

# 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

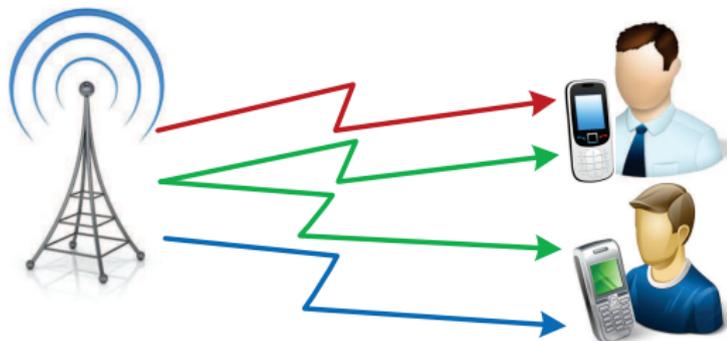
- Gaussian MIMO channels - model wireless communication.
- Susceptibility of wireless communication to eavesdropping.
- Eavesdroppers are not always a malicious entity:
  - ▶ Legitimate recipient of some messages.
  - ▶ Eavesdropper of other.

# 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

The screenshot shows the Bank Hapoalim website homepage. At the top left is the Bank Hapoalim logo. To the right, there are language options: "אתר בנק הופולימ | BHI | Русский | Español". Below the logo is a navigation menu with "Home", "Online Banking", "Technical Support", "Global Presence", and "Contact Us". A search bar is located to the right of the navigation menu. On the left side, there is a "Login Online Banking" button and a list of links: "BHI Online", "FIG Online", "New York", "Israel", "Register to Israel Online", and "Security and Privacy". Below this is another list of links: "BHI Private Banking", "Corporate Banking", "Financial Institutions Group (FIG)", "Investor Relations", "Sustainability and Social Responsibility", "Reports and Forecasts", and "Awards and Recognition". The main content area features a large image of a modern building with a curved roof, with the text "Bank Hapoalim Your Gateway to Israel" overlaid. Below this image is a section titled "Bank Hapoalim Announces Second Quarter 2016" with the text "Net Profit totaled NIS 1,117 million, Return on Equity of 13.9%, Cash Dividend Payout of NIS 223 million". This is followed by a section titled "Bank Hapoalim Named The Banker Magazine's Bank of the Year in Israel for 2015" with the text "Bank Hapoalim has been chosen as Bank of the Year in Israel for 2015, by the prestigious banking magazine The Banker, a publication of the Financial Times Group. The award was announced at a ceremony held by The Banker in London." Below this is a disclaimer: "Services and products are subject to local laws and regulations and may not be offered in each jurisdiction. For example, investment services are not being offered in the United States or to US Persons except via our US licensed business (www.hapoalimusa.com) and are being offered only to Canadian customers who qualify as 'permitted clients' (as that term is defined under Canadian law)." On the right side, there is a "Indices" section with a table of market data:

Indices	Value	Change
* Dow	18419.3	0.10%
* Nasdaq	5227.21	0.27%
* SP500	2170.86	0.00%
Nikkei	16925.7	-0.01%
Tel Aviv 100	1267.03	-0.35%
FTSE	6804.28	0.56%
Dax	10554.9	0.20%
Prime Rate		1.6%

\* Quotes delayed by at least 15 minutes  
[Currency Exchange Rates](#)

Below the indices section is a "BHI Bank Hapoalim B.M." logo and an "Investor Relations" section with an image of a person in a suit pointing.

At the bottom of the page, there is a copyright notice: "Copyright © 2010, Bank Hapoalim. All rights reserved. [Terms and Conditions](#)".

# Motivation - Banking Site

**bank hapoalim** | אתר בנק הופולימ | BHI | Русский | Español

Home | Online Banking | Technical Support | Global Presence | Contact Us

Login Online Banking

- BHI Online
- FIG Online
- New York
- Israel
- Register to Israel Online
- Security and Privacy

▶ BHI Private Banking

▶ Corporate Banking

▶ Financial Institutions Group (FIG)

▶ Investor Relations

▶ Sustainability and Social Responsibility

▶ Reports and Forecasts

▶ Awards and Recognition

**Bank Hapoalim**  
Your Gateway to Israel

**Bank Hapoalim Announces Second Quarter 2016**

Net Profit totaled NIS 1,117 million, Return on Equity of 13.9%, Cash Dividend Payout of NIS 223 million

**Bank Hapoalim Named The Banker Magazine's Bank of the Year in Israel for 2015**

Bank Hapoalim has been chosen as Bank of the Year in Israel for 2015, by the prestigious banking magazine The Banker, a publication of the Financial Times Group. The award was announced at a ceremony held by The Banker in London.

Services and products are subject to local laws and regulations and may not be offered in each jurisdiction. For example, investment services are not being offered in the United States or to US Persons except via our US licensed business ([www.hapoalimusa.com](http://www.hapoalimusa.com)) and are being offered only to Canadian customers who qualify as "permitted clients" (as that term is defined under Canadian law).

**Indices**

Dow	18419.3	0.10%
Nasdaq	5227.21	0.27%
SP500	2170.86	0.00%
Nikkei	16925.7	-0.01%
Tel Aviv 100	1267.03	-0.35%
FTSE	6804.28	0.86%
Dax	10554.9	0.20%
Prime Rate		1.6%

\* Quotes delayed by at least 15 minutes  
Currency Exchange Rates ▶

**BHI**  
Bank Hapoalim B.M.

**Investor Relations**

**Common**

Copyright © 2010, Bank Hapoalim. All rights reserved. [Terms and Conditions](#)

- **Common** - Advertisement.

# Motivation - Banking Site

The screenshot shows the Bank Hapoalim website with the following elements:

- Header:** Bank Hapoalim logo and navigation links: Home, Online Banking, Technical Support, Global Presence, Contact Us. Language options: עברית | BHI | Русский | Español.
- Left Sidebar:** Login Online Banking (with a dropdown arrow), BHI Online, FIG Online, New York, Israel, Register to Israel Online, Security and Privacy. A second menu lists: BHI Private Banking, Corporate Banking, Financial Institutions Group (FIG), Investor Relations, Sustainability and Social Responsibility (highlighted with a blue box), Reports and Forecasts, Awards and Recognition.
- Main Content:** A large banner image of a bridge over water with the text "Bank Hapoalim Your Gateway to Israel". Below it, a news headline: "Bank Hapoalim Announces Second Quarter 2016" with subtext: "Net Profit totaled NIS 1,117 million, Return on Equity of 13.9%, Cash Dividend Payout of NIS 223 million". Another headline: "Bank Hapoalim Named The Banker Magazine's Bank of the Year in Israel for 2015" with subtext: "Bank Hapoalim has been chosen as Bank of the Year in Israel for 2015, by the prestigious banking magazine The Banker, a publication of the Financial Times Group. The award was announced at a ceremony held by The Banker in London." A small disclaimer at the bottom of the main content area states: "Services and products are subject to local laws and regulations and may not be offered in each jurisdiction. For example, investment services are not being offered in the United States or to US Persons except via our US licensed business (www.hapoalimusa.com) and are being offered only to Canadian customers who qualify as 'permitted clients' (as that term is defined under Canadian law)."
- Right Sidebar:** "Indices" table:

Dow	18419.3	0.10%
Nasdaq	5227.21	0.27%
SP500	2170.86	0.00%
Nikkei	16925.7	-0.01%
Tel Aviv 100	1267.03	-0.35%
FTSE	6804.28	0.86%
Dax	10554.9	0.20%
Prime Rate		1.6%

Below the table: "Quotes delayed by at least 15 minutes" and "Currency Exchange Rates ▶". Below that is a "BHI Bank Hapoalim B.M." logo and a "Common" advertisement for "Investor Relations" featuring a person in a suit.

Private

Common

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

# Motivation - Banking Site

The screenshot shows the Bank Hapoalim website with the following elements:

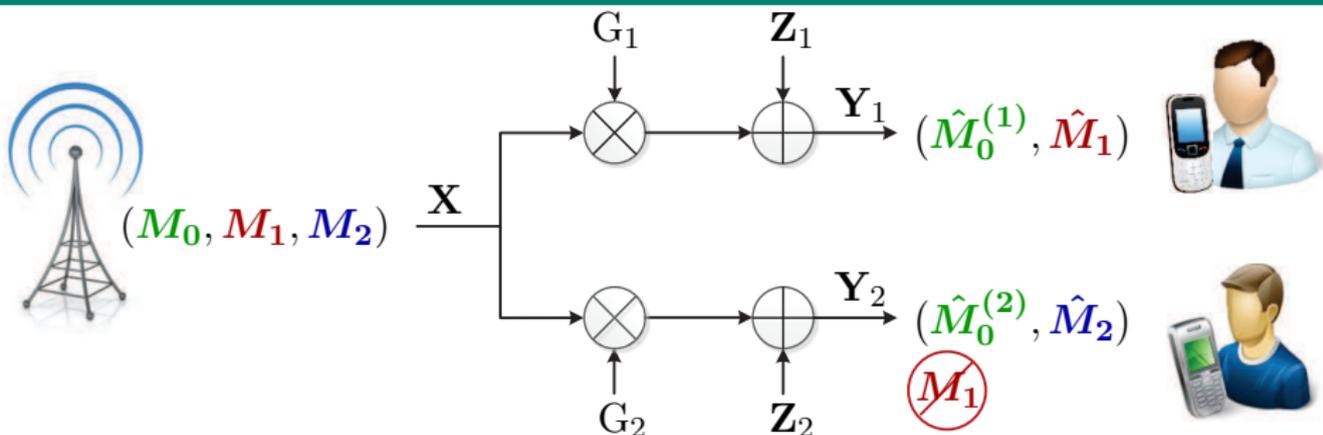
- Header:** Bank Hapoalim logo, navigation menu (Home, Online Banking, Technical Support, Global Presence, Contact Us), and language options (אזורי בנק המזרחיים | BHI | Русский | Español).
- Navigation:** Home, Online Banking, Technical Support, Global Presence, Contact Us.
- Login Section:** Login Online Banking button, links for BHI Online, FIG Online, New York, Israel, Register to Israel Online, and Security and Privacy.
- News Section:**
  - Bank Hapoalim Announces Second Quarter 2016:** Net Profit totaled NIS 1,117 million, Return on Equity of 13.9%, Cash Dividend Payout of NIS 223 million.
  - Bank Hapoalim Named The Banker Magazine's Bank of the Year in Israel for 2015:** Bank Hapoalim has been chosen as Bank of the Year in Israel for 2015, by the prestigious banking magazine The Banker, a publication of the Financial Times Group. The award was announced at a ceremony held by The Banker in London.
- Market Indices:**

Indices	Value	Change
Dow	18419.3	0.10%
Nasdaq	5227.21	0.27%
SP500	2170.86	0.00%
Nikkei	16925.7	-0.01%
Tel Aviv 100	1267.03	-0.35%
FTSE	6804.28	0.86%
Dax	10554.9	0.20%
Prime Rate		1.6%

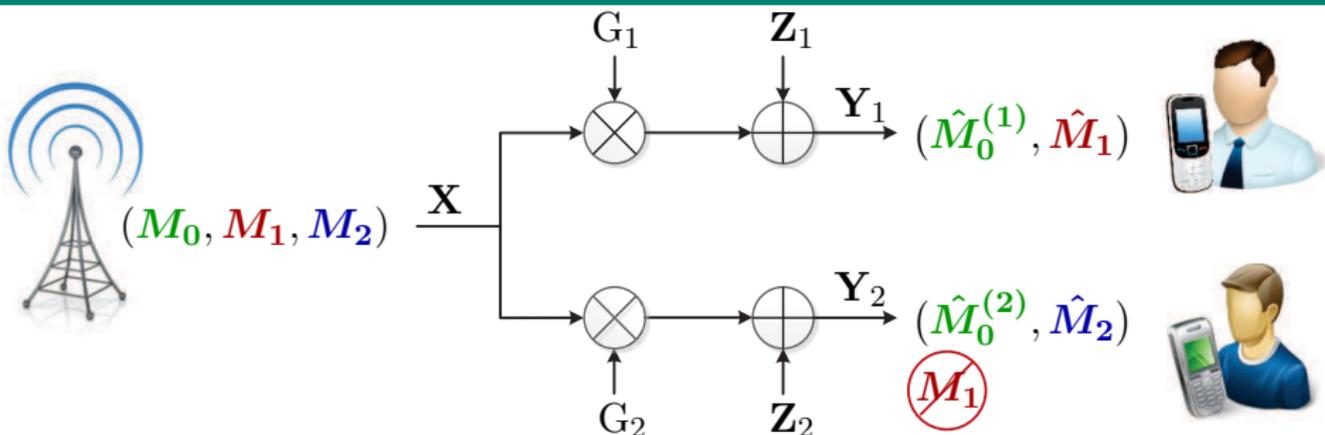
\* Quotes delayed by at least 15 minutes  
Currency Exchange Rates ▶
- Investor Relations:** BHI Bank Hapoalim B.M. logo and an "Investor Relations" button.
- Confidential Section:** A list of links: Corporate Banking, Financial Institutions Group (FIG), Investor Relations, Sustainability and Social Responsibility, Reports and Forecasts, Awards and Recognition.
- Private Section:** A large "Private" text overlay.
- Common Section:** A large "Common" text overlay.

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

# MIMO Gaussian BC - Problem Setup

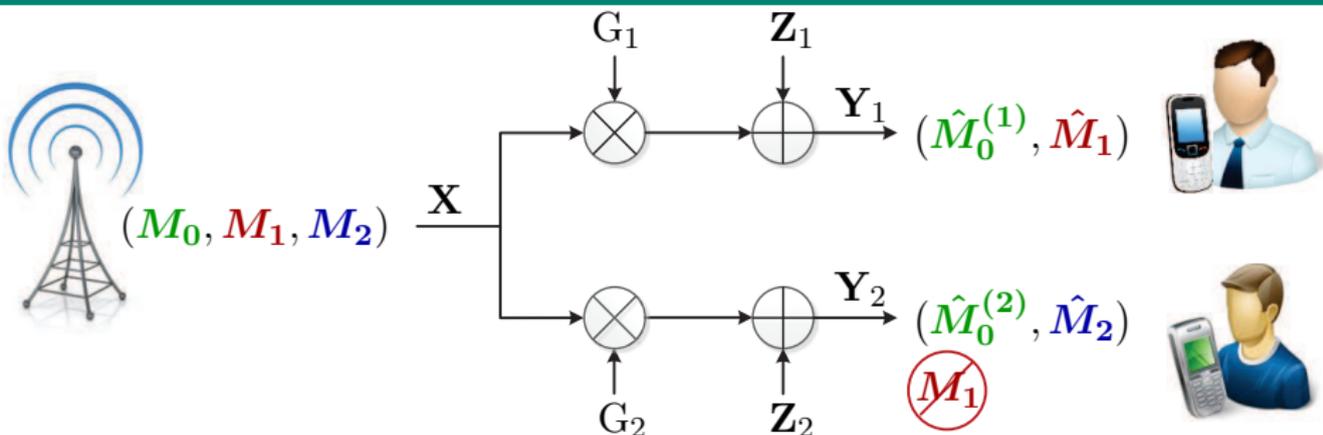


# MIMO Gaussian BC - Problem Setup



User  $j = 1, 2$  Observes:  $Y_j = G_j \mathbf{X} + Z_j.$

# MIMO Gaussian BC - Problem Setup



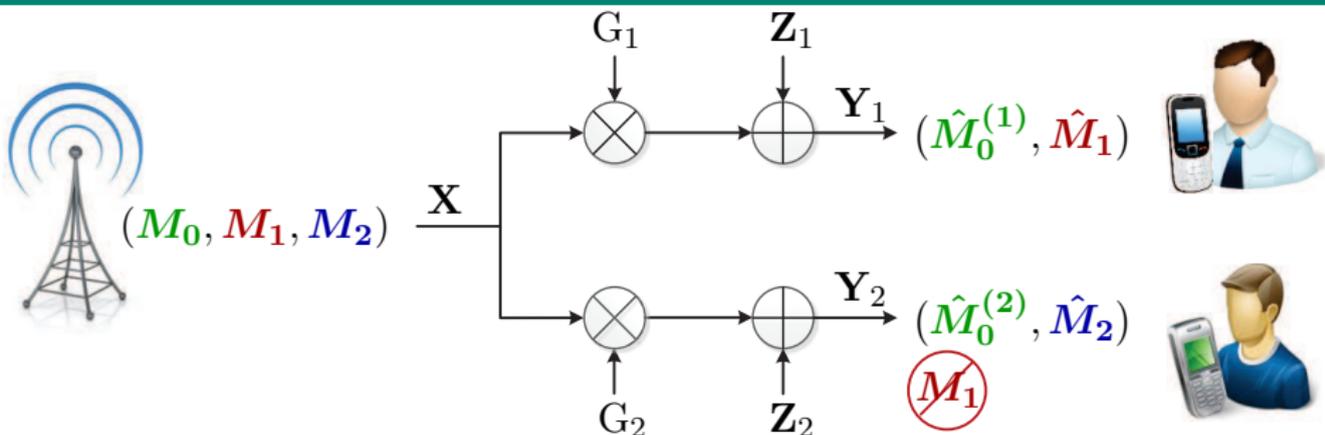
User  $j = 1, 2$  Observes:

$$\mathbf{Y}_j = G_j \mathbf{X} + \mathbf{Z}_j.$$

• Dimensions:

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

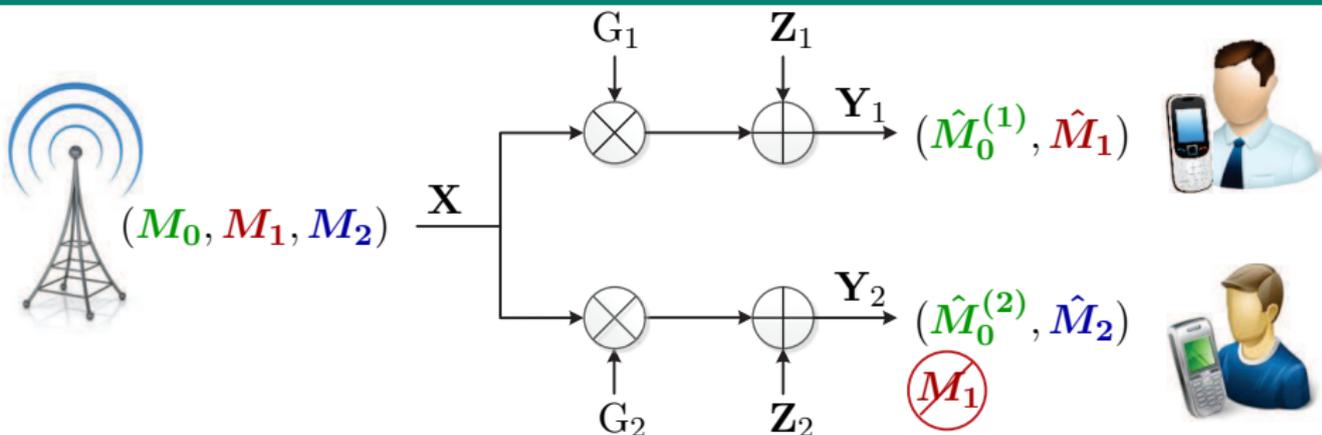
# MIMO Gaussian BC - Problem Setup



User  $j = 1, 2$  Observes:  $Y_j = G_j \mathbf{X} + Z_j$ .

- **Dimensions:**  $\mathbf{X}, Y_1, Y_2, Z_1, Z_2 \in \mathbb{R}^t$  ;  $G_1, G_2 \in \mathbb{R}^{t \times t}$ .
- **Noise Processes:** i.i.d. samples of  $Z_j \sim \mathcal{N}(\mathbf{0}, I_t)$ ,  $j = 1, 2$ .

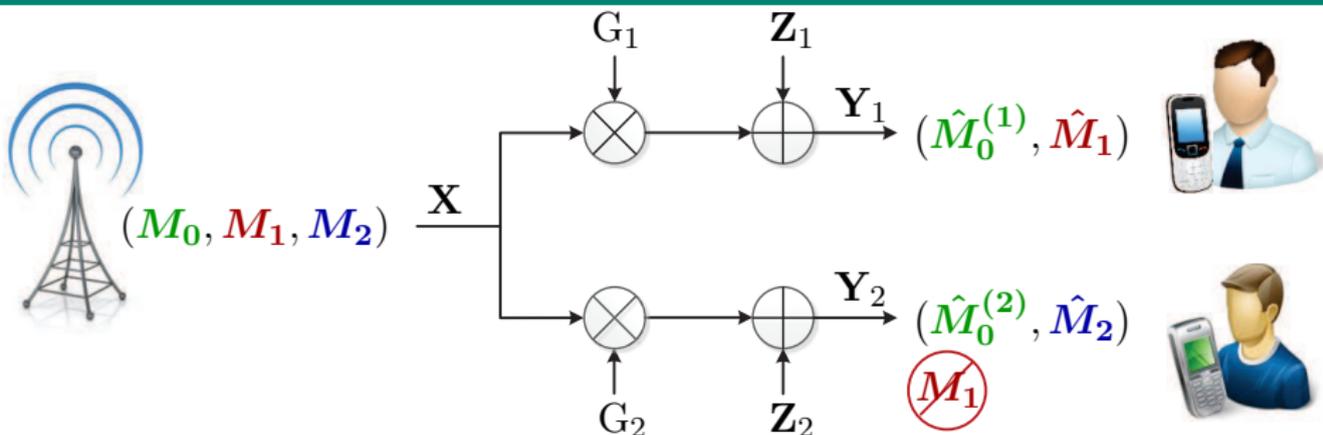
# MIMO Gaussian BC - Problem Setup



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

- **Dimensions:**  $\mathbf{X}, \mathbf{Y}_1, \mathbf{Y}_2, \mathbf{Z}_1, \mathbf{Z}_2 \in \mathbb{R}^t$  ;  $G_1, G_2 \in \mathbb{R}^{t \times t}$ .
- **Noise Processes:** i.i.d. samples of  $\mathbf{Z}_j \sim \mathcal{N}(\mathbf{0}, \mathbf{I}_t)$ ,  $j = 1, 2$ .
- **Input Covariance Constraint:**  $\frac{1}{n} \sum_{i=1}^n \mathbb{E} [\mathbf{X}(i) \mathbf{X}^\top(i)] \preceq \mathbf{K}$ .

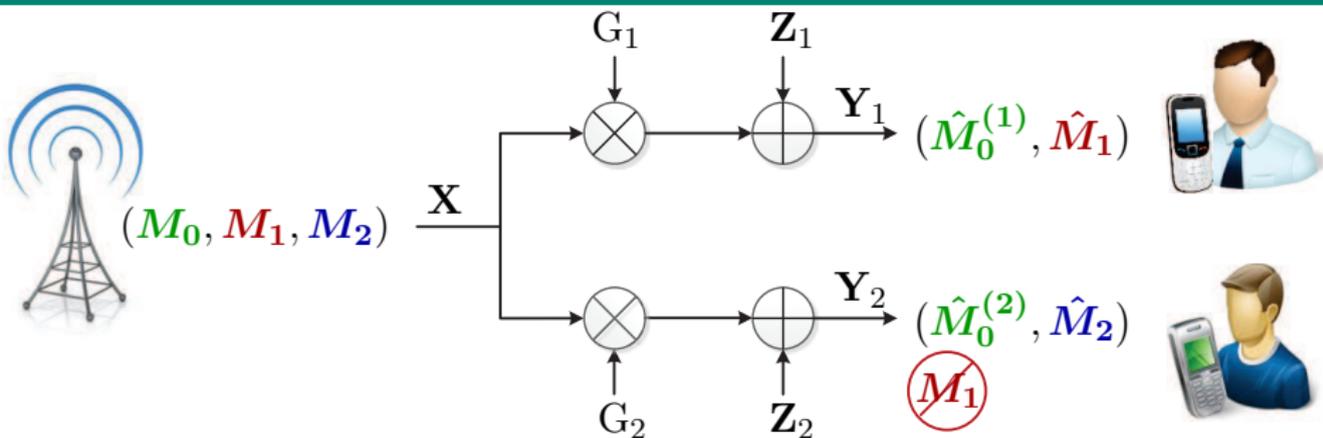
# MIMO Gaussian BC - Problem Setup



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

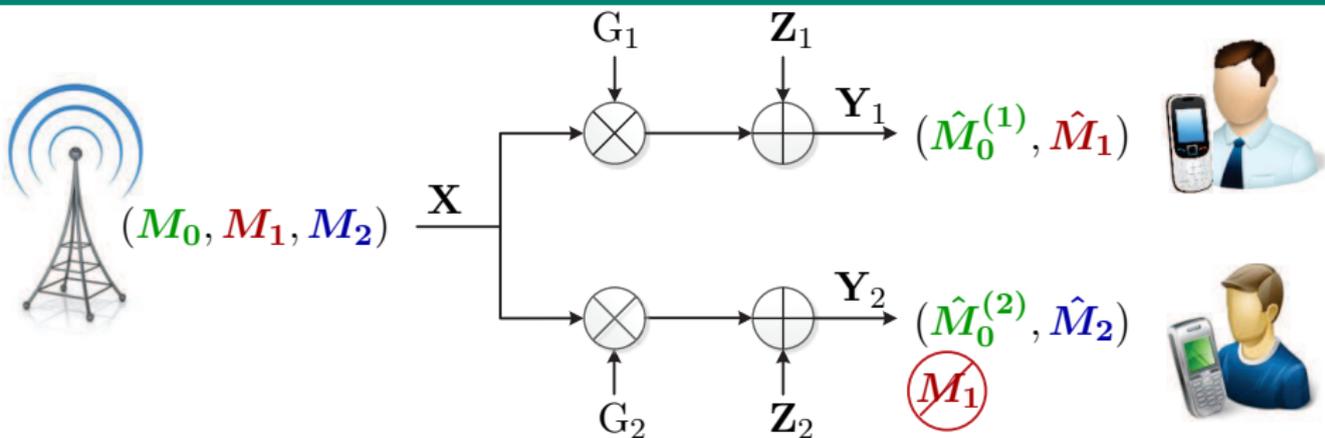
- **Dimensions:**  $\mathbf{X}, \mathbf{Y}_1, \mathbf{Y}_2, \mathbf{Z}_1, \mathbf{Z}_2 \in \mathbb{R}^t$  ;  $G_1, G_2 \in \mathbb{R}^{t \times t}$ .
- **Noise Processes:** i.i.d. samples of  $\mathbf{Z}_j \sim \mathcal{N}(\mathbf{0}, \mathbf{I}_t)$ ,  $j = 1, 2$ .
- **Input Covariance Constraint:**  $\frac{1}{n} \sum_{i=1}^n \mathbb{E} [\mathbf{X}(i) \mathbf{X}^\top(i)] \preceq \mathbf{K}$ .
- **Security Criterion:**  $\frac{1}{n} I(M_1; \mathbf{Y}_2^n) \xrightarrow{n \rightarrow \infty} 0$ .

# MIMO Gaussian BC - Goals



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

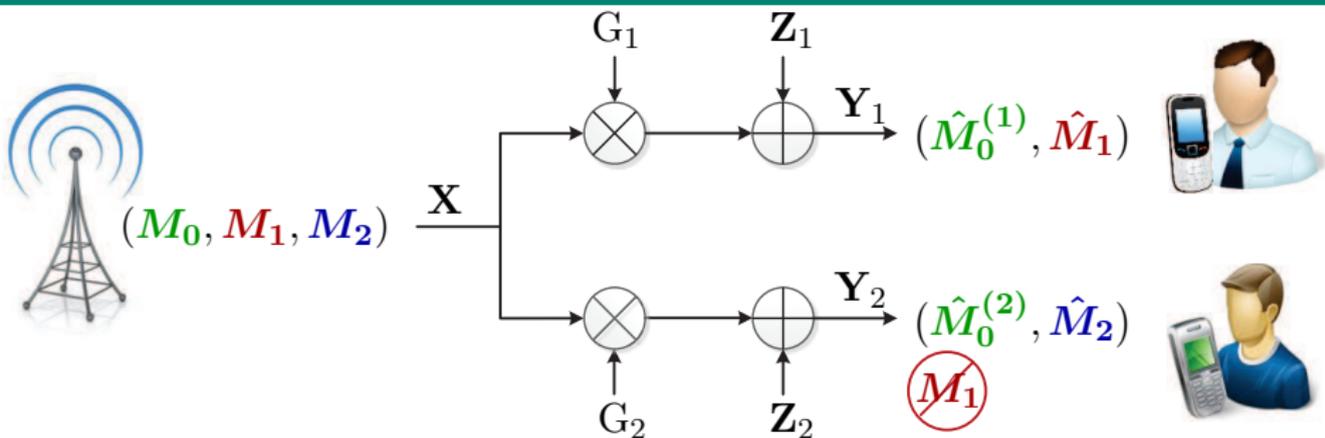
# MIMO Gaussian BC - Goals



- 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 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	<b>This work</b>
Public	Secret	Private	<b>This work</b>

# 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	<b>Geng-Nair 2014</b>
Public	Secret	—	Ly-Liu-Liang 2010
—	Secret	Secret	Liu-Liu-Poor-Shamai 2010
Public	Secret	Secret	Ekrem-Ulukus 2012
—	Secret	Private	<b>This work</b>
Public	Secret	Private	<b>This work</b>

★ 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  $K \succeq 0$  is

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

# 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  $K \succeq 0$  is

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

- **$R_1$  Bound - MIMO Gaussian WTC Secrecy-capacity:**  
User 1 - Legitimate with input covariance  $K^*$  ; 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  $K \succeq 0$  is

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

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

# 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  $\mathbf{K} \succeq 0$  is

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

# 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  $\mathbf{K} \succeq 0$  is

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

- **$R_1$  Bound:** MIMO Gaussian WTC with input  $\mathbf{K}_1$

# 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  $\mathbf{K} \succeq 0$  is

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

- $R_1$  Bound: MIMO Gaussian WTC with input  $\mathbf{K}_1$
- $R_2$  Bound: MIMO Gaussian PTP with input  $\mathbf{K}_2$  ( $\mathbf{K}_1$  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  $\mathbf{K} \succeq 0$  is

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

- $R_1$  Bound: MIMO Gaussian WTC with input  $\mathbf{K}_1$
- $R_2$  Bound: MIMO Gaussian PTP with input  $\mathbf{K}_2$  ( $\mathbf{K}_1$  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  $K \succeq 0$ .

$$\textcircled{1} \text{ [ZG-Kramer-Permuter 2016]} \implies \mathcal{I}_K \subseteq \hat{\mathcal{C}}_K \subseteq \mathcal{O}_K$$

# Secrecy-Capacity without $M_0$ - Proof Outline

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

- 1 [ZG-Kramer-Permuter 2016]  $\implies \mathcal{I}_K \subseteq \hat{\mathcal{C}}_K \subseteq \mathcal{O}_K$
- 2  $\mathcal{O}_K$  bounded & convex

# Secrecy-Capacity without $M_0$ - Proof Outline

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

① [ZG-Kramer-Permuter 2016]  $\implies \mathcal{I}_K \subseteq \hat{\mathcal{C}}_K \subseteq \mathcal{O}_K$

②  $\mathcal{O}_K$  bounded & convex  $\implies$  Supporting hyperplanes  
$$\max_{(R_1, R_2) \in \mathcal{O}_K} \lambda_1 R_1 + \lambda_2 R_2$$

# Secrecy-Capacity without $M_0$ - Proof Outline

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

1 [ZG-Kramer-Permuter 2016]  $\implies \mathcal{I}_K \subseteq \hat{\mathcal{C}}_K \subseteq \mathcal{O}_K$

2  $\mathcal{O}_K$  bounded & convex  $\implies$  Supporting hyperplanes  
$$\max_{(R_1, R_2) \in \mathcal{O}_K} \lambda_1 R_1 + \lambda_2 R_2$$

3 
$$\max_{(R_1, R_2) \in \mathcal{O}_K} \lambda_1 R_1 + \lambda_2 R_2$$

# Secrecy-Capacity without $M_0$ - Proof Outline

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

1 [ZG-Kramer-Permuter 2016]  $\implies \mathcal{I}_K \subseteq \hat{\mathcal{C}}_K \subseteq \mathcal{O}_K$

2  $\mathcal{O}_K$  bounded & convex  $\implies$  Supporting hyperplanes  
$$\max_{(R_1, R_2) \in \mathcal{O}_K} \lambda_1 R_1 + \lambda_2 R_2$$

3 
$$\max_{(R_1, R_2) \in \mathcal{O}_K} \lambda_1 R_1 + \lambda_2 R_2 \leq \text{Upper Concave Envelope}$$

# Secrecy-Capacity without $M_0$ - Proof Outline

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

① [ZG-Kramer-Permuter 2016]  $\implies \mathcal{I}_K \subseteq \hat{\mathcal{C}}_K \subseteq \mathcal{O}_K$

②  $\mathcal{O}_K$  bounded & convex  $\implies$  Supporting hyperplanes  
$$\max_{(R_1, R_2) \in \mathcal{O}_K} \lambda_1 R_1 + \lambda_2 R_2$$

③  $\max_{(R_1, R_2) \in \mathcal{O}_K} \lambda_1 R_1 + \lambda_2 R_2 \leq$  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]  $\implies \mathcal{I}_K \subseteq \hat{\mathcal{C}}_K \subseteq \mathcal{O}_K$

②  $\mathcal{O}_K$  bounded & convex  $\implies$  Supporting hyperplanes  
$$\max_{(R_1, R_2) \in \mathcal{O}_K} \lambda_1 R_1 + \lambda_2 R_2$$

③  $\max_{(R_1, R_2) \in \mathcal{O}_K} \lambda_1 R_1 + \lambda_2 R_2 \leq$  Upper Concave Envelope

④ **UCE maximized by Gaussian inputs**

$\implies \mathcal{O}_K \subseteq$  **Region from Theorem**

# Secrecy-Capacity without $M_0$ - Proof Outline

Achievability:

# Secrecy-Capacity without $M_0$ - Proof Outline

Achievability: Substituting Gaussian inputs into  $\mathcal{I}_K$ .

# Secrecy-Capacity without $M_0$ - Proof Outline

Achievability: Substituting Gaussian inputs into  $\mathcal{I}_K$ .

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

# Secrecy-Capacity without $M_0$ - Proof Outline

Achievability: Substituting Gaussian inputs into  $\mathcal{I}_K$ .

- 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  $\mathcal{I}_K$ .

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



**Region from Theorem**  $\subseteq \mathcal{I}_K$

# Secrecy-Capacity without $M_0$ - Proof Outline

Achievability: Substituting Gaussian inputs into  $\mathcal{I}_K$ .

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

↓

$$\mathcal{O}_K \subseteq \text{Region from Theorem} \subseteq \mathcal{I}_K$$

# Secrecy-Capacity without $M_0$ - Proof Outline

Achievability: Substituting Gaussian inputs into  $\mathcal{I}_K$ .

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

$$\begin{array}{c} \Downarrow \\ \mathcal{O}_K \subseteq \text{Region from Theorem} \subseteq \mathcal{I}_K \\ \Downarrow \end{array}$$

$$\mathcal{O}_K = \text{Region from Theorem} = \mathcal{I}_K$$



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

# Secrecy-Capacity without $M_0$ - Visualization

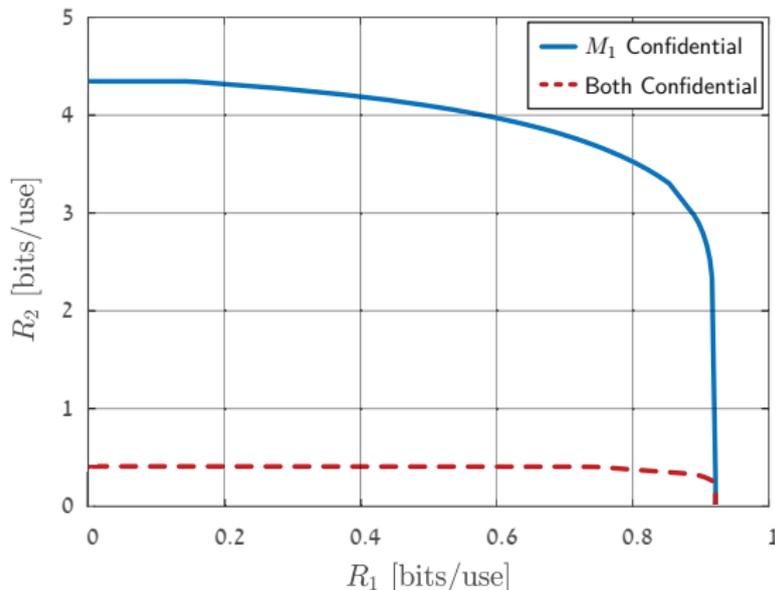
## Secrecy-Capacity Region under Average Power Constraint:

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

# Secrecy-Capacity without $M_0$ - Visualization

## Secrecy-Capacity Region under Average Power Constraint:

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



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

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

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

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

- **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.

- **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.**

- **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!**