Secret-Key Generation from Channel Reciprocity: A Separation Approach

Ashish Khisti

Department of Electrical and Computer Engineering
University of Toronto

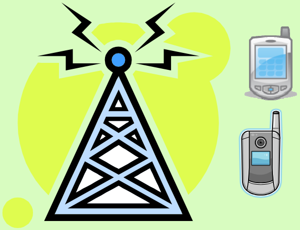
Feb 11, 2013

Security at PHY-Layer

Use PHY Resources for designing security mechanisms.

Application Layer (Semantics of Information)
Transport Layer (End to End Connectivity)
Network Layer (Routing and Path Discovery)
Data Link Layer (Error Correction Codes)
Physical Layer (Signals, RF hardware)

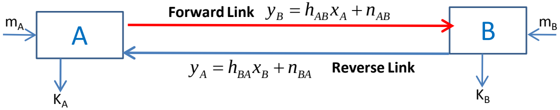
Wireless Systems

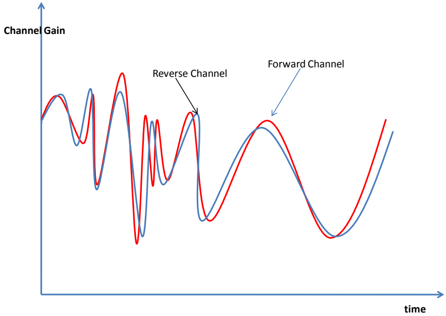


Applications:

- Secret-Key Generation
- Secure Message Transmission
- Physical Layer Authentication
- Jamming Resistance

Secret-Key Generation in Wireless Fading Channels





Fading:

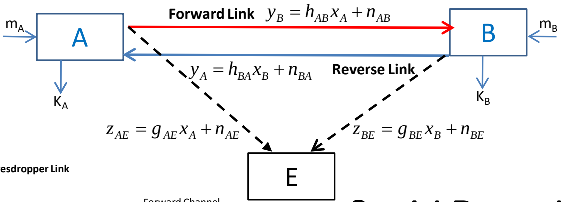
$$y_B(t) = h_{AB}(t) x_A(t) + n_B(t)$$

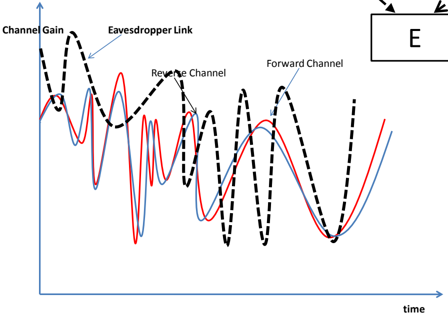
Reciprocity:

$$y_B(t) = h_{AB}(t) x_A(t) + n_B(t)$$
$$y_A(t) = h_{BA}(t) x_B(t) + n_A(t)$$

Motivation

Secret-Key Generation in Wireless Fading Channels





Spatial Decorrelation:

$$y_B(t) = h_{AB}(t) x_A(t) + n_B(t)$$
$$y_A(t) = h_{BA}(t) x_B(t) + n_A(t)$$
$$z_A(t) = g_A(t) x_A(t) + n_{AE}(t)$$
$$z_B(t) = g_B(t) x_B(t) + n_{BE}(t)$$

Secret-Key Generation - A Systems Approach

Key Generation in Wireless Systems

- UWB Systems: Wilson-Tse-Scholz ('07), M. Ko ('07), Madiseh-Neville-McGuire('12)
- Narrowband Systems: Azimi Sadjadi- Kiayias-Mercado-Yener ('07), Mathur-Trappe-Mandayam -Ye-Reznick ('10), Patware and Kasera ('07)
- OFDM reciprocity: Haile ('09), Tsouri and Wulich ('09)

Implementations

- Experimental UWB: Measurements for Key Generation Madiseh ('12)
- Software Radio Implementations: Jana et. al. ('09)
- MIMO systems: Wallace and Sharma ('10), Shimizu et al. Zeng-Wu-Mohapatra

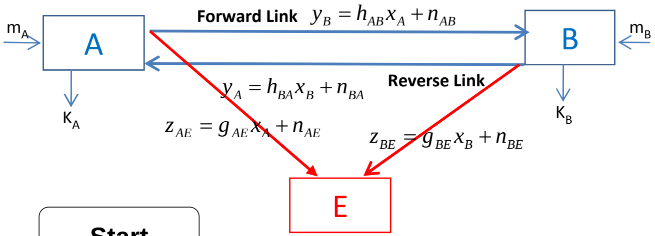
Signal Processing for Secret-Key Generation

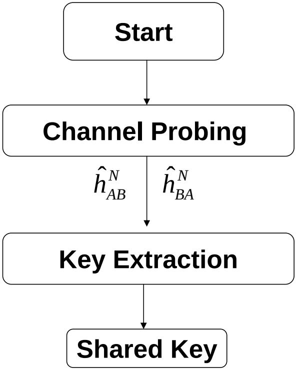
- Quantization Techniques: Ye-Reznik-Shah ('07), Hamida-Pierrot-Castelluccia ('09), Sun-Zhu-Jiang-Zhao ('11)
- Adaptive Channel Probing: Wei-Zheng-Mohapatra ('10)
- Mobility Assisted Key Generation: Gungor-Chen-Koksal ('11)

Attacks

- Active Eavesdroppers: Ebrez et. al ('11) Zafer-Agrawal-Srivatsa ('11),
- Unauthenticated Channels: Mathur et al. ('10), Xiao-Greenstein-Mandayam-Trappe ('07).

Secret-Key Generation: A Systems Approach II





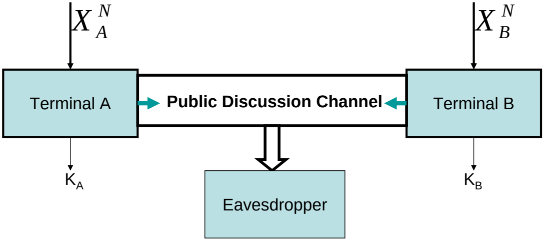
Two Phase Approach:

- **Phase I**: Channel Probing and Estimation: $(\hat{h}_{AB}^{N}, \hat{h}_{BA}^{N})$
- **Phase 2**: Source Reconciliation and Key Extraction

Secret-Key Generation: Capacity Limits

Secret-Key Generation - Source Model

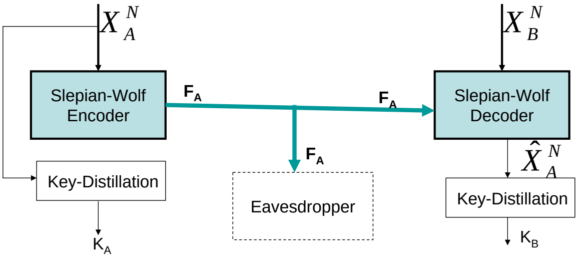
Maurer ('93), Ahlswede-Csiszar ('93)



- DMMS Model: $(x_A^N, x_B^N) \sim \prod_{i=1}^{N} p_{x_A,x_B}(x_A(i), x_B(i))$
- Interactive Public Communication: $\mathbf{F}$
- Key Generation: $k_i = \mathcal{F}_i(x_i^N, \mathbf{F})$, $i \in \{A, B\}$.
- Reliability: $\Pr(k_A \neq k_B) \leq \varepsilon_N$,
- Secrecy: $\frac{1}{N} I(k_A; \mathbf{F}) \leq \varepsilon_N$
- Secret-Key Rate: $R = \frac{1}{N} H(k_A)$

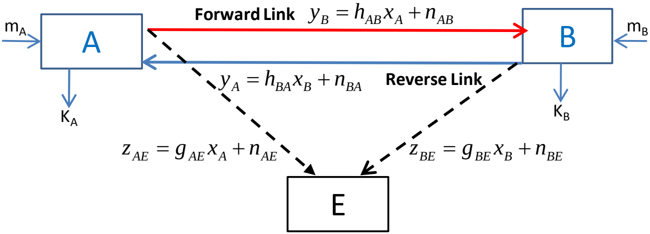
Secret-Key Generation - Source Model

Maurer ('93), Csiszar-Ahlswede ('93)



- Capacity: $C = I(x_A; x_B)$
- One-Round of Communication
- Capacity Unknown when Eavesdropper also observes a source sequence

Problem Setup

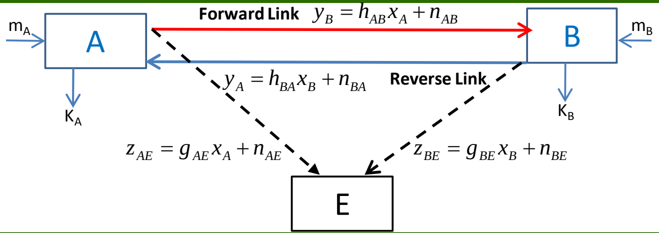


Two-Way Reciprocal Fading Channel

$$y_B(i) = h_{AB}(i)x_A(i) + n_{AB}(i), \qquad y_A(i) = h_{BA}(i)x_B(i) + n_{BA}(i)$$

$$z_A(i) = g_A(i)x_A(i) + n_{AE}(i), \qquad z_B(i) = g_B(i)x_B(i) + n_{BE}(i)$$

Problem Setup



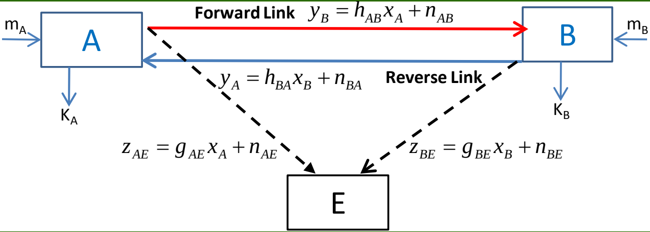
Two-Way Reciprocal Fading Channel

$$y_B(i) = h_{AB}(i)x_A(i) + n_{AB}(i), \qquad y_A(i) = h_{BA}(i)x_B(i) + n_{BA}(i)$$
$$z_A(i) = g_A(i)x_A(i) + n_{AE}(i), \qquad z_B(i) = g_B(i)x_B(i) + n_{BE}(i)$$

Channel Model Assumptions:

- Non-Coherent Model: $h_{AB}(i)$ and $h_{BA}(i)$
- Perfect Eavesdropper CSI: $g_A(i)$ & $g_B(i)$ known to Eve
- Block-Fading Channel with Coherence Period: T.
- Approximate Reciprocity: $(h_{AB}, h_{BA}) \sim p_{h_{AB},h_{BA}}(\cdot,\cdot)$
- Independence: $(g_A, g_B) \perp (h_{AB}, h_{BA})$

Problem Setup



Two-Way Reciprocal Fading Channel

$$y_B(i) = h_{AB}(i) x_A(i) + n_{AB}(i), \qquad y_A(i) = h_{BA}(i) x_B(i) + n_{BA}(i)$$

$$z_A(i) = g_A(i) x_A(i) + n_{AE}(i), \qquad z_B(i) = g_B(i) x_B(i) + n_{BE}(i)$$

Secret-Key Agreement Protocols:

- Interactive: $x_A(i) = f_A(m_A, y_A^{i-1})$, $x_B(i) = f_B(m_B, y_B^{i-1})$
- Average Power Constraints $E[|x_A|^2] \le P$, $E[|x_B|^2] \le P$.
- $k_A = \mathcal{K}_A(y_A^N, m_A)$, $k_B = \mathcal{K}_B(y_B^N, m_B)$
- Reliability and Secrecy Constraint.
- Secret-Key Capacity

Outline

- Upper Bound
- Lower Bound — With Public Discussion
- Lower Bound — No Public Discussion
- Asymptotic Regimes and Numerical Results

Secret-Key Capacity — Upper Bound

Khisti'12

Theorem

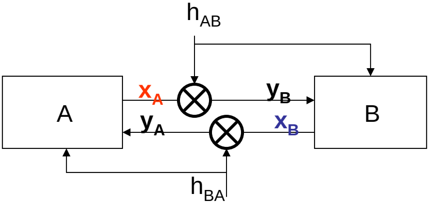
An upper bound on the secret-key capacity is $C \leq R^{+}$*:*

$$R^{+} = \frac{1}{T} I(h_{AB}; h_{BA}) + \max_{P(h_{AB}) \in \mathcal{P}} E\left[\log\left(1 + \frac{P(h_{AB})|h_{AB}|^2)}{1 + P(h_{AB})|g_A|^2}\right)\right]$$

$$+ \max_{P(h_{BA}) \in \mathcal{P}} E\left[\log\left(1 + \frac{P(h_{BA})|h_{BA}|^2}{1 + P(h_{BA})|g_B|^2)}\right)\right]$$

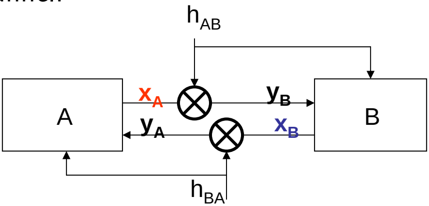
where $P(h_{AB})$ *and* $P(h_{BA})$ *are power allocation function across the fading states.*

Genie-Aided Channel:



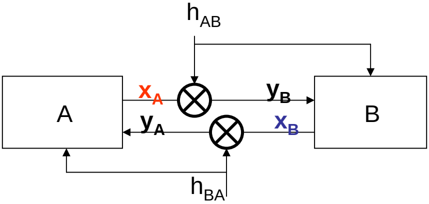
Secret-Key Capacity — Upper Bound

Genie-Aided Channel:



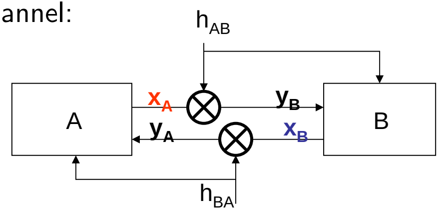
$$NTR \leq I(m_A, h_{BA}^N, y_A^{NT}; m_B, h_{AB}^N, y_B^{NT} | \mathbf{z}^{NT}, \mathbf{g}^N)$$

Genie-Aided Channel:



$$NTR \leq I(m_A, h_{BA}^N, y_A^{NT}; m_B, h_{AB}^N, y_B^{NT} | \mathbf{z}^{NT}, \mathbf{g}^N)$$
$$\leq I(x_A(NT); y_B(NT) | h_{AB}(N), z_A(NT), g_A(N))$$
$$+ I(x_B(NT); y_A(NT) | h_{BA}(N), z_B(NT), g_B(N))$$
$$+ I(m_A, h_{BA}^N, y_A^{NT-1}; m_B, h_{AB}^N, y_B^{NT-1} | \mathbf{z}^{NT-1}, \mathbf{g}^N)$$

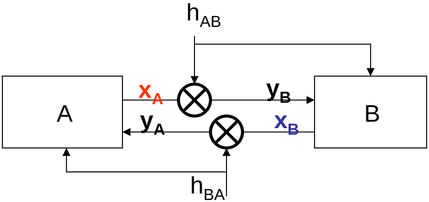
Genie-Aided Channel:



$$
\begin{aligned}
NTR &\le I(m_A, h_{BA}^N, y_A^{NT}; m_B, h_{AB}^N, y_B^{NT} | \mathbf{z}^{NT}, \mathbf{g}^N) \\
&\le \sum_{n=1}^{NT} I(x_A(n); y_B(n) | \bar{h}_{AB}(n), z_A(n), \bar{g}_A(n)) \\
&+ \sum_{n=1}^{NT} I(x_B(n); y_A(n) | \bar{h}_{BA}(n), z_B(n), \bar{g}_B(n)) \\
&+ NI(h_{AB}; h_{BA})
\end{aligned}
$$

Secret-Key Capacity — Upper Bound

Genie-Aided Channel:

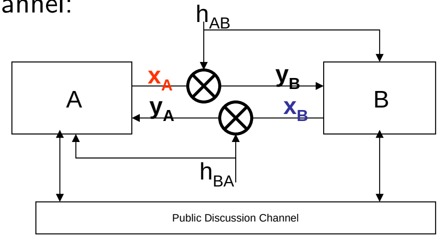


Interpretation of the Upper Bound:

- Channel Reciprocity: $\frac{1}{T}I(h_{AB};h_{BA})$
- Forward Channel: $I(y_B;x_A|h_{AB},z_A,g_A)$
- Reverse Channel: $I(y_A;x_B|h_{BA},z_B,g_B)$

Secret-Key Capacity — Upper Bound

Genie-Aided Channel:



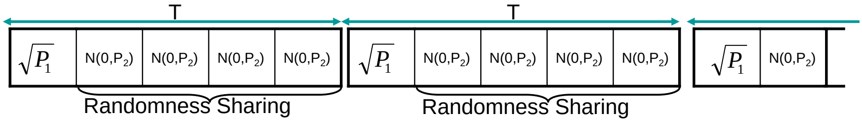
Interpretation of the Upper Bound:

- Channel Reciprocity: $\frac{1}{T} I(h_{AB}; h_{BA})$
- Forward Channel: $I(y_B; x_A | h_{AB}, z_A, g_A)$
- Reverse Channel: $I(y_A; x_B | h_{BA}, z_B, g_B)$

Upper Bound also holds if a public discussion channel is available.

Lower Bound: Separation Based Scheme

Khisti '12

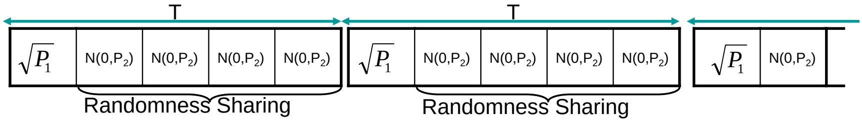


- Training: $x_A(i,1) = \sqrt{P_1}$
- Randomness Sharing: $x_A(i,t) \sim \mathcal{CN}(0, P_2)$ for $t = 2, \dots, T$
  $\mathbf{x}_A(i) = [x_A(i,2), \dots, x_A(i,T)] \in \mathbb{C}^{T-1}$.

- Training: $\hat{h}_{AB}(i)$ and $\hat{h}_{BA}(i)$
- Correlated Sources:
  Forward Channel: $\mathbf{y}_B(i) = h_{AB}(i)\mathbf{x}_A(i) + \mathbf{n}_B(i) \in \mathbb{C}^{T-1}$,
  Reverse Channel: $\mathbf{y}_A(i) = h_{BA}(i)\mathbf{x}_B(i) + \mathbf{n}_A(i) \in \mathbb{C}^{T-1}$.

Lower Bound: Separation Based Scheme

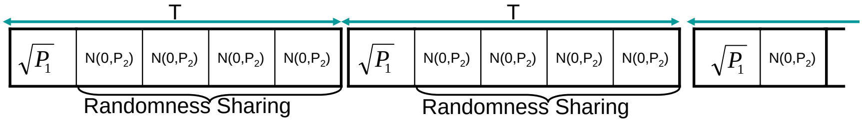
Khisti '12



	A	B	E
Channel State	$\hat{h}_{BA}^K$	$\hat{h}_{AB}^K$	(g_A^K, g_B^K)
Forward Channel	$\mathbf{x}_A^K$	$\mathbf{y}_B^K$	$\mathbf{z}_A^K$
Reverse Channel	$\mathbf{y}_A^K$	$\mathbf{x}_B^K$	$\mathbf{z}_B^K$

Lower Bound: Separation Based Scheme

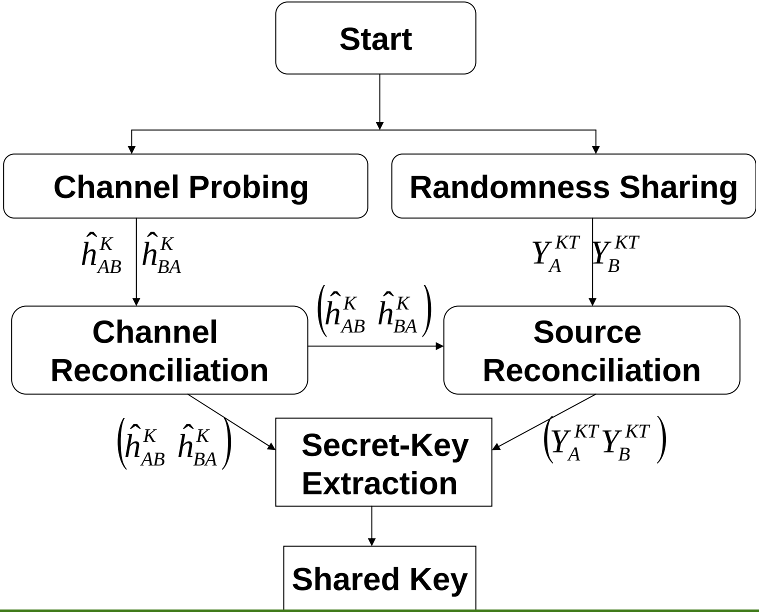
Khisti '12



	A	B	E
Channel State	$\hat{h}_{BA}^K$	$\hat{h}_{AB}^K$	(g_A^K, g_B^K)
Forward Channel	$\mathbf{x}_A^K$	$\mathbf{y}_B^K$	$\mathbf{z}_A^K$
Reverse Channel	$\mathbf{y}_A^K$	$\mathbf{x}_B^K$	$\mathbf{z}_B^K$

Generate a secret-key from these sequences.

Lower Bound — Overview



Achievable Rate with Public Discussion

Theorem (Public Discussion)

An achievable rate when a public discussion channel is available is

$$R_{\text{key}} = \left\{ \frac{1}{T} \underbrace{I(\hat{h}_{AB}; \hat{h}_{BA})}_{\text{Training}} + \frac{T-1}{T} \underbrace{\left[I(y_B; x_A, \hat{h}_{AB}) - I(y_B; z_A, g_A, h_{AB}) \right]}_{\text{Forward Channel}} + \frac{T-1}{T} \underbrace{\left[I(y_A; x_B, \hat{h}_{BA})) - I(y_A; z_B, g_B, h_{BA}) \right]}_{\text{Reverse Channel}} \right\}$$

Achievable Rate with Public Discussion

Theorem (Public Discussion)

An achievable rate when a public discussion channel is available is

$$R_{\text{key}} = \Bigg\{ \frac{1}{T} \underbrace{I(\hat{h}_{AB}; \hat{h}_{BA})}_{\text{Training}} + \frac{T-1}{T} \underbrace{\Big[I(y_B; x_A, \hat{h}_{AB}) - I(y_B; z_A, g_A, h_{AB}) \Big]}_{\text{Forward Channel}} + \frac{T-1}{T} \underbrace{\Big[I(y_A; x_B, \hat{h}_{BA})) - I(y_A; z_B, g_B, h_{BA}) \Big]}_{\text{Reverse Channel}} \Bigg\}$$

High SNR Regime

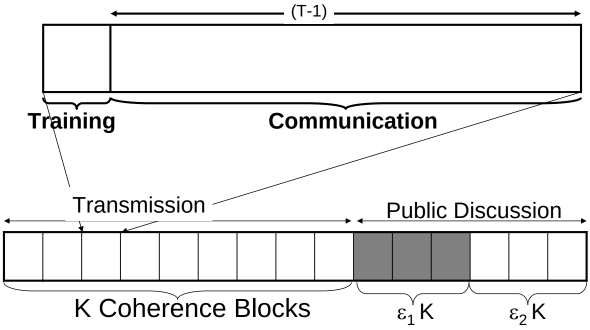
Theorem

In the high SNR regime our upper and lower bound (with public discussion) coincide:

$$\lim_{P\to\infty}\left\{R^{+}(P)-R^{-}_{\mathrm{PD}}(P)\right\}\leq\frac{c}{T}$$

where

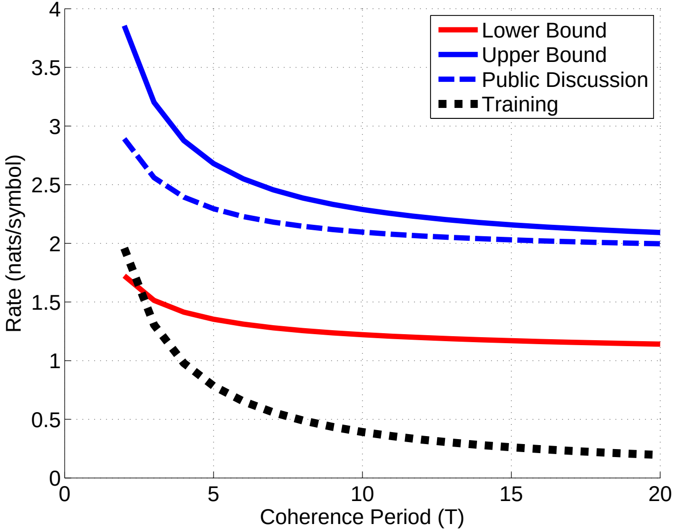
$$c = E\left[\log\left(1+\frac{|h_{AB}|^2}{|g_A|^2}\right)\right] + E\left[\log\left(1+\frac{|h_{BA}|^2}{|g_B|^2}\right)\right]$$



Phase	Coherence Blocks
Probing + Randomness Sharing	K
Channel-Sequence Reconciliation	$\varepsilon_1 \cdot K$
Source-Sequence Reconciliation	$\varepsilon_2 \cdot K$

Numerical Plot

SNR =35 dB, $h_1, h_2 \sim \mathcal{CN}(0,1)$, $\rho = 0.99$.



Symmetric MIMO Extension

M. Andersson, A. Khisti and M. Skoglund, 2012

$$\mathbf{y}_B = \mathbf{H}_{AB}\mathbf{x}_A + \mathbf{n}_{AB}, \quad \mathbf{z}_A = \mathbf{G}_{AE}\mathbf{x}_A + \mathbf{n}_{AE}$$
$$\mathbf{y}_A = \mathbf{H}_{BA}\mathbf{x}_B + \mathbf{n}_{BA}, \quad \mathbf{z}_B = \mathbf{G}_{BE}\mathbf{x}_B + \mathbf{n}_{BE}$$

- $\mathbf{H}_A, \mathbf{H}_B \in \mathbb{C}^{M \times M}$, $\mathbf{G}_{AE}, \mathbf{G}_{BE} \in \mathbb{C}^{N_E \times M}$
- Independent Rayleigh Fading, Approximate Reciprocity
- Block Fading with Coherence Period T
- $T \geq M \geq N_E$

Training + Source Emulation achieves degrees of freedom given by:

$$d = \max_{M^\star \in [1,M]} 2\frac{(T - M^\star)(M^\star - N_E)}{T}$$

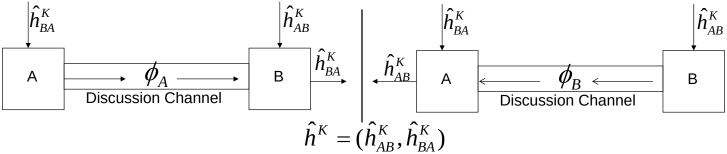
Conclusions

- Secret-Key Agreement in Two-Way fading channels
- Upper and Lower Bounds on Capacity
- Asymptotic Optimality
- Significant Gains over Training Based Schemes

Future Work:

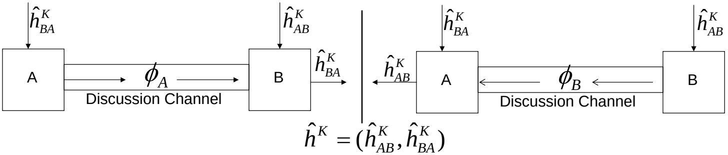
- Upper Bounds with Perfect Reciprocity (See Also Lai-Liang-Poor '12)
- Stationary Fading Channels
- Low SNR Regime
- Stronger Eavesdropper Channels

Reconciliation of Channel-Estimate Sequences $(\hat{h}^K_{AB}, \hat{h}^K_{BA})$

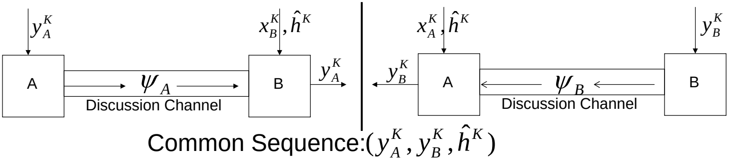


$$\frac{1}{K}H(\phi_A) \approx H(\hat{h}_{AB}|\hat{h}_{BA}), \quad \frac{1}{K}H(\phi_B) \approx H(\hat{h}_{BA}|\hat{h}_{AB})$$

Reconciliation of Channel-Estimate Sequences $(\hat{h}^K_{AB}, \hat{h}^K_{BA})$



Reconciliation of $(\mathbf{y}^K_A, \mathbf{y}^K_B)$



$$\frac{1}{TK} H(\psi_A) \approx H(y_A | x_B, \hat{h}_{AB}, \hat{h}_{BA}), \frac{1}{TK} H(\psi_B) \approx H(y_B | x_A, \hat{h}_{AB}, \hat{h}_{BA})$$