Robust Secure Goodput for Massive MIMO and Optical Fiber Wiretap Channels

Andrew Lonnstrom and Eduard Jorswieck
Communications Theory
TU Dresden
Dresden 01062, Germany
Email: andrew.lonnstrom@tu-dresden.de,
eduard.jorswieck@tu-dresden.de

Daniel Haufe and Juergen W. Czarske
Laboratory of Measurement and Sensor System Technique
TU Dresden
Dresden 01062, Germany
Email: daniel.haufe@tu-dresden.de,
juergen.czarske@tu-dresden.de

***Abstract*—We propose a method for optimizing the information theoretic secure goodput of a multiple-input multiple-output (MIMO) degraded wiretap channel using inverse precoding. We evaluate the secrecy capacity of this method in terms of secure goodput under various aspects using a standard fading massive MIMO system under the assumption of perfect channel state information (CSI) at the transmitter for the legitimate channel and no CSI at the transmitter for the eavesdropper channel. The precoding scheme optimizes two parameters, the number of compromised streams and the channel advantage of the legitimate receiver. The resulting secure goodput can be specialized to massive MIMO or optical channels with single or multiple eavesdroppers. We include a numerical analysis of the secure goodput for a multi-mode fiber (MMF) optical channel to demonstrate the flexibility of our approach.**

I. Introduction

Applications have put demands on ever increasing data rates and technology has kept up with the demand so far. Coupled with this increasing data rate is the desire to transmit securely without fear of losing sensitive information to an unknown eavesdropper. In this regard, Wyner in his seminal paper [1] laid the foundation for evaluating information theoretic security for the wire-tap channel without the use of secret keys. Capacities of peaceful (i.e. non-eavesdropped) MIMO systems under various CSI assumptions were studied in [2]. The fading MIMO wiretap channel, where the eavesdropper also has multiple antennas, is investigated in [3]. More recently there have been investigations into the secrecy rate for fading wiretap channels [4] as well as multiple-input single-output (MISO) channels with channel state information (CSI) [5]. In [6], a massive MIMO system was analyzed from a computational complexity perspective and this was expanded to an information theoretic analysis in [7].

In addition to securing the transmission over wireless networks, there is also an increasing interest in securing the physical layer in fiber optic communication systems. Multi-mode fibers (MMF) are of particular interest since the signal processing techniques used in this technology mirror those used in MIMO wireless signal processing [8]. A comprehensive overview of the various physical layer attacks on evolving optical networks are discussed in [9]. Recently a method for physical layer secret key generation over fiber optic networks was discussed in [10]. A numerical study on the secrecy capacity for free space optical degraded wiretap channels was done in [11] for on-off keying (OOK). MIMO capacities for optical transport networks have been investigated in [12] and the secrecy capacity of space-division multiplexed fiber optical communication systems was investigated in [13].

One interesting aspect, both for massive MIMO as well as massive MMF, is how the large degrees of freedom can be exploited to establish information-theoretic secure links. The channel model as well as the attacker model have a significant impact on the achievable secrecy rates.

The focus of this work is to present an idea for maximizing the information theoretic secure goodput of a wireless MIMO system with perfect CSI for the legitimate receiver. We prove that a secure goodput is achievable by compromising a number of data streams due to the channel uncertainty to the eavesdropper. The solution to the corresponding optimization problem is characterized. Numerical assessments illustrate the performance of the proposed scheme in massive MIMO Rayleigh fading. In particular, we apply this method to an MMF optical system, as proposed in [14], and evaluate its performance.

II. System Model

We consider an $n \times m$ complex-valued MIMO system where n is the number of transmit antennas at Alice and m is the number of receive antennas at Bob as shown in Figure 1. Without loss of generality, we will assume that Bob and Eve both have the same number of antennas at the receiver unless stated otherwise. The received signals can be written as

$$\mathbf{y_b} = \mathbf{H}\mathbf{x} + \mathbf{n_b} \tag{1}$$

$$\mathbf{y_e} = \mathbf{G}\mathbf{x} + \mathbf{n_e} \tag{2}$$

This work is supported in part by the German Research Foundation (DFG) within the Collaborative Research Center 912 "Highly Adaptive Energy-Efficient Computing" (HAEC).

978-1-5090-3009-5/17/$31.00 ©2017 IEEE

for Bob and Eve, where the input signal $\mathbf{x} \in \mathbb{C}^n$, and $\mathbf{H}, \mathbf{G} \in \mathbb{C}^{m \times n}$ are the channel matrices for Bob and Eve respectively. The vectors $\mathbf{n_b}, \mathbf{n_e} \in \mathbb{C}^m$ are the channel noise with independent identically distributed (i.i.d.) Gaussian entries with zero-mean and standard deviations σ_b and σ_e respectively. The SNR is defined as

$$\rho = \frac{p}{\sigma^2}$$

where p is the transmit power and, for the purposes of this work, the noise variance at Bob and Eve is equal, i.e. $\sigma_b^2 = \sigma_e^2 = \sigma^2$.

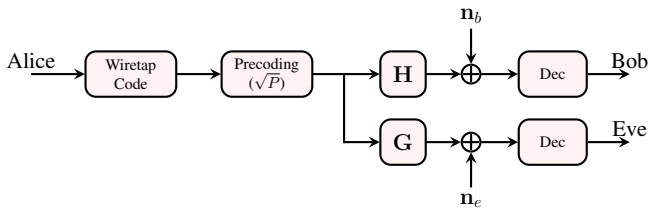

Fig. 1. Wiretap channel model for communication between Alice and Bob with eavesdropper (Eve).

By performing the singular value decomposition (SVD) of $\mathbf{H}$ we obtain $\mathbf{H} = \mathbf{U}\mathbf{\Lambda}\mathbf{V}^\dagger$ where the singular values are $s_1, ..., s_j$, with $j = \min(m, n)$, and $\dagger$ represents the conjugate complex transpose of a matrix.

A message is spread over the n channels through a serial to parallel operation which has the output $d_1, ..., d_n$ where the output signals d_l are multiplied with a beamforming and power allocation, $\mathbf{v}_l$ and $\sqrt{p_l}$ respectively. We write the transmitted signal $\mathbf{x}$ as

$$\mathbf{x} = \sum_{l=1}^{n} \sqrt{p_l}\mathbf{v}_l d_l$$

where p_l is the power of the l^{th} channel. The corresponding transmit covariance matrix can be written as

$$\mathbf{P} = \sum_{l=1}^{n} p_l \mathbf{v}_l \mathbf{v}_l^\dagger \quad . \tag{3}$$

The ordered eigenvalues of the effective channels to Bob

$$\mathbf{H}\mathbf{H}^\dagger \quad : \quad \lambda_l(\mathbf{H}\mathbf{H}^\dagger)$$

are given as λ_l, where $\lambda_1 \geq ... \geq \lambda_n$. Similarly, the ordered eigen-values of the effective channel to Eve

$$\mathbf{G}\mathbf{G}^\dagger \quad : \quad \gamma_l(\mathbf{G}\mathbf{G}^\dagger)$$

are given as γ_l, where $\gamma_1 \geq ... \geq \gamma_n$. When setting $\mathbf{V}$ as our precoder and $\mathbf{U}^\dagger$ as our decoder, the channel is diagonalized and the SNR of the l^{th} MIMO data stream is given as

$$\text{SNR}_l = \frac{p_l \lambda_l}{\sigma^2} = \rho\lambda_l \quad . \tag{4}$$

Similarly, if inverse precoding is used, i.e. $\mathbf{P} = \mathbf{H}^{-1}$, the effects of the channel are removed and the SNR of the l^{th} MIMO data stream is also given as in (4) where $\lambda_l = 1$.
One can define an advantage ratio metric for a linear decoder in terms of a ratio between certain eigenvalues of the effective channels to Bob and Eve as follows:

$$\mathbf{adv_{linDec}} = \frac{\lambda_n}{\gamma_1} < \frac{\lambda_n}{\gamma_n} < \frac{\lambda_1}{\gamma_n} \tag{5}$$

where the middle ratio was used as a performance metric for the advantage of the Zero-Forcing receiver (adv_{zf}) in [7]. Note that it is assumed that $m \geq n$ and that the effective channels are full rank otherwise $\lambda_n = 0$ or $\gamma_n = 0$.

Our idea is to allow Eve to decode up to the k^{th} best stream resulting in $k \cdot R$ bits being compromised (compare to [4]). In total we transmit $n \cdot R$ bits resulting in a privacy amplification where $(n-k) \cdot R$ bits remain "secure" if

$$\gamma_{k+1} < \lambda_n \, . \tag{6}$$

The linear decoding advantage is then given as

$$\mathbf{adv_{linDec}} = \frac{\lambda_n}{\gamma_{k+1}} \, . \tag{7}$$

III. Guaranteed Secure Goodput

Problem Statement: Achieve secure communication in the MIMO wiretap channel with perfect channel state information at the transmitter (CSIT) about $\mathbf{H}$ and no CSIT on $\mathbf{G}$. Inverse precoding and the resulting SNR as described in (4) is to be applied.

Definition: The secure goodput is the amount of bits which can be reliably and information theoretic securely received.

In order for Bob to decode successfully, λ_n is assumed to be above a minimum threshold SNR. The probability of success is then given by

$$Pr_{suc} = Pr[\lambda_n - \gamma_{k+1} > 0]. \tag{8}$$

The secure goodput of the system is now given as the rate multiplied with the probability of success, i.e. $R \cdot Pr_{suc}$. The number of secure bits transferred is $(n-k) \cdot R$. The secure goodput, $Gput_{sec}$, is given as

$$Gput_{sec} = (n-k) \cdot R \cdot Pr[\lambda_n - \gamma_{k+1} > 0] \, . \tag{9}$$

This goodput depends on the SNR at Bob and Eve as well as the statistics of the channel matrices $\mathbf{H}$ and $\mathbf{G}$. In (9), it is necessary to determine the secure transmission rate R. In order to apply the results from Wyner on the degraded wiretap channel, we have to introduce a gap, Δ, between the worst channel for Bob, λ_n, and the $k+1$ best channel to Eve, γ_{k+1}. The rate, R, is dependent on Δ. If Δ is chosen too small (i.e. $\lambda_n \approx \gamma_{k+1}$) then information theoretic secure transmission is not possible.

Theorem 1: The following secure goodput can be achieved

$$Gput_{sec} = \max_{1\le k\le n}\max_{\Delta>0}(n-k)\cdot \log\left(1+\frac{\rho\Delta}{1+\rho(\lambda_n-\Delta)}\right)\cdot \left(Pr(\lambda_n \ge \gamma_{k+1}+\Delta)\right) \quad (10)$$

Proof: In order to show secrecy, we assume that the condition

$$\lambda_n \ge \gamma_{k+1}+\Delta \quad (11)$$

holds. If (11) is not satisfied then the system will be in outage. From (11), it follows that at least $n-k$ data streams have an advantage of at least Δ. We apply a wiretap code from [1] for the equivalent wiretap channel with a channel to Bob of at least λ_n and a channel to Eve of at most $\lambda_n-\Delta$ and achieve a secrecy rate of

$$R_s = \log(1+\rho\lambda_n)-\log(1+\rho\gamma_{k+1}) \quad (12)$$
$$\ge \log(1+\rho\lambda_n)-\log(1+\rho(\lambda_n-\Delta)) \quad (13)$$
$$= \log\left(\frac{1+\rho\lambda_n}{1+\rho(\lambda_n-\Delta)}\right) \quad (14)$$
$$= \log\left(1+\frac{\rho\Delta}{1+\rho(\lambda_n-\Delta)}\right) \quad (15)$$

At this point it is known that $n-k$ data streams are not able to be decoded without error (i.e. unknown) at Eve, however, Alice and Bob do not know which data streams these are. In order to compensate for this we use privacy amplification, according to [15] (see also Theorem 4.4 in [16]) which shows that we can secure the $n-k$ streams with the use of a universal family of hash functions [17]. This results in both weak and strong confidentiality/secrecy as in [16] and [18]. To finish the proof, we show that (11) implies reliability at Bob's decoder as well. Rewriting (12) we obtain

$$\log(1+\rho\lambda_n) = R_s+\log(1+\rho\gamma_{k+1}) \quad (16)$$

and combining (16) and (15) we have

$$\log(1+\rho\lambda_n) \ge \log\left(\frac{1+\rho\lambda_n}{1+\rho(\lambda_n-\Delta)}\cdot(1+\rho\gamma_{k+1})\right). \quad (17)$$

Removing the log operation on both sides, the equation can be simplified to

$$1 \ge \frac{1+\rho\gamma_{k+1}}{1+\rho(\lambda_n-\Delta)} \quad (18)$$
$$1+\rho(\lambda_n-\Delta) \ge 1+\rho\gamma_{k+1} \quad (19)$$
$$\lambda_n-\Delta \ge \gamma_{k+1}. \quad (20)$$

□

In order to solve the programming problem in (10) efficiently, we provide the following lemma.

Lemma 2: The objective function,

$$(n-k)\cdot\log\left(1+\frac{\rho\Delta}{1+\rho(\lambda_n-\Delta)}\right) \cdot Pr(\lambda_n \ge \gamma_{k+1}+\Delta), \quad (21)$$

is a unimodal function w.r.t. Δ for fixed k, and a unimodal function w.r.t. k for fixed Δ.

A few remarks about the optimization problem in (10). A total of k data streams are compromised which means that $n-k$ data streams are secured. The rate, R, in (15) is replaced by a secrecy capacity of an equivalent wiretap channel. The gap between the lowest λ_n and γ_{k+1} is given by Δ and is used for secure transmission. Because the effective channel from Alice to Bob after zero-forcing precoding results in $\lambda_1 = ... = \lambda_n = 1$, the range of the gap ($\Delta$) is $[0,1]$. The probability in (10) reflects the channel statistics, which could be specialized to massive MIMO wireless or optical multi-mode fiber.

IV. Numerical Assessments

A. Massive MIMO

The channel model for the massive MIMO wiretap system is standard i.i.d. Rayleigh fading with spatially uncorrelated matrices $\mathbf{H} \sim \mathcal{CN}(0,\mathbf{I})$ and $\mathbf{G} \sim \mathcal{CN}(0,\mathbf{I})$, both statistically independent, where $\mathbf{I}$ is the identity matrix.

Monte-carlo simulations were done to solve the optimization problem in (10). As shown in Figure IV-A, depending on the choice of Δ, there exists an optimal number of streams which can be compromised in order to maximize the secure goodput. Figure 3 shows that increasing the SNR affects the optimal Δ

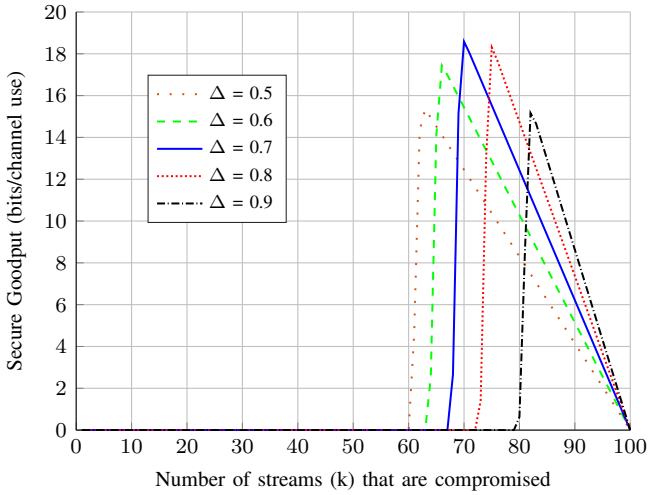

Fig. 2. Secure goodput plotted for various Δ showing an optimal number, k, of compromised streams where Alice, Bob, and Eve all have 100 antennas and inverse precoding is used at the transmitter.

such that higher SNR leads to a higher optimal Δ, although the shift in optimal Δ is not very large. On the other hand, there is a significant shift to the left, i.e. smaller optimal Δ, as the number of antennas at Eve is allowed to increase relative to Alice and Bob, as seen in Figure 4.

In the case where Alice, Bob, and Eve all have the same number of antennas (i.e. square channel transmission matrices), for a given SNR, the optimal Δ was not affected by changing the number of antennas.

Figure 5 shows secure goodput vs. SNR for a symmetric channel as well as cases where Eve has 1.5x and 2x the number

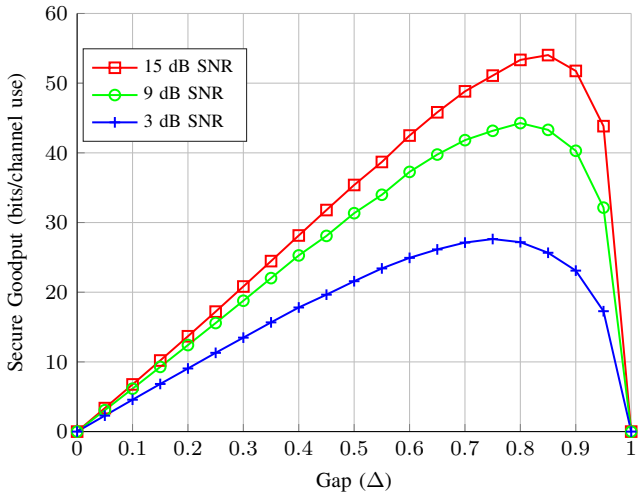

Fig. 3. Change in optimal Δ for various SNR where the number of antennas is set to 100 and inverse precoding is used at the transmitter

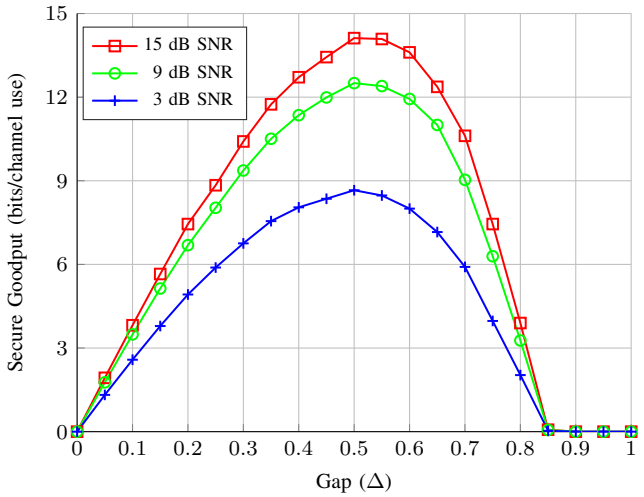

Fig. 4. Optimal Δ at different SNR when Eve has 200 antennas and Alice and Bob each have 100 antennas with inverse precoding applied at the transmitter.

of antennas, compared to Alice and Bob. It can be seen that using inverse precoding, it is still possible to achieve secure goodput even when Eve is allowed to have twice the number of receive antennas. It can also be seen that secure goodput is asymptotically limited for each of the scenarios. In other words, above a certain point, increasing the SNR of the system does not increase the secure goodput. This is due to the SNR, ρ, in the log term in (10) canceling for large SNR.

B. Optical Multi-mode Fiber (MMF)

One of the physical characteristics of a mutli-mode fiber (MMF) is that the modes of the fiber are grouped together in mode groups (MG) as discussed in [19]. The number of modes per mode group increases such that even with a high number of modes, the size of the mode groups remains relatively small.

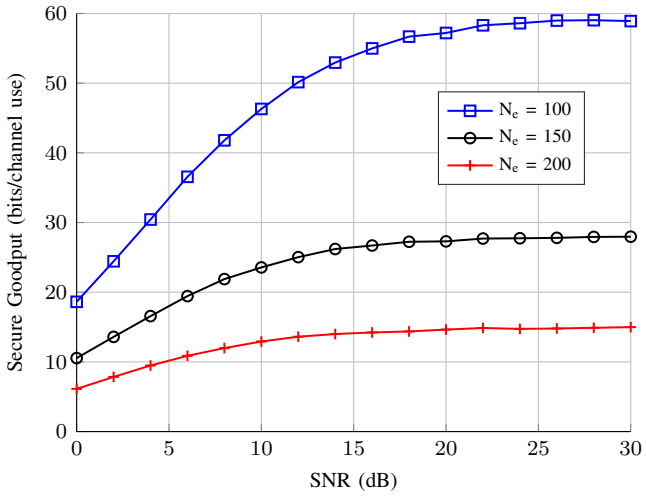

Fig. 5. Secure goodput over SNR compared to increasing the number of antennas at Eve relative to Bob

These mode groups result in a block diagonal structure for the fiber optical transmission matrix $\mathbf{H}_{opt}$

$$\mathbf{H}_{opt} = \begin{bmatrix} \mathbf{H}_{11} & 0 & \cdots & 0 \\ 0 & \mathbf{H}_{22} & & \vdots \\ \vdots & & \ddots & 0 \\ 0 & \cdots & 0 & \mathbf{H}_{jj} \end{bmatrix}$$

where j is the total number of mode groups. For our MMF simulations we use a similar channel statistics as in the wireless MIMO system, i.e. $\mathcal{CN}(0, \mathbf{I})$, however these channel statistics are i.i.d. for the individual mode groups along the block diagonal of the channel transmission matrix and 0 for all off-diagonal blocks.

It is worth noting that there is little gain to be expected from the inverse precoding for the smaller mode group sizes, however, the larger mode groups can benefit from inverse precoding.

This block-diagonal structure limits the information theoretic security of the MMF. It has, however, been shown in [20], that the block diagonal structure decays for high mode numbers. For the purposes of our investigation, we examined a conservative (i.e. worst-case) approach to the transmission matrix where the decaying effects were ignored.

In Figure 6, we show the comparison between two different multi-mode fibers (with 144 and 222 modes) and an 'equivalent' MIMO system where the number of antennas is equal to the number of modes of the multi-mode fiber. Here it can be seen that although there is a penalty in terms of maximum secure goodput due to the block diagonal structure of the channel matrices, information theoretic secure transmission can still be achieved using inverse precoding.

V. Conclusions

In this paper, we consider a general wiretap channel model for large matrix channels. They can either model massive

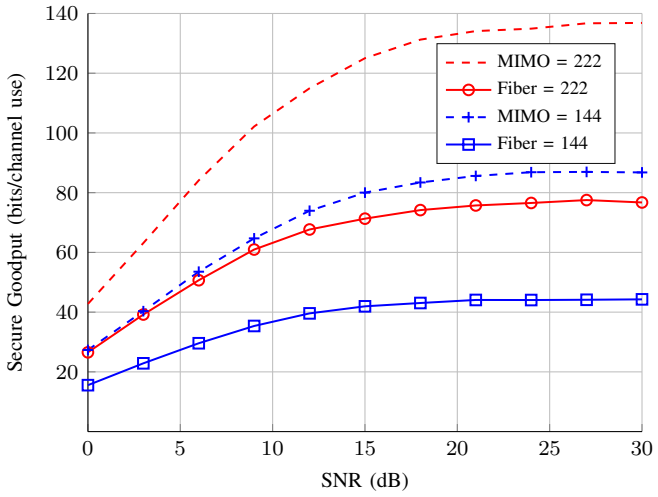

Fig. 6. Comparison of MIMO system with multi-mode fiber system where the number of modes is equal to the number of antennas

MIMO links or optical multi-mode channels. Due to the uncertainty about the channel to the eavesdropper, a conservative precoding and wiretap coding scheme is proposed in which a number of up to k layers/streams are allowed to be compromised. We present an optimization problem for maximizing the secure goodput. We show that using inverse precoding with prefect CSIT, secure goodput can be optimized in terms of the number of streams which are allowed to be compromised. Additionally, we show that the optimal gap can be found as well as how the number of antennas at the eavesdropper effects this gap. Furthermore, we show the secure goodput over a multi-mode fiber using our optimization problem when applying inverse precoding.

In future work, the transmission with artificial noise will be investigated as well as different channel statistics for the multi-mode fiber channel.

REFERENCES

[1] A. D. Wyner, "The wire-tap channel," *The Bell System Technical Journal*, vol. 54, pp. 1355–1387, Oct. 1975.

[2] A. Goldsmith, S. A. Jafar, N. Jindal, and S. Vishwanath, "Capacity limits of MIMO channels," *IEEE Journal on Selected Areas in Communications*, vol. 21, pp. 684–702, June 2003.

[3] A. Khisti and G. W. Wornell, "Secure transmission with multiple antennas II: The MIMOME wiretap channel," *IEEE Transactions on Information Theory*, 2010.

[4] Y. Liang, L. Lai, H. V. Poor, and S. Shamai, "A Broadcast Approach for Fading Wiretap Channels," *IEEE Transactions on Information Theory*, vol. 60, pp. 842–858, Feb. 2014.

[5] S. Gerbracht, C. Scheunert, and E. A. Jorswieck, "Secrecy Outage in MISO Systems With Partial Channel Information," *IEEE Transactions on Information Forensics and Security*, vol. 7, pp. 704–716, April 2012.

[6] T. Dean and A. Goldsmith, "Physical-layer cryptography through massive MIMO," in *2013 IEEE Information Theory Workshop (ITW)*, pp. 1–5, Sept. 2013.

[7] A. Sakzad and R. Steinfeld, "Massive MIMO Physical Layer Cryptosystem through Inverse Precoding." http://arxiv.org/abs/1507.08015, 2015.

[8] S. O. Arik, J. M. Kahn, and K. P. Ho, "MIMO Signal Processing for Mode-Division Multiplexing: An overview of channel models and signal processing architectures," *IEEE Signal Processing Magazine*, vol. 31, pp. 25–34, March 2014.

[9] N. Skorin-Kapov, M. Furdek, S. Zsigmond, and L. Wosinska, "Physical-layer security in evolving optical networks," *IEEE Communications Magazine*, vol. 54, pp. 110–117, August 2016.

[10] K. Kravtsov, Z. Wang, W. Trappe, and P. R. Prucnal, "Physical layer secret key generation for fiber-optical networks," *Opt. Express,*, vol. 21, pp. 23756–23771, Oct. 2013.

[11] H. Endo, T. S. Han, T. Aoki, and M. Sasaki, "Numerical Study on Secrecy Capacity and Code Length Dependence of the Performances in Optical Wiretap Channels," *IEEE Photonics Journal*, vol. 7, pp. 1–18, Oct. 2015.

[12] P. J. Winzer and G. J. Foschini, "MIMO capacities and outage probabilities in spatially multiplexed optical transport systems," *Opt. Express*, vol. 19, pp. 16680–16696, Aug 2011.

[13] K. Guan, A. M. Tulino, P. J. Winzer, and E. Soljanin, "Secrecy Capacities in Space-Division Multiplexed Fiber Optic Communication Systems," *IEEE Transactions on Information Forensics and Security*, vol. 10, pp. 1325–1335, July 2015.

[14] J. W. Czarske, D. Haufe, N. Koukourakis, and L. Buettner, "Transmission of independent signals through a multimode fiber using digital optical phase conjugation," *Opt. Express*, vol. 24, Jun 2016.

[15] C. H. Bennett, G. Brassard, C. Crepeau, and U. M. Maurer, "Generalized privacy amplification," in *Proceedings of 1994 IEEE International Symposium on Information Theory*, June 1994.

[16] M. Bloch and J. Barros, *Physical-Layer Security*. Cambridge University Press, 2011.

[17] J. Carter and M. N. Wegman, "Universal classes of hash functions," *Journal of Computer and System Sciences*, vol. 18, no. 2, pp. 143–154, 1979.

[18] M. R. Bloch and J. N. Laneman, "Strong Secrecy From Channel Resolvability," *IEEE Transactions on Information Theory*, vol. 59, pp. 8077–8098, Dec 2013.

[19] J. Carpenter, B. C. Thomsen, and T. D. Wilkinson, "Degenerate Mode-Group Division Multiplexing," *Journal of Lightwave Technology*, vol. 30, pp. 3946–3952, Dec 2012.

[20] J. Carpenter, B. J. Eggleton, and J. Schröder, "110x110 optical mode transfer matrix inversion," in *39th European Conference and Exhibition on Optical Communication (ECOC 2013)*, pp. 1–3, Sept 2013.