Decomposing the MIMO Wiretap Channel

Anatoly Khina, Tel Aviv University

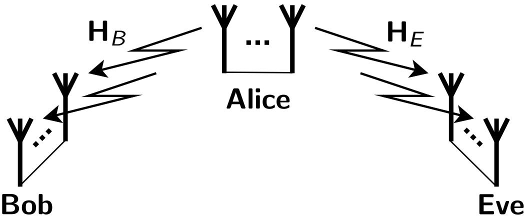
Joint work with:
Yuval Kochman, Hebrew University
Ashish Khisti, University of Toronto

ISIT 2014
Honolulu, Hawai'i, USA
June 30, 2014

Part I

Problem Setting

Channel Model: Gaussian MIMO Wiretap Channel



$$\mathbf{y}_B = \mathbf{H}_B \mathbf{x} + \mathbf{z}_B \qquad \mathbf{y}_E = \mathbf{H}_E \mathbf{x} + \mathbf{z}_E$$

- $\mathbf{x}$ – $N_A \times 1$ input vector of power P
- $\mathbf{y}_B$, $\mathbf{y}_E$ – $N_B \times 1$, $N_E \times 1$ received vectors
- $\mathbf{H}_B$, $\mathbf{H}_E$ – $N_B \times N_A$, $N_E \times N_A$ channel matrices
- $\mathbf{z}_B \sim \mathcal{CN}(\mathbf{0}, \mathbf{I}_{N_B})$, $\mathbf{z}_E \sim \mathcal{CN}(\mathbf{0}, \mathbf{I}_{N_E})$ – noise vectors
- "Closed loop" (full channel knowledge everywhere).

Capacity

Gaussian SISO channel capacity [Leung-Yan-Cheong, Hellman '78]

$$C_S\left(h_B, h_E\right) = \Big[\overbrace{\log\left(1 + |h_B|^2 P\right)}^{I(X;Y_B)} - \overbrace{\log\left(1 + |h_E|^2 P\right)}^{I(X;Y_E)} \Big]_+$$

Gaussian MIMO channel capacity [Khisti,Wornell '10][Oggier,Hassibi '11]

$$C_S\left(\mathbf{H}_B, \mathbf{H}_E\right) = \max_{\mathbf{K}:\,\mathrm{trace}\{\mathbf{K}\}\le P} \Big[\overbrace{\log\left|\mathbf{I} + \mathbf{H}_B\mathbf{K}\mathbf{H}_B^\dagger\right|}^{I(\mathbf{X};\mathbf{Y}_B)} - \overbrace{\log\left|\mathbf{I} + \mathbf{H}_E\mathbf{K}\mathbf{H}_E^\dagger\right|}^{I(\mathbf{X};\mathbf{Y}_E)} \Big]$$

- Maximization over all admissible covariance matrices $\mathbf{K}$
- Power constraint can be replaced with covariance constraint [Liu, Shamai '09]

Capacity-achieving Codes for Gaussian SISO Wiretap

- Great effort in constructing practical capacity-achieving codes:
  - LDPC-based [Klinc et al. '11][Andresson, PhD '11]
  - Lattice-based [Oggier et al., submitted '13]
  - Polar-based [Mahdavifar, Vardy '11]
  - "Black-box approach" [Tyagi, Vardy, ISIT'14]
  - More...

What to do for MIMO?

Goal: Practical MIMO Scheme

Black box approach

- Signal processing
  (SVD-based scheme [Telatar '99], V-BLAST [Foschini '96], ...)
- Any good SISO wiretap codes
- Achieves capacity
- Gap-to-capacity dictated by gap-to-capacity of the SISO codes

Goal: Practical MIMO Scheme

Black box approach

- Signal processing
  (SVD-based scheme [Telatar '99], V-BLAST [Foschini '96], ...)
- Any good SISO wiretap codes
- Achieves capacity
- Gap-to-capacity dictated by gap-to-capacity of the SISO codes

High SNR [Khisti, Wornell '10]

- Generalized SVD (GSVD) + linear zero-forcing
- Any good SISO wiretap codes
- Optimal at $\mathrm{SNR}^B, \mathrm{SNR}^E \to \infty$
- Suboptimal at $\mathrm{SNR}^B, \mathrm{SNR}^E < \infty$ ☹

Part II

Background: MIMO Without Secrecy

Practical Schemes for MIMO Without Secrecy (No Eve)

Singular-Value Decomposition (SVD) Scheme [Telatar '99]

- $\mathbf{H}_B = \mathbf{Q}_B \mathbf{D}_B \mathbf{V}_A^\dagger$
- $\mathbf{Q}_B$ and $\mathbf{V}_A$ — unitary
- Alice applies $\mathbf{V}_A$ and Bob applies $\mathbf{Q}_B$
- $\mathbf{D}_B = \begin{pmatrix} d_1 & 0 & 0 & \cdots & 0 \\ 0 & d_2 & 0 & \cdots & 0 \\ \vdots & \vdots & \ddots & \ddots & \vdots \\ 0 & \cdots & 0 & d_{N-1} & 0 \\ 0 & \cdots & 0 & 0 & d_N \end{pmatrix} \Rightarrow \begin{array}{c} y_1 = d_1 x_1 + z_1 \\ y_2 = d_2 x_2 + z_2 \\ \vdots \\ y_N = d_N x_N + z_N \end{array}$
- Results in parallel scalar sub-channels (each sub-channel has a different SNR)
- Apply water-filling on $\{x_1, \ldots, x_N\}$: $\mathbf{x} = \mathbf{V}_A \mathbf{W} \mathbf{c}$

Practical Schemes for MIMO Without Secrecy (No Eve)

SVD-based scheme for a given input covariance $\mathbf{K}$

- $\mathbf{H}_B\mathbf{K}^{1/2} = \mathbf{Q}_B\mathbf{D}_B\mathbf{V}_A^\dagger$
- $\mathbf{Q}_B$ and $\mathbf{V}_A$ — unitary
- Alice applies $\mathbf{K}^{1/2}\mathbf{V}_A$ and Bob applies $\mathbf{Q}_B$
- $$\mathbf{D}_B = \begin{pmatrix} d_1 & 0 & 0 & \cdots & 0 \\ 0 & d_2 & 0 & \cdots & 0 \\ \vdots & \vdots & \ddots & \ddots & \vdots \\ 0 & \cdots & 0 & d_{N-1} & 0 \\ 0 & \cdots & 0 & 0 & d_N \end{pmatrix} \Rightarrow \begin{aligned} y_1 &= d_1 x_1 + z_1 \\ y_2 &= d_2 x_2 + z_2 \\ &\vdots \\ y_N &= d_N x_N + z_N \end{aligned}$$
- Results in parallel scalar sub-channels (each sub-channel has a different SNR)
- ~~Apply water-filling on~~ $\cancel{\{x_1, \ldots, x_n\}\colon \mathbf{x} = \mathbf{V}_A\mathbf{W}\mathbf{c}}$ $\mathbf{x} = \mathbf{K}^{1/2}\mathbf{V}_A\mathbf{c}$

Practical Schemes for MIMO Without Secrecy (No Eve)

- SVD scheme with given $\mathbf{K}$ achieves : $R = \log \left| \mathbf{I}_{N_A} + \mathbf{H}_B \mathbf{K} \mathbf{H}_B^\dagger \right|$
- For optimal choice of $\mathbf{K}$ attains capacity
- Can be used to attain capacity for other covariance constraint scenarios (e.g., individual power constraints)

Practical Schemes for MIMO Without Secrecy (No Eve)

QR decomp. [Foschini'96][Wolniansky et al.'98] – zero-forcing VBLAST

- $\mathbf{H}_B = \mathbf{Q}_B \mathbf{T}_B$
- $\mathbf{Q}_B$ – unitary; $\mathbf{T}_B$ – triangular
- Bob applies $\mathbf{Q}_B^\dagger$ (no SP is required by Alice)
- $$\mathbf{T}_B = \begin{pmatrix} t_1 & * & * & \cdots & * \\ 0 & t_2 & * & \cdots & * \\ \vdots & \vdots & \ddots & \ddots & \vdots \\ 0 & 0 & \cdots & t_{N-1} & * \\ 0 & 0 & \cdots & 0 & t_N \end{pmatrix} \Rightarrow \begin{aligned} y_1^{\text{eff}} &= t_1 x_1 + z_1 \\ y_2^{\text{eff}} &= t_2 x_2 + z_2 \\ &\vdots \\ y_N^{\text{eff}} &= t_N x_N + z_N \end{aligned}$$
- Off-diagonal elements are canceled via successive interference cancellation (SIC)

Practical Schemes for MIMO Without Secrecy (No Eve)

QRD – MMSE-VBLAST for a given covariance $\mathbf{K}$ [Hassibi '00]

- $\begin{bmatrix} \mathbf{H}_B \mathbf{K}^{1/2} \\ \mathbf{I}_{N_A} \end{bmatrix} = \mathbf{Q}_B \mathbf{T}_B$
- $\mathbf{Q}_B$ – unitary; $\tilde{\mathbf{Q}}_B$ – $N_B \times N_A$ submatrix of $\mathbf{Q}_B$
- Bob applies $\tilde{\mathbf{Q}}_B^\dagger$ (no SP is required by Alice)
- $\tilde{\mathbf{Q}}_B^\dagger$ contains Wiener-filtering ("FFE")
- Effective noise has channel noise and "ISI" components
- Effective SNRs satisfy: $t_i^2 = 1 + \mathrm{SNR}_i$

$$\log(t_i^2) = \log(1 + \mathrm{SNR}_i) = I(c_i; \mathbf{y}_B | c_{i+1}^{N_A})$$

- Off-diagonal elements above diagonal canceled via SIC

Practical Schemes for MIMO Without Secrecy (No Eve)

- For square invertible **H**, ZF-VBLAST achieves: $R = \left|\mathbf{H}_B\mathbf{H}_B^\dagger\right|$

  $\left(\text{Using } \mathbf{K} \text{ at the transmitter achieves: } R = \left|\mathbf{H}_B\mathbf{K}\mathbf{H}_B^\dagger\right| \right)$

- MMSE-VBLAST achieves: $R = \left|\mathbf{I}_{N_B} + \mathbf{H}_B\mathbf{K}\mathbf{H}_B^\dagger\right|$

Practical Schemes for MIMO Without Secrecy (No Eve)

MMSE-VBLAST with precoding for a given covariance $\mathbf{K}$

- $\begin{bmatrix} \mathbf{H}_B \mathbf{K}^{1/2} \mathbf{V}_A \\ \mathbf{I}_{N_A} \end{bmatrix} = \mathbf{Q}_B \mathbf{T}_B$
- $\mathbf{V}_A$ can be used to design diagonal values $\Leftrightarrow$ design SNRs

Practical Schemes for MIMO Without Secrecy (No Eve)

MMSE-VBLAST with precoding for a given covariance $\mathbf{K}$

- $\begin{bmatrix} \mathbf{H}_B \mathbf{K}^{1/2} \mathbf{V}_A \\ \mathbf{I}_{N_A} \end{bmatrix} = \mathbf{Q}_B \mathbf{T}_B$
- $\mathbf{V}_A$ can be used to design diagonal values $\Leftrightarrow$ design SNRs

SVD-scheme as MMSE-VBLAST (QR)

Choosing $\mathbf{V}_A$ of the SVD of $\mathbf{H}_B \mathbf{K}^{1/2}$ $\Rightarrow$ SVD scheme (no SIC needed)

Practical Schemes for MIMO Without Secrecy (No Eve)

MMSE-VBLAST with precoding for a given covariance $\mathbf{K}$

- $\begin{bmatrix} \mathbf{H}_B \mathbf{K}^{1/2} \mathbf{V}_A \\ \mathbf{I}_{N_A} \end{bmatrix} = \mathbf{Q}_B \mathbf{T}_B$
- $\mathbf{V}_A$ can be used to design diagonal values $\Leftrightarrow$ design SNRs

SVD-scheme as MMSE-VBLAST (QR)

Choosing $\mathbf{V}_A$ of the SVD of $\mathbf{H}_B \mathbf{K}^{1/2}$ $\Rightarrow$ SVD scheme (no SIC needed)

Geometric-mean decomposition [Jiang et al. '05]/ QRS [Zhang et al. '05]

- $\mathbf{V}_A$ is choosing s.t. all diagonal values (all SNRs) are equal
- The same codebook can be used over all subchannels
- No need for bit-loading

Part III

Back to Wiretap...

New Scheme for Finite SNR

$$\begin{bmatrix} \mathbf{H}_B \mathbf{K}^{1/2} \mathbf{V}_A \\ \mathbf{I}_{N_A} \end{bmatrix} = \mathbf{Q}_B \overbrace{\begin{pmatrix} b_1 & * & * \\ 0 & \ddots & * \\ 0 & 0 & b_N \end{pmatrix}}^{\mathbf{T}_B}, \qquad b_i^2 = 1 + \mathrm{SNR}_i^B$$

$$\begin{bmatrix} \mathbf{H}_E \mathbf{K}^{1/2} \mathbf{V}_A \\ \mathbf{I}_{N_A} \end{bmatrix} = \mathbf{Q}_E \overbrace{\begin{pmatrix} e_1 & * & * \\ 0 & \ddots & * \\ 0 & 0 & e_N \end{pmatrix}}^{\mathbf{T}_E}, \qquad e_i^2 = 1 + \mathrm{SNR}_i^E$$

- Use any good SISO wiretap codes for SNR-pairs $(b_i^2 - 1, e_i^2 - 1)$

New Scheme for Finite SNR

$$\begin{bmatrix} \mathbf{H}_B \mathbf{K}^{1/2} \mathbf{V}_A \\ \mathbf{I}_{N_A} \end{bmatrix} = \mathbf{Q}_B \overbrace{\begin{pmatrix} b_1 & * & * \\ 0 & \ddots & * \\ 0 & 0 & b_N \end{pmatrix}}^{\mathbf{T}_B}, \quad b_i^2 = 1 + \mathrm{SNR}_i^B$$

$$\begin{bmatrix} \mathbf{H}_E \mathbf{K}^{1/2} \mathbf{V}_A \\ \mathbf{I}_{N_A} \end{bmatrix} = \mathbf{Q}_E \overbrace{\begin{pmatrix} e_1 & * & * \\ 0 & \ddots & * \\ 0 & 0 & e_N \end{pmatrix}}^{\mathbf{T}_E}, \quad e_i^2 = 1 + \mathrm{SNR}_i^E$$

- Use any good SISO wiretap codes for SNR-pairs $(b_i^2 - 1, e_i^2 - 1)$
- $\mathbf{V}_A$ of Eve's SVD $\Rightarrow$ Easy secrecy analysis + strong secrecy

New Scheme for Finite SNR

$$\begin{bmatrix} \mathbf{H}_B \mathbf{K}^{1/2} \mathbf{V}_A \\ \mathbf{I}_{N_A} \end{bmatrix} = \mathbf{Q}_B \overbrace{\begin{pmatrix} b_1 & * & * \\ 0 & \ddots & * \\ 0 & 0 & b_N \end{pmatrix}}^{\mathbf{T}_B}, \qquad b_i^2 = 1 + \mathrm{SNR}_i^B$$

$$\begin{bmatrix} \mathbf{H}_E \mathbf{K}^{1/2} \mathbf{V}_A \\ \mathbf{I}_{N_A} \end{bmatrix} = \mathbf{Q}_E \overbrace{\begin{pmatrix} e_1 & * & * \\ 0 & \ddots & * \\ 0 & 0 & e_N \end{pmatrix}}^{\mathbf{T}_E}, \qquad e_i^2 = 1 + \mathrm{SNR}_i^E$$

- Use any good SISO wiretap codes for SNR-pairs $(b_i^2 - 1, e_i^2 - 1)$
- $\mathbf{V}_A$ of Eve's SVD $\Rightarrow$ Easy secrecy analysis + strong secrecy
- $\mathbf{V}_A$ of Bob's SVD $\Rightarrow$ No need for V-BLAST

New Scheme for Finite SNR

$$\begin{bmatrix} \mathbf{H}_B \mathbf{K}^{1/2} \mathbf{V}_A \\ \mathbf{I}_{N_A} \end{bmatrix} = \mathbf{Q}_B \overbrace{\begin{pmatrix} b_1 & * & * \\ 0 & \ddots & * \\ 0 & 0 & b_N \end{pmatrix}}^{\mathbf{T}_B}, \quad b_i^2 = 1 + \mathrm{SNR}_i^B$$

$$\begin{bmatrix} \mathbf{H}_E \mathbf{K}^{1/2} \mathbf{V}_A \\ \mathbf{I}_{N_A} \end{bmatrix} = \mathbf{Q}_E \overbrace{\begin{pmatrix} e_1 & * & * \\ 0 & \ddots & * \\ 0 & 0 & e_N \end{pmatrix}}^{\mathbf{T}_E}, \quad e_i^2 = 1 + \mathrm{SNR}_i^E$$

- Use any good SISO wiretap codes for SNR-pairs $(b_i^2 - 1, e_i^2 - 1)$
- $\mathbf{V}_A$ of Eve's SVD $\Rightarrow$ Easy secrecy analysis + strong secrecy
- $\mathbf{V}_A$ of Bob's SVD $\Rightarrow$ No need for V-BLAST
- $\mathrm{diag}\{T_B\}, \mathrm{diag}\{T_E\}$ are const. $\Rightarrow$ Same code over all channels

Orthogonalizing Eve's Channel

- Take optimal covariance matrix $\mathbf{K}$

Orthogonalizing Eve's Channel

- Take optimal covariance matrix $\mathbf{K}$
- Use optimal SVD-based scheme matched for $\mathbf{H}_E$ with $\mathbf{K}$:

$$\mathbf{H}_E \mathbf{K}^{1/2} = \mathbf{Q}_E \mathbf{D}_E \mathbf{V}_A^{\dagger}$$

Orthogonalizing Eve's Channel

- Take optimal covariance matrix $\mathbf{K}$
- Use optimal SVD-based scheme matched for $\mathbf{H}_E$ with $\mathbf{K}$:

$$\mathbf{H}_E \mathbf{K}^{1/2} = \mathbf{Q}_E \mathbf{D}_E \mathbf{V}_A^{\dagger}$$

- **Alice:** $\mathbf{x} = \mathbf{K}^{1/2} \mathbf{V}_A \mathbf{c}$

Orthogonalizing Eve's Channel

- Take optimal covariance matrix $\mathbf{K}$
- Use optimal SVD-based scheme matched for $\mathbf{H}_E$ with $\mathbf{K}$:
$$\mathbf{H}_E \mathbf{K}^{1/2} = \mathbf{Q}_E \mathbf{D}_E \mathbf{V}_A^\dagger$$
- **Alice:** $\mathbf{x} = \mathbf{K}^{1/2} \mathbf{V}_A \mathbf{c}$
- **Eve:** $\tilde{\mathbf{y}}_E = \mathbf{Q}_E^\dagger \mathbf{y}_E = \mathbf{Q}_E^\dagger \mathbf{H}_E \mathbf{K}^{1/2} \mathbf{V}_A \mathbf{c} \mathbf{Q}_E^\dagger + \mathbf{z}_E = \mathbf{D}_E \mathbf{c} + \tilde{\mathbf{z}}_E$

Orthogonalizing Eve's Channel

- Take optimal covariance matrix $\mathbf{K}$
- Use optimal SVD-based scheme matched for $\mathbf{H}_E$ with $\mathbf{K}$:

$$\mathbf{H}_E \mathbf{K}^{1/2} = \mathbf{Q}_E \mathbf{D}_E \mathbf{V}_A^\dagger$$

- **Alice:** $\mathbf{x} = \mathbf{K}^{1/2} \mathbf{V}_A \mathbf{c}$
- **Eve:** $\tilde{\mathbf{y}}_E = \mathbf{Q}_E^\dagger \mathbf{y}_E = \mathbf{Q}_E^\dagger \mathbf{H}_E \mathbf{K}^{1/2} \mathbf{V}_A \mathbf{c} \mathbf{Q}_E^\dagger + \mathbf{z}_E = \mathbf{D}_E \mathbf{c} + \tilde{\mathbf{z}}_E$
- Eve sees parallel subchannels $\Rightarrow$ Easy secrecy analysis

Orthogonalizing Eve's Channel

- Take optimal covariance matrix $\mathbf{K}$
- Use optimal SVD-based scheme matched for $\mathbf{H}_E$ with $\mathbf{K}$:
$$\mathbf{H}_E\mathbf{K}^{1/2} = \mathbf{Q}_E\mathbf{D}_E\mathbf{V}_A^\dagger$$
- **Alice:** $\mathbf{x} = \mathbf{K}^{1/2}\mathbf{V}_A\mathbf{c}$
- **Eve:** $\tilde{\mathbf{y}}_E = \mathbf{Q}_E^\dagger\mathbf{y}_E = \mathbf{Q}_E^\dagger\mathbf{H}_E\mathbf{K}^{1/2}\mathbf{V}_A\mathbf{c}\mathbf{Q}_E^\dagger + \mathbf{z}_E = \mathbf{D}_E\mathbf{c} + \tilde{\mathbf{z}}_E$
- Eve sees parallel subchannels $\Rightarrow$ Easy secrecy analysis
- **Bob Uses MMSE-VBLAST**: $\tilde{\mathbf{y}}_B = \tilde{\mathbf{Q}}_B\mathbf{y}_B = \tilde{\mathbf{T}}_B\mathbf{c} + \tilde{\mathbf{z}}_B$

Orthogonalizing Eve's Channel

- Take optimal covariance matrix $\mathbf{K}$
- Use optimal SVD-based scheme matched for $\mathbf{H}_E$ with $\mathbf{K}$:
$$\mathbf{H}_E\mathbf{K}^{1/2} = \mathbf{Q}_E\mathbf{D}_E\mathbf{V}_A^\dagger$$
- **Alice:** $\mathbf{x} = \mathbf{K}^{1/2}\mathbf{V}_A\mathbf{c}$
- **Eve:** $\tilde{\mathbf{y}}_E = \mathbf{Q}_E^\dagger\mathbf{y}_E = \mathbf{Q}_E^\dagger\mathbf{H}_E\mathbf{K}^{1/2}\mathbf{V}_A\mathbf{c}\mathbf{Q}_E^\dagger + \mathbf{z}_E = \mathbf{D}_E\mathbf{c} + \tilde{\mathbf{z}}_E$
- Eve sees parallel subchannels $\Rightarrow$ Easy secrecy analysis
- **Bob Uses MMSE-VBLAST**: $\tilde{\mathbf{y}}_B = \tilde{\mathbf{Q}}_B\mathbf{y}_B = \tilde{\mathbf{T}}_B\mathbf{c} + \tilde{\mathbf{z}}_B$
- Use SISO wiretap codes over parallel wiretap subchannels:
$$(\mathrm{SNR}_i^B, \mathrm{SNR}_i^E) \leftrightarrow (\tilde{t}_i^B, d_i^E)$$

Orthogonalizing Eve's Channel

- Take optimal covariance matrix $\mathbf{K}$
- Use optimal SVD-based scheme matched for $\mathbf{H}_E$ with $\mathbf{K}$:
$$\mathbf{H}_E\mathbf{K}^{1/2} = \mathbf{Q}_E\mathbf{D}_E\mathbf{V}_A^\dagger$$
- **Alice:** $\mathbf{x} = \mathbf{K}^{1/2}\mathbf{V}_A\mathbf{c}$
- **Eve:** $\tilde{\mathbf{y}}_E = \mathbf{Q}_E^\dagger\mathbf{y}_E = \mathbf{Q}_E^\dagger\mathbf{H}_E\mathbf{K}^{1/2}\mathbf{V}_A\mathbf{c}\mathbf{Q}_E^\dagger + \mathbf{z}_E = \mathbf{D}_E\mathbf{c} + \tilde{\mathbf{z}}_E$
- Eve sees parallel subchannels $\Rightarrow$ Easy secrecy analysis
- **Bob Uses MMSE-VBLAST**: $\tilde{\mathbf{y}}_B = \tilde{\mathbf{Q}}_B\mathbf{y}_B = \tilde{\mathbf{T}}_B\mathbf{c} + \tilde{\mathbf{z}}_B$
- Use SISO wiretap codes over parallel wiretap subchannels:
$$(\mathrm{SNR}_i^B, \mathrm{SNR}_i^E) \leftrightarrow (\tilde{t}_i^B, d_i^E)$$
- Achieves capacity for optimal $\mathbf{K}$:
$$R = \underbrace{\left|\mathbf{I}_{N_A} + \mathbf{H}_B\mathbf{K}\mathbf{H}_B^\dagger\right|}_{\text{MMSE-VBLAST @ Bob}} - \underbrace{\left|\mathbf{I}_{N_A} + \mathbf{H}_E\mathbf{K}\mathbf{H}_E^\dagger\right|}_{\text{SVD @ Eve}} \equiv C_S$$

Orthogonalizing Eve's Channel

- SVD of Eve's channel allows easy secrecy-constraints proof
- Strong/weak secrecy of the SISO codes

  $\Downarrow$

  Strong/weak secrecy of the MIMO scheme

Can we use SVD for Bob's channel?

Can the same SISO codebook be used over all subchannels?

Superposition Coding for the Memoryless Wiretap Channel

Theorem

- $p(y_B|x)$ and $p(y_E|x)$ – transition distributions for Bob and Eve
- $x = \varphi(c_1, \ldots, c_{N_A})$
- c_i drawn i.i.d. $p_{c_i}(\cdot)$
- Weak-secrecy rates of

$$R_i = I\left(c_i; y_B \middle| c_{i+1}^{N_A}\right) - I\left(c_i; y_E \middle| c_{i+1}^{N_A}\right), \quad i = 1, \ldots, N_A$$

are achievable

Genie-aided secrecy-proof

- Eve tries to recover sub-messages sequentially (from last to first)
- For the recovery of sub-message i all previous sub-messages ($i = i + 1, \ldots, N_A$) are revealed

General Multi-Stream Scheme for the Gaussian MIMO Wiretap

- Apply QR decompositions for both Bob and Eve:

$$\begin{bmatrix} \mathbf{H}_B \mathbf{K}^{1/2} \mathbf{V}_A \\ \mathbf{I}_{N_A} \end{bmatrix} = \mathbf{Q}_B \mathbf{T}_B \,, \qquad \begin{bmatrix} \mathbf{H}_E \mathbf{K}^{1/2} \mathbf{V}_A \\ \mathbf{I}_{N_A} \end{bmatrix} = \mathbf{Q}_E \mathbf{T}_E$$

- The resulting SNRs satisfy:

$$\log(1 + \mathrm{SNR}_{B;i}) = \log(b_i^2) = I(c_i; \mathbf{y}_B | c_{i+1}^{N_A})$$
$$\log(1 + \mathrm{SNR}_{E;i}) = \log(e_i^2) = I(c_i; \mathbf{y}_E | c_{i+1}^{N_A})$$

- Superpoisition theorem $\Rightarrow$ Capacity is achieved with SISO codebooks of SNR-pairs $(b_i^2 - 1, e_i^2 - 1)$

$\Longrightarrow$ Alice can apply any $\mathbf{V}_A$!

General Multi-Stream Scheme for the Gaussian MIMO Wiretap

SVD @ Bob

Choose $\mathbf{V}_A$ such that

$$\mathbf{H}_B \mathbf{K}^{1/2} = \mathbf{Q}_B \mathbf{D}_B \mathbf{V}_A^\dagger$$

- **Bob:** $\tilde{\mathbf{y}}_B = \mathbf{D}_B \mathbf{c} + \tilde{\mathbf{z}}_B$

Same codebook over all subchannels

- Choose $\mathbf{V}_A$ s.t. $\mathbf{T}_B$ and $\mathbf{T}_E$ have **constant diagonals**:

$$\mathrm{SNR}_1^B = \mathrm{SNR}_2^B = \cdots = \mathrm{SNR}_N^B$$
$$\mathrm{SNR}_1^E = \mathrm{SNR}_2^E = \cdots = \mathrm{SNR}_N^E$$

- Possible using a space–time structure [Khina et al. '11]

Part IV

Supplementary

MIMO Wiretap Scheme for High SNR [Khisti, Wornell '10]

- Apply Generalized SVD (GSVD) to $\mathbf{H}_B$ and $\mathbf{H}_E$:

$$\mathbf{H}_B = \mathbf{Q}_B \mathbf{D}_B \mathbf{A}$$
$$\mathbf{H}_E = \mathbf{Q}_E \mathbf{D}_E \mathbf{A}$$

MIMO Wiretap Scheme for High SNR [Khisti, Wornell '10]

- Apply Generalized SVD (GSVD) to $\mathbf{H}_B$ and $\mathbf{H}_E$:

$$\mathbf{H}_B = \mathbf{Q}_B \mathbf{D}_B \mathbf{A}$$
$$\mathbf{H}_E = \mathbf{Q}_E \mathbf{D}_E \mathbf{A}$$

- $\mathbf{A}$ – invertible matrix; $\mathbf{Q}_B$, $\mathbf{Q}_E$ – unitary

MIMO Wiretap Scheme for High SNR [Khisti, Wornell '10]

- Apply Generalized SVD (GSVD) to $\mathbf{H}_B$ and $\mathbf{H}_E$:

$$\mathbf{H}_B = \mathbf{Q}_B \mathbf{D}_B \mathbf{A}$$
$$\mathbf{H}_E = \mathbf{Q}_E \mathbf{D}_E \mathbf{A}$$

- $\mathbf{A}$ – invertible matrix; $\mathbf{Q}_B$, $\mathbf{Q}_E$ – unitary
- $\mathbf{D}_B$, $\mathbf{D}_E$ – diagonal, s.t. $\mathbf{D}_B^2 + \mathbf{D}_E^2 = \mathbf{I}$

MIMO Wiretap Scheme for High SNR [Khisti, Wornell '10]

- Apply Generalized SVD (GSVD) to $\mathbf{H}_B$ and $\mathbf{H}_E$:

$$\mathbf{H}_B = \mathbf{Q}_B \mathbf{D}_B \mathbf{A}$$
$$\mathbf{H}_E = \mathbf{Q}_E \mathbf{D}_E \mathbf{A}$$

- $\mathbf{A}$ – invertible matrix; $\mathbf{Q}_B$, $\mathbf{Q}_E$ – unitary
- $\mathbf{D}_B$, $\mathbf{D}_E$ – diagonal, s.t. $\mathbf{D}_B^2 + \mathbf{D}_E^2 = \mathbf{I}$
- Alice uses linear zero-forcing — inverts $\mathbf{A}$ @ Tx: $\mathbf{x} = \mathbf{A}^{-1}\mathbf{c}$

MIMO Wiretap Scheme for High SNR [Khisti, Wornell '10]

- Apply Generalized SVD (GSVD) to $\mathbf{H}_B$ and $\mathbf{H}_E$:

$$\mathbf{H}_B = \mathbf{Q}_B \mathbf{D}_B \mathbf{A}$$
$$\mathbf{H}_E = \mathbf{Q}_E \mathbf{D}_E \mathbf{A}$$

- $\mathbf{A}$ – invertible matrix; $\mathbf{Q}_B$, $\mathbf{Q}_E$ – unitary
- $\mathbf{D}_B$, $\mathbf{D}_E$ – diagonal, s.t. $\mathbf{D}_B^2 + \mathbf{D}_E^2 = \mathbf{I}$
- Alice uses linear zero-forcing — inverts $\mathbf{A}$ @ Tx: $\mathbf{x} = \mathbf{A}^{-1}\mathbf{c}$
- Bob and Eve apply $\mathbf{Q}_B^\dagger$ and $\mathbf{Q}_E^\dagger$

MIMO Wiretap Scheme for High SNR [Khisti, Wornell '10]

- Apply Generalized SVD (GSVD) to $\mathbf{H}_B$ and $\mathbf{H}_E$:

$$\mathbf{H}_B = \mathbf{Q}_B \mathbf{D}_B \mathbf{A}$$
$$\mathbf{H}_E = \mathbf{Q}_E \mathbf{D}_E \mathbf{A}$$

- $\mathbf{A}$ – invertible matrix; $\mathbf{Q}_B$, $\mathbf{Q}_E$ – unitary
- $\mathbf{D}_B$, $\mathbf{D}_E$ – diagonal, s.t. $\mathbf{D}_B^2 + \mathbf{D}_E^2 = \mathbf{I}$
- Alice uses linear zero-forcing — inverts $\mathbf{A}$ @ Tx: $\mathbf{x} = \mathbf{A}^{-1}\mathbf{c}$
- Bob and Eve apply $\mathbf{Q}_B^\dagger$ and $\mathbf{Q}_E^\dagger$
- Results in parallel subchannels: $\mathbf{D}_B$, $\mathbf{D}_E$

MIMO Wiretap Scheme for High SNR [Khisti, Wornell '10]

- Apply Generalized SVD (GSVD) to $\mathbf{H}_B$ and $\mathbf{H}_E$:

$$\mathbf{H}_B = \mathbf{Q}_B \mathbf{D}_B \mathbf{A}$$
$$\mathbf{H}_E = \mathbf{Q}_E \mathbf{D}_E \mathbf{A}$$

- $\mathbf{A}$ – invertible matrix; $\mathbf{Q}_B$, $\mathbf{Q}_E$ – unitary
- $\mathbf{D}_B$, $\mathbf{D}_E$ – diagonal, s.t. $\mathbf{D}_B^2 + \mathbf{D}_E^2 = \mathbf{I}$
- Alice uses linear zero-forcing — inverts $\mathbf{A}$ @ Tx: $\mathbf{x} = \mathbf{A}^{-1}\mathbf{c}$
- Bob and Eve apply $\mathbf{Q}_B^\dagger$ and $\mathbf{Q}_E^\dagger$
- Results in parallel subchannels: $\mathbf{D}_B$, $\mathbf{D}_E$
- Transmit only over subchannels with $d_{B;i} > d_{E;i}$ using good SISO wiretap codes

MIMO Wiretap Scheme for High SNR [Khisti, Wornell]

@ High-SNR ($P \to \infty$)

- Approaches capacity: $\sum_{i=1}^{N_A} \log \frac{1+Pd_{B;i}^2}{1+Pd_{E;i}^2} \approx \sum_{i=1}^{N_A} \log \frac{\cancel{P}d_{B;i}^2}{\cancel{P}d_{E;i}^2}$
- Linear zero-forcing attains capacity at high SNR
  (In contrast to communication without secrecy!)
- Strong/weak secrecy of the SISO codes

  $\Downarrow$

  Strong/weak secrecy of the MIMO scheme
- Wasteful at finite SNR! ☹