Physical Layer Security over Wiretap Channels with Random Parameters

Ziv Goldfeld, Paul Cuff and Haim Permuter

Ben Gurion University and Princeton University

2017 International Symposium on Cyber Security Cryptography and Machine Learning Conference
June 29-30, 2017

Physical Layer Security

Physical Layer Security

- Rooted in Information Theory.

Physical Layer Security

- Rooted in Information Theory.
- Alternative approach to cryptography:

Physical Layer Security

- Rooted in Information Theory.
- Alternative approach to cryptography:
  - Exploit the **noisy channel** for secrecy (no shared key).

Physical Layer Security

- Rooted in Information Theory.
- Alternative approach to cryptography:
  - Exploit the **noisy channel** for secrecy (no shared key).
  - **Computationally unlimited** eavesdroppers.

Physical Layer Security

- Rooted in Information Theory.
- Alternative approach to cryptography:
  - Exploit the **noisy channel** for secrecy (no shared key).
  - **Computationally unlimited** eavesdroppers.
- Appropriate for securing **low complexity** devices such as IoT.

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:** $$\begin{aligned} I(X;Y) &= H(X) - H(X|Y) \\ &= H(Y) - H(Y|X). \end{aligned}$$

Physical Layer Communication - IT Perspective

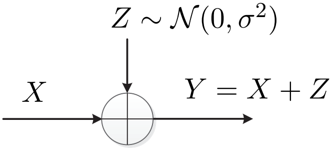
- A mathematical model for a physical communication channel.

Physical Layer Communication - IT Perspective

- A mathematical model for a physical communication channel.
- **Channel Examples:**

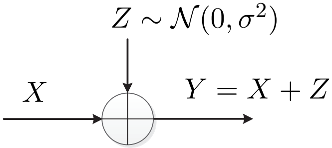
Physical Layer Communication - IT Perspective

- A mathematical model for a physical communication channel.
- **Channel Examples:**
  - **Gaussian Channel:**

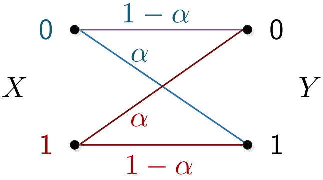


Physical Layer Communication - IT Perspective

- A mathematical model for a physical communication channel.
- **Channel Examples:**
  - **Gaussian Channel:**

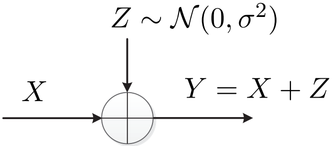


  - **Binary Symmetric Channel:**

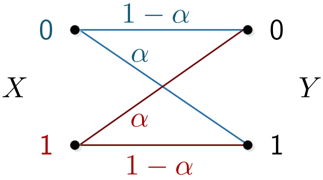


Physical Layer Communication - IT Perspective

- A mathematical model for a physical communication channel.
- **Channel Examples:**
  - **Gaussian Channel:**



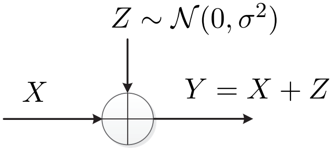
  - **Binary Symmetric Channel:**



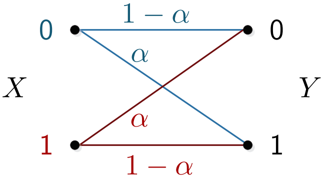
- **Questions we ask:**

Physical Layer Communication - IT Perspective

- A mathematical model for a physical communication channel.
- **Channel Examples:**
  - **Gaussian Channel:**



  - **Binary Symmetric Channel:**



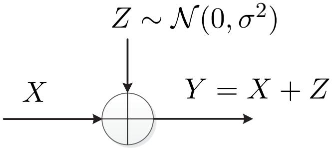
- **Questions we ask:**
  - What is the **maximal** rate [bits/ch. use] of **reliable** communication?

Physical Layer Communication - IT Perspective

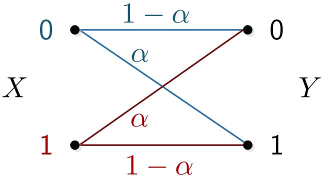
- A mathematical model for a physical communication channel.

- **Channel Examples:**

  - **Gaussian Channel:**



  - **Binary Symmetric Channel:**

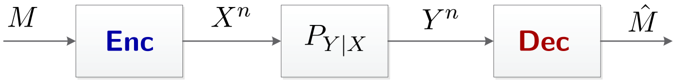


- **Questions we ask:**

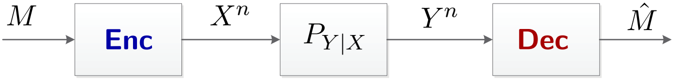
  - What is the **maximal** rate [bits/ch. use] of **reliable** communication?

  - How to design codes at that rate?

Physical Layer Communication - Formal Definition

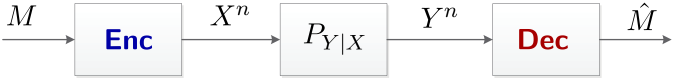


Physical Layer Communication - Formal Definition



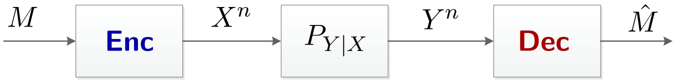
- **Message**: nR information bits.

Physical Layer Communication - Formal Definition



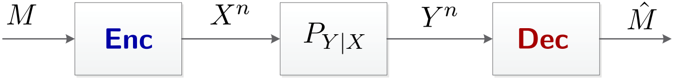
- **Message**: nR information bits.
- $(\boldsymbol{n}, \boldsymbol{R})$**-Code:** Block **Encoding** and **Decoding** functions.

Physical Layer Communication - Formal Definition



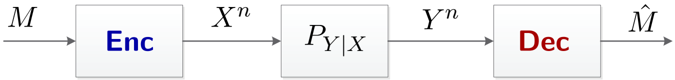
- **Message**: nR information bits.
- **(n, R)-Code:** Block **Encoding** and **Decoding** functions.
- **Channel:** $\mathbb{P}\big(Y^n = y^n \big| X^n = x^n\big) = \prod_{i=1}^{n} P_{Y|X}(y_i|x_i)$.

Physical Layer Communication - Formal Definition



- **Message**: nR information bits.
- **(n, R)-Code:** Block **Encoding** and **Decoding** functions.
- **Channel:** $\mathbb{P}\big(Y^n = y^n \big| X^n = x^n\big) = \prod_{i=1}^{n} P_{Y|X}(y_i|x_i)$.
- **Capacity:** $\mathsf{C} \triangleq \sup\Big\{R \Big| \exists (n,R) - \text{codes s.t. } \mathbb{P}\big(M \neq \hat{M}\big) \underset{n}{\rightarrow} 0\Big\}$.

Physical Layer Communication - Formal Definition



- **Message**: nR information bits.
- **(n,R)-Code:** Block **Encoding** and **Decoding** functions.
- **Channel:** $\mathbb{P}\big(Y^n = y^n \big| X^n = x^n\big) = \prod_{i=1}^{n} P_{Y|X}(y_i|x_i)$.
- **Capacity:** $\mathsf{C} \triangleq \sup\left\{R \middle| \exists (n,R) - \text{codes s.t. } \mathbb{P}\big(M \neq \hat{M}\big) \underset{n}{\to} 0\right\}$.

Theorem (Shannon 1948)

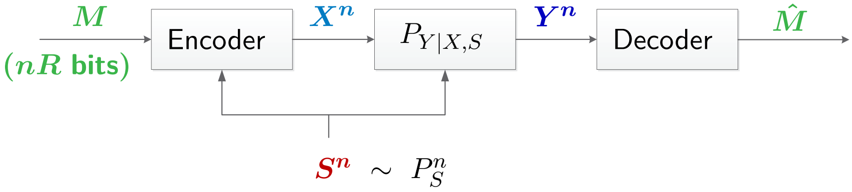
The capacity of a channel $P_{Y|X}$ is $\mathsf{C} = \max_{P_X} I(X;Y)$.

Reminder: $I(X;Y) = H(Y) - H(Y|X)$

State-Dependent Wiretap Channels

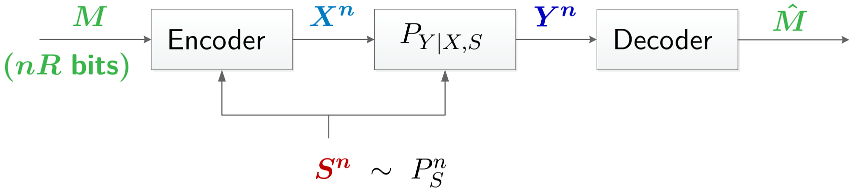
State-Dependent Channels

[Gelfand-Pinsker 1980]



State-Dependent Channels

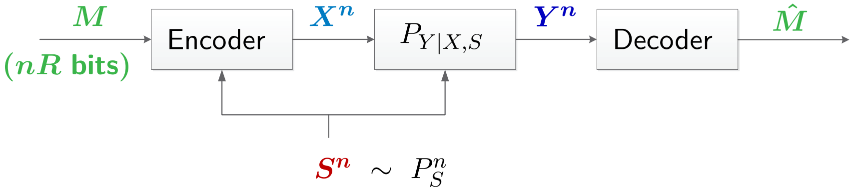
[Gelfand-Pinsker 1980]



State-Dependent Channel:

State-Dependent Channels

[Gelfand-Pinsker 1980]

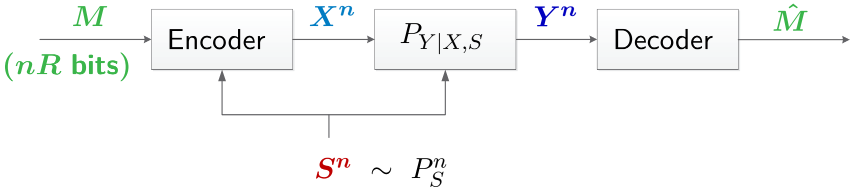


State-Dependent Channel:

- **State:** $S \sim \text{Bernoulli}\left(\frac{1}{2}\right)$, $\mathcal{S} = \{0, 1\}$.

State-Dependent Channels

[Gelfand-Pinsker 1980]

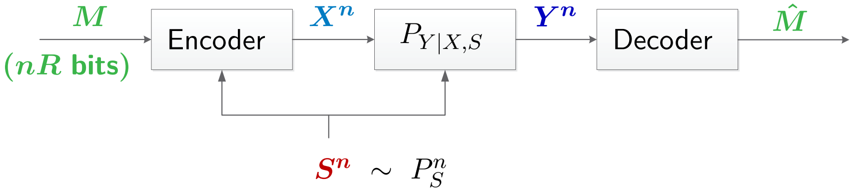


State-Dependent Channel:

- **State:** $S \sim \text{Bernoulli}\left(\frac{1}{2}\right)$, $\mathcal{S} = \{0, 1\}$.
- **AGN Channel:** $Y = X + Z_S$

State-Dependent Channels

[Gelfand-Pinsker 1980]



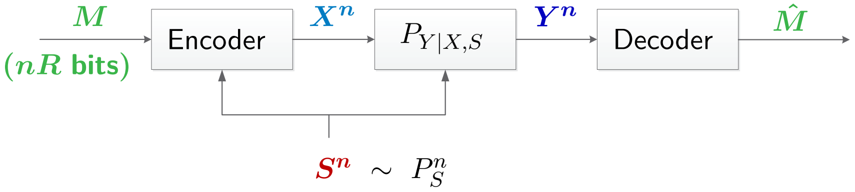
State-Dependent Channel:

- **State:** $S \sim$ Bernoulli $\left(\frac{1}{2}\right)$, $\mathcal{S} = \{0, 1\}$.
- **AGN Channel:** $Y = X + Z_S$

$$Z_0 \sim \mathcal{N}(0, \sigma_0^2), \quad Z_1 \sim \mathcal{N}(0, \sigma_1^2), \quad \sigma_0 \ll \sigma_1.$$

State-Dependent Channels

[Gelfand-Pinsker 1980]



State-Dependent Channel:

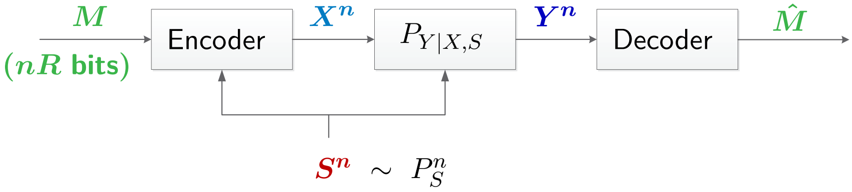
- **State:** $S \sim$ Bernoulli $\left(\frac{1}{2}\right)$, $\mathcal{S} = \{0, 1\}$.
- **AGN Channel:** $Y = X + Z_S$

$$Z_0 \sim \mathcal{N}(0, \sigma_0^2), \quad Z_1 \sim \mathcal{N}(0, \sigma_1^2), \quad \sigma_0 \ll \sigma_1.$$

Time t	1	2	3	4	5	6	...
State S_t							
SNR at time t							

State-Dependent Channels

[Gelfand-Pinsker 1980]



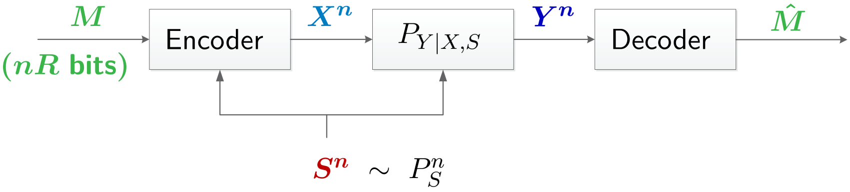
State-Dependent Channel:

- **State:** $S \sim$ Bernoulli $\left(\frac{1}{2}\right)$, $\mathcal{S} = \{0, 1\}$.
- **AGN Channel:** $Y = X + Z_S$

$$Z_0 \sim \mathcal{N}(0, \sigma_0^2), \quad Z_1 \sim \mathcal{N}(0, \sigma_1^2), \quad \sigma_0 \ll \sigma_1.$$

Time t	1	2	3	4	5	6	...
State S_t	1	1	0	1	0	0	...
SNR at time t							

State-Dependent Channels
[Gelfand-Pinsker 1980]



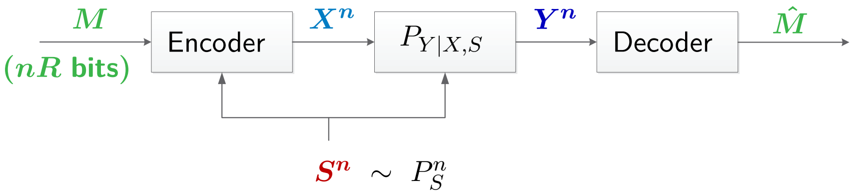
State-Dependent Channel:

- **State:** $S \sim$ Bernoulli $\left(\frac{1}{2}\right)$, $\mathcal{S} = \{0, 1\}$.
- **AGN Channel:** $Y = X + Z_S$

$$Z_0 \sim \mathcal{N}(0, \sigma_0^2), \quad Z_1 \sim \mathcal{N}(0, \sigma_1^2), \quad \sigma_0 \ll \sigma_1.$$

Time t	1	2	3	4	5	6	...
State S_t	1	1	0	1	0	0	...
SNR at time t	Low						

State-Dependent Channels
[Gelfand-Pinsker 1980]



State-Dependent Channel:

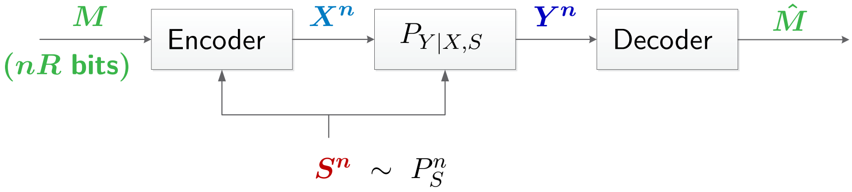
- **State:** $S \sim$ Bernoulli $\left(\frac{1}{2}\right)$, $\mathcal{S} = \{0, 1\}$.
- **AGN Channel:** $Y = X + Z_S$

$$Z_0 \sim \mathcal{N}(0, \sigma_0^2), \quad Z_1 \sim \mathcal{N}(0, \sigma_1^2), \quad \sigma_0 \ll \sigma_1.$$

Time t	1	2	3	4	5	6	...
State S_t	1	1	0	1	0	0	...
SNR at time t	Low	Low					

State-Dependent Channels

[Gelfand-Pinsker 1980]



State-Dependent Channel:

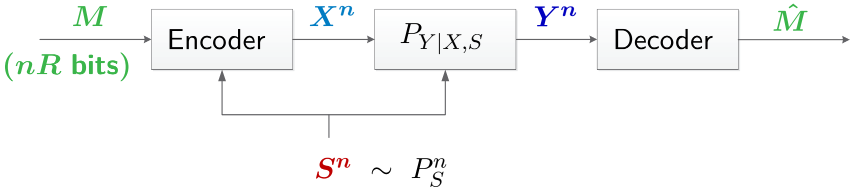
- **State:** $S \sim$ Bernoulli $\left(\frac{1}{2}\right)$, $\mathcal{S} = \{0, 1\}$.
- **AGN Channel:** $Y = X + Z_S$

$$Z_0 \sim \mathcal{N}(0, \sigma_0^2), \quad Z_1 \sim \mathcal{N}(0, \sigma_1^2), \quad \sigma_0 \ll \sigma_1.$$

Time t	1	2	3	4	5	6	...
State S_t	1	1	0	1	0	0	...
SNR at time t	Low	Low	High				

State-Dependent Channels

[Gelfand-Pinsker 1980]



State-Dependent Channel:

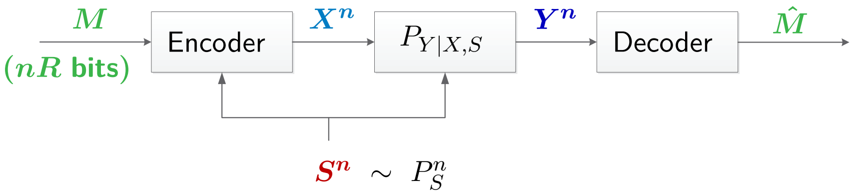
- **State:** $S \sim$ Bernoulli $\left(\frac{1}{2}\right)$, $\mathcal{S} = \{0, 1\}$.
- **AGN Channel:** $Y = X + Z_S$

$$Z_0 \sim \mathcal{N}(0, \sigma_0^2), \quad Z_1 \sim \mathcal{N}(0, \sigma_1^2), \quad \sigma_0 \ll \sigma_1.$$

Time t	1	2	3	4	5	6	...
State S_t	1	1	0	1	0	0	...
SNR at time t	Low	Low	High	Low			

State-Dependent Channels

[Gelfand-Pinsker 1980]



State-Dependent Channel:

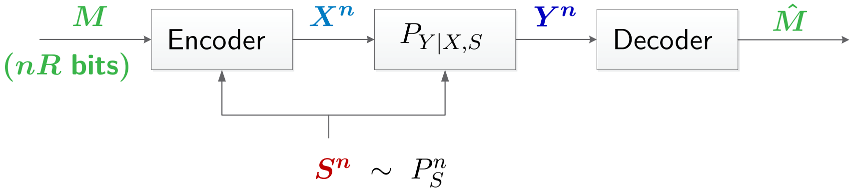
- **State:** $S \sim$ Bernoulli $\left(\frac{1}{2}\right)$, $\mathcal{S} = \{0,1\}$.
- **AGN Channel:** $Y = X + Z_S$

$$Z_0 \sim \mathcal{N}(0, \sigma_0^2), \quad Z_1 \sim \mathcal{N}(0, \sigma_1^2), \quad \sigma_0 \ll \sigma_1.$$

Time t	1	2	3	4	5	6	...
State S_t	1	1	0	1	0	0	...
SNR at time t	Low	Low	High	Low	High		

State-Dependent Channels

[Gelfand-Pinsker 1980]



State-Dependent Channel:

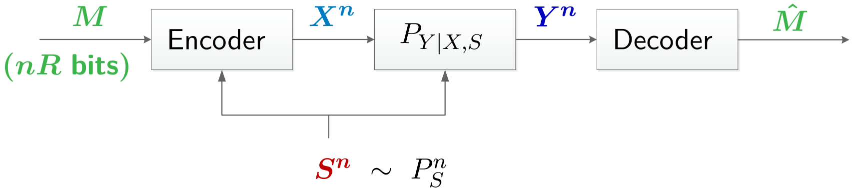
- **State:** $S \sim$ Bernoulli $\left(\frac{1}{2}\right)$, $\mathcal{S} = \{0, 1\}$.
- **AGN Channel:** $Y = X + Z_S$

$$Z_0 \sim \mathcal{N}(0, \sigma_0^2), \quad Z_1 \sim \mathcal{N}(0, \sigma_1^2), \quad \sigma_0 \ll \sigma_1.$$

Time t	1	2	3	4	5	6	...
State S_t	1	1	0	1	0	0	...
SNR at time t	Low	Low	High	Low	High	High	...

State-Dependent Channels

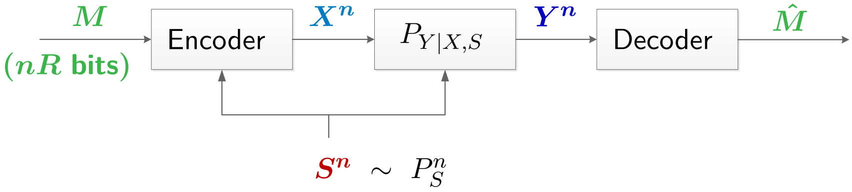
[Gelfand-Pinsker 1980]



- Encoder knows the state sequence non-causally.

State-Dependent Channels

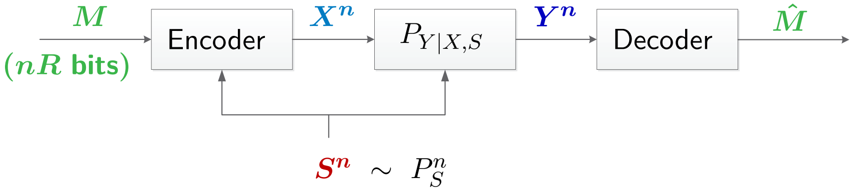
[Gelfand-Pinsker 1980]



- Encoder knows the state sequence non-causally.
- Enhance communication rates via coherent transmission.

State-Dependent Channels

[Gelfand-Pinsker 1980]



- Encoder knows the state sequence non-causally.
- Enhance communication rates via coherent transmission.

Theorem (Gelfand-Pinsker 1980)

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

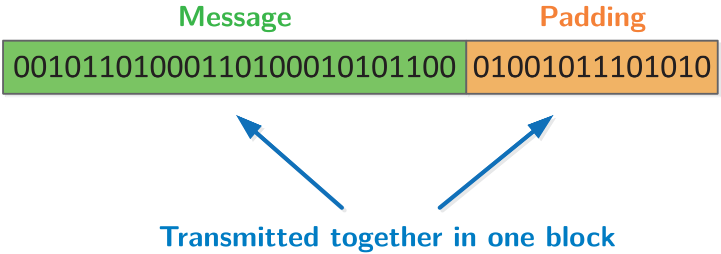
Joint distribution: $P_{U,X|S} P_{Y|X,S}$

The Gelfand-Pinsker Channel - Encoding

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

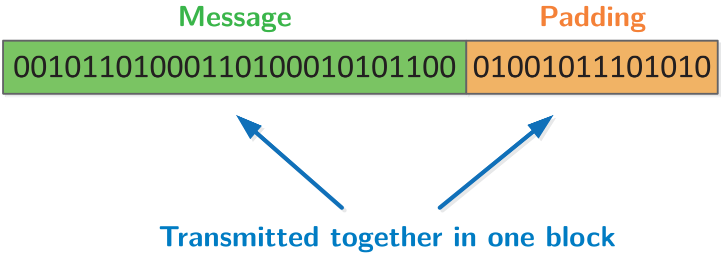
The Gelfand-Pinsker Channel - Encoding

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



The Gelfand-Pinsker Channel - Encoding

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



- **Codebook:** $(\text{Message}, \text{Padding}) \longrightarrow$ Codeword U^n.

The Gelfand-Pinsker Channel - Encoding

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

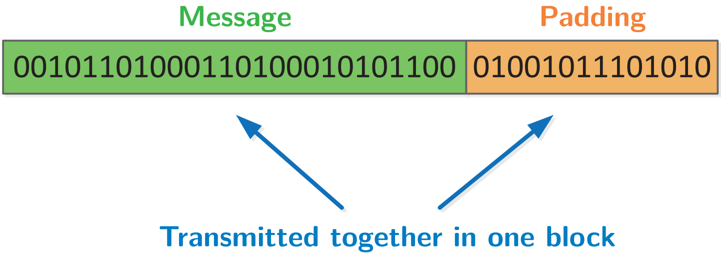
Message	Padding
00101101000110100010101100	01001011101010

Transmitted together in one block

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

The Gelfand-Pinsker Channel - Encoding

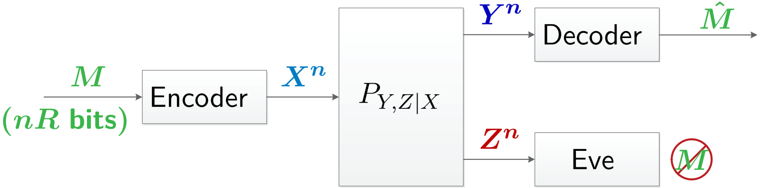
- Pad nR **message bits** with $n\tilde{R}$ **redundancy bits**.



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

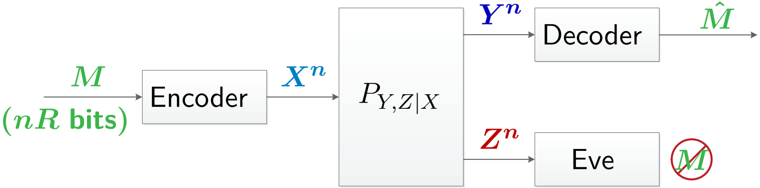
Wiretap Channels

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



Wiretap Channels

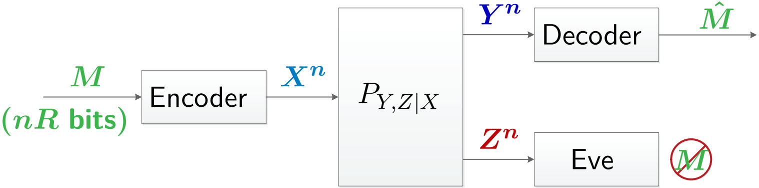
Degraded [Wyner 1975], General [Csiszár-Körner 1978]



Secrecy-Capacity:

Wiretap Channels

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

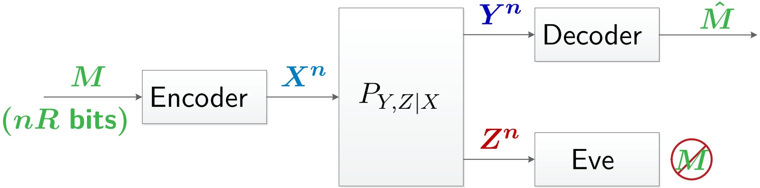


Secrecy-Capacity:

- Reliable Communication.

Wiretap Channels

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

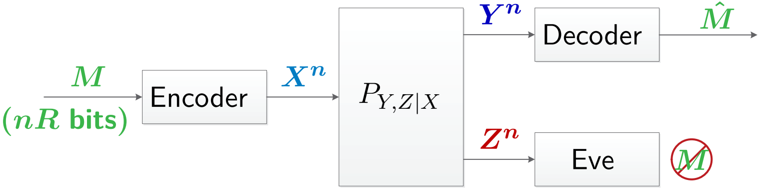


Secrecy-Capacity:

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

Wiretap Channels

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



Secrecy-Capacity:

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

Theorem (Csiszár-Körner 1978)

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

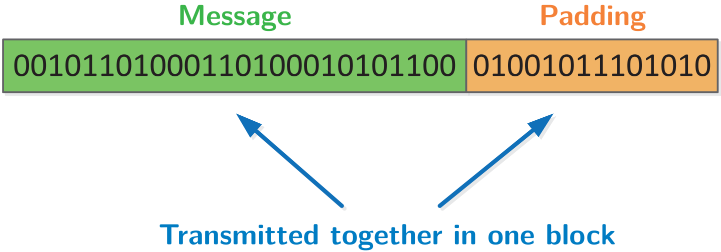
Joint distribution: $P_{U,X} P_{Y,Z|X}$

Wiretap Channels - Encoding

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

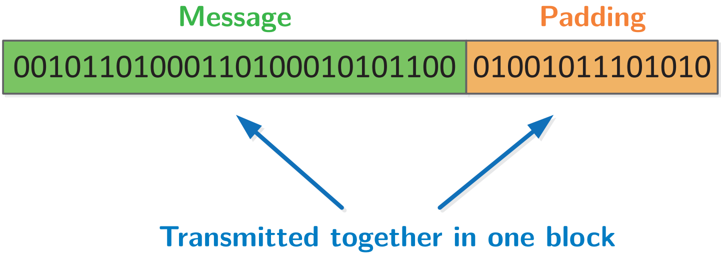
Wiretap Channels - Encoding

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



Wiretap Channels - Encoding

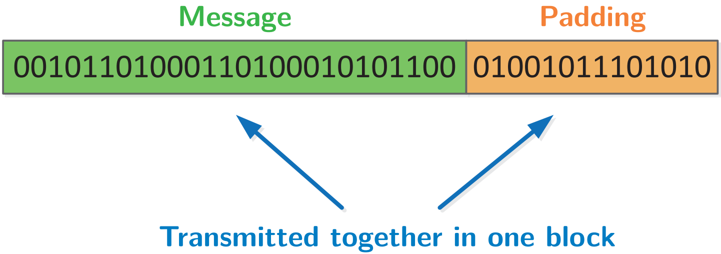
- Pad nR **message bits** with $n\tilde{R}$ **redundancy bits**.



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

Wiretap Channels - Encoding

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



- **Codebook:** (**Message**, **Padding**) $\rightarrow$ Codeword U^n.
- **Security:** $\tilde{R} > I(U;Z)$.

Wiretap Channels - Encoding

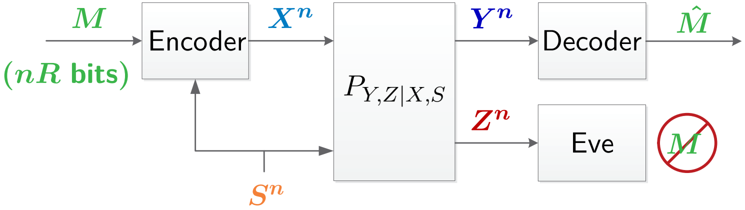
- Pad nR **message bits** with $n\tilde{R}$ **redundancy bits**.

Message	Padding
00101101000110100010101100	01001011101010

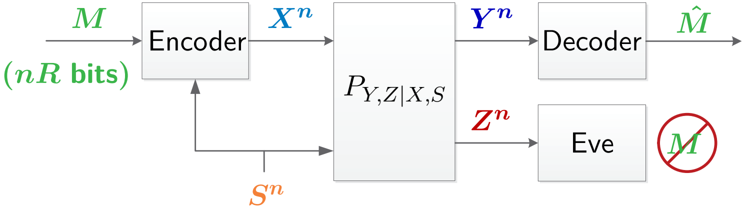
Transmitted together in one block

- **Codebook:** (**Message**, **Padding**) $\rightarrow$ Codeword U^n.
- **Security:** $\tilde{R} > I(U;Z)$.
- **Reliability:** $R + \tilde{R} < I(U;Y)$.

The Gelfand-Pinsker Wiretap Channel

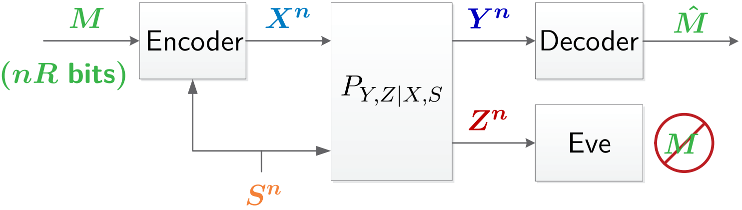


The Gelfand-Pinsker Wiretap Channel



Secrecy Capacity: Reliable and Secure Communication.

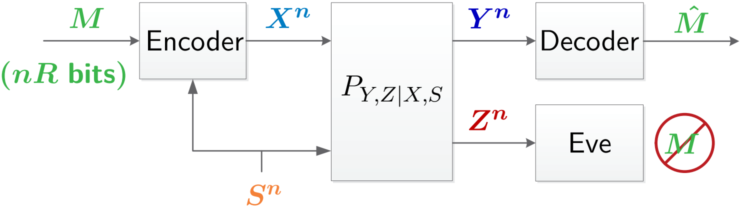
The Gelfand-Pinsker Wiretap Channel



Secrecy Capacity: Reliable and Secure Communication.

Tension: Utilize state knowledge to simultaneously

The Gelfand-Pinsker Wiretap Channel

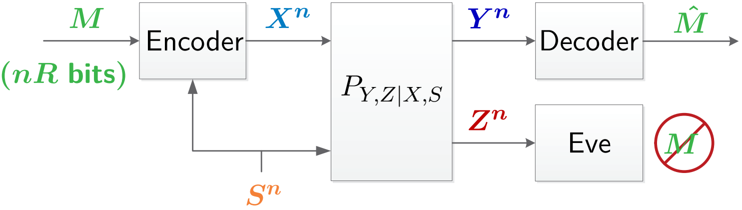


Secrecy Capacity: Reliable and Secure Communication.

Tension: Utilize state knowledge to simultaneously

- Enhance **reliable** communication rate (coherent transmission).

The Gelfand-Pinsker Wiretap Channel

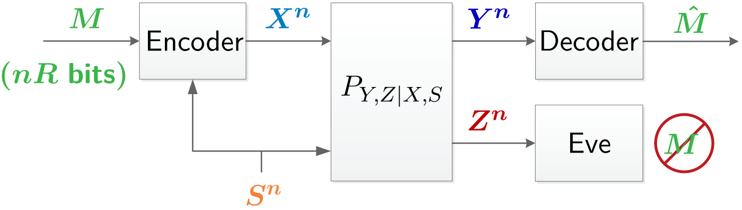


Secrecy Capacity: Reliable and Secure Communication.

Tension: Utilize state knowledge to simultaneously

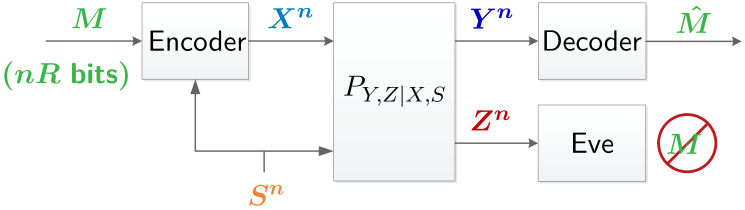
- Enhance **reliable** communication rate (coherent transmission).
- Boost **security** performance (e.g., via secret key agreement).

The Gelfand-Pinsker Wiretap Channel



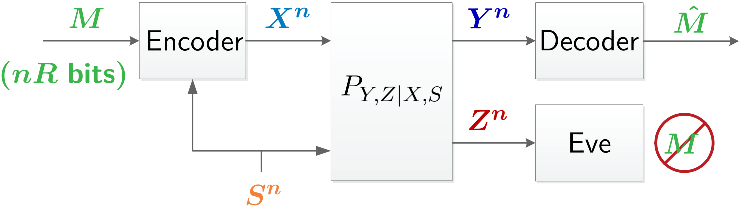
Naive Approach:

The Gelfand-Pinsker Wiretap Channel



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

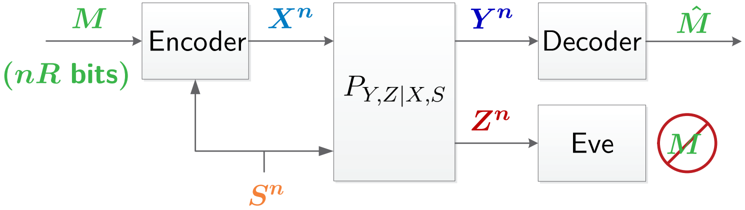
The Gelfand-Pinsker Wiretap Channel



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

00101101000110100010101100	01001011101010

The Gelfand-Pinsker Wiretap Channel



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

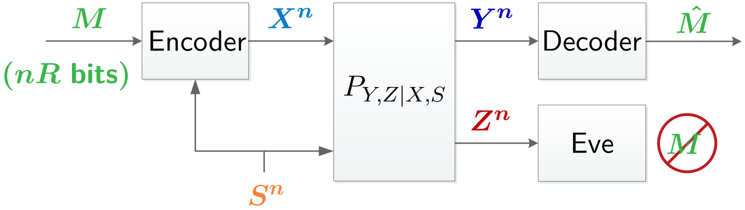
001011010001101000101011000 | 01001011101010

Theorem (Chen-Han Vinck 2006)

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

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

The Gelfand-Pinsker Wiretap Channel



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

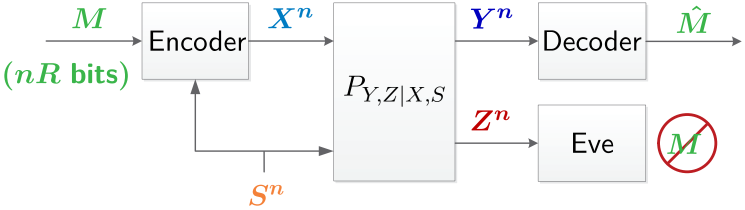
Theorem (Chen-Han Vinck 2006)

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

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

★ Always preforms **wiretap coding**

The Gelfand-Pinsker Wiretap Channel



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

0010110100011010001010l100	01001011101010

Theorem (Chen-Han Vinck 2006)

$$C_{\text{GP-WTC}} \geq \max_{P_{U,X|S}} \left[I(U;Y) - \max\left\{ \boldsymbol{I(U;Z)}, \boldsymbol{I(U;S)} \right\} \right]$$

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

★ Always preforms **wiretap coding** $\Longrightarrow$ Suboptimal vs. **strong Eve**

Improved Two-Layered Coding Scheme

Theorem (ZG-Cuff-Permuter 2016)

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

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

Improved Two-Layered Coding Scheme

Theorem (ZG-Cuff-Permuter 2016)

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

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

Two-Layered Coding Scheme (Superposition Code):

Improved Two-Layered Coding Scheme

Theorem (ZG-Cuff-Permuter 2016)

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

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

Two-Layered Coding Scheme (Superposition Code):

- **Inner Layer:** No wiretap coding - Supports key-agreement strategies.

Improved Two-Layered Coding Scheme

Theorem (ZG-Cuff-Permuter 2016)

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

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

Two-Layered Coding Scheme (Superposition Code):

- **Inner Layer:** No wiretap coding - Supports key-agreement strategies.
- **Outer Layer:** Wiretap coding (when channel favors legit users).

Improved Two-Layered Coding Scheme

Theorem (ZG-Cuff-Permuter 2016)

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

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

Two-Layered Coding Scheme (Superposition Code):

- **Inner Layer:** No wiretap coding - Supports key-agreement strategies.
- **Outer Layer:** Wiretap coding (when channel favors legit users).

Generalization: Captures all past results as special cases.

Improved Two-Layered Coding Scheme

Theorem (ZG-Cuff-Permuter 2016)

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

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

Two-Layered Coding Scheme (Superposition Code):

- **Inner Layer:** No wiretap coding - Supports key-agreement strategies.
- **Outer Layer:** Wiretap coding (when channel favors legit users).

Generalization: Captures all past results as special cases.

Strict Improvement: Explicit example & Analytic derivation.

Summary

- **The Gelfand-Pinsker wiretap channel**

Summary

- **The Gelfand-Pinsker wiretap channel**
  - Combination of two fundamental IT setups.

Summary

- **The Gelfand-Pinsker wiretap channel**
  - Combination of two fundamental IT setups.
  - Simultaneously exploit state for reliability and security.

Summary

- **The Gelfand-Pinsker wiretap channel**
  - Combination of two fundamental IT setups.
  - Simultaneously exploit state for reliability and security.

- **Novel superposition coding scheme**

Summary

- **The Gelfand-Pinsker wiretap channel**
  - Combination of two fundamental IT setups.
  - Simultaneously exploit state for reliability and security.

- **Novel superposition coding scheme**
  - Recovers all past results.

Summary

- **The Gelfand-Pinsker wiretap channel**
  - Combination of two fundamental IT setups.
  - Simultaneously exploit state for reliability and security.

- **Novel superposition coding scheme**
  - Recovers all past results.
  - Strictly outperforms previous benchmark.

Summary

- **The Gelfand-Pinsker wiretap channel**
  - Combination of two fundamental IT setups.
  - Simultaneously exploit state for reliability and security.
- **Novel superposition coding scheme**
  - Recovers all past results.
  - Strictly outperforms previous benchmark.
- **Available on ArXiV**: `https://arxiv.org/abs/1608.00743v1`.

Summary

- **The Gelfand-Pinsker wiretap channel**
  - Combination of two fundamental IT setups.
  - Simultaneously exploit state for reliability and security.

- **Novel superposition coding scheme**
  - Recovers all past results.
  - Strictly outperforms previous benchmark.

- **Available on ArXiV**: `https://arxiv.org/abs/1608.00743v1`.

Thank you!