Strong Secrecy for Cooperative Broadcast Channels

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

Ben Gurion University, Technische Universität München and Princeton University

2016 International Zurich Seminar on Communications

March, 2016

Motivation - Combining Secrecy and Cooperation

- Two important aspects of communication.

Motivation - Combining Secrecy and Cooperation

- Two important aspects of communication.
- Secrecy limits cooperation protocols

Motivation - Combining Secrecy and Cooperation

- Two important aspects of communication.
- Secrecy limits cooperation protocols

  Q1: How to combine?

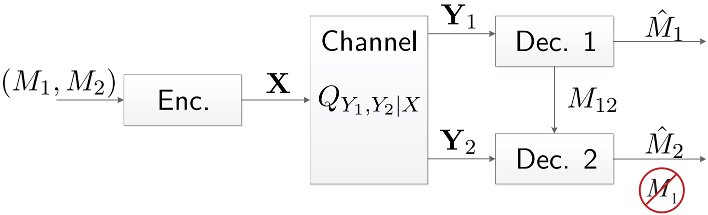
Motivation - Combining Secrecy and Cooperation

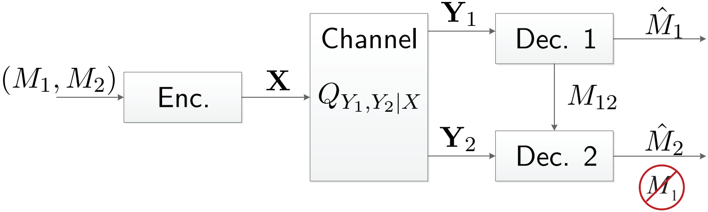
- Two important aspects of communication.
- Secrecy limits cooperation protocols

  Q1: How to combine?

  Q2: Does limited protocol outcome in rate-loss?

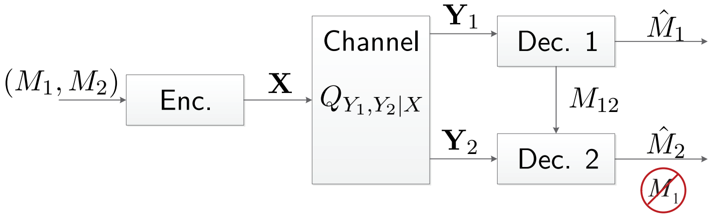
Practical - Secrecy Limits Cooperation Protocols





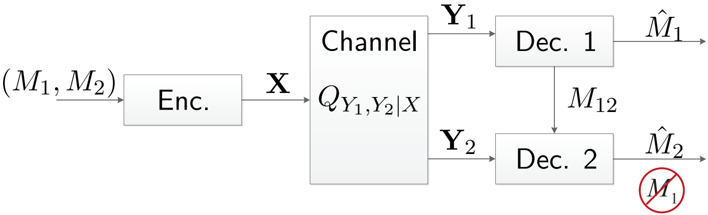
- **No Secrecy:** [ZG-Permuter-Kramer 2015]

Practical - Secrecy Limits Cooperation Protocols



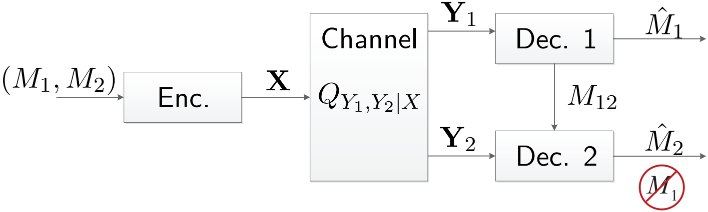
- **No Secrecy:** [ZG-Permuter-Kramer 2015]
  - Share information about (M_1, M_2)

Practical - Secrecy Limits Cooperation Protocols

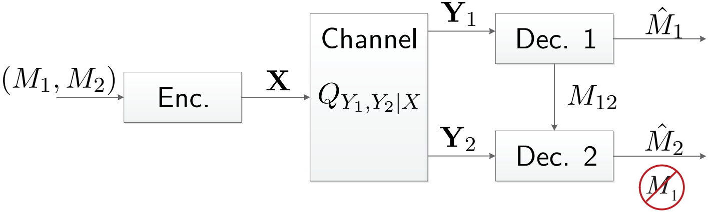


- **No Secrecy:** [ZG-Permuter-Kramer 2015]
  - Share information about $(M_1, M_2) \implies \boldsymbol{M_{12}(M_1, M_2)}$.

Practical - Secrecy Limits Cooperation Protocols



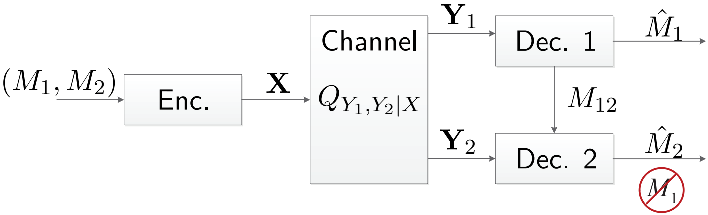
- **No Secrecy:** [ZG-Permuter-Kramer 2015]
  - Share information about $(M_1, M_2) \implies \boldsymbol{M_{12}(M_1, M_2)}$.
- $\boldsymbol{M_1}$ **is Secret:**



- **No Secrecy:** [ZG-Permuter-Kramer 2015]
  - Share information about $(M_1, M_2) \implies \boldsymbol{M_{12}(M_1, M_2)}$.

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

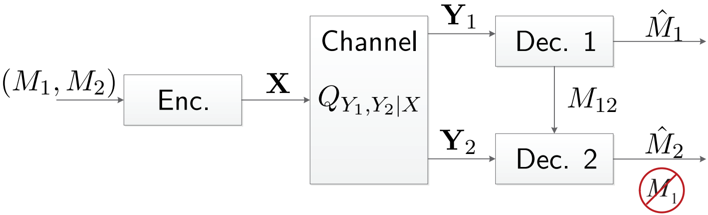
Practical - Secrecy Limits Cooperation Protocols



- **No Secrecy:** [ZG-Permuter-Kramer 2015]
  - Share information about $(M_1, M_2) \implies \boldsymbol{M_{12}(M_1, M_2)}$.

- $\boldsymbol{M_1}$ **is Secret:** No sharing information about $M_1 \implies \boldsymbol{M_{12}(M_2)}$.

Practical - Secrecy Limits Cooperation Protocols

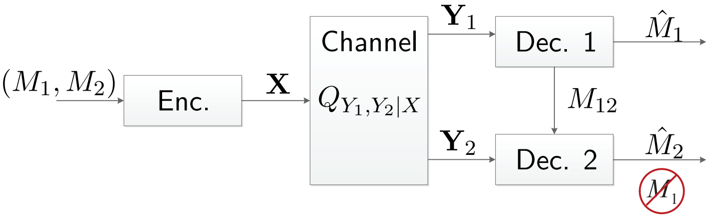


- **No Secrecy:** [ZG-Permuter-Kramer 2015]
  - Share information about $(M_1, M_2) \implies \boldsymbol{M_{12}(M_1, M_2)}$.

- **M_1 is Secret:** No sharing information about $M_1 \implies \boldsymbol{M_{12}(M_2)}$.

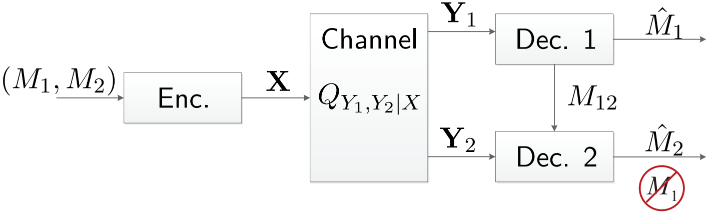
★ Does restricted protocol reduces rates? ★

Theoretical - Strong Secrecy for Marton Codes



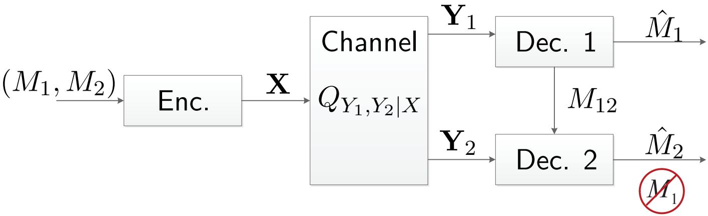
- General BCs

Theoretical - Strong Secrecy for Marton Codes



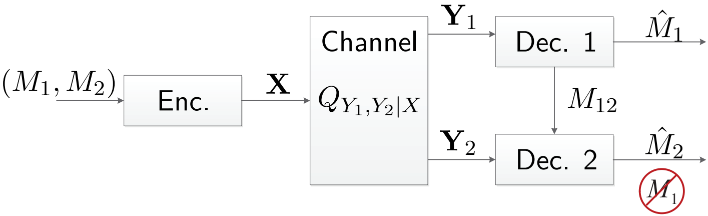
- General BCs $\Longrightarrow$ Marton Coding.

Theoretical - Strong Secrecy for Marton Codes



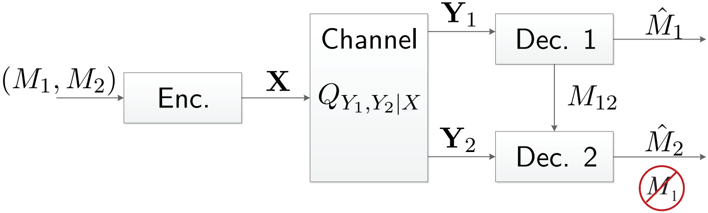
- General BCs $\Longrightarrow$ Marton Coding.
- **Weak-Secrecy:** $\frac{1}{n} I(M_1; M_{12}, Y_2^n) \to 0.$

Theoretical - Strong Secrecy for Marton Codes



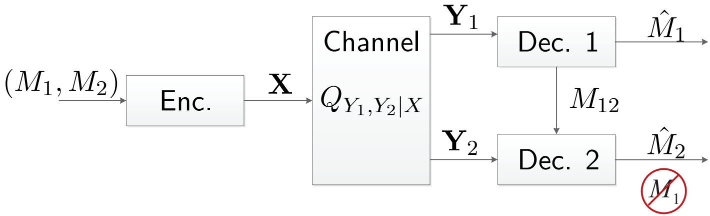
- General BCs $\Longrightarrow$ Marton Coding.
- **Weak-Secrecy:** $\frac{1}{n} I(M_1; M_{12}, Y_2^n) \to 0.$ ✓

Theoretical - Strong Secrecy for Marton Codes



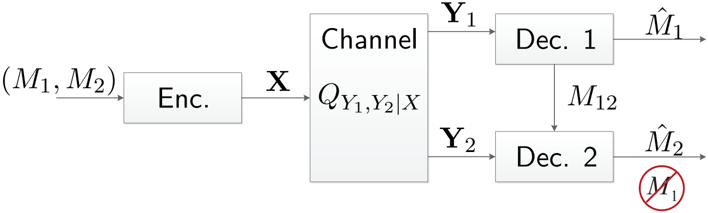
- General BCs $\Longrightarrow$ Marton Coding.
- **Weak-Secrecy:** $\frac{1}{n}I(M_1; M_{12}, Y_2^n) \to 0$. Only leakage **rate** vanishes

Theoretical - Strong Secrecy for Marton Codes



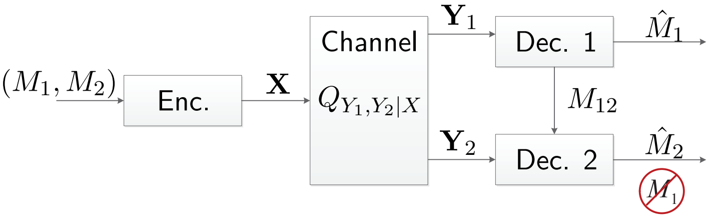
- General BCs $\implies$ Marton Coding.
- **Weak-Secrecy:** ~~$\frac{1}{n}I(M_1; M_{12}, Y_2^n) \to 0$~~. Only leakage **rate** vanishes
- **Strong-Secrecy:** $I(M_1; M_{12}, Y_2^n) \to 0$.

Theoretical - Strong Secrecy for Marton Codes



- General BCs $\implies$ Marton Coding.
- **Weak-Secrecy:** ~~$\frac{1}{n} I(M_1; M_{12}, Y_2^n) \to 0$~~. Only leakage **rate** vanishes
- **Strong-Secrecy:** $I(M_1; M_{12}, Y_2^n) \to 0$. **?**

Theoretical - Strong Secrecy for Marton Codes

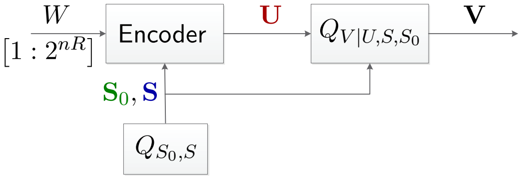


- General BCs $\Longrightarrow$ Marton Coding.
- **Weak-Secrecy:** $\frac{1}{n} I(M_1; M_{12}, Y_2^n) \to 0$. Only leakage **rate** vanishes
- **Strong-Secrecy:** $I(M_1; M_{12}, Y_2^n) \to 0$. **?**

★ Strong-secrecy for Marton codes (joint encoding) ★

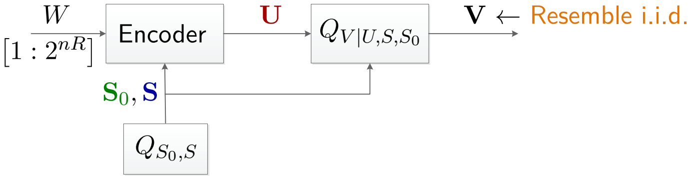
A Soft-Covering Lemma - Setup

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



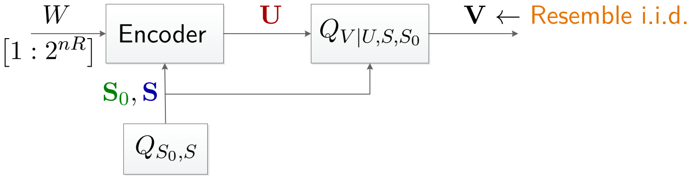
A Soft-Covering Lemma - Setup

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



A Soft-Covering Lemma - Setup

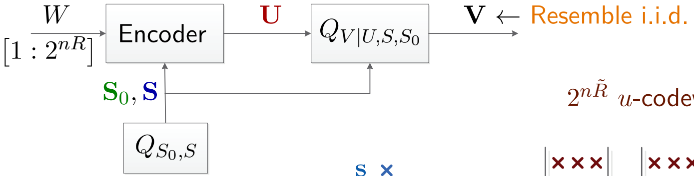
Classic Case - PTP codebook [Wyner 1975], [Han-Verdú 1993]



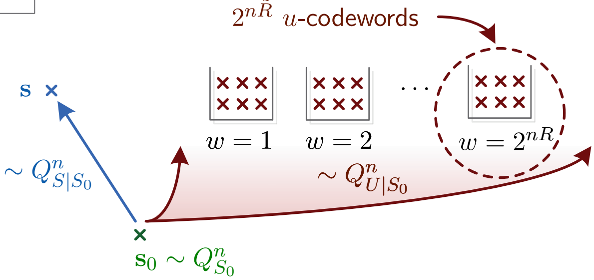
- **Codebook:**

A Soft-Covering Lemma - Setup

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

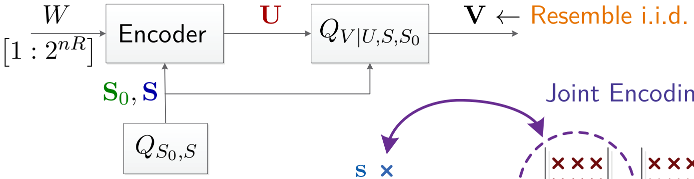


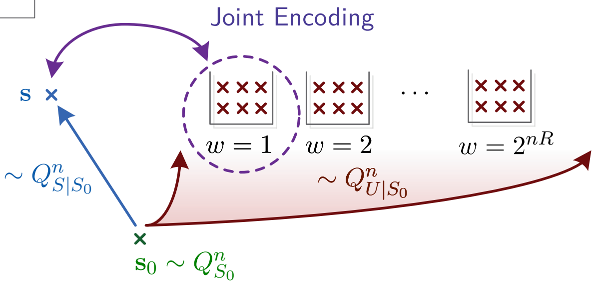
- **Codebook:**



A Soft-Covering Lemma - Setup

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

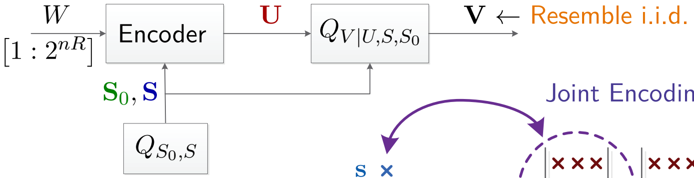


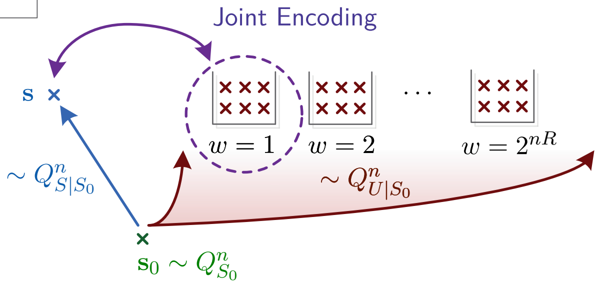


- **Codebook:**
- **Joint Encoding:**

A Soft-Covering Lemma - Setup

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



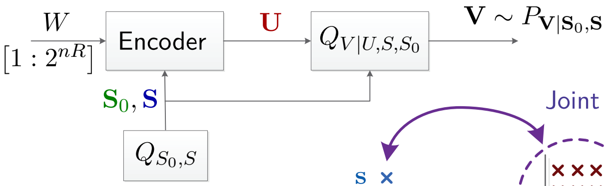


- **Codebook:**

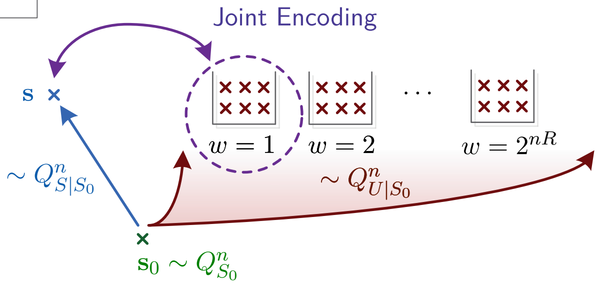
- **Joint Encoding:** via Likelihood Encoder [Song-Cuff-Poor 2015].

A Soft-Covering Lemma - Setup

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



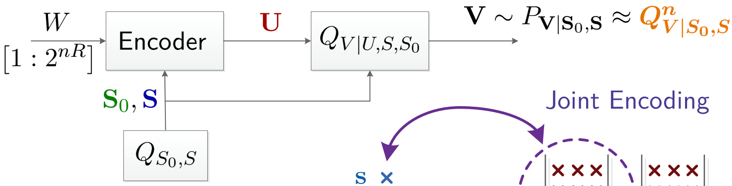
- **Codebook:**



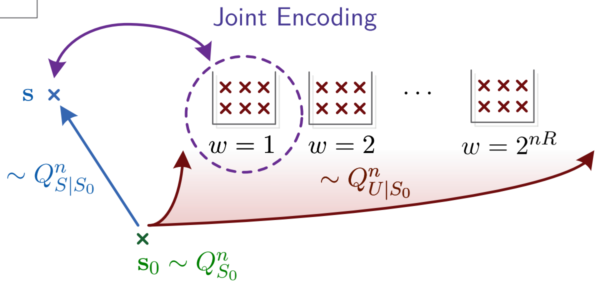
- **Joint Encoding:** via Likelihood Encoder [Song-Cuff-Poor 2015].

A Soft-Covering Lemma - Setup

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



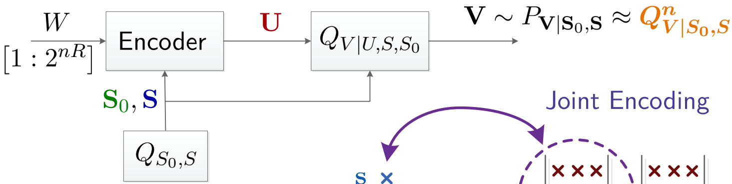
- **Codebook:**



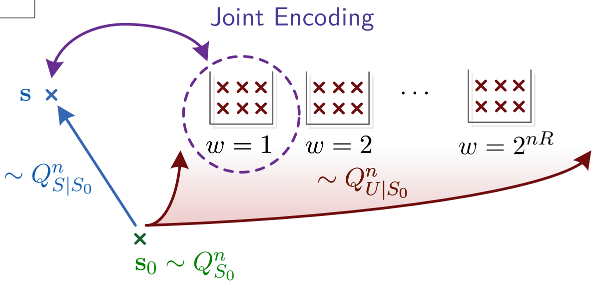
- **Joint Encoding:** via Likelihood Encoder [Song-Cuff-Poor 2015].

A Soft-Covering Lemma - Setup

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



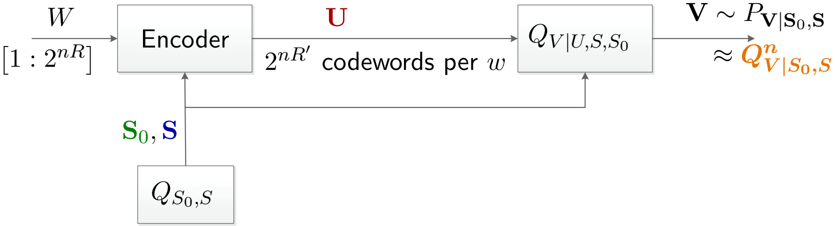
- **Codebook:**



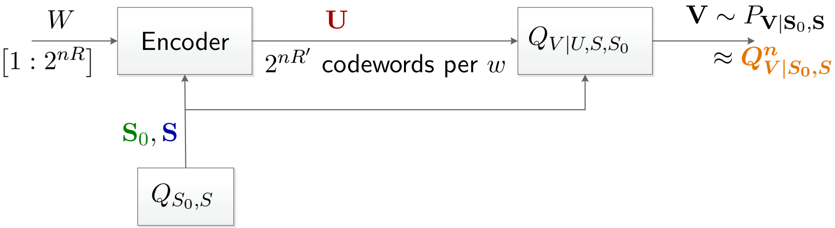
- **Joint Encoding:** via Likelihood Encoder [Song-Cuff-Poor 2015].

- **Goal:** $(R,\tilde{R})$ s.t. $\mathbb{E}_{\mathbb{C}_n}\left[D\left(P_{\mathbf{V}|\mathbf{S}_0,\mathbf{S},\mathbb{C}_n}\middle|\middle|Q^n_{V|S_0,S}\middle|Q^n_{S_0,S}\right)\right] \xrightarrow[n\to\infty]{} 0.$

A Soft-Covering Lemma - Statement



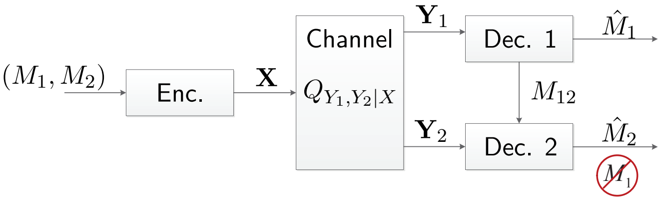
A Soft-Covering Lemma - Statement



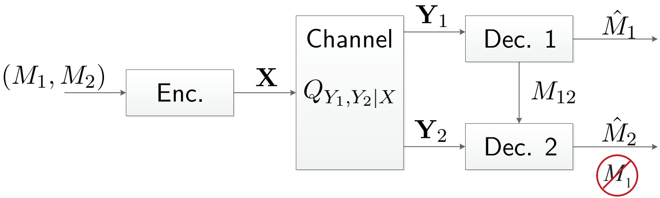
Theorem (Direct Part)

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

Cooperative BCs with a Confidential Message



Cooperative BCs with a Confidential Message



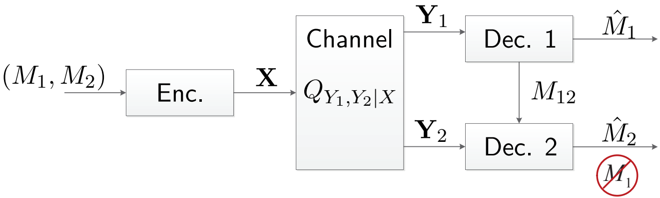
Theorem (Inner Bound)

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



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 $Q_{U_0,U_1,U_2,X}Q_{Y_1,Y_2|X}$.

★ Tight for SD and PD-BCs ★

Inner Bound - Proof Outline

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

Inner Bound - Proof Outline

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

Inner Bound - Proof Outline

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

Inner Bound - Proof Outline

- **Messages:** $M_2 = (M_{20}, M_{22})$.
  - M_{20} - Public;
  - (M_1, M_{22}) - Private.
  - $W \sim \text{Unif}\big[1 : 2^{nR'}\big]$
    (Dummy Message).

Inner Bound - Proof Outline

- **Messages:** $M_2 = (M_{20}, M_{22})$.
  - M_{20} - Public;
  - (M_1, M_{22}) - Private.
  - $W \sim \text{Unif}\big[1 : 2^{nR'}\big]$ (Dummy Message).
- **Encoding:**

Inner Bound - Proof Outline

- **Messages:** $M_2 = (M_{20}, M_{22})$.
  - M_{20} - Public;
  - (M_1, M_{22}) - Private.
  - $W \sim \text{Unif}\left[1 : 2^{nR'}\right]$
    (Dummy Message).

- **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} - Public;
  - (M_1, M_{22}) - Private.
  - $W \sim \text{Unif}\left[1 : 2^{nR'}\right]$
    (Dummy Message).

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

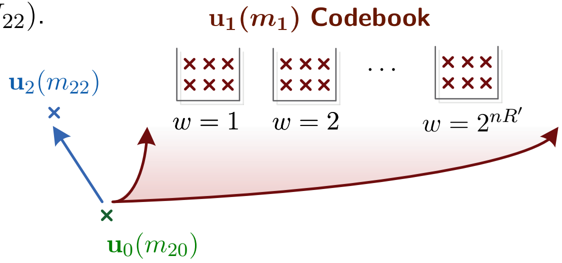
Inner Bound - Proof Outline

- **Messages:** $M_2 = (M_{20}, M_{22})$.
  - M_{20} - Public;
  - (M_1, M_{22}) - Private.
  - $W \sim$ Unif$\left[1 : 2^{nR'}\right]$ (Dummy Message).

- **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. $M_1 \longrightarrow$ Soft-covering code $\sim Q^n_{U_1|U_0}$

Inner Bound - Proof Outline

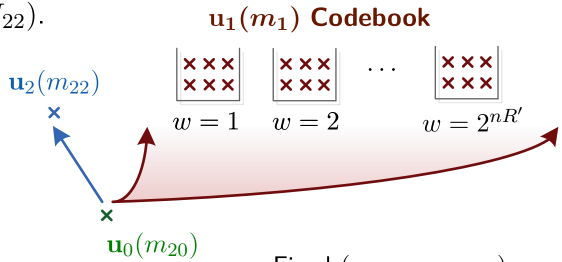
- **Messages:** $M_2 = (M_{20}, M_{22})$.
  - M_{20} - Public;
  - (M_1, M_{22}) - Private.
  - $W \sim$ Unif$\left[1 : 2^{nR'}\right]$ (Dummy Message).



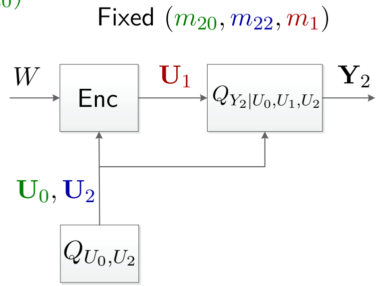
- **Encoding:**
  1. $M_{20} \longrightarrow \mathbf{U}_0 \sim Q^n_{U_0}$.
  2. $M_{22} \longrightarrow \mathbf{U}_2 \sim Q^n_{U_2|U_0}$.
  3. $M_1 \longrightarrow$ Soft-covering code $\sim Q^n_{U_1|U_0}$

Inner Bound - Proof Outline

- **Messages:** $M_2 = (M_{20}, M_{22})$.
  - M_{20} - Public;
  - (M_1, M_{22}) - Private.
  - $W \sim \text{Unif}[1 : 2^{nR'}]$ (Dummy Message).

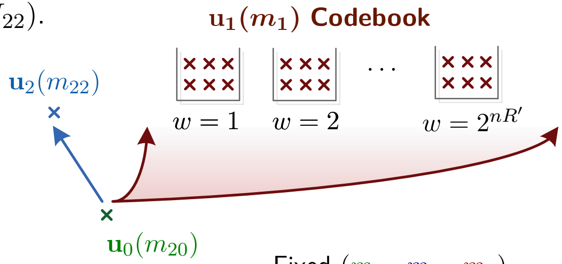


- **Encoding:**
  1. $M_{20} \longrightarrow \mathbf{U}_0 \sim Q^n_{U_0}$.
  2. $M_{22} \longrightarrow \mathbf{U}_2 \sim Q^n_{U_2|U_0}$.
  3. $M_1 \longrightarrow$ Soft-covering code $\sim Q^n_{U_1|U_0}$



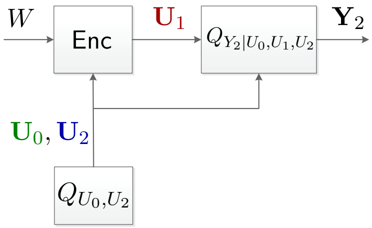
Inner Bound - Proof Outline

- **Messages:** $M_2 = (M_{20}, M_{22})$.
  - M_{20} - Public;
  - (M_1, M_{22}) - Private.
  - $W \sim \text{Unif}[1 : 2^{nR'}]$ (Dummy Message).



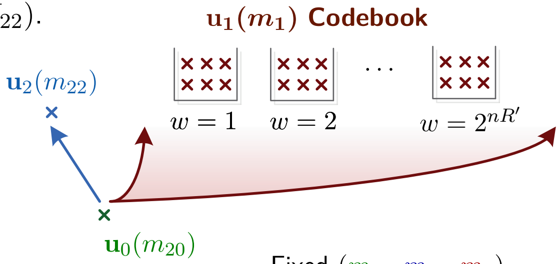
- **Encoding:**
  1. $M_{20} \longrightarrow \mathbf{U}_0 \sim Q^n_{U_0}$.
  2. $M_{22} \longrightarrow \mathbf{U}_2 \sim Q^n_{U_2|U_0}$.
  3. $M_1 \longrightarrow$ Soft-covering code $\sim Q^n_{U_1|U_0}$
     - Choose $\mathbf{U}_1$ - Likelihood encoder.

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

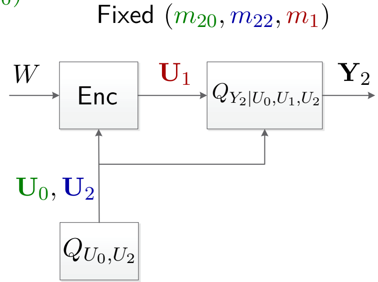


Inner Bound - Proof Outline

- **Messages:** $M_2 = (M_{20}, M_{22})$.
  - M_{20} - Public;
  - (M_1, M_{22}) - Private.
  - $W \sim \text{Unif}[1 : 2^{nR'}]$ (Dummy Message).

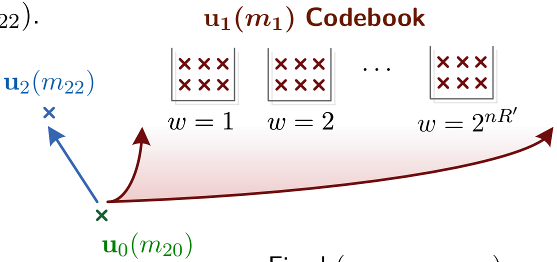


- **Encoding:**
  1. $M_{20} \longrightarrow \mathbf{U}_0 \sim Q^n_{U_0}$.
  2. $M_{22} \longrightarrow \mathbf{U}_2 \sim Q^n_{U_2|U_0}$.
  3. $M_1 \longrightarrow$ Soft-covering code $\sim Q^n_{U_1|U_0}$
     - Choose $\mathbf{U}_1$ - Likelihood encoder.

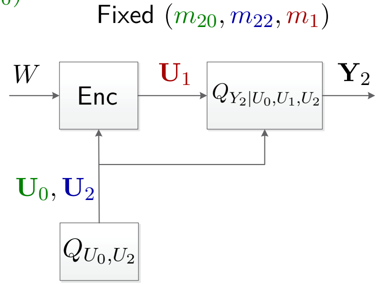


- **Cooperation:**

- **Messages:** $M_2 = (M_{20}, M_{22})$.
  - M_{20} - Public;
  - (M_1, M_{22}) - Private.
  - $W \sim \text{Unif}[1 : 2^{nR'}]$ (Dummy Message).



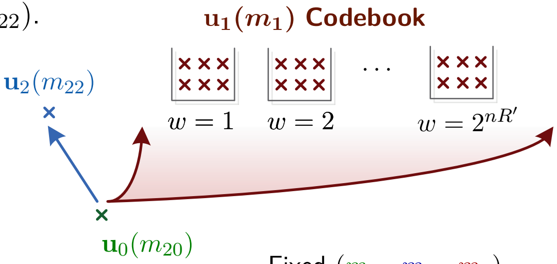
- **Encoding:**
  1. $M_{20} \longrightarrow \mathbf{U}_0 \sim Q^n_{U_0}$.
  2. $M_{22} \longrightarrow \mathbf{U}_2 \sim Q^n_{U_2|U_0}$.
  3. $M_1 \longrightarrow$ Soft-covering code $\sim Q^n_{U_1|U_0}$
     - Choose $\mathbf{U}_1$ - Likelihood encoder.



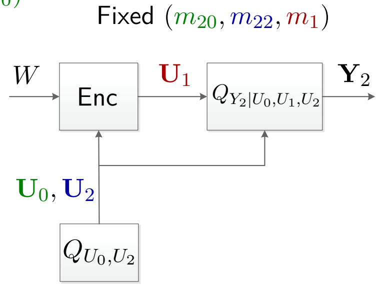
- **Cooperation:**
  1. Bin M_{20} codebook into $2^{nR_{12}}$ bins.

Inner Bound - Proof Outline

- **Messages:** $M_2 = (M_{20}, M_{22})$.
  - M_{20} - Public;
  - (M_1, M_{22}) - Private.
  - $W \sim$ Unif$\left[1 : 2^{nR'}\right]$ (Dummy Message).



- **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. $M_1 \longrightarrow$ Soft-covering code $\sim Q^n_{U_1|U_0}$
     - Choose $\mathbf{U}_1$ - 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:

1. **LE Encoding Error:**

Inner Bound - Proof Outline

Key Arguments:

1. **LE Encoding Error:** Chosen $(\mathbf{U_0}, \mathbf{U_1}, \mathbf{U_2})$ jointly typical w.h.p.

Inner Bound - Proof Outline

Key Arguments:

1. **LE Encoding Error:** Chosen $(\mathbf{U_0}, \mathbf{U_1}, \mathbf{U_2})$ jointly typical w.h.p.

2. **Strong-Secrecy via Soft-Covering:**

Inner Bound - Proof Outline

Key Arguments:

1. **LE Encoding Error:** Chosen $(\mathbf{U_0}, \mathbf{U_1}, \mathbf{U_2})$ jointly typical w.h.p.

2. **Strong-Secrecy via Soft-Covering:**

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

Inner Bound - Proof Outline

Key Arguments:

1. **LE Encoding Error:** Chosen $(\mathbf{U_0}, \mathbf{U_1}, \mathbf{U_2})$ jointly typical w.h.p.

2. **Strong-Secrecy via Soft-Covering:**

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

Inner Bound - Proof Outline

Key Arguments:

1. **LE Encoding Error:** Chosen $(\mathbf{U_0}, \mathbf{U_1}, \mathbf{U_2})$ jointly typical w.h.p.

2. **Strong-Secrecy via Soft-Covering:**

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

★ The soft-covering setup w.r.t. W! ★

Key Arguments:

1. **LE Encoding Error:** Chosen $(\mathbf{U_0}, \mathbf{U_1}, \mathbf{U_2})$ jointly typical w.h.p.

2. **Strong-Secrecy via Soft-Covering:**

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

⋆ The soft-covering setup w.r.t. W! ⋆

Restricted Cooperation is Sub-Optimal

- **Without Secrecy:** $M_{12}(M_1, M_2)$.

Restricted Cooperation is Sub-Optimal

- **Without Secrecy:** $M_{12}(M_1, M_2)$.
- **M_1 is Secret:** $M_{12}(M_2)$.

Restricted Cooperation is Sub-Optimal

- **Without Secrecy:** $M_{12}(M_1, M_2)$.
- **M_1 is Secret:** $M_{12}(M_2)$.

Q: Does restriction makes a difference?

Restricted Cooperation is Sub-Optimal

- **Without Secrecy:** $M_{12}(M_1, M_2)$.
- $\boldsymbol{M_1}$ **is Secret:** $M_{12}(M_2)$.

Q: Does restriction makes a difference?

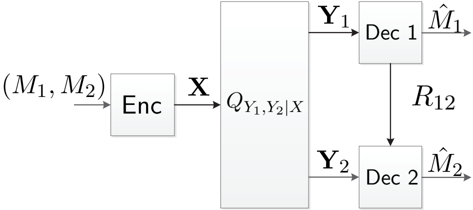
- **Comparison**: Cooperative BC without secrecy.

Restricted Cooperation is Sub-Optimal

- **Without Secrecy:** $M_{12}(M_1, M_2)$.
- $\boldsymbol{M_1}$ **is Secret:** $M_{12}(M_2)$.

Q: Does restriction makes a difference?

- **Comparison**: Cooperative BC without secrecy.

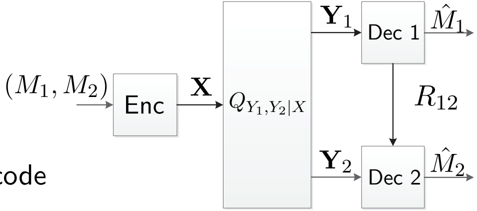


Restricted Cooperation is Sub-Optimal

- **Without Secrecy:** $M_{12}(M_1, M_2)$.
- **M_1 is Secret:** $M_{12}(M_2)$.

Q: Does restriction makes a difference?

- **Comparison**: Cooperative BC without secrecy.



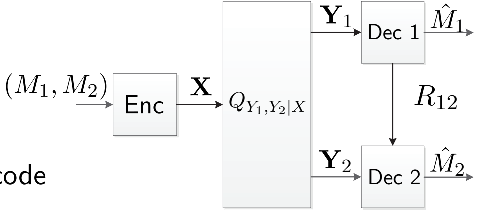
- **Dichotomy**: User 1 can decode

Restricted Cooperation is Sub-Optimal

- **Without Secrecy:** $M_{12}(M_1, M_2)$.
- ***M_1* is Secret:** $M_{12}(M_2)$.

Q: Does restriction makes a difference?

- **Comparison**: Cooperative BC without secrecy.



- **Dichotomy**: User 1 can decode

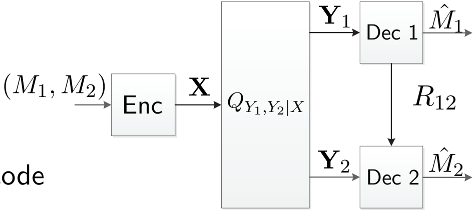
  1. More than nR_{12} bits of M_2 .

Restricted Cooperation is Sub-Optimal

- **Without Secrecy:** $M_{12}(M_1, M_2)$.
- $\boldsymbol{M_1}$ **is Secret:** $M_{12}(M_2)$.

Q: Does restriction makes a difference?

- **Comparison**: Cooperative BC without secrecy.



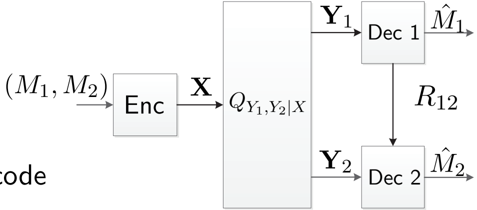
- **Dichotomy**: User 1 can decode
  1. More than nR_{12} bits of M_2 $\implies$ **Schemes are the same**.

Restricted Cooperation is Sub-Optimal

- **Without Secrecy:** $M_{12}(M_1, M_2)$.
- ***M_1* is Secret:** $M_{12}(M_2)$.

Q: Does restriction makes a difference?

- **Comparison**: Cooperative BC without secrecy.



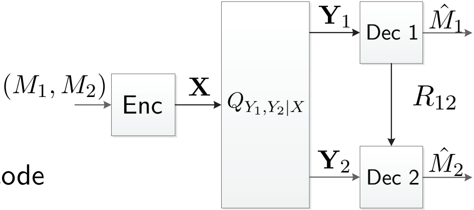
- **Dichotomy**: User 1 can decode
  1. More than nR_{12} bits of M_2 $\Longrightarrow$ **Schemes are the same**.
  2. Less than nR_{12} bits of M_2

Restricted Cooperation is Sub-Optimal

- **Without Secrecy:** $M_{12}(M_1, M_2)$.
- **M_1 is Secret:** $M_{12}(M_2)$.

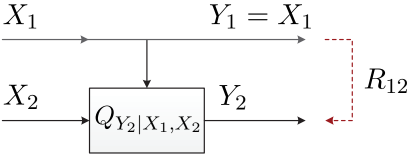
Q: Does restriction makes a difference?

- **Comparison**: Cooperative BC without secrecy.

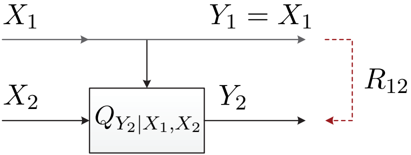


- **Dichotomy**: User 1 can decode
  1. More than nR_{12} bits of M_2 $\implies$ **Schemes are the same**.
  2. Less than nR_{12} bits of M_2 $\implies$ **Restricted scheme sub-optimal!**

Restricted Protocol Sub-Optimal - SD-BC Example



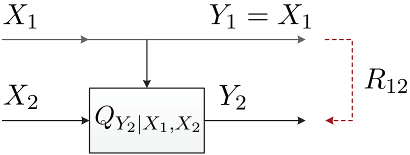
Restricted Protocol Sub-Optimal - SD-BC Example



Assume:

- $X = (X_1, X_2)$.

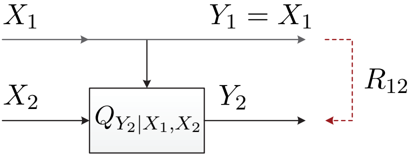
Restricted Protocol Sub-Optimal - SD-BC Example



Assume:

- $X = (X_1, X_2)$.
- $\mathcal{X}_1 = \mathcal{X}_2 = \mathcal{Y}_2 = \{0, 1\}$.

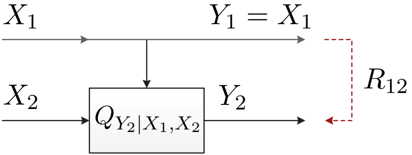
Restricted Protocol Sub-Optimal - SD-BC Example



Assume:

- $X = (X_1, X_2)$.
- $\mathcal{X}_1 = \mathcal{X}_2 = \mathcal{Y}_2 = \{0, 1\}$.
- $R_{12} = 1$.

Restricted Protocol Sub-Optimal - SD-BC Example

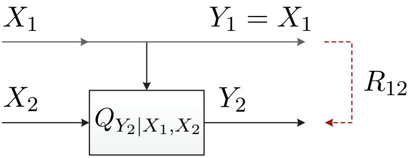


Assume:

- $X = (X_1, X_2)$.
- $\mathcal{X}_1 = \mathcal{X}_2 = \mathcal{Y}_2 = \{0, 1\}$.
- $R_{12} = 1$.

- **Starting Point:** $(R_1, R_2) = (1, 0)$ achievable by both schemes.

Restricted Protocol Sub-Optimal - SD-BC Example



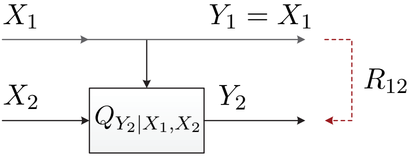
Assume:

- $X = (X_1, X_2)$.
- $\mathcal{X}_1 = \mathcal{X}_2 = \mathcal{Y}_2 = \{0, 1\}$.
- $R_{12} = 1$.

- **Starting Point:** $(R_1, R_2) = (1, 0)$ achievable by both schemes.

  Q: **What is the maximal achievable R_2 when $R_1 = 1$?**

Restricted Protocol Sub-Optimal - SD-BC Example



Assume:

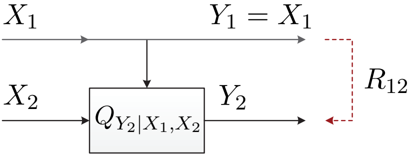
- $X = (X_1, X_2)$.
- $\mathcal{X}_1 = \mathcal{X}_2 = \mathcal{Y}_2 = \{0, 1\}$.
- $R_{12} = 1$.

- **Starting Point:** $(R_1, R_2) = (1, 0)$ achievable by both schemes.

  Q: **What is the maximal achievable $\boldsymbol{R_2}$ when $\boldsymbol{R_1 = 1}$?**

  A: $R_1 = 1$

Restricted Protocol Sub-Optimal - SD-BC Example



Assume:

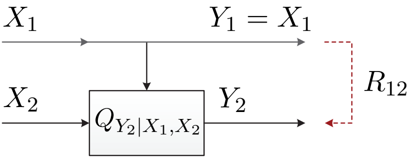
- $X = (X_1, X_2)$.
- $\mathcal{X}_1 = \mathcal{X}_2 = \mathcal{Y}_2 = \{0, 1\}$.
- $R_{12} = 1$.

- **Starting Point:** $(R_1, R_2) = (1, 0)$ achievable by both schemes.

  Q: **What is the maximal achievable R_2 when $R_1 = 1$?**

  A: $R_1 = 1 \implies X_1^n = M_1$

Restricted Protocol Sub-Optimal - SD-BC Example



Assume:

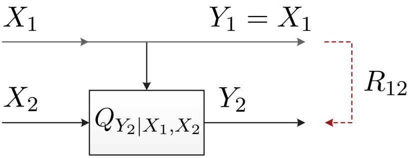
- $X = (X_1, X_2)$.
- $\mathcal{X}_1 = \mathcal{X}_2 = \mathcal{Y}_2 = \{0, 1\}$.
- $R_{12} = 1$.

- **Starting Point:** $(R_1, R_2) = (1, 0)$ achievable by both schemes.

  Q: **What is the maximal achievable $\boldsymbol{R_2}$ when $\boldsymbol{R_1 = 1}$?**

  A: $R_1 = 1 \implies X_1^n = M_1 \implies$ Dec. 1 has only M_1.

Restricted Protocol Sub-Optimal - SD-BC Example



Assume:

- $X = (X_1, X_2)$.
- $\mathcal{X}_1 = \mathcal{X}_2 = \mathcal{Y}_2 = \{0, 1\}$.
- $R_{12} = 1$.

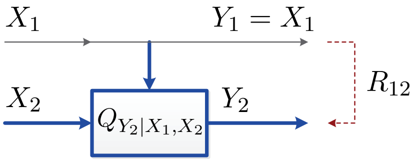
- **Starting Point:** $(R_1, R_2) = (1, 0)$ achievable by both schemes.

  Q: **What is the maximal achievable R_2 when $R_1 = 1$?**

  A: $R_1 = 1 \implies X_1^n = M_1 \implies$ Dec. 1 has only M_1.

  - **Permissive Scheme:** $M_{12} = X_1^n$

Restricted Protocol Sub-Optimal - SD-BC Example



Full (Enc. and Dec.) CSI

Assume:

- $X = (X_1, X_2)$.
- $\mathcal{X}_1 = \mathcal{X}_2 = \mathcal{Y}_2 = \{0, 1\}$.
- $R_{12} = 1$.

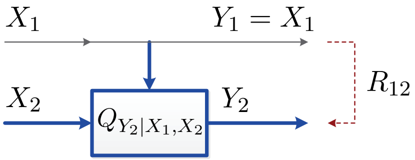
- **Starting Point:** $(R_1, R_2) = (1, 0)$ achievable by both schemes.

  Q: **What is the maximal achievable R_2 when $R_1 = 1$?**

  A: $R_1 = 1 \implies X_1^n = M_1 \implies$ Dec. 1 has only M_1.

  - **Permissive Scheme:** $M_{12} = X_1^n$

Restricted Protocol Sub-Optimal - SD-BC Example



Full (Enc. and Dec.) CSI

Assume:

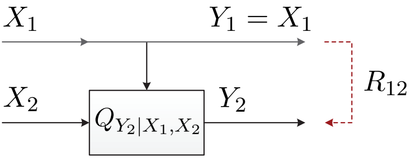
- $X = (X_1, X_2)$.
- $\mathcal{X}_1 = \mathcal{X}_2 = \mathcal{Y}_2 = \{0, 1\}$.
- $R_{12} = 1$.

- **Starting Point:** $(R_1, R_2) = (1, 0)$ achievable by both schemes.

  Q: **What is the maximal achievable R_2 when $R_1 = 1$?**

  A: $R_1 = 1 \implies X_1^n = M_1 \implies$ Dec. 1 has only M_1.

  - **Permissive Scheme:** $M_{12} = X_1^n \implies \boldsymbol{R_{2,\max} \geq C_{\mathrm{Full-CSI}}}$



Assume:

- $X = (X_1, X_2)$.
- $\mathcal{X}_1 = \mathcal{X}_2 = \mathcal{Y}_2 = \{0, 1\}$.
- $R_{12} = 1$.

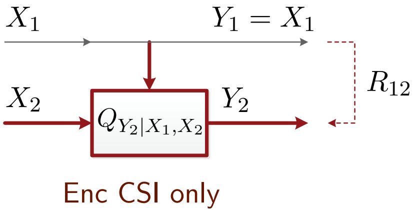
- **Starting Point:** $(R_1, R_2) = (1, 0)$ achievable by both schemes.

  Q: **What is the maximal achievable R_2 when $R_1 = 1$?**

  A: $R_1 = 1 \implies X_1^n = M_1 \implies$ Dec. 1 has only M_1.

  - **Permissive Scheme:** $M_{12} = X_1^n \implies \boldsymbol{R_{2,\max} \geq C_{\text{Full-CSI}}}$
  - **Restricted Scheme:** $M_{12} = 0$

Restricted Protocol Sub-Optimal - SD-BC Example



Assume:

- $X = (X_1, X_2)$.
- $\mathcal{X}_1 = \mathcal{X}_2 = \mathcal{Y}_2 = \{0, 1\}$.
- $R_{12} = 1$.

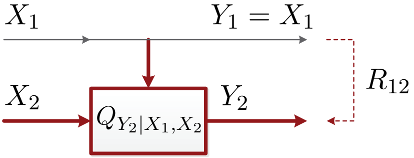
- **Starting Point:** $(R_1, R_2) = (1, 0)$ achievable by both schemes.

  Q: What is the maximal achievable R_2 when $R_1 = 1$?

  A: $R_1 = 1 \implies X_1^n = M_1 \implies$ Dec. 1 has only M_1.

  - **Permissive Scheme:** $M_{12} = X_1^n \implies R_{2,\max} \geq C_{\text{Full-CSI}}$
  - **Restricted Scheme:** $M_{12} = 0$

Restricted Protocol Sub-Optimal - SD-BC Example



Enc CSI only

Assume:

- $X = (X_1, X_2)$.
- $\mathcal{X}_1 = \mathcal{X}_2 = \mathcal{Y}_2 = \{0, 1\}$.
- $R_{12} = 1$.

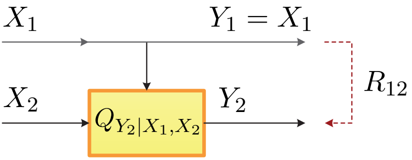
- **Starting Point:** $(R_1, R_2) = (1, 0)$ achievable by both schemes.

  Q: **What is the maximal achievable R_2 when $R_1 = 1$?**

  A: $R_1 = 1 \implies X_1^n = M_1 \implies$ Dec. 1 has only M_1.

  - **Permissive Scheme:** $M_{12} = X_1^n \implies R_{2,\max} \geq C_{\text{Full}-\text{CSI}}$
  - **Restricted Scheme:** $M_{12} = 0 \implies \tilde{R}_{2,\max} \leq C_{\text{Enc}-\text{CSI}}$

Restricted Protocol Sub-Optimal - SD-BC Example



Assume:

- $X = (X_1, X_2)$.
- $\mathcal{X}_1 = \mathcal{X}_2 = \mathcal{Y}_2 = \{0, 1\}$.
- $R_{12} = 1$.

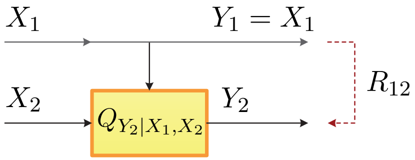
- **Starting Point:** $(R_1, R_2) = (1, 0)$ achievable by both schemes.

  Q: **What is the maximal achievable R_2 when $R_1 = 1$?**

  A: $R_1 = 1 \implies X_1^n = M_1 \implies$ Dec. 1 has only M_1.

  - **Permissive Scheme:** $M_{12} = X_1^n \implies \boldsymbol{R_{2,\max} \geq C_{\text{Full}-\text{CSI}}}$
  - **Restricted Scheme:** $M_{12} = 0 \implies \boldsymbol{\tilde{R}_{2,\max} \leq C_{\text{Enc}-\text{CSI}}}$

Restricted Protocol Sub-Optimal - SD-BC Example



Assume:

- $X = (X_1, X_2)$.
- $\mathcal{X}_1 = \mathcal{X}_2 = \mathcal{Y}_2 = \{0, 1\}$.
- $R_{12} = 1$.

- **Starting Point:** $(R_1, R_2) = (1, 0)$ achievable by both schemes.

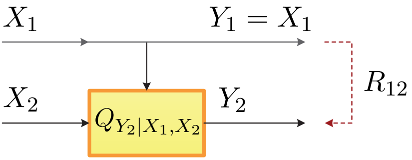
  Q: **What is the maximal achievable $\boldsymbol{R_2}$ when $\boldsymbol{R_1 = 1}$?**

  A: $R_1 = 1 \implies X_1^n = M_1 \implies$ Dec. 1 has only M_1.

  - **Permissive Scheme:** $M_{12} = X_1^n \implies \boldsymbol{R_{2,\max} \geq C_{\text{Full}-\text{CSI}}}$
  - **Restricted Scheme:** $M_{12} = 0 \implies \boldsymbol{\tilde{R}_{2,\max} \leq C_{\text{Enc}-\text{CSI}}}$

$\implies$ **Binary dirty paper channel:** $Y_2 = X_2 \oplus X_1 \oplus Z$

Restricted Protocol Sub-Optimal - SD-BC Example



Assume:

- $X = (X_1, X_2)$.
- $\mathcal{X}_1 = \mathcal{X}_2 = \mathcal{Y}_2 = \{0, 1\}$.
- $R_{12} = 1$.

- **Starting Point:** $(R_1, R_2) = (1, 0)$ achievable by both schemes.

  Q: **What is the maximal achievable R_2 when $R_1 = 1$?**

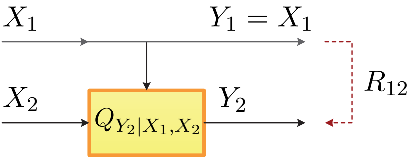
  A: $R_1 = 1 \implies X_1^n = M_1 \implies$ Dec. 1 has only M_1.

  - **Permissive Scheme:** $M_{12} = X_1^n \implies R_{2,\max} \geq C_{\text{Full-CSI}}$
  - **Restricted Scheme:** $M_{12} = 0 \implies \tilde{R}_{2,\max} \leq C_{\text{Enc-CSI}}$

$\implies$ **Binary dirty paper channel:** $Y_2 = X_2 \oplus X_1 \oplus Z$

$$C_{\text{Enc-CSI}} < C_{\text{Full-CSI}}$$

Restricted Protocol Sub-Optimal - SD-BC Example



Assume:

- $X = (X_1, X_2)$.
- $\mathcal{X}_1 = \mathcal{X}_2 = \mathcal{Y}_2 = \{0, 1\}$.
- $R_{12} = 1$.

- **Starting Point:** $(R_1, R_2) = (1, 0)$ achievable by both schemes.

  Q: **What is the maximal achievable R_2 when $R_1 = 1$?**

  A: $R_1 = 1 \implies X_1^n = M_1 \implies$ Dec. 1 has only M_1.

  - **Permissive Scheme:** $M_{12} = X_1^n \implies \boldsymbol{R_{2,\max} \geq C_{\text{Full}-\text{CSI}}}$
  - **Restricted Scheme:** $M_{12} = 0 \implies \boldsymbol{\tilde{R}_{2,\max} \leq C_{\text{Enc}-\text{CSI}}}$

$\implies$ **Binary dirty paper channel:** $Y_2 = X_2 \oplus X_1 \oplus Z$

$$\tilde{R}_{2,\max} \leq C_{\text{Enc}-\text{CSI}} < C_{\text{Full}-\text{CSI}} \leq R_{2,\max}$$

Summary

- **Soft-Covering for Strong-Secrecy:** Superposition & Multicoding.

Summary

- **Soft-Covering for Strong-Secrecy:** Superposition & Multicoding.
  - Adequate for Marton-based code constructions

Summary

- **Soft-Covering for Strong-Secrecy:** Superposition & Multicoding.
  - Adequate for Marton-based code constructions
- **Cooperative BCs with a Confidential Message:**

Summary

- **Soft-Covering for Strong-Secrecy:** Superposition & Multicoding.
  - Adequate for Marton-based code constructions
- **Cooperative BCs with a Confidential Message:**
  - Inner bound on strong-secrecy-capacity region.

Summary

- **Soft-Covering for Strong-Secrecy:** Superposition & Multicoding.
  - Adequate for Marton-based code constructions
- **Cooperative BCs with a Confidential Message:**
  - Inner bound on strong-secrecy-capacity region.
  - Restricted cooperation protocol sub-optimal in general.

Summary

- **Soft-Covering for Strong-Secrecy:** Superposition & Multicoding.
  - Adequate for Marton-based code constructions
- **Cooperative BCs with a Confidential Message:**
  - Inner bound on strong-secrecy-capacity region.
  - Restricted cooperation protocol sub-optimal in general.

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:**
     - $W \sim \text{Unif}[1 : 2^{nR'}]$ 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:**
     - 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:**
     - $W \sim \text{Unif}[1 : 2^{nR'}]$ 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:**
     - 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:**
     - $W \sim \text{Unif}[1 : 2^{nR'}]$ 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)).

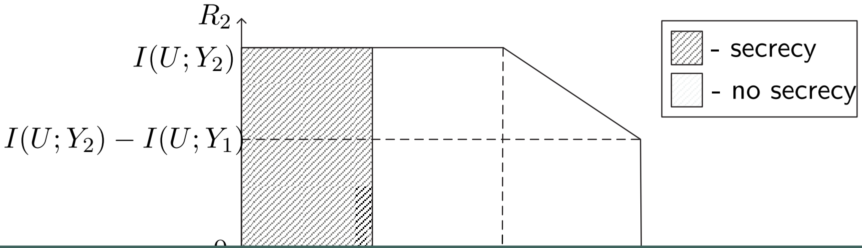
  2. **Superposition & Cooperation:**
     - No secrecy - superposition on (M_{10}, M_{20}).
     - Superposing on M_{10} violates secrecy constraint!
     - Superposition on M_{20} only.

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)	$\big(H(Y_1\|U)\,,\,I(U;Y_2)\big)$ $\big(H(Y_1)\,,\,I(U;Y_2) - I(U;Y_1)\big)$	$\big(H(Y_1\|U,Y_2)\,,\,I(U;Y_2)\big)$

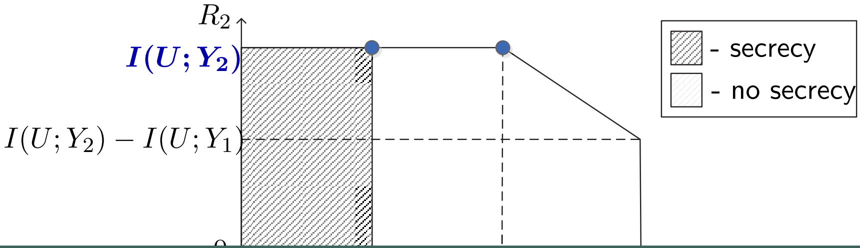
SD-BC without Cooperation - Effect of Secrecy

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)	$\left(H(Y_1\|U)\,,\,I(U;Y_2)\right)$ $\left(H(Y_1)\,,\,I(U;Y_2) - I(U;Y_1)\right)$	$\left(H(Y_1\|U,Y_2)\,,\,I(U;Y_2)\right)$



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)	$\boldsymbol{(H(Y_1\|U), I(U;Y_2))}$ $(H(Y_1), I(U;Y_2) - I(U;Y_1))$	$\boldsymbol{(H(Y_1\|U,Y_2), I(U;Y_2))}$



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!**