Secret-Key Generation over Reciprocal Fading Channels

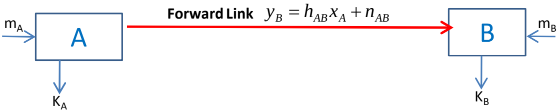
Ashish Khisti

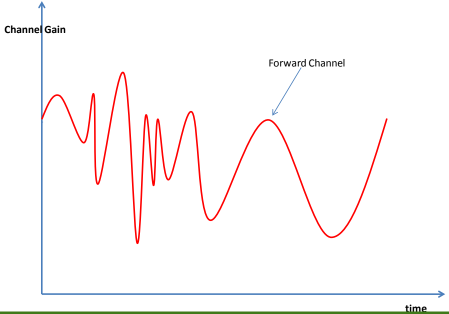
Department of Electrical and Computer Engineering
University of Toronto

Nov. 14, 2012

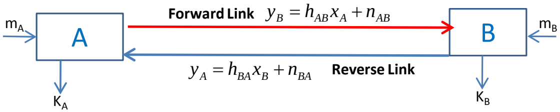
Motivation

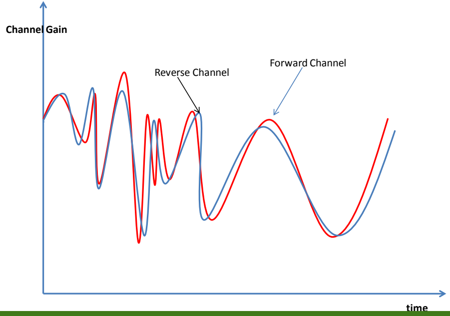
Secret-Key Generation in Wireless Fading Channels





Secret-Key Generation in Wireless Fading Channels





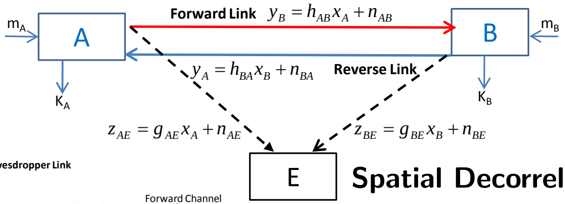
Fading:

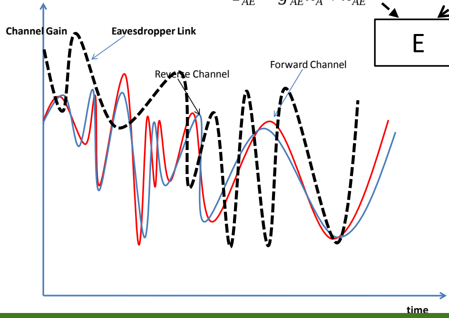
$$y_B(t) = h_{AB}(t)x_A(t) + n_B(t)$$

Reciprocity:

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

Secret-Key Generation in Wireless Fading Channels





Spatial Decorrelation:

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

Secret-Key Generation : Prior Literature

Secret-Key Generation in Wireless Systems

- A. Hassan, W. Stark, J. Hershey, and S. Chennakeshu ('96)
- UWB Systems: Wilson-Tse-Scholz ('07), M. Ko ('07), Madiseh-Neville-McGuire('12)
- Experimental UWB: Measurements for Key Generation Madiseh ('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)
- Quantization Techniques: Ye-Reznik-Shah ('07), Hamida-Pierrot-Castelluccia ('09), Sun-Zhu-Jiang-Zhao ('11)
- Adaptive Channel Probing: Wei-Zheng-Mohapatra ('10)
- Unauthenticated Channels, Impersonation Attacks, Spoofing: Mathur et al. ('10), Xiao-Greenstein-Mandayam-Trappe ('07).
- Mobility Assisted Key Generation: Zhang-Kasera-Patwari ('10), Gungor-Chen-Koksal ('11)
- Active Eavesdroppers: Zafer-Agrawal-Srivatsa
- Software Radio Implementations: Jana et. al. ('09)
- MIMO systems: Wallace and Sharma ('10), Shimizu et al. Zeng-Wu-Mohapatra

Secret-Key Generation : Prior Literature

Information Theoretic Secret-Key Generation:

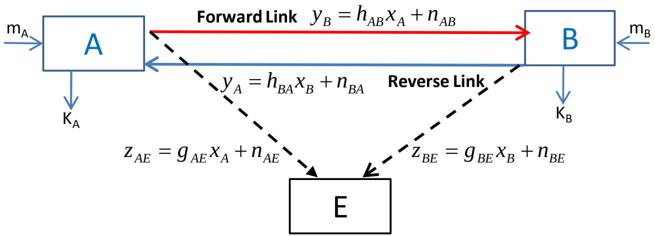
- Information Theoretic Secrecy: Shannon '49
- Secret-Key Generation from Correlated Randomness: Maurer ('93), Csiszar-Ahlswede ('93)
- Strong Secrecy: Csiszar ('96), Maurer-Wolf ('00), Watanabe ('11)
- Secret-Key Generation over Unauthenticated Channels: Maurer and Wolf ('03)
- Multi-terminal Secret-Key Generation: Csiszar-Narayan ('04)
- Joint Source-Channel Coding: Khisti-Diggavi-Wornell ('12), Prabhakaran-Eswaran-Ramchandran ('12)
- Secret-Key Generation over Channels with State: Khisti-Diggavi-Wornell ('12), Khisti ('10), Zibaeenejad ('12)
- Secret-Key generation over Two-Way channels: Ahmadi and Safavi-Naini ('11)
- Network Coding for Secret-Key Agreement: Chan ('11)
- Authentication based on Secret-Key Generation: Willems and T. Ignatenko ('12)
- Minimum Rate for Secret-Key Generation: Tyagi ('12)

Gap between Theory and Practice

Observation

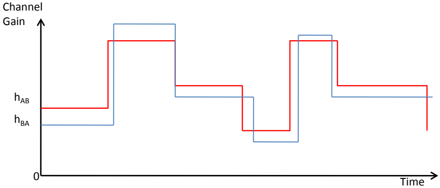
- There exists a disconnect between the Information Theoretic Models and Practical Systems for Secret-Key Generation
- No Information Theoretic limits are known!
- No provably optimal signalling scheme is known.

Problem Setup

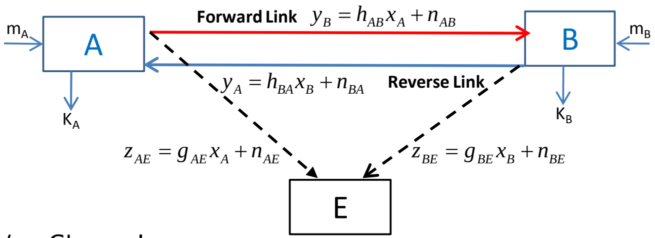


- No CSI: $h_{AB}(i)$ and $h_{BA}(i)$
- $g_A(i)$ & $g_B(i)$ known to Eve
- Block-Fading:
  Coherence Period: T.
- Approximate Reciprocity:
  $(h_{AB}, h_{BA}) \sim p_{h_{AB},h_{BA}}(\cdot,\cdot)$
- Independence:
  $(g_{AE}, g_{BE}) \perp (h_{AB}, h_{BA})$

Channel Reciprocity



Problem Setup



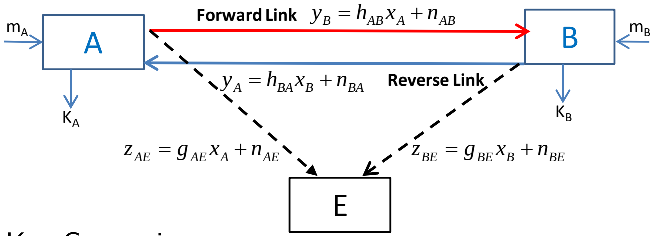
Two Way Channel:

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

Interactive Comm.: $x_A(i) = f_A(m_A, y_A^{i-1})$, $x_B(i) = f_B(m_B, y_B^{i-1})$

Average Power Constraint $E[|x_A|^2] \leq P$, $E[|x_B|^2] \leq P$.

Problem Setup



Secret-Key Generation

- $k_A = \mathcal{K}_A(y_A^N, m_A), \;\; k_B = \mathcal{K}_B(y_B^N, m_B)$
- Reliability: $\Pr(k_A \neq k_B) \leq \varepsilon_N$
- Secrecy: $I(k_A; z_A^N, z_B^N, g_A^N, g_B^N) \leq N\varepsilon_N$
- Rate $R = \frac{1}{N} H(k_A)$

Secret-Key Capacity.

Theorem

An upper bound on the secret-key capacity is given by:

$$R^+ \leq \frac{1}{T} I(h_{AB}; h_{BA}) + \max_{P(h_{AB}) \in \mathcal{P}} \{ I(y_B; x_A | h_{AB}, z_A, g_A) \}$$
$$+ \max_{P(h_{BA}) \in \mathcal{P}} I(y_A; x_B | h_{BA}, z_B, g_B)$$

where: $p_{x_A | h_{AB}} \equiv \mathcal{CN}\left(0, P(h_{AB})\right), \, p_{x_B | h_{BA}} \equiv \mathcal{CN}\left(0, P(h_{BA})\right).$

Secret-Key Capacity — Upper Bound

Khisti'12

Theorem

An upper bound on the secret-key capacity is given by:

$$R^+ \leq \frac{1}{T} I(h_{AB}; h_{BA}) + \max_{P(h_{AB}) \in \mathcal{P}} \{ I(y_B; x_A | h_{AB}, z_A, g_A) \} + \max_{P(h_{BA}) \in \mathcal{P}} I(y_A; x_B | h_{BA}, z_B, g_B)$$

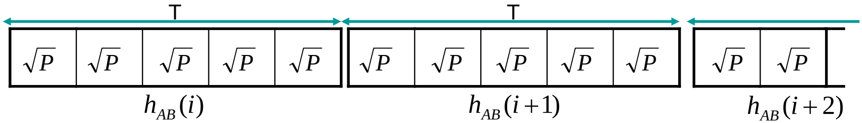
where: $p_{x_A | h_{AB}} \equiv \mathcal{CN}\left(0, P(h_{AB})\right), \; p_{x_B | h_{BA}} \equiv \mathcal{CN}\left(0, P(h_{BA})\right)$.

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: $I(y_A; x_B | h_{BA}, z_B, g_B)$

Training-Only Scheme

Probe K Coherence Blocks

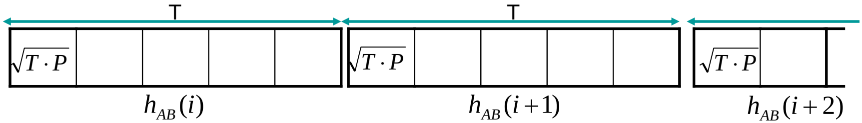


- $x_A(i,t) = \sqrt{P}$
- $\mathbf{y}_B(i) = \sqrt{P} \cdot h_{AB}(i) \cdot \mathbf{1} + \mathbf{n}(i)$
- $\hat{h}_{AB}(i)$: MMSE estimate
- Estimate $\hat{h}_{AB}^K$ on the forward link; $\hat{h}_{BA}^K$ on the reverse link.

Secret-Key Rate: $R^+ = \frac{1}{T} I(\hat{h}_{AB}; \hat{h}_{BA})$

Training-Only Scheme

Probe K Coherence Blocks

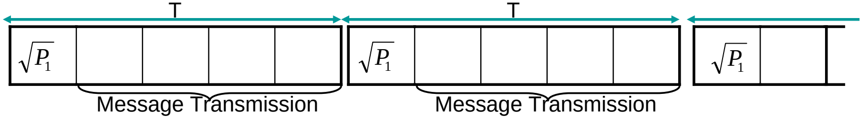


- $x_A(i,1) = \sqrt{T \cdot P}$, $x_A(i,t) = 0$, $i = 1 \ldots, K$, $t = 2, \ldots, T$.
- $y_B(i) = \sqrt{T \cdot P} h_{AB}(i) + n(i)$, $i = 1, 2, \ldots, K$
- $\hat{h}_{AB}(i)$: MMSE estimate
- Estimate $\hat{h}_{AB}^K$ on the forward link; $\hat{h}_{BA}^K$ on the reverse link.

Secret-Key Rate: $R^+ = \frac{1}{T} I(\hat{h}_{AB}; \hat{h}_{BA})$

Message Transmission

Lai-Liang-Poor '12



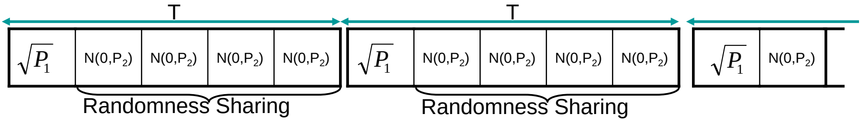
- Training: $x_A(i,1) = \sqrt{P_1}$, $R_T = \frac{1}{T} I(\hat{h}_{AB}; \hat{h}_{BA})$
- Secure Msg. Transmission: $\{x_A(i,2), \ldots, x_A(i,T)\}_{i=1,2\ldots,K}$
  $R_M = \frac{T-1}{T} E\left[\log(1 + P_2(\hat{h}_{AB})|\hat{h}_{AB}|^2) - \log(1 + P_2(\hat{h}_{AB})|g_A|^2)\right]$

The overall rate is NOT: $R_T + R_M$

- Power Allocation in R_M leaks $\hat{h}_{AB}$ to Eavesdropper
- Without Power Allocation, R_M is generally zero.

Proposed Scheme: Randomness Sharing

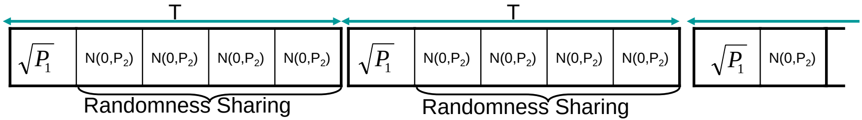
Khisti '12



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

- 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: $\mathbf{y}_A(i) = h_{BA}(i)\mathbf{x}_B(i) + \mathbf{n}_A(i) \in \mathbb{C}^{T-1}$.

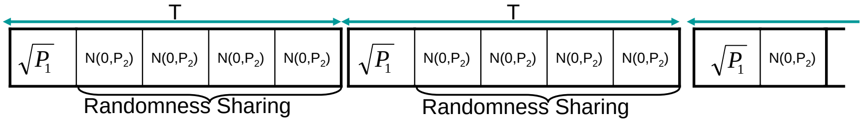
Proposed Scheme: Randomness Sharing
Khisti '12



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

Proposed Scheme: Randomness Sharing

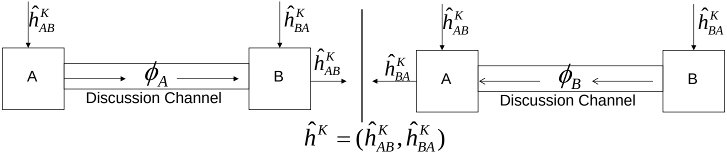
Khisti '12



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

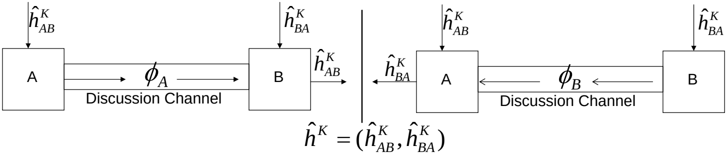
Generate a secret-key from these sequences.

Channel-Sequence Reconciliation

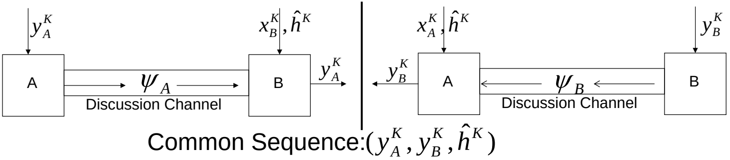


$$H(\phi_A) = H(\hat{h}_{BA}|\hat{h}_{AB}), \quad H(\phi_B) = H(\hat{h}_{AB}|\hat{h}_{BA})$$

Channel-Sequence Reconciliation



Source-Sequence Reconciliation



$$H(\psi_A) \le H(y_A | x_B, \hat{h}_{AB}, \hat{h}_{BA}), \quad H(\psi_B) \le H(y_B | x_A, \hat{h}_{AB}, \hat{h}_{BA})$$

Equivocation Bound

- Public Messages: $\{\phi_A, \phi_B, \psi_A, \psi_B\}$
- Common Sequences: $(\mathbf{y}_A^K, \mathbf{y}_B^K, \hat{h}_{AB}^K, \hat{h}_{BA}^K)$
- Equivocation Rate:
  $\frac{1}{T \cdot K} H(\mathbf{y}_A^K, \mathbf{y}_B^K, \hat{h}_{AB}^K, \hat{h}_{BA}^K | \phi_A, \phi_B, \psi_A, \psi_B, \mathbf{z}^K, \mathbf{g}^K)$

Equivocation Bound

Equivocation-Rate Bound:

$$
\begin{aligned}
&\frac{1}{T\cdot K}H(\mathbf{y}_A^K,\mathbf{y}_B^K,\hat{h}_{AB}^K,\hat{h}_{BA}^K|\phi_A,\phi_B,\psi_A,\psi_B,\mathbf{z}^K,\mathbf{g}^K)\\
&\geq \frac{1}{T\cdot K}\Bigg\{H(\mathbf{y}_A^K,\mathbf{y}_B^K,\hat{h}_{AB}^K,\hat{h}_{BA}^K|\mathbf{z}_A^K,\mathbf{z}_B^K,g_A^K,g_B^K)\\
&\qquad -\underbrace{H(\phi_A)-H(\phi_B)-H(\psi_A)-H(\psi_B)}_{=\Delta}\Bigg\}\\
&\geq \frac{1}{T\cdot K}\Bigg\{H(\hat{h}_{AB}^K,\hat{h}_{BA}^K)+H(\mathbf{y}_A^K,\mathbf{y}_B^K|\mathbf{z}_A^K,\mathbf{z}_B^K,g_A^K,g_B^K,\hat{h}_{AB}^K,\hat{h}_{BA}^K)-\Delta\Bigg\}\\
&\geq \frac{1}{T\cdot K}\Bigg\{H(\mathbf{y}_A^K|h_{BA}^K,\mathbf{z}_B^K,\mathbf{g}^K)+H(\mathbf{y}_B^K|h_{AB}^K,\mathbf{z}_A^K,\mathbf{g}^K)\\
&\qquad +H(\hat{h}_{AB}^K,\hat{h}_{BA}^K)-\Delta\Bigg\}
\end{aligned}
$$

Equivocation Bound

$$\frac{1}{T \cdot K} H(\mathbf{y}_A^K, \mathbf{y}_B^K, \hat{h}_{AB}^K, \hat{h}_{BA}^K | \phi_A, \phi_B, \psi_A, \psi_B, \mathbf{z}^K, \mathbf{g}^K)$$

$$\geq \Bigg\{ \frac{1}{T} \underbrace{I(\hat{h}_{AB}; \hat{h}_{BA})}_{\text{Training}} + \frac{T-1}{T} \underbrace{\Big[I(y_B; x_A, \hat{h}_{AB}) - I(y_B; z_A, g_A, h_{AB}) \Big]}_{\text{Forward Channel}}$$

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

Equivocation Bound

$$\frac{1}{T\cdot K}H(\mathbf{y}_A^K,\mathbf{y}_B^K,\hat{h}_{AB}^K,\hat{h}_{BA}^K|\phi_A,\phi_B,\psi_A,\psi_B,\mathbf{z}^K,\mathbf{g}^K)$$

$$\geq\left\{\frac{1}{T}\underbrace{I(\hat{h}_{AB};\hat{h}_{BA})}_{\text{Training}}+\frac{T-1}{T}\underbrace{\left[I(y_B;x_A,\hat{h}_{AB})-I(y_B;z_A,g_A,h_{AB})\right]}_{\text{Forward Channel}}\right.$$

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

$$R^+\leq\frac{1}{T}I(h_{AB};h_{BA})+\max_{P(h_{AB})\in\mathcal{P}}\{I(y_B;x_A|h_{AB},z_A,g_A)\}$$

$$+\max_{P(h_{BA})\in\mathcal{P}}I(y_A;x_B|h_{BA},z_B,g_B)$$

High SNR Regime

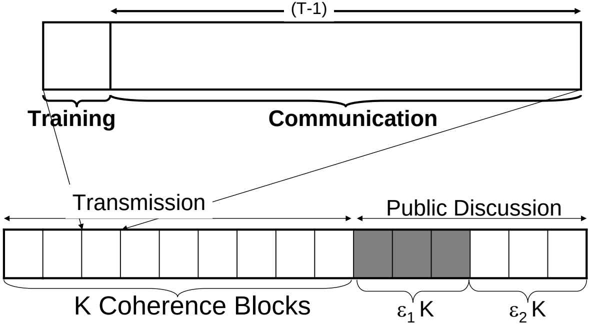
Theorem

In the high SNR regime our upper and lower bounds coincide:

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

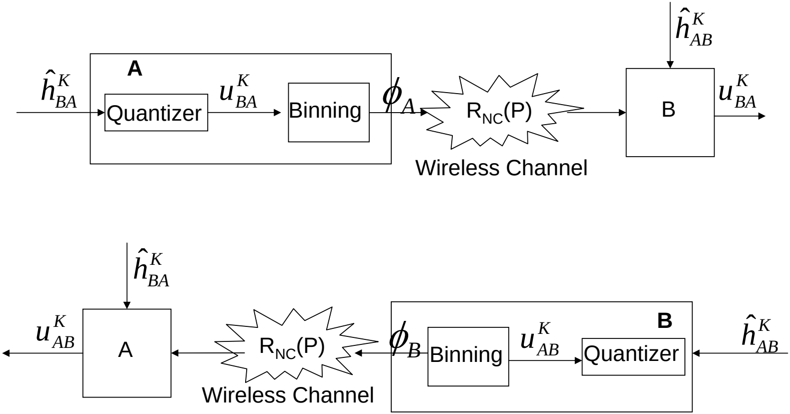
where

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



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

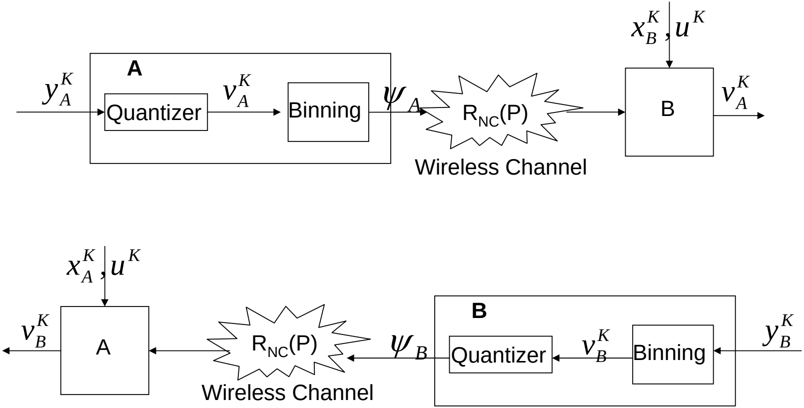
Error Reconciliation - Channel Sequences



Common Sequence: $\mathbf{u}^K \triangleq (u_{AB}^K, u_{BA}^K)$.
Rate Constraints:

- $I(u_{BA}; \hat{h}_{BA} | \hat{h}_{AB}) \leq \varepsilon_1 (T-1) R_{\mathrm{NC}}(P)$
- $I(u_{AB}; \hat{h}_{AB} | \hat{h}_{BA}) \leq \varepsilon_1 (T-1) R_{\mathrm{NC}}(P)$

Error Reconciliation - Source Sequences



Rate Constraints:

$I(v_A; y_A | x_B, \mathbf{u}) \leq \varepsilon_2 \cdot R_{\text{NC}}(P)$, $I(v_B; y_B | x_A, \mathbf{u}) \leq \varepsilon_2 \cdot R_{\text{NC}}(P)$

Secret-Key Rate

Without Public Discussion

$$R = \frac{1}{1+\varepsilon_1+\varepsilon_2}\left(\frac{1}{T}R_T + \frac{T-1}{T}R_F + \frac{T-1}{T}R_B\right)$$

Secret-Key Rate

Without Public Discussion

$$R = \frac{1}{1+\varepsilon_1+\varepsilon_2}\left(\frac{1}{T}R_T + \frac{T-1}{T}R_F + \frac{T-1}{T}R_B\right)$$

$$R_T = I(u_{AB};\hat{h}_{BA}) + I(u_{BA};\hat{h}_{AB}) - I(u_{AB};u_{BA})$$
$$R_F = I(v_A;x_B,u_{AB},u_{BA}) - I(v_A;z_B,g_B,h_{BA})$$
$$R_B = I(v_B;x_A,u_{AB},u_{BA}) - I(v_B;z_A,g_A,h_{AB})$$

Rate Constraints:

$$I(u_{BA};\hat{h}_{BA}|\hat{h}_{AB}) \le \varepsilon_1(T-1)R_{\mathrm{NC}}(P)$$
$$I(u_{AB};\hat{h}_{AB}|\hat{h}_{BA}) \le \varepsilon_1(T-1)R_{\mathrm{NC}}(P)$$
$$I(v_A;y_A|x_B,u_{AB},u_{BA}) \le \varepsilon_2 R_{\mathrm{NC}}(P)$$
$$I(v_B;y_B|x_A,u_{AB},u_{BA}) \le \varepsilon_2 R_{\mathrm{NC}}(P)$$

High SNR Regime

Theorem

In the high SNR regime our upper and lower bounds coincide:

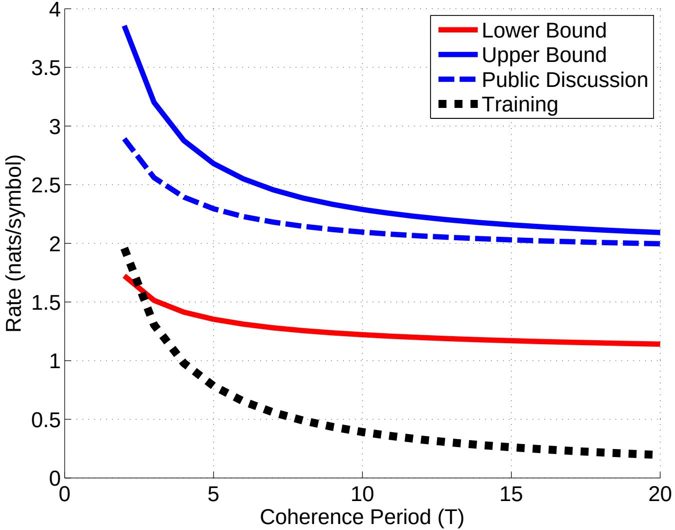
$$\lim_{P \to \infty} \left\{ R^{+}(P) - R^{-}(P) \right\} \leq \frac{c}{T}$$

where

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

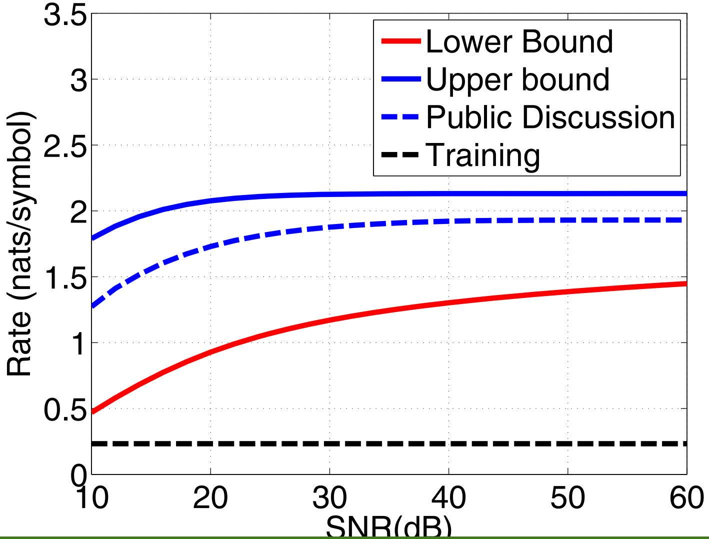
Numerical Plot

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



Numerical Plot

$$T = 10,\ h_1, h_2 \sim \mathcal{CN}(0,1),\ \rho = 0.95$$



Theorem

An upper bound on the secret-key capacity is given by:

$$R^{+} \leq \frac{1}{T} I(\mathsf{h}_{AB}; \mathsf{h}_{BA}) + \max_{P(\mathsf{h}_{AB}) \in \mathcal{P}} \{ I(\mathsf{y}_B; \mathsf{x}_A | \mathsf{h}_{AB}, \mathsf{z}_A, \mathsf{g}_A) \}$$
$$+ \max_{P(\mathsf{h}_{BA}) \in \mathcal{P}} I(\mathsf{y}_A; \mathsf{x}_B | \mathsf{h}_{BA}, \mathsf{z}_B, \mathsf{g}_B)$$

where: $p_{\mathsf{x}_A|\mathsf{h}_{AB}} \equiv \mathcal{CN}\left(0, P(\mathsf{h}_{AB})\right)$, $p_{\mathsf{x}_B|\mathsf{h}_{BA}} \equiv \mathcal{CN}\left(0, P(\mathsf{h}_{BA})\right)$.

Upper Bound - Proof

Maurer '93

$$
\begin{aligned}
NR &\leq I(k_A; k_B) - I(k_A; \mathbf{z}^N, \mathbf{g}^K) \\
&\leq I(k_A; k_B | \mathbf{z}^N, \mathbf{g}^K) \\
&\leq I(m_A, h_{BA}^N, y_A^N; m_B, h_{AB}^N, y_B^N | \mathbf{z}^N, \mathbf{g}^N)
\end{aligned}
$$

Upper Bound - Proof

Maurer '93

$$
\begin{aligned}
NR &\leq I(k_A; k_B) - I(k_A; \mathbf{z}^N, \mathbf{g}^K) \\
&\leq I(k_A; k_B | \mathbf{z}^N, \mathbf{g}^K) \\
&\leq I(m_A, h_{BA}^N, y_A^N; m_B, h_{AB}^N, y_B^N | \mathbf{z}^N, \mathbf{g}^N) \\
&= I(m_A, h_{BA}^N, y_A^{N-1}; m_B, h_{AB}^N, y_B^{N-1} | \mathbf{z}^N, \mathbf{g}^K) + \\
&\quad I(y_A(N); m_B, h_{AB}^N, y_B^{N-1} | \mathbf{z}^N, \mathbf{g}^K, m_A, h_{BA}^N, y_A^{N-1}) + \\
&\quad I(m_A, h_{BA}^N, y_A^{N-1}; y_B(N) | \mathbf{z}^N, \mathbf{g}^K, m_B, h_{AB}^N, y_B^{N-1}) + \\
&\quad I(y_A(N); y_B(N) | \mathbf{z}^N, \mathbf{g}^K, m_B, h_{AB}^N, y_B^{N-1}, m_A, h_{BA}^N, y_A^{N-1}).
\end{aligned}
$$

Upper Bound - Proof

Maurer '93

$$
\begin{aligned}
NR &\le I(k_A; k_B) - I(k_A; \mathbf{z}^N, \mathbf{g}^K) \\
&\le I(k_A; k_B | \mathbf{z}^N, \mathbf{g}^K) \\
&\le I(m_A, h_{BA}^N, y_A^N; m_B, h_{AB}^N, y_B^N | \mathbf{z}^N, \mathbf{g}^N) \\
&= \underbrace{I(m_A, h_{BA}^N, y_A^{N-1}; m_B, h_{AB}^N, y_B^{N-1} | \mathbf{z}^N, \mathbf{g}^K)}_{\le I(m_A, h_{BA}^N, y_A^{N-1}; m_B, h_{AB}^N, y_B^{N-1} | \mathbf{z}^{N-1}, \mathbf{g}^K)} + \\
&\quad \underbrace{I(y_A(N); m_B, h_{AB}^N, y_B^{N-1} | \mathbf{z}^N, \mathbf{g}^K, m_A, h_{BA}^N, y_A^{N-1})}_{\le I(x_B(N); y_A(N) | z_B(N), g_B(N), h_{BA}(N))} + \\
&\quad \underbrace{I(y_B(N); m_A, h_{BA}^N, y_A^{N-1} | \mathbf{z}^N, \mathbf{g}^K, m_B, h_{AB}^N, y_B^{N-1})}_{\le I(x_A(N); y_B(N) | z_A(N), g_A(N), h_{AB}(N))} + \\
&\quad \underbrace{I(y_A(N); y_B(N) | \mathbf{z}^N, \mathbf{g}^K, m_B, h_{AB}^N, y_B^{N-1}, m_A, h_{BA}^N, y_A^{N-1})}.
\end{aligned}
$$

Upper Bound - Proof

Maurer '93

$$
\begin{aligned}
NR &\leq I(k_A; k_B) - I(k_A; \mathbf{z}^N, \mathbf{g}^K) \\
&\leq I(k_A; k_B | \mathbf{z}^N, \mathbf{g}^K) \\
&\leq I(m_A, h_{BA}^N, y_A^N; m_B, h_{AB}^N, y_B^N | \mathbf{z}^N, \mathbf{g}^N)
\end{aligned}
$$

$$
\leq I(h_{AB}^N; h_{BA}^N) + \sum_{i=1}^{N} I(x_B(i); y_A(i) | z_B(i), g_B(i), h_{BA}(i)) +
$$

$$
\sum_{i=1}^{N} I(x_A(i); y_B(i) | z_A(i), g_A(i), h_{AB}(i))
$$

Optimality of Gaussian Inputs, Power Constraints ...

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:

- Improved Upper Bounds
- Stationary Fading Channels
- Low SNR Regime
- Stronger Eavesdropper Channels