Semantically-Secured Message-Key Trade-off over Wiretap Channels with Random Parameters

Shlomo Shamai (Shitz)[1]

Joint work with:
Alexander Bunin[1], Ziv Goldfeld[2], Haim H. Permuter[3],
Paul Cuff[4] and Pablo Piantanida[5]

[1] Technion – Israel Institute of Technology
[2] Massachusetts Institute of Technology (MIT)
[3] Ben-Gurion University of the Negev, Israel
[4] Renaissance Technologies, US
[5] CentraleSupélec-CNRS-Université, Paris-Sud, France

Supported by the European Union's Horizon 2020,
Research And Innovation Program: ERC 694630

Princeton: July 30, 2018

European Research Council
Established by the European Commission

Outline

1. The Wiretap Channel (WTC) - Different metrics for security
2. Soft Covering
3. The Gelfand-Pinsker (GP) Channel - Analysis using Likelihood Enc.
4. The GP-WTC
5. Secret Key-Message Trade-Off over the GP-WTC

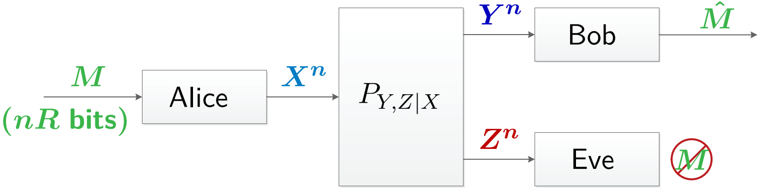
Outline

1. The Wiretap Channel (WTC) - Different metrics for security
2. Soft Covering
3. The Gelfand-Pinsker (GP) Channel - Analysis using Likelihood Enc.
4. The GP-WTC
5. Secret Key-Message Trade-Off over the GP-WTC

★ The results are **existential** and **asymptotic**

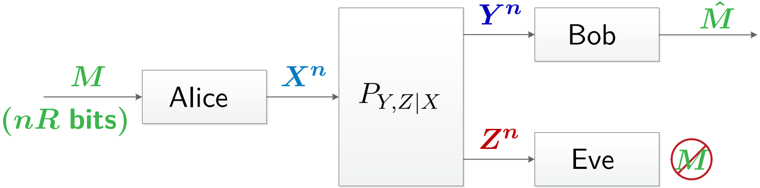
The Wiretap Channel

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



The Wiretap Channel

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

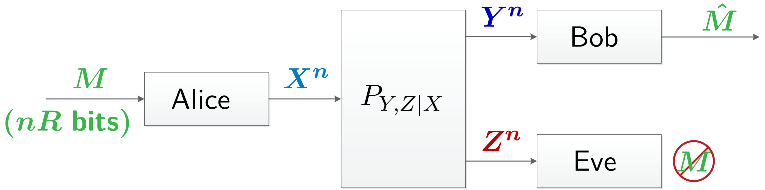


Secrecy-Capacity:

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

The Wiretap Channel

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



Secrecy-Capacity:

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

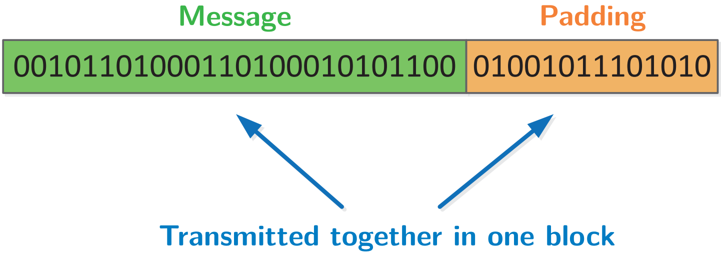
Theorem (Csiszár-Körner 1978)

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

Joint distribution: $P_{U,X} P_{Y,Z|X} \quad \Big\{ U -\!\!\circ\!\!- X -\!\!\circ\!\!- (Y,Z) \Big\}$

The Wiretap Channel - Encoding

- **Random codebook:** (Message, Padding) $\rightarrow$ $U^n \sim P_U^n$.
- **Codebook binning:** Pad nR **message bits** with $n\tilde{R}$ **random bits**.



The **message** chooses the bin, and the **padding** a specific codeword.

The Wiretap Channel - Encoding

- **Random codebook:** (Message, Padding) $\rightarrow$ $U^n \sim P_U^n$.
- **Codebook binning:** Pad nR **message bits** with $n\tilde{R}$ **random bits**.

Message	Padding
00101101000110100010101100	01001011101010

Transmitted together in one block

The **message** chooses the bin, and the **padding** a specific codeword.

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

The Wiretap Channel - Encoding

- **Random codebook:** (Message, Padding) $\rightarrow$ $U^n \sim P_U^n$.
- **Codebook binning:** Pad nR **message bits** with $n\tilde{R}$ **random bits**.

Message	Padding
00101101000110100010101100	01001011101010

Transmitted together in one block

The **message** chooses the bin, and the **padding** a specific codeword.

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

The Wiretap Channel - Analysis

Analysis - Main Ideas:

Analysis - Main Ideas:

1. **Reliability:** Decode **Message**+**Padding**
   - Successful if $R + \tilde{R} < I(U;Y)$.

Analysis - Main Ideas:

1. **Reliability:** Decode Message+Padding
   - Successful if $R + \tilde{R} < I(U;Y)$.
2. **Security:**

Different Security Types

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

Different Security Types

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

- **Weak-Secrecy:**
  $\frac{1}{n} I_{\mathcal{C}_n}(\boldsymbol{M}; \boldsymbol{Z^n}) \xrightarrow[n\to\infty]{} 0$ for $\boldsymbol{M} \sim Unif\left[1, 2^{nR}\right]$

Different Security Types

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

- **Weak-Secrecy:**
  $$\frac{1}{n} I_{\mathcal{C}_n}(\boldsymbol{M};\boldsymbol{Z^n}) \xrightarrow[n\to\infty]{} 0 \quad \text{for} \quad \boldsymbol{M} \sim Unif\left[1, 2^{nR}\right]$$

- **Strong-Secrecy:**
  $$I_{\mathcal{C}_n}(\boldsymbol{M};\boldsymbol{Z^n}) \xrightarrow[n\to\infty]{} 0 \quad \text{for} \quad \boldsymbol{M} \sim Unif\left[1, 2^{nR}\right]$$

Different Security Types

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

- **Weak-Secrecy:**

  $$\frac{1}{n} I_{\mathcal{C}_n}(\boldsymbol{M};\boldsymbol{Z^n}) \xrightarrow[n\to\infty]{} 0 \quad \text{for} \quad \boldsymbol{M} \sim Unif\left[1,2^{nR}\right]$$

- **Strong-Secrecy:**

  $$I_{\mathcal{C}_n}(\boldsymbol{M};\boldsymbol{Z^n}) \xrightarrow[n\to\infty]{} 0 \quad \text{for} \quad \boldsymbol{M} \sim Unif\left[1,2^{nR}\right]$$

- **Semantic-Security:**

  $$I_{\mathcal{C}_n}(\boldsymbol{M};\boldsymbol{Z^n}) \xrightarrow[n\to\infty]{} 0 \quad \text{for} \quad \textbf{any } \boldsymbol{P_M}$$

Different Security Types

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

- **Weak-Secrecy:**

  $\frac{1}{n}I_{\mathcal{C}_n}(M;Z^n) \xrightarrow[n\to\infty]{} 0$ for $M \sim Unif\left[1,2^{nR}\right]$

- **Strong-Secrecy:**

  $I_{\mathcal{C}_n}(M;Z^n) \xrightarrow[n\to\infty]{} 0$ for $M \sim Unif\left[1,2^{nR}\right]$

- **Semantic-Security:**

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

$$I_{\mathcal{C}_n}(M;Z^n) = D\Big(P^{(\mathcal{C}_n)}_{Z^n,M}\Big|\Big|P^{(\mathcal{C}_n)}_{Z^n}P^{(\mathcal{C}_n)}_{M}\Big) = \sum_m p(m) D\Big(P^{(\mathcal{C}_n)}_{Z^n|M=m}\Big|\Big|P^{(\mathcal{C}_n)}_{Z^n}\Big)$$

Different Security Types

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

- **Weak-Secrecy:** Only leakage **rate** vanishes

  $$\frac{1}{n} I_{\mathcal{C}_n}(M;Z^n) \xrightarrow[n\to\infty]{} 0 \quad \text{for} \quad M \sim Unif\left[1, 2^{nR}\right]$$

- **Strong-Secrecy:**

  $$I_{\mathcal{C}_n}(M;Z^n) \xrightarrow[n\to\infty]{} 0 \quad \text{for} \quad M \sim Unif\left[1, 2^{nR}\right]$$

- **Semantic-Security:**

  $$I_{\mathcal{C}_n}(M;Z^n) \xrightarrow[n\to\infty]{} 0 \quad \text{for} \quad \textbf{any } P_M$$

$$I_{\mathcal{C}_n}(M;Z^n) = D\Big(P^{(\mathcal{C}_n)}_{Z^n,M} \Big|\Big| P^{(\mathcal{C}_n)}_{Z^n} P^{(\mathcal{C}_n)}_{M}\Big) = \sum_m p(m) D\Big(P^{(\mathcal{C}_n)}_{Z^n|M=m} \Big|\Big| P^{(\mathcal{C}_n)}_{Z^n}\Big)$$

Different Security Types

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

- **Weak-Secrecy:** Only leakage **rate** vanishes

  $\frac{1}{n}I_{\mathcal{C}_n}(\boldsymbol{M};\boldsymbol{Z^n}) \xrightarrow[n\to\infty]{} 0$ for $\boldsymbol{M} \sim Unif\left[1,2^{nR}\right]$

- **Strong-Secrecy:** Security only on **average**

  $I_{\mathcal{C}_n}(\boldsymbol{M};\boldsymbol{Z^n}) \xrightarrow[n\to\infty]{} 0$ for $\boldsymbol{M} \sim Unif\left[1,2^{nR}\right]$

- **Semantic-Security:**

  $I_{\mathcal{C}_n}(\boldsymbol{M};\boldsymbol{Z^n}) \xrightarrow[n\to\infty]{} 0$ for **any** P_M

$$I_{\mathcal{C}_n}(\boldsymbol{M};\boldsymbol{Z^n}) = D\Big(P^{(\mathcal{C}_n)}_{\boldsymbol{Z^n},M}\Big|\Big|P^{(\mathcal{C}_n)}_{\boldsymbol{Z^n}}P^{(\mathcal{C}_n)}_{M}\Big) = \sum_m p(\boldsymbol{m})D\Big(P^{(\mathcal{C}_n)}_{\boldsymbol{Z^n}|M=m}\Big|\Big|P^{(\mathcal{C}_n)}_{\boldsymbol{Z^n}}\Big)$$

Different Security Types

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

- **Weak-Secrecy:** Only leakage **rate** vanishes

  $\frac{1}{n} I_{\mathcal{C}_n}(M; Z^n) \xrightarrow[n\to\infty]{} 0$ for $M \sim Unif\left[1, 2^{nR}\right]$

- **Strong-Secrecy:** Security only on **average**

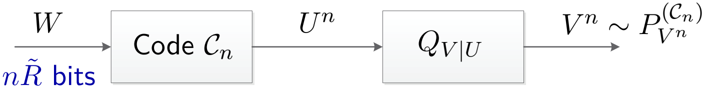
  $I_{\mathcal{C}_n}(M; Z^n) \xrightarrow[n\to\infty]{} 0$ for $M \sim Unif\left[1, 2^{nR}\right]$

- **Semantic-Security:** Security for **each message**

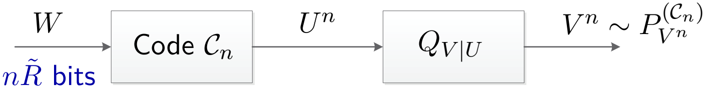
  $I_{\mathcal{C}_n}(M; Z^n) \xrightarrow[n\to\infty]{} 0$ for **any** P_M

$$I_{\mathcal{C}_n}(M; Z^n) = D\Big(P^{(\mathcal{C}_n)}_{Z^n, M} \Big|\Big| P^{(\mathcal{C}_n)}_{Z^n} P^{(\mathcal{C}_n)}_{M}\Big) = \sum_m p(m) D\Big(P^{(\mathcal{C}_n)}_{Z^n|M=m} \Big|\Big| P^{(\mathcal{C}_n)}_{Z^n}\Big)$$

Soft-Covering

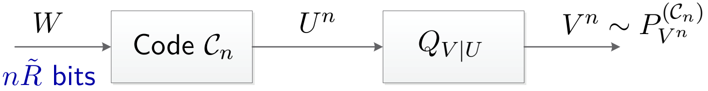


Soft-Covering



- **Random Code:** $\mathcal{C}_n = \left\{U^n(w)\right\}_w \overset{iid}{\sim} Q_U^n.$ $\qquad \left(Q_U^n \triangleq \prod_{i=1}^{n} Q_U(u_i)\right)$

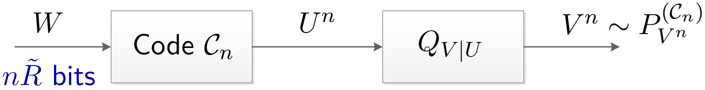
Soft-Covering



- **Random Code:** $\mathcal{C}_n = \{U^n(w)\}_w \overset{iid}{\sim} Q_U^n$. $\quad \left(Q_U^n \triangleq \prod_{i=1}^n Q_U(u_i)\right)$

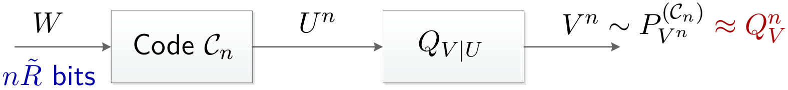
- **Uniform Choice:** $W \sim \mathsf{Unif}\big[1 : 2^{n\tilde{R}}\big]$.

Soft-Covering



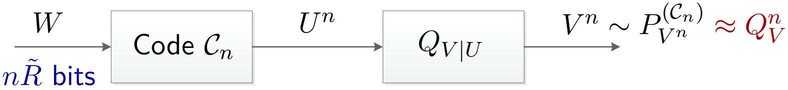
- **Random Code:** $\mathcal{C}_n = \left\{U^n(w)\right\}_w \overset{iid}{\sim} Q_U^n$. $\quad \left(Q_U^n \triangleq \prod_{i=1}^{n} Q_U(u_i)\right)$
- **Uniform Choice:** $W \sim \text{Unif}\big[1 : 2^{n\tilde{R}}\big]$.
- **Induced Output PMF:** $P_{V^n}^{(\mathcal{C}_n)}(v^n) = 2^{-n\tilde{R}} \sum_w Q_{V|U}^n\big(v^n \big| u^n(w, \mathcal{C}_n)\big)$.

Soft-Covering



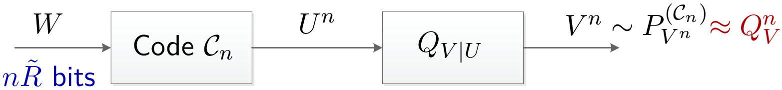
- **Random Code:** $\mathcal{C}_n = \{U^n(w)\}_w \overset{iid}{\sim} Q_U^n$. $\qquad \left(Q_U^n \triangleq \prod_{i=1}^n Q_U(u_i)\right)$
- **Uniform Choice:** $W \sim \text{Unif}\big[1 : 2^{n\tilde{R}}\big]$.
- **Induced Output PMF:** $P_{V^n}^{(\mathcal{C}_n)}(v^n) = 2^{-n\tilde{R}} \sum_w Q_{V|U}^n\big(v^n \big| u^n(w, \mathcal{C}_n)\big)$.
- **Desired Output PMF:** $Q_V^n(v^n) = \prod_{i=1}^n \left[\sum_u Q_U(u) Q_{V|U}(v_i|u)\right]$.

Soft-Covering



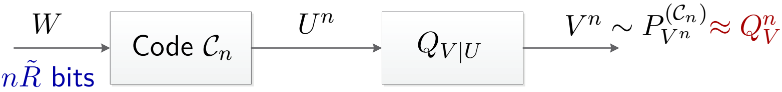
- **Random Code:** $\mathcal{C}_n = \{U^n(w)\}_w \overset{iid}{\sim} Q_U^n$. $\quad \left(Q_U^n \triangleq \prod_{i=1}^{n} Q_U(u_i)\right)$
- **Uniform Choice:** $W \sim \text{Unif}\left[1 : 2^{n\tilde{R}}\right]$.
- **Induced Output PMF:** $P_{V^n}^{(\mathcal{C}_n)}(v^n) = 2^{-n\tilde{R}} \sum_{w} Q_{V|U}^n\left(v^n \middle| u^n(w, \mathcal{C}_n)\right)$.
- **Desired Output PMF:** $Q_V^n(v^n) = \prod_{i=1}^{n} \left[\sum_{u} Q_U(u) Q_{V|U}(v_i|u)\right]$.
- **Goal:** Choose $\tilde{R}$ (codebook size) s.t. $P_{V^n}^{(\mathcal{C}_n)} \approx Q_V^n$.

Soft-Covering - Results



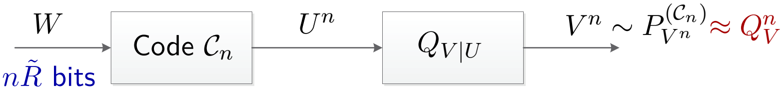
$$\boldsymbol{\tilde{R} > I_Q(U;V) \implies P_{V^n}^{(\mathcal{C}_n)} \approx Q_V^n}$$

Soft-Covering - Results



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

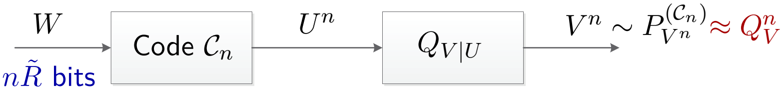
- **Wyner 1975**: $\mathbb{E}_{\mathbb{C}_n} \frac{1}{n} D\left(P_{V^n}^{(\mathcal{C}_n)} \middle\| Q_V^n\right) \xrightarrow[n\to\infty]{} 0.$



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

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

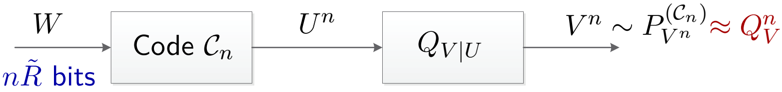
Soft-Covering - Results



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

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

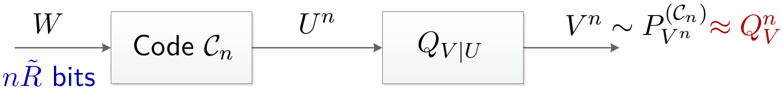
Soft-Covering - Results



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

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

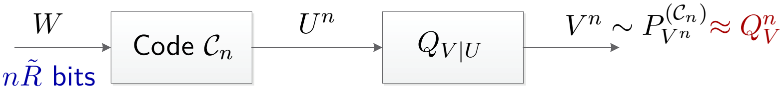
Soft-Covering - Results



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

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

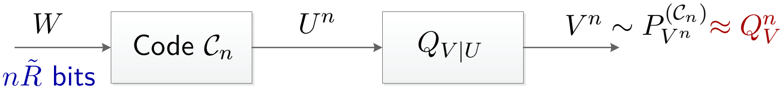
Soft-Covering - Results



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

- **Wyner 1975**: $\mathbb{E}_{\mathbb{C}_n} \frac{1}{n} D\left(P_{V^n}^{(\mathcal{C}_n)} \middle\| Q_V^n\right) \xrightarrow[n\to\infty]{} 0.$ Weak Secrecy
- **Han-Verdú 1993**: $\mathbb{E}_{\mathbb{C}_n} \left\| P_{V^n}^{(\mathcal{C}_n)} - Q_V^n \right\|_{\mathrm{TV}} \xrightarrow[n\to\infty]{} 0.$ Strong Secrecy
- **Hou-Kramer 2014**: $\mathbb{E}_{\mathbb{C}_n} D\left(P_{V^n}^{(\mathcal{C}_n)} \middle\| Q_V^n\right) \xrightarrow[n\to\infty]{} 0.$ Strong Secrecy
- **Cuff 2015**: $\mathbb{P}_{\mathbb{C}_n}\left(D\left(P_{V^n}^{(\mathcal{C}_n)} \middle\| Q_V^n\right) > e^{-n\gamma_1} \right) \leq e^{-e^{n\gamma_2}}$

Soft-Covering - Results



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

- **Wyner 1975**: $\mathbb{E}_{\mathbb{C}_n} \frac{1}{n} D\left(P_{V^n}^{(\mathcal{C}_n)} \middle\| Q_V^n\right) \xrightarrow[n\to\infty]{} 0.$ Weak Secrecy
- **Han-Verdú 1993**: $\mathbb{E}_{\mathbb{C}_n} \left\| P_{V^n}^{(\mathcal{C}_n)} - Q_V^n \right\|_{\mathrm{TV}} \xrightarrow[n\to\infty]{} 0.$ Strong Secrecy
- **Hou-Kramer 2014**: $\mathbb{E}_{\mathbb{C}_n} D\left(P_{V^n}^{(\mathcal{C}_n)} \middle\| Q_V^n\right) \xrightarrow[n\to\infty]{} 0.$ Strong Secrecy
- **Cuff 2015**: $\mathbb{P}_{\mathbb{C}_n}\left(D\left(P_{V^n}^{(\mathcal{C}_n)} \middle\| Q_V^n\right) > e^{-n\gamma_1} \right) \leq e^{-e^{n\gamma_2}}$

Semantic Security

The Wiretap Channel - Analysis

Analysis - Main Ideas:

1. **Reliability:** Decode **Message**+**Padding**
   - Successful if $R + \tilde{R} < I(U;Y)$.
2. **Security:**

The Wiretap Channel - Analysis

Analysis - Main Ideas:

1. **Reliability:** Decode Message+Padding
   - Successful if $R + \tilde{R} < I(U;Y)$.
2. **Security:** Assure $P^{(\mathcal{C}_n)}_{Z^n|M} \approx P^n_Z$

The Wiretap Channel - Analysis

Analysis - Main Ideas:

1. **Reliability:** Decode Message+Padding
   - Successful if $R + \tilde{R} < I(U;Y)$.
2. **Security:** Assure $P^{(\mathcal{C}_n)}_{Z^n|M} \approx P^n_Z$
   - **Soft-Covering Lemma (SCL):** Approximation holds if $\tilde{R} > I(U;Z)$.

     (Inflates the eavesdropper *ala* Massey.)

Analysis - Main Ideas:

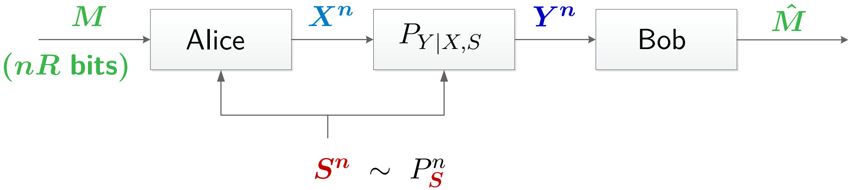
1. **Reliability:** Decode Message+Padding
   - Successful if $R + \tilde{R} < I(U;Y)$.
2. **Security:** Assure $P^{(\mathcal{C}_n)}_{Z^n|M} \approx P^n_Z$
   - **Soft-Covering Lemma (SCL):** Approximation holds if $\tilde{R} > I(U;Z)$.

     (Inflates the eavesdropper *ala* Massey.)

$$\Longrightarrow \quad \boxed{R < I(U;Y) - I(U;Z)}$$

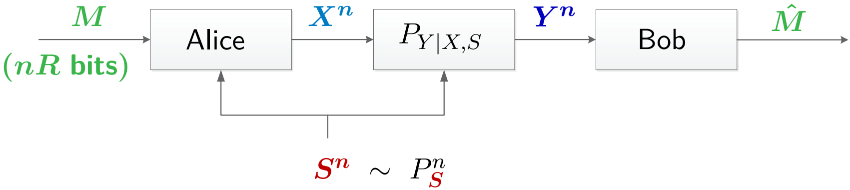
The Gelfand-Pinsker Channel

[Gelfand-Pinsker 1980]



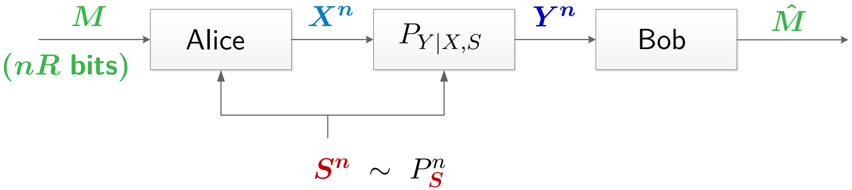
The Gelfand-Pinsker Channel

[Gelfand-Pinsker 1980]



Capacity: Reliable communication.

The Gelfand-Pinsker Channel
[Gelfand-Pinsker 1980]



Capacity: Reliable communication.

Theorem (Gelfand-Pinsker 1980)

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

Joint distribution: $P_{U,X|S} P_{Y|X,S}$ $\Big\{ U - (X,S) - Y \Big\}$

The Gelfand-Pinsker Channel - Encoding

- **Random codebook:** (Message, Padding) $\rightarrow$ $U^n \sim P_U^n$.
- **Codebook binning:**
  Pad nR **message bits** with $n\tilde{R}$ **skillfully chosen bits**.

Message	Padding
00101101000110100010101100	01001011101010

Transmitted together in one block

The **message** chooses the bin, and the **padding** a specific codeword.

The Gelfand-Pinsker Channel - Analysis

Standard Analysis - Main Ideas:

The Gelfand-Pinsker Channel - Analysis

Standard Analysis - Main Ideas:

1. **Encoding:** Find U^n jointly typical with S^n

The Gelfand-Pinsker Channel - Analysis

Standard Analysis - Main Ideas:

1. **Encoding:** Find U^n jointly typical with S^n
   - Successful if $\tilde{R} > I(U;S)$.

The Gelfand-Pinsker Channel - Analysis

Standard Analysis - Main Ideas:

1. **Encoding:** Find U^n jointly typical with S^n
   - Successful if $\tilde{R} > I(U;S)$.
2. **Decoding:** Decode Message+Padding

Standard Analysis - Main Ideas:

1. **Encoding:** Find U^n jointly typical with S^n
   - Successful if $\tilde{R} > I(U;S)$.
2. **Decoding:** Decode Message+Padding
   - Successful if $R + \tilde{R} < I(U;Y)$.

The Gelfand-Pinsker Channel - Analysis

Standard Analysis - Main Ideas:

1. **Encoding:** Find U^n jointly typical with S^n
   - Successful if $\tilde{R} > I(U;S)$.
2. **Decoding:** Decode Message+Padding
   - Successful if $R + \tilde{R} < I(U;Y)$.

$$\Longrightarrow \quad \boxed{R < I(U;Y) - I(U;S)}$$

The Gelfand-Pinsker Channel - Analysis

Alternative Analysis - Likelihood Encoder + SCL:

- For simplicity assume: $U = X$

The Gelfand-Pinsker Channel - Analysis

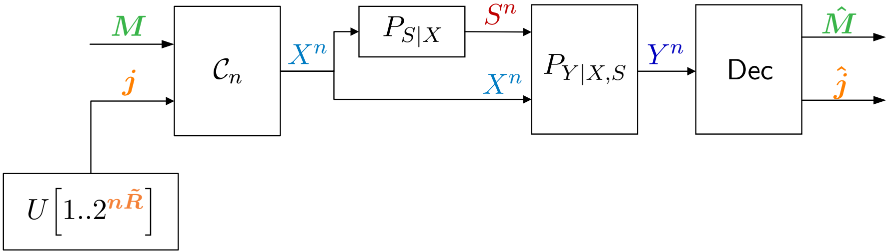
Alternative Analysis - Likelihood Encoder + SCL:

- Use **Binned Random Codebook**: $\mathcal{C}_n = \{\boldsymbol{x^n}(\boldsymbol{m}, \boldsymbol{j})\}$

The Gelfand-Pinsker Channel - Analysis

Alternative Analysis - Likelihood Encoder + SCL:

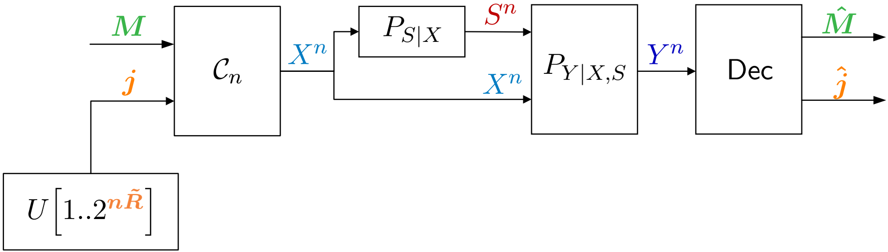
- Use **Binned Random Codebook**: $\mathcal{C}_n = \{\boldsymbol{x^n}(\boldsymbol{m}, \boldsymbol{j})\}$
- Try to approximate distribution by



The Gelfand-Pinsker Channel - Analysis

Alternative Analysis - Likelihood Encoder + SCL:

- Use **Binned Random Codebook**: $\mathcal{C}_n = \{\boldsymbol{x^n}(\boldsymbol{m}, \boldsymbol{j})\}$
- Try to approximate distribution by



- Difference from original distribution: $\tilde{P}^{(\mathcal{C}_n)}_{\boldsymbol{J},\boldsymbol{S^n}|M}$.

The Gelfand-Pinsker Channel - Analysis
Alternative Analysis

- Define the encoder by the marginal $\tilde{P}^{(\mathcal{C}_n)}_{\boldsymbol{J}|M,\boldsymbol{S^n}}$
  (Likelihood encoder, Cuff 2008):

$$P^{(\mathcal{C}_n)}_{\boldsymbol{J}|M,\boldsymbol{S^n}}(\boldsymbol{j}|\boldsymbol{m},\boldsymbol{s^n}) = \frac{P^n_{\boldsymbol{S}|\boldsymbol{X}}(\boldsymbol{s^n}|\boldsymbol{x^n}(\boldsymbol{m},\boldsymbol{j}))}{\sum_{j'} P^n_{\boldsymbol{S}|\boldsymbol{X}}(\boldsymbol{s^n}|\boldsymbol{x^n}(\boldsymbol{m},j'))}$$

where $P^n_{\boldsymbol{S}|\boldsymbol{X}}$ is the n-fold extension of the marginal $P_{\boldsymbol{S}|\boldsymbol{X}}$ of $P_{\boldsymbol{S},\boldsymbol{X}}$.

The Gelfand-Pinsker Channel - Analysis

Alternative Analysis

- Define the encoder by the marginal $\tilde{P}^{(\mathcal{C}_n)}_{\boldsymbol{J}|M,\boldsymbol{S^n}}$ (Likelihood encoder, Cuff 2008):

$$P^{(\mathcal{C}_n)}_{\boldsymbol{J}|M,\boldsymbol{S^n}}(\boldsymbol{j}|\boldsymbol{m},\boldsymbol{s^n}) = \frac{P^n_{\boldsymbol{S}|\boldsymbol{X}}(\boldsymbol{s^n}|\boldsymbol{x^n}(\boldsymbol{m},\boldsymbol{j}))}{\sum_{j'} P^n_{\boldsymbol{S}|\boldsymbol{X}}(\boldsymbol{s^n}|\boldsymbol{x^n}(\boldsymbol{m},j'))}$$

  where $P^n_{\boldsymbol{S}|\boldsymbol{X}}$ is the n-fold extension of the marginal $P_{\boldsymbol{S}|\boldsymbol{X}}$ of $P_{\boldsymbol{S},\boldsymbol{X}}$.

⋆ In standard analysis **Joint Typicality Encoder** is used instead.

- Define the encoder by the marginal $\tilde{P}^{(\mathcal{C}_n)}_{\boldsymbol{J}|M,\boldsymbol{S^n}}$ (Likelihood encoder, Cuff 2008):

$$P^{(\mathcal{C}_n)}_{\boldsymbol{J}|M,\boldsymbol{S^n}}(\boldsymbol{j}|\boldsymbol{m},\boldsymbol{s^n}) = \frac{P^n_{\boldsymbol{S}|\boldsymbol{X}}(\boldsymbol{s^n}|\boldsymbol{x^n}(\boldsymbol{m},\boldsymbol{j}))}{\sum_{j'} P^n_{\boldsymbol{S}|\boldsymbol{X}}(\boldsymbol{s^n}|\boldsymbol{x^n}(\boldsymbol{m},j'))}$$

  where $P^n_{\boldsymbol{S}|\boldsymbol{X}}$ is the n-fold extension of the marginal $P_{\boldsymbol{S}|\boldsymbol{X}}$ of $P_{\boldsymbol{S},\boldsymbol{X}}$.

- If $\tilde{\boldsymbol{R}} > \boldsymbol{I(X;S)}$ SCL gurantees $\tilde{P}^{(\mathcal{C}_n)}_{\boldsymbol{S^n}|M} \sim P^n_{\boldsymbol{S}}$.

The Gelfand-Pinsker Channel - Analysis

Alternative Analysis

- Define the encoder by the marginal $\tilde{P}^{(\mathcal{C}_n)}_{J|M,S^n}$ (Likelihood encoder, Cuff 2008):

$$P^{(\mathcal{C}_n)}_{J|M,S^n}(j|m,s^n) = \frac{P^n_{S|X}(s^n|x^n(m,j))}{\sum_{j'} P^n_{S|X}(s^n|x^n(m,j'))}$$

where $P^n_{S|X}$ is the n-fold extension of the marginal $P_{S|X}$ of $P_{S,X}$.

- If $\tilde{R} > I(X;S)$ SCL gurantees $\tilde{P}^{(\mathcal{C}_n)}_{S^n|M} \sim P^n_S$.

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

$$\Longrightarrow \quad \boxed{R < I(X;Y) - I(X;S)}$$

Gelfand-Pinsker Channel vs. Wiretap Channel

Similarities:

Gelfand-Pinsker Channel vs. Wiretap Channel

Similarities:

- Target asymptotic relations:
  - **Gelfand-Pinsker Channel:** $\hat{M} = M$ (and M independent of S^n).
  - **Wiretap Channel:** $\hat{M} = M$ and M independent of Z^n.

Gelfand-Pinsker Channel vs. Wiretap Channel

Similarities:

- Target asymptotic relations:
  - **Gelfand-Pinsker Channel:** $\hat{M} = M$ (and M independent of S^n).
  - **Wiretap Channel:** $\hat{M} = M$ and M independent of Z^n.
- Capacity expression

Gelfand-Pinsker Channel vs. Wiretap Channel

Similarities:

- Target asymptotic relations:
  - **Gelfand-Pinsker Channel:** $\hat{M} = M$ (and M independent of S^n).
  - **Wiretap Channel:** $\hat{M} = M$ and M independent of Z^n.
- Capacity expression
- Coding scheme:
  - Codebook
  - Padding bits carry no message information
  - Analysis: Soft Covering of the Sub-Codebook

Gelfand-Pinsker Channel vs. Wiretap Channel

Similarities:

- Target asymptotic relations:
  - **Gelfand-Pinsker Channel:** $\hat{M} = M$ (and M independent of S^n).
  - **Wiretap Channel:** $\hat{M} = M$ and M independent of Z^n.
- Capacity expression
- Coding scheme:
  - Codebook
  - Padding bits carry no message information
  - Analysis: Soft Covering of the Sub-Codebook
- Converse (Csiszár Sum Identity)

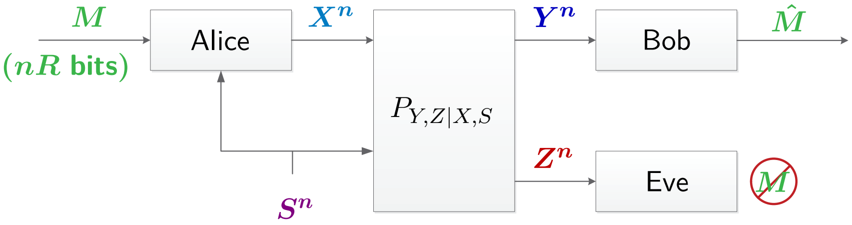
Gelfand-Pinsker Channel vs. Wiretap Channel

Similarities:

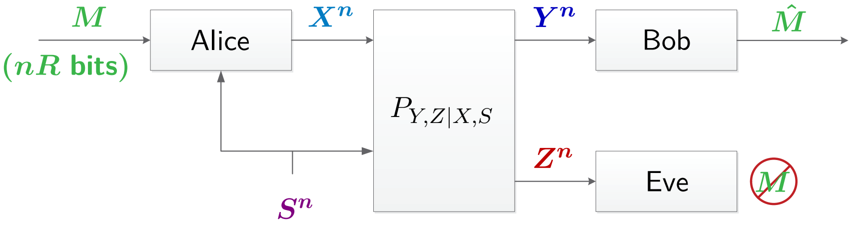
- Target asymptotic relations:
  - **Gelfand-Pinsker Channel:** $\hat{M} = M$ (and M independent of S^n).
  - **Wiretap Channel:** $\hat{M} = M$ and M independent of Z^n.
- Capacity expression
- Coding scheme:
  - Codebook
  - Padding bits carry no message information
  - Analysis: Soft Covering of the Sub-Codebook
- Converse (Csiszár Sum Identity)

★ Ziv Goldfeld (MIT, USA); Haim H Permuter (Ben-Gurion University, Israel), "A Useful Analogy Between Wiretap and Gelfand-Pinsker Channels," ISIT 2018, Vail, Colorado.

The Gelfand-Pinsker Wiretap Channel



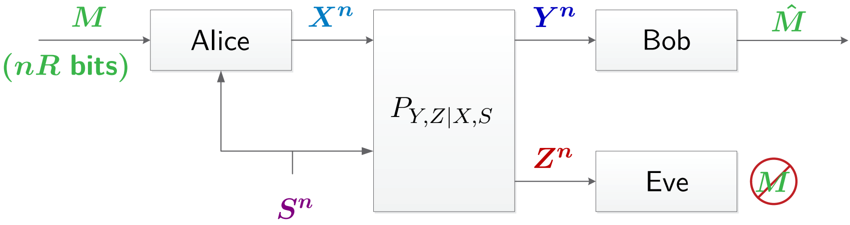
The Gelfand-Pinsker Wiretap Channel



Secrecy-Capacity:

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

The Gelfand-Pinsker Wiretap Channel



The State Information Plays a Double Role:

- Enhancing the total reliable communication rate
- Enhancing Bob's advantage over Eve

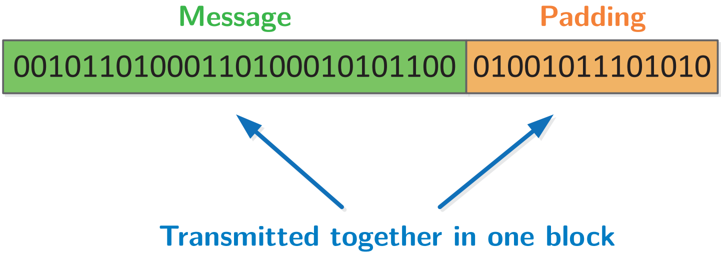
The Gelfand-Pinsker Wiretap Channel
[Chen-Han Vinck 2006]

Observation1: Use same padding bits for **GP** and **wiretap** coding.

The Gelfand-Pinsker Wiretap Channel
[Chen-Han Vinck 2006]

Observation1: Use same padding bits for **GP** and **wiretap** coding.

- **Random codebook:** (**Message**, **Padding**) $\rightarrow$ $U^n \sim P_U^n$.
- **Codebook binning:** Pad nR **message bits** with $n\tilde{R}$ **padding bits**.



The Gelfand-Pinsker Wiretap Channel

[Chen-Han Vinck 2006]

Observation1: Use same padding bits for **GP** and **wiretap** coding.

- **Random codebook:** $(\text{Message}, \text{Padding}) \rightarrow U^n \sim P_U^n$.
- **Codebook binning:** Pad nR **message bits** with $n\tilde{R}$ **padding bits**.
- **Correlating U^n with S^n:** $\tilde{R} > I(U;S)$.

The Gelfand-Pinsker Wiretap Channel

[Chen-Han Vinck 2006]

Observation1: Use same padding bits for **GP** and **wiretap** coding.

- **Random codebook:** (Message, Padding) $\rightarrow$ $U^n \sim P_U^n$.
- **Codebook binning:** Pad nR **message bits** with $n\tilde{R}$ **padding bits**.
- **Correlating U^n with S^n:** $\tilde{R} > I(U;S)$.
- **Security:** $\tilde{R} > I(U;Z)$.

The Gelfand-Pinsker Wiretap Channel

[Chen-Han Vinck 2006]

Observation1: Use same padding bits for **GP** and **wiretap** coding.

- **Random codebook:** (Message, Padding) $\rightarrow$ $U^n \sim P_U^n$.
- **Codebook binning:** Pad nR **message bits** with $n\tilde{R}$ **padding bits**.
- **Correlating U^n with S^n:** $\tilde{R} > I(U;S)$.
- **Security:** $\tilde{R} > I(U;Z)$.
- **Reliability:** $R + \tilde{R} < I(U;Y)$.

The Gelfand-Pinsker Wiretap Channel

[Chen-Han Vinck 2006]

Observation1: Use same padding bits for **GP** and **wiretap** coding.

- **Random codebook:** (Message, Padding) $\rightarrow$ $U^n \sim P_U^n$.
- **Codebook binning:** Pad nR **message bits** with $n\tilde{R}$ **padding bits**.
- **Correlating U^n with S^n:** $\tilde{R} > I(U;S)$.
- **Security:** $\tilde{R} > I(U;Z)$.
- **Reliability:** $R + \tilde{R} < I(U;Y)$.

Theorem (Chen-Han Vinck 2006)

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

Joint distribution: $P_S P_{U,X|S} P_{Y,Z|X,S}$ $\Big\{ U -\!\!\circ\!\!- (X,S) -\!\!\circ\!\!- (Y,Z) \Big\}$

The Gelfand-Pinsker Wiretap Channel

[Prabhakaran *et al.* 2012] (Special Case)

Observation2: Padding bits used for **GP correlation** may be **secret**.

The Gelfand-Pinsker Wiretap Channel

[Prabhakaran *et al.* 2012] (Special Case)

Observation2: Padding bits used for **GP correlation** may be **secret**.

- Split $\tilde{R}$ to $\tilde{R}_1 + \tilde{R}_2$

The Gelfand-Pinsker Wiretap Channel
[Prabhakaran *et al.* 2012] (Special Case)

Observation2: Padding bits used for **GP correlation** may be **secret**.

- Split $\tilde{R}$ to $\tilde{R}_1 + \tilde{R}_2$
- **Reliability:** $R + \tilde{R}_1 + \tilde{R}_2 < I(U;Y)$.
- **Correlating U^n with S^n:** $\tilde{R}_1 + \tilde{R}_2 > I(U;S)$.

The Gelfand-Pinsker Wiretap Channel

[Prabhakaran *et al.* 2012] (Special Case)

Observation2: Padding bits used for **GP correlation** may be **secret**.

- Split $\tilde{R}$ to $\tilde{R}_1 + \tilde{R}_2$
- **Reliability:** $R + \tilde{R}_1 + \tilde{R}_2 < I(U;Y)$.
- **Correlating U^n with S^n:** $\tilde{R}_1 + \tilde{R}_2 > I(U;S)$.
- **Security:** $\tilde{R}_1 > I(U;Z)$.

The Gelfand-Pinsker Wiretap Channel

[Prabhakaran *et al.* 2012] (Special Case)

Observation2: Padding bits used for **GP correlation** may be **secret**.

- Split $\tilde{R}$ to $\tilde{R}_1 + \tilde{R}_2$
- **Reliability:** $R + \tilde{R}_1 + \tilde{R}_2 < I(U;Y)$.
- **Correlating U^n with S^n:** $\tilde{R}_1 + \tilde{R}_2 > I(U;S)$.
- **Security:** $\tilde{R}_1 > I(U;Z)$.

As a result:

- When $I(U;S) > I(U;Z)$: $\tilde{R}_2 > 0$ is achieved.

$$\overbrace{\boxed{00101101000110100010101100}}^{nR}\overbrace{\underbrace{\boxed{01001011}}_{nI(U;Z)}\underbrace{\boxed{101010}}_{n\tilde{R}_2}}^{nI(U;S)}$$

The Gelfand-Pinsker Wiretap Channel

[Prabhakaran *et al.* 2012] (Special Case)

Observation2: Padding bits used for **GP correlation** may be **secret**.

- Split $\tilde{R}$ to $\tilde{R}_1 + \tilde{R}_2$
- **Reliability:** $R + \tilde{R}_1 + \tilde{R}_2 < I(U;Y)$.
- **Correlating U^n with S^n:** $\tilde{R}_1 + \tilde{R}_2 > I(U;S)$.
- **Security:** $\tilde{R}_1 > I(U;Z)$.

As a result:

- When $I(U;S) > I(U;Z)$: $\tilde{R}_2 > 0$ is achieved.
- $\tilde{R}_2$ is the rate of **secret padding** bits.

The Gelfand-Pinsker Wiretap Channel

[Prabhakaran *et al.* 2012] (Special Case)

Observation2: Padding bits used for **GP correlation** may be **secret**.

- Split $\tilde{R}$ to $\tilde{R}_1 + \tilde{R}_2$
- **Reliability:** $R + \tilde{R}_1 + \tilde{R}_2 < I(U;Y)$.
- **Correlating U^n with S^n:** $\tilde{R}_1 + \tilde{R}_2 > I(U;S)$.
- **Security:** $\tilde{R}_1 > I(U;Z)$.

As a result:

- When $I(U;S) > I(U;Z)$: $\tilde{R}_2 > 0$ is achieved.
- $\tilde{R}_2$ is the rate of **secret padding** bits.
- These bits may be used as a **Secret Key**!

The Gelfand-Pinsker Wiretap Channel

[Prabhakaran *et al.* 2012] (Special Case)

Observation2: Padding bits used for **GP correlation** may be **secret**.

- Split $\tilde{R}$ to $\tilde{R}_1 + \tilde{R}_2$
- **Reliability:** $R + \tilde{R}_1 + \tilde{R}_2 < I(U;Y)$.
- **Correlating U^n with S^n:** $\tilde{R}_1 + \tilde{R}_2 > I(U;S)$.
- **Security:** $\tilde{R}_1 > I(U;Z)$.

As a result:

- When $I(U;S) > I(U;Z)$: $\tilde{R}_2 > 0$ is achieved.
- $\tilde{R}_2$ is the rate of **secret padding** bits.
- These bits may be used as a **Secret Key**!
  - Secure
  - Uniformly distributed
  - Not (necessarily) controllable

The Gelfand-Pinsker Wiretap Channel

Theorem (Prabhakaran *et al.* 2012 – Special Case)

A secret message-key rate couple $(\boldsymbol{R_m}, \boldsymbol{R_k})$ *such that:*

$$\boldsymbol{R_m} < \boldsymbol{I(U;Y)} - \boldsymbol{I(U;S)}$$
$$\boldsymbol{R_k} + \boldsymbol{R_m} < \boldsymbol{I(U;Y)} - \boldsymbol{I(U;Z)}$$

for joint distribution: $P_S P_{U,X|S} P_{Y,Z|X,S}$, *is achievable.*

The Gelfand-Pinsker Wiretap Channel

Theorem (Prabhakaran *et al.* 2012 – Special Case)

A secret message-key rate couple $(\boldsymbol{R_m}, \boldsymbol{R_k})$ *such that:*

$$\begin{aligned} \boldsymbol{R_m} &< \boldsymbol{I(U;Y)} - \boldsymbol{I(U;S)} \\ \boldsymbol{R_k} + \boldsymbol{R_m} &< \boldsymbol{I(U;Y)} - \boldsymbol{I(U;Z)} \end{aligned}$$

for joint distribution: $P_S P_{U,X|S} P_{Y,Z|X,S}$*, is achievable.*

Proposition - Achievable Secret Key Rate ($R_m = 0$) (Khisti 2010)

$$\mathsf{C}^{\mathsf{SK}}_{\mathsf{GP-WTC}} \geq \max_{\substack{P_{U,X|S}: \\ I(U;Y)-I(U;S)\geq 0}} \Big[\boldsymbol{I(U;Y)} - \boldsymbol{I(U;Z)} \Big]$$

Joint distribution: $P_S P_{U,X|S} P_{Y,Z|X,S}$

The GP WTC - Two Layer Scheme

Motivation:

The GP WTC - Two Layer Scheme

Motivation:

1. U that is **good for reliability** might be **bad for security**:

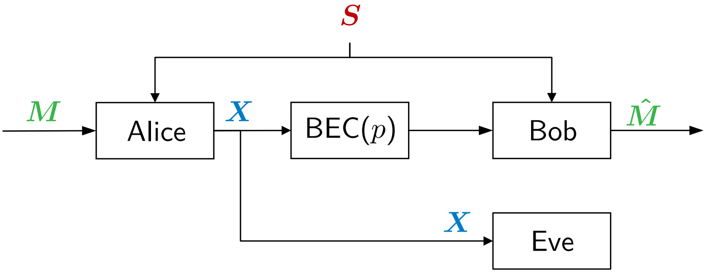
   High $\left[I(U;Y) - I(U;S)\right] \iff$ **Low** $\left[I(U;Y) - I(U;Z)\right]$

The GP WTC - Two Layer Scheme

Motivation:

1. U that is **good for reliability** might be **bad for security**:

High $\left[I(U;Y) - I(U;S)\right] \iff$ **Low** $\left[I(U;Y) - I(U;Z)\right]$

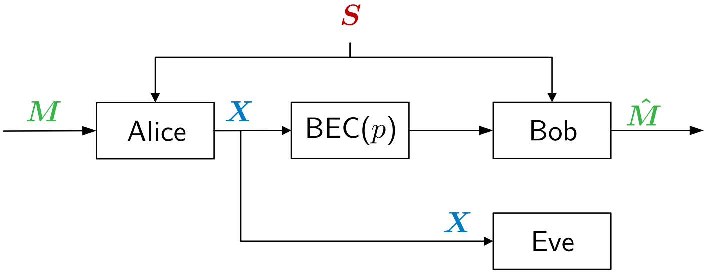


The GP WTC - Two Layer Scheme

Motivation:

1. U that is **good for reliability** might be **bad for security**:

   High $\left[\boldsymbol{I(U;Y)} - \boldsymbol{I(U;S)}\right] \Longleftrightarrow$ **Low** $\left[\boldsymbol{I(U;Y)} - \boldsymbol{I(U;Z)}\right]$



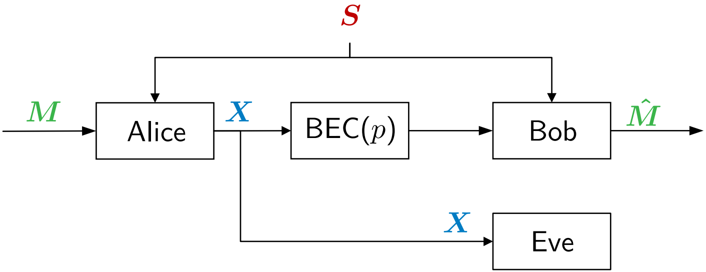
- For reliability: $\boldsymbol{X} = f(\boldsymbol{U})$

The GP WTC - Two Layer Scheme

Motivation:

1. $\boldsymbol{U}$ that is **good for reliability** might be **bad for security**:

$$\text{High } \left[\boldsymbol{I(U;Y)} - \boldsymbol{I(U;S)}\right] \Longleftrightarrow \text{Low } \left[\boldsymbol{I(U;Y)} - \boldsymbol{I(U;Z)}\right]$$



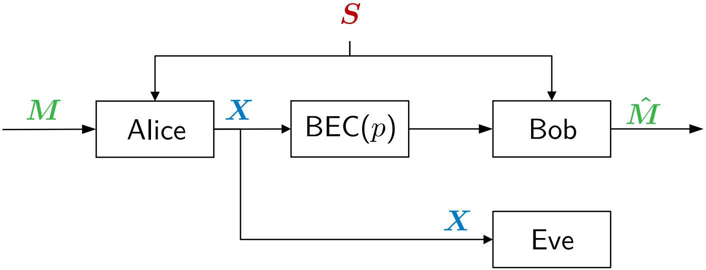
- For reliability: $\boldsymbol{X} = f(\boldsymbol{U})$
- Harms secrecy as **Eve** has a better observation of X than **Bob**

The GP WTC - Two Layer Scheme

Motivation:

1. U that is **good for reliability** might be **bad for security**:

   High $\left[I(U;Y) - I(U;S)\right] \iff$ **Low** $\left[I(U;Y) - I(U;Z)\right]$

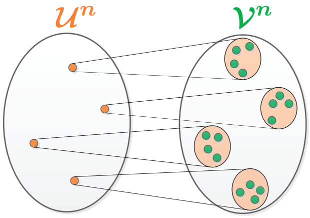


   - For reliability: $X = f(U)$
   - Harms secrecy as **Eve** has a better observation of X than **Bob**

2. Enhance reliability without harming security by adding an inner coding layer.

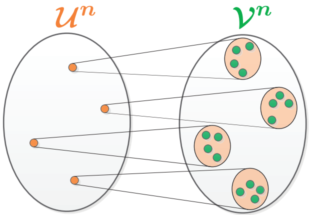
The GP WTC - Two Layer Scheme

Superposition Code:



The GP WTC - Two Layer Scheme

Superposition Code:



- U^n is decodable by **Eve** with redundancy $\Longrightarrow$ waste channel resources.
- All secrecy comes from V^n.

The GP WTC - Two Layer Scheme

Theorem (Prabhakaran *et al.* 2012)

A secret message-key rate couple $(\boldsymbol{R_m}, \boldsymbol{R_k})$ *such that:*

$$\begin{aligned} \boldsymbol{R_m} &\leq I(U,V;Y) - I(U,V;S) \\ \boldsymbol{R_k} + \boldsymbol{R_m} &\leq I(V;Y|U) - I(V;Z|U) \end{aligned}$$

for joint distribution: $P_S P_U P_{V,X|S,U} P_{Y,Z|X,S}$ *is achievable.*

The GP WTC - Two Layer Scheme

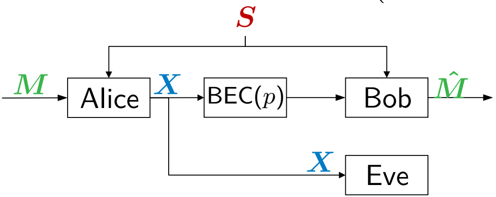
Theorem (Prabhakaran *et al.* 2012)

A secret message-key rate couple $(\boldsymbol{R_m}, \boldsymbol{R_k})$ *such that:*

$$\boldsymbol{R_m} \leq I(U,V;Y) - I(U,V;S)$$
$$\boldsymbol{R_k} + \boldsymbol{R_m} \leq I(V;Y|U) - I(V;Z|U)$$

for joint distribution: $P_S P_U P_{V,X|S,U} P_{Y,Z|X,S}$ *is achievable.*

- Achieves secrecy capacity for the example: $\Big(U = \boldsymbol{X}, V = \{\boldsymbol{X}, \boldsymbol{S}\}\Big)$



The GP WTC - Two Layer Scheme

Theorem (Prabhakaran *et al.* 2012)

A secret message-key rate couple $(\boldsymbol{R_m}, \boldsymbol{R_k})$ *such that:*

$$\begin{aligned} \boldsymbol{R_m} &\leq I(U,V;Y) - I(U,V;S) \\ \boldsymbol{R_k} + \boldsymbol{R_m} &\leq I(V;Y|U) - I(V;Z|U) \end{aligned}$$

for joint distribution: $\boldsymbol{P_S P_U} P_{V,X|S,U} P_{Y,Z|X,S}$ *is achievable.*

- Achieves secrecy capacity for the example: $\Big(U = \boldsymbol{X}, V = \{\boldsymbol{X}, \boldsymbol{S}\}\Big)$
- $\boldsymbol{U} \perp \boldsymbol{S} \implies$ No GP coding in the inner layer

The GP WTC - Two Layer Scheme

Theorem (Prabhakaran *et al.* 2012)

A secret message-key rate couple $(\boldsymbol{R_m}, \boldsymbol{R_k})$ *such that:*

$$\boldsymbol{R_m} \leq I(U,V;Y) - I(U,V;S)$$
$$\boldsymbol{R_k} + \boldsymbol{R_m} \leq I(V;Y|U) - I(V;Z|U)$$

for joint distribution: $\boldsymbol{P_S P_U} P_{V,X|S,U} P_{Y,Z|X,S}$ *is achievable.*

- Achieves secrecy capacity for the example: $\Big(U = \boldsymbol{X}, V = \{\boldsymbol{X}, \boldsymbol{S}\}\Big)$
- $\boldsymbol{U} \perp \boldsymbol{S} \implies$ No GP coding in the inner layer
- **Weak** secrecy only!

The GP WTC - Two Layer Scheme

Theorem (Goldfeld *et al.* 2016)

A secret message rate $\boldsymbol{R_m}$ *such that*

$$\boldsymbol{R_m} \leq \min \begin{Bmatrix} I(U,V;Y) - I(U,V;S) \\ I(V;Y|U) - I(V;Z|U) - [I(U;S) - I(U;Y)]_+ \end{Bmatrix}$$

for joint distribution: $P_S P_{U,V,X|S} P_{Y,Z|X,S}$ *is achievable.*

The GP WTC - Two Layer Scheme

Theorem (Goldfeld *et al.* 2016)

A secret message rate $\boldsymbol{R_m}$ *such that*

$$\boldsymbol{R_m} \leq \min \begin{Bmatrix} I(U,V;Y) - I(U,V;S) \\ I(V;Y|U) - I(V;Z|U) - [I(U;S) - I(U;Y)]_+ \end{Bmatrix}$$

for joint distribution: $\boldsymbol{P_S P_{U,V,X|S}} P_{Y,Z|X,S}$ *is achievable.*

- **Allows dependence between inner layer and state.**

The GP WTC - Two Layer Scheme

Theorem (Goldfeld *et al.* 2016)

A secret message rate $\boldsymbol{R_m}$ *such that*

$$\boldsymbol{R_m} \leq \min \begin{Bmatrix} I(U,V;Y) - I(U,V;S) \\ I(V;Y|U) - I(V;Z|U) - [I(U;S) - I(U;Y)]_+ \end{Bmatrix}$$

for joint distribution: $P_S P_{U,V,X|S} P_{Y,Z|X,S}$ *is achievable.*

- Allows dependence between inner layer and state.
- **Semantic security** is guaranteed!

The GP WTC - Two Layer Scheme

Theorem (Goldfeld *et al.* 2016)

A secret message rate $\boldsymbol{R_m}$ *such that*

$$\boldsymbol{R_m} \leq \min \begin{Bmatrix} I(U,V;Y) - I(U,V;S) \\ I(V;Y|U) - I(V;Z|U) - [I(U;S) - I(U;Y)]_+ \end{Bmatrix}$$

for joint distribution: $P_S P_{U,V,X|S} P_{Y,Z|X,S}$ *is achievable.*

- Allows dependence between inner layer and state.
- **Semantic security** is guaranteed!
- **Strictly suboptimal for secret key generation!**

The GP WTC - Two Layer Scheme

Our results

Theorem (Bunin *et al.* 2017)

A secret message-key rate couple $(\boldsymbol{R_m}, \boldsymbol{R_k})$ *such that:*

$$\boldsymbol{R_m} \leq I(U,V;Y) - I(U,V;S)$$
$$\boldsymbol{R_k} + \boldsymbol{R_m} \leq I(V;Y|U) - I(V;Z|U) - [I(U;S) - I(U;Y)]_+$$

for joint distribution: $P_S P_{U,V,X|S} P_{Y,Z|X,S}$ *is achievable.*

The GP WTC - Two Layer Scheme

Our results

Theorem (Bunin *et al.* 2017)

A secret message-key rate couple $(\boldsymbol{R_m}, \boldsymbol{R_k})$ *such that:*

$$\boldsymbol{R_m} \leq \boldsymbol{I(U,V;Y) - I(U,V;S)}$$
$$\boldsymbol{R_k} + \boldsymbol{R_m} \leq I(V;Y|U) - I(V;Z|U) - [I(U;S) - I(U;Y)]_+$$

for joint distribution: $P_S P_{U,V,X|S} P_{Y,Z|X,S}$ *is achievable.*

- **Total reliable communication rate**

The GP WTC - Two Layer Scheme

Our results

Theorem (Bunin *et al.* 2017)

A secret message-key rate couple $(\boldsymbol{R_m}, \boldsymbol{R_k})$ *such that:*

$$\boldsymbol{R_m} \leq I(U,V;Y) - I(U,V;S)$$

$$\boldsymbol{R_k} + \boldsymbol{R_m} \leq \boldsymbol{I(V;Y|U) - I(V;Z|U)} - [I(U;S) - I(U;Y)]_+$$

for joint distribution: $P_S P_{U,V,X|S} P_{Y,Z|X,S}$ *is achievable.*

- **Total secrecy rate of the outer layer**

The GP WTC - Two Layer Scheme

Our results

Theorem (Bunin *et al.* 2017)

A secret message-key rate couple $(\boldsymbol{R_m}, \boldsymbol{R_k})$ *such that:*

$$\boldsymbol{R_m} \leq I(U,V;Y) - I(U,V;S)$$
$$\boldsymbol{R_k} + \boldsymbol{R_m} \leq I(V;Y|U) - I(V;Z|U) - [\boldsymbol{I(U;S)} - \boldsymbol{I(U;Y)}]_+$$

for joint distribution: $P_S P_{U,V,X|S} P_{Y,Z|X,S}$ *is achievable.*

- **Insufficient resolution in the inner layer reduces secrecy!**

The GP WTC - Two Layer Scheme

Our results

Theorem (Bunin *et al.* 2017)

A secret message-key rate couple $(\boldsymbol{R_m}, \boldsymbol{R_k})$ *such that:*

$$\boldsymbol{R_m} \leq I(U,V;Y) - I(U,V;S)$$

$$\boldsymbol{R_k} + \boldsymbol{R_m} \leq I(V;Y|U) - I(V;Z|U) - [\boldsymbol{I(U;S)} - \boldsymbol{I(U;Y)}]_+$$

for joint distribution: $P_S P_{U,V,X|S} P_{Y,Z|X,S}$ *is achievable.*

- **Insufficient resolution in the inner layer reduces secrecy!**
  - This penalty term is essential!
    Zibaeenejad 2015: The penalty term is missing.

The GP WTC - Two Layer Scheme

Our results

Theorem (Bunin *et al.* 2017)

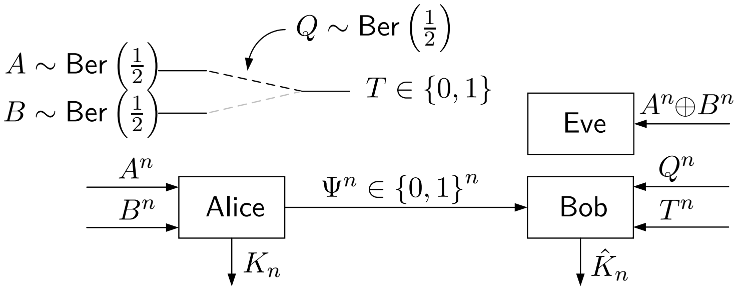
A secret message-key rate couple $(\boldsymbol{R_m}, \boldsymbol{R_k})$ *such that:*

$$\boldsymbol{R_m} \leq I(U,V;Y) - I(U,V;S)$$
$$\boldsymbol{R_k} + \boldsymbol{R_m} \leq I(V;Y|U) - I(V;Z|U) - [\boldsymbol{I(U;S)} - \boldsymbol{I(U;Y)}]_+$$

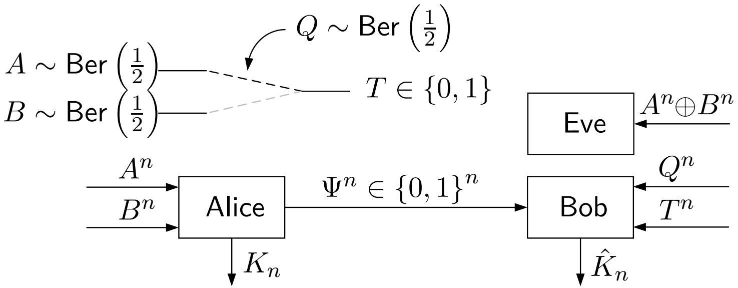
for joint distribution: $P_S P_{U,V,X|S} P_{Y,Z|X,S}$ *is achievable.*

- **Insufficient resolution in the inner layer reduces secrecy!**
  - This penalty term is essential!
    Zibaeenejad 2015: The penalty term is missing.
  - For $R_k = 0$ it is always beneficial to take $I(U;Y) - I(U;S) \geq 0$ (Goldfeld *et al.* 2016).

Example of the necessity of the penalty term:

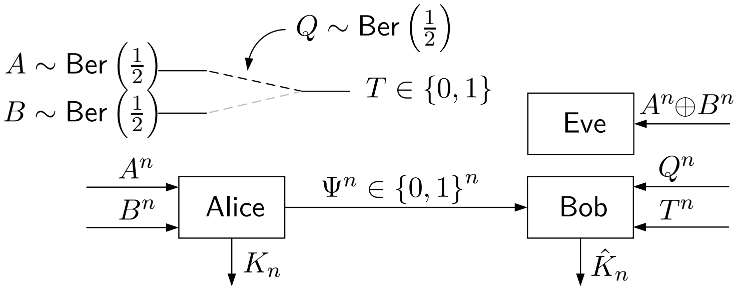


Example of the necessity of the penalty term:



- The maximal rate of *common randomness* between Alice and Bob is 2.
- In such case $K_n \approx (A^n, B^n)$. $\implies$ The secret key rate is 1.

Example of the necessity of the penalty term:



- The maximal rate of *common randomness* between Alice and Bob is 2.
- In such case $K_n \approx (A^n, B^n)$. $\implies$ The secret key rate is 1.
- $\implies$ A secret key rate of 2 is not attainable.
- However, we can choose (U, V, Ψ) such that $I(V; Y^n|U) - I(V; Z^n|U) = 2$.

- Construct a two-layered superposition codebook.

The GP WTC - Two Layer Scheme

Our results - Proof idea

- Construct a two-layered superposition codebook.
- Perform binning of the outer codebook layer.
  - The entire secret message is encoded in the outer layer.

The GP WTC - Two Layer Scheme

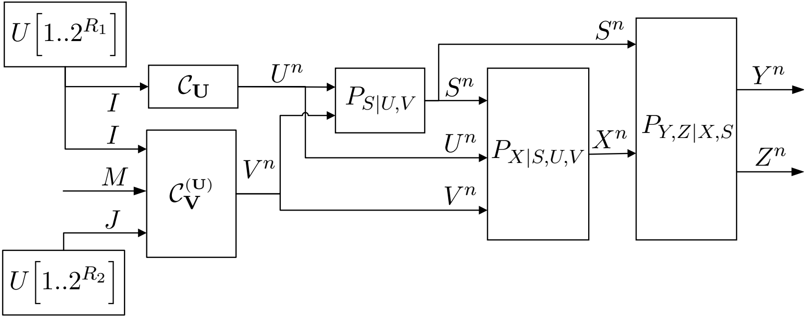
Our results - Proof idea

- Construct a two-layered superposition codebook.
- Perform binning of the outer codebook layer.
  - The entire secret message is encoded in the outer layer.
- Correlate the codeword with the state via the Likelihood Encoder.

The GP WTC - Two Layer Scheme

Our results - Proof idea

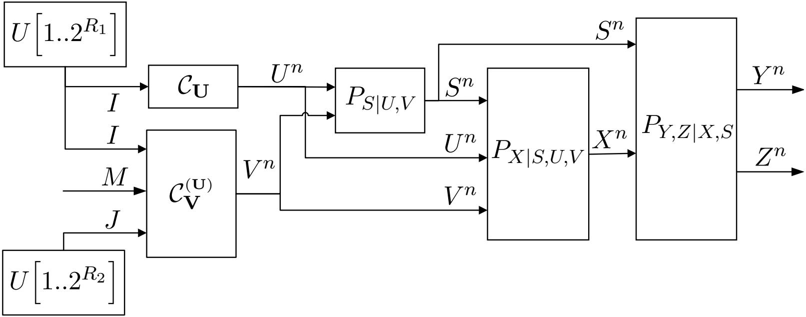
- Construct a two-layered superposition codebook.
- Perform binning of the outer codebook layer.
  - The entire secret message is encoded in the outer layer.
- Correlate the codeword with the state via the Likelihood Encoder.
- Analysis: Use the SCL to approximate the joint distribution by



The GP WTC - Two Layer Scheme

Our results - Proof idea

- Construct a two-layered superposition codebook.
- Perform binning of the outer codebook layer.
  - The entire secret message is encoded in the outer layer.
- Correlate the codeword with the state via the Likelihood Encoder.
- Analysis: Use the SCL to approximate the joint distribution by



- Part of the redundancy index J may be used as a SK.

The GP WTC - Two Layer Scheme

Our results - Proof idea

What happens when $I(U;Y) < I(U;S)$?

- $I(U;S)$ is the rate of the inner layer.
- When $I(U;Y) < I(U;S)$ the decoder lacks the resolution to decode.

What happens when $I(U;Y) < I(U;S)$?

- $I(U;S)$ is the rate of the inner layer.
- When $I(U;Y) < I(U;S)$ the decoder lacks the resolution to decode.
- However, the coding scheme requires reliably decoding both layers.

The GP WTC - Two Layer Scheme

Our results - Proof idea

What happens when $I(U;Y) < I(U;S)$?

- $I(U;S)$ is the rate of the inner layer.
- When $I(U;Y) < I(U;S)$ the decoder lacks the resolution to decode.
- However, the coding scheme requires reliably decoding both layers.
- Hence, the outer layer has to convey part of the inner layer index.

What happens when $I(U;Y) < I(U;S)$?

- $I(U;S)$ is the rate of the inner layer.
- When $I(U;Y) < I(U;S)$ the decoder lacks the resolution to decode.
- However, the coding scheme requires reliably decoding both layers.
- Hence, the outer layer has to convey part of the inner layer index.
- However, the inner layer is decodable by the eavesdropper.
- This results in a loss of $[I(U;S) - I(U;Y)]_+$ in the secrecy rate.

The GP WTC - Two Layer Scheme

Our results

Theorem (Bunin *et al.* 2017)

A secret message-key rate couple $(\boldsymbol{R_m}, \boldsymbol{R_k})$ *such that:*

$$\boldsymbol{R_m} \leq I(U,V;Y) - I(U,V;S)$$
$$\boldsymbol{R_k} + \boldsymbol{R_m} \leq I(V;Y|U) - I(V;Z|U) - \left[I(U;S) - I(U;Y)\right]_+$$

for joint distribution: $P_S P_{U,V,X|S} P_{Y,Z|X,S}$ *is achievable.*

Relation to Previous Schemes:

The GP WTC - Two Layer Scheme

Our results

Theorem (Bunin *et al.* 2017)

A secret message-key rate couple $(\boldsymbol{R_m}, \boldsymbol{R_k})$ *such that:*

$$\boldsymbol{R_m} \leq I(U,V;Y) - I(U,V;S)$$
$$\boldsymbol{R_k} + \boldsymbol{R_m} \leq I(V;Y|U) - I(V;Z|U) - [I(U;S) - I(U;Y)]_+$$

for joint distribution: $P_S P_{U,V,X|S} P_{Y,Z|X,S}$ *is achievable.*

Relation to Previous Schemes:

- Recovers all previous secret key or message results.

Theorem (Bunin *et al.* 2017)

A secret message-key rate couple $(\boldsymbol{R_m}, \boldsymbol{R_k})$ *such that:*

$$\begin{aligned} \boldsymbol{R_m} &\leq I(U,V;Y) - I(U,V;S) \\ \boldsymbol{R_k} + \boldsymbol{R_m} &\leq I(V;Y|U) - I(V;Z|U) - \left[I(U;S) - I(U;Y)\right]_+ \end{aligned}$$

for joint distribution: $P_S P_{U,V,X|S} P_{Y,Z|X,S}$ *is achievable.*

Relation to Previous Schemes:

- Recovers all previous secret key or message results.
    - Improves over Prabhakaran *et al.* by allowing GP in the inner layer.

The GP WTC - Two Layer Scheme

Our results

Theorem (Bunin *et al.* 2017)

A secret message-key rate couple $(\boldsymbol{R_m}, \boldsymbol{R_k})$ *such that:*

$$\boldsymbol{R_m} \leq I(U,V;Y) - I(U,V;S)$$
$$\boldsymbol{R_k} + \boldsymbol{R_m} \leq I(V;Y|U) - I(V;Z|U) - [I(U;S) - I(U;Y)]_+$$

for joint distribution: $P_S P_{U,V,X|S} P_{Y,Z|X,S}$ *is achievable.*

Relation to Previous Schemes:

- Recovers all previous secret key or message results.
  - Improves over Prabhakaran *et al.* by allowing GP in the inner layer.
  - Improves over Goldfeld *et al.* by utilizing secret padding bits for key.

Theorem (Bunin *et al.* 2017)

A secret message-key rate couple $(\boldsymbol{R_m}, \boldsymbol{R_k})$ *such that:*

$$\boldsymbol{R_m} \leq I(U,V;Y) - I(U,V;S)$$
$$\boldsymbol{R_k} + \boldsymbol{R_m} \leq I(V;Y|U) - I(V;Z|U) - \left[I(U;S) - I(U;Y)\right]_+$$

for joint distribution: $P_S P_{U,V,X|S} P_{Y,Z|X,S}$ *is achievable.*

Relation to Previous Schemes:

- Recovers all previous secret key or message results.
  - Improves over Prabhakaran *et al.* by allowing GP in the inner layer.
  - Improves over Goldfeld *et al.* by utilizing secret padding bits for key.
- Upgrades all results to **semantic-security**.

The GP WTC - Two Layer Scheme

Additional Well Known Results Recovered as Special Cases:

The GP WTC - Two Layer Scheme

Additional Well Known Results Recovered as Special Cases:

- Secret key generation using correlated sources and public channel (Ahlswede-Csiszár 1993, Csiszár-Narayan 2000)

The GP WTC - Two Layer Scheme

Additional Well Known Results Recovered as Special Cases:

- Secret key generation using correlated sources and public channel (Ahlswede-Csiszár 1993, Csiszár-Narayan 2000)
- Secret key generation using state dependent WTC (Khisti *et al.* 2011, Zibaeenejad 2015)

The GP WTC - Two Layer Scheme

Additional Well Known Results Recovered as Special Cases:

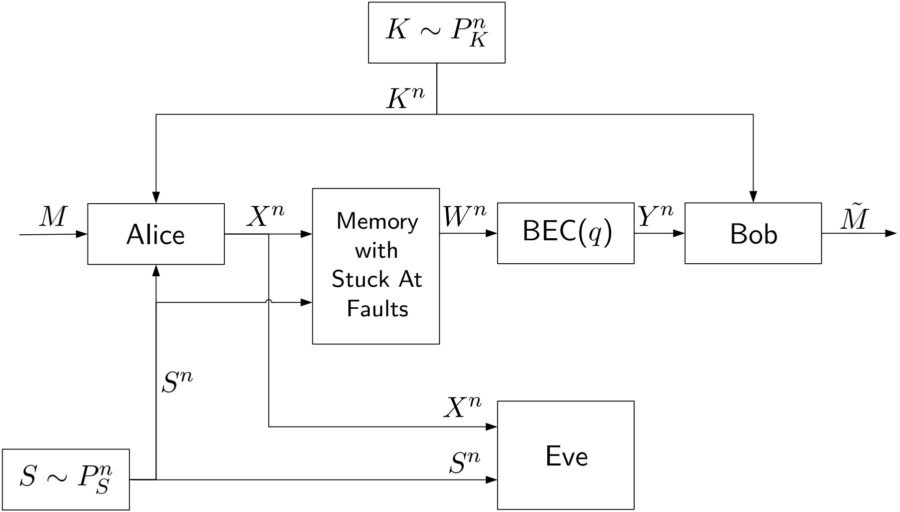
- Secret key generation using correlated sources and public channel (Ahlswede-Csiszár 1993, Csiszár-Narayan 2000)
- Secret key generation using state dependent WTC (Khisti *et al.* 2011, Zibaeenejad 2015)
- WTC with identical side information at both legitimate parties (Khisti *et al.* 2009, Chia-El Gamal 2012)

The GP WTC - Two Layer Scheme

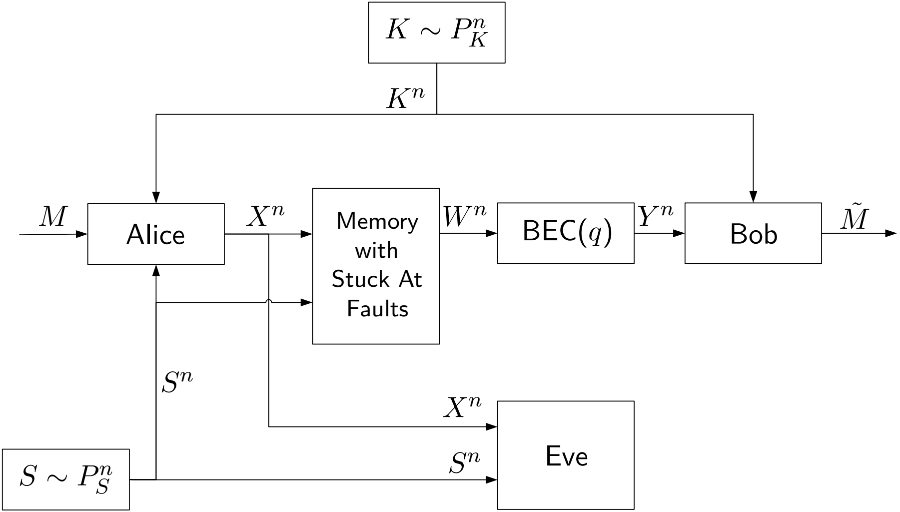
Additional Well Known Results Recovered as Special Cases:

- Secret key generation using correlated sources and public channel (Ahlswede-Csiszár 1993, Csiszár-Narayan 2000)
- Secret key generation using state dependent WTC (Khisti *et al.* 2011, Zibaeenejad 2015)
- WTC with identical side information at both legitimate parties (Khisti *et al.* 2009, Chia-El Gamal 2012)
- Secrecy results for correlated sources over an independent WTC (Khisti *et al.* 2012, Bassi *et al.* 2016)

Example – Improving over Prabhakaran *et al.* 2012



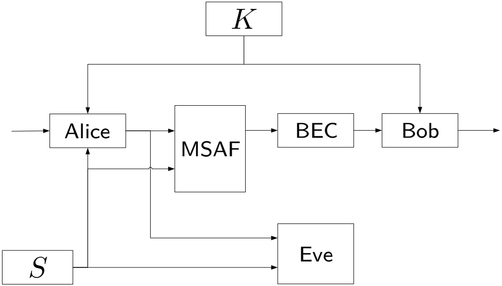
Example – Improving over Prabhakaran *et al.* 2012



★ This example is a special case of the *state dependent less-noisy eavesdropper WTC with a key*, for which our region attains capacity.

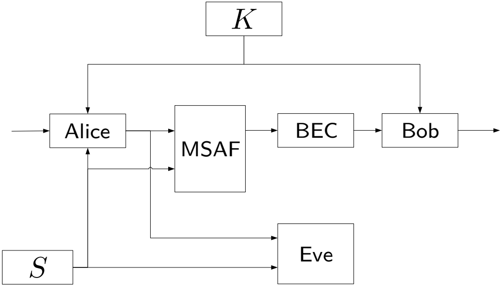
Example – Improving over Prabhakaran *et al.* 2012

Proof Idea



Example – Improving over Prabhakaran *et al.* 2012

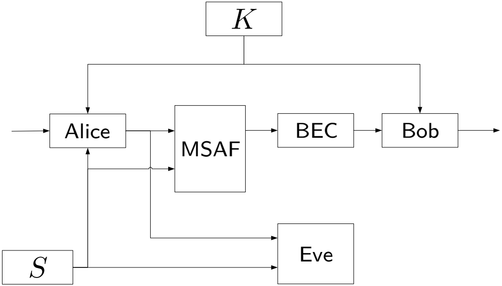
Proof Idea



1. Secrecy will come from an external source K, as side info.

Example – Improving over Prabhakaran *et al.* 2012

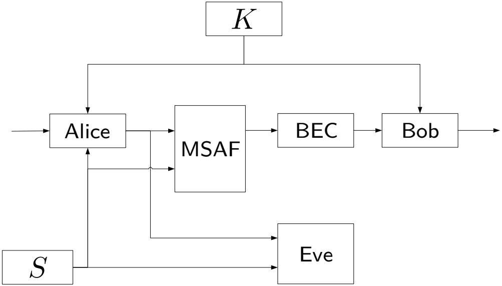
Proof Idea



1. Secrecy will come from an external source K, as side info.
2. Eve has a **strictly** better channel observation.

Example – Improving over Prabhakaran *et al.* 2012

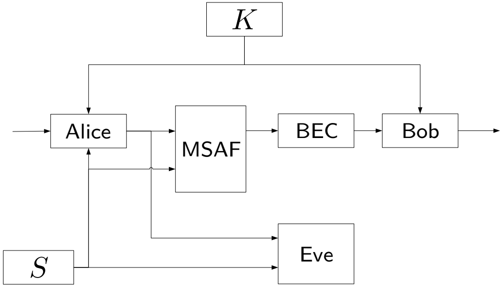
Proof Idea



1. Secrecy will come from an external source K, as side info.
2. Eve has a **strictly** better channel observation.
3. Therefore, all communications has to be in the inner layer.

Example – Improving over Prabhakaran *et al.* 2012

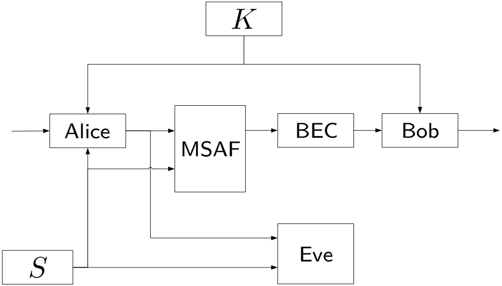
Proof Idea



1. Secrecy will come from an external source K, as side info.
2. Eve has a **strictly** better channel observation.
3. Therefore, all communications has to be in the inner layer.
4. To optimize the total reliable rate, GP coding is needed.

Example – Improving over Prabhakaran *et al.* 2012

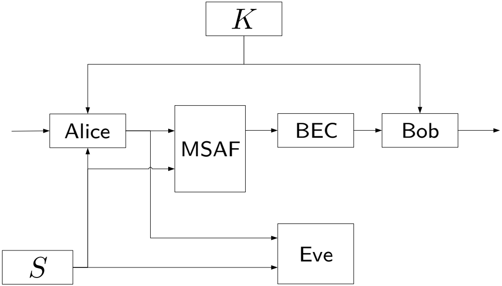
Proof Idea



1. Secrecy will come from an external source K, as side info.
2. Eve has a **strictly** better channel observation.
3. Therefore, all communications has to be in the inner layer.
4. To optimize the total reliable rate, GP coding is needed.
5. Prabhakaran does **not** allow it in the inner layer.

Example – Improving over Prabhakaran *et al.* 2012

Proof Idea



1. Secrecy will come from an external source K, as side info.
2. Eve has a **strictly** better channel observation.
3. Therefore, all communications has to be in the inner layer.
4. To optimize the total reliable rate, GP coding is needed.
5. Prabhakaran does **not** allow it in the inner layer.

We do!

Summary

- Several achievability results are generalized in a single scheme:
  - **Secret message** transmission over a wiretap channel
  - **Secret key** generation using sources over a public channel
  - **Secret key** generation using a wiretap channel
  - **Secret message** transmission and **Secret key** generation for the Gelfand-Pinsker wiretap channel.

Summary

- Several achievability results are generalized in a single scheme:
  - **Secret message** transmission over a wiretap channel
  - **Secret key** generation using sources over a public channel
  - **Secret key** generation using a wiretap channel
  - **Secret message** transmission and **Secret key** generation for the Gelfand-Pinsker wiretap channel.
- All these results are upgraded to **Semantic Security**.

Summary

- Several achievability results are generalized in a single scheme:
  - **Secret message** transmission over a wiretap channel
  - **Secret key** generation using sources over a public channel
  - **Secret key** generation using a wiretap channel
  - **Secret message** transmission and **Secret key** generation for the Gelfand-Pinsker wiretap channel.
- All these results are upgraded to **Semantic Security**.
- Strict improvement over each of the previous results. (For the general setup)

Outlook

- Outer bounds
- Multi-terminal settings
- Action dependent state
- Lossy source reconstruction over the SD-WTC
- Covert/stealthy communication
- Construction of practical codes

Central References I

- A. Bunin, Z. Goldfeld, H. H. Permuter, S. Shamai (Shitz), P. Cuff, and P. Piantanida, *Key and message semantic-security over state-dependent channels*, IEEE Transactions on Information Forensics and Security (2018), *In Press*.
- ———, *Key-message security over state-dependent wiretap channels*, 2018 IEEE Int. Symp. Inf. Theory (ISIT), June 2018, pp. 136–140.
- ———, *Semantically-secured message-key trade-off over wiretap channels with random parameters*, Proceedings of the 2nd Workshop on Communication Security (WCS2017, Springer International Publishing, 2018, pp. 33–48.
- G. Bassi, P. Piantanida, and S. Shamai (Shitz), *Secret key generation over noisy channels with common randomness*, ArXiv preprint (2016), Available at https://arxiv.org/abs/1609.08330.
- I. Csiszár and J. Körner, *Broadcast channels with confidential messages*, IEEE Trans. Inf. Theory **24** (1978), no. 3, 339–348.
- I. Csiszár and P. Narayan, *Common randomness and secret key generation with a helper*, IEEE Trans. Inf. Theory **46** (2000), no. 2, 344–366.

Central References II

- Y. Chen and A. J. Han Vinck, *Wiretap channel with side information*, IEEE Trans. Inf. Theory **54** (2008), no. 1, 395–402.
- B. Dai, A. J. Han Vinck, Y. Luo, and X. Tang, *Wiretap channel with action-dependent channel state information*, Entropy **15** (2013), 445–473.
- Z. Goldfeld, P. Cuff, and H. H. Permuter, *Semantic-security capacity for wiretap channels of type II*, IEEE Trans. Inf. Theory **62** (2016), no. 7, 3863–3879.
- ______, *Wiretap channel with random states non-causally available at the encoder*, Submitted to IEEE Trans. Inf. Theory (2016), Available on ArXiv at https://arxiv.org/abs/1608.00743.
- S. I. Gelfand and M. S. Pinsker, *Coding for channel with random parameters*, Problemy Pered. Inform. (Problems of Inf. Trans.) **9** (1980), no. 1, 19–31.
- Z. Goldfeld and H. H. Permuter, *A useful analogy between wiretap and gelfand-pinsker channels*, 2018 IEEE Int. Symp. Inf. Theory (ISIT), June 2018, pp. 121–125.

Central References III

- G. Keshet, Y. Steinberg, and N. Merhav, *Channel coding in the presence of side information*, Foundations and Trends in Commun. and Inf. Theory **4** (2007), no. 6, 445–586.
- Y. Liang, H. V. Poor, and S. Shamai, *Information theoretic security*, Foundations and Trends in Commun. and Inf. Theory **5** (2009), no. 4-5, 355–580.
- V. Prabhakaran, K. Eswaran, and K. Ramchandran, *Secrecy via sources and channels*, IEEE Trans. Inf. Theory **58** (2012), no. 11, 6747–6765.
- E. Song, P. Cuff, and V. Poor, *The likelihood encoder for lossy compression*, IEEE Trans. Inf. Theory **62** (2016), no. 4, 1836–1849.
- T. Weissman, *Capacity of channels with action-dependent states*, IEEE Trans. Inf. Theory **56** (2010), no. 11, 5396–5411.
- A. Zibaeenejad, *Key generation over wiretap models with non-causal side information*, IEEE Trans. Inf. Forensic Secur. **10** (2015), no. 7, 1456–1471.

Thank you!

Abstract

Two fundamental questions in physical layer security are those related to the best achievable transmission rate of a secret message (SM) over a noisy channel, and the highest attainable secret key (SK) rate that distributed parties can agree upon. We study the trade-off between SM and SK rates simultaneously achievable over a state-dependent wiretap channel with non-causal channel state information (CSI) at the encoder. This model subsumes all other instances of CSI availability as special cases, and calls for an efficient utilization of the state sequence both for reliability and security purposes.

We derive an inner bound on the SM-SK capacity region based on a novel superposition coding scheme. This inner bound improves upon the previously best known SM-SK trade-off result by Prabhakaran et al, and to the best of our knowledge, upon all other existing lower bounds for either SM or SK for this setup. The results are derived under the strict semantic-security metric that requires negligible information leakage for all message-key distributions. The achievability proof uses the likelihood encoder and the strong soft-covering lemma for superposition codes. We conclude by a short outlook.