Semantic Security in the Presence of Active Adversaries

Ziv Goldfeld
Joint work with Paul Cuff and Haim Permuter

Ben Gurion University

Advanced Communications Center Annual Workshop

February 22nd, 2016

Motivation

Information Theoretic Security over Noisy Channels

Motivation

Information Theoretic Security over Noisy Channels

Pros:

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.

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:

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** & **constant in time**.

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** & **constant in time**.
2. Security metrics **insufficient for (some) applications**.

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:

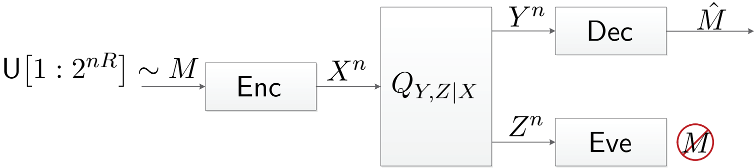
1. Eve's channel assumed to be **fully known** & **constant in time**.
2. Security metrics **insufficient for (some) applications**.

Our Goal: Stronger metric and remove "known channel" assumption.

Wiretap Channels - Security Metrics

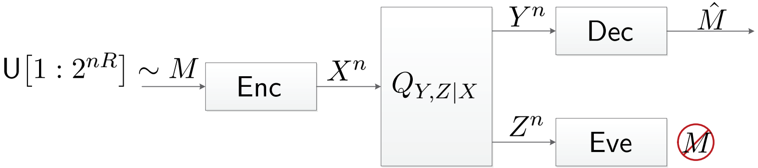
Wiretap Channels and Security Metrics

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



Wiretap Channels and Security Metrics

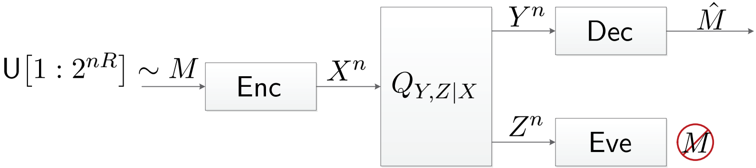
Degraded [Wyner 1975], General [Csiszár-Körner 1978]



$\{\mathcal{C}_n\}_{n\in\mathbb{N}}$ - a sequence of (n,R)-codes

Wiretap Channels and Security Metrics

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

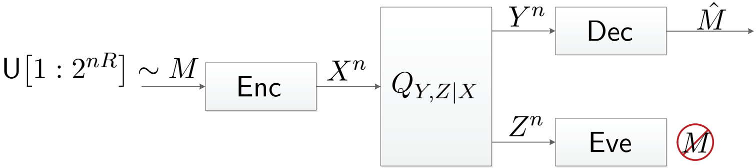


$\{\mathcal{C}_n\}_{n\in\mathbb{N}}$ - a sequence of (n,R)-codes

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

Wiretap Channels and Security Metrics

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

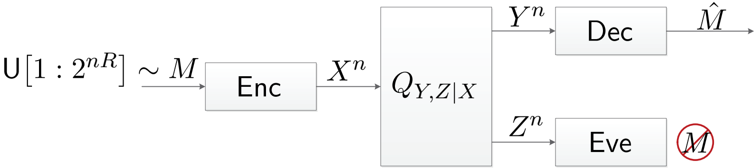


$\{\mathcal{C}_n\}_{n\in\mathbb{N}}$ - a sequence of (n, R)-codes

- **Weak-Secrecy:** $\frac{1}{n} I_{\mathcal{C}_n}(M; Z^n) \xrightarrow[n\to\infty]{} 0.$ Only leakage **rate** vanishes

Wiretap Channels and Security Metrics

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

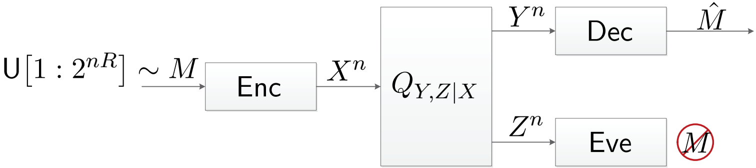


$\{\mathcal{C}_n\}_{n\in\mathbb{N}}$ - a sequence of (n,R)-codes

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

Wiretap Channels and Security Metrics

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

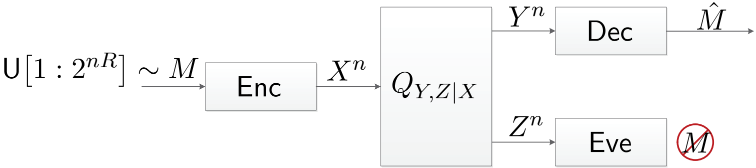


$\{\mathcal{C}_n\}_{n\in\mathbb{N}}$ - a sequence of (n,R)-codes

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

Wiretap Channels and Security Metrics

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

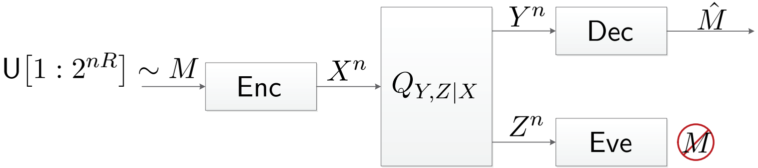


$\{\mathcal{C}_n\}_{n\in\mathbb{N}}$ - a sequence of (n,R)-codes

- **Weak-Secrecy:** $\frac{1}{n} I_{\mathcal{C}_n}(M;Z^n) \xrightarrow[n\to\infty]{} 0.$
- **Strong-Secrecy:** $I_{\mathcal{C}_n}(M;Z^n) \xrightarrow[n\to\infty]{} 0.$ Security only on **average**

Wiretap Channels and Security Metrics

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

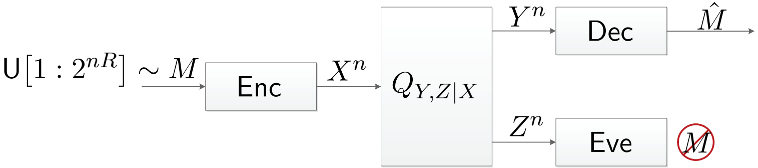


$\{\mathcal{C}_n\}_{n\in\mathbb{N}}$ - a sequence of (n,R)-codes

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

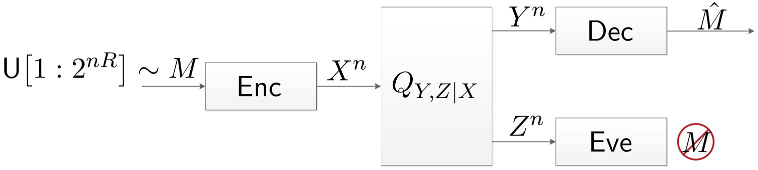
Wiretap Channels and Security Metrics

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



$\{\mathcal{C}_n\}_{n\in\mathbb{N}}$ - a sequence of (n, R)-codes

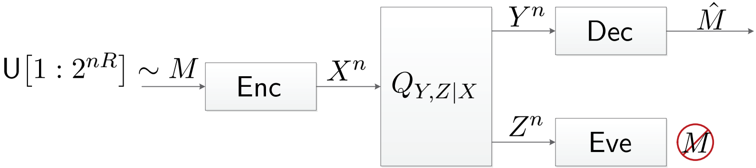
- **Weak-Secrecy:** $\frac{1}{n} I_{\mathcal{C}_n}(M; Z^n) \xrightarrow[n\to\infty]{} 0.$
- **Strong-Secrecy:** $I_{\mathcal{C}_n}(M; Z^n) \xrightarrow[n\to\infty]{} 0.$
- **Semantic Security:**



$\{\mathcal{C}_n\}_{n\in\mathbb{N}}$ - a sequence of (n,R)-codes

- **Weak-Secrecy:** $\frac{1}{n} I_{\mathcal{C}_n}(M;Z^n) \xrightarrow[n\to\infty]{} 0.$
- **Strong-Secrecy:** $I_{\mathcal{C}_n}(M;Z^n) \xrightarrow[n\to\infty]{} 0.$
- **Semantic Security:** [Bellare-Tessaro-Vardy 2012]

$$\max_{P_M} I_{\mathcal{C}_n}(M;Z^n) \xrightarrow[n\to\infty]{} 0.$$



$\{\mathcal{C}_n\}_{n\in\mathbb{N}}$ - a sequence of (n, R)-codes

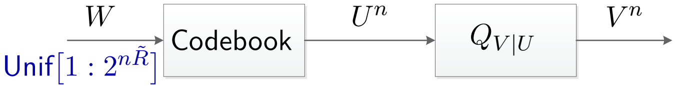
- **Weak-Secrecy:** $\frac{1}{n} I_{\mathcal{C}_n}(M; Z^n) \xrightarrow[n\to\infty]{} 0.$
- **Strong-Secrecy:** $I_{\mathcal{C}_n}(M; Z^n) \xrightarrow[n\to\infty]{} 0.$
- **Semantic Security:** [Bellare-Tessaro-Vardy 2012]

$$\max_{P_M} I_{\mathcal{C}_n}(M; Z^n) \xrightarrow[n\to\infty]{} 0.$$

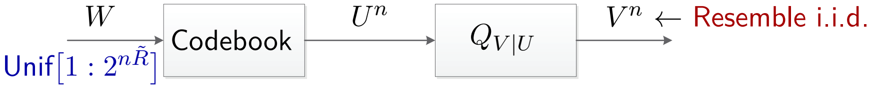
⋆ A single code must work well for all message PMFs ⋆

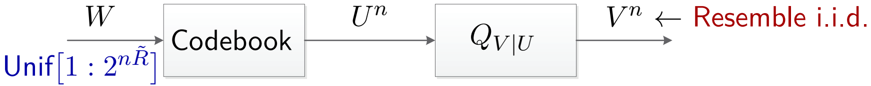
A Stronger Soft-Covering Lemma

Soft-Covering - Setup



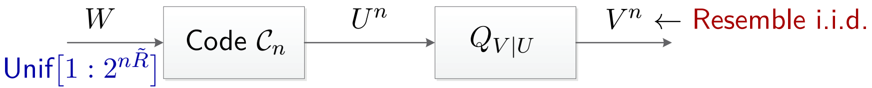
 Soft-Covering - Setup





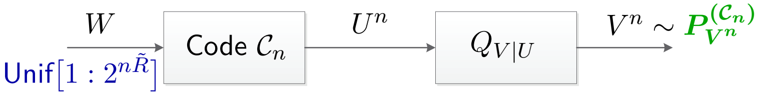
- **Random Codebook:** $\mathbb{C}_n = \left\{U^n(w)\right\}_w \overset{iid}{\sim} Q_U^n$.

Soft-Covering - Setup



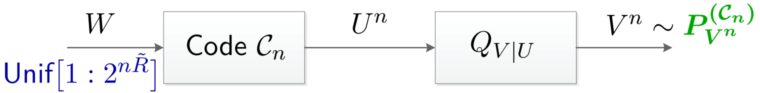
- **Random Codebook:** $\mathbb{C}_n = \{U^n(w)\}_w \overset{iid}{\sim} Q_U^n$.

Soft-Covering - Setup



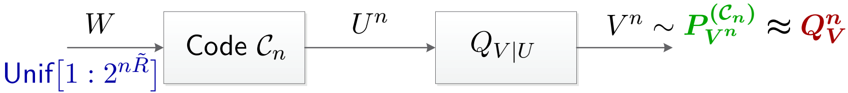
- **Random Codebook:** $\mathbb{C}_n = \{U^n(w)\}_w \overset{iid}{\sim} Q_U^n$.
- **Induced Output Distribution:** Codebook $\mathcal{C}_n \implies V^n \sim P_{V^n}^{(\mathcal{C}_n)}$.

Soft-Covering - Setup

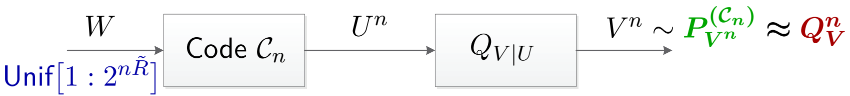


- **Random Codebook:** $\mathbb{C}_n = \{U^n(w)\}_w \overset{iid}{\sim} Q_U^n$.
- **Induced Output Distribution:** Codebook $\mathcal{C}_n \implies V^n \sim P_{V^n}^{(\mathcal{C}_n)}$.
- **Target IID Distribution:** Q_V^n marginal of $Q_U^n Q_{V|U}^n$.

Soft-Covering - Setup



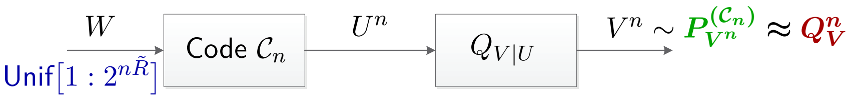
- **Random Codebook:** $\mathbb{C}_n = \{U^n(w)\}_w \stackrel{iid}{\sim} Q_U^n$.
- **Induced Output Distribution:** Codebook $\mathcal{C}_n \implies V^n \sim P_{V^n}^{(\mathcal{C}_n)}$.
- **Target IID Distribution:** Q_V^n marginal of $Q_U^n Q_{V|U}^n$.



- **Random Codebook:** $\mathbb{C}_n = \{U^n(w)\}_w \overset{iid}{\sim} Q_U^n$.
- **Induced Output Distribution:** Codebook $\mathcal{C}_n \implies V^n \sim P_{V^n}^{(\mathcal{C}_n)}$.
- **Target IID Distribution:** Q_V^n marginal of $Q_U^n Q_{V|U}^n$.

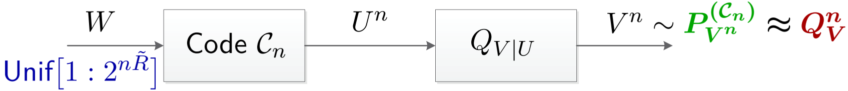
⋆ **Goal:** Choose $\tilde{R}$ (codebook size) s.t. $P_{V^n}^{(\mathcal{C}_n)} \approx Q_V^n$ ⋆

Soft-Covering - Results



$$\tilde{R} > I_Q(U;V) \implies P_{V^n}^{(\mathcal{C}_n)} \approx Q_V^n$$

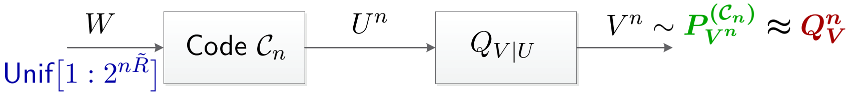
Soft-Covering - Results



$$\tilde{R} > I_Q(U;V) \implies P_{V^n}^{(\mathcal{C}_n)} \approx Q_V^n$$

- **Wyner 1975**: $\mathbb{E}_{\mathbb{C}_n} \frac{1}{n} D\left(P_{V^n}^{(\mathbb{C}_n)} \middle|\middle| Q_V^n\right) \xrightarrow[n\to\infty]{} 0.$

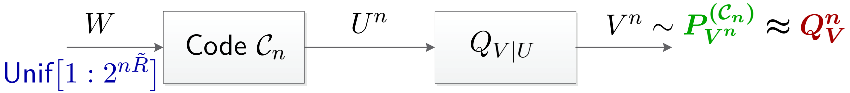
Soft-Covering - Results



$$\tilde{R} > I_Q(U;V) \implies P_{V^n}^{(\mathcal{C}_n)} \approx Q_V^n$$

- **Wyner 1975**: $\mathbb{E}_{\mathbb{C}_n} \frac{1}{n} D\left(P_{V^n}^{(\mathbb{C}_n)} \middle|\middle| Q_V^n\right) \xrightarrow[n\to\infty]{} 0.$
- **Han-Verdú 1993**: $\mathbb{E}_{\mathbb{C}_n} \left|\left| P_{V^n}^{(\mathbb{C}_n)} - Q_V^n \right|\right|_{\mathrm{TV}} \xrightarrow[n\to\infty]{} 0.$

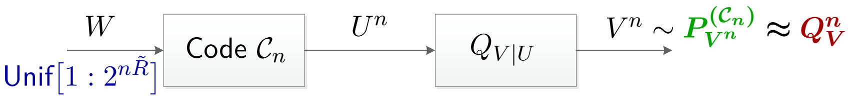
Soft-Covering - Results



$$\tilde{R} > I_Q(U;V) \implies P_{V^n}^{(\mathcal{C}_n)} \approx Q_V^n$$

- **Wyner 1975**: $\mathbb{E}_{\mathbb{C}_n} \frac{1}{n} D\left(P_{V^n}^{(\mathbb{C}_n)} \middle|\middle| Q_V^n\right) \xrightarrow[n\to\infty]{} 0.$
- **Han-Verdú 1993**: $\mathbb{E}_{\mathbb{C}_n} \left|\left| P_{V^n}^{(\mathbb{C}_n)} - Q_V^n \right|\right|_{\mathrm{TV}} \xrightarrow[n\to\infty]{} 0.$
  - Also provided converse.

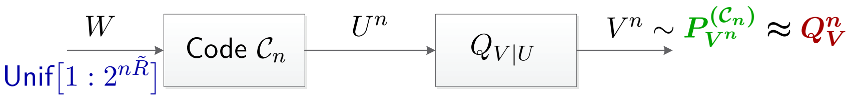
Soft-Covering - Results



$$\tilde{R} > I_Q(U;V) \implies P_{V^n}^{(\mathcal{C}_n)} \approx Q_V^n$$

- **Wyner 1975**: $\mathbb{E}_{\mathbb{C}_n} \frac{1}{n} D\left(P_{V^n}^{(\mathbb{C}_n)} \middle|\middle| Q_V^n\right) \xrightarrow[n\to\infty]{} 0.$
- **Han-Verdú 1993**: $\mathbb{E}_{\mathbb{C}_n} \left|\left| P_{V^n}^{(\mathbb{C}_n)} - Q_V^n \right|\right|_{\mathrm{TV}} \xrightarrow[n\to\infty]{} 0.$
  - Also provided converse.
- **Hou-Kramer 2014**: $\mathbb{E}_{\mathbb{C}_n} D\left(P_{V^n}^{(\mathbb{C}_n)} \middle|\middle| Q_V^n\right) \xrightarrow[n\to\infty]{} 0.$

A Stronger Soft-Covering Lemma



Theorem

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

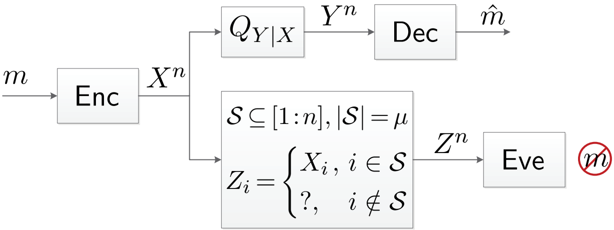
$$\mathbb{P}_{\mathbb{C}_n}\left(D\left(P_{V^n}^{(\mathbb{C}_n)} \middle\| Q_V^n \right) > e^{-n\gamma_1} \right) \leq e^{-e^{n\gamma_2}}$$

for n *sufficiently large.*

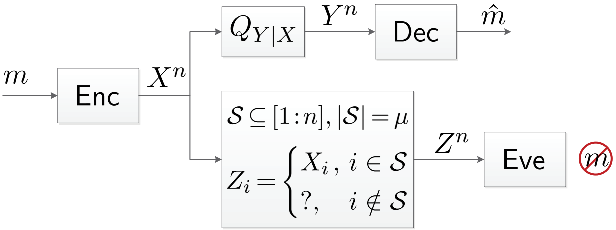
Wiretap Channels of Type II

Wiretap Channels of Type II - Definition

[Ozarow-Wyner 1984]



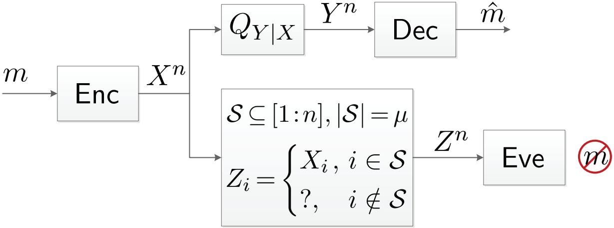
Wiretap Channels of Type II - Definition
[Ozarow-Wyner 1984]



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

Wiretap Channels of Type II - Definition

[Ozarow-Wyner 1984]



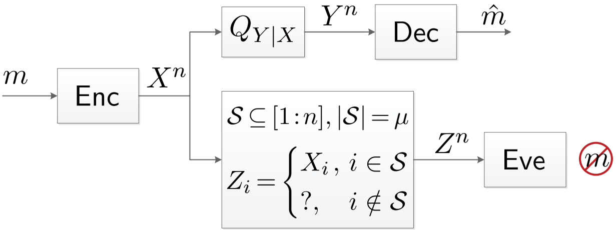
- **Eavesdropper:** Can observe a subset $\boldsymbol{\mathcal{S}} \subseteq [1:n]$ of size $\boldsymbol{\mu = \lfloor \alpha n \rfloor}$, $\boldsymbol{\alpha \in [0,1]}$, of transmitted symbols.
- **Transmitted:**

0	0	1	0	1	1	1	0	1	0

$n = 10$ $\boldsymbol{\alpha = 0.63}$

Wiretap Channels of Type II - Definition

[Ozarow-Wyner 1984]

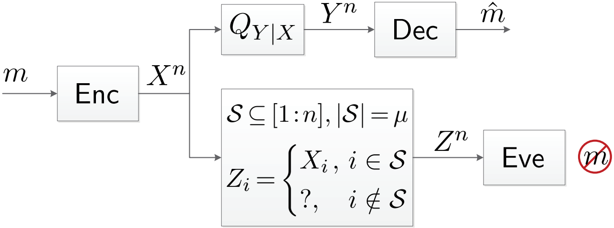


- **Eavesdropper:** Can observe a subset $\mathcal{S} \subseteq [1:n]$ of size $\mu = \lfloor \alpha n \rfloor$, $\alpha \in [0,1]$, of transmitted symbols.

- **Transmitted:** 0 0 1 0 1 1 1 0 1 0 $n = 10$ $\alpha = 0.63$
- **Observed:** ? 0 ? ? 1 1 1 ? 1 0

Wiretap Channels of Type II - Definition

[Ozarow-Wyner 1984]



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

- **Transmitted:**
- **Observed:**

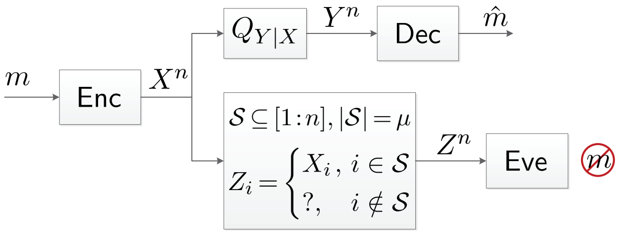
Transmitted:	0	0	1	0	1	1	1	0	1	0
Observed:	?	0	?	?	1	1	1	?	1	0

$n = 10$ $\boldsymbol{\alpha = 0.63}$

⋆ Ensure security versus all possible choices of $\boldsymbol{\mathcal{S}}$ ⋆

Wiretap Channels of Type II - Past Results

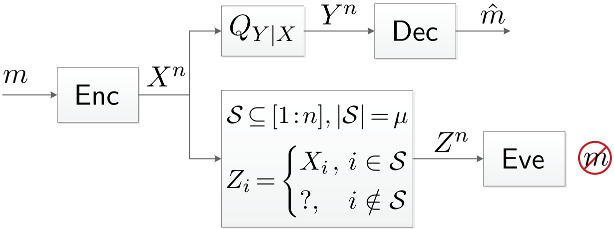
[Ozarow-Wyner 1984]



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

Wiretap Channels of Type II - Past Results

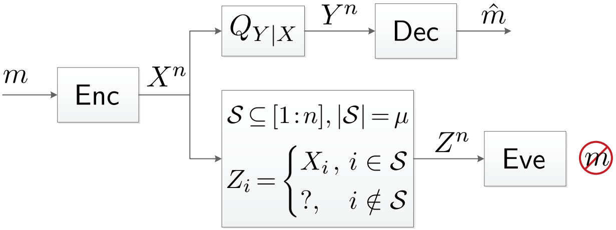
[Ozarow-Wyner 1984]



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

Wiretap Channels of Type II - Past Results

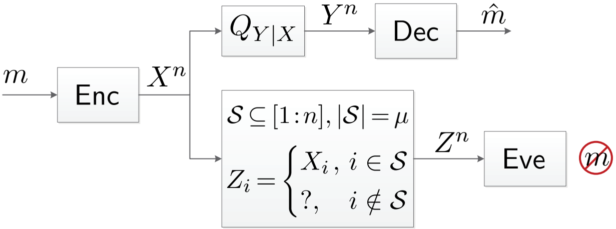
[Ozarow-Wyner 1984]



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

Wiretap Channels of Type II - Past Results

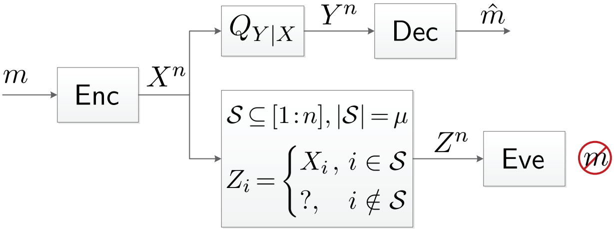
[Ozarow-Wyner 1984]



- **Ozarow-Wyner 1984:** Noiseless main channel
  - Rate equivocation region.
  - Coset coding.
- **Nafea-Yener 2015:** Noisy main channel

Wiretap Channels of Type II - Past Results

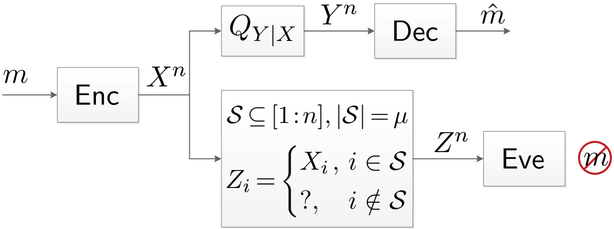
[Ozarow-Wyner 1984]



- **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:

Wiretap Channels of Type II - SS-Capacity

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

Wiretap Channels of Type II - SS-Capacity

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

Theorem

For any $\alpha \in [0,1]$

$$C^{(\mathrm{II})}_{\mathrm{Semantic}}(\alpha) = C^{(\mathrm{II})}_{\mathrm{Weak}}(\alpha) = \max_{Q_{U,X}} \Big[I(U;Y) - \alpha I(U;X) \Big]$$

Wiretap Channels of Type II - SS-Capacity

Semantic Security:

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

Theorem

For any $\alpha \in [0,1]$

$$C^{(\mathrm{II})}_{\mathrm{Semantic}}(\alpha) = C^{(\mathrm{II})}_{\mathrm{Weak}}(\alpha) = \max_{Q_{U,X}} \Big[I(U;Y) - \alpha I(U;X) \Big]$$

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

Wiretap Channels of Type II - SS-Capacity

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

Theorem

For any $\alpha \in [0,1]$

$$C^{(\text{II})}_{\text{Semantic}}(\alpha) = C^{(\text{II})}_{\text{Weak}}(\alpha) = \max_{Q_{U,X}} \Big[I(U;Y) - \alpha I(U;X) \Big]$$

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

Wiretap Channels of Type II - SS-Capacity

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

Theorem

For any $\alpha \in [0,1]$

$$C^{(\mathrm{II})}_{\mathrm{Semantic}}(\alpha) = C^{(\mathrm{II})}_{\mathrm{Weak}}(\alpha) = \max_{Q_{U,X}} \Big[I(U;Y) - \alpha I(U;X)\Big]$$

- RHS is the secrecy-capacity of WTC I with erasure DMC to Eve.
- Standard (erasure) wiretap code & Stronger tools for analysis.
- Practical implementations of binary erasure wiretap codes exist.

WTC II SS-Capacity - Achievability for U=X

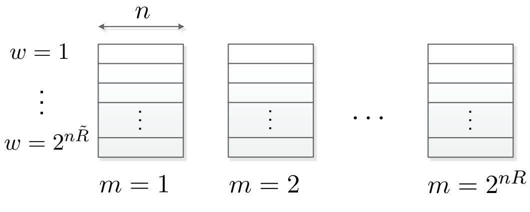
1. **Wiretap Code:**

WTC II SS-Capacity - Achievability for U=X

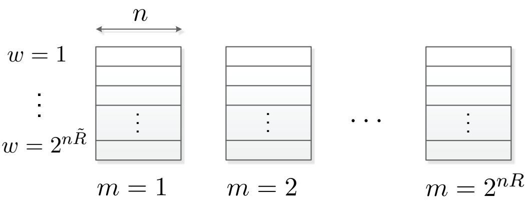
1. **Wiretap Code:**
   - $W \sim \mathsf{Unif}\big[1 : 2^{n\tilde{R}}\big]$.

WTC II SS-Capacity - Achievability for U=X

1. **Wiretap Code:**
   - $W \sim \text{Unif}\big[1 : 2^{n\tilde{R}}\big]$.
   - $\mathbb{C}_n = \big\{X^n(m,w)\big\}_{m,w} \overset{iid}{\sim} Q_X^n$



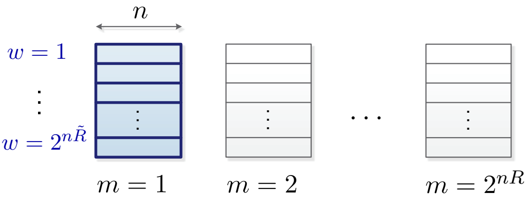
1. **Wiretap Code:**
   - $W \sim \text{Unif}\big[1:2^{n\tilde{R}}\big]$.
   - $\mathbb{C}_n = \big\{X^n(m,w)\big\}_{m,w} \overset{iid}{\sim} Q_X^n$



2. **Preliminary Step:** $\max_{\substack{P_M,\mathcal{S}:\\ |\mathcal{S}|=\mu}} I_{\mathcal{C}_n}(M;Z^n) \leq \max_{\substack{m,\mathcal{S}:\\ |\mathcal{S}|=\mu}} D\Big(P^{(\mathcal{C}_n,\mathcal{S})}_{Z^\mu|M=m}\Big|\Big|Q_Z^\mu\Big)$

WTC II SS-Capacity - Achievability for U=X

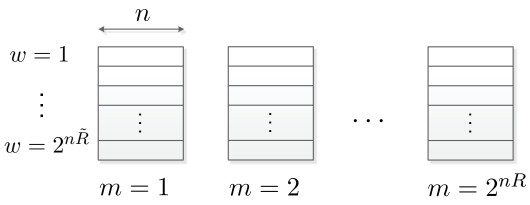
1. **Wiretap Code:**
   - $W \sim \text{Unif}\big[1:2^{n\tilde{R}}\big]$.
   - $\mathbb{C}_n = \big\{X^n(m,w)\big\}_{m,w} \overset{iid}{\sim} Q_X^n$



2. **Preliminary Step:** $\max_{\substack{P_M,\mathcal{S}:\\|\mathcal{S}|=\mu}} I_{\mathcal{C}_n}(M;Z^n) \leq \max_{\substack{m,\mathcal{S}:\\|\mathcal{S}|=\mu}} \boldsymbol{D}\Big(\boldsymbol{P}^{(\mathcal{C}_n,\mathcal{S})}_{Z^\mu|M=m}\Big|\Big|\boldsymbol{Q}^\mu_Z\Big)$

WTC II SS-Capacity - Achievability for U=X

1. **Wiretap Code:**
   - $W \sim \text{Unif}\big[1 : 2^{n\tilde{R}}\big]$.
   - $\mathbb{C}_n = \big\{X^n(m,w)\big\}_{m,w} \overset{iid}{\sim} Q_X^n$

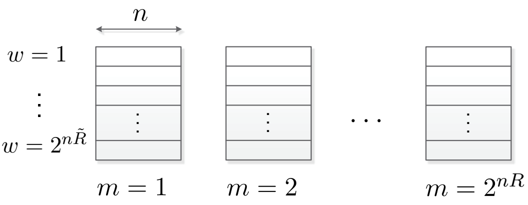


2. **Preliminary Step:** $$\max_{\substack{P_M,\mathcal{S}:\\|\mathcal{S}|=\mu}} I_{\mathcal{C}_n}(M;Z^n) \leq \max_{\substack{m,\mathcal{S}:\\|\mathcal{S}|=\mu}} D\Big(P^{(\mathcal{C}_n,\mathcal{S})}_{Z^\mu|M=m}\Big|\Big|Q_Z^\mu\Big)$$

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

WTC II SS-Capacity - Achievability for U=X

1. **Wiretap Code:**
   - $W \sim \text{Unif}\big[1 : 2^{n\tilde{R}}\big]$.
   - $\mathbb{C}_n = \big\{X^n(m,w)\big\}_{m,w} \overset{iid}{\sim} Q_X^n$



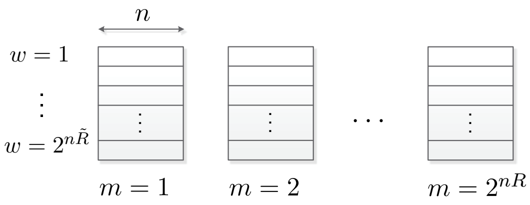
2. **Preliminary Step:** $$\max_{\substack{P_M,\mathcal{S}:\\ |\mathcal{S}|=\mu}} I_{\mathcal{C}_n}(M;Z^n) \leq \max_{\substack{m,\mathcal{S}:\\ |\mathcal{S}|=\mu}} D\left(P^{(\mathcal{C}_n,\mathcal{S})}_{Z^\mu|M=m}\middle|\middle| Q_Z^\mu\right)$$

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

$$\mathbb{P}\left(\left\{\max_{P_M,\mathcal{S}} I_{\mathbb{C}_n}(M;Z^n) \leq e^{-n\gamma_1}\right\}^c\right)$$

WTC II SS-Capacity - Achievability for U=X

1. **Wiretap Code:**
   - $W \sim \text{Unif}\left[1 : 2^{n\tilde{R}}\right]$.
   - $\mathbb{C}_n = \left\{X^n(m,w)\right\}_{m,w} \overset{iid}{\sim} Q_X^n$



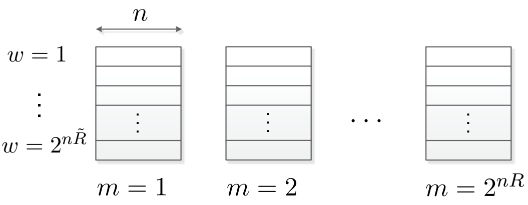
2. **Preliminary Step:** $$\max_{\substack{P_M,\mathcal{S}:\\ |\mathcal{S}|=\mu}} I_{\mathcal{C}_n}(M;Z^n) \leq \max_{\substack{m,\mathcal{S}:\\ |\mathcal{S}|=\mu}} D\left(P_{Z^\mu|M=m}^{(\mathcal{C}_n,\mathcal{S})}\middle|\middle|Q_Z^\mu\right)$$

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

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

WTC II SS-Capacity - Achievability for U=X

1. **Wiretap Code:**
   - $W \sim \text{Unif}\big[1 : 2^{n\tilde{R}}\big]$.
   - $\mathbb{C}_n = \big\{X^n(m,w)\big\}_{m,w} \overset{iid}{\sim} Q_X^n$



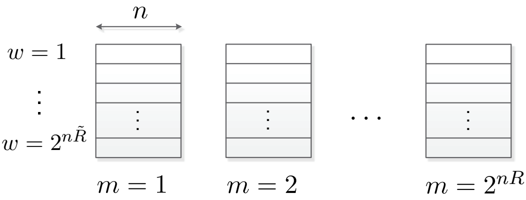
2. **Preliminary Step:** $$\max_{\substack{P_M,\mathcal{S}:\\|\mathcal{S}|=\mu}} I_{\mathcal{C}_n}(M;Z^n) \leq \max_{\substack{m,\mathcal{S}:\\|\mathcal{S}|=\mu}} D\left(P^{(\mathcal{C}_n,\mathcal{S})}_{Z^\mu|M=m}\middle|\middle|Q^\mu_Z\right)$$

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

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

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

1. **Wiretap Code:**
   - $W \sim \text{Unif}\left[1:2^{n\tilde{R}}\right]$.
   - $\mathbb{C}_n = \left\{X^n(m,w)\right\}_{m,w} \overset{iid}{\sim} Q_X^n$



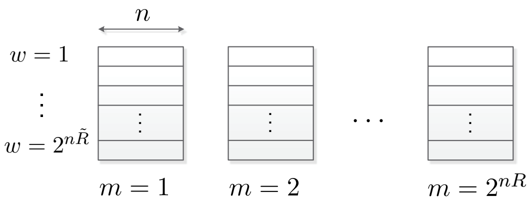
2. **Preliminary Step:** $\max_{\substack{P_M,\mathcal{S}:\\|\mathcal{S}|=\mu}} I_{\mathcal{C}_n}(M;Z^n) \leq \max_{\substack{m,\mathcal{S}:\\|\mathcal{S}|=\mu}} D\left(P^{(\mathcal{C}_n,\mathcal{S})}_{Z^\mu|M=m}\middle|\middle|Q_Z^\mu\right)$

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

$$\mathbb{P}\left(\left\{\max_{P_M,\mathcal{S}} I_{\mathbb{C}_n}(M;Z^n) \leq e^{-n\gamma_1}\right\}^c\right) \leq \mathbb{P}\left(\max_{m,\mathcal{S}} D\left(P^{(\mathcal{C}_n,\mathcal{S})}_{Z^\mu|M=m}\middle|\middle|Q_Z^\mu\right) > e^{-n\gamma_1}\right)$$

$$\leq \sum_{m,\mathcal{S}} \mathbb{P}\left(\boldsymbol{D\left(P^{(\mathcal{C}_n,\mathcal{S})}_{Z^\mu|M=m}\middle|\middle|Q_Z^\mu\right) > e^{-n\gamma_1}}\right)$$

1. **Wiretap Code:**
   - $W \sim \text{Unif}\left[1 : 2^{n\tilde{R}}\right]$.
   - $\mathbb{C}_n = \left\{X^n(m,w)\right\}_{m,w} \overset{iid}{\sim} Q_X^n$



2. **Preliminary Step:** $$\max_{\substack{P_M,\mathcal{S}:\\|\mathcal{S}|=\mu}} I_{\mathcal{C}_n}(M;Z^n) \leq \max_{\substack{m,\mathcal{S}:\\|\mathcal{S}|=\mu}} D\left(P^{(\mathcal{C}_n,\mathcal{S})}_{Z^\mu|M=m}\middle|\middle|Q_Z^\mu\right)$$

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

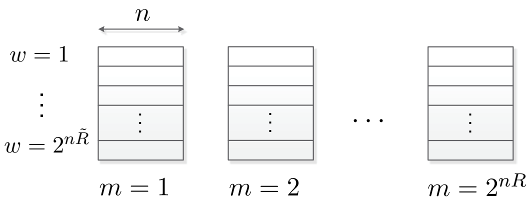
$$\mathbb{P}\left(\left\{\max_{P_M,\mathcal{S}} I_{\mathbb{C}_n}(M;Z^n) \leq e^{-n\gamma_1}\right\}^c\right) \leq \mathbb{P}\left(\max_{m,\mathcal{S}} D\left(P^{(\mathcal{C}_n,\mathcal{S})}_{Z^\mu|M=m}\middle|\middle|Q_Z^\mu\right) > e^{-n\gamma_1}\right)$$

$$\leq \sum_{m,\mathcal{S}} \mathbb{P}\left(D\left(P^{(\mathcal{C}_n,\mathcal{S})}_{Z^\mu|M=m}\middle|\middle|Q_Z^\mu\right) > e^{-n\gamma_1}\right)$$

Taking $\boxed{\tilde{R} > \alpha H(X)}$ $\implies$

WTC II SS-Capacity - Achievability for U=X

1. **Wiretap Code:**
   - $W \sim \text{Unif}\big[1:2^{n\tilde{R}}\big]$.
   - $\mathbb{C}_n = \big\{X^n(m,w)\big\}_{m,w} \overset{iid}{\sim} Q_X^n$



2. **Preliminary Step:** $$\max_{\substack{P_M,\mathcal{S}:\\|\mathcal{S}|=\mu}} I_{\mathcal{C}_n}(M;Z^n) \leq \max_{\substack{m,\mathcal{S}:\\|\mathcal{S}|=\mu}} D\Big(P^{(\mathcal{C}_n,\mathcal{S})}_{Z^\mu|M=m}\Big|\Big|Q_Z^\mu\Big)$$

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

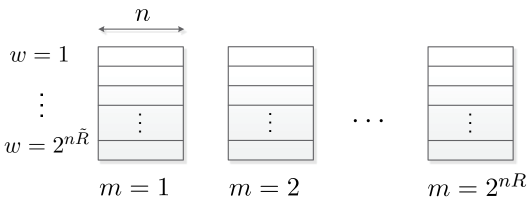
$$\mathbb{P}\bigg(\Big\{\max_{P_M,\mathcal{S}} I_{\mathbb{C}_n}(M;Z^n) \leq e^{-n\gamma_1}\Big\}^c\bigg) \leq \mathbb{P}\bigg(\max_{m,\mathcal{S}} D\Big(P^{(\mathcal{C}_n,\mathcal{S})}_{Z^\mu|M=m}\Big|\Big|Q_Z^\mu\Big) > e^{-n\gamma_1}\bigg)$$

$$\leq \sum_{m,\mathcal{S}} \mathbb{P}\bigg(D\Big(P^{(\mathcal{C}_n,\mathcal{S})}_{Z^\mu|M=m}\Big|\Big|Q_Z^\mu\Big) > e^{-n\gamma_1}\bigg)$$

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

WTC II SS-Capacity - Achievability for U=X

1. **Wiretap Code:**
   - $W \sim \text{Unif}\big[1 : 2^{n\tilde{R}}\big]$.
   - $\mathbb{C}_n = \big\{X^n(m,w)\big\}_{m,w} \overset{iid}{\sim} Q_X^n$



2. **Preliminary Step:**

$$\max_{\substack{P_M,\mathcal{S}:\\ |\mathcal{S}|=\mu}} I_{\mathcal{C}_n}(M;Z^n) \leq \max_{\substack{m,\mathcal{S}:\\ |\mathcal{S}|=\mu}} D\left(P^{(\mathcal{C}_n,\mathcal{S})}_{Z^\mu|M=m}\middle|\middle|Q_Z^\mu\right)$$

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

$$\mathbb{P}\left(\left\{\max_{P_M,\mathcal{S}} I_{\mathbb{C}_n}(M;Z^n) \leq e^{-n\gamma_1}\right\}^c\right) \leq \mathbb{P}\left(\max_{m,\mathcal{S}} D\left(P^{(\mathcal{C}_n,\mathcal{S})}_{Z^\mu|M=m}\middle|\middle|Q_Z^\mu\right) > e^{-n\gamma_1}\right)$$

$$\leq \sum_{m,\mathcal{S}} \mathbb{P}\left(D\left(P^{(\mathcal{C}_n,\mathcal{S})}_{Z^\mu|M=m}\middle|\middle|Q_Z^\mu\right) > e^{-n\gamma_1}\right)$$

Taking $\boxed{\tilde{R} > \alpha H(X)}$ $\implies \leq 2^n 2^{nR} e^{-e^{n\gamma_2}} \xrightarrow[n\to\infty]{} 0$

WTC II SS-Capacity - Converse

SS-capacity WTC II $\leq$ Weak-secrecy-capacity WTC I

WTC II SS-Capacity - Converse

SS-capacity WTC II $\leq$ Weak-secrecy-capacity WTC I

- **WTC I** with erasure DMC to Eve - Transition probability α.

WTC II SS-Capacity - Converse

SS-capacity WTC II $\leq$ Weak-secrecy-capacity WTC I

- **WTC I** with erasure DMC to Eve - Transition probability α.

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

WTC II SS-Capacity - Converse

SS-capacity WTC II $\leq$ Weak-secrecy-capacity WTC I

- **WTC I** with erasure DMC to Eve - Transition probability α.

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

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

Summary

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

Summary

- **Semantic Security:** [Bellare-Tessaro-Vardy 2012]
  - Gold standard in cryptography - relevant for applications.

Summary

- **Semantic Security:** [Bellare-Tessaro-Vardy 2012]
  - Gold standard in cryptography - relevant for applications.
  - Equivalent to vanishing inf. leakage for all P_M.

Summary

- **Semantic Security:** [Bellare-Tessaro-Vardy 2012]
  - Gold standard in cryptography - relevant for applications.
  - Equivalent to vanishing inf. leakage for all P_M.

- **Stronger Soft-Covering Lemma:**

Summary

- **Semantic Security:** [Bellare-Tessaro-Vardy 2012]
  - Gold standard in cryptography - relevant for applications.
  - Equivalent to vanishing inf. leakage for all P_M.
- **Stronger Soft-Covering Lemma:**
  - Double-exponential decay of prob. of soft-covering not happening.

Summary

- **Semantic Security:** [Bellare-Tessaro-Vardy 2012]
  - Gold standard in cryptography - relevant for applications.
  - Equivalent to vanishing inf. leakage for all P_M.
- **Stronger Soft-Covering Lemma:**
  - Double-exponential decay of prob. of soft-covering not happening.
  - Satisfy exponentially many soft-covering constraints.

Summary

- **Semantic Security:** [Bellare-Tessaro-Vardy 2012]
  - Gold standard in cryptography - relevant for applications.
  - Equivalent to vanishing inf. leakage for all P_M.
- **Stronger Soft-Covering Lemma:**
  - Double-exponential decay of prob. of soft-covering not happening.
  - Satisfy exponentially many soft-covering constraints.
- **Wiretap Channel II:** Noisy Main Channel

Summary

- **Semantic Security:** [Bellare-Tessaro-Vardy 2012]
  - Gold standard in cryptography - relevant for applications.
  - Equivalent to vanishing inf. leakage for all P_M.
- **Stronger Soft-Covering Lemma:**
  - Double-exponential decay of prob. of soft-covering not happening.
  - Satisfy exponentially many soft-covering constraints.
- **Wiretap Channel II:** Noisy Main Channel
  - Derivation of SS-capacity & Equality to weak-secrecy-capacity.

Summary

- **Semantic Security:** [Bellare-Tessaro-Vardy 2012]
  - Gold standard in cryptography - relevant for applications.
  - Equivalent to vanishing inf. leakage for all P_M.
- **Stronger Soft-Covering Lemma:**
  - Double-exponential decay of prob. of soft-covering not happening.
  - Satisfy exponentially many soft-covering constraints.
- **Wiretap Channel II:** Noisy Main Channel
  - Derivation of SS-capacity & Equality to weak-secrecy-capacity.
  - Classic erasure wiretap codes achieve SS-capacity.

Summary

- **Semantic Security:** [Bellare-Tessaro-Vardy 2012]
  - Gold standard in cryptography - relevant for applications.
  - Equivalent to vanishing inf. leakage for all P_M.
- **Stronger Soft-Covering Lemma:**
  - Double-exponential decay of prob. of soft-covering not happening.
  - Satisfy exponentially many soft-covering constraints.
- **Wiretap Channel II:** Noisy Main Channel
  - Derivation of SS-capacity & Equality to weak-secrecy-capacity.
  - Classic erasure wiretap codes achieve SS-capacity.

Thank You!