IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received July 10, 2020, accepted July 27, 2020, date of publication August 3, 2020, date of current version August 12, 2020.

Digital Object Identifier 10.1109/ACCESS.2020.3013635

Secure Massive MIMO Downlink With Low-Resolution ADCs/DACs in the Presence of Active Eavesdropping

QIAN XU, (Graduate Student Member, IEEE), AND PINYI REN, (Member, IEEE)
School of Information and Communications Engineering, Xi'an Jiaotong University, Xi'an 710049, China
Shaanxi Smart Networks and Ubiquitous Access Research Center, Xi'an 710049, China

Corresponding author: Pinyi Ren (pyren@mail.xjtu.edu.cn)

This work was supported in part by the National Natural Science Foundation of China under Grant 61941119 and Grant 61431011; and in part by the Fundamental Research Funds for the Central Universities.

ABSTRACT In this paper we study the secrecy performance of a downlink massive multiple-input multiple-output (MIMO) system in the presence of pilot spoofing attack (PSA). Specifically, the base station (BS), which is equipped with low-resolution analog-to-digital converters (ADCs) and digital-to-analog converters (DACs), exploits the low-complexity random artificial noise (AN) to improve secrecy. With the aid of the additive quantization noise model, the ergodic secrecy rate is derived. Based on the derived results, we study the impact of ADCs' and DACs' resolutions on the secrecy performance for the two different scenarios: the scenarios with and without the knowledge of the PSA power. The optimal power allocation parameter, which allocates power between the information-bearing signal and AN, is derived for the scenario with the knowledge of the PSA power. For ADCs, our theoretical results indicate that high-resolution ADCs are always favorable for improving secrecy, regardless of the availability of the PSA power. However, the impact of DACs' resolution is related to the knowledge of the PSA power. For the scenario without the PSA power, enhancing the resolution of DACs does not necessarily improve the secrecy performance due to the inappropriate power allocation. For the scenario with the PSA power, DACs with different resolutions can achieve the same ergodic secrecy rate in most cases, since the optimal power allocation can make a balance between mitigating the rate loss due to coarse quantization and injecting AN for anti-eavesdropping. Only in the case where the PSA power is small, high-resolution DACs achieve a higher ergodic secrecy rate. Finally, we propose a PSA detection method and study the effect of low-resolution ADCs on the detection performance. It is found that the resolution of ADCs has little effect on the performance of PSA detection.

INDEX TERMS Physical layer security, massive MIMO, low-resolution ADCs, low-resolution DACs, active eavesdropping.

I. INTRODUCTION

Due to the increasingly ubiquitous information exchange among mobile users, the secrecy assurance of private messages is becoming more and more important and has aroused great research interests. However, the broadcast nature of wireless channels exposes the confidential messages to eavesdroppers, which greatly increases the risk of information leakage. The traditional anti-eavesdropping strategy is based on cryptography. For this cryptographic method, secret keys are needed to encrypt the confidential message before transmission. Thus, the generation and distribution of secret keys is the most important issue for this method. Different from the cryptographic method, physical layer security (PLS) [1], which has been considered as another promising anti-eavesdropping strategy, can achieve secure transmission without secret keys. Moreover, PLS can achieve information-theoretical secrecy. That is, the achieved secrecy is always guaranteed regardless of the eavesdropper's computing capability. The core idea of PLS is exploiting the randomness and independence of wireless channels to guarantee the secrecy of the transmitted message. By using the wiretap codes [2], the confidential message can be successfully obtained by the intended user while unaccessible to

The associate editor coordinating the review of this manuscript and approving it for publication was Ki-Hong Park.

the eavesdropper. Based on the theoretical work in [2]–[4], a great number of PLS-based secure transmission strategies have been proposed, including artificial noise injection [5], secure precoding [6], and cooperative transmission [7], [8].

Among many PLS-based secure transmission techniques, multi-antenna transmission is an important technique, since it can boost the signal power at intended users while degrade that at eavesdroppers. From this perspective, massive multiple-input multiple-output (MIMO) is naturally beneficial for secrecy improvement due to the large number of antennas at the base station (BS) [9], [10]. With the channel state information (CSI) of intended users, the signal beams can be directed to intended users with little signal intercepted by eavesdroppers. Note that the eavesdroppers in [9], [10] are passive eavesdroppers who keep silent without transmitting any signals. In contrast, the eavesdroppers who can transmit to facilitate eavesdropping are called active eavesdroppers. Typically, the active eavesdropper can launch two kinds of attacks, jamming attack [11], [12] and pilot spoofing attack (PSA) [13]–[17]. For jamming attack, the eavesdropper broadcasts jamming signal or random noise to block the signal reception at intended users. On the contrary, PSA focuses on the channel estimation phase instead of the message transmission phase. By sending the same pilot sequence as the intended user's, the estimated channel of the intended user is contaminated by the eavesdropping link, which will make the BS beamform the confidential message to the eavesdropper. In this paper, we only consider the threat of PSA as in [13]–[17]. The research in [13] evaluated the achievable secrecy rate of a massive MIMO relay system and concluded that the detrimental effect of PSA cannot be mitigated even with infinite number of antennas at the BS. The works in [14] and [15] first detected the existence of PSA using energy detectors and then performed secure downlink precoding. The authors in [16] exploited random pilot sequences for PSA detection while the authors in [17] proposed a double training method for PSA detection.

The aforementioned research works all assume perfect analog-to-digital converters (ADCs) and digital-to-analog converters (DACs). However, according to [18], the energy consumption of ADCs and DACs grows exponentially with the quantization bits. For a practical massive MIMO system with hundreds of antennas, the power consumption will be prohibitively high if each antenna is connected to an infinite-resolution ADC for signal receiving and infinite-resolution DAC for signal transmission. To tackle this issue, great research effort has been devoted to low-resolution ADCs/DACs [19]–[24] and mixed-ADCs/DACs [25], [26] for reducing power consumption. For low-resolution ADCs/DACs in [19]–[24], the ADC/DAC for each antenna has the same number of quantization bits (e.g., 1-3 bits). The work in [19] studied the channel estimation with low-resolution ADCs. It is concluded that massive MIMO with low-resolution ADCs requires more training time compared with the system with infinite-resolution ADCs. The work in [20] investigated the energy efficiency of massive MIMO system with low-resolution ADCs while the work in [21] considered both the low-resolution ADCs and DACs. The above study is then extended to full-duplex massive MIMO as in [22] and [23]. Different from [19]–[23] where the Rayleigh fading was assumed, the work in [24] studied the uplink spectral efficiency of massive MIMO with low-resolution ADCs in Rician fading environment. For mixed-ADCs/DACs in [25], [26], both low-resolution and infinite-resolution ADCs/DACs are employed. The work in [25] showed that the mixed-ADC/DAC system can achieve a favorable trade-off between throughput and power consumption. The performance of the above mixed-ADC/DAC structure is also studied for Rician fading channels in [26]. A comprehensive study of millimeter-wave massive MIMO systems with low-resolution ADCs was presented in [27], where several key issues such as channel estimation and signal detection were investigated.

Although there have been plenty of studies on massive MIMO with low-resolution ADCs/DACs, to the best of our knowledge, only a few research works [28]–[30] have investigated the secrecy performance of such systems when exposed to eavesdroppers. The authors in [28] considered a massive MIMO amplify-and-forward (AF) relay system where the relay is equipped with low-resolution ADCs but infinite-resolution DACs. The achievable secrecy rate and the secrecy energy efficiency were analyzed. A similar scenario was considered in [29] but with an injected null-space artificial noise (AN) for secrecy improvement. Different from the above two works, the work in [30] assumed low-resolution DACs. By studying the ergodic secrecy rate, it was found in [30] that the quantization noise of low-resolution DACs can be regarded as another form of AN, which may enhance the secrecy rate in some scenarios.

Inspired by the above considerations, in this paper, we study the secrecy performance[1] of a downlink massive MIMO system where the BS is equipped with low-resolution ADCs/DACs. Different from [28]–[30], we study the impact of the coarse quantization of both ADCs and DACs. More importantly, the eavesdroppers in our work are assumed to be able to launch PSA to facilitate eavesdropping, which has not been addressed in [28]–[30]. With PSA, it is important to study both the impact of low-resolution DACs and the impact of low-resolution ADCs. Due to PSA, the estimated channel at the BS includes both the channel for the intended user and that for the eavesdropper. Increasing the quantization bits of ADCs not only improves the estimation accuracy for the intended user's channel but also for the eavesdropper's channel. Consequently, it is unclear whether increasing the resolution of ADCs is beneficial for secrecy improvement or not. Moreover, the BS can employ some PSA detection methods to discover the existence of PSA. It is

[1]The secrecy performance considered in this paper mainly includes the ergodic secrecy rate and the maximum tolerable PSA power. The energy efficiency [25], [26], which is specified as secrecy energy efficiency [28], [29] in the context of PLS-based secure communications, is beyond the scope of this paper and left for our future work.

obvious that ADCs with different quantization bits lead to different PSA detection performances. As for DACs, due to the existence of PSA, the impact of low-resolution DACs is related to the knowledge of the PSA power, i.e., the eavesdropper's pilot transmit power. More detailed analyses are given in the following sections. We now summarize our major contributions as below.

1) We consider a time-division-duplex (TDD) massive MIMO system where the BS is equipped with low-resolution ADCs and low-resolution DACs. The BS performs channel estimation in the presence of PSA, based on which the matched filter (MF) precoding and random AN are exploited for downlink transmission. By using the additive quantization noise model (AQNM) as in [19]–[29], we derive the ergodic secrecy rate for the system. Then, the maximum tolerable PSA power is derived, which is the PSA power that reduces the secrecy rate to zero. The optimal power allocation parameter is also derived, which however needs the knowledge of the PSA power.
2) The impact of low-resolution ADCs and low-resolution DACs on the secrecy performance is studied for the following two scenarios: the scenario where the BS knows the PSA power; the scenario where the PSA power is unknown to the BS. It is found that for both the two scenarios, enhancing the number of quantization bits of ADCs is useful for secrecy improvement.
3) The impact of low-resolution DACs depends on the knowledge of the PSA power. For the scenario without the PSA power, the optimal power allocation parameter is unavailable. In this case, when the power allocated to AN is sufficient, high-resolution DACs achieve larger secrecy rate than low-resolution DACs. In contrast, when the power allocated to AN is small, low-resolution DACs are better. For the scenario with the PSA power, the BS can exploit the optimal power allocation parameter. With the optimal power allocation, it is found that the same ergodic secrecy rate can be achieved for DACs with different quantization bits. Only in the case with a small PSA power, high-resolution DACs are preferred.
4) A PSA detection method is proposed based on the energy of the received signal. The impact of ADCs' resolution on the detection performance is studied. It is found that given a predetermined false alarm probability, the resolution of ADCs has little impact on the successful detection probability of PSA.

The outline of this paper is given as follows. Section II introduces the system model including system topology, quantization model, channel estimation, and downlink transmission. Section III evaluates the secrecy performance from the perspective of ergodic secrecy rate as well as maximum tolerable PSA power. The optimization of power allocation is also studied in Section III. Then, the impact of ADCs' and DACs' resolution is studied in Section IV. Section V proposes a PSA detection method and evaluates the impact of low-resolution ADCs on the detection performance. Numerical results are presented in Section VI to verify our analytical results. Finally, the paper concludes with Section VII.

Notations: In this paper, we use bold lower-case and bold upper-case letters to denote vectors and matrices, respectively. $(\cdot)^T$, $(\cdot)^*$, and $(\cdot)^H$ represent the transpose, conjugate, and conjugate transpose of a matrix or vector, respectively. For a square matrix $\mathbf{A}$, we use $\mathbf{A}^{-1}$ to denote the inverse of $\mathbf{A}$. The $N \times N$ identity matrix is denoted as $\mathbf{I}_N$. $\mathbf{x} \in \mathbb{C}^{N\times 1}$ means that $\mathbf{x}$ is a $N \times 1$ complex-valued vector. Finally, $\mathcal{CN}(\mathbf{0}, \Omega)$ represents the circular symmetric complex Gaussian distribution with mean zero and covariance Ω.

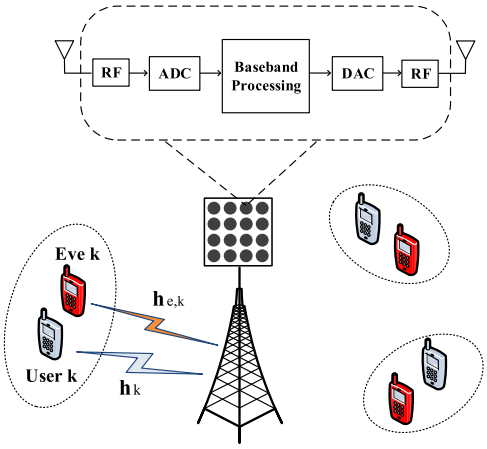


FIGURE 1. System model: Downlink massive MIMO system exposed to active eavesdroppers.

II. SYSTEM MODEL

A. SYSTEM DESCRIPTION

We consider a downlink massive MIMO system where the N_t-antenna BS transmits confidential messages to K single-antenna intended users, as illustrated in Fig. 1. Meantime, there are also K single-antenna active eavesdroppers Eves who can transmit to help eavesdrop the confidential messages. Similar to [17], we assume that each user is eavesdropped by a single Eve, i.e., the kth user is eavesdropped by the kth Eve, which is typical enough for studying the threat of PSA attack. The massive MIMO system works in the TDD mode, where the channel reciprocity holds. The wireless channel between the BS and the kth user is denoted as $\mathbf{h}_k \in \mathbb{C}^{N_t\times 1}$ while the wireless channel between the BS and the kth Eve is denoted as $\mathbf{h}_{e,k} \in \mathbb{C}^{N_t\times 1}$. As discussed in Section I, the active eavesdropper can launch jamming attack or PSA. In this paper, we only consider PSA, since the Eves in this paper are assumed to work in half-duplex mode. Therefore, they cannot eavesdrop the downlink transmission if they perform jamming at the same time.

B. QUANTIZATION MODEL

In general, it is difficult to accurately characterize the effect of quantization since the quantization operation is nonlinear.

Fortunately, the AQNM has been proposed for efficiently evaluating the performance of a quantized system, and has been widely adopted in quantized massive MIMO systems [19]–[29]. With AQNM, the signal after quantization can be approximated as the sum of two uncorrelated terms

$$\mathbf{y} = \mathcal{Q}(\widetilde{\mathbf{y}}) = \alpha\widetilde{\mathbf{y}} + \mathbf{q}, \tag{1}$$

where $\mathcal{Q}(\cdot)$ denotes the quantization operation, $\widetilde{\mathbf{y}}$ and $\mathbf{y}$ are the input and the output of the quantizer, respectively. In addition, $\mathbf{q}$ is the additive Gaussian quantization noise which is uncorrelated with $\widetilde{\mathbf{y}}$. According to [22], the covariance of $\mathbf{q}$ is given by

$$\mathbf{C}_{\mathbf{qq}} = \alpha(1-\alpha)\text{diag}\left(\mathbb{E}\left\{\widetilde{\mathbf{y}}\widetilde{\mathbf{y}}^H\right\}\right). \tag{2}$$

The parameter α is the linear gain, the value of which depends on the quantization bits b of the quantizer. The typical values of α are given in Table 1 [22]. For $b > 5$, the value of α is $\alpha = 1 - \frac{\sqrt{3}\pi}{2}2^{-2b}$ [31]. We can see that the value of α is smaller than 1, which characterizes the attenuation of the signal due to quantization.

TABLE 1. Values of α for different quantization bits b.

b	1	2	3	4	5
α	0.6366	0.8825	0.96546	0.990503	0.997501

C. CHANNEL ESTIMATION

Before downlink transmission, the BS needs to acquire the instantaneous CSI for downlink precoder design. In TDD communications systems, the channel between the BS and intended users can be estimated through uplink channel training due to channel reciprocity. To avoid pilot contamination, τ-length ($\tau \geq K$) orthogonal pilot sequences are exploited. Specifically, the pilot sequence of user k, which is denoted as $\boldsymbol{\varphi}_k$, is designed as the kth column of the unnormalized $\tau \times \tau$ discrete Fourier transform (DFT) matrix with $\boldsymbol{\varphi}_k^H\boldsymbol{\varphi}_k = \tau$ and $\boldsymbol{\varphi}_k^H\boldsymbol{\varphi}_i = 0$ for $\forall i \neq k$. Since the pilot sequences are usually publicly known, after being synchronized with the BS, the kth Eve can send the identical pilot sequence with user k to make the BS beamform the confidential message of user k towards herself. Thus, the received pilot signal at the BS is given by

$$\widetilde{\mathbf{Y}}_p = \sqrt{P_p}\sum_{k=1}^{K}\mathbf{h}_k\boldsymbol{\varphi}_k^T + \sqrt{P_e}\sum_{k=1}^{K}\mathbf{h}_{e,k}\boldsymbol{\varphi}_k^T + \mathbf{N}_p, \tag{3}$$

where P_p is the pilot transmit power of intended users; P_e represents the PSA power, which is the pilot transmit power for Eves; $\mathbf{N}_p \in \mathbb{C}^{N_t\times\tau}$ is the receiver noise at the BS with independent and identically distributed (i.i.d.) $\mathcal{CN}(0, 1)$ element. To gain some simple but insightful results, we adopt a simplified channel model as in [10], [30] where the entries of $\mathbf{h}_k$ and $\mathbf{h}_{e,k}, k = 1, \ldots, K$, are modeled as i.i.d. complex-valued Gaussian variables with mean zero and unit variance.[2] With this model, the strength of the PSA is mainly determined by the value of P_e compared with P_p.

As shown in Fig. 1, the received signal $\widetilde{\mathbf{Y}}_p$ needs to be quantized by the ADC before being further processed for channel estimation. With the aid of the AQNM in (1), the quantized signal can be expressed as [20], [22]

$$\mathbf{Y}_p = \mathcal{Q}(\widetilde{\mathbf{Y}}_p) = \alpha_{\text{A}}\widetilde{\mathbf{Y}}_p + \mathbf{Q}_p, \tag{4}$$

where α_{A} depends on the number of quantization bits of ADCs, as shown in Table 1. $\mathbf{Q}_p = [\mathbf{q}_{p,1}, \ldots, \mathbf{q}_{p,\tau}]$ is the quantization noise with $\mathbf{q}_{p,t} \sim \mathcal{CN}(\mathbf{0}, \mathbf{C}_{\mathbf{q}_p\mathbf{q}_p})$, $t = 1, \ldots, \tau$. According to [19], [20], the covariance matrix $\mathbf{C}_{\mathbf{q}_p\mathbf{q}_p}$ can be calculated as

$$\mathbf{C}_{\mathbf{q}_p\mathbf{q}_p} = \alpha_{\text{A}}(1-\alpha_{\text{A}})\text{diag}\left(\mathbb{E}\{\widetilde{\mathbf{y}}_{p,t}\widetilde{\mathbf{y}}_{p,t}^H\}\right) = \sigma_{q_p}^2\mathbf{I}_{N_t}, \tag{5}$$

where $\widetilde{\mathbf{y}}_{p,t}$ is the tth column of $\widetilde{\mathbf{Y}}_p$, and

$$\sigma_{q_p}^2 = \alpha_{\text{A}}(1-\alpha_{\text{A}})\left(KP_p + KP_e + 1\right). \tag{6}$$

For estimating the channel between the BS and user k, we project the quantized signal $\mathbf{Y}_p$ onto $\boldsymbol{\varphi}_k^*$ and obtain

$$\begin{aligned}\widehat{\mathbf{y}}_k &= \mathbf{Y}_p\boldsymbol{\varphi}_k^* \\ &= \tau\alpha_{\text{A}}\sqrt{P_p}\mathbf{h}_k + \tau\alpha_{\text{A}}\sqrt{P_e}\mathbf{h}_{e,k} + \alpha_{\text{A}}\mathbf{N}_p\boldsymbol{\varphi}_k^* + \mathbf{Q}_p\boldsymbol{\varphi}_k^*.\end{aligned} \tag{7}$$

Based on $\widehat{\mathbf{y}}_k$, the linear minimum mean squared error (LMMSE) estimate of $\mathbf{h}_k$ is given by [20]

$$\widehat{\mathbf{h}}_k = \mathbf{C}_{\mathbf{yh}}^H\mathbf{C}_{\mathbf{yy}}^{-1}\widehat{\mathbf{y}}_k, \tag{8}$$

where

$$\mathbf{C}_{\mathbf{yh}}^H = \mathbb{E}\left\{\mathbf{h}_k\widehat{\mathbf{y}}_k^H\right\} = \tau\alpha_{\text{A}}\sqrt{P_p}\mathbf{I}_{N_t} \tag{9}$$

and

$$\begin{aligned}\mathbf{C}_{\mathbf{yy}} &= \mathbb{E}\left\{\widehat{\mathbf{y}}_k\widehat{\mathbf{y}}_k^H\right\} \\ &= \left(\tau^2\alpha_{\text{A}}^2P_p + \tau^2\alpha_{\text{A}}^2P_e + \tau\alpha_{\text{A}}^2 + \tau\sigma_{q_p}^2\right)\mathbf{I}_{N_t}.\end{aligned} \tag{10}$$

Note that although the theoretical expression for $\mathbf{C}_{\mathbf{yy}}$ in (10) involves P_e, $\mathbf{C}_{\mathbf{yy}}$ can be obtained empirically by calculating $\mathbb{E}\left\{\widehat{\mathbf{y}}_k\widehat{\mathbf{y}}_k^H\right\}$ based on the observed $\widehat{\mathbf{y}}_k$. From (8)–(10), the estimated channel between the BS and user k can be formulated as

$$\widehat{\mathbf{h}}_k = \xi\tau\alpha_{\text{A}}\sqrt{P_p}\mathbf{h}_k + \xi\tau\alpha_{\text{A}}\sqrt{P_e}\mathbf{h}_{e,k} + \xi\alpha_{\text{A}}\mathbf{N}_p\boldsymbol{\varphi}_k^* + \xi\mathbf{Q}_p\boldsymbol{\varphi}_k^* \tag{11}$$

[2]Similar to many existing studies on massive MIMO [9], [10], [16], [17], [21]–[23], [25], [28]–[30], the independent Rayleigh fading is assumed in this paper, where the correlation among antennas and users is not considered. In real propagation environment, the correlation usually exists due to limited number of scatters, and thus there will be gap between the theoretical result based on the i.i.d. Rayleigh fading and the one based on measured channels. As shown in [32], [33], the gap can be very small in several scenarios for different types of antenna arrays, which implies that the use of i.i.d. Rayleigh fading can provide a theoretical evaluation for the realistic system. Therefore, in this paper we use the i.i.d. Rayleigh fading model for performance analysis. More specific channel models such as the cluster based model in [34] and the corresponding performance difference will be considered in our future work.

with

$$\xi = \frac{\alpha_{\mathrm{A}}\sqrt{P_p}}{\tau\alpha_{\mathrm{A}}^2 P_p + \tau\alpha_{\mathrm{A}}^2 P_e + \alpha_{\mathrm{A}}^2 + \sigma_{q_p}^2}. \tag{12}$$

As indicated in (11), due to the PSA, the estimated channel for user k is contaminated by the eavesdropping link $\mathbf{h}_{e,k}$, which will leak user k's downlink confidential message to Eve k.

From (11), the estimated channel $\widehat{\mathbf{h}}_k$ follows a complex Gaussian distribution with mean zero and covariance given by

$$\mathbf{C}_{\widehat{\mathbf{h}}_k\widehat{\mathbf{h}}_k} = \mathbb{E}\left\{\widehat{\mathbf{h}}_k\widehat{\mathbf{h}}_k^H\right\} = \widehat{\sigma}_0^2\mathbf{I}_{N_t}, \tag{13}$$

where

$$\widehat{\sigma}_0^2 = \frac{\tau\alpha_{\mathrm{A}}^2 P_p}{\tau\alpha_{\mathrm{A}}^2 P_p + \tau\alpha_{\mathrm{A}}^2 P_e + \alpha_{\mathrm{A}}^2 + \sigma_{q_p}^2}. \tag{14}$$

Denoting the channel estimation error for user k as $\Delta\mathbf{h}_k$, we have

$$\mathbf{h}_k = \widehat{\mathbf{h}}_k + \Delta\mathbf{h}_k. \tag{15}$$

Based on the orthogonality property of LMMSE estimation, $\widehat{\mathbf{h}}_k$ and $\Delta\mathbf{h}_k$ are uncorrelated. Moreover, since they are both complex Gaussian distributed, $\widehat{\mathbf{h}}_k$ and $\Delta\mathbf{h}_k$ are independent [20], [22].

D. DOWNLINK TRANSMISSION

With the estimated channel, the BS can design downlink precoders for achieving secure message transmission to each user. Considering that the zero-forcing precoding needs to calculate the inverse of the estimated channel $\widehat{\mathbf{H}} = [\widehat{\mathbf{h}}_1, \ldots, \widehat{\mathbf{h}}_K]$, the computational complexity of which is prohibitively high for massive MIMO with large N_t, we exploit the simpler MF precoding for downlink transmission. To enhance secrecy, AN is injected into the information-bearing signal. Also, for reducing computational complexity, we employ the random AN [13], [30], which is proved to be beneficial for secrecy improvement in massive MIMO although the AN is inevitably leaked to intended users. Thus, the downlink transmit signal before quantization can be formulated as

$$\widetilde{\mathbf{x}} = \gamma_1\sqrt{\theta P_d}\widehat{\mathbf{H}}^*\mathbf{s} + \gamma_2\sqrt{(1-\theta)P_d}\mathbf{W}\mathbf{z}, \tag{16}$$

where $\mathbf{s}$ and $\mathbf{z}$ are the information-bearing symbol vector and AN vector, respectively, where $\mathbb{E}\left\{\mathbf{s}\mathbf{s}^H\right\} = \mathbf{I}_K$ and $\mathbf{z} \sim \mathcal{CN}(\mathbf{0}, \mathbf{I}_{N_t-K})$; $\mathbf{W} = [\mathbf{w}_1, \ldots, \mathbf{w}_{N_t-K}]$ is the AN shaping matrix, where $\mathbf{w}_i$ is randomly generated as $\mathbf{w}_i = \frac{\bar{\mathbf{w}}_i}{\|\bar{\mathbf{w}}_i\|}$ with $\bar{\mathbf{w}}_i \sim \mathcal{CN}(\mathbf{0}, \mathbf{I}_{N_t})$; P_d denotes the average downlink transmit power at the BS, and $\theta \in [0, 1]$ represents the power allocation between the information-bearing signal and AN. To satisfy the average power constraint at the BS, the constant amplification factors γ_1 and γ_2 are given by

$$\gamma_1 = \frac{1}{\sqrt{\mathbb{E}\{\|\widehat{\mathbf{H}}^*\mathbf{s}\|^2\}}} = \frac{1}{\sqrt{KN_t\widehat{\sigma}_0^2}}, \tag{17a}$$

$$\gamma_2 = \frac{1}{\sqrt{\mathbb{E}\{\|\mathbf{W}\mathbf{z}\|^2\}}} = \frac{1}{\sqrt{N_t - K}}. \tag{17b}$$

Note that although the value of γ_1 depends on $\widehat{\sigma}_0^2$ which is related to P_e, $\widehat{\sigma}_0^2$ can be obtained empirically based on the observed covariance of $\widehat{\mathbf{h}}_k$.

Similar to the uplink channel estimation, for the downlink transmission phase, the signal $\widetilde{\mathbf{x}}$ needs to be quantized by DACs before transmission. By using the AQNM in (1), the signal after quantization can be expressed as

$$\mathbf{x} = \mathcal{Q}(\widetilde{\mathbf{x}}) = \alpha_{\mathrm{D}}\widetilde{\mathbf{x}} + \mathbf{q}_d, \tag{18}$$

where α_{D} is determined by the number of quantization bits of DACs, and $\mathbf{q}_d$ is the quantization noise whose covariance matrix is [25], [30]

$$\begin{aligned}&\mathbf{C}_{\mathbf{q}_d\mathbf{q}_d}\\ &= \alpha_{\mathrm{D}}(1-\alpha_{\mathrm{D}})\mathrm{diag}\left(\mathbb{E}\{\widetilde{\mathbf{x}}\widetilde{\mathbf{x}}^H\}\right)\\ &= \alpha_{\mathrm{D}}(1-\alpha_{\mathrm{D}})\mathrm{diag}\Big(\theta P_d\gamma_1^2\widehat{\mathbf{H}}^*\widehat{\mathbf{H}}^T + (1-\theta)P_d\gamma_2^2\mathbf{W}\mathbf{W}^H\Big).\end{aligned} \tag{19}$$

The average power of the quantized signal equals

$$\begin{aligned}&\mathbb{E}\{\|\mathbf{x}\|^2\}\\ &= \mathbb{E}\left\{\mathrm{Tr}(\mathbf{x}\mathbf{x}^H)\right\} = \mathrm{Tr}\Big(\alpha_{\mathrm{D}}^2\mathbb{E}\{\widetilde{\mathbf{x}}\widetilde{\mathbf{x}}^H\} + \mathbf{C}_{\mathbf{q}_d\mathbf{q}_d}\Big)\\ &= \mathrm{Tr}\Big(\alpha_{\mathrm{D}}^2\mathrm{diag}\left(\mathbb{E}\{\widetilde{\mathbf{x}}\widetilde{\mathbf{x}}^H\}\right) + \alpha_{\mathrm{D}}(1-\alpha_{\mathrm{D}})\mathrm{diag}\left(\mathbb{E}\{\widetilde{\mathbf{x}}\widetilde{\mathbf{x}}^H\}\right)\Big)\\ &= \alpha_{\mathrm{D}}\mathbb{E}\left\{\|\widetilde{\mathbf{x}}\|^2\right\} = \alpha_{\mathrm{D}}P_d.\end{aligned} \tag{20}$$

From (20), the average power of the quantized signal scales with α_{D}. To make a fair comparison among DACs with different quantization bits, similar to [21], [25], we introduce a normalization factor $\frac{1}{\sqrt{\alpha_{\mathrm{D}}}}$ and the final transmit signal can be expressed as

$$\mathbf{x}_d = \frac{1}{\sqrt{\alpha_{\mathrm{D}}}}\mathbf{x} = \sqrt{\alpha_{\mathrm{D}}}\widetilde{\mathbf{x}} + \frac{1}{\sqrt{\alpha_{\mathrm{D}}}}\mathbf{q}_d \tag{21}$$

with $\mathbb{E}\{\|\mathbf{x}_d\|^2\} = P_d$.

III. SECRECY PERFORMANCE ANALYSIS

First of all, we focus on the achievable ergodic rates at intended users and Eves, respectively. Accordingly, the ergodic secrecy rate for each user is derived. Then, the maximum tolerable PSA power, which reduces the secrecy rate to zero, is investigated. Finally, the optimal θ which maximizes the ergodic secrecy rate is derived.

A. ERGODIC RATE AT INTENDED USER

With the normalized quantized signal $\mathbf{x}_d$ in (21), the received signal at user k, $k = 1, \ldots, K$, is given by

$$\begin{aligned}\mathbf{r}_k &= \mathbf{h}_k^T\mathbf{x}_d + n_k\\ &= \sqrt{\theta P_d\alpha_{\mathrm{D}}}\gamma_1\mathbf{h}_k^T\widehat{\mathbf{h}}_k^* s_k + \sqrt{\theta P_d\alpha_{\mathrm{D}}}\gamma_1\sum_{i\neq k}^{K}\mathbf{h}_k^T\widehat{\mathbf{h}}_i^* s_i\\ &\quad + \sqrt{(1-\theta)P_d\alpha_{\mathrm{D}}}\gamma_2\mathbf{h}_k^T\mathbf{W}\mathbf{z} + \frac{1}{\sqrt{\alpha_{\mathrm{D}}}}\mathbf{h}_k^T\mathbf{q}_d + n_k,\end{aligned} \tag{22}$$

where $n_k \sim \mathcal{CN}(0,1)$ is the receiver noise. As in [10], the ergodic rate at user k is given by (23) at the bottom of the page. However, it is difficult to obtain an analytically tractable result for the expected value in (23). Therefore, we use the method in [10], [13], [16] to find a tractable lower bound for (23), which will finally provide a lower bound for the ergodic secrecy rate of the system.

Considering that there is no downlink channel training for users to acquire the CSI, as in [10], [13], [16] we assume that the statistical CSI is exploited by each intended user for signal detection. Thus, the received signal at user k can be rewritten as

$$\mathbf{r}_k = \sqrt{\theta P_d \alpha_{\mathrm{D}}}\gamma_1 \mathbb{E}\{\mathbf{h}_k^T \widehat{\mathbf{h}}_k^*\} s_k + \widetilde{n}_k \tag{24}$$

with effective noise $\widetilde{n}_k$ defined as

$$\begin{aligned}\widetilde{n}_k &= \sqrt{\theta P_d \alpha_{\mathrm{D}}}\gamma_1 \left(\mathbf{h}_k^T \widehat{\mathbf{h}}_k^* - \mathbb{E}\{\mathbf{h}_k^T \widehat{\mathbf{h}}_k^*\}\right) s_k \\ &\quad + \sqrt{\theta P_d \alpha_{\mathrm{D}}}\gamma_1 \sum_{i\neq k}^{K} \mathbf{h}_k^T \widehat{\mathbf{h}}_i^* s_i + \sqrt{(1-\theta) P_d \alpha_{\mathrm{D}}}\gamma_2 \mathbf{h}_k^T \mathbf{W}\mathbf{z} \\ &\quad + \frac{1}{\sqrt{\alpha_{\mathrm{D}}}} \mathbf{h}_k^T \mathbf{q}_d + n_k. \end{aligned} \tag{25}$$

Note that the effective noise is uncorrelated with the desired signal. Considering that the worst uncorrelated additive noise is Gaussian distributed, the ergodic rate of user k, which is given in (23), can be finally lower bounded by [10], [13], [16]

$$R_k = \log_2\left(1 + \mathrm{SINR}_k\right) \tag{26}$$

with

$$\mathrm{SINR}_k = \frac{A_k}{B_k + C_k + D_k + E_k + 1}, \tag{27}$$

where

$$A_k = \theta P_d \alpha_{\mathrm{D}} \gamma_1^2 \left|\mathbb{E}\{\mathbf{h}_k^T \widehat{\mathbf{h}}_k^*\}\right|^2, \tag{28a}$$

$$B_k = \theta P_d \alpha_{\mathrm{D}} \gamma_1^2 \mathrm{Var}\left(\mathbf{h}_k^T \widehat{\mathbf{h}}_k^*\right), \tag{28b}$$

$$C_k = \theta P_d \alpha_{\mathrm{D}} \gamma_1^2 \sum_{i\neq k}^{K} \mathbb{E}\left\{|\mathbf{h}_k^T \widehat{\mathbf{h}}_i^*|^2\right\}, \tag{28c}$$

$$D_k = (1-\theta) P_d \alpha_{\mathrm{D}} \gamma_2^2 \mathbb{E}\left\{\mathbf{h}_k^T \mathbf{W}\mathbf{W}^H \mathbf{h}_k^*\right\}, \tag{28d}$$

$$E_k = \frac{1}{\alpha_{\mathrm{D}}} \mathbb{E}\left\{\mathbf{h}_k^T \mathbf{C}_{\mathbf{q}_d \mathbf{q}_d} \mathbf{h}_k^*\right\}. \tag{28e}$$

The tightness of the lower bound R_k in (26) will be evaluated in Section VI.

By calculating the expectations and the variance in (28a)–(28e), for $N_t \to \infty$, the achievable ergodic rate of each user converges to

$$R_k \xrightarrow{N_t \to \infty} R_{\mathrm{u}}^{\infty} = \log_2\left(1 + \frac{\theta P_d \alpha_{\mathrm{D}} N_t \widehat{\sigma}_0^2}{K P_d + K}\right), \tag{29}$$

where $\widehat{\sigma}_0^2$ has been given in (14). The derivation of (29) is summarized in Appendix A. From (29), one can observe that R_{u}^{∞} increases as θ increases, which is expected since the power of the information-bearing signal improves. Moreover, R_{u}^{∞} decreases with the increase of P_e, since $\widehat{\sigma}_0^2$ is a monotonic decreasing function of P_e. Therefore, with the increase of the PSA power P_e, the downlink signal beam is more significantly directed to Eve, which causes the leakage of the confidential message.

B. ERGODIC RATE AT EVE

Similar to (22), the received signal at Eve k, $k = 1, \ldots, K$, can be written as

$$\begin{aligned}\mathbf{r}_{e,k} &= \mathbf{h}_{e,k}^T \mathbf{x}_d + n_{e,k} \\ &= \sqrt{\theta P_d \alpha_{\mathrm{D}}}\gamma_1 \sum_{k=1}^{K} \mathbf{h}_{e,k}^T \widehat{\mathbf{h}}_k^* s_k + \sqrt{(1-\theta) P_d \alpha_{\mathrm{D}}}\gamma_2 \mathbf{h}_{e,k}^T \mathbf{W}\mathbf{z} \\ &\quad + \frac{1}{\sqrt{\alpha_{\mathrm{D}}}} \mathbf{h}_{e,k}^T \mathbf{q}_d + n_{e,k}, \end{aligned} \tag{30}$$

where $n_{e,k} \sim \mathcal{CN}(0,1)$ is the additive noise at Eve k's receiver. When Eve k tries to detect s_k, we make a pessimistic assumption that the inter-user interference (IUI) has been successfully removed [9], [10], [30], which actually describes a worst-case scenario for secrecy. Thus, the observed signal for Eve k to detect s_k can be rewritten as

$$\begin{aligned}\mathbf{y}_{e,k} &= \sqrt{\theta P_d \alpha_{\mathrm{D}}}\gamma_1 \mathbf{h}_{e,k}^T \widehat{\mathbf{h}}_k^* s_k + \sqrt{(1-\theta) P_d \alpha_{\mathrm{D}}}\gamma_2 \mathbf{h}_{e,k}^T \mathbf{W}\mathbf{z} \\ &\quad + \frac{1}{\sqrt{\alpha_{\mathrm{D}}}} \mathbf{h}_{e,k}^T \mathbf{q}_d + n_{e,k}. \end{aligned} \tag{31}$$

Based on (31), the ergodic rate at Eve k is given by

$$\tilde{R}_{e,k} = \mathbb{E}\left\{\log_2\left(1 + \mathrm{SINR}_{e,k}\right)\right\} \tag{32}$$

with

$$\begin{aligned}&\mathrm{SINR}_{e,k} \\ &= \frac{\theta P_d \alpha_{\mathrm{D}} \gamma_1^2 |\mathbf{h}_{e,k}^T \widehat{\mathbf{h}}_k^*|^2}{(1-\theta) P_d \alpha_{\mathrm{D}} \gamma_2^2 \mathbf{h}_{e,k}^T \mathbf{W}\mathbf{W}^H \mathbf{h}_{e,k}^* + \frac{1}{\alpha_{\mathrm{D}}} \mathbf{h}_{e,k}^T \mathbf{C}_{\mathbf{q}_d \mathbf{q}_d} \mathbf{h}_{e,k}^* + 1}. \end{aligned} \tag{33}$$

However, it is difficult to obtain the exact value of $R_{e,k}$. Here, we adopt a common approximation for massive MIMO, i.e., $\mathbb{E}\left\{\log_2(1 + X/Y)\right\} \approx \log_2(1 + \mathbb{E}\{X\}/\mathbb{E}\{Y\})$, which is

$$\tilde{R}_k = \mathbb{E}\left\{\log_2\left(1 + \frac{\theta P_d \alpha_{\mathrm{D}} \gamma_1^2 |\mathbf{h}_k^T \widehat{\mathbf{h}}_k^*|^2}{\theta P_d \alpha_{\mathrm{D}} \gamma_1^2 \sum_{i\neq k}^{K} |\mathbf{h}_k^T \widehat{\mathbf{h}}_i^*|^2 + (1-\theta) P_d \alpha_{\mathrm{D}} \gamma_2^2 \mathbf{h}_k^T \mathbf{W}\mathbf{W}^H \mathbf{h}_k^* + \frac{1}{\alpha_{\mathrm{D}}} \mathbf{h}_k^T \mathbf{C}_{\mathbf{q}_d \mathbf{q}_d} \mathbf{h}_k^* + 1}\right)\right\} \tag{23}$$

shown to be accurate for large N_t [35], [36]. By using this approximation method, $\tilde{R}_{e,k}$ can be approximated as

$$R_{e,k} = \log_2\left(1 + \frac{A_{e,k}}{B_{e,k} + C_{e,k} + 1}\right), \tag{34}$$

where

$$A_{e,k} = \theta P_d \alpha_{\mathrm{D}} \gamma_{\mathrm{I}}^2 \mathbb{E}\left\{|\mathbf{h}_{e,k}^T \widehat{\mathbf{h}}_k^*|^2\right\}, \tag{35a}$$

$$B_{e,k} = (1-\theta) P_d \alpha_{\mathrm{D}} \gamma_2^2 \mathbb{E}\left\{\mathbf{h}_{e,k}^T \mathbf{W}\mathbf{W}^H \mathbf{h}_{e,k}^*\right\}, \tag{35b}$$

$$C_{e,k} = \frac{1}{\alpha_{\mathrm{D}}} \mathbb{E}\left\{\mathbf{h}_{e,k}^T \mathbf{C}_{\mathbf{q}_d \mathbf{q}_d} \mathbf{h}_{e,k}^*\right\}. \tag{35c}$$

After calculating the above expectations, the approximate ergodic rate at Eve k when $N_t \to \infty$ is given by

$$R_{e,k} \xrightarrow{N_t \to \infty} R_{\mathrm{e}}^{\infty} = \log_2\left(1 + \frac{\theta P_d \alpha_{\mathrm{D}} \gamma_{\mathrm{I}}^2 \lambda_0}{(1-\theta\alpha_{\mathrm{D}}) P_d + 1}\right), \tag{36}$$

where

$$\lambda_0 = \tau \xi^2 \alpha_{\mathrm{A}}^2 N_t [\tau P_p + \tau P_e (N_t + 1) + 1] + \tau \xi^2 N_t \sigma_{q_p}^2. \tag{37}$$

The derivation of (36) is summarized in Appendix B. As shown in (36), R_{e}^{∞} is a monotonically increasing function of θ, which is expected since as θ increases, the power for the information-bearing signal increases while the power for AN decreases. However, the monotonicity of R_{e}^{∞} with respect to P_e cannot be directly obtained from (36). An intuitive conclusion is that R_{e}^{∞} increases as P_e increases. The mathematical proof is given as below.

From (36), the monotonicity of R_{e}^{∞} with respect to P_e depends on the term $\gamma_{\mathrm{I}}^2 \lambda_0$. Recalling (6), (12), (14), (17) and (37), we have

$$\begin{aligned}
\gamma_{\mathrm{I}}^2 \lambda_0 &= \frac{\tau \alpha_{\mathrm{A}}^2}{K}\left[\tau P_p + \tau P_e (N_t + 1) + 1\right] \frac{\xi^2}{\widehat{\sigma}_0^2} + \frac{\tau \sigma_{q_p}^2}{K} \frac{\xi^2}{\widehat{\sigma}_0^2} \\
&= \frac{\tau \alpha_{\mathrm{A}}^2 P_p + \tau \alpha_{\mathrm{A}}^2 P_e (N_t + 1) + \alpha_{\mathrm{A}}^2 + \sigma_{q_p}^2}{K(\tau \alpha_{\mathrm{A}}^2 P_p + \tau \alpha_{\mathrm{A}}^2 P_e + \alpha_{\mathrm{A}}^2 + \sigma_{q_p}^2)} \\
&= \frac{1}{K} + \frac{\tau \alpha_{\mathrm{A}}^2 N_t P_e}{K(\tau \alpha_{\mathrm{A}}^2 P_p + \tau \alpha_{\mathrm{A}}^2 P_e + \alpha_{\mathrm{A}}^2 + \sigma_{q_p}^2)} \\
&= \frac{1}{K} + \frac{1}{K} \frac{\tau \alpha_{\mathrm{A}} N_t P_e}{\alpha_{\mathrm{A}}(\tau - K)(P_p + P_e) + K P_p + K P_e + 1}.
\end{aligned} \tag{38}$$

It can be easily observed from (38) that $\gamma_{\mathrm{I}}^2 \lambda_0$ is a monotonically increasing function of P_e. Consequently, R_{e}^{∞} is a monotonically increasing function of P_e.

C. ERGODIC SECRECY RATE

Based on (26) and (34), the ergodic secrecy rate for each user is defined as [9], [10], [13]

$$R_{\mathrm{sec},k} = [R_k - R_{e,k}]^+, \tag{39}$$

where $[x]^+ = \max(x, 0)$. With the aid of (29) and (36), a tractable approximation of $R_{\mathrm{sec},k}$ when $N_t \to \infty$ is given by

$$R_{\mathrm{sec},k} \xrightarrow{N_t \to \infty} R_{\mathrm{sec}}^{\infty} = [R_{\mathrm{u}}^{\infty} - R_{\mathrm{e}}^{\infty}]^+. \tag{40}$$

The accuracy of $R_{\mathrm{sec}}^{\infty}$ will be evaluated in Section VI. In the following sections, we use $R_{\mathrm{sec}}^{\infty}$ to analyze the secrecy performance as well as the impact of low-resolution ADCs and DACs.

Remark 1: As discussed in [9], [10], the secrecy rate in (39) *is actually a lower bound of the ergodic secrecy rate in fading channels [4], which is a widely-adopted metric for evaluating the secrecy performance of a system. According to [4], to achieve this ergodic secrecy rate, the eavesdropper's CSI is not needed while the PSA power P_e is required. When the eavesdroppers are registered users in the network, the PSA power can be obtained through the periodic interchange between the registered users and the BS. In this case, the PSA is usually referred to as pilot contamination [20]. When the eavesdroppers are external devices, we first use the PSA detector proposed in Section V to identify the cases that PSA occurs. Based on the identified cases, the value of $\sigma_{\mathcal{H}_1}^2$ in* (69) *can be obtained empirically. Then, the value of the PSA power P_e can be estimated using the method in [14, Appendix A].*

D. MAXIMUM TOLERABLE PSA POWER

In this section, we study the PSA power that makes the secrecy rate $R_{\mathrm{sec}}^{\infty}$ equal to zero. As discussed in Sections III-A and III-B, with the increase of P_e, R_{u}^{∞} decreases while R_{e}^{∞} increases. Therefore, the ergodic secrecy rate $R_{\mathrm{sec}}^{\infty}$ decreases as P_e increases, which indicates that when P_e increases from 0 to ∞, there is a critical point $P_e^{\max}$ which reduces $R_{\mathrm{sec}}^{\infty}$ to zero. The value of $P_e^{\max}$ is defined as the maximum tolerable PSA power.

According to (40), $P_e^{\max}$ is the root of $R_{\mathrm{u}}^{\infty} - R_{\mathrm{e}}^{\infty} = 0$, which is equivalent to

$$\frac{\theta P_d \alpha_{\mathrm{D}} N_t \widehat{\sigma}_0^2}{K P_d + K} - \frac{\theta P_d \alpha_{\mathrm{D}} \gamma_{\mathrm{I}}^2 \lambda_0}{(1-\theta\alpha_{\mathrm{D}}) P_d + 1} = 0. \tag{41}$$

Plugging (14) and (38) into (41), the maximum tolerable PSA power $P_e^{\max}$ can be obtained, which is given in (42) at the bottom of the next page. It is worth noting that the derived $P_e^{\max}$ in (42) does not apply to the case $\theta = 0$. Actually, when $\theta = 0$ the secrecy rate is always zero, regardless of the value of P_e.

E. OPTIMIZATION OF θ

With the derived ergodic secrecy rate in (40), we can optimize θ to maximize $R_{\mathrm{sec}}^{\infty}$. Assuming a positive secrecy rate and plugging (29) and (36) into (40), we have

$$R_{\mathrm{sec}}^{\infty} = \log_2\left(\frac{1}{K P_d + K} f(\theta, \alpha_{\mathrm{D}})\right), \tag{43}$$

where

$$f(\theta, \alpha_{\mathrm{D}}) = \frac{-a_1 \alpha_{\mathrm{D}}^2 \theta^2 + b_1 \alpha_{\mathrm{D}} \theta + c_1}{a_2 \alpha_{\mathrm{D}} \theta + c_2} \tag{44}$$

with $a_1 = P_d^2 N_t \widehat{\sigma}_0^2$, $b_1 = P_d(P_d + 1)(N_t \widehat{\sigma}_0^2 - K)$, $c_1 = K(P_d + 1)^2$, $a_2 = P_d(\gamma_{\mathrm{I}}^2 \lambda_0 - 1)$, and $c_2 = P_d + 1$. Thus, the monotonicity of $R_{\mathrm{sec}}^{\infty}$ with respect to θ is determined

by $f(\theta, \alpha_{\mathrm{D}})$. The derivative of $f(\theta, \alpha_{\mathrm{D}})$ with respect to θ is given by

$$\frac{\partial f(\theta, \alpha_{\mathrm{D}})}{\partial \theta} = \frac{-a_1 a_2 \alpha_{\mathrm{D}}^3 \theta^2 - 2a_1 c_2 \alpha_{\mathrm{D}}^2 \theta + (b_1 c_2 - a_2 c_1)\alpha_{\mathrm{D}}}{(a_2 \alpha_{\mathrm{D}} \theta + c_2)^2}. \tag{45}$$

By forcing $\frac{\partial f(\theta,\alpha_{\mathrm{D}})}{\partial \theta} = 0$, we can find a local maximum point of $f(\theta, \alpha_{\mathrm{D}})$, which is given by

$$\theta^* = \frac{a_1 c_2 - \sqrt{a_1^2 c_2^2 + a_1 a_2 (b_1 c_2 - a_2 c_1)}}{-a_1 a_2 \alpha_{\mathrm{D}}}. \tag{46}$$

Note that θ^* exists only when $a_1^2 c_2^2 + a_1 a_2 (b_1 c_2 - a_2 c_1) > 0$; otherwise, $f(\theta, \alpha_{\mathrm{D}})$ is a monotonically increasing or decreasing function of θ, which indicates that the maximum $f(\theta, \alpha_{\mathrm{D}})$ is achieved at $\theta = 1$ or $\theta = 0$. Therefore, the optimal power allocation parameter θ_{opt} which maximizes $R_{\mathrm{sec}}^{\infty}$ belongs to

$$\theta_{\mathrm{opt}} \in \{0, 1, \theta^*\}. \tag{47}$$

When $\theta_{\mathrm{opt}} = 0$, the maximum ergodic secrecy rate is zero. For the case $\theta_{\mathrm{opt}} = 1$, all the power is allocated to the information-bearing signal, which indicates that there is no need to inject AN. Moreover, note that θ^* involves a_2, which is related to λ_0. Recalling the expression for λ_0 in (37), one can see that the availability of θ^* requires the knowledge of the PSA power P_e.

IV. IMPACT OF LOW-RESOLUTION ADCs/DACs

In this section, we study the impact of the quantization bits of ADCs and DACs on the secrecy performance. From Table 1, the impact of the quantization bits of ADCs and DACs can be described by the corresponding parameters α_{A} and α_{D}, respectively. Therefore, in the following sections we investigate the impact of α_{A} and α_{D} on the secrecy performance. Recalling that the optimal power allocation parameter θ_{opt} requires the knowledge of the PSA power P_e, we consider the following two scenarios: the scenario without P_e and the scenario with P_e. The impact of α_{A} and α_{D} is studied for both the two scenarios.

A. THE SCENARIO WITHOUT P_e

When P_e is unavailable, the optimal power allocation parameter is also unavailable. In this case, the value of θ is predetermined and fixed according to certain system requirements. For example, the value of θ may be determined according to the minimum required ergodic rate at intended users or with the assumption that there is no PSA. Therefore, in what follows the impact of α_{A} and α_{D} on the secrecy performance is analyzed for a fixed θ.

1) IMPACT OF ADC PARAMETER α_{A}

When $\theta = 0$, the secrecy rate is always zero. Thus, we only consider the case that $\theta \in (0, 1]$. First, we study the impact of α_{A} on the maximum tolerable PSA power $P_e^{\max}$. Taking the derivative of $P_e^{\max}$ in (42) with respect to α_{A}, we have

$$\frac{\partial P_e^{\max}}{\partial \alpha_{\mathrm{A}}} = \frac{c_0}{\big((P_d+1)(\tau - K + \tau N_t)\alpha_{\mathrm{A}} + K(P_d+1)\big)^2}, \tag{48}$$

where

$$c_0 = (P_d+1)\Big(\tau K N_t P_p\big((1-\theta\alpha_{\mathrm{D}})P_d+1\big)+(\tau-K)(P_d+1) + \tau N_t (P_d+1)(KP_p+1)\Big) > 0. \tag{49}$$

From (48), $P_e^{\max}$ is a monotonically increasing function of α_{A} for any $\theta \neq 0$. Consequently, using high resolution ADCs is beneficial for combating against PSA, since a higher PSA power is needed by Eve to force the secrecy rate to zero.

Then, we focus on the ergodic secrecy rate. Assuming a positive secrecy rate, $R_{\mathrm{sec}}^{\infty}$ in (40) can be reformulated as

$$\begin{aligned} R_{\mathrm{sec}}^{\infty} &= R_{\mathrm{u}}^{\infty} - R_{\mathrm{e}}^{\infty} \\ &= \log_2\left(1 + l_1 \widehat{\sigma}_0^2\right) - \log_2\left(1 + l_2 \widehat{\sigma}_0^2 + l_3\right) \\ &= \log_2\left(f(\widehat{\sigma}_0^2)\right) \end{aligned} \tag{50}$$

with

$$f(\widehat{\sigma}_0^2) = \frac{1 + l_1 \widehat{\sigma}_0^2}{1 + l_2 \widehat{\sigma}_0^2 + l_3}, \tag{51}$$

where

$$l_1 = \frac{\theta P_d \alpha_{\mathrm{D}} N_t}{KP_d + K}, \tag{52a}$$

$$l_2 = \frac{\theta P_d \alpha_{\mathrm{D}}}{(1-\theta\alpha_{\mathrm{D}})P_d + 1} \frac{N_t P_e}{KP_p}, \tag{52b}$$

$$l_3 = \frac{\theta P_d \alpha_{\mathrm{D}}}{K(1-\theta\alpha_{\mathrm{D}})P_d + K}. \tag{52c}$$

$$\begin{aligned} &\frac{\theta P_d \alpha_{\mathrm{D}} N_t \widehat{\sigma}_0^2}{KP_d + K} - \frac{\theta P_d \alpha_{\mathrm{D}} \gamma_1^2 \lambda_0}{(1-\theta\alpha_{\mathrm{D}})P_d + 1} = 0 \\ &\Longrightarrow N_t \widehat{\sigma}_0^2 \big((1-\theta\alpha_{\mathrm{D}})P_d + 1\big) - \gamma_1^2 \lambda_0 K (P_d+1) = 0 \\ &\Longrightarrow \frac{\tau\alpha_{\mathrm{A}} N_t P_p \big((1-\theta\alpha_{\mathrm{D}})P_d + 1\big)}{(\tau-K)\alpha_{\mathrm{A}}(P_p+P_e) + KP_p + KP_e + 1} - (P_d+1)\left(1 + \frac{\tau\alpha_{\mathrm{A}} N_t P_e}{(\tau-K)\alpha_{\mathrm{A}}(P_p+P_e) + KP_p + KP_e + 1}\right) = 0 \\ &\Longrightarrow \tau\alpha_{\mathrm{A}} N_t P_p\big((1-\theta\alpha_{\mathrm{D}})P_d + 1\big) - \tau\alpha_{\mathrm{A}} N_t P_e (P_d+1) - (P_d+1)\big((\tau-K)\alpha_{\mathrm{A}}(P_p+P_e) + KP_p + KP_e + 1\big) = 0 \\ &\Longrightarrow P_e^{\max} = \frac{\tau\alpha_{\mathrm{A}} N_t P_p\big((1-\theta\alpha_{\mathrm{D}})P_d + 1\big) - (P_d+1)\big((\tau-K)\alpha_{\mathrm{A}} P_p + KP_p + 1\big)}{\big((\tau-K)\alpha_{\mathrm{A}} + K + \tau\alpha_{\mathrm{A}} N_t\big)(P_d+1)}. \end{aligned} \tag{42}$$

The first order derivative of $f(\widehat{\sigma}_0^2)$ with respect to $\widehat{\sigma}_0^2$ is given by

$$\frac{\partial f(\widehat{\sigma}_0^2)}{\partial \widehat{\sigma}_0^2} = \frac{l_1 - l_2 + l_1 l_3}{(1 + l_2\widehat{\sigma}_0^2 + l_3)^2}. \tag{53}$$

When $R_{\text{sec}}^{\infty} > 0$, there is $(l_1 - l_2)\widehat{\sigma}_0^2 > l_3$, which indicates that $l_1 > l_2 > 0$, since $l_3 > 0$. Therefore, $\frac{\partial f(\widehat{\sigma}_0^2)}{\partial \widehat{\sigma}_0^2} > 0$ when $R_{\text{sec}}^{\infty} > 0$. Meantime, it can be easily verified that $\frac{\partial \widehat{\sigma}_0^2}{\partial \alpha_{\text{A}}} > 0$. Based on the above discussions and the fact that $\log_2(x)$ is an increasing function of x, we have the conclusion that $\frac{\partial R_{\text{sec}}^{\infty}}{\partial \alpha_{\text{A}}} > 0$ when $R_{\text{sec}}^{\infty} > 0$, which shows that higher-resolution ADCs yield larger ergodic secrecy rate. Note that for the case $R_{\text{sec}}^{\infty} = 0$, a larger α_{A} may help to improve R_{sec}^{∞} from zero to a positive value, since $P_e^{\max}$ increases with the increase of α_{A}.

From the above results, we can see that given a fixed θ, improving the quantization bits of ADC is beneficial for improving both the maximum tolerable PSA power and the ergodic secrecy rate. Although from (50), increasing α_{A} can also increase eavesdropper's achievable rate R_{e}^{∞}, since higher-resolution ADCs yield a more accurate estimated channel, which benefits both the intended user and the eavesdropper. However, once a positive secrecy rate is achieved, enhancing the quantization bits of ADCs is beneficial for secrecy rate improvement.

2) IMPACT OF DAC PARAMETER α_{D}

Now, we study the impact of α_{D}. Similarly, we consider the case that $\theta \neq 0$. Recalling (42), we can see that $P_e^{\max}$ decreases with the increase of α_{D}, which implies that for a fixed θ, enhancing the quantization bits of DACs will reduce the maximum tolerable PSA power. This is because for the same PSA power, the downlink signal beam will be more accurately directed to Eve when the BS is equipped with higher-resolution DACs.

Then, we concentrate on the ergodic secrecy rate R_{sec}^{∞}, the monotonicity of which depends on the function $f(\theta, \alpha_{\text{D}})$ given in (43). According to (43), the derivative of $f(\theta, \alpha_{\text{D}})$ with respect to α_{D} is given by

$$\frac{\partial f(\theta, \alpha_{\text{D}})}{\partial \alpha_{\text{D}}} = \frac{-a_1 a_2 \theta^3 \alpha_{\text{D}}^2 - 2a_1 c_2 \theta^2 \alpha_{\text{D}} + (b_1 c_2 - a_2 c_1)\theta}{(a_2 \theta \alpha_{\text{D}} + c_2)^2}. \tag{54}$$

From (54), the value of $\frac{\partial f(\theta,\alpha_{\text{D}})}{\partial \alpha_{\text{D}}}$ depends on the parameters a_1, a_2, b_1, c_1, c_2, and θ, the definitions of which are the same as those in (44). Thus, it is nontrivial to tell the monotonicity of $f(\theta, \alpha_{\text{D}})$ with respect to α_{D}. In the following, we study several special cases to get some insightful results. Specifically, we consider the following two special cases: 1) $\theta \to 0$ and $P_e = 0$; 2) $\theta = 1$ and $P_e = 0$.

For the case $\theta \to 0$ and $P_e = 0$, combining the fact that $\alpha_{\text{D}} \in (0, 1)$, we can see that whether $\frac{\partial f(\theta,\alpha_{\text{D}})}{\partial \alpha_{\text{D}}} > 0$ or $\frac{\partial f(\theta,\alpha_{\text{D}})}{\partial \alpha_{\text{D}}} < 0$ is mainly determined by the term $b_1 c_2 - a_2 c_1$. When $P_e = 0$, we have that $a_2 = P_d(\frac{1}{K} - 1) < 0$. Besides, for $N_t \gg K$, there is $b_1 > 0$. Recalling the fact that $c_1 > c_2 > 0$, we have $b_1 c_2 - a_2 c_1 > 0$, which yields $\frac{\partial f(\theta,\alpha_{\text{D}})}{\partial \alpha_{\text{D}}} > 0$. Therefore, for the case $\theta \to 0$ and $P_e = 0$, R_{sec}^{∞} increases with the increase of α_{D}.

For the case $\theta = 1$ and $P_e = 0$, the derivative in (54) can be simplified as

$$\frac{\partial f(\theta, \alpha_{\text{D}})}{\partial \alpha_{\text{D}}} = \frac{-a_1 a_2 \alpha_{\text{D}}^2 - 2a_1 c_2 \alpha_{\text{D}} + b_1 c_2 - a_2 c_1}{(a_2 \alpha_{\text{D}} + c_2)^2}. \tag{55}$$

For notational simplicity, we define $g(\alpha_{\text{D}}) = -a_1 a_2 \alpha_{\text{D}}^2 - 2a_1 c_2 \alpha_{\text{D}} + b_1 c_2 - a_2 c_1$. As aforementioned, when $P_e = 0$, there is $a_2 < 0$. Since $a_1 > 0$, we have that $g(\alpha_{\text{D}})$ is convex. The axis of symmetry of the parabola of $g(\alpha_{\text{D}})$ is at $x_{\text{sym}} = -\frac{c_2}{a_2} = \frac{P_d+1}{P_d(\frac{1}{K}-1)} > 1$. Recalling that $b_1 > 0$ generally holds, it can be easily verified that $g(\alpha_{\text{D}})|_{\alpha_{\text{D}}=0} > 0$. However, the value of $g(\alpha_{\text{D}})|_{\alpha_{\text{D}}=1}$ is relevant to P_d. When $P_d \ll 1$, we have

$$\begin{aligned} g(\alpha_{\text{D}})|_{\alpha_{\text{D}}=1} &= -a_1 a_2 - 2a_1 c_2 + b_1 c_2 - a_2 c_1 \\ &\overset{(a)}{=} -P_d^3 N_t \widehat{\sigma}_0^2 \left(\frac{1}{K} - 1\right) - 2P_d^2 N_t \widehat{\sigma}_0^2 (P_d + 1) \\ &\quad + P_d (P_d + 1)^2 (N_t \widehat{\sigma}_0^2 - 1) \\ &\overset{(b)}{\approx} -P_d^3 N_t \widehat{\sigma}_0^2 \left(\frac{1}{K} - 1\right) - 2P_d^2 N_t \widehat{\sigma}_0^2 \\ &\quad + P_d (N_t \widehat{\sigma}_0^2 - 1) \\ &= P_d N_t \widehat{\sigma}_0^2 \left(-\frac{1}{K} P_d^2 + (1 - P_d)^2\right) - P_d \\ &\overset{(c)}{\approx} P_d (N_t \widehat{\sigma}_0^2 - 1), \end{aligned} \tag{56}$$

where (a) is obtained by plugging $P_e = 0$ into (38); steps (b) and (c) are obtained based on $P_d \ll 1$. In general, we have $N_t \widehat{\sigma}_0^2 > 1$. Therefore, $g(\alpha_{\text{D}})|_{\alpha_{\text{D}}=1} > 0$ for $P_d \ll 1$. In contrast, for the case $P_d \gg 1$, we have

$$\begin{aligned} &g(\alpha_{\text{D}})|_{\alpha_{\text{D}}=1} \\ &\quad = -a_1 a_2 - 2a_1 c_2 + b_1 c_2 - a_2 c_1 \\ &\quad = -P_d^3 N_t \widehat{\sigma}_0^2 \left(\frac{1}{K} - 1\right) - 2P_d^2 N_t \widehat{\sigma}_0^2 (P_d + 1) \\ &\qquad + P_d (P_d + 1)^2 (N_t \widehat{\sigma}_0^2 - 1) \\ &\quad \overset{(d)}{\approx} -P_d^3 N_t \widehat{\sigma}_0^2 \left(\frac{1}{K} - 1\right) - 2P_d^3 N_t \widehat{\sigma}_0^2 + P_d^3 (N_t \widehat{\sigma}_0^2 - 1) \\ &\quad = -\frac{1}{K} P_d^3 N_t \widehat{\sigma}_0^2 - P_d^3 < 0, \end{aligned} \tag{57}$$

where step (d) is from $P_d \gg 1$. By using the convexity of $g(\alpha_{\text{D}})$, the axis of symmetry $x_{\text{sym}} > 1$, and the values of $g(\alpha_{\text{D}})|_{\alpha_{\text{D}}=0}$ and $g(\alpha_{\text{D}})|_{\alpha_{\text{D}}=1}$, when $P_d \ll 1$, we have $g(\alpha_{\text{D}}) > 0$, $\forall \alpha_{\text{D}} \in (0, 1)$, which indicates that R_{sec}^{∞} is an increasing function of α_{D}. However, for the case $P_d \gg 1$, there exists a point α_{D}^*. When $\alpha_{\text{D}} < \alpha_{\text{D}}^*$, $g(\alpha_{\text{D}}) > 0$; while when $\alpha_{\text{D}} > \alpha_{\text{D}}^*$, $g(\alpha_{\text{D}}) < 0$. Consequently, as α_{D} increases, R_{sec}^{∞} first increases and then decreases.

Based on the above discussions, we can see that different from the case for ADCs, increasing the resolution of

DACs cannot always guarantee an improvement in secrecy performance. However, if the power allocation parameter θ can adjust according to the PSA power P_e, the conclusion is different, which will be discussed in the following sections.

B. THE SCENARIO WITH P_e

When the PSA power P_e is known by the BS, the optimal power allocation parameter θ_{opt} in (47) can be exploited. With θ_{opt}, we then study the impact of α_{A} and α_{D} on the secrecy performance in terms of maximum tolerable PSA power and ergodic secrecy rate.

1) IMPACT OF ADC PARAMETER α_{A}

We first focus on the maximum tolerable PSA power. Different from the analysis in Section IV-A1, the derivative in (48) is not applicable to the case with θ_{opt}, since θ_{opt} is a function of both α_{A} and P_e. Note that θ_{opt} corresponds to the optimal power allocation parameter which maximize R_{sec}^{∞}. Therefore, if $\theta_{\text{opt}} \to 0$, the maximum achievable ergodic secrecy rate will tend to zero. Based on the definition that $P_e^{\max}$ is the PSA power which reduces R_{sec}^{∞} to zero, the maximum tolerable PSA power when θ can adapt to P_e is given by

$$\begin{aligned} P_{e,\text{opt}}^{\max} &= P_e^{\max}|_{\theta\to 0} \\ &\overset{(e)}{=} \frac{\tau\alpha_{\text{A}}N_tP_p - (\tau-K)\alpha_{\text{A}}P_p - KP_p - 1}{(\tau-K)\alpha_{\text{A}} + K + \tau\alpha_{\text{A}}N_t}, \end{aligned} \tag{58}$$

where step (e) is obtained by plugging $\theta \to 0$ into (42). Note that $P_{e,\text{opt}}^{\max} \geq P_e^{\max}$, since when P_e is available, the BS can adjust θ to maximize $P_e^{\max}$. It is straightforward to obtain that $\frac{\partial P_{e,\text{opt}}^{\max}}{\partial \alpha_{\text{A}}} > 0$. Therefore, when P_e is available, increasing the resolution of ADCs is still useful for improving the maximum tolerable PSA power.

As for the ergodic secrecy rate, the conclusion based on the derivative in (53) is inapplicable, since θ_{opt} is also a function of $\widehat{\sigma}_0^2$. The following proposition summarizes the effect of α_{A} on the ergodic secrecy rate with θ_{opt}. In the proposition below, for any ADC parameter $\alpha_{\text{A},i}$, $\theta_{\text{opt},i}$ denotes the optimal power allocation parameter corresponding to $\alpha_{\text{A},i}$, and $R_{\text{sec}}^{\infty}(\theta_{\text{opt},i}, \alpha_{\text{A},i})$ denotes the value of R_{sec}^{∞} with $\theta = \theta_{\text{opt},i}$ and $\alpha_{\text{A}} = \alpha_{\text{A},i}$.

Proposition 1: For two ADC parameters $0 < \alpha_{\text{A},1} < \alpha_{\text{A},2} < 1$, *we have*

$$R_{\text{sec}}^{\infty}(\theta_{\text{opt},1}, \alpha_{\text{A},1}) \leq R_{\text{sec}}^{\infty}(\theta_{\text{opt},2}, \alpha_{\text{A},2}). \tag{59}$$

The equality in (59) *holds when* $R_{\text{sec}}^{\infty}(\theta_{\text{opt},1}, \alpha_{\text{A},1}) = R_{\text{sec}}^{\infty}(\theta_{\text{opt},2}, \alpha_{\text{A},2}) = 0$.

Proof: According to the results in Section IV-A1, for a fixed θ, increasing α_{A} helps to increase the ergodic secrecy rate. Thus, we have $R_{\text{sec}}^{\infty}(\theta_{\text{opt},1}, \alpha_{\text{A},1}) \leq R_{\text{sec}}^{\infty}(\theta_{\text{opt},1}, \alpha_{\text{A},2})$, where the equality holds when both the two terms equal to zero. Besides, since $\theta_{\text{opt},2}$ maximizes the ergodic secrecy rate for $\alpha_{\text{A},2}$, we have $R_{\text{sec}}^{\infty}(\theta_{\text{opt},1}, \alpha_{\text{A},2}) \leq R_{\text{sec}}^{\infty}(\theta_{\text{opt},2}, \alpha_{\text{A},2})$, where the equality holds when $R_{\text{sec}}^{\infty}(\theta_{\text{opt},2}, \alpha_{\text{A},2}) = 0$. Combining the above results, we finally have $R_{\text{sec}}^{\infty}(\theta_{\text{opt},1}, \alpha_{\text{A},1}) \leq R_{\text{sec}}^{\infty}(\theta_{\text{opt},2}, \alpha_{\text{A},2})$, which completes the proof. □

Based on the above discussions, we can see that when the PSA power is available, high-resolution ADCs are preferred compared with low-resolution ADCs, in terms of maximum tolerable PSA power and ergodic secrecy rate.

2) IMPACT OF DAC PARAMETER α_{D}

Based on the discussion in Section IV-B1, when P_e is known by the BS, the maximum tolerable PSA power is $P_{e,\text{opt}}^{\max}$ in (58). From (58), we can see that $P_{e,\text{opt}}^{\max}$ is independent of α_{D}. Therefore, for the case with P_e, DACs with different quantization bits can guarantee the same maximum tolerable PSA power.

Now, we study the ergodic secrecy rate. According to (47), the value of θ_{opt} can be 0, 1, or θ^*. Therefore, the impact of α_{D} on the ergodic secrecy rate with θ_{opt} is studied by the following three propositions. In the propositions below, for any DAC parameter $\alpha_{\text{D},i}$, $\theta_{\text{opt},i}$ denotes the optimal power allocation parameter corresponding to $\alpha_{\text{D},i}$, and $R_{\text{sec}}^{\infty}(\theta_{\text{opt},i}, \alpha_{\text{D},i})$ denotes the value of R_{sec}^{∞} with $\theta = \theta_{\text{opt},i}$ and $\alpha_{\text{D}} = \alpha_{\text{D},i}$.

Proposition 2: For any two different DAC parameters $\alpha_{\text{D},i}$ *and* $\alpha_{\text{D},j}$, *once* $\theta_{\text{opt},i} = 0$, *we have*

$$\theta_{\text{opt},j} = \theta_{\text{opt},i} = 0, \tag{60a}$$

$$R_{\text{sec}}^{\infty}(\theta_{\text{opt},j}, \alpha_{\text{D},j}) = R_{\text{sec}}^{\infty}(\theta_{\text{opt},i}, \alpha_{\text{D},i}) = 0. \tag{60b}$$

Proof: Since $\theta_{\text{opt},i} = 0$, we can know that the PSA power P_e is already larger than $P_{e,\text{opt}}^{\max}$. From (58), $P_{e,\text{opt}}^{\max}$ is independent of α_{D}, which implies that changing α_{D} cannot improve $P_{e,\text{opt}}^{\max}$. Therefore, when $P_e \geq P_{e,\text{opt}}^{\max}$, the maximum ergodic secrecy rate for any α_{D} is zero. The corresponding optimal power allocation parameter for any α_{D} is also zero. □

Proposition 3: For any two different DAC parameters $\alpha_{\text{D},i}$ *and* $\alpha_{\text{D},j}$, *if* $\theta_{\text{opt},i} \in (0, 1)$ *and* $\theta_{\text{opt},j} \in (0, 1)$, *we have*

$$R_{\text{sec}}^{\infty}(\theta_{\text{opt},i}, \alpha_{\text{D},i}) = R_{\text{sec}}^{\infty}(\theta_{\text{opt},j}, \alpha_{\text{D},j}) = \Pi_c, \tag{61}$$

where

$$\Pi_c = \log_2\left(\frac{1}{KP_d + K}\frac{-a_1\Lambda^2 + b_1\Lambda + c_1}{a_2\Lambda + c_2}\right) \tag{62}$$

with $\Lambda = \frac{a_1c_2 - \sqrt{a_1^2c_2^2 + a_1a_2(b_1c_2 - a_2c_1)}}{-a_1a_2}$. *The definitions of* a_1, a_2, b_1, c_1, *and* c_2 *are the same as those in* (44).

Proof: According to (47), when $\theta_{\text{opt}} \in (0, 1)$ we have $\theta_{\text{opt}} = \theta^*$. Plugging the expression for θ^* in (46) into (43), the conclusion in Proposition 3 can be proved.[3] □

Before giving Proposition 4, we first introduce the following lemma, which is needed by the proof of Proposition 4.

Lemma 1: For two DAC parameters $0 < \alpha_{\text{D},1} < \alpha_{\text{D},2} < 1$, *if* $\theta_{\text{opt},2} = 1$, *we have*

$$\theta_{\text{opt},1} = 1, \quad \text{and} \quad R_{\text{sec}}^{\infty}(\theta_{\text{opt},1}, \alpha_{\text{D},1}) < R_{\text{sec}}^{\infty}(\theta_{\text{opt},2}, \alpha_{\text{D},2}). \tag{63}$$

[3] Note that a similar result was found in [30] that DACs with different quantization bits can achieve the same ergodic secrecy rate with the optimal power allocation parameters. However, the result in [30] was obtained numerically while we in this paper provide a theoretical explanation for this phenomenon. Moreover, we study the scenario with PSA and channel estimation error, while the work in [30] assumed perfect CSI without the threat of PSA.

Proof: Recalling (43)-(45), we can see that the monotonicity of R_{sec}^{∞} with respect to θ is totally determined by the function $g_{\alpha_{\text{D}}}(\theta) \triangleq -a_1a_2\alpha_{\text{D}}^2\theta^2 - 2a_1c_2\alpha_{\text{D}}\theta + b_1c_2 - a_2c_1$, which is a quadratic function of $\theta \in [0, 1]$ with a given α_{D}. In the following analysis, we consider a relaxed range of values where $\theta \in (-\infty, +\infty)$. When $a_2 > 0$, $g_{\alpha_{\text{D}}}(\theta)$ is concave. The axis of symmetry of the parabola of $g_{\alpha_{\text{D}}}(\theta)$ is at $x = -\frac{c_2}{a_2\alpha_{\text{D}}} < 0$. In contrast, when $a_2 < 0$, $g_{\alpha_{\text{D}}}(\theta)$ is convex, and the axis of symmetry of the parabola of $g_{\alpha_{\text{D}}}(\theta)$ is at $x = -\frac{c_2}{a_2\alpha_{\text{D}}} = \frac{P_d+1}{P_d(1-\gamma_1^2\lambda_0)\alpha_{\text{D}}} > 1$. Therefore, for any a_2, when θ increases from 0 to 1, R_{sec}^{∞} can only monotonically increase, monotonically decrease, or first increase and then decrease.

Based on the above discussions, when $\theta_{\text{opt},2} = 1$, we can conclude that R_{sec}^{∞} is a monotonically increasing function of $\theta \in [0, 1]$, which indicates that $g_{\alpha_{\text{D},2}}(\theta) > 0$ for $\theta \in [0, 1]$. Introduce the variable $\tilde{\theta} = \frac{\alpha_{\text{D},1}}{\alpha_{\text{D},2}}\theta$ with $\theta \in [0, 1]$. Due to the fact that $\tilde{\theta} \in [0, 1)$, we have

$$\begin{aligned}
&g_{\alpha_{\text{D},2}}(\tilde{\theta}) > 0,\ \tilde{\theta} \in [0, 1) \\
&\Longleftrightarrow g_{\alpha_{\text{D},2}}(\frac{\alpha_{\text{D},1}}{\alpha_{\text{D},2}}\theta) > 0,\ \theta \in [0, 1] \\
&\Longleftrightarrow -a_1a_2\alpha_{\text{D},1}^2\theta^2 - 2a_1c_2\alpha_{\text{D},1}\theta + b_1c_2 - a_2c_1 > 0,\ \theta \in [0, 1] \\
&\Longleftrightarrow g_{\alpha_{\text{D},1}}(\theta) > 0,\ \theta \in [0, 1]. \qquad (64)
\end{aligned}$$

From (64), given $\alpha_{\text{D},1}$, R_{sec}^{∞} is also a monotonically increasing function of $\theta \in [0, 1]$, which yields $\theta_{\text{opt},1} = 1$. Based on (43), the maximum ergodic secrecy rate for $\alpha_{\text{D},1}$ can be calculated as

$$R_{\text{sec}}^{\infty}(\theta_{\text{opt},1}, \alpha_{\text{D},1}) = \log_2\left(\frac{1}{KP_d + K} f(1, \alpha_{\text{D},1})\right). \qquad (65)$$

It can be easily verified that $f(1, \alpha_{\text{D},1}) = f(\frac{\alpha_{\text{D},1}}{\alpha_{\text{D},2}}, \alpha_{\text{D},2})$, which means $R_{\text{sec}}^{\infty}(\theta_{\text{opt},1}, \alpha_{\text{D},1}) = R_{\text{sec}}^{\infty}(\frac{\alpha_{\text{D},1}}{\alpha_{\text{D},2}}, \alpha_{\text{D},2})$. Since the maximum ergodic secrecy rate for $\alpha_{\text{D},2}$ is achieved at $\theta_{\text{opt},2} = 1$, combining the fact that $\frac{\alpha_{\text{D},1}}{\alpha_{\text{D},2}} \neq 1$, we finally have $R_{\text{sec}}^{\infty}(\theta_{\text{opt},1}, \alpha_{\text{D},1}) = R_{\text{sec}}^{\infty}(\frac{\alpha_{\text{D},1}}{\alpha_{\text{D},2}}, \alpha_{\text{D},2}) < R_{\text{sec}}^{\infty}(\theta_{\text{opt},2}, \alpha_{\text{D},2})$, which completes the proof. □

Proposition 4: For three different DAC parameters $0 < \alpha_{\text{D},1} < \alpha_{\text{D},2} < \alpha_{\text{D},3} < 1$, *if* $\theta_{\text{opt},2} = 1$, *we have*

$$\theta_{\text{opt},1} = 1 \qquad (66)$$

and also

$$R_{\text{sec}}^{\infty}(\theta_{\text{opt},1}, \alpha_{\text{D},1}) < R_{\text{sec}}^{\infty}(\theta_{\text{opt},2}, \alpha_{\text{D},2}) \leq R_{\text{sec}}^{\infty}(\theta_{\text{opt},3}, \alpha_{\text{D},3}). \qquad (67)$$

Proof: By using Lemma 1, (66) and $R_{\text{sec}}^{\infty}(\theta_{\text{opt},1}, \alpha_{\text{D},1}) < R_{\text{sec}}^{\infty}(\theta_{\text{opt},2}, \alpha_{\text{D},2})$ in (67) can be directly obtained. Based on (43) and (44), it can be easily verified that $R_{\text{sec}}^{\infty}(1, \alpha_{\text{D},2}) = R_{\text{sec}}^{\infty}(\frac{\alpha_{\text{D},2}}{\alpha_{\text{D},3}}, \alpha_{\text{D},3})$, which shows that $R_{\text{sec}}^{\infty}(\theta_{\text{opt},2}, \alpha_{\text{D},2})$ is achievable for the DAC parameter $\alpha_{\text{D},3}$. Due to the fact that $R_{\text{sec}}^{\infty}(\frac{\alpha_{\text{D},2}}{\alpha_{\text{D},3}}, \alpha_{\text{D},3}) \leq R_{\text{sec}}^{\infty}(\theta_{\text{opt},3}, \alpha_{\text{D},3})$, we finally have $R_{\text{sec}}^{\infty}(\theta_{\text{opt},2}, \alpha_{\text{D},2}) \leq R_{\text{sec}}^{\infty}(\theta_{\text{opt},3}, \alpha_{\text{D},3})$, which completes the proof. □

Based on the above discussions, we can see that when θ_{opt} is adopted by the BS, in most cases DACs with different quantization bits can achieve the same secrecy performance. Thus, from the perspective of secrecy energy efficiency [28], [29], one-bit DACs are preferred since the power consumption of DACs grows exponentially with the increase of quantization bits [18]. Only for the case where $\theta_{\text{opt}} = 1$, higher-resolution DACs are expected to achieve higher ergodic secrecy rate, which usually occurs when P_e is small.

V. PSA DETECTION

To avoid the leakage of the confidential message, the BS can perform PSA detection before downlink transmission. Up to now, a great deal of research effort has been devoted to PSA detection with emphasis mostly on detection strategy design. Different from the existing work, we focus on the impact of low-resolution ADCs on PSA detection.

For PSA detection, we first define two hypotheses, $\mathcal{H}_0$ and $\mathcal{H}_1$. The hypothesis $\mathcal{H}_0$ states that there is no PSA while $\mathcal{H}_1$ states that the PSA exists. From (7), the quantized signal for estimating user k's channel can be formulated as

$$\widehat{\mathbf{y}}_k = \begin{cases} \tau\alpha_{\text{A}}\sqrt{P_p}\mathbf{h}_k + \alpha_{\text{A}}\mathbf{N}_p\boldsymbol{\varphi}_k^* + \mathbf{Q}_p\boldsymbol{\varphi}_k^*, & \mathcal{H}_0, \\ \tau\alpha_{\text{A}}\sqrt{P_p}\mathbf{h}_k + \tau\alpha_{\text{A}}\sqrt{P_e}\mathbf{h}_{e,k} + \alpha_{\text{A}}\mathbf{N}_p\boldsymbol{\varphi}_k^* + \mathbf{Q}_p\boldsymbol{\varphi}_k^*, & \mathcal{H}_1. \end{cases} \qquad (68)$$

According to (68), the distribution of $\widehat{\mathbf{y}}_k$ is given by

$$\widehat{\mathbf{y}}_k \sim \begin{cases} \mathcal{CN}\left(0, \sigma_{\mathcal{H}_0}^2\mathbf{I}_{N_t}\right), & \mathcal{H}_0, \\ \mathcal{CN}\left(0, \sigma_{\mathcal{H}_1}^2\mathbf{I}_{N_t}\right), & \mathcal{H}_1, \end{cases} \qquad (69)$$

where $\sigma_{\mathcal{H}_0}^2 = \tau^2\alpha_{\text{A}}^2P_p + \tau\alpha_{\text{A}}^2 + \tau\alpha_{\text{A}}(1 - \alpha_{\text{A}})\left(KP_p + 1\right)$ and $\sigma_{\mathcal{H}_1}^2 = \tau^2\alpha_{\text{A}}^2P_p + \tau^2\alpha_{\text{A}}^2P_e + \tau\alpha_{\text{A}}^2 + \tau\alpha_{\text{A}}(1 - \alpha_{\text{A}})\left(KP_p + KP_e + 1\right)$. Similar to [37], we exploit the statistical difference between the two hypotheses for PSA detection. Specifically, we adopt the following PSA detector

$$\|\widehat{\mathbf{y}}_k\|^2 \underset{\mathcal{H}_0}{\overset{\mathcal{H}_1}{\gtrless}} \beta_0, \qquad (70)$$

where β_0 is the detection threshold.

The false alarm probability can be calculated as

$$\begin{aligned}
P_{\text{false}} &= \Pr\left\{\|\widehat{\mathbf{y}}_k\|^2 > \beta_0 | \mathcal{H}_0\right\} \\
&= \Pr\left\{\frac{2\|\widehat{\mathbf{y}}_k\|^2}{\sigma_{\mathcal{H}_0}^2} > \frac{2\beta_0}{\sigma_{\mathcal{H}_0}^2}\Big| \mathcal{H}_0\right\} \\
&= 1 - F_{2N_t}\left(\frac{2\beta_0}{\sigma_{\mathcal{H}_0}^2}\right), \qquad (71)
\end{aligned}$$

where $F_{2N_t}(x)$ is the cumulative distribution function (CDF) of the chi-squared distribution $\chi^2(2N_t)$ with $2N_t$ degrees of freedom. Given a predetermined false alarm probability $P_{\text{false},0}$, the detection threshold can be derived as

$$\beta_0 = \frac{\sigma_{\mathcal{H}_0}^2}{2} F_{2N_t}^{-1}(1 - P_{\text{false},0}), \qquad (72)$$

where $F^{-1}_{2N_t}(y)$ is the inverse function of $F_{2N_t}(x)$. From (72), the value of β_0 is determined by parameters $\sigma^2_{\mathcal{H}_0}$ and $P_{\text{false},0}$, both of which are independent of eavesdropper's CSI and the PSA power. Therefore, the PSA detection in (70) can be performed without the knowledge of eavesdropper's CSI and the PSA power.

Similar to (71), the successful detection probability can be calculated as

$$P_{\text{dect}} = \Pr\left\{\|\widehat{\mathbf{y}}_k\|^2 > \beta_0 | \mathcal{H}_1\right\} = 1 - F_{2N_t}\left(\frac{2\beta_0}{\sigma^2_{\mathcal{H}_1}}\right)$$
$$= 1 - F_{2N_t}\left(\frac{\sigma^2_{\mathcal{H}_0} F^{-1}_{2N_t}(1-P_{\text{false},0})}{\sigma^2_{\mathcal{H}_1}}\right). \quad (73)$$

From (73), the impact of the ADC parameter α_{A} on P_{dect} is determined by the term $\mathcal{I}(\alpha_{\text{A}}) \triangleq \frac{\sigma^2_{\mathcal{H}_0}}{\sigma^2_{\mathcal{H}_1}}$, which equals

$$\mathcal{I}(\alpha_{\text{A}}) = \frac{\sigma^2_{\mathcal{H}_0}}{\sigma^2_{\mathcal{H}_1}} = \frac{\tau^2\alpha_{\text{A}}P_p + \tau\alpha_{\text{A}} + \tau(1-\alpha_{\text{A}})\left(KP_p+1\right)}{\tau^2\alpha_{\text{A}}P_p+\tau^2\alpha_{\text{A}}P_e+\tau\alpha_{\text{A}}+\tau(1-\alpha_{\text{A}})\left(KP_p+KP_e+1\right)}. \quad (74)$$

The first derivative of $\mathcal{I}(\alpha_{\text{A}})$ with respect to α_{A} can be derived as

$$\frac{\partial\mathcal{I}(\alpha_{\text{A}})}{\partial\alpha_{\text{A}}} = \frac{\tau^2\, P_e(K-\tau)}{(\tau^2\alpha_{\text{A}}P_p+\tau^2\alpha_{\text{A}}P_e+\tau\alpha_{\text{A}}+\tau(1-\alpha_{\text{A}})\left(KP_p+KP_e+1\right))^2}. \quad (75)$$

Since $\tau \geq K$, we have $\frac{\partial\mathcal{I}(\alpha_{\text{A}})}{\partial\alpha_{\text{A}}} \leq 0$. Recalling (73) and the fact that $F_{2N_t}(x)$ is an increasing function of x, we can conclude that if $\tau > K$, P_{dect} increases with the increase of α_{A}; if $\tau = K$, which is a widely-adopted choice for minimizing the cost of channel estimation, ADCs with different quantization bits can achieve the same successful detection probability.

Remark 2: By using the PSA detector in (70)*, if a PSA is suspected to exist, the BS can choose to suspend the downlink transmission to avoid information leakage. On the other hand, after identifying a number of cases where the PSA exists, the value of the PSA power P_e can be estimated using the method in [14], as discussed in Remark 1. With the estimated P_e, the optimization of the power allocation parameter in Section III-E can be performed to maximize the secrecy rate.*

VI. NUMERICAL RESULTS

In this section, we present some numerical examples to verify our theoretical results and evaluate the impact of low-resolution ADCs and DACs. In the following numerical results, we use b_{ADC} and b_{DAC} to denote the quantization bits of ADCs and DACs, respectively. The relationship between b_{ADC} and the corresponding ADC parameter α_{A}, b_{DAC} and the corresponding DAC parameter α_{D}, can be found in Table 1. For infinite-resolution quantization, i.e, $b_{\text{ADC}} = \infty$ ($b_{\text{DAC}} = \infty$), the corresponding ADC (DAC) parameter is $\alpha_{\text{A}} = 1$ ($\alpha_{\text{D}} = 1$), which indicates that there is no signal distortion and no quantization noise. Unless otherwise notified, we set $N_t = 128$, $K = 16$, $\tau = 16$, and $P_p = P_d = 5$ dB.

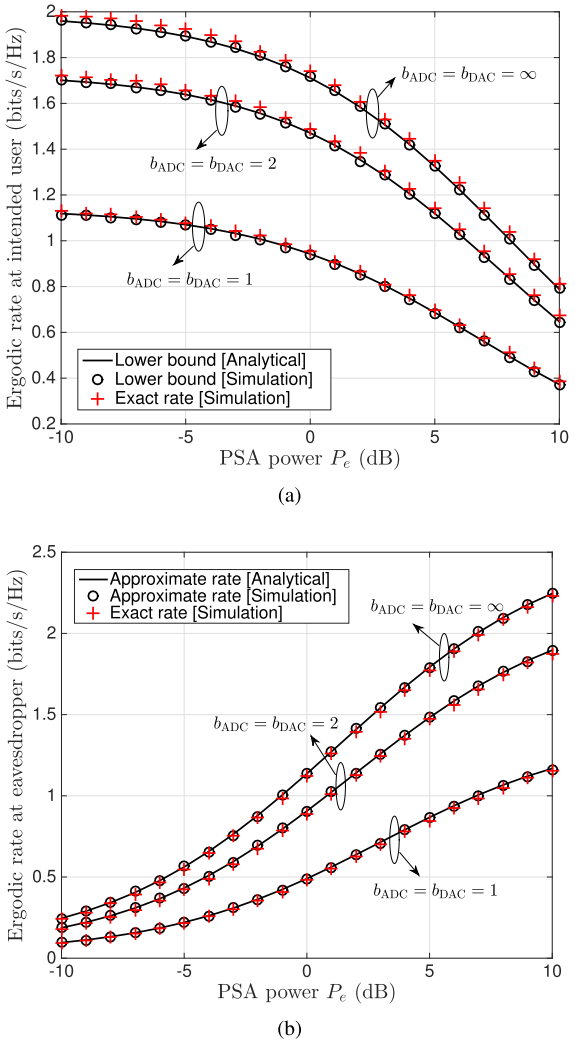
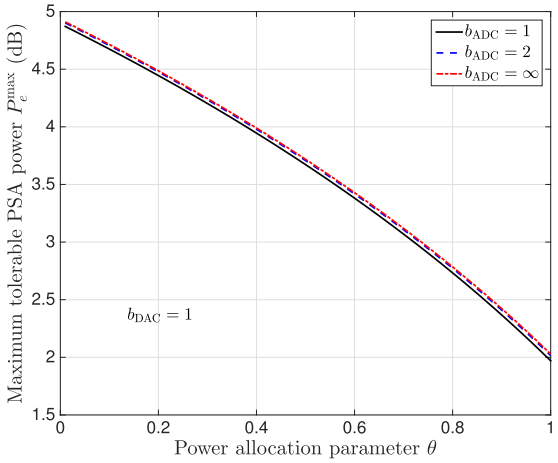


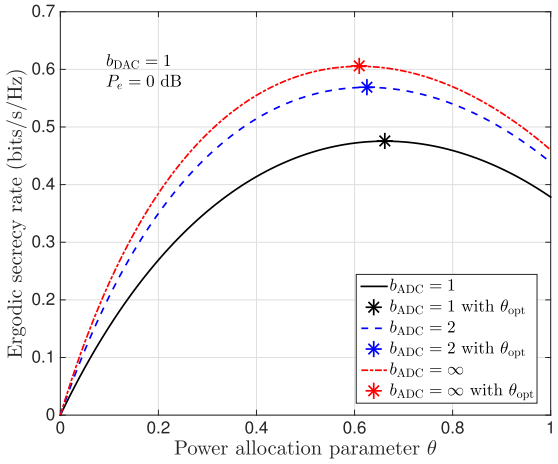
FIGURE 2. Monte Carlo simulation results and the analytical results with $\theta = 0.5$. (a) Ergodic rate at intended user. (b) Ergodic rate at eavesdropper.

First of all, we run Monte Carlo simulations to verify the accuracy of our derived analytical results. In Fig. 2(a), we compare the exact ergodic rate in (23), the simulation result of the lower bound in (26), and the analytical result of the lower bound given by R_{u}^{∞} in (29). In the Monte Carlo simulations for (23) and (26), we take user 1 as an example and the simulation results are obtained based on 2000 randomly generated wireless channels. As illustrated in Fig. 2(a), the analytical lower bound is very close to the simulation lower bound, which indicates that R_{u}^{∞} is accurate for finite number of antennas, e.g., $N_t = 128$. In addition, comparing the exact

rate and the lower bounds, one can see that the lower bounds are tight. Similarly, in Fig. 2(b) we compare the exact ergodic rate in (32), the simulation result of the approximate rate in (34), and the analytical result of the approximate rate given by R_{e}^{∞} in (36). One can observe that the approximate rates are close to the exact one. Moreover, as shown in Fig. 2(b), the analytical result R_{e}^{∞} provides an accurate closed-form expression for (34). Based on the above observations, one can see that R_{u}^{∞} and R_{e}^{∞} are accurate for calculating the lower bound in (26) and the approximate rate in (34), respectively. For simplicity, the following numerical results are directly obtained based on R_{u}^{∞}, R_{e}^{∞}, and the corresponding $R_{\mathrm{sec}}^{\infty} = [R_{\mathrm{u}}^{\infty} - R_{\mathrm{e}}^{\infty}]^{+}$ without giving Monte Carlo results.



(a)



(b)

FIGURE 3. The scenario without P_e for different ADCs: Secrecy performance with θ varying from 0 to 1, where $b_{\mathrm{DAC}} = 1$. (a) Maximum tolerable PSA power versus θ. (b) Ergodic secrecy rate versus θ, where $P_e = 0$ dB.

A. IMPACT OF LOW-RESOLUTION ADCs

In this subsection, we investigate the effect of low-resolution ADCs. Fig. 3 depicts the secrecy performance for the scenario without P_e, where the optimal power allocation parameter θ_{opt} is unavailable. Therefore, the secrecy performance is evaluated for each θ varying from 0 to 1. Fig. 3(a) shows the maximum tolerable PSA power $P_e^{\max}$ for ADCs with different quantization bits. As illustrated in Fig. 3(a), $P_e^{\max}$ decreases with the increase of θ. This is because with the increase of θ, less power is allocated to AN, which significantly increases R_{e}^{∞}. Thus, a small P_e can make R_{e}^{∞} larger than R_{u}^{∞}. On the contrary, if $\theta = 0$, R_{e}^{∞} is always zero, no matter how big P_e is. Besides, it can be observed that for given θ, a larger b_{ADC} can increase $P_e^{\max}$, which is consistent with the analysis in Section IV-A1. However, the improvement of $P_e^{\max}$ is not significant. Fig. 3(b) plots the ergodic secrecy rate versus θ for ADCs with different quantization bits. The ergodic secrecy rate is $R_{\mathrm{sec}}^{\infty}$ in (40). As illustrated in Fig. 3(b), for any θ, higher-resolution ADCs can achieve higher ergodic secrecy rate, which agrees with the analysis in Section IV-A1. Finally, in Fig. 3(b) we also validate the correctness of θ_{opt}. The star markers in Fig. 3(b) are obtained using θ_{opt} in (47), each of which matches the maximum point of each curve. Thus, the derived θ_{opt} is indeed the optimal power allocation parameter.

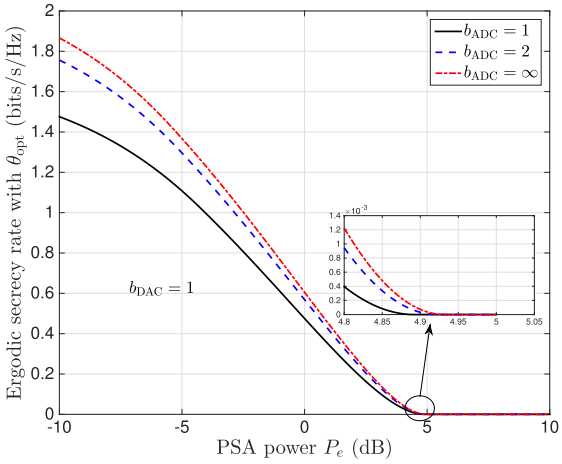
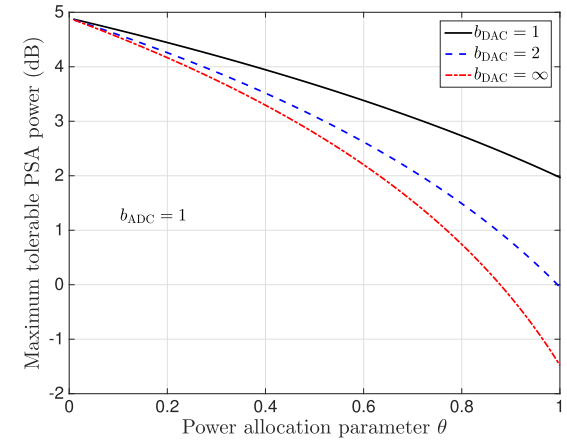


FIGURE 4. The scenario with P_e for different ADCs: Ergodic secrecy rate with θ_{opt} as a function of P_e, where $b_{\mathrm{DAC}} = 1$.

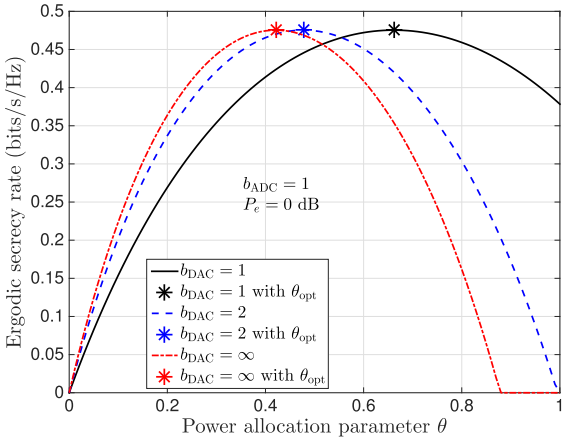
Fig. 4 studies the scenario where P_e is known by the BS. In this case, the BS can exploit θ_{opt} to maximize the ergodic secrecy rate. As illustrated in Fig. 4, when using θ_{opt}, higher-resolution ADCs can also achieve higher ergodic secrecy rate. Moreover, with the increase of P_e, the ergodic secrecy rate decreases. As discussed in Section IV-B, the PSA power which reduces the ergodic secrecy rate with θ_{opt} to zero is defined as $P_{e,\mathrm{opt}}^{\max}$. From Fig. 4 one can see that increasing b_{ADC} can slightly increase $P_{e,\mathrm{opt}}^{\max}$, which verifies our analysis in Section IV-B1.

B. IMPACT OF LOW-RESOLUTION DACs

In this subsection, we focus on the impact of low-resolution DACs. First, we focus on the scenario without P_e. Fig. 5(a) depicts the maximum tolerable PSA power $P_e^{\max}$ for DACs with different quantization bits. It is observed from Fig. 5(a)

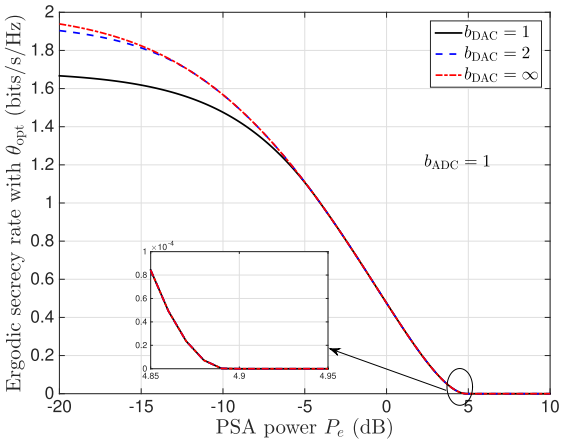


(a)

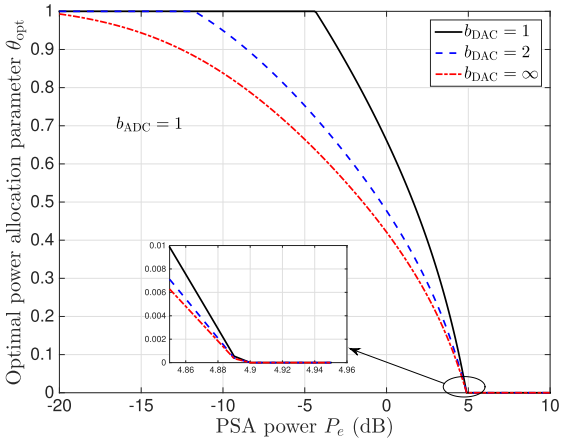


(b)

FIGURE 5. The scenario without P_e for different DACs: Secrecy performance with θ varying from 0 to 1, where $b_{\mathrm{ADC}}=1$. (a) Maximum tolerable PSA power versus θ. (b) Ergodic secrecy rate versus θ, where $P_e=0$ dB.



(a)



(b)

FIGURE 6. The scenario with P_e for different DACs, where $b_{\mathrm{ADC}}=1$. (a) Ergodic secrecy rate with θ_{opt} versus P_e. (b) θ_{opt} versus P_e.

that one-bit resolution DACs can achieve higher $P_e^{\max}$ than infinite-resolution DACs, which indicates that the quantization noise can serve as another form of AN for reducing eavesdropper's channel capacity [30]. Fig. 5(b) plots the ergodic secrecy rate versus θ for DACs with different quantization bits. As analyzed in Section IV-A2, for given θ, enhancing the quantization bits of DACs does not necessarily improve the ergodic secrecy rate. From Fig. 5(b) one can observe that when θ is small, DACs with infinite quantization bits achieve the largest ergodic secrecy rate, which indicates that high-resolution DACs are necessary for mitigating the rate loss due to quantization. When θ is large, the power allocated to AN is small. In this case, it is observed that one-bit DACs are the optimal, which implies that the quantization noise is another anti-eavesdropping resource similar to AN. Finally, as illustrated in Fig. 5(b), each star marker obtained based on θ_{opt} agrees with the maximum point of each curve, which validates the optimality of θ_{opt}.

When P_e is known by the BS, the optimal power allocation parameter θ_{opt} is employed to maximize the ergodic secrecy rate. Fig. 6(a) depicts the ergodic secrecy rate with θ_{opt} while Fig. 6(b) plots the corresponding θ_{opt}. As illustrated in Fig. 6, when P_e is small, the θ_{opt} for lower-resolution DACs first reaches 1, and the θ_{opt} for higher-resolution DACs is not necessarily equal to 1. In this case, higher-resolution DACs can achieve a higher ergodic secrecy rate, which verifies Proposition 4. When $\theta_{\mathrm{opt}} \in (0, 1)$, DACs with different quantization bits can achieve the same ergodic secrecy rate, which agrees with Proposition 3. Moreover, for given P_e, the θ_{opt} for lower-resolution DACs is larger than that for higher-resolution DACs. This is because for lower-resolution DACs, it is necessary to improve the power allocated to the information-bearing signal to mitigate the rate loss due to coarse quantization. Finally, when P_e is large, the ergodic secrecy rate is zero, regardless of the quantization bits of DACs, as proved in Proposition 2.

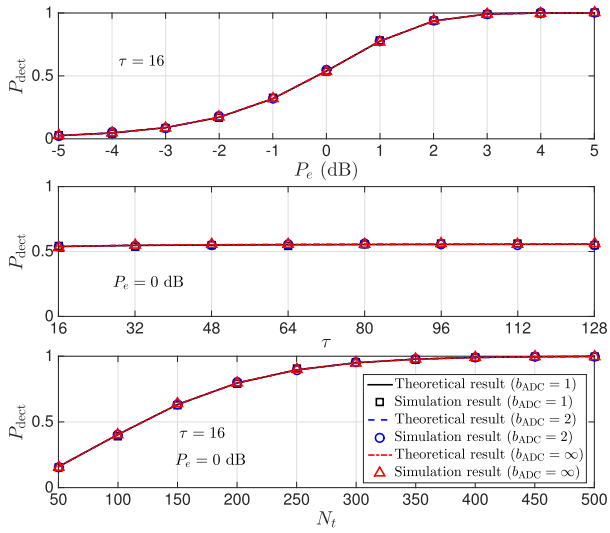


FIGURE 7. Successful detection probability for ADCs with different quantization bits, where $P_{\text{false},0} = 0.001$.

C. PSA DETECTION

In this subsection, we focus on the performance of PSA detection with low-resolution ADCs. Fig. 7 depicts the successful detection probability for ADCs with different quantization bits. The predetermined false alarm probability is set as $P_{\text{false},0} = 0.001$. The theoretical result is obtained using (73) while the simulation result is obtained through Monte Carlo simulations. As illustrated in Fig. 7, for the case where $\tau = K = 16$, the same detection performance can be achieved regardless of the quantization bits of ADCs, which agrees with the analysis in Section V that the successful detection probability is independent of α_{D} when $\tau = K$. Besides, for the case $\tau \neq K$, the resolution of ADCs also has little effect on PSA detection. Moreover, it can be observed that the successful detection probability increases with the increase of N_t. This is because a large N_t can provide a high spatial degrees of freedom for PSA detection. Finally, it is observed that the successful detection probability increases with the increase of P_e, which indicates that the PSA power of the eavesdropper cannot be too large.

VII. CONCLUSION

In this paper, we studied the impact of low-resolution ADCs/DACs on the secrecy performance of a downlink massive MIMO system with the threat of PSA. The MF precoding and the random AN were adopted for the downlink transmission. With the aid of AQNM, we derived the ergodic secrecy rate and the maximum tolerable PSA power. Then, the optimal power allocation parameter was derived, which however needs the knowledge of the PSA power. Therefore, the impact of ADCs' and DACs' resolutions was studied for the two scenarios: the scenario where the PSA power is known by the BS; the scenario where the PSA power is unknown. It is found that for both the two scenarios, high-resolution ADCs outperform low-resolution ADCs in terms of secrecy performance. However, for DACs, when the PSA power is unavailable, increasing the resolution of DACs is not necessarily beneficial for secrecy improvement, due to the absence of the optimal power allocation parameter. When the PSA power is available, by using the optimal power allocation parameter, DACs with different quantization bits can achieve the same ergodic secrecy rate except the case where the PSA power is small. Finally, an energy-based PSA detection method was proposed. The analytical and numerical results show that the resolution of ADCs has little impact on the PSA detection performance.

APPENDIX A
DERIVATION OF (29)

First, we calculate $\mathbb{E}\{\mathbf{h}_k^T\widehat{\mathbf{h}}_k^*\}$ and $\mathbb{E}\left\{|\mathbf{h}_k^T\widehat{\mathbf{h}}_k^*|^2\right\}$ as below.

$$\mathbb{E}\{\mathbf{h}_k^T\widehat{\mathbf{h}}_k^*\} = \mathbb{E}\{(\widehat{\mathbf{h}}_k^T+\Delta\mathbf{h}_k^T)\widehat{\mathbf{h}}_k^*\} = \mathbb{E}\{\|\widehat{\mathbf{h}}_k\|^2\} = N_t\widehat{\sigma}_0^2. \quad (76)$$

$$\begin{aligned}\mathbb{E}\left\{|\mathbf{h}_k^T\widehat{\mathbf{h}}_k^*|^2\right\} &= \mathbb{E}\left\{(\widehat{\mathbf{h}}_k^T+\Delta\mathbf{h}_k^T)\widehat{\mathbf{h}}_k^*\widehat{\mathbf{h}}_k^T(\widehat{\mathbf{h}}_k^*+\Delta\mathbf{h}_k^*)\right\}\\ &= \mathbb{E}\left\{\|\widehat{\mathbf{h}}_k\|^4\right\} + \mathrm{Tr}\left(\mathbb{E}\left\{\Delta\mathbf{h}_k^*\Delta\mathbf{h}_k^T\right\}\mathbb{E}\left\{\widehat{\mathbf{h}}_k^*\widehat{\mathbf{h}}_k^T\right\}\right)\\ &= N_t\widehat{\sigma}_0^2(N_t\widehat{\sigma}_0^2+1) \quad (77)\end{aligned}$$

Based on (76) and (77), the variance of $\mathbf{h}_k^T\widehat{\mathbf{h}}_k^*$ can be calculated as

$$\mathrm{Var}\left(\mathbf{h}_k^T\widehat{\mathbf{h}}_k^*\right) = \mathbb{E}\left\{|\mathbf{h}_k^T\widehat{\mathbf{h}}_k^*|^2\right\} - \left|\mathbb{E}\{\mathbf{h}_k^T\widehat{\mathbf{h}}_k^*\}\right|^2 = N_t\widehat{\sigma}_0^2. \quad (78)$$

Plugging (76) and (78) into (28a) and (28b), respectively, we have

$$A_k = \theta P_d\alpha_{\text{D}}\gamma_1^2N_t^2\widehat{\sigma}_0^4 = \frac{\theta P_d\alpha_{\text{D}}N_t\widehat{\sigma}_0^2}{K}. \quad (79)$$

$$B_k = \theta P_d\alpha_{\text{D}}\gamma_1^2N_t\widehat{\sigma}_0^2 = \frac{\theta P_d\alpha_{\text{D}}}{K}. \quad (80)$$

Then, we focus on the calculation of C_k, which is detailed as

$$\begin{aligned}C_k &= \theta P_d\alpha_{\text{D}}\gamma_1^2\sum_{i\neq k}^{K}\mathbb{E}\left\{|\mathbf{h}_k^T\widehat{\mathbf{h}}_i^*|^2\right\}\\ &= \theta P_d\alpha_{\text{D}}\gamma_1^2\sum_{i\neq k}^{K}\mathbb{E}\left\{\mathrm{Tr}\left(\mathbf{h}_k^*\mathbf{h}_k^T\widehat{\mathbf{h}}_i^*\widehat{\mathbf{h}}_i^T\right)\right\}\\ &= \theta P_d\alpha_{\text{D}}\gamma_1^2(K-1)N_t\widehat{\sigma}_0^2\\ &= \theta P_d\alpha_{\text{D}}\left(1-\frac{1}{K}\right). \quad (81)\end{aligned}$$

Similarly, we have

$$\begin{aligned}D_k &= (1-\theta)P_d\alpha_{\text{D}}\gamma_2^2\mathbb{E}\left\{\mathbf{h}_k^T\mathbf{W}\mathbf{W}^H\mathbf{h}_k^*\right\}\\ &= (1-\theta)P_d\alpha_{\text{D}}\gamma_2^2\mathbb{E}\left\{\mathrm{Tr}\left(\mathbf{h}_k^*\mathbf{h}_k^T\mathbf{W}\mathbf{W}^H\right)\right\}\\ &= (1-\theta)P_d\alpha_{\text{D}}. \quad (82)\end{aligned}$$

For finding a simple expression of E_k, the focus is on the approximation of $\mathbf{C}_{\mathbf{q}_d\mathbf{q}_d}$ for large N_t. Recalling (19), when $N_t \to \infty$, we have

$$\widehat{\mathbf{H}}^*\widehat{\mathbf{H}}^T \xrightarrow{N_t\to\infty} K\widehat{\sigma}_0^2\mathbf{I}_{N_t} \quad (83)$$

and

$$\mathbf{W}\mathbf{W}^H \xrightarrow{N_t\to\infty} \frac{N_t-K}{N_t}\mathbf{I}_{N_t} \tag{84}$$

due to the law of large numbers. Plugging (83) and (84) into (19), we have

$$\mathbf{C}_{\mathbf{q}_d\mathbf{q}_d} \xrightarrow{N_t\to\infty} \alpha_{\mathrm{D}}(1-\alpha_{\mathrm{D}})\frac{P_d}{N_t}\mathbf{I}_{N_t}. \tag{85}$$

With (85), when $N_t \to \infty$, E_k will converge to

$$E_k \xrightarrow{N_t\to\infty} (1-\alpha_{\mathrm{D}})\frac{P_d}{N_t}\mathbb{E}\{\mathbf{h}_k^T\mathbf{h}_k^*\} = (1-\alpha_{\mathrm{D}})P_d. \tag{86}$$

Finally, combining the above derived results and (26), and after some simple mathematical operations, the expression in (29) can be readily obtained.

APPENDIX B
DERIVATION OF (36)

First, we focus on the calculation of $A_{e,k}$. Recalling the expression on $\widehat{\mathbf{h}}_k$ in (11), we have

$$\begin{aligned}
&\mathbb{E}\left\{|\mathbf{h}_{e,k}^T\widehat{\mathbf{h}}_k^*|^2\right\}\\
&=\mathbb{E}\left\{\mathbf{h}_{e,k}^T\widehat{\mathbf{h}}_k^*\widehat{\mathbf{h}}_k^T\mathbf{h}_{e,k}^*\right\}\\
&=\tau^2\xi^2\alpha_{\mathrm{A}}^2\,P_p\mathbb{E}\left\{\mathbf{h}_{e,k}^T\mathbf{h}_k^*\mathbf{h}_k^T\mathbf{h}_{e,k}^*\right\}+\tau^2\xi^2\alpha_{\mathrm{A}}^2P_e\mathbb{E}\left\{\|\mathbf{h}_{e,k}\|^4\right\}\\
&\quad+\xi^2\alpha_{\mathrm{A}}^2\mathbb{E}\left\{\mathbf{h}_{e,k}^T\mathbf{N}_p^*\boldsymbol{\varphi}_k\boldsymbol{\varphi}_k^H\mathbf{N}_p^T\mathbf{h}_{e,k}^*\right\}\\
&\quad+\xi^2\mathbb{E}\left\{\mathbf{h}_{e,k}^T\mathbf{Q}_p^*\boldsymbol{\varphi}_k\boldsymbol{\varphi}_k^H\mathbf{Q}_p^T\mathbf{h}_{e,k}^*\right\}\\
&=\tau^2\xi^2\alpha_{\mathrm{A}}^2P_pN_t+\tau^2\xi^2\alpha_{\mathrm{A}}^2P_eN_t(N_t+1)+\xi^2\alpha_{\mathrm{A}}^2N_t\tau\\
&\quad+\xi^2N_t\tau\sigma_{q_p}^2\\
&=\tau\xi^2\alpha_{\mathrm{A}}^2N_t[\tau P_p+\tau P_e(N_t+1)+1]+\tau\xi^2N_t\sigma_{q_p}^2.
\end{aligned}\tag{87}$$

Thus, we have $A_{e,k} = \theta P_d\alpha_{\mathrm{D}}\gamma_{\mathrm{I}}^2\lambda_0$, where $\lambda_0 = \tau\xi^2\alpha_{\mathrm{A}}^2 N_t[\tau P_p+\tau P_e(N_t+1)+1]+\tau\xi^2N_t\sigma_{q_p}^2$. The calculation of $B_{e,k}$ is then given by

$$\begin{aligned}
B_{e,k} &= (1-\theta)P_d\alpha_{\mathrm{D}}\gamma_2^2\mathbb{E}\left\{\mathbf{h}_{e,k}^T\mathbf{W}\mathbf{W}^H\mathbf{h}_{e,k}^*\right\}\\
&=(1-\theta)P_d\alpha_{\mathrm{D}}\gamma_2^2\mathbb{E}\left\{\mathrm{Tr}\left(\mathbf{h}_{e,k}^*\mathbf{h}_{e,k}^T\mathbf{W}\mathbf{W}^H\right)\right\}\\
&=(1-\theta)P_d\alpha_{\mathrm{D}}.
\end{aligned}\tag{88}$$

By using the the approximation in (85), we have

$$C_{e,k} \xrightarrow{N_t\to\infty} (1-\alpha_{\mathrm{D}})\frac{P_d}{N_t}\mathbb{E}\{\mathbf{h}_{e,k}^T\mathbf{h}_{e,k}^*\} = (1-\alpha_{\mathrm{D}})P_d. \tag{89}$$

With the above derived results, the expression in (36) can be obtained.

REFERENCES

[1] M. Bloch and J. Barros, *Physical-layer Security: From Information Theory to Security Engineering*. New York, NY, USA: Cambridge Univ. Press, 2011.
[2] A. D. Wyner, "The wire-tap channel," *Bell Syst. Tech. J.*, vol. 54, no. 8, pp. 1355–1387, Oct. 1975.
[3] I. Csiszár and J. Korner, "Broadcast channels with confidential messages," *IEEE Trans. Inf. Theory*, vol. IT-24, no. 3, pp. 339–348, May 1978.
[4] 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.
[5] X. Zhang, X. Zhou, and M. R. McKay, "On the design of artificial-noise-aided secure multi-antenna transmission in slow fading channels," *IEEE Trans. Veh. Technol.*, vol. 62, no. 5, pp. 2170–2181, Jun. 2013.
[6] Y. Li, R. Zhao, Y. Wang, G. Pan, and C. Li, "Artificial noise aided precoding with imperfect CSI in full-duplex relaying secure communications," *IEEE Access*, vol. 6, pp. 44107–44119, Jul. 2018.
[7] D. Wang, P. Ren, Q. Du, Y. Wang, and L. Sun, "Secure cooperative transmission against jamming-aided eavesdropper for ARQ based wireless networks," *IEEE Access*, vol. 5, pp. 3763–3776, Mar. 2017.
[8] Y. Zou, X. Wang, and W. Shen, "Optimal relay selection for physical-layer security in cooperative wireless networks," *IEEE J. Sel. Areas Commun.*, vol. 31, no. 10, pp. 2099–2111, Oct. 2013.
[9] 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.
[10] 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.
[11] X. Tang, P. Ren, Y. Wang, and Z. Han, "Combating full-duplex active eavesdropper: A hierarchical game perspective," *IEEE Trans. Commun.*, vol. 65, no. 3, pp. 1379–1395, Mar. 2017.
[12] X. Tang, P. Ren, and Z. Han, "Power-efficient secure transmission against full-duplex active eavesdropper: A game-theoretic framework," *IEEE Access*, vol. 5, pp. 24632–24645, 2017.
[13] D. Kudathanthirige, S. Timilsina, and G. A. Aruma Baduge, "Secure communication in relay-assisted massive MIMO downlink with active pilot attacks," *IEEE Trans. Inf. Forensics Security*, vol. 14, no. 11, pp. 2819–2833, Nov. 2019.
[14] T. M. Hoang, H. Q. Ngo, T. Q. Duong, H. D. Tuan, and A. Marshall, "Cell-free massive MIMO networks: Optimal power control against active eavesdropping," *IEEE Trans. Commun.*, vol. 66, no. 10, pp. 4724–4737, Oct. 2018.
[15] W. Wang, Z. Yin, F. Lyu, H. Wu, Q. Wu, and X. S. Shen, "Pilot spoofing attack detection and downlink precoding in massive MIMO systems," in *Proc. IEEE WCSP*, Xi'an, China, Oct. 2019, pp. 1–6.
[16] X. Zhang, D. Guo, K. An, X. Liang, and W. Ma, "Secure transmission in multi-pair AF relaying massive MIMO networks against active pilot spoofing attacks," *IEEE Access*, vol. 7, pp. 3547–3560, 2019.
[17] W. Wang, N. Cheng, K. C. Teh, X. Lin, W. Zhuang, and X. Shen, "On countermeasures of pilot spoofing attack in massive MIMO systems: A double channel training based approach," *IEEE Trans. Veh. Technol.*, vol. 68, no. 7, pp. 6697–6708, Jul. 2019.
[18] S. Cui, A. J. Goldsmith, and A. Bahai, "Energy-constrained modulation optimization," *IEEE Trans. Wireless Commun.*, vol. 4, no. 5, pp. 2349–2360, Sep. 2005.
[19] L. Fan, D. Qiao, S. Jin, C. K. Wen, and M. Matthaiou, "Optimal pilot length for uplink massive MIMO systems with low-resolution ADC," in *Proc. IEEE SAM*, Rio de Janeiro, Brazil, Jul. 2016, pp. 1–5.
[20] T. Liu, J. Tong, Q. Guo, J. Xi, Y. Yu, and Z. Xiao, "Energy efficiency of massive MIMO systems with low-resolution ADCs and successive interference cancellation," *IEEE Trans. Wireless Commun.*, vol. 18, no. 8, pp. 3987–4002, Aug. 2019.
[21] 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.
[22] C. Kong, C. Zhong, S. Jin, S. Yang, H. Lin, and Z. Zhang, "Full-duplex massive MIMO relaying systems with low-resolution ADCs," *IEEE Trans. Wireless Commun.*, vol. 16, no. 8, pp. 5033–5047, Aug. 2017.
[23] J. Dai, J. Liu, J. Wang, J. Zhao, C. Cheng, and J.-Y. Wang, "Achievable rates for full-duplex massive MIMO systems with low-resolution ADCs/DACs," *IEEE Access*, vol. 7, pp. 24343–24353, 2019.
[24] J. Zhang, L. Dai, S. Sun, and Z. Wang, "On the spectral efficiency of massive MIMO systems with low-resolution ADCs," *IEEE Commun. Lett.*, vol. 20, no. 5, pp. 842–845, May 2016.
[25] J. Zhang, L. Dai, Z. He, B. Ai, and O. A. Dobre, "Mixed-ADC/DAC multipair massive MIMO relaying systems: Performance analysis and power optimization," *IEEE Trans. Commun.*, vol. 67, no. 1, pp. 140–153, Jan. 2019.

[26] J. Zhang, L. Dai, Z. He, S. Jin, and X. Li, "Performance analysis of mixed-ADC massive MIMO systems over Rician fading channels," *IEEE J. Sel. Areas Commun.*, vol. 35, no. 6, pp. 1327–1338, Jun. 2017.

[27] J. Zhang, L. Dai, X. Li, Y. Liu, and L. Hanzo, "On low-resolution ADCs in practical 5G millimeter-wave massive MIMO systems," *IEEE Commun. Mag.*, vol. 56, no. 7, pp. 205–211, Jul. 2018.

[28] X. Jia, M. Zhou, M. Xie, L. Yang, and H. Zhu, "Optimal design of secrecy massive MIMO amplify-and-forward relaying systems with double-resolution ADCs antenna array," *IEEE Access*, vol. 4, pp. 8757–8774, 2016.

[29] Q. Xu and P. Ren, "Secrecy energy efficiency of massive MIMO AF relaying system with low-resolution ADCs," in *Proc. IEEE Global Commun. Conf. (GLOBECOM)*, Abu Dhabi, United Arab Emirates, Dec. 2018, pp. 1–6.

[30] J. Xu, W. Xu, J. Zhu, D. W. K. Ng, and A. Lee Swindlehurst, "Secure massive MIMO communication with low-resolution DACs," *IEEE Trans. Commun.*, vol. 67, no. 5, pp. 3265–3278, May 2019.

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

[32] X. Gao, O. Edfors, F. Rusek, and F. Tufvesson, "Massive MIMO performance evaluation based on measured propagation data," *IEEE Trans. Wireless Commun.*, vol. 14, no. 7, pp. 3899–3911, Jul. 2015.

[33] F. Rusek, D. Persson, B. Kiong Lau, E. G. Larsson, T. L. Marzetta, and F. Tufvesson, "Scaling up MIMO: Opportunities and challenges with very large arrays," *IEEE Signal Process. Mag.*, vol. 30, no. 1, pp. 40–60, Jan. 2013.

[34] X. Xia, K. Xu, D. Zhang, Y. Xu, and Y. Wang, "Beam-domain full-duplex massive MIMO: Realizing co-time co-frequency uplink and downlink transmission in the cellular system," *IEEE Trans. Veh. Technol.*, vol. 66, no. 10, pp. 8845–8862, Oct. 2017.

[35] Q. Ding and Y. Jing, "Receiver energy efficiency and resolution profile design for massive MIMO uplink with mixed ADC," *IEEE Trans. Veh. Technol.*, vol. 67, no. 2, pp. 1840–1844, Feb. 2018.

[36] Q. Zhang, S. Jin, K.-K. Wong, H. Zhu, and M. Matthaiou, "Power scaling of uplink massive MIMO systems with arbitrary-rank channel means," *IEEE J. Sel. Topics Signal Process.*, vol. 8, no. 5, pp. 966–981, Oct. 2014.

[37] X. Liu, B. Li, H. Chen, Z. Sun, Y.-C. Liang, and C. Zhao, "Detecting pilot spoofing attack in MISO systems with trusted user," *IEEE Commun. Lett.*, vol. 23, no. 2, pp. 314–317, Feb. 2019.

QIAN XU (Graduate Student Member, IEEE) received the B.S. degree from Xi'an Jiaotong University, China, in 2014, where she is currently pursuing the Ph.D. degree with the School of Information and Communications Engineering. From October 2018 to October 2019, she was a Visiting Student with the Department of Electrical Engineering and Computer Science, Henry Samueli School of Engineering, University of California, Irvine, CA, USA. Her research interests include physical layer security, massive MIMO systems, and cooperative relaying networks.

PINYI REN (Member, IEEE) received the B.S. degree in information and control engineering, the M.S. degree in information and communications engineering, and the Ph.D. degree in electronics and communications systems from Xi'an Jiaotong University, China, in 1994, 1997, and 2001, respectively. He is currently a Professor with the Department of Information and Communications Engineering, Xi'an Jiaotong University. He has published over 100 technical papers in international journals and conferences. He is selected as a Fellow of the China Institute of Communications (CIC). He is a member of the IEEE Communications Society. He received the Best Letter Award from the IEICE Communications Society, in 2010. He has served as the General Chair of ICST WICON, in 2011, and serves frequently as the Technical Program Committee Member of the IEEE GLOBECOM, the IEEE ICC, and the IEEE CCNC. He serves as an Editor for the *Journal of Xi'an Jiaotong University* and the *Journal of Electronics and Information Technology*, and he has served as the Leading Guest Editor for the Special Issue on Distributed Wireless Networks and Services for *Mobile Networks and Applications*.