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

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.

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 **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**.

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**.

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:

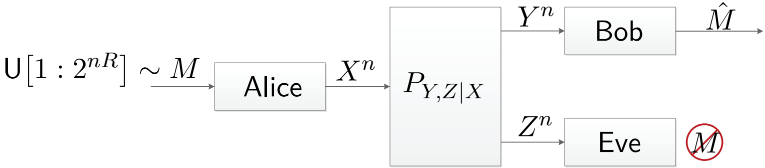
1. Eve's channel assumed to be **fully known**.
2. Security metrics **insufficient for (some) applications**.

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

Wiretap Channels - Security Metrics

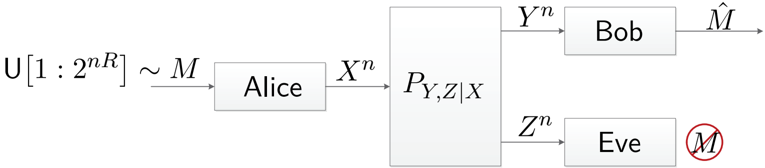
Wiretap Channels and Security Metrics

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



Wiretap Channels and Security Metrics

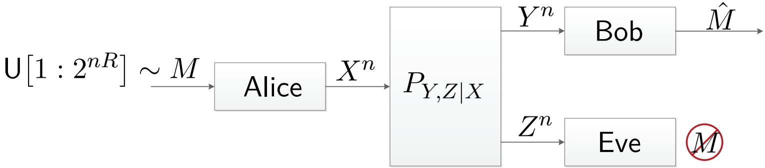
Degraded [Wyner 1975], General [Csiszár-Körner 1978]



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

Wiretap Channels and Security Metrics

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

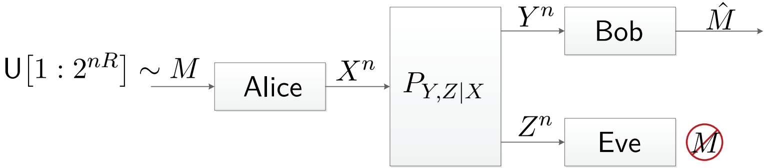


$\{\mathcal{C}_n\}_{n\in\mathbb{N}}$ - a sequence of (n,R)-codes

- **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]

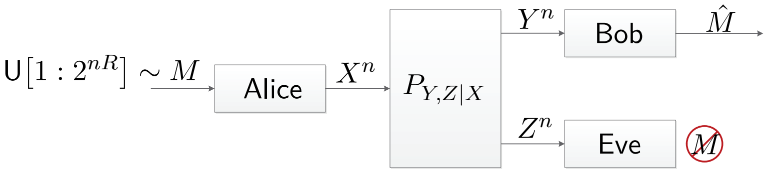


$\{\mathcal{C}_n\}_{n\in\mathbb{N}}$ - a sequence of (n,R)-codes

- **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]

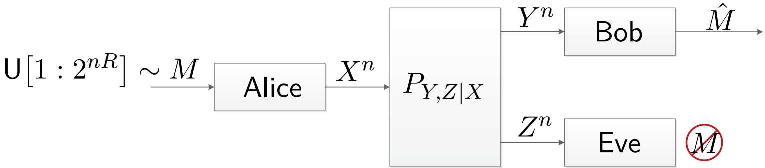


$\{\mathcal{C}_n\}_{n\in\mathbb{N}}$ - a sequence of (n, R)-codes

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

Wiretap Channels and Security Metrics

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

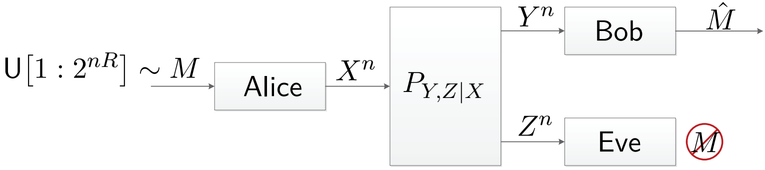


$\{\mathcal{C}_n\}_{n\in\mathbb{N}}$ - a sequence of (n,R)-codes

- **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]

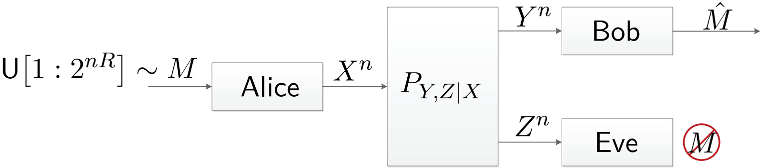


$\{\mathcal{C}_n\}_{n\in\mathbb{N}}$ - a sequence of (n, R)-codes

- **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]

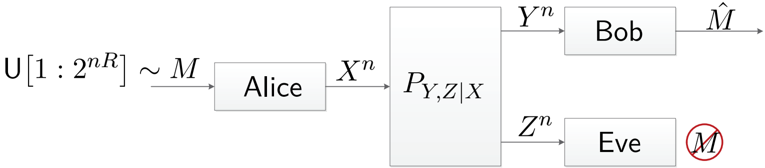


$\{\mathcal{C}_n\}_{n\in\mathbb{N}}$ - a sequence of (n,R)-codes

- **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]

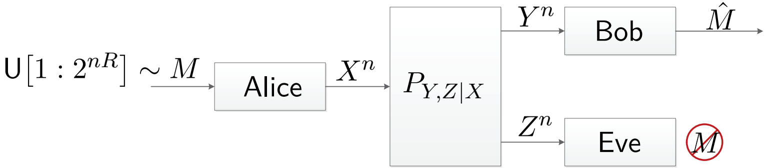


$\{\mathcal{C}_n\}_{n\in\mathbb{N}}$ - a sequence of (n,R)-codes

- **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:**

Wiretap Channels and Security Metrics

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



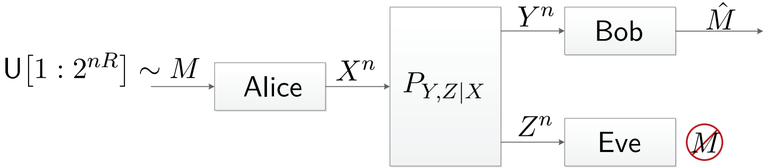
$\{\mathcal{C}_n\}_{n\in\mathbb{N}}$ - a sequence of (n, R)-codes

- **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:** [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

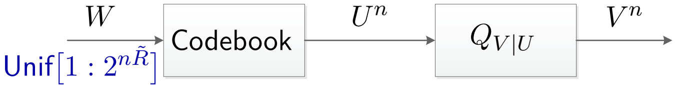
- **Weak-Secrecy:** $\frac{1}{n}I_{\mathcal{C}_n}(M;Z^n)\xrightarrow[n\to\infty]{}0.$
- **Strong-Secrecy:** $I_{\mathcal{C}_n}(M;Z^n)\xrightarrow[n\to\infty]{}0.$
- **Semantic Security:** [Bellare-Tessaro-Vardy 2012]

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

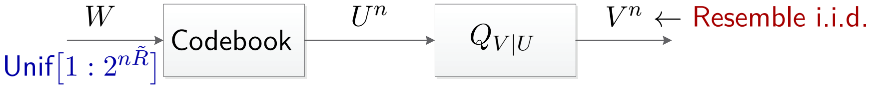
⋆ A single code that satisfied exponentially many secrecy constraints ⋆

Strong Soft-Covering Lemma

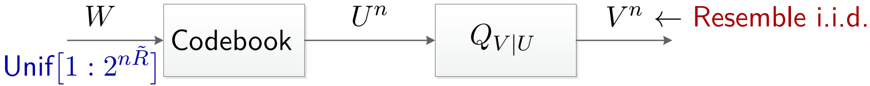
Soft-Covering - Setup



Soft-Covering - Setup

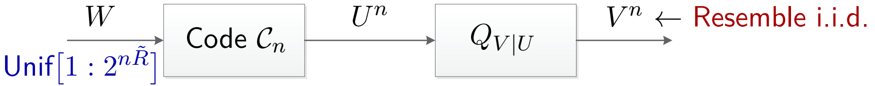


Soft-Covering - Setup

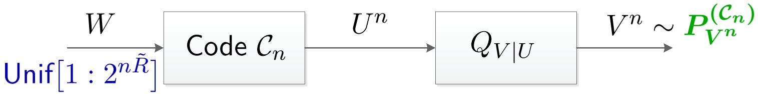


- **Random Codebook:** $\mathsf{C}_n = \left\{U^n(w)\right\}_w \overset{iid}{\sim} Q_U^n$.

Soft-Covering - Setup



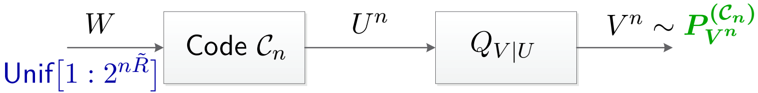
- **Random Codebook:** $\mathsf{C}_n = \{U^n(w)\}_w \overset{iid}{\sim} Q_U^n$.



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

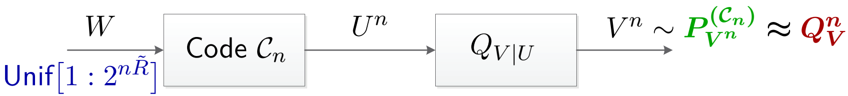
- **Induced Output Distribution:** Codebook $\mathcal{C}_n \implies V^n \sim \boldsymbol{P_{V^n}^{(\mathcal{C}_n)}}$.

Soft-Covering - Setup



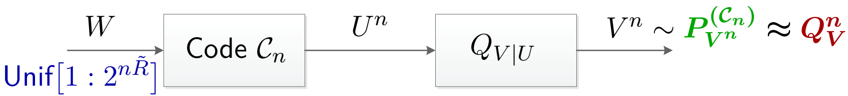
- **Random Codebook:** $\mathsf{C}_n = \{U^n(w)\}_w \overset{iid}{\sim} Q_U^n$.
- **Induced Output Distribution:** Codebook $\mathcal{C}_n \implies V^n \sim P_{V^n}^{(\mathcal{C}_n)}$.
- **Target IID Distribution:** Q_V^n marginal of $Q_U^n Q_{V|U}^n$.

Soft-Covering - Setup



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

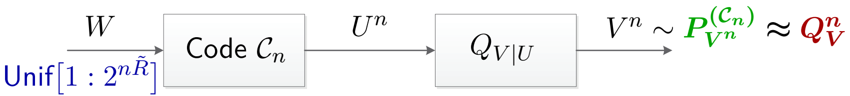
Soft-Covering - Setup



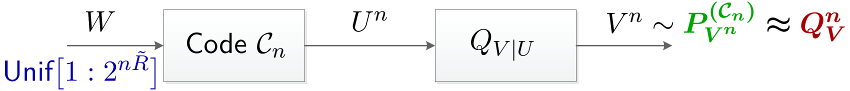
- **Random Codebook:** $\mathsf{C}_n = \{U^n(w)\}_w \overset{iid}{\sim} Q_U^n$.
- **Induced Output Distribution:** Codebook $\mathcal{C}_n \implies V^n \sim P_{V^n}^{(\mathcal{C}_n)}$.
- **Target IID Distribution:** Q_V^n marginal of $Q_U^n Q_{V|U}^n$.

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

Soft-Covering - Results



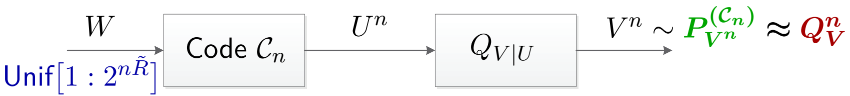
$$\tilde{R} > I_Q(U;V) \implies P_{V^n}^{(\mathcal{C}_n)} \approx Q_V^n$$



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

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

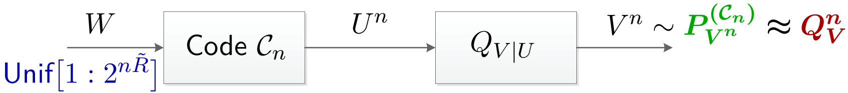
Soft-Covering - Results



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

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

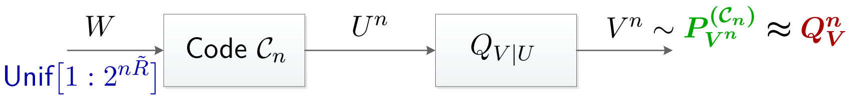
Soft-Covering - Results



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

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

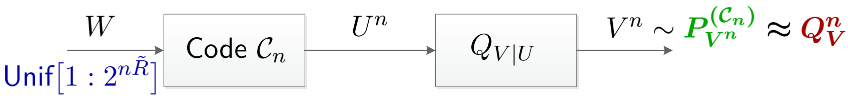
Soft-Covering - Results



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

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

Strong 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.*

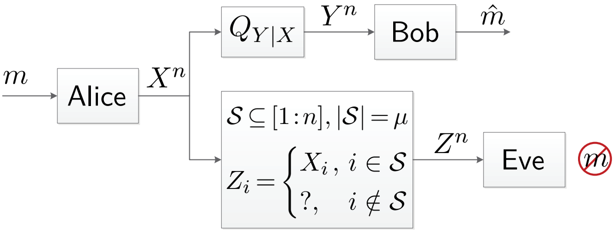
$$\mathbb{P}_{\mathsf{C}_n}\left(D\left(P_{V^n}^{(\mathsf{C}_n)} \middle\| Q_V^n\right) > e^{-n\gamma_1}\right) \leq e^{-e^{n\gamma_2}}$$

for n *sufficiently large.*

Wiretap Channels of Type II

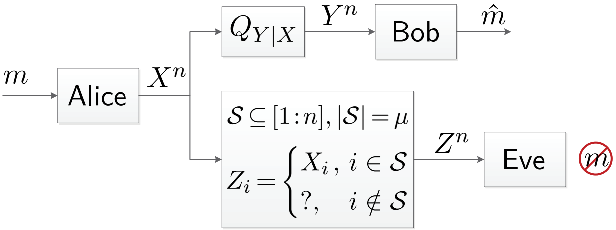
Wiretap Channels of Type II - Definition

[Ozarow-Wyner 1984]



Wiretap Channels of Type II - Definition

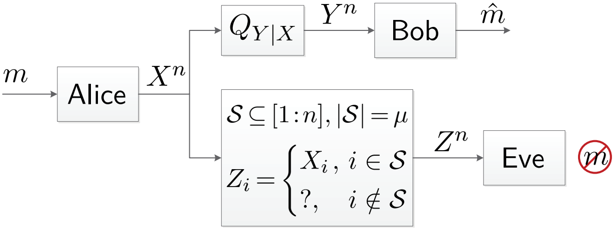
[Ozarow-Wyner 1984]



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

Wiretap Channels of Type II - Definition

[Ozarow-Wyner 1984]



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

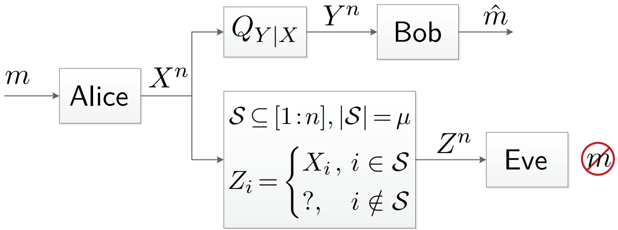
- **Transmitted:**

0	0	1	0	1	1	1	0	1	0

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

Wiretap Channels of Type II - Definition

[Ozarow-Wyner 1984]



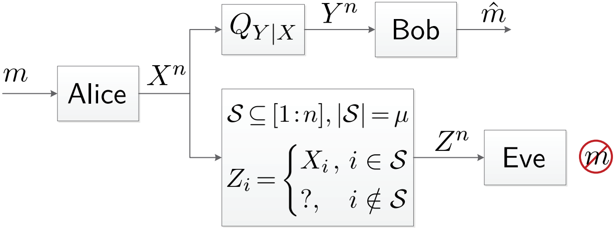
- **Eavesdropper:** Can observe a subset $\mathcal{S} \subseteq [1:n]$ of size $\mu = \lfloor \alpha n \rfloor$, $\alpha \in [0,1]$, of transmitted symbols.

$n = 10$ $\alpha = 0.6$

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 $\mathcal{S} \subseteq [1:n]$ of size $\mu = \lfloor \alpha n \rfloor$, $\alpha \in [0, 1]$, of transmitted symbols.

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

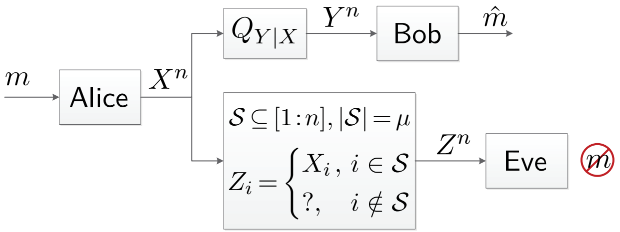
Transmitted:	0	0	1	0	1	1	1	0	1	0
Observed:	?	0	?	?	1	1	1	?	1	0

$n = 10 \quad \alpha = 0.6$

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

Wiretap Channels of Type II - Past Results

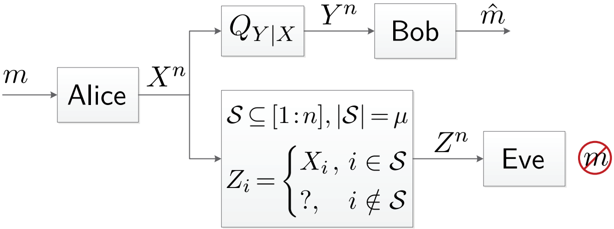
[Ozarow-Wyner 1984]



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

Wiretap Channels of Type II - Past Results

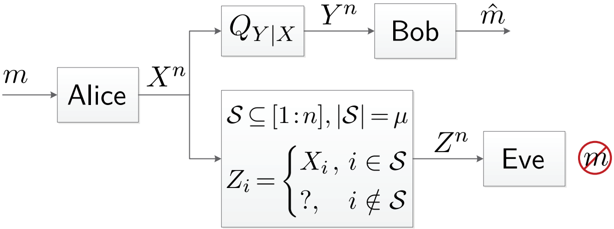
[Ozarow-Wyner 1984]



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

Wiretap Channels of Type II - Past Results

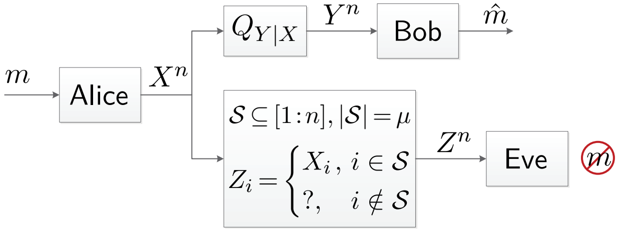
[Ozarow-Wyner 1984]



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

Wiretap Channels of Type II - Past Results

[Ozarow-Wyner 1984]

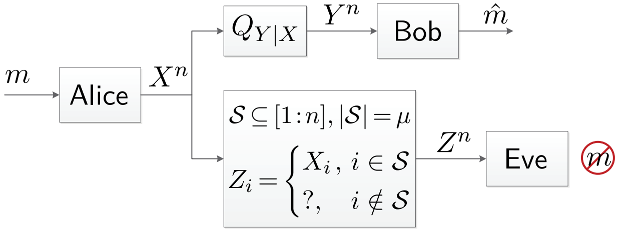


- **Ozarow-Wyner 1984:** Noiseless main channel
  - Rate equivocation region.
  - Coset coding.

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

Wiretap Channels of Type II - Past Results

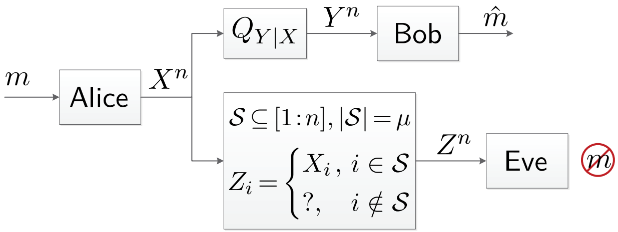
[Ozarow-Wyner 1984]



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

$$C_{\mathsf{Semantic}}(\alpha) = C_{\mathsf{Weak}}(\alpha) = \max_{Q_{U,X}} \Big[I(U;Y) - \alpha I(U;X) \Big]$$

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 $\alpha \in [0,1]$

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

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

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 $\alpha \in [0,1]$

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

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

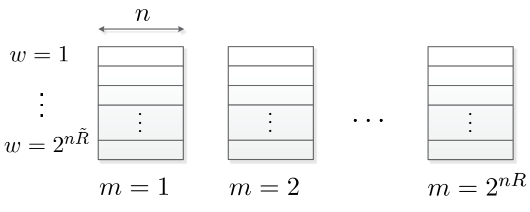
1. **Wiretap Code:**

WTC II SS-Capacity - Security Analysis

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

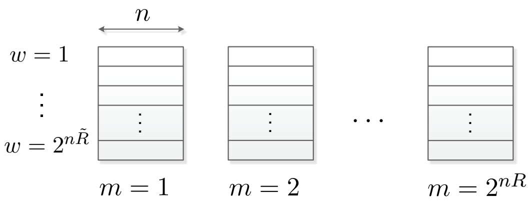
WTC II SS-Capacity - Security Analysis

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



WTC II SS-Capacity - Security Analysis

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



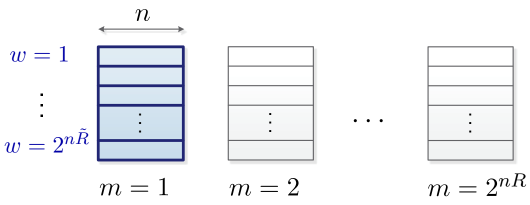
2. **Preliminary Step:**

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

WTC II SS-Capacity - Security Analysis

1. **Wiretap Code:**

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

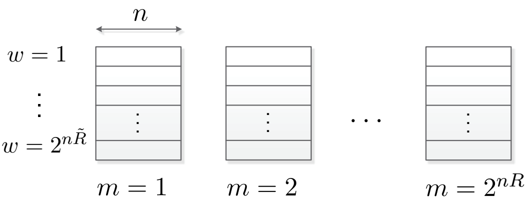


2. **Preliminary Step:**

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

WTC II SS-Capacity - Security Analysis

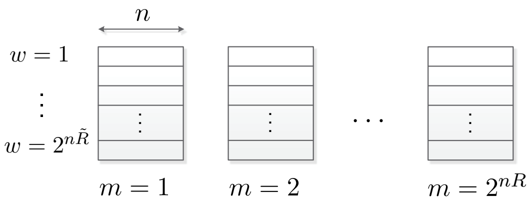
1. **Wiretap Code:**
   - $W \sim \text{Unif}\big[1 : 2^{n\tilde{R}}\big]$.
   - $\mathsf{C}_n = \big\{X^n(m,w)\big\}_{m,w} \overset{iid}{\sim} Q_X^n$



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

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

WTC II SS-Capacity - Security Analysis



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

2. **Preliminary Step:**

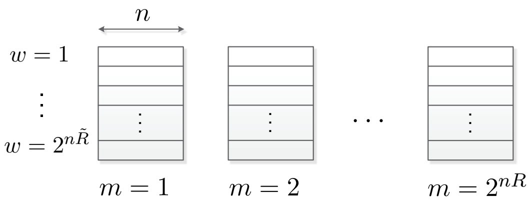
$$\max_{\substack{P_M,\mathcal{S}:\\ |\mathcal{S}|=\mu}} I_{\mathcal{C}_n}(M;Z^n) \leq \max_{\substack{m,\mathcal{S}:\\ |\mathcal{S}|=\mu}} D\left(P^{(\mathcal{C}_n,\mathcal{S})}_{Z^\mu|M=m}\middle|\middle| Q_Z^\mu\right)$$

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

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

WTC II SS-Capacity - Security Analysis

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



2. **Preliminary Step:**

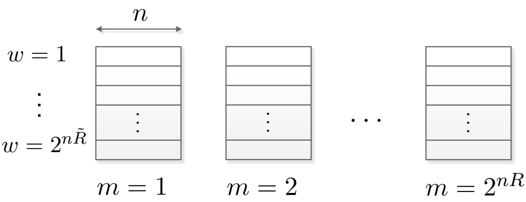
$$\max_{\substack{P_M,\mathcal{S}:\\ |\mathcal{S}|=\mu}} I_{\mathcal{C}_n}(M;Z^n) \leq \max_{\substack{m,\mathcal{S}:\\ |\mathcal{S}|=\mu}} D\Big(P_{Z^\mu|M=m}^{(\mathcal{C}_n,\mathcal{S})}\Big|\Big|Q_Z^\mu\Big)$$

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

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

WTC II SS-Capacity - Security Analysis

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



2. **Preliminary Step:**

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

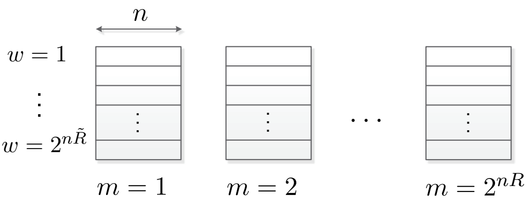
3. **Union Bound & Strong SCL:**

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

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

WTC II SS-Capacity - Security Analysis

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



2. **Preliminary Step:**

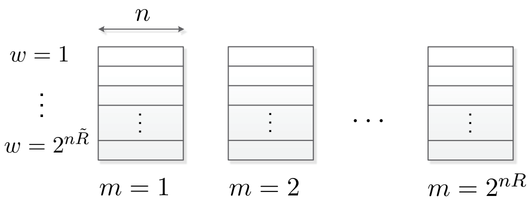
$$\max_{\substack{P_M,\mathcal{S}:\\|\mathcal{S}|=\mu}} I_{\mathcal{C}_n}(M;Z^n) \leq \max_{\substack{m,\mathcal{S}:\\|\mathcal{S}|=\mu}} D\left(P^{(\mathcal{C}_n,\mathcal{S})}_{Z^\mu|M=m}\middle|\middle|Q_Z^\mu\right)$$

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

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

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

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



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

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

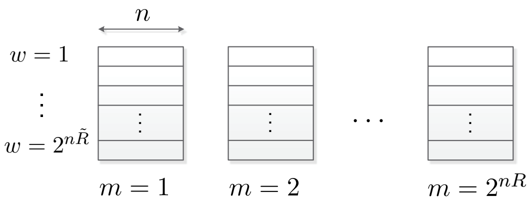
$$\mathbb{P}\left(\left\{\max_{P_M,\mathcal{S}} I_{\mathsf{C}_n}(M;Z^n) \leq e^{-n\gamma_1}\right\}^c\right) \leq \mathbb{P}\left(\max_{m,\mathcal{S}} D\Big(P^{(\mathcal{C}_n,\mathcal{S})}_{Z^\mu|M=m}\Big|\Big|Q^\mu_Z\Big) > e^{-n\gamma_1}\right)$$

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

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

WTC II SS-Capacity - Security Analysis

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



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

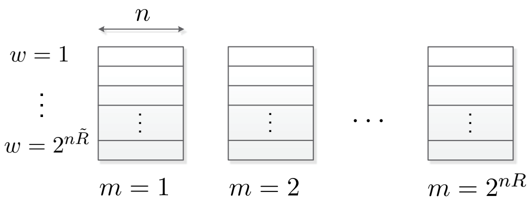
3. **Union Bound & Strong SCL:**

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

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

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

WTC II SS-Capacity - Security Analysis



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

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

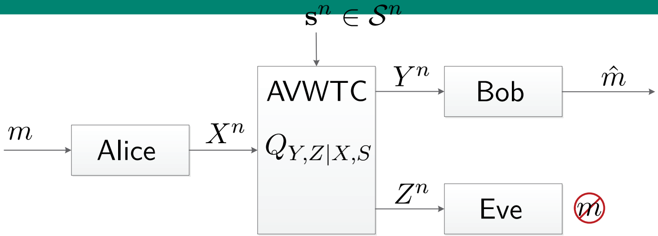
3. **Union Bound & Strong SCL:**

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

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

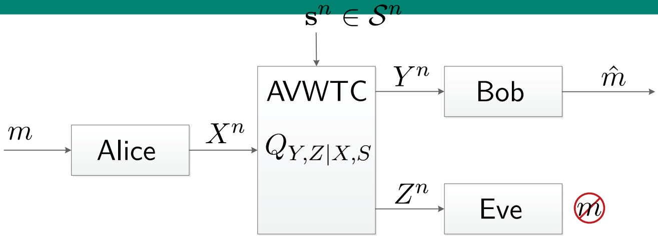
Taking $\boxed{\tilde{R} > \alpha H(X)}$ $\implies \leq 2^n 2^{nR} e^{-e^{n\gamma_2}} \xrightarrow[n\to\infty]{} 0$

Arbitrarily Varying Wiretap Channels - Generalization



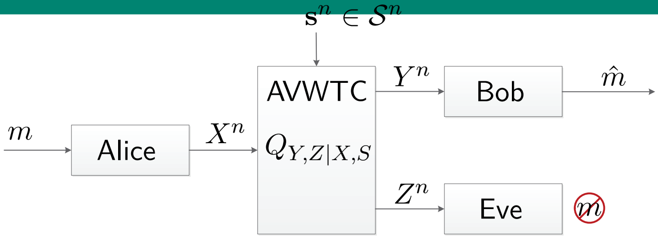
- Models **main** and **eavesdropper** channel uncertainty.

Arbitrarily Varying Wiretap Channels - Generalization



- Models **main** and **eavesdropper** channel uncertainty.
- **Type Constrained States:** Allowed s^n have empirical dist. $\approx Q_S$:

Arbitrarily Varying Wiretap Channels - Generalization

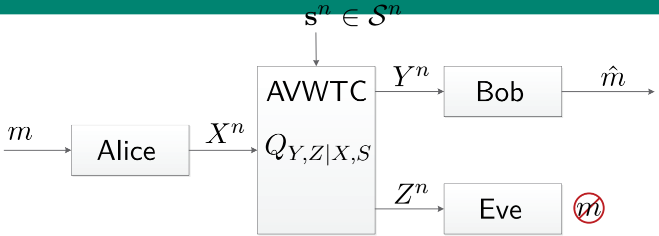


- Models **main** and **eavesdropper** channel uncertainty.
- **Type Constrained States:** Allowed s^n have empirical dist. $\approx Q_S$:

Theorem (ZG-Cuff-Permuter 2016)

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

Arbitrarily Varying Wiretap Channels - Generalization



- Models **main** and **eavesdropper** channel uncertainty.
- **Type Constrained States:** Allowed s^n have empirical dist. $\approx Q_S$:

Theorem (ZG-Cuff-Permuter 2016)

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

⋆ 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.

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.

Thank You!

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 $R + \tilde{R} < I(X;Y)$.

7. **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.

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 $R + \tilde{R} < I(X;Y)$.

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

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

$\square$

WTC II SS-Capacity - Converse

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.