Semantic Security versus Active Adversaries and Wiretap Channels with Random States

Ziv Goldfeld
Joint work with Paul Cuff and Haim Permuter

Ben Gurion University

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:

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**.

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**.

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:

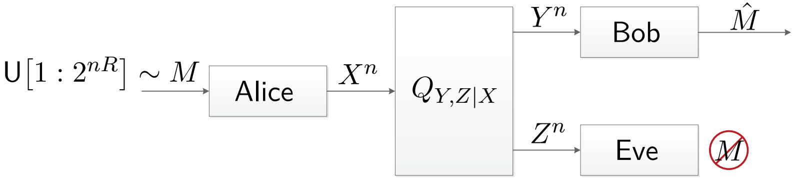
1. Eve's channel assumed to be **fully known** & **constant in time**.
2. Security metrics **insufficient for (some) applications**.

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

Wiretap Channels - Security Metrics

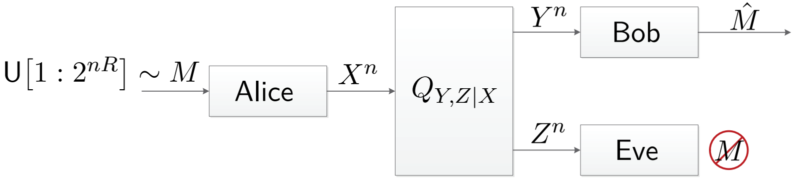
Wiretap Channels and Security Metrics

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



Wiretap Channels and Security Metrics

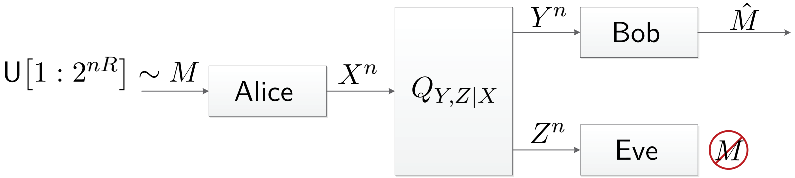
Degraded [Wyner 1975], General [Csiszár-Körner 1978]



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

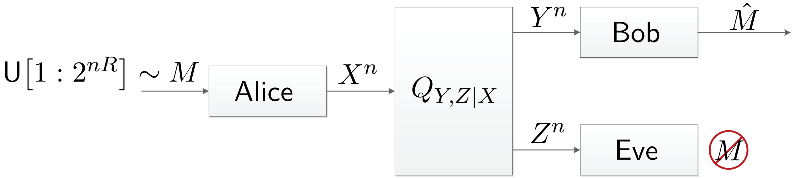
Wiretap Channels and Security Metrics

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



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

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

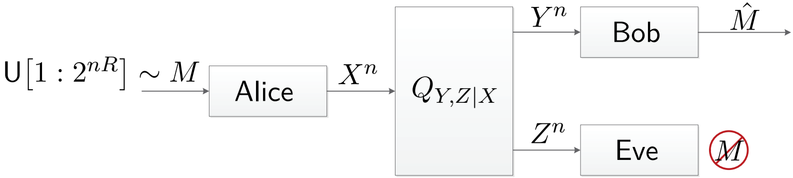


$\{\mathcal{C}_n\}_{n\in\mathbb{N}}$ - a sequence of (n, R)-codes

- **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]

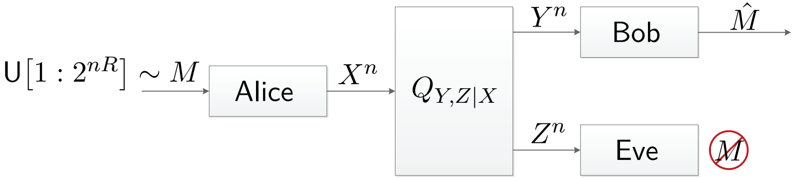


$\{\mathcal{C}_n\}_{n\in\mathbb{N}}$ - a sequence of (n,R)-codes

- **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]

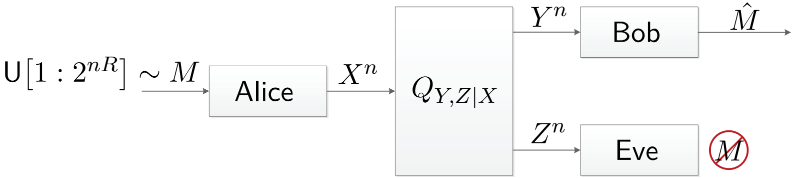


$\{\mathcal{C}_n\}_{n\in\mathbb{N}}$ - a sequence of (n, R)-codes

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

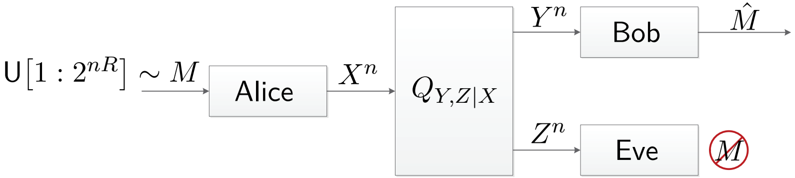
Wiretap Channels and Security Metrics

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**

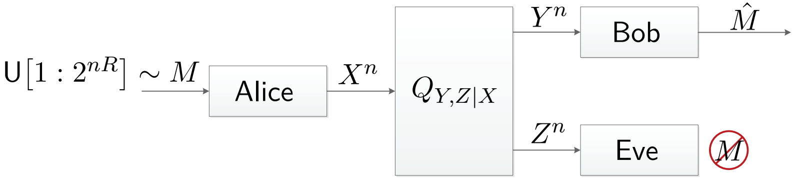


$\{\mathcal{C}_n\}_{n\in\mathbb{N}}$ - a sequence of (n,R)-codes

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

★ A stronger secrecy metric is required for applications ★

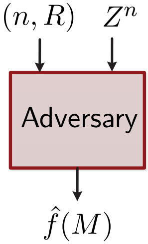
Semantic Security
[Goldwasser-Micali 1982]

- **Test:** For any P_M learn about any $f(M)$

Semantic Security

[Goldwasser-Micali 1982]

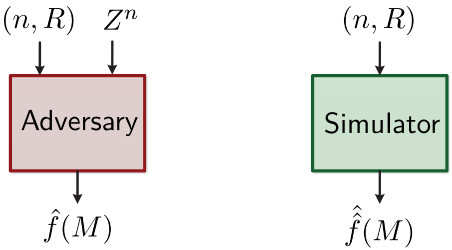
- **Test:** For any P_M learn about any $f(M)$



Semantic Security

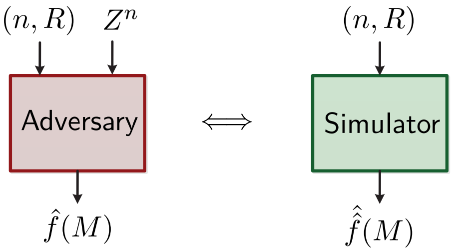
[Goldwasser-Micali 1982]

- **Test:** For any P_M learn about any $f(M)$



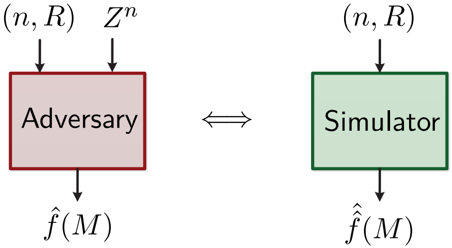
Semantic Security
[Goldwasser-Micali 1982]

- **Test:** For any P_M learn about any $f(M)$



Semantic Security
[Goldwasser-Micali 1982]

- **Test:** For any P_M learn about any $f(M)$

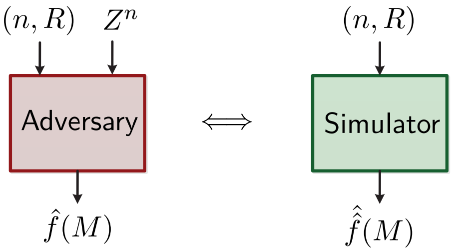


- **Equivalence:** [Bellare-Tessaro-Vardy 2012]

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

Semantic Security
[Goldwasser-Micali 1982]

- **Test:** For any P_M learn about any $f(M)$



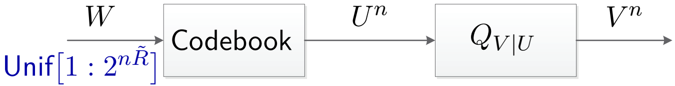
- **Equivalence:** [Bellare-Tessaro-Vardy 2012]

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

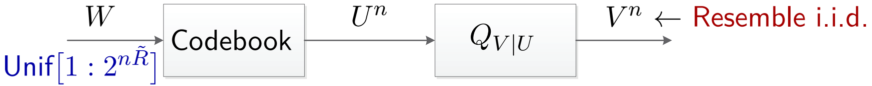
★ A single code must work well for all message PMFs ★

Strong Soft-Covering Lemma

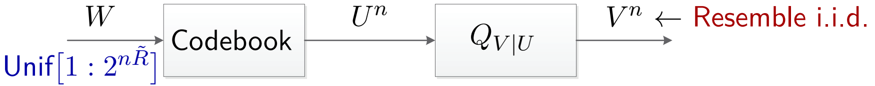
Soft-Covering - Setup



Soft-Covering - Setup

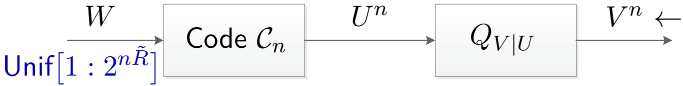


Soft-Covering - Setup



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

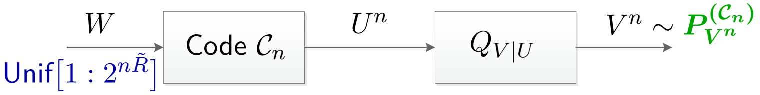
Soft-Covering - Setup



$\leftarrow$ Resemble i.i.d.

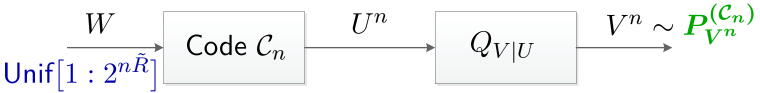
- **Random Codebook:** $\mathsf{C}_n = \{U^n(w)\}_w \overset{iid}{\sim} Q_U^n$.

Soft-Covering - Setup



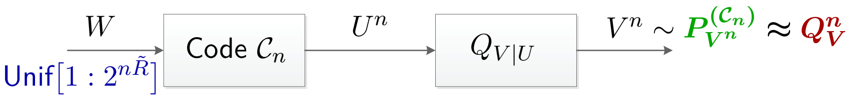
- **Random Codebook:** $\mathsf{C}_n = \{U^n(w)\}_w \overset{iid}{\sim} Q_U^n$.
- **Induced Output Distribution:** Codebook $\mathcal{C}_n \implies V^n \sim P_{V^n}^{(\mathcal{C}_n)}$

Soft-Covering - Setup



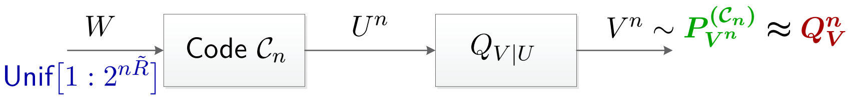
- **Random Codebook:** $\mathsf{C}_n = \{U^n(w)\}_w \overset{iid}{\sim} Q_U^n$.
- **Induced Output Distribution:** Codebook $\mathcal{C}_n \implies V^n \sim P_{V^n}^{(\mathcal{C}_n)}$
- **Target IID Distribution:** Q_V^n marginal of $Q_U^n Q_{V|U}^n$.

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

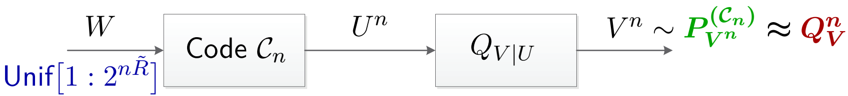
Soft-Covering - Setup



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

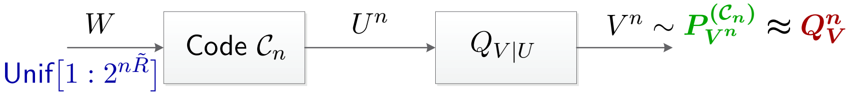
⋆ **Goal:** Choose $\tilde{R}$ (codebook size) s.t. $P_{V^n}^{(\mathcal{C}_n)} \approx Q_V^n$ ⋆

Soft-Covering - Results



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

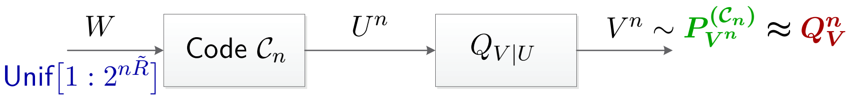
Soft-Covering - Results



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

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

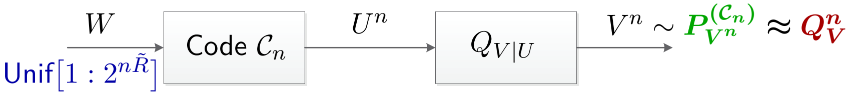
Soft-Covering - Results



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

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

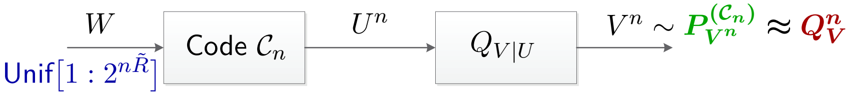
Soft-Covering - Results



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

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

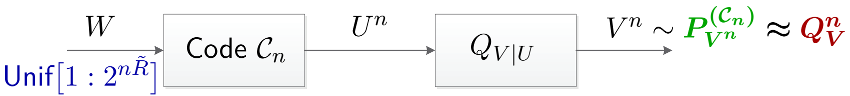
Soft-Covering - Results



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

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



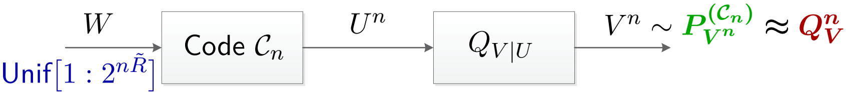
Lemma (ZG-Cuff-Permuter 2016)

If $\tilde{R} > I_Q(U;V)$*, then there exist* $\gamma_1, \gamma_2 > 0$ *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.*

Strong Soft-Covering Lemma



Lemma (ZG-Cuff-Permuter 2016)

If $\tilde{R} > I_Q(U;V)$, *then there exist* $\gamma_1, \gamma_2 > 0$ *s.t.*

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

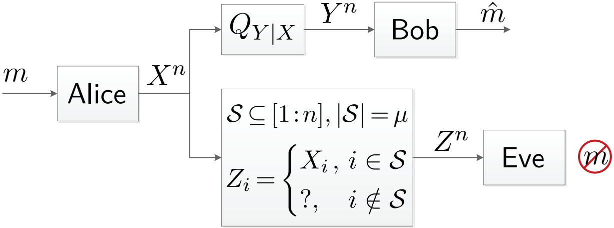
for n *sufficiently large.*

- New proof via concentration of measure (McDiarmid Theorem).

Wiretap Channels of Type II

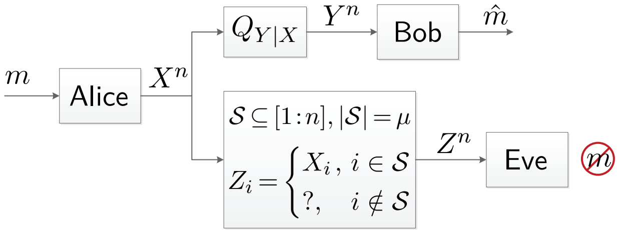
Wiretap Channels of Type II - Definition

[Ozarow-Wyner 1984]



Wiretap Channels of Type II - Definition

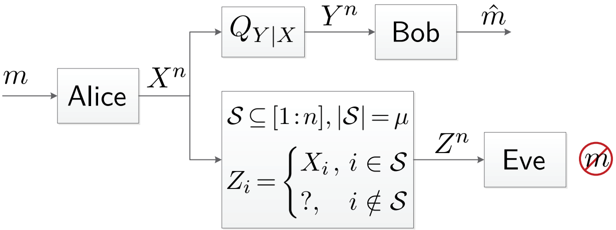
[Ozarow-Wyner 1984]



- **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 $\boldsymbol{\mu = \lfloor \alpha n \rfloor}$, $\boldsymbol{\alpha \in [0,1]}$, of transmitted symbols.

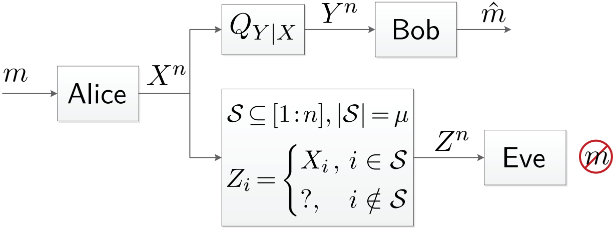
- **Transmitted:**

0	0	1	0	1	1	1	0	1	0

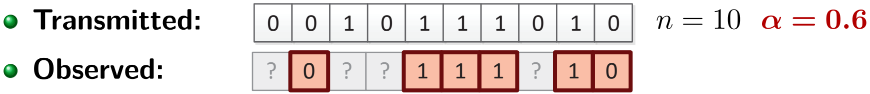
$n = 10$ $\boldsymbol{\alpha = 0.6}$

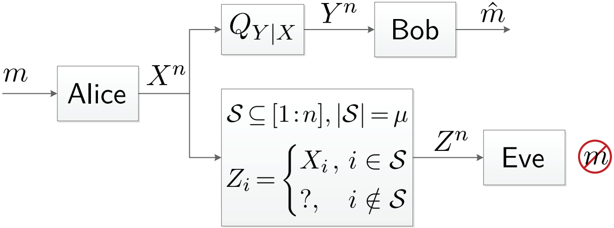
Wiretap Channels of Type II - Definition

[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.





- **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.

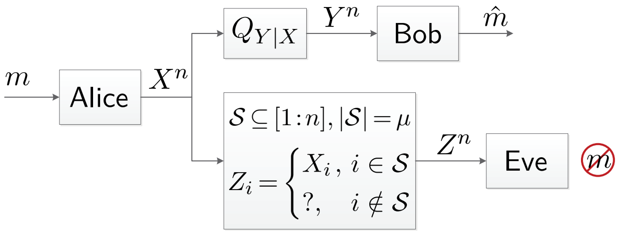
Transmitted:	0	0	1	0	1	1	1	0	1	0
Observed:	?	0	?	?	1	1	1	?	1	0

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

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

Wiretap Channels of Type II - Past Results

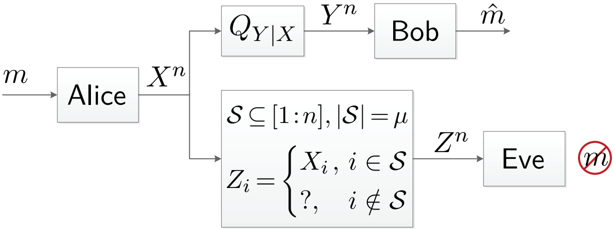
[Ozarow-Wyner 1984]



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

Wiretap Channels of Type II - Past Results

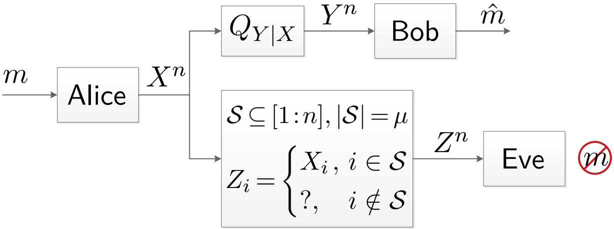
[Ozarow-Wyner 1984]



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

Wiretap Channels of Type II - Past Results

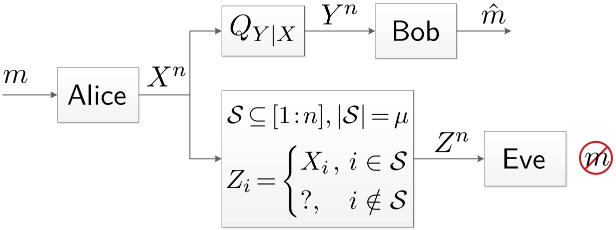
[Ozarow-Wyner 1984]



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

Wiretap Channels of Type II - Past Results

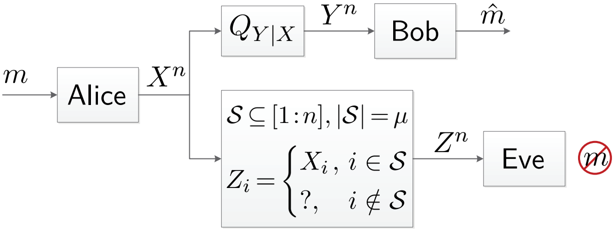
[Ozarow-Wyner 1984]



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

Wiretap Channels of Type II - Past Results

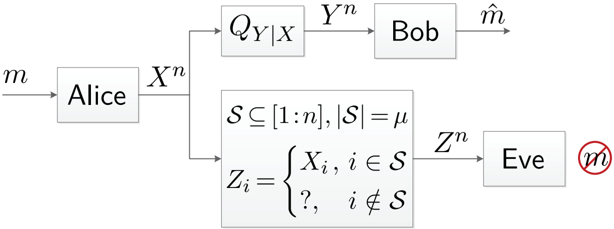
[Ozarow-Wyner 1984]



- **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.

Wiretap Channels of Type II - SS-Capacity

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 (ZG-Cuff-Permuter 2016)

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 (ZG-Cuff-Permuter 2016)

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

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

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

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 (ZG-Cuff-Permuter 2016)

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.

WTC II SS-Capacity - Achievability for U=X

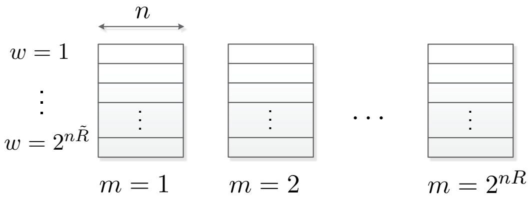
1. **Wiretap Code:**

WTC II SS-Capacity - Achievability for U=X

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

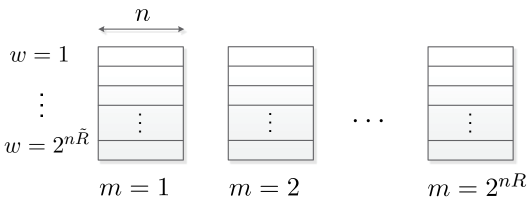
WTC II SS-Capacity - Achievability for U=X

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



WTC II SS-Capacity - Achievability for U=X

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

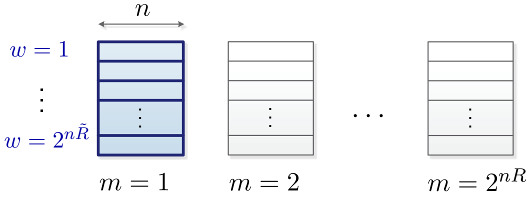


2. **Preliminary Step:**

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

WTC II SS-Capacity - Achievability for U=X

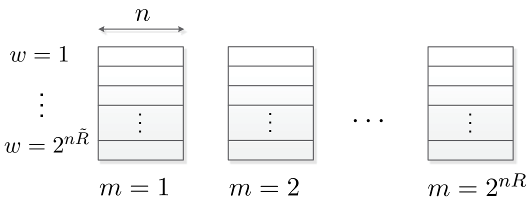
1. **Wiretap Code:**
   - $W \sim \text{Unif}\big[1:2^{n\tilde{R}}\big]$.
   - $\mathsf{C}_n = \big\{X^n(m,w)\big\}_{m,w} \overset{iid}{\sim} Q_X^n$



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

WTC II SS-Capacity - Achievability for U=X

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

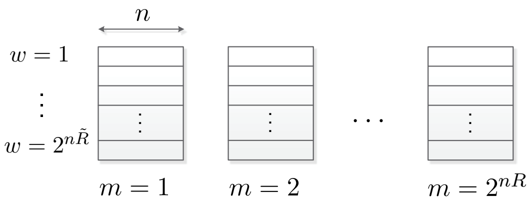


2. **Preliminary Step:** $$\max_{\substack{P_M,\mathcal{S}:\\|\mathcal{S}|=\mu}} I_{\mathcal{C}_n}(M;Z^n) \leq \max_{\substack{m,\mathcal{S}:\\|\mathcal{S}|=\mu}} D\left(P^{(\mathcal{C}_n,\mathcal{S})}_{Z^\mu|M=m}\middle|\middle|Q_Z^\mu\right)$$

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

WTC II SS-Capacity - Achievability for U=X

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

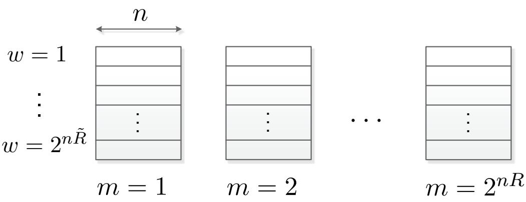


2. **Preliminary Step:** $$\max_{\substack{P_M,\mathcal{S}:\\|\mathcal{S}|=\mu}} I_{\mathcal{C}_n}(M;Z^n) \leq \max_{\substack{m,\mathcal{S}:\\|\mathcal{S}|=\mu}} D\left(P^{(\mathcal{C}_n,\mathcal{S})}_{Z^\mu|M=m}\middle|\middle|Q_Z^\mu\right)$$

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 - Achievability for U=X



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

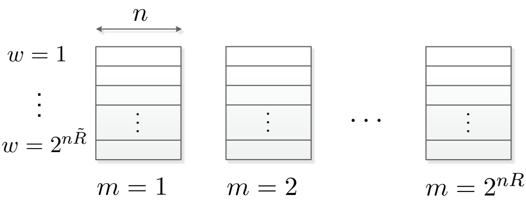
3. **Union Bound & Strong SCL:**

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

WTC II SS-Capacity - Achievability for U=X

1 Wiretap Code:

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



2 Preliminary Step:

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

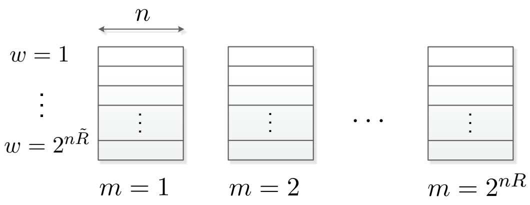
3 Union Bound & Strong SCL:

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

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

WTC II SS-Capacity - Achievability for U=X

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:**

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

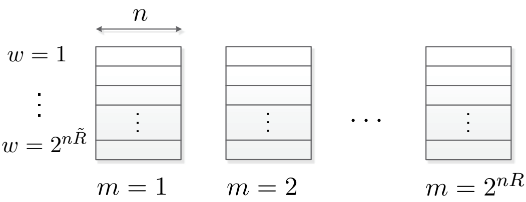
3. **Union Bound & Strong SCL:**

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

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

WTC II SS-Capacity - Achievability for U=X

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



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

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

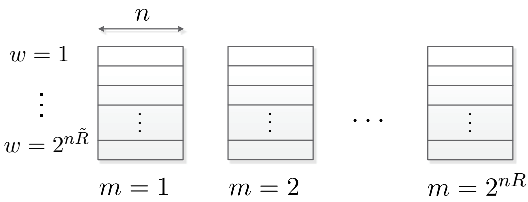
$$\mathbb{P}\left(\left\{\max_{P_M,\mathcal{S}} I_{\mathsf{C}_n}(M;Z^n) \leq e^{-n\gamma_1}\right\}^c\right) \leq \mathbb{P}\left(\max_{m,\mathcal{S}} D\Big(P^{(\mathsf{C}_n,\mathcal{S})}_{Z^\mu|M=m}\Big|\Big|Q^\mu_Z\Big) > e^{-n\gamma_1}\right)$$

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

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

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:

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

3 Union Bound & Strong SCL:

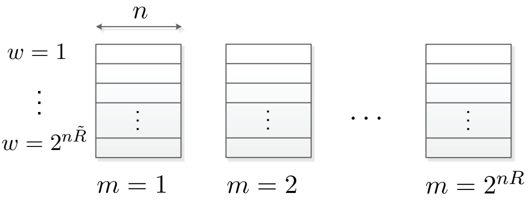
$$\mathbb{P}\left(\left\{\max_{P_M,\mathcal{S}} I_{\mathsf{C}_n}(M;Z^n) \leq e^{-n\gamma_1}\right\}^c\right) \leq \mathbb{P}\left(\max_{m,\mathcal{S}} D\Big(P^{(\mathsf{C}_n,\mathcal{S})}_{Z^\mu|M=m}\Big|\Big|Q_Z^\mu\Big) > e^{-n\gamma_1}\right)$$

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

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

WTC II SS-Capacity - Achievability for U=X

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

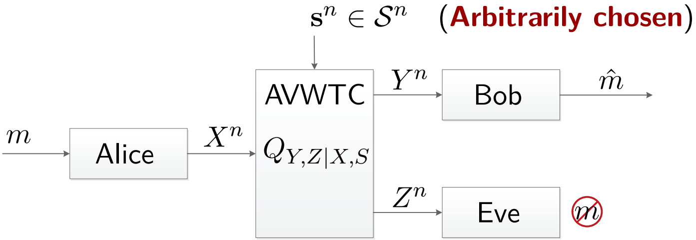
3. **Union Bound & Strong SCL:**

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

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

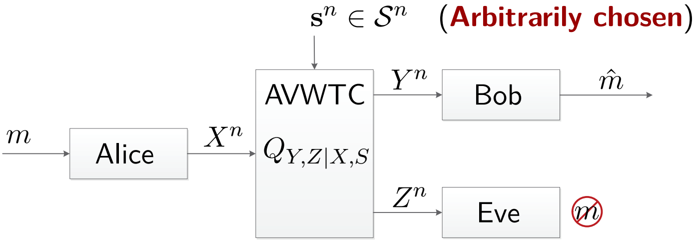
Taking $\boxed{\tilde{R} > \alpha H(X)}$ $\implies \leq 2^n 2^{nR} e^{-e^{n\gamma_2}} \xrightarrow[n\to\infty]{} 0$

A Generalization - Arbitrarily Varying WTCs



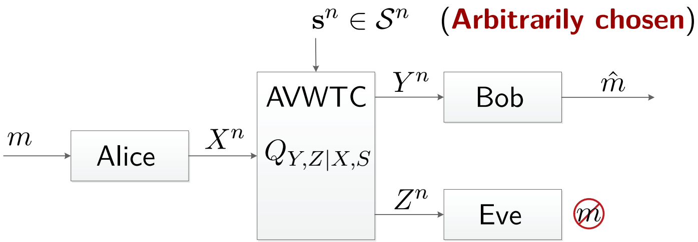
- Models **main** and **eavesdropper** channel uncertainty.

A Generalization - Arbitrarily Varying WTCs



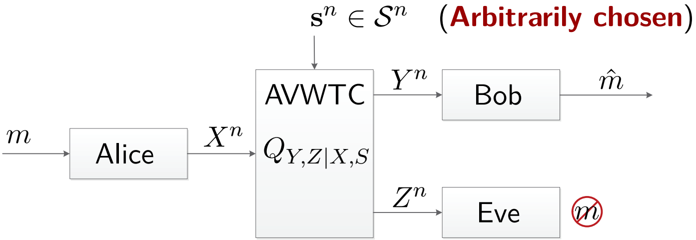
- Models **main** and **eavesdropper** channel uncertainty.
- Worst case analysis for **reliability** and **security**.

A Generalization - Arbitrarily Varying WTCs



- Models **main** and **eavesdropper** channel uncertainty.
- Worst case analysis for **reliability** and **security**.
- **Type Constrained States:** Allowed $\boldsymbol{s^n}$ have empirical dist. $\approx \boldsymbol{Q_S}$:

A Generalization - Arbitrarily Varying WTCs



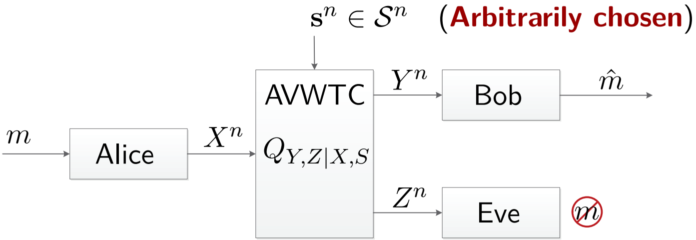
- Models **main** and **eavesdropper** channel uncertainty.
- Worst case analysis for **reliability** and **security**.
- **Type Constrained States:** Allowed s^n have empirical dist. $\approx Q_S$:

Theorem (ZG-Cuff-Permuter 2016)

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

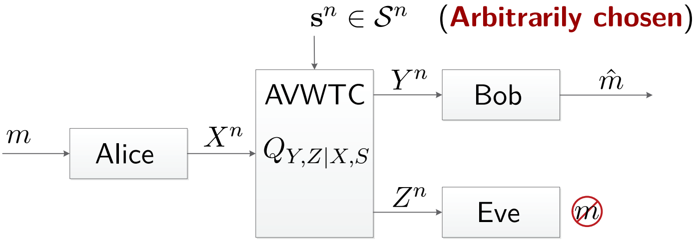
Joint PMF: $Q_S Q_{U,X} Q_{Y,Z|X,S}$.

A Generalization - Arbitrarily Varying WTCs



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

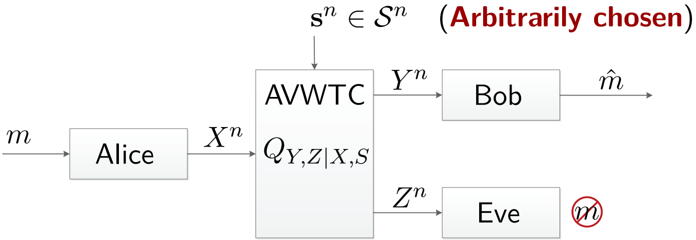
A Generalization - Arbitrarily Varying WTCs



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

- Type constrained scenario subsumes WTC II model and result.

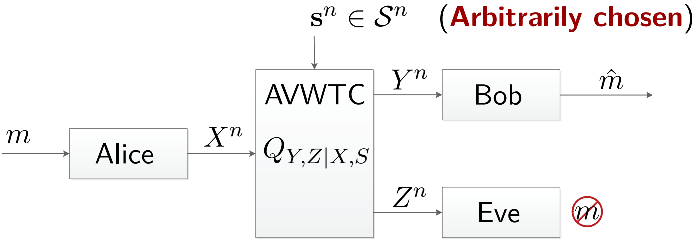
A Generalization - Arbitrarily Varying WTCs



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

- Type constrained scenario subsumes WTC II model and result.
- General single-letter lower and upper bounds for any constraining set.

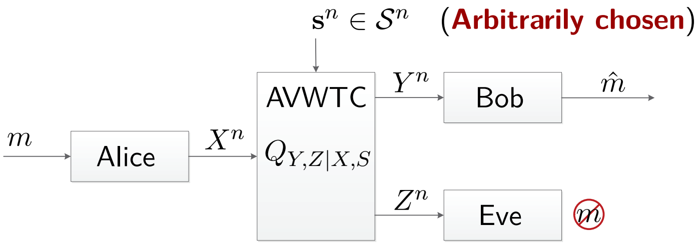
A Generalization - Arbitrarily Varying WTCs



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

- Type constrained scenario subsumes WTC II model and result.
- General single-letter lower and upper bounds for any constraining set.
- **Proofs:**

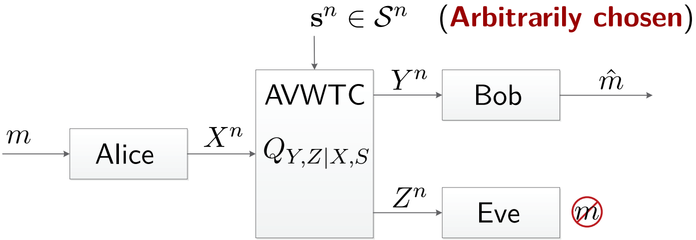
A Generalization - Arbitrarily Varying WTCs



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

- Type constrained scenario subsumes WTC II model and result.
- General single-letter lower and upper bounds for any constraining set.
- Proofs: ▸ Achievability: Random coding & Heterogeneous Strong SCL.

A Generalization - Arbitrarily Varying WTCs



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

- Type constrained scenario subsumes WTC II model and result.
- General single-letter lower and upper bounds for any constraining set.
- **Proofs:**
  - Achievability: Random coding & Heterogeneous Strong SCL.
  - Upper Bound: Distribution coupling & continuity arguments.

Semantic-Security vs. Active Adversaries - Recap

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

Semantic-Security vs. Active Adversaries - Recap

- **Semantic Security:** [Bellare-Tessaro-Vardy 2012]
  - Cryptographic gold standard in.

Semantic-Security vs. Active Adversaries - Recap

- **Semantic Security:** [Bellare-Tessaro-Vardy 2012]
  - Cryptographic gold standard in.
  - Equivalent to vanishing inf. leakage for all P_M.

Semantic-Security vs. Active Adversaries - Recap

- **Semantic Security:** [Bellare-Tessaro-Vardy 2012]
  - Cryptographic gold standard in.
  - Equivalent to vanishing inf. leakage for all P_M.

- **Strong Soft-Covering Lemma:**

Semantic-Security vs. Active Adversaries - Recap

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

Semantic-Security vs. Active Adversaries - Recap

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

Semantic-Security vs. Active Adversaries - Recap

- **Semantic Security:** [Bellare-Tessaro-Vardy 2012]
  - Cryptographic gold standard in.
  - Equivalent to vanishing inf. leakage for all P_M.
- **Strong 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

Semantic-Security vs. Active Adversaries - Recap

- **Semantic Security:** [Bellare-Tessaro-Vardy 2012]
  - Cryptographic gold standard in.
  - Equivalent to vanishing inf. leakage for all P_M.
- **Strong 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.

Semantic-Security vs. Active Adversaries - Recap

- **Semantic Security:** [Bellare-Tessaro-Vardy 2012]
  - Cryptographic gold standard in.
  - Equivalent to vanishing inf. leakage for all P_M.
- **Strong 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.

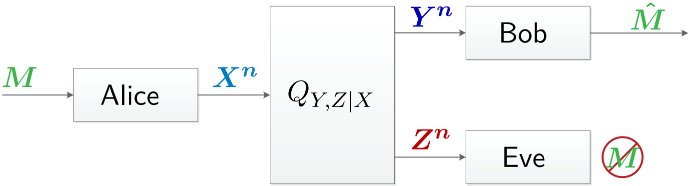
Semantic-Security vs. Active Adversaries - Recap

- **Semantic Security:** [Bellare-Tessaro-Vardy 2012]
  - Cryptographic gold standard in.
  - Equivalent to vanishing inf. leakage for all P_M.
- **Strong 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.
  - Generalization to arbitrarily varying wiretap channel.

Wiretap Channels with Random States

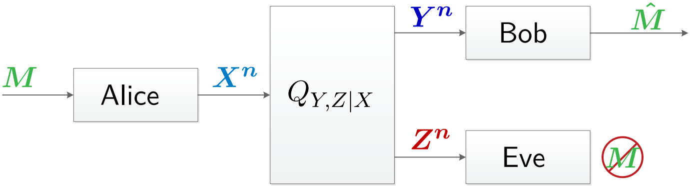
The Wiretap Channel

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



The Wiretap Channel

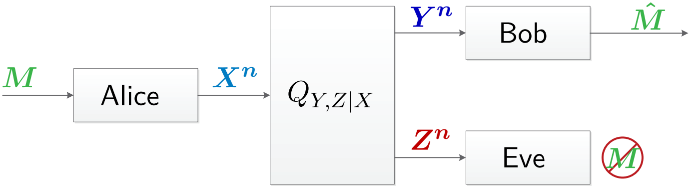
Degraded [Wyner 1975], General [Csiszár-Körner 1978]



Secrecy-Capacity:

The Wiretap Channel

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

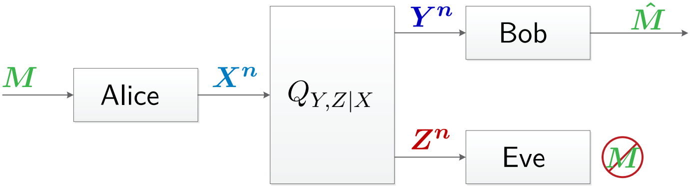


Secrecy-Capacity:

- Reliable Communication.

The Wiretap Channel

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

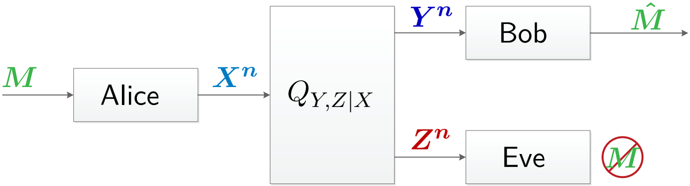


Secrecy-Capacity:

- Reliable Communication.
- Z^n contains no information about M.

The Wiretap Channel

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



Secrecy-Capacity:

- Reliable Communication.
- Z^n contains no information about M.

Theorem (Csiszár-Körner 1978)

$$\mathsf{C}_{\mathsf{WTC}} = \max_{Q_{U,X}} \Big[I(U;Y) - I(U;Z) \Big]$$

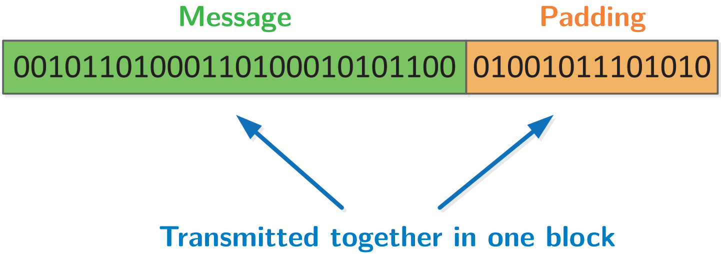
Joint PMF: $Q_{U,X}Q_{Y,Z|X}$

The Wiretap Channel - Encoding

- Pad nR **message bits** with $n\tilde{R}$ **random garbage bits**.

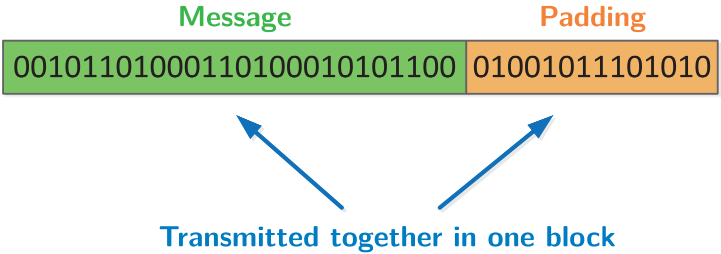
The Wiretap Channel - Encoding

- Pad nR **message bits** with $n\tilde{R}$ **random garbage bits**.



The Wiretap Channel - Encoding

- Pad nR **message bits** with $n\tilde{R}$ **random garbage bits**.



- **Random Codebook:** $(\text{Message}, \text{Padding}) \rightarrow \; U^n \sim Q_U^n$.

The Wiretap Channel - Encoding

- Pad nR **message bits** with $n\tilde{R}$ **random garbage bits**.

Message	Padding
0010110100011010001010110 0	01001011101010

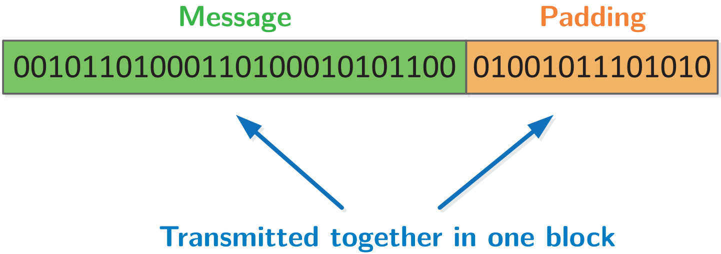
Transmitted together in one block

- **Random Codebook:** (**Message**, **Padding**) $\rightarrow$ $U^n \sim Q_U^n$.

- **Reliability:** $R + \tilde{R} < I(U;Y)$.

The Wiretap Channel - Encoding

- Pad nR **message bits** with $n\tilde{R}$ **random garbage bits**.



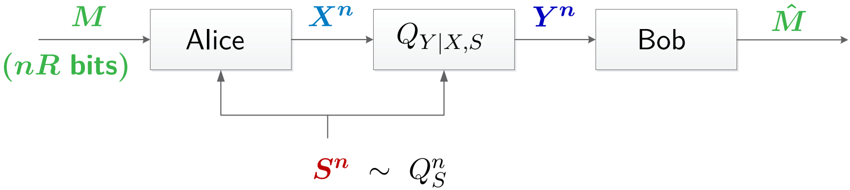
- **Random Codebook:** (Message, Padding) $\rightarrow$ $U^n \sim Q_U^n$.

- **Reliability:** $R + \tilde{R} < I(U;Y)$.

- **Security:** $\tilde{R} > I(U;Z)$.

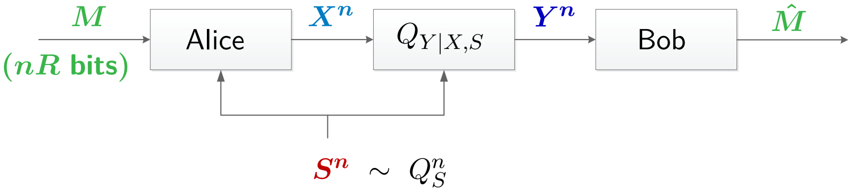
The Gelfand-Pinsker Channel

[Pelfand-Pinsker 1980]



The Gelfand-Pinsker Channel

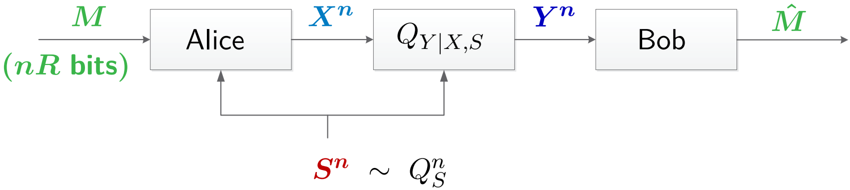
[Pelfand-Pinsker 1980]



Capacity:

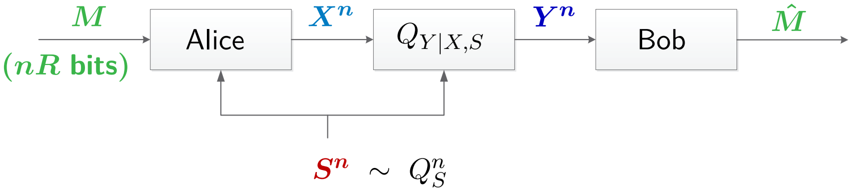
The Gelfand-Pinsker Channel

[Pelfand-Pinsker 1980]



Capacity: Reliable Communication.

The Gelfand-Pinsker Channel
[Pelfand-Pinsker 1980]



Capacity: Reliable Communication.

Theorem (Gelfand-Pinsker 1980)

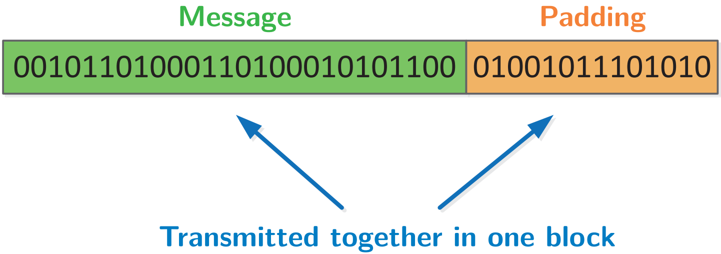
$$\mathsf{C}_{\mathsf{GP}} = \max_{Q_{U,X|S}} \Big[I(U;Y) - I(U;S) \Big]$$

Joint PMF: $Q_{U,X|S} Q_{Y|X,S}$

The Gelfand-Pinsker Channel - Encoding

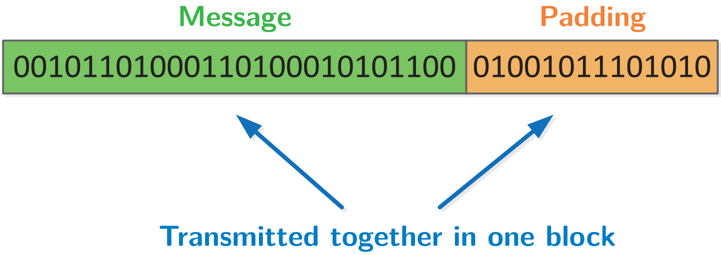
- Pad nR **message bits** with $n\tilde{R}$ **skillfully chosen bits**.

- Pad nR **message bits** with $n\tilde{R}$ **skillfully chosen bits**.



The Gelfand-Pinsker Channel - Encoding

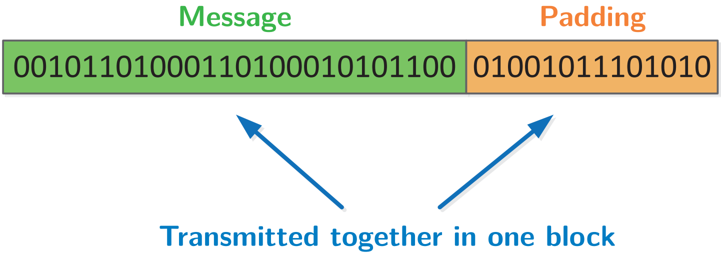
- Pad nR **message bits** with $n\tilde{R}$ **skillfully chosen bits**.



- **Random Codebook:** $(\text{Message}, \text{Padding}) \rightarrow U^n \sim Q_U^n$.

The Gelfand-Pinsker Channel - Encoding

- Pad nR **message bits** with $n\tilde{R}$ **skillfully chosen bits**.



- **Random Codebook:** (Message, Padding) $\rightarrow$ $U^n \sim Q_U^n$.
- **Correlating U^n with S^n:** $\tilde{R} > I(U;S)$.

The Gelfand-Pinsker Channel - Encoding

- Pad nR **message bits** with $n\tilde{R}$ **skillfully chosen bits**.

Message	Padding
00101101000110100010101100	01001011101010

Transmitted together in one block

- **Random Codebook:** (Message, Padding) $\rightarrow$ $U^n \sim Q_U^n$.
- **Correlating U^n with S^n:** $\tilde{R} > I(U;S)$.
- **Reliability:** $R + \tilde{R} < I(U;Y)$.

Gelfand-Pinsker Channel vs. Wiretap Channel

Similarities:

Gelfand-Pinsker Channel vs. Wiretap Channel

Similarities:

- Capacity expression.

Gelfand-Pinsker Channel vs. Wiretap Channel

Similarities:

- Capacity expression.
- Encoding.

Gelfand-Pinsker Channel vs. Wiretap Channel

Similarities:

- Capacity expression.
- Encoding.
- Converse (i.i.d. S^n in GP setting allows skipping a step).

Gelfand-Pinsker Channel vs. Wiretap Channel

Similarities:

- Capacity expression.
- Encoding.
- Converse (i.i.d. S^n in GP setting allows skipping a step).
- Target asymptotic probabilistic relations:

Gelfand-Pinsker Channel vs. Wiretap Channel

Similarities:

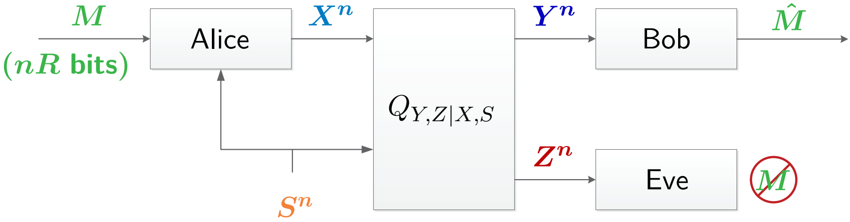
- Capacity expression.
- Encoding.
- Converse (i.i.d. S^n in GP setting allows skipping a step).
- Target asymptotic probabilistic relations:
  - **Gelfand-Pinsker Channel:** $\hat{M} = M$ (and M independent of S^n).

Gelfand-Pinsker Channel vs. Wiretap Channel

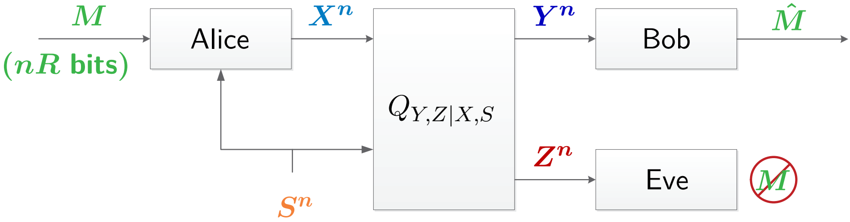
Similarities:

- Capacity expression.
- Encoding.
- Converse (i.i.d. S^n in GP setting allows skipping a step).
- Target asymptotic probabilistic relations:
  - **Gelfand-Pinsker Channel:** $\hat{M} = M$ (and M independent of S^n).
  - **Wiretap Channel:** $\hat{M} = M$ and M independent of Z^n.

The Gelfand-Pinsker Wiretap Channel

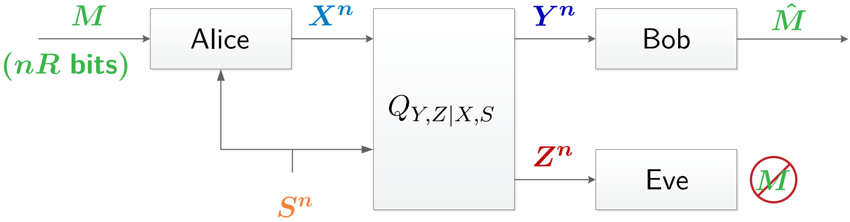


The Gelfand-Pinsker Wiretap Channel



Secrecy-Capacity:

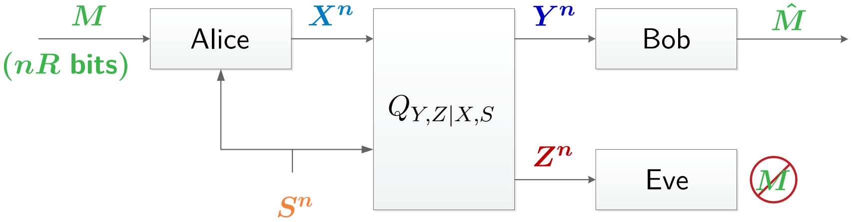
The Gelfand-Pinsker Wiretap Channel



Secrecy-Capacity:

- Reliable Communication.

The Gelfand-Pinsker Wiretap Channel



Secrecy-Capacity:

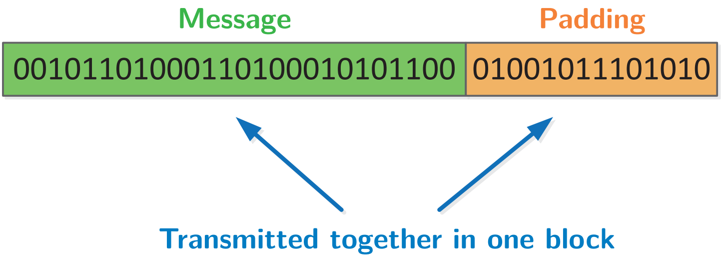
- Reliable Communication.
- Z^n contains no information about M.

Naive Approach:

The Gelfand-Pinsker Wiretap Channel

Same Encoding [Chen-Han Vinck 2006]

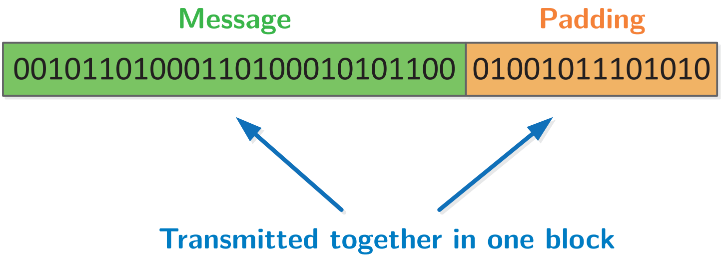
Naive Approach: Combining **wiretap coding** with **GP coding**.



The Gelfand-Pinsker Wiretap Channel

Same Encoding [Chen-Han Vinck 2006]

Naive Approach: Combining **wiretap coding** with **GP coding**.



Theorem (Chen-Han Vinck 2006)

$$\mathsf{C}_{\mathsf{GP-WTC}} \geq \max_{Q_{U,X|S}} \Big[I(U;Y) - \max\big\{ \boldsymbol{I(U;Z)}, \boldsymbol{I(U;S)} \big\} \Big]$$

Joint PMF: $Q_S Q_{U,X|S} Q_{Y,Z|X,S}$

Wiretap Channels with Encoder and Decoder CSI

Key Extraction Scheme [Chia-El Gamal 2012]

Assume S^n is know to Receiver $\mathbf{Y} = (\mathbf{Y}, \mathbf{S})$.

Wiretap Channels with Encoder and Decoder CSI

Key Extraction Scheme [Chia-El Gamal 2012]

Assume S^n is know to Receiver $\boldsymbol{Y} = (\boldsymbol{Y}, \boldsymbol{S})$.

- Extract secret random bits from S^n.

Wiretap Channels with Encoder and Decoder CSI

Key Extraction Scheme [Chia-El Gamal 2012]

Assume S^n is know to Receiver $\boldsymbol{Y} = (\boldsymbol{Y}, \boldsymbol{S})$.

- Extract secret random bits from S^n.
- One-Time-Pad the message $\boldsymbol{M}$.

Wiretap Channels with Encoder and Decoder CSI

Key Extraction Scheme [Chia-El Gamal 2012]

Assume S^n is know to Receiver $\mathbf{Y} = (\mathbf{Y}, S)$.

- Extract secret random bits from S^n.
- One-Time-Pad the message M.
- Point-to-point transmission (ignore **Eve**).

Wiretap Channels with Encoder and Decoder CSI

Key Extraction Scheme [Chia-El Gamal 2012]

Assume S^n is know to Receiver $\mathbf{Y} = (Y, S)$.

- Extract secret random bits from S^n.
- One-Time-Pad the message M.
- Point-to-point transmission (ignore **Eve**).

Theorem (Chia-El Gamal 2012)

$$\mathsf{C}_{\mathsf{GP-WTC}} \geq \max_{Q_{U,X|S}} \min\Big\{H(S|U,Z), I(U;Y|S)\Big\}$$

Joint PMF: $Q_S Q_{U,X|S} Q_{Y,Z|X,S}$

Note: They consider causal state information.
This region is adapted to take advantage of non-causal state information.

Assume S^n is know to Receiver $\mathbf{Y} = (\mathbf{Y}, \mathbf{S})$.

- Extract secret random bits from S^n.
- One-Time-Pad the message M.
- Point-to-point transmission (ignore **Eve**).

Theorem (Chia-El Gamal 2012)

$$\mathsf{C}_{\mathsf{GP-WTC}} \geq \max_{Q_{U,X|S}} \min\left\{H(S|U,Z), I(U;Y|S)\right\}$$

Joint PMF: $Q_S Q_{U,X|S} Q_{Y,Z|X,S}$

Better than previous scheme!

Note: They consider causal state information.
This region is adapted to take advantage of non-causal state information.

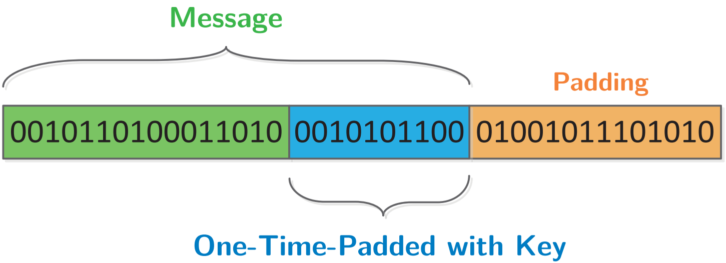
Combine Wiretap Codes with Key Extraction:

Combine Wiretap Codes with Key Extraction: Assume $\mathbf{Y} = (\mathbf{Y}, \mathbf{S})$.

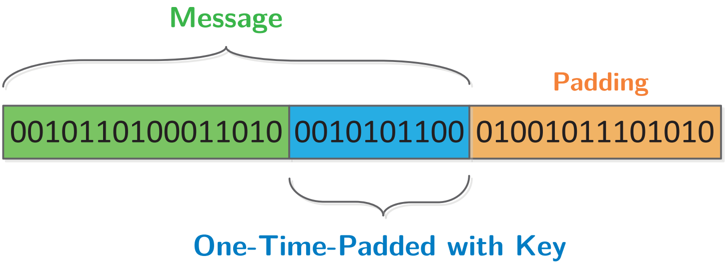
Wiretap Channels with Encoder and Decoder CSI

Combined Scheme [Chia-El Gamal 2012]

Combine Wiretap Codes with Key Extraction: Assume $\mathbf{Y} = (\mathbf{Y}, \mathbf{S})$.



Combine Wiretap Codes with Key Extraction: Assume $\mathbf{Y} = (Y, S)$.



Theorem (Chia-El Gamal 2012)

$$\mathsf{C}_{\mathsf{GP-WTC}} \geq \max_{Q_{U,X|S}} \min \left\{ \begin{array}{c} H(S|U,Z) + \left[I(U;Y,S) - I(U;Z)\right]^{+}, \\ I(U;Y|S) \end{array} \right\}$$

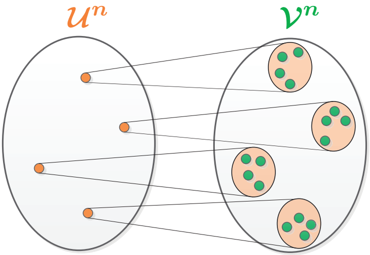
Joint PMF: $Q_S Q_{U,X|S} Q_{Y,Z|X,S}$

The Gelfand-Pinsker Wiretap Channel - Our Scheme

Superposition Code:

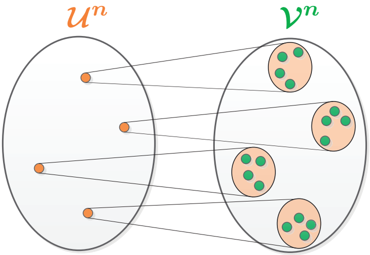
The Gelfand-Pinsker Wiretap Channel - Our Scheme

Superposition Code:



The Gelfand-Pinsker Wiretap Channel - Our Scheme

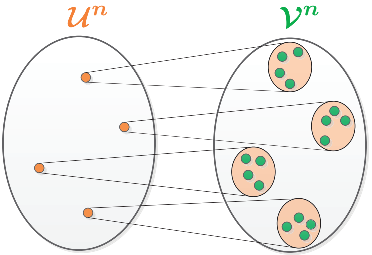
Superposition Code:



- U^n index is **padding** only.

The Gelfand-Pinsker Wiretap Channel - Our Scheme

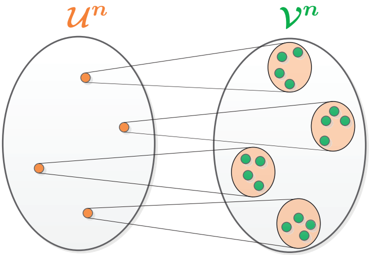
Superposition Code:



- U^n index is **padding** only.
- V^n index is **massage** and **padding** only.

The Gelfand-Pinsker Wiretap Channel - Our Scheme

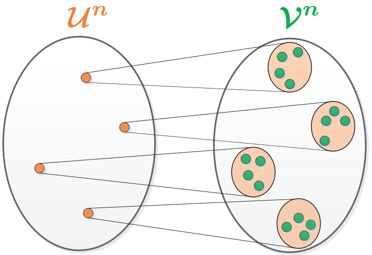
Superposition Code:



- U^n index is **padding** only.
- V^n index is **massage** and **padding** only.
- U^n decoded by **Eve**

The Gelfand-Pinsker Wiretap Channel - Our Scheme

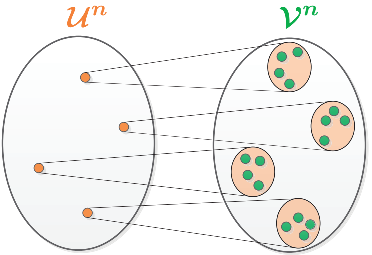
Superposition Code:



- U^n index is **padding** only.
- V^n index is **massage** and **padding** only.
- U^n decoded by **Eve** $\implies$ waste channel resources (i.e., "decoy").

The Gelfand-Pinsker Wiretap Channel - Our Scheme

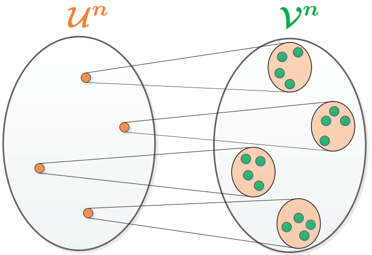
Superposition Code:



- U^n index is **padding** only.
- V^n index is **massage** and **padding** only.
- U^n decoded by **Eve** $\implies$ waste channel resources (i.e., "decoy").
- All secrecy comes from V^n.

The Gelfand-Pinsker Wiretap Channel - Our Scheme

Superposition Code:



- U^n index is **padding** only.
- V^n index is **massage** and **padding** only.
- U^n decoded by **Eve** $\implies$ waste channel resources (i.e., "decoy").
- All secrecy comes from V^n.

⋆ **Analysis:** Likelihood Encoder & Superposition Strong SCL ⋆

The Gelfand-Pinsker Wiretap Channel - Our Scheme

Theorem (ZG-Cuff-Permuter 2016)

$$\mathsf{C}_{\mathsf{GP-WTC}} \geq \max_{\substack{Q_{U,V,X|S}: \\ I(U;Y)-I(U;S)\geq 0}} \min \left\{ \begin{array}{c} I(V;Y|U) - I(V;Z|U), \\ I(U,V;Y) - I(U,V;S) \end{array} \right\}$$

Joint PMF: $Q_S Q_{U,V,X|S} Q_{Y,Z|X,S}$.

The Gelfand-Pinsker Wiretap Channel - Our Scheme

Theorem (ZG-Cuff-Permuter 2016)

$$\mathsf{C}_{\mathsf{GP-WTC}} \geq \max_{\substack{Q_{U,V,X|S}: \\ \boldsymbol{I(U;Y)-I(U;S)\geq 0}}} \min \left\{ \begin{array}{c} I(V;Y|U) - I(V;Z|U), \\ I(U,V;Y) - I(U,V;S) \end{array} \right\}$$

Joint PMF: $Q_S Q_{U,V,X|S} Q_{Y,Z|X,S}$.

- **Inner layer** reliably decodable by the receiver.

The Gelfand-Pinsker Wiretap Channel - Our Scheme

Theorem (ZG-Cuff-Permuter 2016)

$$\mathsf{C}_{\mathsf{GP-WTC}} \geq \max_{\substack{Q_{U,V,X|S}: \\ I(U;Y)-I(U;S)\geq 0}} \min \left\{ \begin{array}{c} \boldsymbol{I(V;Y|U) - I(V;Z|U)}, \\ I(U,V;Y) - I(U,V;S) \end{array} \right\}$$

Joint PMF: $Q_S Q_{U,V,X|S} Q_{Y,Z|X,S}$.

- Inner layer reliably decodable by the receiver.
- **Total secrecy** rate of outer layer.

The Gelfand-Pinsker Wiretap Channel - Our Scheme

Theorem (ZG-Cuff-Permuter 2016)

$$\mathsf{C}_{\mathsf{GP-WTC}} \geq \max_{\substack{Q_{U,V,X|S}: \\ I(U;Y)-I(U;S)\geq 0}} \min \left\{ \begin{array}{c} I(V;Y|U) - I(V;Z|U), \\ \boldsymbol{I(U,V;Y) - I(U,V;S)} \end{array} \right\}$$

Joint PMF: $Q_S Q_{U,V,X|S} Q_{Y,Z|X,S}$.

- Inner layer reliably decodable by the receiver.
- Total secrecy rate of outer layer.
- **Total communication** rate of entire superposition codebook.

The Gelfand-Pinsker Wiretap Channel - Our Scheme

Theorem (ZG-Cuff-Permuter 2016)

$$\mathsf{C}_{\mathsf{GP-WTC}} \geq \max_{\substack{Q_{U,V,X|S}: \\ I(U;Y)-I(U;S)\geq 0}} \min \left\{ \begin{array}{c} I(V;Y|U) - I(V;Z|U), \\ I(U,V;Y) - I(U,V;S) \end{array} \right\}$$

Joint PMF: $Q_S Q_{U,V,X|S} Q_{Y,Z|X,S}$.

Relation to Previous Schemes:

The Gelfand-Pinsker Wiretap Channel - Our Scheme

Theorem (ZG-Cuff-Permuter 2016)

$$\mathsf{C}_{\mathsf{GP-WTC}} \geq \max_{\substack{Q_{U,V,X|S}: \\ I(U;Y)-I(U;S)\geq 0}} \min \left\{ \begin{array}{c} I(V;Y|U) - I(V;Z|U), \\ I(U,V;Y) - I(U,V;S) \end{array} \right\}$$

Joint PMF: $Q_S Q_{U,V,X|S} Q_{Y,Z|X,S}$.

Relation to Previous Schemes:

- Upgrade from **weak-secrecy** to **semantic-security**.

The Gelfand-Pinsker Wiretap Channel - Our Scheme

Theorem (ZG-Cuff-Permuter 2016)

$$\mathsf{C}_{\mathsf{GP-WTC}} \geq \max_{\substack{Q_{U,V,X|S}: \\ I(U;Y)-I(U;S)\geq 0}} \min \left\{ \begin{array}{c} I(V;Y|U) - I(V;Z|U), \\ I(U,V;Y) - I(U,V;S) \end{array} \right\}$$

Joint PMF: $Q_S Q_{U,V,X|S} Q_{Y,Z|X,S}$.

Relation to Previous Schemes:

- Upgrade from **weak-secrecy** to **semantic-security**.
- Recovers Chia-El Gamal's result when $Y = (Y,S)$.

The Gelfand-Pinsker Wiretap Channel - Our Scheme

Theorem (ZG-Cuff-Permuter 2016)

$$\mathsf{C}_{\mathsf{GP-WTC}} \geq \max_{\substack{Q_{U,V,X|S}: \\ I(U;Y)-I(U;S)\geq 0}} \min \left\{ \begin{array}{c} I(V;Y|U) - I(V;Z|U), \\ I(U,V;Y) - I(U,V;S) \end{array} \right\}$$

Joint PMF: $Q_S Q_{U,V,X|S} Q_{Y,Z|X,S}$.

Relation to Previous Schemes:

- Upgrade from **weak-secrecy** to **semantic-security**.
- Recovers Chia-El Gamal's result when $Y = (Y,S)$.
- Beats previous regions even when S^n **not** known to Receiver.

Wiretap Channels with Random States - Recap

- **Gelfand-Pinsker wiretap channel**

Wiretap Channels with Random States - Recap

- **Gelfand-Pinsker wiretap channel**
  - Combination of two fundamental problems.

Wiretap Channels with Random States - Recap

- **Gelfand-Pinsker wiretap channel**
  - Combination of two fundamental problems.
- **Novel superposition coding scheme**

Wiretap Channels with Random States - Recap

- **Gelfand-Pinsker wiretap channel**
  - Combination of two fundamental problems.

- **Novel superposition coding scheme**
  - Upgrades previous results from weak-secrecy to semantic-security.

Wiretap Channels with Random States - Recap

- **Gelfand-Pinsker wiretap channel**
  - Combination of two fundamental problems.
- **Novel superposition coding scheme**
  - Upgrades previous results from weak-secrecy to semantic-security.
  - Recovers best known rate when S^n known to Receiver [Chia-El Gamal].

Wiretap Channels with Random States - Recap

- **Gelfand-Pinsker wiretap channel**
  - Combination of two fundamental problems.

- **Novel superposition coding scheme**
  - Upgrades previous results from weak-secrecy to semantic-security.
  - Recovers best known rate when S^n known to Receiver [Chia-El Gamal].
  - Strictly better than best known rate when S^n not known to Receiver.

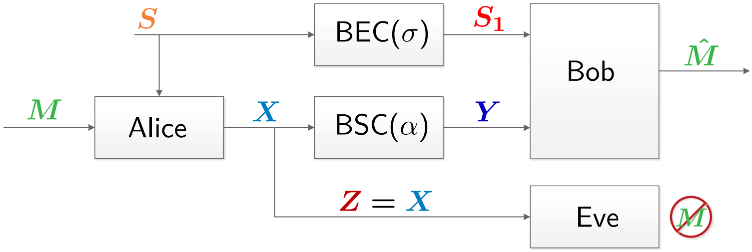
Wiretap Channels with Random States - Recap

- **Gelfand-Pinsker wiretap channel**
  - Combination of two fundamental problems.

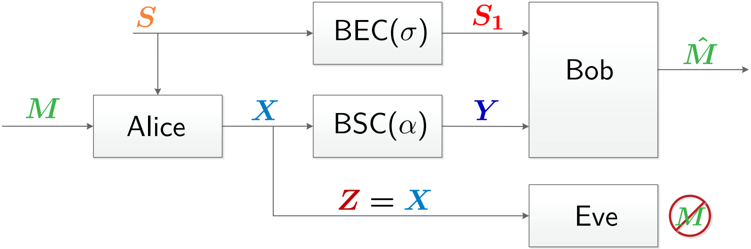
- **Novel superposition coding scheme**
  - Upgrades previous results from weak-secrecy to semantic-security.
  - Recovers best known rate when S^n known to Receiver [Chia-El Gamal].
  - Strictly better than best known rate when S^n not known to Receiver.

Thank you!

Outperforming Previous Schemes - An Example

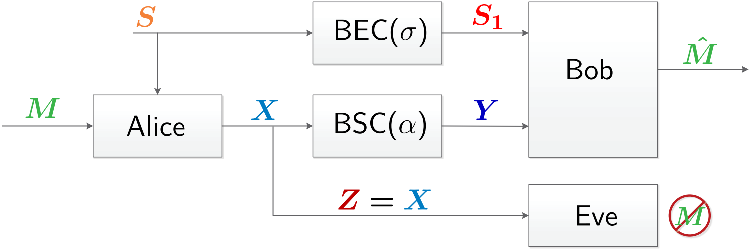


Outperforming Previous Schemes - An Example



- **Our scheme is optimal**: [Khisti-Diggavi-Wornell 2011]

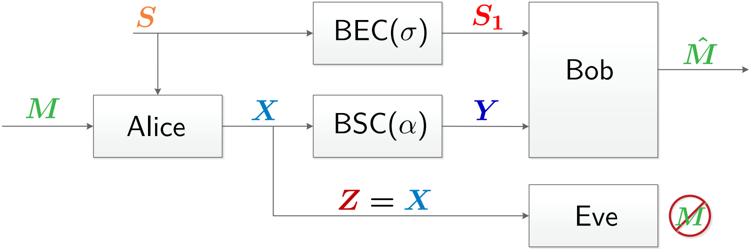
Outperforming Previous Schemes - An Example



- **Our scheme is optimal**: [Khisti-Diggavi-Wornell 2011]

$$C = \max_{Q_{A|S}} \min \Big\{ I(A;S_1), 1 - h(\alpha) - I(A;S|S_1) \Big\}$$

Outperforming Previous Schemes - An Example

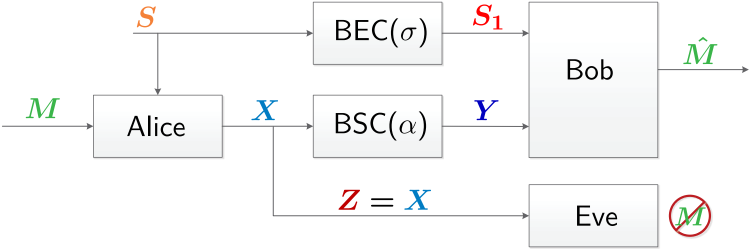


- **Our scheme is optimal**: [Khisti-Diggavi-Wornell 2011]

$$C = \max_{Q_{A|S}} \min \left\{ I(A;S_1), 1 - h(\alpha) - I(A;S|S_1) \right\}$$

  - 1st auxiliary - key agreement over BEC.

Outperforming Previous Schemes - An Example

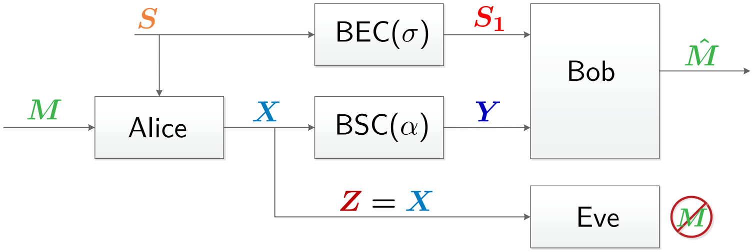


- **Our scheme is optimal**: [Khisti-Diggavi-Wornell 2011]

$$C = \max_{Q_{A|S}} \min \left\{ I(A;S_1), 1 - h(\alpha) - I(A;S|S_1) \right\}$$

  - 1st auxiliary - **key agreement** over BEC.
  - 2nd auxiliary - **transmission** over BSC (indep. of state and key).

Outperforming Previous Schemes - An Example



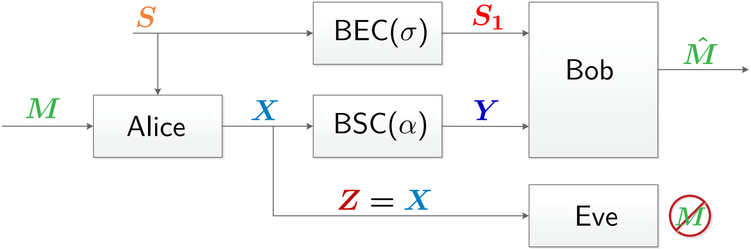
- **Our scheme is optimal**: [Khisti-Diggavi-Wornell 2011]

$$C = \max_{Q_{A|S}} \min \left\{ I(A;S_1), 1 - h(\alpha) - I(A;S|S_1) \right\}$$

  - 1st auxiliary - **key agreement** over BEC.
  - 2nd auxiliary - **transmission** over BSC (indep. of state and key).

- **Chen-Han Vinck scheme is suboptimal:**

Outperforming Previous Schemes - An Example



- **Our scheme is optimal**: [Khisti-Diggavi-Wornell 2011]

$$C = \max_{Q_{A|S}} \min \left\{ I(A;S_1), 1 - h(\alpha) - I(A;S|S_1) \right\}$$

  - 1st auxiliary - **key agreement** over BEC.
  - 2nd auxiliary - **transmission** over BSC (indep. of state and key).

- **Chen-Han Vinck scheme is suboptimal:**
  - Only one auxiliary - lacks flexibility to play both roles!

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.