Semantic Security versus Active Adversaries

Ziv Goldfeld
Joint work with Paul Cuff and Haim Permuter

Ben Gurion University

Information Theory and Applications Workshop

February 15th, 2017

Motivation

Information Theoretic Security over Noisy Channels

Motivation

Information Theoretic Security over Noisy Channels

Pros:

Motivation

Information Theoretic Security over Noisy Channels

Pros:

1. Security versus **computationally unbounded** eavesdroppers.

Information Theoretic Security over Noisy Channels

Pros:

1. Security versus **computationally unbounded** eavesdroppers.
2. **No shared key** - Harness intrinsic randomness of noisy channel.

Information Theoretic Security over Noisy Channels

Pros:

1. Security versus **computationally unbounded** eavesdroppers.
2. **No shared key** - Harness intrinsic randomness of noisy channel.

Cons:

Motivation

Information Theoretic Security over Noisy Channels

Pros:

1. Security versus **computationally unbounded** eavesdroppers.
2. **No shared key** - Harness intrinsic randomness of 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 unbounded** eavesdroppers.
2. **No shared key** - Harness intrinsic randomness of 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 unbounded** eavesdroppers.
2. **No shared key** - Harness intrinsic randomness of noisy channel.

Cons:

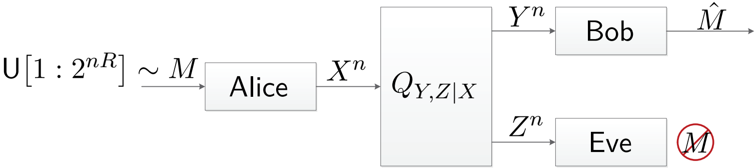
1. Eve's channel assumed to be **fully known** & **constant in time**.
2. Security metrics **insufficient for (some) applications**.

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

Wiretap Channels - Security Metrics

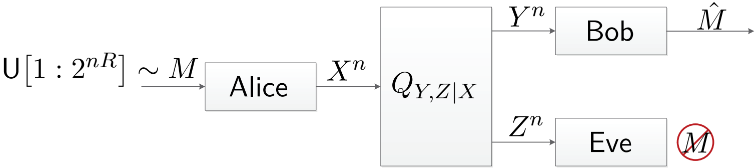
Wiretap Channels and Security Metrics

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

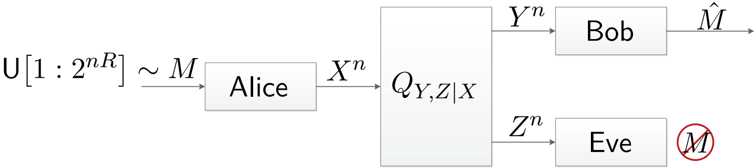


Wiretap Channels and Security Metrics

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



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

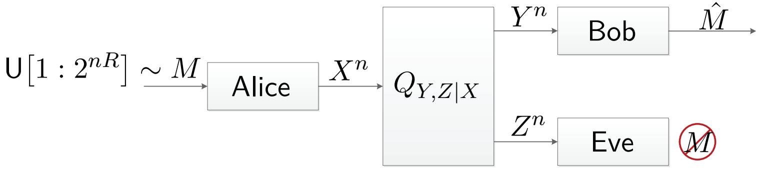


$\{\mathcal{C}_n\}_{n\in\mathbb{N}}$ - a sequence of (n,R)-codes

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

Wiretap Channels and Security Metrics

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

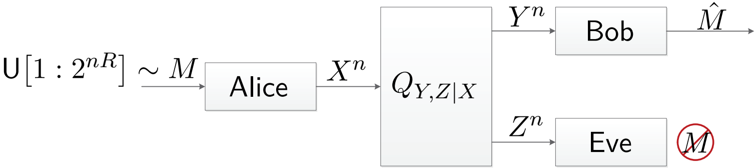


$\{\mathcal{C}_n\}_{n\in\mathbb{N}}$ - a sequence of (n, R)-codes

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

Wiretap Channels and Security Metrics

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

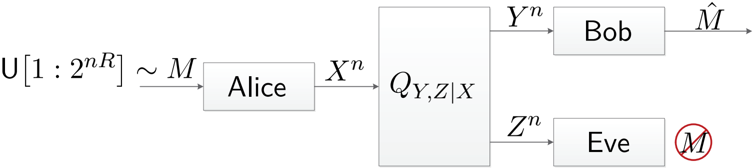


$\{\mathcal{C}_n\}_{n\in\mathbb{N}}$ - a sequence of (n,R)-codes

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

Wiretap Channels and Security Metrics

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

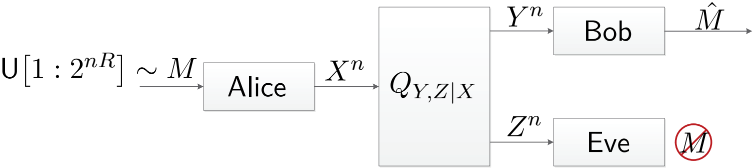


$\{\mathcal{C}_n\}_{n\in\mathbb{N}}$ - a sequence of (n,R)-codes

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

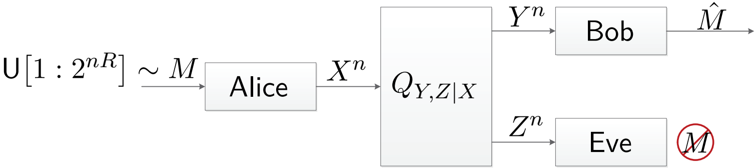
Wiretap Channels and Security Metrics

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



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

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

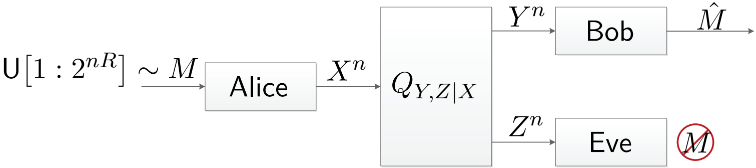


$\{\mathcal{C}_n\}_{n\in\mathbb{N}}$ - a sequence of (n,R)-codes

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

Wiretap Channels and Security Metrics

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

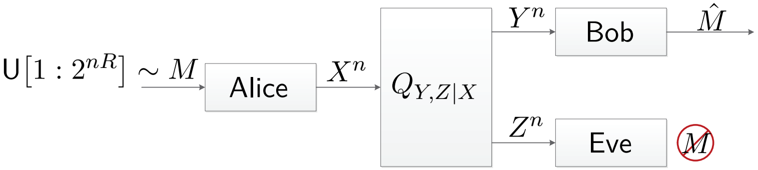


$\{\mathcal{C}_n\}_{n\in\mathbb{N}}$ - a sequence of (n,R)-codes

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

Wiretap Channels and Security Metrics

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



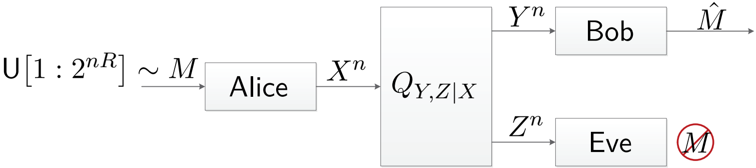
$\{\mathcal{C}_n\}_{n\in\mathbb{N}}$ - a sequence of (n, R)-codes

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

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

Wiretap Channels and Security Metrics

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



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

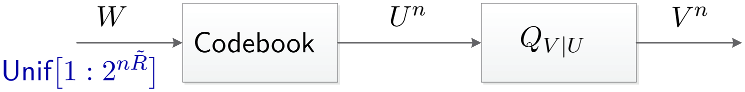
- **Weak Secrecy:** $\cancel{\frac{1}{n} I_{\mathcal{C}_n}(M;Z^n) \xrightarrow[n\to\infty]{} 0}$.
- **Strong Secrecy:** $\cancel{I_{\mathcal{C}_n}(M;Z^n) \xrightarrow[n\to\infty]{} 0}$.
- **Semantic Security:** [Bellare-Tessaro-Vardy 2012]

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

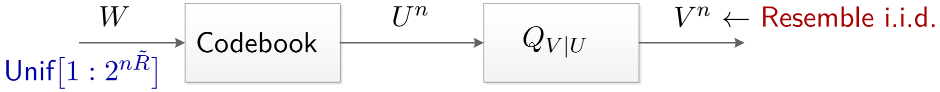
★ A single code must work well for all message PMFs ★

Strong Soft-Covering Lemmas

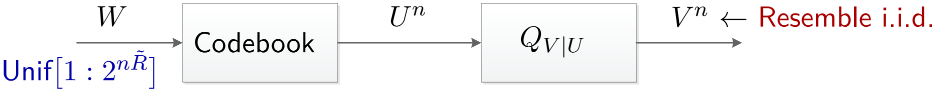
Soft-Covering - Setup



Soft-Covering - Setup

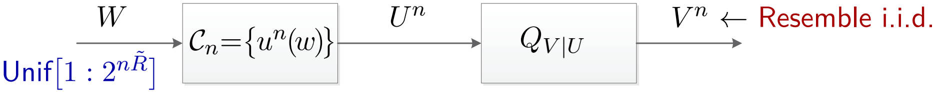


Soft-Covering - Setup

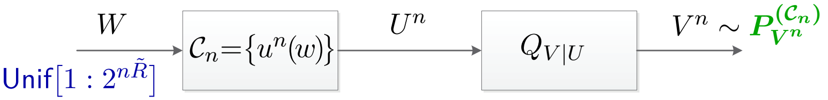


- **Random Codebook:** $\mathsf{C}_n = \{U^n(w)\}_w \overset{iid}{\sim} Q_U^n$.

Soft-Covering - Setup



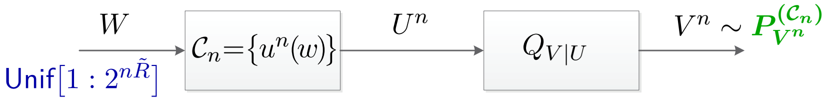
- **Random Codebook:** $\mathsf{C}_n = \{U^n(w)\}_w \overset{iid}{\sim} Q_U^n$.



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

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

Soft-Covering - Setup

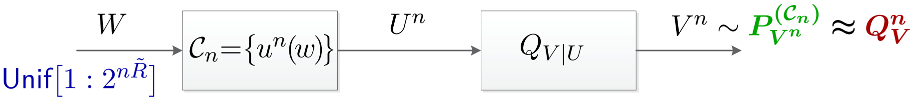


- **Random Codebook:** $\mathsf{C}_n = \{U^n(w)\}_w \overset{iid}{\sim} Q_U^n$.

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

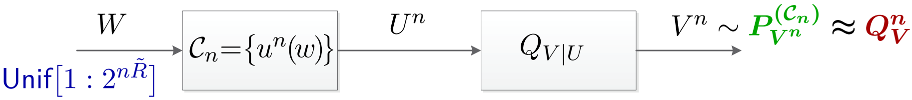
- **Target IID Distribution:** Q_V^n (Q_V is the marginal of $Q_U Q_{V|U}$).

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 (Q_V is the marginal of $Q_U Q_{V|U}$).

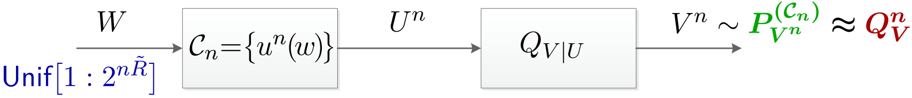
Soft-Covering - Setup



- **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 (Q_V is the marginal of $Q_U Q_{V|U}$).

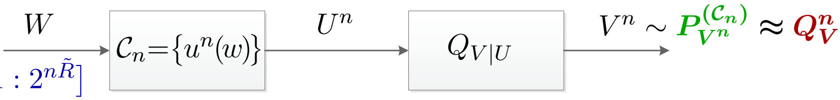
⋆ **Goal:** Choose $\tilde{R}$ (codebook size) s.t. $P_{V^n}^{(\mathcal{C}_n)} \approx Q_V^n$ ⋆

Soft-Covering - Results



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

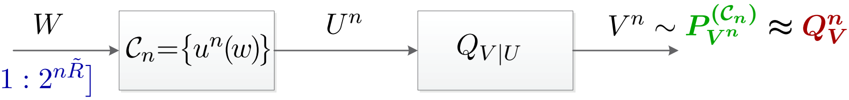
Soft-Covering - Results



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

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

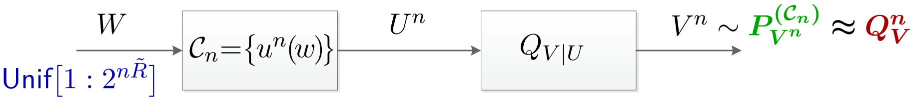
Soft-Covering - Results



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

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

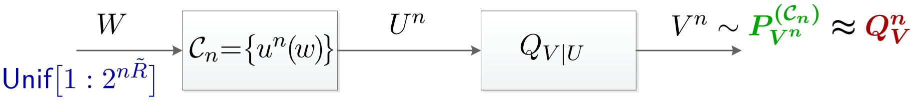
Soft-Covering - Results



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

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

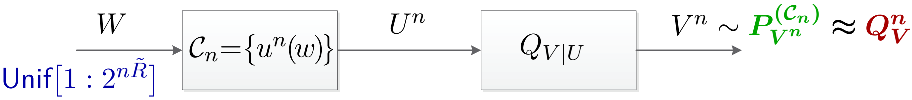
Soft-Covering - Results



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

- **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

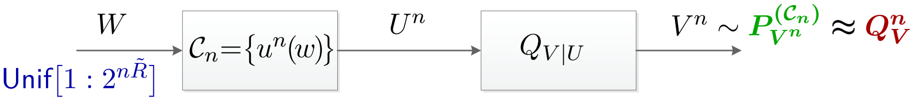


Lemma (ZG-Cuff-Permuter 2016)

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

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

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. for n large enough

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

- **Satisfy exponentially many security constraints:**

Strong Soft-Covering Lemma

$$\underset{\text{Unif}\left[1\,:\,2^{n\tilde{R}}\right]}{\xrightarrow{\;W\;}} \boxed{\mathcal{C}_n=\{u^n(w)\}} \xrightarrow{\;U^n\;} \boxed{Q_{V|U}} \xrightarrow{\;V^n \sim P_{V^n}^{(\mathcal{C}_n)} \approx Q_V^n\;}$$

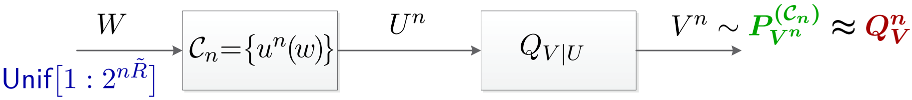
Lemma (ZG-Cuff-Permuter 2016)

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

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

- **Satisfy exponentially many security constraints:**
  - Semantic security.

Strong Soft-Covering Lemma



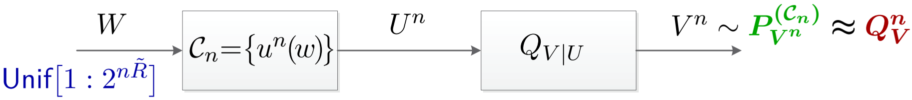
Lemma (ZG-Cuff-Permuter 2016)

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

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

- **Satisfy exponentially many security constraints:**
  - Semantic security.
  - Eavesdropper's channel uncertainty & active adversaries.

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. for* n *large enough*

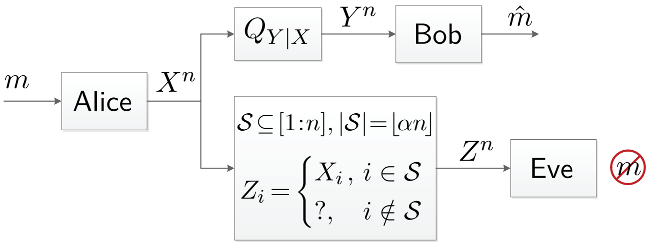
$$\mathbb{P}_{\mathsf{C}_n}\left(D\left(P^{(\mathsf{C}_n)}_{V^n} \middle\| Q^n_V \right) > e^{-n\gamma_1} \right) \leq e^{-e^{n\gamma_2}}$$

- **Satisfy exponentially many security constraints:**
  - Semantic security.
  - Eavesdropper's channel uncertainty & active adversaries.
- **Extensions:** Heterogeneous version, superposition codes.

Some Applications

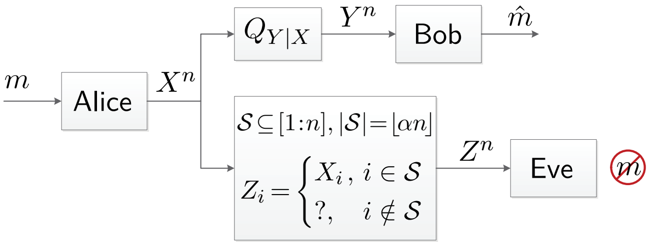
Wiretap Channels of Type II - Definition

[Ozarow-Wyner 1984]



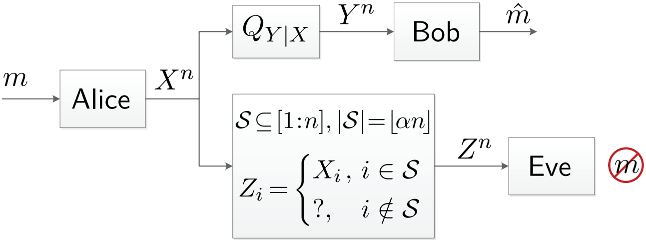
Wiretap Channels of Type II - Definition

[Ozarow-Wyner 1984]



- **Eve:** Can observe any $\lfloor\alpha n\rfloor$, $\alpha\in[0,1]$, of transmitted symbols.

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



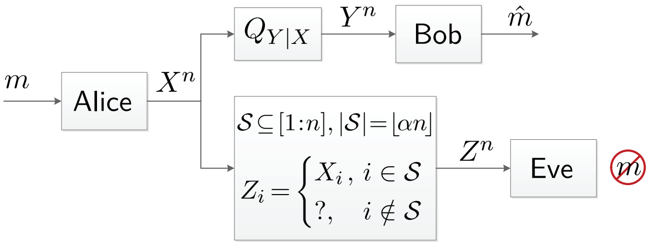
- **Eve:** Can observe any $\lfloor \alpha n \rfloor$, $\alpha \in [0, 1]$, of transmitted symbols.
- **Transmitted:**

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]

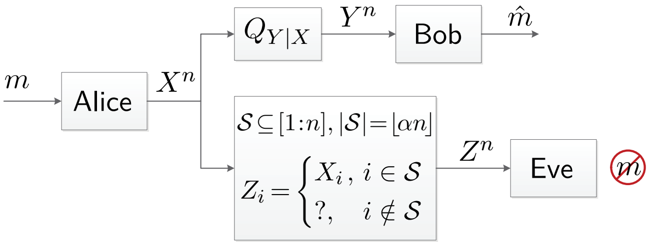


- **Eve:** Can observe any $\lfloor \alpha n \rfloor$, $\alpha \in [0, 1]$, of transmitted symbols.

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

$n = 10$ $\quad \alpha = 0.6$

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



- **Eve:** Can observe any $\lfloor\alpha n\rfloor$, $\alpha\in[0,1]$, of transmitted symbols.
- **Transmitted:**
- **Observed:**

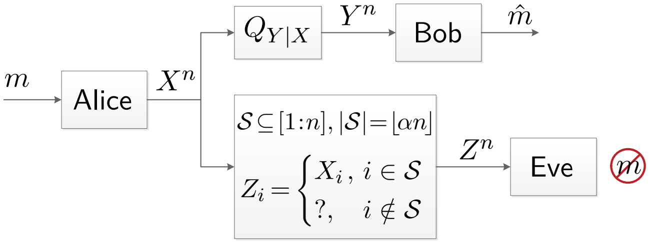
Transmitted:	0	0	1	0	1	1	1	0	1	0
Observed:	?	0	?	?	1	1	1	?	1	0

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

⋆ Ensure security versus all possible choices of observations ⋆

Wiretap Channels of Type II - Past Results

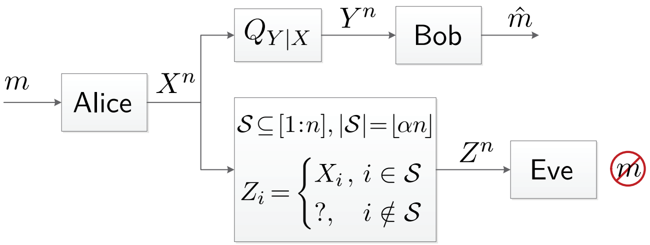
[Ozarow-Wyner 1984]



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

Wiretap Channels of Type II - Past Results

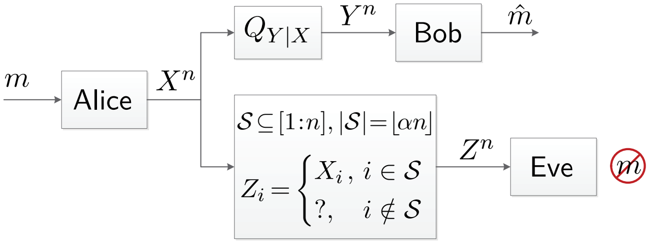
[Ozarow-Wyner 1984]



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

Wiretap Channels of Type II - Past Results

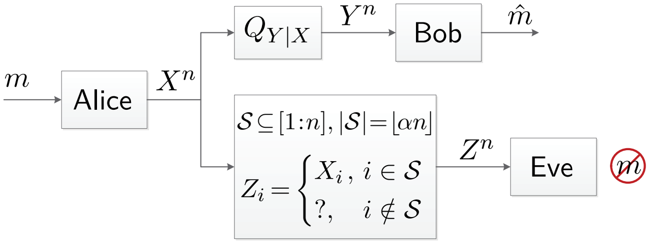
[Ozarow-Wyner 1984]



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

Wiretap Channels of Type II - Past Results

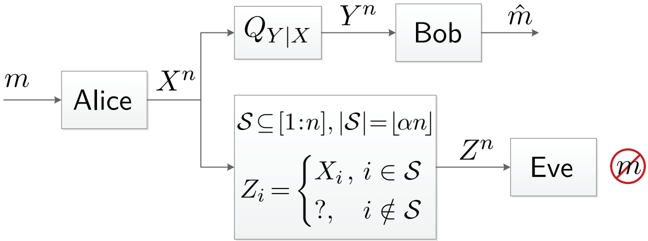
[Ozarow-Wyner 1984]



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

Wiretap Channels of Type II - Past Results

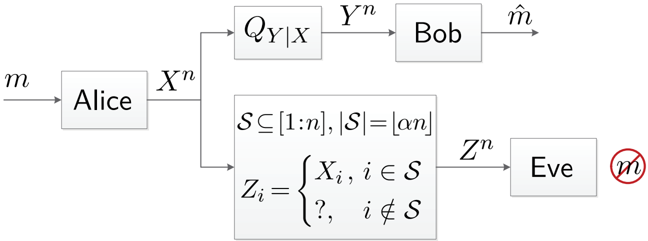
[Ozarow-Wyner 1984]



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

Wiretap Channels of Type II - SS-Capacity

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

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

Theorem (ZG-Cuff-Permuter 2016)

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

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

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

Wiretap Channels of Type II - SS-Capacity

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

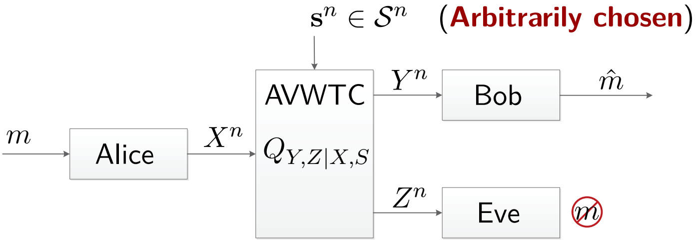
Theorem (ZG-Cuff-Permuter 2016)

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

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

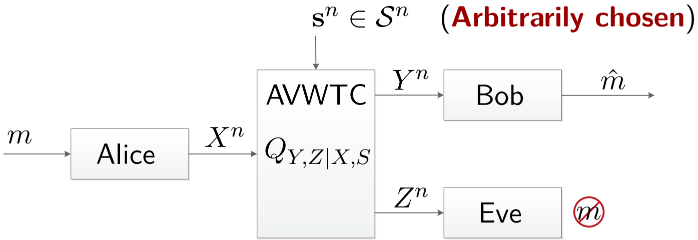
- RHS is the secrecy-capacity of WTC I with erasure DMC to Eve.
- Standard (erasure) wiretap code & Stronger tools for analysis.

A Generalization - Arbitrarily Varying WTCs



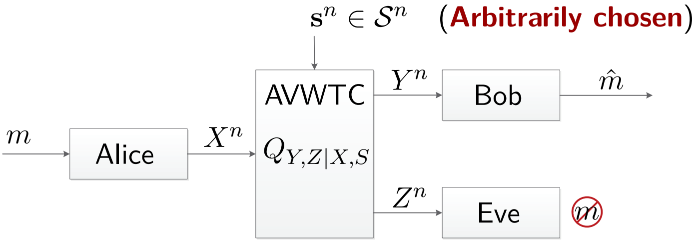
- Models **main** and **eavesdropper** channel uncertainty.

A Generalization - Arbitrarily Varying WTCs



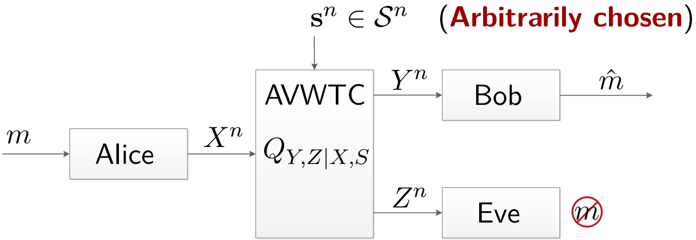
- Models **main** and **eavesdropper** channel uncertainty.
- Worst case analysis for **reliability** and **security**.

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

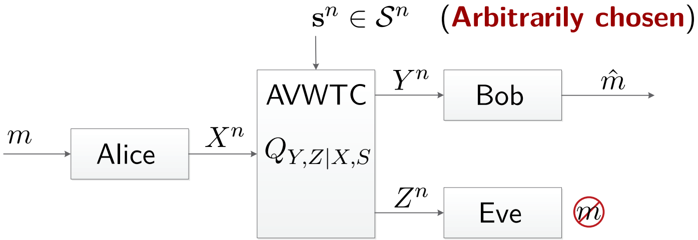


- Models **main** and **eavesdropper** channel uncertainty.
- Worst case analysis for **reliability** and **security**.
- **Type Constrained States:** Allowed $\boldsymbol{s^n}$ have empirical dist. $\approx \boldsymbol{Q_S}$:

Theorem (ZG-Cuff-Permuter 2016)

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

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. $\approx \boldsymbol{Q_S}$:

Theorem (ZG-Cuff-Permuter 2016)

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

★ **Subsumes WTC II model and result** ★

Summary

- **Strong SCLs:** Homogeneous, Heterogeneous, Superposition

Summary

- **Strong SCLs:** Homogeneous, Heterogeneous, Superposition
  - Double-exponential decay of $\mathbb{P}\big(\text{soft-covering not happening}\big)$.

Summary

- **Strong SCLs:** Homogeneous, Heterogeneous, Superposition
  - Double-exponential decay of $\mathbb{P}\big(\text{soft-covering not happening}\big)$.
  - Satisfy exponentially many soft-covering constraints.

Summary

- **Strong SCLs:** Homogeneous, Heterogeneous, Superposition
  - Double-exponential decay of $\mathbb{P}\big(\text{soft-covering not happening}\big)$.
  - Satisfy exponentially many soft-covering constraints.
- **Some Applications:**

Summary

- **Strong SCLs:** Homogeneous, Heterogeneous, Superposition
  - Double-exponential decay of $\mathbb{P}\big(\text{soft-covering not happening}\big)$.
  - Satisfy exponentially many soft-covering constraints.
- **Some Applications:**
  - Upgrade IT proofs to semantic security.

Summary

- **Strong SCLs:** Homogeneous, Heterogeneous, Superposition
  - Double-exponential decay of $\mathbb{P}\big(\text{soft-covering not happening}\big)$.
  - Satisfy exponentially many soft-covering constraints.
- **Some Applications:**
  - Upgrade IT proofs to semantic security.
  - Wiretap channels of type II with a noisy main channel.

Summary

- **Strong SCLs:** Homogeneous, Heterogeneous, Superposition
  - Double-exponential decay of $\mathbb{P}\big(\text{soft-covering not happening}\big)$.
  - Satisfy exponentially many soft-covering constraints.
- **Some Applications:**
  - Upgrade IT proofs to semantic security.
  - Wiretap channels of type II with a noisy main channel.
  - Arbitrarily varying wiretap channels.

Summary

- **Strong SCLs:** Homogeneous, Heterogeneous, Superposition
  - Double-exponential decay of $\mathbb{P}\big(\text{soft-covering not happening}\big)$.
  - Satisfy exponentially many soft-covering constraints.

- **Some Applications:**
  - Upgrade IT proofs to semantic security.
  - Wiretap channels of type II with a noisy main channel.
  - Arbitrarily varying wiretap channels.

Thank you!