D\left( P_{V^n}^{(C_n)} \parallel Q_V^n \right) \xrightarrow{n \to \infty} 0.
\]

Z. Goldfeld, P. Cuff and H. Permuter  
Ben-Gurion University and Princeton University

Arbitrarily Varying WTCs with Type Constrained States
7
Soft-Covering - Results

\[ W \xrightarrow{\text{Unif}[1 : 2^n\tilde{R}]} \text{Code } C_n \xrightarrow{U^n} Q_{V|U} \xrightarrow{V^n \sim P_{V^n}^{(C_n)}} \approx Q^n_V \]

\[ \tilde{R} > I_Q(U; V) \implies P_{V^n}^{(C_n)} \approx Q^n_V \]

- **Wyner 1975**: \( \mathbb{E}_{C_n} \frac{1}{n} D \left( P_{V^n}^{(C_n)} \parallel Q^n_V \right) \xrightarrow{n \to \infty} 0 \).
- **Han-Verdú 1993**: \( \mathbb{E}_{C_n} \| P_{V^n}^{(C_n)} - Q^n_V \|_{TV} \xrightarrow{n \to \infty} 0 \).
Soft-Covering - Results

\[ W \xrightarrow{\text{Unif}[1:2^n\tilde{R}]} \text{Code } C_n \xrightarrow{U^n} \text{ } Q_{V|U} \xrightarrow{V^n \sim P_{V^n}^{(C_n)}} \approx Q^n_V \]

\[ \tilde{R} > I_Q(U;V) \implies P_{V^n}^{(C_n)} \approx Q^n_V \]

- **Wyner 1975**: \( \mathbb{E}_{C_n} \frac{1}{n} D\left( P_{V^n}^{(C_n)} \right| Q^n_V ) \xrightarrow{n \to \infty} 0. \)

- **Han-Verdú 1993**: \( \mathbb{E}_{C_n} \left\| P_{V^n}^{(C_n)} - Q^n_V \right\|_{\text{TV}} \xrightarrow{n \to \infty} 0. \)
  - Also provided converse.
Soft-Covering - Results

\[
\begin{align*}
W &\xrightarrow{\text{Unif}[1:2^n\tilde{R}]} \text{Code } C_n \\
&\xrightarrow{U^n} Q_{V|U} \\
&\xrightarrow{V^n \sim P_{V_n}^{(C_n)}} \approx Q_{V_n}^n
\end{align*}
\]

\[\tilde{R} > I_Q(U;V) \implies P_{V_n}^{(C_n)} \approx Q_{V_n}^n\]

- **Wyner 1975**: \(\mathbb{E}_{C_n} \frac{1}{n} D\left(P_{V_n}^{(C_n)} \parallel Q_V^n\right) \xrightarrow{n \to \infty} 0.\)
- **Han-Verdú 1993**: \(\mathbb{E}_{C_n} \left\| P_{V_n}^{(C_n)} - Q_V^n \right\|_{TV} \xrightarrow{n \to \infty} 0.\)
  - Also provided converse.
- **Hou-Kramer 2014**: \(\mathbb{E}_{C_n} D\left(P_{V_n}^{(C_n)} \parallel Q_V^n\right) \xrightarrow{n \to \infty} 0.\)
Theorem (Cuff 2015, ZG-Cuff-Permuter 2016)

If \( \tilde{R} > I_Q(U; V) \) and \( |V| < \infty \), then there exists \( \gamma_1, \gamma_2 > 0 \) s.t.

\[
P_{C_n}(D(P_{V^n|U}^{(C_n)} || Q^n_V) > e^{-n\gamma_1}) \leq e^{-e^{n\gamma_2}}
\]

for \( n \) sufficiently large.
Wiretap Channels of Type II
Wiretap Channels of Type II - Definition

[Ozarow-Wyner 1984]

\[ \mathcal{Q}_{Y|X} \quad Y^n \quad Bob \quad \hat{m} \]

\[ m \quad X^n \quad Alice \]

\[ S \subseteq [1:n], |S| = \mu \]

\[ Z_i = \begin{cases} X_i, & i \in S \\ ?, & i \notin S \end{cases} \]

\[ m \quad Z^n \quad Eve \]

\[ \mu \]

Alice sends a message \( m \) to Bob over the channel \( \mathcal{Q}_{Y|X} \). Bob receives a message \( Y^n \). Eve intercepts the channel and receives an output \( Z^n \). The condition is that \( S \subseteq [1:n], |S| = \mu \) for some subset \( S \) of the channel inputs, and the messages are defined accordingly.
Wiretap Channels of Type II - Definition

[Ozarow-Wyner 1984]

- **Eavesdropper**: Can observe a subset $S \subseteq [1:n]$ of size $\mu = \lfloor \alpha n \rfloor$, $\alpha \in [0, 1]$, of transmitted symbols.
Wiretap Channels of Type II - Definition

[Ozarow-Wyner 1984]

\[ m \xrightarrow{{m}} \text{Alice} \xrightarrow{X^n} Q_{Y|X} \xrightarrow{Y^n} \text{Bob} \xrightarrow{\hat{m}} \text{Eve} \]

- **Eavesdropper:** Can observe a subset \( S \subseteq [1:n], |S| = \mu \) of transmitted symbols.

- **Transmitted:**
  
  \[
  \begin{array}{cccccccccc}
  0 & 0 & 1 & 0 & 1 & 1 & 1 & 0 & 1 & 0 \\
  \end{array}
  \]

  \( n = 10 \quad \alpha = 0.6 \)
**Wiretap Channels of Type II - Definition**

[Ozarow-Wyner 1984]

- **Eavesdropper:** Can observe a subset $S \subseteq [1:n]$ of size $\mu = \lfloor \alpha n \rfloor$, $\alpha \in [0, 1]$, of transmitted symbols.

- **Transmitted:**

  |   |   |   |   |   |   |   |   |   |
  |---|---|---|---|---|---|---|---|---|
  | 0 | 0 | 1 | 0 | 1 | 1 | 1 | 0 | 1 |

  $n = 10$, $\alpha = 0.6$

- **Observed:**

  |   |   |   |   |   |   |   |   |   |
  |---|---|---|---|---|---|---|---|---|
  | ? | 0 | ? | ? | 1 | 1 | 1 | ? | 1 |

  |   |   |   |   |   |   |   |   |   |
  |---|---|---|---|---|---|---|---|---|
  | ? | ? | ? | 1 | 1 | 1 | ? | 1 | 0 |
Wiretap Channels of Type II - Definition

[Ozarow-Wyner 1984]

Eavesdropper: Can observe a subset $S \subseteq [1:n]$ of size $\mu = \lfloor \alpha n \rfloor$, $\alpha \in [0, 1]$, of transmitted symbols.

Transmitted: $n = 10$ $\alpha = 0.6$

Observed:

★ Ensure security versus all possible choices of $S$ ★
Wiretap Channels of Type II - Past Results

[Ozarow-Wyner 1984]

- Ozarow-Wyner 1984: Noiseless main channel
Wiretap Channels of Type II - Past Results

[Ozarow-Wyner 1984]

- **Ozarow-Wyner 1984**: Noiseless main channel
  - Rate equivocation region.
Wiretap Channels of Type II - Past Results
[Ozarow-Wyner 1984]

\[ S \subseteq [1:n], |S| = \mu \]

\[ Z_i = \begin{cases} 
X_i, & i \in S \\
?, & i \notin S 
\end{cases} \]

- **Ozarow-Wyner 1984:** Noiseless main channel
  - Rate equivocation region.
  - Coset coding.
Wiretap Channels of Type II - Past Results

[Ozarow-Wyner 1984]

\[ S \subseteq [1:n], |S| = \mu \]

\[ Z_i = \begin{cases} 
X_i, & i \in S \\
?, & i \notin S 
\end{cases} \]

**Ozarow-Wyner 1984:** Noiseless main channel

- Rate equivocation region.
- Coset coding.

**Nafea-Yener 2015:** Noisy main channel
Wiretap Channels of Type II - Past Results

[Ozarow-Wyner 1984]

**Ozarow-Wyner 1984:** Noiseless main channel
- Rate equivocation region.
- Coset coding.

**Nafea-Yener 2015:** Noisy main channel
- Built on coset code construction.
Wiretap Channels of Type II - Past Results

[Ozarow-Wyner 1984]

- **Ozarow-Wyner 1984**: Noiseless main channel
  - Rate equivocation region.
  - Coset coding.

- **Nafea-Yener 2015**: Noisy main channel
  - Built on coset code construction.
  - Lower & upper bounds - Not match in general.
Semantic Security:
Semantic Security: \[
\max_{P_M,S: |S|=\mu} I_{C_n}(M;Z^n) \xrightarrow{n \to \infty} 0.
\]
Wiretap Channels of Type II - SS-Capacity

Semantic Security: \[
\max_{P_{M}, S: |S| = \mu} I_{C_{n}}(M; Z^{n}) \xrightarrow{n \to \infty} 0.
\]

Theorem

For any \( \alpha \in [0, 1] \)

\[
C_{\text{Semantic}}(\alpha) = C_{\text{Weak}}(\alpha) = \max_{Q_{U,X}} \left[ I(U; Y) - \alpha I(U; X) \right]
\]
Wiretap Channels of Type II - SS-Capacity

Semantic Security: \[
\max_{P_M, S: |S| = \mu} I_{C_n}(M; Z^n) \xrightarrow{n \to \infty} 0.
\]

**Theorem**

For any \( \alpha \in [0, 1] \)
\[
C_{\text{Semantic}}(\alpha) = C_{\text{Weak}}(\alpha) = \max_{Q_{U,X}} \left[ I(U; Y) - \alpha I(U; X) \right]
\]

- **RHS** is the secrecy-capacity of WTC I with erasure DMC to Eve.

Z. Goldfeld, P. Cuff and H. Permuter Ben-Gurion University and Princeton University
Arbitrarily Varying WTCs with Type Constrained States
Semantic Security:

\[
\max_{P_M,S: |S|=\mu} I_{C_n}(M;Z^n) \xrightarrow{n\to\infty} 0.
\]

**Theorem**

*For any* \( \alpha \in [0, 1] \)

\[
C_{\text{Semantic}}(\alpha) = C_{\text{Weak}}(\alpha) = \max_{Q_{U,X}} \left[ I(U;Y) - \alpha I(U;X) \right]
\]

- RHS is the secrecy-capacity of WTC I with erasure DMC to Eve.
- Standard (erasure) wiretap code & Stronger tools for analysis.
Wiretap Code:
Wiretap Code:

\[ W \sim \text{Unif}[1 : 2^{n\tilde{R}}]. \]
Wiretap Code:

- $W \sim \text{Unif}[1 : 2^{n\tilde{R}}]$.
- $C_n = \{X^n(m, w)\}_{m,w} \sim \mathcal{Q}_X^n$.
Wiretap Code:

1. $W \sim \text{Unif}[1 : 2^n\tilde{R}]$.
2. $C_n = \{X^n(m, w)\}_{m, w} \overset{iid}{\sim} Q^n_X$.

Preliminary Step:

$$\max_{P_{M,S}, |S| = \mu} I_{C_n}(M; Z^n) \leq \max_{m, S: |S| = \mu} D\left(P_{Z\mu|M=m}^{(C_n,S)} \middle| Q^\mu_Z\right)$$
Wiretap Code:

- $W \sim \text{Unif}[1 : 2^{n\hat{R}}]$.
- $C_n = \{X^n(m, w)\}_{m,w} \sim Q^n_X$

Preliminary Step:

$$\max_{P_M,S: |S|=\mu} I_{C_n}(M; Z^n) \leq \max_{m,S: |S|=\mu} D\left( P^{(C_n,S)}_{Z\mu|M=m} \parallel Q^\mu_Z \right)$$
1 Wiretap Code:
   - $W \sim \text{Unif}[1 : 2^{n\tilde{R}}]$.
   - $C_n = \{ X^n(m, w) \}_{m, w \sim Q_X}$

2 Preliminary Step:
   $\max_{P_{M,S} : |S| = \mu} I_{C_n}(M ; Z^n) \leq \max_{m,S : |S| = \mu} D \left( P_{Z^\mu | M=m}^{(C_n,S)} \right | Q_Z^\mu)$

3 Union Bound & Strong SCL:
Wiretap Code:

1. $W \sim \text{Unif}[1 : 2^{n\tilde{R}}]$. 
2. $C_n = \{X^n(m, w)\}_{m, w \sim Q_X^n}^{iid}$. 

Preliminary Step:

$$\max_{P_M, S: |S| = \mu} I_{C_n}(M; Z^n) \leq \max_{m, S: |S| = \mu} D(P_{Z_M|\mu|\mu}^{(C_n, S)} || Q_Z^\mu)$$

Union Bound & Strong SCL:

$$\mathbb{P}\left( \max_{P_M, S} I_{C_n}(M; Z^n) \leq e^{-n\gamma_1} \right)^c$$
1 **Wiretap Code:**

- \( W \sim \text{Unif}[1 : 2^{nR}] \).
- \( C_n = \{ X^n(m, w) \}_{m, w} \overset{iid}{\sim} Q_X^n \).

2 **Preliminary Step:**

\[
\max_{P_M, S: |S| = \mu} I_{C_n}(M; Z^n) \leq \max_{m, S: |S| = \mu} D \left( P_{Z|M=m}^{(C_n, S)} \left| Q_Z^\mu \right. \right)
\]

3 **Union Bound & Strong SCL:**

\[
P \left( \left\{ \max_{P_M, S} I_{C_n}(M; Z^n) \leq e^{-n\gamma_1} \right\}^c \right) \leq P \left( \max_{m, S} D \left( P_{Z|M=m}^{(C_n, S)} \left| Q_Z^\mu \right. \right) > e^{-n\gamma_1} \right)
\]
1. **Wiretap Code:**

- $W \sim \text{Unif}[1 : 2^{nR}]$.
- $C_n = \{X^n(m, w)\}_{m, w} \overset{iid}{\sim} Q^n_X$

2. **Preliminary Step:**

$$\max_{P_M, S: |S| = \mu} I_{C_n}(M; Z^n) \leq \max_{m, S: |S| = \mu} D\left(P_{Z\mu|M=m}^{(C_n,S)} || Q^\mu_Z\right)$$

3. **Union Bound & Strong SCL:**

$$\mathbb{P}\left(\left\{ \max_{P_M, S} I_{C_n}(M; Z^n) \leq e^{-n\gamma_1} \right\}^c \right) \leq \mathbb{P}\left( \max_{m, S} D\left(P_{Z\mu|M=m}^{(C_n,S)} || Q^\mu_Z\right) > e^{-n\gamma_1} \right)$$

$$\leq \sum_{m, S} \mathbb{P}\left( D\left(P_{Z\mu|M=m}^{(C_n,S)} || Q^\mu_Z\right) > e^{-n\gamma_1} \right)$$
1 Wiretap Code:

- $W \sim \text{Unif}[1 : 2^n \tilde{R}]$.
- $C_n = \{ X^n(m, w) \}_{m, w} \overset{iid}{\sim} Q_X^n$.

2 Preliminary Step:

$$\max_{P_{M, S}: |S| = \mu} I_{C_n}(M; Z^n) \leq \max_{m, S: |S| = \mu} D(P^{(C_n, S)}_{Z^\mu | M = m} \parallel Q_Z^\mu)$$

3 Union Bound & Strong SCL:

$$\mathbb{P} \left( \left\{ \max_{P_{M, S}} I_{C_n}(M; Z^n) \leq e^{-n\gamma_1} \right\}^c \right) \leq \mathbb{P} \left( \max_{m, S} D(P^{(C_n, S)}_{Z^\mu | M = m} \parallel Q_Z^\mu) > e^{-n\gamma_1} \right) \leq \sum_{m, S} \mathbb{P} \left( D(P^{(C_n, S)}_{Z^\mu | M = m} \parallel Q_Z^\mu) > e^{-n\gamma_1} \right)$$
1 Wiretap Code:

- $W \sim \text{Unif}[1 : 2^n\hat{R}]$.
- $C_n = \{ X^n(m, w) \}_{m, w}^{iid} \sim Q^n_X$

2 Preliminary Step:

$$\max_{P_M, S: |S| = \mu} I_{C_n}(M; Z^n) \leq \max_{m, S: |S| = \mu} D\left( P_{Z^\mu|M=m}^{(C_n, S)} \parallel Q^\mu_Z \right)$$

3 Union Bound & Strong SCL:

$$\mathbb{P}\left( \left\{ \max_{P_M, S} I_{C_n}(M; Z^n) \leq e^{-n\gamma_1} \right\}^c \right) \leq \mathbb{P}\left( \max_{m, S} D\left( P_{Z^\mu|M=m}^{(C_n, S)} \parallel Q^\mu_Z \right) > e^{-n\gamma_1} \right)$$

$$\leq \sum_{m, S} \mathbb{P}\left( D\left( P_{Z^\mu|M=m}^{(C_n, S)} \parallel Q^\mu_Z \right) > e^{-n\gamma_1} \right)$$

Taking $\hat{R} > \alpha H(X)$ $\implies$
Wiretap Code:

1. $W \sim \text{Unif}[1 : 2^n\tilde{R}]$.

2. $C_n = \{X^n(m, w)\}_{m, w} \overset{iid}{\sim} Q^n_X$

Preliminary Step:

$$\max_{P_M, S: |S|=\mu} I_{C_n}(M; Z^n) \leq \max_{m, S: |S|=\mu} D(P^{(c_n, S)}_{Z^\mu|M=m} \ || Q^\mu_Z)$$

Union Bound & Strong SCL:

$$\mathbb{P}\left(\left\{\max_{P_M, S} I_{C_n}(M; Z^n) \leq e^{-n\gamma_1}\right\}^c\right) \leq \mathbb{P}\left(\max_{m, S} D(P^{(c_n, S)}_{Z^\mu|M=m} \ || Q^\mu_Z) > e^{-n\gamma_1}\right)$$

$$\leq \sum_{m, S} \mathbb{P}\left(D(P^{(c_n, S)}_{Z^\mu|M=m} \ || Q^\mu_Z) > e^{-n\gamma_1}\right)$$

Taking $\tilde{R} > \alpha H(X) \implies 2^n 2^{nR} e^{-e^{n\gamma_2}}$
Wiretap Code:

1. \( W \sim \text{Unif}[1 : 2^n\tilde{R}] \).

2. \( C_n = \{ X^n(m, w) \}_{m,w} \sim Q_X^n \).

Preliminary Step:

\[
\max_{P_{M,S}: |S| = \mu} I_{C_n}(M; Z^n) \leq \max_{m,S: |S| = \mu} D \left( P^{(C_n,S)}_{Z\mu|M=m} \bigg| Q^\mu_Z \right)
\]

Union Bound & Strong SCL:

\[
P\left( \max_{P_{M,S}} I_{C_n}(M; Z^n) \leq e^{-n\gamma_1} \right)^c \leq P\left( \max_{m,S} D \left( P^{(C_n,S)}_{Z\mu|M=m} \bigg| Q^\mu_Z \right) > e^{-n\gamma_1} \right)
\]

\[
\leq \sum_{m,S} P \left( D \left( P^{(C_n,S)}_{Z\mu|M=m} \bigg| Q^\mu_Z \right) > e^{-n\gamma_1} \right)
\]

Taking \( \tilde{R} > \alpha H(X) \),

\[
\leq 2^n2^{nR} e^{-en\gamma_2} \xrightarrow{n \to \infty} 0
\]
Arbitrarily Varying Wiretap Channels - Generalization

Models **main** and **eavesdropper** channel uncertainty.
Models *main* and *eavesdropper* channel uncertainty.

**Type Constrained States:** Allowed $s^n$ have empirical dist. $\approx Q_s$: 

\[ s^n \in S^n \]

\[ X^n \rightarrow_{\text{AVWTC}} Q_{Y,Z|X,S} \rightarrow Y^n \rightarrow \hat{m} \]

\[ m \rightarrow m \rightarrow \text{Alice} \]

\[ m \rightarrow \text{Bob} \]

\[ m \rightarrow \text{Eve} \]

\[ Z^n \rightarrow \text{Eve} \]
Models **main** and **eavesdropper** channel uncertainty.

**Type Constrained States:** Allowed $s^n$ have empirical dist. $\approx Q_S$:

Theorem (ZG-Cuff-Permuter 2016)

\[
C_{\text{Semantic}} = \max_{Q_{U,X}} \left[ I(U;Y) - I(U;Z|S) \right]
\]
Models **main** and **eavesdropper** channel uncertainty.

**Type Constrained States:** Allowed $s^n$ have empirical dist. $\approx Q_S$:

**Theorem (ZG-Cuff-Permuter 2016)**

$$C_{\text{Semantic}} = \max_{Q_{U,X}} \left[ I(U; Y) - I(U; Z|S) \right]$$

★ Subsumes WTC II model and result. ★
Recap

- **Strong Soft-Covering Lemma:**
Recap

**Strong Soft-Covering Lemma:**
- Double-exponential decay of probability of soft-covering not happening.
Recap

- **Strong Soft-Covering Lemma:**
  - Double-exponential decay of probability of soft-covering not happening.
  - Satisfy exponentially many soft-covering constraints at once.
Recap

**Strong Soft-Covering Lemma:**
- Double-exponential decay of probability of soft-covering not happening.
- Satisfy exponentially many soft-covering constraints at once.

**Semantic Security:**
Recap

- **Strong Soft-Covering Lemma:**
  - Double-exponential decay of probability of soft-covering not happening.
  - Satisfy exponentially many soft-covering constraints at once.

- **Semantic Security:**
  - Gold standard in cryptography - relevant for applications.
Recap

- **Strong Soft-Covering Lemma:**
  - Double-exponential decay of probability of soft-covering not happening.
  - Satisfy exponentially many soft-covering constraints at once.

- **Semantic Security:**
  - Gold standard in cryptography - relevant for applications.
  - Equivalent to vanishing information leakage when maximized over $P_M$. 
Recap

- **Strong Soft-Covering Lemma:**
  - Double-exponential decay of probability of soft-covering not happening.
  - Satisfy exponentially many soft-covering constraints at once.

- **Semantic Security:**
  - Gold standard in cryptography - relevant for applications.
  - Equivalent to vanishing information leakage when maximized over $P_M$.

- **Wiretap Channel II:**
Recap

- **Strong Soft-Covering Lemma:**
  - Double-exponential decay of probability of soft-covering not happening.
  - Satisfy exponentially many soft-covering constraints at once.

- **Semantic Security:**
  - Gold standard in cryptography - relevant for applications.
  - Equivalent to vanishing information leakage when maximized over $P_M$.

- **Wiretap Channel II:**
  - Noisy main channel - Open problem since 1984.
Recap

- **Strong Soft-Covering Lemma:**
  - Double-exponential decay of probability of soft-covering not happening.
  - Satisfy exponentially many soft-covering constraints at once.

- **Semantic Security:**
  - Gold standard in cryptography - relevant for applications.
  - Equivalent to vanishing information leakage when maximized over $P_M$.

- **Wiretap Channel II:**
  - Noisy main channel - Open problem since 1984.
  - Derivation of SS-capacity & Equality to weak-secrecy-capacity.
Recap

- **Strong Soft-Covering Lemma:**
  - Double-exponential decay of probability of soft-covering not happening.
  - Satisfy exponentially many soft-covering constraints at once.

- **Semantic Security:**
  - Gold standard in cryptography - relevant for applications.
  - Equivalent to vanishing information leakage when maximized over $P_M$.

- **Wiretap Channel II:**
  - Noisy main channel - Open problem since 1984.
  - Derivation of SS-capacity & Equality to weak-secrecy-capacity.

- **Type Constrained AVWTC:**
Recap

- **Strong Soft-Covering Lemma:**
  - Double-exponential decay of probability of soft-covering not happening.
  - Satisfy exponentially many soft-covering constraints at once.

- **Semantic Security:**
  - Gold standard in cryptography - relevant for applications.
  - Equivalent to vanishing information leakage when maximized over $P_M$.

- **Wiretap Channel II:**
  - Noisy main channel - Open problem since 1984.
  - Derivation of SS-capacity & Equality to weak-secrecy-capacity.

- **Type Constrained AVWTC:**
  - Single-letter characterization of type constrained AVWTC CR-capacity.
Recap

- **Strong Soft-Covering Lemma:**
  - Double-exponential decay of probability of soft-covering not happening.
  - Satisfy exponentially many soft-covering constraints at once.

- **Semantic Security:**
  - Gold standard in cryptography - relevant for applications.
  - Equivalent to vanishing information leakage when maximized over $P_M$.

- **Wiretap Channel II:**
  - Noisy main channel - Open problem since 1984.
  - Derivation of SS-capacity & Equality to weak-secrecy-capacity.

- **Type Constrained AVWTC:**
  - Single-letter characterization of type constrained AVWTC CR-capacity.
  - General single-letter lower and upper bounds.
Recap

- **Strong Soft-Covering Lemma:**
  - Double-exponential decay of probability of soft-covering not happening.
  - Satisfy exponentially many soft-covering constraints at once.

- **Semantic Security:**
  - Gold standard in cryptography - relevant for applications.
  - Equivalent to vanishing information leakage when maximized over $P_M$.

- **Wiretap Channel II:**
  - Noisy main channel - Open problem since 1984.
  - Derivation of SS-capacity & Equality to weak-secrecy-capacity.

- **Type Constrained AVWTC:**
  - Single-letter characterization of type constrained AVWTC CR-capacity.
  - General single-letter lower and upper bounds.

Thank You!
Summary

- **Semantic Security**: [Bellare-Tessaro-Vardy 2012]
Summary

- **Semantic Security**: [Bellare-Tessaro-Vardy 2012]
  - Cryptographic benchmark - relevant for applications.
Summary

- **Semantic Security:** [Bellare-Tessaro-Vardy 2012]
  - Cryptographic benchmark - relevant for applications.

- **Strong Soft-Covering Lemma:**
Summary

- **Semantic Security**: [Bellare-Tessaro-Vardy 2012]
  - Cryptographic benchmark - relevant for applications.

- **Strong Soft-Covering Lemma**:
  - Codes that satisfy exponentially many secrecy constraints.
Summary

- **Semantic Security**: [Bellare-Tessaro-Vardy 2012]
  - Cryptographic benchmark - relevant for applications.

- **Strong Soft-Covering Lemma**:  
  - Codes that satisfy exponentially many secrecy constraints.

- **Wiretap Channel II**: A model for channel uncertainty
Summary

- **Semantic Security**: [Bellare-Tessaro-Vardy 2012]
  - Cryptographic benchmark - relevant for applications.

- **Strong Soft-Covering Lemma**:
  - Codes that satisfy exponentially many secrecy constraints.

- **Wiretap Channel II**: A model for channel uncertainty
  - Noisy main channel - Open problem since 1984.
Summary

- **Semantic Security**: [Bellare-Tessaro-Vardy 2012]
  - Cryptographic benchmark - relevant for applications.

- **Strong Soft-Covering Lemma**:
  - Codes that satisfy exponentially many secrecy constraints.

- **Wiretap Channel II**: A model for channel uncertainty
  - Noisy main channel - Open problem since 1984.
  - Derivation of SS-capacity.
Summary

- **Semantic Security:** [Bellare-Tessaro-Vardy 2012]
  - Cryptographic benchmark - relevant for applications.

- **Strong Soft-Covering Lemma:**
  - Codes that satisfy exponentially many secrecy constraints.

- **Wiretap Channel II:** A model for channel uncertainty
  - Noisy main channel - Open problem since 1984.
  - Derivation of SS-capacity.
  - Extensions to AVWTC.
• **Semantic Security:** [Bellare-Tessaro-Vardy 2012]
  ▶ Cryptographic benchmark - relevant for applications.

• **Strong Soft-Covering Lemma:**
  ▶ Codes that satisfy exponentially many secrecy constraints.

• **Wiretap Channel II:** A model for channel uncertainty
  ▶ Noisy main channel - Open problem since 1984.
  ▶ Derivation of SS-capacity.
  ▶ Extensions to AVWTC.

Thank You!
Finalization:
Finalization:

- **Semantic Security**: Ensured if $\tilde{R} > \alpha H(X)$. 

Z. Goldfeld, P. Cuff and H. Permuter Ben-Gurion University and Princeton University

Arbitrarily Varying WTCs with Type Constrained States
Finalization:

- **Semantic Security:** Ensured if $\tilde{R} > \alpha H(X)$.

- **Reliability:** Successfully decode $(M, W)$ if $R + \tilde{R} < I(X; Y)$. 
Finalization:

- **Semantic Security:** Ensured if $\tilde{R} > \alpha H(X)$.

- **Reliability:** Successfully decode $(M, W)$ if $R + \tilde{R} < I(X; Y)$.

  $$\implies R < I(X; Y) - \alpha H(X)$$ is achievable.
Finalization:

- **Semantic Security:** Ensured if $\tilde{R} > \alpha H(X)$.

- **Reliability:** Successfully decode $(M, W)$ if $R + \tilde{R} < I(X; Y)$.

  \[ \implies R < I(X; Y) - \alpha H(X) \text{ is achievable.} \]

**Channel Prefixing:** Prefixing $Q_{X|U}$ achieves $I(U; Y) - \alpha I(U; X)$. 

---

Z. Goldfeld, P. Cuff and H. Permuter
Ben-Gurion University and Princeton University
Arbitrarily Varying WTCs with Type Constrained States
\text{SS-capacity WTC II} \leq \text{Weak-secrecy-capacity WTC I}
WTC II SS-Capacity - Converse

SS-capacity WTC II \leq \text{Weak-secrecy-capacity WTC I}

- WTC I with erasure DMC to Eve - Transition probability $\alpha$. 
SS-capacity WTC II ≤ Weak-secrecy-capacity WTC I

- **WTC I** with erasure DMC to Eve - Transition probability $\alpha$.

**Difficulty:** Eve might observe more $X_i$-s in **WTC I** than in **WTC II**.
WTC II SS-Capacity - Converse

\[
\text{SS-capacity WTC II} \leq \text{Weak-secrecy-capacity WTC I}
\]

- **WTC I** with erasure DMC to Eve - Transition probability \( \alpha \).

- **Difficulty:** Eve might observe more \( X_i \)-s in **WTC I** than in **WTC II**.

- **Solution:** Sanov’s theorem & Continuity of mutual information.