On the Secrecy Capacity of the Space-Division Multiplexed Fiber Optical Communication Systems

Kyle Guan, Peter J. Winzer, Emina Soljanin, and Antonia M. Tulino
Bell Labs, Alcatel-Lucent, Holmdel, NJ, USA

***Abstract*—Recent developments in the field of space-division multiplexing (SDM) for fiber-optic communication systems suggest that the spatial diversity offered by SDM can be used not only to increase system capacity, but also to achieve provable security against physical layer attacks. We examine the information-theoretic security of SDM with a focus on frequency-selective and rapidly-varying frequency-flat channels. We analytically evaluate the outage-free secrecy capacity – the maximal data rate that guarantees perfect security within a class of channel realizations. Using analysis and simulations, we evaluate the impact of key system parameters on the secrecy capacity of SDM systems. Our results show that, with a proper code design that balances the trade-off between data rate and confidentiality, we can take full advantage of SDM to offer a secure information rate that could be orders of magnitude higher than what can be achieved through quantum key distribution (QKD).**

I. Introduction

Fiber-optic communication systems are vulnerable to various types of physical-layer attacks [1]-[3]. A common form of attack is fiber tapping, where an attacker with physical access to the fiber can retrieve a portion of the propagating signals by bending the fiber and detecting the evanescent field at the bend. The fact that eavesdropping is relatively easy to implement and could remain unnoticed is a major concern for physical-layer security. Quantum key distribution (QKD) addresses these issues by allowing the exchange of a secure key between a transmitter and a receiver while at the same time providing for intrusion detection [4]. However, the benefits of QKD are offset by the stringent limitations in terms of data rate and reach (e.g., 1 Mb/s over 50 km of fiber [5]) as well as by severe problems arising from optical amplifier noise and from interactions between classical communications and QKD signals on a common optical networking infrastructure [6].

Recently, space-division multiplexing (SDM) has been shown as a viable solution to overcome the coming capacity crunch in optical networks [7]-[9]. Using parallel strands of a single-mode fiber, uncoupled or coupled cores of a multi-core fiber, or even individual modes of a few-mode fiber in combination with *multiple-input-multiple-output* (MIMO) digital signal processing, SDM can drastically increase system capacity and at the same time reduce cost and energy per bit via the integration of components. Independent of its network capacity scaling benefits, SDM also shows the potential of providing provable physical-layer security at data rates orders of magnitude higher than what can be achieved through QKD [10], [11].

Building upon the initial results reported in [10], [11], we study the MIMO-SDM fiber tapping problem further in this paper. In addition to substantiating the previous results with more rigorous interpretations and new insights, we make the following new contributions:

- In addition to the slowly-varying and frequency-flat channels studied in [10], [11], we analyze the rapidly-varying frequency-flat and the frequency-selective channels. In particular, we provide an information-theoretic problem formulation of secure communication over these types of channels and evaluate the associated secrecy capacities.
- We study the *outage-free secrecy capacity*, which guarantees perfect security within a class of channel realizations. We provide an analytical characterization of the outage-free secrecy capacity and evaluate its scalability with the number of modes for SDM systems.
- We assess the impact of system parameters on the secrecy capacity. We find that as a result of the trade-off between the eavesdropper's mode-dependentl loss (MDL) and signal-to-noise ratio (SNR), information-theoretic security can still be achieved when the eavesdropper's channel has a better average signal-to-noise ratio (SNR) than that of the legitimate receiver.

A. Related Work

The fundamental results from the vast body of research [12]-[20] in information theoretic security provide the theoretical foundations for this work. The concepts of equivocation and secrecy capacity were first introduced by Wyner [12]. In [13], Leung-Yan-Cheong and Hellman studied the single-input-single-output (SISO) Gaussian channel and showed that the secrecy capacity equals to the difference between the capacities of main and eavesdropping channel. This result implies that the capacity of the main channel needs to be larger than that of the eavesdropping channel; otherwise fundamental secure communication is impossible. Also, we note that the secrecy capacity, like the Shannon limit, provides an information theoretic limit without a prescription on the codes that may actually approach it. The secrecy capacity of SISO fading channels was characterized in [14]. The security issues of MIMO systems have been extensively studied recently for wireless and free space optical communication systems [15]-[20]. The security benefit of MIMO system was first studied in [15] in terms of low probability of interception. The results in [16]-[19] provide the theoretical framework for analyzing the secrecy capacity of a deterministic MIMO wire-tap channel. The use of spatial diversity to improve the confidentiality of

978-1-4799-0895-0/13/$31.00 ©2013 IEEE

atmospheric free space optical communication was studied in [20].

In comparison, we adopt a system model that reflects the unique physical characteristics of optical fiber MIMO-SDM channels [21]. We accordingly assume that each individual transmitter is per-mode power constrained and has no instantaneous channel state information (CSI) for the main and eavesdropping channel.

The remainder of this paper is organized as follows. In Section II, we provide an overview of fiber-optic MIMO-SDM systems. We then describe the system model for SDM waveguide tapping. In Section III, we characterize the secrecy capacity of SDM systems for different channel dynamics. The main results and their implications are finally discussed in Section IV. In Section V, we summarize our main findings.

II. SDM Waveguide and Fiber Tapping Model

A. Space-division Multiplexing

In its most trivial form, SDM systems can be deployed as parallel uncoupled optical line systems. However, this is not an economically sustainable path forward, since this approach does not reduce the cost or energy per bit compared to today's systems: M parallel systems carry M times the capacity at M times the cost or energy. Commercially successful SDM technologies will need to leverage *integration* and sharing of system components among channels. Since integration generally comes at the expense of *crosstalk* among parallel paths, proper crosstalk management will be an important aspect of SDM systems. In the low crosstalk regime, nominally uncoupled long-haul transmissions over 7-core fiber have been reported [22], [23]. In the high crosstalk regime, MIMO techniques, originally developed for wireless systems, can be used to mitigate the crosstalk. Recently, several impressive experimental demonstrations of coupled-mode MIMO-SDM transport have been reported, including MIMO-SDM transmission over microstructured [24] and few-mode [25] fiber. It is key for reliable MIMO-SDM that the transmitter and receiver are able to selectively address all M modes supported by the waveguide or fiber [21].

B. System Model

As shown in Fig. 1, we consider an SDM system that supports a set of M orthogonal propagation modes. These modes may be subject to coupling and differential gain or loss. In addition, we ignore inter- and intra-modal fiber nonlinearities and model the SDM system as a linear matrix MIMO channel. That is, we use $M \times M$ (normalized) matrices $\mathbf{H}$ and $\mathbf{H^e}$ to represent, the realizations of the legitimate (main) and eavesdropping channels, respectively. Assuming that noise generated within the receiver dominates, the received signals of the legitimate receiver $\mathbf{y}$ and the eavesdropper $\mathbf{y^e}$ are:

$$\mathbf{y} = \sqrt{E_0}\sqrt{L}\mathbf{H}\mathbf{x} + \mathbf{n}, \quad (1)$$

$$\mathbf{y^e} = \sqrt{E_0}\sqrt{L^e}\mathbf{H^e}\mathbf{x} + \mathbf{n^e}, \quad (2)$$

where L and L^e are normalization factors with $L = \mathrm{tr}\{\tilde{\mathbf{H}}\tilde{\mathbf{H}}^\dagger\}/M$ and $L^e = \mathrm{tr}\{\tilde{\mathbf{H}}^\mathbf{e}\tilde{\mathbf{H}}^{\mathbf{e}\dagger}\}/M$ that characterizes the mode-average loss of the respective channels $\tilde{\mathbf{H}}$ and $\tilde{\mathbf{H}}^\mathbf{e}$ [21]. The channel noise $\mathbf{n}$ and $\mathbf{n^e}$ is symmetric complex Gaussian with per-mode power spectral density N_0 and N_0^e for the legitimate and eavesdropping receiver, respectively.

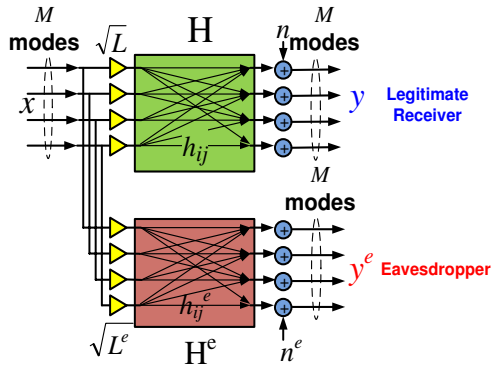

Fig. 1. A MIMO-SDM system that supports a set of M orthogonal propagation modes. The signals received by the legitimate receiver and the eavesdropper are denoted as $\mathbf{y}$ and $\mathbf{y^e}$, respectively.

In our model, we make the assumption that CSI is not available at the transmitter, motivated by the fact that the receiver-to-transmitter feedback delays in optical transport systems are much longer than the channel dynamics. However, with the use of the training symbols, the legitimate receiver can estimate the channel states of the MIMO-SDM system. We thus assume that the individual realization of $\mathbf{H}$ is known to the legitimate receiver. Similarly, the channel realization of $\mathbf{H^e}$ can be estimated by (and thus is known to) the eavesdropper, but unknown to the transmitter.

We consider a phenomenological channel model for the effects of fiber bending and tapping, motivated by the eavesdroppers desire of coupling as little light out of the SDM fiber as possible (to avoid being detected):. The legitimate channel remains essentially unperturbed (apart from a unitary transform) while the eavesdropper sees a mode-dependent loss (MDL) channel. Mathematically, we model $\mathbf{H}$ as a random unitary matrix, i.e., $\mathbf{H} = \mathbf{U}$, with $\mathbf{U}\mathbf{U}^\dagger = \mathbf{I}$. For $\mathbf{H}^e$, we provide two different models as follows.

- *Uniformly distributed MDL model*: the eavesdropper's channel is a concatenation of two operations – a rotation operation followed by a scaling operation. That is, $\mathbf{H}^e = \sqrt{\mathbf{V}}\mathbf{U}^\mathbf{e}$, where $\mathbf{U}^\mathbf{e}$ is a random unitary matrix and $\mathbf{V}$ is a diagonal matrix. We refer to $\mathbf{V}$ as the MDL matrix. The diagonal elements v_is, on a linear scale, satisfy $\sum_{i=1}^{M} v_i = M$ and are randomly drawn from a uniform distribution: $[\min\{v_i\}, \max\{v_i\}]$. The MDL, expressed in decibels, is defined as $\mathrm{MDL} = 10\log_{10}(\max\{v_i\}/\min\{v_i\})$.
- *Log-uniformly distributed MDL model*: similar to the uniformly distributed MDL model, we have $\mathbf{H}^e = \sqrt{\mathbf{V}}\mathbf{U}^\mathbf{e}$. But, instead of being picked from a linear uniform distribution, the diagonal elements of $\mathbf{V}$ are randomly drawn from a uniform logarithmic distribution $[\min\{10\log_{10}(v_i)\}, \max\{10\log_{10}(v_i)\}]$.

III. Secrecy Capacity of the MIMO-SDM Systems

An important performance metric that characterizes the security of communication systems is the *secrecy capacity*. The secrecy capacity quantifies the maximum amount of information that can be transmitted from a legitimate transmitter to a legitimate receiver such that an eavesdropper in principle cannot receive any useful information [12]. Mathematically, this means that the randomness of the source (also referred to as the equivocation), measured by the information entropy, is not reduced when the eavesdropper observes the outputs from the wiretap channel.

A. The Secrecy Capacity of Deterministic MIMO-SDM Systems

When the channel realizations $\mathbf{H}$ and $\mathbf{H}^e$ are known to the transmitter, the secrecy capacity C_s of an SDM channel can be derived using the well established formalisms [16]-[19], with a modification that reflects the physical characteristics of the MIMO-SDM channels:

$$\begin{aligned} C_s = &\max_{\mathbf{Q_x}} \log_2 \left[\det(\mathbf{I} + \mathrm{SNR}\mathbf{H}\mathbf{Q_x}\mathbf{H}^\dagger)\right] \\ &- \log_2 \left[\det(\mathbf{I} + \mathrm{SNR}^e\mathbf{H^e}\mathbf{Q_x}\mathbf{H}^{e\dagger})\right] \\ &\text{subject to } \; E[x_i^2] < P_0, \; i \in 1, ..., M, \end{aligned}$$

where det and $\mathbf{Q_x}$ are the determinant of the matrix and the covariance matrix of the transmitted signal x, respectively, and $\mathrm{SNR} = LE_0/N_0$ and $\mathrm{SNR}^e = L^eE_0/N_0^e$ are the mode-averaged signal-to-noise ratios of the legitimate and wiretap channels, respectively. In optical SDM systems, the power is constrained by fiber nonlinearity on a *per mode* basis. As such we set an upper bound for the power of each mode individually, as opposed to the total average power constraint that is normally used in studying wireless MIMO systems [21].

Solving the above optimization formulation involves finding the covariance matrix $\mathbf{Q_x}$ that achieves the capacity. Because of the channel models used in this work ($\mathbf{H} = \mathbf{U}$ and $\mathbf{H^e} = \mathbf{U^e}\sqrt{\mathbf{V^e}}$), we showed that we can reduce the solution space of $\mathbf{Q_x}$ by optimizing over only the diagonal covariance matrices $\mathbf{\Lambda^Q}$ [11], [26]. That is, all the statistical characteristics of $\mathbf{Q_x}$ are fully captured by $\mathbf{\Lambda^Q}$ as the result of the underlying channel models.

B. Secrecy Capacity with $\mathbf{\Lambda^Q} = \mathbf{I}$

When CSI is unavailable at the transmitter, it is reasonable to make the assumption that $\mathbf{\Lambda^Q} = \mathbf{I}$. That is, uncorrelated signals of equal power are sent on all the modes (In Section III. D and E and the appendix, we will provide justifications that this is indeed the optimal power allocation strategy under our assumption of an uninformed transmitter). As such, the expression for C_s can be simplified to:

$$C_s = \sum_{i=1}^{M} [\log_2(1 + \mathrm{SNR}\lambda_i) - \log_2(1 + \mathrm{SNR}^e\lambda_i^e)], \qquad (3)$$

where λ_i and λ_i^e are the non-zero eigenvalues of $\mathbf{HH}^\dagger$ and $\mathbf{H^eH}^{e\dagger}$, respectively. For uniformly and log-uniformly distributed models, the expression can be further simplified to:

$$C_s = \sum_{i=1}^{M} [\log_2(1 + \mathrm{SNR}) - \log_2(1 + \mathrm{SNR}^e v_i)]. \qquad (4)$$

We further normalize C_s by the capacity per mode of the legitimate channel C_0, which due to our unitary assumption of $\mathbf{H}$ is given by $C_0 = \log_2(1 + \mathrm{SNR})$, and arrive at

$$\frac{C_s}{C_0} = M - \frac{\sum_{i=1}^{M} \log_2(1 + \mathrm{SNR}^e v_{ii}^e)}{\log_2(1 + \mathrm{SNR})}. \qquad (5)$$

This is the maximum rate, in units of raw SDM channel capacity per mode, that can be transmitted in perfect information-theoretic secrecy over a particular MIMO-SDM channel instantiation. The secrecy capacity is determined by the values of SNR, SNR^e, and v_i. We also note that the minimal value of the secrecy capacity is zero, if the capacity of the eavesdropper's channel is larger than that of the legitimate receiver ($\sum_{i=1}^{M} \log_2(1 + \mathrm{SNR}^e v_i) > MC_0$).

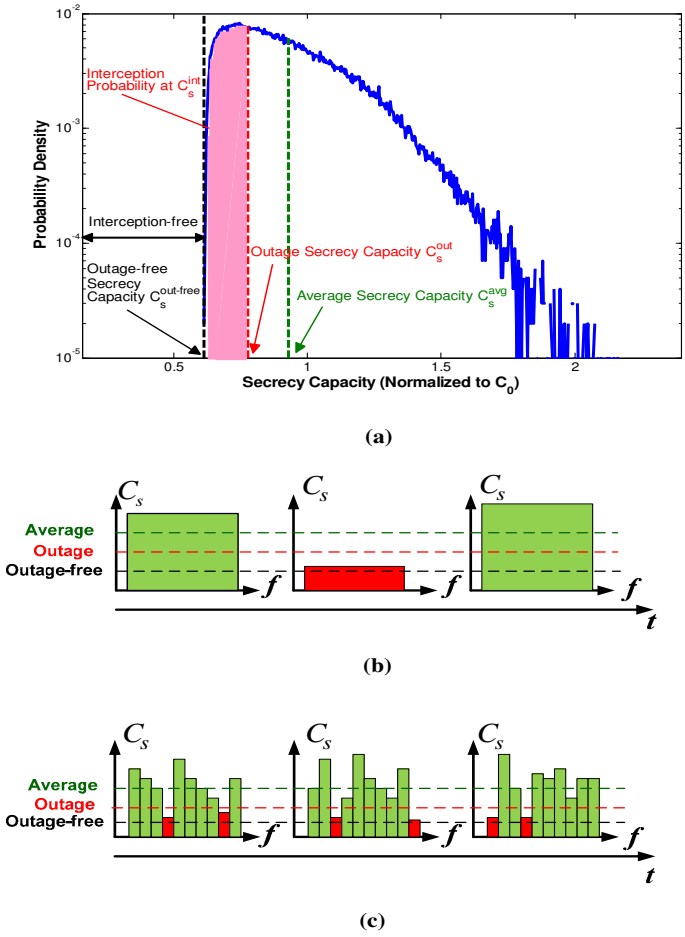

Fig. 2. (a) Histogram of the secrecy capacities (normalized to MC_0) generated from 10^5 random realizations; (b) the visualization of slowly-varying temporal capacity evolution over a frequency-flat channel; and (c) the visualization of a strongly frequency-selective channel. In (b) and (c), the green boxes indicate that the channel secrecy capacities are above the transmitted capacity; while the red boxes indicate that the secrecy capacities are below the transmitted capacity, where an outage would occur.

C. Outage-free Secrecy Capacity

Due to random mode coupling within the SDM fiber, we cannot predict which of the transmitting modes will be extracted stronger than others by the eavesdropper. As a result, the secrecy capacity of the MIMO-SDM channel will be inherently a random quantity. This is illustrated in Fig. 2(a), which shows the statistical distribution of the secrecy capacity C_s based on 10^5 random channel realizations for the case of $M = 8$ modes, SNR=SNR^e=20 dB, and MDL=20 dB. There is a sharp cutoff on the left side of the histogram. Transmission at a rate smaller than this cutoff capacity (indicated by the dashed black line in Fig. 2 (a)) will be perfectly secure regardless of the channel realizations. We refer to this capacity as *outage-free secrecy capacity* and denote it as $C_s^{out-free}$. For uniformly and log-uniformly distributed models, the outage-free secrecy capacity can be derived as follows.

We first consider the uniformly distributed model, where v_i is expressed in linear units. With an identical power allocation on all the modes ($\mathbf{P} = P_0\mathbf{I}$), the capacity of the eavesdropping channel is:

$$C_e = \sum_{i=1}^{M} \log_2(1 + \text{SNR}^e v_i). \tag{6}$$

Note that for given SNR^e and MDL, the capacity depends only on the values of v_i. As such, we can obtain the upper bound of C_e by maximizing over the choices of v_i:

$$\begin{aligned} \max_{v_i}: \quad & \sum_{i=1}^{M} \log_2(1 + \text{SNR}^e v_i) \\ \text{s.t.}: \quad & \sum_{i=1}^{M} v_i = M, \\ & v_2 = \text{MDL} v_1, \\ & v_1 \le v_i \le v_2, \quad i = 3, 4, ..., M. \end{aligned} \tag{7}$$

Without the loss of generality, we let $v_1 = \min\{v_i\}$ and $v_2 = \max\{v_i\}$. Since the objective function is concave and the constraints are linear and bounded, a unique maximum exists [27]. Let $C_e^{\max}$ be the maximal capacity achieved by the eavesdropper. We then have the outage-free secrecy capacity as:

$$\frac{C_s^{out-free}}{C_0} = M - \frac{C_e^{\max}}{C_0}. \tag{8}$$

For very high SNR^{e}s (40 dB and above) and moderate MDL (5-20 dB), we can approximate the optimal v_i and $C_s^{out-free}$ to much simpler forms (the details of the derivation are provided in the appendix):

$$\begin{aligned} v_1 &\approx \frac{2}{1+\text{MDL}} \\ v_2 &\approx 2\frac{\text{MDL}}{1+\text{MDL}} \\ v_i &\approx 1, \quad i = 3, 4, ..., M, \end{aligned} \tag{9}$$

and

$$\begin{aligned} C_s^{out-free} &\approx 2C_0 - \log_2(1 + \frac{2}{1+\text{MDL}}\text{SNR}^e) \\ &- \log_2(1 + \frac{2\text{MDL}}{1+\text{MDL}}\text{SNR}^e) \\ &+ (M-2)\log_2\frac{\text{SNR}}{\text{SNR}^e}. \end{aligned} \tag{10}$$

The above equation indicates that MDL, SNR, SNR^e, and the SNR-to-SNR^e ratio all contribute to the outage-free secrecy capacity. However, only the contribution from the SNR-to-SNR^e ratio scales with the M, as shown by the last term of Eq. (10). If the main and the eavesdropping channels have the same SNR, $C_s^{out-free}$ can be further simplified to:

$$\begin{aligned} C_s^{out-free} &\approx 2C_0 - \log_2(1 + \frac{2}{1+\text{MDL}}\text{SNR}) \\ &- \log_2(1 + \frac{2\text{MDL}}{1+\text{MDL}}\text{SNR}). \end{aligned} \tag{11}$$

In this case, the outage-free secrecy capacity is independent of the number of modes M, thus does not change as M increases.

For the log-uniformly distributed model, we can obtain an upper bound of C_e by solving a similar optimization problem:

$$\begin{aligned} \max_{\tilde{v}_i}: \quad & \sum_{i=1}^{M} \log_2(1 + \text{SNR}^e 10^{\frac{\tilde{v}_i}{10}}) \\ \text{s.t.}: \quad & \sum_{i=1}^{M} 10^{\frac{\tilde{v}_i}{10}} = M, \\ & \tilde{v}_2 - \tilde{v}_1 = \text{MDL}_{dB}, \\ & \tilde{v}_1 \le \tilde{v}_i \le \tilde{v}_2, \quad i = 3, 4, ..., M. \end{aligned} \tag{12}$$

Note that both $\tilde{v}_i$ and MDL$_{dB}$ are in the unit of decibels. It can be easily shown that, with the change of variables of $v_i = 10^{\tilde{v}_i/10}$ and MDL $= 10^{\text{MDL}_{dB}/10}$, the above optimization problem is equivalent to the optimization problem of Eq. (7). As such, the outage-free capacity derived for the uniformly distributed model also applies to the log-uniformly distributed model.

As shown in Eq. (11), designing the entire system based on the worst-case scenario could yield very poor scalability for the secrecy capacity. Depending on the nature of the channels, we take the following alternative approaches.

D. Outage Secrecy Capacity

For slowly-varying frequency-flat channels (Fig. 2(b)), the channel characteristics are constant across the signal bandwidth and change very slowly in time. In this case, a transmission rate smaller than the outage-free secrecy capacity (as represented by the dashed black line) will guarantee perfect secrecy independent of the channel instantiations. If the transmitter chooses to communicate at a rate R (vertical and horizontal red dashed lines in Fig. 2 (a) and (b), respectively) that is higher than the outage-free secrecy capacity, there is a finite probability (as shown by the shaded area in Fig. 2(a)) that the eavesdropper can, at least in principle, learn something

about the secret information. We refer to this probability as the *probability of interception* $p_{int}(R)$, which can be expressed as:

$$\begin{aligned} p_{int}(R) = &\min_{\mathbf{\Lambda^Q}} Pr[\log_2\left(\det(\mathbf{I}+\text{SNR}\mathbf{H}\mathbf{\Lambda^Q}\mathbf{H}^\dagger)\right) \\ &- \log_2\left[\det(\mathbf{I}+\text{SNR}^e\mathbf{H^e}\mathbf{\Lambda^Q}\mathbf{H}^{e\dagger}) < R\right] \\ &\text{subject to } \; E[x_i^2] < P_0, \end{aligned}$$

where the minimization is over all diagonal covariance matrices $\mathbf{\Lambda^Q}$. In [11] we showed that with the per-mode power constraint, $\mathbf{\Lambda^Q} = \mathbf{I}$ is optimal in the sense that it has the least interception probability among all the power allocation schemes. We refer to the associated maximal secrecy rate such that the interception probability is less than ϵ as the *outage secrecy capacity* at ϵ [14]. That is,

$$p_{int}(C_s^{out}(\epsilon)) = \epsilon. \tag{13}$$

The operational meaning of the outage secrecy capacity lies in the the trade-off between secrecy rate and interception probability: a higher secrecy rate can be achieved at the expense of a higher interception probability.

E. Average Secrecy Capacity

For rapidly-varying frequency-flat channels, the channel characteristics are constant across the signal bandwidth, but change rapidly over time. We can average many channel realizations by coding over long time intervals and a secrecy rate of $C_s^{avg} = \langle C_s \rangle$ can indeed be achieved. We refer to this capacity as *average secrecy capacity*. For frequency-selective channel, the channel characteristics vary rapidly across the signal's bandwidth, as shown in Fig. 2(c). If each signal frequency component experiences a different channel instantiation, the system ultimately sees the average capacity (as shown by the vertical and horizontal green dashed lines in Fig. 2(a) and (c), respectively). In the idealized limiting case of a highly frequency-selective channel, the average secrecy capacity can be guaranteed. That is, if the transmitter codes for C_s^{avg}, the legitimate receiver can extract the information at rate C_s^{avg} without being intercepted. Formally, C_s^{avg} can be expressed as:

$$\begin{aligned} C_s^{avg} = &\max_{\mathbf{\Lambda^Q}} \mathbb{E}[\log_2\left(\det(\mathbf{I}+\text{SNR}\mathbf{H}\mathbf{\Lambda^Q}\mathbf{H}^\dagger)\right) \\ &- \log_2(\det(\mathbf{I}+\text{SNR}^e\mathbf{H^e}\mathbf{\Lambda^Q}\mathbf{H}^{e\dagger}))] \\ &\text{subject to } \; E[x_i^2] < P_0. \end{aligned}$$

We show in the appendix that $\mathbf{\Lambda^Q} = \mathbf{I}$ is also an optimal average secrecy capacity-achieving covariance matrix, by using the fundamental relationship between the mutual information and the minimum mean-square error (MMSE) in Gaussian channels [28], and the properties of Schur concavity [29].

IV. Results and Discussion

Section III shows that the secrecy capacities depend on the distribution of MDL matrices, the number of modes, as well as the SNRs of the main and eavesdropping channels. In this section, we evaluate the impact of each of these system parameters on the secrecy capacity of SDM systems.

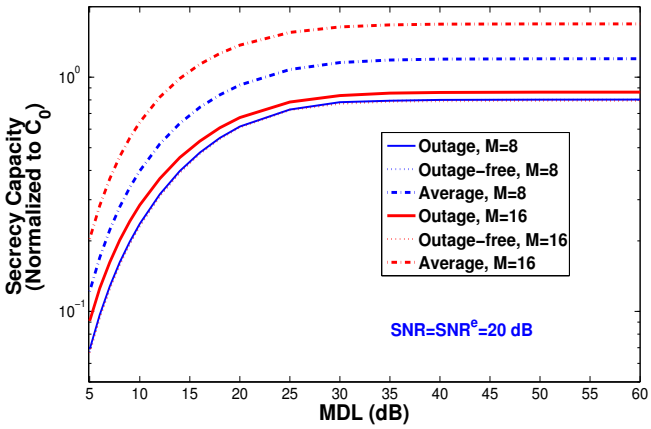

Fig. 3. Secrecy capacity vs. average MDL experienced by the eavesdropper.

To evaluate outage or average secrecy capacity for a given set of parameters M, MDL SNR and SNR^e, we first run a simulation that generates 10^5 random channel realizations of $\mathbf{H} = \mathbf{U}$ and $\mathbf{H^e} = \mathbf{U^e}\sqrt{\mathbf{V^e}}$, respectively. For each channel realization, we calculate the corresponding C_s using Eq. (3) or Eq. (4). With 10^5 instantiations of C_s, we then obtain outage or average secrecy capacity numerically. To evaluate outage-free secrecy capacity, we solve the optimization problems of Eq. (7) or Eq. (12) numerically using MATLAB Optimization Toolbox [30].

A. Influence of MDL

In Fig. 3, we show the outage-free secrecy capacity, outage secrecy capacity (with $p_{int} = 10^{-4}$), and average secrecy capacity vs. the average MDL of the eavesdropping channel, for the uniformly distributed MDL model. Here we assume that both the legitimate receiver and the eavesdropper have the same SNR of 20 dB. For $M = 8$ and $M = 16$, the secrecy capacities quickly saturate as the eavesdropper's MDL increases beyond about 25 dB. For $M = 8$, the outage-free and outage secrecy capacities are very close; while for $M = 16$, the outage secrecy capacity is slightly higher than outage-free secrecy capacity. We also observe that the curves for outage-free secrecy capacities for $M = 8$ and $M = 16$ overlap with each other, as predicted by Eq. (11). However, the average secrecy capacities are much higher than both outage-free and outage secrecy capacities. For MDL values ranging from 5 to 60 dB, the average secrecy capacities of $M = 8$ and $M = 16$ are at least 50% and 100% higher than the respective outage-free secrecy capacity. This clearly demonstrate the advantage of coding at average secrecy capacity for frequency-selective channels.

B. Comparison Between Uniform and Log-uniform MDL Models

In Fig. 4, we compare the outage secrecy capacity and the average secrecy capacity generated by uniformly and log-uniformly distributed v_is of the MDL matrix $\mathbf{V}$. Here we assume that both the legitimate receiver and the eavesdropper

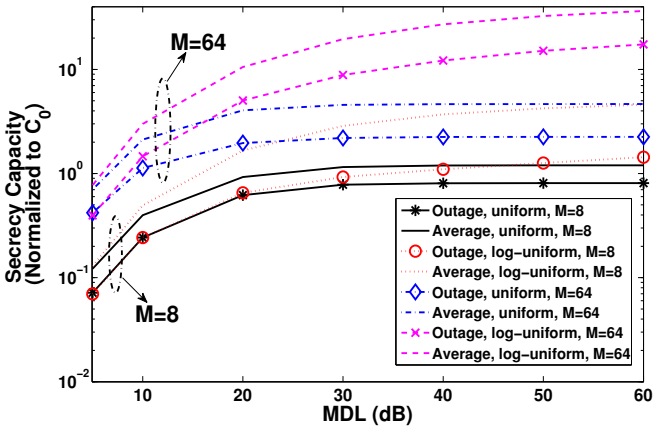

Fig. 4. Secrecy capacity vs. average MDL experienced by the eavesdropper for $M = 8$ and $M = 64$.

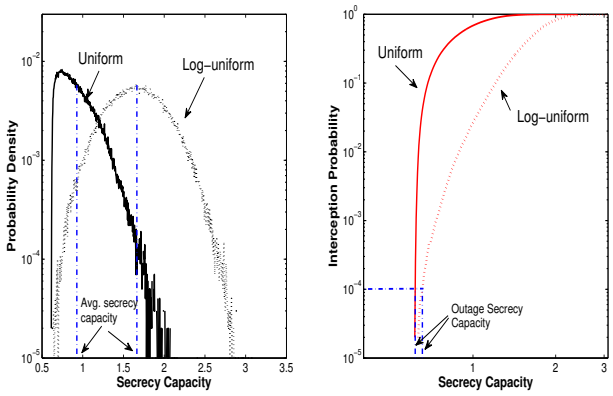

Fig. 5. (a) Histograms of the secrecy capacities for the uniformly and the log-uniformly distributed models; (b) interception probability vs. data rate for the uniformly and the log-uniformly distributed models.

have the same SNR of 20 dB . For both $M = 8$ and $M = 64$, the differences between two models are insignificant when MDL $\leq$ 10 dB. However, for MDL $>$ 10 dB, the secrecy capacities of log-uniformly distributed MDLs are higher. In addition, the gap between the capacities generated by the two models increases as both the values of MDL and M increase. To better understand this, we also compare the histograms of the capacities (Fig. 5 (a)) and interception probability vs. secrecy capacity curves (Fig. 5 (b))) of the two models for the case of $M = 8$, MDL $= 20$ dB, SNR $=$ SNR$^e = 20$ dB. As shown in the plots, the distribution generated by the log-uniform model is skewed towards higher secrecy capacities. As such. the log-uniformly distributed model yields higher average and outage secrecy capacities. In this context the MDL distribution is, to some extent, part of the design freedom for SDM fibers.

C. Influence of SNRs of the Main and the Eavesdropping Channels

Motivated by the possibility that the eavesdropper's receiver could be located very close to the transmitter and thus experience higher SNR than the legitimate receiver, we assess

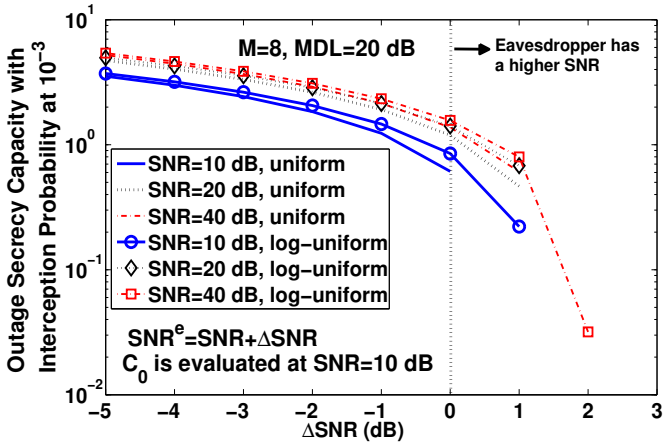

Fig. 6. Outage secrecy capacities (normalized to C_0) vs. the ΔSNR of the eavesdropper.

the impact of an eavesdropper's higher SNR on the secrecy capacity achieved by the legitimate channel. Fig. 6 illustrates the outage secrecy capacity as a function of the SNR difference (in dB) between the eavesdropper and the legitimate receiver (denoted as ΔSNR) for uniform and log-uniform channel models with MDL=20 dB. Here, the SDM system supports 8 modes ($M = 8$) and the legitimate receiver has an SNR of $[10, 20, 40]$ dB. We observe that higher SNRs of the legitimate receiver and MDLs for the eavesdropper in general enhance security, even if the eavesdropper has higher SNR than the legitimate receiver. The figures also show that the log-uniform model results in better resilience against an eavesdropper with higher SNR than the uniform model, again pointing towards tapping-resilient SDM fiber designs.

In Fig. 7 we plot the average secrecy capacity as a function of the SNR difference between the eavesdropper and the legitimate receiver, for the same set of parameters used in plotting Fig. 6. We observe a similar trend that higher SNRs of the legitimate receiver and MDLs for the eavesdropper in general improve security. Consistent with the results obtained so far, the average secrecy capacity can tolerate much higher SNR differences between the eavesdropper and the legitimate receiver.

These results shows that MDL plays an important role in enhancing the robustness of the security guarantees. With large MDLs, fundamental security can still be achieved even if the eavesdropper has a higher SNR. This is in great contrast with the results of SISO Gaussian wiretap channels [13], which show that confidential communication is possible only when the eavesdropping channel is degraded (by a lower SNR). Also, the necessity of degrading the eavesdropper's SNR is obvious, since such an approach is theoretically equivalent of establishing an upper bound on the capacity that an eavesdropper can extract from the MIMO-SDM system.

V. Conclusions

Coupling spatial information out of an MIMO-SDM waveguide through bending leads to inherent changes in the spatial

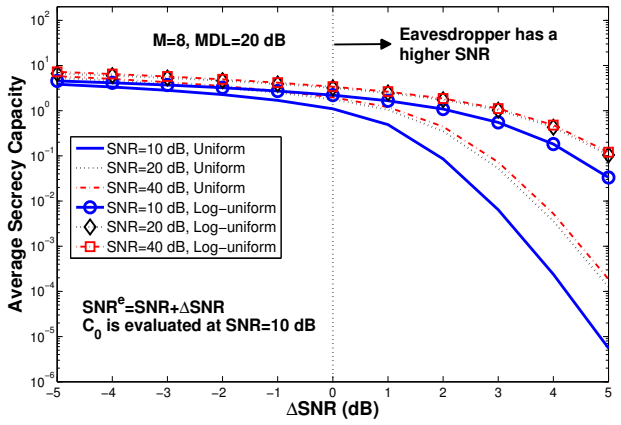

Fig. 7. Average secrecy capacities (normalized to C_0) vs. the ΔSNR of the eavesdropper.

information content, both for an eavesdropper and for the legitimate transmiter-receiver pair. As a result, the eavesdropper's MIMO channel will generally be less favorably conditioned than that of the legitimate user; at the same time, a bend-induced MDL recorded at the legitimate receiver will reveal the presence of the eavesdropper. As such, MIMO-SDM has the potential of providing a provably secure high-capacity medium of transmission. In this work, we evaluated the security benefits of MIMO-SDM using equivocation as a measure of secrecy. Our results show that the secrecy capacity achieved by an SDM system can potentially be orders of magnitude higher than what can be offered by QKD. In addition, SDM systems can provide fundamental security even if the eavesdropper has a higher SNR than that of the legitimate receiver.

In our future work, we plan to gain further insight into the practical implementation of secure MIMO-SDM systems, especially the design of secure modulation/coding schemes. As an extension of this work, we are currently investigating the secrecy capacity of MIMO-SDM channel with finite complex constellation inputs. In addition to equivocation, we are also looking into *rate-distortion* as an alternative metric for secrecy.

VI. Appendix

A. Derivations of Eq.(9) and Eq.(10)

We first obtain the upper bound on v_1, which follows directly from the constraints of the problem Eq. (7). That is,

$$\begin{aligned} M &= \sum_{i=1}^{M} v_i \geq v_1^e[(M-1)+\text{MDL}] \\ &\Rightarrow \quad v_1 \leq \frac{M}{M-1+\text{MDL}} \end{aligned} \tag{14}$$

We can similarly find a lower bound on v_1:

$$\begin{aligned} M &= \sum_{i=1}^{M} v_i \leq v_1^e[1+(M-1)\text{MDL}] \\ &\Rightarrow \quad v_1 \geq \frac{M}{1+(M-1)\text{MDL}} \end{aligned} \tag{15}$$

Using the arithmetic-geometric mean inequality [27],

$$\begin{aligned} \prod_{i=3}^{M}(1+v_i\text{SNR}^e) &\leq \left[\frac{1}{M-2}\sum_{i=3}^{M}(1+v_i\text{SNR}^e)\right]^{M-2} \\ &= \left[1+\frac{\text{SNR}^e}{M-2}\sum_{i=3}^{M}v_i\right]^{M-2} \end{aligned} \tag{16}$$

Note that the equality holds only for $v_i = v_j$, with $3 \leq i \leq M$ and $3 \leq j \leq M$. That is

$$v_i = \frac{M - v_1(1+\text{MDL})}{M-2}, \ i = 3, 4, ..., M. \tag{17}$$

The optimization problem can be simplified to the maximization of $\varphi(v_1)$ over the interval of $[M/(1+(M-1)\text{MDL}), M/(M-1+\text{MDL})]$, where $\varphi(v_1)$ is expressed as:

$$\begin{aligned} \varphi(v_1) &= \log_2(1+\text{SNR}^e v_1) + \log_2(1+\text{MDL}\cdot\text{SNR}^e v_1) \\ &+ (M-2)\log_2\left[1+\frac{M-v_1(1+\text{MDL})}{M-2}\text{SNR}^e\right] \end{aligned} \tag{18}$$

When the value of SNR^e is large enough (e.g. SNR=40 dB), we can approximate $\varphi(v_1)$ by using $\log_2(1+x) \approx \log_2(x)$ for $x \gg 1$:

$$\begin{aligned} \varphi(v_1) &\approx \log_2(\text{SNR}^e v_1) + \log_2(\text{MDL}\cdot\text{SNR}^e v_1) \\ &+ (M-2)\log_2\left[\frac{M-v_1(1+\text{MDL})}{M-2}\text{SNR}^e\right] \end{aligned} \tag{19}$$

In this case, we can find the optimal v_1 by solving

$$\frac{\partial\varphi}{\partial v_1} = 0, \tag{20}$$

which leads to $v_1 = 2/(1+\text{MDL})$. By definition, we have

$$v_2 = 2\frac{\text{MDL}}{(1+\text{MDL})}. \tag{21}$$

Substituting $v_1 = 2/(1+\text{MDL})$ into Eq. (17) yields $v_i = 1$ for $i = 3, 4, ..., M$.

B. $\mathbf{Q_x} = \mathbf{I}$ achieves average secrecy capacity

In this section, we outline the three key steps in proving that $\mathbf{Q_x} = \mathbf{I}$ maximizes the average of secrecy rate $\mathbb{E}[I(x,y) - I(x,y^e)]$.

In the first step, we show that we can greatly reduce the solution space of the optimization problem (of $\mathbb{E}[I(x,y) - I(x,y^e)]$) by considering only diagonal covariance matrices, using the properties of unitary matrices $\mathbf{\Lambda^Q}$ [26]. In other words, all the statistical characteristics of $\mathbf{Q_x}$ are preserved in

$\mathbf{\Lambda^Q}$. As such, the received signals of the legitimate receiver and the eavesdropper can be equivalently expressed as:

$$\mathbf{y} = \sqrt{\gamma}\sqrt{\mathbf{\Lambda^Q}}\mathbf{x} + \mathbf{n}, \quad (22)$$

$$\mathbf{y}^e = \sqrt{\gamma^e}\sqrt{\mathbf{V}}\tilde{\mathbf{U}}^{\mathbf{e}}\sqrt{\mathbf{\Lambda^Q}}\mathbf{x} + \mathbf{n}^{\mathbf{e}}. \quad (23)$$

In the second step, we show that $\mathbb{E}[I(\mathbf{x},\mathbf{y}) - I(\mathbf{x},\mathbf{y}^e)]$ is an increasing function of λ_i^Q (diagonal elements of the covariance matrix $\mathbf{\Lambda^Q}$). Using the fundamental relationship between the mutual information and the minimum mean-square error in Gaussian channels [28], we have:

$$\nabla_{\mathbf{\Lambda^Q}} I(\mathbf{x},\mathbf{y}) = \gamma\left(\mathbf{I} + \gamma\ \mathbf{\Lambda^Q}\right)^{-1}, \quad (24)$$

$$\nabla_{\mathbf{\Lambda^Q}} I(\tilde{\mathbf{x}},\tilde{\mathbf{y}^e}) = \gamma^e\tilde{\mathbf{U}}^{\mathbf{e}}\mathbf{V}\tilde{\mathbf{U}}^{\mathbf{e}\dagger}\left(\mathbf{I} + \gamma^e\ \mathbf{\Lambda^Q}\tilde{\mathbf{U}}^{\mathbf{e}}\mathbf{V}\tilde{\mathbf{U}}^{\mathbf{e}\dagger}\right)^{-1} \quad (25)$$

Since $\tilde{\mathbf{U}}^{\mathbf{e}}$ is a Haar matrix, $\nabla_{\mathbf{\Lambda^Q}}\mathbb{E}[I(\tilde{\mathbf{x}},\tilde{\mathbf{y}^e})]$ is concave and symmetric with respect to $\mathbf{V}$, and thus Schur concave. Using the fact that [29, Theorem 4.3.26]:

$$[(\tilde{\mathbf{U}}^{\mathbf{e}}\mathbf{V}\tilde{\mathbf{U}}^{\mathbf{e}\dagger})_{11},\ldots,(\tilde{\mathbf{U}}^{\mathbf{e}}\mathbf{V}\tilde{\mathbf{U}}^{\mathbf{e}\dagger})_{MM}] \preceq [v_1,\ldots,v_M] \quad (26)$$

and Jensen's inequality, we arrive at:

$$\begin{aligned}
&\nabla_{\mathbf{\Lambda^Q}}\mathbb{E}[I(x,y) - I(x,y^e)] \\
=\ &\gamma\left(\mathbf{I} + \gamma\ \mathbf{\Lambda^Q}\right)^{-1} \\
&-\gamma^e\mathbb{E}\left[\tilde{\mathbf{U}}^{\mathbf{e}\dagger}\mathbf{V}\tilde{\mathbf{U}}^{\mathbf{e}}\left(\mathbf{I} + \gamma^e\ \mathbf{\Lambda^Q}\tilde{\mathbf{U}}^{\mathbf{e}\dagger}\mathbf{V}\tilde{\mathbf{U}}^{\mathbf{e}}\right)^{-1}\right] \\
\succeq\ &\gamma\left(\mathbf{I} + \gamma\ \mathbf{\Lambda^Q}\right)^{-1} \\
&-\gamma^e\ \mathbb{E}\left[\text{diag}(\tilde{\mathbf{U}}^{\mathbf{e}}\mathbf{V}\tilde{\mathbf{U}}^{\mathbf{e}\dagger})\right]\left(\mathbf{I} + \gamma^e\ \mathbf{\Lambda^Q}\ \mathbb{E}\left[\text{diag}(\tilde{\mathbf{U}}^{\mathbf{e}}\mathbf{V}\tilde{\mathbf{U}}^{\mathbf{e}\dagger})\right]\right)^{-1} \quad (27)
\end{aligned}$$

Finally, using the fact that:

$$\mathbb{E}[\tilde{\mathbf{U}}^{\mathbf{e}}\mathbf{V}\tilde{\mathbf{U}}^{\mathbf{e}\dagger}]) = \frac{1}{M}\mathbb{E}\left[\mathbf{I}\cdot\text{tr}(\mathbf{V})\right] = \mathbf{I}, \quad (28)$$

and substituting (28) into Eq.(27), we have:

$$\nabla_{\mathbf{\Lambda^Q}}\mathbb{E}[I(x,y) - I(x,y^e)] \succeq \mathbf{0}, \quad (29)$$

which shows that $\mathbb{E}[I(x,y) - I(x,y^e)]$ indeed is an increasing function of λ_i^Qs.

The last step is straight forward. Since the power is constrained on a per mode basis ($0 \geq \lambda_i^Q \leq 1$) and $\mathbb{E}[I(x,y) - I(x,y^e)]$ is an increasing function of λ_i^Qs, it follows that $\lambda_i^Q = 1$ maximizes $\mathbb{E}[I(x,y) - I(x,y^e)]$. We thus prove that $\mathbf{Q_x} = \mathbf{\Lambda^Q} = \mathbf{I}$ achieves the average secrecy capacity.

REFERENCES

[1] K. Shaneman, "Optical network security: technical analysis of fiber tapping mechanisms and methods for detection and prevention," MILCOM 2004, vol. 2, pp.711, Oct. 2004.

[2] M. Medard, et al,"Security issues in all-optical network," *IEEE Networks*, vol. 11, no. 3, pp. 42-48, May/June, 1997.

[3] M. P. Fok, Z. Wang, Y. Deng, and P. R. Pucnal, "Optical layer security in fiber-fptic networks," *IEEE Transactions on Information Security and Forensics*, vol., no. , pp. 725-736, Sept. 2011.

[4] V. Scarani et al.,"The security of practical quantum key distribution,", Rev. Mod. Phys, vol. 81, no. 3, pp. 1301-1350, July-Sept. 2009.

[5] A. R. Dixon, et al., "Continuous operation of high bit rate quantum key distribution," Appl. Phys. Lett. vol. 96, pp. 161102, 2010.

[6] N. Peters, et al., "Quantum Communications in Reconfigurable Optical Networks: DWDM QKD through a ROADM,", OFC 2010, paper OTuk1, Mar. 2010.

[7] P. J. Winzer, "Modulation and multiplexing in optical communication systems," IEEE/LEOS Newsletter, February 2009

[8] T. Morioka, "New generation optical infrastructure technologies: EXAT initiative towards 2020 and beyond," Proc. OECC, FT4 (2009).

[9] P. J. Winzer, "Energy-Efficient Optical Transport Capacity Scaling Through Spatial. Multiplexing," IEEE Photon. Technol. Lett., vol. 23, pp.851-853, 2011.

[10] K. Guan, P. J. Winzer, and E. Soljanin, "Information-theoretic security in space-division multiplexed fiber optic networks," ECOC 2012, Tu.3.C.4, Sep. 2012.

[11] K. Guan, E. C. Song, E. Soljanin, and P. J. Winzer, "Physical Layer Security in Space-division Multiplexed Fiber Optic Commmunications,"*Asilomar Conference on Signals, Systems, and Computers*, TA1A-4, Nov. 2012.

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

[13] S. K. Cheong and M. Hellman,"The Gaussian wire-tap channel", IEEE Trans. Inf. Theory, vol. 24, no. 4, pp.451-456, Jul. 1978.

[14] J. Barros and M. R. D. Rodrigues, "Secrecy capacity of wireless channels,", *ISIT* 2006, Seattle, WA, USA, July 2006.

[15] A. Hero, "Secure space-time communication," IEEE Trans. Inf. Theory, vol. 49, no. 12, pp. 3235-3249, Dec. 2003.

[16] F. Oggier and B. Hassibi, "The secrecy capacity of the MIMO wiretap channel," IEEE Trans. Inf. Theory, vol. 57, no. 8, pp. 4961-497, Aug. 2011.

[17] A. Khisti and G. W. Wornell, "Secure Transmission with Multiple Antennas-I: The MISOME Wiretap Channel, IEEE Trans. Inf. Theory, Vol. 56, No. 7, pp. 3088-3104, July 2010.

[18] A. Khisti and G. W. Wornell, "Secure Transmission with Multiple Antennas-II: The MIMOME Wiretap Channel, IEEE. Trans. Inf. Theory, Vol. 56, No. 11, pp. 5515-5532, Nov. 2010

[19] R. Bustin, R. Liu, H. V. Poor, and S. Shamai, "An MMSE approach to the secrecy capacity of the MIMO Gaussian wiretap channel," *EURASIP Journ. Wireless Commun. Network.*, 2009

[20] A. Pruyear, and V. W. S. Chan, "Using spatial diversity to improve the confidentiality of atmospheric free space optical communication," IEEE Globecomm 2011, Houston, TX, USA, Dec. 2011.

[21] P. J. Winzer and G. J. Foschini, "MIMO capacities and outage probabilities in spatially multiplexed optical transport systems," Optical Express, vol. 19, no. 17, pp. 16680-16696, Aug. 2011.

[22] S. Chandrasekhar et al.,"WDM/SDM Transmission of 10 x 128-Gb/s PDM-QPSK over 2688-km 7-Core Fiber with a per-Fiber Net Aggregate Spectral-Efficiency Distance Product of 40,320 km.b/s/Hz", ECOC 2011, Th.13.C.4, Sept. 2011.

[23] H. Takahashi et al., "First Demonstration of MC-EDFA-Repeatered SDM Transmission of 40 x 128-Gbit/s PDM-QPSK Signals per Core over 6,160-km 7-core MCF," Proc. ECOC, Th3.C.3 (2012).

[24] R. Ryf et al.,"Analysis of Mode-Dependent Gain in Raman Amplified Few-Mode Fiber," OFC 2012, PDP5C.2, Mar. 2012.

[25] S. Randel et al., "Adaptive MIMO signal processing for mode-division multiplexing," OFC 2012," PDP5C.5, Mar. 2012.

[26] A. M. Tulino and S. Verdú, "Random Matrix Theory and Wireless Communications," *Foundations and Trends In Communications and Information Theory*, vol. 1, no. 1, pp. 1–184, 2004.

[27] D. P. Bertsekas, *Nonlinear Programming*, 2nd. Edition, Athena Scientific, Belmont, MA, 2003.

[28] D. Guo, S. Shamai, and S. Verdu, "Mutual Information and Minimum Mean-Square Error in Gaussian Channels," IEEE. Trans. Inf. Theory, Vol. 51, No. 4, pp. 1261-1283, Apr. 2005.

[29] R. A. Horn and C. R. Johnson, *Matrix Analysis*, Cambridge University Press, Cambridge, UK, 1991.

[30] *MATLAB Optimization Toolbox User's Guide*, the Mathworks Inc., Natick, MA