Linear Precoding for Finite-Alphabet Signaling Over MIMOME Wiretap Channels

Yongpeng Wu, *Student Member, IEEE*, Chengshan Xiao, *Fellow, IEEE*, Zhi Ding, *Fellow, IEEE*, Xiqi Gao, *Senior Member, IEEE*, and Shi Jin, *Member, IEEE*

***Abstract*—In this paper, we investigate the secrecy rate of finite-alphabet communications over multiple-input–multiple-output–multiple-antenna eavesdropper (MIMOME) channels. Traditional precoding designs based on Gaussian input assumption may lead to substantial secrecy rate loss when the Gaussian input is replaced by practical finite-alphabet input. To address this issue, we investigate linear precoding designs to directly maximize the secrecy rate for MIMOME systems under the constraint of finite-alphabet input. By exploiting the theory of Karush–Kuhn–Tucker (KKT) analysis and matrix calculus, we first present necessary conditions of the optimal precoding design when instantaneous channel-state information (CSI) of the eavesdropper is known at the transmitter. In this light, an iterative algorithm for finding the optimal precoding matrix is developed, utilizing a gradient decent method with backtracking line search. Moreover, we find that the beamforming design in MIMONE systems, which is a secrecy-capacity-achieving approach for Gaussian signaling, no longer provides the maximum secrecy rate for finite-alphabet input data. This case is substantially different from the Gaussian input case. In addition, we derive the closed-form results on the precoding matrix, which maximizes the secrecy rate in the low signal-to-noise ratio (SNR) region, and reveal the optimal precoding structure in the high-SNR region. A novel jamming signal generation method that draws on the CSI of the eavesdropper to additionally increase the secrecy rate is further proposed. The precoding design with only statistical CSI of the eavesdropper available at the transmitter is also considered. Numerical results show that the proposed designs provide significant gains over recent precoding designs through a power control policy and the precoding design with the Gaussian input assumption in various scenarios.**

***Index Terms*—Finite alphabet, multiple-input–multiple-output–multiple-antenna eavesdropper (MIMOME), transmit precoding, wiretap channel.**

I. Introduction

THE OPEN-ACCESS nature of radio transmission makes wireless communications inherently prone to security breaches such as eavesdropping and jamming. Traditional means for secure communications against unauthorized reception by eavesdroppers relies on encryption technologies. Still, encryption requires careful key distribution and service management [1], [2]. More recently, there has been a tide of rising interest in physical-layer security from an information-theoretic perspective. This paper focuses on security issues that are related to physical-layer security against eavesdropping, particularly under finite-alphabet user signals.

In the seminal work of Wyner on information-theoretic security [3], a "wiretap channel" model was introduced along with the associated secrecy capacity. A well-known result from the work of Wyner reveals that, if the eavesdropper has a degraded channel compared with the channel of the intended receiver, then there exists a secrecy rate under which the transmitter can reliably send a secret message to the receiver without the risk of eavesdropping. The work of Wyner was extended to more general nondegraded channels [4].

More recently, the secrecy capacity (rate) of multiple-antenna wiretap channels has received increasing research interests. For multiple-input–single-output–multiple-antenna eavesdropper (MISOME) wiretap channels, [5] shows that the optimal transmission scheme that achieves secrecy capacity admits a beamforming design. Furthermore, the secrecy capacity of multiple-input–multiple-output–multiple-antenna eavesdropper (MIMOME) wiretap channels has been considered in [6]–[8]. Optimizations of a precoding matrix for wiretap channels were further analyzed in [9]–[16]. In addition, transmit designs with imperfect channel knowledge of the eavesdropper have been investigated in [17]–[24].

However, most existing results rely on a critical assumption of Gaussian input signals for deriving transmission precoding aimed at secrecy rate maximization in multiple-antenna wiretap

Manuscript received August 13, 2011; revised December 30, 2011 and March 1, 2012; accepted March 19, 2012. Date of publication April 19, 2012; date of current version July 10, 2012. The work of Y. Wu, X. Gao, and S. Jin was supported in part by the National Natural Science Foundation of China under Grant 60925004, Grant 60902009, and Grant 61101089, the Supporting Program for New Century Excellent Talents in University, and the Scientific Research Foundation of Graduate School, Southeast University. The work of C. Xiao was supported in part by the U.S. National Science Foundation under Grant CCF-0915846. The work of Z. Ding was supported in part by the National Science Foundation under Grant 0520126. This paper will be presented in part at the 2012 IEEE International Conference on Communications (ICC). The review of this paper was coordinated by Prof. J. Chun.

Y. Wu was with Missouri University of Science and Technology, Rolla, MO 65409 USA. He is currently with the National Mobile Communications Research Laboratory, Southeast University, Nanjing 210096, China (e-mail: ypwu@seu.edu.cn).

C. Xiao is with the Department of Electrical and Computer Engineering, Missouri University of Science and Technology, Rolla, MO 65409 USA (e-mail: xiaocmst.edu).

Z. Ding is with the Department of Electrical and Computer Engineering, University of California, Davis, CA 95616 USA, and also with the Southeast University, Nanjing 210096, China (e-mail: zding@ucdavis.edu).

X. Gao and S. Jin are with the National Mobile Communications Research Laboratory, Southeast University, Nanjing 210096, China (e-mail: xqgao@seu.edu.cn; jinshi@seu.edu.cn).

Color versions of one or more of the figures in this paper are available online at http://ieeexplore.ieee.org.

Digital Object Identifier 10.1109/TVT.2012.2195339

channels. Despite the information-theoretic optimality of the Gaussian input, practical signals are non-Gaussian and are often of a finite alphabet. Typically, transmitters utilize phase-shift keying (PSK) or quadrature-amplitude modulation (QAM). In fact, faced with finite-alphabet input constraints, precoding design optimization in practical communication systems may substantially differ from designs that were obtained under the Gaussian input assumption, as shown in basic multiple-input–multiple-output (MIMO) transceiver setups [25]–[33], without wiretapping. Thus, it is of practical interest and importance to examine the effect of discrete finite-alphabet constellations on the secrecy rate of multiple-antenna wiretap channels.

In this paper, we study the design of linear precoding for MIMOME wiretap channels with finite-alphabet input. Similar to the case of Gaussian input, when the transmit power [or signal-to-noise ratio (SNR)] is low, neither the receiver nor the eavesdropper can accurately decode the transmitted data. Hence, the secrecy rate is low at a low SNR (or power). However, unlike the case that involves the Gaussian input, the finite-alphabet input may allow both the receiver and the eavesdropper to accurately decode a transmitted message, given high-enough transmit power. Thus, it is likely that the secrecy rate would not be high at a high SNR.

This phenomenon has been observed in single-input–single-output–single-antenna eavesdropper wiretap channels [34], [35] through simulations. Therefore, [36] suggested to find an optimum power control policy at the transmitter for maximizing the secrecy rate. For multiple-input–single-output–single-antenna eavesdropper (MISOSE) wiretap channels, [36] investigated the power control optimization issue at the transmitter hinged on the conventional beamforming transmission for the Gaussian input case and developed a numerical algorithm to find the optimal transmission power. This idea was extended to MIMOME wiretap channels by exploiting a generalized singular value decomposition (GSVD) precoding structure to decompose the MIMOME channel into a bank of parallel subchannels [37]. Then, numerical algorithms were proposed to obtain the adequate power allocated to each subchannel. Although the precoding design in [37] achieves significant performance gains over the conventional design that relies on the Gaussian input assumption, it is still suboptimal. The reasons are twofold. First, part of the transmission symbols is lost by both the desired user and the eavesdropper according to the GSVD structure. This condition may result in a constant performance loss. Second, the power control policy compels the transmitter to utilize only a fraction of power to transmit in the high-SNR region, which may impede the further improvement of the performance in some scenarios (see [37, Fig. 3] as an example).

This paper investigates the secrecy rate of MIMOME wiretap channels by exploring an important relationship between MIMO mutual information and the receive minimum mean square error (MMSE). For scenarios where the instantaneous channel-state information (CSI) of the eavesdropper is available at the transmitter, we establish necessary conditions of the optimal transmit precoding design for the finite-alphabet input based on the Karush–Kuhn–Tucker (KKT) analysis and develop an iterative algorithm for secrecy rate maximization through a gradient method. We adopt the backtracking line search algorithm [40] to regulate the convergence speed. We show that this iterative algorithm achieves substantial rate gains over the GSVD-based precoding design in [37]. Then, we analyze the optimal transmission design in asymptotic-SNR regions. We prove that, at a low SNR, the beamforming design is the optimal transmission scheme and the maximum available power is needed. We further find that, when the number of transmit antennas is larger than the number of the eavesdropper's antennas, the *nonbeamforming* transmit precoding along the null space of the channel matrix of the eavesdropper achieves the optimal performance for the finite-alphabet input data at a high SNR and the power control policy in [37] is *unnecessary*. Interestingly, this finding also holds for the MISOME wiretap channels, which is a sharp contrast to the optimal beamforming precoding structure under the Gaussian input assumption [5]. For systems where the number of transmit antennas is less than or equal to the number of the eavesdropper's antennas, only partial transmission power is necessary for maximizing the secrecy rate at a high SNR. Accordingly, we utilize the excess unused transmission power to construct an artificial jamming signal to further improve the secrecy rate. Finally, by invoking a recent lower bound of the average mutual information in fading MIMO channels with the finite-alphabet input [38], we extend our study to scenarios where the transmitter only has the statistical CSI of the eavesdropper.

The reminder of this paper is organized as follows. Section II describes the mathematical model under consideration. In Section III, we establish necessary conditions of the optimal precoding design when the transmitter completely possesses the instantaneous CSI of the eavesdropper, and we propose an iterative algorithm to determine the precoding matrix. In addition, theoretical results on the transmission design for maximizing the secrecy rate in low- and high-SNR regions are analyzed. A new artificial jamming signal design to additionally increase the secrecy rate performance is further investigated in Section III. The precoding design that relies on the statistical CSI of the eavesdropper is studied in Section IV. Numerical results are provided in Section V before the conclusions in Section VI. All of the major mathematical proofs are provided in Appendices.

The following are adopted throughout this paper. Vectors are represented as columns and are denoted in lowercase boldface letters, and matrices are represented in uppercase boldface letters. The superscripts $(\cdot)^T$, $(\cdot)^*$, and $(\cdot)^h$ stand for the matrix transpose, conjugate, and conjugate–transpose operations, respectively. We use $\mathrm{tr}(\mathbf{A})$ and $\mathbf{A}^{-1}$ to denote the trace operation and the inverse of matrix $\mathbf{A}$, respectively, and $\|\cdot\|$ denotes the Euclidean norm of a vector. The $M \times M$ identity matrix is denoted by $\mathbf{I}_M$, and the all-zero matrix is denoted by $\mathbf{0}$. The complex number field is represented by $\mathbb{C}$, and $E[\cdot]$ evaluates the expectation of all the random variables within the bracket.

II. System Model

We consider the MIMOME model where the transmitter (Alice), the intended receiver (Bob), and the eavesdropper (Eve) all have multiple antennas, with antenna numbers of N_t, N_r,

and N_e, respectively. Bob and Eve receive signals $\mathbf{y}_b$ and $\mathbf{y}_e$, respectively, which can be represented as

$$\mathbf{y}_b = \mathbf{H}_{ba}\mathbf{G}\mathbf{x}_a + \mathbf{v}_b \tag{1}$$

$$\mathbf{y}_e = \mathbf{H}_{ea}\mathbf{G}\mathbf{x}_a + \mathbf{v}_e \tag{2}$$

where $\mathbf{x}_a \in \mathbb{C}^{N_t \times 1}$ is the transmitted signal vector with zero mean and identity covariance matrix, and $\mathbf{H}_{ba} \in \mathbb{C}^{N_r \times N_t}$ and $\mathbf{H}_{ea} \in \mathbb{C}^{N_e \times N_t}$ are the channel matrices from the perspective of the receiver and the eavesdropper, respectively. The effective MIMO channel noises $\mathbf{v}_b \sim \mathcal{CN}(0, \sigma_b^2 \mathbf{I}_{N_r})$ and $\mathbf{v}_e \sim \mathcal{CN}(0, \sigma_e^2 \mathbf{I}_{N_e})$ denote complex independent and identically distributed (i.i.d.) channel noise vectors. $\mathbf{G} \in \mathbb{C}^{N_t \times N_t}$ is a linear precoding matrix whose secrecy rate we seek to optimize. The precoding matrix does not increase the transmission power. Hence, we have the power constraint as

$$\mathrm{tr}\left\{E\left[\mathbf{G}\mathbf{x}_a\mathbf{x}_a^h\mathbf{G}^h\right]\right\} = \mathrm{tr}\{\mathbf{G}\mathbf{G}^h\} \le N_t. \tag{3}$$

Moreover, the average SNR at the intended receiver side is given by

$$\mathrm{SNR}_b = \frac{\mathrm{tr}\left(\mathbf{H}_{ba}\mathbf{H}_{ba}^h\right)}{N_r\sigma_b^2}. \tag{4}$$

We assume that the instantaneous CSI of the intended receiver is available at the transmitter. For the eavesdropper, we consider the following two cases, which rely on the type of CSI known at the transmitter.

1) The transmitter has the instantaneous perfect knowledge of the eavesdropper's channel. Then, the average SNR at the eavesdropper side is given by[1]

$$\mathrm{SNR}_{e,i} = \frac{\mathrm{tr}\left(\mathbf{H}_{ea}\mathbf{H}_{ea}^h\right)}{N_e\alpha\sigma_b^2} \tag{5}$$

where we define $\alpha = \sigma_e^2/\sigma_b^2$. Here, we normalize the MIMO channels of the receiver and the eavesdropper as $\mathrm{tr}(\mathbf{H}_{ba}\mathbf{H}_{ba}^h) = N_t$ and $\mathrm{tr}(\mathbf{H}_{ea}\mathbf{H}_{ea}^h) = N_t$, respectively. Then, the secrecy capacity has the expression of [7]

$$C_{\mathrm{sec}}(\mathbf{G}) = \max_{\mathrm{tr}(\mathbf{G}\mathbf{G}^h)\le N_t} \{R(\mathbf{G})\} \tag{6}$$

$$R(\mathbf{G}) = I(\mathbf{y}_b;\mathbf{x}_a)I(\mathbf{y}_e;\mathbf{x}_a) \tag{7}$$

where $I(\mathbf{y};\mathbf{x})$ represents the mutual information function between input $\mathbf{x}$ and output $\mathbf{y}$.

2) The transmitter knows the statistical distribution of the eavesdropper's channel. Then, the average SNR at the eavesdropper side is given by

$$\mathrm{SNR}_{e,s} = \frac{E\left[\mathrm{tr}\left(\mathbf{H}_{ea}\mathbf{H}_{ea}^h\right)\right]}{N_e\alpha\sigma_b^2}. \tag{8}$$

[1]The path between "Alice and Bob" is independent of the path between "Alice and Eve." Thus, at the Bob and Eve sides, the SNR should separately be evaluated.

We model $\mathbf{H}_{ea}$ as the doubly correlated fading MIMO channels, i.e.,

$$\mathbf{H}_{ea} = \frac{1}{\sqrt{N_e}}\mathbf{R}_{N_e}^{1/2}\mathbf{H}_w\mathbf{R}_{N_t}^{1/2} \tag{9}$$

where $\mathbf{H}_w$ is a complex random matrix with independent random entries following $\mathcal{CN}(0,1)$. The matrices $\mathbf{R}_{N_t} \in \mathbb{C}^{N_t \times N_t}$ and $\mathbf{R}_{N_e} \in \mathbb{C}^{N_e \times N_e}$ denote the transmit and receive correlation matrices of the eavesdropper channels, respectively. In addition, we normalize the MIMO channels of the receiver as $\mathrm{tr}(\mathbf{H}_{ba}\mathbf{H}_{ba}^h) = N_t$. The ergodic secrecy rate is given by [36]

$$R_{\mathrm{erg-sec}}(\mathbf{G}) = \max_{\mathrm{tr}(\mathbf{G}\mathbf{G}^h)\le N_t} \{R_{\mathrm{erg}}((\mathbf{G}))\} \tag{10}$$

$$R_{\mathrm{erg}}(\mathbf{G}) = I(\mathbf{y}_b;\mathbf{x}_a) - E\left[I(\mathbf{y}_e;\mathbf{x}_a)\right]. \tag{11}$$

Our design objective of transmit precoding is to find the optimum $\mathbf{G}$ to maximize (7) or (11).

III. Transmit Precoding With the Instantaneous Channel-State Information of the Eavesdropper

In this section, we investigate the transmit precoding when the instantaneous CSI of the eavesdropper is available at the transmitter. We begin by establishing necessary conditions of the optimal design and develop a numerical algorithm to iteratively optimize the precoder $\mathbf{G}$. Then, we study the precoding design in asymptotic-SNR regions.

A. Necessary Conditions for Optimum Transmit Precoding

Generally, transmitted signals are generated as equiprobable symbols from discrete constellations such as M-ary QAM. For M-ary data input, the expressions of mutual information in (7) are given by [33]

$$I(\mathbf{y}_b;\mathbf{x}_a) = N_t\log_2 M - \frac{1}{M^{N_t}} \times \sum_{m=1}^{M^{N_t}} E_{\mathbf{v}_b}\left\{\log_2 \sum_{k=1}^{M^{N_t}} \exp\left(\frac{-f_{b,m,k} + \|\mathbf{v}_b\|^2}{\sigma_b^2}\right)\right\} \tag{12}$$

$$I(\mathbf{y}_e;\mathbf{x}_a) = N_t\log_2 M - \frac{1}{M^{N_t}} \times \sum_{m=1}^{M^{N_t}} E_{\mathbf{v}_e}\left\{\log_2 \sum_{k=1}^{M^{N_t}} \exp\left(\frac{-f_{e,m,k} + \|\mathbf{v}_e\|^2}{\alpha\sigma_b^2}\right)\right\} \tag{13}$$

where we denote $f_{b,m,k} = \|\mathbf{H}_{ba}\mathbf{G}(\mathbf{x}_m - \mathbf{x}_k) + \mathbf{v}_b\|^2$ and $f_{e,m,k} = \|\mathbf{H}_{ea}\mathbf{G}(\mathbf{x}_m - \mathbf{x}_k) + \mathbf{v}_e\|^2$. Here, M is the number of points in the signal constellation, whereas $\mathbf{x}_k$ consists of N_t independent symbols from the M-ary constellation $\mathcal{A}$.

Our objective is to develop an algorithm for solving the linear precoding matrix $\mathbf{G}$, under the power constraint[2] $\mathrm{tr}\{\mathbf{G}\mathbf{G}^h\} \leq N_t$, by maximizing the secrecy rate in (7). Here, we define the complex gradient operator as $\nabla_{\mathbf{G}} f = \partial f / \partial \mathbf{G}^*$ [39]. Then, based on the KKT conditions [40], we obtain necessary conditions for the optimal $\widetilde{\mathbf{G}}$ as follows.

Proposition 1: The optimal precoder $\widetilde{\mathbf{G}}$, which maximizes the secrecy rate given in (7), satisfies the following conditions:

$$\mathbf{H}_{ba}^h \mathbf{H}_{ba} \widetilde{\mathbf{G}} \boldsymbol{\Sigma}_b(\widetilde{\mathbf{G}}) \frac{\log_2 e}{\sigma_b^2} - \mathbf{H}_{ea}^h \mathbf{H}_{ea} \widetilde{\mathbf{G}} \boldsymbol{\Sigma}_e(\widetilde{\mathbf{G}}) \frac{\log_2 e}{\alpha \sigma_b^2} = \theta \widetilde{\mathbf{G}} \tag{14}$$

$$\theta \left(\mathrm{tr}(\widetilde{\mathbf{G}}\widetilde{\mathbf{G}}^h) - N_t \right) = 0 \tag{15}$$

$$\theta \geq 0 \tag{16}$$

$$\mathrm{tr}(\widetilde{\mathbf{G}}\widetilde{\mathbf{G}}^h) - N_t \leq 0. \tag{17}$$

Note that $\boldsymbol{\Sigma}_b(\cdot)$ and $\boldsymbol{\Sigma}_e(\cdot)$ are known as the MMSE matrices [41]. More particularly, we note that

$$\boldsymbol{\Sigma}_b(\mathbf{G}) = E\left[(\mathbf{x} - E[\mathbf{x}|\mathbf{y}_b]) (\mathbf{x} - E[\mathbf{x}|\mathbf{y}_b])^h \right] \tag{18}$$

$$\boldsymbol{\Sigma}_e(\mathbf{G}) = E\left[(\mathbf{x} - E[\mathbf{x}|\mathbf{y}_e]) (\mathbf{x} - E[\mathbf{x}|\mathbf{y}_e])^h \right]. \tag{19}$$

Proof: See Appendix A. ■

B. Algorithm for Precoder Optimization

In general, finding a closed-form expression for the optimal solution $\widetilde{\mathbf{G}}$ based on Proposition 1 is a difficult task, if not intractable. The problems are complex because of their nonconvexity and highly expansive representation. Indeed, the ensemble average $E\{\cdot\}$ in (18) and (19) for finite-alphabet input requires averaging over all M^{N_t} possible combinations of input data sequences and poses a serious challenge. In this paper, we focus on the numerical algorithm to iteratively search for the optimal $\widetilde{\mathbf{G}}$.

Among various numerical iterative algorithms, the gradient descent method searches for the optimal solution along the decent direction and performs *linear convergence* behaviors [40]. Therefore, we apply the gradient descent method by utilizing the partial mutual information derivatives of $\mathbf{G}$, which are specified by the left term of (14). We incorporate the backtracking line search algorithm in [40] for fast convergence. Moreover, based on the conclusion in [41], if the obtained solution satisfies $\mathrm{tr}\{\mathbf{G}\mathbf{G}^h\} > N_t$, we can project $\mathbf{G}$ to the feasible set through a normalization step: $\mathbf{G} := \sqrt{N_t}\mathbf{G}/\sqrt{\mathrm{tr}(\mathbf{G}\mathbf{G}^h)}$. Then, an optimization algorithm can be developed to maximize the secrecy rate (7).

Algorithm 1: Gradient descent for maximizing the secrecy rate (7) over $\mathbf{G}$ with arbitrary N_t, N_r, and N_e.

Step 1: Initialize $\mathbf{G}_1$ with constraints $\mathrm{tr}(\mathbf{G}_1\mathbf{G}_1^h) \leq N_t$. Set step size $u = u_{\mathrm{int}}$, and set the minimum tolerance step size $u_{\min}$.
Step 2: Set $k = 1$ and compute the secrecy rate $R_1 = R(\mathbf{G}_1)$.
Step 3: Compute the gradient value $\nabla_{\mathbf{G}_k} R(\mathbf{G})$.
Step 4: If $u > u_{\min}$, go to **step 5**. Otherwise, return $\mathbf{G}_k$ and R_k, and stop the algorithm.
Step 5: Calculate $\mathbf{G}'_k = \mathbf{G}_k + u\nabla_{\mathbf{G}_k} R(\mathbf{G}, \gamma)$. If $\mathrm{tr}(\mathbf{G}'_k(\mathbf{G}'_k)^h) > N_t$, set $\mathbf{G}'_k := \sqrt{N_t}\mathbf{G}'_k / \sqrt{\mathrm{tr}(\mathbf{G}'_k(\mathbf{G}'_k)^h)}$.
Step 6: Compute $R' = R(\mathbf{G}'_k)$.
Step 7: If $R' > R_k$, update $R_{k+1} = R'$, $\mathbf{G}_{k+1} = \mathbf{G}'_k$, and $u = u_{\mathrm{int}}$. Go to **step 8**. Otherwise, let $u = 1/2u$ and go to **step 4**.
Step 8: $k := k + 1$. Go to **step 3** until the stopping criterion is reached.

Note that Algorithm 1 iterates over $\mathbf{G}$, in each step increasing the secrecy rate in (7). Based on the expressions in (12) and (13), we know that the secrecy rate in the context of the finite-alphabet input in (7) is upper bounded. This case implies that Algorithm 1, which produces increasing sequences that are upper bounded, is convergent. To avoid the algorithm converging to a local optimum, we randomly initialize $\mathbf{G}_1$ multiple times and choose the resulting precoder that achieves the maximum secrecy rate of (7) [8], [42], [43].

C. Precoding in Asymptotic-SNR Regions

In this section, we derive analytical expressions for the optimal transmit design in extreme-SNR regions. For an arbitrary precoder $\mathbf{G}$, we define $\mathrm{tr}(\mathbf{G}\mathbf{G}^h) = \gamma N_t$, where $0 \leq \gamma \leq 1$ is the power allocation factor that indicates the ratio of the available power used for transmission at the transmitter. Then, the following results hold.

Proposition 2: The optimal precoder $\widetilde{\mathbf{G}}_L$ that maximizes the secrecy rate (7) in the low-SNR region[3] is given by

$$\widetilde{\mathbf{G}}_L = H(\lambda_{\max})\sqrt{N_t}\left[\mathbf{v}_{\max} \quad \mathbf{0}_{N_t \times (N_t - 1)}\right] \tag{20}$$

where $\lambda_{\max}$ is the largest eigenvalue of the matrix $\boldsymbol{\Omega} = \mathbf{H}_{ba}^h \mathbf{H}_{ba} - 1/\alpha \mathbf{H}_{ea}^h \mathbf{H}_{ea}$, and $\mathbf{v}_{\max}$ is the corresponding unit-norm eigenvector. $H(\cdot)$ is the Heaviside step function where $H(x) = 1$ when $x > 0$ and $H(x) = 0$ elsewhere.

Proof: See Appendix B. ■

[2]We know that, for point-to-point MIMO scenarios, utilizing full power for transmission achieves the optimum performance [33]. However, for wiretap channels, increasing the power of the precoder $\mathbf{G}$ may enhance the rates of both the receiver and the eavesdropper. Thus, the equality in (3) is not guaranteed to be fulfilled for wiretap channels.

[3]In this paper, we refer to the low-SNR region as $\sigma_b^2 \to \infty$, $\sigma_e^2 \to \infty$, and with fixed α.

Proposition 2 characterizes the optimal transmission design in the low-SNR region. We observe from Proposition 2 that the beamforming transmission along the strongest eigenmode of the "effective" channel $\mathbf{H}_{ba}^h\mathbf{H}_{ba} - 1/\alpha\mathbf{H}_{ea}^h\mathbf{H}_{ea}$ is optimal in the low-SNR case, which is similar to the conclusions in single-user systems (without wiretapping) [29], [44]–[46]. Moreover, it is revealed in Proposition 2 that, when the SNR is low and $\lambda_{\max} > 0$, it is optimal to use all the available power to transmit with finite-alphabet input signals.

Proposition 3: The optimal precoder $\widetilde{\mathbf{G}}_H$ that maximizes the secrecy rate (7) in the high-SNR region ($\sigma_b^2 \to 0$) when $N_t > N_e$ satisfies the following structure:

$$\widetilde{\mathbf{G}}_H = \mathbf{V}_e\mathbf{P} \tag{21}$$

where $\mathbf{V}_e \in \mathbb{C}^{N_t\times(N_t-N_e)}$ is an orthonormal basis of the null space of $\mathbf{H}_{ea}$, and $\mathbf{P} \in \mathbb{C}^{(N_t-N_e)\times N_t}$ fulfils the power constraint $\mathrm{tr}(\mathbf{P}\mathbf{P}^h) = N_t$.

Proof: See Appendix C. ■

Proposition 3 demonstrates an appealing result that, when $N_t > N_e$, utilizing *all* the available power to transmit is still optimal at a high SNR and the secrecy rate will saturate at $N_t \log_2 M$ b/s/Hz as the SNR increases. This case is because, for the finite-alphabet input, when $N_t > N_e$, there are enough dimensions at the transmitter to construct a precoder to effectively suppress the achievable rate of the eavesdropper to zero. Then, the useful signals can be transmitted in the remaining dimensions with full power.

Based on the precoding structure in (21), we can design a low-complexity null-space algorithm to search for the precoder $\widehat{\mathbf{G}}$ as follows.

Algorithm 2: Low-complexity null-space algorithm for maximizing the secrecy rate (7) over $\mathbf{G}$ with $N_t > N_e$.

Step 1: Calculate $\mathbf{V}_e$ as the orthonormal basis of the null space of $\mathbf{H}_{ea}$.
Step 2: Set $f_{b,m,k} = \|\mathbf{H}_{ba}\mathbf{V}_e\mathbf{P}(\mathbf{x}_m - \mathbf{x}_k) + \mathbf{v}_b\|^2$.
Step 3: Set $\mathbf{H}_{ba,\mathrm{eff}} = \mathbf{H}_{ba}\mathbf{V}_e$ as the effective channel for the intended receiver.
Step 4: Find the optimal $\widehat{\mathbf{P}}$ that maximizes (12) by algorithms in conventional point-to-point MIMO scenarios under the finite-alphabet input assumption.
Step 5: Set the precoder $\widehat{\mathbf{G}} = \mathbf{V}_e\widehat{\mathbf{P}}$.

The computation complexity of Algorithm 2 is considerably lower than Algorithm 1, because it iteratively searches for the optimal $\widehat{\mathbf{P}}$ based solely on the mutual information of the intended receiver (12). In addition, the optimization in step 4 can be performed through various highly efficient algorithms for point-to-point MIMO scenarios with the finite-alphabet input (for example, see [32], [33], and the references therein). Based on Proposition 3, we know that Algorithm 2 is asymptotically optimal in the high-SNR region. Numerical results in Section V illustrate that Algorithm 2 also achieves robust performances at moderate SNRs.

When $N_t \le N_e$, the null space of $\mathbf{H}_{ea}$ does not exist. Hence, both the receiver and the eavesdropper may accurately decode the transmitted message, given high-enough transmit power. In this case, only a portion of the available power is needed for the optimal transmission. We utilize the remaining unused power to transmit a jamming signal along the null space of $\mathbf{H}_{ba}$ to further improve the secrecy rate. Here, we provide a novel method for constructing the jamming signal. Given the assumption that the instantaneous CSI is available at the transmitter, we can generate an equivalent jamming that lies in the direction of the channel noise $\mathbf{v}_e$. This approach is more effective in suppressing the achievable rate of the eavesdropper. Details of the algorithm are given as follows.

Algorithm 3: Algorithm with additional jamming for maximizing the secrecy rate (7) with $N_t \le N_e$.

Step 1: Compute $\widetilde{\mathbf{G}}$ through Algorithm 1.
Step 2: Calculate $\mathbf{V}_b$ as the orthonormal basis of the null of $\mathbf{H}_{ba}$.
Step 3: Calculate the singular value decomposition (SVD) as

$$\mathbf{H}_{ea}\mathbf{V}_b = \mathbf{U}_{\mathrm{jam}}\begin{bmatrix}\mathbf{\Lambda}_{\mathrm{jam}} & \mathbf{0}\\ \mathbf{0} & \mathbf{0}\end{bmatrix}\mathbf{V}_{\mathrm{jam}}^h.$$

Step 4: Design the jamming precoder:

$$\mathbf{G}_{\mathrm{jam}}^{\mathrm{new}} = \sqrt{\beta}\mathbf{V}_b\mathbf{V}_{\mathrm{jam}}\begin{bmatrix}\mathbf{\Lambda}_{\mathrm{jam}}^{-1} & \mathbf{0}\\ \mathbf{0} & \mathbf{0}\end{bmatrix}$$

where β is the coefficient to fulfill the power constraint $\mathrm{tr}(\mathbf{G}_{\mathrm{jam}}^{\mathrm{new}}(\mathbf{G}_{\mathrm{jam}}^{\mathrm{new}})^h) = N_t - \mathrm{tr}(\widetilde{\mathbf{G}}\widetilde{\mathbf{G}}^h)$.
Step 5: Generate the artificial noise $\mathbf{u} \sim \mathcal{CN}(\mathbf{0}, \mathbf{I}_{N_t-N_r})$.
Step 6: Construct the precoded signal:

$$\mathbf{G}\mathbf{x}_a = \widetilde{\mathbf{G}}\mathbf{x}_a + \mathbf{G}_{\mathrm{jam}}^{\mathrm{new}}\mathbf{u}$$

We define r as the rank of the matrix $\mathbf{H}_{ea}\mathbf{V}_b$. Based on the design of Algorithm 3 and the equality in [47, eq. (9.67)], the equivalent model between the transmitter and the eavesdropper can be expressed as

$$\mathbf{y}_e' = \mathbf{U}_{\mathrm{jam}}^h\mathbf{H}_e\widetilde{\mathbf{G}}\mathbf{x}_a + \mathbf{n_e} \tag{22}$$

where $\mathbf{n_e}$ is the $N_e \times 1$ zero-mean Gaussian noise vector with covariance matrix

$$\mathbf{\Sigma}_{n_e} = \begin{bmatrix}\left(\beta + \alpha\sigma_b^2\right)\mathbf{I}_r & 0\\ 0 & \alpha\sigma_b^2\mathbf{I}_{N_e-r}\end{bmatrix}. \tag{23}$$

According to the definition of the conditional entropy and the mutual information [47], we can easily obtain the mutual information rate between $\mathbf{x}_a$ and $\mathbf{y}_e'$ as $I(\mathbf{y}_e'; \mathbf{x}_a)$, given in (24), shown at the bottom of the next page.

Then, we can evaluate the secrecy rate after jamming as

$$R\left(\widetilde{\mathbf{G}}, \mathbf{G}_{\mathrm{jam}}^{\mathrm{new}}\right) = I(\mathbf{y}_b; \mathbf{x}_a) - I\left(\mathbf{y}_e'; \mathbf{x}_a\right). \tag{25}$$

We note from (23) that the jamming design directly heightens the energy of the noise $\mathbf{v}_e$ in the first rth dimension. This will result in a further decrease of the achievable rate of the eavesdropper in (24), which in turn yields a promotion of the secrecy rate in (25).

IV. Transmit Precoding With the Statistical Channel-State Information of the Eavesdropper

We now turn our attention to the scenarios where only the statistical CSI of eavesdropper is available at the transmitter. Due to the prohibitive computations of directly evaluating the expectation in (11), we resort to designing the precoder $\widetilde{\mathbf{G}}$ in terms of an upper bound. We start by employing a lower bound[4] of the average mutual information in doubly correlated fading MIMO channels [38] to obtain

$$R_{\mathrm{erg}}(\mathbf{G}) \le R_{\mathrm{erg,UB}}(\mathbf{G}) = I(\mathbf{y}_b;\mathbf{x}_a) - I_{\mathrm{LB}}(\mathbf{y}_e;\mathbf{x}_a) \quad (26)$$

where

$$I_{\mathrm{LB}}(\mathbf{y}_e;\mathbf{x}_a) = N_t \log M - N_e\left(\frac{1}{\ln 2}-1\right) - \frac{1}{M^{N_t}} \times \sum_{m=1}^{M^{N_t}} \log \sum_{k=1}^{M^{N_t}} \prod_{p=1}^{N_e} \left(1+\frac{r_p}{2N_e\alpha\sigma_b^2}\mathbf{b}_{mk}^h\mathbf{G}^h\mathbf{R}_{N_t}\mathbf{G}\mathbf{b}_{mk}\right)^{-1} \quad (27)$$

in which $\mathbf{b}_{mk} = \mathbf{x}_m - \mathbf{x}_k$, and r_p represents the pth diagonal element of $\mathbf{R}_{N_e}$. By exploiting the complex matrix differentiation technique in [48], [49], the gradient of $R_{\mathrm{erg,UB}}(\mathbf{G})$ with respect to $\mathbf{G}$ is given by

$$\nabla_{\mathbf{G}} R_{\mathrm{erg,UB}}(\mathbf{G}) = \frac{\log_2 e}{\sigma_b^2}\left[\mathbf{H}_{ba}^h\mathbf{H}_{ba}\mathbf{G}\boldsymbol{\Sigma}_b(\mathbf{G}) - \frac{1}{2N_e\alpha M^{N_t}} \times \sum_{m=1}^{M^{N_t}}\sum_{k=1}^{M^{N_t}} g_m t_{mk} \prod_{p=1}^{N_e} \omega_{mkp}\mathbf{R}_t\mathbf{G}\mathbf{b}_{mk}\mathbf{b}_{mk}^h\right] \quad (28)$$

where

$$g_m = \left[\sum_{k=1}^{M^{N_t}}\prod_{p=1}^{N_e}\left(1+\frac{r_p}{2N_e\alpha\sigma_b^2}\mathbf{b}_{mk}^h\mathbf{G}^h\mathbf{R}_t\mathbf{G}\mathbf{b}_{mk}\right)^{-1}\right]^{-1} \quad (29)$$

[4]The effectiveness and the accuracy of the precoding design based on this low bound have been investigated and validated in [38] for various scenarios.

$$\omega_{mkp} = \left(1+\frac{r_p}{2N_e\alpha\sigma_b^2}\mathbf{b}_{mk}^h\mathbf{G}^h\mathbf{R}_t\mathbf{G}\mathbf{b}_{mk}\right)^{-1} \quad (30)$$

and $t_{mk} = \sum_{p=1}^{N_e} r_p\omega_{mkp}$.

In addition, it is intractable to construct a precoder to make the eavesdropper's rate to zero in the context of the statistical CSI of the eavesdropper. Thus, excessive power will be available at the transmitter to form an additional jamming signal at a high SNR. When the transmitter does not have complete knowledge of $\mathbf{H}_{ea}$, we send the jamming signal along all directions orthonormal to the intended receiver channels $\mathbf{H}_{ba}$ [50]. To summarize, we perform the following precoding design:

Algorithm 4: Algorithm to maximize the secrecy rate (11) through the statistical CSI of the eavesdropper.

Step 1: Compute $\widetilde{\mathbf{G}}$ through Algorithm 1 by replacing: $R(\mathbf{G})$ and $\nabla_{\mathbf{G}}R(\mathbf{G})$ with $R_{\mathrm{erg,UB}}(\mathbf{G})$ and $\nabla_{\mathbf{G}}R_{\mathrm{erg,UB}}(\mathbf{G})$, respectively.
Step 2: Calculate $\mathbf{V}_b$ as the orthonormal basis of the null space of $\mathbf{H}_{ba}$.
Step 3: Generate the artificial noise $\mathbf{u} \sim \mathcal{CN}(\mathbf{0}, \mathbf{I}_{N_t-N_r})$.
Step 4: Construct the precoded signal:

$$\mathbf{G}\mathbf{x}_a = \widetilde{\mathbf{G}}\mathbf{x}_a + \sqrt{\left(N_t - \mathrm{tr}(\widetilde{\mathbf{G}}\widetilde{\mathbf{G}}^h)\right)/(N_t-N_r)}\mathbf{V}_b\mathbf{u}.$$

V. Numerical Results

This section provides several different examples to demonstrate the benefits of the precoding designs and to illustrate the efficacy of the proposed algorithms. In all these examples, we normalize the channels for the receiver and the eavesdropper as in Section II.

A. Scenarios With the Instantaneous CSI of the Eavesdropper

First, we examine the precoding design in Algorithm 1 for the MISOSE channels. We consider Example 1 as following[5]:

$$\mathbf{h}_{ba} = [0.0991 - 0.8676i \quad 1.0814 + 1.1281i] \quad (31)$$

$$\mathbf{h}_{ea} = [0.3880 + 1.2024i \quad -0.9825 + 0.5914i]. \quad (32)$$

Fig. 1 illustrates the secrecy rate results of Example 1 under finite-alphabet constraints achieved for different modulations and $\alpha = 1$. We compare the precoding designs in Algorithm 1 with the GSVD-based design in [37], which we denote as "Finite Alphabet, Algorithm 1" and "Finite Alphabet, GSVD

[5]Note that Example 1 was also considered in [5].

$$I(\mathbf{y}_e';\mathbf{x}_a) = N_t\log_2 M - \sum_{m=1}^{M^{N_t}} E_{\mathbf{n}_e}\log_2\sum_{k=1}^{M^{N_t}}\exp\left(-\left\|\boldsymbol{\Sigma}_{n_e}^{-1/2}\left(\mathbf{U}_{\mathrm{jam}}^h\mathbf{H}_e\widetilde{\mathbf{G}}(\mathbf{x}_m-\mathbf{x}_k)+\mathbf{n}_e\right)\right\|^2 + \left\|\boldsymbol{\Sigma}_{n_e}^{-1/2}\mathbf{n}_e\right\|^2\right) \quad (24)$$

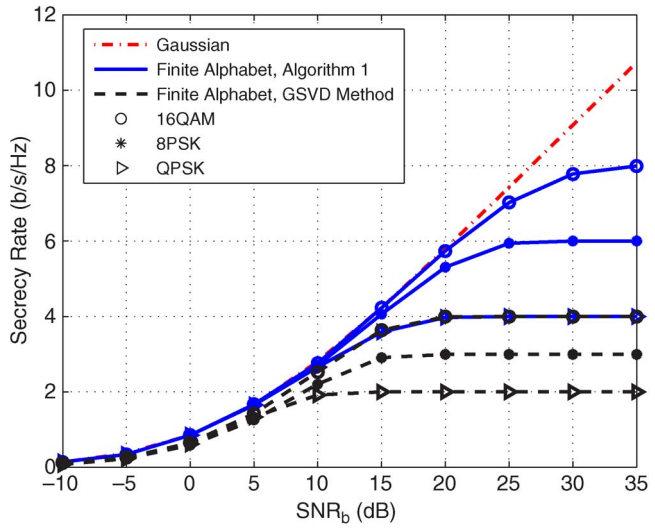


Fig. 1. Secrecy rate of the MISOSE channels (31) and (32) with different designs and modulations.

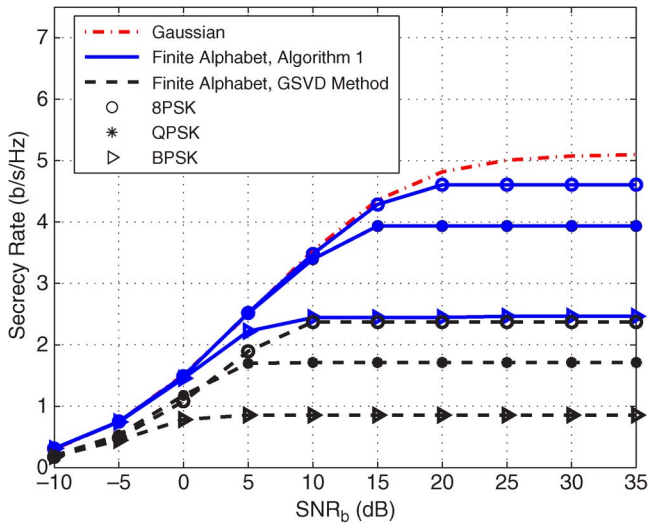


Fig. 2. Secrecy rate of the MISOME channels (36) and (37) with different designs and modulations.

Method," respectively. The secrecy capacity with the Gaussian input is also provided as a benchmark comparison. We observe from Fig. 1 that the GSVD-based design may lead to noticeable performance losses (in terms of secrecy rate), particularly in the moderate-to-high-SNR region. This case is because, in the context of the GSVD structure, there is only one effective subchannel for Example 1 and the precoding design in [37] allocates all the available power to this subchannel. Thus, the GSVD-based design performs as a beamforming precoding for Example 1, which will result in a constant performance loss $\log_2 M$ b/s/Hz at a high SNR. Algorithm 1, in contrast, achieves superior performance for different modulations over large-SNR regions and saturates at $N_t \log_2 M$ b/s/Hz in the high-SNR region, as expected.

It has been shown in [5] that the secrecy capacity in the MISOME (including MISOSE) model with the Gaussian input is achieved by a beamforming eigenvector that corresponds to the largest generalized eigenvalue of $(\mathbf{H}_{ba}, \mathbf{H}_{ea})$. Here, we illustrate the final precoding matrix $\mathbf{G}$ from Algorithm 1, given quadrature phase-shift keying (QPSK) inputs at the following two different SNR levels.

1) SNR$_b = 5$ dB

$$\mathbf{G}_1 = \begin{bmatrix} 0.5342 + 0.1959i & -0.3405 - 0.5196i \\ -0.5700 + 0.5188i & 0.8302 - 0.0841i \end{bmatrix}. \quad (33)$$

2) SNR$_b = 30$ dB

$$\mathbf{G}_2 = \begin{bmatrix} 0.5748 + 0.3465i & -0.3096 - 0.5976i \\ -0.5159 + 0.5297i & 0.7188 - 0.1823i \end{bmatrix}. \quad (34)$$

We now verify the optimality of the obtained precoders. By setting $\theta_1 = 0.8181$ and $\theta_2 = 0$, it holds that

$$\nabla_{\mathbf{G}_1} R(\mathbf{G}) \simeq \theta_1 \mathbf{G}_1 \quad \nabla_{\mathbf{G}_2} R(\mathbf{G}) = \theta_2 \mathbf{G}_2 \quad (35)$$

which indicates that $\mathbf{G}_1$ and $\mathbf{G}_2$ satisfy the necessary conditions (14)–(17). Moreover, (33) and (34) imply that, for MISOSE channels, the optimal precoding matrix follows the *nonbeamforming* structure in the medium-to-high-SNR region and the beamforming design, which is optimal for the Gaussian input, is no longer optimal for the finite-alphabet input. This condition reveals that optimum precoding design criteria for the finite-alphabet input substantially differ from cases that involve the conventional Gaussian input.

Second, we verify the precoding design in Algorithm 1 for MISOME channels. We consider Example 2, which is given by

$$\mathbf{h}_{ba} = [0.51 - 0.32i \quad -0.89 - 0.03i \quad -0.55 - 0.04i] \quad (36)$$

$$\mathbf{H}_{ea} = \begin{bmatrix} -0.08 + 0.14i & -0.10 - 0.10i & 0.00 - 0.07i \\ -0.04 - 0.12i & 0.16 - 0.11i & -0.08 + 0.15i \\ 0.14 - 0.04i & -0.08 - 0.06i & -0.00 + 0.11i \end{bmatrix}. \quad (37)$$

Fig. 2 depicts the secrecy rate performances of Example 2 under finite-alphabet constraints with different precoding designs, different modulations, and $\alpha = 1$. We also plot the Gaussian input secrecy capacity as a reference. Again, the GSVD-based design will result in lower secrecy rates, whereas Algorithm 1 achieves much better performance. Moreover, the performances of Algorithm 1 exceed $\log_2 M$ b/s/Hz in the high-SNR region for all the modulations, which is the upper bound for the optimal beamforming design under the Gaussian input formulas. To further exemplify this case, we present the final precoding matrix $\mathbf{G}$ in Algorithm 1, given binary phase-shift keying (BPSK) inputs at SNR$_b = 5$ dB, i.e.,

$$\mathbf{G}_3 = \begin{bmatrix} 0.52 + 0.15i & 0.36 - 0.24i & 0.06 - 0.55i \\ 0.17 + 0.60i & 0.45 + 0.20i & 0.57 - 0.26i \\ 0.21 + 0.64i & 0.49 + 0.19i & 0.60 - 0.31i \end{bmatrix}. \quad (38)$$

Again, by setting $\theta_3 = 0.5289$, we have $\nabla_{\mathbf{G}_3} R(\mathbf{G}) \simeq \theta_3 \mathbf{G}_3$. Thus, $\mathbf{G}_3$ fulfills the necessary conditions (14)–(17). We observe that the precoding matrix in (38) is not a beamforming matrix, confirming that the optimality of the beamforming design for MISOME channels under the Gaussian input assumption no longer holds for the finite-alphabet input.

Figs. 3 and 4 illustrate the convergence behaviors of Algorithm 1 under different modulations for Examples 1 and 2 at

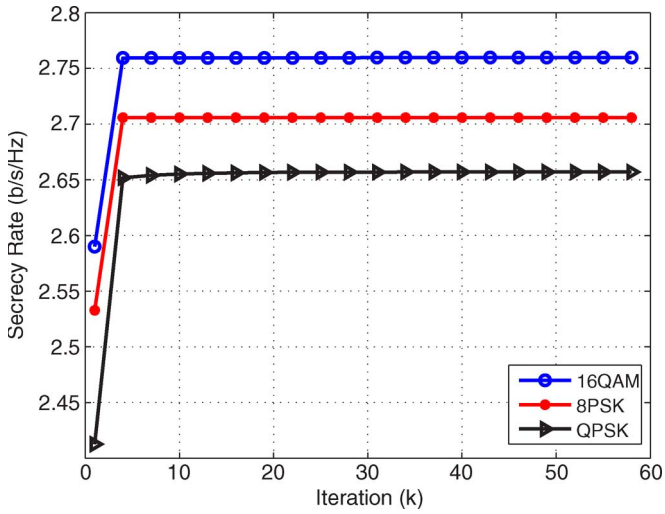


Fig. 3. Convergence of Algorithm 1 for the MISOSE channels (31) and (32) with different modulations at $\mathrm{SNR}_b = 10$ dB.

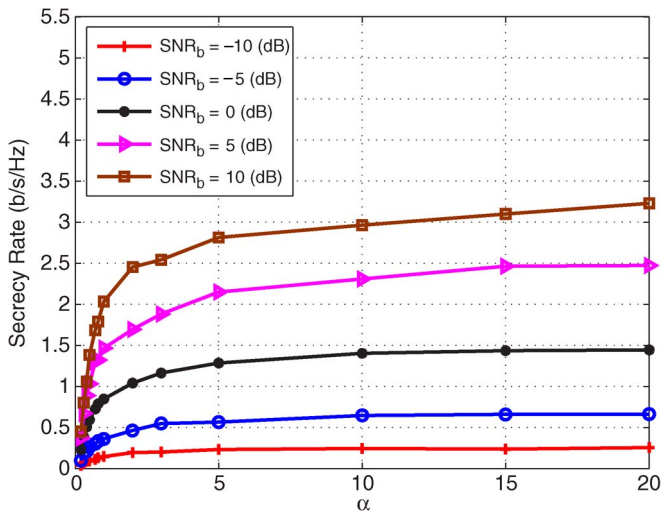


Fig. 5. Secrecy rate of the MISOME channels (39) and (40) for Algorithm 1 and QPSK modulation with different values of SNR_b and α.

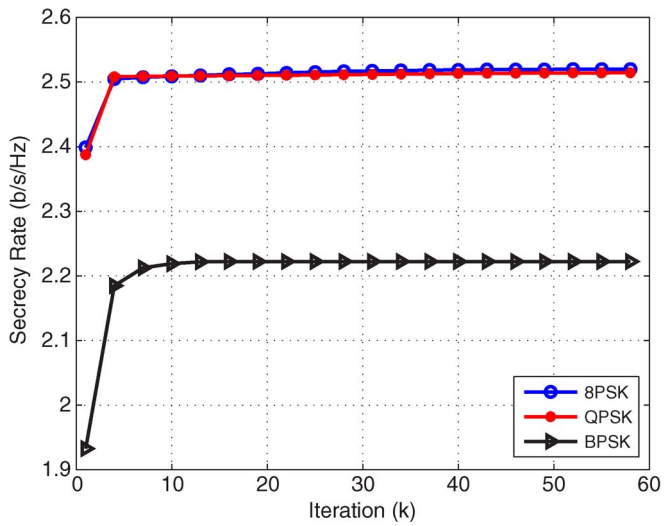


Fig. 4. Convergence of Algorithm 1 for the MISOME channels (36) and (37) with different modulations at $\mathrm{SNR}_b = 5$ dB.

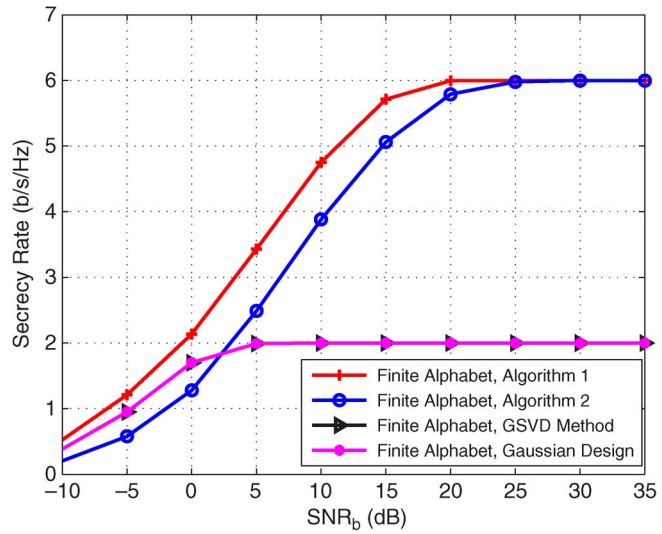


Fig. 6. Secrecy rate of the MIMOME channels (41) and (42) with different designs and QPSK modulation.

different SNR levels, respectively. We can see that, in all cases, Algorithm 1 quickly converges.

Third, we investigate the secrecy rate performance with different SNR levels at the eavesdropper side. We consider Example 3, which is given by

$$\mathbf{h}_{ba} = [0.0991 - 0.8676i \quad 1.0814 + 1.1281i] \tag{39}$$

$$\mathbf{H}_{ea} = \begin{bmatrix} 0.3880 + 1.2024i & -0.9825 + 0.5914i \\ 0.4709 - 0.3073i & 0.6815 - 0.2125i \end{bmatrix}. \tag{40}$$

Fig. 5 plots the secrecy rate results of Example 3 under finite-alphabet constraints with the precoding design in Algorithm 1 and QPSK inputs. We examine the performances with different values of SNR_b and α. In Fig. 5, we observe that, when the SNR at the eavesdropper side is substantially higher (α is small) than the receiver side, the eavesdropper may more accurately decode the transmitter message than the receiver, which will result in an extremely low secrecy rate. As the SNR at the eavesdropper side decreases, the secrecy rate performances can significantly increase, as illustrated in Fig. 5.

Fourth, we study the precoding design in Algorithms 1 and 2 for the MIMOME channels. We consider Example 4, which is given by

$$\mathbf{H}_{ba} = \begin{bmatrix} 0.41 - 0.30i & -0.69 - 0.01i & -0.35 - 0.03i \\ -0.04 - 0.12i & 0.12 - 0.11i & -0.08 + 0.15i \end{bmatrix} \tag{41}$$

$$\mathbf{H}_{ea} = \begin{bmatrix} 0.15 - 0.12i & 0.41 + 0.45i & 0.25 - 0.33i \\ -0.05 + 0.29i & -0.49 + 0.05i & 0.01 - 0.35i \end{bmatrix}. \tag{42}$$

Fig. 6 compares the secrecy rate performances of Example 4 under finite-alphabet constraints with different transmit precoding designs, given QPSK inputs and $\alpha = 1$. We denote Algorithm 2 and the design under the Gaussian input assumption in [37] as "Finite Alphabet, Algorithm 2" and "Finite

Alphabet, Gaussian Design," respectively. Based on Fig. 6, we can make several observations as follows.

1) Algorithm 1 offers positive gains in secrecy rate performance compared to other precoding designs throughout the entire SNR region.
2) When SNR_b is larger than 2 dB, Algorithm 2 achieves better performance than the GSVD-based design and the Gaussian input design.
3) At a high SNR, the secrecy rates of Algorithms 1 and 2 saturate at $N_t \log_2 M = 6$ b/s/Hz.
4) Both the GSVD-based and the Gaussian input designs lead to a secrecy rate loss $(N_t - 1)\log_2 M = 4$ b/s/Hz, because they act as beamforming precoders in the high-SNR region.

The final precoding matrix that was obtained through Algorithm 1 at $\text{SNR}_b = 30$ dB is given by

$$\mathbf{G}_4 = \begin{bmatrix} 1.09 + 0.26i & -0.46 - 0.87i & -0.12 - 0.40i \\ 0.20 + 0.47i & 0.42 - 0.15i & 0.19 - 0.02i \\ 0.18 + 0.17i & 0.01 - 0.22i & 0.02 - 0.09i \end{bmatrix}. \tag{43}$$

It is easy to verify that precoder $\mathbf{G}_4$ meets the necessary conditions (14)–(17) when $\theta_4 = 0$. After the SVD of $\mathbf{G}_4 = \mathbf{U}\mathbf{\Lambda}\mathbf{V}$, there is $\mathbf{\Lambda} = \text{diag}\{1.7321, 0.0000, 0.0000\}$. We note that the rank of $\mathbf{G}_4$ is $N_t - N_e = 1$, which coincides with the conclusion in Proposition 3. In fact, here, all the useful signals $\mathbf{x}_a$ in (1) are combined together by the unitary matrix $\mathbf{V}$ and transmitted along the first diagonal element of $\mathbf{\Lambda}$.

To further validate the performance of Algorithm 1 for the MIMOME channels, we consider Example 5, which is given in (44) and (45), shown at the bottom of the page.

Fig. 7 shows the secrecy rate performances of Example 5 under finite-alphabet constraints with different transmit precoding designs, given QPSK inputs and $\alpha = 1$. Similar to Example 4, we observe that Algorithm 1 outperforms other precoding schemes. In Example 5, by virtue of the increase of transmit antenna (more dimensions available to transmit the useful signals), Algorithm 2 performs superior to the GSVD-based design and the Gaussian input design throughout the whole SNR region. The GSVD-based design will result in a 4-b/s/Hz rate loss at a high SNR, because there are only two effective subchannels available after the GSVD operation of $(\mathbf{H}_{ba}, \mathbf{H}_{ea})$. For the Gaussian input design, the secrecy rate in the high-SNR region leads to a 6-b/s/Hz rate loss.

Next, we examine the optimality of Proposition 2. Fig. 8 illustrates the secrecy rate results of Examples 1, 2, and 5 under finite-alphabet constraints with different precoding designs, given QPSK modulation and $\alpha = 1$ in the low-SNR region.

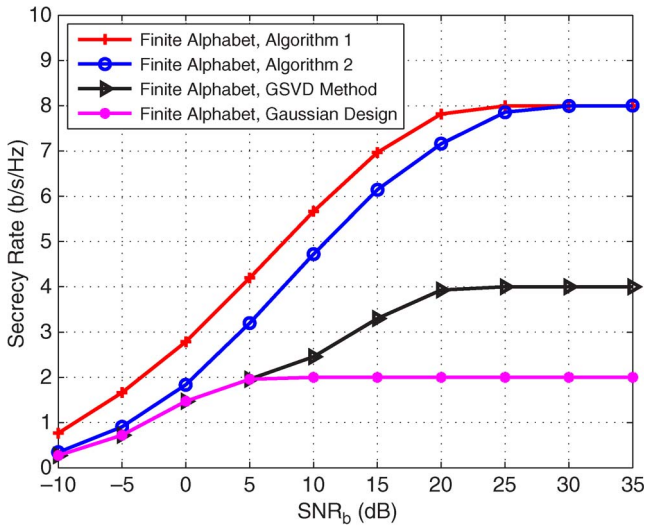


Fig. 7. Secrecy rate of the MIMOME channels (44) and (45) with different designs and QPSK modulation.

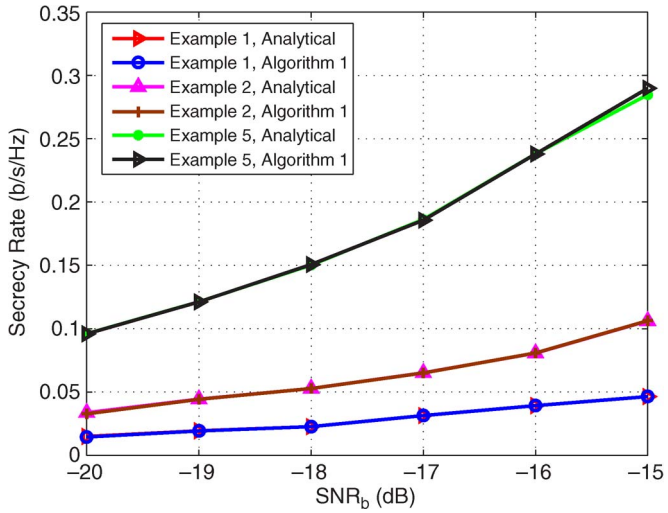


Fig. 8. Secrecy rate of Examples 1, 2, and 5 with different designs and QPSK modulation in the low-SNR region.

As shown, the secrecy rates obtained by Algorithm 1 exhibit excellent agreement with the analytical optimal transmission design in Proposition 2 in the low-SNR region.

To illustrate the additional gain by generating the jamming signal, we consider Examples 6 and 7, which are given in (46)–(49), shown at the bottom of the next page.

Fig. 9 shows the secrecy rate results of Examples 6 and 7 under finite-alphabet constraints for Algorithms 1 and 3 with BPSK modulation and $\alpha = 1$. In Fig. 9, we observe that Algorithm 3 provides additional performance gains over Algorithm 1. The advantages become more obvious as the

$$\mathbf{H}_{ba} = \begin{bmatrix} 0.51 - 0.32i & -0.89 - 0.03i & -0.55 - 0.04i & -0.21 + 0.30i \\ 0.14 - 0.04i & -0.08 - 0.06i & -0.00 + 0.11i & -0.04 + 0.11i \end{bmatrix} \tag{44}$$

$$\mathbf{H}_{ea} = \begin{bmatrix} -0.08 + 0.14i & -0.10 - 0.10i & 0.00 - 0.07i & 0.06 + 0.04i \\ -0.04 - 0.12i & 0.16 - 0.11i & -0.08 + 0.15i & -0.02 + 0.11i \end{bmatrix} \tag{45}$$

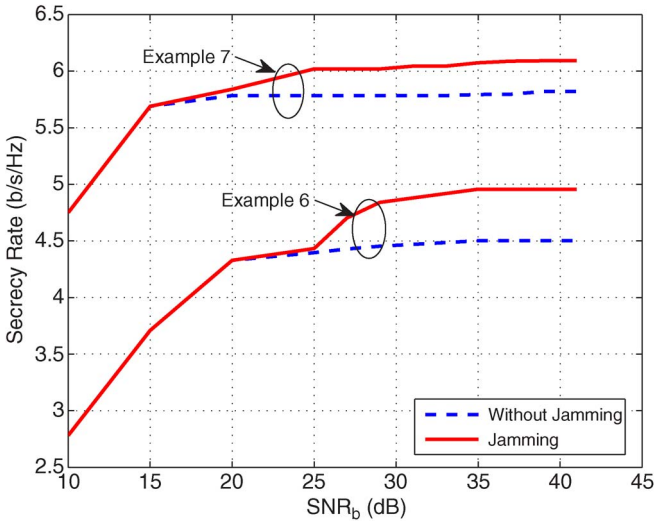


Fig. 9. Secrecy rate of Examples 6 and 7 with jamming design and BPSK modulation.

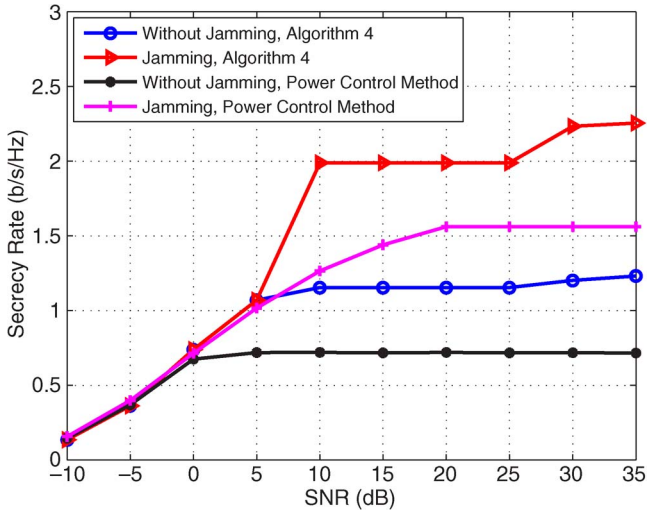


Fig. 10. Ergodic secrecy rate of the MISOSE channels (50) and (51) with different designs and QPSK modulation.

SNR increases. This case indicates that generating the jamming signal can effectively suppress the achievable rate of the eavesdropper to further improve the secrecy rate.

B. Scenarios With the Statistical CSI of the Eavesdropper

In some scenarios, as an eavesdropper, Eve does not want to reveal her presence. Thus, it may be difficult to know the instantaneous CSI of the eavesdropper at each transmission. In the following paragraphs, we present some examples where only the statistical CSI of the eavesdropper is available.

First, we investigate the performance of Algorithm 4 for the MISOSE channels, with the i.i.d. fading eavesdropper's channel. We consider Example 8, which is given by

$$\mathbf{h}_{ba} = [0.5128 - 0.3239i \quad -0.8903 - 0.0318i] \tag{50}$$

$$r_{N_e} = 1 \quad \mathbf{R}_{N_t} = \mathbf{I}_2. \tag{51}$$

Fig. 10 plots the ergodic secrecy rate results of Example 8 under finite-alphabet constraints for the precoding strategy in Algorithm 4 with QPSK inputs and $\alpha = 1$. The power control algorithm in [36] is also simulated and denoted as the power control method. The numerical results[6] indicate that Algorithm 4 provides better performances than the power control algorithm for a wide SNR range, from -10 dB to 35 dB. In addition, at a high SNR, after additional jamming, the secrecy

[6]Example 8 represents scenarios where no channel knowledge of the eavesdropper can be utilized at the transmitter. The transmit designs for Example 8 are exclusively based on the channel of the receiver $\mathbf{h}_{\mathrm{ea}}$. In addition, when the SNR is high, Algorithm 4 needs to determine both the utilized power and the precoding structure of $\mathbf{G}$. Henceforth, at a high SNR, the precoding design based only on $\mathbf{h}_{\mathrm{ea}}$ may result in precoders $\mathbf{G}$ that are quite different, even when the SNR changes only a little. Thus, the performance curves may exhibit step change behaviors in the high-SNR region.

$$\mathbf{h}_{ba} = [\,0.09 + 0.30i \quad 1.32 + 0.78i \quad 0.78 + 1.02i \quad 0.57 + 0.71i \quad 0.69 + 0.86i \quad 0.45 + 0.28i \quad 0.58 + 0.51i\,] \tag{46}$$

$$\mathbf{H}_{ea} = \begin{bmatrix} 0.43+0.09i & 0.00+0.17i & 0.08+0.29i & 0.16+0.33i & 0.12+0.20i & 0.19+0.08i & 0.31+0.00i \\ 0.10+0.09i & 0.37+0.39i & 0.18+0.37i & 0.36+0.14i & 0.09+0.31i & 0.38+0.44i & 0.17+0.40i \\ 0.27+0.31i & 0.20+0.38i & 0.42+0.30i & 0.00+0.38i & 0.00+0.28i & 0.24+0.12i & 0.37+0.09i \\ 0.22+0.14i & 0.28+0.27i & 0.41+0.15i & 0.06+0.25i & 0.33+0.36i & 0.09+0.11i & 0.23+0.13i \\ 0.40+0.24i & 0.36+0.22i & 0.18+0.13i & 0.09+0.17i & 0.20+0.43i & 0.30+0.39i & 0.32+0.30i \\ 0.34+0.07i & 0.41+0.40i & 0.40+0.15i & 0.09+0.32i & 0.42+0.23i & 0.38+0.33i & 0.19+0.13i \\ 0.20+0.31i & 0.33+0.37i & 0.03+0.24i & 0.27+0.25i & 0.21+0.39i & 0.00+0.06i & 0.14+0.21i \end{bmatrix} \tag{47}$$

$$\mathbf{H}_{ba} = \begin{bmatrix} 0.06+0.78i & 0.58+0.46i & 0.52+0.79i & 0.43+0.60i & 0.58+0.42i & 0.53+0.87i & 0.21+0.77i \\ 0.99+0.68i & 0.42+0.57i & 0.33+0.06i & 0.23+0.05i & 0.76+0.30i & 0.64+0.02i & 0.38+0.97i \end{bmatrix} \tag{48}$$

$$\mathbf{H}_{ea} = \begin{bmatrix} 0.43+0.09i & 0.01+0.17i & 0.08+0.29i & 0.16+0.33i & 0.12+0.20i & 0.19+0.08i & 0.31+0.01i \\ 0.10+0.09i & 0.37+0.39i & 0.18+0.37i & 0.36+0.14i & 0.09+0.31i & 0.38+0.44i & 0.17+0.40i \\ 0.27+0.31i & 0.20+0.38i & 0.42+0.30i & 0.00+0.38i & 0.00+0.28i & 0.24+0.12i & 0.37+0.09i \\ 0.22+0.14i & 0.28+0.27i & 0.41+0.15i & 0.06+0.25i & 0.33+0.36i & 0.09+0.11i & 0.23+0.13i \\ 0.40+0.24i & 0.36+0.22i & 0.18+0.13i & 0.09+0.17i & 0.20+0.43i & 0.30+0.39i & 0.32+0.30i \\ 0.34+0.07i & 0.41+0.40i & 0.40+0.15i & 0.09+0.32i & 0.42+0.23i & 0.38+0.33i & 0.19+0.13i \\ 0.20+0.31i & 0.33+0.37i & 0.03+0.24i & 0.27+0.25i & 0.21+0.39i & 0.01+0.06i & 0.14+0.21i \end{bmatrix} \tag{49}$$

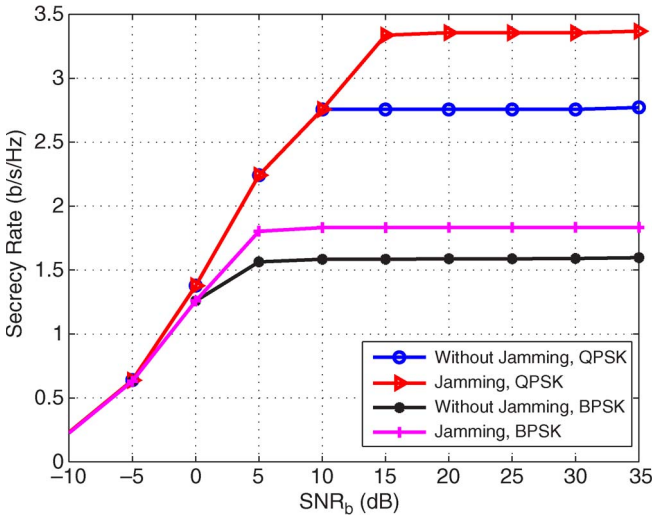


Fig. 11. Ergodic secrecy rate of the MISOSE channels (50) and (52) with different modulations and Algorithm 4.

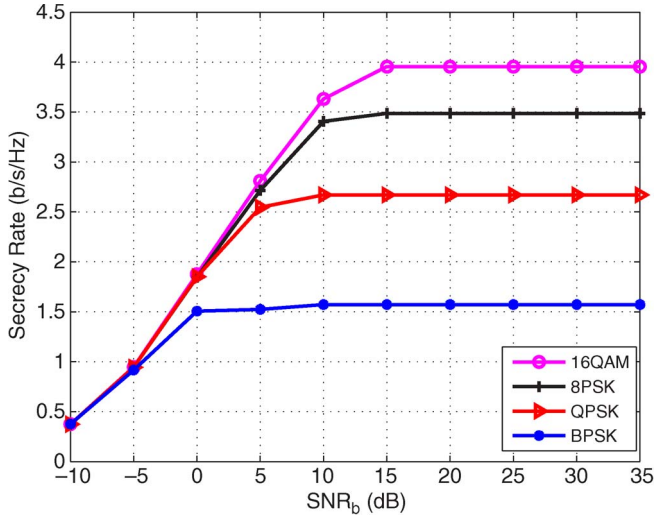


Fig. 12. Ergodic secrecy rate of the MIMOME channels (53) and (54) with different modulations and Algorithm 4.

rates that are achieved by Algorithm 4 surpass the upper bound rate $\log_2 M$ b/s/Hz for the beamforming precoder.

Second, we extend our simulation to the correlated fading eavesdropper's channel. For Example 9, we consider MISOSE channels where $\mathbf{h}_{ba}$ is the same with Example 8 and $\mathbf{h}_{ea}$ is the correlated fading channel as

$$r_{N_e} = 1 \quad \mathbf{R}_{N_t} = \begin{bmatrix} 1 & 0.9 \\ 0.9 & 1 \end{bmatrix}. \tag{52}$$

Fig. 11 examines the precoding strategy in Algorithm 4 for Example 9 with various input types and $\alpha = 1$. In these cases, Algorithm 4 offers very good performances over large-SNR variations, and the additional jamming operation further increases the ergodic secrecy rates. Moreover, we observe that secrecy rates in Fig. 11 are higher than the corresponding secrecy rates in Fig. 10. This result is reasonable, because the precoding strategies for Example 9 are jointly performed through $\mathbf{h}_{ba}$ and $\mathbf{R}_{N_t}$ in (52).

Finally, we study the precoding design in Algorithm 4 for MIMOME channels with the correlated fading eavesdropper's channel. We consider Example 10, which is given by

$$\mathbf{H}_{ba} = \begin{bmatrix} 0.5128 - 0.3239i & -0.8903 - 0.0318i \\ 0.2135 - 0.2534i & 0.1234 - 0.0125i \end{bmatrix} \tag{53}$$

$$\mathbf{R}_{N_t} = \begin{bmatrix} 1 & 0.9 \\ 0.9 & 1 \end{bmatrix}, \quad \mathbf{R}_{N_e} = \begin{bmatrix} 1 & 0.2 \\ 0.2 & 1 \end{bmatrix}. \tag{54}$$

Fig. 12 plots the ergodic secrecy rate performances of Example 10 under finite-alphabet constraints for Algorithm 4, with $\alpha = 1$. These results show that the precoding design based on the statistical knowledge of the eavesdropper's channel $\mathbf{R}_{N_t}$ and $\mathbf{R}_{N_e}$ can achieve robust performances for a large-SNR range with various modulations.

VI. Conclusion

This paper has investigated the design of optimum linear transmit precoding for the maximum secrecy rate over MIMOME wiretap channels. Venturing beyond the traditional information-theoretic assumption of Gaussian input, we formulated the design optimization of transmit precoding for practical data communications of finite discrete input into the following two cases: 1) scenarios with the instantaneous CSI of the eavesdropper and 2) scenarios with the statistical CSI of the eavesdropper.

To address the first case, we obtained necessary conditions of the secrecy rate maximization with the power constraint and proposed an iterative algorithm utilizing the gradient descent update at each iteration to find the optimal precoding matrix. The backtracking line search method is employed to accelerate the convergence speed. Simulations illustrated the convergence behaviors and the performance gains of the proposed algorithm. Compared with the recent GSVD-based precoding design and the design based on the Gaussian input assumption, our precoding method achieves substantial secrecy rate improvement. We also provided closed-form expressions for the optimal transmit design in the low-SNR region and the optimal transmission structure in the high-SNR region. Typically, we have proved that, as long as $N_t > N_e$, the nonbeamforming precoding structure is optimal at a high SNR. This result sharply contrasts with the optimal beamforming precoding design for the MISOME case with the Gaussian input. Moreover, we have shown that the power control policy is unnecessary for the $N_t > N_e$ scenarios and that utilizing full power to transmit can enable the secrecy rate saturate at $N_t \log_2 M$ b/s/Hz at a high SNR. When $N_t \leq N_e$, a novel jamming signal design method that exploits the CSI of the eavesdropper has been proposed to further enhance the secrecy rate. The heuristic extension of the proposed designs to the statistical CSI has also been provided. Similar observations for the performance gains and the precoding structure were obtained.

Appendix A
Proof of Proposition 1

First, we construct the cost function as

$$L(\mathbf{G}, \theta) = -R(\mathbf{G}) + \theta \left(\mathrm{tr}(\mathbf{G}\mathbf{G}^h) - N_t\right) \tag{55}$$

where θ is a Lagrange multiplier that is associated with the constraint $\mathrm{tr}\{\mathbf{G}\mathbf{G}^h\} \le N_t$. Then, the KKT analysis in [40] enables us to establish the necessary conditions for the optimal design as

$$\nabla_{\mathbf{G}} L(\mathbf{G}, \theta) = 0 \tag{56}$$

$$\theta(\mathrm{tr}(\mathbf{G}\mathbf{G}^h) - N_t) = 0 \tag{57}$$

$$\theta \ge 0 \tag{58}$$

$$\mathrm{tr}(\mathbf{G}\mathbf{G}^h) - N_t \le 0. \tag{59}$$

By exploiting the relationship between the derivative of the mutual information and the MMSE matrices in [41], along with the complex matrix differentiation results in [4, Tab. 4.3], we have

$$\nabla_{\mathbf{G}} R(\mathbf{G}) = \mathbf{H}_{ba}^h \mathbf{H}_{ba} \mathbf{G} \mathbf{\Sigma}_b(\mathbf{G}) \frac{\log_2 e}{\sigma_b^2} - \mathbf{H}_{ea}^h \mathbf{H}_{ea} \mathbf{G} \mathbf{\Sigma}_e(\mathbf{G}) \frac{\log_2 e}{\alpha \sigma_b^2} \tag{60}$$

$$\nabla_{\mathbf{G}} \mathrm{tr}(\mathbf{G}\mathbf{G}^h) = \mathbf{G}. \tag{61}$$

Plugging (60) and (61) into (56) completes the proof. ■

Appendix B
Proof of Proposition 2

Based on [29, eq. (12)], when $\sigma_b^2 \to \infty$, we can have the first-order expansions of $I(\mathbf{y}_b; \mathbf{x}_a)$ and $I(\mathbf{y}_e; \mathbf{x}_a)$, i.e.,

$$I(\mathbf{y}_b; \mathbf{x}_a) = \frac{1}{\sigma_b^2} \mathrm{tr}\left\{\mathbf{H}_{ba} \mathbf{G}\mathbf{G}^h \mathbf{H}_{ba}^h\right\} + o\left(\frac{1}{\sigma_b^4}\right) \tag{62}$$

$$I(\mathbf{y}_e; \mathbf{x}_a) = \frac{1}{\alpha\sigma_b^2} \mathrm{tr}\left\{\mathbf{H}_{ea} \mathbf{G}\mathbf{G}^h \mathbf{H}_{ea}^h\right\} + o\left(\frac{1}{\sigma_b^4}\right). \tag{63}$$

We define $\mathbf{Q} = \mathbf{G}\mathbf{G}^h$, which is a $N_t \times N_t$ Hermitian matrix and can be expressed as [51]

$$\mathbf{Q} = \sum_{i=1}^{N_t} q_i \mathbf{v}_i \mathbf{v}_i^h \tag{64}$$

where $\{\mathbf{v}_i\}$ are the column eigenvectors of the matrix $\mathbf{Q}$, and $\{q_i\}$ are the associated eigenvalues that satisfy the power constraint $\sum_{i=1}^{N_t} q_i = \gamma N_t$.

Combining (7) and (62)–(64), yields

$$R(\mathbf{G}) = \frac{1}{\sigma_b^2} \left(\mathrm{tr}\left\{ \mathbf{H}_{ba} \left(\sum_{i=1}^{N_t} q_i \mathbf{v}_i \mathbf{v}_i^h \right) \mathbf{H}_{ba}^h \right\} - \frac{1}{\alpha} \mathrm{tr}\left\{ \mathbf{H}_{ea} \sum_{i=1}^{N_t} \left(q_i \mathbf{v}_i \mathbf{v}_i^h \right) \mathbf{H}_{ea}^h \right\} \right) + o\left(\frac{1}{\sigma_b^4}\right) \tag{65}$$

$$= \frac{1}{\sigma_b^2} \sum_{i=1}^{N_t} q_i \left(\mathbf{v}_i^h \mathbf{H}_{ba}^h \mathbf{H}_{ba} \mathbf{v}_i - \frac{1}{\alpha} \mathbf{v}_i^h \mathbf{H}_{ea}^h \mathbf{H}_{ea} \mathbf{v}_i \right) + o\left(\frac{1}{\sigma_b^4}\right) \tag{66}$$

$$= \frac{1}{\sigma_b^2} \sum_{i=1}^{N_t} q_i \mathbf{v}_i^h \mathbf{\Omega} \mathbf{v}_i + o\left(\frac{1}{\sigma_b^4}\right). \tag{67}$$

Here, $\mathbf{\Omega}$ is a Hermitian matrix, and $\{\mathbf{v}_i\}$ is a unit orthonormal base. If $0 \le \gamma \le 1$ and $\lambda_{\max}(\mathbf{\Omega}) > 0$, then the first-order term of $R(\mathbf{G})$ is upper bounded by [51]

$$R(\mathbf{G}) \le \frac{\lambda_{\max}(\mathbf{\Omega})}{\sigma_b^2} \sum_{i=1}^{N_t} q_i = \frac{\lambda_{\max}(\mathbf{\Omega}) \gamma N_t}{\sigma_b^2} \le \frac{\lambda_{\max}(\mathbf{\Omega}) N_t}{\sigma_b^2} \tag{68}$$

where $\lambda_{\max}(\mathbf{\Omega})$ represents the maximum eigenvalue of the matrix $\mathbf{\Omega}$. The upper bound is achievable by choosing $\mathbf{v}_1$ as the eigenvector that is associated with $\lambda_{\max}(\mathbf{\Omega})$, $q_1 = N_t, q_i = 0, i = 2, \ldots, N_t$, and $\gamma = 1$, which leads to the optimal design in (20). The function $H(\lambda_{\max})$ denotes that, if the condition of the receiver's channel is much worse than the eavesdropper's channel and there is no possibility of conducting a reliable transmission between the transmitter and the receiver without the risk of eavesdropping, then nothing should be transmitted. ■

Appendix C
Proof of Proposition 3

Plugging (21) into (13) yields

$$I_h(\mathbf{y}_e; \mathbf{x}_a) = N_t \log_2 M - \frac{1}{M^{N_t}} \sum_{m=1}^{M^{N_t}} \log_2 M^{N_t} = 0. \tag{69}$$

The precoding structure in (21) results in the zero achievable rate of the eavesdropper. In the meantime, the achievable rate of the receiver can be formulated as in (70), shown at the bottom of the page, where $\mathbf{H}_{ba,\mathrm{eff}} = \mathbf{H}_{ba}\mathbf{V}_e$.

By substituting (69) and (70) into (7), the secrecy rate is equivalent to the finite-alphabet rate expression in point-to-point MIMO scenarios with the effective channel $\mathbf{H}_{ba,\mathrm{eff}} = \mathbf{H}_{ba}\mathbf{V}_e$. Thus, the precoding matrix $\mathbf{P}$ fulfills the equality constraint $\mathrm{tr}(\mathbf{P}\mathbf{P}^h) = N_t$ [33]. Moreover, when $\sigma_b^2 \to 0$, (70) approaches

$$\lim_{\sigma_b^2 \to 0} I_h(\mathbf{y}_b; \mathbf{x}_a) = N_t \log_2 M \tag{71}$$

which is the maximum rate that can be achieved for the intended receiver in the context of finite-alphabet constraints. Combining (69) and (71), we know that the precoding structure in (21) maximizes the secrecy rate at a high SNR. ■

$$I_h(\mathbf{y}_b; \mathbf{x}_a) = N_t \log_2 M - \frac{1}{M^{N_t}} \sum_{m=1}^{M^{N_t}} E_{\mathbf{v}_b} \left\{ \log_2 \sum_{k=1}^{M^{N_t}} \exp\left(- \frac{\|\mathbf{H}_{ba,\mathrm{eff}} \mathbf{P}(\mathbf{x}_m - \mathbf{x}_k) + \mathbf{v}_b\|^2 - \|\mathbf{v}_b\|^2}{\sigma_b^2} \right) \right\} \tag{70}$$

ACKNOWLEDGMENT

The authors would like to thank W. Zeng for helpful discussion on the nonbeamforming precoding for MISOME wiretap channels, M. Wang for his invaluable help throughout this paper, and the reviewers for their helpful comments and suggestions, which greatly improved the quality of this paper.

REFERENCES

[1] B. Schnerier, "Cryptographic design vulnerabilities," *Computer*, vol. 31, no. 9, pp. 29–33, Sep. 1998.

[2] Y.-L. Huang, C.-Y. Shen, and S. W. Shieh, "S-AKA: A provable and secure authentication key agreement protocol for UMTS networks," *IEEE Trans. Veh. Technol.*, vol. 60, no. 9, pp. 4509–4519, Nov. 2011.

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

[4] I. Csiszár and J. Körner, "Broadcast channels with confidential messages," *IEEE Trans. Inf. Theory*, vol. IT-24, no. 3, pp. 339–348, May 1978.

[5] A. Khisti and G. W. Wornell, "Secure transmission with multiple antennas—Part I: The MISOME wiretap channel," *IEEE Trans. Inf. Theory*, vol. 56, no. 7, pp. 3088–3104, Jul. 2010.

[6] A. Khisti and G. W. Wornell, "Secure transmission with multiple antennas—Part II: The MIMOME wiretap channel," *IEEE Trans. Inf. Theory*, vol. 56, no. 11, pp. 5515–5532, Nov. 2010.

[7] F. Oggier and B. Hassibi, "The secrecy capacity of the MIMO wiretap channel," *IEEE Trans. Inf. Theory*, vol. 57, no. 8, pp. 4961–4972, Aug. 2011.

[8] J. Li and A. P. Petropulu, "Transmitter optimization for achieving secrecy capacity in Gaussian MIMO wiretap channels," *IEEE Trans. Inf. Theory*, Sep. 2009, submitted for publication. [Online]. Available: http://arxiv.org/abs/arXiv:0909.2622

[9] L. Dong, Z. Han, A. P. Petropulu, and H. V. Poor, "Improving wireless physical-layer security via cooperating relay," *IEEE Trans. Signal Process.*, vol. 58, no. 3, pp. 1875–1888, Mar. 2011.

[10] T.-H. Chang, W.-C. Chiang, Y.-W. P. Hong, and C.-Y. Chi, "Training sequence design for discriminatory channel estimation in wireless MIMO systems," *IEEE Trans. Signal Process.*, vol. 58, no. 12, pp. 6223–6237, Dec. 2010.

[11] W.-C. Liao, T.-H. Chang, W.-K. Ma, and C.-Y. Chi, "QoS-based transmit beamforming in the presence of eavesdropper: An optimized artificial-noise-aided approach," *IEEE Trans. Signal Process.*, vol. 59, no. 3, pp. 1202–1216, Mar. 2011.

[12] G. Zheng, L.-C. Choo, and K.-K. Wong, "Optimal cooperative jamming to enhance physical-layer security using relays," *IEEE Trans. Signal Process.*, vol. 59, no. 3, pp. 1317–1322, Mar. 2011.

[13] J. Li, A. P. Petropulu, and S. Weber, "On cooperative relaying schemes for wireless physical-layer security," *IEEE Trans. Signal Process.*, vol. 59, no. 10, pp. 4985–4997, Oct. 2011.

[14] S. A. A. Fakoorian and A. L. Swindlehurst, "Solutions for the MIMO Gaussian wiretap channel with a cooperative jammer," *IEEE Trans. Signal Process.*, vol. 59, no. 10, pp. 5013–5022, Oct. 2011.

[15] J. Huang and A. L. Swindlehurst, "Cooperative jamming for secure communications in MIMO relay networks," *IEEE Trans. Signal Process.*, vol. 59, no. 10, pp. 4871–4884, Oct. 2011.

[16] S. A. A. Fakoorian and A. L. Swindlehurst, *Optimal Power Allocation for GSVD-Based Beamforming in the MIMO Wiretap Channel*, Jun. 2010. [Online]. Available: http://arxiv.org/abs/1006.1890

[17] S. Shafiee and S. Ulukus, "Achievable rates in Gaussian MISO channels with secrecy constraints," in *Proc. IEEE ISIT*, Nice, France, Jun. 2007, pp. 2466–2470.

[18] P. K. Gopala, L. Lai, and H. E. Gammal, "On the secrecy capacity of fading channels," *IEEE Trans. Inf. Theory*, vol. 54, no. 10, pp. 4687–4689, Oct. 2008.

[19] X. Zhou and M. R. McKay, "Secure transmission with artificial noise over fading channels: Achievable rate and optimal power allocation," *IEEE Trans. Veh. Technol.*, vol. 59, no. 8, pp. 3831–3842, Oct. 2010.

[20] A. Mukherjee and A. L. Swindlehurst, "Robust beamforming for security in MIMO wiretap channels with imperfect CSI," *IEEE Trans. Signal Process.*, vol. 59, no. 1, pp. 351–361, Jan. 2011.

[21] S. Bashar, Z. Ding, and G. Y. Li, "On secrecy of codebook-based transmission beamforming under receiver-limited feedback," *IEEE Trans. Wireless Commun.*, vol. 10, no. 4, pp. 1212–1223, Apr. 2011.

[22] J. Li and A. P. Petropulu, "On ergodic secrecy capacity for Gaussian MISO wiretap channels," *IEEE Trans. Wireless Commun.*, vol. 10, no. 4, pp. 1176–1187, Apr. 2011.

[23] J. Li, A. P. Petropulu, and H. V. Poor, "On cooperative beamforming based on second-order statistic of channel-state information," *IEEE Trans. Signal Process.*, vol. 59, no. 3, pp. 1280–1291, Mar. 2011.

[24] J. Huang and A. L. Swindlehurst, "Robust secure transmission in MISO channels based on worst case optimization," *IEEE Trans. Signal Process.*, vol. 60, no. 4, pp. 1696–1707, Apr. 2012.

[25] A. Lozano, A. M. Tulino, and S. Verdú, "Optimum power allocation for parallel Gaussian channels with arbitrary input distributions," *IEEE Trans. Inf. Theory*, vol. 52, no. 7, pp. 3033–3051, Jul. 2006.

[26] F. Gao, A. Nallanathan, and C. Tellambura, "Blind channel estimation for cyclic-prefixed single-carrier systems by exploiting real symbol characteristics," *IEEE Trans. Veh. Technol.*, vol. 56, no. 1, pp. 2487–2498, Sep. 2007.

[27] C. Xiao and Y. R. Zheng, "On the mutual information and power allocation for vector Gaussian channels with finite discrete inputs," in *Proc. IEEE GLOBECOM*, New Orleans, LA, Dec. 2008, pp. 1–5.

[28] C. Xiao and Y. R. Zheng, "Transmit precoding for MIMO systems with partial CSI and discrete-constellation inputs," in *Proc. IEEE ICC*, Dresden, Germany, Jun. 2009, pp. 1–5.

[29] F. Pérez-Cruz, M. R. D. Rodrigues, and S. Verdú, "MIMO Gaussian channels with arbitrary input: Optimal precoding and power allocation," *IEEE Trans. Inf. Theory*, vol. 56, no. 3, pp. 1070–1084, Mar. 2010.

[30] J. Harshan and B. S. Rajan, "On two-user Gaussian multiple access channels with finite input constellations," *IEEE Trans. Inf. Theory*, vol. 57, no. 3, pp. 1299–1327, Mar. 2011.

[31] G. Abhinav and B. S. Rajan, "Two-user Gaussian interference channel with finite constellation input and FDMA," in *Proc. IEEE WCNC*, Quintana-Roo, Mexico, Mar. 2011, pp. 25–30.

[32] S. K. Mohammed, E. Viterbo, Y. Hong, and A. Chockalingam, "Precoding by pairing subchannels to increase MIMO capacity with discrete input alphabets," *IEEE Trans. Inf. Theory*, vol. 57, no. 7, pp. 4156–4169, Jul. 2011.

[33] C. Xiao, Y. R. Zheng, and Z. Ding, "Globally optimal linear precoders for finite alphabet signals over complex vector Gaussian channels," *IEEE Trans. Signal Process.*, vol. 59, no. 7, pp. 3301–3314, Jul. 2011.

[34] M. R. D. Rodrigues, A. Somekh-Baruch, and M. Bloch, "On Gaussian wiretap channels with M-PAM inputs," in *Proc. Eur. Wireless Conf.*, Lucca, Italy, Apr. 2010, pp. 774–781.

[35] G. D. Raghava and B. S. Rajan, *Secrecy Capacity of the Gaussian Wire-Tap Channel With Finite Complex Constellation*, Oct. 2010. [Online]. Available: http://arxiv.org/abs/1010.1163v1

[36] S. Bashar, Z. Ding, and C. Xiao, "On the secrecy rate of multi-antenna wiretap channel under finite-alphabet input," *IEEE Commun. Lett.*, vol. 15, no. 5, pp. 527–529, May 2011.

[37] S. Bashar, Z. Ding, and C. Xiao, "On secrecy rate analysis of MIMO wiretap channels driven by finite-alphabet input," *IEEE Trans. Commun.*, accepted for publication. [Online]. Available: http://arxiv.org/abs/1104.1014

[38] W. Zeng, C. Xiao, M. Wang, and J. Lu, "Linear precoding for finite-alphabet inputs over MIMO fading channels with statistical CSI," *IEEE Trans. Signal Process.*, vol. 60, no. 7, July 2012.

[39] S. S. Christensen, R. Agarwal, E. de Carvlho, and J. M. Cioffi, "Weighted sum-rate maximization using weighted MMSE for MIMO-BC beamforming design," *IEEE Trans. Wireless Commun.*, vol. 7, no. 12, pp. 4792–4799, Dec. 2008.

[40] S. Boyd and L. Vandenberghe, *Convex Optimization*. New York: Cambridge Univ. Press, 2004.

[41] D. P. Palomar and S. Verdú, "Gradient of mutual information in linear vector Gaussian channels," *IEEE Trans. Inf. Theory*, vol. 52, no. 1, pp. 141–154, Jan. 2006.

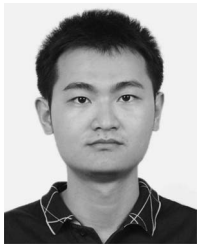
[42] S. Serbetli and A. Yener, "Transceiver optimization for multiuser MIMO systems," *IEEE Trans. Signal Process.*, vol. 52, no. 1, pp. 214–226, Jan. 2004.

[43] J. Dumont, W. Hachem, S. Lasaulce, P. Loubaton, and J. Najim, "On the capacity achieving covariance matrix for Rician MIMO channels: An asymptotic approach," *IEEE Trans. Inf. Theory*, vol. 56, no. 3, pp. 1048–1069, Mar. 2010.

[44] V. Veeravalli, Y. Liang, and A. M. Sayeed, "Correlated MIMO Rayleigh fading channels: Capacity, optimal signalling and asymptotics," *IEEE Trans. Inf. Theory*, vol. 51, no. 6, pp. 2058–2072, Jun. 2008.

[45] A. M. Tulino, A. Lozano, and S. Verdú, "Capacity-achieving input covariance for single-user multiantenna channels," *IEEE Trans. Wireless Commun.*, vol. 5, no. 3, pp. 662–671, Mar. 2006.

[46] X. Gao, B. Jiang, X. Li, A. B. Gershman, and M. R. McKay, "Statistical eigenmode transmission over jointly correlated MIMO channels," *IEEE Trans. Inf. Theory*, vol. 55, no. 8, pp. 3735–3750, Aug. 2009.
[47] T. M. Cover and J. A. Thomas, *Elements of Information Theory*, 2nd ed. New York: Wiley, 2006.
[48] A. Hjørungnes, *Complex-Valued Matrix Derivatives*. New York: Cambridge Univ. Press, 2011.
[49] K. B. Petersen and M. S. Petersen, *The Matrix Cookbook*, Feb. 2007. [Online]. Available: http://www2.imm.dtu.dk/pubdb/p.php?3274
[50] S. Goel and R. Negi, "Guaranteeing secrecy using artificial noise," *IEEE Trans. Wireless Commun.*, vol. 7, no. 6, pp. 2180–2189, Jun. 2008.
[51] R. A. Horn and C. R. Johnson, *Matrix Analysis*. New York: Cambridge Univ. Press, 1999.



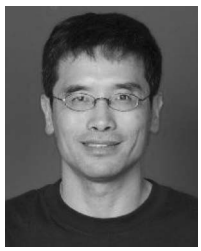
Yongpeng Wu (S'08) received the B.S. degree in communications engineering from Wuhan University, Wuhan, China, in July 2007. He is currently working toward the Ph.D. degree in communications and signal processing with the National Mobile Communications Research Laboratory, Southeast University, Nanjing, China.

During his Ph.D. studies, he has conducted cooperative research with the Department of Electrical Engineering, Missouri University of Science and Technology, Rolla. His research interests include multiple-input–multiple-output systems, signal processing for wireless communications, and multivariate statistical theory.

Chengshan Xiao (M'99–SM'02–F'10) received the B.S. degree in electronic engineering from the University of Electronic Science and Technology of China, Chengdu, China, in 1987, the M.S. degree in electronic engineering from Tsinghua University, Beijing, China, in 1989, and the Ph.D. degree in electrical engineering from the University of Sydney, Sydney, Australia, in 1997.

From 1989 to 1993, he was with the Department of Electronic Engineering, Tsinghua University, where he was a Member of Research Staff and then a Lecturer. From 1997 to 1999, he was a Senior Member of Scientific Staff with Nortel, Ottawa, ON, Canada. From 1999 to 2000, he was a Faculty Member with the University of Alberta, Edmonton, AB, Canada. From 2000 to 2007, he was with the University of Missouri, Columbia, where he was an Assistant Professor and then an Associate Professor. He is currently a Professor with the Department of Electrical and Computer Engineering, Missouri University of Science and Technology, Rolla (formerly the University of Missouri, Rolla). He was an Associate Editor for the *International Journal of Multidimensional Systems and Signal Processing*. He is the holder of three U.S. patents. His algorithms have been implemented into Nortel base station radios after successful technical field trials and network integration. His research interests include wireless communications, signal processing, and underwater acoustic communications.

Dr. Xiao is a Member of the Fellow Evaluation Committee, a Member at Large of the Board of Governors, and a Distinguished Lecturer of the IEEE Communications Society. He is also a Distinguished Lecturer of the IEEE Vehicular Technology Society and the Editor-in-Chief of the IEEE TRANSACTIONS ON WIRELESS COMMUNICATIONS. He served as the Founding Area Editor for Transmission Technology for the IEEE TRANSACTIONS ON WIRELESS COMMUNICATIONS and an Associate Editor for the IEEE TRANSACTIONS ON VEHICULAR TECHNOLOGY and the IEEE TRANSACTIONS ON CIRCUITS AND SYSTEMS PART I. He was the Technical Program Chair of the 2010 IEEE International Conference on Communications (ICC), a Lead Cochair of the 2008 IEEE ICC Wireless Communications Symposium, a PHY/MAC Program Cochair of the 2007 IEEE Wireless Communications and Networking Conference, and the Founding Chair of the IEEE Technical Committee on Wireless Communications.



Zhi Ding (S'88–M'90–SM'95–F'03) received the Ph.D. degree in electrical engineering from Cornell University, Ithaca, NY, in 1990.

From 1990 to 2000, he was a Faculty Member with Auburn University, Auburn, AL, and, later, with the University of Iowa, Iowa City. He has held visiting positions with the Australian National University, Canberra, Australia; Hong Kong University of Science and Technology, Kowloon, Hong Kong; the Lewis Research Center, National Aeronautics and Space Administration, Cleveland, OH; and the Wright Laboratory, United States Air Force, Dayton, OH. He was a Visiting Professor with the Northwestern Polytechnical University, Xian, China. He is currently a Child Family Endowed Professor of Engineering and Entrepreneurship with the Department of Electrical and Computer Engineering, University of California, Davis. He also holds a 1000 Plan appointment with the Southeast University, Nanjing, China. He is a coauthor of the textbook *Modern Digital and Analog Communication Systems* (4th ed., Oxford University Press, 2009). He has active collaboration with researchers from several countries, including Australia, China, Japan, Canada, Taiwan, Korea, Singapore, and Hong Kong.

Dr. Ding was a Distinguished Lecturer of the IEEE Circuits and Systems Society from 2004 to 2006 and the IEEE Communications Society from 2008 to 2009. He was a Member of the Technical Committee on Statistical Signal and Array Processing and the Technical Committee on Signal Processing for Communications from 1994 to 2003. He was the Technical Program Chair of the 2006 IEEE Global Telecommunications Conference. He has served on the technical programs of several workshops and conferences. He was an Associate Editor for the IEEE TRANSACTIONS ON SIGNAL PROCESSING from 1994 to 1997 and from 2001 to 2004 and the IEEE SIGNAL PROCESSING LETTERS from 2002 to 2005.

Xiqi Gao (SM'07) received the Ph.D. degree in electrical engineering from the Southeast University, Nanjing, China, in 1997.

In April 1992, he joined the Department of Radio Engineering, Southeast University, where he has been a Professor of information systems and communications with the National Mobile Communications Research Laboratory since May 2001. From September 1999 to August 2000, he was a Visiting Scholar with Massachusetts Institute of Technology, Cambridge, and Boston University, Boston, MA. From August 2007 to July 2008, he visited the Darmstadt University of Technology, Darmstadt, Germany, as a Humboldt Scholar. His research interests include broadband multicarrier communications, multiple-input–multiple-output wireless communications, channel estimation and turbo equalization, and multirate signal processing for wireless communications.

Dr. Gao serves as an Associate Editor for the IEEE TRANSACTIONS ON SIGNAL PROCESSING and the IEEE TRANSACTIONS ON WIRELESS COMMUNICATIONS. He received the Science and Technology Award in 1998, 2006, and 2009 from the State Education Ministry of China, the National Technological Invention Award of China in 2011, and the Stephen O. Rice Prize Paper Award in Communications Theory from the IEEE Communications Society in 2011.

Shi Jin (S'06–M'07) received the B.S. degree in communications engineering from Guilin University of Electronic Technology, Guilin, China, in 1996, the M.S. degree from Nanjing University of Posts and Telecommunications, Nanjing, China, in 2003, and the Ph.D. degree in communications and information systems from the Southeast University, Nanjing, in 2007.

From June 2007 to October 2009, he was a Research Fellow with the Adastral Park Research Campus, University College London, London, U.K. He is currently with the faculty of the National Mobile Communications Research Laboratory, Southeast University. His research interests include space–time wireless communications, random matrix theory, and information theory.

Dr. Jin received the Young Author Best Paper Award from the IEEE Signal Processing Society in 2010 and was a corecipient of the Stephen O. Rice Prize Paper Award in Communication Theory from the IEEE Communications Society in 2011.