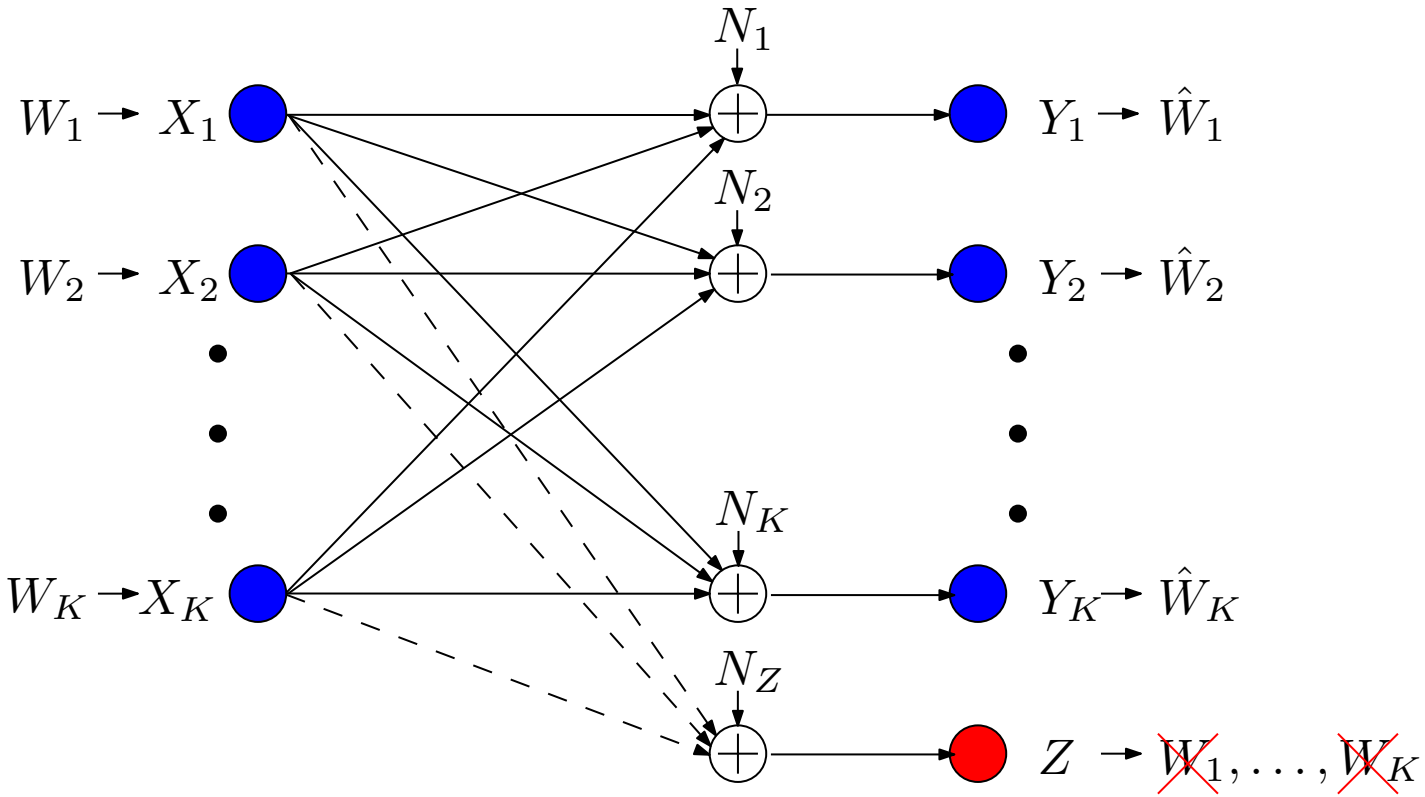
# Secure Degrees of Freedom of the Interference Channel with No Eavesdropper CSI

Pritam Mukherjee  Şennur Ulukuş

University of Maryland

# The Interference Channel with an External Eavesdropper

- $K$-user interference channel with an external eavesdropper (IC-EE).




- **Key factor:** Channel state information at the transmitters (CSIT).
- Channel gains of legitimate users are known at all the transmitters.
- In practice, channel gains of eavesdropper are not known at the transmitters.

# A Degrees of Freedom View

- Recall the capacity of a real Gaussian channel

$$Y = X + N$$

  is given by

$$C_G = \frac{1}{2}\log(1+P) \approx \frac{1}{2}\log P \quad \text{at high SNR.}$$

- *Degrees of freedom* (d.o.f.) is defined as

$$d = \lim_{P\to\infty} \frac{C}{C_G} = \lim_{P\to\infty} \frac{C}{\frac{1}{2}\log P}.$$

- Thus,

$$\text{d.o.f} = d \quad \Rightarrow \quad C = \frac{d}{2}\log P + o(\log P).$$

- With security constraints: *secure degrees of freedom* (s.d.o.f.):

$$d_s = \lim_{P\to\infty} \frac{C_s}{\frac{1}{2}\log P}.$$

# Known Results: IC-EE with Eavesdropper CSI

**Theorem (Xie, Ulukus, ISIT 2013)**

*With eavesdropper CSI, the* **exact** *sum s.d.o.f. of both the $K$-user Gaussian IC-CM and IC-EE is*

$$D_s = \frac{K(K-1)}{2K-1}$$

*with probability one.*

- The sum s.d.o.f. increases with the number of users $K$.
- The converse:
  - Gaussian version of the secrecy penalty lemma
  - Gaussian version of the role of a helper lemma
- The achievable scheme:
  - asymptotic real interference alignment

# Known Results: Converse

- Secrecy penalty lemma (Gaussian version):

$$n\sum_{i=1}^{K} R_i = \sum_{j=1}^{K} h(\tilde{\mathbf{X}}_j) - h(\mathbf{Z}) + nc$$
$$\leq \sum_{j=1, j\neq k}^{K} h(\tilde{\mathbf{X}}_j) + nc'$$

  where $\tilde{\mathbf{X}}_j = \mathbf{X}_j + \tilde{\mathbf{N}}_j$, and $\tilde{N}_j$ are zero-mean Gaussian rvs with small variance.

- Role of a helper lemma (Gaussian version):

$$nR_i \leq h(\mathbf{Y}_i) - h(\tilde{\mathbf{X}}_j) + nc'', \quad i \neq j$$

  or, equivalently,

$$h(\tilde{\mathbf{X}}_j) \leq h(\mathbf{Y}_i) - nR_i + nc'', \quad i \neq j$$

# Known Results: Converse

- Secrecy penalty lemma (Gaussian version):

$$n\sum_{i=1}^{K} R_i = \sum_{j=1}^{K} h(\tilde{\mathbf{X}}_j) - h(\mathbf{Z}) + nc$$
$$\leq \sum_{j=1, j\neq k}^{K} h(\tilde{\mathbf{X}}_j) + nc'$$

  where $\tilde{\mathbf{X}}_j = \mathbf{X}_j + \tilde{\mathbf{N}}_j$, and $\tilde{N}_j$ are zero-mean Gaussian rvs with small variance.

- Role of a helper lemma (Gaussian version):

$$nR_i \leq h(\mathbf{Y}_i) - h(\tilde{\mathbf{X}}_j) + nc'', \quad i \neq j$$

  or, equivalently,

$$h(\tilde{\mathbf{X}}_j) \leq h(\mathbf{Y}_i) - nR_i + nc'', \quad i \neq j$$

# Known Results: Converse (contd.)

- Using the role of a helper lemma in secrecy penalty lemma:

$$\begin{aligned} n\sum_{i=1}^{K} R_i \leq & h(\tilde{\mathbf{X}}_1) + h(\tilde{\mathbf{X}}_2) + \ldots + h(\tilde{\mathbf{X}}_{k-1}) + h(\tilde{\mathbf{X}}_{k+1}) + \ldots + h(\tilde{\mathbf{X}}_K) + nc' \\ \leq & [h(\mathbf{Y}_2) - nR_2] + [h(\mathbf{Y}_3) - nR_3] + \ldots + [h(\mathbf{Y}_1) - nR_1] + n\bar{c} \\ = & \sum_{i=1, i\neq\hat{k}}^{K} h(\mathbf{Y}_i) - n\sum_{i=1, i\neq\hat{k}}^{K} R_i + n\bar{c} \end{aligned}$$

  where $\hat{k} = (k+1) \bmod K$.

- Thus,

$$2n\sum_{i=1}^{K} R_i \leq \sum_{i=1, i\neq\hat{k}}^{K} h(\mathbf{Y}_i) + nR_{\hat{k}} + n\bar{c}$$

- Note $h(\mathbf{Y}_i) \leq \frac{n}{2}\log P + \hat{c}$.

# Known Results: Converse (contd.)

- Dividing by $n$,

$$2\sum_{i=1}^{K} R_i \leq (K-1)\frac{1}{2}\log P + R_{\hat{k}} + \tilde{c}, \quad \hat{k} = 1, \ldots, K$$

- Summing over all $\hat{k}$,

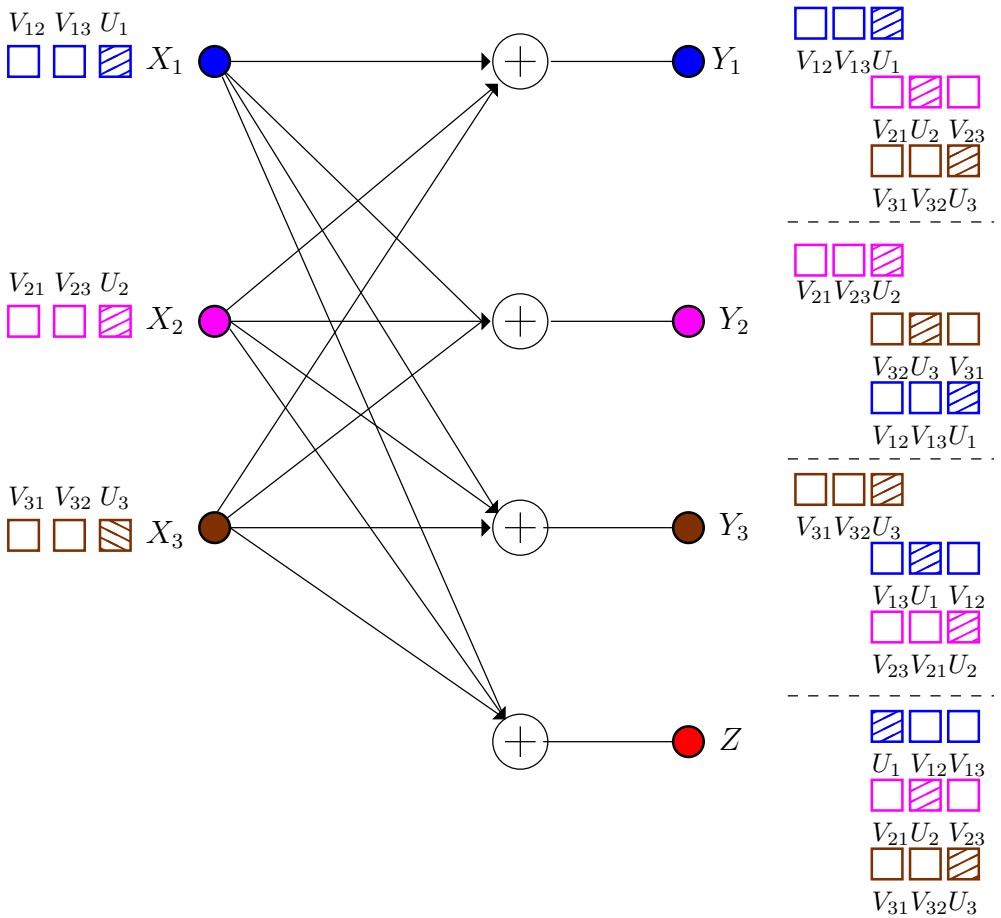
$$(2K-1)\sum_{i=1}^{K} R_i \leq K(K-1)\frac{1}{2}\log P + K\tilde{c}$$

- Diving by $\frac{1}{2}\log P$ and taking limit $P \to \infty$,

$$\sum_{i=1}^{K} d_i \leq \frac{K(K-1)}{2K-1}$$

# Known Results: Achievable Scheme

- Achievability: Asymptotic interference alignment [Motahari, *et. al.*, 2009].




- At each user: $K-1$ signal dimensions and $K$ jamming dimensions.
- Therefore, sum s.d.o.f. $= K \cdot \frac{K-1}{K-1+K} = \frac{K(K-1)}{2K-1}$.

# Known Results: Related Channel Models

**Question:** What is the **exact** sum s.d.o.f. with no eavesdropper CSI?

| | with Eve CSI | without Eve CSI | what needed? |
|---|---|---|---|
| **helper wiretap channel** | $\frac{K-1}{K}$ | $\frac{K-1}{K}$ | **achievability** [CISS, 2013] |
| **MAC wiretap channel** | $\frac{K(K-1)}{K(K-1)+1}$ | $\frac{K-1}{K}$ | **converse** [ISIT, 2015] |
| **interference channel** | $\frac{K(K-1)}{2K-1}$ | | |

# Our Results

**Question:** What is the **exact** sum s.d.o.f. with no eavesdropper CSI?

| | with Eve CSI | without Eve CSI | what needed? |
|---|---|---|---|
| **helper wiretap channel** | $\frac{K-1}{K}$ | $\frac{K-1}{K}$ | **achievability** [CISS, 2013] |
| **MAC wiretap channel** | $\frac{K(K-1)}{K(K-1)+1}$ | $\frac{K-1}{K}$ | **converse** [ISIT, 2015] |
| **interference channel** | $\frac{K(K-1)}{2K-1}$ | $\frac{K-1}{2}$ | **converse and achievability** |

# Our Results: IC-EE with **No** Eavesdropper CSI

## Theorem

*Without eavesdropper CSI, the* **exact** *sum s.d.o.f. of the K-user IC-EE is*

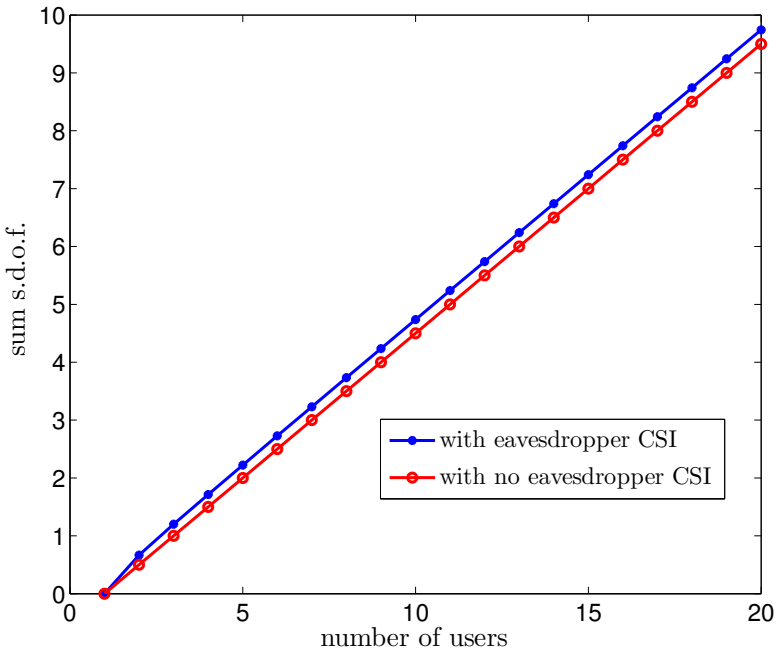
$$D_s = \frac{K-1}{2}$$

*with probability one.*

- The converse:
  - linear deterministic version of the secrecy penalty lemma
  - linear deterministic version of the role of a helper lemma
  - MISO channel with no CSI, least alignment bound [Davoodi, Jafar, 2014]
- The achievable scheme:
  - asymptotic real interference alignment [Motahari, *et. al.*, 2009].

# Our Result: Loss in S.d.o.f.

- Optimal sum s.d.o.f., $d_s$ scales with $K$ irrespective of eavesdropper CSIT.




- S.d.o.f. cost of security $= \frac{1}{2}$, irrespective of $K$, i.e., $\frac{K}{2}$ vs $\frac{K-1}{2}$.
- S.d.o.f loss due to no eavesdropper CSI is bounded by $\frac{1}{4}$, i.e., $\frac{K(K-1)}{2K-1}$ vs $\frac{K-1}{2}$.

# Converse

- **Step 1**: Consider the linear deterministic IC-EE.

$$Y_k(t) = \sum_{i=1}^{K} \lfloor h_{ik}(t) X_i(t) \rfloor$$

$$Z(t) = \sum_{i=1}^{K} \lfloor g_i(t) X_i(t) \rfloor$$

with the constraint that

$$X_i \in \left\{0, 1, \ldots, \lfloor \sqrt{P} \rfloor\right\}$$

- Any s.d.o.f. in the Gaussian channel can be achieved on this channel.
- This channel has a **larger** s.d.o.f. region.
- A converse for this channel $\Rightarrow$ A converse for the original channel.
- Consider this channel for the rest of the converse.

# Converse (Contd.)

- **Step 2**: Use the secrecy penalty and the role of a helper lemmas.
- Secrecy penalty lemma (linear deterministic version):

$$n\sum_{i=1}^{K} R_i \leq \sum_{j=1}^{K} H(\mathbf{X}_j) - H(\mathbf{Z}) + nc$$

$$\leq \sum_{j=1, j\neq k}^{K} H(\mathbf{X}_j) + nc'$$

- Role of a helper lemma (linear deterministic version):

$$nR_i \leq H(\mathbf{Y}_i) - H(\mathbf{X}_j) + nc'', \quad i \neq j$$

or, equivalently,

$$H(\mathbf{X}_j) \leq H(\mathbf{Y}_i) - nR_i + nc'', \quad i \neq j$$

# Converse (Contd.)

- **Step 2**: Use the secrecy penalty and the role of a helper lemmas.
- Secrecy penalty lemma (linear deterministic version):

$$n\sum_{i=1}^{K} R_i \leq \sum_{j=1}^{K} H(\mathbf{X}_j) - H(\mathbf{Z}) + nc$$

$$\leq \sum_{j=1, j\neq k}^{K} H(\mathbf{X}_j) + nc'$$

- Role of a helper lemma (linear deterministic version):

$$nR_i \leq H(\mathbf{Y}_i) - H(\mathbf{X}_j) + nc'', \quad i \neq j$$

or, equivalently,

$$H(\mathbf{X}_j) \leq H(\mathbf{Y}_i) - nR_i + nc'', \quad i \neq j$$

# Converse (Contd.)

- Using the role of a helper lemma in secrecy penalty lemma

$$\begin{aligned} n\sum_{i=1}^{K} R_i \leq & H(\mathbf{X}_1) + \ldots + H(\mathbf{X}_K) - H(\mathbf{Z}) + nc \\ \leq & [H(\mathbf{Y}_2) - nR_2] + \ldots + [H(\mathbf{Y}_1) - nR_1] - H(\mathbf{Z}) + n\bar{c} \\ = & \sum_{i=1}^{K} H(\mathbf{Y}_i) - n\sum_{i=1}^{K} R_i - H(\mathbf{Z}) + n\bar{c} \end{aligned}$$

- Thus, we have

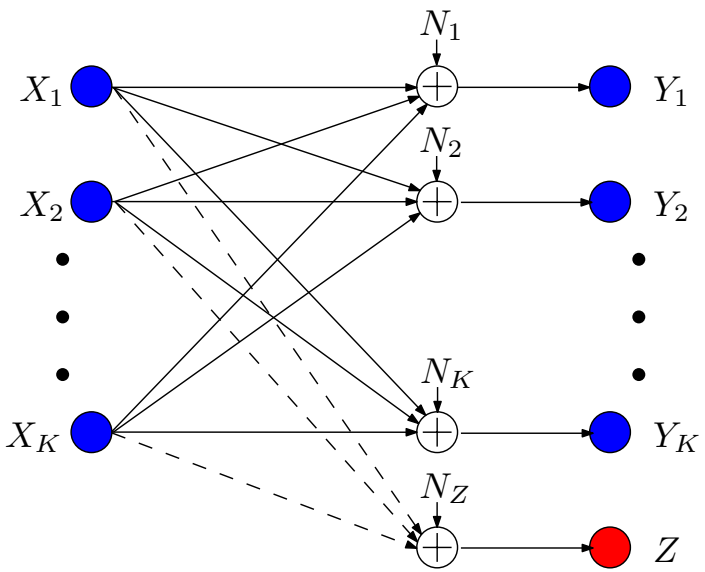
$$\begin{aligned} 2n\sum_{i=1}^{K} R_i \leq & \sum_{i=1}^{K} H(\mathbf{Y}_i) - H(\mathbf{Z}) + n\bar{c} \\ = & \sum_{i=1}^{K-1} H(\mathbf{Y}_i) + (H(\mathbf{Y}_K) - H(\mathbf{Z})) + n\bar{c} \end{aligned}$$

- Note that $H(\mathbf{Y}_i) \leq \frac{n}{2}\log P + n\hat{c}$

# Converse (Contd.)

- **Step 3**: Show that

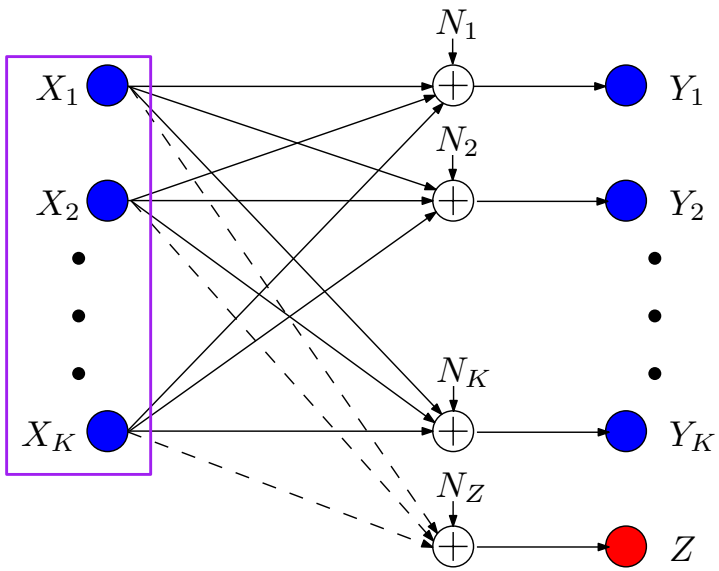
$$H(\mathbf{Y}_K) - H(\mathbf{Z}) \leq n\, o(\log P)$$



# Converse (Contd.)

- **Step 3**: Show that

$$H(\mathbf{Y}_K) - H(\mathbf{Z}) \leq n\, o(\log P)$$




- **Enhance** to MISO broadcast channel and drop security constraints.
- With no CSIT from user with output $\mathbf{Z}$, this holds [Davoodi, Jafar, 2014].

# Converse (Contd.)

- Thus we have,

$$\begin{aligned} 2n\sum_{i=1}^{K} R_i \leq & (K-1)\frac{n}{2}\log P + (H(\mathbf{Y}_K) - H(\mathbf{Z})) + n\tilde{c} \\ \leq & (K-1)\frac{n}{2}\log P + n\, o(\log P) \end{aligned}$$

- Dividing by $n$,

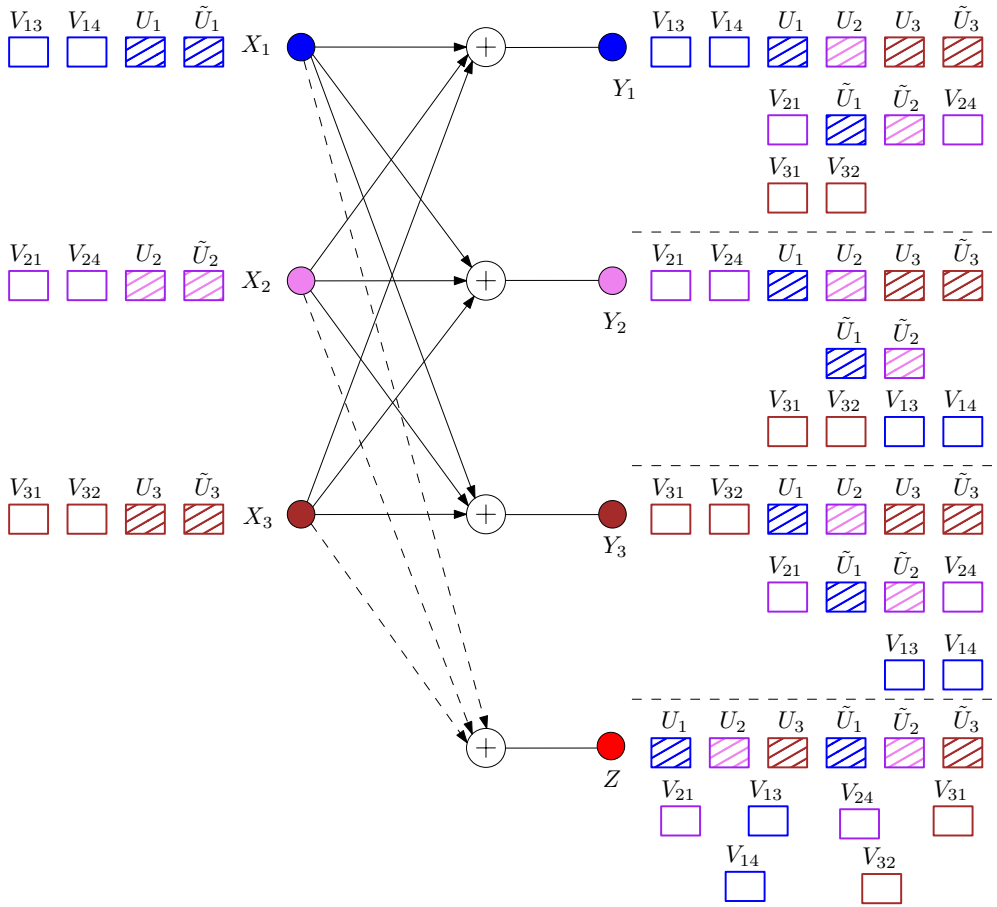
$$2\sum_{i=1}^{K} R_i \leq (K-1)\frac{1}{2}\log P + o(\log P)$$

- Dividing by $\frac{1}{2}\log P$ and taking the limit $P \to \infty$,

$$\sum_{i=1}^{K} d_i \leq \frac{K-1}{2}$$

# Achievable Scheme

- Achievability: asymptotic interference alignment [Motahari, *et. al.*, 2009].




- At each user: $K-1$ signal dimensions and $K+1$ jamming dimensions.
- Therefore, sum s.d.o.f. $= K \cdot \frac{K-1}{(K-1)+(K+1)} = K \cdot \frac{K-1}{2K} = \frac{K-1}{2}$.

# Remarks on the Achievable Scheme

- The scheme provides confidentiality from unintended receivers for free.
  - Aimed for IC-EE, got IC-CM for free.
- Each transmitter sends two cooperative jamming blocks (instead of one).
- The message symbols do not align with the cooperative jamming signals at the eavesdropper.
- However, the cooperative jamming signals exhaust the decoding ability of the eavesdropper.

# Conclusions

- Determined the optimal sum s.d.o.f. of the IC-EE without eavesdropper CSI.
- The converse:
  - linear deterministic version of the secrecy penalty lemma
  - linear deterministic version of the role of a helper lemma
  - MISO wiretap channel with no CSI, least alignment bound
- The achievable scheme:
  - asymptotic real interference alignment.