On Quantization for Masked Beamforming Secrecy Systems

Chia-Hua Lin, Shang-Ho Tsai, *Senior Member, IEEE*, and Yuan-Pei Lin, *Senior Member, IEEE*

***Abstract*—This study investigates how to quantize the masked beamforming systems to maximize the secrecy rate for MISOSE (multiple-input, single-output, single-eavesdropper) channels and assume that this eavesdropper equipped with only single antenna, where only partial channel state information (CSI) at the legitimate receiver is available to the transmitter. In this case, the artificial noise (AN) leaks to the legitimate receiver due to CSI quantization. In the literature, all quantization bits are used to quantize the beamforming vector. Then the null space of this quantized beamforming vector is used to transmit the AN. We find that such quantization schemes can result in serious interference at the legitimate receiver. To overcome this issue, we propose that the beamforming vector and the AN vector should be quantized separately, where the beamforming vector should be selected from a codebook to maximize the beamforming gain and the AN vector should be selected from another codebook to minimize the leakage (or interference). Theoretical results show that separate quantization can significantly reduce the AN leakage at the legitimate receiver. Furthermore, based on the proposed quantization scheme, we show how to allocate bits to separately quantize the beamforming vector and the AN vector to maximize the secrecy rate. By using the proposed quantization and bit allocation schemes, the secrecy rates of masked beamforming systems can be improved compared to the conventional quantization schemes. Simulation results corroborate the theoretical results.**

***Index Terms*—Artificial-noise, masked beamforming, MISOSE, quantization, codebook and secrecy rate.**

I. Introduction

ACHIEVING security in the physical layer has received extensive attention recently, especially in wireless communications, because wireless signals can be easily intercepted by unauthorized users. Research has been conducted on this issue and there have been several interesting results, see e.g., [1]–[21].

In [1], Csiszár and Körner investigate the maximum secrecy rate between the transmitter and the legitimate receiver by taking the eavesdropper into consideration. To attain a non-zero secrecy rate, this study addresses that the channel condition between the transmitter and the legitimate receiver should be better than that between the transmitter and the eavesdropper. To reflect the nature of randomness in wireless channels, the authors in [2] evaluated the achievable secrecy rate, and proposed an on-off transmission scheme to avoid eavesdropping. Notably the authors in [3] considered the secrecy capacity for multiple-input single-output (MISO) channels assuming that the CSIs (channel state information) of both the legitimate receiver and the eavesdropper are known to the transmitter. In this case, the secrecy capacity is achieved by beamforming/precoding toward a direction that is as orthogonal to the eavesdropper as possible, while simultaneously being as close to the legitimate receiver as possible. The authors in [4] considered the secrecy capacity for MISO channels with multiple eavesdroppers in colluding fashion, and generalized the model to multiple-input, single-output, multiple-eavesdropper (MISOME) channels. A capacity bound for MISOME channels was derived assuming that the CSI from both the legitimate receiver and the eavesdropper are known to the transmitter. The problems for multiple-input, multiple-output, multiple-eavesdroppers (MIMOME) channels were investigated by the same authors in [5]. Also, the secrecy capacity of MIMO channels has been further widely treated, e.g., [6]–[9]. In addition, recently the authors in [10] used alternating optimization to maximize the secrecy rate of a MIMOME channel.

The above research assumes that the CSI at the legitimate receiver (CSI between the transmitter and the legitimate receiver) and at the eavesdropper (CSI between the transmitter and the eavesdropper) are known to the transmitter. However, the eavesdropper is in general passive and hence the CSI at the eavesdropper is usually unknown to the transmitter. Under this situation, the authors in [11] proposed to transmit artificial-noise (AN) in the null space of the signal directions, so as to impair the channel conditions at the eavesdropper. In this work, we call this scheme "masked beamforming (MB)" [4]. When full CSI at the legitimate receiver is known to the transmitter, the AN in masked beamforming systems is transmitted in the direction orthogonal to the signal directions. Thus, the legitimate receiver does not receive the AN. Also, the MB method is usually used with multiple antenna settings. However, as pointed out in [11], some system models such as wireless relay networks can also be manipulated and apply this method to avoid eavesdropping. In [13] and [14], MB was analyzed assuming that the transmitter knows partial CSI at the eavesdropper while knows full CSI at the legitimate receiver. In [15], the authors considered that masked beamforming has channel estimation error and path loss. An important result was presented in [15] that more power should be allocated to beamforming vector to improve secrecy rates when the channel estimation error is

Manuscript received July 30, 2014; revised January 16, 2015 and May 27, 2015; accepted May 27, 2015. Date of publication June 2, 2015; date of current version October 8, 2015. This work is supported by the National Science Council (NSC), Taiwan, Cooperative Agreement No. 102-2221-E-009-017-MY3. The associate editor coordinating the review of this paper and approving it for publication was E. Koksal.

The authors are with the Department of Electrical Engineering, National Chiao Tung University, Hsinchu 300, Taiwan (e-mail: chlin.ece98g@nctu.edu.tw; shanghot@alumni.usc.edu; ypl@mail.nctu.edu.tw).

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/TWC.2015.2440352

large. In addition, for MISOSE channels, when full CSI at the legitimate receiver is known to the transmitter, it was suggested in [16] that the power allocation of AN is around half of the total transmit power in the high SNR regime, and is around zero in the low SNR regime; power allocation of AN for MIMOME channels was also studied in that work.

In some systems, only partial CSI at the legitimate receiver is available to the transmitter, e.g., Frequency Division Duplexing (FDD) systems. Thus the legitimate receiver needs to quantize the CSI and sends it back to the transmitter. Assume that the transmitter can receive the feedback information correctly [22]–[28]. In general, the quantized CSI is represented by a selected codeword from a predetermined codebook. The construction of codebooks and selection criterions for codewords have been extensively discussed in the literature, e.g., see [23]–[27]. For the legitimate receiver, the leakage of AN leads to interference and it can significantly degrade the outage secrecy probability and the average secrecy rate at the legitimate receiver. This issue was treated separately in [17] and [18]. In these two studies, the authors proposed to quantize the beamforming vector using all bit budget. Then the vectors in the null space of this quantized beamforming vector are used to transmit the AN. That is, the vectors in AN directions are determined once the quantized beamforming vector is determined. We refer to this scheme as "quantized masked beamforming (QMB)." More specifically, [17] analyzed the achievable secrecy rate due to quantization, and pointed out that with only partial CSI, sometimes the conventional beamforming system (without using AN) can outperform the QMB scheme. The work [18] considered how to allocate transmit power between the beamforming vector and the AN, and found that when the number of quantization bits is sufficiently large, one should allocate power evenly between the transmitted signal and the AN, whereas when the number of quantization bits is small, one should be more conservative in allocating power to the AN. We notice that, however, the quantization method in [17] and [18] in general results in serious interference at the legitimate receiver when the number of quantization bits is not sufficiently large. Our goal here is to propose methods for reducing the interference at the legitimate receiver due to quantization.

In this work, we consider multiple-input single-output single-eavesdropper (MISOSE) channels, and assume that this eavesdropper equipped with only single antenna. The MISOSE channel can also be regarded as multiple-eavesdropper equipped with single antenna operating in non-colluding fashion. Also the eavesdropper is able to obtain full CSIs at both the legitimate receiver and the eavesdroppers; while the transmitter only knows partial CSI at the legitimate receiver and no CSI at the eavesdropper. We propose that the beamforming vector and the AN vector should be quantized separately for minimizing the interference at the legitimate receiver. In addition, the overall quantization bits should be properly allocated to quantize the beamforming vector and the AN vector, so as to maximize the average secrecy rate. We theoretically show that under a fixed bit budget, the induced interference at the legitimate receiver using separate quantization can be significantly reduced compared to that using all bits to quantize the beamforming vector solely. This result is interesting because in the literature, e.g., see [17] and [18], intuitively all bits should be used to quantize the beamforming vector.

Thus in the proposed quantization scheme, there are two separate codebooks, both have dimension of $M_t \times 1$, where M_t is the number of transmit antennas. One codebook is used to quantize the beamforming vector and the other is used to quantize the AN vector. Based on the proposed quantization scheme, we analyze the average secrecy rate. From this theoretical result, we show how to allocate the quantization bits to represent the beamforming vector and the AN vector for maximizing the average secrecy rate. The results show that more bits should be allocated to quantize the AN vector when the number of total quantization bits is small. Simulation results corroborate the theoretical results, and provide useful references for practical designs. For instance, a provided simulation result shows that when the total number of quantization bits is 10, one should allocate 8 bits to quantize the AN vector and only 2 bits to quantize the beamforming vector.

The rest of this paper is organized as follows. Section II introduces the system model and formulate the problems according to whether or not full CSI is known to the transmitter. In Section III, we show that the induced interference at the legitimate receiver can be significantly reduced if the beamforming vector and the AN vector directions are quantized separately. In Section IV, based on the proposed quantization scheme, the average secrecy rate is analyzed. From this analytical result, we also derive the proposed bit allocation for quantizing the beamforming vector and the AN vector, so as to maximize the average secrecy rate. Simulation results are provided in Section V, and conclusions are made in Section VI.

Notation: All vectors are in lowercase boldface and matrices are in uppercase boldface. $(\cdot)^T$ and $(\cdot)^H$ denote the transpose and conjugate transpose of a matrix, respectively. The $n \times n$ identity matrix is defined as $\mathbf{I}_n$. $tr(\cdot)$ is the trace of a square matrix. $\mathbb{E}\{\cdot\}$ and $\sigma^2_{\{\cdot\}}$ denote the mean and variance, respectively. $\|\cdot\|$ is the ℓ_2 vector norm. $|\mathcal{S}|$ is the size of a set $\mathcal{S}$. *round*$[\cdot]$ is a function which rounds a variable to an integer. The $\log(\cdot)$ function is with base 2. $\mathbf{x} \backsim \mathcal{CN}(\mathbf{0}, \sigma^2\mathbf{I}_n)$ represents that $\mathbf{x}$ is an $n \times 1$ complex Gaussian vector with zero mean and covariance matrix $\sigma^2\mathbf{I}_n$. Also, e is the base of the natural logarithm.

II. System Model and Background Review

Masked beamforming (MB) systems are introduced in this section. The discussions are divided into two subsections depending on whether or not the transmitter knows full CSI about the legitimate re ceiver.

A. Secrecy Rate With Full CSI

We consider a system model, in which the transmitter sends information to the legitimate receiver; the eavesdropper attempts to decode the information. In this subsection, the eavesdropper is assumed to know full CSI at the legitimate receiver, and full CSI at the eavesdropper. The transmitter knows full CSI at the legitimate receiver but no CSI at the eavesdropper. This communication system is shown in Fig. 1. The transmitter has M_t transmit antennas, the legitimate receiver has one receiving

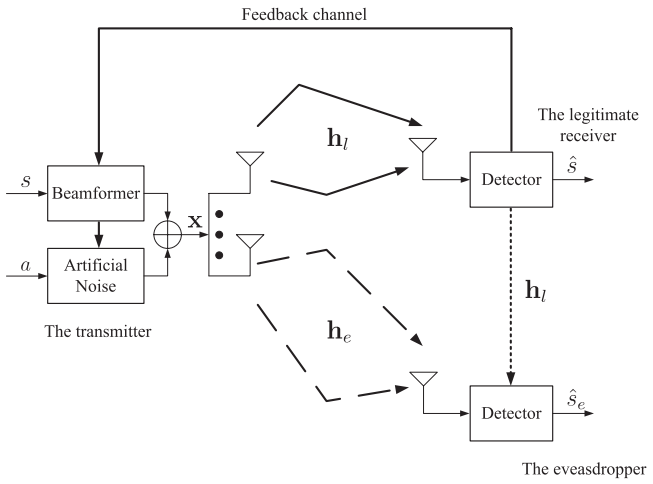

Fig. 1. A block diagram of the proposed scheme.

antenna, and the eavesdropper also has one receiving antenna. Thus, we focus the discussion on MISOSE scenario, where $M_t > 1$. Let $\mathbf{x} \in \mathbb{C}^{M_t \times 1}$ be the data vector, and P be the transmit power. The transmit power is constrained by $\mathbb{E}\{\|\mathbf{x}\|^2\} \leq P$. The signal received by the legitimate receiver and the eavesdropper are expressed, respectively, as

$$y_l = \mathbf{h}_l \mathbf{x} + z_l \text{ and } y_e = \mathbf{h}_e \mathbf{x} + z_e, \tag{1}$$

where $\mathbf{h}_l \in \mathbb{C}^{1 \times M_t}$ is the channel at the legitimate receiver, and $\mathbf{h}_e \in \mathbb{C}^{1 \times M_t}$ is the channel at the eavesdropper. Moreover, we assume that $\mathbf{h}_l$ and $\mathbf{h}_e \sim \mathcal{CN}(\mathbf{0}, \mathbf{I}_{M_t})$; in addition $\mathbf{h}_l$ and $\mathbf{h}_e$ are statistically independent. The channel is assumed to have quasi-static Rayleigh fading. In other words, fading coefficients are fixed during a transmission block for both $\mathbf{h}_l$ and $\mathbf{h}_e$. Nevertheless, the channels are still random from block to block. The terms z_l and z_e in (1) are the additive white Gaussian noise (AWGN) and are both with zero mean and unit variance. That is, we assume that the eavesdropper and the legitimate receiver have comparable noise strength.

To achieve physical-layer secrecy, the transmitter encodes the information using a wire-tap code and transmits $\mathbf{x}$ in the direction of $\mathbf{h}_l$. Under the transmit power constraint P, the rate of the legitimate receiver and the eavesdropper are given, respectively, by

$$R_l = \log\left(1 + P|\mathbf{h}_l \mathbf{x}|^2\right), \tag{2}$$

$$R_e = \log\left(1 + P|\mathbf{h}_e \mathbf{x}|^2\right). \tag{3}$$

The authors in [11] propose to transmit *artificial-noise* (AN) in the null space of $\mathbf{h}_l$ to impair the receive quality at the eavesdropper, and the scheme is referred to as "masked beamforming (MB)" [4]. Thus the transmit signal can be expressed as

$$\mathbf{x} = \mathbf{p}s + \mathbf{N}\mathbf{a} = \mathbf{p}s + \mathbf{g}, \tag{4}$$

where $\mathbf{p} \in \mathbb{C}^{M_t \times 1}$ is the beamforming vector with unit norm, s is the transmitted symbol with signal power $\mathbb{E}\{|s|^2\} = \sigma_s^2$, $\mathbf{N} \in \mathbb{C}^{M_t \times (M_t - 1)}$ is a semi-unitary matrix that belongs to the null space of the channel $\mathbf{h}_l$; that is, each column of $\mathbf{N}$ is orthogonal to the channel $\mathbf{h}_l$, and $\mathbf{a} \in \mathbb{C}^{(M_t-1)\times 1} \sim \mathcal{CN}(\mathbf{0}, \sigma_a^2 \mathbf{I}_{M_t - 1})$. We assume that s, $\mathbf{N}$ and $\mathbf{a}$ are statistically independent. In addition, we define $\mathbf{g} = \mathbf{N}\mathbf{a}$ and call it "the vector of AN direction" for convenience. From (4), the power constraint becomes $\mathbb{E}\{\|\mathbf{x}\|^2\} = \sigma_s^2 + (M_t - 1)\sigma_a^2 \leq P$. MB systems use partial power, say αP, to transmit signals, and distribute the residual power, $(1 - \alpha)P$, to the AN, where $\alpha \in (0, 1]$. Thus $\sigma_s^2 = \alpha P$ and $\sigma_a^2 = (1 - \alpha)P/(M_t - 1)$. When full CSI at the legitimate receiver is available to the transmitter, it is reasonable to use the normalized channel vector of $\mathbf{h}_l$ as the beamforming vector [3] and [11], i.e.,

$$\mathbf{p} = \frac{\mathbf{h}_l^H}{\|\mathbf{h}_l\|}. \tag{5}$$

Moreover, due to the use of the AN, the received signals at the legitimate receiver and the eavesdropper in (1) can be rewritten respectively as

$$y_l = \|\mathbf{h}_l\| s + z_l, \tag{6}$$

and

$$y_e = \mathbf{h}_e \mathbf{p} s + \mathbf{h}_e \mathbf{N}\mathbf{a} + z_e. \tag{7}$$

In addition, the rates in (2) and (3) can be reformulated as

$$R_l^{MB} = \log\left(1 + \alpha P \|\mathbf{h}_l\|^2\right), \tag{8}$$

$$R_e^{MB} = \log\left(1 + \frac{\alpha P |\mathbf{h}_e \mathbf{p}|^2}{\frac{(1-\alpha)P}{M_t - 1}\|\mathbf{h}_e \mathbf{N}\|^2 + 1}\right). \tag{9}$$

The achievable secrecy rate R_s^{MB} for Gaussian input signals was investigated in [3] and [4] and was defined as

$$R_s^{MB} = R_l^{MB} - R_e^{MB}.$$

When $R_s^{MB} \geq 0$, a secure transmission can be achieved by using wire-tap code; on the other hand, when $R_s^{MB} < 0$, the error rate at the eavesdropper does not go to infinity and perfect secrecy is not guaranteed. The average secrecy rate was defined as

$$\begin{aligned} \mathbb{E}\left\{R_s^{MB}\right\} &= \mathbb{E}\left\{R_l^{MB} - R_e^{MB}\right\} \\ &= \mathbb{E}\left\{\log\left(1 + \alpha P \|\mathbf{h}_l\|^2\right)\right\} \\ &\quad - \mathbb{E}\left\{\log\left(1 + \frac{\alpha P |\mathbf{h}_e \mathbf{p}|^2}{\frac{(1-\alpha)P}{M_t - 1}\|\mathbf{h}_e \mathbf{N}\|^2 + 1}\right)\right\}. \end{aligned} \tag{10}$$

Note that the average secrecy rate is not an achievable rate in the Shannon sense [19]; rather it is a performance metric that is widely used in physical layer security (e.g., [2], [11], and [18]).

B. Secrecy Rate With Partial CSI

In this subsection, we consider a case that only partial CSI at the legitimate receiver is known to the transmitter. We will use the random vector quantization (RVQ)-based codebooks [18] to analyze the relationship between the number of quantization bits and the average the secrecy rate.

An RVQ-based codebook $\mathcal{W}$ consists of 2^B unit norm codewords $\mathcal{W} \triangleq \{\mathbf{w}_1, \ldots, \mathbf{w}_{2^B}\}$ and is usually called *quantized beamforming codebook* (QB codebook), where the codeword is $\mathbf{w}_i \in \mathbb{C}^{M_t \times 1}$ for $i = 1, \ldots, 2^B$, and B is the number of the quantization bits. Moreover, $\mathbf{w}_i$ for $i = 1, \ldots, 2^B$, are isotropically distributed in $\mathbb{C}^{M_t \times 1}$, and $\mathbf{w}_i$ and $\mathbf{w}_j$ for $i \neq j$ are random and statistically independent. In the literature, e.g., see [17] and [18], the legitimate receiver quantizes the beamforming vector $\mathbf{p}$ by selecting a codeword that can maximize the rate at the legitimate receiver, where the maximization is measured by the inner product of the beamforming vector $\mathbf{p}$ and the vectors in the codebook. Then the selected codeword can be denoted as

$$\mathbf{w}_o = \arg \max_{\mathbf{v} \in \{\mathbf{w}_1, \ldots, \mathbf{w}_{2^B}\}} |\mathbf{p}^H \mathbf{v}|^2, \tag{11}$$

and

$$\cos^2 \theta = \left|\mathbf{p}^H \mathbf{w}_o\right|^2, \tag{12}$$

where $\mathbf{w}_o$ is called *quantized beamforming* (QB) vector, and $\cos^2 \theta$ is the maximum value of vector inner product between the beamforming vector $\mathbf{p}$ and the quantized beamforming vector $\mathbf{w}_o$. Due to the limited feedback, the null space of $\mathbf{p}$ is not available to the transmitter. Hence, the authors in [17] and [18] proposed to use the null space of $\mathbf{w}_o$ instead of $\mathbf{p}$. For presentation convenience, we call this scheme "quantized masked beamforming (QMB)." We define $\mathbf{N}_{\mathbf{w}_o} \in \mathbb{C}^{M_t \times (M_t - 1)}$ as the semi-unitary matrix that belongs to the null space of $\mathbf{w}_o^H$. From (4), the data vector with limited feedback becomes

$$\mathbf{x} = \mathbf{w}_o s + \mathbf{N}_{\mathbf{w}_o} \mathbf{a}. \tag{13}$$

From (13), the received signal at the legitimate receiver and the eavesdropper are rewritten respectively as

$$y_l = \|\mathbf{h}_l\| \mathbf{p}^H \mathbf{w}_o s + \|\mathbf{h}_l\| \mathbf{p}^H \mathbf{N}_{\mathbf{w}_o} \mathbf{a} + z_l, \tag{14}$$

and

$$y_e = \mathbf{h}_e \mathbf{w}_o s + \mathbf{h}_e \mathbf{N}_{\mathbf{w}_o} \mathbf{a} + z_e. \tag{15}$$

The average secrecy rate for the QMB scheme can be expressed as

$$\begin{aligned} \mathbb{E}\left\{R_s^{QMB}\right\} &= \mathbb{E}\left\{R_l^{QMB} - R_e^{QMB}\right\} \\ &= \mathbb{E}\left\{\log\left(1 + \frac{\alpha P \|\mathbf{h}_l\|^2 \cos^2 \theta}{\frac{(1-\alpha)P\|\mathbf{h}_l\|^2}{M_t - 1} \sin^2 \theta + 1}\right)\right\} \\ &\quad - \mathbb{E}\left\{\log\left(1 + \frac{\alpha P |\mathbf{h}_e \mathbf{w}_o|^2}{\frac{(1-\alpha)P}{M_t - 1} \|\mathbf{h}_e \mathbf{N}_{\mathbf{w}_o}\|^2 + 1}\right)\right\}, \end{aligned} \tag{16}$$

where R_l^{QMB} and R_e^{QMB} are the achievable rates of the legitimate receiver and the eavesdropper, respectively, under limited-feedback environments. Also, note that $\|\mathbf{p}^H \mathbf{N}_{\mathbf{w}_o}\|^2$ can be formulated as below,

$$\left\|\mathbf{p}^H \mathbf{N}_{\mathbf{w}_o}\right\|^2 = 1 - \left|\mathbf{p}^H \mathbf{w}_o\right|^2 = \sin^2 \theta, \tag{17}$$

due to (12).

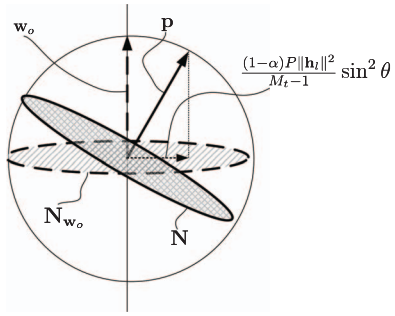

Fig. 2. A geometric interpretation for interference in the QMB scheme, in which the value of $\sin^2 \theta$ is decided once the quantized beamforming vector is determined.

III. Proposed Quantization Schemes

This section begins with quantizing all vectors in AN directions. Then we show that better performance can generally be achieved by quantizing a linearly combined vector of the AN directions instead of quantizing all vectors.

A. Quantization of Vectors in AN Directions

The studies in [17] and [18] pair the quantized beamforming vector $\mathbf{w}_o$ and the semi-unitary matrix $\mathbf{N}_{\mathbf{w}_o}$. Thus $\mathbf{N}_{\mathbf{w}_o}$ is determined once $\mathbf{w}_o$ is determined. When full CSI at the legitimate receiver is not available, $\mathbf{w}_o$ does not lie in the direction of $\mathbf{p}$ precisely. Hence, $\mathbf{N}_{\mathbf{w}_o}$ is different from $\mathbf{N}$, and $\mathbf{p}$ is not orthogonal to each column of $\mathbf{N}_{\mathbf{w}_o}$, which induces interference at the legitimate receiver. This is demonstrated in a geometry viewpoint shown in Fig. 2. The interference power appears at the denominator of R_l^{QMB} in (16) and (17) that is defined as

$$I_l = \frac{(1-\alpha)P\|\mathbf{h}_l\|^2}{M_t - 1} \sin^2 \theta. \tag{18}$$

From (18), the interference at the legitimate receiver is highly related to the value of $\sin^2 \theta$. In general, this value is large in QMB schemes, because it only quantizes the beamforming vector, and the corresponding AN vectors are completely determined by the quantized beamforming vector. If one can quantize the beamforming vector and the vectors in AN directions individually, the value of $\sin^2 \theta$ can be reduced.

Thus, the proposed scheme has an extra codebook called *quantized AN codebook* (QA codebook). Let the number of total quantization bits be B, the value of B is divided into two parts. One is the number of bits for quantizing the optimal beamforming vector B_{QB}, and the other is the number of bits for quantizing the AN vector B_{QA}, i.e.,

$$B = B_{QB} + B_{QA}. \tag{19}$$

Moreover, we define the size of QB codebook as $N_{QB} = 2^{B_{QB}}$, and that of QA as $N_{QA} = 2^{B_{QA}}$. The quantized vectors (represented by a matrix) in AN directions can then be expressed as

$$\overline{\mathbf{N}} = \arg \min_{\mathbf{M} \in \left\{\overline{\mathbf{N}}_1, \ldots, \overline{\mathbf{N}}_{N_{QA}}\right\}} \|\mathbf{p}^H \mathbf{M}\|^2, \tag{20}$$

where $\overline{\mathbf{N}}_i \in \mathbb{C}^{M_t \times (M_t-1)}$ is a semi-unitary matrix for $i = 1, \ldots, N_{QA}$, and the columns of $\overline{\mathbf{N}}_i$ are isotropically distributed in $\mathbb{C}^{M_t \times 1}$. By the use of QA codebook and (20), $\overline{\mathbf{N}}$ is obtained; hence, (18) is redefined as

$$I_l^{\overline{\mathbf{N}}} = \frac{(1-\alpha)P\|\mathbf{h}_l\|^2}{M_t - 1}\|\mathbf{p}^H\overline{\mathbf{N}}\|^2. \tag{21}$$

To evaluate the interference power at the legitimate receiver in (21), one needs to know the mean value of $\|\mathbf{p}^H\overline{\mathbf{N}}\|^2$. The following lemma analyzes the mean value of $\|\mathbf{p}^H\overline{\mathbf{N}}\|^2$:

Lemma 1: Let the size of QA codebook be N_{QA}, and the best codeword is selected using (20) to minimize $\|\mathbf{p}^H\overline{\mathbf{N}}\|^2$. Then the mean value of $\|\mathbf{p}^H\overline{\mathbf{N}}\|^2$ can be shown to be

$$\mathbb{E}\left\{\|\mathbf{p}^H\overline{\mathbf{N}}\|^2\right\} = N_{QA} \cdot \beta\left(N_{QA}, \frac{M_t}{M_t - 1}\right), \tag{22}$$

where $\beta(a, b)$ is the beta function defined by

$$\beta(a, b) = \int_0^1 t^{a-1}(1-t)^{b-1}dt.$$

Proof: Let $\overline{\mathbf{n}}$ belong to the null space of $\overline{\mathbf{N}}$. Obviously, $\overline{\mathbf{n}}$ is isotropically distributed in $\mathbb{C}^{M_t \times 1}$ as well. We know the fact that

$$\|\mathbf{p}^H\overline{\mathbf{N}}\|^2 = 1 - |\mathbf{p}^H\overline{\mathbf{n}}|^2 = 1 - \cos^2\left(\angle(\mathbf{p}, \overline{\mathbf{n}})\right) = \sin^2\left(\angle(\mathbf{p}, \overline{\mathbf{n}})\right),$$

where $\angle(\mathbf{p}, \overline{\mathbf{n}})$ is the angle between $\mathbf{p}$ and $\overline{\mathbf{n}}$. Then this Lemma is proved by applying the derived mean value of $\sin^2(\angle(\mathbf{p}, \overline{\mathbf{n}}))$ in [26, Eq. (13)]. □

From Lemma 1, substituting $\sin^2(\angle(\mathbf{p}, \overline{\mathbf{n}}))$ into (21) yields

$$\mathbb{E}\left\{I_l^{\overline{\mathbf{N}}}\right\} = \frac{(1-\alpha)PM_tN_{QA}}{M_t - 1}\beta\left(N_{QA}, \frac{M_t}{M_t - 1}\right), \tag{23}$$

where $\mathbb{E}\{\|\mathbf{h}_l\|^2\} = M_t$ is used to obtain this equality.

$I_l^{\overline{\mathbf{N}}}$ in (23) is the interference at the legitimate receiver when all vectors in AN directions are quantized. In the following subsection, we show that quantizing a linearly combined vector of the AN directions generally leads to a smaller interference than quantizing all vectors in AN directions.

B. Proposed Quantization Scheme and Induced Interference

In this subsection, instead of quantizing all vectors in AN directions, we propose to quantize a linearly combined vector of AN directions, and this vector should minimize the leakage. We notice that when the number of quantization bits is moderate, the proposed quantization method can significantly reduce the interference power in (18).

To reduce the interference power at the legitimate receiver, we quantize a linearly combined vector $\mathbf{g}$ of AN directions, and this vector should minimize the leakage. From a geometric viewpoint, $\mathbf{g}$ should be orthogonal to the beamforming vector $\mathbf{p}$, i.e.,

$$|\mathbf{p}^H\mathbf{g}|^2 = 0.$$

However since only partial CSI at the legitimate receiver is available to the transmitter, $|\mathbf{p}^H\mathbf{g}|^2 \neq 0$, and quantization is needed. Thus we construct a QA codebook $\mathcal{N}$ and each codeword in $\mathcal{N}$ has dimension $\mathbb{C}^{M_t \times 1}$; that is $\mathcal{N} \triangleq \{\mathbf{n}_1, \ldots, \mathbf{n}_{N_{QA}}\}$, where $\mathbf{n}_i$ has the isotropically distribution in $\mathbb{C}^{M_t \times 1}$, and N_{QA} is the size of the QA codebook. The best codeword can be selected via minimizing the interference power at the legitimate receiver,

$$\begin{aligned}\mathbf{n}_o &= \arg\max_{\mathbf{v} \in \{\mathbf{n}_1, \ldots, \mathbf{n}_{N_{QA}}\}} |\mathbf{g}^H\mathbf{v}|^2 \\ &= \arg\min_{\mathbf{v} \in \{\mathbf{n}_1, \ldots, \mathbf{n}_{N_{QA}}\}} |\mathbf{p}^H\mathbf{v}|^2,\end{aligned} \tag{24}$$

and

$$\cos^2\phi = \left|\mathbf{p}^H\mathbf{n}_o\right|^2, \tag{25}$$

where $\cos^2\phi$ is the minimum value of vector inner product between $\mathbf{p}$ and the selected codeword in $\mathcal{N}$. Note that $\mathbf{n}_o$ is a "quantized linearly combined vector of all AN directions." Moreover, $\mathbf{n}_o$ changes as the wireless channel $\mathbf{h}_l$ changes, and is not fixed. As a result, it is unlikely that the eavesdropper can always lie in a direction that is orthogonal to $\mathbf{n}_o$.

From discussion above, now we have two codebooks; one is the QB codebook $\mathcal{W}$ for quantizing the beamforming vector, and the other is the QA codebook $\mathcal{N}$ for quantizing the vector in AN directions. Because $\mathcal{W}$ and $\mathcal{N}$ are individually and randomly generated, these two codebooks are statistically independent. The legitimate receiver uses (11) and (24) to obtain $\mathbf{w}_o$ and $\mathbf{n}_o$ respectively. Note that the number of quantization bits of the proposed scheme does not increase because we constrain the total number of bits as $B = B_{QB} + B_{QA}$. Moreover, because $\mathbf{n}_o$ is of dimension $M_t \times 1$, the memory requirement for quantizing the vector in AN directions is actually less than that for quantizing all vectors in AN directions, which has dimension $M_t \times (M_t - 1)$.

Next, we analyze the interference at the legitimate receiver for the proposed scheme, like what has been done for the interference induced by quantizing all AN vector directions in (23). After that we will show that quantizing a linearly combined vector of AN directions indeed leads to a smaller interference at the legitimate receiver than that obtained by quantizing all vectors in AN directions.

From the discussion above, the transmitted signal of the proposed scheme can be rewritten as

$$\mathbf{x} = \mathbf{w}_o s + \mathbf{n}_o a, \tag{26}$$

where $a \sim \mathcal{CN}(0, (1-\alpha)P)$. The received signals at the legitimate receiver and the eavesdropper can be rewritten respectively given by

$$y_l = \|\mathbf{h}_l\|\mathbf{p}^H\mathbf{w}_o s + \|\mathbf{h}_l\|\mathbf{p}^H\mathbf{n}_o a + z_l, \tag{27}$$

and

$$y_e = \mathbf{h}_e\mathbf{w}_o s + \mathbf{h}_e\mathbf{n}_o a + z_e. \tag{28}$$

The second term of the right-hand side (RHS) in (27) is the interference due to the quantization of $\mathbf{n}_o$. Thus the interference

power at the legitimate receiver for the proposed scheme can be expressed as

$$I_l^{\mathbf{n}_o} = (1-\alpha)P\|\mathbf{h}_l\|^2\cos^2\phi, \tag{29}$$

According to [26], the two terms $\|\mathbf{h}_l\|^2$ and $\cos\phi$ are independent random variables with chi-square and beta distributions, respectively. Hence we are able to treat them separately. Let us evaluate the mean value of $\cos^2\phi$ first, which is defined in (25). It has been shown in [24, Section III.C] that x is defined as $|\mathbf{u}^H\mathbf{v}|^2$ where $\mathbf{u}$ and $\mathbf{v}$ are statistical independent and isotropically distributed unit norm vector, then x has beta distribution with parameters $(1, M_t-1)$. Furthermore, the probability density function (PDF) of x is $f(x) = (M_t-1)(1-x)^{(M_t-1)-1}$ and the cumulative density function (CDF) of x is $F(x) = 1-(1-x)^{M_t-1}$. With the aid of order statistics [29], the PDF of the minimum sample $x_{\min}$, selected from N_{QA} i.i.d. random variables $x_1, \ldots, x_{N_{QA}}$, is given by

$$f_{x_{\min}}(x) = N_{QA}f(x)\,(1-F(x))^{N_{QA}-1}. \tag{30}$$

As mentioned above, we define $x_i = |\mathbf{p}^H\mathbf{n}_i|^2$ for $i \in \{1, 2, \cdots, N_{QA}\}$. Moreover, from (24) and (25) we know that $x_{\min} = |\mathbf{p}^H\mathbf{n}_o|^2$, so $f_{x_{\min}}(x)$ can be obtained by substituting $f(x)$ and $F(x)$ of the beta distribution with parameters $(1, M_t-1)$, which yields

$$f_{x_{\min}}(x) = N_{QA}(M_t-1)(1-x)^{N_{QA}(M_t-1)-1}. \tag{31}$$

Similarly, the CDF of $x_{\min}$ can be obtained as follows:

$$F_{x_{\min}}(x) = 1-(1-x)^{N_{QA}(M_t-1)}. \tag{32}$$

From (31) and (32), the mean value of $x_{\min}$ is obtained in the following lemma:

Lemma 2: The mean value of $x_{\min}$ is given by

$$\mathbb{E}\{x_{\min}\} = \frac{1}{N_{QA}(M_t-1)+1}. \tag{33}$$

Proof: The mean value can be obtained by the definition $\mathbb{E}\{x_{\min}\} = \int_0^1 x dF_{x_{\min}}(x)$ and using (31), to yield (33). □

From Lemma 2, by substituting $x_{\min} = \cos^2\phi$ into (29), the mean value of $I_l^{\mathbf{n}_o}$ in (29) is obtained as follows:

$$\mathbb{E}\left\{I_l^{\mathbf{n}_o}\right\} = \frac{(1-\alpha)PM_t}{N_{QA}(M_t-1)+1}. \tag{34}$$

From (23) and (34), one can compare the interference values induced by the proposed quantization and by quantizing all vectors in AN directions in the following proposition:

Proposition 1: In a MISO system with M_t transmit antennas and codebook size N_{QA}, the ratio γ of the interference power obtained by quantizing all vectors in AN directions and by quantizing a linearly combined vector of AN directions can be expressed as follows:

$$\gamma = \frac{\mathbb{E}\left\{I_l^{\overline{\mathbf{N}}}\right\}}{\mathbb{E}\left\{I_l^{\mathbf{n}_o}\right\}} = \left[N_{QA}^2 + \frac{N_{QA}}{M_t-1}\right]\cdot\beta\left(N_{QA}, \frac{M_t}{M_t-1}\right). \tag{35}$$

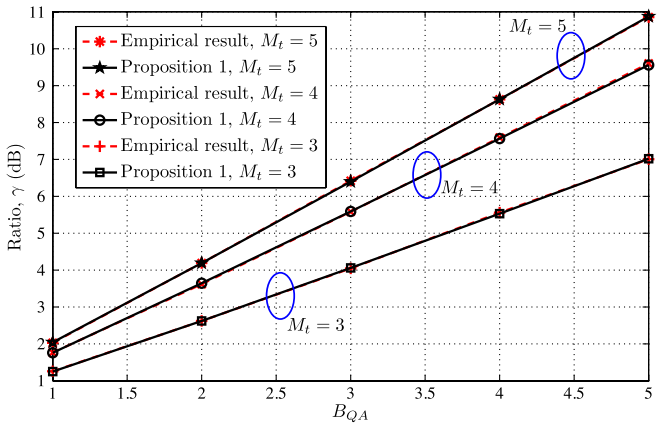

Fig. 3. The values of γ as functions of B_{QA} for $M_t = 3$, 4, and 5.

Proof: This proposition is a direct result and obtained by using (23) and (34). □

Experiment 1. The ratio γ for Various Values of N_{QA}: This experiment is to show that the proposed quantization indeed leads to a better performance than quantizing all vectors in AN directions. Let $M_t = 3$, 4, and 5. Fig. 3 shows the values of γ as functions of $N_{QA} = 2^{B_{QA}}$. The theoretical results are evaluated using Proposition 1. Observe that the empirical results corroborate the theoretical results in Proposition 1. Also, the value of γ is greater than 1; this implies that the proposed quantization leads to a smaller interference than quantizing all vectors in AN directions. Moreover, we see that the value of γ increases as the values of M_t and B_{QA} increase. Note that when $M_t = 2$, the nullity is one, and $\gamma = 1$. Thus $I_l^{\overline{\mathbf{N}}}$ is equal to $I_l^{\mathbf{n}_o}$ in this case.

IV. Secrecy Rate and Proposed Bit Allocations

In this section, we analyze the average secrecy rate for the proposed scheme and derive an approximated upper bound for the average secrecy rate. From this bound, we suggest how to allocate bits to B_{QB} and B_{QA} under the total bit constraint in (19).

A. Approximated Upper Bound for Average Secrecy Rate

In the proposed scheme, both the transmitter and the legitimate receiver have two codebooks $\mathcal{W}$ and $\mathcal{N}$, and the received signals at the legitimate receiver and the eavesdropper are given respectively in (27) and (28). Hence the average secrecy rate of the proposed scheme can be formulated as follows:

$$\begin{aligned}\mathbb{E}\left\{R_s^\star\right\} &= \mathbb{E}\left\{R_l^\star - R_e^\star\right\}\\ &= \mathbb{E}\left\{\log\left(1+\frac{\alpha P\|\mathbf{h}_l\|^2\cos^2\theta}{(1-\alpha)P\|\mathbf{h}_l\|^2\cos^2\phi+1}\right)\right\}\\ &\quad - \mathbb{E}\left\{\log\left(1+\frac{\alpha P\,|\mathbf{h}_e\mathbf{w}_o|^2}{(1-\alpha)P|\mathbf{h}_e\mathbf{n}_o|^2+1}\right)\right\}.\end{aligned} \tag{36}$$

From (36), because $\mathbf{h}_l$ and $\mathbf{h}_e$ are independent and two independent codebooks $\mathcal{W}$ and $\mathcal{N}$ are used, the mean values of $R_l^\star$ and $R_e^\star$ can be treated separately. We apply Jensen's inequality

to the mean value of $R_l^\star$ in (36). Then (36) can be upper bounded by

$$\mathbb{E}\left\{R_s^\star\right\} \le \log\left(1+\mathbb{E}\left\{\frac{\alpha P\|\mathbf{h}_l\|^2\cos^2\theta}{(1-\alpha)P\|\mathbf{h}_l\|^2\cos^2\phi+1}\right\}\right) - \mathbb{E}\left\{\log\left(1+\frac{\alpha P|\mathbf{h}_e\mathbf{w}_o|^2}{(1-\alpha)P|\mathbf{h}_e\mathbf{n}_o|^2+1}\right)\right\}. \quad (37)$$

We will maximize the bound in (37). Note that similar technique to use a derived bound to analyze the relationship between the capacity loss due to quantization can also be found in [23]. The bound in (37) is generally tight when N_{QA} is sufficiently large. This is because the interference leakage to the legitimate receiver decreases as N_{QA} increases; in addition, the random variable $\alpha P\|\mathbf{h}_l\|^2\cos^2\theta$ is generally concentrated to its mean and it turns out to be more concentrated when logarithm is performed to this random variable. As a result, the analytical results are close to the simulation results as will be verified later in simulations.

To obtain a close-form expression for the approximated upper bound of $\mathbb{E}\{R_s^\star\}$, we need to analyze two terms, i.e., $R_l^\star$ and $R_e^\star$ in the RHS of (37). The following Lemmas will help the analysis of $\mathbb{E}\{R_s^\star\}$.

Lemma 3: In the proposed system, $\mathbf{h}_e\mathbf{w}_o$ and $\mathbf{h}_e\mathbf{n}_o$ are statistically independent.

Proof: See Appendix A. □

From Lemma 3, we know that $|\mathbf{h}_e\mathbf{w}_o|^2$ and $|\mathbf{h}_e\mathbf{n}_o|^2$ are also statistically independent. Thus we are able to further analyze the mean value to $R_e^\star$ in the following Lemma.

Lemma 4: The mean value of $R_e^\star$ is defined as Z and can be expressed as in (38), shown at the bottom of the page. and$E_1(x)=\int_x^\infty \frac{e^{-t}}{t}dt$ is the exponential integral.

Proof: See Appendix B. □

For $R_l^\star$ in (37), the analysis of statistically relationship between $\|\mathbf{h}_l\|^2\cos^2\theta$ and $\|\mathbf{h}_l\|^2\cos^2\phi$ is necessary; thus, we give the following Lemma.

Lemma 5: In the proposed system, the covariance between $|\mathbf{h}_l\mathbf{w}_o|^2=\|\mathbf{h}_l\|^2\cos^2\theta$ and $|\mathbf{h}_l\mathbf{n}_o|^2=\|\mathbf{h}_l\|^2\cos^2\phi$ tends to be zero as N_{QA} approaches infinity.

Proof: See Appendix C. □

From Lemma 5, when N_{QA} is sufficiently large, we know that the covariance between numerator and dinominator of $R_l^\star$ in (37) is equal to zero approximately, so that we can obtain the approximated mean value to the SINR in (37).

Lemma 6: If N_{QA} is sufficiently large, the approximated mean value of the SINR in (37) at the legitimate receiver can be approximated by a product of X and Y given by

$$\mathbb{E}\left\{\frac{\alpha P\|\mathbf{h}_l\|^2\cos^2\theta}{(1-\alpha)P\|\mathbf{h}_l\|^2\cos^2\phi+1}\right\} \approx XY, \quad (39)$$

where X and Y are given in (40) and (41),

$$X=\frac{\alpha PM_t\left(1-N_{QB}\beta\left(N_{QB},\frac{M_t}{M_t-1}\right)\right)}{\frac{(1-\alpha)PM_t}{N_{QA}(M_t-1)+1}+1}, \quad (40)$$

$$Y=1+\frac{1}{\left(\frac{N_{QA}(M_t-1)+1}{(1-\alpha)PM_t}+1\right)^2} \times\left[\frac{2(M_t+1)\left(N_{QA}(M_t-1)+1\right)}{M_t\left(N_{QA}(M_t-1)+2\right)}-1\right]. \quad (41)$$

Proof: See Appendix D. □

From Lemmas 4 and 6, the following proposistion is obtained to approximated upper bound the average rate for the proposed scheme.

Proposition 2: In MISOSE channels, if N_{QA} is sufficiently large, the average secrecy rate for the proposed scheme can be approximately upper bounded by

$$\mathbb{E}\{R_s\} \lessapprox \log(1+XY)-Z, \quad (42)$$

where X, Y, and Z are defined in (40), (41) and (38), respectively.

Proof: This is a direct result using Lemmas 4 and 6. □

B. Bit Allocations for B_{QB} and B_{QA}

In this subsection, we consider how to distribute the total number of quantization bits B for B_{QB} and B_{QA} to maximize the average secrecy rate, which is described in the following proposition.

Proposition 3: In MISOSE channels, if N_{QA} is sufficiently large, the proposed bit allocation for maximizing the average secrecy rate for the proposed quantization scheme is given by

$$B_{QA}^\star=\begin{cases}B_{QA}^{round}, & B_{QA}^{round}<B,\\ B, & B_{QA}^{round}\ge B,\end{cases} \quad (43)$$

where B_{QA}^{round} is given in (44),

$$B_{QA}^{round}\approx round\left[\frac{B}{M_t}+\frac{M_t-1}{M_t}\left\{\log\left((1-\alpha)P\right)+\log \times\left(\frac{M_t}{(M_t-1)\Gamma\left(\frac{M_t}{M_t-1}\right)}\right)\right\}\right]. \quad (44)$$

Proof: See Appendix E. □

Some observations can be made from (43) and (44). First the proposed bit allocation is related to the number M_t of

$$Z=\mathbb{E}\left\{\log\left(1+\frac{\alpha P|\mathbf{h}_e\mathbf{w}_o|^2}{(1-\alpha)P|\mathbf{h}_e\mathbf{n}_o|^2+1}\right)\right\}=\begin{cases}\log e\cdot\left(1-\frac{2}{P}e^{\frac{2}{P}}E_1\left(\frac{2}{P}\right)\right), & \alpha=0.5,\\ \log e\cdot\left(\frac{\alpha}{1-2\alpha}\left[e^{\frac{1}{(1-\alpha)P}}E_1\left(\frac{1}{(1-\alpha)P}\right)-e^{\frac{1}{\alpha P}}E_1\left(\frac{1}{\alpha P}\right)\right]\right), & \text{otherwise}\end{cases} \quad (38)$$

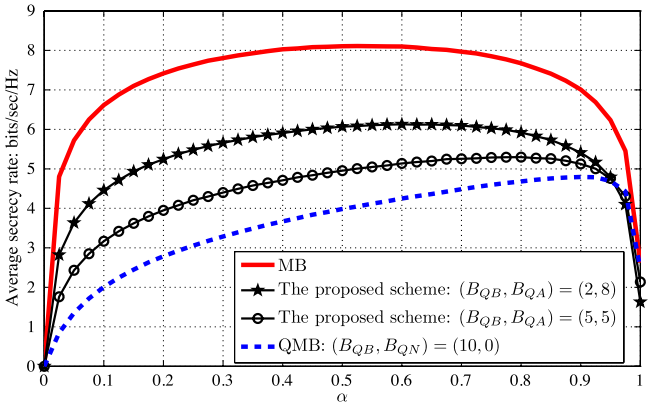

Fig. 4. Average secrecy rates as functions of α for various schemes with $P = 25$ dB and $M_t = 4$.

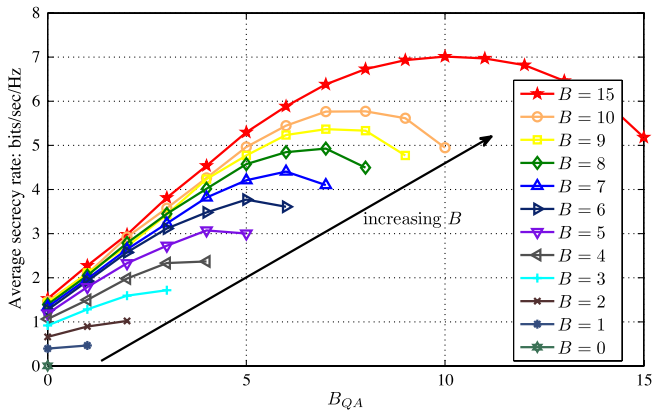

Fig. 5. Average secrecy rates as functions of B_{QA} for $B = 10$ and 15 with $P = 25$ dB, $M_t = 4$, and $\alpha = 0.5$.

transmit antennas, the parameter α of power allocation and the total transmission power P. For general value of P, as M_t increases, $B^{\star}_{QA}$ decreases and this implies that more bits should be allocated to the beamforming vector. Thus when M_t is sufficiently large, the proposed scheme reduces to the QMB scheme. Moreover, when the power of AN increases, i.e., decreasing α, or when the transmission power P increases, $B^{\star}_{QA}$ increases and this implies that more bits should be allocated to quantize one AN vector direction to maximize the average secrecy rate. On the other hand, for large value of P, $B^{\star}_{QA} = B$. This implies that using high transmission power leads to eavesdropping more easily. Thus so we need to increase B_{QA} to combat the eavesdropping.

V. Simulation Results

Simulation results are provided to verify the analytical results in this section. The settings of the simulations are as follows: The channel coefficients of $\mathbf{h}_l$ are i.i.d. complex Gaussian distributed with zero mean and unit variance. The number M_t of transmit antennas is 4. The RVQ-based codebooks are generated using the numerical methods in [24] and [26]. The average secrecy rate is computed using more than 100 000 iterations. The total number of quantization bits is $B = B_{QB} + B_{QA}$. For the proposed scheme, we use (B_{QB}, B_{QA}) to represent the numbers of quantization bits for the beamforming vector and linearly combined vector of AN directions, respectively. For the conventional scheme, i.e., QMB in Section II-B, we use $(B, 0)$ to represent that all bits are used to quantize the beamforming vector, and all AN directions are generated via the quantized beamforming vector.

Experiment 2. Secrecy Rates for Various Values of Power Allocation α: Let SNR $= 25$ dB and $B = 10$, Fig. 4 shows the average secrecy rates as functions of various values of α in MISOSE channels. The average secrecy rate with full CSI is provided to serve as a performance benchmark. Observe that the proposed idea to allocate some bits to quantize the vector in AN directions indeed lead to a better performance than to allocate all bits to quantize the beamforming vector (see the star, circle and dash lines). The proposed bit allocation for B_{QB} and B_{QA} in Proposition 3 can further improve the performance (see the star and the circle lines). To see this, we run all combinations of bit allocations. i.e., $(B_{QB}, B_{QA}) \in \{(0, 10), (1, 9), \ldots, (10, 0)\}$, the maximum average secrecy rate is obtained when the bit allocation is (2,8) and $\alpha \approx 0.6$. Note that when we set $\alpha = 0.6$, $M_t = 5$, and $P = 25$ dB, and substitute it to (44), we can theoretically obtain the bit allocation (2, 8) as well. Therefore from this example, the proposed quantization and bit allocation schemes can significantly increase the average secrecy rate when full CSI is not available.

Experiment 3. Secrecy Rates for Various Values of B_{QA}: Let SNR $= 25$ dB and the power allocation $\alpha = 0.5$, the average secrecy rates as functions of B_{QA} are shown in Fig. 5 for $B = 0, 1, \ldots, 10$ and 15. Observe that allocating an appropriate value for B_{QA} is important because it significantly affects the average secrecy rate. That is, using inappropriate value of B_{QA} can seriously degrade the average secrecy rate. This again shows that the proposed bit allocation is important in improving the average secrecy rate. To verify the correctness of the proposed bit allocation $B^{\star}_{QA}$ in (44), we use this equation to plot $B^{\star}_{QA}$ as a function of B in Fig. 6. From Fig. 6, the proposed bit allocations $B^{\star}_{QA} = 8$ when $B = 10$, and $B^{\star}_{QA} = 10$ for $B = 15$. Also the size of step in Fig. 6 is equal to 4 determined by the number of transmit antennas M_t due to the first term of B^{round}_{QA} in (44). These analytical results are accurate because the simulation results in Fig. 5 also show that the proposed bit allocations are 8 for $B = 10$. Moreover, from these two figures, we find that as the value of B decreases, the importance of $B^{\star}_{QA}$ becomes more pronounced. That is, when B is moderate, one should allocate most of the bits to quantize the vector in AN directions instead of the beamforming vector; for instance, when $B = 10$, $B^{\star}_{QA} = 8$ and thus $B^{\star}_{QB} = 2$. Because in practical systems, the number of quantization bits (feedback bits) is moderate to avoid long latency, these observations show valuable contributions of the proposed scheme in practical designs. Further, when $B \leq 8$, Fig. 6 shows that we should allocate all feedback bits for $B^{\star}_{QA}$ to improve the average secrecy rate.

Experiment 4. Average Secrecy Rates for Various Values of Total Transmit Power P: Let $B = 10$, Fig. 7 shows the average secrecy rates as functions of P for the proposed scheme and the conventional scheme QMB. For each scheme, the value of α is obtained by observing Fig. 4, where $\alpha = 0.6$ for the

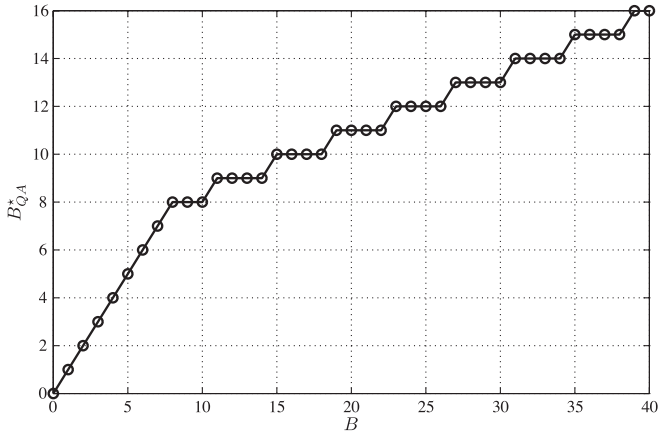

Fig. 6. $B^{\star}_{QA}$ as functions of B with $P = 25$ dB, $M_t = 4$, and $\alpha = 0.5$.

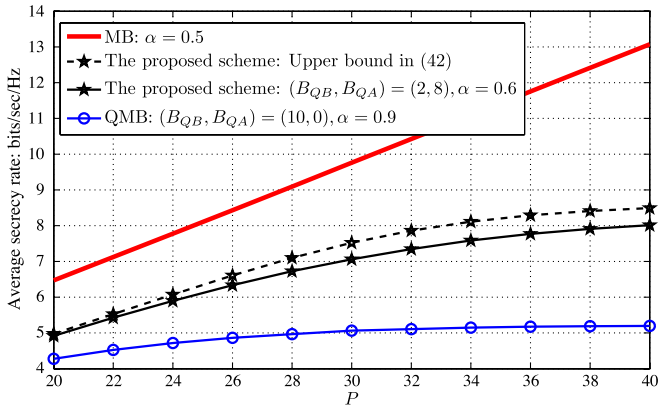

Fig. 7. Average secrecy rates as functions of P for various schemes with $M_t = 4$.

proposed scheme and $\alpha = 0.9$ for QMB. Observe that the derived result in (42) and the simulation result have similar trend. Also, the average the secrecy rate of QMB tends to saturate as P increases; that is, increasing SNR does not improve the average secrecy rate because it increases the interference at the legitimate receiver as well. On the other hand, the proposed scheme can still improve the average secrecy rate as P increases thanks to the reduced interference at the legitimate receiver.

Experiment 5. Secrecy Outage Probability for Various Outage Transmission Rates: In this example, the secrecy outage probability $Prob[R_s \leq R_{outage}]$ is evaluated, where $Prob[\cdot]$ represents the probability function and R_{outage} is a outage transmission rate. Let $M_t = 4$, $P = 25$ dB, and $B = 10$. For each scheme, the suitable value of α and the proposed bit allocation can be obtained by observing Figs. 4 and 6, where $\alpha = 0.6$ and bit allocation (2,8) for the proposed scheme, and $\alpha = 0.9$ for QMB. The outage performance is shown in Fig. 8. Observe that although the performance of the proposed scheme and QMB is comparable for $0 \leq R_{outgae} \leq 1$, the proposed scheme outperforms QMB when $R_{outage} > 1$. This is reasonable because the interference at the legitimate receiver is reduced significantly.

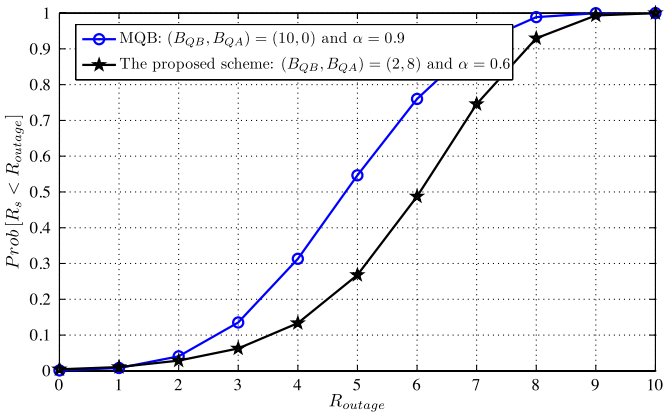

Fig. 8. Secrecy outage rates as functions of R_{outage} for various schemes with $M_t = 4$, $B = 10$, and $P = 25$ dB.

VI. Conclusion

In this paper, we have investigated how to quantize masked beamforming systems with only partial CSI at the legitimate receiver, so as to maximize the secrecy rate. Analytical results have shown that the interference at the legitimate receiver can be significantly reduced by separately quantizing the beamforming vector and the AN vector. Hence, the proposed quantization scheme has two codebooks; one is for the beamforming vector and the other is for the AN vector. Moreover, we have analyzed the secrecy rate of the proposed quantization scheme. Form this analytical result, we have further derived the best bit allocation for the two codebooks of the proposed quantization scheme. The proposed bit allocation has indicated that more bits should be allocated to quantize the AN vector when the total bit budget is not large. That is, when the bit budget is moderate, the leaked interference at the legitimate receiver dominates the performance. In this case, allocating more bits to quantize the AN vector for better preventing the leakage can significantly improve the performance. On the other hand, when the bit budget is sufficiently high, allocating all bits to quantize the beamforming vector and then determining the null space based on the quantized beamforming vector is good enough to control the leakage; hence the conventional quantization scheme in [17] and [18] may work well in this case. Finally, simulation results have been provided to show the correctness of the analytical results, and demonstrate that the proposed quantization together with the bit allocation schemes can significantly improve the secrecy rate compared to the conventional quantization scheme.

Appendix

A. Proof of Lemma 3

Using the definitions of (12) and (25), the quantized beamforming vector and the null space can be represented, respectively, by $\mathbf{p} = \sqrt{\cos^2\theta}\mathbf{w}_o + \sqrt{1-\cos^2\theta}\mathbf{e}_w$ and $\mathbf{n} = \sqrt{\cos^2\phi}\mathbf{n}_o + \sqrt{1-\cos^2\phi}\mathbf{e}_n$ [24], where $\mathbf{n}$ is a unit norm random vector that belongs to the null space of $\mathbf{h}_l$, $\mathbf{e}_w$ is the quantization error of the beamforming vector, and $\mathbf{e}_n$ is the

quantization error of the null space. Both $\mathbf{e}_w$ and $\mathbf{e}_n$ are unit norm random vectors because $\|\mathbf{p}\|^2 = 1$ and $\|\mathbf{n}\|^2 = 1$. Since RVQ is used to generate the two independent codebooks $\mathcal{W}$ and $\mathcal{N}$, $\mathbf{e}_w$ and $\mathbf{e}_n$ are independent and zero mean. Also, $\mathbf{e}_w$ and $\mathbf{e}_n$ are independent of $\mathbf{p}$ and $\mathbf{n}$; that is, the quantization error is independent of the value to be quantized due to the use of RVQ. Therefore, $\mathbf{e}_w$ and $\sqrt{1-\cos^2\theta}$ are independent, and $\mathbf{e}_n$ and $\sqrt{1-\cos^2\phi}$ are independent.

Because $\mathbf{h}_e \sim \mathcal{CN}(\mathbf{0}, \mathbf{I}_{M_t})$ and the linear combination of independent Gaussian random variables is still a Gaussian random variable, both $\mathbf{h}_e\mathbf{w}_o$ and $\mathbf{h}_e\mathbf{n}_o$ have Gaussian distribution. Also, two Gaussian random variables are independent if they are uncorrelated. Therefore, the dependence of $\mathbf{h}_e\mathbf{w}_o$ and $\mathbf{h}_e\mathbf{n}_o$ is characterized by the correlation. Then the correlation is given by

$$\begin{aligned}\mathbb{E}\left\{\mathbf{w}_o^H\mathbf{h}_e^H\mathbf{h}_e\mathbf{n}_o\right\} &= \mathbb{E}\left\{\mathbf{w}_o^H\mathbf{n}_o\right\} \\ &= \mathbb{E}\left\{\left(\sqrt{\frac{1}{\cos^2\theta}}\mathbf{p}^H - \sqrt{\frac{1-\cos^2\theta}{\cos^2\theta}}\mathbf{e}_w^H\right)\right. \\ &\quad \left.\cdot\left(\sqrt{\frac{1}{\cos^2\phi}}\mathbf{n} - \sqrt{\frac{1-\cos^2\phi}{\cos^2\phi}}\mathbf{e}_n\right)\right\} = 0,\end{aligned}$$

where the second equality holds due to that $\mathbf{h}_e \sim \mathcal{CN}(\mathbf{0}, \mathbf{I}_{M_t})$. In addition, $\mathbf{p}$ is orthogonal to $\mathbf{n}$, i.e., $|\mathbf{p}^H\mathbf{n}| = 0$ and $\mathbb{E}\{\mathbf{p}^H\mathbf{e}_n\} = \mathbb{E}\{\mathbf{p}^H\}\mathbb{E}\{\mathbf{e}_n\} = 0$ since $\mathbf{p}$ is independent of $\mathbf{e}_n$ and $\mathbb{E}\{\mathbf{e}_n\} = 0$. Similarly, one can show that $\mathbb{E}\{\mathbf{e}_w^H\mathbf{n}\} = 0$. The correlation is equal to zero; hence, $\mathbf{h}_e\mathbf{w}_o$ is independent of $\mathbf{h}_e\mathbf{n}_o$.

B. Proof of Lemma 4

From [33, chapter 5], we know that if $\mathbf{h}_e \in \mathbb{C}^{1\times M_t} \sim \mathcal{CN}(\mathbf{0}, \mathbf{I}_{M_t})$ and $\mathbf{U} \in \mathbb{C}^{M_t\times d}$ is a semi-unitary matrix, then $\|\mathbf{h}_e\mathbf{U}\|^2 \sim \chi^2_{2d}/2$ where χ^2_{2d} defines chi-square distribution withe degrees of freedom $2d$. Thus $|\mathbf{h}_e\mathbf{w}_o|^2 = w/2 \sim \chi^2_2/2$ and $|\mathbf{h}_e\mathbf{n}_o|^2 = v/2 \sim \chi^2_2/2$, and w and v both have exponential distribution with parameter 1/2, according to the definition of chi-square distribution. Hence the mean value of $R_e^\star$ in (37) can be expressed as

$$\begin{aligned}\mathbb{E}\left\{R_e^\star\right\} &= \mathbb{E}\left\{\log\left(\frac{\alpha w + (1-\alpha)v + \frac{2}{P}}{(1-\alpha)v + \frac{2}{P}}\right)\right\} \\ &= \mathbb{E}\left\{\log\left(z + \frac{2}{P}\right)\right\} - \mathbb{E}\left\{\log\left((1-\alpha)v + \frac{2}{P}\right)\right\},\end{aligned} \tag{45}$$

where $z = \alpha w + (1-\alpha)v$, $z \in [0, \infty)$. From Lemma 3, w and v are statistically independent. Let $z = \alpha w + (1-\alpha)v$, the PDF of z that is given by

$$f_z(z) = \begin{cases} ze^{-z}, & \alpha = 0.5, \\ \frac{1}{2(1-2\alpha)}\left(e^{-\frac{z}{2(1-\alpha)}} - e^{-\frac{z}{2\alpha}}\right), & \text{otherwise.}\end{cases} \tag{46}$$

By applying the integration formulation in (47), [34],

$$\begin{aligned}\int_0^\infty \ln(1+ax)x^b e^{-x}dx &= \sum_{i=0}^{b}\frac{b!}{(b-i)!} \\ &\times\left[\sum_{j=1}^{b-i}(j-1)!\left(-\frac{1}{a}\right)^{b-i-j} - \frac{(-1)^{b-i-1}}{a^{b-i}}e^{1/a}E_1\left(\frac{1}{a}\right)\right],\end{aligned} \tag{47}$$

the equation (45) can be further manipulated to obtain (38). □

C. Proof of Lemma 5

For presentation convenience, let $|\mathbf{h}_l\mathbf{w}_o|^2 = \zeta$, $|\mathbf{h}_l\mathbf{n}_o|^2 = \delta$, and the covariance between ζ and δ be $C_{\zeta,\delta}$. The following inequality holds for random variables with the finite variance:

$$|C_{\zeta,\delta}| \le \sqrt{\sigma_\zeta^2 \cdot \sigma_\delta^2}, \tag{48}$$

where σ_ζ^2 and σ_δ^2 is the variance of ζ and δ respectively; thus, $C_{\zeta,\delta}$ is upper bounded by (48). From (12), σ_ζ^2 can be formulated as

$$\sigma_\zeta^2 = \mathbb{E}\left\{\|\mathbf{h}_l\|^4\cos^4\theta\right\} - \left(\mathbb{E}\left\{\|\mathbf{h}_l\|^2\cos^2\theta\right\}\right)^2.$$

The author in [30, Section 7] showed that $\|\mathbf{h}_l\|^2$ is independent of $\cos^2\theta$ and $\cos^2\phi$; hence, σ_ζ^2 can be rewritten below:

$$\sigma_\zeta^2 = \mathbb{E}\left\{\|\mathbf{h}_l\|^4\right\}\mathbb{E}\{\cos^4\theta\} - \left(\mathbb{E}\left\{\|\mathbf{h}_l\|^2\right\}\mathbb{E}\left\{\cos^2\theta\right\}\right)^2. \tag{49}$$

To obtain σ_ζ^2, we discuss each term in (49) as follows: Using the following integral representation for the beta function [31, p. 5]:

$$\beta\left(c, \frac{a}{b}\right) = b\int_0^1 x^{a-1}(1-x^b)^{c-1}dx, \text{ for } a, b, \text{ and } c > 0,$$

and the CDF of $1-\cos^2\theta$ in [24, p. 11], we have the following formula:

$$\mathbb{E}\left\{(1-\cos^2\theta)^2\right\} = N_{QB}\beta\left(N_{QB}, \frac{M_t+1}{M_t-1}\right).$$

Because $\mathbb{E}\{\cos^4\theta\} = \mathbb{E}\{(1-\cos^2\theta)^2\} + 2\mathbb{E}\{\cos^2\theta\} - 1$, and from [26, Lemma 1 and Eq. (13)] $\mathbb{E}\{\cos^2\theta\}$ has the following representation:

$$\mathbb{E}\{\cos^2\theta\} \equiv \mu_{\cos^2\theta} = 1 - N_{QB}\beta\left(N_{QB}, \frac{M_t}{M_t-1}\right), \tag{50}$$

$\mathbb{E}\{\cos^4\theta\}$ can be written as

$$\mathbb{E}\{\cos^4\theta\} = N_{QB}\beta\left(N_{QB}, \frac{M_t+1}{M_t-1}\right) + 2\mu_{\cos^2\theta} - 1. \tag{51}$$

In addition, since the random variable $\|\mathbf{h}_l\|^2$ has the chi-square distribution with $2M_t$ degrees of freedom, the moments of $\|\mathbf{h}_l\|^2$ can be expressed as $\mathbb{E}\{\|\mathbf{h}_l\|^{2m}\} = \Gamma(m+M_t)/\Gamma(M_t)$ [32]. Hence we have

$$\mathbb{E}\left\{\|\mathbf{h}_l\|^4\right\} = M_t(M_t+1). \tag{52}$$

By substituting (50), (51), and (52) into (49), a closed-form of σ_ζ^2 can be expressed as (53),

$$\sigma_\zeta^2 = M_t(M_t+1)\left[N_{QB}\beta\left(N_{QB}, \frac{M_t+1}{M_t-1}\right) + 2\mu_{\cos^2\theta} - 1\right] - (M_t\mu_{\cos^2\theta})^2. \tag{53}$$

Similarly, σ_δ^2 can be written as

$$\sigma_\delta^2 = \mathbb{E}\left\{\|\mathbf{h}_l\|^4\right\}\mathbb{E}\{\cos^4\phi\} - \left(\mathbb{E}\left\{\|\mathbf{h}_l\|^2\right\}\mathbb{E}\{\cos^2\phi\}\right)^2. \tag{54}$$

Using (32) and $\mathbb{E}\{\cos^4\phi\} = \int_0^1 x^2 dF(x_{\min})$, $\mathbb{E}\{\cos^4\phi\}$ can be expressed as

$$\mathbb{E}\{\cos^4\phi\} = \frac{2}{\left(N_{QA}(M_t-1)+1\right)\left(N_{QA}(M_t-1)+2\right)}. \tag{55}$$

Substituting (33), (52), and (55) into (54), a closed-form of σ_δ^2 can be expressed as (56),

$$\sigma_\delta^2 = \left[\frac{M_t}{N_{QA}(M_t-1)+1}\right]^2\left[\frac{2(M_t+1)\left(N_{QA}(M_t-1)+1\right)}{M_t\left(N_{QA}(M_t-1)+2\right)} - 1\right]. \tag{56}$$

From (56), σ_δ^2 tends to be zero when N_{QA} approaches ∞. Since $C_{\zeta,\delta}$ is upper bounded by the square root of the product of σ_ζ^2 and σ_δ^2, $C_{\zeta,\delta}$ tends to be zero as the value of N_{QA} approaches ∞, and this completes the proof. □

D. Proof of Lemma 6

Let us define $x = \alpha P\|\mathbf{h}_l\|^2\cos^2\theta$, $y = (1-\alpha)P\|\mathbf{h}_l\|^2\cos^2\phi + 1$ and $g(x,y) = x/y$. The mean value of a function $g(x,y)$ of two random variables can be expressed approximately to (57) [32, p. 215],

$$\mathbb{E}\{g(x,y)\} \approx g(\mu_x,\mu_y) + \frac{1}{2}\left(\frac{\partial^2 g(\mu_x,\mu_y)}{\partial x^2}\sigma_x^2 + 2\frac{\partial^2 g(\mu_x,\mu_y)}{\partial x\partial y}C_{xy} + \frac{\partial^2 g(\mu_x,\mu_y)}{\partial y^2}\sigma_y^2\right), \tag{57}$$

where the mean values of x and y are μ_x and μ_y respectively, and σ_y^2 is the variance of y. Also, C_{xy} is the covariance between x and y. From Lemma 5, the covariance C_{xy} is approximately zero when N_{QA} is sufficiently large. Therefore we have

$$\mathbb{E}\left\{\frac{\alpha P\|\mathbf{h}_l\|^2\cos^2\theta}{(1-\alpha)P\|\mathbf{h}_l\|^2\cos^2\phi+1}\right\} \approx \frac{\mu_x}{\mu_y}\left(1+\frac{1}{\mu_y^2}\sigma_y^2\right). \tag{58}$$

A closed-form expression for μ_x in (58) is equal to $\alpha PM_t\mu_{\cos^2\theta}$, where $\mu_{\cos^2\theta}$ is given by (50), which is expressed as

$$\mu_x = \alpha PM_t\mu_{\cos^2\theta} = \alpha PM_t\left(1 - N_{QB}\cdot\beta\left(N_{QB}, \frac{M_t}{M_t-1}\right)\right). \tag{59}$$

From (34), μ_y in (58) can be expressed as

$$\mu_y = \mathbb{E}\left\{(1-\alpha)P\|\mathbf{h}_l\|^2\cos^2\phi + 1\right\} = \frac{(1-\alpha)PM_t}{N_{QA}(M_t-1)+1} + 1, \tag{60}$$

and σ_y^2 is equal to $(1-\alpha)^2P^2\sigma_\delta^2$; hence, the variance of y can be expressed as (61),

$$\sigma_y^2 = \left[\frac{(1-\alpha)PM_t}{N_{QA}(M_t-1)+1}\right]^2\left[\frac{2(M_t+1)\left(N_{QA}(M_t-1)+1\right)}{M_t\left(N_{QA}(M_t-1)+2\right)} - 1\right]. \tag{61}$$

Using (58), (59), (60), and (61), the lemma is proved. □

E. Proof of Proposition 3

We take the derivatives of X, Y and Z in (42) respectively to obtain the proposed bit allocation B_{QA}. Since Z in (42) is irrelevant to B_{QA}, this term can be ignored. We assume that $N_{QA} = 2^{B_{QA}}$ is sufficiently large, so σ_y^2 in (61) is approximately zero. That is, Y in (42) can be approximated by $Y \approx 1$. In this case, the problem is simplified to taking the derivative of X in (42) and setting it to zero, i.e.,

$$\frac{\partial X}{\partial N_{QA}} = \frac{\partial}{\partial N_{QA}}\left(\frac{\mu_x}{\mu_y}\right) = 0, \tag{62}$$

where μ_x and μ_y are both functions of $N_{QB} = N/N_{QA}$ defined in (59) and (60). From (59) and (60), we know that $\mu_x \geq 0$ and $\mu_y \geq 1$ for arbitrary N_{QA}; hence, (62) can be rewritten as

$$\frac{\partial\mu_x}{\partial N_{QA}}\mu_y - \mu_x\frac{\partial\mu_y}{\partial N_{QA}} = 0. \tag{63}$$

The bit allocation can be obtained by taking the derivatives of μ_x and μ_y with respect to N_{QB}. Once a suggested value of N_{QB} is obtained, denoted by $N_{QA}^\star$, the value of N_{QA} can be determined from $N_{QB}^\star = N/N_{QA}^\star$, as defined in (19).

The derivative of μ_x can be expressed as

$$\frac{\partial\mu_x}{\partial N_{QA}} = \frac{2^B}{N_{QA}}\beta\left(\frac{2^B}{N_{QA}}, \frac{M_t}{M_t-1}\right)h = \left(1-\frac{\mu_x}{\alpha PM_t}\right)h, \tag{64}$$

where h is defined

$$h = \alpha PM_t\left\{\frac{1}{N_{QA}} + \frac{2^B}{N_{QA}^2}\left[\psi\left(\frac{2^B}{N_{QA}}\right) - \psi\left(\frac{2^B}{N_{QA}} + \frac{M_t}{M_t-1}\right)\right]\right\},$$

and $\psi(\cdot)$ is the digamma function.

The derivative of μ_y is given by

$$\frac{\partial \mu_y}{\partial N_{QA}} = -\frac{(1-\alpha)PM_t(M_t-1)}{\left[N_{QA}(M_t-1)+1\right]^2} = -\frac{M_t-1}{(1-\alpha)PM_t}(\mu_y-1)^2. \quad (65)$$

By using (64) and (65), one can rewrite (62) as

$$\left(1-\frac{\mu_x}{\alpha PM_t}\right)h\mu_y + \frac{M_t-1}{(1-\alpha)PM_t}\mu_x(\mu_y-1)^2 = 0. \quad (66)$$

From (66), an obvious solution can be obtained by satisfying the following conditions:

$$\begin{cases} \frac{\mu_x}{\alpha PM_t} = 1, \\ \mu_y = 1. \end{cases}$$

Using these conditions, one can obtain the following result:

$$\frac{2^B}{N_{QA}^\star}\beta\left(\frac{2^B}{N_{QA}^\star}, \frac{M_t}{M_t-1}\right) = \frac{(1-\alpha)PM_t}{N_{QA}^\star(M_t-1)+1}. \quad (67)$$

Because $N_{QA}^\star$ in the RHS of (67) is larger than one, (67) can be approximated by

$$\frac{2^B}{N_{QA}^\star}\beta\left(\frac{2^B}{N_{QA}^\star}, \frac{M_t}{M_t-1}\right) \approx \frac{(1-\alpha)PM_t}{N_{QA}^\star(M_t-1)}. \quad (68)$$

In addition, we know that for beta function $\beta(a,b)$ if b is fixed and a is larger than b, then we have the following approximation:

$$\beta(a,b) \approx \Gamma(b)a^{-b}.$$

Using this approximation, (68) can be approximated by

$$2^B\left[\Gamma\left(\frac{M_t}{M_t-1}\right)\left(\frac{N_{QA}^\star}{2^B}\right)^{\frac{M_t}{M_t-1}}\right] \approx \frac{(1-\alpha)PM_t}{(M_t-1)}. \quad (69)$$

From (69), the suggested value of N_{QA} should be

$$N_{QA}^\star \approx 2^B\left[2^{-B}\frac{(1-\alpha)PM_t}{(M_t-1)\Gamma\left(\frac{M_t}{M_t-1}\right)}\right]^{\frac{M_t-1}{M_t}}. \quad (70)$$

It is worth pointing out that letting $\alpha = 1$ in (70) and thus $N_{QA} = 0$ can be regarded as a special case of the derived solution in (70); letting $\alpha = 1$ implies that the bit budget B is all assigned to quantize the beamforming vector.

In deriving N^{QA}, we use the approximated upper bound of the average secrecy rate in (42) and the assumption of large value of $N_{QA} = 2^{B_{QA}}$. Thus, the value B^{QA} may exceed the total bit budget B, when B is small or P is large. To avoid exceeding total bit budget, we take the log and *round* functions to (70), and this new term becomes $B_{QA}^{round} = round[\log(N_{QA}^\star)]$ as that in (44). □

ACKNOWLEDGMENT

The authors would like to thank the anonymous reviewers and the editor for their constructive suggestions, which have significantly improved the quality of this work.

REFERENCES

[1] I. Csiszár and J. Körner, "Broadcast channels with confidential messages," *IEEE Trans. Inf. Theory*, vol. IT-24, no. 3, pp. 339–348, May 1978.
[2] P. Gopala, L. Lai, and H. El Gamal, "On the secrecy capacity of fading channels," *IEEE Trans. Inf. Theory*, vol. 54, no. 10, pp. 4687–4698, Oct. 2008.
[3] S. Shafiee and S. Ulukus, "Achievable rates in Gaussian MISO channels with secrecy constraints," in *Proc. IEEE Int. Symp. Inf. Theory*, 2007, pp. 2466–2470.
[4] A. Khisti and G. W. Wornell, "Secure transmission with multiple antennas I: The MISOME wiretap channel," *IEEE Trans. Inf. Theory*, vol. 56, no. 7, pp. 3088–3104, Jul. 2010.
[5] A. Khisti and G. W. Wornell, "Secure transmission with multiple antennas II: The MIMOME wiretap channel," *IEEE Trans. Inf. Theory*, vol. 56, no. 11, pp. 5515–5532, Nov. 2010.
[6] R. Bustin, R. Liu, H. V. Poor, and S. Shamai, "An MMSE approach to secrecy capacity of the MIMO Gaussian wiretap channel," *EURASIP J. Wireless Commun. Netw.*, vol. 2009, no. 1, Jul. 2009, Art. ID. 370 970.
[7] R. Liu, T. Liu, H. V. Poor, and S. Shamai, "Multiple-input multiple-output Gaussian broadcast channels with confidential messages," *IEEE Trans. Inf. Theory*, vol. 56, no. 9 pp. 4215–4227, Sep. 2010.
[8] 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.
[9] S. A. A. Fakoorian and A. L. Swindlehurst, "MIMO interference channel with confidential messages: Achievable secrecy rates and precoder design," *IEEE Trans. Inf. Forensics Security*, vol. 6, no. 3, pp. 640–649, Sep. 2011.
[10] Q. Li *et al.*, "Transmit solutions for MIMO wiretap channels using alternating optimization," *IEEE J. Sel. Areas Commun.*, vol. 31, no. 9, pp. 1714–1726, Sep. 2013.
[11] S. Goel and R. Negi, "Guaranteeing secrecy using artificial noise," *IEEE Trans. Wireless Commun.*, vol. 7, no. 6, pp. 2180–2189, Jun. 2008.
[12] 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.
[13] S. Gerbracht, C. Scheunert, and E. A. Jorswieck, "Secrecy outage in MISO systems with partial channel information," *IEEE Trans. Inf. Forensics Security*, vol. 7, no. 2, pp. 704–716, Apr. 2012.
[14] Q. Li and W.-K. Ma, "A robust artificial noise aided transmit design for MISO secrecy," in *Proc. IEEE ICASSP*, Prague, Czech Republic, May 2011, pp. 3436–3439
[15] N. Romero-Zurita, D. McLernon, and M. Ghogho, "Physical layer security by robust masked beamforming and protected zone optimisation," *IET Commun.*, vol. 8, no. 8, pp. 1248–1257, May 2014.
[16] S.-H. Tsai and H. V. Poor, "Power allocation for artificial-noise secure MIMO precoding systems," *IEEE Trans. Signal Process.*, vol. 62, no. 13, pp. 3479–3493, Jul. 2014.
[17] 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.
[18] S. C. Lin, T. H. Chang, Y. L. Liang, Y. W. Hong, and C. Y. Chi, "On the impact of quantized channel feedback in guaranteeing secrecy with artificial noise: The noise leakage problem," *IEEE Trans. Wireless Commun.*, vol. 10, no. 3, pp. 901–915, Mar. 2011.
[19] A. El Gamal and Y. H. Kim, *Network Information Theory*. Cambridge, U.K.: Cambridge Univ. Press, 2011.
[20] N. Romero-Zurita, M. Ghogho, and D. McLernon, "Outage probability based power distribution between data and artificial noise for physical layer security," *IEEE Trans. Signal Lett.*, vol. 19, no. 2, pp. 71–74, Feb. 2012.
[21] 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.
[22] R. W. Heath, Jr. and A. Paulraj, "A simple scheme for transmit diversity using partial channel feedback," in *Proc. 32nd Annu. Asilomar Conf. Signal Syst. Comput.*, Nov. 1998, vol. 2, pp. 1073–1078.
[23] D. Love, R. W. Heath, Jr., and T. Strohmer, "Grassmannian beamforming for multiple-input multiple-output wireless systems," *IEEE Trans. Inf. Theory*, vol. 49, no. 10, pp. 2735–2747, Oct. 2003.

[24] N. Jindal, "MIMO broadcast channels with finite-rate feedback," *IEEE Trans. Inf. Theory*, vol. 52, no. 11, pp. 5045–5060, Nov. 2006.
[25] J. C. Roh and B. D. Rao, "Transmit beamforming in multiple-antenna systems with finite rate feedback: A VQ-based approach," *IEEE Trans. Inf. Theory*, vol. 52, no. 3, pp. 1101–1112, Mar. 2006.
[26] C. Au-Yeung and D. J. Love, "On the performance of random vector quantization limited feedback beamforming in a MISO system," *IEEE Trans. Wireless Commun.*, vol. 6, no. 2, pp. 458–462, Feb. 2007.
[27] T. Yoo, N. Jindal, and A. Goldsmith, "Multi-antenna broadcast channels with limited feedback and user selection," *IEEE J. Sel. Areas Commun.*, vol. 25, no. 7, pp. 1478–1491, Sep. 2007.
[28] M. Sharif and B. Hassibi, "On the capacity of MIMO broadcast channels with partial side information," *IEEE Trans. Inf. Theory*, vol. 51, no. 2, pp. 506–522, Feb. 2005.
[29] B. C. Arnold, N. Balakrishnan, and H. N. Nagaraja, *A First Course in Order Statistics*. New York, NY, USA: Wiley, 1992.
[30] A. T. James, "Distributions of matrix variates and latent roots derived from normal samples," *Ann. Math. Statist.*, vol. 35, no. 2, pp. 475–501, Jun. 1964.
[31] A. Gupta and S. Nadarajah, *Handbook of Beta Distribution and Its Application*. New York, NY, USA: Marcel Dekker, 2004.
[32] A. Papoulis and S. U. Pillai, *Probability, Random Variables and Stochastic Process*. New York, NY, USA: McGraw-Hill, 2002.
[33] A. M. Mathai and S. B. Provost, *Quadratic Forms in Random Variables*. New York, NY, USA: Marcel Dekker, 1992.
[34] I. S. Gradshteyn and I. M. Ryzhik, *Table of Integrals, Series, and Products*, 6th ed. New York, NY, USA: Academic, 2000.

Chia-Hua Lin was born in Hsinchu, Taiwan, in 1983. He received the M.S. and Ph.D. degrees in electrical and control engineering (ECE) from National Chiao-Tung University (NCTU), Hsinchu, Taiwan, in 2007 and 2015, respectively. From 2007 to 2009, he worked in MediaTek, Inc. (MTK), Taiwan, where he participated in the digital signal processing design for global positioning system (GPS).

His research interests include signal processing for communications, particularly in the areas of GPS, multiple-input-multiple-output (MIMO) wireless communications, physical-layer security, precoder design, and statistical signal processing.

Shang-Ho (Lawrence) Tsai (SM'12) was born in Kaohsiung, Taiwan, in 1973. He received the Ph.D. degree in electrical engineering from the University of Southern California (USC), Los Angeles, CA, USA, in August 2005. From June 1999 to July 2002, he was with the Silicon Integrated Systems Corp. (SiS), where he participated in the VLSI design for DMT-ADSL systems. From September 2005 to January 2007, he was with the MediaTek Inc. (MTK) participating in the VLSI design for MIMO-OFDM systems and standard specifications for IEEE 802.11n. From June 2013 to December 2013, he was a Visiting Fellow in the Department of Electrical Engineering, Princeton University. In February 2007, he joined the Department of Electrical and Control Engineering (now Department of Electrical Engineering), National Chiao Tung University where he is now an Associate Professor. His research interests are in the areas of signal processing for communications, statistical signal processing, and signal processing for VLSI designs.

Dr. Tsai was awarded a government scholarship for overseas study from the Ministry of Education, Taiwan, in 2002–2005.

Yuan-Pei Lin (S'93–M'97–SM'03) was born in Taipei, Taiwan, in 1970. She received the B.S. degree in control engineering from the National Chiao-Tung University, Hsinchu, Taiwan, in 1992, and the M.S. and Ph.D. degrees in electrical engineering from California Institute of Technology, Pasadena, CA, USA, in 1993 and 1997, respectively. In 1997, she joined the Department of Electrical and Control Engineering, National Chiao-Tung University, Hsinchu. Her research interests include digital signal processing, multirate filter banks, and signal processing for digital communications.

She was a recipient of the Ta-You Wu Memorial Award in 2004. She served as an associate editor for IEEE TRANSACTIONS ON SIGNAL PROCESSING, IEEE TRANSACTIONS ON CIRCUITS AND SYSTEMS II, IEEE SIGNAL PROCESSING LETTERS, IEEE TRANSACTIONS ON CIRCUITS AND SYSTEMS I, *EURASIP Journal on Applied Signal Processing*, and *Multidimensional Systems and Signal Processing*, Academic Press. She was a Distinquished Lecturer of the IEEE Circuits and Systems Society for 2006–2007. She has also coauthored two books, *Signal Processing and Optimization for Transmitter Systems*, and *Filter Bank Transmitters for OFDM and DMT Systems*, both by Cambridge University Press, 2010.