Wiretap Channels with Random States Non-Causally Available at the Encoder

Ziv Goldfeld
Joint work with Paul Cuff and Haim Permuter

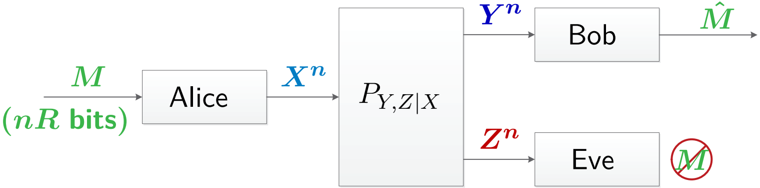
Ben-Gurion University

2016 International Conference on the Science of Electrical Engineering

November 18th, 2016

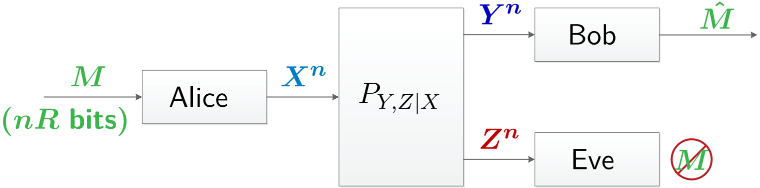
The Wiretap Channel

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



The Wiretap Channel

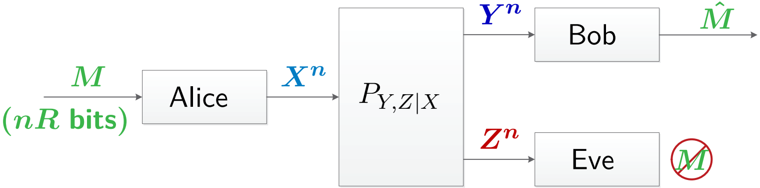
Degraded [Wyner 1975], General [Csiszár-Körner 1978]



Secrecy-Capacity:

The Wiretap Channel

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

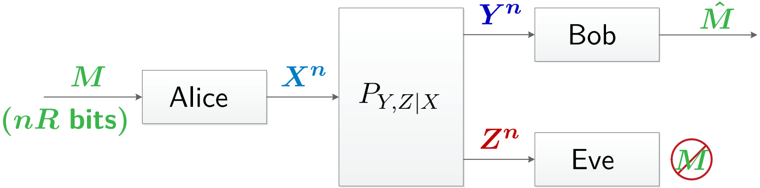


Secrecy-Capacity:

- Reliable Communication.

The Wiretap Channel

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

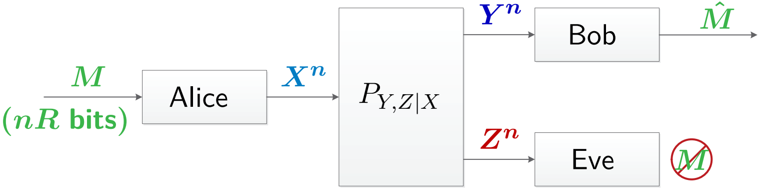


Secrecy-Capacity:

- 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)

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

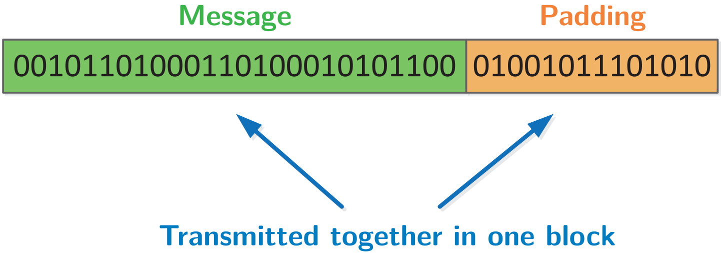
Joint distribution: $P_{U,X} P_{Y,Z|X}$

The Wiretap Channel - Encoding

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

The Wiretap Channel - Encoding

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



Message

Padding

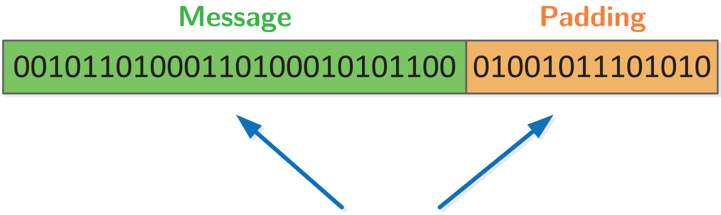
00101101000110100010101100

01001011101010

Transmitted together in one block

The Wiretap Channel - Encoding

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



Message

Padding

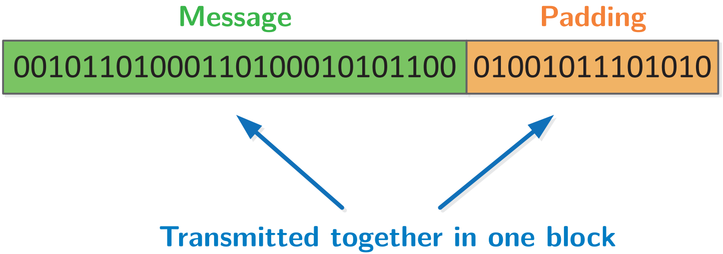
00101101000110100010101100 | 01001011101010

Transmitted together in one block

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

The Wiretap Channel - Encoding

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



Message

Padding

00101101000110100010101100 | 01001011101010

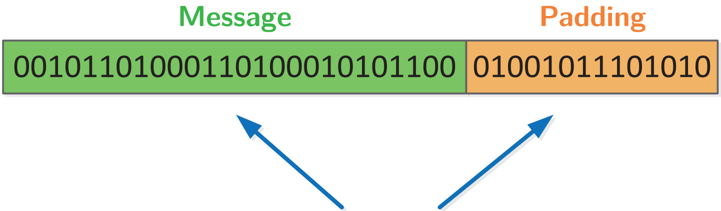
Transmitted together in one block

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

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

The Wiretap Channel - Encoding

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



Message

Padding

00101101000110100010101100 | 01001011101010

Transmitted together in one block

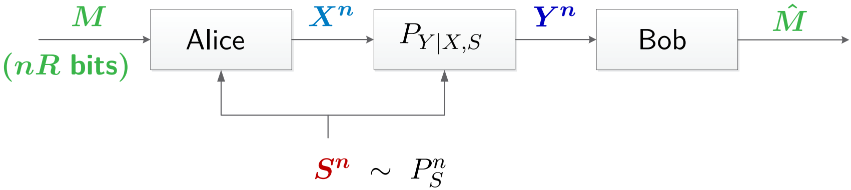
- **Random Codebook:** (Message, Padding) $\rightarrow$ $U^n \sim P_U^n$.

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

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

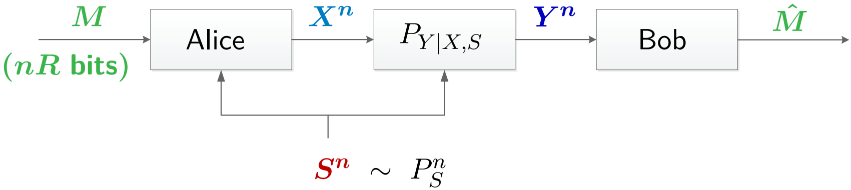
The Gelfand-Pinsker Channel

[Pelfand-Pinsker 1980]



The Gelfand-Pinsker Channel

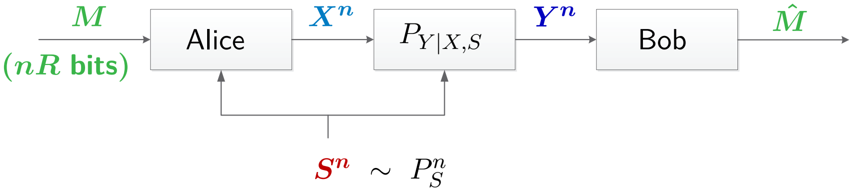
[Pelfand-Pinsker 1980]



Capacity:

The Gelfand-Pinsker Channel

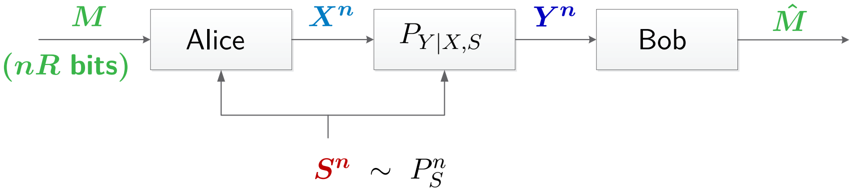
[Pelfand-Pinsker 1980]



Capacity: Reliable Communication.

The Gelfand-Pinsker Channel

[Pelfand-Pinsker 1980]



Capacity: Reliable Communication.

Theorem (Gelfand-Pinsker 1980)

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

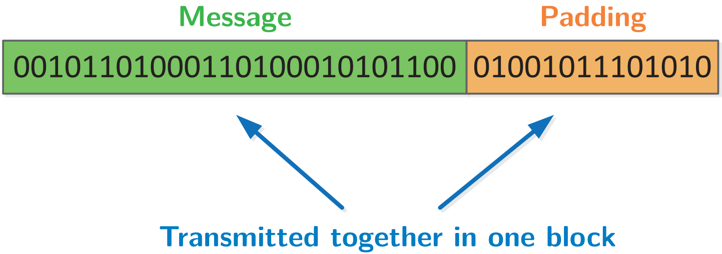
Joint distribution: $P_{U,X|S} P_{Y|X,S}$

The Gelfand-Pinsker Channel - Encoding

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

The Gelfand-Pinsker Channel - Encoding

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



Message

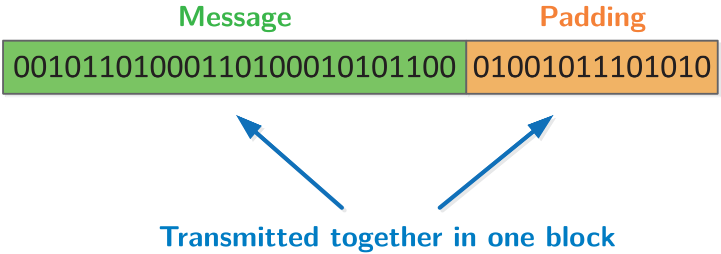
Padding

00101101000110100010101100 | 01001011101010

Transmitted together in one block

The Gelfand-Pinsker Channel - Encoding

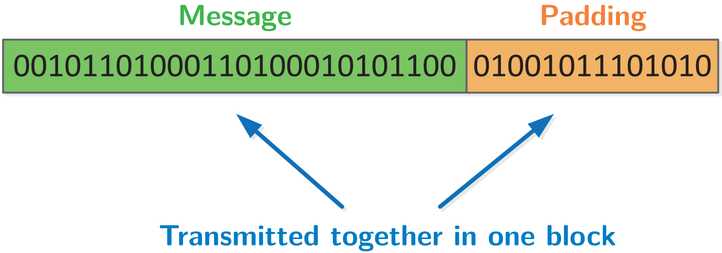
- Pad nR **message bits** with $n\tilde{R}$ **skillfully chosen bits**.



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

The Gelfand-Pinsker Channel - Encoding

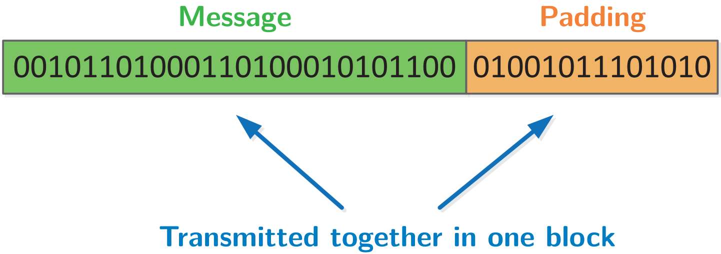
- Pad nR message bits with $n\tilde{R}$ skillfully chosen bits.



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

The Gelfand-Pinsker Channel - Encoding

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



Message

Padding

00101101000110100010101100 | 01001011101010

Transmitted together in one block

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

- **Correlating U^n with S^n:** $\tilde{R} > I(U;S)$.

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

Gelfand-Pinsker Channel vs. Wiretap Channel

Similarities:

Gelfand-Pinsker Channel vs. Wiretap Channel

Similarities:

- Capacity expression.

Gelfand-Pinsker Channel vs. Wiretap Channel

Similarities:

- Capacity expression.
- Encoding.

Gelfand-Pinsker Channel vs. Wiretap Channel

Similarities:

- Capacity expression.
- Encoding.
- Converse (i.i.d. S^n in GP setting allows skipping a step).

Gelfand-Pinsker Channel vs. Wiretap Channel

Similarities:

- Capacity expression.
- Encoding.
- Converse (i.i.d. S^n in GP setting allows skipping a step).
- Target asymptotic probabilistic relations:

Gelfand-Pinsker Channel vs. Wiretap Channel

Similarities:

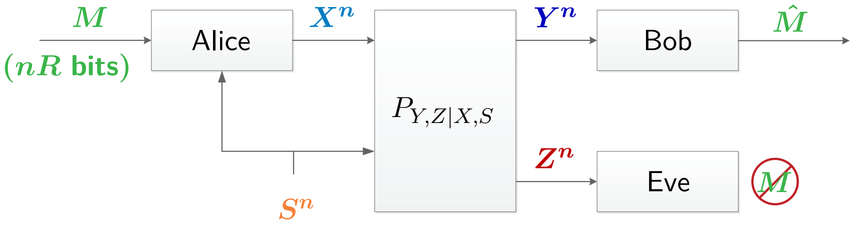
- Capacity expression.
- Encoding.
- Converse (i.i.d. S^n in GP setting allows skipping a step).
- Target asymptotic probabilistic relations:
  - **Gelfand-Pinsker Channel:** $\hat{M} = M$ (and M independent of S^n).

Gelfand-Pinsker Channel vs. Wiretap Channel

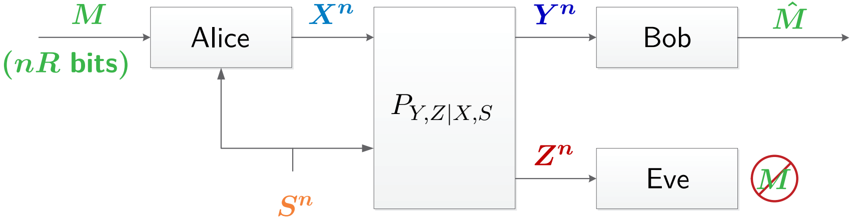
Similarities:

- Capacity expression.
- Encoding.
- Converse (i.i.d. S^n in GP setting allows skipping a step).
- Target asymptotic probabilistic relations:
  - **Gelfand-Pinsker Channel:** $\hat{M} = M$ (and M independent of S^n).
  - **Wiretap Channel:** $\hat{M} = M$ and M independent of Z^n.

The Gelfand-Pinsker Wiretap Channel

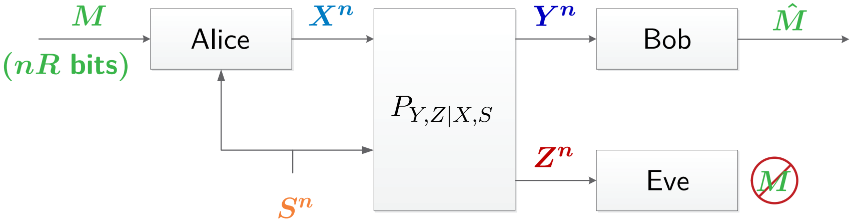


The Gelfand-Pinsker Wiretap Channel



Secrecy-Capacity:

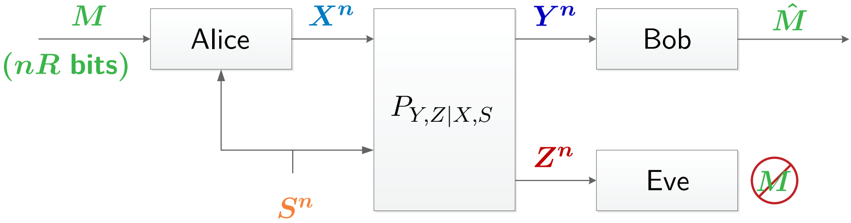
The Gelfand-Pinsker Wiretap Channel



Secrecy-Capacity:

- Reliable Communication.

The Gelfand-Pinsker Wiretap Channel



Secrecy-Capacity:

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

The Gelfand-Pinsker Wiretap Channel

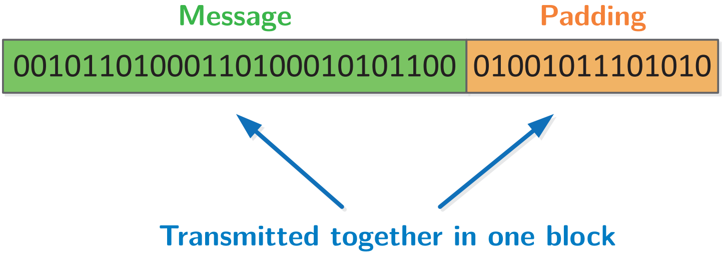
Same Encoding [Chen-Han Vinck 2006]

Naive Approach:

The Gelfand-Pinsker Wiretap Channel

Same Encoding [Chen-Han Vinck 2006]

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



Message

Padding

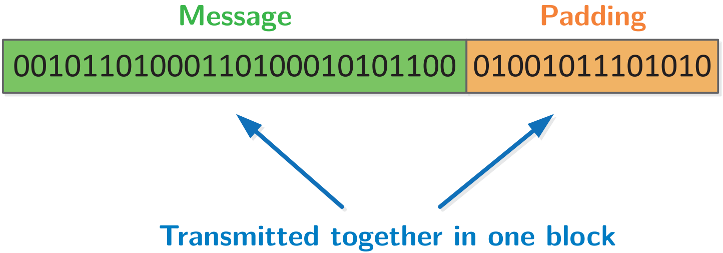
00101101000110100010101100 | 01001011101010

Transmitted together in one block

The Gelfand-Pinsker Wiretap Channel

Same Encoding [Chen-Han Vinck 2006]

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



Theorem (Chen-Han Vinck 2006)

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

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

Wiretap Channels with Encoder and Decoder CSI

Key Extraction Scheme [Chia-El Gamal 2012]

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

Wiretap Channels with Encoder and Decoder CSI

Key Extraction Scheme [Chia-El Gamal 2012]

Assume S^n is know to Receiver $\mathbf{Y} = (\mathbf{Y}, \mathbf{S})$.

- Extract secret random bits from S^n.

Wiretap Channels with Encoder and Decoder CSI

Key Extraction Scheme [Chia-El Gamal 2012]

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

- Extract secret random bits from S^n.
- One-Time-Pad the message $\boldsymbol{M}$.

Wiretap Channels with Encoder and Decoder CSI

Key Extraction Scheme [Chia-El Gamal 2012]

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

- Extract secret random bits from S^n.
- One-Time-Pad the message $\boldsymbol{M}$.
- Point-to-point transmission (ignore **Eve**).

Wiretap Channels with Encoder and Decoder CSI

Key Extraction Scheme [Chia-El Gamal 2012]

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

- Extract secret random bits from S^n.
- One-Time-Pad the message M.
- Point-to-point transmission (ignore **Eve**).

Theorem (Chia-El Gamal 2012)

$$\mathsf{C}_{\mathsf{GP-WTC}} \geq \max_{P_{U,X|S}} \min\Big\{H(S|U,Z), I(U;Y|S)\Big\}$$

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

Note: They consider causal state information.
This region is adapted to take advantage of non-causal state information.

Wiretap Channels with Encoder and Decoder CSI

Key Extraction Scheme [Chia-El Gamal 2012]

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

- Extract secret random bits from $\boldsymbol{S}^n$.
- One-Time-Pad the message $\boldsymbol{M}$.
- Point-to-point transmission (ignore **Eve**).

Theorem (Chia-El Gamal 2012)

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

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

Better than previous scheme!

Note: They consider causal state information.
This region is adapted to take advantage of non-causal state information.

Wiretap Channels with Encoder and Decoder CSI

Combined Scheme [Chia-El Gamal 2012]

Combine Wiretap Codes with Key Extraction:

Wiretap Channels with Encoder and Decoder CSI

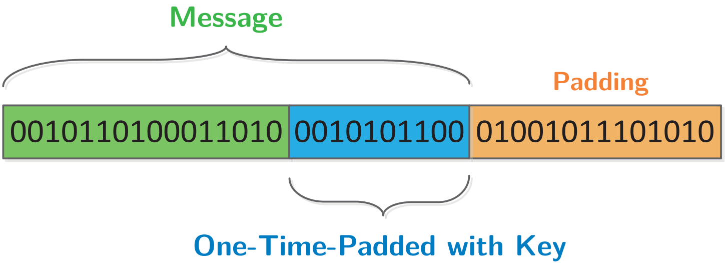
Combined Scheme [Chia-El Gamal 2012]

Combine Wiretap Codes with Key Extraction: Assume $\boldsymbol{Y} = (\boldsymbol{Y}, \boldsymbol{S})$.

Wiretap Channels with Encoder and Decoder CSI

Combined Scheme [Chia-El Gamal 2012]

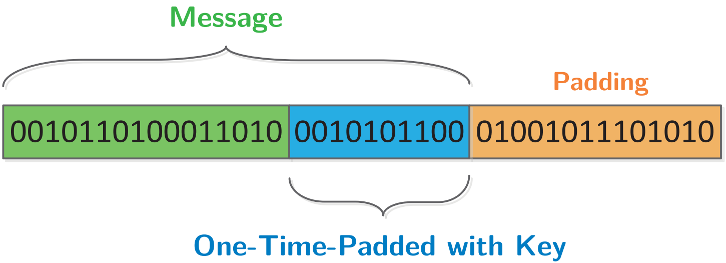
Combine Wiretap Codes with Key Extraction: Assume $\boldsymbol{Y} = (\boldsymbol{Y}, \boldsymbol{S})$.



Wiretap Channels with Encoder and Decoder CSI

Combined Scheme [Chia-El Gamal 2012]

Combine Wiretap Codes with Key Extraction: Assume $\mathbf{Y} = (\mathbf{Y}, \mathbf{S})$.



Message

Padding

0010110100011010 0010101100 01001011101010

One-Time-Padded with Key

Theorem (Chia-El Gamal 2012)

$$\mathsf{C}_{\mathsf{GP-WTC}} \geq \max_{P_{U,X|S}} \min \left\{ \begin{array}{c} H(S|U,Z) + \left[I(U;Y,S) - I(U;Z)\right]^{+}, \\ I(U;Y|S) \end{array} \right\}$$

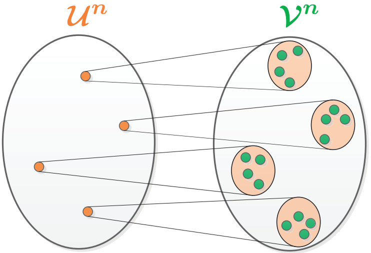
Joint distribution: $P_S P_{U,X|S} P_{Y,Z|X,S}$

The Gelfand-Pinsker Wiretap Channel - Our Scheme

Superposition Code:

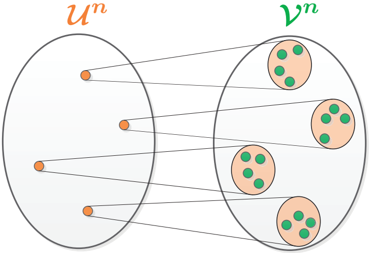
The Gelfand-Pinsker Wiretap Channel - Our Scheme

Superposition Code:



The Gelfand-Pinsker Wiretap Channel - Our Scheme

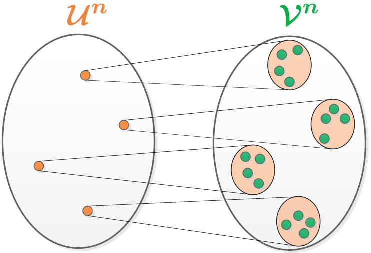
Superposition Code:



- U^n index is **padding** only.

The Gelfand-Pinsker Wiretap Channel - Our Scheme

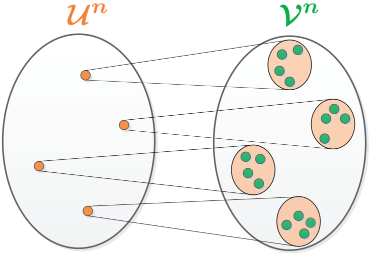
Superposition Code:



- U^n index is **padding** only.
- V^n index is **massage** and **padding** only.

The Gelfand-Pinsker Wiretap Channel - Our Scheme

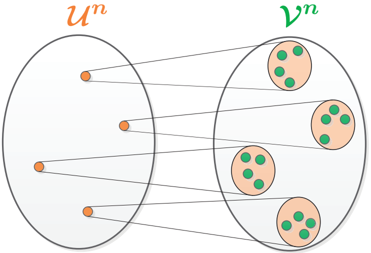
Superposition Code:



- U^n index is **padding** only.
- V^n index is **massage** and **padding** only.
- U^n decoded by **Eve**

The Gelfand-Pinsker Wiretap Channel - Our Scheme

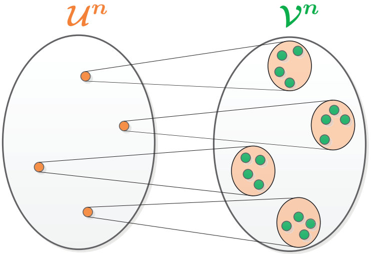
Superposition Code:



- U^n index is **padding** only.
- V^n index is **massage** and **padding** only.
- U^n decoded by **Eve** $\Longrightarrow$ waste channel resources.

The Gelfand-Pinsker Wiretap Channel - Our Scheme

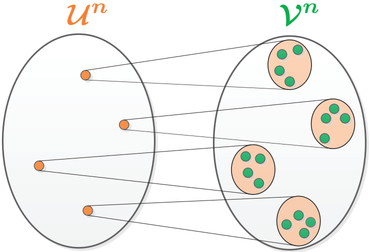
Superposition Code:



- U^n index is **padding** only.
- V^n index is **massage** and **padding** only.
- U^n decoded by **Eve** $\Longrightarrow$ waste channel resources.
- All secrecy comes from V^n.

The Gelfand-Pinsker Wiretap Channel - Our Scheme

Superposition Code:



- U^n index is **padding** only.
- V^n index is **massage** and **padding** only.
- U^n decoded by **Eve** $\Longrightarrow$ waste channel resources.
- All secrecy comes from V^n.

★ **Analysis:** Likelihood Encoder & Strong Soft-Covering Lemma ★

The Gelfand-Pinsker Wiretap Channel - Our Scheme

Theorem (ZG-Cuff-Permuter 2016)

$$\mathsf{C}_{\mathsf{GP-WTC}} \geq \max_{\substack{P_{U,V,X|S}: \\ I(U;Y)-I(U;S)\geq 0}} \min \left\{ \begin{array}{c} I(V;Y|U) - I(V;Z|U), \\ I(U,V;Y) - I(U,V;S) \end{array} \right\}$$

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

The Gelfand-Pinsker Wiretap Channel - Our Scheme

Theorem (ZG-Cuff-Permuter 2016)

$$\mathsf{C}_{\mathsf{GP-WTC}} \geq \max_{\substack{P_{U,V,X|S}: \\ \boldsymbol{I(U;Y)-I(U;S)\geq 0}}} \min\left\{ \begin{array}{c} I(V;Y|U)-I(V;Z|U), \\ I(U,V;Y)-I(U,V;S) \end{array} \right\}$$

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

- **Inner layer** reliably decodable by the receiver.

The Gelfand-Pinsker Wiretap Channel - Our Scheme

Theorem (ZG-Cuff-Permuter 2016)

$$\mathsf{C}_{\mathsf{GP-WTC}} \geq \max_{\substack{P_{U,V,X|S}: \\ I(U;Y)-I(U;S)\geq 0}} \min \left\{ \begin{array}{c} \boldsymbol{I(V;Y|U) - I(V;Z|U)}, \\ I(U,V;Y) - I(U,V;S) \end{array} \right\}$$

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

- Inner layer reliably decodable by the receiver.
- **Total secrecy** rate of outer layer.

The Gelfand-Pinsker Wiretap Channel - Our Scheme

Theorem (ZG-Cuff-Permuter 2016)

$$\mathsf{C}_{\mathsf{GP-WTC}} \geq \max_{\substack{P_{U,V,X|S}: \\ I(U;Y)-I(U;S)\geq 0}} \min \left\{ \begin{array}{c} I(V;Y|U) - I(V;Z|U), \\ \boldsymbol{I(U,V;Y) - I(U,V;S)} \end{array} \right\}$$

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

- Inner layer reliably decodable by the receiver.
- Total secrecy rate of outer layer.
- **Total communication** rate of entire superposition codebook.

The Gelfand-Pinsker Wiretap Channel - Our Scheme

Theorem (ZG-Cuff-Permuter 2016)

$$\mathsf{C}_{\mathsf{GP-WTC}} \geq \max_{\substack{P_{U,V,X|S}: \\ I(U;Y)-I(U;S)\geq 0}} \min \left\{ \begin{array}{c} I(V;Y|U) - I(V;Z|U), \\ I(U,V;Y) - I(U,V;S) \end{array} \right\}$$

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

Relation to Previous Schemes:

The Gelfand-Pinsker Wiretap Channel - Our Scheme

Theorem (ZG-Cuff-Permuter 2016)

$$\mathsf{C}_{\mathsf{GP-WTC}} \geq \max_{\substack{P_{U,V,X|S}: \\ I(U;Y)-I(U;S)\geq 0}} \min \left\{ \begin{array}{c} I(V;Y|U) - I(V;Z|U), \\ I(U,V;Y) - I(U,V;S) \end{array} \right\}$$

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

Relation to Previous Schemes:

- Upgrade from **weak-secrecy** to **semantic-security**.

The Gelfand-Pinsker Wiretap Channel - Our Scheme

Theorem (ZG-Cuff-Permuter 2016)

$$\mathsf{C}_{\mathsf{GP-WTC}} \geq \max_{\substack{P_{U,V,X|S}: \\ I(U;Y)-I(U;S)\geq 0}} \min \left\{ \begin{array}{c} I(V;Y|U) - I(V;Z|U), \\ I(U,V;Y) - I(U,V;S) \end{array} \right\}$$

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

Relation to Previous Schemes:

- Upgrade from **weak-secrecy** to **semantic-security**.
- Recovers Chia-El Gamal's result when $Y = (Y,S)$.

The Gelfand-Pinsker Wiretap Channel - Our Scheme

Theorem (ZG-Cuff-Permuter 2016)

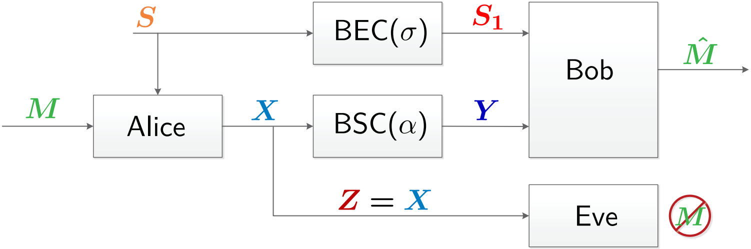
$$\mathsf{C}_{\mathsf{GP-WTC}} \geq \max_{\substack{P_{U,V,X|S}:\\ I(U;Y)-I(U;S)\geq 0}} \min \left\{ \begin{array}{c} I(V;Y|U) - I(V;Z|U), \\ I(U,V;Y) - I(U,V;S) \end{array} \right\}$$

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

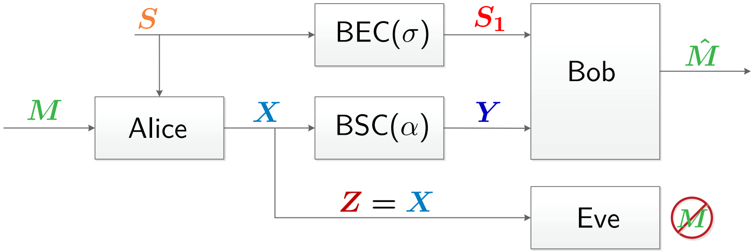
Relation to Previous Schemes:

- Upgrade from **weak-secrecy** to **semantic-security**.
- Recovers Chia-El Gamal's result when $Y = (Y, S)$.
- Beats previous regions even when S^n **not** known to Receiver.

Outperforming Previous Schemes - An Example

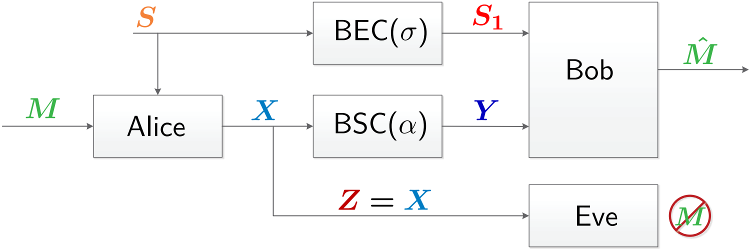


Outperforming Previous Schemes - An Example



- **Our scheme is optimal** [Bassi-Pinatanida-Shamai 2016]:

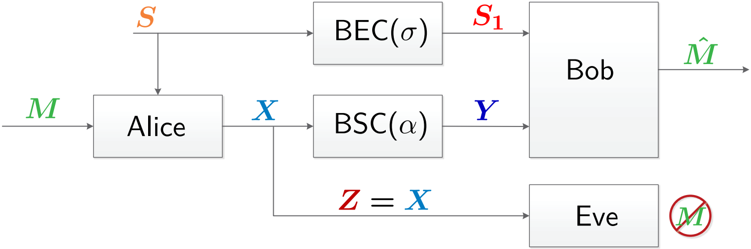
Outperforming Previous Schemes - An Example



- **Our scheme is optimal** [Bassi-Pinatanida-Shamai 2016]:

$$\boxed{C = \max_{P_{A|S}} \min \left\{ I(A;S_1), 1 - h(\alpha) - I(A;S|S_1) \right\}}$$

Outperforming Previous Schemes - An Example

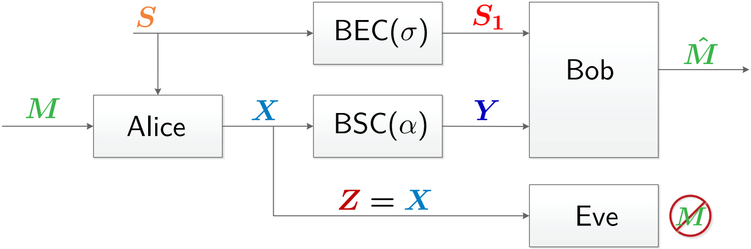


- **Our scheme is optimal** [Bassi-Pinatanida-Shamai 2016]:

$$\boxed{C = \max_{P_{A|S}} \min \left\{ I(A;S_1), 1 - h(\alpha) - I(A;S|S_1) \right\}}$$

  - 1st auxiliary - key agreement over BEC.

Outperforming Previous Schemes - An Example

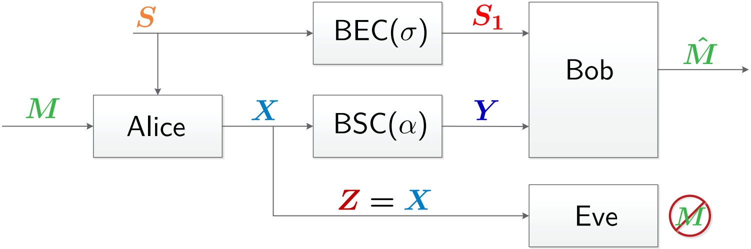


- **Our scheme is optimal** [Bassi-Pinatanida-Shamai 2016]:

$$\boxed{C = \max_{P_{A|S}} \min \left\{ I(A;S_1), 1 - h(\alpha) - I(A;S|S_1) \right\}}$$

  - 1st auxiliary - **key agreement** over BEC.
  - 2nd auxiliary - **transmission** over BSC (indep. of state and key).

Outperforming Previous Schemes - An Example



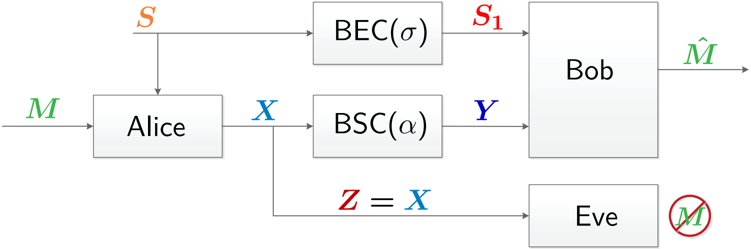
- **Our scheme is optimal** [Bassi-Pinatanida-Shamai 2016]:

$$\boxed{C = \max_{P_{A|S}} \min \left\{ I(A;S_1), 1 - h(\alpha) - I(A;S|S_1) \right\}}$$

  - 1st auxiliary - **key agreement** over BEC.
  - 2nd auxiliary - **transmission** over BSC (indep. of state and key).

- **Chen-Han Vinck scheme is suboptimal:**

Outperforming Previous Schemes - An Example



- **Our scheme is optimal** [Bassi-Pinatanida-Shamai 2016]:

$$\boxed{C = \max_{P_{A|S}} \min \left\{ I(A;S_1), 1 - h(\alpha) - I(A;S|S_1) \right\}}$$

  - 1st auxiliary - **key agreement** over BEC.
  - 2nd auxiliary - **transmission** over BSC (indep. of state and key).

- **Chen-Han Vinck scheme is suboptimal:**
  - Only one auxiliary - lacks flexibility to play both roles!

Summary

- **Gelfand-Pinsker wiretap channel**

Summary

- **Gelfand-Pinsker wiretap channel**
    - Combination of two fundamental problems.

Summary

- **Gelfand-Pinsker wiretap channel**
  - Combination of two fundamental problems.
- **Novel superposition coding scheme**

Summary

- **Gelfand-Pinsker wiretap channel**
  - Combination of two fundamental problems.
- **Novel superposition coding scheme**
  - Recovers best known rate when S^n known to Receiver [Chia-El Gamal].

Summary

- **Gelfand-Pinsker wiretap channel**
  - Combination of two fundamental problems.

- **Novel superposition coding scheme**
  - Recovers best known rate when S^n known to Receiver [Chia-El Gamal].
  - Strictly better than best known rate when S^n not known to Receiver.

Summary

- **Gelfand-Pinsker wiretap channel**
  - Combination of two fundamental problems.

- **Novel superposition coding scheme**
  - Recovers best known rate when S^n known to Receiver [Chia-El Gamal].
  - Strictly better than best known rate when S^n not known to Receiver.

Thank you!