MIMO Gaussian Broadcast Channels with Common, Private and Confidential Messages

Ziv Goldfeld

Ben Gurion University

IEEE Information Theory Workshop

September, 2016

Motivation

- Gaussian MIMO channels - model wireless communication.

Motivation

- Gaussian MIMO channels - model wireless communication.
- Susceptibility of wireless communication to eavesdropping.

Motivation

- Gaussian MIMO channels - model wireless communication.
- Susceptibility of wireless communication to eavesdropping.
- Eavesdroppers are not always a malicious entity:

Motivation

- Gaussian MIMO channels - model wireless communication.
- Susceptibility of wireless communication to eavesdropping.
- Eavesdroppers are not always a malicious entity:
  - Legitimate recipient of some messages.

Motivation

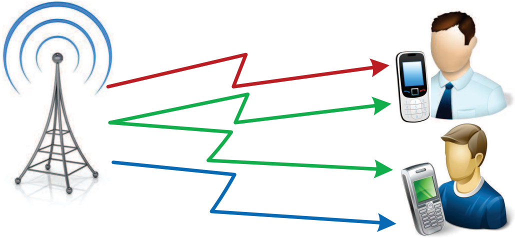
- Gaussian MIMO channels - model wireless communication.
- Susceptibility of wireless communication to eavesdropping.
- Eavesdroppers are not always a malicious entity:
  - Legitimate recipient of some messages.
  - Eavesdropper of other.

Motivation

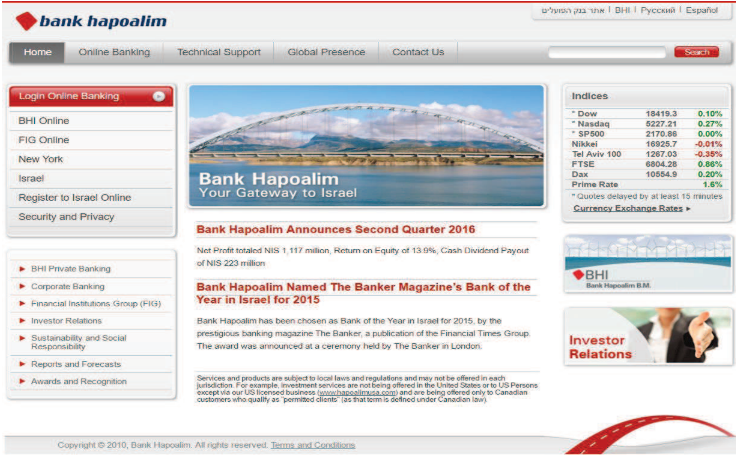
- Gaussian MIMO channels - model wireless communication.
- Susceptibility of wireless communication to eavesdropping.
- Eavesdroppers are not always a malicious entity:
  - Legitimate recipient of some messages.
  - Eavesdropper of other.
- Modern BC scenario - **Common**, **Private** and **Confidential** messages.

Motivation

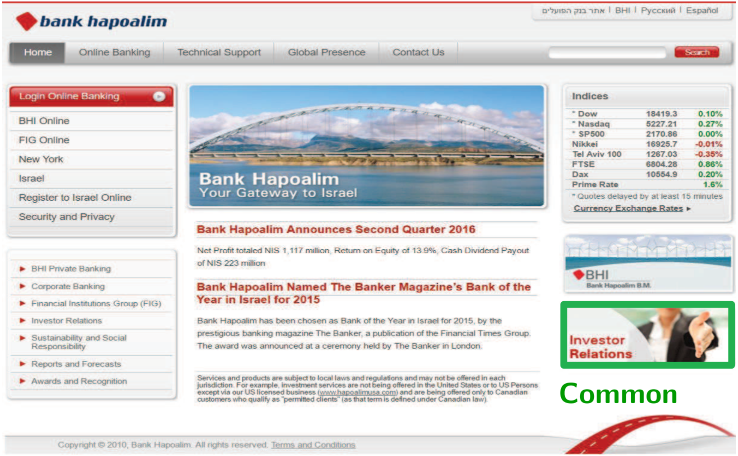
- Gaussian MIMO channels - model wireless communication.
- Susceptibility of wireless communication to eavesdropping.
- Eavesdroppers are not always a malicious entity:
  - Legitimate recipient of some messages.
  - Eavesdropper of other.
- Modern BC scenario - **Common**, **Private** and **Confidential** messages.



Motivation - Banking Site

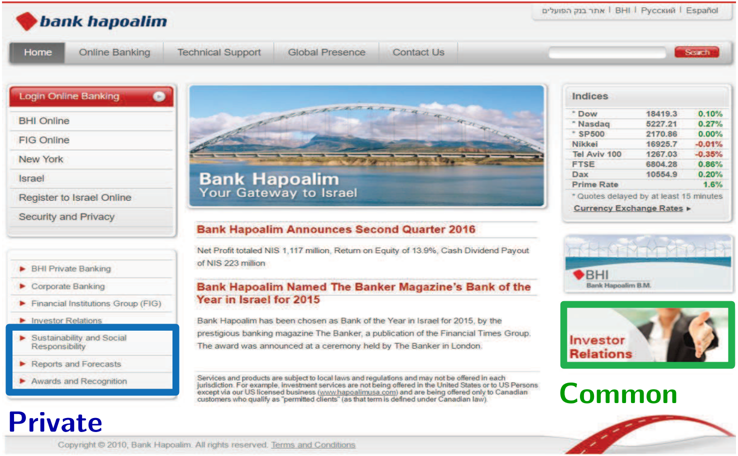


Motivation - Banking Site



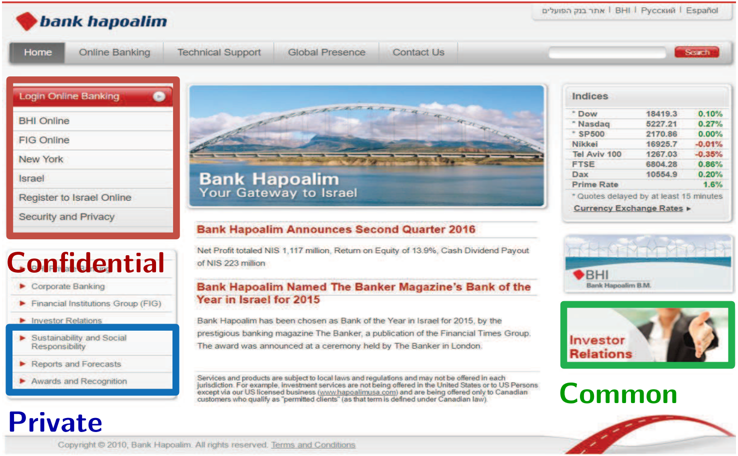
- **Common** - Advertisement.

Motivation - Banking Site



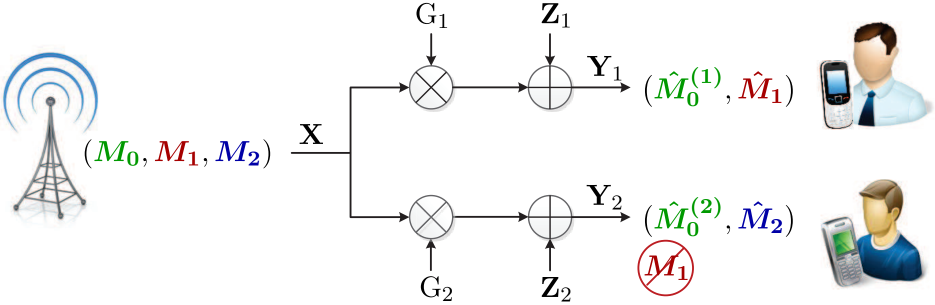
- **Common** - Advertisement.
- **Private** - On-demand Public info (programs, reports, forecasts).

Motivation - Banking Site

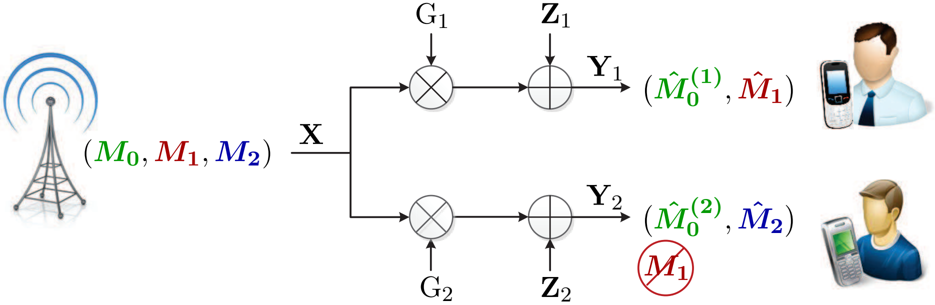


- **Common** - Advertisement.
- **Private** - On-demand Public info (programs, reports, forecasts).
- **Confidential** - Online banking (access account, transactions).

MIMO Gaussian BC - Problem Setup

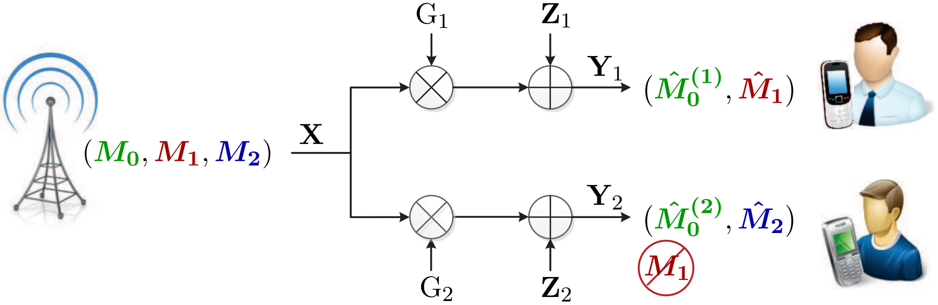


MIMO Gaussian BC - Problem Setup



User $j = 1, 2$ Observes: $\mathbf{Y}_j = \mathrm{G}_j \mathbf{X} + \mathbf{Z}_j .$

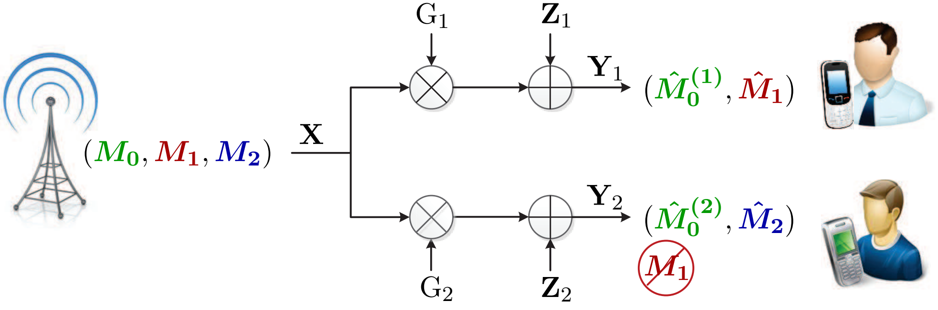
MIMO Gaussian BC - Problem Setup



User $j = 1, 2$ Observes: $\mathbf{Y}_j = G_j \mathbf{X} + \mathbf{Z}_j$.

- **Dimensions:** $\mathbf{X}, \mathbf{Y}_1, \mathbf{Y}_2, \mathbf{Z}_1, \mathbf{Z}_2 \in \mathbb{R}^t \;\; ; \; G_1, G_2 \in \mathbb{R}^{t \times t}$.

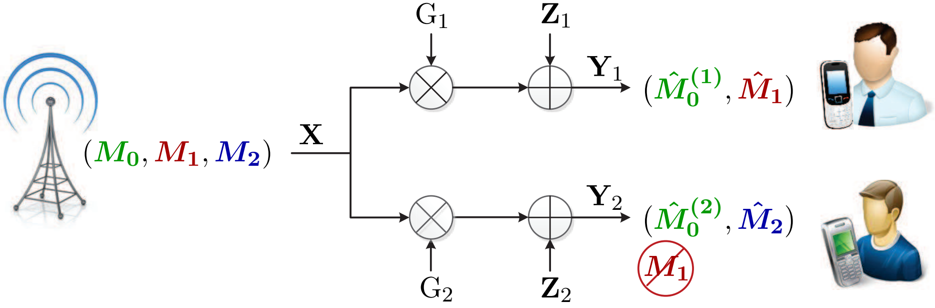
MIMO Gaussian BC - Problem Setup



User $j = 1, 2$ Observes: $\mathbf{Y}_j = \mathrm{G}_j\mathbf{X} + \mathbf{Z}_j.$

- **Dimensions:** $\mathbf{X}, \mathbf{Y}_1, \mathbf{Y}_2, \mathbf{Z}_1, \mathbf{Z}_2 \in \mathbb{R}^t$; $\mathrm{G}_1, \mathrm{G}_2 \in \mathbb{R}^{t \times t}$.
- **Noise Processes:** i.i.d. samples of $\mathbf{Z}_j \sim \mathcal{N}(\mathbf{0}, \mathrm{I}_t)$, $j = 1, 2$.

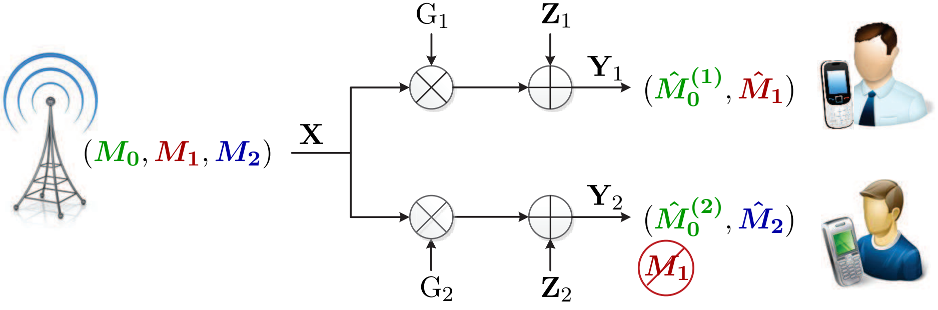
MIMO Gaussian BC - Problem Setup



User $j = 1, 2$ Observes: $\mathbf{Y}_j = \mathrm{G}_j\mathbf{X} + \mathbf{Z}_j$.

- **Dimensions:** $\mathbf{X}, \mathbf{Y}_1, \mathbf{Y}_2, \mathbf{Z}_1, \mathbf{Z}_2 \in \mathbb{R}^t$; $\mathrm{G}_1, \mathrm{G}_2 \in \mathbb{R}^{t\times t}$.
- **Noise Processes:** i.i.d. samples of $\mathbf{Z}_j \sim \mathcal{N}(\mathbf{0}, \mathrm{I}_t)$, $j = 1, 2$.
- **Input Covariance Constraint:** $\frac{1}{n}\sum_{i=1}^{n} \mathbb{E}\left[\mathbf{X}(i)\mathbf{X}^\top(i)\right] \preceq \mathrm{K}$.

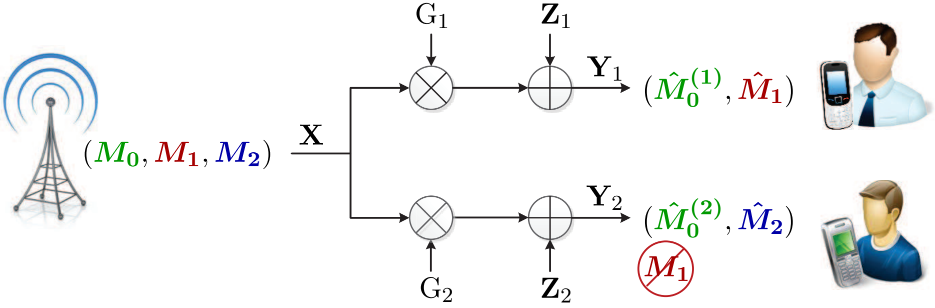
MIMO Gaussian BC - Problem Setup



User $j = 1, 2$ Observes: $\mathbf{Y}_j = \mathrm{G}_j\mathbf{X} + \mathbf{Z}_j$.

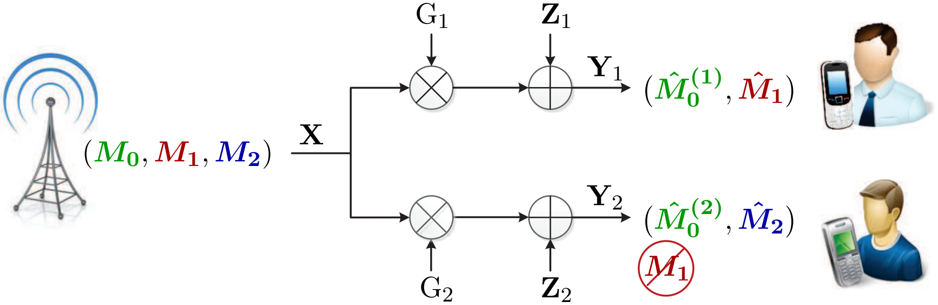
- **Dimensions:** $\mathbf{X}, \mathbf{Y}_1, \mathbf{Y}_2, \mathbf{Z}_1, \mathbf{Z}_2 \in \mathbb{R}^t$; $\mathrm{G}_1, \mathrm{G}_2 \in \mathbb{R}^{t\times t}$.
- **Noise Processes:** i.i.d. samples of $\mathbf{Z}_j \sim \mathcal{N}(\mathbf{0}, \mathrm{I}_t)$, $j = 1, 2$.
- **Input Covariance Constraint:** $\frac{1}{n}\sum_{i=1}^{n} \mathbb{E}\left[\mathbf{X}(i)\mathbf{X}^\top(i)\right] \preceq \mathrm{K}$.
- **Security Criterion:** $\frac{1}{n} I(M_1; \mathbf{Y}_2^n) \xrightarrow[n\to\infty]{} 0$.

MIMO Gaussian BC - Goals



- Known inner and outer bounds on secrecy-capacity region.

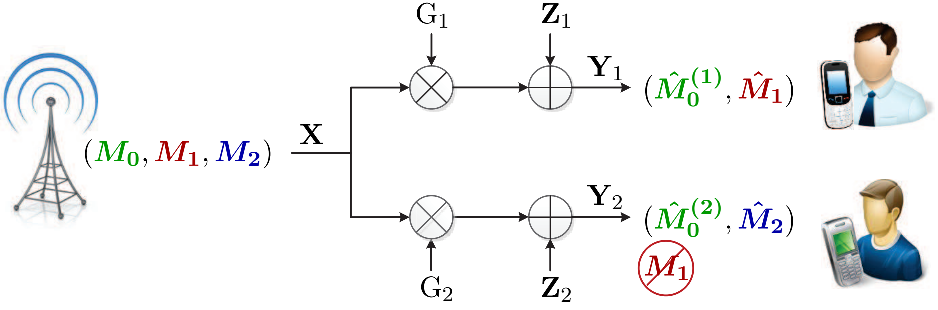
MIMO Gaussian BC - Goals



- Known inner and outer bounds on secrecy-capacity region.

  Q: Do they match for the MIMO Gaussian case?

MIMO Gaussian BC - Goals



- Known inner and outer bounds on secrecy-capacity region.

  Q: Do they match for the MIMO Gaussian case?

  Q: Do Gaussian inputs achieve boundary points?

MIMO Gaussian BC - Some Literature

MIMO Gaussian BCs with Eavesdropping Receivers:

MIMO Gaussian BC - Some Literature

MIMO Gaussian BCs with Eavesdropping Receivers:

M_0	M_1	M_2	**Solution**
—	Private	Private	Weingarten-Steinberg-Shamai 2006

MIMO Gaussian BC - Some Literature

MIMO Gaussian BCs with Eavesdropping Receivers:

M_0	M_1	M_2	**Solution**
—	Private	Private	Weingarten-Steinberg-Shamai 2006
Public	Private	Private	Geng-Nair 2014

MIMO Gaussian BC - Some Literature

MIMO Gaussian BCs with Eavesdropping Receivers:

M_0	M_1	M_2	**Solution**
—	Private	Private	Weingarten-Steinberg-Shamai 2006
Public	Private	Private	Geng-Nair 2014
Public	Secret	—	Ly-Liu-Liang 2010

MIMO Gaussian BC - Some Literature

MIMO Gaussian BCs with Eavesdropping Receivers:

M_0	M_1	M_2	Solution
—	Private	Private	Weingarten-Steinberg-Shamai 2006
Public	Private	Private	Geng-Nair 2014
Public	Secret	—	Ly-Liu-Liang 2010
—	Secret	Secret	Liu-Liu-Poor-Shamai 2010

MIMO Gaussian BC - Some Literature

MIMO Gaussian BCs with Eavesdropping Receivers:

M_0	M_1	M_2	Solution
—	Private	Private	Weingarten-Steinberg-Shamai 2006
Public	Private	Private	Geng-Nair 2014
Public	Secret	—	Ly-Liu-Liang 2010
—	Secret	Secret	Liu-Liu-Poor-Shamai 2010
Public	Secret	Secret	Ekrem-Ulukus 2012

MIMO Gaussian BC - Some Literature

MIMO Gaussian BCs with Eavesdropping Receivers:

M_0	M_1	M_2	Solution
—	Private	Private	Weingarten-Steinberg-Shamai 2006
Public	Private	Private	Geng-Nair 2014
Public	Secret	—	Ly-Liu-Liang 2010
—	Secret	Secret	Liu-Liu-Poor-Shamai 2010
Public	Secret	Secret	Ekrem-Ulukus 2012
—	Secret	Private	

MIMO Gaussian BC - Some Literature

MIMO Gaussian BCs with Eavesdropping Receivers:

M_0	M_1	M_2	Solution
—	Private	Private	Weingarten-Steinberg-Shamai 2006
Public	Private	Private	Geng-Nair 2014
Public	Secret	—	Ly-Liu-Liang 2010
—	Secret	Secret	Liu-Liu-Poor-Shamai 2010
Public	Secret	Secret	Ekrem-Ulukus 2012
—	Secret	Private	
Public	Secret	Private	

MIMO Gaussian BC - Some Literature

MIMO Gaussian BCs with Eavesdropping Receivers:

M_0	M_1	M_2	**Solution**
—	Private	Private	Weingarten-Steinberg-Shamai 2006
Public	Private	Private	Geng-Nair 2014
Public	Secret	—	Ly-Liu-Liang 2010
—	Secret	Secret	Liu-Liu-Poor-Shamai 2010
Public	Secret	Secret	Ekrem-Ulukus 2012
—	Secret	Private	**This work**
Public	Secret	Private	**This work**

MIMO Gaussian BC - Some Literature

MIMO Gaussian BCs with Eavesdropping Receivers:

M_0	M_1	M_2	Solution
—	Private	Private	Weingarten-Steinberg-Shamai 2006
Public	Private	Private	**Geng-Nair 2014**
Public	Secret	—	Ly-Liu-Liang 2010
—	Secret	Secret	Liu-Liu-Poor-Shamai 2010
Public	Secret	Secret	Ekrem-Ulukus 2012
—	Secret	Private	**This work**
Public	Secret	Private	**This work**

⋆ Solution for two last unsolved cases via **Upper Concave Envelopes** ⋆

MIMO Gaussian BC - Secrecy-Capacity Results

Without a Common Message: M_1 - Confidential ; M_2 - Private

Theorem (ZG 2016)

The secrecy-capacity region for a covariance constraint $\mathrm{K} \succeq 0$ *is*

$$\hat{\mathcal{C}}_{\mathrm{K}} = \bigcup_{0 \preceq \mathrm{K}^\star \preceq \mathrm{K}} \left\{ (R_1, R_2) \in \mathbb{R}_+^2 \;\middle|\; \begin{array}{l} R_1 \leq \frac{1}{2} \log \left| \dfrac{\mathrm{I} + \mathrm{G}_1 \mathrm{K}^\star \mathrm{G}_1^\top}{\mathrm{I} + \mathrm{G}_2 \mathrm{K}^\star \mathrm{G}_2^\top} \right| \\ R_2 \leq \frac{1}{2} \log \left| \dfrac{\mathrm{I} + \mathrm{G}_2 \mathrm{K} \mathrm{G}_2^\top}{\mathrm{I} + \mathrm{G}_2 \mathrm{K}^\star \mathrm{G}_2^\top} \right| \end{array} \right\}.$$

MIMO Gaussian BC - Secrecy-Capacity Results

Without a Common Message: M_1 - Confidential ; M_2 - Private

Theorem (ZG 2016)

The secrecy-capacity region for a covariance constraint $\mathrm{K} \succeq 0$ *is*

$$\hat{\mathcal{C}}_{\mathrm{K}} = \bigcup_{0 \preceq \mathrm{K}^\star \preceq \mathrm{K}} \left\{ (R_1, R_2) \in \mathbb{R}_+^2 \;\middle|\; \begin{array}{l} R_1 \leq \frac{1}{2} \log \left| \frac{\mathbf{I} + \mathbf{G}_1 \mathbf{K}^\star \mathbf{G}_1^\top}{\mathbf{I} + \mathbf{G}_2 \mathbf{K}^\star \mathbf{G}_2^\top} \right| \\ R_2 \leq \frac{1}{2} \log \left| \frac{\mathrm{I} + \mathrm{G}_2 \mathrm{K} \mathrm{G}_2^\top}{\mathrm{I} + \mathrm{G}_2 \mathrm{K}^\star \mathrm{G}_2^\top} \right| \end{array} \right\}.$$

- **R_1 Bound - MIMO Gaussian WTC Secrecy-capacity:**
  User 1 - Legitimate with input covariance $\mathrm{K}^\star$; User 2- Eavesdropper.

MIMO Gaussian BC - Secrecy-Capacity Results

Without a Common Message: M_1 - Confidential ; M_2 - Private

Theorem (ZG 2016)

The secrecy-capacity region for a covariance constraint $\mathrm{K} \succeq 0$ *is*

$$\hat{\mathcal{C}}_{\mathrm{K}} = \bigcup_{0 \preceq \mathrm{K}^\star \preceq \mathrm{K}} \left\{ (R_1, R_2) \in \mathbb{R}_+^2 \;\middle|\; \begin{array}{l} R_1 \leq \frac{1}{2} \log \left| \frac{\mathrm{I} + \mathrm{G}_1 \mathrm{K}^\star \mathrm{G}_1^\top}{\mathrm{I} + \mathrm{G}_2 \mathrm{K}^\star \mathrm{G}_2^\top} \right| \\ R_2 \leq \frac{1}{2} \log \left| \frac{\mathbf{I} + \mathbf{G}_2 \mathbf{K} \mathbf{G}_2^\top}{\mathbf{I} + \mathbf{G}_2 \mathbf{K}^\star \mathbf{G}_2^\top} \right| \end{array} \right\}.$$

- R_1 Bound - MIMO Gaussian WTC Secrecy-capacity:
  User 1 - Legitimate with input covariance $\mathrm{K}^\star$; User 2- Eavesdropper.
- $\boldsymbol{R_2}$ **Bound - Capacity of MIMO Gaussian PTP to User 2:**
  Input covariance $\mathrm{K} - \mathrm{K}^\star$; Noise covariance $\mathrm{I} + \mathrm{G}_2 \mathrm{K}^\star \mathrm{G}_2^\top$.

MIMO Gaussian BC - Secrecy-Capacity Results

M_0 - Common ; M_1 - Confidential ; M_2 - Private

Theorem (ZG 2016)

The secrecy-capacity region for a covariance constraint $\mathrm{K} \succeq 0$ *is*

$$\mathcal{C}_{\mathrm{K}} = \bigcup_{\substack{0 \preceq \mathrm{K}_1, \mathrm{K}_2: \\ \mathrm{K}_1 + \mathrm{K}_2 \preceq \mathrm{K}}} \left\{ \begin{array}{l} R_0 \leq \min_{j=1,2} \left\{ \frac{1}{2} \log \left| \frac{\mathrm{I} + \mathrm{G}_j \mathrm{K} \mathrm{G}_j^\top}{\mathrm{I} + \mathrm{G}_j(\mathrm{K}_1 + \mathrm{K}_2)\mathrm{G}_j^\top} \right| \right\} \\ R_1 \leq \frac{1}{2} \log \left| \frac{\mathrm{I} + \mathrm{G}_1 \mathrm{K}_1 \mathrm{G}_1^\top}{\mathrm{I} + \mathrm{G}_2 \mathrm{K}_1 \mathrm{G}_2^\top} \right| \\ R_2 \leq \frac{1}{2} \log \left| \frac{\mathrm{I} + \mathrm{G}_2(\mathrm{K}_1 + \mathrm{K}_2)\mathrm{G}_2^\top}{\mathrm{I} + \mathrm{G}_2 \mathrm{K}_1 \mathrm{G}_2^\top} \right| \end{array} \right\}.$$

MIMO Gaussian BC - Secrecy-Capacity Results

M_0 - **Common** ; M_1 - **Confidential** ; M_2 - **Private**

Theorem (ZG 2016)

The secrecy-capacity region for a covariance constraint $\mathrm{K} \succeq 0$ *is*

$$\mathcal{C}_\mathrm{K} = \bigcup_{\substack{0 \preceq \mathrm{K}_1, \mathrm{K}_2: \\ \mathrm{K}_1 + \mathrm{K}_2 \preceq \mathrm{K}}} \left\{ \begin{array}{l} R_0 \leq \min_{j=1,2} \left\{ \frac{1}{2} \log \left| \frac{\mathrm{I} + \mathrm{G}_j \mathrm{K} \mathrm{G}_j^\top}{\mathrm{I} + \mathrm{G}_j (\mathrm{K}_1 + \mathrm{K}_2) \mathrm{G}_j^\top} \right| \right\} \\ R_1 \leq \boldsymbol{\frac{1}{2} \log \left| \frac{\mathrm{I} + \mathrm{G}_1 \mathrm{K}_1 \mathrm{G}_1^\top}{\mathrm{I} + \mathrm{G}_2 \mathrm{K}_1 \mathrm{G}_2^\top} \right|} \\ R_2 \leq \frac{1}{2} \log \left| \frac{\mathrm{I} + \mathrm{G}_2 (\mathrm{K}_1 + \mathrm{K}_2) \mathrm{G}_2^\top}{\mathrm{I} + \mathrm{G}_2 \mathrm{K}_1 \mathrm{G}_2^\top} \right| \end{array} \right\}.$$

- R_1 **Bound: MIMO Gaussian WTC with input** K_1

MIMO Gaussian BC - Secrecy-Capacity Results

M_0 - Common ; M_1 - Confidential ; M_2 - Private

Theorem (ZG 2016)

The secrecy-capacity region for a covariance constraint $\mathrm{K} \succeq 0$ *is*

$$\mathcal{C}_{\mathrm{K}} = \bigcup_{\substack{0 \preceq \mathrm{K}_1, \mathrm{K}_2: \\ \mathrm{K}_1 + \mathrm{K}_2 \preceq \mathrm{K}}} \left\{ \begin{array}{l} R_0 \leq \min_{j=1,2} \left\{ \frac{1}{2} \log \left| \frac{\mathrm{I} + \mathrm{G}_j \mathrm{K} \mathrm{G}_j^\top}{\mathrm{I} + \mathrm{G}_j (\mathrm{K}_1 + \mathrm{K}_2) \mathrm{G}_j^\top} \right| \right\} \\ R_1 \leq \frac{1}{2} \log \left| \frac{\mathrm{I} + \mathrm{G}_1 \mathrm{K}_1 \mathrm{G}_1^\top}{\mathrm{I} + \mathrm{G}_2 \mathrm{K}_1 \mathrm{G}_2^\top} \right| \\ R_2 \leq \frac{1}{2} \log \left| \frac{\mathrm{I} + \mathrm{G}_2 (\mathrm{K}_1 + \mathrm{K}_2) \mathrm{G}_2^\top}{\mathrm{I} + \mathrm{G}_2 \mathrm{K}_1 \mathrm{G}_2^\top} \right| \end{array} \right\}.$$

- R_1 Bound: MIMO Gaussian WTC with input K_1
- **R_2 Bound: MIMO Gaussian PTP with input K_2 (K_1 is noise).**

MIMO Gaussian BC - Secrecy-Capacity Results

M_0 - Common ; M_1 - Confidential ; M_2 - Private

Theorem (ZG 2016)

The secrecy-capacity region for a covariance constraint $\mathrm{K} \succeq 0$ *is*

$$\mathcal{C}_{\mathrm{K}} = \bigcup_{\substack{0 \preceq \mathrm{K}_1, \mathrm{K}_2: \\ \mathrm{K}_1 + \mathrm{K}_2 \preceq \mathrm{K}}} \left\{ \begin{array}{l} R_0 \leq \min_{j=1,2} \left\{ \frac{1}{2} \log \left| \frac{\mathbf{I} + \mathbf{G}_j \mathbf{K} \mathbf{G}_j^\top}{\mathbf{I} + \mathbf{G}_j (\mathbf{K}_1 + \mathbf{K}_2) \mathbf{G}_j^\top} \right| \right\} \\ R_1 \leq \frac{1}{2} \log \left| \frac{\mathrm{I} + \mathrm{G}_1 \mathrm{K}_1 \mathrm{G}_1^\top}{\mathrm{I} + \mathrm{G}_2 \mathrm{K}_1 \mathrm{G}_2^\top} \right| \\ R_2 \leq \frac{1}{2} \log \left| \frac{\mathrm{I} + \mathrm{G}_2 (\mathrm{K}_1 + \mathrm{K}_2) \mathrm{G}_2^\top}{\mathrm{I} + \mathrm{G}_2 \mathrm{K}_1 \mathrm{G}_2^\top} \right| \end{array} \right\}.$$

- R_1 Bound: MIMO Gaussian WTC with input K_1
- R_2 Bound: MIMO Gaussian PTP with input K_2 (K_1 is noise).
- **R_0 Bound: MIMO Gaussian PTP with remaining covariance $\mathbf{K} - (\mathbf{K}_1 + \mathbf{K}_2)$ ($\mathbf{K}_1, \mathbf{K}_2$ are noises).**

Secrecy-Capacity without M_0 - Proof Outline

Outer Bound:

Secrecy-Capacity without M_0 - Proof Outline

Outer Bound: Fix a covariance constraint $K \succeq 0$.

Secrecy-Capacity without M_0 - Proof Outline

Outer Bound: Fix a covariance constraint $K \succeq 0$.

1. **[ZG-Kramer-Permuter 2016]**

Secrecy-Capacity without M_0 - Proof Outline

Outer Bound: Fix a covariance constraint $K \succeq 0$.

1. **[ZG-Kramer-Permuter 2016]** $\implies$ $\mathcal{I}_{\mathbf{K}} \subseteq \hat{\mathcal{C}}_{\mathbf{K}} \subseteq \mathcal{O}_{\mathbf{K}}$

Secrecy-Capacity without M_0 - Proof Outline

Outer Bound: Fix a covariance constraint $K \succeq 0$.

1. [ZG-Kramer-Permuter 2016] $\implies$ $\mathcal{I}_\mathrm{K} \subseteq \hat{\mathcal{C}}_\mathrm{K} \subseteq \mathcal{O}_\mathrm{K}$
2. **$\mathcal{O}_\mathbf{K}$ bounded & convex**

Secrecy-Capacity without M_0 - Proof Outline

Outer Bound: Fix a covariance constraint $K \succeq 0$.

1. [ZG-Kramer-Permuter 2016] $\Longrightarrow$ $\mathcal{I}_{\mathrm{K}} \subseteq \hat{\mathcal{C}}_{\mathrm{K}} \subseteq \mathcal{O}_{\mathrm{K}}$

2. **$\mathcal{O}_{\mathbf{K}}$ bounded & convex** $\Longrightarrow$ **Supporting hyperplanes**

$$\max_{(R_1,R_2)\in\mathcal{O}_{\mathbf{K}}} \lambda_1 R_1 + \lambda_2 R_2$$

Secrecy-Capacity without M_0 - Proof Outline

Outer Bound: Fix a covariance constraint $K \succeq 0$.

1. [ZG-Kramer-Permuter 2016] $\implies$ $\mathcal{I}_{\mathrm{K}} \subseteq \hat{\mathcal{C}}_{\mathrm{K}} \subseteq \mathcal{O}_{\mathrm{K}}$
2. $\mathcal{O}_{\mathrm{K}}$ bounded & convex $\implies$ Supporting hyperplanes
$$\max_{(R_1,R_2)\in\mathcal{O}_{\mathrm{K}}} \lambda_1 R_1 + \lambda_2 R_2$$
3. $$\boldsymbol{\max_{(R_1,R_2)\in\mathcal{O}_{\mathrm{K}}} \lambda_1 R_1 + \lambda_2 R_2}$$

Secrecy-Capacity without M_0 - Proof Outline

Outer Bound: Fix a covariance constraint $K \succeq 0$.

1. [ZG-Kramer-Permuter 2016] $\Longrightarrow$ $\mathcal{I}_{\mathrm{K}} \subseteq \hat{\mathcal{C}}_{\mathrm{K}} \subseteq \mathcal{O}_{\mathrm{K}}$
2. $\mathcal{O}_{\mathrm{K}}$ bounded & convex $\Longrightarrow$ Supporting hyperplanes
$$\max_{(R_1,R_2)\in\mathcal{O}_{\mathrm{K}}} \lambda_1 R_1 + \lambda_2 R_2$$
3. $\max_{(R_1,R_2)\in\mathcal{O}_{\mathrm{K}}} \lambda_1 R_1 + \lambda_2 R_2 \leq$ **Upper Concave Envelope**

Secrecy-Capacity without M_0 - Proof Outline

Outer Bound: Fix a covariance constraint $K \succeq 0$.

1. [ZG-Kramer-Permuter 2016] $\Longrightarrow$ $\mathcal{I}_{\mathrm{K}} \subseteq \hat{\mathcal{C}}_{\mathrm{K}} \subseteq \mathcal{O}_{\mathrm{K}}$
2. $\mathcal{O}_{\mathrm{K}}$ bounded & convex $\Longrightarrow$ Supporting hyperplanes
$$\max_{(R_1,R_2)\in\mathcal{O}_{\mathrm{K}}} \lambda_1 R_1 + \lambda_2 R_2$$
3. $\max_{(R_1,R_2)\in\mathcal{O}_{\mathrm{K}}} \lambda_1 R_1 + \lambda_2 R_2 \leq$ Upper Concave Envelope
4. **UCE maximized by Gaussian inputs**

Secrecy-Capacity without M_0 - Proof Outline

Outer Bound: Fix a covariance constraint $K \succeq 0$.

1. [ZG-Kramer-Permuter 2016] $\implies$ $\mathcal{I}_\mathrm{K} \subseteq \hat{\mathcal{C}}_\mathrm{K} \subseteq \mathcal{O}_\mathrm{K}$
2. $\mathcal{O}_\mathrm{K}$ bounded & convex $\implies$ Supporting hyperplanes
$$\max_{(R_1,R_2)\in\mathcal{O}_\mathrm{K}} \lambda_1 R_1 + \lambda_2 R_2$$
3. $\max_{(R_1,R_2)\in\mathcal{O}_\mathrm{K}} \lambda_1 R_1 + \lambda_2 R_2 \leq$ Upper Concave Envelope
4. **UCE maximized by Gaussian inputs**

$\implies$ $\boldsymbol{\mathcal{O}_\mathrm{K}} \subseteq$ **Region from Theorem**

Secrecy-Capacity without M_0 - Proof Outline

Achievevability:

Secrecy-Capacity without M_0 - Proof Outline

Achievability: Substituting Gaussian inputs into $\mathcal{I}_{\mathrm{K}}$.

Secrecy-Capacity without M_0 - Proof Outline

Achievability: Substituting Gaussian inputs into $\mathcal{I}_{\mathrm{K}}$.

- **Dirty Paper Coding to cancel M_2 signal at Receiver 1.**

Secrecy-Capacity without M_0 - Proof Outline

Achievability: Substituting Gaussian inputs into $\mathcal{I}_{\mathrm{K}}$.

- Dirty Paper Coding to cancel M_2 signal at Receiver 1.

  ⋆ **Other variant of DPC (cancel M_1 at Rec. 2) not necessary.**

Secrecy-Capacity without M_0 - Proof Outline

Achievability: Substituting Gaussian inputs into $\mathcal{I}_{\mathrm{K}}$.

- Dirty Paper Coding to cancel M_2 signal at Receiver 1.
  - ★ Other variant of DPC (cancel M_1 at Rec. 2) not necessary.

$$\Downarrow$$

Region from Theorem $\subseteq$ $\boldsymbol{\mathcal{I}_{\mathrm{K}}}$

Secrecy-Capacity without M_0 - Proof Outline

Achievability: Substituting Gaussian inputs into $\mathcal{I}_{\mathrm{K}}$.

- Dirty Paper Coding to cancel M_2 signal at Receiver 1.
  - ★ Other variant of DPC (cancel M_1 at Rec. 2) not necessary.

$$\Downarrow$$

$$\mathcal{O}_{\mathbf{K}} \quad \subseteq \quad \textbf{Region from Theorem} \quad \subseteq \quad \mathcal{I}_{\mathbf{K}}$$

Secrecy-Capacity without M_0 - Proof Outline

Achievability: Substituting Gaussian inputs into $\mathcal{I}_{\mathrm{K}}$.

- Dirty Paper Coding to cancel M_2 signal at Receiver 1.
  - ★ Other variant of DPC (cancel M_1 at Rec. 2) not necessary.

$$\Downarrow$$

$$\mathcal{O}_{\mathbf{K}} \quad \subseteq \quad \textbf{Region from Theorem} \quad \subseteq \quad \mathcal{I}_{\mathbf{K}}$$

$$\Downarrow$$

$$\boxed{\mathcal{O}_{\mathbf{K}} \quad = \quad \textbf{Region from Theorem} \quad = \quad \mathcal{I}_{\mathbf{K}}}$$

■

Secrecy-Capacity without M_0 - Visualization

Secrecy-Capacity Region under Average Power Constraint:

Secrecy-Capacity without M_0 - Visualization

Secrecy-Capacity Region under Average Power Constraint:

- **Corollary:**

Secrecy-Capacity without M_0 - Visualization

Secrecy-Capacity Region under Average Power Constraint:

- **Corollary:** $$\frac{1}{n}\sum_{i=1}^{n}\mathbb{E}\left[\left|\left|\mathbf{X}(i)\right|\right|^2\right] \leq P$$

Secrecy-Capacity without M_0 - Visualization

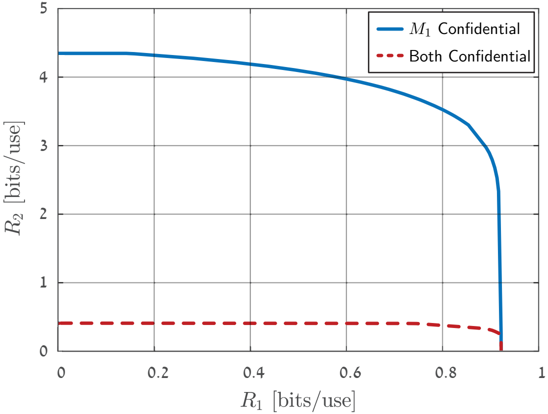
Secrecy-Capacity Region under Average Power Constraint:

- **Corollary:** $$\frac{1}{n}\sum_{i=1}^{n}\mathbb{E}\left[\left|\left|\mathbf{X}(i)\right|\right|^2\right]\leq P \quad \Longrightarrow \quad \hat{\mathcal{C}}_P = \bigcup_{\substack{0\preceq \mathrm{K}:\\ \mathrm{Tr}(\mathrm{K})\leq P}} \hat{\mathcal{C}}_{\mathrm{K}}$$

Secrecy-Capacity without M_0 - Visualization

Secrecy-Capacity Region under Average Power Constraint:

- **Corollary:** $$\frac{1}{n}\sum_{i=1}^{n}\mathbb{E}\left[\left|\left|\mathbf{X}(i)\right|\right|^2\right]\leq P \quad\Longrightarrow\quad \hat{\mathcal{C}}_P=\bigcup_{\substack{0\preceq\mathrm{K}:\\ \mathrm{Tr}(\mathrm{K})\leq P}}\hat{\mathcal{C}}_{\mathrm{K}}$$



Summary

- **MIMO Gaussian BC - Common, Private and Conf. Messages:**

Summary

- **MIMO Gaussian BC - Common, Private and Conf. Messages:**
  - **Practical:** Natural broadcasting scenario.

Summary

- **MIMO Gaussian BC - Common, Private and Conf. Messages:**
  - **Practical:** Natural broadcasting scenario.
  - **Theoretical:** Last two unsolved cases.

Summary

- **MIMO Gaussian BC - Common, Private and Conf. Messages:**
  - **Practical:** Natural broadcasting scenario.
  - **Theoretical:** Last two unsolved cases.
- **Secrecy-Sapacity Results:**

Summary

- **MIMO Gaussian BC - Common, Private and Conf. Messages:**
  - **Practical:** Natural broadcasting scenario.
  - **Theoretical:** Last two unsolved cases.
- **Secrecy-Sapacity Results:**
  - Characterization & Optimality of Gaussian inputs.

Summary

- **MIMO Gaussian BC - Common, Private and Conf. Messages:**
  - **Practical:** Natural broadcasting scenario.
  - **Theoretical:** Last two unsolved cases.
- **Secrecy-Sapacity Results:**
  - Characterization & Optimality of Gaussian inputs.
  - Proof via **Upper Concave Envelopes** & **Dirty-Paper Coding**.

Summary

- **MIMO Gaussian BC - Common, Private and Conf. Messages:**
  - **Practical:** Natural broadcasting scenario.
  - **Theoretical:** Last two unsolved cases.
- **Secrecy-Sapacity Results:**
  - Characterization & Optimality of Gaussian inputs.
  - Proof via **Upper Concave Envelopes** & **Dirty-Paper Coding**.

Thank You!