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

\[ A \xrightarrow{X^n} P_{Y,Z|X} \xrightarrow{Y^n} B \xrightarrow{\hat{M}} \]

M

\[ M \]

\[ Z^n \]
The Wiretap Channel

The Wiretap Channel

- Reliable & Secure Commun.
The Wiretap Channel & The GP Channel

The Wiretap Channel

![Diagram of the Wiretap Channel]

- Reliable & Secure Commun.

Theorem (Csiszár-Körner 1978)

\[ C_{\text{WTC}} = \max_{P_{U,X}} \left[ I(U;Y) - I(U;Z) \right] \]

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

Ziv Goldfeld, Paul Cuff and Haim Permuter
Ben Gurion University and Princeton University
The Gelfand-Pinsker Wiretap Channel: Higher Rates via a Novel Superposition Code
The Wiretap Channel & The GP Channel

The Wiretap Channel

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

(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)

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

(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)

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

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

The Gelfand-Pinsker Channel

Reliable Communication.
The Wiretap Channel & The GP Channel

### The Wiretap Channel

- **Input:** $M$, $X^n$
- **Source:** $P_{Y,Z|X}$
- **Encoder:** $E$
- **Message:** $M$
- **Output:** $Y^n$, $Z^n$
- **Decoder:** $B$
- **Reliable & Secure Commun.**

#### Theorem (Csiszár-Körner 1978)

$$C_{WT} = \max_{P_{U,X}} \left[ I(U;Y) - I(U;Z) \right]$$

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

### The Gelfand-Pinsker Channel

- **Input:** $M$, $X^n$
- **Source:** $P_{Y|X,S}$
- **Encoder:** $E$
- **Message:** $M$
- **Output:** $Y^n$
- **Decoder:** $B$
- **Reliable Communication.**

#### Theorem (Gelfand-Pinsker 1980)

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

(Joint dist. $P_{U,X|S}P_{Y|X,S}$)
Pad \( nR \text{ message bits} \) with \( n\tilde{R} \text{ redundancy bits} \).
Pad $nR$ message bits with $n\tilde{R}$ redundancy bits.

Transmitted together in one block
Reminiscent Optimal Coding Schemes

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

Message

```
00101101000110100010101100
```

Padding

```
01001011101010
```

Transmitted together in one block

- **Random Codebook:** $\langle \text{Message, Padding} \rangle \rightarrow U^n \sim P^n_U$
Reminiscent Optimal Coding Schemes

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

![Message and Padding Diagram]

- **Random Codebook:** $(\text{Message}, \text{Padding}) \rightarrow U^n \sim P^n_{U}$
- **Padding:**
Pad $nR$ message bits with $n\tilde{R}$ redundancy bits.

---

**Random Codebook:** \( (\text{Message}, \text{Padding}) \rightarrow U^n \sim P^n_U \)

**Padding:**
- **WTC - Security:** \( \tilde{R} > I(U; Z) \)
Reminiscent Optimal Coding Schemes

- Pad \( nR \) message bits with \( n\tilde{R} \) redundancy bits.

```
00101101000110100010101100
01001011101010
```

Transmitted together in one block

- **Random Codebook:** \((\text{Message}, \text{Padding}) \to U^n \sim P^n_U\)

- **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:  $(\text{Message}, \text{Padding}) \rightarrow U^n \sim P^n_U$

- Padding:
  - WTC - Security: $\tilde{R} > I(U; Z)$
  - GP Channel - Correlation: $\tilde{R} > I(U; S)$

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

00101101100110100010101100 01001011101010

Message Padding

Transmitted together in one block
The Gelfand-Pinsker Wiretap Channel

M (nR bits) Alice

X^n P_{Y,Z|X,S} Bob

S^n Eve

Y^n Z^n

\hat{M}
Secrecy Capacity: Reliable and Secure Communication.
**The Gelfand-Pinsker Wiretap Channel**

**Secrecy Capacity:** Reliable and Secure Communication.

**Naive Approach:**
**Secrecy Capacity:** Reliable and Secure Communication.

**Naive Approach:** Combine wiretap coding with GP coding.
Secrecy Capacity: Reliable and Secure Communication.

Naive Approach: Combine wiretap coding with GP coding.

Theorem (Chen-Han Vinck 2006)

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

(Joint distribution \( P_{SP_{U,X|S}P_{Y,Z|X,S}} \))
Suboptimality of Naive Approach

Key Extraction Scheme [Chia-El Gamal 2012]

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

Key Extraction Scheme [Chia-El Gamal 2012]

\[
C_{\text{GP-WTC}} > \max_{P_{U,X|S}} \left[ I(U;Y) - \max \left\{ I(U;Z), I(U;S) \right\} \right]
\]
Suboptimality of Naive Approach

Key Extraction Scheme [Chia-El Gamal 2012]

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

Why and When?
Suboptimality of Naive Approach

Key Extraction Scheme [Chia-El Gamal 2012]

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

Why and When?

- Chen-Han Vinck scheme always preforms wiretap coding.
Suboptimality of Naive Approach

Key Extraction Scheme [Chia-El Gamal 2012]

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

Why and When?

- Chen-Han Vinck scheme **always** preforms wiretap coding.
- Strong **Eavesdropper**
Suboptimality of Naive Approach

Key Extraction Scheme [Chia-El Gamal 2012]

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

Why and When?

- Chen-Han Vinck scheme **always** preforms wiretap coding.
- Strong **Eavesdropper** \( \Rightarrow \) Wiretap coding is useless
Suboptimality of Naive Approach

Key Extraction Scheme [Chia-El Gamal 2012]

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

Why and When?

- Chen-Han Vinck scheme always preforms wiretap coding.
- Strong **Eavesdropper** \( \rightarrow \) Wiretap coding is useless

A Simple Alternative:
Suboptimality of Naive Approach

Key Extraction Scheme [Chia-El Gamal 2012]

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

Why and When?

- Chen-Han Vinck scheme always preforms wiretap coding.
- Strong Eavesdropper \( \Rightarrow \) Wiretap coding is useless

A Simple Alternative: \( S^n \) is known to Receiver \( Y = (Y, S) \)
Suboptimality of Naive Approach
Key Extraction Scheme [Chia-El Gamal 2012]

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

Why and When?

- Chen-Han Vinck scheme \textbf{always} preforms wiretap coding.
- Strong \textbf{Eavesdropper} \implies Wiretap coding is useless

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

1. Extract secret random bits from \( S^n \).
Suboptimality of Naive Approach

Key Extraction Scheme [Chia-El Gamal 2012]

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

Why and When?

- Chen-Han Vinck scheme **always** preforms wiretap coding.
- Strong **Eavesdropper** \(\Rightarrow\) Wiretap coding is useless

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

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]

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

Why and When?

- Chen-Han Vinck scheme **always** performs wiretap coding.
- Strong **Eavesdropper** \( \implies \) Wiretap coding is useless

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

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]

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

Why and When?

- Chen-Han Vinck scheme \textbf{always} preforms wiretap coding.
- Strong \textbf{Eavesdropper} \implies Wiretap coding is useless

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

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

\[ \implies \text{Achieves:} \max_{P_{U,X|S}} \min \left\{ H(S|U,Z), I(U;Y|S) \right\} \]
Suboptimality of Naive Approach

Key Extraction Scheme [Chia-El Gamal 2012]

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

Why and When?

- Chen-Han Vinck scheme **always** preforms wiretap coding.
- Strong **Eavesdropper** \(\Rightarrow\) Wiretap coding is useless

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

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

\[\Rightarrow\] Achieves:

\[
\max_{P_{U,X|S}} \min \left\{H(S|U, Z), I(U; Y|S)\right\}
\]

Can strictly outperform previous scheme!
Main Ideas:
Superposition Coding for the GP Wiretap Channel

Main Ideas:
Main Ideas:
Main Ideas:

- $\mathcal{U}^n$ better seen by Eve
  (no inner layer wiretap coding).
Main Ideas:

- $U^n$ better seen by Eve
  (no inner layer wiretap coding).
Main Ideas:

- $\mathcal{U}^n$ better seen by Eve
  (no inner layer wiretap coding).
Main Ideas:

- \( U^n \) better seen by \textbf{Eve} (no inner layer wiretap coding).
- Advantage to legitimate users in \textbf{outer layer}.
Main Ideas:

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

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

\[010010111010101101000010101100010101100\]
Main Ideas:

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

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

$010010111010101\, 11010101110\, 00101101000\, 10101100$

Correlation
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

01001011101010110100010101100010101100
Main Ideas:

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

Use extra security resources as key to OTP data in inner layer.
Superposition Coding for the GP Wiretap Channel

**Theorem (Prabhakaran-Eswaran-Ramchandran 2012)**

\[
C_{GP-WTC} \geq \max_{P_{U,V,X|S}} \min_{U \perp S} \left\{ \begin{array}{l}
I(V;Y|U) - I(V;Z|U), \\
I(U,V;Y) - I(U,V;S)
\end{array} \right\}
\]

*Joint distribution* \(P_S P_U P_{V,X|S} P_{Y,Z|X,S} \).
Superposition Coding for the GP Wiretap Channel

Theorem (Prabhakaran-Eswaran-Ramchandran 2012)

\[
C_{GP-WTC} \geq \max_{P_{U,V,X|S}: \, U \perp \! \! \! \perp S} \min \left\{ I(V; Y|U) - I(V; Z|U), \quad \quad \right. \\
\left. I(U, V; Y) - I(U, V; S) \right\}
\]

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

- **Total secrecy** rate of outer layer.
Theorem (Prabhakaran-Eswaran-Ramchandran 2012)

\[ C_{\text{GP-WTC}} \geq \max_{P_{U,V,X|S}: \quad U \perp S} \min \left\{ \begin{array}{c} I(V; Y|U) - I(V; Z|U), \\ I(U, V; Y) - I(U, V; S) \end{array} \right\} \]

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.
Theorem (Prabhakaran-Eswaran-Ramchandran 2012)

\[ C_{GP-WTC} \geq \max_{P_{U,V,X|S}: \ U \perp S} \min \left\{ I(V;Y|U) - I(V;Z|U), \ I(U,V;Y) - I(U,V;S) \right\} \]

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.
- \( U \perp S \)
Theorem (Prabhakaran-Eswaran-Ramchandran 2012)

\[
C_{\text{GP-WTC}} \geq \max_{P_{U,V,X|S}: U \perp S} \min \left\{ I(V; Y|U) - I(V; Z|U), \quad \begin{array}{l} I(U, V; Y) - I(U, V; S) \end{array} \right\}
\]

Joint distribution \(P_SP_UP_V,X|S,U P_Y,Z|X,S\).

- 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 ★
Relax Independence:

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

**Theorem (ZG-Cuff-Permuter 2016)**

\[
C_{GP-WTC} \geq \max_{P_{U,V,X|S}: I(U;Y) \geq I(U;S)} \min \left\{ \begin{array}{c}
I(V;Y|U) - I(V;Z|U), \\
I(U,V;Y) - I(U,V;S)
\end{array} \right\}
\]

*Joint distribution* \(P_S P_{U,V,X|S} P_{Y,Z|X,S} \).
Relax Independence:

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

**Theorem (ZG-Cuff-Permuter 2016)**

\[
C_{\text{GP-WTC}} \geq \max_{P_{U,V,X|S}} \min \left\{ \begin{array}{l}
I(V; Y|U) - I(V; Z|U), \\
I(U, V; Y) - I(U, V; S)
\end{array} \right\}
\]

Subject to \(I(U; Y) \geq I(U; S)\)

*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)

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

Joint distribution \( P_S P_{U,V,X|S} P_{Y,Z|X,S} \).

- **Inner layer** supports GP coding.

\[\Longrightarrow \text{ Required for achieving optimality in some cases.}\]
Superposition Coding for the GP Wiretap Channel

Relax Independence:

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

**Theorem (ZG-Cuff-Permuter 2016)**

\[
C_{GP-WTC} \geq \max_{P_{U,V,X|S}: I(U;Y) \geq I(U;S)} \min \left\{ I(V;Y|U) - I(V;Z|U), \quad I(U,V;Y) - I(U,V;S) \right\}
\]

Joint distribution \( P_S P_{U,V,X|S} P_{Y,Z|X,S} \).

- **Inner layer** supports GP coding.
  
  \[\Rightarrow\] Required for achieving optimality in some cases.

- Captures all previous results & Upgrades to semantic security.
**Main Channel:** Memory with Stuck-at-Faults + Binary Erasure.
**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

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 $Z = (X, S) \implies$ No wiretap coding.
- **Secrecy**: Shared key $K$
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.
The Gelfand-Pinsker wiretap channel
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.
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.
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.


Thank you!
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: 0010110100011100
Padding: 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:** $U^n \sim Q^n_U$
The Wiretap Channel

Pad \( n\tilde{R} \) message bits with \( n\tilde{R} \) random garbage bits.

Message: 0010110100011100
Padding: 0100010011

Trans. together in one block

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

---

The Gelfand-Pinsker Channel

Ziv Goldfeld, Paul Cuff and Haim Permuter
Ben Gurion University and Princeton University
The Gelfand-Pinsker Wiretap Channel: Higher Rates via a Novel Superposition Code
The Wiretap Channel

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

Message: 0010110100011100
Padding: 0100010011

Trans. together in one block

- **Codebook:** \( U^n \sim Q^n_U \)
- **Security:** \( \tilde{R} > I(U; Z) \)
- **Reliability:** \( R + \tilde{R} < I(U; Y) \)
The Wiretap Channel

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

Message: 0010110100011100
Padding: 0100010011

Trans. together in one block

- **Codebook:** $U^n \sim Q^n_U$
- **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 & The GP Channel - Coding

**The Wiretap Channel**

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

<table>
<thead>
<tr>
<th>Message</th>
<th>Padding</th>
</tr>
</thead>
<tbody>
<tr>
<td>0010110100011100</td>
<td>0100010011</td>
</tr>
</tbody>
</table>

Trans. together in one block

- **Codebook:** \( U^n \sim Q^n_U \)
- **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.

<table>
<thead>
<tr>
<th>Message</th>
<th>Padding</th>
</tr>
</thead>
<tbody>
<tr>
<td>0010110100011100</td>
<td>0100010011</td>
</tr>
</tbody>
</table>

Trans. together in one block
The Wiretap Channel

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

Message | Padding
--- | ---
0010110100011100 | 0100010011

Trans. together in one block

- **Codebook:** $U^n \sim Q^n_U$
- **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:** $U^n \sim Q^n_U$
The Wiretap Channel

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

- **Message**: 0010110100011100
- **Padding**: 0100010011

Trans. together in one block

- **Codebook**: $U^n \sim Q^n_U$
- **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**: 0010110100011100
- **Padding**: 0100010011

Trans. together in one block

- **Codebook**: $U^n \sim Q^n_U$
- **Correlation**: $\tilde{R} > I(U; S)$
The Wiretap Channel

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

Message_padding

<table>
<thead>
<tr>
<th>Message</th>
<th>Padding</th>
</tr>
</thead>
<tbody>
<tr>
<td>001011010011100</td>
<td>0100010011</td>
</tr>
</tbody>
</table>

Trans. together in one block

- **Codebook:** $U^n \sim Q^n_U$
- **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

<table>
<thead>
<tr>
<th>Message</th>
<th>Padding</th>
</tr>
</thead>
<tbody>
<tr>
<td>001011010011100</td>
<td>0100010011</td>
</tr>
</tbody>
</table>

Trans. together in one block

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