Secure Massive MIMO Communication With Low-Resolution DACs

Jindan Xu, *Student Member, IEEE*, Wei Xu, *Senior Member, IEEE*, Jun Zhu, *Member, IEEE*, Derrick Wing Kwan Ng, *Senior Member, IEEE*, and A. Lee Swindlehurst, *Fellow, IEEE*

Abstract—**In this paper, we investigate secure transmission in a massive multiple-input multiple-output system adopting low-resolution digital-to-analog converters (DACs). Artificial noise (AN) is deliberately transmitted simultaneously with the confidential signals to degrade the eavesdropper's channel quality. By applying the Bussgang theorem, a DAC quantization model is developed which facilitates the analysis of the asymptotic achievable secrecy rate. Interestingly, for a fixed power allocation factor ϕ, low-resolution DACs typically result in a secrecy rate loss, but in certain cases, they provide superior performance, e.g., at low signal-to-noise ratio (SNR). Specifically, we derive a closed-form SNR threshold which determines whether low-resolution or high-resolution DACs are preferable for improving the secrecy rate. Furthermore, a closed-form expression for the optimal ϕ is derived. With AN generated in the null-space of the user channel and the optimal ϕ, low-resolution DACs inevitably cause secrecy rate loss. On the other hand, for random AN with the optimal ϕ, the secrecy rate is hardly affected by the DAC resolution because the negative impact of the quantization noise can be compensated by reducing the AN power. All the derived analytical results are verified by numerical simulations.**

Index Terms—**Physical layer security, massive multiple-input multiple-output (MIMO), digital-to-analog converter (DAC), artificial noise (AN).**

I. Introduction

SECRECY plays an important role in wireless communications since it is difficult for a broadcast channel to shield transmit signals from unintended recipients. Traditionally, secure transmission relies on key-based cryptographic methods implemented at the network and application layers [1]. However, these cryptographic measures are based on the assumption that it is computationally infeasible for the encrypted message to be deciphered within a reasonable amount of time. Consequently, they inevitably become more vulnerable as the computational capability of the adversary grows. In the past decade, physical layer security, as a complement to existing cryptographic methods, has gained increasing attention [2]–[4]. With appropriate designs, physical layer techniques enable secure communication over a wireless medium without the help of encryption keys [5]–[7]. In addition, they can be used to augment already existing security measures at higher layers, leading to a multilayer secure transmission [8].

The classical three-terminal security model, known as the wiretap channel, was originally proposed in [9], consisting of a transmitter (Alice), an intended receiver (Bob), and an unauthorized receiver (Eve) referred to as an eavesdropper. This concept has been extended to multi-antenna networks [10], [11], while beamforming techniques have been utilized in multiple-input multiple-output (MIMO) systems to improve secrecy [12]. When the instantaneous channel state information (CSI) of the eavesdropper is known at the transmitter, it has been demonstrated in [13] that the generalized singular value decomposition (GSVD) precoding scheme can achieve the secrecy capacity in the high signal-to-noise ratio (SNR) limit. The study in [14] showed that secret communication is possible if the eavesdropper's channel is more noisy than the user channel. When the eavesdropper happens to have a better channel than the legitimate user (e.g., if the eavesdropper is much closer to the transmitter), artificial noise (AN) has been proposed in [15] and [16] to help degrade the channel quality of the eavesdropper. The AN is usually designed to be orthogonal to the channel of the intended receivers, thus causing no additional interference to the legitimate users [17], [18]. In order to further combat the uncertainty of channel information at the transmitter, robust beamforming design for physical layer security with the aid of AN has been studied in [19].

Recently, massive MIMO has become a candidate technology for next-generation wireless communication systems [20]–[23] and its application to guarantee communication security has attracted significant attention. In massive MIMO, hundreds, or even thousands, of antennas are equipped at the base station (BS) [24]–[26] and the corresponding spatial-wideband effect has been studied in [27]. For instance, downlink secure transmission at the physical layer in a multi-cell MIMO network has been investigated in [28] and

Manuscript received August 12, 2018; revised December 9, 2018; accepted January 18, 2019. Date of publication January 25, 2019; date of current version May 15, 2019. This work of W. Xu was supported in part by the NSFC under 61871109, the Open Research Fund of the State Key Lab of ISN under ISN18-03, and the Six Talent Peaks project in Jiangsu Province under GDZB-005. The work of D. W. K. Ng was supported in part by the Australian Research Council's Discovery Early Career Researcher Award under DE170100137 and Discovery Project under DP190101363. The work of A. L. Swindlehurst was supported in part by the U.S. National Science Foundation under grants ECCS-1547155 and CCF-1703635. The associate editor coordinating the review of this paper and approving it for publication was X. Wang. *(Corresponding author: Wei Xu).*

J. Xu and W. Xu are with the National Mobile Communications Research Laboratory, Southeast University, Nanjing 210096, China, and also with the State Key Laboratory of Integrated Services Networks, Xidian University, Xi'an 710071, China (e-mail: jdxu@seu.edu.cn; wxu@seu.edu.cn).

J. Zhu is with Qualcomm Inc., San Diego, CA 92121 USA (e-mail: junzhu@qti.qualcomm.com).

D. W. K. Ng is with the School of Electrical Engineering and Telecommunications, The University of New South Wales, Sydney, NSW 2052, Australia (e-mail: w.k.ng@unsw.edu.au).

A. L. Swindlehurst is with the Henry Samueli School of Engineering, University of California at Irvine, Irvine, CA 92697-2625 USA (e-mail: swindle@uci.edu).

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/TCOMM.2019.2895023

the impact of a massive MIMO relay on secrecy has been studied in [29]. Zhu *et al.* [30] have derived two tight lower bounds for the ergodic secrecy rate considering a maximal-ratio-combining (MRC) precoder. In order to strike a balance between complexity and performance, linear precoders based on matrix polynomials have been proposed in [31] and a phase-only zero-forcing (ZF) AN scheme has been presented in [32]. Yan *et al.* [33] proposed a pilot-based channel training scheme for a full-duplex receiver to enhance the physical layer security. As demonstrated in [34], AN can also be injected into the downlink training signals to prevent the eavesdropper from obtaining accurate CSI for the eavesdropping link.

Despite the promising performance gain brought by massive MIMO, it suffers from a challenging issue of high cost and power consumption due to the fact that each antenna requires a separate radio-frequency (RF) chain for signal processing. One potential approach to reducing the required cost and power is to use digital-to-analog converters (DACs) with lower resolution for downlink transmissions [35]. A number of authors have considered various direct nonlinear precoding schemes that constrain the transmit signals to match the DAC resolution. For example, a novel precoding technique using 1-bit DACs has been presented in [36] and a nonlinear beamforming algorithm has been proposed in [37]. Also, perturbation methods minimizing the probability of error at the receivers have been studied in [38]. An alternative simpler approach is to quantize the output of standard linear precoders, which is referred to as quantized linear precoding [39]–[41]. Although it is generally difficult to analytically characterize the performance degradation due to nonlinear quantization, the well-known Bussgang theorem can be applied to develop an equivalent linear model [42], [43]. This model decomposes the quantized signal into a linearly distorted version of the signal together with an uncorrelated quantization noise source [44]. It is noteworthy that the DAC quantization noise shares some similarities with the AN injected by the BS as both are transmitted along with the information-carrying signals and produce interference at the eavesdropper. In other words, the DAC quantization noise can be regarded, in some sense, as a special type of AN. Hence, it can also decrease the received signal-to-interference-and-noise ratio (SINR) at the eavesdropper, while unavoidably interfering with legitimate users at the same time. While common sense dictates that low-resolution DAC quantization degrades system performance in conventional massive MIMO systems, it is interesting to consider the possibility that DAC quantization could enhance secrecy capacity in some scenarios. To the best of our knowledge, only few of the existing works (e.g., [9]–[19], [28]–[34]) have investigated secure massive MIMO communications using low-resolution DACs.

On the other hand, although the effect of hardware impairments on secure massive MIMO systems has been analyzed in [45], only ideal converters with infinite resolution were considered. In this paper, we investigate secure transmission in a multiuser massive MIMO downlink network equipped with low-resolution DACs at the BS. We assume that there exists a multi-antenna eavesdropper that intends to eavesdrop the information transmitted from the BS to multiple legitimate users. The eavesdropper is passive in order to conceal its presence. We assume for simplicity that perfect CSI is available at the BS since there are already a number of studies, i.e., [46]–[49], focusing on the problem of channel estimation. We consider two popular AN methods for injecting AN at the BS in order to prevent the unintended receiver from eavesdropping. One method is based on AN which lies in the null-space spanned by the channels of all the desired users, while the other assumes random AN. We also study the impact of low-resolution DACs on the achievable secrecy rate. The main contributions of this work are summarized as follows:

1) For the case of low-resolution DAC quantization in secure massive MIMO, we derive tight lower bounds for the secrecy rate of the system using different types of AN methods. We observe that lower-resolution DACs provide superior secrecy performance under certain circumstances, e.g., at low SNR. This is explained by the fact that the quantization noise degrades the eavesdropper's capacity more significantly than that of the users. Specifically, we derive a closed-from expression for a threshold SNR $\bar{\gamma}_0$, such that if the transmit SNR γ_0 satisfies $\gamma_0 < \bar{\gamma}_0$, lower-resolution DACs enhance the secrecy rate, while if $\gamma_0 > \bar{\gamma}_0$, higher-resolution DACs are preferred.

2) It is found that secure transmission with low-resolution DACs depends heavily on the power allocation factor $\phi \in (0, 1]$, which denotes the proportion of power used for confidential signals, with the remainder of the power allocated for AN. Generally, the secrecy rate first increases with ϕ but then subsequently decreases. A closed-form expression for an approximate optimal ϕ^* is obtained. We observe that ϕ^* increases with a decreasing DAC resolution. This suggests that less power can be utilized to generate AN for DACs with a lower resolution.

3) For the null-space AN method with the optimal ϕ^*, we observe that low-resolution DACs lead to secrecy rate loss for all SNR values. On the other hand, for the random AN method, the secrecy rate with ϕ^* is insensitive to the DAC resolution. This is because the DAC quantization noise behaves the same as random AN at both the intended user and eavesdropper. As the quantization noise increases, we can maintain the same secrecy rate by reducing the power of the random AN with an increasing ϕ.

4) If extremely low-resolution DACs, i.e., 1-bit DACs, are employed at the BS, the advantage of null-space AN over random AN becomes marginal, while the null-space AN also suffers from a much higher computational complexity especially in massive MIMO. In this scenario, the null-space AN method is not cost-efficient and random AN is preferred.

The rest of this paper is structured as follows. The DAC quantization model, channel model, and two AN design methods are introduced in Section II. We derive a tight lower bound for the achievable secrecy rate in Section III assuming low-resolution DACs. Section IV analyzes the effect of various system parameters on secure communication. Simulation results are presented in Section V, and conclusions are drawn in Section VI.

Notation: $\mathbf{A}^T$, $\mathbf{A}^*$, and $\mathbf{A}^H$ represent the transpose, conjugate, and conjugate transpose of $\mathbf{A}$, respectively. $\mathbf{a} \sim \mathcal{CN}(\mathbf{0}, \mathbf{\Sigma})$ denotes a circularly symmetric complex

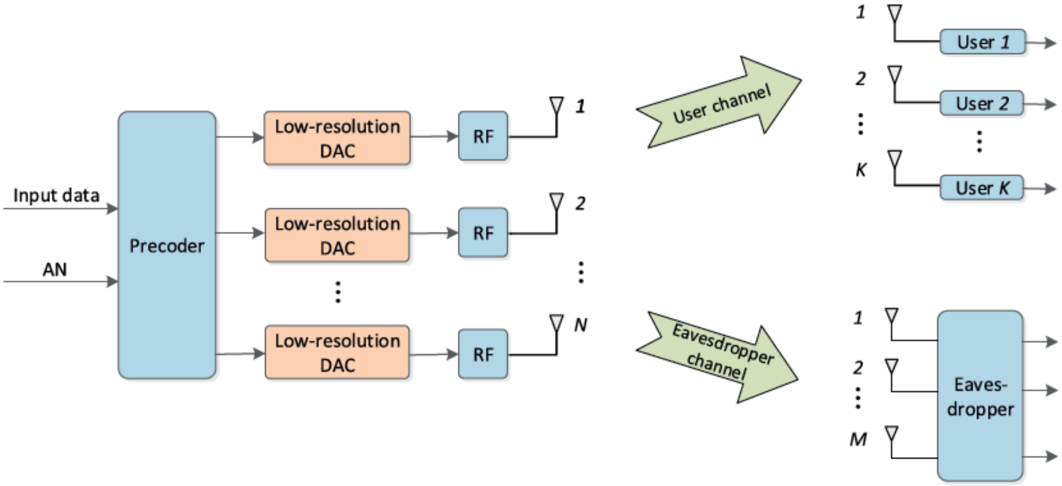

Fig. 1. Block diagram of the secure multiuser massive MIMO system.

Gaussian vector with zero mean and covariance matrix $\mathbf{\Sigma}$. $\mathrm{tr}\{\mathbf{A}\}$ denotes the trace of $\mathbf{A}$ and $\mathrm{diag}(\mathbf{A})$ is a matrix that retains only the diagonal entries of $\mathbf{A}$. $\mathbb{E}\{\cdot\}$ is the expectation operator. $\|\cdot\|^2$ denotes the Euclidean norm. $\xrightarrow{a.s.}$ denotes almost sure convergence. $[x]^+ = \max\{0, x\}$ chooses the maximum between 0 and x.

II. System Model

In this section, we investigate a multiuser massive MIMO security network employing low-resolution DACs. The DAC quantization model and two AN design methods are introduced.

A. Quantization Model for Low-Resolution DACs

It is in general difficult to accurately characterize the quantization error of an arbitrary low-resolution DAC. Fortunately, an equivalent linear representation has been widely adopted by using the Bussgang theorem [42]. This model has been verified to be accurate enough for most DAC quantization levels in practice [50]. In this model, the quantized data is decomposed into two uncorrelated parts as

$$\mathcal{Q}_{\mathrm{DA}}(\mathbf{x}) = \mathbf{F}\mathbf{x} + \mathbf{n}_{\mathrm{DA}}, \tag{1}$$

where $\mathcal{Q}_{\mathrm{DA}}(\cdot)$ denotes the quantization operation, $\mathbf{x}$ denotes the input data vector to the DAC, $\mathbf{F}$ represents the equivalent linear transformation matrix, and $\mathbf{n}_{\mathrm{DA}} \sim \mathcal{CN}(\mathbf{0}, \mathbf{C}_{\mathrm{DA}})$ denotes the Gaussian quantization noise. It was shown in [50] that

$$\mathbf{F} = \sqrt{1-\rho}\,\mathbf{I}, \tag{2}$$

and

$$\mathbf{C}_{\mathrm{DA}} = \rho\,\mathbb{E}\left\{\mathrm{diag}\left(\mathbf{x}\mathbf{x}^H\right)\right\}, \tag{3}$$

where $\rho \in (0,1)$ is a distortion factor that depends on the DAC resolution b_{DA}, which represents the number of quantized bits for the DAC.

B. Secure Massive MIMO Transmission

In the considered massive MIMO downlink network as illustrated in Fig. 1, K single-antenna users are served by an N-antenna BS, where each transmit antenna employs a pair of low-resolution DACs for processing the in-phase and quadrature signals. Meanwhile, a passive eavesdropper equipped with M antennas strives to eavesdrop the information sent to the users. In order to protect the confidential data from eavesdropping, the BS injects AN into the information-bearing signals. Before transmission, the signal vector $\mathbf{s} \in \mathbb{C}^{K\times 1}$ with $\mathbb{E}\{\mathbf{s}\mathbf{s}^H\} = \mathbf{I}_K$ is precoded by a matrix $\mathbf{W} \in \mathbb{C}^{N\times K}$ with $\mathrm{tr}\{\mathbf{W}\mathbf{W}^H\} = K$, while the AN vector $\mathbf{z} \sim \mathcal{CN}(\mathbf{0}, \mathbf{I}_{N-K})$ is multiplied by an AN shaping matrix $\mathbf{V} \in \mathbb{C}^{N\times(N-K)}$ with $\mathrm{tr}\{\mathbf{V}\mathbf{V}^H\} = N-K$. The weighted data vector at the BS before transmission is expressed as

$$\mathbf{x} = \sqrt{\frac{\phi P}{K}}\mathbf{W}\mathbf{s} + \sqrt{\frac{(1-\phi)P}{N-K}}\mathbf{V}\mathbf{z}$$
$$\triangleq \sqrt{p}\mathbf{W}\mathbf{s} + \sqrt{q}\mathbf{V}\mathbf{z}, \tag{4}$$

where P denotes the total transmit power and $\phi \in (0,1]$ is a power allocation factor. For notational simplicity, we define

$$p \triangleq \frac{\phi P}{K} \tag{5}$$

and

$$q \triangleq \frac{(1-\phi)P}{N-K}. \tag{6}$$

Applying the quantization model in (1), the transmit vector after DAC quantization is given by

$$\mathbf{x}_{\mathrm{q}} = \mathcal{Q}_{\mathrm{DA}}(\mathbf{x}) = \sqrt{1-\rho}\,\mathbf{x} + \mathbf{n}_{\mathrm{DA}}, \tag{7}$$

where $\mathbf{n}_{\mathrm{DA}} \sim \mathcal{CN}(\mathbf{0}, \mathbf{C}_{\mathrm{DA}})$ represents the quantization noise which is uncorrelated with $\mathbf{x}$. By substituting (4) into (3), the quantization noise covariance matrix $\mathbf{C}_{\mathrm{DA}}$ is obtained as

$$\mathbf{C}_{\mathrm{DA}} = \rho\Big[p\ \mathrm{diag}\left(\mathbf{W}\mathbf{W}^H\right) + q\ \mathrm{diag}\left(\mathbf{V}\mathbf{V}^H\right)\Big]. \tag{8}$$

Then, from (4) and (7), the received vector at the K users can be expressed as

$$\begin{aligned}\mathbf{y} &= \mathbf{H}\mathbf{x}_{\mathrm{q}} + \mathbf{n}\\ &= \sqrt{1-\rho}\Big(\sqrt{p}\mathbf{H}\mathbf{W}\mathbf{s} + \sqrt{q}\mathbf{H}\mathbf{V}\mathbf{z}\Big) + \mathbf{H}\mathbf{n}_{\mathrm{DA}} + \mathbf{n}, \quad (9)\end{aligned}$$

where $\mathbf{n} \sim \mathcal{CN}(\mathbf{0}, \sigma_n^2\mathbf{I}_K)$ represents the thermal additive white Gaussian noise (AWGN) at the users, and $\mathbf{H} \in \mathbb{C}^{K\times N}$ denotes the channel matrix between the BS and K users. In this work, we assume that long-term power control is employed to compensate for the large-scale fading of the different users. Furthermore, the entries of $\mathbf{H}$ are modeled as independent and identically distributed (i.i.d.) complex Gaussian random variables with zero mean and unit variance. Similarly, the received vector at the eavesdropper is

$$\begin{aligned}\mathbf{y}_{\mathrm{e}} &= \mathbf{H}_{\mathrm{e}}\mathbf{x}_{\mathrm{q}} + \mathbf{n}_{\mathrm{e}}\\ &= \sqrt{1-\rho}\Big(\sqrt{p}\mathbf{H}_{\mathrm{e}}\mathbf{W}\mathbf{s} + \sqrt{q}\mathbf{H}_{\mathrm{e}}\mathbf{V}\mathbf{z}\Big) + \mathbf{H}_{\mathrm{e}}\mathbf{n}_{\mathrm{DA}} + \mathbf{n}_{\mathrm{e}},\end{aligned} \tag{10}$$

where $\mathbf{n}_{\mathrm{e}} \sim \mathcal{CN}(\mathbf{0}, \sigma_{\mathrm{e}}^2\mathbf{I}_M)$ represents the thermal AWGN at the eavesdropper, and $\mathbf{H}_e \in \mathbb{C}^{M\times N}$ denotes the channel matrix between the BS and the eavesdropper, whose entries are also modeled as i.i.d. complex Gaussian random variables with zero mean and unit variance. To guarantee secure communication in the worst case, we assume that σ_{e}^2 is sufficiently small at the eavesdropper and can be ignored in the sequel [16], [30], [31].

C. AN Design Methods

In this paper, we consider two common methods to generate the AN shaping matrix $\mathbf{V}$. Let $\mathbf{v}_i$, $\forall\ i \in \{1, 2, \ldots, N-K\}$, denote the ith column of $\mathbf{V}$ satisfying the constraint $\|\mathbf{v}_i\|^2 = 1$.

1) Null-Space Artificial Noise: For downlink data transmission, AN is added to the transmit signals at the BS to degrade the decoding ability of the eavesdropper. However, it can simultaneously interfere with the legitimate users as well. In order to avoid any potential leakage of the AN to the intended users, the AN is often designed to lie in the null-space of the channel matrix $\mathbf{H}$, i.e., $\mathbf{HV} = \mathbf{0}$, assuming $\mathbf{H}$ is available at the transmitter. However, taking low-resolution DACs into account, the AN no longer perfectly lies in the channel null-space after quantization and thus additional interference still exists.

2) Random Artificial Noise: For massive MIMO communication, the computational complexity of the null-space of $\mathbf{H}$ becomes prohibitively large with a large dimension N. Therefore, a much simpler but effective method to design $\mathbf{V}$ was introduced in [30]. In this method, the columns of $\mathbf{V}$ are generated as mutually independent random vectors satisfying $\|\mathbf{v}_i\|^2 = 1$, $\forall\ i \in \{1, 2, \ldots, N-K\}$. The random AN is inevitably leaked to the intended users but it offers much lower computational complexity compared to the null-space based AN.

Note that for both AN design methods, the columns of $\mathbf{V}$ asymptotically form an incomplete orthogonal basis with large N due to the strong law of large numbers [30]. In the following, we refer to the above two AN design methods by using superscripts, $\mathcal{N}$ and $\mathcal{R}$, respectively.

III. Achievable Ergodic Secrecy Rate

Given the expressions of the received signals at both the users and eavesdropper, we derive the achievable secrecy rate per user in this section, under the assumption of large numbers of antennas and users but with fixed ratios given as:

$$\alpha \triangleq \frac{M}{N} \tag{11}$$

and

$$\beta \triangleq \frac{K}{N}, \tag{12}$$

where β denotes the user loading ratio [44]. To start, we first recall the following lemma from [30, Lemma 1].

Lemma 1: The achievable ergodic secrecy rate for the kth user is given by

$$R_{\mathrm{sec},k} = [R_k - C_k]^+, \tag{13}$$

where $[x]^+ = \max\{0, x\}$, R_k represents the achievable ergodic rate of the kth user, and C_k denotes the ergodic capacity between the BS and the eavesdropper seeking to decode the information of the kth user.

In the following, we derive a lower bound for R_k and an upper bound for C_k assuming low-resolution DACs, which then provides us a lower bound for the achievable ergodic secrecy rate.

A. Achievable Ergodic Rate of Each User

From (9), the received signal of user k, i.e., y_k, can be expressed as

$$y_k = \sqrt{1-\rho}\left(\sqrt{p}\mathbf{h}_k^T\mathbf{W}\mathbf{s} + \sqrt{q}\mathbf{h}_k^T\mathbf{V}\mathbf{z}\right) + \mathbf{h}_k^T\mathbf{n}_{\mathrm{DA}} + n_k, \tag{14}$$

where $\mathbf{h}_k^T$ denotes the kth row of $\mathbf{H}$ and n_k is the kth element of $\mathbf{n}$. We also express $\mathbf{W} = [\mathbf{w}_1, \mathbf{w}_2, \ldots, \mathbf{w}_k]$ where $\mathbf{w}_k \in \mathbb{C}^{N\times 1}$, $\forall k \in \{1, 2, \ldots, K\}$, is the kth column of $\mathbf{W}$. Then, the signal-to-interference-quantization-and-noise ratio (SIQNR) of the kth user, γ_k, can be expressed as (15) at the top of next page, where S_k is the power of the desired signal and I_k represents the power of the inter-user interference. Variables Q_k and A_k denote the interference power caused by DAC quantization and AN, respectively. Then, by imposing the worst-case assumption of Gaussian distributed interference and applying Shannon's formula, a lower bound for the achievable ergodic rate of user k can be evaluated as

$$R_k = \mathbb{E}\Big\{\log_2\left(1+\gamma_k\right)\Big\}. \tag{16}$$

In order to characterize the user rate performance, we derive the asymptotic behavior of γ_k with both AN and DAC quantization in the following lemma.

Lemma 2: Under the assumption of $N \to \infty$ with fixed α and β, the SIQNR of each user almost surely converges to

$$\gamma_k^{\mathcal{N}} \xrightarrow{a.s.} \frac{(1-\rho)\left(\frac{1}{\beta}-1\right)\phi\gamma_0}{\rho\gamma_0+1} \triangleq \gamma^{\mathcal{N}}, \tag{17}$$

$$\gamma_k = \frac{\overbrace{(1-\rho)p|\mathbf{h}_k^T\mathbf{w}_k|^2}^{S_k}}{\underbrace{(1-\rho)p\sum_{j\neq k}|\mathbf{h}_k^T\mathbf{w}_j|^2}_{I_k} + \underbrace{\mathbf{h}_k^T\mathbf{C}_{\mathrm{DA}}\mathbf{h}_k^*}_{Q_k} + \underbrace{(1-\rho)q\mathbf{h}_k^T\mathbf{V}\mathbf{V}^H\mathbf{h}_k^*}_{A_k} + \sigma_n^2}, \tag{15}$$

for null-space AN and

$$\gamma_k^{\mathcal{R}} \xrightarrow{a.s.} \frac{(1-\rho)\left(\frac{1}{\beta}-1\right)\phi\gamma_0}{\rho\gamma_0+(1-\rho)(1-\phi)\gamma_0+1} \triangleq \gamma^{\mathcal{R}}, \tag{18}$$

for random AN, where $\gamma_0 = \frac{P}{\sigma_n^2}$ represents the average transmit SNR.

Proof: See Appendix A. ■

Since convergence is preserved for continuous functions according to the Continuous Mapping Theorem [51], we apply *Lemma 2* to (16) and thus the asymptotic achievable rates of each user for both the AN design methods are respectively obtained as

$$R^{\mathcal{N}} = \log_2\left(1+\frac{(1-\rho)\left(\frac{1}{\beta}-1\right)\phi\gamma_0}{\rho\gamma_0+1}\right) \tag{19}$$

and

$$R^{\mathcal{R}} = \log_2\left(1+\frac{(1-\rho)\left(\frac{1}{\beta}-1\right)\phi\gamma_0}{\rho\gamma_0+(1-\rho)(1-\phi)\gamma_0+1}\right). \tag{20}$$

From (19) and (20), it can be observed that both $R^{\mathcal{N}}$ and $R^{\mathcal{R}}$ increase with decreasing β, which implies that the achievable rate increases with more BS antennas or fewer users. In addition, lower-resolution DACs cause higher quantization distortion with larger ρ, which leads to more severe user rate loss. As ϕ increases, both $R^{\mathcal{N}}$ and $R^{\mathcal{R}}$ grow since more signal power is allocated to the users. By comparing (19) and (20) with the same parameter values, it can be easily verified that $R^{\mathcal{N}} > R^{\mathcal{R}}$, as expected. This is because random AN causes additional interference to the legitimate receivers while the more complicated null-space based AN mitigates interference leakage to the users except for the leakage due to the DAC quantization noise. Considering extremely low-resolution DACs with $\rho \to 1$, we have $R^{\mathcal{R}} \to R^{\mathcal{N}}$ and thus random AN achieves almost the same rate performance as the null-space based AN. Under this condition, hardly any of the AN lies in the null-space of the user's channel matrix after DAC quantization and the performance of null-space based AN tends to that of random AN.

B. Ergodic Capacity of Eavesdropper

Without loss of generality, suppose that the data of user k is of interest to the eavesdropper. In order to characterize the achievable secrecy rate, we assume the worst case that the eavesdropper has perfect knowledge of all the data channels and is able to cancel all inter-user interference before attempting to decode the message of user k [16], [30], [31]. This assumption is reasonable because the quantization noise dominates the rate performance compared to the multiuser interference, especially for low-resolution DACs. Using (10) and under the assumption of large N and K, the ergodic capacity of the eavesdropper can be evaluated as [52]

$$C_k = \mathbb{E}\Big\{\log_2\left(1+(1-\rho)p\mathbf{w}_k^H\mathbf{H}_{\mathrm{e}}^H\mathbf{X}^{-1}\mathbf{H}_{\mathrm{e}}\mathbf{w}_k\right)\Big\}, \tag{21}$$

where $\mathbf{X}$ is defined as

$$\mathbf{X} \triangleq (1-\rho)q\mathbf{H}_{\mathrm{e}}\mathbf{V}\mathbf{V}^H\mathbf{H}_{\mathrm{e}}^H + \mathbf{H}_{\mathrm{e}}\mathbf{C}_{\mathrm{DA}}\mathbf{H}_{\mathrm{e}}^H. \tag{22}$$

Since analysis of the eavesdropper's capacity in (21) appears less tractable, as an alternative, we derive a tight upper bound for C_k, as given in the following theorem.

Theorem 1: For $N \to \infty$ and $\alpha+\beta<1$, an upper bound for the ergodic capacity of the eavesdropper is given by

$$\bar{C} \triangleq \log_2 \times\left(1+\frac{\frac{\alpha}{\beta}\phi(1-\phi+\tilde{\rho})}{\left(1-\frac{\alpha}{1-\beta}\right)(1-\phi)^2+2(1-\alpha)(1-\phi)\tilde{\rho}+(1-\alpha)\tilde{\rho}^2}\right), \tag{23}$$

where $\tilde{\rho} \triangleq \frac{\rho}{1-\rho}$.

Proof: See Appendix B. ■

From *Theorem 1*, we have the following observations.

1) The expression for the eavesdropper's capacity in (21) only exists if $\mathbf{X}$ in (22) is invertible. When $\rho \to 0$, we have $\mathbf{X} \to q\mathbf{H}_{\mathrm{e}}\mathbf{V}\mathbf{V}^H\mathbf{H}_{\mathrm{e}}^H$ since $\mathbf{C}_{\mathrm{DA}} \to \mathbf{0}$ from (8). In this case, $\mathbf{X}$ is invertible if $N-K>M$ since the columns of the tall matrix, $\mathbf{V}$, form an orthogonal basis for asymptotically large N and the elements of $\mathbf{H}_{\mathrm{e}}$ are i.i.d. complex Gaussian distributed. Similarly for $\rho \to 1$, $\mathbf{X} \to \mathbf{H}_{\mathrm{e}}\left[p\ \mathrm{diag}(\mathbf{W}\mathbf{W}^H)+q\ \mathrm{diag}(\mathbf{V}\mathbf{V}^H)\right]\mathbf{H}_{\mathrm{e}}^H$ is invertible if $N>M$. Combining the above two conditions, we see that $\mathbf{X}$ is invertible when $N-K>M$ regardless of the value of $\rho\in(0,1)$. This results in the same constraint, i.e., $\alpha+\beta<1$, as in *Theorem 1*, and is a common condition for massive MIMO systems with a large N.

2) From (23), it is obvious that $\bar{C}$ is monotonically increasing with α. This implies that the BS can reduce the amount of private information leaked to the eavesdropper by deploying more transmit antennas, while the eavesdropper can improve its wiretapping capability by employing more receive antennas.

3) Given α, ρ, and ϕ, the effect of β on $\bar{C}$ is generally not monotonic. By characterizing the derivative of $\bar{C}$ with respect to (w.r.t.) β, we find that $\bar{C}$ decreases for $\beta\in(0,\bar{\beta})$, while it

$$\underline{R}_{\text{sec}}^{\mathcal{N}} = \left[\log_2\left(1+\frac{(1-\rho)\left(\frac{1}{\beta}-1\right)\phi\gamma_0}{\rho\gamma_0+1}\right) - \log_2\left(1+\frac{\alpha\phi\left(\frac{1}{\beta}-1\right)\mu}{(\nu+\alpha\beta)\mu^2-\zeta}\right)\right]^+. \tag{27}$$

$$\underline{R}_{\text{sec}}^{\mathcal{R}} = \left[\log_2\left(1+\frac{(1-\rho)\left(\frac{1}{\beta}-1\right)\phi\gamma_0}{\rho\gamma_0+(1-\rho)(1-\phi)\gamma_0+1}\right) - \log_2\left(1+\frac{\alpha\phi\left(\frac{1}{\beta}-1\right)\mu}{(\nu+\alpha\beta)\mu^2-\zeta}\right)\right]^+. \tag{28}$$

increases when $\beta \in (\bar{\beta}, 1-\alpha)$, where

$$\bar{\beta} \triangleq 1 - \sqrt{\frac{\alpha(1-\phi)^2}{(1-\alpha)\left[(1-\phi)+\tilde{\rho}\right]^2+\alpha(1-\phi)^2}}. \tag{24}$$

This can be explained as follows. When β is small, the transmit power allocated to each user decreases significantly with increasing β and thus the eavesdropper's capacity decreases accordingly. As β continues increasing, the impact of the reduced power per user becomes less significant. When β approaches $1-\alpha$, $\mathbf{X}$ becomes ill-conditioned and the eavesdropper's capacity improves. In addition, it is noted that $\bar{\beta}$ can be larger than $1-\alpha$ for large values of ρ and ϕ. Under this condition, $\bar{C}$ decreases monotonically for $\beta \in (0, 1-\alpha)$.

4) The parameter $\tilde{\rho} \in (0, \infty)$ represents the influence of the low-resolution DACs on the capacity of the eavesdropper. By characterizing the derivative of $\bar{C}$ w.r.t. $\tilde{\rho}$, we find that $\frac{\partial \bar{C}}{\partial \tilde{\rho}} < 0$, $\forall \tilde{\rho}$. It implies that $\bar{C}$ decreases with $\tilde{\rho}$, and hence with ρ. Since ρ increases with decreasing DAC resolution b_{DA}, a smaller b_{DA} leads to a lower $\bar{C}$ due to the increasing power of the quantization noise. This implies that the utilization of low-resolution DACs makes some contribution to protecting the legitimate users from eavesdropping, although it concurrently decreases the achievable user rate.

5) It is found that $\bar{C}$ increases with ϕ, i.e., $\frac{\partial \bar{C}}{\partial \phi} > 0$, as the eavesdropper's capacity increases with decreasing AN power. Assuming that there is no AN, i.e., $\phi = 1$, $\bar{C}$ in (23) achieves the maximum which is given by

$$\bar{C} = \log_2\left[1 + \frac{\alpha}{(1-\alpha)\beta\tilde{\rho}}\right]. \tag{25}$$

Note that $\bar{C}$ does not grow without an upper bound even if AN is not present due to the low-resolution DAC quantization. To a certain extent, the quantization noise acts as a type of AN which helps to degrade the eavesdropper's capacity by producing unavoidable interference. In this case, $\bar{C}$ becomes a monotonically decreasing function w.r.t. $\beta \in (0, 1-\alpha)$ because $\bar{\beta} = 1 > 1-\alpha$ by substituting $\phi = 1$ into (24).

C. Lower Bound for the Achievable Secrecy Rate

Applying *Lemma 1* and using (19), (20), and (23), a lower bound for the achievable secrecy rate of each user is obtained as follows

$$\underline{R}_{\text{sec}}^{\Psi} = \left[R^{\Psi} - \bar{C}\right]^+, \tag{26}$$

where $\Psi \in \{\mathcal{N}, \mathcal{R}\}$. Using the results derived above, expressions for $\underline{R}_{\text{sec}}^{\mathcal{N}}$ and $\underline{R}_{\text{sec}}^{\mathcal{R}}$ are respectively obtained as in (27) and (28) at the top of this page, where we define $\nu \triangleq 1-\alpha-\beta$, $\mu \triangleq 1-\phi+\tilde{\rho}$, and $\zeta \triangleq \alpha\beta(1-\phi)^2$ for notational simplicity. These closed-form expressions allow us to gain insight into the impact of the various system parameters, as detailed in the next sections.

IV. Secrecy Rate Analysis

In this section, we analyze the impact of various parameters, including α, β, ρ, and ϕ, on the secrecy rate in massive MIMO systems using low-resolution DACs.

A. Impact of Antenna and User Loading Ratios

We first analyze the impact of the antenna ratio α defined in (11). In (26), $\bar{C}$ increases monotonically with α as indicated before while R^{Ψ} is independent of α. As a consequence, $\underline{R}_{\text{sec}}^{\Psi}$ is monotonically decreasing w.r.t. α. Thus, a threshold value, $\bar{\alpha}$, may exist such that no positive secrecy rate can be achieved when $\alpha > \bar{\alpha}$, regardless of the values of other parameters. In other words, secure transmission cannot be achieved if the eavesdropper possesses enough antennas.

Since AN is injected to enhance the secrecy rate, we consider the special case that almost all the power is allocated to generate AN, i.e., $\phi \to 0$. By setting $\underline{R}_{\text{sec}}^{\Psi} = 0$ in (27) and (28), $\bar{\alpha}$ is obtained as

$$\bar{\alpha}^{\mathcal{N}} = \frac{(1-\beta)\gamma_0}{(\rho+1)\gamma_0+1-\beta\gamma_0\rho(2-\rho)} \tag{29}$$

and

$$\bar{\alpha}^{\mathcal{R}} = \frac{(1-\beta)\gamma_0}{2\gamma_0+1-\beta\gamma_0\rho(2-\rho)}. \tag{30}$$

Since $\rho \in (0,1)$, we have $\bar{\alpha}^{\mathcal{N}} > \bar{\alpha}^{\mathcal{R}}$, which implies that the null-space based AN can tolerate a larger number of eavesdropper antennas than the random AN at the expense of higher computational complexity and the need for CSI. Interestingly, it can be observed that $\bar{\alpha}^{\mathcal{N}} \to \bar{\alpha}^{\mathcal{R}}$ when $\rho \to 1$. This is because the null-space based AN tends to be randomly distributed in the signal space after low-resolution DAC quantization. Note that both $\bar{\alpha}^{\mathcal{N}}$ and $\bar{\alpha}^{\mathcal{R}}$ decrease with β. Next, we focus on the extreme condition when β reduces to near 0:

$$\lim_{\beta\to 0} \bar{\alpha}^{\mathcal{N}} = \frac{\gamma_0}{(\rho+1)\gamma_0+1} \tag{31}$$

and

$$\lim_{\beta\to 0} \bar{\alpha}^{\mathcal{R}} = \frac{\gamma_0}{2\gamma_0+1}. \tag{32}$$

Under this circumstance, $\lim_{\beta\to 0}\bar{\alpha}^{\mathcal{R}}$ is independent of ρ because the DAC quantization does not statistically change the randomness of the random AN. By increasing γ_0, both $\lim_{\beta\to 0}\bar{\alpha}^{\mathcal{N}}$ and $\lim_{\beta\to 0}\bar{\alpha}^{\mathcal{R}}$ grow accordingly, thus improving the robustness for both AN design methods. In all cases, however, the two thresholds are ultimately bounded above by $\lim_{\beta\to 0}\bar{\alpha}^{\mathcal{N}} < \frac{1}{\rho+1}$ and $\lim_{\beta\to 0}\bar{\alpha}^{\mathcal{R}} < \frac{1}{2}$, respectively.

One can also study the impact of user loading ratio β defined in (12). We take the derivative of $\underline{R}_{\text{sec}}^{\Psi}$ w.r.t. β and obtain that $\frac{\partial \underline{R}_{\text{sec}}^{\Psi}}{\partial \beta} < 0$. Hence, by combining the observations from (23), it is reasonable to expect that the secrecy rate will be enhanced with a smaller β. Furthermore, adding more antennas at the BS can offer a larger beamforming gain, or alternatively, a smaller number of users leads to higher per-user transmit power.

B. Impact of DAC Distortion Parameter

Since both R^{Ψ} and $\bar{C}$ decrease with increasing ρ due to the low-resolution DAC quantization, the impact of ρ on the secrecy rate, $\underline{R}_{\text{sec}}^{\Psi}$, is unclear. According to (26) and assuming a positive secrecy rate, we have

$$\frac{\partial \underline{R}_{\text{sec}}^{\Psi}}{\partial \rho} = \frac{\partial R^{\Psi}}{\partial \rho} - \frac{\partial \bar{C}}{\partial \rho}. \tag{33}$$

On one hand, $\frac{\partial \bar{C}}{\partial \rho} < 0$ is independent of γ_0 since we assume a near-zero thermal noise power at the eavesdropper. On the other hand, $\frac{\partial R^{\Psi}}{\partial \rho} < 0$ and decreases with large γ_0 because the quantization noise dominates the thermal noise at high SNRs. Thus, we conclude that there exists a $\bar{\gamma}_0^{\Psi} \in (0, \infty)$ which guarantees that $\frac{\partial \underline{R}_{\text{sec}}^{\Psi}}{\partial \rho} > 0$ for $\gamma_0 \in (0, \bar{\gamma}_0^{\Psi})$ and $\frac{\partial \underline{R}_{\text{sec}}^{\Psi}}{\partial \rho} < 0$ for $\gamma_0 \in (\bar{\gamma}_0^{\Psi}, \infty)$. Interestingly, lower-resolution DACs can achieve higher secrecy rate at low SNR, because the eavesdropper's capacity $\bar{C}$ decreases faster than R^{Ψ} does with an increasing ρ. On the other hand, at high SNR, higher-resolution DACs are advantageous compared to those with lower-resolution.

For the null-space AN method, the expression for $\frac{\partial \underline{R}_{\text{sec}}^{\Psi}}{\partial \rho}$ is given below:

$$\begin{aligned}
&\frac{\partial \underline{R}_{\text{sec}}^{\mathcal{N}}}{\partial \rho}\\
&= -\frac{\left(\frac{1}{\beta}-1\right)\phi(\gamma_0+1)\gamma_0}{\ln 2(\rho\gamma_0+1)\left[\rho\gamma_0+(1-\rho)\left(\frac{1}{\beta}-1\right)\phi\gamma_0+1\right]}\\
&\quad+\frac{\alpha\phi\left(\frac{1}{\beta}-1\right)\left[(\nu+\alpha\beta)\mu^2+\zeta\right]}{\ln 2(1-\rho)^2\left[(\nu+\alpha\beta)\mu^2-\zeta\right]\left[(\nu+\alpha\beta)\mu^2-\zeta+\alpha\phi\left(\frac{1}{\beta}-1\right)\mu\right]} \qquad (34)\\
&\triangleq \frac{1}{\ln 2}\frac{a^{\mathcal{N}}\gamma_0^2+b^{\mathcal{N}}\gamma_0+c^{\mathcal{N}}}{d^{\mathcal{N}}}, \qquad (35)
\end{aligned}$$

where (34) utilizes $\frac{\partial \mu}{\partial \rho} = \frac{\partial \tilde{\rho}}{\partial \rho} = \frac{1}{(1-\rho)^2}$. Obviously, the sign of $\frac{\partial \underline{R}_{\text{sec}}^{\mathcal{N}}}{\partial \rho}$ depends on the values of the parameters α, β, ρ, and ϕ. We have focused on the impact of γ_0 and regard the derivative as a quadratic equation w.r.t γ_0 as in (35). In general, we have that $d^{\mathcal{N}} > 0$, $a^{\mathcal{N}} < 0$, and $c^{\mathcal{N}} > 0$. This implies that a solution for $\bar{\gamma}_0^{\mathcal{N}}$ exists by forcing (35) to zero. Solving the quadratic yields

$$\bar{\gamma}_0^{\mathcal{N}} = \frac{-b^{\mathcal{N}} - \sqrt{{b^{\mathcal{N}}}^2 - 4a^{\mathcal{N}}c^{\mathcal{N}}}}{2a^{\mathcal{N}}}. \tag{36}$$

If $\gamma_0 < \bar{\gamma}_0^{\mathcal{N}}$, lower-resolution DACs can be used to enhance the secrecy rate since quantization noise degrades the eavesdropper's capacity more pronouncedly than the user rate. While for $\gamma_0 > \bar{\gamma}_0^{\mathcal{N}}$, the infinite-resolution DACs achieve the best performance. Since the expressions for $a^{\mathcal{N}}$, $b^{\mathcal{N}}$, $c^{\mathcal{N}}$, and $d^{\mathcal{N}}$ are generally complicated, we consider a special case with $\rho \to 0$, which means that ideal DACs with infinite resolution are assumed. Under this condition, the related parameters are obtained as

$$a^{\mathcal{N}} = -\nu(1-\phi)\phi\left[\nu(1-\phi)+\alpha\phi\left(\frac{1}{\beta}-1\right)\right], \tag{37}$$

$$b^{\mathcal{N}} = 2\alpha^2\phi^2(1-\beta)+\alpha\phi^3\nu\left(\frac{1}{\beta}-1\right)-\nu^2(1-\phi)^2\phi, \tag{38}$$

$$c^{\mathcal{N}} = \alpha\phi(\nu+2\alpha\beta), \tag{39}$$

$$d^{\mathcal{N}} = \ln 2\,\nu(1-\phi)\left[\frac{\nu(1-\phi)\beta}{1-\beta}+\alpha\phi\right]\left[\left(\frac{1}{\beta}-1\right)\phi\gamma_0+1\right]. \tag{40}$$

By substituting (37)-(40) into (36), the threshold $\bar{\gamma}_0^{\mathcal{N}}$ for $\rho \to 0$ is obtained. Although the threshold relies on ρ in general, the obtained $\bar{\gamma}_0^{\mathcal{N}}$ can approximately be applied to all values of $\rho \in (0, 1)$, which is verified by the simulation results in Section V.

For the random AN design method, similar manipulations can be conducted and the threshold SNR $\bar{\gamma}_0^{\mathcal{R}}$ is obtained as follows

$$\bar{\gamma}_0^{\mathcal{R}} = \frac{-b^{\mathcal{R}} - \sqrt{{b^{\mathcal{R}}}^2 - 4a^{\mathcal{R}}c^{\mathcal{R}}}}{2a^{\mathcal{R}}}, \tag{41}$$

where

$$\begin{aligned}
a^{\mathcal{R}} &= -\nu(1-\phi)\phi\left[\nu(1-\phi)+\alpha\phi\left(\frac{1}{\beta}-1\right)\right]\\
&\quad+\alpha\phi(1-\phi)(\nu+2\alpha\beta)\left[\left(\frac{1}{\beta}-1\right)\phi+1-\phi\right], \qquad (42)\\
b^{\mathcal{R}} &= 2\alpha^2\phi^2(1-\beta)+\alpha\phi^3\nu\left(\frac{1}{\beta}-1\right)-\nu^2(1-\phi)^2\phi\\
&\quad+2\alpha\phi(1-\phi)(\nu+2\alpha\beta), \qquad (43)\\
c^{\mathcal{R}} &= \alpha\phi(\nu+2\alpha\beta), \qquad (44)\\
d^{\mathcal{R}} &= \ln 2\nu(1-\phi)\left[\frac{\nu(1-\phi)\beta}{1-\beta}+\alpha\phi\right]\left[(1-\phi)\gamma_0+1\right]\\
&\quad\times\left[\left(\frac{1}{\beta}-1\right)\phi\gamma_0+(1-\phi)\gamma_0+1\right]. \qquad (45)
\end{aligned}$$

Similarly, $a^{\mathcal{R}}$, $b^{\mathcal{R}}$, $c^{\mathcal{R}}$, and $d^{\mathcal{R}}$ are obtained under the assumption of $\rho \to 0$ and $\bar{\gamma}_0^{\mathcal{R}}$ is also insensitive to the value of ρ.

C. Impact of the Power Allocation Factor

The above analysis was conducted assuming a fixed ϕ. Now, we investigate the effect of this power allocation factor on the secrecy rate. Since $\frac{\partial R^{\Psi}}{\partial \phi} > 0$ and $\frac{\partial \bar{C}}{\partial \phi} > 0$ as indicated above, the sign of $\frac{\partial \underline{R}^{\Psi}_{\text{sec}}}{\partial \phi} = \frac{\partial R^{\Psi}}{\partial \phi} - \frac{\partial \bar{C}}{\partial \phi}$ cannot be immediately determined.

Take the secrecy rate in (27) with the null-space AN for instance. The derivative of $\underline{R}^{\mathcal{N}}_{\text{sec}}$ w.r.t. ϕ is calculated as

$$\begin{aligned}\frac{\partial \underline{R}^{\mathcal{N}}_{\text{sec}}}{\partial \phi} &= \frac{(1-\rho)(\frac{1}{\beta}-1)\gamma_0}{\ln\ 2\left[\rho\gamma_0 + 1 + (1-\rho)(\frac{1}{\beta}-1)\gamma_0\phi\right]} \\ &\quad - \frac{\alpha\left(\frac{1}{\beta}-1\right)\left[\frac{(\nu+\alpha\beta)\mu^2}{1-\rho} - 2\alpha\beta\mu\phi(1-\phi) - \alpha\beta(1-\phi)^2(\mu-\phi)\right]}{\ln 2\ [(\nu+\alpha\beta)\mu^2-\zeta]\left[(\nu+\alpha\beta)\mu^2-\zeta+\alpha\phi\left(\frac{1}{\beta}-1\right)\mu\right]},\end{aligned} \tag{46}$$

where we use the fact that $\frac{\partial \mu}{\partial \phi} = -1$. For small ϕ we have $\frac{\partial \underline{R}^{\mathcal{N}}_{\text{sec}}}{\partial \phi} > 0$ while for large ϕ we have $\frac{\partial \underline{R}^{\mathcal{N}}_{\text{sec}}}{\partial \phi} < 0$. Thus, there exists an optimal ϕ, i.e., ϕ^*, that achieves the highest secrecy rate. By forcing $\frac{\partial \underline{R}^{\mathcal{N}}_{\text{sec}}}{\partial \phi} = 0$, the optimal ϕ^* is directly obtained. Since the expression in (46) is generally intractable, we resort to the numerical bisection method to determine ϕ^*. In addition, we derive a closed-form expression for an approximate ϕ^* in the following. We assume that $\alpha\beta \ll 1$, which generally holds in massive MIMO networks with large antenna arrays at the BS. Then, $\frac{\partial \underline{R}^{\mathcal{N}}_{\text{sec}}}{\partial \phi}$ in (46) approximately becomes

$$\begin{aligned}\frac{\partial \underline{R}^{\mathcal{N}}_{\text{sec}}}{\partial \phi} &= \frac{(1-\rho)(\frac{1}{\beta}-1)\gamma_0}{\ln\ 2\left[\rho\gamma_0 + 1 + (1-\rho)(\frac{1}{\beta}-1)\gamma_0\phi\right]} \\ &\quad - \frac{\alpha\left(\frac{1}{\beta}-1\right)\frac{\nu\mu^2}{1-\rho}}{\ln 2\ \nu\mu^2\left[\nu\mu^2+\alpha\phi\left(\frac{1}{\beta}-1\right)\mu\right]}.\end{aligned} \tag{47}$$

Setting $\frac{\partial \underline{R}^{\mathcal{N}}_{\text{sec}}}{\partial \phi} = 0$, the optimal ϕ^* is obtained as

$$\phi^{\mathcal{N}*} = \frac{\nu - \sqrt{\nu^2 + \left(\alpha\rho + \frac{\alpha}{\gamma_0} - \nu\right)\left(1-\beta-\frac{\alpha}{\beta}\right)}}{(1-\rho)\left(1-\beta-\frac{\alpha}{\beta}\right)}. \tag{48}$$

For random AN, a similar analysis can be conducted. Under the same assumption $\alpha\beta \ll 1$, the optimal $\phi^{\mathcal{R}*}$ is given by (49) at the bottom of next page.

Due to the constraint that $\phi \in (0,1]$, we set $\phi^* = 1$ if the obtained ϕ^* in (48) and (49) is larger than 1. Under this condition, the secrecy rate increases monotonically with $\phi \in (0,1]$. In Section V, we will show that both $\phi^{\mathcal{N}*}$ in (48) and $\phi^{\mathcal{R}*}$ in (49), shown at the bottom of the next page, are accurate for various combinations of system parameters.

V. Simulation Results

In this section, we verify the tightness of the derived bounds and the obtained insights via numerical simulation. We use the typical values for the distortion parameter ρ in [53] for each DAC using b_{DA} bits for quantization. For perfect DACs with $b_{\text{DA}} \to \infty$, we set $\rho \to 0$.

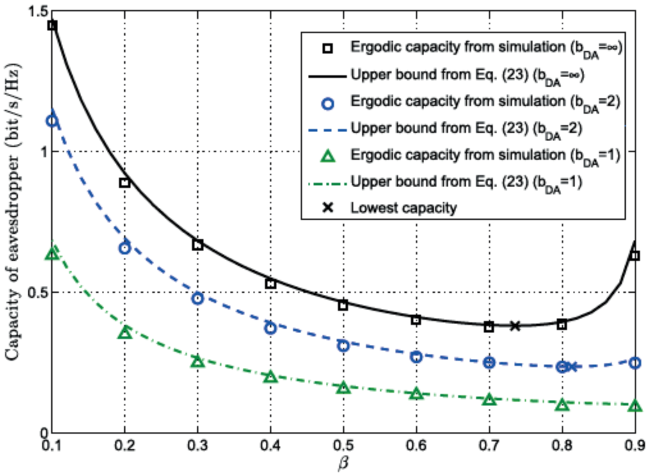

Fig. 2. Eavesdropper's capacity and the corresponding upper bounds versus β ($N = 100$, $M = 7$, and $\phi = 0.7$).

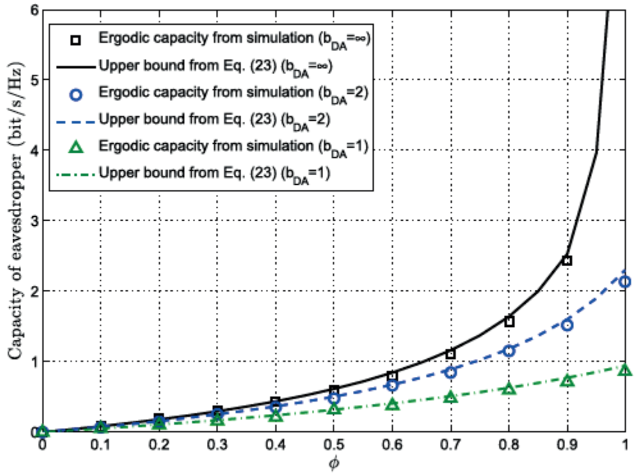

Fig. 3. Eavesdropper's capacity and our derived upper bound versus power allocation factor ϕ ($N = 100$, $K = 10$, and $M = 5$).

A. Ergodic Capacity of Eavesdropper

We first study the tightness of the derived upper bound for the eavesdropper's capacity. Fig. 2 compares the eavesdropper's capacity in (21) and the upper bound in (23), for DAC resolutions $b_{\text{DA}} = 1, 2$, and ∞. In general, our derived upper bound is tight for β ranging from 0.1 to 0.9. Clearly, the low-resolution DACs result in a capacity loss due to the interference caused by the quantization noise. As accurately predicted by our analysis in (24), the eavesdropper achieves the lowest capacity for $\bar{\beta} = 0.7354$ and $\bar{\beta} = 0.8133$ with $b_{\text{DA}} = \infty$ and $b_{\text{DA}} = 2$, respectively. These two points are denoted by markers $\times$ in the figure. For $b_{\text{DA}} = 1$, we have $\bar{\beta} = 0.9059$ according to (24) and thus $\bar{C}$ decreases monotonically for $\beta \in (0.1, 0.9)$.

Fig. 3 shows the capacity of the eavesdropper for ϕ ranging from 0 to 1. Obviously, $\bar{C}$ increases monotonically with ϕ. The lower the AN power, the higher the eavesdropper's capacity will be due to the power reduction in the interference. In addition, we see that low-resolution DACs help to degrade the channel quality of the eavesdropper regardless of the

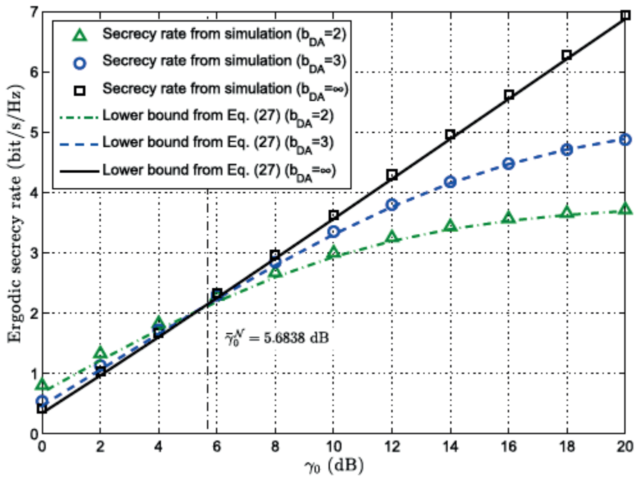

Fig. 4. Ergodic secrecy rate and lower bound versus SNR with null-space AN ($N = 128$, $K = 8$, $M = 16$, and $\phi = 0.8$).

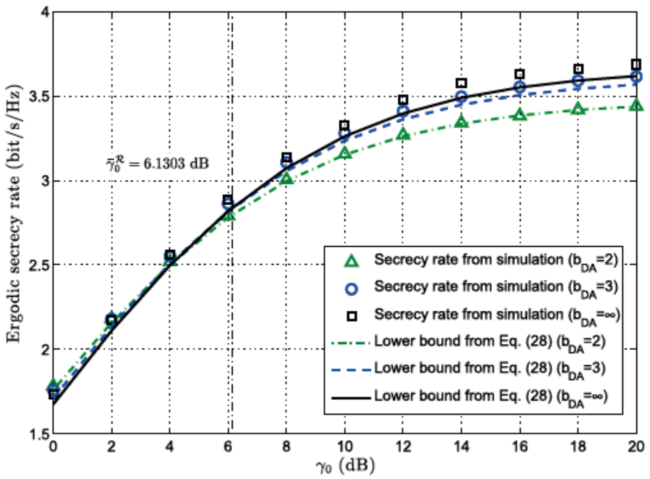

Fig. 5. Ergodic secrecy rate and lower bound versus SNR with random AN ($N = 128$, $K = 8$, $M = 6$, and $\phi = 0.7$).

value of ϕ. Assuming the eavesdropper is able to perfectly cancel the inter-user interference and the thermal noise is negligibly small, the capacity approaches infinity with $\phi \to 1$ and $b_{\mathrm{DA}} = \infty$ since there is no remaining interference. Thus, AN is necessary for conventional secure communication when perfect DACs are available. However, this is not the case for low-resolution DACs since the quantization noise can protect the confidential information from eavesdropping. Under the assumption of $\phi \to 1$, the capacity converges to 2.2985 and 0.9407, instead of infinity, for $b_{\mathrm{DA}} = 2$ and $b_{\mathrm{DA}} = 1$, respectively.

B. Achievable Ergodic Secrecy Rate

In the following, we verify the accuracy of the derived lower bound for the achievable secrecy rate. Fig. 4 shows the ergodic secrecy rate and its lower bound in (27) with the null-space AN method. The dotted markers correspond to the simulation results while the solid lines correspond to the lower bound. We observe that the derived bound is tight for γ_0 ranging from 0 dB to 20 dB. With infinite-resolution DACs, the secrecy rate increases proportionally with γ_0 while the low-resolution DAC quantization causes significant rate loss at high SNR. From (36), the SNR threshold is computed as $\bar{\gamma}_0^{\mathcal{N}} = 5.6838$ dB with $\rho \to 0$, i.e., $b_{\mathrm{DA}} \to \infty$. When $\gamma_0 < \bar{\gamma}_0^{\mathcal{N}}$, lower-resolution DACs can provide higher secrecy rate since the achievable rate of each user decreases more slowly than the eavesdropper's capacity as the DAC resolution decreases. At low SNR, thermal noise dominates at the users and the DAC quantization affects the eavesdropper's capacity more pronouncedly. On the other hand, when $\gamma_0 > \bar{\gamma}_0^{\mathcal{N}}$, infinite-resolution DACs achieve the highest secrecy rate. In addition, we observe that the obtained $\bar{\gamma}_0^{\mathcal{N}}$ can also be applied to low-resolution DACs with $b_{\mathrm{DA}} = 3$ and $b_{\mathrm{DA}} = 2$ as indicated before, although technically $\bar{\gamma}_0^{\mathcal{N}}$ depends on the quantization distortion parameter ρ. This makes the DAC resolution allocation much simpler and appealing in practice since only one $\bar{\gamma}_0^{\mathcal{N}}$ needs to be calculated.

Fig. 5 illustrates the ergodic secrecy rate and the derived lower bound in (28) with random AN. The secrecy rate increases with SNR but saturates eventually at high SNR, even if infinite-resolution DACs are adopted. This is because the random AN degrades the achievable rate of the legitimate users while the null-space AN only causes interference to the eavesdropper. From (41), $\bar{\gamma}_0^{\mathcal{R}}$ is calculated as 6.1303 dB. In order to enhance the secrecy rate, increasing the DAC resolution is recommended if $\gamma_0 > 6.1303$ dB but not if $\gamma_0 \leq 6.1303$ dB. In both Fig. 4 and Fig. 5, a fixed ϕ is assumed since it is in general difficult to optimize ϕ analytically. In order to alleviate the performance degradation of fixed power allocation, we present an approximate ϕ^* in (48) and (49) for the null-space AN and the random AN methods, respectively. Corresponding simulations are illustrated in Fig. 8 and Fig. 10 in the next subsection.

Fig. 6 depicts $\bar{\alpha}$ in (29) and (30) for null-space and random AN, respectively. As indicated in Section IV.A, a positive secrecy rate can be achieved only if $\alpha < \bar{\alpha}$. It is observed from Fig. 6 that $\bar{\alpha}$ decreases monotonically with β. Given a fixed N, the transmit power of each user decreases with an increasing number of users K, i.e., increasing β, and thus fewer antennas are required at the eavesdropper to decode the information. Note that even with $\beta \to 0$, a threshold $\bar{\alpha} < 1$ exists, which implies that the eavesdropper is still able to successfully wiretap as long as it employs enough antennas. Comparing null-space and random AN, we find that

$$\phi^{\mathcal{R}*} = \frac{(1+\gamma_0)(\nu-\alpha) - \sqrt{\alpha(1+\gamma_0)\left[\left(\frac{1}{\beta}+1\right)(\nu-\alpha)+\frac{1}{\gamma_0}\left(1-\beta-\frac{\alpha}{\beta}\right)\right]}}{(1-\rho)\left[1-\beta-\frac{\alpha}{\beta}+\gamma_0(\nu-\alpha)\right]}. \tag{49}$$

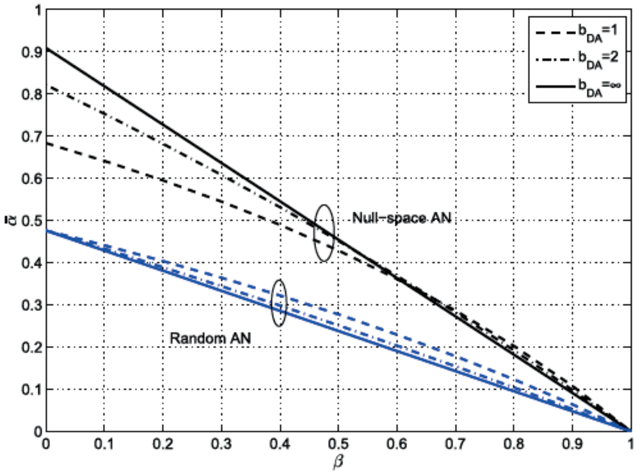

Fig. 6. Threshold ratio $\bar{\alpha}$ for positive secrecy rate versus β ($\gamma_0 = 10$ dB).

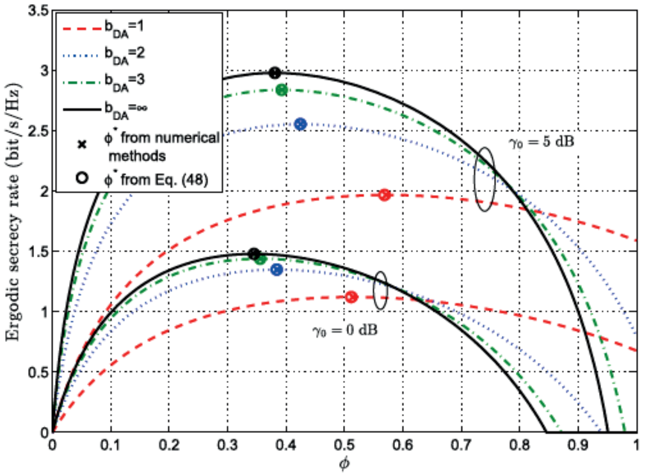

Fig. 7. Ergodic secrecy rate versus ϕ with null-space AN ($N = 128$, $K = 8$, and $M = 16$).

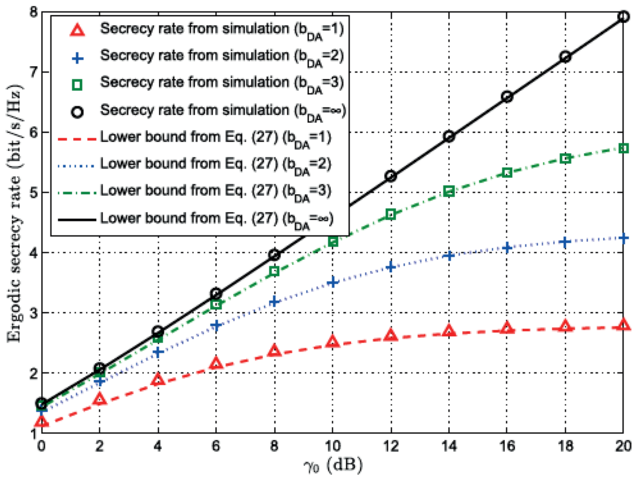

Fig. 8. Ergodic secrecy rate with the optimal ϕ^* versus SNR for null-space AN method ($N = 128$, $K = 8$, and $M = 16$).

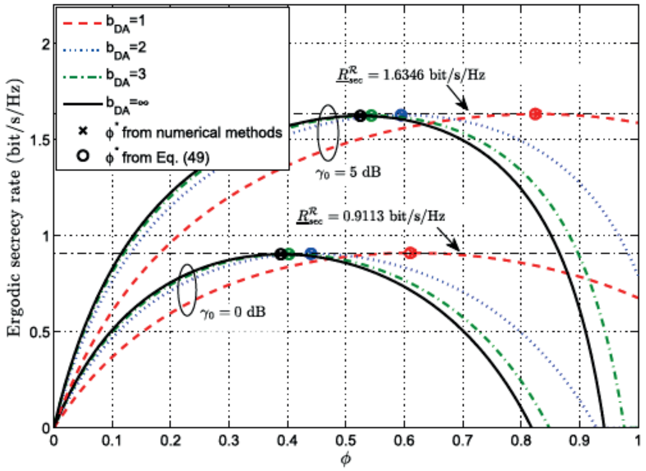

Fig. 9. Ergodic secrecy rate versus ϕ with random AN ($N = 128$, $K = 8$, and $M = 16$).

$\bar{\alpha}^{\mathcal{N}} > \bar{\alpha}^{\mathcal{R}}$ for $\gamma_0 = 10$ dB. This implies that higher hardware cost is required at the eavesdropper to resist null-space AN than random AN.

C. Optimal Power Allocation

In the following, the accuracy of the obtained closed-form expressions for the approximately optimal ϕ are verified. For null-space AN, Fig. 7 shows the ergodic secrecy rate with ϕ ranging from 0 to 1. We consider 1-3 bit DACs compared with the infinite-resolution case. Interestingly, the infinite-resolution DACs achieve the highest secrecy rate when ϕ is small while the lower-resolution DACs provide better rate performance for large ϕ. On one hand, a high DAC resolution is needed when most of the transmit power is allocated to generate AN. On the other hand, lower-resolution DACs can achieve higher secrecy rates when most of the power is used to transmit information signals. In fact, DAC quantization noise serves as a kind of AN to improve communication security. The markers × in the figure denote the optimal ϕ^* obtained by numerical methods while the circles represent the $\phi^{\mathcal{N}*}$ in (48). We can see that the two match exactly. Specifically when $\gamma_0 = 0$ dB, we have $\phi^{\mathcal{N}*} = 0.5117, 0.3841, 0.3552, 0.3452$ for $b_{\text{DA}} = 1, 2, 3, \infty$, respectively. For $\gamma_0 = 5$ dB, $\phi^{\mathcal{N}*} = 0.5687, 0.4247, 0.3926, 0.3808$ for $b_{\text{DA}} = 1, 2, 3, \infty$, respectively. For the same value of γ_0, the optimal ϕ^* increases with decreasing DAC resolution. This implies that more power should be allocated to the transmit signals with lower-resolution DACs. Furthermore, Fig. 8 shows the secrecy rate with the optimal ϕ^*. Comparing Fig. 4 with a fixed $\phi = 0.8$, we see that low-resolution DACs inevitably degrade the secrecy rate regardless of the SNR. If the optimal ϕ^* is achievable, higher-resolution DACs always provide more secure transmission.

For random AN, Fig. 9 shows the achievable secrecy rate versus ϕ using low-resolution DACs. The optimal ϕ^* obtained by numerical methods is denoted by × while the derived $\phi^{\mathcal{R}*}$ in (49) is denoted by circles. For the case that $\gamma_0 = 0$ dB, we have $\phi^{\mathcal{R}*} = 0.6103, 0.4402, 0.4024, 0.3885$ while for $\gamma_0 = 5$ dB, we have $\phi^{\mathcal{R}*} = 0.8243, 0.5960, 0.5435, 0.5247$, for $b_{\text{DA}} = 1, 2, 3, \infty$, respectively. Unlike the results of the null-space AN method shown in Fig. 7, the highest secrecy

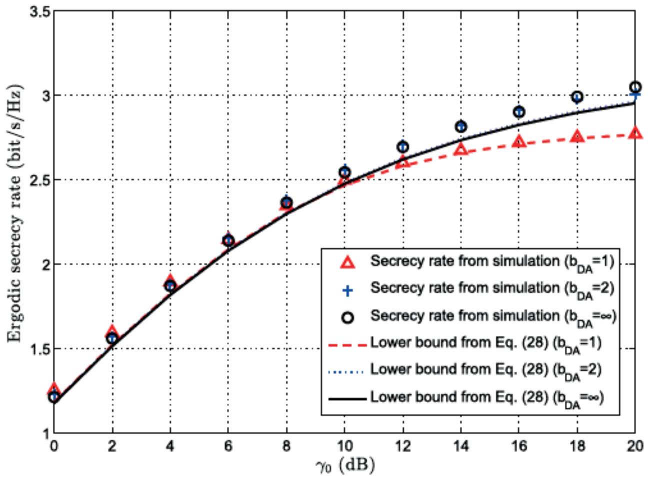

Fig. 10. Ergodic secrecy rate with the optimal ϕ^* versus SNR for random AN method ($N = 128$, $K = 8$, and $M = 12$).

rates with the optimal ϕ^* are approximately equal for $b_{\mathrm{DA}} = 1, 2, 3$, and ∞, i.e., $\underline{R}_{\mathrm{sec}}^{\mathcal{R}} = 1.6346$ and 0.9113 for $\gamma_0 = 5$ and 0 dB, respectively. For various DAC resolutions, the same peak secrecy rate can be achieved as long as the optimal ϕ^* is used. In other words, the impact of low-resolution DACs on secure transmission is insignificant. This is because the DAC quantization noise acts as random AN at both the users and eavesdropper. Although the quantization noise increases with a lower b_{DA}, the same maximum secrecy rate can still be achieved by increasing ϕ to reduce the AN power. Compare Fig. 7 and Fig. 9 and take $\gamma_0 = 0$ dB for instance. When infinite-resolution DACs are deployed and using the optimal ϕ^*, the highest secrecy rate is $\underline{R}_{\mathrm{sec}}^{\mathcal{N}} = 1.4788$ with null-space AN, which is much larger than $\underline{R}_{\mathrm{sec}}^{\mathcal{R}} = 0.9113$ with random AN. When 1-bit DACs are considered, we have $\underline{R}_{\mathrm{sec}}^{\mathcal{N}} = 1.1217$, which is closer to $\underline{R}_{\mathrm{sec}}^{\mathcal{R}} = 0.9113$. This implies that random AN becomes cost-efficient when low-resolution DACs are adopted. The advantage of null-space AN is marginal in this case. The achievable secrecy rates are displayed in Fig. 10 when the optimal ϕ^* is used. As observed from Fig. 9, the secrecy rates are generally not degraded by low-resolution DACs, except at high SNR with $b_{\mathrm{DA}} = 1$. Hence, using DAC resolutions beyond 1 bit is not beneficial in terms of secrecy rate. This implies that low-resolution DACs can provide almost the same secure performance as infinite resolution DACs with random AN. For the scenario in Fig. 10 where 1-bit DACs are employed and $\gamma_0 > 9.8$ dB, the secrecy rate increases monotonically with $\phi \in (0, 1]$ and therefore $\phi^* = 1$, which is different from the cases with low SNR shown in Fig. 9. Under this condition, at least a two-bit DAC is needed at the BS to achieve the same secrecy rate as that in the infinite resolution case.

VI. Conclusions

In this paper, we investigate the physical layer security of a multiuser massive MIMO system employing low-resolution DACs at the transmitter, in the presence of a passive eavesdropper. A tight lower bound for the achievable secrecy rate of each user is derived. We find that the DAC quantization noise can be regarded as additional AN provided by the BS and may contribute to the secure transmission. Given a fixed power allocation factor ϕ, low-resolution DACs can achieve superior secrecy performance under certain conditions, e.g., at low SNR or with large ϕ. If the optimal ϕ^* can be obtained, low-resolution DACs inevitably lead to secrecy rate loss with the null-space AN design method. On the other hand, for random AN, low-resolution DACs achieve the same secrecy performance as high-resolution DACs at low SNR and thus the former are cost-efficient in this scenario. Note that our derived results directly apply for the system with multi-antenna users if multiple data streams are transmitted to each user. This is because in massive MIMO, an L-antenna user can be equivalently regarded as L single-antenna users, due to the asymptotic orthogonality among channel vectors. However, the extension becomes more complicated if a single data stream is transmitted. Interesting future work includes further extending our current results to such a general secnario with multi-antenna users.

Appendix A
Proof of Lemma 2

In order to obtain the asymptotic expression for γ_k, we derive S_k, I_k, Q_k, and A_k in (15) one by one. Consider a typical ZF-precoder under the constraint that $\mathrm{tr}\{\mathbf{W}\mathbf{W}^H\} = K$, i.e.,

$$\mathbf{W} = \sqrt{\frac{K}{\mathrm{tr}\{(\mathbf{H}\mathbf{H}^H)^{-1}\}}}\mathbf{H}^H(\mathbf{H}\mathbf{H}^H)^{-1}. \tag{50}$$

It is well known that $\mathbf{H}\mathbf{H}^H \sim \mathcal{W}_k(N, \mathbf{I}_k)$, where $\mathcal{W}_m(n, \mathbf{\Sigma})$ denotes an $m \times m$ Wishart matrix with n degrees of freedom and $\mathbf{\Sigma}$ is the covariance matrix of each column. Assuming that K and N grow to infinity with a fixed ratio $\beta = \frac{K}{N}$, we have [54]

$$\mathrm{tr}\{(\mathbf{H}\mathbf{H}^H)^{-1}\} \xrightarrow{a.s.} \frac{\beta}{1-\beta}. \tag{51}$$

Substituting (51) in (50) yields

$$\mathbf{H}\mathbf{W} \xrightarrow{a.s.} \sqrt{K\left(\frac{1}{\beta} - 1\right)}\mathbf{I}_k. \tag{52}$$

Thus, S_k and I_k converge to

$$S_k \xrightarrow{a.s.} (1-\rho)\phi P\left(\frac{1}{\beta} - 1\right) \tag{53}$$

and

$$I_k \xrightarrow{a.s.} 0, \tag{54}$$

respectively.

As for Q_k, the emphasis lies on the asymptotic characterizations of $\mathbf{C}_{\mathrm{DA}}$ in (8). For large N and K, $\mathbf{C}_{\mathrm{DA}}$ converges to a scaled identity matrix as follows

$$\mathbf{C}_{\mathrm{DA}} \xrightarrow{a.s.} \rho\frac{P}{N}\mathbf{I}_N, \tag{55}$$

where we use (5), (6), and the fact that

$$\mathrm{diag}(\mathbf{W}\mathbf{W}^H) \xrightarrow{a.s.} \frac{K}{N}\mathbf{I}_N \tag{56}$$

and

$$\mathrm{diag}(\mathbf{V}\mathbf{V}^H) \xrightarrow{a.s.} \frac{N-K}{N}\mathbf{I}_N, \tag{57}$$

due to the strong law of large numbers. Then, by substituting (55) into (15), we have

$$\begin{aligned} Q_k &\xrightarrow{a.s.} \rho\frac{P}{N}\mathbf{h}_k^T\mathbf{h}_k^* \\ &= \rho P. \end{aligned} \tag{58}$$

Finally for A_k, the result depends on the AN shaping matrix $\mathbf{V}$. For the null-space AN method with $\mathbf{HV} = \mathbf{0}$, it is obvious that

$$A_k^{\mathcal{N}} = 0. \tag{59}$$

For the random AN method, $A_k^{\mathcal{R}}$ in (15) can be regarded as a matrix comprised of one single element, i.e., $A_k^{\mathcal{R}} \sim \mathcal{W}_1(N-K, (1-\rho)q)$, and it follows that

$$\begin{aligned} A_k^{\mathcal{R}} &= \mathrm{tr}\left\{A_k^{\mathcal{R}}\right\} \\ &= (N-K)(1-\rho)q \qquad (60) \\ &= (1-\rho)(1-\phi)P, \qquad (61) \end{aligned}$$

where (60) comes from the fact that $\mathrm{tr}\{\mathbf{A}\} = mn$ for a Wishart matrix $\mathbf{A} \sim \mathcal{W}_m(n, \mathbf{I}_m)$ [54], and (61) uses (6).

Now, by substituting (53), (54), (58), (59), and (61) into (15), the asymptotic SIQNRs for the null-space and random AN methods are respectively obtained in (17) and (18).

Appendix B
Proof of Theorem 1

To begin with, we demonstrate that $\mathbf{X}$ defined in (22) can be approximated as a scaled Wishart matrix. Substituting (55) into (22) yields

$$\begin{aligned} \mathbf{X} &\xrightarrow{a.s.} (1-\rho)q\mathbf{H}_\mathrm{e}\mathbf{V}\mathbf{V}^H\mathbf{H}_\mathrm{e}^H + \rho\frac{P}{N}\mathbf{H}_\mathrm{e}\mathbf{H}_\mathrm{e}^H \\ &= (1-\rho)q\mathbf{H}_\mathrm{e}\mathbf{V}\mathbf{V}^H\mathbf{H}_\mathrm{e}^H + \rho\frac{P}{N}\mathbf{H}_\mathrm{e}[\mathbf{V}\ \mathbf{V}_0][\mathbf{V}\ \mathbf{V}_0]^H\mathbf{H}_\mathrm{e}^H \qquad (62) \\ &= \left[(1-\rho)q + \rho\frac{P}{N}\right]\underbrace{\mathbf{H}_1\mathbf{H}_1^H}_{\mathbf{W}_1} + \rho\frac{P}{N}\underbrace{\mathbf{H}_2\mathbf{H}_2^H}_{\mathbf{W}_2}, \qquad (63) \end{aligned}$$

where (62) uses the fact that $[\mathbf{V}\ \mathbf{V}_0][\mathbf{V}\ \mathbf{V}_0]^H = \mathbf{I}_M$ since $[\mathbf{V}\ \mathbf{V}_0]$ is a complete orthogonal basis with dimension N, and (63) utilizes the definitions $\mathbf{H}_1 \triangleq \mathbf{H}_\mathrm{e}\mathbf{V}$ and $\mathbf{H}_2 \triangleq \mathbf{H}_\mathrm{e}\mathbf{V}_0$. From (63), $\mathbf{X}$ is statistically equivalent to a weighted sum of two scaled Wishart matrices, i.e., $\mathbf{X}_1 \sim \mathcal{W}_M(N-K, \mathbf{I}_M)$ and $\mathbf{X}_2 \sim \mathcal{W}_M(K, \mathbf{I}_M)$. Strictly speaking, $\mathbf{X}$ is not a Wishart matrix and the exact distribution of $\mathbf{X}$ is intractable. However, $\mathbf{X}$ may be accurately approximated as a single scaled Wishart matrix, $\mathbf{X} \sim \mathcal{W}_M(\eta, \lambda\mathbf{I}_M)$, where the parameters η and λ are chosen such that the first two moments of $\mathbf{X}$ and $\left[(1-\rho)q + \rho\frac{P}{N}\right]\mathbf{W}_1 + \rho\frac{P}{N}\mathbf{W}_2$ are identical [30], which yields

$$\eta\lambda = (N-K)\left[(1-\rho)q + \rho\frac{P}{N}\right] + K\rho\frac{P}{N} \tag{64}$$

and

$$\eta\lambda^2 = (N-K)\left[(1-\rho)q + \rho\frac{P}{N}\right]^2 + K\left(\rho\frac{P}{N}\right)^2. \tag{65}$$

Substituting (6) into (64) and (65), η and λ are obtained as

$$\eta = N\frac{[(1-\rho)(1-\phi)+\rho]^2}{[(1-\rho)(1-\phi)+\rho]^2 + (1-\rho)^2(1-\phi)^2\frac{K}{N-K}} \tag{66}$$

and

$$\lambda = \frac{P}{N}\frac{[(1-\rho)(1-\phi)+\rho]^2 + (1-\rho)^2(1-\phi)^2\frac{K}{N-K}}{(1-\rho)(1-\phi)+\rho}, \tag{67}$$

respectively.

Next, we apply Jensen's inequality which yields an upper bound for the eavesdropper's capacity:

$$\begin{aligned} C_k &\leq \log_2\left[1 + (1-\rho)p\,\mathbb{E}\left\{\mathbf{w}_k^H\mathbf{H}_\mathrm{e}^H\mathbf{X}^{-1}\mathbf{H}_\mathrm{e}\mathbf{w}_k\right\}\right] \\ &= \log_2\left[1 + \frac{(1-\rho)p}{\lambda(\eta-M)}\,\mathbb{E}\left\{\mathbf{w}_k^H\mathbf{H}_\mathrm{e}^H\mathbf{H}_\mathrm{e}\mathbf{w}_k\right\}\right] \qquad (68) \\ &= \log_2\left[1 + \frac{(1-\rho)pM}{\lambda(\eta-M)}\,\mathbb{E}\left\{\mathbf{w}_k^H\mathbf{w}_k\right\}\right] \qquad (69) \\ &= \log_2\left[1 + \frac{(1-\rho)pM}{\lambda(\eta-M)}\right], \qquad (70) \end{aligned}$$

where (68) utilizes the property that $\mathbf{A}^{-1} \xrightarrow{a.s.} \frac{1}{n-m}\mathbf{I}_m$ for a Wishart matrix $\mathbf{A} \sim \mathcal{W}_m(n, \mathbf{I}_m)$ with $n > m$ [39], (69) uses the fact that $\frac{1}{M}\mathbf{H}_\mathrm{e}^H\mathbf{H}_\mathrm{e} - \mathbf{I}_N \xrightarrow{a.s.} \mathbf{0}_N$ due to the Central Limit Theorem, and (70) applies the weak law of large numbers and $\mathbb{E}\{\mathbf{w}_k^H\mathbf{w}_k\} = \frac{1}{K}\sum_{k=1}^{K}\mathbf{w}_k^H\mathbf{w}_k = \frac{1}{K}\mathrm{tr}\{\mathbf{W}^H\mathbf{W}\} = 1$. Note that the derivation in (68) only holds for an invertible $\mathbf{X} \sim \mathcal{W}_M(\eta, \lambda\mathbf{I}_M)$, which yields $\eta - M > 0$. By substituting (11), (12), and (66), we have

$$\begin{aligned} &\eta - M \\ &= N\frac{(1-\alpha)(1-\beta)[(1-\rho)(1-\phi)+\rho]^2 - \alpha\beta(-\rho)^2(1-\phi)^2}{(1-\beta)[(1-\rho)(1-\phi)+\rho]^2 + \beta(1-\rho)^2(1-\phi)^2} \\ &= N\frac{(1-\alpha)(1-\beta)(1-\rho)^2(1-\phi)^2}{(1-\beta)[(1-\rho)(1-\phi)+\rho]^2 + \beta(1-\rho)^2(1-\phi)^2} \\ &\quad \times \left[\left(1 + \frac{\rho}{(1-\rho)(1-\phi)}\right)^2 - \frac{\alpha\beta}{(1-\alpha)(1-\beta)}\right] > 0. \end{aligned} \tag{71}$$

Regardless of the values of $\rho \in (0,1)$ and $\phi \in (0,1]$, (71) holds if $\frac{\alpha\beta}{(1-\alpha)(1-\beta)} < 1$, which yields $\alpha + \beta < 1$ with $\beta \in (0,1)$ and $\alpha \in (0,1)$. Fortunately, this is a common condition for massive MIMO systems with large N.

Finally by substituting (5), (66), and (67) into (70), the upper bound in (23) is directly obtained.

REFERENCES

[1] J. L. Massey, "An introduction to contemporary cryptology," *Proc. IEEE*, vol. 76, no. 5, pp. 533–549, May 1988.

[2] S. A. A. Fakoorian and A. L. Swindlehurst, "On the optimality of linear precoding for secrecy in the MIMO broadcast channel," *IEEE J. Sel. Areas Commun.*, vol. 31, no. 9, pp. 1701–1713, Sep. 2013.

[3] H. Alves, R. D. Souza, M. Debbah, and M. Bennis, "Performance of transmit antenna selection physical layer security schemes," *IEEE Signal Process. Lett.*, vol. 19, no. 6, pp. 372–375, Jun. 2012.

[4] E. Boshkovska, D. W. K. Ng, L. Dai, and R. Schober, "Power-efficient and secure WPCNs with hardware impairments and non-linear EH circuit," *IEEE Trans. Commun.*, vol. 66, no. 6, pp. 2642–2657, Jun. 2018.

[5] C. Mitrpant, A. J. H. Vinck, and Y. Luo, "An achievable region for the Gaussian wiretap channel with side information," *IEEE Trans. Inf. Theory*, vol. 52, no. 5, pp. 2181–2190, May 2006.

[6] Z. Li, R. Yates, and W. Trappe, "Secret communication with a fading eavesdropper channel," in *Proc. IEEE ISIT*, Nice, France, Jun. 2007, pp. 1296–1300.

[7] P. K. 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.

[8] A. Mukherjee, S. A. A. Fakoorian, J. Huang, and A. L. Swindlehurst, "Principles of physical layer security in multiuser wireless networks: A survey," *IEEE Commun. Surveys Tuts.*, vol. 16, no. 3, pp. 1550–1573, 3rd Quart., 2014.

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

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

[11] X. Yu, C. Li, J. Zhang, and K. B. Letaief, "A tractable framework for performance analysis of dense multi-antenna networks," in *Proc. IEEE ICC*, Paris, France, May 2017, pp. 1–6.

[12] 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.

[13] A. Khisti, G. Wornell, A. Wiesel, and Y. Eldar, "On the Gaussian MIMO wiretap channel," in *Proc. IEEE ISIT*, Nice, France, Jun. 2007, pp. 2471–2475.

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

[15] S. Goel and R. Negi, "Guaranteeing secrecy using artificial noise," *IEEE Trans. Wireless Commun.*, vol. 7, no. 6, pp. 2180–2189, Jun. 2008.

[16] 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.

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

[18] 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.

[19] F. Zhu, F. Gao, H. Lin, S. Jin, J. Zhao, and G. Qian, "Robust beamforming for physical layer security in BDMA massive MIMO," *IEEE J. Sel. Areas Commun.*, vol. 36, no. 4, pp. 775–787, Apr. 2018.

[20] E. G. Larsson, O. Edfors, F. Tufvesson, and T. L. Marzetta, "Massive MIMO for next generation wireless systems," *IEEE Commun. Mag.*, vol. 52, no. 2, pp. 186–195, Feb. 2014.

[21] L. Lu, G. Y. Li, A. L. Swindlehurst, A. Ashikhmin, and R. Zhang, "An overview of massive MIMO: Benefits and challenges," *IEEE J. Sel. Topics Signal Process.*, vol. 8, no. 5, pp. 742–758, Oct. 2014.

[22] H. Xie, F. Gao, S. Zhang, and S. Jin, "A unified transmission strategy for TDD/FDD massive MIMO systems with spatial basis expansion model," *IEEE Trans. Veh. Technol.*, vol. 66, no. 4, pp. 3170–3184, Apr. 2017.

[23] V. W. S. Wong, R. Schober, D. W. K. Ng, and L.-C. Wang, *Key Technologies for 5G Wireless Systems*. Cambridge, U.K.: Cambridge Univ. Press, 2017.

[24] J. Hoydis, S. ten Brink, and M. Debbah, "Massive MIMO in the UL/DL of cellular networks: How many antennas do we need?" *IEEE J. Sel. Areas Commun.*, vol. 31, no. 2, pp. 160–171, Feb. 2013.

[25] H. Q. Ngo, E. G. Larsson, and T. L. Marzetta, "Energy and spectral efficiency of very large multiuser MIMO systems," *IEEE Trans. Commun.*, vol. 61, no. 4, pp. 1436–1449, Apr. 2013.

[26] W. Xu, J. Liu, S. Jin, and X. Dong, "Spectral and energy efficiency of multi-pair massive MIMO relay network with hybrid processing," *IEEE Trans. Commun.*, vol. 65, no. 9, pp. 3794–3809, Sep. 2017.

[27] B. Wang *et al.*, "Spatial-wideband effect in massive MIMO with application in mmWave systems," *IEEE Commun. Mag.*, vol. 56, no. 12, pp. 134–141, Dec. 2018.

[28] G. Geraci, H. S. Dhillon, J. G. Andrews, J. Yuan, and I. B. Collings, "Physical layer security in downlink multi-antenna cellular networks," *IEEE Trans. Commun.*, vol. 62, no. 6, pp. 2006–2021, Jun. 2014.

[29] X. Chen, L. Lei, H. Zhang, and C. Yuen, "Large-scale MIMO relaying techniques for physical layer security: AF or DF?" *IEEE Trans. Wireless Commun.*, vol. 14, no. 9, pp. 5135–5146, Sep. 2015.

[30] J. Zhu, R. Schober, and V. K. Bhargava, "Secure transmission in multicell massive MIMO systems," *IEEE Trans. Wireless Commun.*, vol. 13, no. 9, pp. 4766–4781, Sep. 2014.

[31] J. Zhu, R. Schober, and V. K Bhargava, "Linear precoding of data and artificial noise in secure massive MIMO systems," *IEEE Trans. Wireless Commun.*, vol. 15, no. 3, pp. 2245–2261, Mar. 2016.

[32] W. Zhao, S.-H. Lee, and A. Khisti, "Phase-only zero forcing for secure communication with multiple antennas," *IEEE J. Sel. Topics Signal Process.*, vol. 10, no. 8, pp. 1334–1345, Dec. 2016.

[33] S. Yan, X. Zhou, N. Yang, T. D. Abhayapala, and A. L. Swindlehurst, "Secret channel training to enhance physical layer security with a full-duplex receiver," *IEEE Trans. Inf. Forensics Security*, vol. 13, no. 11, pp. 2788–2800, May 2018.

[34] N.-P. Nguyen, H. Q. Ngo, T. Q. Duong, H. D. Tuan, and K. Tourki, "Secure massive MIMO with the artificial noise-aided downlink training," *IEEE J. Sel. Areas Commun.*, vol. 36, no. 4, pp. 802–816, Apr. 2018.

[35] S. Jacobsson, G. Durisi, M. Coldrey, T. Goldstein, and C. Studer, "Quantized precoding for massive MU-MIMO," *IEEE Trans. Commun.*, vol. 65, no. 11, pp. 4670–4684, Nov. 2017.

[36] H. Jedda, A. Mezghani, A. L. Swindlehurst, and J. A. Nossek, "Quantized constant envelope precoding with PSK and QAM signaling," *IEEE Trans. Wireless Commun.*, vol. 17, no. 12, pp. 8022–8034, Dec. 2018.

[37] O. Castañeda, T. Goldstein, and C. Studer, "POKEMON: A non-linear beamforming algorithm for 1-bit massive MIMO," in *Proc. IEEE ICASSP*, New Orleans, LA, USA, Jun. 2017, pp. 3464–3468.

[38] A. Swindlehurst, A. Saxena, A. Mezghani, and I. Fijalkow, "Minimum probability-of-error perturbation precoding for the one-bit massive MIMO downlink," in *Proc. IEEE ICASSP*, New Orleans, LA, USA, Mar. 2017, pp. 6483–6487.

[39] A. K. Saxena, I. Fijalkow, and A. L. Swindlehurst, "Analysis of one-bit quantized precoding for the multiuser massive MIMO downlink," *IEEE Trans. Signal Process.*, vol. 65, no. 17, pp. 4624–4634, Sep. 2017.

[40] O. Bin Usman, H. Jedda, A. Mezghani, and J. A. Nossek, "MMSE precoder for massive MIMO using 1-bit quantization," in *Proc. IEEE ICASSP*, Shanghai, China, May 2016, pp. 3381–3385.

[41] Y. Li, C. Tao, A. L. Swindlehurst, A. Mezghani, and L. Liu, "Downlink achievable rate analysis in massive MIMO systems with one-bit DACs," *IEEE Commun. Lett.*, vol. 21, no. 7, pp. 1669–1672, Jul. 2017.

[42] J. J. Bussgang, "Crosscorrelation functions of amplitude-distorted Gaussian signals," Res. Lab. Electron., Massachusetts Inst. Technol., Cambridge, MA, USA, Tech. Rep. 216, Mar. 1952.

[43] A. Mezghani and J. Nossek, "Capacity lower bound of MIMO channels with output quantization and correlated noise," in *Proc. IEEE ISIT*, Cambridge, MA, USA, Jul. 2012, pp. 1–5.

[44] J. Xu, W. Xu, F. Gong, H. Zhang, and X. You, "Optimal multiuser loading in quantized massive MIMO under spatially correlated channels," *IEEE Trans. Veh. Technol.*, to be published.

[45] J. Zhu, D. W. K. Ng, N. Wang, R. Schober, and V. K. Bhargava, "Analysis and design of secure massive MIMO systems in the presence of hardware impairments," *IEEE Trans. Wireless Commun.*, vol. 16, no. 3, pp. 2001–2016, Jan. 2017.

[46] H. Yin, D. Gesbert, M. Filippou, and Y. Liu, "A coordinated approach to channel estimation in large-scale multiple-antenna systems," *IEEE J. Sel. Areas Commun.*, vol. 31, no. 2, pp. 264–271, Feb. 2013.

[47] C. Lu, W. Xu, H. Shen, J. Zhu, and K. Wang, "MIMO channel information feedback using deep recurrent network," *IEEE Commun. Lett.*, vol. 23, no. 1, pp. 188–191, Jan. 2019.

[48] S. Noh, M. D. Zoltowski, Y. Sung, and D. J. Love, "Pilot beam pattern design for channel estimation in massive MIMO systems," *IEEE J. Sel. Topics Signal Process.*, vol. 8, no. 5, pp. 787–801, Oct. 2014.

[49] H. Xie, F. Gao, and S. Jin, "An overview of low-rank channel estimation for massive MIMO systems," *IEEE Access*, vol. 4, pp. 7313–7321, Nov. 2016.

[50] J. Xu, W. Xu, and F. Gong, "On performance of quantized transceiver in multiuser massive MIMO downlinks," *IEEE Wireless Commun. Lett.*, vol. 6, no. 5, pp. 562–565, Oct. 2017.

[51] P. Billingsley, *Convergence of Probability Measures*, Hoboken, NJ, USA: Wiley, 1969.

[52] A. Goldsmith, S. A. Jafar, N. Jindal, and S. Vishwanath, "Capacity limits of MIMO channels," *IEEE J. Sel. Areas Commun.*, vol. 21, no. 5, pp. 684–702, Jun. 2003.

[53] J. Max, "Quantizing for minimum distortion," *IRE Trans. Inf. Theory*, vol. 6, no. 1, pp. 7–12, Mar. 1960.

[54] A. M. Tulino and S. Verdú, *Random Matrix Theory and Wireless Communications*. Boston, MA, USA: Now, 2004.

Jindan Xu (S'16) received the B.E. degree in electrical engineering from Southeast University, Nanjing, China, in 2015, where she is currently pursuing the Ph.D. degree with the National Mobile Communications Research Laboratory, School of Information Science and Engineering. She is a Visiting Student with the Department of Electrical Engineering and Computer Science, University of California at Irvine, Irvine, CA, USA. Her current research interests include massive multiple-input multiple-output, mm-wave communications, and machine learning for wireless communications.

Wei Xu (S'07–M'09–SM'15) received the B.Sc. degree in electrical engineering and the M.S. and Ph.D. degrees in communication and information engineering from Southeast University, Nanjing, China, in 2003, 2006, and 2009, respectively. Between 2009 and 2010, he was a Post-Doctoral Research Fellow with the Department of Electrical and Computer Engineering, University of Victoria, Canada. He is currently a Professor with the National Mobile Communications Research Laboratory, Southeast University. He is also an Adjunct Professor with the University of Victoria and a Distinguished Visiting Fellow of the Royal Academy of Engineering, U.K. He has co-authored over 100 refereed journal papers and holds 36 granted domestic patents and four U.S. patents. His research interests include cooperative communications, information theory, signal processing, and machine learning for wireless communications. He was a co-recipient of the First Prize of the Science and Technology Award in Jiangsu, China, in 2014, and the Youth Science and Technology Award of the China Institute of Communications in 2018. He received the best paper awards from the IEEE MAPE 2013, the IEEE/CIC ICCC 2014, the IEEE Globecom 2014, the IEEE ICUWB 2016, WCSP 2017, and ISWCS 2018. He was an Editor of the IEEE COMMUNICATIONS LETTERS from 2012 to 2017. He is currently an Editor of the IEEE TRANSACTIONS ON COMMUNICATIONS and the IEEE ACCESS.

Jun Zhu (S'10–M'16) was born in Nanjing, China. He received the B.Sc. degree (Hons.) in information engineering from Southeast University, Nanjing, China, in 2008, the M.A.Sc. degree (Hons.) in electrical engineering from the University of Victoria, Victoria, Canada, in 2011, and the Ph.D. degree (Hons.) in electrical engineering from The University of British Columbia, Vancouver, Canada, in 2016. During 2014–2015, he was a Visiting Researcher with the Institute for Digital Communications, Friedrich–Alexander University, Erlangen, Germany. In 2016, he joined The University of British Columbia, as a Post-Doctoral Research Fellow. He is currently a Senior System Engineer with Qualcomm, San Diego, CA, USA. His main focus is on 5G wireless system design. He also serves as an Adjunct Professor with the University of Victoria. His research interests include multiple-input multiple-output (MIMO) OFDM wireless systems, massive MIMO, energy-efficient (green) communications, and physical layer security. He has served on the technical program committees for many international conferences including the IEEE Globecom, the IEEE PacRim, and the IEEE WCSP.

Dr. Zhu was a Finalist of the Lieutenant Governor's Silver Medal for Outstanding Master Thesis at the University of Victoria. He was a recipient of the Dr. Esme Foord Scholarship in 2011, the Pei-Huang Tung and Tan-Wen Tung Fellowship in 2012, the Graduate Support Initiative Award in 2013, the Chinese Government Award for Outstanding Self-Financed Students Abroad in 2014, the German Academic Exchange Service (DAAD) Grant, and the UBC International Research Award in 2015. He received the Four-Year-Fellowship from The University of British Columbia in 2011 and the QualStar Award from Qualcomm for three times in 2017.

Derrick Wing Kwan Ng (S'06–M'12–SM'17) received the bachelor's (Hons.) and M.Phil. degrees in electronic engineering from The Hong Kong University of Science and Technology in 2006 and 2008, respectively, and the Ph.D. degree from The University of British Columbia in 2012. He was a Senior Post-Doctoral Fellow with the Institute for Digital Communications, Friedrich–Alexander University Erlangen–Nürnberg, Germany. He is currently a Senior Lecturer and an ARC DECRA Research Fellow with The University of New South Wales, Sydney, Australia. His research interests include convex and non-convex optimization, physical layer security, wireless information and power transfer, and green (energy-efficient) wireless communications. Dr. Ng received the best paper awards at the IEEE TCGCC Best Journal Paper Award 2018, INISCOM 2018, IEEE International Conference on Communications 2018, IEEE International Conference on Computing, Networking and Communications 2016, IEEE Wireless Communications and Networking Conference 2012, the IEEE Global Telecommunication Conference (Globecom) 2011, and the IEEE Third International Conference on Communications and Networking in China in 2008. He is listed as a 2018 Highly Cited Researcher by Clarivate Analytics. He has been serving as an Editorial Assistant to the Editor-in-Chief of the IEEE TRANSACTIONS ON COMMUNICATIONS since 2012.

A. Lee Swindlehurst (S'83–M'84–SM'99–F'04) received the B.S. and M.S. degrees in electrical engineering from Brigham Young University (BYU), Provo, UT, USA, in 1985 and 1986, respectively, and the Ph.D. degree in electrical engineering from Stanford University, Stanford, CA, USA, in 1991. From 1990 to 2007, he was with the Department of Electrical and Computer Engineering, BYU. During 1996–1997, he was a Visiting Scholar with Uppsala University and the Royal Institute of Technology, Sweden. From 2003 to 2006, he was the Department Chair with BYU. From 2006 to 2007, he was on leave as a Vice President of research from ArrayComm LLC, San Jose, CA, USA. From 2013 to 2016, he served as an Associate Dean for research and graduate studies with the Samueli School of Engineering, University of California at Irvine, Irvine, CA, USA. During 2014–2017, he was a Hans Fischer Senior Fellow with the Institute for Advanced Studies, Technical University of Munich. Since 2007, he has been a Professor with the Electrical Engineering and Computer Science Department, University of California at Irvine. His research focuses on array signal processing for radar, wireless communications, and biomedical applications. He has over 300 publications in these areas. He is a fellow of the IEEE. He was a recipient of the 2000 IEEE W. R. G. Baker Prize Paper Award, the 2006 IEEE Communications Society Stephen O. Rice Prize in the Field of Communication Theory, the 2006 and 2010 IEEE Signal Processing Society's best paper awards, and the 2017 IEEE Signal Processing Society Donald G. Fink Overview Paper Award. He was the Inaugural Editor-in-Chief of the IEEE JOURNAL OF SELECTED TOPICS IN SIGNAL PROCESSING.