Semantic Security in the Presence of Active Adversaries

Ziv Goldfeld
Joint work with Paul Cuff and Haim Permuter

Ben Gurion University

ECE Department Seminar, NJIT

March 8th, 2016

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 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.

Some Background

Basic Information Measures

$(X, Y) \sim P_{X,Y}$ discrete RVs

Basic Information Measures

$(X, Y) \sim P_{X,Y}$ discrete RVs

- **Entropy:** $$H(X) = H(P_X) = -\sum_{x \in \mathcal{X}} P_X(x) \log P_X(x).$$

Basic Information Measures

$(X,Y) \sim P_{X,Y}$ discrete RVs

- **Entropy:** $H(X) = H(P_X) = -\sum_{x\in\mathcal{X}} P_X(x)\log P_X(x).$
- **Conditional Entropy:** $H(X|Y) = \sum_{y\in\mathcal{Y}} P_Y(y)H(P_{X|Y=y}).$

Basic Information Measures

$(X,Y) \sim P_{X,Y}$ discrete RVs

- **Entropy:** $H(X) = H(P_X) = -\sum_{x\in\mathcal{X}} P_X(x)\log P_X(x).$
- **Conditional Entropy:** $H(X|Y) = \sum_{y\in\mathcal{Y}} P_Y(y) H(P_{X|Y=y}).$
- **Mutual Information:** $$\begin{aligned} I(X;Y) &= H(X) - H(X|Y) \\ &= H(Y) - H(Y|X). \end{aligned}$$

Basic Information Measures

$(X,Y) \sim P_{X,Y}$ discrete RVs

- **Entropy:** $H(X) = H(P_X) = -\sum_{x\in\mathcal{X}} P_X(x)\log P_X(x)$.
- **Conditional Entropy:** $H(X|Y) = \sum_{y\in\mathcal{Y}} P_Y(y) H(P_{X|Y=y})$.
- **Mutual Information:** $\begin{aligned} I(X;Y) &= H(X) - H(X|Y) \\ &= H(Y) - H(Y|X). \end{aligned}$
- **Relative Entropy:** P and Q PMFs on $\mathcal{X}$

$$D(P||Q) = \sum_{x\in\mathcal{X}} P(x)\log\frac{P(x)}{Q(x)}$$

Basic Information Measures

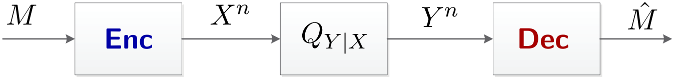
$(X, Y) \sim P_{X,Y}$ discrete RVs

- **Entropy:** $H(X) = H(P_X) = -\sum_{x\in\mathcal{X}} P_X(x)\log P_X(x).$
- **Conditional Entropy:** $H(X|Y) = \sum_{y\in\mathcal{Y}} P_Y(y)H(P_{X|Y=y}).$
- **Mutual Information:**
$$\begin{aligned} I(X;Y) &= H(X) - H(X|Y) \\ &= H(Y) - H(Y|X). \end{aligned}$$
- **Relative Entropy:** P and Q PMFs on $\mathcal{X}$
$$D(P||Q) = \sum_{x\in\mathcal{X}} P(x)\log\frac{P(x)}{Q(x)}$$

$$\star \quad I(X;Y) = D(P_{X,Y}||P_XP_Y) \quad \star$$

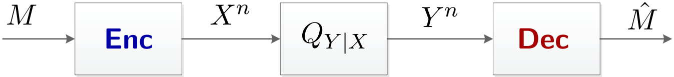
Channel Coding Theorem

[Shannon 1948]



Channel Coding Theorem

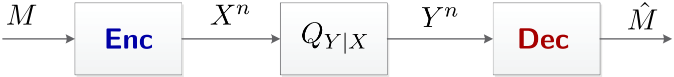
[Shannon 1948]



- **Message:** $M \sim \text{Unif}\big[1 : 2^{nR}\big]$.

Channel Coding Theorem

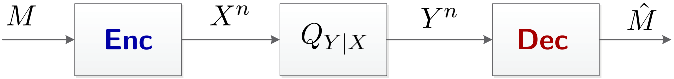
[Shannon 1948]



- **Message:** $M \sim \text{Unif}\big[1:2^{nR}\big]$.
- **$(\boldsymbol{n},\boldsymbol{R})$-Code:** **Enc:** $\big[1:2^{nR}\big] \to \mathcal{X}^n$; **Dec:** $\mathcal{Y}^n \to \big[1:2^{nR}\big]$.

Channel Coding Theorem

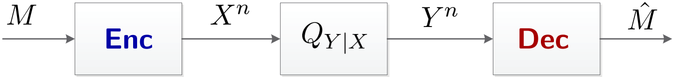
[Shannon 1948]



- **Message:** $M \sim \mathsf{Unif}\big[1:2^{nR}\big]$.
- **$(\boldsymbol{n},\boldsymbol{R})$-Code:** **Enc:** $\big[1:2^{nR}\big] \to \mathcal{X}^n$; **Dec:** $\mathcal{Y}^n \to \big[1:2^{nR}\big]$.
- **Channel:** $\mathbb{P}\big(Y^n = y^n \big| X^n = x^n\big) = \prod_{i=1}^{n} Q_{Y|X}(y_i|x_i) \triangleq Q^n_{Y|X}(y^n|x^n)$.

Channel Coding Theorem

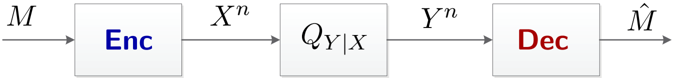
[Shannon 1948]



- **Message:** $M \sim \text{Unif}\big[1:2^{nR}\big]$.
- **(n,R)-Code:** **Enc:** $\big[1:2^{nR}\big] \to \mathcal{X}^n$; **Dec:** $\mathcal{Y}^n \to \big[1:2^{nR}\big]$.
- **Channel:** $\mathbb{P}\big(Y^n = y^n \big| X^n = x^n\big) = \prod_{i=1}^{n} Q_{Y|X}(y_i|x_i) \triangleq Q_{Y|X}^n(y^n|x^n)$.
- **Capacity:** $C \triangleq \sup\Big\{R \Big| \exists(n,R) - \text{codes s.t. } \mathbb{P}\big(M \neq \hat{M}\big) \underset{n}{\to} 0\Big\}$.

Channel Coding Theorem

[Shannon 1948]



- **Message:** $M \sim \text{Unif}\big[1:2^{nR}\big]$.
- **(n,R)-Code:** **Enc:** $\big[1:2^{nR}\big] \to \mathcal{X}^n$; **Dec:** $\mathcal{Y}^n \to \big[1:2^{nR}\big]$.
- **Channel:** $\mathbb{P}\big(Y^n = y^n \big| X^n = x^n\big) = \prod_{i=1}^{n} Q_{Y|X}(y_i|x_i) \triangleq Q^n_{Y|X}(y^n|x^n)$.
- **Capacity:** $C \triangleq \sup\left\{ R \middle| \exists (n,R) - \text{codes s.t. } \mathbb{P}\big(M \neq \hat{M}\big) \underset{n}{\to} 0 \right\}$.

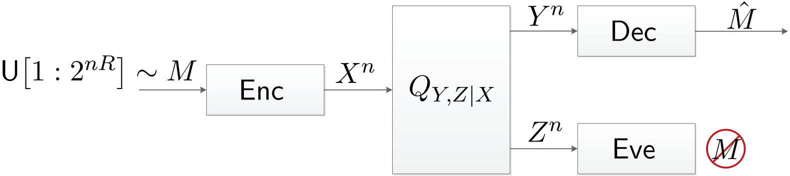
Theorem (Shannon 1948)

The capacity of a DMC $Q_{Y|X}$ *is* $C = \max_{Q_X} I(X;Y)$.

Wiretap Channels - Security Metrics

Wiretap Channels and Security Metrics

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



$\mathsf{U}\left[1:2^{nR}\right] \sim M$

Enc

X^n

$Q_{Y,Z|X}$

Y^n

Dec

$\hat{M}$

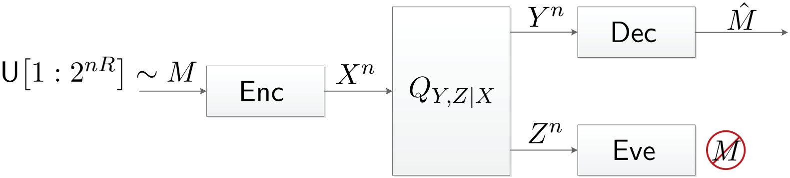
Z^n

Eve

$\cancel{M}$

Wiretap Channels and Security Metrics

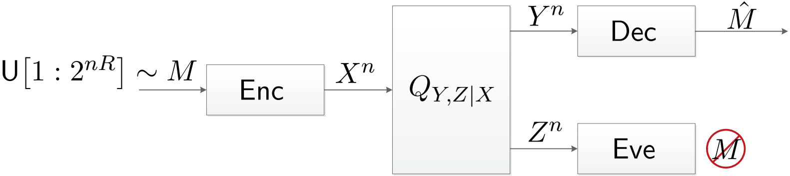
Degraded [Wyner 1975], General [Csiszár-Körner 1978]



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

Wiretap Channels and Security Metrics

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

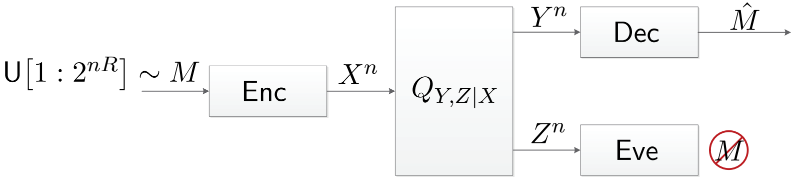


$\{\mathcal{C}_n\}_{n\in\mathbb{N}}$ - a sequence of (n,R)-codes

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

Wiretap Channels and Security Metrics

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

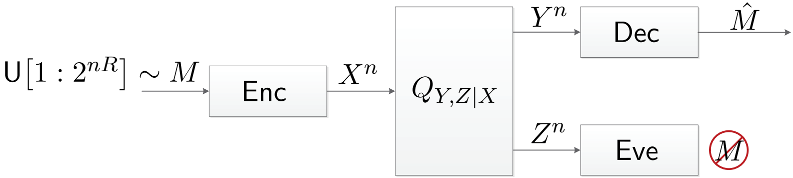


$\{\mathcal{C}_n\}_{n\in\mathbb{N}}$ - a sequence of (n,R)-codes

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

Wiretap Channels and Security Metrics

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

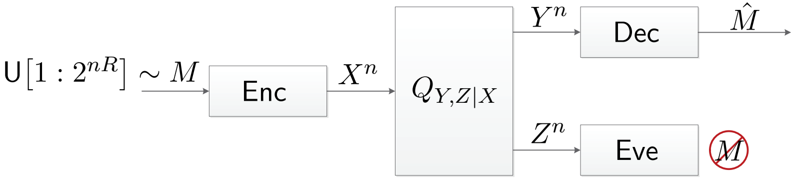


$\{\mathcal{C}_n\}_{n\in\mathbb{N}}$ - a sequence of (n,R)-codes

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

Wiretap Channels and Security Metrics

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

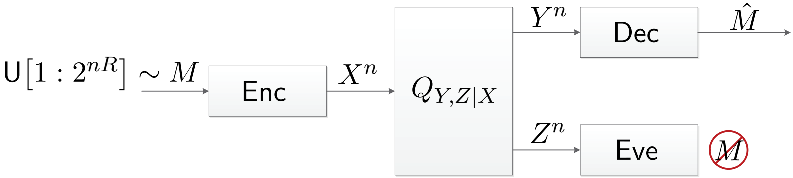


$\{\mathcal{C}_n\}_{n\in\mathbb{N}}$ - a sequence of (n,R)-codes

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

Wiretap Channels and Security Metrics

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

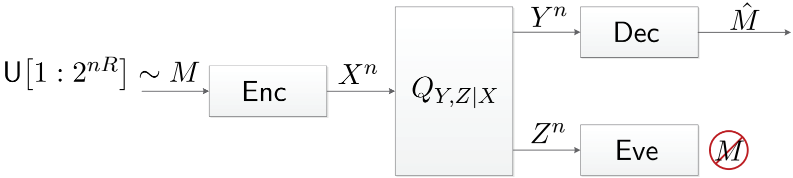


$\{\mathcal{C}_n\}_{n\in\mathbb{N}}$ - a sequence of (n,R)-codes

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

Wiretap Channels and Security Metrics

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

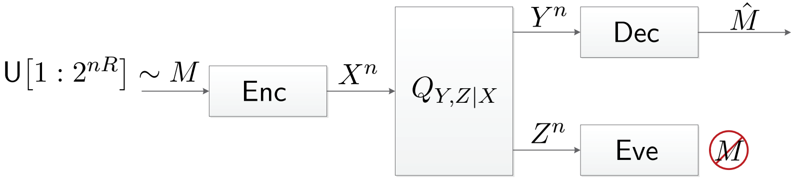


$\{\mathcal{C}_n\}_{n\in\mathbb{N}}$ - a sequence of (n,R)-codes

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

Wiretap Channels and Security Metrics

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



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

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

★ A stronger secrecy metric is required for applications ★

Semantic Security

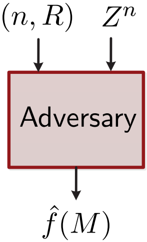
[Goldwasser-Micali 1982]

- **Test:** For <u>any</u> P_M learn about <u>any</u> $f(M)$

Semantic Security

[Goldwasser-Micali 1982]

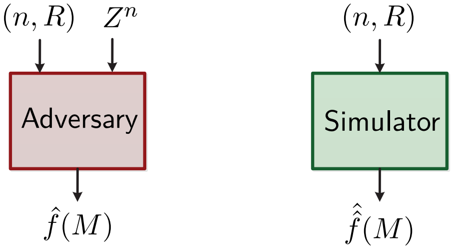
- **Test:** For <u>any</u> P_M learn about <u>any</u> $f(M)$



Semantic Security

[Goldwasser-Micali 1982]

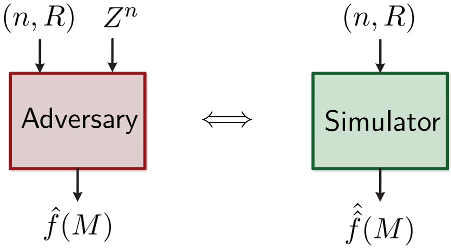
- **Test:** For <u>any</u> P_M learn about <u>any</u> $f(M)$



Semantic Security

[Goldwasser-Micali 1982]

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



(n, R) Z^n

Adversary

$\Longleftrightarrow$

(n, R)

Simulator

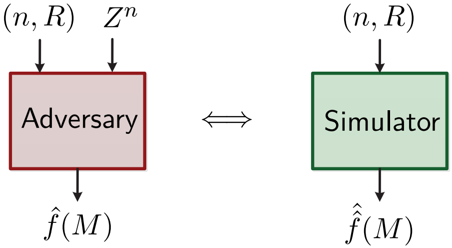
$\hat{f}(M)$

$\hat{\hat{f}}(M)$

Semantic Security

[Goldwasser-Micali 1982]

- **Test:** For <u>any</u> P_M learn about <u>any</u> $f(M)$



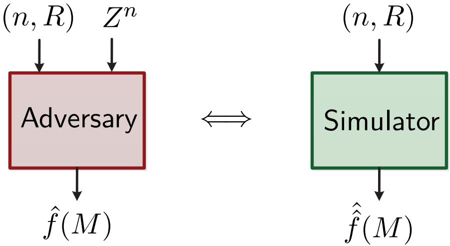
- **Equivalence:** [Bellare-Tessaro-Vardy 2012]

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

Semantic Security

[Goldwasser-Micali 1982]

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



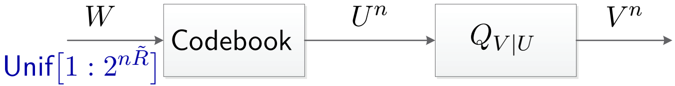
- **Equivalence:** [Bellare-Tessaro-Vardy 2012]

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

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

A Stronger Soft-Covering Lemma

Soft-Covering - Setup



W

$\mathsf{Unif}[1:2^{n\tilde{R}}]$

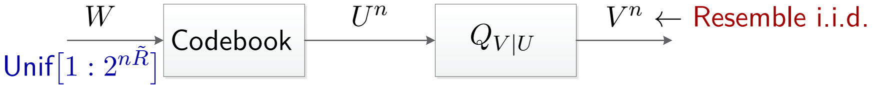
Codebook

U^n

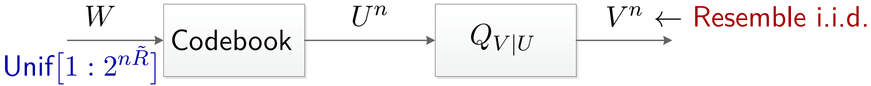
$Q_{V|U}$

V^n

Soft-Covering - Setup



Soft-Covering - Setup



W

Unif$[1 : 2^{n\tilde{R}}]$

Codebook

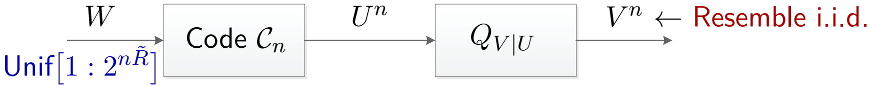
U^n

$Q_{V|U}$

$V^n \leftarrow$ Resemble i.i.d.

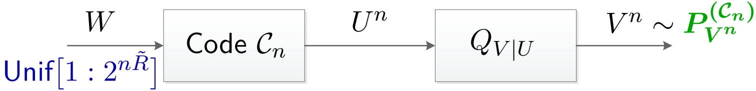
- **Random Codebook:** $\mathbb{C}_n = \left\{U^n(w)\right\}_w \overset{iid}{\sim} Q_U^n$.

Soft-Covering - Setup



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

Soft-Covering - Setup



W

Unif$[1:2^{n\tilde{R}}]$

Code $\mathcal{C}_n$

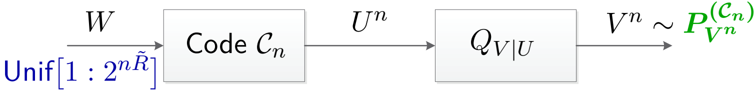
U^n

$Q_{V|U}$

$V^n \sim \boldsymbol{P_{V^n}^{(\mathcal{C}_n)}}$

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

Soft-Covering - Setup



W

Unif$[1:2^{n\tilde{R}}]$

Code $\mathcal{C}_n$

U^n

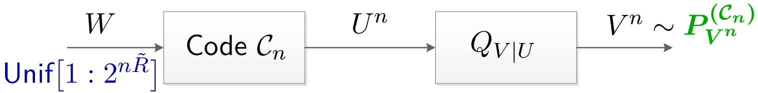
$Q_{V|U}$

$V^n \sim \boldsymbol{P_{V^n}^{(\mathcal{C}_n)}}$

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

$$P_{V^n}^{(\mathcal{C}_n)}(\mathbf{v}) = \sum_w 2^{-n\tilde{R}} Q_{V|U}^n\big(\mathbf{v}\big|\mathbf{u}(w,\mathcal{C}_n)\big).$$

Soft-Covering - Setup

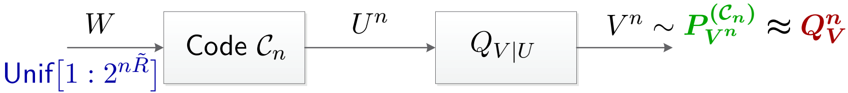


- **Random Codebook:** $\mathbb{C}_n = \{U^n(w)\}_w \overset{iid}{\sim} Q_U^n$.
- **Induced Output Distribution:** Codebook $\mathcal{C}_n \implies V^n \sim P_{V^n}^{(\mathcal{C}_n)}$

$$P_{V^n}^{(\mathcal{C}_n)}(\mathbf{v}) = \sum_w 2^{-n\tilde{R}} Q_{V|U}^n\big(\mathbf{v}\big|\mathbf{u}(w,\mathcal{C}_n)\big).$$

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

Soft-Covering - Setup

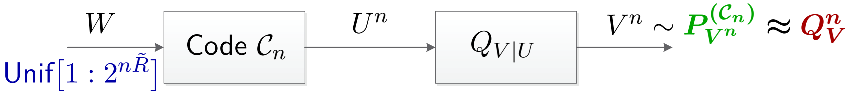


- **Random Codebook:** $\mathbb{C}_n = \{U^n(w)\}_w \overset{iid}{\sim} Q_U^n$.
- **Induced Output Distribution:** Codebook $\mathcal{C}_n \implies V^n \sim \boldsymbol{P_{V^n}^{(\mathcal{C}_n)}}$

$$P_{V^n}^{(\mathcal{C}_n)}(\mathbf{v}) = \sum_w 2^{-n\tilde{R}} Q_{V|U}^n\big(\mathbf{v}\big|\mathbf{u}(w,\mathcal{C}_n)\big).$$

- **Target IID Distribution:** $\boldsymbol{Q_V^n}$ marginal of $Q_U^n Q_{V|U}^n$.

Soft-Covering - Setup



W

Unif$[1:2^{n\tilde{R}}]$

Code $\mathcal{C}_n$

U^n

$Q_{V|U}$

$V^n \sim \boldsymbol{P_{V^n}^{(\mathcal{C}_n)}} \approx \boldsymbol{Q_V^n}$

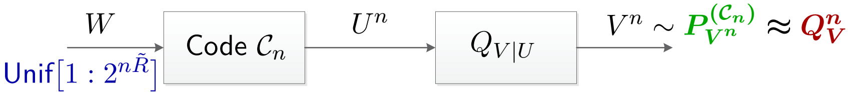
- **Random Codebook:** $\mathbb{C}_n = \{U^n(w)\}_w \overset{iid}{\sim} Q_U^n$.
- **Induced Output Distribution:** Codebook $\mathcal{C}_n \implies V^n \sim \boldsymbol{P_{V^n}^{(\mathcal{C}_n)}}$

$$P_{V^n}^{(\mathcal{C}_n)}(\mathbf{v}) = \sum_w 2^{-n\tilde{R}} Q_{V|U}^n\big(\mathbf{v}\big|\mathbf{u}(w,\mathcal{C}_n)\big).$$

- **Target IID Distribution:** $\boldsymbol{Q_V^n}$ marginal of $Q_U^n Q_{V|U}^n$.

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

Soft-Covering - Setup



W

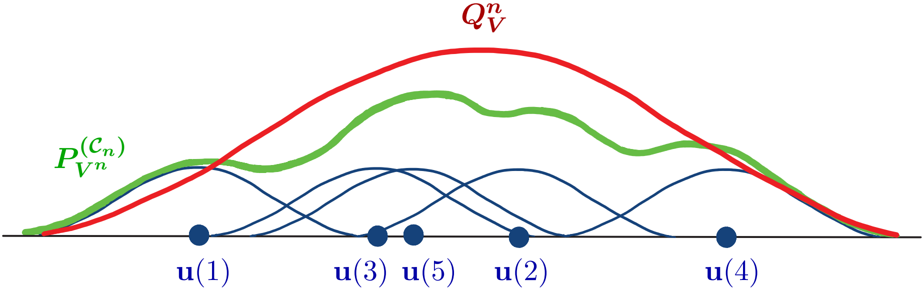
Unif$[1:2^{n\tilde{R}}]$

Code $\mathcal{C}_n$

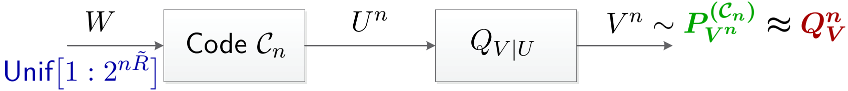
U^n

$Q_{V|U}$

$V^n \sim P_{V^n}^{(\mathcal{C}_n)} \approx Q_V^n$

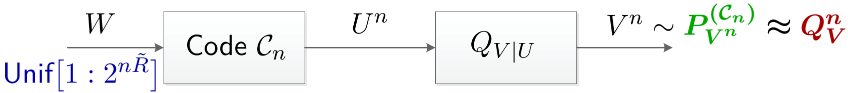


Soft-Covering - Results



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

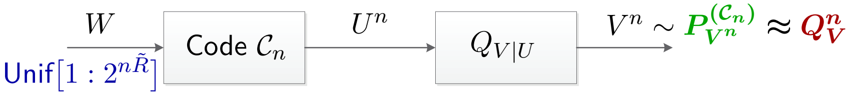
Soft-Covering - Results



$$\boldsymbol{\tilde{R} > I_Q(U;V)} \implies \boldsymbol{P^{(\mathcal{C}_n)}_{V^n}} \approx \boldsymbol{Q^n_V}$$

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

Soft-Covering - Results



W

$\text{Unif}[1:2^{n\tilde{R}}]$

Code $\mathcal{C}_n$

U^n

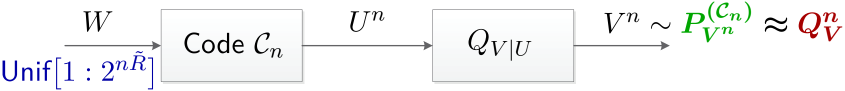
$Q_{V|U}$

$V^n \sim P_{V^n}^{(\mathcal{C}_n)} \approx Q_V^n$

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

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

Soft-Covering - Results



W

Unif$[1:2^{n\tilde{R}}]$

Code $\mathcal{C}_n$

U^n

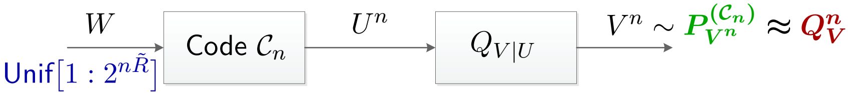
$Q_{V|U}$

$V^n \sim P_{V^n}^{(\mathcal{C}_n)} \approx Q_V^n$

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

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

Soft-Covering - Results



W

Unif$[1:2^{n\tilde{R}}]$

Code $\mathcal{C}_n$

U^n

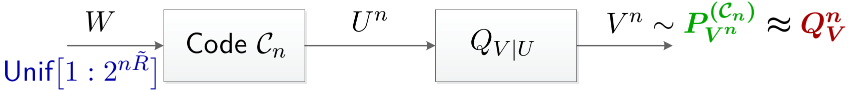
$Q_{V|U}$

$V^n \sim P_{V^n}^{(\mathcal{C}_n)} \approx Q_V^n$

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

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

A Stronger Soft-Covering Lemma



Lemma (Cuff 2015)

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

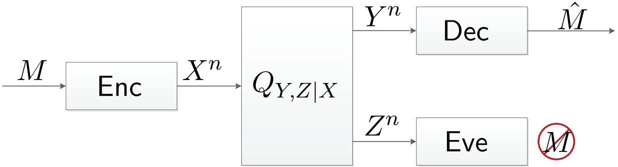
$$\mathbb{P}_{\mathbb{C}_n}\left(D\left(P_{V^n}^{(\mathbb{C}_n)} \middle\| Q_V^n \right) > e^{-n\gamma_1} \right) \leq e^{-e^{n\gamma_2}}$$

for n *sufficiently large.*

Revisit Wiretap Channels - Semantic Security

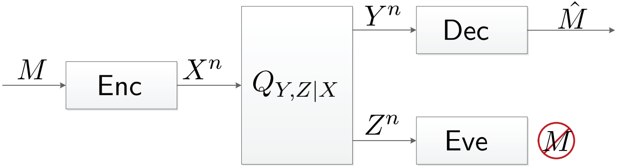
Semantic Security for Wiretap Channels

DM [Bellare-Tessaro-Vardy 2012], Gaussian [Tyagi-Vardy 2014]



Semantic Security for Wiretap Channels

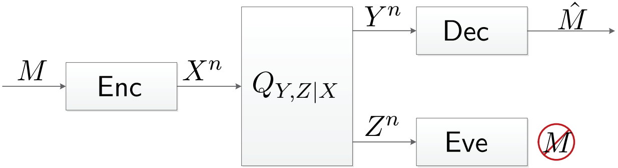
DM [Bellare-Tessaro-Vardy 2012], Gaussian [Tyagi-Vardy 2014]



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

Semantic Security for Wiretap Channels

DM [Bellare-Tessaro-Vardy 2012], Gaussian [Tyagi-Vardy 2014]



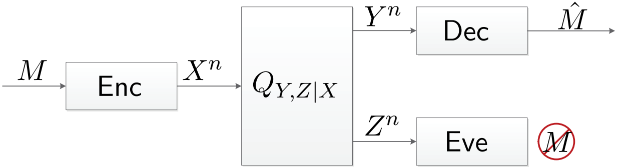
- **Security Metric:** $\max_{P_M} I_{\mathcal{C}_n}(M;Z^n) \xrightarrow[n\to\infty]{} 0.$

Theorem

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

Semantic Security for Wiretap Channels

DM [Bellare-Tessaro-Vardy 2012], Gaussian [Tyagi-Vardy 2014]



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

Theorem

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

- **Our Derivation:** **Union bound** & **Stronger soft-covering lemma**.

Semantic Security for Wiretap Channels - Derivation

1. **Wiretap Code:**

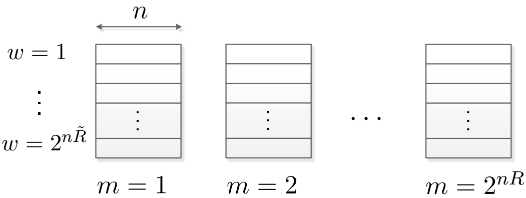
Semantic Security for Wiretap Channels - Derivation

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

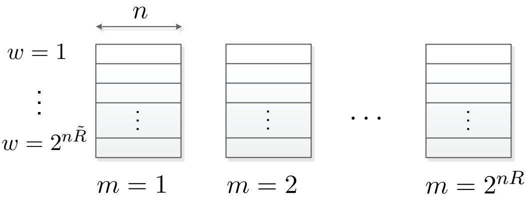
Semantic Security for Wiretap Channels - Derivation

① **Wiretap Code:**

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



Semantic Security for Wiretap Channels - Derivation

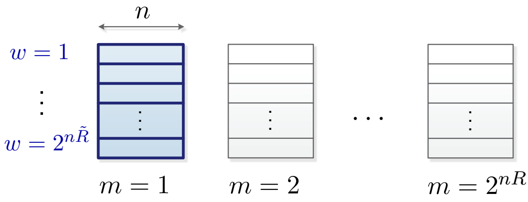


1. **Wiretap Code:**
   - $W \sim \mathsf{Unif}\big[1:2^{n\tilde{R}}\big]$.
   - $\mathbb{C}_n = \big\{X^n(m,w)\big\}_{m,w} \overset{iid}{\sim} Q_X^n$
2. **Preliminary Step:** $\max_{P_M} I_{\mathcal{C}_n}(M;Z^n) \leq \max_m D\Big(P^{(\mathcal{C}_n)}_{Z^n|M=m}\Big|\Big|Q_Z^n\Big)$

Semantic Security for Wiretap Channels - Derivation

① **Wiretap Code:**

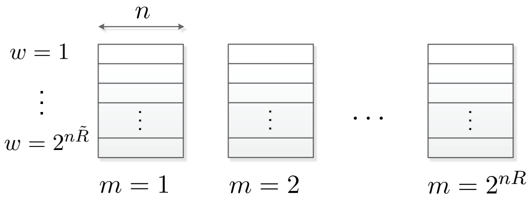
- $W \sim \mathsf{Unif}\big[1:2^{n\tilde{R}}\big]$.
- $\mathbb{C}_n = \big\{X^n(m,w)\big\}_{m,w} \overset{iid}{\sim} Q_X^n$



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

Semantic Security for Wiretap Channels - Derivation

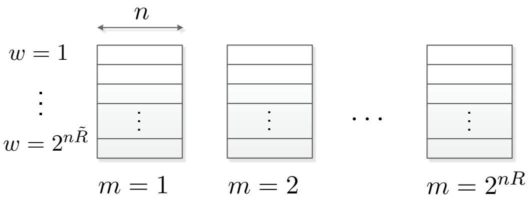
1. **Wiretap Code:**
   - $W \sim \text{Unif}\big[1:2^{n\tilde{R}}\big]$.
   - $\mathbb{C}_n = \big\{X^n(m,w)\big\}_{m,w} \overset{iid}{\sim} Q_X^n$



2. **Preliminary Step:** $\max\limits_{P_M} I_{\mathcal{C}_n}(M;Z^n) \leq \max\limits_{m} D\Big(P_{Z^n|M=m}^{(\mathcal{C}_n)}\Big|\Big|Q_Z^n\Big)$
3. **Union Bound & Stronger SCL:**

Semantic Security for Wiretap Channels - Derivation

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

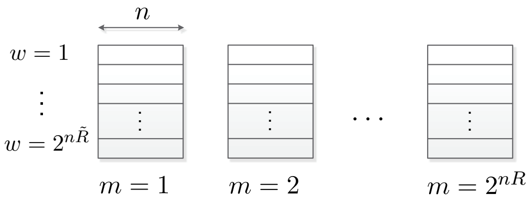


2. **Preliminary Step:** $\max\limits_{P_M} I_{\mathcal{C}_n}(M; Z^n) \leq \max\limits_{m} D\Big(P^{(\mathcal{C}_n)}_{Z^n|M=m}\Big|\Big|Q_Z^n\Big)$

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

$$\mathbb{P}\bigg(\Big\{\max_{P_M} I_{\mathbb{C}_n}(M; Z^n) \leq e^{-n\gamma_1}\Big\}^c\bigg)$$

Semantic Security for Wiretap Channels - Derivation



① **Wiretap Code:**

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

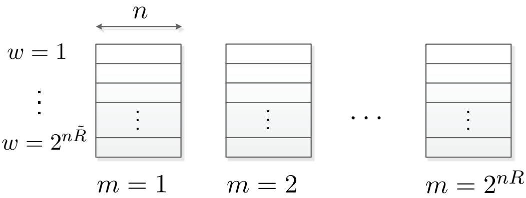
② **Preliminary Step:** $\max_{P_M} I_{\mathcal{C}_n}(M;Z^n)\leq\max_m D\left(P^{(\mathcal{C}_n)}_{Z^n|M=m}\middle|\middle|Q^n_Z\right)$

③ **Union Bound & Stronger SCL:**

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

Semantic Security for Wiretap Channels - Derivation

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



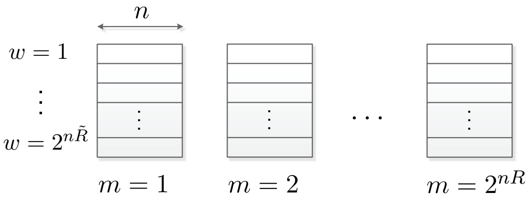
2. **Preliminary Step:** $\max\limits_{P_M} I_{\mathcal{C}_n}(M;Z^n) \le \max\limits_{m} D\Big(P^{(\mathcal{C}_n)}_{Z^n|M=m}\Big|\Big|Q_Z^n\Big)$

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

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

$$\le \sum_m \mathbb{P}\left(D\Big(P^{(\mathbb{C}_n)}_{Z^n|M=m}\Big|\Big|Q_Z^n\Big) > e^{-n\gamma_1}\right)$$

Semantic Security for Wiretap Channels - Derivation

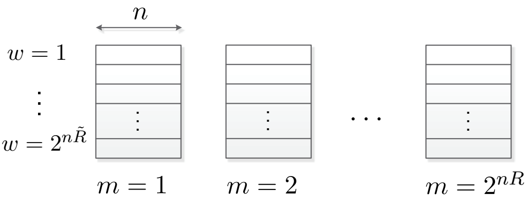


1. **Wiretap Code:**
   - $W \sim \text{Unif}\big[1:2^{n\tilde{R}}\big]$.
   - $\mathbb{C}_n = \big\{X^n(m,w)\big\}_{m,w} \overset{iid}{\sim} Q_X^n$
2. **Preliminary Step:** $\max\limits_{P_M} I_{\mathcal{C}_n}(M;Z^n) \leq \max\limits_{m} D\Big(P^{(\mathcal{C}_n)}_{Z^n|M=m}\Big|\Big|Q_Z^n\Big)$
3. **Union Bound & Stronger SCL:**

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

$$\leq \sum_m \mathbb{P}\bigg(\boldsymbol{D\Big(P^{(\mathbb{C}_n)}_{Z^n|M=m}\Big|\Big|Q_Z^n\Big) > e^{-n\gamma_1}}\bigg)$$

Semantic Security for Wiretap Channels - Derivation



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

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

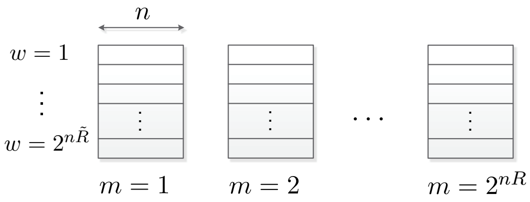
3. **Union Bound & Stronger SCL:**

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

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

Taking $\boxed{\tilde{R} > I(X;Z)}$ $\Longrightarrow$

Semantic Security for Wiretap Channels - Derivation



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

2. **Preliminary Step:** $\max\limits_{P_M} I_{\mathcal{C}_n}(M;Z^n) \le \max\limits_m D\left(P^{(\mathcal{C}_n)}_{Z^n|M=m}\middle\|Q^n_Z\right)$

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

$$\mathbb{P}\left(\left\{\max_{P_M} I_{\mathbb{C}_n}(M;Z^n) \le e^{-n\gamma_1}\right\}^c\right) \le \mathbb{P}\left(\max_m D\left(P^{(\mathbb{C}_n)}_{Z^n|M=m}\middle\|Q^n_Z\right) > e^{-n\gamma_1}\right)$$

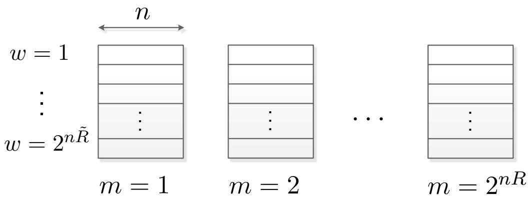
$$\le \sum_m \mathbb{P}\left(\boldsymbol{D\left(P^{(\mathbb{C}_n)}_{Z^n|M=m}\middle\|Q^n_Z\right) > e^{-n\gamma_1}}\right)$$

Taking $\boxed{\boldsymbol{\tilde{R} > I(X;Z)}}$ $\implies \le 2^{nR} e^{-e^{n\gamma_2}}$

Semantic Security for Wiretap Channels - Derivation

① **Wiretap Code:**

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



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

③ **Union Bound & Stronger SCL:**

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

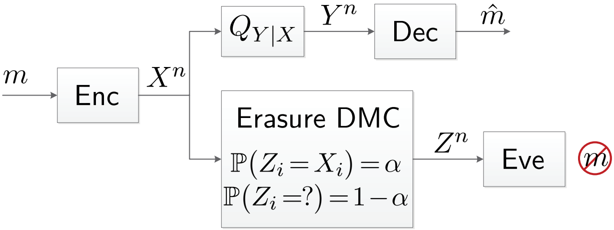
$$\leq \sum_m \mathbb{P}\bigg(\boldsymbol{D\Big(P^{(\mathbb{C}_n)}_{Z^n|M=m}\Big|\Big|Q_Z^n\Big) > e^{-n\gamma_1}}\bigg)$$

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

Wiretap Channels of Type II

Wiretap Channels of Type II - Preliminary

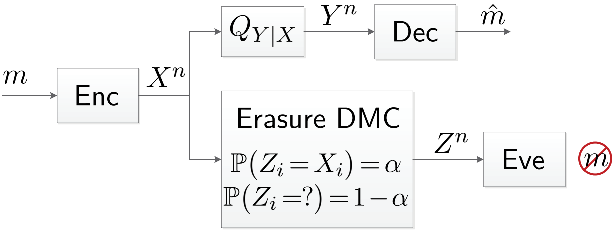
[Ozarow and Wyner 1984]



- **WTC I with Erasure DMC to Eve:**

Wiretap Channels of Type II - Preliminary

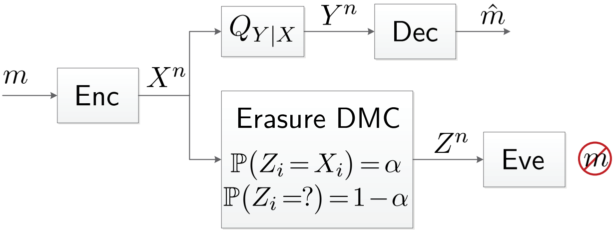
[Ozarow and Wyner 1984]



- **WTC I with Erasure DMC to Eve:**
  - **Eavesdropper** Observes $\approx \alpha n$ symbols of X^n.

Wiretap Channels of Type II - Preliminary

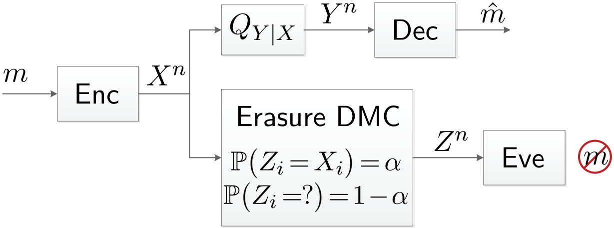
[Ozarow and Wyner 1984]



- **WTC I with Erasure DMC to Eve:**
  - **Eavesdropper** Observes $\approx \alpha n$ symbols of X^n.
  - Observed subset controlled by nature (i.i.d. process).

Wiretap Channels of Type II - Preliminary

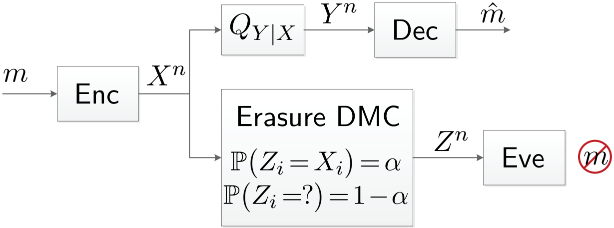
[Ozarow and Wyner 1984]



- WTC I with Erasure DMC to Eve:
  - **Eavesdropper** Observes $\approx \alpha n$ symbols of X^n.
  - Observed subset controlled by nature (i.i.d. process).
- WTC II: **Stronger Eve**.

Wiretap Channels of Type II - Preliminary

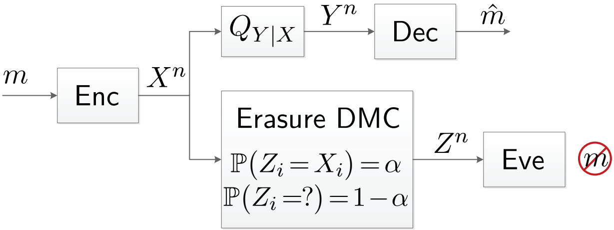
[Ozarow and Wyner 1984]



- **WTC I with Erasure DMC to Eve:**
  - **Eavesdropper** Observes $\approx \alpha n$ symbols of X^n.
  - Observed subset controlled by nature (i.i.d. process).
- **WTC II: Stronger Eve.**
  - Eve chooses which αn symbols of X^n to observe.

Wiretap Channels of Type II - Preliminary

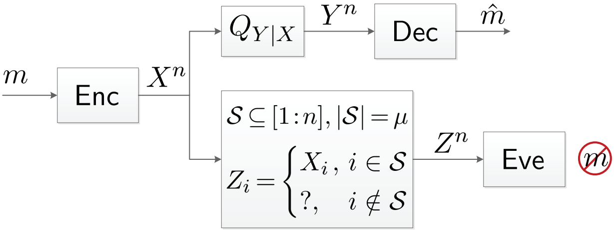
[Ozarow and Wyner 1984]



- **WTC I with Erasure DMC to Eve:**
  - **Eavesdropper** Observes $\approx \alpha n$ symbols of X^n.
  - Observed subset controlled by nature (i.i.d. process).
- **WTC II: Stronger Eve.**
  - Eve chooses which αn symbols of X^n to observe.
  - Ensure security versus all possible choices of observations.

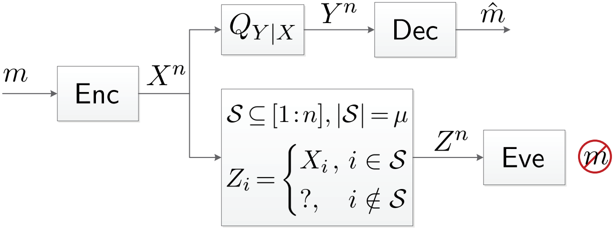
Wiretap Channels of Type II - Definition

[Ozarow-Wyner 1984]



Wiretap Channels of Type II - Definition

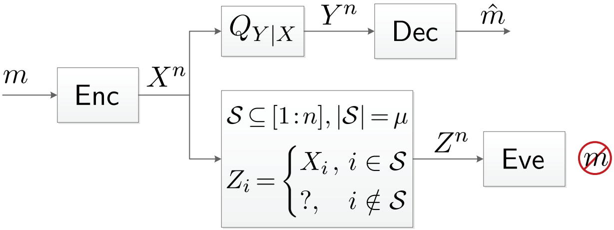
[Ozarow-Wyner 1984]



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

Wiretap Channels of Type II - Definition

[Ozarow-Wyner 1984]



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

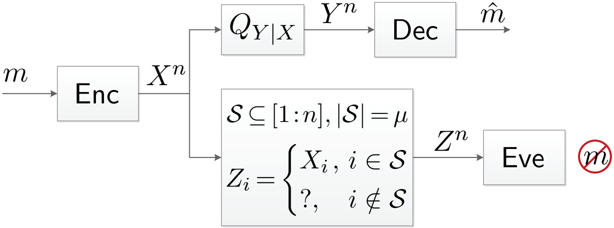
- **Transmitted:**

0	0	1	0	1	1	1	0	1	0

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

Wiretap Channels of Type II - Definition

[Ozarow-Wyner 1984]



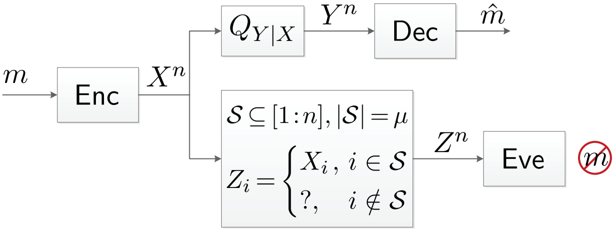
- **Eavesdropper:** Can observe a subset $\boldsymbol{\mathcal{S}} \subseteq [1:n]$ of size $\boldsymbol{\mu = \lfloor \alpha n \rfloor}$, $\boldsymbol{\alpha \in [0,1]}$, of transmitted symbols.

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

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

Wiretap Channels of Type II - Past Results

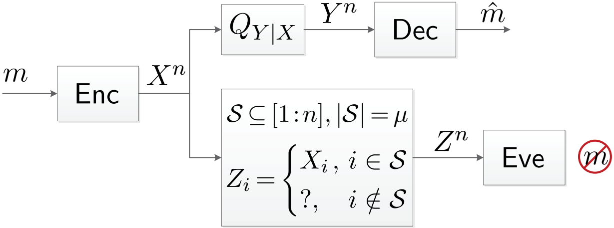
[Ozarow-Wyner 1984]



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

Wiretap Channels of Type II - Past Results

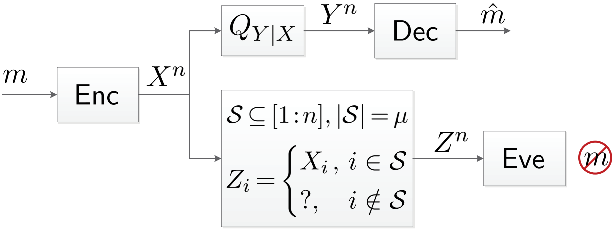
[Ozarow-Wyner 1984]



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

Wiretap Channels of Type II - Past Results

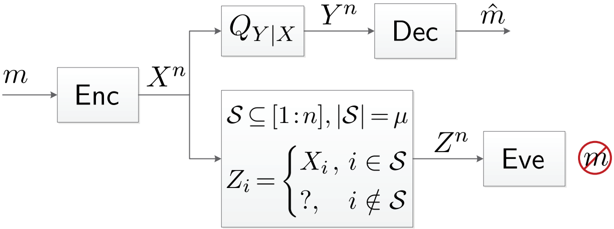
[Ozarow-Wyner 1984]



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

Wiretap Channels of Type II - Past Results

[Ozarow-Wyner 1984]

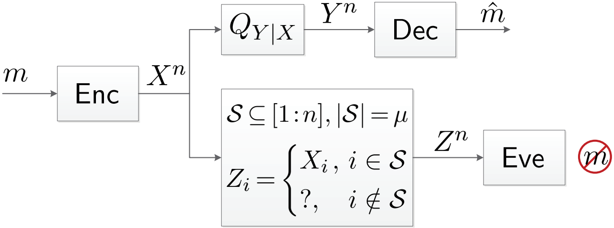


- **Ozarow-Wyner 1984:** Noiseless main channel
    - Rate equivocation region.
    - Coset coding.

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

Wiretap Channels of Type II - Past Results

[Ozarow-Wyner 1984]

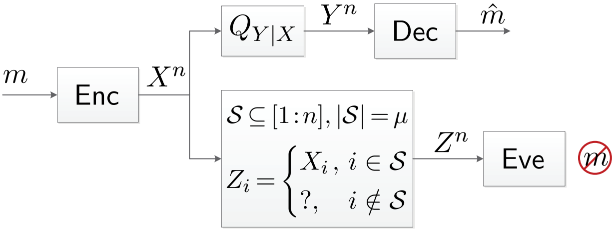


- **Ozarow-Wyner 1984:** Noiseless main channel
  - Rate equivocation region.
  - Coset coding.

- **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 2015)

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

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

Wiretap Channels of Type II - SS-Capacity

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

Theorem (ZG-Cuff-Permuter 2015)

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

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

- **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 (ZG-Cuff-Permuter 2015)

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

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

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

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 2015)

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

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

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

WTC II SS-Capacity - Achievability for U=X

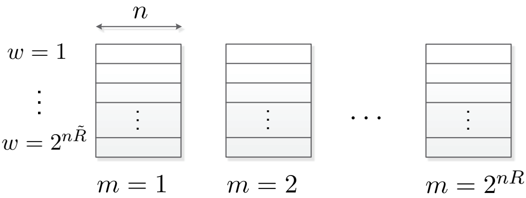
1. **Wiretap Code:**

WTC II SS-Capacity - Achievability for U=X

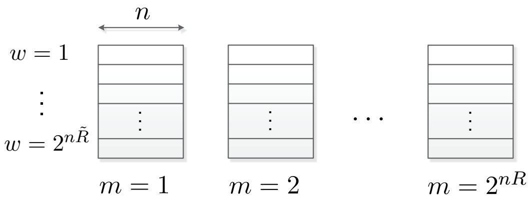
1. **Wiretap Code:**
   - $W \sim \mathsf{Unif}\big[1:2^{n\tilde{R}}\big]$.

WTC II SS-Capacity - Achievability for U=X

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



WTC II SS-Capacity - Achievability for U=X



① **Wiretap Code:**

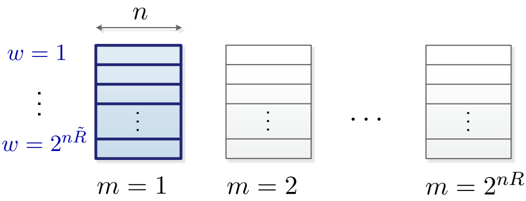
- $W\sim\text{Unif}\big[1:2^{n\tilde{R}}\big]$.
- $\mathbb{C}_n=\big\{X^n(m,w)\big\}_{m,w}\overset{iid}{\sim}Q_X^n$

② **Preliminary Step:**

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

WTC II SS-Capacity - Achievability for U=X

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

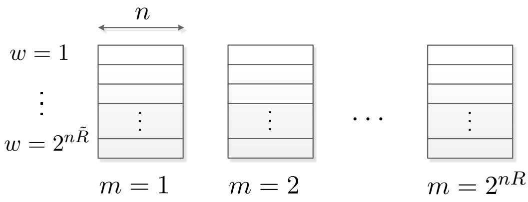


2. **Preliminary Step:**

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

WTC II SS-Capacity - Achievability for U=X

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

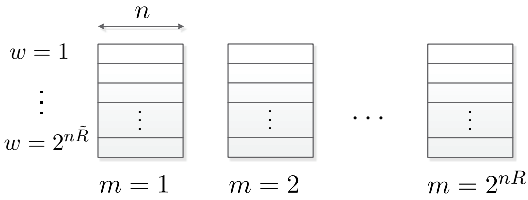


2. **Preliminary Step:** $$\max_{\substack{P_M,\mathcal{S}:\\|\mathcal{S}|=\mu}} I_{\mathcal{C}_n}(M;Z^n) \leq \max_{\substack{m,\mathcal{S}:\\|\mathcal{S}|=\mu}} D\Big(P^{(\mathcal{C}_n,\mathcal{S})}_{Z^\mu|M=m}\Big|\Big|Q_Z^\mu\Big)$$

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

WTC II SS-Capacity - Achievability for U=X

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

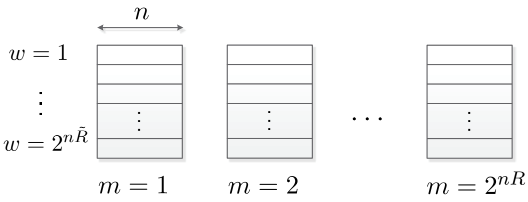


2. **Preliminary Step:** $\max_{\substack{P_M,\mathcal{S}:\\|\mathcal{S}|=\mu}} I_{\mathcal{C}_n}(M;Z^n) \leq \max_{\substack{m,\mathcal{S}:\\|\mathcal{S}|=\mu}} D\left(P^{(\mathcal{C}_n,\mathcal{S})}_{Z^\mu|M=m}\middle|\middle| Q_Z^\mu\right)$

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

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

WTC II SS-Capacity - Achievability for U=X



① **Wiretap Code:**

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

② **Preliminary Step:**

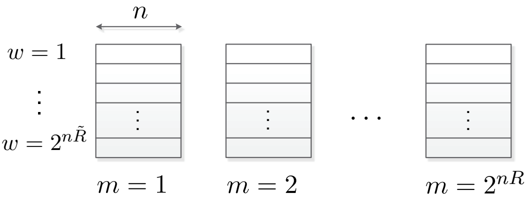
$$\max_{\substack{P_M,\mathcal{S}:\\ |\mathcal{S}|=\mu}} I_{\mathcal{C}_n}(M;Z^n) \leq \max_{\substack{m,\mathcal{S}:\\ |\mathcal{S}|=\mu}} D\Big(P^{(\mathcal{C}_n,\mathcal{S})}_{Z^\mu|M=m}\Big|\Big|Q^\mu_Z\Big)$$

③ **Union Bound & Stronger SCL:**

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

WTC II SS-Capacity - Achievability for U=X

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



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

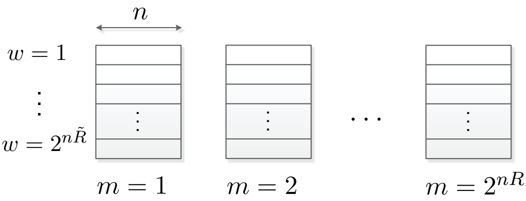
3. **Union Bound & Stronger SCL:**

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

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

WTC II SS-Capacity - Achievability for U=X

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



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

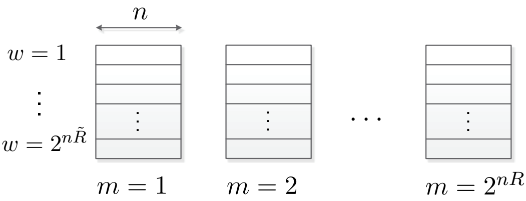
3. **Union Bound & Stronger SCL:**

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

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

WTC II SS-Capacity - Achievability for U=X

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



2. **Preliminary Step:**

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

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

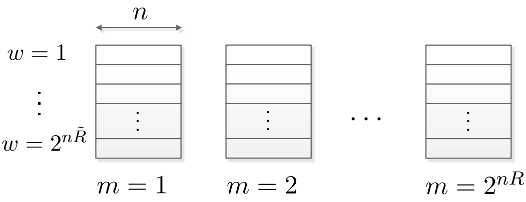
$$\mathbb{P}\left(\left\{\max_{P_M,\mathcal{S}} I_{\mathbb{C}_n}(M;Z^n)\le e^{-n\gamma_1}\right\}^c\right)\le\mathbb{P}\left(\max_{m,\mathcal{S}} D\left(P^{(\mathbb{C}_n,\mathcal{S})}_{Z^\mu|M=m}\middle|\middle|Q^\mu_Z\right)>e^{-n\gamma_1}\right)$$

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

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

WTC II SS-Capacity - Achievability for U=X

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



2. **Preliminary Step:**

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

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

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

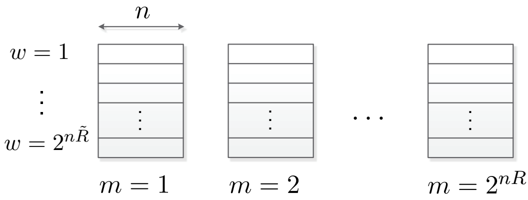
$$\leq \sum_{m,\mathcal{S}} \mathbb{P}\bigg(\boldsymbol{D\Big(P^{(\mathbb{C}_n,\mathcal{S})}_{Z^\mu|M=m}\Big|\Big|Q_Z^\mu\Big) > e^{-n\gamma_1}}\bigg)$$

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

WTC II SS-Capacity - Achievability for U=X

① **Wiretap Code:**

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



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

③ **Union Bound & Stronger SCL:**

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

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

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

WTC II SS-Capacity - Achievability for U=X

Finalization:

WTC II SS-Capacity - Achievability for U=X

Finalization:

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

WTC II SS-Capacity - Achievability for U=X

Finalization:

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

WTC II SS-Capacity - Achievability for U=X

Finalization:

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

WTC II SS-Capacity - Achievability for U=X

Finalization:

- **Semantic Security:** Satisfied if $\tilde{R} > \alpha H(X)$
- **Reliability:** Successfully decode (M, W) if $R + \tilde{R} < I(X;Y)$.
- **Rate Bound:** $R < I(X;Y) - \alpha H(X)$ is achievable.
- **Channel Prefixing:** Prefixing $Q_{X|U}$ achieves $I(U;Y) - \alpha I(U;X)$.

WTC II SS-Capacity - Converse

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

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

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

- **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

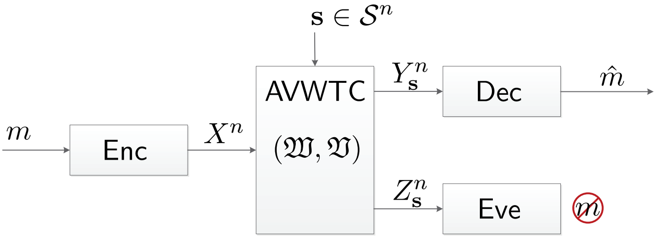
SS-capacity WTC II $\leq$ **Weak-secrecy-capacity WTC I**

- **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.

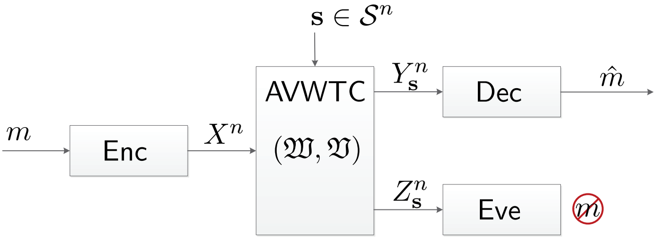
Arbitrarily Varying Wiretap Channels

Arbitrarily Varying Wiretap Channels - Definition



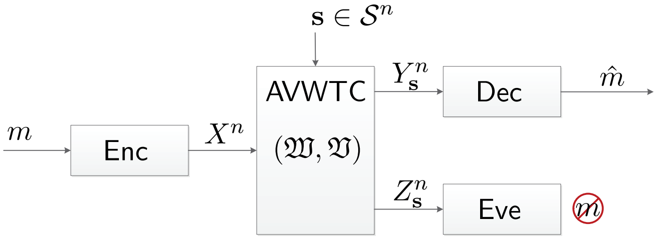
- Models **main** and **eavesdropper** channel uncertainty:

Arbitrarily Varying Wiretap Channels - Definition



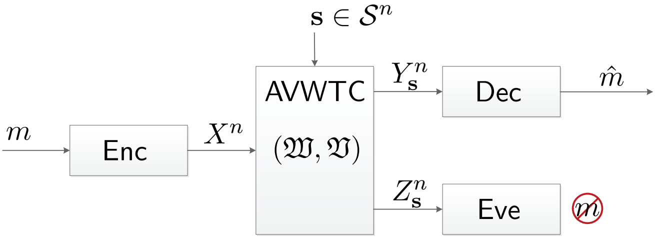
- Models **main** and **eavesdropper** channel uncertainty:
    - $\mathfrak{W} = \left\{ W_s : \mathcal{X} \to \mathcal{P}(\mathcal{Y}) \middle| s \in \mathcal{S} \right\}$.

Arbitrarily Varying Wiretap Channels - Definition



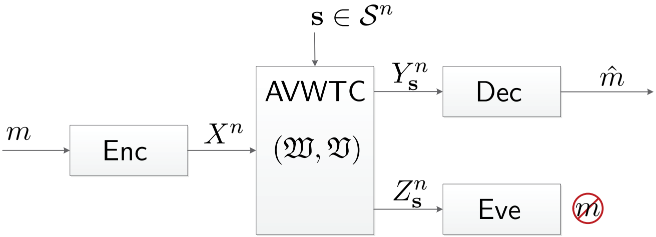
- Models **main** and **eavesdropper** channel uncertainty:
  - $\mathfrak{W} = \Big\{ W_s : \mathcal{X} \to \mathcal{P}(\mathcal{Y}) \Big| s \in \mathcal{S} \Big\}$.
  - $\mathfrak{V} = \Big\{ V_s : \mathcal{X} \to \mathcal{P}(\mathcal{Z}) \Big| s \in \mathcal{S} \Big\}$.

Arbitrarily Varying Wiretap Channels - Definition



- Models **main** and **eavesdropper** channel uncertainty:
  - $\mathfrak{W} = \left\{ W_s : \mathcal{X} \to \mathcal{P}(\mathcal{Y}) \middle| s \in \mathcal{S} \right\}$.
  - $\mathfrak{V} = \left\{ V_s : \mathcal{X} \to \mathcal{P}(\mathcal{Z}) \middle| s \in \mathcal{S} \right\}$.
- **DMC:** $W_{\mathbf{s}}^n(y^n|x^n) = \prod_{i=1}^{n} W_{s_i}(y_i|x_i)$; similarly for $V_{\mathbf{s}}^n$.

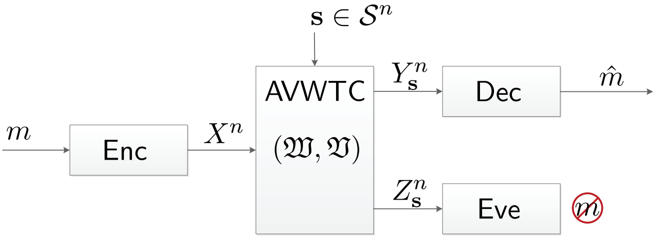
Arbitrarily Varying Wiretap Channels - Definition



- Models **main** and **eavesdropper** channel uncertainty:
  - $\mathfrak{W} = \left\{W_s : \mathcal{X} \to \mathcal{P}(\mathcal{Y}) \middle| s \in \mathcal{S}\right\}$.
  - $\mathfrak{V} = \left\{V_s : \mathcal{X} \to \mathcal{P}(\mathcal{Z}) \middle| s \in \mathcal{S}\right\}$.
- **DMC:** $W^n_{\mathbf{s}}(y^n|x^n) = \prod_{i=1}^{n} W_{s_i}(y_i|x_i)$; similarly for $V^n_{\mathbf{s}}$.

★ **Challenge:** Subsumes compound WTC & Exp. many states.★

Arbitrarily Varying Wiretap Channels - Definition



- Models **main** and **eavesdropper** channel uncertainty:
  - $\mathfrak{W} = \left\{ W_s : \mathcal{X} \to \mathcal{P}(\mathcal{Y}) \middle| s \in \mathcal{S} \right\}$.
  - $\mathfrak{V} = \left\{ V_s : \mathcal{X} \to \mathcal{P}(\mathcal{Z}) \middle| s \in \mathcal{S} \right\}$.
- **DMC:** $W^n_{\mathbf{s}}(y^n|x^n) = \prod_{i=1}^{n} W_{s_i}(y_i|x_i)$; similarly for $V^n_{\mathbf{s}}$.

★ **Challenge:** Subsumes compound WTC & **Exp. many states**.★

Arbitrarily Varying Wiretap Channels - Codes

- **Deterministic Code:** $c_n = (f, \phi)$ standard definition

Arbitrarily Varying Wiretap Channels - Codes

- **Deterministic Code:** $c_n = (f, \phi)$ standard definition
  - f - Stochastic encoder (local randomness).

Arbitrarily Varying Wiretap Channels - Codes

- **Deterministic Code:** $c_n = (f, \phi)$ standard definition
    - f - Stochastic encoder (local randomness).
    - ϕ - Decoder.

Arbitrarily Varying Wiretap Channels - Codes

- **Deterministic Code:** $c_n = (f, \phi)$ standard definition
    - f - Stochastic encoder (local randomness).
    - ϕ - Decoder.
- **Correlated Random Code:** $\mathbb{C}_n = (\mathcal{C}_n, \Gamma_n, \mu_n)$

Arbitrarily Varying Wiretap Channels - Codes

- **Deterministic Code:** $c_n = (f, \phi)$ standard definition
  - f - Stochastic encoder (local randomness).
  - ϕ - Decoder.
- **Correlated Random Code:** $\mathbb{C}_n = (\mathcal{C}_n, \Gamma_n, \mu_n)$
  - $\mathcal{C}_n = \left\{c_n(\gamma)\right\}_{\gamma \in \Gamma_n}$ - Family of deterministic codes $c_n(\gamma) = (f_\gamma, \phi_\gamma)$.

Arbitrarily Varying Wiretap Channels - Codes

- **Deterministic Code:** $c_n = (f, \phi)$ standard definition
  - f - Stochastic encoder (local randomness).
  - ϕ - Decoder.
- **Correlated Random Code:** $\mathbb{C}_n = (\mathcal{C}_n, \Gamma_n, \mu_n)$
  - $\mathcal{C}_n = \big\{c_n(\gamma)\big\}_{\gamma \in \Gamma_n}$ - Family of deterministic codes $c_n(\gamma) = (f_\gamma, \phi_\gamma)$.
  - μ_n - PMF on Γ_n that chooses a code.

Arbitrarily Varying Wiretap Channels - Codes

- **Deterministic Code:** $c_n = (f, \phi)$ standard definition
  - f - Stochastic encoder (local randomness).
  - ϕ - Decoder.
- **Correlated Random Code:** $\mathbb{C}_n = (\mathcal{C}_n, \Gamma_n, \mu_n)$
  - $\mathcal{C}_n = \big\{c_n(\gamma)\big\}_{\gamma\in\Gamma_n}$ - Family of deterministic codes $c_n(\gamma) = (f_\gamma, \phi_\gamma)$.
  - μ_n - PMF on Γ_n that chooses a code.
- **CR Code Interpretation:**

Arbitrarily Varying Wiretap Channels - Codes

- **Deterministic Code:** $c_n = (f, \phi)$ standard definition
  - f - Stochastic encoder (local randomness).
  - ϕ - Decoder.
- **Correlated Random Code:** $\mathbb{C}_n = (\mathcal{C}_n, \Gamma_n, \mu_n)$
  - $\mathcal{C}_n = \big\{c_n(\gamma)\big\}_{\gamma\in\Gamma_n}$ - Family of deterministic codes $c_n(\gamma) = (f_\gamma, \phi_\gamma)$.
  - μ_n - PMF on Γ_n that chooses a code.
- **CR Code Interpretation:**
  - Legit parties choose code by a random experiment available to both.

Arbitrarily Varying Wiretap Channels - Codes

- **Deterministic Code:** $c_n = (f, \phi)$ standard definition
  - f - Stochastic encoder (local randomness).
  - ϕ - Decoder.
- **Correlated Random Code:** $\mathbb{C}_n = (\mathcal{C}_n, \Gamma_n, \mu_n)$
  - $\mathcal{C}_n = \big\{c_n(\gamma)\big\}_{\gamma \in \Gamma_n}$ - Family of deterministic codes $c_n(\gamma) = (f_\gamma, \phi_\gamma)$.
  - μ_n - PMF on Γ_n that chooses a code.
- **CR Code Interpretation:**
  - Legit parties choose code by a random experiment available to both.
  - CR is an additional resource for reliable communication.

Arbitrarily Varying Wiretap Channels - Codes

- **Deterministic Code:** $c_n = (f, \phi)$ standard definition
  - f - Stochastic encoder (local randomness).
  - ϕ - Decoder.
- **Correlated Random Code:** $\mathbb{C}_n = (\mathcal{C}_n, \Gamma_n, \mu_n)$
  - $\mathcal{C}_n = \big\{c_n(\gamma)\big\}_{\gamma\in\Gamma_n}$ - Family of deterministic codes $c_n(\gamma) = (f_\gamma, \phi_\gamma)$.
  - μ_n - PMF on Γ_n that chooses a code.
- **CR Code Interpretation:**
  - Legit parties choose code by a random experiment available to both.
  - CR is an additional resource for reliable communication.
  - CR should **not** be viewed as cryptographic key for secrecy.

Arbitrarily Varying Wiretap Channels - CR Codes

For a CR code $\mathbb{C}_n = (\mathcal{C}_n, \Gamma_n, \mu_n)$:

Arbitrarily Varying Wiretap Channels - CR Codes

For a CR code $\mathbb{C}_n = (\mathcal{C}_n, \Gamma_n, \mu_n)$:

- **Error Prob:** $\max\limits_{\substack{\mathbf{s}\in\mathcal{S}^n \\ m\in\mathcal{M}}} \quad \sum_{\gamma\in\Gamma_n} \mu_n(\gamma)\mathbb{P}_{c_n(\gamma)}\Big(\phi_\gamma(Y_{\mathbf{s}}^n) \neq m \Big| M = m\Big)$.

Arbitrarily Varying Wiretap Channels - CR Codes

For a CR code $\mathbb{C}_n = (\mathcal{C}_n, \Gamma_n, \mu_n)$:

- **Error Prob:** $\max_{\substack{\mathbf{s}\in\mathcal{S}^n \\ m\in\mathcal{M}}} \sum_{\gamma\in\Gamma_n} \mu_n(\gamma)\mathbb{P}_{c_n(\gamma)}\Big(\phi_\gamma(Y_\mathbf{s}^n) \neq m \Big| M = m\Big).$
  - **Maximal (states & messages) expected (codes)** error probability.

Arbitrarily Varying Wiretap Channels - CR Codes

For a CR code $\mathbb{C}_n = (\mathcal{C}_n, \Gamma_n, \mu_n)$:

- **Error Prob:** $$\max_{\substack{\mathbf{s}\in\mathcal{S}^n \\ m\in\mathcal{M}}} \sum_{\gamma\in\Gamma_n} \mu_n(\gamma)\mathbb{P}_{c_n(\gamma)}\Big(\phi_\gamma(Y_\mathbf{s}^n) \neq m \Big| M = m\Big).$$
  - Maximal (states & messages) expected (codes) error probability.
- **Semantic Security:** $$\max_{\substack{\mathbf{s}\in\mathcal{S}^n \\ P_M\in\mathcal{P}(\mathcal{M}) \\ \gamma\in\Gamma_n}} I_{c_n(\gamma)}(M; Z_\mathbf{s}^n).$$

Arbitrarily Varying Wiretap Channels - CR Codes

For a CR code $\mathbb{C}_{\boldsymbol{n}} = (\boldsymbol{\mathcal{C}_n}, \boldsymbol{\Gamma_n}, \boldsymbol{\mu_n})$:

- **Error Prob:** $$\max_{\substack{\mathbf{s}\in\mathcal{S}^n\\ m\in\mathcal{M}}} \sum_{\gamma\in\Gamma_n} \mu_n(\gamma)\mathbb{P}_{c_n(\gamma)}\Big(\phi_\gamma(Y_{\mathbf{s}}^n) \neq m \Big| M = m\Big).$$
  - Maximal (states & messages) expected (codes) error probability.
- **Semantic Security:** $$\max_{\substack{\mathbf{s}\in\mathcal{S}^n\\ P_M\in\mathcal{P}(\mathcal{M})\\ \gamma\in\Gamma_n}} I_{c_n(\gamma)}(M;Z_{\mathbf{s}}^n).$$
  - **Maximal (states & message PMFs & codes)** information leakage.

Arbitrarily Varying Wiretap Channels - CR Codes

For a CR code $\mathbb{C}_n = (\mathcal{C}_n, \Gamma_n, \mu_n)$:

- **Error Prob:** $\max\limits_{\substack{\mathbf{s}\in\mathcal{S}^n\\ m\in\mathcal{M}}} \sum_{\gamma\in\Gamma_n} \mu_n(\gamma)\mathbb{P}_{c_n(\gamma)}\Big(\phi_\gamma(Y_\mathbf{s}^n) \neq m \Big| M = m\Big).$
  - Maximal (states & messages) expected (codes) error probability.
- **Semantic Security:** $\max\limits_{\substack{\mathbf{s}\in\mathcal{S}^n\\ P_M\in\mathcal{P}(\mathcal{M})\\ \gamma\in\Gamma_n}} I_{c_n(\gamma)}(M; Z_\mathbf{s}^n).$
  - Maximal (states & message PMFs & codes) information leakage.
  - Removes benefit of correlated randomness for secrecy purposes.

Arbitrarily Varying Wiretap Channels - CR Codes

For a CR code $\mathbb{C}_n = (\mathcal{C}_n, \Gamma_n, \mu_n)$:

- **Error Prob:** $\max_{\substack{\mathbf{s}\in\mathcal{S}^n \\ m\in\mathcal{M}}} \sum_{\gamma\in\Gamma_n} \mu_n(\gamma)\mathbb{P}_{c_n(\gamma)}\Big(\phi_\gamma(Y_{\mathbf{s}}^n) \neq m\Big|M=m\Big).$
  - Maximal (states & messages) expected (codes) error probability.
- **Semantic Security:** $\max_{\substack{\mathbf{s}\in\mathcal{S}^n \\ P_M\in\mathcal{P}(\mathcal{M}) \\ \gamma\in\Gamma_n}} I_{c_n(\gamma)}(M;Z_{\mathbf{s}}^n).$
  - Maximal (states & message PMFs & codes) information leakage.
  - Removes benefit of correlated randomness for secrecy purposes.

Type Constrained AVWC: $Q_S\in\mathcal{P}(\mathcal{S})$ replace $\mathbf{s}\in\mathcal{S}^n$ with $\mathbf{s}\in\mathcal{T}_\delta^n(Q_S)$.

Arbitrarily Varying Wiretap Channels - CR Codes

For a CR code $\mathbb{C}_n = (\mathcal{C}_n, \Gamma_n, \mu_n)$:

- **Error Prob:** $\max\limits_{\substack{\mathbf{s}\in\mathcal{T}_\delta^n(Q_S)\\ m\in\mathcal{M}}} \sum_{\gamma\in\Gamma_n} \mu_n(\gamma)\mathbb{P}_{c_n(\gamma)}\Big(\phi_\gamma(Y_\mathbf{s}^n) \neq m \Big| M = m\Big).$
  - Maximal (states & messages) expected (codes) error probability.
- **Semantic Security:** $\max\limits_{\substack{\mathbf{s}\in\mathcal{T}_\delta^n(Q_S)\\ P_M\in\mathcal{P}(\mathcal{M})\\ \gamma\in\Gamma_n}} I_{c_n(\gamma)}(M; Z_\mathbf{s}^n).$
  - Maximal (states & message PMFs & codes) information leakage.
  - Removes benefit of correlated randomness for secrecy purposes.

Type Constrained AVWC: $Q_S\in\mathcal{P}(\mathcal{S})$ replace $\mathbf{s}\in\mathcal{S}^n$ with $\mathbf{s}\in\mathcal{T}_\delta^n(Q_S)$.

Arbitrarily Varying Wiretap Channels - Past Results

Unconstrained States:

Arbitrarily Varying Wiretap Channels - Past Results

Unconstrained States:

- **MolavianJazi Ph.D. 2009:** Weak-secrecy expected over codes

Arbitrarily Varying Wiretap Channels - Past Results

Unconstrained States:

- **MolavianJazi Ph.D. 2009:** Weak-secrecy expected over codes
  - Model.

Arbitrarily Varying Wiretap Channels - Past Results

Unconstrained States:

- **MolavianJazi Ph.D. 2009:** Weak-secrecy expected over codes
  - Model.
  - Single-letter lower and upper bounds on CR-capacity.

Arbitrarily Varying Wiretap Channels - Past Results

Unconstrained States:

- **MolavianJazi Ph.D. 2009:** Weak-secrecy expected over codes
  - Model.
  - Single-letter lower and upper bounds on CR-capacity.
  - Relation between CR-capacity and DC-capacity.

Arbitrarily Varying Wiretap Channels - Past Results

Unconstrained States:

- **MolavianJazi Ph.D. 2009:** Weak-secrecy expected over codes
  - Model.
  - Single-letter lower and upper bounds on CR-capacity.
  - Relation between CR-capacity and DC-capacity.
- **Wiese-Nötzel-Boche 2014:** Strong-secrecy maximal over codes

Arbitrarily Varying Wiretap Channels - Past Results

Unconstrained States:

- **MolavianJazi Ph.D. 2009:** Weak-secrecy expected over codes
    - Model.
    - Single-letter lower and upper bounds on CR-capacity.
    - Relation between CR-capacity and DC-capacity.
- **Wiese-Nötzel-Boche 2014:** Strong-secrecy maximal over codes
    - Multi-letter characterization of CR-capacity.

Arbitrarily Varying Wiretap Channels - Past Results

Unconstrained States:

- **MolavianJazi Ph.D. 2009:** Weak-secrecy expected over codes
  - Model.
  - Single-letter lower and upper bounds on CR-capacity.
  - Relation between CR-capacity and DC-capacity.
- **Wiese-Nötzel-Boche 2014:** Strong-secrecy maximal over codes
  - Multi-letter characterization of CR-capacity.
  - Relation between CR-capacity and DC-capacity.

Arbitrarily Varying Wiretap Channels - Past Results

Unconstrained States:

- **MolavianJazi Ph.D. 2009:** Weak-secrecy expected over codes
    - Model.
    - Single-letter lower and upper bounds on CR-capacity.
    - Relation between CR-capacity and DC-capacity.
- **Wiese-Nötzel-Boche 2014:** Strong-secrecy maximal over codes
    - Multi-letter characterization of CR-capacity.
    - Relation between CR-capacity and DC-capacity.
- **Boche-Schaefer-Poor 2015:** Strong-secrecy maximal over codes

Arbitrarily Varying Wiretap Channels - Past Results

Unconstrained States:

- **MolavianJazi Ph.D. 2009:** Weak-secrecy expected over codes
  - Model.
  - Single-letter lower and upper bounds on CR-capacity.
  - Relation between CR-capacity and DC-capacity.

- **Wiese-Nötzel-Boche 2014:** Strong-secrecy maximal over codes
  - Multi-letter characterization of CR-capacity.
  - Relation between CR-capacity and DC-capacity.

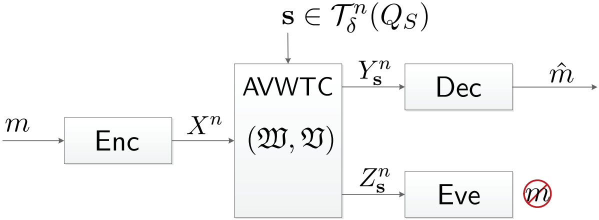
- **Boche-Schaefer-Poor 2015:** Strong-secrecy maximal over codes
  - CR-capacity is continuous in $(\mathfrak{W}, \mathfrak{V})$.

Arbitrarily Varying Wiretap Channels - Past Results

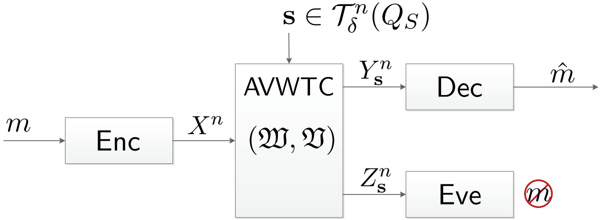
Unconstrained States:

- **MolavianJazi Ph.D. 2009:** Weak-secrecy expected over codes
    - Model.
    - Single-letter lower and upper bounds on CR-capacity.
    - Relation between CR-capacity and DC-capacity.
- **Wiese-Nötzel-Boche 2014:** Strong-secrecy maximal over codes
    - Multi-letter characterization of CR-capacity.
    - Relation between CR-capacity and DC-capacity.
- **Boche-Schaefer-Poor 2015:** Strong-secrecy maximal over codes
    - CR-capacity is continuous in $(\mathfrak{W}, \mathfrak{V})$.
    - DC-capacity is discontinuous in $(\mathfrak{W}, \mathfrak{V})$.

Type Constrained AVWTCs



Type Constrained AVWTCs

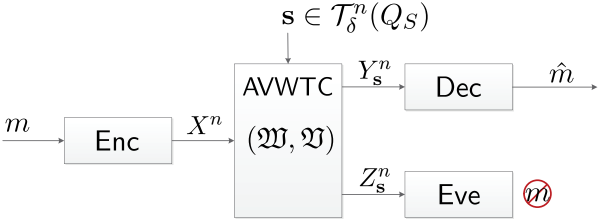


Theorem

$$C_{\mathrm{R}}(\mathfrak{W}, \mathfrak{V}, Q_S) = \max_{Q_{U,X}} \Big[I(U;Y) - I(U;Z|S) \Big]$$

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

Type Constrained AVWTCs



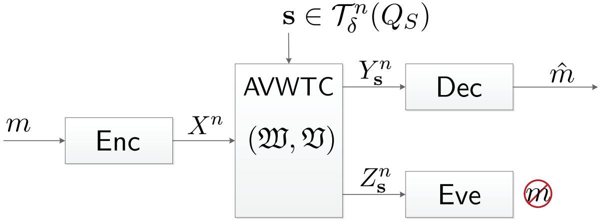
Theorem

$$C_{\mathrm{R}}(\mathfrak{W},\mathfrak{V},Q_S) = \max_{Q_{U,X}} \Big[\boldsymbol{I(U;Y)} - I(U;Z|S)\Big]$$

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

- **Reliability:** Average channel $\boldsymbol{W_Q(y|x) = \sum_{s\in\mathcal{S}} Q_S(s) W_s(y|x)}$.

Type Constrained AVWTCs



Theorem

$$C_\mathrm{R}(\mathfrak{W}, \mathfrak{V}, Q_S) = \max_{Q_{U,X}} \Big[I(U;Y) - \boldsymbol{I(U;Z|S)} \Big]$$

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

- **Reliability:** Average channel $W_Q(y|x) = \sum_{s\in\mathcal{S}} Q_S(s) W_s(y|x)$.
- **Security:** Eve who knows $\mathbf{s}$ as $\boldsymbol{I(U;Z|S) = I(U;Z,S)}$.

Type Constrained AVWTCs - Achievability Outline

1. **Reliable (Large) CR Code:** $\tilde{\mathbb{C}}_n = (\tilde{\mathcal{C}}_n, \tilde{\Gamma}_n, \tilde{\mu}_n)$

Type Constrained AVWTCs - Achievability Outline

1. **Reliable (Large) CR Code:** $\tilde{\mathbb{C}}_n=(\tilde{\mathcal{C}}_n,\tilde{\Gamma}_n,\tilde{\mu}_n)$
    - $\tilde{\mathcal{C}}_n=\big\{$All realization of i.i.d. wiretap code$\big\}$.

Type Constrained AVWTCs - Achievability Outline

1. **Reliable (Large) CR Code:** $\tilde{\mathbb{C}}_n = (\tilde{\mathcal{C}}_n, \tilde{\Gamma}_n, \tilde{\mu}_n)$
    - $\tilde{\mathcal{C}}_n = \big\{$All realization of i.i.d. wiretap code$\big\}$.
    - $|\tilde{\Gamma}_n| = |\mathcal{X}|^{n2^{n(R+\tilde{R})}}$ - Double-exponential in n.

Type Constrained AVWTCs - Achievability Outline

1. **Reliable (Large) CR Code:** $\tilde{\mathbb{C}}_n = (\tilde{\mathcal{C}}_n, \tilde{\Gamma}_n, \tilde{\mu}_n)$
   - $\tilde{\mathcal{C}}_n = \big\{$All realization of i.i.d. wiretap code$\big\}$.
   - $|\tilde{\Gamma}_n| = |\mathcal{X}|^{n2^{n(R+\tilde{R})}}$ - Double-exponential in n.
   - $\tilde{\mu}_n = \prod_{m,w} Q_X^n$ - Prob. of an i.i.d. wiretap code.

Type Constrained AVWTCs - Achievability Outline

① **Reliable (Large) CR Code:** $\tilde{\mathbb{C}}_n = (\tilde{\mathcal{C}}_n, \tilde{\Gamma}_n, \tilde{\mu}_n)$

- $\tilde{\mathcal{C}}_n = \big\{$All realization of i.i.d. wiretap code$\big\}$.
- $|\tilde{\boldsymbol{\Gamma}}_{\boldsymbol{n}}| = |\boldsymbol{\mathcal{X}}|^{\boldsymbol{n2^{n(R+\tilde{R})}}}$ **- Double-exponential in $\boldsymbol{n}$.**
- $\tilde{\mu}_n = \prod_{m,w} Q_X^n$ - Prob. of an i.i.d. wiretap code.

⚠ $\tilde{\mathbb{C}}_{\boldsymbol{n}}$ **is too large for semantic-security** ⚠

Type Constrained AVWTCs - Achievability Outline

1. **Reliable (Large) CR Code:** $\tilde{\mathbb{C}}_n = (\tilde{\mathcal{C}}_n, \tilde{\Gamma}_n, \tilde{\mu}_n)$
   - $\tilde{\mathcal{C}}_n = \big\{$All realization of i.i.d. wiretap code$\big\}$.
   - $|\tilde{\Gamma}_n| = |\mathcal{X}|^{n2^{n(R+\tilde{R})}}$ - Double-exponential in n.
   - $\tilde{\mu}_n = \prod_{m,w} Q_X^n$ - Prob. of an i.i.d. wiretap code.

2. **CR Code Reduction:** Chernoff bound

Type Constrained AVWTCs - Achievability Outline

1. **Reliable (Large) CR Code:** $\tilde{\mathbb{C}}_n = (\tilde{\mathcal{C}}_n, \tilde{\Gamma}_n, \tilde{\mu}_n)$
    - $\tilde{\mathcal{C}}_n = \big\{$All realization of i.i.d. wiretap code$\big\}$.
    - $|\tilde{\Gamma}_n| = |\mathcal{X}|^{n2^{n(R+\tilde{R})}}$ - Double-exponential in n.
    - $\tilde{\mu}_n = \prod_{m,w} Q_X^n$ - Prob. of an i.i.d. wiretap code.

2. **CR Code Reduction:** Chernoff bound $\Longrightarrow$ Reliable $\mathbb{C}_n = (\mathcal{C}_n, \Gamma_n, \mu_n)$

Type Constrained AVWTCs - Achievability Outline

1. **Reliable (Large) CR Code:** $\tilde{\mathbb{C}}_n = (\tilde{\mathcal{C}}_n, \tilde{\Gamma}_n, \tilde{\mu}_n)$
    - $\tilde{\mathcal{C}}_n = \big\{$All realization of i.i.d. wiretap code$\big\}$.
    - $|\tilde{\Gamma}_n| = |\mathcal{X}|^{n2^{n(R+\tilde{R})}}$ - Double-exponential in n.
    - $\tilde{\mu}_n = \prod_{m,w} Q_X^n$ - Prob. of an i.i.d. wiretap code.

2. **CR Code Reduction:** Chernoff bound $\Longrightarrow$ Reliable $\mathbb{C}_n = (\mathcal{C}_n, \Gamma_n, \mu_n)$
    - $\mathcal{C}_n \subsetneq \tilde{\mathcal{C}}_n$.

Type Constrained AVWTCs - Achievability Outline

1. **Reliable (Large) CR Code:** $\tilde{\mathbb{C}}_n = (\tilde{\mathcal{C}}_n, \tilde{\Gamma}_n, \tilde{\mu}_n)$
   - $\tilde{\mathcal{C}}_n = \big\{$All realization of i.i.d. wiretap code$\big\}$.
   - $|\tilde{\Gamma}_n| = |\mathcal{X}|^{n2^{n(R+\tilde{R})}}$ - Double-exponential in n.
   - $\tilde{\mu}_n = \prod_{m,w} Q_X^n$ - Prob. of an i.i.d. wiretap code.

2. **CR Code Reduction:** Chernoff bound $\Longrightarrow$ Reliable $\mathbb{C}_n = (\mathcal{C}_n, \Gamma_n, \mu_n)$
   - $\mathcal{C}_n \subsetneq \tilde{\mathcal{C}}_n$.
   - $|\Gamma_n| = n^3$ - Polynomial in n.

Type Constrained AVWTCs - Achievability Outline

1. **Reliable (Large) CR Code:** $\tilde{\mathbb{C}}_n = (\tilde{\mathcal{C}}_n, \tilde{\Gamma}_n, \tilde{\mu}_n)$
   - $\tilde{\mathcal{C}}_n = \big\{$All realization of i.i.d. wiretap code$\big\}$.
   - $|\tilde{\Gamma}_n| = |\mathcal{X}|^{n2^{n(R+\tilde{R})}}$ - Double-exponential in n.
   - $\tilde{\mu}_n = \prod_{m,w} Q_X^n$ - Prob. of an i.i.d. wiretap code.

2. **CR Code Reduction:** Chernoff bound $\Longrightarrow$ Reliable $\mathbb{C}_n = (\mathcal{C}_n, \Gamma_n, \mu_n)$
   - $\mathcal{C}_n \subsetneq \tilde{\mathcal{C}}_n$.
   - $|\Gamma_n| = n^3$ - Polynomial in n.
   - μ_n is uniform over Γ_n.

Type Constrained AVWTCs - Achievability Outline

1. **Reliable (Large) CR Code:** $\tilde{\mathbb{C}}_n = (\tilde{\mathcal{C}}_n, \tilde{\Gamma}_n, \tilde{\mu}_n)$
   - $\tilde{\mathcal{C}}_n = \big\{$All realization of i.i.d. wiretap code$\big\}$.
   - $|\tilde{\Gamma}_n| = |\mathcal{X}|^{n2^{n(R+\tilde{R})}}$ - Double-exponential in n.
   - $\tilde{\mu}_n = \prod_{m,w} Q_X^n$ - Prob. of an i.i.d. wiretap code.

2. **CR Code Reduction:** Chernoff bound $\Longrightarrow$ Reliable $\mathbb{C}_n = (\mathcal{C}_n, \Gamma_n, \mu_n)$
   - $\mathcal{C}_n \subsetneq \tilde{\mathcal{C}}_n$.
   - $|\Gamma_n| = n^3$ - Polynomial in n.
   - μ_n is uniform over Γ_n.

$$\mathbb{P}_{\mathbb{C}_n}\Big(\text{Error Prob.} \nrightarrow 0\Big) \xrightarrow[n\to\infty]{} 0$$

Type Constrained AVWTCs - Achievability Outline

① **Reliable (Large) CR Code:** $\tilde{\mathbb{C}}_n = (\tilde{\mathcal{C}}_n, \tilde{\Gamma}_n, \tilde{\mu}_n)$

- $\tilde{\mathcal{C}}_n = \big\{$All realization of i.i.d. wiretap code$\big\}$.
- $|\tilde{\Gamma}_n| = |\mathcal{X}|^{n2^{n(R+\tilde{R})}}$ - Double-exponential in n.
- $\tilde{\mu}_n = \prod_{m,w} Q_X^n$ - Prob. of an i.i.d. wiretap code.

② **CR Code Reduction:** Chernoff bound $\Longrightarrow$ Reliable $\mathbb{C}_n = (\mathcal{C}_n, \Gamma_n, \mu_n)$

- $\mathcal{C}_n \subsetneq \tilde{\mathcal{C}}_n$.
- $|\Gamma_n| = n^3$ - Polynomial in n.
- μ_n is uniform over Γ_n.

$$\mathbb{P}_{\mathbb{C}_n}\Big(\text{Error Prob.} \nrightarrow 0\Big) \xrightarrow[n\to\infty]{} 0$$

③ **Semantic Security:** Union bound & Stronger SCL

Type Constrained AVWTCs - Achievability Outline

1. **Reliable (Large) CR Code:** $\tilde{\mathbb{C}}_n = (\tilde{\mathcal{C}}_n, \tilde{\Gamma}_n, \tilde{\mu}_n)$
    - $\tilde{\mathcal{C}}_n = \big\{$All realization of i.i.d. wiretap code$\big\}$.
    - $|\tilde{\Gamma}_n| = |\mathcal{X}|^{n2^{n(R+\tilde{R})}}$ - Double-exponential in n.
    - $\tilde{\mu}_n = \prod_{m,w} Q_X^n$ - Prob. of an i.i.d. wiretap code.

2. **CR Code Reduction:** Chernoff bound $\Longrightarrow$ Reliable $\mathbb{C}_n = (\mathcal{C}_n, \Gamma_n, \mu_n)$
    - $\mathcal{C}_n \subsetneq \tilde{\mathcal{C}}_n$.
    - $|\Gamma_n| = n^3$ - Polynomial in n.
    - μ_n is uniform over Γ_n.

$$\mathbb{P}_{\mathbb{C}_n}\Big(\text{Error Prob.} \nrightarrow 0\Big) \xrightarrow[n\to\infty]{} 0$$

3. **Semantic Security:** Union bound & Stronger SCL
    - Combined number of states, message and codes $\leq$ $|\mathcal{S}|^n \cdot 2^{nR} \cdot n^3$.

Type Constrained AVWTCs - Achievability Outline

1. **Reliable (Large) CR Code:** $\tilde{\mathbb{C}}_n = (\tilde{\mathcal{C}}_n, \tilde{\Gamma}_n, \tilde{\mu}_n)$
   - $\tilde{\mathcal{C}}_n = \{$All realization of i.i.d. wiretap code$\}$.
   - $|\tilde{\Gamma}_n| = |\mathcal{X}|^{n2^{n(R+\tilde{R})}}$ - Double-exponential in n.
   - $\tilde{\mu}_n = \prod_{m,w} Q_X^n$ - Prob. of an i.i.d. wiretap code.

2. **CR Code Reduction:** Chernoff bound $\Longrightarrow$ Reliable $\mathbb{C}_n = (\mathcal{C}_n, \Gamma_n, \mu_n)$
   - $\mathcal{C}_n \subsetneq \tilde{\mathcal{C}}_n$.
   - $|\Gamma_n| = n^3$ - Polynomial in n.
   - μ_n is uniform over Γ_n.

$$\mathbb{P}_{\mathbb{C}_n}\Big(\text{Error Prob.} \nrightarrow 0\Big) \xrightarrow[n\to\infty]{} 0$$

3. **Semantic Security:** Union bound & Stronger SCL
   - Combined number of states, message and codes $\leq$ $|\mathcal{S}|^n \cdot 2^{nR} \cdot n^3$.

$$\mathbb{P}_{\mathbb{C}_n}\Big(\text{Violating SS}\Big) \leq |\mathcal{S}|^n \cdot 2^{nR} \cdot n^3 \cdot e^{-e^{n\gamma_2}} \xrightarrow[n\to\infty]{} 0$$

Type Constrained AVWTCs - Achievability Outline

1. **Reliable (Large) CR Code:** $\tilde{\mathbb{C}}_n = (\tilde{\mathcal{C}}_n, \tilde{\Gamma}_n, \tilde{\mu}_n)$
   - $\tilde{\mathcal{C}}_n = \{$All realization of i.i.d. wiretap code$\}$.
   - $|\tilde{\Gamma}_n| = |\mathcal{X}|^{n2^{n(R+\tilde{R})}}$ - Double-exponential in n.
   - $\tilde{\mu}_n = \prod_{m,w} Q_X^n$ - Prob. of an i.i.d. wiretap code.

2. **CR Code Reduction:** Chernoff bound $\implies$ Reliable $\mathbb{C}_n = (\mathcal{C}_n, \Gamma_n, \mu_n)$
   - $\mathcal{C}_n \subsetneq \tilde{\mathcal{C}}_n$.
   - $|\Gamma_n| = n^3$ - Polynomial in n.
   - μ_n is uniform over Γ_n.

$$\boxed{\mathbb{P}_{\mathbb{C}_n}\Big(\text{Error Prob.} \nrightarrow 0\Big) \xrightarrow[n\to\infty]{} 0}$$

3. **Semantic Security:** Union bound & Stronger SCL
   - Combined number of states, message and codes $\leq$ $|\mathcal{S}|^n \cdot 2^{nR} \cdot n^3$.

$$\boxed{\mathbb{P}_{\mathbb{C}_n}\Big(\text{Violating SS}\Big) \leq |\mathcal{S}|^n \cdot 2^{nR} \cdot n^3 \cdot e^{-e^{n\gamma_2}} \xrightarrow[n\to\infty]{} 0}$$

Type Constrained AVWTCs - Converse Outline

1. **Main Idea:** Reliability & SS under a type constraint Q_S

Type Constrained AVWTCs - Converse Outline

1. **Main Idea:** Reliability & SS under a type constraint Q_S

   $\Longrightarrow$ Reliability & SS when $S^n \sim Q_S^n$.

Type Constrained AVWTCs - Converse Outline

1. **Main Idea:** Reliability & SS under a type constraint Q_S

   $\Longrightarrow$ Reliability & SS when $S^n \sim Q_S^n$.

2. **Difficulty:** Show that $\frac{1}{n}H_{Q_S^n}(M|Y^n) \xrightarrow[n\to\infty]{} 0$.

Type Constrained AVWTCs - Converse Outline

1. **Main Idea:** Reliability & SS under a type constraint Q_S

   $\Longrightarrow$ Reliability & SS when $S^n \sim Q_S^n$.

2. **Difficulty:** Show that $\frac{1}{n}H_{Q_S^n}(M|Y^n) \xrightarrow[n\to\infty]{} 0$.

   - **Have:** $\max_{\mathbf{s}\in\mathcal{T}_\delta^n(Q_S)} \frac{1}{n}H(M|Y_\mathbf{s}^n) \xrightarrow[n\to\infty]{} 0$.

Type Constrained AVWTCs - Converse Outline

1. **Main Idea:** Reliability & SS under a type constraint Q_S

   $\Longrightarrow$ Reliability & SS when $S^n \sim Q_S^n$.

2. **Difficulty:** Show that $\frac{1}{n} H_{Q_S^n}(M|Y^n) \xrightarrow[n\to\infty]{} 0$.

   - **Have:** $\max_{\mathbf{s}\in\mathcal{T}_\delta^n(Q_S)} \frac{1}{n} H(M|Y_\mathbf{s}^n) \xrightarrow[n\to\infty]{} 0$.

     ★ Reliability over each $W_\mathbf{s}^n$, for $\mathbf{s} \in \mathcal{T}_\delta^n(Q_S)$ ★

Type Constrained AVWTCs - Converse Outline

1. **Main Idea:** Reliability & SS under a type constraint Q_S

   $\Longrightarrow$ Reliability & SS when $S^n \sim Q_S^n$.

2. **Difficulty:** Show that $\frac{1}{n} H_{Q_S^n}(M|Y^n) \xrightarrow[n\to\infty]{} 0$.

   - **Have:** $\max_{\mathbf{s}\in\mathcal{T}_\delta^n(Q_S)} \frac{1}{n} H(M|Y_{\mathbf{s}}^n) \xrightarrow[n\to\infty]{} 0$.

     ★ Reliability over each $W_{\mathbf{s}}^n$, for $\mathbf{s} \in \mathcal{T}_\delta^n(Q_S)$ ★

   - **Need:** Reliability over average channel $W_Q(y|x) = \sum_{s\in\mathcal{S}} Q_S(s) W_s(y|x)$.

Type Constrained AVWTCs - Converse Outline

1. **Main Idea:** Reliability & SS under a type constraint Q_S

   $\Longrightarrow$ Reliability & SS when $S^n \sim Q_S^n$.

2. **Difficulty:** Show that $\frac{1}{n} H_{Q_S^n}(M|Y^n) \xrightarrow[n\to\infty]{} 0$.

   - **Have:** $\max_{\mathbf{s}\in\mathcal{T}_\delta^n(Q_S)} \frac{1}{n} H(M|Y_{\mathbf{s}}^n) \xrightarrow[n\to\infty]{} 0$.

     ★ Reliability over each $W_{\mathbf{s}}^n$, for $\mathbf{s} \in \mathcal{T}_\delta^n(Q_S)$ ★

   - **Need:** Reliability over average channel $W_Q(y|x) = \sum_{s\in\mathcal{S}} Q_S(s) W_s(y|x)$.

     ★ W_Q is worse than any $W_s \in \mathfrak{W}$ ★

Type Constrained AVWTCs - Converse Outline

1. **Main Idea:** Reliability & SS under a type constraint Q_S

   $\Longrightarrow$ Reliability & SS when $S^n \sim Q_S^n$.

2. **Difficulty:** Show that $\frac{1}{n}H_{Q_S^n}(M|Y^n) \xrightarrow[n\to\infty]{} 0$.

   - **Have:** $\max_{\mathbf{s}\in\mathcal{T}_\delta^n(Q_S)} \frac{1}{n}H(M|Y_{\mathbf{s}}^n) \xrightarrow[n\to\infty]{} 0$.

     ★ Reliability over each $W_{\mathbf{s}}^n$, for $\mathbf{s} \in \mathcal{T}_\delta^n(Q_S)$ ★

   - **Need:** Reliability over average channel $W_Q(y|x) = \sum_{s\in\mathcal{S}} Q_S(s)W_s(y|x)$.

     ★ W_Q is worse than any $W_s \in \mathfrak{W}$ ★

3. **Solution:**

Type Constrained AVWTCs - Converse Outline

1. **Main Idea:** Reliability & SS under a type constraint Q_S

   $\Longrightarrow$ Reliability & SS when $S^n \sim Q_S^n$.

2. **Difficulty:** Show that $\frac{1}{n}H_{Q_S^n}(M|Y^n) \xrightarrow[n\to\infty]{} 0$.

   - **Have:** $\max_{\mathbf{s}\in\mathcal{T}_\delta^n(Q_S)} \frac{1}{n}H(M|Y_\mathbf{s}^n) \xrightarrow[n\to\infty]{} 0$.

     ★ Reliability over each $W_\mathbf{s}^n$, for $\mathbf{s} \in \mathcal{T}_\delta^n(Q_S)$ ★

   - **Need:** Reliability over average channel $W_Q(y|x) = \sum_{s\in\mathcal{S}} Q_S(s)W_s(y|x)$.

     ★ W_Q is worse than any $W_s \in \mathfrak{W}$ ★

3. **Solution:**

   - Equivocation is continuous in types that are δ-close to Q_S.

Type Constrained AVWTCs - Converse Outline

1. **Main Idea:** Reliability & SS under a type constraint Q_S

   $\Longrightarrow$ Reliability & SS when $S^n \sim Q_S^n$.

2. **Difficulty:** Show that $\frac{1}{n}H_{Q_S^n}(M|Y^n) \xrightarrow[n\to\infty]{} 0$.

   - **Have:** $\max_{\mathbf{s}\in\mathcal{T}_\delta^n(Q_S)} \frac{1}{n}H(M|Y_{\mathbf{s}}^n) \xrightarrow[n\to\infty]{} 0$.

     ★ Reliability over each $W_{\mathbf{s}}^n$, for $\mathbf{s} \in \mathcal{T}_\delta^n(Q_S)$ ★

   - **Need:** Reliability over average channel $W_Q(y|x) = \sum_{s\in\mathcal{S}} Q_S(s)W_s(y|x)$.

     ★ W_Q is worse than any $W_s \in \mathfrak{W}$ ★

3. **Solution:**
   - Equivocation is continuous in types that are δ-close to Q_S.
   - Continuity proof via novel distribution coupling argument.

Type Constrained AVWTCs - General Results

- **$\mathcal{Q}$-constrained AVWTC:** $\mathcal{Q} \subseteq \mathcal{P}(\mathcal{S})$ define $\mathcal{S}^n_{\mathcal{Q}} = \left\{ \mathbf{s} \in \mathcal{S}^n \middle| \nu_{\mathbf{s}} \in \mathcal{Q} \right\}$

Type Constrained AVWTCs - General Results

- **$\mathcal{Q}$-constrained AVWTC:** $\mathcal{Q} \subseteq \mathcal{P}(\mathcal{S})$ define $\mathcal{S}^n_{\mathcal{Q}} = \left\{\mathbf{s} \in \mathcal{S}^n \middle| \nu_{\mathbf{s}} \in \mathcal{Q}\right\}$

  $\implies$ allowed state sequences are $\mathbf{s} \in \mathcal{S}^n_{\mathcal{Q}}$.

Type Constrained AVWTCs - General Results

- **$\mathcal{Q}$-constrained AVWTC:** $\mathcal{Q} \subseteq \mathcal{P}(\mathcal{S})$ define $\mathcal{S}^n_{\mathcal{Q}} = \left\{ \mathbf{s} \in \mathcal{S}^n \middle| \nu_{\mathbf{s}} \in \mathcal{Q} \right\}$

$\Longrightarrow$ allowed state sequences are $\mathbf{s} \in \mathcal{S}^n_{\mathcal{Q}}$.

Lower Bound

$\mathcal{Q}$ is convex and closed

$$C_{\mathrm{R}}(\mathfrak{W}, \mathfrak{V}, \mathcal{Q}) \geq \max_{Q_{U,X}} \left[\min_{Q_S^{(1)} \in \mathcal{Q}} I(U;Y) - \max_{Q_S^{(2)} \in \mathcal{Q}} I(U;Z|S) \right]$$

Joint PMFs: $Q_S^{(j)} Q_{U,X} W_{Y|X,S} V_{Z|X,S}$, *for* $j = 1, 2$.

Type Constrained AVWTCs - General Results

- **$\mathcal{Q}$-constrained AVWTC:** $\mathcal{Q} \subseteq \mathcal{P}(\mathcal{S})$ define $\mathcal{S}^n_{\mathcal{Q}} = \left\{\mathbf{s} \in \mathcal{S}^n \middle| \nu_{\mathbf{s}} \in \mathcal{Q}\right\}$

$\implies$ allowed state sequences are $\mathbf{s} \in \mathcal{S}^n_{\mathcal{Q}}$.

Lower Bound

$\mathcal{Q}$ is convex and closed

$$C_{\mathrm{R}}(\mathfrak{W}, \mathfrak{V}, \mathcal{Q}) \geq \max_{Q_{U,X}} \left[\min_{Q_S^{(1)} \in \mathcal{Q}} I(U;Y) - \max_{Q_S^{(2)} \in \mathcal{Q}} I(U;Z|S) \right]$$

Joint PMFs: $Q_S^{(j)} Q_{U,X} W_{Y|X,S} V_{Z|X,S}$, *for* $j = 1, 2$.

Upper Bound

$\mathcal{Q}$ contains only rational PMFs

$$C_{\mathrm{R}}(\mathfrak{W}, \mathfrak{V}, \mathcal{Q}) \leq \inf_{Q_S \in \mathcal{Q}} \max_{Q_{U,X}} \Big[I(U;Y) - I(U;Z|S) \Big]$$

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

Type Constrained AVWTCs - Concluding Remarks

- **Upgraded Security:**

Type Constrained AVWTCs - Concluding Remarks

- **Upgraded Security:**
    - No assumption of a best channel to Eve.

Type Constrained AVWTCs - Concluding Remarks

- **Upgraded Security:**
  - No assumption of a best channel to Eve.
  - SS versus Eve with access to the CR.

Type Constrained AVWTCs - Concluding Remarks

- **Upgraded Security:**
  - No assumption of a best channel to Eve.
  - SS versus Eve with access to the CR.

- **Polynomial CR Code:** DC-capacity $> 0 \implies$ same rates achievable.

Type Constrained AVWTCs - Concluding Remarks

- **Upgraded Security:**
  - No assumption of a best channel to Eve.
  - SS versus Eve with access to the CR.

- **Polynomial CR Code:** DC-capacity $> 0 \implies$ same rates achievable.
  - Prefix index of selected code to transmitted sequence (vanising rate).

Type Constrained AVWTCs - Concluding Remarks

- **Upgraded Security:**
  - No assumption of a best channel to Eve.
  - SS versus Eve with access to the CR.
- **Polynomial CR Code:** DC-capacity $> 0 \implies$ same rates achievable.
  - Prefix index of selected code to transmitted sequence (vanising rate).
  - Missing Piece: Dichotomy between DC-capacity> 0 and DC-capacity$= 0$.

Summary

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

Summary

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

Summary

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

Summary

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

- **Stronger Soft-Covering Lemma:**

Summary

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

- **Stronger Soft-Covering Lemma:**
  - Double-exponential decay of prob. of soft-covering not happening.

Summary

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

Summary

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

Summary

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

Summary

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

- **Stronger Soft-Covering Lemma:**
  - Double-exponential decay of prob. of soft-covering not happening.
  - Satisfy exponentially many soft-covering constraints.

- **Wiretap Channel II:** Noisy Main Channel
  - Derivation of SS-capacity & Equality to weak-secrecy-capacity.
  - Classic erasure wiretap codes achieve SS-capacity.

Summary

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

Summary

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

Summary

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

Summary

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

- **Stronger Soft-Covering Lemma:**
  - Double-exponential decay of prob. of soft-covering not happening.
  - Satisfy exponentially many soft-covering constraints.

- **Wiretap Channel II:** Noisy Main Channel
  - Derivation of SS-capacity & Equality to weak-secrecy-capacity.
  - Classic erasure wiretap codes achieve SS-capacity.

- **Type Constrained AVWTC:**
  - Single-letter characterization of type constrained AVWTC CR-capacity.
  - General single-letter lower and upper bounds.

Thank You!