Secret-Key Agreement over a Non-Coherent Block-Fading MIMO Wiretap Channel

Mattias Andersson*, Ashish Khisti† and Mikael Skoglund*
*School of Electrical Engineering and the ACCESS Linnaeus Centre,
Royal Institute of Technology (KTH),
Stockholm, Sweden
email: {amattias,skoglund}@ee.kth.se
†Electr. & Comput. Eng. Dept.,
Univ. of Toronto,
Toronto, ON, Canada
email: akhisti@comm.utoronto.ca

Abstract—**We study secret-key agreement over a non-coherent block-fading multiple input multiple output (MIMO) wiretap channel. We give an achievable scheme based on training and source emulation and analyze the rate in the high SNR regime. Based on this analysis we find the optimal number of antennas to use for training. Our main result is that if the sum of the number of antennas at Alice and Bob is larger than the coherence time of the channel, the achievable rate does not depend on the number of antennas at Eve. In this case source emulation is not needed, and using only training is optimal. We also consider the case when there is no public channel available. In this case we show that secret-key agreement is still possible by using the wireless channel for discussion, giving the same number of secure degrees of freedom as in the case with a public channel.**

I. Introduction

Information theoretic security was first studied in [1], and since then there has been a large interest in studying security from this perspective [2]–[4]. We consider secret-key agreement over a non-coherent block-fading MIMO channel. The goal in secret-key agreement is for two legitimate parties Alice and Bob to agree on a key K, which is to be kept secret from an adversary Eve [5], [6]. Secret-key agreement over fading channels has been extensively studied [7]–[14]. In [12] the secret-key capacity for the coherent fast fading MIMO wiretap channel was found. The non-coherent fast fading case was studied in [15]. [13] is closest to our work and considers secret-key agreement for non-coherent slow fading single antenna channels using a two-phase scheme with training and secret message transmission. In the first phase Alice and Bob transmit known training signals to each other. Assuming channel reciprocity, they in this way obtain an estimate of the channel gain. In the second phase Alice uses a wiretap channel code and transmits a random codeword to Bob. The achievable secret-key rate in the first phase scales with the power P as $(\log P)/T$, where T is the coherence time of the channel, while the achievable rate from the second phase is bounded. We consider a similar multi-phase scheme with training, but instead of secret message transmission, we suggest source emulation in the last phase, where Alice transmits random sequences instead of a codeword from a wiretap channel code.

II. Channel Model

We consider the channel type model from [5] with a wiretapper. Alice and Bob communicate over a two way block-fading (MIMO) channel. In addition they can also use a public discussion channel with unlimited capacity. We pose the constraint that a node cannot transmit and receive at the same time. We assume that Alice, Bob, and Eve have n_A, n_B, and n_E antennas, respectively, with $n_A \geq n_B$ without loss of generality. If Alice uses the channel, the received signals at Bob and Eve at time t are given by

$$\begin{aligned}\mathbf{Y_B}(t) &= \mathbf{H}(t)\mathbf{X_A}(t) + \mathbf{V_B}(t),\\ \mathbf{Y_E}(t) &= \mathbf{G_A}(t)\mathbf{X_A}(t) + \mathbf{V_E}(t),\end{aligned}$$

and if Bob uses the channel, the received signals at Alice and Eve are given by

$$\begin{aligned}\mathbf{Y_A}(t) &= \mathbf{H}^{\dagger}(t)\mathbf{X_B}(t) + \mathbf{V_A}(t),\\ \mathbf{Y_E}(t) &= \mathbf{G_B}(t)\mathbf{X_B}(t) + \mathbf{V_E}(t).\end{aligned}$$

Here $\mathbf{X_A}(t) \in \mathbb{C}^{n_A}$, or $\mathbf{X_B}(t) \in \mathbb{C}^{n_B}$ is the transmitted signal, $\mathbf{Y_A}(t) \in \mathbb{C}^{n_A}$, $\mathbf{Y_B}(t) \in \mathbb{C}^{n_B}$, and $\mathbf{Y_E}(t) \in \mathbb{C}^{n_E}$ are Alice's, Bob's, and Eve's received signals, respectively. $\mathbf{H}(t)$ represents the channel matrix between Alice and Bob, and $\mathbf{G_A}(t)$ and $\mathbf{G_B}(t)$ are the channel matrices between Alice and Eve, and Bob and Eve, respectively. The noise terms $\mathbf{V_A}(t) \sim \mathcal{CN}(0, \mathbf{I}_{n_A})$, $\mathbf{V_B}(t) \sim \mathcal{CN}(0, \mathbf{I}_{n_B})$, and $\mathbf{V_E}(t) \sim \mathcal{CN}(0, \mathbf{I}_{n_E})$ are i.i.d. and independent of each other and all other variables. We assume that the entries of $\mathbf{H}(t)$, $\mathbf{G_A}(t)$, and $\mathbf{G_B}(t)$ are distributed as $\mathcal{CN}(0, 1)$, independent of each other, and stay fixed for T channel uses, but are independent between different fading blocks. We further assume a short-term average power constraint on the input symbols

$$\mathbb{E}[\mathbf{X_A}^{\dagger}(t)\mathbf{X_A}(t)] \leq P,\ \mathbb{E}[\mathbf{X_B}^{\dagger}(t)\mathbf{X_B}(t)] \leq P. \tag{1}$$

M. Andersson would like to thank the Ericsson Research Foundation for partially funding his visit to the University of Toronto.

Denote the message sent over the public channel by Alice at time k by Φ_k and the message sent by Bob at time k by Ψ_k. We consider key agreement over several coherence blocks N, and denote the symbols transmitted and received by Alice and Bob in these N blocks by $(\mathbf{X_A^N}, \mathbf{Y_A^N})$ and $(\mathbf{X_B^N}, \mathbf{Y_B^N})$, respectively. The message transmitted over the public channel at time k can depend on previous observed symbols: $\Phi_k = \Phi_k(\mathbf{X_A^{k-1}}, \mathbf{Y_A^{k-1}}, \Psi^{k-1}, \Phi^{k-1})$, and $\Psi_k = \Psi_k(\mathbf{X_B^{k-1}}, \mathbf{Y_B^{k-1}}, \Psi^{k-1}, \Phi^{k-1})$. After N coherence blocks, and K uses of the public channel Alice generates a key $K_A = K_1(\mathbf{X_A^K}, \mathbf{Y_A^K}, \Psi^K, \Phi^K) \in \mathcal{K}$, and Bob generates a key $K_B = K_B(\mathbf{X_A^K}, \mathbf{Y_A^K}, \Psi^K, \Phi^K) \in \mathcal{K}$. A key rate R is achievable if for every $\epsilon > 0$, and large enough N, there exists a secret-sharing strategy of this form such that

$$\Pr(K_A \neq K_B) < \epsilon$$

$$\frac{1}{N} I(\mathbf{Z}^N, \Phi^K, \Psi^K; K) < \epsilon$$

$$\frac{1}{N} H(K) > R - \epsilon$$

$$\frac{1}{N} \log |\mathcal{K}| < \frac{1}{N} H(K) + \epsilon.$$

The supremum of all achievable key rates is called the secret-key capacity.

III. Achievable Scheme

We consider a three-phase scheme based on transmitting known training symbols between Alice and Bob in the first two phases, and source emulation in the third phase. By source emulation we mean that Alice generates random symbols $\mathbf{X_A}$ and transmits them over the channel. Bob then quantizes his observations from the training phase and the source emulation phase, and sends enough information over the public channel in order for Alice and Bob to agree on a secret key K.

In phase one Alice transmits known training symbols between time 1 and $M_A < n_A$. Alice's transmitted symbols at antenna j at time t are given by

$$\mathbf{X}_{\mathbf{A},j}(t) = \delta_{t,j} \sqrt{P},$$

where

$$\delta_{i,j} = \begin{cases} 1 & \text{if } i = j, \\ 0 & \text{otherwise.} \end{cases}$$

In phase two Bob transmits known training symbols between time M_A+1 and M_A+M_B, with $M_B < n_B$. Bob's transmitted symbols at antenna j at time t are given by

$$\mathbf{X}_{\mathbf{B},j}(t) = \delta_{(t-M_A),j} \sqrt{P}.$$

As in [16], Alice and Bob can estimate parts of $\mathbf{H}$ from their received signals during the training phases using component-wise minimum mean square error (MMSE) estimation. Let

$$\mathbf{H} = \begin{bmatrix} \mathbf{H_1} & \mathbf{H_2} \\ \mathbf{H_3} & \mathbf{H_4} \end{bmatrix},$$

where $\mathbf{H_1} \in \mathbb{C}^{M_B \times M_A}$, $\mathbf{H_2} \in \mathbb{C}^{M_B \times (n_A - M_A)}$, $\mathbf{H_3} \in \mathbb{C}^{(n_B - M_B) \times M_A}$, and $\mathbf{H_4} \in \mathbb{C}^{(n_B - M_B) \times (n_A - M_A)}$. Bob's received signal at time j at antenna i is

$$y_{B,i}(j) = H_{i,j} \sqrt{P} + v_{B,i}(j). \tag{2}$$

The MMSE estimate $\hat{H}_{B,i,j}$ of $H_{i,j}$ is a circularly symmetric Gaussian random variable with variance $P/(P+1)$ given by

$$\hat{H}_{B,i,j} = \frac{\sqrt{P}}{P+1} y_{B,i}(j). \tag{3}$$

The estimation error $e_{B,i,j} = H_{i,j} - \hat{H}_{B,i,j}$ is distributed as $\mathcal{CN}(0, 1/(P+1))$. The estimation errors $e_{B,i,j}$ and the estimates $\hat{H}_{B,i,j}$ are all independent of each other. In this way Bob obtains an MMSE estimate $\mathbf{\hat{H}_B} = \left[\mathbf{\hat{H}_{B,1}^{\mathit{T}}}\ \mathbf{\hat{H}_{B,3}^{\mathit{T}}}\right]^T$ of $\left[\mathbf{H_1}^T\ \mathbf{H_3}^T\right]^T$, and in the same way Alice can form an MMSE estimate $\mathbf{\hat{H}_A} = \left[\mathbf{\hat{H}_{A,1}} \mathbf{\hat{H}_{A,2}}\right]$ of $[\mathbf{H_{A,1}} \mathbf{H_{A,2}}]$ from her observations in the second phase. Eve can also estimate the channel matrix $\mathbf{G_A}$ from Alice's transmission in the first phase. We assume that Eve's estimate of $\mathbf{G_A}$ is perfect, since this gives a lower bound on the achievable secret-key rate.

In phase three Alice uses the first M_A antennas to transmit i.i.d. vectors $\mathbf{X_A}(t) \sim \mathcal{CN}(0, P/M_A \mathbf{I}_{M_A})$, between time $M_A + M_B + 1$ and T. To simplify the notation we will refer to these transmitted signals $\{\mathbf{X_A}(t)\}_{t=M_A+M_B+1}^T$ simply as $\mathbf{X_A}$, and to the received signals at Bob and Eve in the third phase as $\mathbf{Y_B}$ and $\mathbf{Y_E}$, respectively. We choose $\mathbf{X_A}$ to be independent of Alice's estimate $\mathbf{\hat{H}_A}$ in order to simplify the analysis of the achievable rate. We have the following result:

Theorem III.1. *The rate achieved by the described training based scheme is bounded from below by*

$$\frac{M_A M_B}{T} \log\left(1 + \frac{P^2}{2P+1}\right) + \frac{T - M_A - M_B}{T} R_{SE},$$

where R_{SE} is given by

$$\mathbb{E}\left[\log \frac{\det\left(\mathbf{I}_{M_A} + P/M_A \mathbf{G_A}^\dagger \mathbf{G_A} + P/M_A \mathbf{H}^\dagger \mathbf{H}\right)}{\det\left(\mathbf{I}_{M_A} + P/M_A \mathbf{G_A}^\dagger \mathbf{G_A}\right)}\right] +$$

$$- M_B \log \tilde{\sigma}_{A,B}^2 - (n_B - M_B) \log(\tilde{\sigma}_B^2),$$

with $\tilde{\sigma}_{A,B}^2 = \frac{P}{M_A(2P+1)} + 1$, *and* $\tilde{\sigma}_B^2 = \frac{P}{M_A(P+1)} + 1$.

Proof: The random variables involved in our scheme satisfy the following Markov chain:

$$(\mathbf{Y_E}, \mathbf{G_A}) \leftrightarrow (\mathbf{X_A}, \mathbf{\hat{H}_A}) \leftrightarrow (\mathbf{Y_B}, \mathbf{H}) \leftrightarrow (\mathbf{Y_B}, \mathbf{\hat{H}_B}). \tag{4}$$

If we consider our scheme as a Source-Type Model with Wiretapper, and code over a large number of coherence blocks, the achievable secret-key rate is bounded from below by [5, Theorem 1]:

$$R_- = \frac{1}{T}(\mathbf{X_A}, \mathbf{\hat{H}_A}; \mathbf{Y_B}, \mathbf{\hat{H}_B} | \mathbf{Y_E}, \mathbf{G_A}).$$

This rate is achieved by quantizing Bob's observations $(\mathbf{Y_B}, \mathbf{\hat{H}_B})$ into a quantization codebook generated by auxiliary random variables $(\mathbf{U_Y}, \mathbf{U_H})$ and using Wyner-Ziv coding to transmit the indices over the public channel. By making the quantization fine enough we can achieve the rate R_-.

We can bound this rate from below using (4) as follows:

$$\begin{aligned}
TR_- =&I(\mathbf{X_A}, \hat{\mathbf{H}}_\mathbf{A}; \mathbf{Y_B}, \hat{\mathbf{H}}_\mathbf{B} | \mathbf{Y_E}, \mathbf{G_A})\\
=&I(\mathbf{X_A}, \hat{\mathbf{H}}_\mathbf{A}; \mathbf{Y_B}, \hat{\mathbf{H}}_\mathbf{B}) - I(\mathbf{Y_B}, \hat{\mathbf{H}}_\mathbf{B}; \mathbf{Y_E}, \mathbf{G_A})\\
\geq&I(\mathbf{X_A}, \hat{\mathbf{H}}_\mathbf{A}; \mathbf{Y_B}, \hat{\mathbf{H}}_\mathbf{B}) - I(\mathbf{Y_B}, \mathbf{H}; \mathbf{Y_E}, \mathbf{G_A})\\
\geq&I(\hat{\mathbf{H}}_\mathbf{A}; \hat{\mathbf{H}}_\mathbf{B}) + I(\mathbf{X_A}; \mathbf{Y_B} | \hat{\mathbf{H}}_\mathbf{A}, \hat{\mathbf{H}}_\mathbf{B})\\
&- I(\mathbf{Y_B}; \mathbf{Y_E} | \mathbf{H}, \mathbf{G_A})\\
=&I(\hat{\mathbf{H}}_\mathbf{A}; \hat{\mathbf{H}}_\mathbf{B}) + h(\mathbf{Y_B} | \hat{\mathbf{H}}_\mathbf{A}, \hat{\mathbf{H}}_\mathbf{B}) - h(\mathbf{Y_B} | \mathbf{H}, \mathbf{G_A})\\
&- h(\mathbf{Y_B} | \hat{\mathbf{H}}_\mathbf{A}, \hat{\mathbf{H}}_\mathbf{B}, \mathbf{X_A}) + h(\mathbf{Y_B} | \mathbf{H}, \mathbf{G_A} \mathbf{Y_E})\\
\geq&I(\hat{\mathbf{H}}_\mathbf{A}; \hat{\mathbf{H}}_\mathbf{B}) - h(\mathbf{Y_B} | \hat{\mathbf{H}}_\mathbf{A}, \hat{\mathbf{H}}_\mathbf{B}, \mathbf{X_A})\\
&+ h(\mathbf{Y_B} | \mathbf{H}, \mathbf{G_A} \mathbf{Y_E}), \qquad (5)
\end{aligned}$$

where we have used that $\mathbf{X_A}$ and $\hat{\mathbf{H}}_\mathbf{A}$ are independent in the second inequality. We see that we have two contributions to the secret-key rate. $I(\hat{\mathbf{H}}_\mathbf{A}; \hat{\mathbf{H}}_\mathbf{B})$ comes from the training phases, and $h(\mathbf{Y_B} | \mathbf{H}, \mathbf{G_A} \mathbf{Y_E}) - h(\mathbf{Y_B} | \hat{\mathbf{H}}_\mathbf{A}, \hat{\mathbf{H}}_\mathbf{B}, \mathbf{X_A})$ is the rate from the source emulation phase.

To calculate the first contribution, we note that $\mathbf{H_1}$ is the only part of $\mathbf{H}$ for which both Alice and Bob have estimates. Using (2) and (3), we get

$$\begin{aligned}
I(\hat{\mathbf{H}}_\mathbf{A}; \hat{\mathbf{H}}_\mathbf{B}) &= M_A M_B I(Y_{A,i}(j); Y_{B,i}(j))\\
&= M_A M_B \log\left(1 + \frac{P^2}{2P+1}\right). \qquad (6)
\end{aligned}$$

We now bound the contribution $h(\mathbf{Y_B} | \mathbf{H}, \mathbf{G_A} \mathbf{Y_E}) - h(\mathbf{Y_B} | \hat{\mathbf{H}}_\mathbf{A}, \hat{\mathbf{H}}_\mathbf{B}, \mathbf{X_A})$ from the source emulation phase from below using the following Lemma from [12]:

Lemma III.2. *Let $\mathbf{U}$ and $\mathbf{V}$ be two jointly distributed complex random vectors of dimensions $m_\mathbf{U}$ and $m_\mathbf{V}$, respectively. Let $\mathbf{K_U}$, $\mathbf{K_V}$, and $\mathbf{K_{UV}}$ be the covariance of $\mathbf{U}$, covariance of $\mathbf{V}$ and cross-covariance of $\mathbf{U}$ and $\mathbf{V}$, respectively. If $\mathbf{K_V}$ is invertible, then*

$$h(\mathbf{U}|\mathbf{V}) \leq \log\det\left(\mathbf{K_U} - \mathbf{K_{UV}} \mathbf{K_V}^{-1} \mathbf{K_{VU}}\right) + m_\mathbf{U} \log(\pi e),$$

with equality if $[\mathbf{U}^T \ \mathbf{V}^T]^T$ is a circularly symmetric complex Gaussian random vector.

We first create a new MMSE estimate $\hat{\mathbf{H}}$ of $\mathbf{H}$ using both $\hat{\mathbf{H}}_\mathbf{A}$ and $\hat{\mathbf{H}}_\mathbf{B}$. Note that since only the first M_A entries of $\mathbf{X_A}$ are nonzero, we only need an estimate of $\left[\mathbf{H_1}^T \ \mathbf{H_3}^T\right]^T$. If Bob assumes that $\hat{\mathbf{H}}$ is the true value of $\mathbf{H}$, his received signal is

$$\mathbf{Y_B}(t) = \hat{\mathbf{H}} \mathbf{X_A}(t) + \mathcal{E} \mathbf{X_A}(t) + \mathbf{V_B}(t),$$

where $\mathcal{E} = \left[\mathcal{E}_\mathbf{1}^T \ \mathcal{E}_\mathbf{3}^T\right]^T = \left[\mathbf{H_1}^T - \hat{\mathbf{H}}_\mathbf{1}^T \ \mathbf{H_3}^T - \hat{\mathbf{H}}_\mathbf{3}^T\right]^T$.

The estimate of $\mathbf{H_1}$ is based on $\hat{\mathbf{H}}_\mathbf{A}$ and $\hat{\mathbf{H}}_\mathbf{B}$ and the entries have MSE $1/(2P+1)$, while the estimate of $\mathbf{H_3}$ is based only on $\hat{\mathbf{H}}_\mathbf{B}$ and the entries have MSE $1/(P+1)$. Thus the covariance of $\mathcal{E} \mathbf{X_A}(t) + \mathbf{V_B}(t)$ is

$$\begin{bmatrix} \tilde{\sigma}^2_{A,B} \mathbf{I}_{M_B} & 0 \\ 0 & \tilde{\sigma}^2_B \mathbf{I}_{n_B - M_B} \end{bmatrix},$$

where

$$\tilde{\sigma}^2_{A,B} = \frac{P}{M_A(2P+1)} + 1, \qquad (7)$$

$$\tilde{\sigma}^2_B = \frac{P}{M_A(P+1)} + 1. \qquad (8)$$

We now bound $h(\mathbf{Y_B} | \hat{\mathbf{H}}_\mathbf{A}, \hat{\mathbf{H}}_\mathbf{B}, \mathbf{X_A})$ from above as follows:

$$\begin{aligned}
&h(\mathbf{Y_B} | \hat{\mathbf{H}}_\mathbf{A}, \hat{\mathbf{H}}_\mathbf{B}, \mathbf{X_A}) \leq\\
&\mathbb{E}_{\hat{\mathbf{H}}}\left[\log\det(K_{\mathbf{Y}|\hat{\mathbf{H}}} - K_{\mathbf{YX}|\hat{\mathbf{H}}} K^{-1}_{\mathbf{X}|\hat{\mathbf{H}}} K_{\mathbf{XY}|\hat{\mathbf{H}}})\right] +\\
&n_B \log(\pi e)\\
&\ = \log\det K_{\mathcal{E}\mathbf{X_A}(t) + \mathbf{V_B}(t)} + n_B \log(\pi e)\\
&\ = M_B \log(\pi e \tilde{\sigma}^2_{A,B}) + (n_B - M_B) \log(\pi e \tilde{\sigma}^2_B) \qquad (9)
\end{aligned}$$

where we have used Lemma III.2 in the first inequality.

$h(\mathbf{Y_B} | \mathbf{H}, \mathbf{G_A} \mathbf{Y_E})$ is given by [12] as

$$\begin{aligned}
&\mathbb{E}\left[\log \frac{\det\left(\mathbf{I}_{M_A} + P/M_A \mathbf{G_A}^\dagger \mathbf{G_A} + P/M_A \mathbf{H}^\dagger \mathbf{H}\right)}{\det\left(\mathbf{I}_{M_A} + P/M_A \mathbf{G_A}^\dagger \mathbf{G_A}\right)}\right]\\
&+ n_B \log(\pi e). \qquad (10)
\end{aligned}$$

Combining (5) - (10) gives the desired result. ■

A. High SNR Regime

In [12] the secret-key capacity $C_K(P)$ for the fast fading coherent MIMO wiretap channel with M_A transmit antennas was calculated and found to be

$$\mathbb{E}\left[\log \frac{\det\left(\mathbf{I}_{M_A} + P/M_A \mathbf{G_A}^\dagger \mathbf{G_A} + P/M_A \mathbf{H}^\dagger \mathbf{H}\right)}{\det\left(\mathbf{I}_{n_A} + P/M_A \mathbf{G_A}^\dagger \mathbf{G_A}\right)}\right].$$

Note that R_{SE} differs from $C_K(P)$ only by the negative terms $M_B \log(\tilde{\sigma}^2_{A,B}) + (n_B - M_B) \log(\tilde{\sigma}^2_B)$, due to not knowing the channel perfectly at Bob. From (7) and (8), we see that these terms scale with P as $\Theta(1)$. Further, from [12, Corollary 1], if $M_A > n_E$, we have that $\lim_{P\to\infty} C_K(P)/C_\infty(P) = 1$, where $C_\infty(P)$ is defined as

$$\begin{aligned}
&\mathbb{E}\Big[\log\det(\mathbf{I}_{n_B} +\\
&\frac{P}{M_A} \mathbf{H}\left[\mathbf{I}_{M_A} - \mathbf{G_A}^\dagger (\mathbf{G_A} \mathbf{G_A}^\dagger)^{-1} \mathbf{G_A}\right] \mathbf{H}^\dagger)\Big],
\end{aligned}$$

and if $M_A \leq n_E$, $C_K(P)$ scales with P as $\Theta(1)$. As in [12], we can interpret $\mathbf{I}_{M_A} - \mathbf{G_A}^\dagger (\mathbf{G_A} \mathbf{G_A}^\dagger)^{-1} \mathbf{G_A}$ as a projection matrix onto the null space of $\mathbf{G_A}$. Thus, at high SNR, the number of secure degrees of freedom per channel use (s.d.o.f.) from the third phase is given by $\min(M_A - n_E, n_B)(T - M_A - M_B)/T$. Further, from (6) we see that the number of s.d.o.f. per channel use from the first two phases is given by $M_A M_B/T$. Combining these results we get:

Theorem III.3. *The number of s.d.o.f. per channel use at high SNR is given by*

$$\frac{[\min(M_A - n_E, n_B)]^+ (T - M_A - M_B) + M_A M_B}{T}. \qquad (11)$$

Proof: See above. ■

We can use Theorem III.3 to find the optimal M_A and M_B.

Corollary III.4. *The optimal number of time slots $M_A^\star$ and $M_B^\star$ to use for training in the high SNR regime is given by*

$$M_A^\star = \min(n_A, \max(T/2, T - n_B)),$$
$$M_B^\star = \min(T - M_A^\star, n_B).$$

Proof: See Appendix. ■

Remark 1. *We note two facts from Corollary III.4. First, $M_A^\star$ and $M_B^\star$ do not depend on n_E, and second, it is either optimal to train all antennas (if $n_A + n_B < T$), or to only use training and no source emulation (if $n_A + n_B \geq T$). In the latter case the number of s.d.o.f. does not depend on n_E.*

We can also use Corollary III.4 to find the optimal number of antennas n_A and n_B for a given coherence time T.

Corollary III.5. *Increasing the number of transmit and receive antennas over*

$$n_A^\star = n_B^\star = T/2$$

does not increase the degrees of freedom.

Proof: For given T and n_B the optimal choice of n_A is $n_A^\star = \max(T/2, T - n_B)$. Thus the optimal choice of n_B is

$$M_B^\star = \min(n_B, T - max(T/2, T - n_B)) = \min(T/2, n_B).$$

Thus $n_B^\star = T/2$, which gives $n_A^\star = T/2$. ■

With this choice of n_A and n_B there is only training, and we can guarantee a secret key rate of

$$R_- = \frac{T}{4} \log\left(1 + \frac{P^2}{2P+1}\right),$$

regardless of the number of antennas n_E at Eve.

IV. Key Agreement without a public channel

The presence of a public channel with unlimited rate is unrealistic. Therefore we consider a scenario in which some coherence blocks are used for public discussion between Alice and Bob over the wireless channel. In the high SNR regime this does not give a loss of s.d.o.f. We have the following result:

Theorem IV.1. *At high SNR it is possible to achieve*

$$\frac{[\min(M_A - n_E, n_B)]^+ (T - M_A - M_B) + M_A M_B}{T}$$

s.d.o.f. per channel use without using a public channel, if M_A and M_B are chosen as in Corollary III.4.

Proof: Let $\mathbf{Y_{AT}}$ and $\mathbf{Y_{BT}}$ denote Alice's and Bob's observations in the training phase. As before, we quantize Bob's observation $(\mathbf{Y_B}, \mathbf{Y_{BT}})$ into a codebook generated by the auxiliary random variables $(\mathbf{U_Y}, \mathbf{U_H})$. From [17], the rate needed for public discussion and the achievable secret-key rate are given by

$$R_p = I(\mathbf{Y_B}, \mathbf{Y_{BT}}; \mathbf{U_Y}, \mathbf{U_H}) - I(\mathbf{X_A}, \mathbf{Y_{AT}}; \mathbf{U_Y}, \mathbf{U_H}),$$

and

$$R_-^{np} = I(\mathbf{X_A}, \mathbf{Y_{AT}}; \mathbf{U_Y}, \mathbf{U_H} | \mathbf{Y_E}, \mathbf{G_A}), \tag{12}$$

respectively. As in [13], we let $\mathbf{U_Y} = \mathbf{Y_B} + \mathbf{W_Y}$ and $\mathbf{U_H} = \mathbf{Y_B} + \mathbf{W_H}$, where $\mathbf{W_Y} \sim \mathcal{CN}(0, \sigma_Y^2 \mathbf{I}_{M_B})$ and $\mathbf{W_H} \sim \mathcal{CN}(0, \sigma_H^2 \mathbf{I}_{M_B})$ are i.i.d. and independent of all other random variables. Note that with the optimal choice of M_A and M_B above, either $M_B = n_B$, or all time slots are used for training. In the latter case the measurements at the last $n_B - M_B$ antennas at Bob cannot be used for key agreement, so only the first M_B measurements are used. We first analyze the rate needed for public discussion. We have

$$\begin{aligned} R_p =& I(\mathbf{Y_B}, \mathbf{Y_{BT}}; \mathbf{U_Y}, \mathbf{U_H}) - I(\mathbf{X_A}, \mathbf{Y_{AT}}; \mathbf{U_Y}, \mathbf{U_H}) \\ =& I(\mathbf{Y_B}, \mathbf{Y_{BT}}; \mathbf{U_H}) + I(\mathbf{Y_B}, \mathbf{Y_{BT}}; \mathbf{U_Y} | \mathbf{U_H}) + \\ & - I(\mathbf{X_A}, \mathbf{Y_{AT}}; \mathbf{U_H}) - I(\mathbf{X_A}, \mathbf{Y_{AT}}; \mathbf{U_Y} | \mathbf{U_H}) \\ =& I(\mathbf{Y_{BT}}; \mathbf{U_H}) - I(\mathbf{Y_{AT}}; \mathbf{U_H}) + \\ & h(\mathbf{U_Y} | \mathbf{Y_{AT}}, \mathbf{U_H}, \mathbf{X_A}) - h(\mathbf{U_Y} | \mathbf{Y_B}, \mathbf{Y_{AT}}, \mathbf{U_H}). \end{aligned}$$

The first term is given by $I(\mathbf{Y_{BT}}; \mathbf{U_H}) = M_A M_B \log(1 + \frac{P+1}{\sigma_H^2})$. For the second term we have

$$I(\mathbf{Y_{AT}}; \mathbf{U_H}) = M_A M_B \log\left(\frac{(P+1)(P+1+\sigma_H^2)}{2P+1+\sigma_H^2(P+1)}\right)$$

The third term can be bounded using the MMSE estimate of $\mathbf{H_1}$ calculated from $(\mathbf{Y_{AT}}, \mathbf{U_H})$ and Lemma III.2:

$$h(\mathbf{U_Y} | \mathbf{Y_{AT}}, \mathbf{U_H}, \mathbf{X_A}) \leq M_B \log(\pi e \tilde{\sigma}_{A,U_H}^2)$$

where $\tilde{\sigma}_{A,U_H}^2 = \frac{P(1+\sigma_H^2)}{M_A(2P+1+\sigma_H^2(P+1))} + 1 + \sigma_Y^2$. Finally, the last term is $h(\mathbf{U_Y} | \mathbf{Y_B}, \mathbf{Y_{AT}}, \mathbf{U_H}) = h(\mathbf{U_Y} | \mathbf{Y_B}) = M_B \log(\pi e \sigma_Y^2)$. In total we get

$$R_p = M_A M_B \log\left(1 + \frac{2P+1}{\sigma_H^2(P+1)}\right) + M_B \log\left(\frac{\tilde{\sigma}_{A,U_H}^2}{\sigma_Y^2}\right).$$

We see that, for fixed σ_Y^2 and σ_H^2, R_p scales as $\Theta(1)$ with P. Now let a fraction α of the coherence blocks at the end of the transmission be dedicated to public discussion. This lowers the achievable secret-key rate to $(1-\alpha)R_-^{np}$. When used for communication, the capacity $C(P)$ of the channel between Bob and Alice scales with P as $\min(T/2, n_A, n_B) \log P$ [16]. Since R_p scales as $\Theta(1)$ with P, it is possible to have $\alpha C(P) > R_p$, for any $\alpha > 0$, provided that P is large enough. Thus we can achieve any secret-key rate below R_-^{np}, provided that P is large enough.

It remains to show that the quantized observations give the same number of s.d.o.f. as in the case with a public channel. We expand R_-^{np} in the same way as in (5) and get

$$\begin{aligned} R_-^{np} =& I(\mathbf{Y_{AT}}; \mathbf{U_H}) - h(\mathbf{U_Y} | \mathbf{Y_{AT}}, \mathbf{U_H}, \mathbf{X_A}) + \\ & h(\mathbf{U_Y} | \mathbf{H}, \mathbf{G_A}, \mathbf{Y_E}). \end{aligned}$$

For fixed σ_Y^2 and σ_H^2 the first term gives $M_A M_B$ s.d.o.f. Using Lemma III.2, the second term scales as $\Theta(1)$ with P, and the last term gives $(T - M_A - M_B)\,[\min(M_A - n_E, M_B)]^+$ s.d.o.f. The optimal choice of M_A and M_B implies that $T - M_A - M_B$ is positive only when $M_B = n_B$, so the result follows. ■

V. Conclusions

We have considered secret-key agreement over a noncoherent block-fading MIMO wiretap channel. Utilizing channel reciprocity we have developed a three-phase scheme based on training and source emulation. By analyzing the number of s.d.o.f. in the high SNR regime, we have characterized the optimal number of antennas to use for training. We have found that when the sum of the number of antennas at Alice and Bob is larger than the coherence time of the channel, the number of s.d.o.f. does not depend on the number of antennas at Eve, since Alice and Bob can use the channel gains as common randomness which Eve has no access to. We have also considered secret-key agreement in the absence of a public channel and have found that, in the high SNR regime, the number of s.d.o.f. remain the same as in the case with a public channel.

References

[1] C. Shannon, "Communication theory of secrecy systems," *Bell system technical journal*, vol. 28, no. 4, pp. 656–715, 1949.

[2] A. D. Wyner, "The wire-tap channel," *Bell. Syst. Tech. J.*, vol. 54, no. 8, pp. 1355–1387, Oct. 1975.

[3] I. Csiszár and J. Körner, "Broadcast channels with confidential messages," *IEEE Transactions on Information Theory*, vol. 24, no. 3, pp. 339 – 348, May 1978.

[4] Y. Liang, H. V. Poor, and S. Shamai (Shitz), "Information theoretic security," *Foundations and Trends in Communications and Information Theory*, vol. 5, no. 4-5, pp. 355–580, 2009.

[5] R. Ahlswede and I. Csiszar, "Common randomness in information theory and cryptography. I. secret sharing," *IEEE Transactions on Information Theory*, vol. 39, no. 4, pp. 1121 –1132, Jul. 1993.

[6] U. Maurer, "Secret key agreement by public discussion from common information," *IEEE Transactions on Information Theory*, vol. 39, no. 3, pp. 733–742, May 1993.

[7] R. Wilson, D. Tse, and R. Scholtz, "Channel identification: Secret sharing using reciprocity in ultrawideband channels," *IEEE Transactions on Information Forensics and Security*, vol. 2, no. 3, pp. 364–375, Sep. 2007.

[8] S. Draper, A. Sayeed, and T. Chou, "Minimum energy per bit for secret key acquisition over multipath wireless channels," in *Information Theory Proceedings (ISIT), 2009 IEEE International Symposium on*. IEEE, 2009, pp. 2296–2300.

[9] T. Chou, S. Draper, and A. Sayeed, "Impact of channel sparsity and correlated eavesdropping on secret key generation from multipath channel randomness," in *Information Theory Proceedings (ISIT), 2010 IEEE International Symposium on*. IEEE, 2010, pp. 2518–2522.

[10] A. Sayeed and A. Perrig, "Secure wireless communications: Secret keys through multipath," in *Acoustics, Speech and Signal Processing, 2008. ICASSP. IEEE International Conference on*. IEEE, 2008, pp. 3013–3016.

[11] C. Ye, S. Mathur, A. Reznik, Y. Shah, W. Trappe, and N. Mandayam, "Information-theoretically secret key generation for fading wireless channels," *IEEE Transactions on Information Forensics and Security*, vol. 5, no. 2, pp. 240 –254, Jun. 2010.

[12] T. F. Wong, M. Bloch, and J. M. Shea, "Secret sharing over fast-fading MIMO wiretap channels," *EURASIP J. Wireless Comm. and Networking*, vol. 2009, Dec. 2009.

[13] L. Lai, Y. Liang, and H. V. Poor, "A unified framework for key agreement over wireless fading channels," *IEEE Transactions on Information Forensics and Security. To appear.*

[14] L. Lai, Y. Liang, and W. Du, "Cooperative key generation in wireless networks," *IEEE Journal on Selected Areas in Communications, Special Issue on Theories and Methods for Advanced Wireless Relays. In revision.*

[15] A. Agrawal, Z. Rezki, A. Khisti, and M. Alouini, "Noncoherent capacity of secret-key agreement with public discussion," *IEEE Transactions on Information Forensics and Security*, vol. 6, no. 3, pp. 565–574, Sep. 2011.

[16] L. Zheng and D. Tse, "Communication on the Grassmann manifold: a geometric approach to the noncoherent multiple-antenna channel," *IEEE Transactions on Information Theory*, vol. 48, no. 2, pp. 359 –383, Feb. 2002.

[17] I. Csiszár and P. Narayan, "Common randomness and secret key generation with a helper," *IEEE Transactions on Information Theory*, vol. 46, no. 2, pp. 344–366, Mar. 2000.

Appendix
Proof of Cor. III.4

Proof: Let

$$\begin{aligned} F =& \left[\min(M_A - n_E, n_B)\right]^+ (T - M_A - M_B) + M_A M_B \\ =& M_B(M_A - \left[\min(M_A - n_E, n_B)\right]^+) + \\ & \left[\min(M_A - n_E, n_B)\right]^+ (T - M_A). \end{aligned} \tag{13}$$

Since $(M_A - [\min(M_A - n_E, n_B)]^+) \geq 0$, F is maximized by maximizing M_B:

$$M_B^\star = \min(n_B, T - M_A). \tag{14}$$

By inserting (14) into (13) we get

$$\begin{aligned} F =& \min(n_B, T - M_A)(M_A - \left[\min(M_A - n_E, n_B)\right]^+) \\ & + \left[\min(M_A - n_E, n_B)\right]^+ (T - M_A). \end{aligned}$$

We get three cases, depending on T. First, if $T \leq n_E + n_B$,

$$F = \begin{cases} M_A n_B & \text{if } M_A \leq T - n_B \\ M_A(T - M_A) & \text{if } M_A > T - n_B. \end{cases}$$

If $T/2 < n_B$, the maximum of F occurs at $M_A = T/2$, and otherwise it occurs at $M_A = T - n_B$.

In the second case, if $n_E + n_B \leq T \leq n_E + 2n_B$, we have

$$F = \begin{cases} M_A n_B & M_A \leq n_E \\ M_A(T + n_E - M_A) + & \\ n_E(n_B - T) & n_E < M_A \leq T - n_B \\ M_A(T - M_A) & M_A > T - n_B. \end{cases}$$

As in the first case, if $T/2 < n_B$, the maximum occurs at $M_A = T/2$, and otherwise it occurs at $M_A = T - n_B$.

Finally, if $T > n_E + 2n_B$, we have

$$F = \begin{cases} M_A n_B & M_A \leq n_E, \\ M_A(T + n_E - M_A) + & \\ n_E(n_B - T) & n_E < M_A \leq n_B + n_E, \\ n_B(T - n_B) & n_B + n_E < M_A \leq T - n_B, \\ M_A(T - M_A) & M_A > T - n_B. \end{cases}$$

As before, if $T/2 < n_B$, the maximum occurs at $M_A = T/2$. If $T \geq 2n_B$, there are several maxima, for $n_B + n_E \leq M_A \leq T - n_B$.

In all three cases above, at least one maximum occurs at $M_A = \max(T/2, T - n_B)$, and, since F is non-decreasing for $M_A < \max(T/2, T - n_B)$, we get

$$M_A^\star = \min(n_A, \max(T/2, T - n_B)).$$

■