The Gelfand-Pinsker Wiretap Channel: Higher Secrecy Rates via a Novel Superposition Code

Ziv Goldfeld, Paul Cuff and Haim Permuter

Ben Gurion University and Princeton University

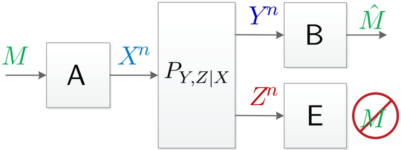
The 2017 IEEE International Symposium on Information Theory
Aachen

June 29th, 2017

The Wiretap Channel & The GP Channel

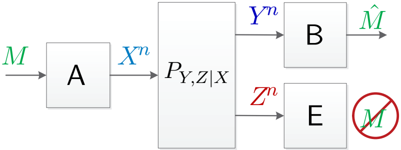
The Wiretap Channel & The GP Channel

The Wiretap Channel



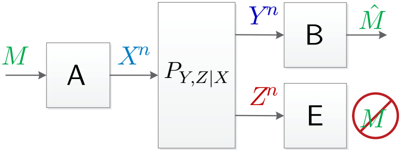
The Wiretap Channel & The GP Channel

The Wiretap Channel



- Reliable & Secure Commun.

The Wiretap Channel



- Reliable & Secure Commun.

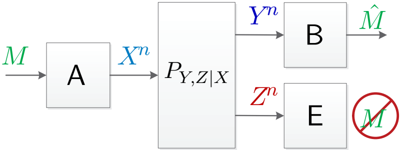
Theorem (Csiszár-Körner 1978)

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

(Joint dist. $P_{U,X}P_{Y,Z|X}$*)*

The Wiretap Channel & The GP Channel

The Wiretap Channel



- Reliable & Secure Commun.

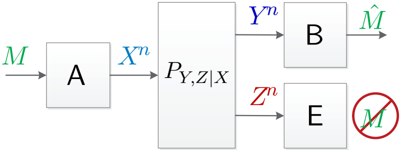
Theorem (Csiszár-Körner 1978)

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

(Joint dist. $P_{U,X} P_{Y,Z|X}$)

The Wiretap Channel & The GP Channel

The Wiretap Channel



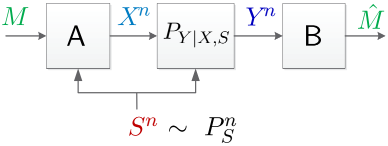
- Reliable & Secure Commun.

Theorem (Csiszár-Körner 1978)

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

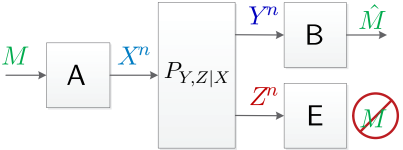
(Joint dist. $P_{U,X} P_{Y,Z|X}$*)*

The Gelfand-Pinsker Channel



The Wiretap Channel & The GP Channel

The Wiretap Channel



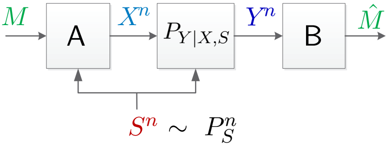
- Reliable & Secure Commun.

Theorem (Csiszár-Körner 1978)

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

(Joint dist. $P_{U,X}P_{Y,Z|X}$)

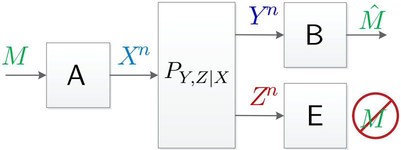
The Gelfand-Pinsker Channel



- Reliable Communication.

The Wiretap Channel & The GP Channel

The Wiretap Channel



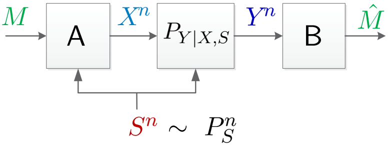
- Reliable & Secure Commun.

Theorem (Csiszár-Körner 1978)

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

(Joint dist. $P_{U,X} P_{Y,Z|X}$*)*

The Gelfand-Pinsker Channel



- Reliable Communication.

Theorem (Gelfand-Pinsker 1980)

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

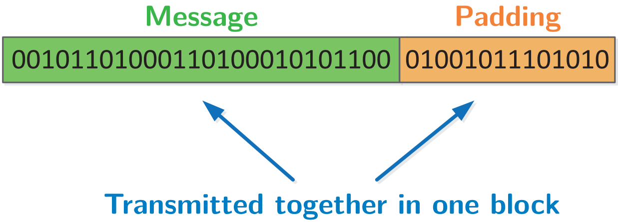
(Joint dist. $P_{U,X|S} P_{Y|X,S}$*)*

Reminiscent Optimal Coding Schemes

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

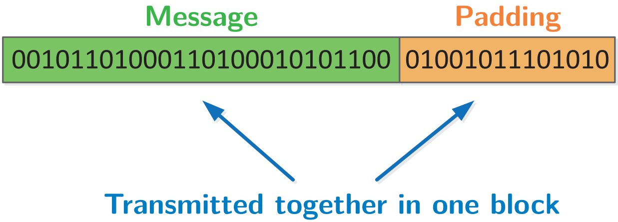
Reminiscent Optimal Coding Schemes

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



Reminiscent Optimal Coding Schemes

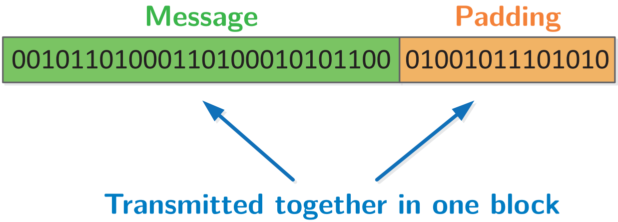
- Pad nR **message bits** with $n\tilde{R}$ **redundancy bits**.



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

Reminiscent Optimal Coding Schemes

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



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

Reminiscent Optimal Coding Schemes

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

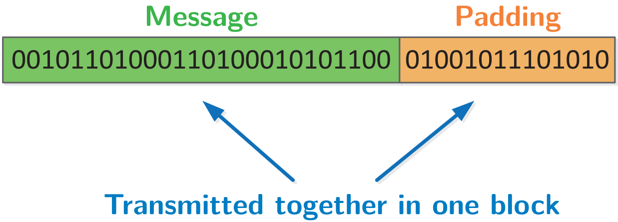
Message	Padding
00101101000110100010101100	01001011101010

Transmitted together in one block

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

Reminiscent Optimal Coding Schemes

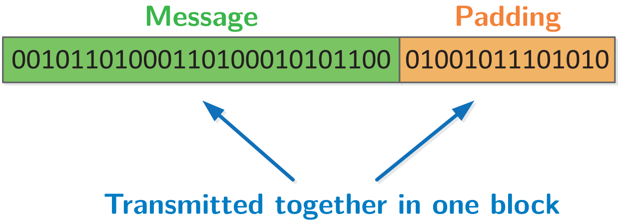
- Pad nR **message bits** with $n\tilde{R}$ **redundancy bits**.



- **Random Codebook:** (**Message**, **Padding**) $\rightarrow$ $U^n \sim P_U^n$
- **Padding:**
  - **WTC - Security:** $\tilde{R} > I(U;Z)$
  - **GP Channel - Correlation:** $\tilde{R} > I(U;S)$

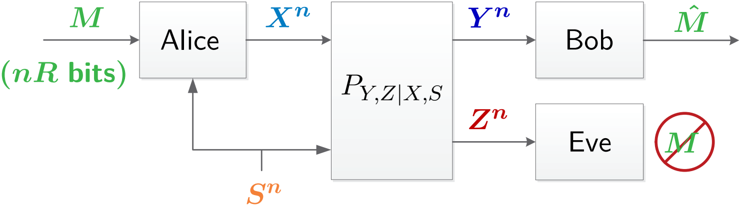
Reminiscent Optimal Coding Schemes

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

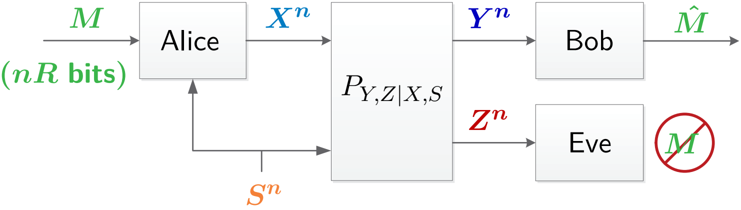


- **Random Codebook:** (Message, Padding) $\rightarrow \quad U^n \sim P_U^n$
- **Padding:**
  - **WTC - Security:** $\tilde{R} > I(U;Z)$
  - **GP Channel - Correlation:** $\tilde{R} > I(U;S)$
- **Reliability:** $R + \tilde{R} < I(U;Y)$.

The Gelfand-Pinsker Wiretap Channel

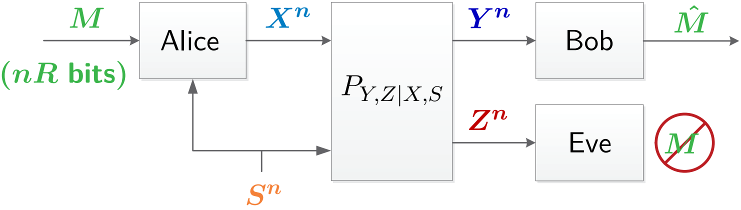


The Gelfand-Pinsker Wiretap Channel



Secrecy Capacity: Reliable and Secure Communication.

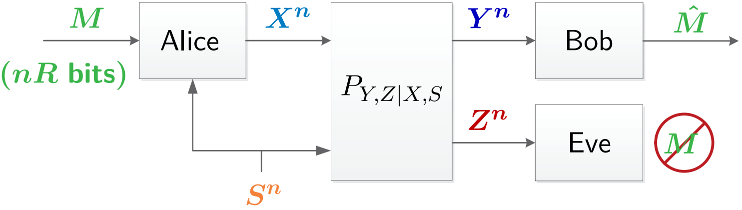
The Gelfand-Pinsker Wiretap Channel



Secrecy Capacity: Reliable and Secure Communication.

Naive Approach:

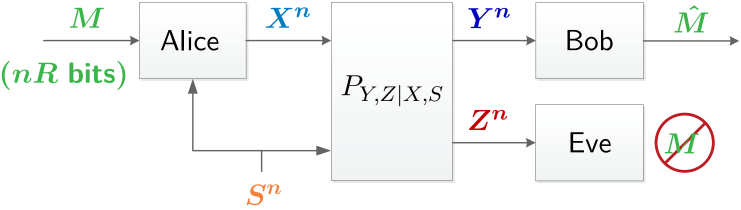
The Gelfand-Pinsker Wiretap Channel



Secrecy Capacity: Reliable and Secure Communication.

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

The Gelfand-Pinsker Wiretap Channel



Secrecy Capacity: Reliable and Secure Communication.

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 $P_S P_{U,X|S} P_{Y,Z|X,S}$)

Suboptimality of Naive Approach

Key Extraction Scheme [Chia-El Gamal 2012]

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

Suboptimality of Naive Approach

Key Extraction Scheme [Chia-El Gamal 2012]

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

Suboptimality of Naive Approach

Key Extraction Scheme [Chia-El Gamal 2012]

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

Why and When?

Suboptimality of Naive Approach

Key Extraction Scheme [Chia-El Gamal 2012]

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

Why and When?

- Chen-Han Vinck scheme **always** preforms wiretap coding.

Suboptimality of Naive Approach

Key Extraction Scheme [Chia-El Gamal 2012]

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

Why and When?

- Chen-Han Vinck scheme **always** preforms wiretap coding.
- Strong **Eavesdropper**

Suboptimality of Naive Approach

Key Extraction Scheme [Chia-El Gamal 2012]

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

Why and When?

- Chen-Han Vinck scheme **always** preforms wiretap coding.
- Strong **Eavesdropper** $\implies$ Wiretap coding is useless

Suboptimality of Naive Approach

Key Extraction Scheme [Chia-El Gamal 2012]

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

Why and When?

- Chen-Han Vinck scheme **always** preforms wiretap coding.
- Strong **Eavesdropper** $\Longrightarrow$ Wiretap coding is useless

A Simple Alternative:

Suboptimality of Naive Approach

Key Extraction Scheme [Chia-El Gamal 2012]

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

Why and When?

- Chen-Han Vinck scheme **always** preforms wiretap coding.
- Strong **Eavesdropper** $\implies$ Wiretap coding is useless

A Simple Alternative:

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

Suboptimality of Naive Approach

Key Extraction Scheme [Chia-El Gamal 2012]

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

Why and When?

- Chen-Han Vinck scheme **always** preforms wiretap coding.
- Strong **Eavesdropper** $\implies$ Wiretap coding is useless

A Simple Alternative: S^n is known to Receiver $\boldsymbol{Y} = (\boldsymbol{Y}, \boldsymbol{S})$

1. Extract secret random bits from S^n.

Suboptimality of Naive Approach

Key Extraction Scheme [Chia-El Gamal 2012]

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

Why and When?

- Chen-Han Vinck scheme **always** preforms wiretap coding.
- Strong **Eavesdropper** $\implies$ Wiretap coding is useless

A Simple Alternative: S^n is known to Receiver $\boldsymbol{Y} = (\boldsymbol{Y}, S)$

1. Extract secret random bits from S^n.
2. One-time pad the message M.

Suboptimality of Naive Approach

Key Extraction Scheme [Chia-El Gamal 2012]

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

Why and When?

- Chen-Han Vinck scheme **always** preforms wiretap coding.
- Strong **Eavesdropper** $\implies$ Wiretap coding is useless

A Simple Alternative: S^n is known to Receiver $\boldsymbol{Y} = (\boldsymbol{Y}, S)$

1. Extract secret random bits from S^n.
2. One-time pad the message M.
3. Point-to-point transmission (ignore **Eve**).

Suboptimality of Naive Approach

Key Extraction Scheme [Chia-El Gamal 2012]

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

Why and When?

- Chen-Han Vinck scheme **always** preforms wiretap coding.
- Strong **Eavesdropper** $\implies$ Wiretap coding is useless

A Simple Alternative: S^n is known to Receiver $\boldsymbol{Y} = (\boldsymbol{Y}, S)$

1. Extract secret random bits from S^n.
2. One-time pad the message M.
3. Point-to-point transmission (ignore **Eve**).

$\implies$ **Achieves:** $\boxed{\max_{P_{U,X|S}} \min\Big\{H(S|U,Z), I(U;Y|S)\Big\}}$

Suboptimality of Naive Approach

Key Extraction Scheme [Chia-El Gamal 2012]

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

Why and When?

- Chen-Han Vinck scheme **always** preforms wiretap coding.
- Strong **Eavesdropper** $\Longrightarrow$ Wiretap coding is useless

A Simple Alternative: S^n is known to Receiver $\boldsymbol{Y} = (\boldsymbol{Y}, S)$

1. Extract secret random bits from S^n.
2. One-time pad the message M.
3. Point-to-point transmission (ignore **Eve**).

$\Longrightarrow$ **Achieves:** $\boxed{\max_{P_{U,X|S}} \min\Big\{H(S|U,Z), I(U;Y|S)\Big\}}$

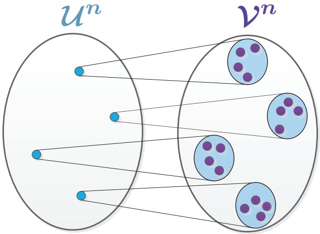
Can strictly outperform previous scheme!

Superposition Coding for the GP Wiretap Channel

Main Ideas:

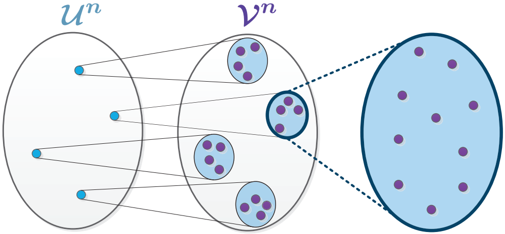
Superposition Coding for the GP Wiretap Channel

Main Ideas:



Superposition Coding for the GP Wiretap Channel

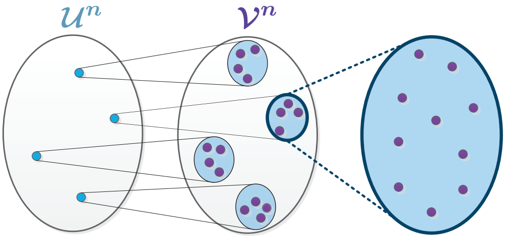
Main Ideas:



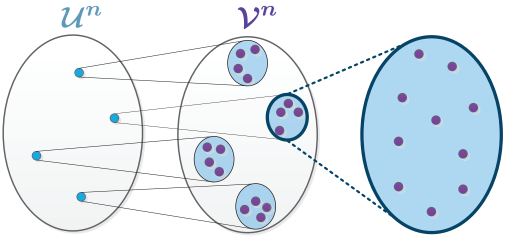
Superposition Coding for the GP Wiretap Channel

Main Ideas:

- U^n better seen by **Eve** (no **inner layer** wiretap coding).



Superposition Coding for the GP Wiretap Channel



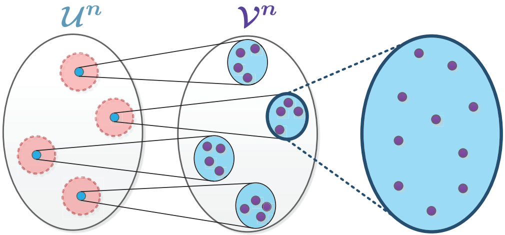
Main Ideas:

- U^n better seen by **Eve**
  (no **inner layer** wiretap coding).

Superposition Coding for the GP Wiretap Channel

Main Ideas:

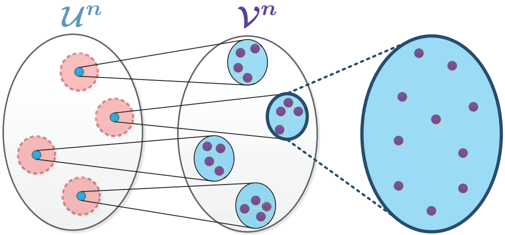
- U^n better seen by **Eve**
  (no **inner layer** wiretap coding).



Superposition Coding for the GP Wiretap Channel

Main Ideas:

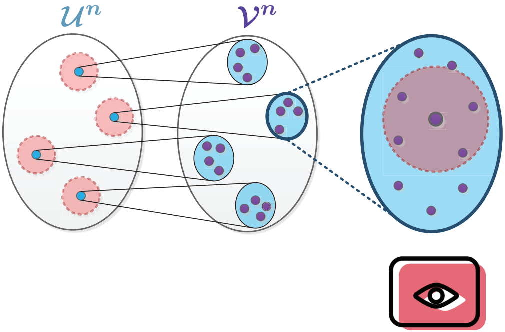
- U^n better seen by **Eve** (no **inner layer** wiretap coding).
- Advantage to legitimate users in **outer layer**.



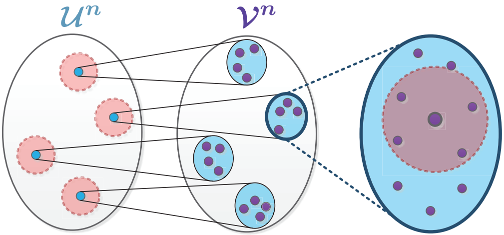
Superposition Coding for the GP Wiretap Channel

Main Ideas:

- U^n better seen by **Eve** (no **inner layer** wiretap coding).
- Advantage to legitimate users in **outer layer**.



Superposition Coding for the GP Wiretap Channel

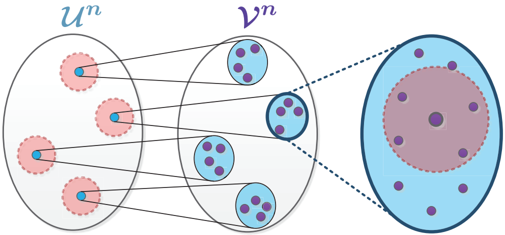


Main Ideas:

- U^n better seen by **Eve** (no **inner layer** wiretap coding).
- Advantage to legitimate users in **outer layer**.

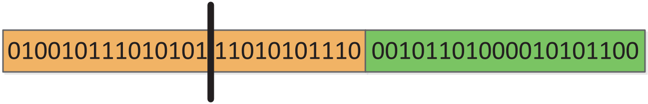
010010111010101 11010101110 00101101000010101100

Superposition Coding for the GP Wiretap Channel

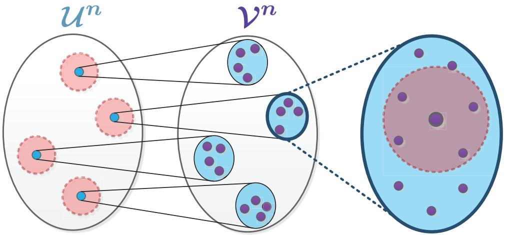


Main Ideas:

- U^n better seen by **Eve** (no **inner layer** wiretap coding).
- Advantage to legitimate users in **outer layer**.

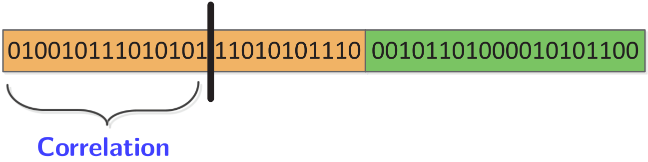


Superposition Coding for the GP Wiretap Channel

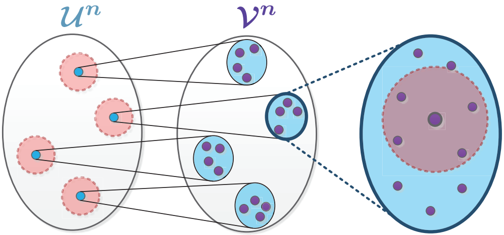


Main Ideas:

- U^n better seen by **Eve** (no **inner layer** wiretap coding).
- Advantage to legitimate users in **outer layer**.

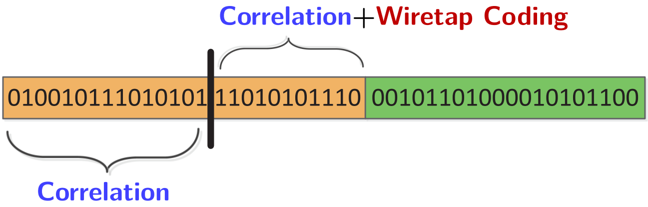


Superposition Coding for the GP Wiretap Channel

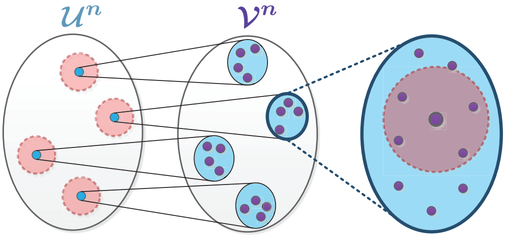


Main Ideas:

- U^n better seen by **Eve** (no **inner layer** wiretap coding).
- Advantage to legitimate users in **outer layer**.



Superposition Coding for the GP Wiretap Channel



Main Ideas:

- U^n better seen by **Eve** (no **inner layer** wiretap coding).
- Advantage to legitimate users in **outer layer**.

Correlation+Wiretap Coding

$\underbrace{010010111010101}_{\text{Correlation}}$ | $\overbrace{11010101110}^{\text{Correlation+Wiretap Coding}}$ 0010110100001010110 0

Correlation

★ Use extra **security** resources as key to OTP **data** in **inner layer** ★

Superposition Coding for the GP Wiretap Channel

Theorem (Prabhakaran-Eswaran-Ramchandran 2012)

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

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

Superposition Coding for the GP Wiretap Channel

Theorem (Prabhakaran-Eswaran-Ramchandran 2012)

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

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

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

Superposition Coding for the GP Wiretap Channel

Theorem (Prabhakaran-Eswaran-Ramchandran 2012)

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

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

- Total secrecy rate of outer layer.
- **Total communication** rate of entire superposition codebook.

Superposition Coding for the GP Wiretap Channel

Theorem (Prabhakaran-Eswaran-Ramchandran 2012)

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

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

- Total secrecy rate of outer layer.
- Total communication rate of entire superposition codebook.
- $U \perp S$

Superposition Coding for the GP Wiretap Channel

Theorem (Prabhakaran-Eswaran-Ramchandran 2012)

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

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

- Total secrecy rate of outer layer.
- Total communication rate of entire superposition codebook.
- $U \perp S \implies$ No GP coding in the **inner layer**!

Superposition Coding for the GP Wiretap Channel

Relax Independence:

Superposition Coding for the GP Wiretap Channel

Relax Independence:

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

Superposition Coding for the GP Wiretap Channel

Relax Independence:

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

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

Superposition Coding for the GP Wiretap Channel

Relax Independence:

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

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

- **Inner layer** supports GP coding.

Superposition Coding for the GP Wiretap Channel

Relax Independence:

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

Theorem (ZG-Cuff-Permuter 2016)

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

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

- **Inner layer** supports GP coding.

$\Longrightarrow$ Required for achieving optimality in some cases.

Superposition Coding for the GP Wiretap Channel

Relax Independence:

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

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

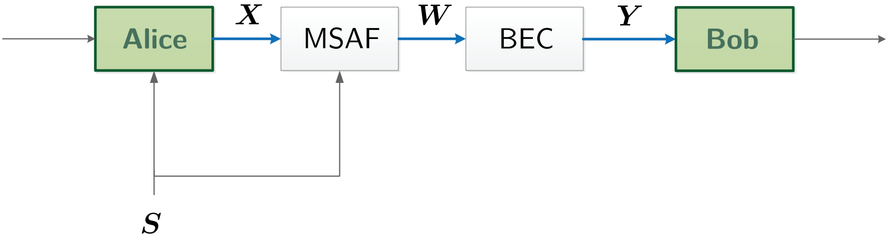
- **Inner layer** supports GP coding.

  $\Longrightarrow$ Required for achieving optimality in some cases.

- Captures all previous results & Upgrades to semantic security.

Example of Strict Improvement

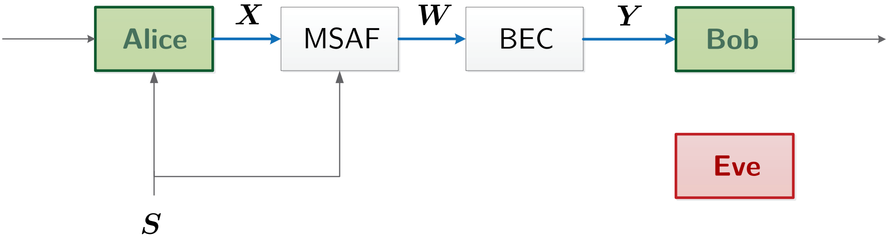
Special Thanks to A. Bunin, S. Shamai and P. Piantanida



- **Main Channel:** Memory with Stuck-at-Faults + Binary Erasure.

Example of Strict Improvement

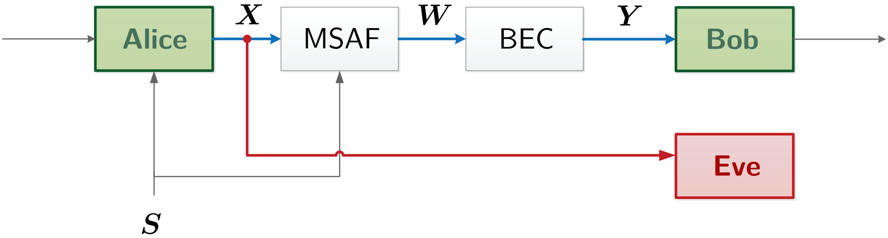
Special Thanks to A. Bunin, S. Shamai and P. Piantanida



- **Main Channel:** Memory with Stuck-at-Faults + Binary Erasure.
- **Eve:** Knows input & state $Z = (X, S)$

Example of Strict Improvement

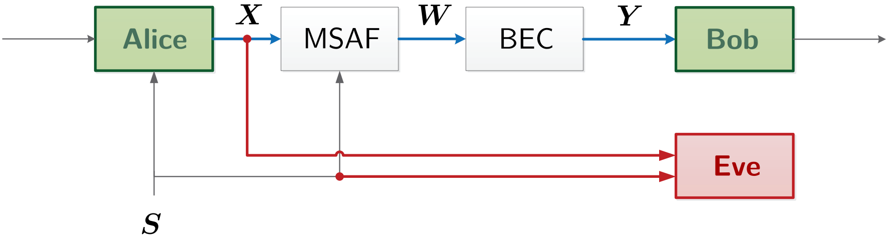
Special Thanks to A. Bunin, S. Shamai and P. Piantanida



- **Main Channel:** Memory with Stuck-at-Faults + Binary Erasure.
- **Eve:** Knows input & state $Z = (X, S)$

Example of Strict Improvement

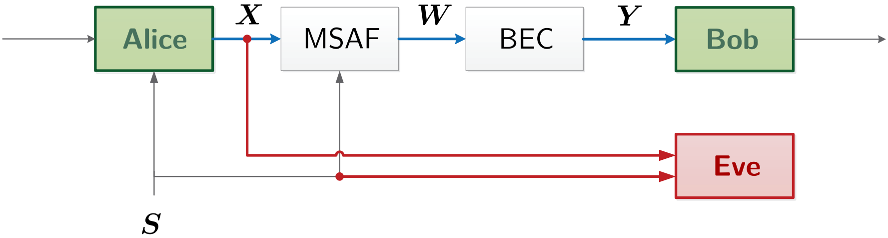
Special Thanks to A. Bunin, S. Shamai and P. Piantanida



- **Main Channel:** Memory with Stuck-at-Faults + Binary Erasure.
- **Eve:** Knows input & state $Z = (X, S)$

Example of Strict Improvement

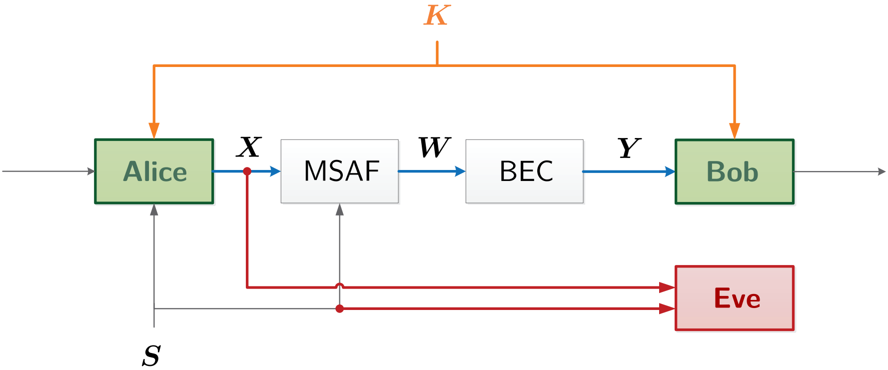
Special Thanks to A. Bunin, S. Shamai and P. Piantanida



- **Main Channel:** Memory with Stuck-at-Faults + Binary Erasure.
- **Eve:** Knows input & state $Z = (X, S) \implies$ No wiretap coding.

Example of Strict Improvement

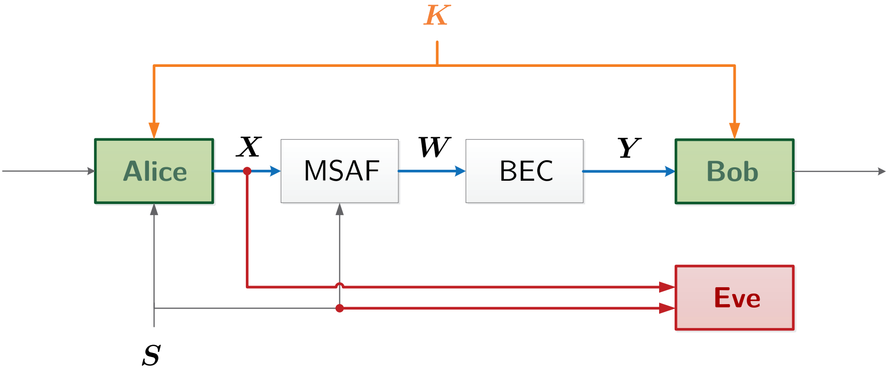
Special Thanks to A. Bunin, S. Shamai and P. Piantanida



- **Main Channel:** Memory with Stuck-at-Faults + Binary Erasure.
- **Eve:** Knows input & state $Z = (X, S)$ $\Longrightarrow$ No wiretap coding.
- **Secrecy:** Shared key K

Example of Strict Improvement

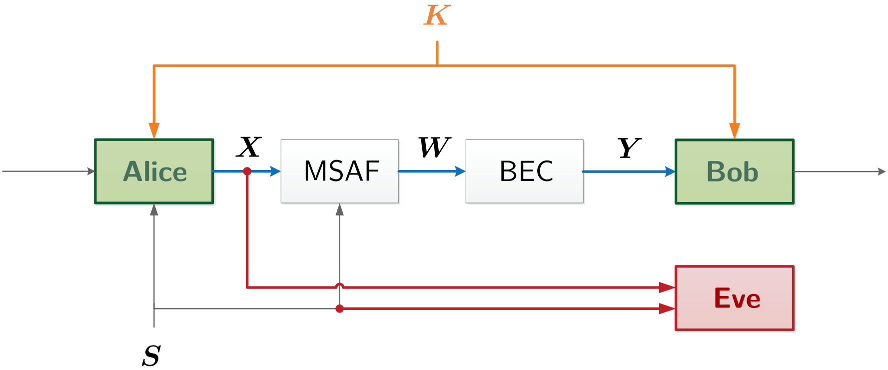
Special Thanks to A. Bunin, S. Shamai and P. Piantanida



- **Main Channel:** Memory with Stuck-at-Faults + Binary Erasure.
- **Eve:** Knows input & state $Z = (X, S) \implies$ No wiretap coding.
- **Secrecy:** Shared key $K \implies$ OTP + Inner layer GP coding.

Example of Strict Improvement

Special Thanks to A. Bunin, S. Shamai and P. Piantanida

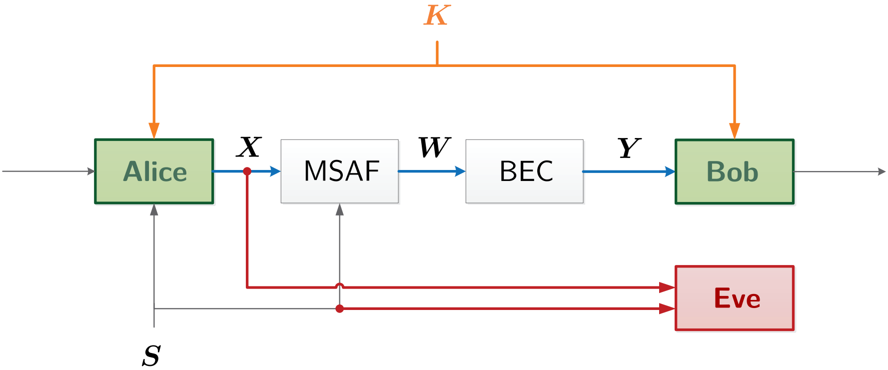


- **Main Channel:** Memory with Stuck-at-Faults + Binary Erasure.
- **Eve:** Knows input & state $Z = (X, S)$ $\implies$ No wiretap coding.
- **Secrecy:** Shared key K $\implies$ OTP + Inner layer GP coding.

$\implies$ Capacity = Our Results

Example of Strict Improvement

Special Thanks to A. Bunin, S. Shamai and P. Piantanida



- **Main Channel:** Memory with Stuck-at-Faults + Binary Erasure.
- **Eve:** Knows input & state $Z = (X, S)$ $\implies$ No wiretap coding.
- **Secrecy:** Shared key K $\implies$ OTP + Inner layer GP coding.

$\implies$ Capacity = Our Results > Prabhakaran *et al.*

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 lower bounds**

Summary

- **The Gelfand-Pinsker wiretap channel**
  - Combination of two fundamental IT setups.
  - Simultaneously exploit state for reliability and security.
- **Novel superposition coding lower bounds**
  - 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 lower bounds**
  - Recovers all past results.
  - Strictly outperforms previous benchmark [Prabhakaran *et al.* 2012].

Summary

- **The Gelfand-Pinsker wiretap channel**
  - Combination of two fundamental IT setups.
  - Simultaneously exploit state for reliability and security.
- **Novel superposition coding lower bounds**
  - Recovers all past results.
  - Strictly outperforms previous benchmark [Prabhakaran *et al.* 2012].
  - Upgrades all previous results to semantic security.

Summary

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

- **Novel superposition coding lower bounds**
  - Recovers all past results.
  - Strictly outperforms previous benchmark [Prabhakaran *et al.* 2012].
  - Upgrades all previous results to semantic security.

- **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 lower bounds**
  - Recovers all past results.
  - Strictly outperforms previous benchmark [Prabhakaran *et al.* 2012].
  - Upgrades all previous results to semantic security.
- **Available on arXiv**: `https://arxiv.org/abs/1608.00743v1`.

Thank you!

The Wiretap Channel & The GP Channel - Coding

The Wiretap Channel

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

The Gelfand-Pinsker Channel

The Wiretap Channel

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

Message	Padding
0010110100011100	0100010011

Trans. together in one block

The Gelfand-Pinsker Channel

The Wiretap Channel

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

Message	Padding
0010110100011100	0100010011

Trans. together in one block

- **Codebook:** $\boldsymbol{U^n} \sim Q_U^n$

The Gelfand-Pinsker Channel

The Wiretap Channel & The GP Channel - Coding

The Wiretap Channel

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

Message	Padding
00101101000111 00	0100010011

Trans. together in one block

- **Codebook:** $U^n \sim Q_U^n$
- **Security:** $\tilde{R} > I(U;Z)$

The Gelfand-Pinsker Channel

The Wiretap Channel

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

Message	Padding
0010110100011100	0100010011

Trans. together in one block

- **Codebook:** $U^n \sim Q_U^n$
- **Security:** $\tilde{R} > I(U;Z)$
- **Reliability:** $R+\tilde{R} < I(U;Y)$

The Gelfand-Pinsker Channel

The Wiretap Channel & The GP Channel - Coding

The Wiretap Channel

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

Message	Padding
0010110100011100	0100010011

Trans. together in one block

- **Codebook:** $U^n \sim Q_U^n$
- **Security:** $\tilde{R} > I(U;Z)$
- **Reliability:** $R + \tilde{R} < I(U;Y)$

The Gelfand-Pinsker Channel

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

The Wiretap Channel

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

Message	Padding
0010110100011100	0100010011

Trans. together in one block

- **Codebook:** $U^n \sim Q_U^n$
- **Security:** $\tilde{R} > I(U;Z)$
- **Reliability:** $R+\tilde{R}<I(U;Y)$

The Gelfand-Pinsker Channel

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

Message	Padding
0010110100011100	0100010011

Trans. together in one block

The Wiretap Channel & The GP Channel - Coding

The Wiretap Channel

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

Message	Padding
0010110100011100	0100010011

Trans. together in one block

- **Codebook:** $U^n \sim Q_U^n$
- **Security:** $\tilde{R} > I(U;Z)$
- **Reliability:** $R + \tilde{R} < I(U;Y)$

The Gelfand-Pinsker Channel

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

Message	Padding
0010110100011100	0100010011

Trans. together in one block

- **Codebook:** $U^n \sim Q_U^n$

The Wiretap Channel & The GP Channel - Coding

The Wiretap Channel

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

Message	Padding
0010110100011100	0100010011

Trans. together in one block

- **Codebook:** $U^n \sim Q_U^n$
- **Security:** $\tilde{R} > I(U;Z)$
- **Reliability:** $R + \tilde{R} < I(U;Y)$

The Gelfand-Pinsker Channel

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

Message	Padding
0010110100011100	0100010011

Trans. together in one block

- **Codebook:** $U^n \sim Q_U^n$
- **Correlation:** $\tilde{R} > I(U;S)$

The Wiretap Channel & The GP Channel - Coding

The Wiretap Channel

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

Message	Padding
0010110100011100	0100010011

Trans. together in one block

- **Codebook:** $U^n \sim Q_U^n$
- **Security:** $\tilde{R} > I(U;Z)$
- **Reliability:** $R+\tilde{R} < I(U;Y)$

The Gelfand-Pinsker Channel

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

Message	Padding
0010110100011100	0100010011

Trans. together in one block

- **Codebook:** $U^n \sim Q_U^n$
- **Correlation:** $\tilde{R} > I(U;S)$
- **Reliability:** $R+\tilde{R} < I(U;Y)$