Semantic-Security Capacity for Wiretap Channels of Type II

Ziv Goldfeld, Paul Cuff and Haim Permuter

Ben-Gurion University and Princeton University

IEEE International Symposium on Information Theory 2016

July 15th, 2016

Motivation

Information Theoretic Security over Noisy Channels

Information Theoretic Security over Noisy Channels

Pros:

Motivation

Information Theoretic Security over Noisy Channels

Pros:

1. Security versus **computationally unlimited** eavesdropper.

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:

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**.

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**.

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:

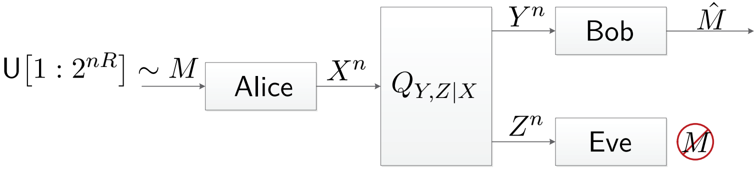
1. Eve's channel assumed to be **fully known**.
2. Security metrics **insufficient for (some) applications**.

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

Wiretap Channels - Security Metrics

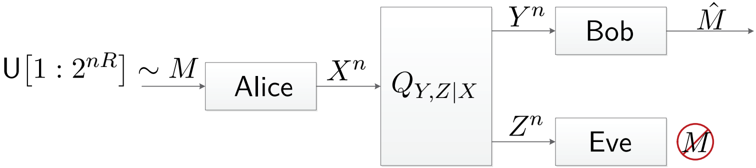
Wiretap Channels and Security Metrics

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



Wiretap Channels and Security Metrics

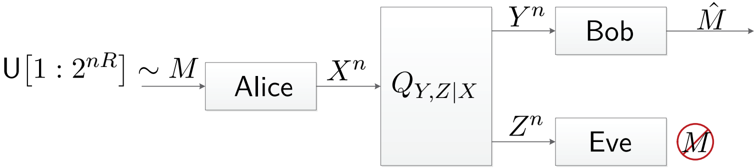
Degraded [Wyner 1975], General [Csiszár-Körner 1978]



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

Wiretap Channels and Security Metrics

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

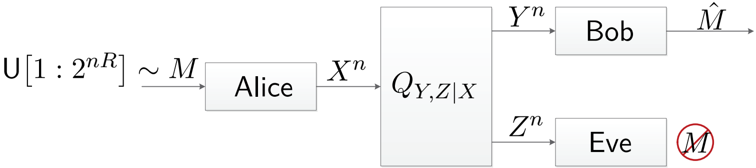


$\{\mathcal{C}_n\}_{n\in\mathbb{N}}$ - a sequence of (n,R)-codes

- **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]

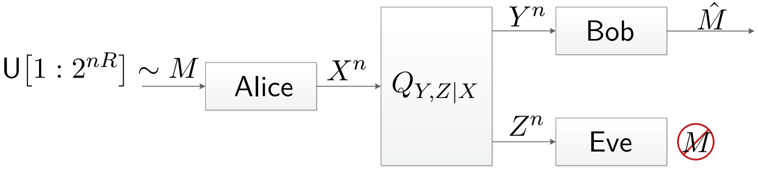


$\{\mathcal{C}_n\}_{n\in\mathbb{N}}$ - a sequence of (n, R)-codes

- **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]

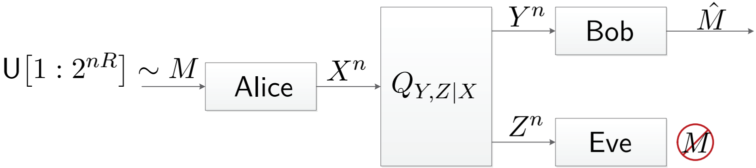


$\{\mathcal{C}_n\}_{n\in\mathbb{N}}$ - a sequence of (n,R)-codes

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

Wiretap Channels and Security Metrics

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

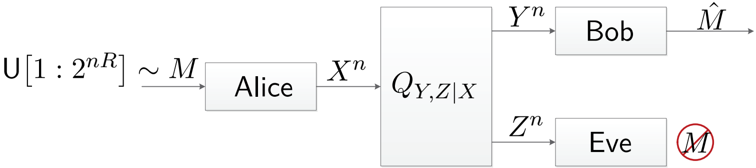


$\{\mathcal{C}_n\}_{n\in\mathbb{N}}$ - a sequence of (n,R)-codes

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

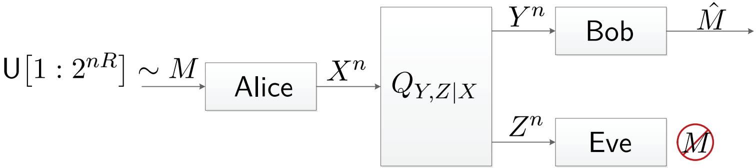


$\{\mathcal{C}_n\}_{n\in\mathbb{N}}$ - a sequence of (n,R)-codes

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

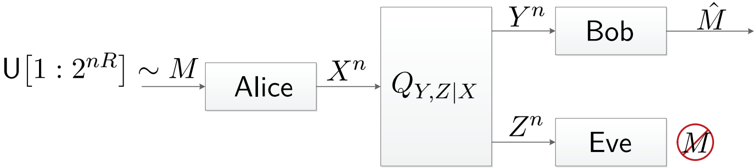


$\{\mathcal{C}_n\}_{n\in\mathbb{N}}$ - a sequence of (n, R)-codes

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

Wiretap Channels and Security Metrics

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

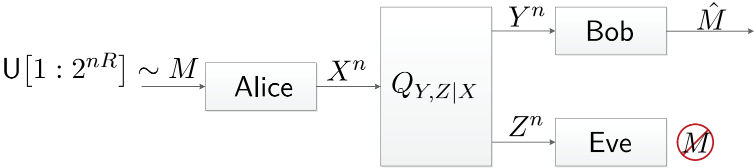


$\{\mathcal{C}_n\}_{n\in\mathbb{N}}$ - a sequence of (n,R)-codes

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

Wiretap Channels and Security Metrics

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



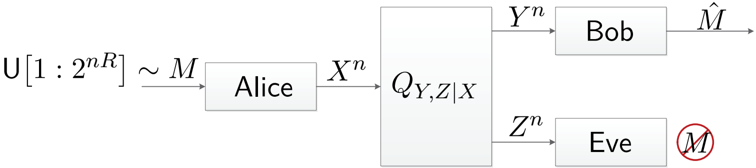
$\{\mathcal{C}_n\}_{n\in\mathbb{N}}$ - a sequence of (n, R)-codes

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

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

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

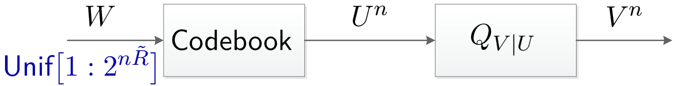
- **Weak-Secrecy:** $\cancel{\frac{1}{n} I_{\mathcal{C}_n}(M;Z^n) \xrightarrow[n\to\infty]{} 0}.$
- **Strong-Secrecy:** $\cancel{I_{\mathcal{C}_n}(M;Z^n) \xrightarrow[n\to\infty]{} 0}.$
- **Semantic Security:** [Bellare-Tessaro-Vardy 2012]

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

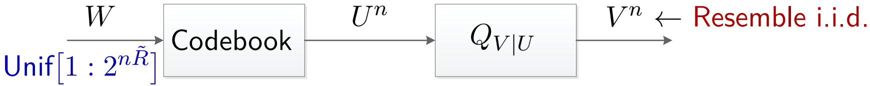
⋆ A single code that satisfied exponentially many secrecy constraints ⋆

A Stronger Soft-Covering Lemma

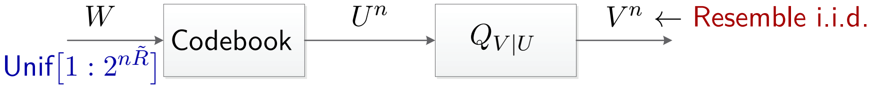
Soft-Covering - Setup



Soft-Covering - Setup

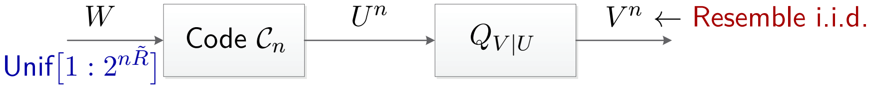


Soft-Covering - Setup



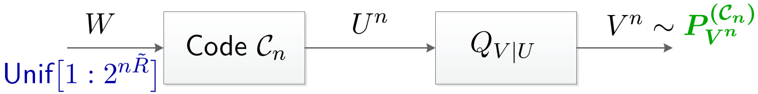
- **Random Codebook:** $\mathbb{C}_n = \{U^n(w)\}_w \overset{iid}{\sim} Q_U^n$.

Soft-Covering - Setup



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

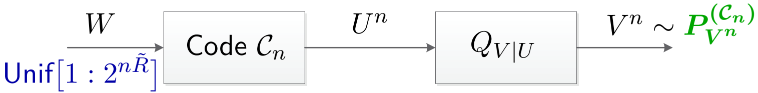
Soft-Covering - Setup



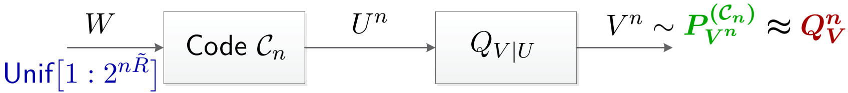
- **Random Codebook:** $\mathbb{C}_n = \{U^n(w)\}_w \overset{iid}{\sim} Q_U^n$.

- **Induced Output Distribution:** Codebook $\mathcal{C}_n \implies V^n \sim P_{V^n}^{(\mathcal{C}_n)}$.

Soft-Covering - Setup

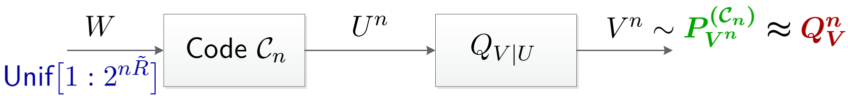


- **Random Codebook:** $\mathbb{C}_n = \{U^n(w)\}_w \overset{iid}{\sim} Q_U^n$.
- **Induced Output Distribution:** Codebook $\mathcal{C}_n \implies V^n \sim P_{V^n}^{(\mathcal{C}_n)}$.
- **Target IID Distribution:** Q_V^n marginal of $Q_U^n Q_{V|U}^n$.



- **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 $Q_U^n Q_{V|U}^n$.

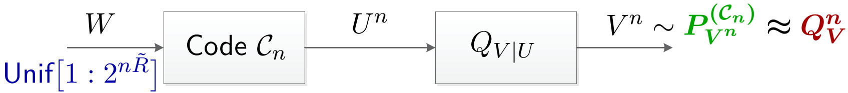
Soft-Covering - Setup



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

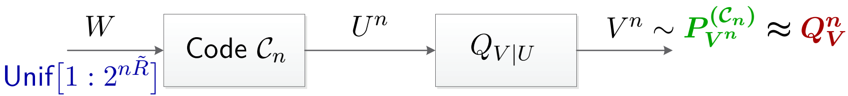
⋆ **Goal:** Choose $\tilde{R}$ (codebook size) s.t. $P_{V^n}^{(\mathcal{C}_n)} \approx Q_V^n$ ⋆

Soft-Covering - Results



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

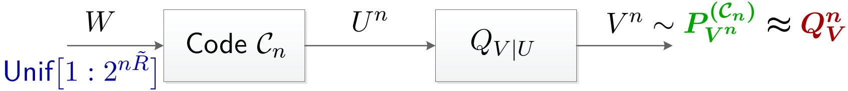
Soft-Covering - Results



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

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

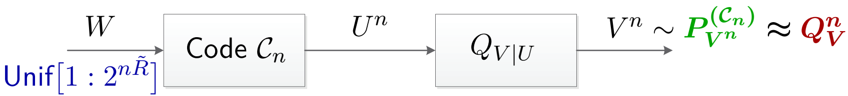
Soft-Covering - Results



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

- **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**: $\mathbb{E}_{\mathbb{C}_n} \left|\left| P_{V^n}^{(\mathbb{C}_n)} - Q_V^n \right|\right|_{\mathrm{TV}} \xrightarrow[n\to\infty]{} 0.$

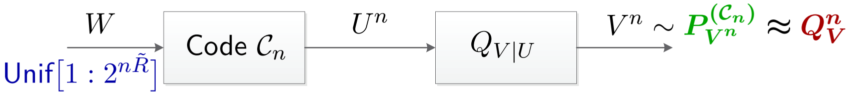
Soft-Covering - Results



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

- **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.

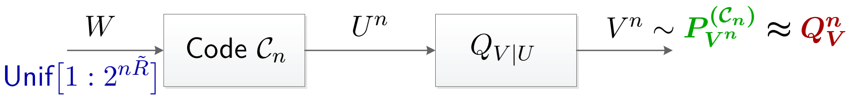
Soft-Covering - Results



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

- **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



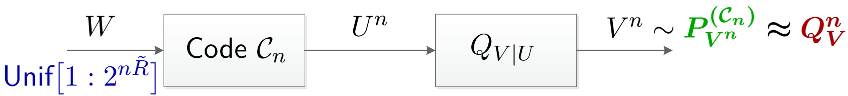
Theorem (Cuff 2015, ZG-Cuff-Permuter 2016)

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.*

A Stronger Soft-Covering Lemma



Theorem (Cuff 2015, ZG-Cuff-Permuter 2016)

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

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

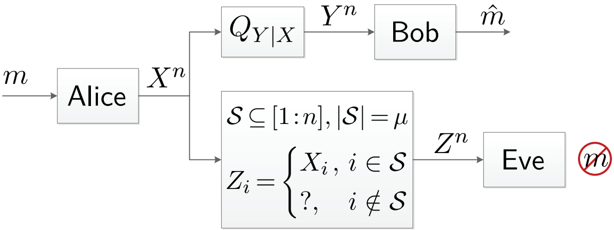
for n *sufficiently large.*

- **More on the stronger SCL:** Paul Cuff on Fr-PM-1-7 at 15:50.

Wiretap Channels of Type II

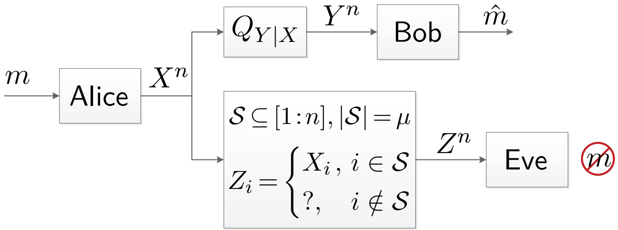
Wiretap Channels of Type II - Definition

[Ozarow-Wyner 1984]



Wiretap Channels of Type II - Definition

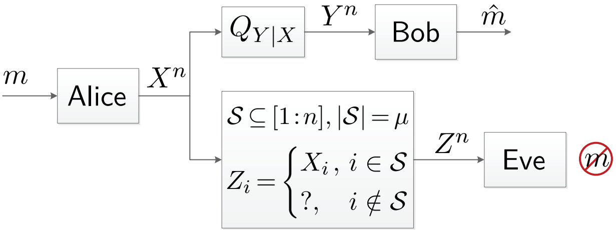
[Ozarow-Wyner 1984]



- **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.

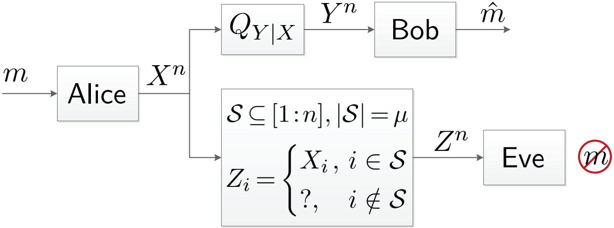
- **Transmitted:**

0	0	1	0	1	1	1	0	1	0

$n = 10$ $\quad \boldsymbol{\alpha = 0.6}$

Wiretap Channels of Type II - Definition

[Ozarow-Wyner 1984]



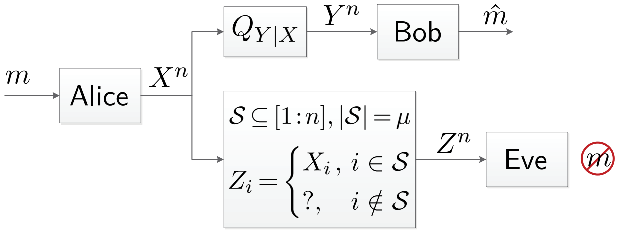
- **Eavesdropper:** Can observe a subset $\mathcal{S} \subseteq [1:n]$ of size $\mu = \lfloor \alpha n \rfloor$, $\alpha \in [0, 1]$, of transmitted symbols.

- **Transmitted:** $n = 10$ $\alpha = 0.6$
- **Observed:**

Transmitted:	0	0	1	0	1	1	1	0	1	0
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.

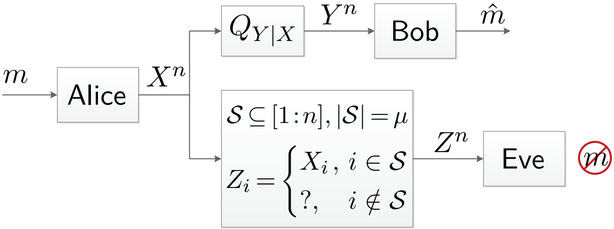
Transmitted:	0	0	1	0	1	1	1	0	1	0
Observed:	?	0	?	?	1	1	1	?	1	0

$n = 10$ $\quad \boldsymbol{\alpha = 0.6}$

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

Wiretap Channels of Type II - Past Results

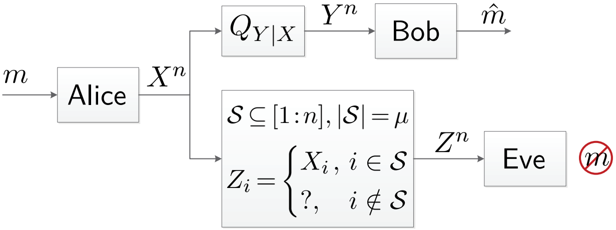
[Ozarow-Wyner 1984]



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

Wiretap Channels of Type II - Past Results

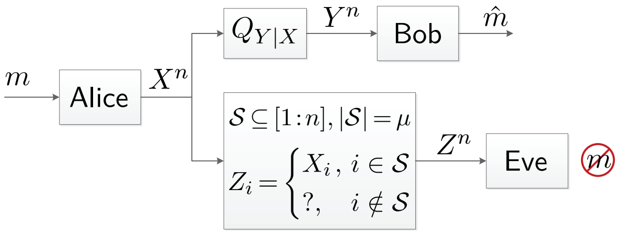
[Ozarow-Wyner 1984]



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

Wiretap Channels of Type II - Past Results

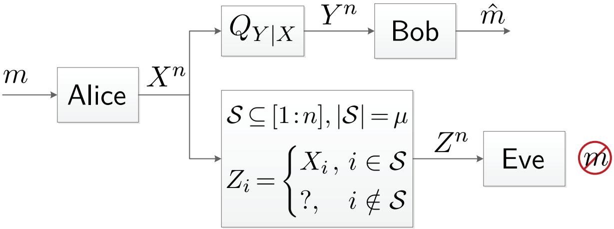
[Ozarow-Wyner 1984]



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

Wiretap Channels of Type II - Past Results

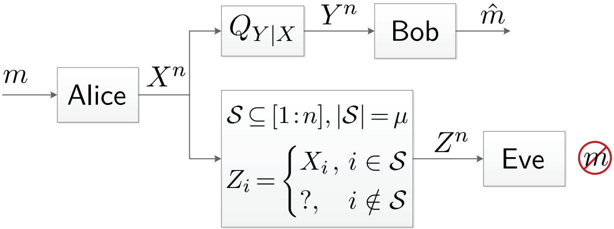
[Ozarow-Wyner 1984]



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

- **Nafea-Yener 2015:** Noisy main channel

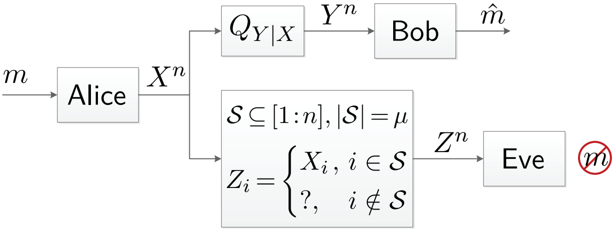
Wiretap Channels of Type II - Past Results
[Ozarow-Wyner 1984]



- **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 $\alpha \in [0,1]$

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

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

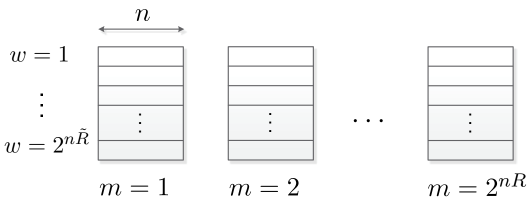
WTC II SS-Capacity - Security Analysis

1. **Wiretap Code:**

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

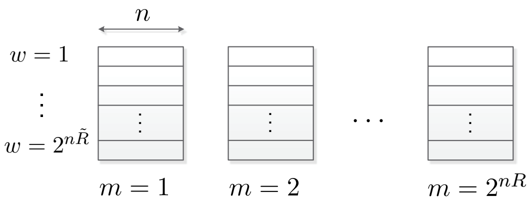
WTC II SS-Capacity - Security Analysis

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



WTC II SS-Capacity - Security Analysis

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

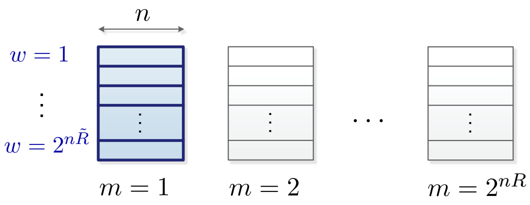


2. **Preliminary Step:**

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

WTC II SS-Capacity - Security Analysis

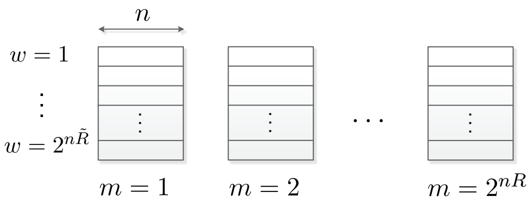
1. **Wiretap Code:**
   - $W \sim \mathsf{Unif}\big[1:2^{n\tilde{R}}\big]$.
   - $\mathbb{C}_n = \big\{X^n(m,w)\big\}_{m,w} \overset{iid}{\sim} Q_X^n$



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

WTC II SS-Capacity - Security Analysis

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



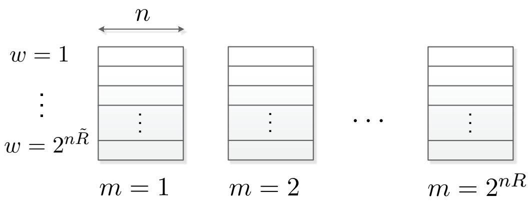
2. **Preliminary Step:**

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

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

WTC II SS-Capacity - Security Analysis

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



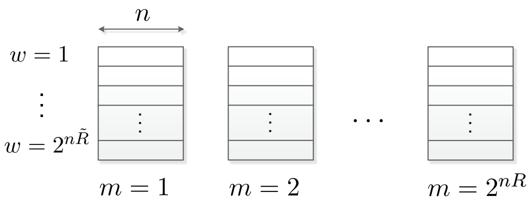
2. **Preliminary Step:** $$\max_{\substack{P_M,\mathcal{S}:\\|\mathcal{S}|=\mu}} I_{\mathcal{C}_n}(M;Z^n) \leq \max_{\substack{m,\mathcal{S}:\\|\mathcal{S}|=\mu}} D\left(P^{(\mathcal{C}_n,\mathcal{S})}_{Z^\mu|M=m}\middle|\middle|Q_Z^\mu\right)$$

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

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

WTC II SS-Capacity - Security Analysis

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

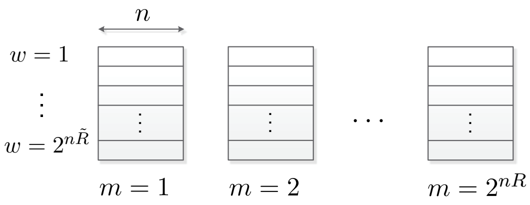


2. **Preliminary Step:**
$$\max_{\substack{P_M,\mathcal{S}:\\ |\mathcal{S}|=\mu}} I_{\mathcal{C}_n}(M;Z^n) \leq \max_{\substack{m,\mathcal{S}:\\ |\mathcal{S}|=\mu}} D\left(P^{(\mathcal{C}_n,\mathcal{S})}_{Z^\mu|M=m}\middle|\middle| Q_Z^\mu\right)$$

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

WTC II SS-Capacity - Security Analysis

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



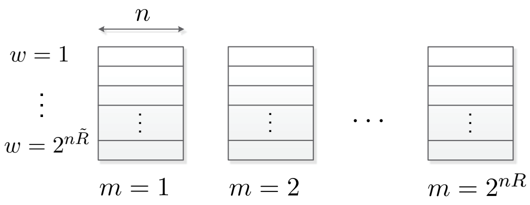
2. **Preliminary Step:** $$\max_{\substack{P_M, \mathcal{S}: \\ |\mathcal{S}|=\mu}} I_{\mathcal{C}_n}(M;Z^n) \leq \max_{\substack{m, \mathcal{S}: \\ |\mathcal{S}|=\mu}} D\left(P^{(\mathcal{C}_n,\mathcal{S})}_{Z^\mu|M=m} \middle|\middle| Q_Z^\mu\right)$$

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

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

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

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:**

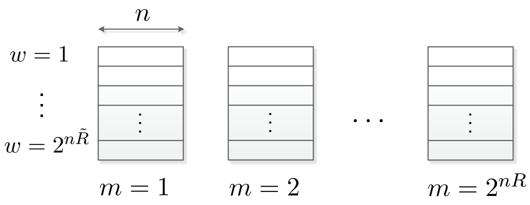
$$\max_{\substack{P_M,\mathcal{S}:\\ |\mathcal{S}|=\mu}} I_{\mathcal{C}_n}(M;Z^n) \leq \max_{\substack{m,\mathcal{S}:\\ |\mathcal{S}|=\mu}} D\Big(P_{Z^\mu|M=m}^{(\mathcal{C}_n,\mathcal{S})}\Big|\Big|Q_Z^\mu\Big)$$

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

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

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

WTC II SS-Capacity - Security Analysis



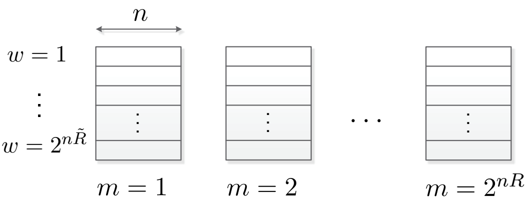
1. **Wiretap Code:**
   - $W\sim$ Unif$\left[1:2^{n\tilde{R}}\right]$.
   - $\mathbb{C}_n=\left\{X^n(m,w)\right\}_{m,w}\overset{iid}{\sim}Q_X^n$
2. **Preliminary Step:** $\max\limits_{\substack{P_M,\mathcal{S}:\\|\mathcal{S}|=\mu}} I_{\mathcal{C}_n}(M;Z^n)\leq\max\limits_{\substack{m,\mathcal{S}:\\|\mathcal{S}|=\mu}} D\left(P^{(\mathcal{C}_n,\mathcal{S})}_{Z^\mu|M=m}\middle|\middle|Q_Z^\mu\right)$
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 $\boxed{\tilde{R}>\alpha H(X)}$ $\Longrightarrow$

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

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

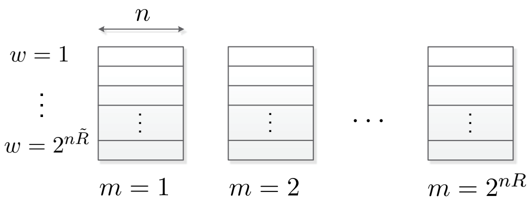
$$\mathbb{P}\left(\left\{\max_{P_M,\mathcal{S}} I_{\mathbb{C}_n}(M;Z^n) \leq e^{-n\gamma_1}\right\}^c\right) \leq \mathbb{P}\left(\max_{m,\mathcal{S}} D\left(P^{(\mathcal{C}_n,\mathcal{S})}_{Z^\mu|M=m}\middle|\middle|Q_Z^\mu\right) > e^{-n\gamma_1}\right)$$

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

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

WTC II SS-Capacity - Security Analysis

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



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

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

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

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

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

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.

- **Stronger Soft-Covering Lemma:**

Summary

- **Semantic Security:** [Bellare-Tessaro-Vardy 2012]
  - Cryptographic benchmark - relevant for applications.
- **Stronger Soft-Covering Lemma:**
  - Codes that satisfy exponentially many secrecy constraints.

Summary

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

Summary

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

WTC II SS-Capacity - Achievability Outline $U = X$

7. **Finalization:**

7. **Finalization:**

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

WTC II SS-Capacity - Achievability Outline $U = X$

7. **Finalization:**

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

WTC II SS-Capacity - Achievability Outline $U = X$

7. **Finalization:**
   - **Semantic Security:** Ensured if $\tilde{R} > \alpha H(X)$.
   - **Reliability:** Successfully decode (M, W) if $R + \tilde{R} < I(X;Y)$.

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

WTC II SS-Capacity - Achievability Outline $U = X$

7. **Finalization:**

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

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

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

$\square$

WTC II SS-Capacity - Converse

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

WTC II SS-Capacity - Converse

$$\boxed{\textbf{SS-capacity WTC II} \ \leq \ \textbf{Weak-secrecy-capacity WTC I}}$$

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

WTC II SS-Capacity - Converse

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

- **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

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

- **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.