Cooperative Broadcast Channels with a Secret Message

Ziv Goldfeld, Gerhard Kramer and Haim H. Permuter
Joint work with Paul Cuff

Ben Gurion University, Technische Universität München and Princeton University

IEEE International Symposium on Information Theory

June, 2015

Outline

- Motivation
- Channel resolvability for strong-secrecy in Marton codes
- Cooperative BCs with a confidential message
- Strong-secrecy-capacity results
- Summary

Motivation - Combining Secrecy and Cooperation

- Two important aspects of communication today.

Motivation - Combining Secrecy and Cooperation

- Two important aspects of communication today.
- Secrecy constraints limit viable cooperation protocols.

Motivation - Combining Secrecy and Cooperation

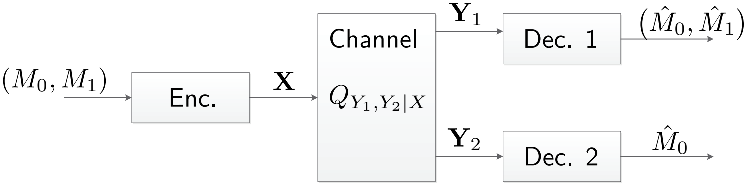
- Two important aspects of communication today.
- Secrecy constraints limit viable cooperation protocols.
- Help while concealing.

Combining Secrecy and Cooperation - Simple Example

BCs with Degraded Message Set [Körner & Marton, 1977]:

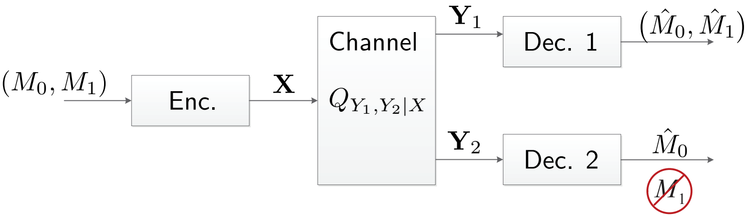
Combining Secrecy and Cooperation - Simple Example

BCs with Degraded Message Set [Körner & Marton, 1977]:



Combining Secrecy and Cooperation - Simple Example

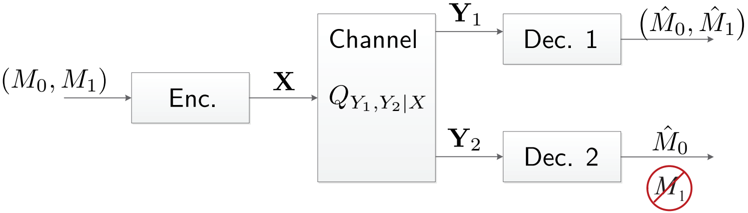
BCs with Degraded Message Set [Körner & Marton, 1977]:



- **Strong-secrecy M_1 (no cooperation):** $I(M_1; \mathbf{Y}_2) \to 0$

Combining Secrecy and Cooperation - Simple Example

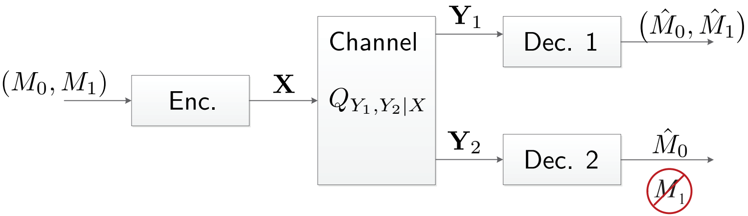
BCs with Degraded Message Set [Körner & Marton, 1977]:



- **Strong-secrecy M_1 (no cooperation):** $I(M_1; \mathbf{Y}_2) \to 0$ ✓

Combining Secrecy and Cooperation - Simple Example

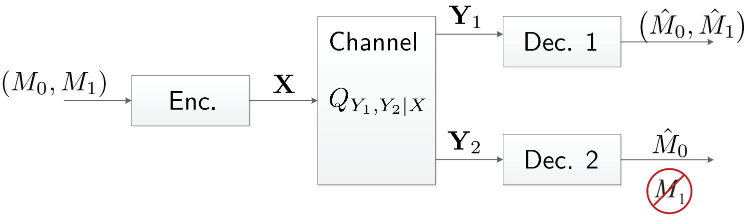
BCs with Degraded Message Set [Körner & Marton, 1977]:



- **Strong-secrecy M_1 (no cooperation):** $I(M_1; \mathbf{Y}_2) \to 0$ ✓
  [Bloch & Laneman, 2013], [Hou & Kramer, 2014]

Combining Secrecy and Cooperation - Simple Example

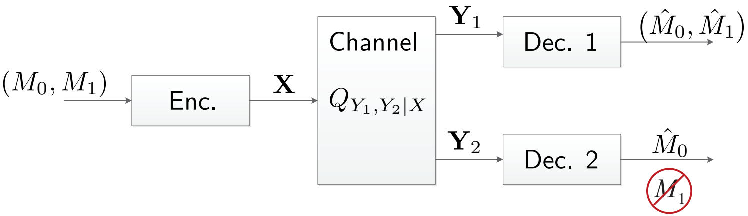
BCs with Degraded Message Set [Körner & Marton, 1977]:



- **Strong-secrecy M_1 (no cooperation):** $I(M_1; \mathbf{Y}_2) \to 0$ ✓ [Bloch & Laneman, 2013], [Hou & Kramer, 2014]
  - Channel-resolvability superposition code:

Combining Secrecy and Cooperation - Simple Example

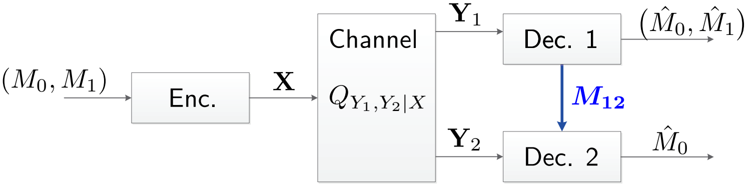
BCs with Degraded Message Set [Körner & Marton, 1977]:



- **Strong-secrecy M_1 (no cooperation):** $I(M_1; \mathbf{Y}_2) \to 0$ ✓
  [Bloch & Laneman, 2013], [Hou & Kramer, 2014]
  - Channel-resolvability superposition code: Conceal outer (M_1) layer

Combining Secrecy and Cooperation - Simple Example

BCs with Degraded Message Set [Körner & Marton, 1977]:

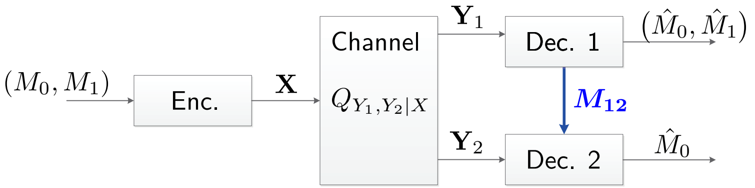


- Strong-secrecy M_1 (no cooperation): $I(M_1; \mathbf{Y}_2) \to 0$ ✓
  [Bloch & Laneman, 2013], [Hou & Kramer, 2014]
  - Channel-resolvability superposition code: Conceal outer (M_1) layer

- **Partially cooperative decoders (no secrecy)**

Combining Secrecy and Cooperation - Simple Example

BCs with Degraded Message Set [Körner & Marton, 1977]:

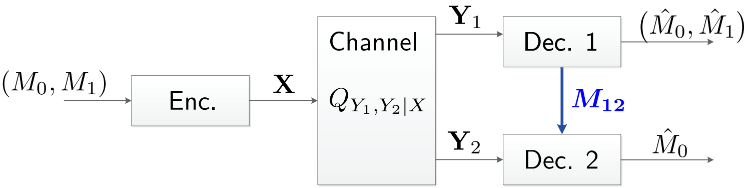


- Strong-secrecy M_1 (no cooperation): $I(M_1; \mathbf{Y}_2) \to 0$ ✓
  [Bloch & Laneman, 2013], [Hou & Kramer, 2014]
  - Channel-resolvability superposition code: Conceal outer (M_1) layer

- **Partially cooperative decoders (no secrecy)** ✓

Combining Secrecy and Cooperation - Simple Example

BCs with Degraded Message Set [Körner & Marton, 1977]:

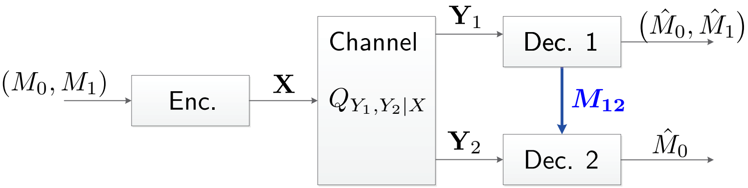


- Strong-secrecy M_1 (no cooperation): $I(M_1; \mathbf{Y}_2) \to 0$ ✓
  [Bloch & Laneman, 2013], [Hou & Kramer, 2014]
  - Channel-resolvability superposition code: Conceal outer (M_1) layer

- **Partially cooperative decoders (no secrecy)** ✓
  [Liang & Kramer, 2007], [Steinberg, 2015]

Combining Secrecy and Cooperation - Simple Example

BCs with Degraded Message Set [Körner & Marton, 1977]:

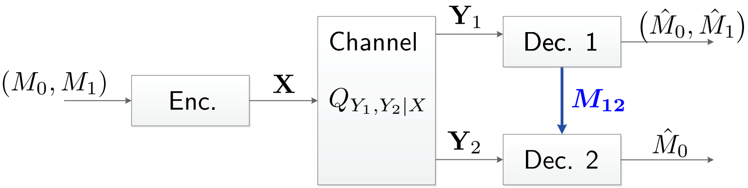


- Strong-secrecy M_1 (no cooperation): $I(M_1; \mathbf{Y}_2) \to 0$ ✓
  [Bloch & Laneman, 2013], [Hou & Kramer, 2014]
  - Channel-resolvability superposition code: Conceal outer (M_1) layer

- **Partially cooperative decoders (no secrecy)** ✓
  [Liang & Kramer, 2007], [Steinberg, 2015]
  - Superposition code:

Combining Secrecy and Cooperation - Simple Example

BCs with Degraded Message Set [Körner & Marton, 1977]:

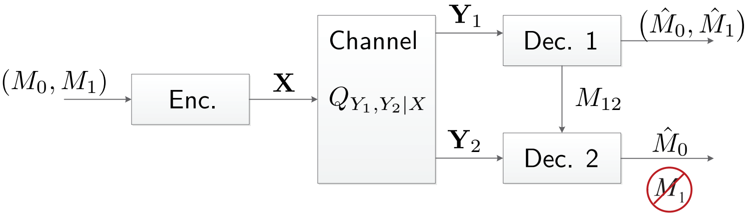


- Strong-secrecy M_1 (no cooperation): $I(M_1; \mathbf{Y}_2) \to 0$ ✓
  [Bloch & Laneman, 2013], [Hou & Kramer, 2014]
  - Channel-resolvability superposition code: Conceal outer (M_1) layer

- **Partially cooperative decoders (no secrecy)** ✓
  [Liang & Kramer, 2007], [Steinberg, 2015]
  - Superposition code: Bin inner (M_0) layer and share #bin.

Combining Secrecy and Cooperation - Simple Example

BCs with Degraded Message Set [Körner & Marton, 1977]:



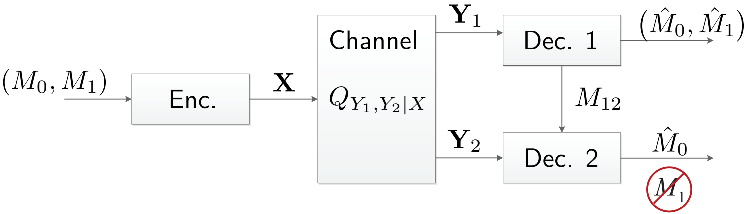
- Strong-secrecy M_1 (no cooperation): $I(M_1; \mathbf{Y}_2) \to 0$ ✓
  [Bloch & Laneman, 2013], [Hou & Kramer, 2014]
  - Channel-resolvability superposition code: Conceal outer (M_1) layer

- Partially cooperative decoders (no secrecy) ✓
  [Liang & Kramer, 2007], [Steinberg, 2015]
  - Superposition code: Bin inner (M_0) layer and share #bin.

Q: How to optimally combine secrecy and cooperation?

Combining Secrecy and Cooperation - Simple Example

BCs with Degraded Message Set [Körner & Marton, 1977]:

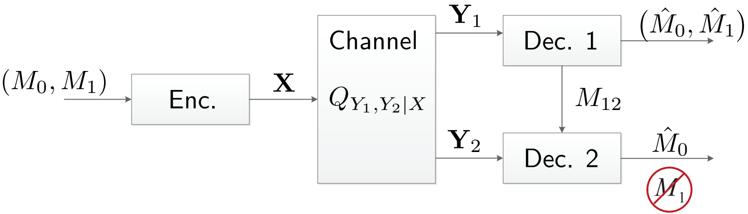


- Strong-secrecy M_1 (no cooperation): $I(M_1; \mathbf{Y}_2) \to 0$ ✓
  [Bloch & Laneman, 2013], [Hou & Kramer, 2014]
  - Channel-resolvability superposition code: Conceal outer (M_1) layer
- Partially cooperative decoders (no secrecy) ✓
  [Liang & Kramer, 2007], [Steinberg, 2015]
  - Superposition code: Bin inner (M_0) layer and share #bin.

Q: How to optimally combine secrecy and cooperation? Trivial!

Combining Secrecy and Cooperation - Simple Example

BCs with Degraded Message Set [Körner & Marton, 1977]:



- Strong-secrecy M_1 (no cooperation): $I(M_1; \mathbf{Y}_2) \to 0$ ✓
  [Bloch & Laneman, 2013], [Hou & Kramer, 2014]
  - Channel-resolvability superposition code: Conceal outer (M_1) layer

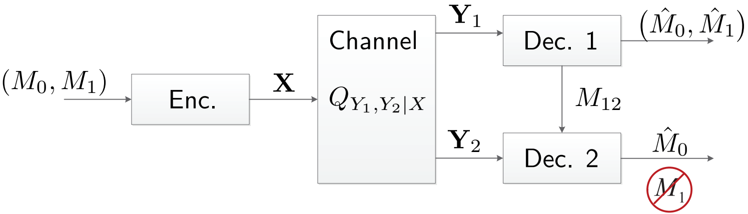
- Partially cooperative decoders (no secrecy) ✓
  [Liang & Kramer, 2007], [Steinberg, 2015]
  - Superposition code: Bin inner (M_0) layer and share #bin.

Q: How to optimally combine secrecy and cooperation? Trivial!

- Both use superposition code.

Combining Secrecy and Cooperation - Simple Example

BCs with Degraded Message Set [Körner & Marton, 1977]:



- Strong-secrecy M_1 (no cooperation): $I(M_1; \mathbf{Y}_2) \to 0$ ✓
  [Bloch & Laneman, 2013], [Hou & Kramer, 2014]
  - Channel-resolvability superposition code: Conceal outer (M_1) layer

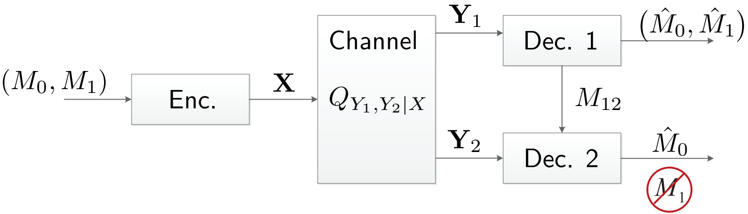
- Partially cooperative decoders (no secrecy) ✓
  [Liang & Kramer, 2007], [Steinberg, 2015]
  - Superposition code: Bin inner (M_0) layer and share #bin.

Q: How to optimally combine secrecy and cooperation? Trivial!

- Both use superposition code.
- No collision

Combining Secrecy and Cooperation - Simple Example

BCs with Degraded Message Set [Körner & Marton, 1977]:

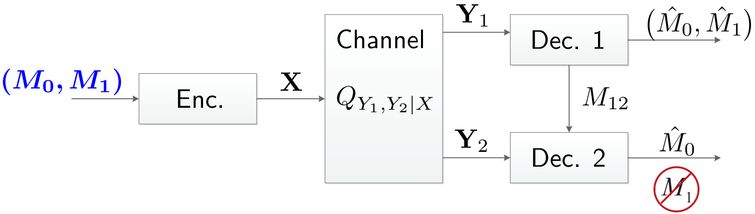


- Strong-secrecy M_1 (no cooperation): $I(M_1; \mathbf{Y}_2) \to 0$ ✓
  [Bloch & Laneman, 2013], [Hou & Kramer, 2014]
  - Channel-resolvability superposition code: Conceal outer (M_1) layer
- Partially cooperative decoders (no secrecy) ✓
  [Liang & Kramer, 2007], [Steinberg, 2015]
  - Superposition code: Bin inner (M_0) layer and share #bin.

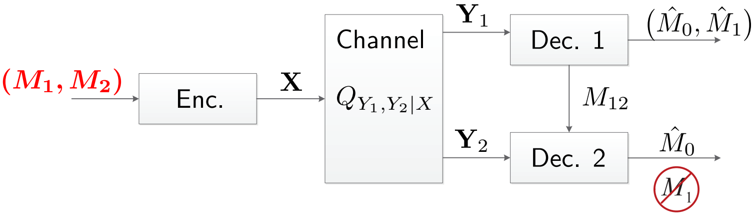
Q: How to optimally combine secrecy and cooperation? Trivial!

- Both use superposition code.
- No collision $\Longrightarrow$ No tradeoff.

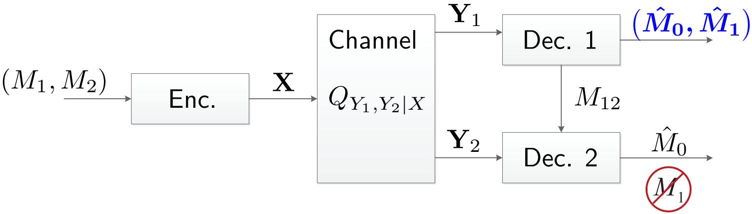
Cooperative BCs with a Confidential Message - Definition



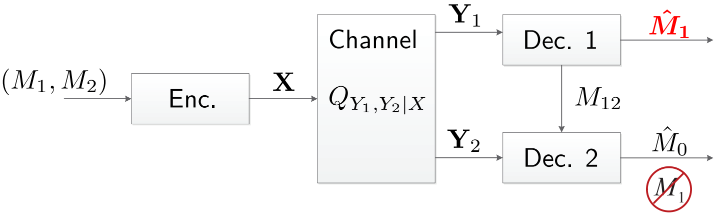
Cooperative BCs with a Confidential Message - Definition



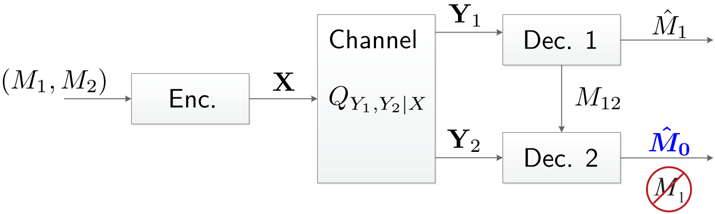
Cooperative BCs with a Confidential Message - Definition



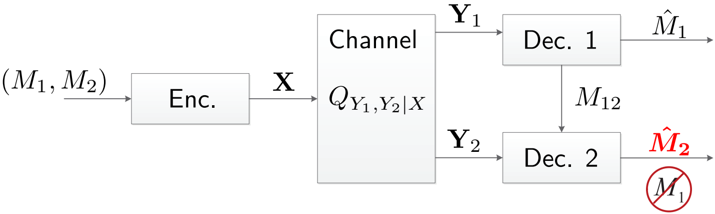
Cooperative BCs with a Confidential Message - Definition



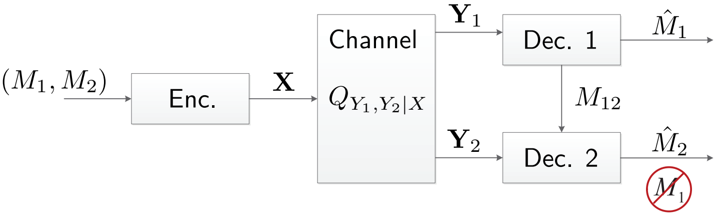
Cooperative BCs with a Confidential Message - Definition



Cooperative BCs with a Confidential Message - Definition

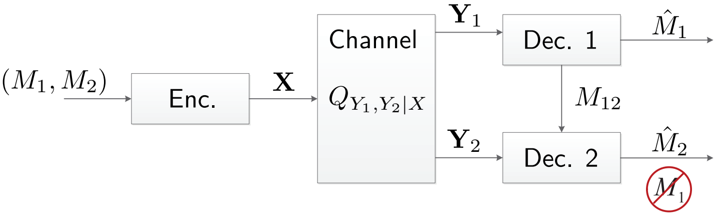


Cooperative BCs with a Confidential Message - Definition



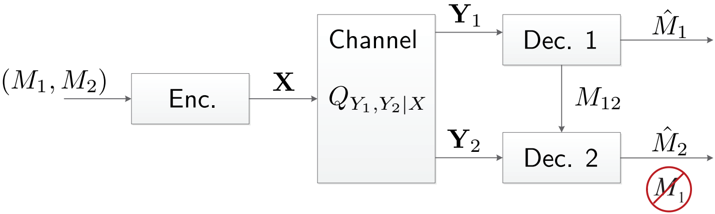
- **Best coding (no secrecy):** [ZG & Permuter & Kramer, 2013]

Cooperative BCs with a Confidential Message - Definition



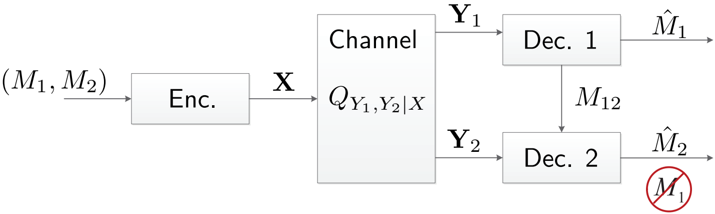
- **Best coding (no secrecy):** [ZG & Permuter & Kramer, 2013]
  - **Message Splitting:** $(M_1, M_2) \rightarrow \big((M_{10}, M_{20}), M_{11}, M_{22}\big)$.

Cooperative BCs with a Confidential Message - Definition



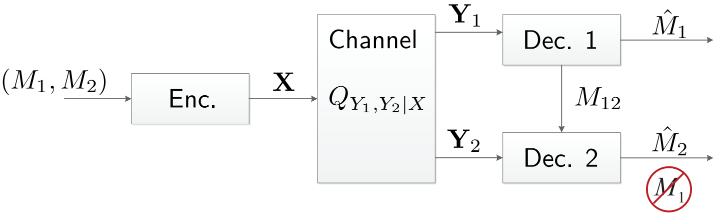
- **Best coding (no secrecy):** [ZG & Permuter & Kramer, 2013]
  - **Message Splitting:** $(M_1, M_2) \to \big((M_{10}, M_{20}), M_{11}, M_{22}\big)$.
  - **Coding:** Marton with common message.

Cooperative BCs with a Confidential Message - Definition



- **Best coding (no secrecy):** [ZG & Permuter & Kramer, 2013]
  - **Message Splitting:** $(M_1, M_2) \rightarrow \big((M_{10}, M_{20}), M_{11}, M_{22}\big)$.
  - **Coding:** Marton with common message.
  - **Cooperation Protocol:** Bin (M_{10}, M_{20})-codebook and convey #bin.

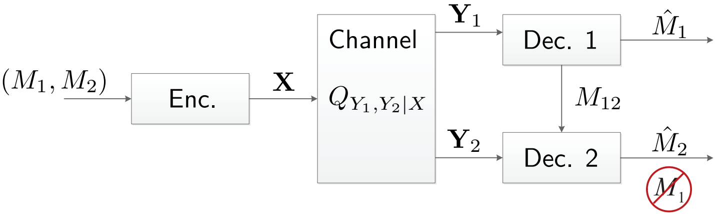
Cooperative BCs with a Confidential Message - Definition



- **Best coding (no secrecy):** [ZG & Permuter & Kramer, 2013]
  - **Message Splitting:** $(M_1, M_2) \to \big((M_{10}, M_{20}), M_{11}, M_{22}\big)$.
  - **Coding:** Marton with common message.
  - **Cooperation Protocol:** Bin (M_{10}, M_{20})-codebook and convey #bin.

- M_1 **is secret:** No sharing information about M_1!

Cooperative BCs with a Confidential Message - Definition

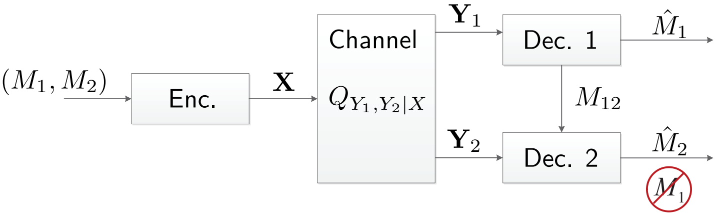


- **Best coding (no secrecy):** [ZG & Permuter & Kramer, 2013]
  - **Message Splitting:** $(M_1, M_2) \to \big((M_{10}, M_{20}), M_{11}, M_{22}\big)$.
  - **Coding:** Marton with common message.
  - **Cooperation Protocol:** Bin (M_{10}, M_{20})-codebook and convey #bin.

- $\boldsymbol{M_1}$ **is secret:** No sharing information about M_1!

⋆ Modify code construction and/or cooperation protocol ⋆

Cooperative BCs with a Confidential Message - Definition



- **Best coding (no secrecy):** [ZG & Permuter & Kramer, 2013]
  - **Message Splitting:** $(M_1, M_2) \to \big((M_{10}, M_{20}), M_{11}, M_{22}\big)$.
  - **Coding:** Marton with common message.
  - **Cooperation Protocol:** Bin (M_{10}, M_{20})-codebook and convey #bin.

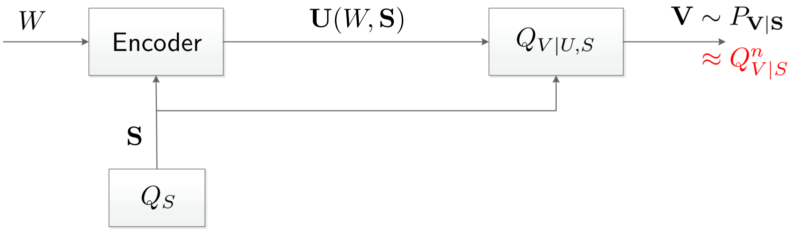
- ***M_1* is secret:** No sharing information about M_1!

⋆ Modify code construction and/or cooperation protocol ⋆

⋆ Strong-secrecy for Marton codes (superposing & multi-coding) ⋆

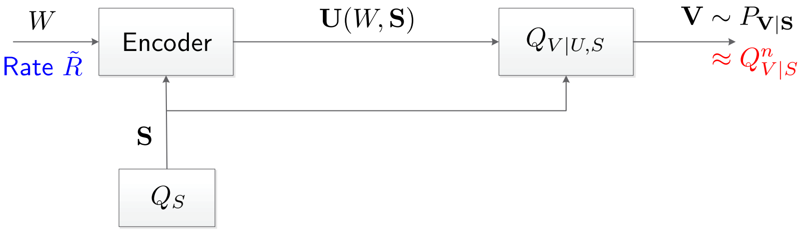
Channel Resolvability and Multi-coding (Simplified)

Classic Case - PTP codebook [Wyner, 1975], [Han & Verdú, 1993]



Channel Resolvability and Multi-coding (Simplified)

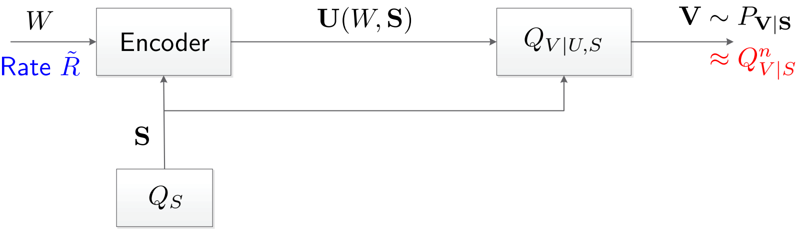
Classic Case - PTP codebook [Wyner, 1975], [Han & Verdú, 1993]



- **Message:** $W \sim$ Unif$[1 : 2^{n\tilde{R}}]$.

Channel Resolvability and Multi-coding (Simplified)

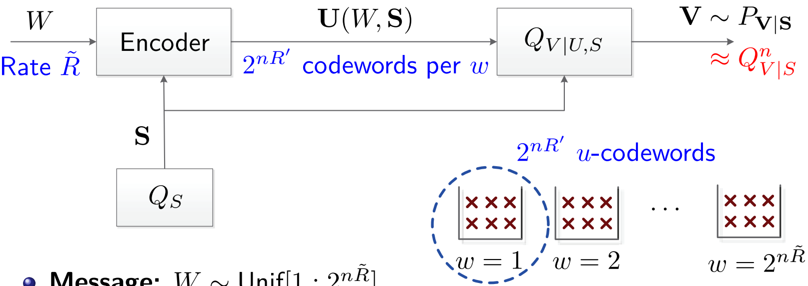
Classic Case - PTP codebook [Wyner, 1975], [Han & Verdú, 1993]



- **Message:** $W \sim$ Unif$[1:2^{n\tilde{R}}]$.
- **Codebook:** $\mathbb{C}_n = \left\{\mathbf{U}(w,i)\right\}$ i.i.d. $\sim Q_U$, $i \in [1:2^{nR'}]$.

Channel Resolvability and Multi-coding (Simplified)

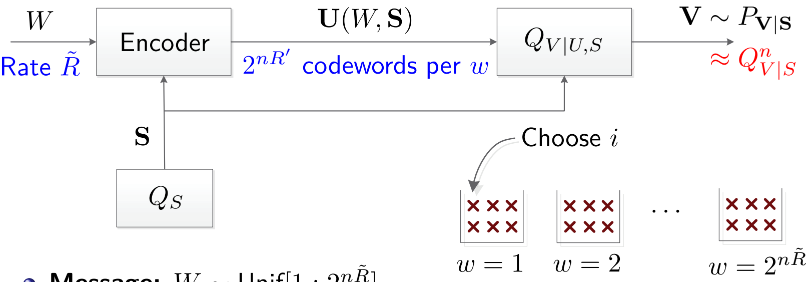
Classic Case - PTP codebook [Wyner, 1975], [Han & Verdú, 1993]



- **Message:** $W \sim \text{Unif}[1 : 2^{n\tilde{R}}]$.
- **Codebook:** $\mathbb{C}_n = \big\{\mathbf{U}(w,i)\big\}$ i.i.d. $\sim Q_U$, $i \in [1 : 2^{nR'}]$.

Channel Resolvability and Multi-coding (Simplified)

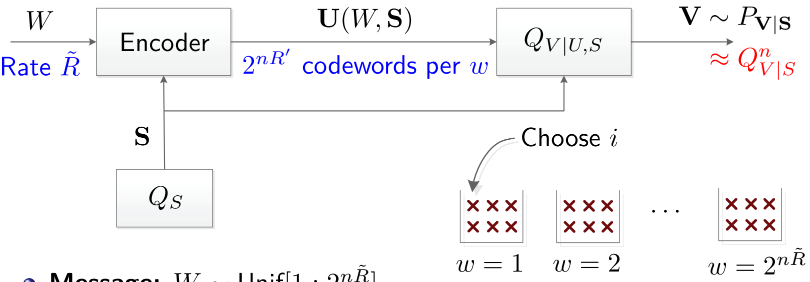
Classic Case - PTP codebook [Wyner, 1975], [Han & Verdú, 1993]



- **Message:** $W \sim \text{Unif}[1:2^{n\tilde{R}}]$.
- **Codebook:** $\mathbb{C}_n = \{\mathbf{U}(w,i)\}$ i.i.d. $\sim Q_U$, $i \in [1:2^{nR'}]$.
- **Encoding:** Likelihood encoder [Song & Cuff & Poor, 2014] choose i

Channel Resolvability and Multi-coding (Simplified)

Classic Case - PTP codebook [Wyner, 1975], [Han & Verdú, 1993]

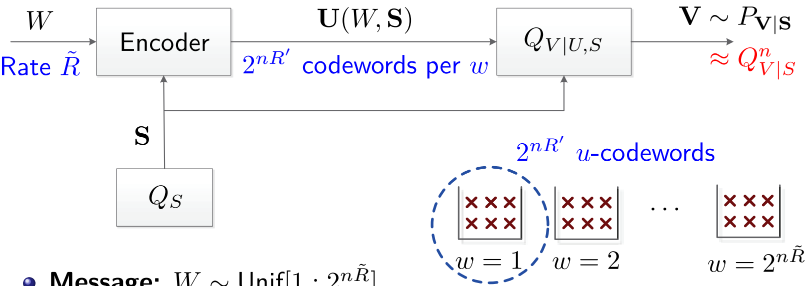


- **Message:** $W \sim$ Unif$[1:2^{n\tilde{R}}]$.
- **Codebook:** $\mathbb{C}_n = \big\{\mathbf{U}(w,i)\big\}$ i.i.d. $\sim Q_U$, $i \in [1:2^{nR'}]$.
- **Encoding:** Likelihood encoder [Song & Cuff & Poor, 2014] choose i

$$P^{(LE)}(i|w,\mathbf{s},\mathcal{C}_n) = \frac{Q^n_{S|U}\big(\mathbf{s}\big|\mathbf{u}(w,i,\mathcal{C}_n)\big)}{\sum_{i'\in\mathcal{I}} Q^n_{S|U}\big(\mathbf{s}\big|\mathbf{u}(w,i',\mathcal{C}_n)\big)}.$$

Channel Resolvability and Multi-coding (Simplified)

Classic Case - PTP codebook [Wyner, 1975], [Han & Verdú, 1993]

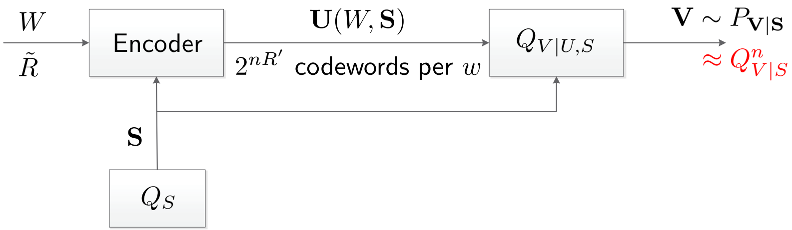


- **Message:** $W \sim \text{Unif}[1:2^{n\tilde{R}}]$.
- **Codebook:** $\mathbb{C}_n = \left\{\mathbf{U}(w,i)\right\}$ i.i.d. $\sim Q_U$, $i \in [1:2^{nR'}]$.
- **Encoding:** Likelihood encoder [Song & Cuff & Poor, 2014] choose i

$$P^{(LE)}(i|w,\mathbf{s},\mathcal{C}_n) = \frac{Q^n_{S|U}\big(\mathbf{s}\big|\mathbf{u}(w,i,\mathcal{C}_n)\big)}{\sum_{i'\in\mathcal{I}} Q^n_{S|U}\big(\mathbf{s}\big|\mathbf{u}(w,i',\mathcal{C}_n)\big)}.$$

- **Goal:** Choose $(\tilde{R}, R')$ s.t. $\mathbb{E}_{\mathbb{C}_n}\Big[D\big(P_{\mathbf{V}|\mathbf{S},\mathbb{C}_n}\big|\big|Q^n_{V|S}\big|Q^n_S\big)\Big] \to 0$.

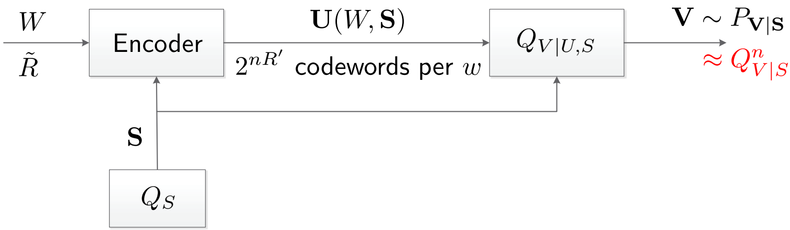
Channel Resolvability and Multi-coding (Simplified)



Theorem (Direct Part)

$$\begin{aligned} R' &> I(S;U) \\ R' + \tilde{R} &> I(U;S,V) \end{aligned} \quad \Longrightarrow \quad \mathbb{E}_{\mathbb{C}_n}\left[D\left(P_{\mathbf{V}|\mathbf{S},\mathbb{C}_n}\middle|\middle|Q^n_{V|S}\middle|Q^n_S\right)\right] \to 0$$

Channel Resolvability and Multi-coding (Simplified)

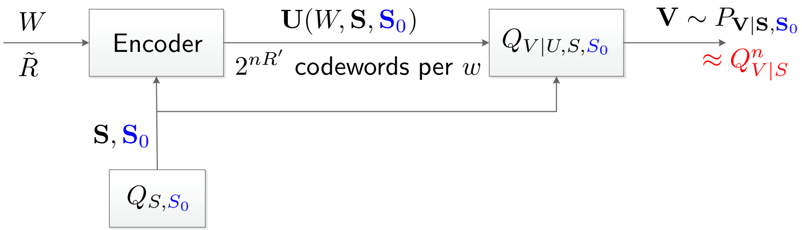


Theorem (Direct Part)

$$\begin{matrix} R' > I(S;U) \\ R' + \tilde{R} > I(U;S,V) \end{matrix} \implies \mathbb{E}_{\mathbb{C}_n}\left[D\left(P_{\mathbf{V}|\mathbf{S},\mathbb{C}_n}\middle|\middle|Q^n_{V|S}\middle|Q^n_S\right)\right] \to 0$$

- When **superposing** on $\mathbf{S}_0$:

Channel Resolvability and Multi-coding (Simplified)

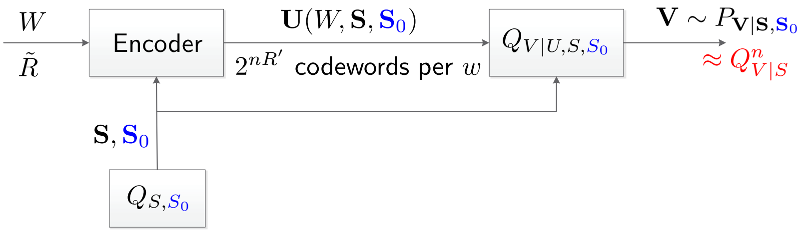


Theorem (Direct Part)

$$\begin{aligned} R' &> I(S;U) \\ R' + \tilde{R} &> I(U;S,V) \end{aligned} \implies \mathbb{E}_{\mathbb{C}_n}\Big[D\big(P_{\mathbf{V}|\mathbf{S},\mathbb{C}_n}\big|\big|Q^n_{V|S}\big|Q^n_S\big)\Big] \to 0$$

- When **superposing** on $\mathbf{S}_0$:

Channel Resolvability and Multi-coding (Simplified)



Theorem (Direct Part)

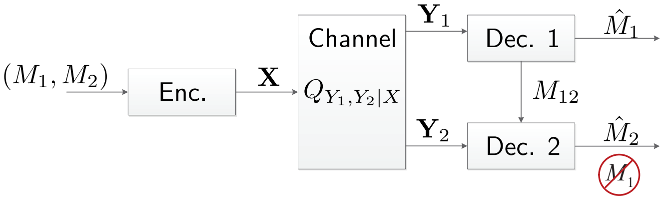
$$\begin{array}{r} R' > I(S;U) \\ R' + \tilde{R} > I(U;S,V) \end{array} \implies \mathbb{E}_{\mathbb{C}_n}\left[D\left(P_{\mathbf{V}|\mathbf{S},\mathbb{C}_n}||Q^n_{V|S}|Q^n_S\right)\right] \to 0$$

- When **superposing** on $\mathbf{S}_0$:

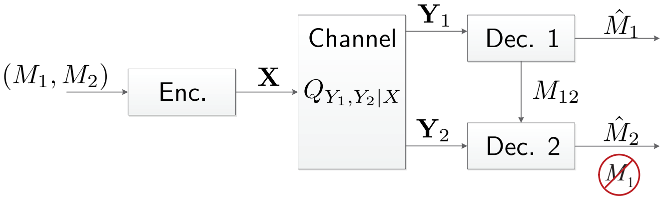
Theorem (Direct Part with Superposing)

$$\begin{array}{r} R' > I(S;U|S_0) \\ R' + \tilde{R} > I(U;S,V|S_0) \end{array} \implies \mathbb{E}_{\mathbb{C}_n}\left[D\left(P_{\mathbf{V}|\mathbf{S},\mathbf{S}_0,\mathbb{C}_n}||Q^n_{V|S,S_0}|Q^n_{S,S_0}\right)\right] \to 0$$

Cooperative BCs with a Confidential Message

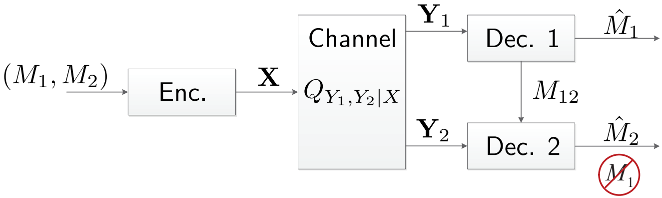


Cooperative BCs with a Confidential Message



Strong-Secrecy: $I(M_1; M_{12}, \mathbf{Y}_2) \to 0.$

Cooperative BCs with a Confidential Message



Strong-Secrecy: $I(M_1; M_{12}, \mathbf{Y}_2) \to 0.$

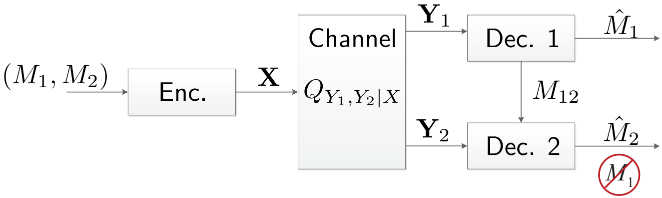
Theorem (Inner Bound)

An inner bound on the strong-secrecy-capacity region is:

$$\mathcal{R}_I = \bigcup \left\{ \begin{array}{r} R_1 \leq I(U_1;Y_1|U_0) - I(U_1;U_2|U_0) - I(U_1;Y_2|U_0,U_2) \\ R_2 \leq I(U_0,U_2;Y_2) + R_{12} \\ R_1 + R_2 \leq I(U_0,U_1;Y_1) - I(U_1;U_2|U_0) - I(U_1;Y_2|U_0,U_2) \\ +I(U_2;Y_2|U_0) \end{array} \right\}$$

where the union is over all $Q_{U_0,U_1,U_2,X}Q_{Y_1,Y_2|X}$.

Cooperative BCs with a Confidential Message



Strong-Secrecy: $I(M_1; M_{12}, \mathbf{Y}_2) \to 0.$

Theorem (Inner Bound)

An inner bound on the strong-secrecy-capacity region is:

$$\mathcal{R}_I = \bigcup \left\{ \begin{array}{r} R_1 \leq I(U_1;Y_1|U_0) - I(U_1;U_2|U_0) - I(U_1;Y_2|U_0,U_2) \\ R_2 \leq I(U_0,U_2;Y_2) + R_{12} \\ R_1 + R_2 \leq I(U_0,U_1;Y_1) - I(U_1;U_2|U_0) - I(U_1;Y_2|U_0,U_2) \\ +I(U_2;Y_2|U_0) \end{array} \right\}$$

where the union is over all $Q_{U_0,U_1,U_2,X}Q_{Y_1,Y_2|X}$.

⋆ Extension to common+private messages ⋆

Inner Bound - Proof Outline

- **Messages:** $M_2 = (M_{20}, M_{22})$.

Inner Bound - Proof Outline

- **Messages:** $M_2 = (M_{20}, M_{22})$.
  - M_{20} - Common message;

Inner Bound - Proof Outline

- **Messages:** $M_2 = (M_{20}, M_{22})$.
  - M_{20} - Common message;
  - (M_1, M_{22}) - Private messages.

Inner Bound - Proof Outline

- **Messages:** $M_2 = (M_{20}, M_{22})$.
  - M_{20} - Common message;
  - (M_1, M_{22}) - Private messages.
  - $W \sim$ Unif$[1 : 2^{n\tilde{R}}]$ - Randomizer.

Inner Bound - Proof Outline

- **Messages:** $M_2 = (M_{20}, M_{22})$.
  - M_{20} - Common message;
  - (M_1, M_{22}) - Private messages.
  - $W \sim \text{Unif}[1 : 2^{n\tilde{R}}]$ - Randomizer.
- **Encoding:**

Inner Bound - Proof Outline

- **Messages:** $M_2 = (M_{20}, M_{22})$.
  - M_{20} - Common message;
  - (M_1, M_{22}) - Private messages.
  - $W \sim$ Unif$[1 : 2^{n\tilde{R}}]$ - Randomizer.

- **Encoding:**
  1. $M_{20} \longrightarrow \mathbf{U}_0 \sim Q^n_{U_0}$.

Inner Bound - Proof Outline

- **Messages:** $M_2 = (M_{20}, M_{22})$.
  - M_{20} - Common message;
  - (M_1, M_{22}) - Private messages.
  - $W \sim \text{Unif}[1 : 2^{n\tilde{R}}]$ - Randomizer.

- **Encoding:**
  1. $M_{20} \longrightarrow \mathbf{U}_0 \sim Q^n_{U_0}$.
  2. $M_{22} \longrightarrow \mathbf{U}_2 \sim Q^n_{U_2|U_0}$.

Inner Bound - Proof Outline

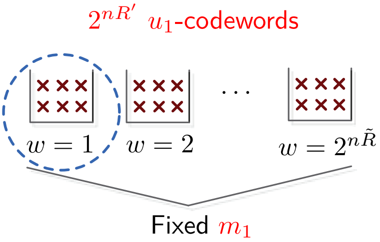
- **Messages:** $M_2 = (M_{20}, M_{22})$.
  - M_{20} - Common message;
  - (M_1, M_{22}) - Private messages.
  - $W \sim \text{Unif}[1 : 2^{n\tilde{R}}]$ - Randomizer.

- **Encoding:**
  1. $M_{20} \longrightarrow \mathbf{U}_0 \sim Q^n_{U_0}$.
  2. $M_{22} \longrightarrow \mathbf{U}_2 \sim Q^n_{U_2|U_0}$.
  3. $M_1 \longrightarrow$ Resolvability codebook.

Inner Bound - Proof Outline

- **Messages:** $M_2 = (M_{20}, M_{22})$.
  - M_{20} - Common message;
  - (M_1, M_{22}) - Private messages.
  - $W \sim \text{Unif}[1 : 2^{n\tilde{R}}]$ - Randomizer.

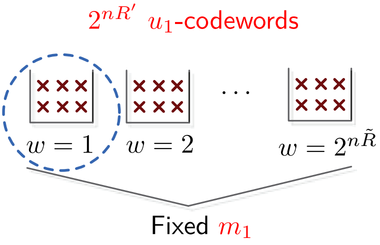
- **Encoding:**
  1. $M_{20} \longrightarrow \mathbf{U}_0 \sim Q^n_{U_0}$.
  2. $M_{22} \longrightarrow \mathbf{U}_2 \sim Q^n_{U_2|U_0}$.
  3. $M_1 \longrightarrow$ Resolvability codebook.



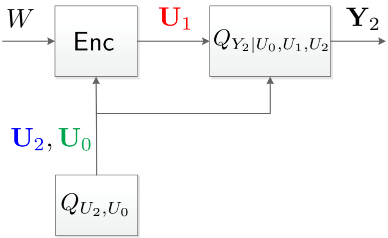
Inner Bound - Proof Outline

- **Messages:** $M_2 = (M_{20}, M_{22})$.
  - M_{20} - Common message;
  - (M_1, M_{22}) - Private messages.
  - $W \sim \text{Unif}[1 : 2^{n\tilde{R}}]$ - Randomizer.

- **Encoding:**
  1. $M_{20} \longrightarrow \mathbf{U}_0 \sim Q^n_{U_0}$.
  2. $M_{22} \longrightarrow \mathbf{U}_2 \sim Q^n_{U_2|U_0}$.
  3. $M_1 \longrightarrow$ Resolvability codebook.



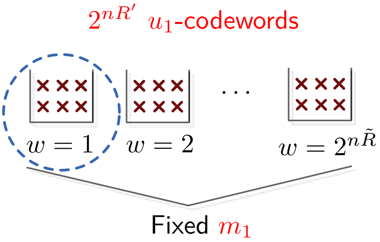
Fixed (m_{20}, m_{22}, m_1)

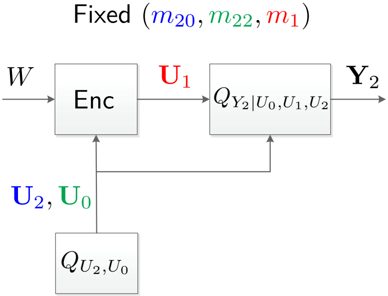


Inner Bound - Proof Outline

- **Messages:** $M_2 = (M_{20}, M_{22})$.
  - M_{20} - Common message;
  - (M_1, M_{22}) - Private messages.
  - $W \sim \text{Unif}[1 : 2^{n\tilde{R}}]$ - Randomizer.

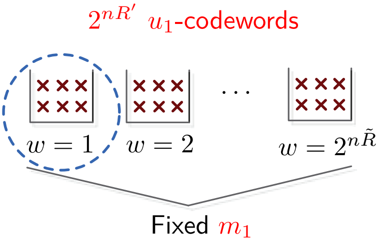
- **Encoding:**
  1. $M_{20} \longrightarrow \mathbf{U}_0 \sim Q^n_{U_0}$.
  2. $M_{22} \longrightarrow \mathbf{U}_2 \sim Q^n_{U_2|U_0}$.
  3. $M_1 \longrightarrow$ Resolvability codebook.
     - Choose $\mathbf{U}_1$ - The likelihood encoder.





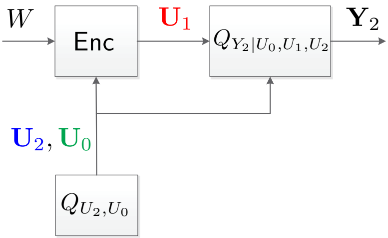
Inner Bound - Proof Outline

- **Messages:** $M_2 = (M_{20}, M_{22})$.
  - M_{20} - Common message;
  - (M_1, M_{22}) - Private messages.
  - $W \sim \text{Unif}[1:2^{n\tilde{R}}]$ - Randomizer.



- **Encoding:**
  1. $M_{20} \longrightarrow \mathbf{U}_0 \sim Q^n_{U_0}$.
  2. $M_{22} \longrightarrow \mathbf{U}_2 \sim Q^n_{U_2|U_0}$.
  3. $M_1 \longrightarrow$ Resolvability codebook.
     - Choose $\mathbf{U}_1$ - The likelihood encoder.

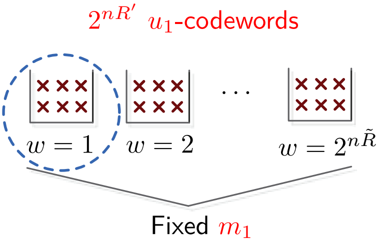
Fixed (m_{20}, m_{22}, m_1)



- **Cooperation:**

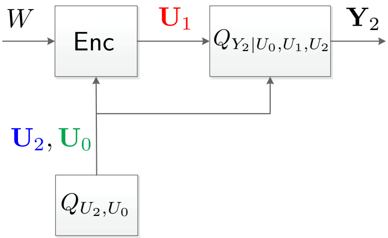
Inner Bound - Proof Outline

- **Messages:** $M_2 = (M_{20}, M_{22})$.
  - M_{20} - Common message;
  - (M_1, M_{22}) - Private messages.
  - $W \sim \text{Unif}[1 : 2^{n\tilde{R}}]$ - Randomizer.



- **Encoding:**
  1. $M_{20} \longrightarrow \mathbf{U}_0 \sim Q^n_{U_0}$.
  2. $M_{22} \longrightarrow \mathbf{U}_2 \sim Q^n_{U_2|U_0}$.
  3. $M_1 \longrightarrow$ Resolvability codebook.
     - Choose $\mathbf{U}_1$ - The likelihood encoder.

Fixed (m_{20}, m_{22}, m_1)



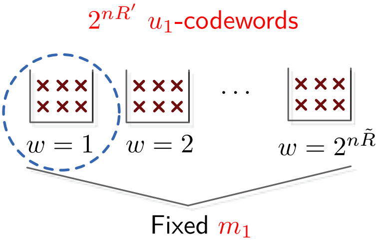
- **Cooperation:**
  1. Bin M_{20} codebook into $2^{nR_{12}}$ bins.

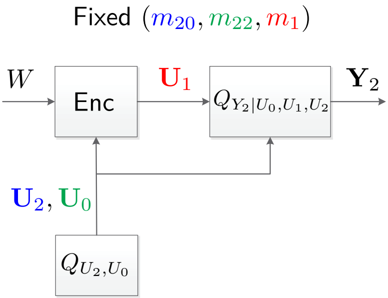
Inner Bound - Proof Outline

- **Messages:** $M_2 = (M_{20}, M_{22})$.
  - M_{20} - Common message;
  - (M_1, M_{22}) - Private messages.
  - $W \sim$ Unif$[1:2^{n\tilde{R}}]$ - Randomizer.

- **Encoding:**
  1. $M_{20} \longrightarrow \mathbf{U}_0 \sim Q^n_{U_0}$.
  2. $M_{22} \longrightarrow \mathbf{U}_2 \sim Q^n_{U_2|U_0}$.
  3. $M_1 \longrightarrow$ Resolvability codebook.
     - Choose $\mathbf{U}_1$ - The likelihood encoder.

- **Cooperation:**
  1. Bin M_{20} codebook into $2^{nR_{12}}$ bins.
  2. Convey bin number via link.





Inner Bound - Proof Outline

Key Arguments:

Inner Bound - Proof Outline

Key Arguments:

- **Likelihood encoder induced encoding error:**

Inner Bound - Proof Outline

Key Arguments:

- **Likelihood encoder induced encoding error:** The chosen u_0-, u_1-, u_2-codewords are jointly ϵ-typical with high probability.

Inner Bound - Proof Outline

Key Arguments:

- **Likelihood encoder induced encoding error:** The chosen u_0-, u_1-, u_2-codewords are jointly ϵ-typical with high probability.
- **Strong-secrecy via channel resolvability:**

Inner Bound - Proof Outline

Key Arguments:

- **Likelihood encoder induced encoding error:** The chosen u_0-, u_1-, u_2-codewords are jointly ϵ-typical with high probability.

- **Strong-secrecy via channel resolvability:**

  $I(M_1; M_{12}, \mathbf{Y}_2 | \mathbb{C})$

Inner Bound - Proof Outline

Key Arguments:

- **Likelihood encoder induced encoding error:** The chosen u_0-, u_1-, u_2-codewords are jointly ϵ-typical with high probability.
- **Strong-secrecy via channel resolvability:**

$$I(M_1; M_{12}, \mathbf{Y}_2|\mathbb{C}) \leq \mathbb{E}_{\mathbb{C}}\left[D\left(P_{\mathbf{Y}_2|M_1=1,M_2=1,\mathbf{U}_0,\mathbf{U}_2,\mathbb{C}}\middle|\middle|Q^n_{Y_2|U_0,U_2}\middle|Q^n_{U_0,U_2}\right)\right]$$

Inner Bound - Proof Outline

Key Arguments:

- **Likelihood encoder induced encoding error:** The chosen u_0-, u_1-, u_2-codewords are jointly ϵ-typical with high probability.
- **Strong-secrecy via channel resolvability:**

$$I(M_1; M_{12}, \mathbf{Y}_2 | \mathbb{C}) \leq \mathbb{E}_{\mathbb{C}}\left[D\big(P_{\mathbf{Y}_2|M_1=1,M_2=1,\mathbf{U}_0,\mathbf{U}_2,\mathbb{C}} \big|\big| Q^n_{Y_2|U_0,U_2} \big| Q^n_{U_0,U_2}\big)\right]$$

⋆ A channel resolvability problem w.r.t. W! ⋆

Inner Bound - Proof Outline

Key Arguments:

- **Likelihood encoder induced encoding error:** The chosen u_0-, u_1-, u_2-codewords are jointly ϵ-typical with high probability.
- **Strong-secrecy via channel resolvability:**

$$I(M_1; M_{12}, \mathbf{Y}_2|\mathbb{C}) \leq \mathbb{E}_{\mathbb{C}}\Big[D\Big(P_{\mathbf{Y}_2|M_1=1,M_2=1,\mathbf{U}_0,\mathbf{U}_2,\mathbb{C}}\Big|\Big|Q^n_{Y_2|U_0,U_2}\Big|Q^n_{U_0,U_2}\Big)\Big] \xrightarrow[n\to\infty]{} 0$$

⋆ A channel resolvability problem w.r.t. W! ⋆

Strong-Secrecy Capacity Results

The inner bound is tight for SD-BCs $(U_1 = Y_1)$

Strong-Secrecy Capacity Results

The inner bound is tight for SD-BCs $(U_1 = Y_1)$

Theorem (SD-BCs Strong-Secrecy-Capacity)

$$\mathcal{C}_{SD} = \bigcup \left\{ \begin{array}{c} R_1 \leq H(Y_1|U_0, U_1, Y_2) \\ R_2 \leq I(U_0, U_2; Y_2) + R_{12} \\ R_1 + R_2 \leq H(Y_1|U_0, U_1, Y_2) + I(U_2; Y_2|U_0) + I(U_0; Y_1) \end{array} \right\}$$

The union is over all $Q_{U_0,U_2,Y_1,X} Q_{Y_2|X}$ *for which* $Y_1 = f(X)$.

Strong-Secrecy Capacity Results

The inner bound is tight for SD-BCs $(U_1 = Y_1)$

Theorem (SD-BCs Strong-Secrecy-Capacity)

$$\mathcal{C}_{SD} = \bigcup \left\{ \begin{array}{c} R_1 \leq H(Y_1|U_0, U_1, Y_2) \\ R_2 \leq I(U_0, U_2; Y_2) + R_{12} \\ R_1 + R_2 \leq H(Y_1|U_0, U_1, Y_2) + I(U_2; Y_2|U_0) + I(U_0; Y_1) \end{array} \right\}$$

The union is over all $Q_{U_0,U_2,Y_1,X} Q_{Y_2|X}$ *for which* $Y_1 = f(X)$.

and PD-BCs $(U_1 = X \ \& \ U_2 = 0)$**:**

Strong-Secrecy Capacity Results

The inner bound is tight for SD-BCs $(U_1 = Y_1)$

Theorem (SD-BCs Strong-Secrecy-Capacity)

$$\mathcal{C}_{SD} = \bigcup \left\{ \begin{array}{r} R_1 \leq H(Y_1|U_0, U_1, Y_2) \\ R_2 \leq I(U_0, U_2; Y_2) + R_{12} \\ R_1 + R_2 \leq H(Y_1|U_0, U_1, Y_2) + I(U_2; Y_2|U_0) + I(U_0; Y_1) \end{array} \right\}$$

The union is over all $Q_{U_0,U_2,Y_1,X} Q_{Y_2|X}$ *for which* $Y_1 = f(X)$.

and PD-BCs $(U_1 = X \ \& \ U_2 = 0)$**:**

Theorem (PD-BCs Strong-Secrecy-Capacity)

$$\mathcal{C}_{PD} = \bigcup \left\{ \begin{array}{r} R_1 \leq I(X; Y_1|U_0) - I(X; Y_2|U_0) \\ R_2 \leq I(U_0; Y_2) + R_{12} \\ R_1 + R_2 \leq I(X; Y_1) - I(X; Y_2|U_0) \end{array} \right\}$$

where the union is over all $Q_{U_0,X} Q_{Y_1|X} Q_{Y_2|Y_1}$.

Summary

- Channel-resolvability for secrecy: Superposing & multi-coding.

Summary

- Channel-resolvability for secrecy: Superposing & multi-coding.
  - Proof via Likelihood encoder.

Summary

- Channel-resolvability for secrecy: Superposing & multi-coding.
  - Proof via Likelihood encoder.
  - Adequate for Marton-based code constructions

Summary

- Channel-resolvability for secrecy: Superposing & multi-coding.
  - Proof via Likelihood encoder.
  - Adequate for Marton-based code constructions

- Cooperative BCs with a Confidential Message:

Summary

- Channel-resolvability for secrecy: Superposing & multi-coding.
  - Proof via Likelihood encoder.
  - Adequate for Marton-based code constructions
- Cooperative BCs with a Confidential Message:
  - Inner bound on strong-secrecy-capacity region.

Summary

- Channel-resolvability for secrecy: Superposing & multi-coding.
  - Proof via Likelihood encoder.
  - Adequate for Marton-based code constructions
- Cooperative BCs with a Confidential Message:
  - Inner bound on strong-secrecy-capacity region.
  - Tight for SD and PD-BCs.

Summary

- Channel-resolvability for secrecy: Superposing & multi-coding.
  - Proof via Likelihood encoder.
  - Adequate for Marton-based code constructions
- Cooperative BCs with a Confidential Message:
  - Inner bound on strong-secrecy-capacity region.
  - Tight for SD and PD-BCs.
- Take-home message: Channel-resolvability lemma for strong-secrecy in Marton codes.

Summary

- Channel-resolvability for secrecy: Superposing & multi-coding.
  - Proof via Likelihood encoder.
  - Adequate for Marton-based code constructions
- Cooperative BCs with a Confidential Message:
  - Inner bound on strong-secrecy-capacity region.
  - Tight for SD and PD-BCs.
- Take-home message: Channel-resolvability lemma for strong-secrecy in Marton codes.

Thank you!

Cooperative BCs with a Confidential Message - Achievability Outline

- Code construction similar to case without secrecy.

Cooperative BCs with a Confidential Message - Achievability Outline

- Code construction similar to case without secrecy.
- Main differences:

Cooperative BCs with a Confidential Message - Achievability Outline

- Code construction similar to case without secrecy.
- Main differences:
  1. **Randomizer:**

Cooperative BCs with a Confidential Message - Achievability Outline

- Code construction similar to case without secrecy.
- Main differences:
  1. **Randomizer:**
     - $W \sim \text{Unif}[1 : 2^{nR'}]$ and $W \perp\!\!\!\perp (M_1, M_2)$.

Cooperative BCs with a Confidential Message - Achievability Outline

- Code construction similar to case without secrecy.
- Main differences:
  1. **Randomizer:**
     - $W \sim \text{Unif}[1 : 2^{nR'}]$ and $W \perp\!\!\!\perp (M_1, M_2)$.
     - Used to conceal M_1 from Decoder 2.

Cooperative BCs with a Confidential Message - Achievability Outline

- Code construction similar to case without secrecy.
- Main differences:
  1. **Randomizer:**
     - $W \sim \text{Unif}[1 : 2^{nR'}]$ and $W \perp\!\!\!\perp (M_1, M_2)$.
     - Used to conceal M_1 from Decoder 2.
     - Decoded by Decoder 1 (along with (M_{20}, M_1)).

Cooperative BCs with a Confidential Message - Achievability Outline

- Code construction similar to case without secrecy.

- Main differences:

  1. **Randomizer:**
     - $W \sim \text{Unif}[1 : 2^{nR'}]$ and $W \perp\!\!\!\perp (M_1, M_2)$.
     - Used to conceal M_1 from Decoder 2.
     - Decoded by Decoder 1 (along with (M_{20}, M_1)).

  2. **Superposition & Cooperation:**

Cooperative BCs with a Confidential Message - Achievability Outline

- Code construction similar to case without secrecy.

- Main differences:
  1. **Randomizer:**
     - $W \sim$ Unif$[1:2^{nR'}]$ and $W \perp\!\!\!\perp (M_1, M_2)$.
     - Used to conceal M_1 from Decoder 2.
     - Decoded by Decoder 1 (along with (M_{20}, M_1)).

  2. **Superposition & Cooperation:**
     - No secrecy - superposition on (M_{10}, M_{20}).

Cooperative BCs with a Confidential Message - Achievability Outline

- Code construction similar to case without secrecy.
- Main differences:
  1. **Randomizer:**
     - $W \sim$ Unif$[1:2^{nR'}]$ and $W \perp\!\!\!\perp (M_1, M_2)$.
     - Used to conceal M_1 from Decoder 2.
     - Decoded by Decoder 1 (along with (M_{20}, M_1)).
  2. **Superposition & Cooperation:**
     - No secrecy - superposition on (M_{10}, M_{20}).
     - Superposing on M_{10} violates secrecy constraint!

Cooperative BCs with a Confidential Message - Achievability Outline

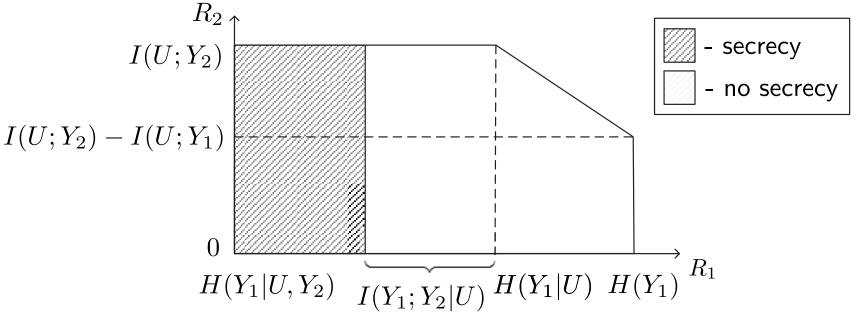
- Code construction similar to case without secrecy.
- Main differences:
  1. **Randomizer:**
     - $W \sim$ Unif$[1:2^{nR'}]$ and $W \perp\!\!\!\perp (M_1, M_2)$.
     - Used to conceal M_1 from Decoder 2.
     - Decoded by Decoder 1 (along with (M_{20}, M_1)).
  2. **Superposition & Cooperation:**
     - No secrecy - superposition on (M_{10}, M_{20}).
     - Superposing on M_{10} violates secrecy constraint!
     - Superposition on M_{20} only.

SD-BC without Cooperation - Effect of Secrecy

Criterion	SD-BC Without Secrecy	SD-BC With M_1 Secret
Capacity	$R_1 \leq H(Y_1)$ $R_2 \leq I(U;Y_2)$ $R_1 + R_2 \leq H(Y_1\|U) + I(U;Y_2)$	$R_1 \leq H(Y_1\|U,Y_2)$ $R_2 \leq I(U;Y_2)$
CP(s)	$\big(H(Y_1\|U), I(U;Y_2)\big)$ $\big(H(Y_1), I(U;Y_2) - I(U;Y_1)\big)$	$\big(H(Y_1\|U,Y_2), I(U;Y_2)\big)$

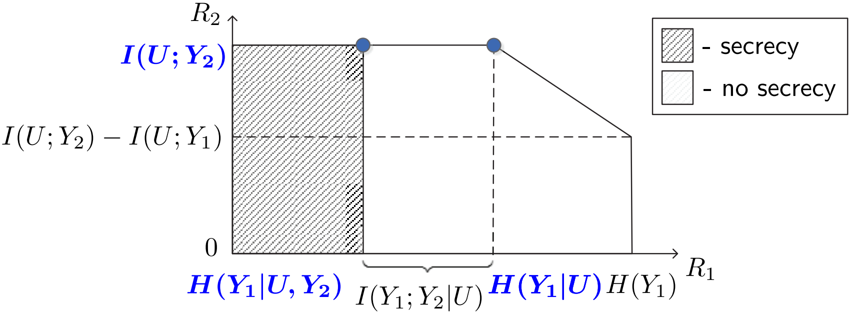
SD-BC without Cooperation - Effect of Secrecy

Criterion	SD-BC Without Secrecy	SD-BC With M_1 Secret
Capacity	$R_1 \leq H(Y_1)$ $R_2 \leq I(U;Y_2)$ $R_1 + R_2 \leq H(Y_1\|U) + I(U;Y_2)$	$R_1 \leq H(Y_1\|U,Y_2)$ $R_2 \leq I(U;Y_2)$
CP(s)	$\big(H(Y_1\|U), I(U;Y_2)\big)$ $\big(H(Y_1), I(U;Y_2) - I(U;Y_1)\big)$	$\big(H(Y_1\|U,Y_2), I(U;Y_2)\big)$



SD-BC without Cooperation - Effect of Secrecy

Criterion	SD-BC Without Secrecy	SD-BC With M_1 Secret
Capacity	$R_1 \leq H(Y_1)$ $R_2 \leq I(U;Y_2)$ $R_1 + R_2 \leq H(Y_1\|U) + I(U;Y_2)$	$R_1 \leq H(Y_1\|U,Y_2)$ $R_2 \leq I(U;Y_2)$
CP(s)	$\boldsymbol{\big(H(Y_1\|U), I(U;Y_2)\big)}$ $\big(H(Y_1), I(U;Y_2) - I(U;Y_1)\big)$	$\boldsymbol{\big(H(Y_1\|U,Y_2), I(U;Y_2)\big)}$



SD-BC without Cooperation - Effect of Secrecy

Criterion	SD-BC Without Secrecy	SD-BC With M_1 Secret
Capacity	$R_1 \leq H(Y_1)$ $R_2 \leq I(U;Y_2)$ $R_1 + R_2 \leq H(Y_1\|U) + I(U;Y_2)$	$R_1 \leq H(Y_1\|U,Y_2)$ $R_2 \leq I(U;Y_2)$
CP(s)	$\big(H(Y_1\|U), I(U;Y_2)\big)$ $\boldsymbol{\big(H(Y_1), I(U;Y_2) - I(U;Y_1)\big)}$	$\big(H(Y_1\|U,Y_2), I(U;Y_2)\big)$ **Violates Secrecy!**