Artificial Noise Revisited

Shuiyin Liu, Yi Hong, and Emanuele Viterbo

Abstract

The artificial noise (AN) scheme, proposed by Goel and Negi, is being considered as one of the key enabling technology for secure communications over MIMO wiretap channels. However, the decrease in secrecy rate due to the increase in the number of Eve's antennas is not well understood. In this paper, we develop an analytical framework to characterize the secrecy rate of the AN scheme as a function of Eve's SNR, Bob's SNR, the number of antennas in each terminal, and the power allocation scheme. We first derive a closed-form expression for the average secrecy rate. We then derive a closed-form expression for the asymptotic instantaneous secrecy rate with large number of antennas at all terminals. Finally, we derive simple lower and upper bounds on the average/instantaneous secrecy rate that provide a tool for the system design.

Index Terms

artificial noise, secrecy capacity, physical layer security, wiretap channel.

I. Introduction

The security of data transmissions is a fundamental issue in wireless communication systems, where the broadcast characteristics make it difficult to prevent eavesdropping. Traditional key-based cryptography [1–3] usually is based on the assumption that the eavesdropper (Eve) has limited computational resources. These algorithms ensure that it is computational infeasible to decipher the encrypted messages without knowledge of the secret key. On the other hand, assuming Eve has unlimited computational power, Wyner, in [4], analyzed how one can reliably send information over a discrete memoryless wiretap channel. Wyner showed that, if Eve intercepts a degraded version of the intended receiver's (Bob's) signal, the transmitter (Alice) can limit the information leakage by means of channel coding. The associated notion of *secrecy*

S. Liu, Y. Hong and E. Viterbo are with the Department of Electrical and Computer Systems Engineering, Monash University, Clayton, VIC 3800, Australia (e-mail: {shuiyin.liu, yi.hong, emanuele.viterbo}@monash.edu). This work was performed at the Monash Software Defined Telecommunications Lab and the authors were supported by the Monash Professorial Fellowship, 2013 Monash Faculty of Engineering Seed Funding Scheme, and the Australian Research Council Discovery Project with ARC DP130100336.

capacity was introduced to characterize the maximum transmission rate from Alice to Bob, below which Eve is unable to obtain any information.

Wyner's original work provided the theoretical foundation for keyless security, namely *physical layer security*. Several studies have been made to generalize Wyner's wiretap channel model. For example, in [5], Leung-Yan-Cheong and Hellman studied the Gaussian wiretap channel and showed that a positive secrecy capacity exists only when Eve's channel is of lower quality than that of Bob. In [6], the authors considered a non-degraded version of Wyner's wiretap channel. The notion of wiretap channel has also been extended to fading channels. For quasi-static fading channels, the outage probability of secrecy capacity is derived in [7]. For the ergodic fading channel, [8] provides a detailed analysis of secrecy capacity. In [9], the secrecy capacity region of a multiple-access channel with confidential messages is derived. The secure transmissions over multiple-output multiple-input (MIMO) wiretap channels are studied in [10]. The achievable average secrecy rate has been widely adopted as a metric of security [7–11].

In the context of wiretap code design, Csiszár [12] proposed the *strong secrecy* criterion, i.e., $\lim_{n\to\infty} I(\mathbf{u};\mathbf{y}) = 0$, which implies that the overall information leakage between the message $\mathbf{u}$ and Eve's channel output $\mathbf{y}$ should vanish as the codeword length n tends to infinity. Polar codes achieving strong secrecy over discrete memoryless channels have been proposed in [13]. For Gaussian wiretap channels, nested lattice codes achieving strong secrecy were proposed in [14]. In particular, polar codes in [13] and lattice codes in [14] were shown to achieve semantic security [2]. In [15], Oggier *et al.* showed that it is possible to construct lattice codes that maximizes Eve's error probability.

Instead of only relying on the randomness of communication channels, physical layer jamming techniques were proposed to increase secrecy rate. In [11], Goel and Negi showed that it is possible to align additive white Gaussian noise (AWGN), so called "artificial noise" (AN), within the null space of a MIMO channel between Alice and Bob, thus only Eve is jammed. The idea of AN has been extended to various system models [16–20]. When the number of Bob's antennas N_{B} is one, the asymptotic analysis of the secrecy capacity was derived in [16], and its power allocation scheme was presented in [17]. In the case of imperfect channel state information, an average minimum mean square (MSE) uplink-downlink duality was derived in [18]. More recently, we have shown that Eve's error probability can be maximized by any randomly distributed AN (not necessarily Gaussian) [19]. In the existing AN-based schemes, it is commonly assumed that the number of Eve's antennas N_{E} is smaller than the number of Alice's antennas N_{A}, i.e., $N_{\mathrm{E}} < N_{\mathrm{A}}$ [11,17,20]. However, the relationship between the secrecy rate and unbounded N_{E} has never been explored.

In this work, we characterize the exact secrecy rate of the original AN scheme [11] for any Eve-to-Bob channel noise-power ratios using various AN power allocation schemes, with arbitrary number of antennas at each terminal. Our contributions are three-fold: firstly, we derive a closed-form expression for the *average secrecy rate*; secondly, we derive a closed-form expression for the asymptotic *instantaneous secrecy rate* as the number of antennas in each terminal becomes large; and finally, we derive lower and upper bounds on the average/instantaneous secrecy rate, leading to simple sufficient and necessary conditions that guarantee positive average/instantaneous secrecy rate.

The paper is organized as follows: Section II presents the system model, followed by the analysis of secrecy rate in Section III. Section IV provides lower and upper bounds on the secrecy rate. Conclusions are drawn in Section V. Proofs of the theorems are given in Appendix.

Notation: Matrices and column vectors are denoted by upper and lowercase boldface letters, and the Hermitian transpose, inverse, pseudoinverse of a matrix $\mathbf{B}$ by $\mathbf{B}^H$, $\mathbf{B}^{-1}$, and $\mathbf{B}^{\dagger}$, respectively. $|\mathbf{B}|$ denotes the determinant of $\mathbf{B}$. Let the random variables $\{X_n\}$ and X be defined on the same probability space. We write $X_n \overset{a.s.}{\to} X$ if X_n converges to X almost surely or with probability one. $\mathbf{I}_n$ denotes the identity matrix of size n. An $m \times n$ null matrix is denoted by $\mathbf{0}_{m\times n}$. A circularly symmetric complex Gaussian random variable x with variance σ^2 is defined as $x \backsim \mathcal{N}_{\mathbb{C}}(0, \sigma^2)$. The real, complex, integer and complex integer numbers are denoted by $\mathbb{R}$, $\mathbb{C}$, $\mathbb{Z}$ and $\mathbb{Z}[i]$, respectively. $I(x; y)$ represents the mutual information of two random variables x and y. We use the standard asymptotic notation $f(x) = O(g(x))$ when $\limsup_{x\to\infty} |f(x)/g(x)| < \infty$. $\lceil x \rfloor$ rounds to the closest integer. A central complex Wishart matrix $\mathbf{A} \in \mathbb{C}^{m\times m}$ with n degrees of freedom and covariance matrix $\mathbf{\Sigma}$, is defined as $\mathbf{A} \backsim W_m(n,\mathbf{\Sigma})$. We write $\triangleq$ for equality in definition.

II. System Model

We consider secure communications over a three-terminal system, including a transmitter (Alice), the intended receiver (Bob), and an unauthorized receiver (Eve), equipped with N_{A}, N_{B}, and N_{E} antennas, respectively. The signal vectors received by Bob and Eve are

$$\mathbf{z} = \mathbf{H}\mathbf{x} + \mathbf{n}_{\mathrm{B}}, \tag{1}$$

$$\mathbf{y} = \mathbf{G}\mathbf{x} + \mathbf{n}_{\mathrm{E}}, \tag{2}$$

where $\mathbf{x} \in \mathbb{C}^{N_{\mathrm{A}}\times 1}$ is the transmit signal vector, $\mathbf{H} \in \mathbb{C}^{N_{\mathrm{B}}\times N_{\mathrm{A}}}$ and $\mathbf{G} \in \mathbb{C}^{N_{\mathrm{E}}\times N_{\mathrm{A}}}$ are the respective channel matrices between Alice to Bob and Alice to Eve, and $\mathbf{n}_{\mathrm{B}}$, $\mathbf{n}_{\mathrm{E}}$ are AWGN vectors with i.i.d.

entries $\sim \mathcal{N}_{\mathbb{C}}(0,\, \sigma_{\mathrm{B}}^2)$ and $\mathcal{N}_{\mathbb{C}}(0,\, \sigma_{\mathrm{E}}^2)$. We assume that the entries of $\mathbf{H}$ and $\mathbf{G}$ are i.i.d. complex random variables $\sim \mathcal{N}_{\mathbb{C}}(0,\, 1)$.

Without loss of generality, we normalize Bob's channel noise variance to one, i.e.,

$$\sigma_{\mathrm{B}}^2 = 1, \tag{3}$$

and accordingly normalize the total average transmission power $\mathrm{E}(||\mathbf{x}||^2)$, as in [21].

A. Artificial Noise Scheme

The AN scheme assumes $N_{\mathrm{B}} < N_{\mathrm{A}}$, in order to ensure that $\mathbf{H}$ has a non-trivial null space $\mathbf{Z} = \mathrm{null}(\mathbf{H})$ (such that $\mathbf{HZ} = \mathbf{0}_{N_{\mathrm{B}} \times (N_{\mathrm{A}} - N_{\mathrm{B}})}$) [11]. Let $\mathbf{H} = \mathbf{U}\mathbf{\Lambda}\mathbf{V}^H$ be the singular value decomposition (SVD) of $\mathbf{H}$, then we can write the unitary matrix $\mathbf{V}$ as

$$\mathbf{V} = [\mathbf{V}_1, \mathbf{Z}], \tag{4}$$

where the N_{B} columns of $\mathbf{V}_1$ span the orthogonal complement subspace to the null space spanned by the columns of $\mathbf{Z}$.

Using the AN scheme, Alice transmits

$$\mathbf{x} = \mathbf{V}_1\mathbf{u} + \mathbf{Z}\mathbf{v} = \mathbf{V}\begin{bmatrix} \mathbf{u} \\ \mathbf{v} \end{bmatrix}, \tag{5}$$

where $\mathbf{u} \in \mathbb{C}^{N_{\mathrm{B}} \times 1}$ is the information vector and $\mathbf{v} \in \mathbb{C}^{(N_{\mathrm{A}} - N_{\mathrm{B}}) \times 1}$ is the "artificial noise". For the purpose of evaluating the achievable secrecy rate, both $\mathbf{u}$ and $\mathbf{v}$ are assumed to be Gaussian circularly symmetric random vectors with i.i.d. complex entries $\sim \mathcal{N}_{\mathbb{C}}(0,\, \sigma_{\mathrm{u}}^2)$ and $\mathcal{N}_{\mathbb{C}}(0,\, \sigma_{\mathrm{v}}^2)$, respectively.

Equations (1) and (2) can then be rewritten as

$$\mathbf{z} = \mathbf{H}\mathbf{V}_1\mathbf{u} + \mathbf{HZ}\mathbf{v} + \mathbf{n}_{\mathrm{B}} = \mathbf{H}\mathbf{V}_1\mathbf{u} + \mathbf{n}_{\mathrm{B}}, \tag{6}$$

$$\mathbf{y} = \mathbf{G}\mathbf{V}_1\mathbf{u} + \mathbf{GZ}\mathbf{v} + \mathbf{n}_{\mathrm{E}}. \tag{7}$$

From (6) and (7), we note that $\mathbf{v}$ only degrades Eve's channel, but does not affect Bob.

In our paper, we assume the worst-case scenario for Alice and Bob described in [11]:

- Alice has only the knowledge of $\mathbf{H}$.
- Eve has the knowledge of $\mathbf{H}$, $\mathbf{G}$, $\mathbf{Z}$ and $\mathbf{V}_1$.

Different from [11], we assume no upper bound on N_{E}.

Since $\mathbf{V}$ is a unitary matrix, the total transmission power can be written as

$$||\mathbf{x}||^2 = \begin{bmatrix} \mathbf{u} \\ \mathbf{v} \end{bmatrix}^H \mathbf{V}^H\mathbf{V} \begin{bmatrix} \mathbf{u} \\ \mathbf{v} \end{bmatrix} = ||\mathbf{u}||^2 + ||\mathbf{v}||^2. \tag{8}$$

We set the average transmit power constraint P,

$$P = \mathrm{E}(||\mathbf{x}||^2) = P_{\mathrm{u}} + P_{\mathrm{v}}, \tag{9}$$

where

$$\begin{aligned} P_{\mathrm{u}} &= \mathrm{E}(||\mathbf{u}||^2) = \sigma_{\mathrm{u}}^2 N_{\mathrm{B}}, \\ P_{\mathrm{v}} &= \mathrm{E}(||\mathbf{v}||^2) = \sigma_{\mathrm{v}}^2 (N_{\mathrm{A}} - N_{\mathrm{B}}), \end{aligned} \tag{10}$$

are fixed by the power allocation scheme that selects the balance between σ_{u}^2 and σ_{v}^2.

B. *Instantaneous and Average Secrecy Capacities*

The idea underpinning the AN scheme is to increase secrecy capacity by jamming Eve. We recall from [22] the definition of instantaneous secrecy capacity:

$$C_{\mathrm{S}} \triangleq \max_{p(\mathbf{u})} \left\{ I(\mathbf{u};\mathbf{z}) - I(\mathbf{u};\mathbf{y}) \right\}. \tag{11}$$

where the maximum is taken over all possible input distributions $p\left(\mathbf{u}\right)$.

We remark that C_{S} is a function of $\mathbf{H}$ and $\mathbf{G}$, which are embedded in $\mathbf{z}$ and $\mathbf{y}$. To average out the randomness of C_{S}, we further define the average secrecy capacity, as in [11]

$$\bar{C}_{\mathrm{S}} \triangleq \max_{p(\mathbf{u})} \left\{ I(\mathbf{u};\mathbf{z}|\mathbf{H}) - I(\mathbf{u};\mathbf{y}|\mathbf{H},\, \mathbf{G}) \right\}, \tag{12}$$

where $I\left(X;Y|Z\right) \triangleq \mathrm{E}_Z\left[I\left(X;Y\right)|Z\right]$, following the notation in [21].

Since closed form expressions for C_{S} and $\bar{C}_{\mathrm{S}}$ are not always available (except for the following Theorem 3 given in Sec. III.E), we often resort to the corresponding secrecy rates, given by

$$R_{\mathrm{S}} \triangleq I(\mathbf{u};\mathbf{z}) - I(\mathbf{u};\mathbf{y}), \tag{13}$$

$$\bar{R}_{\mathrm{S}} \triangleq I(\mathbf{u};\mathbf{z}|\mathbf{H}) - I(\mathbf{u};\mathbf{y}|\mathbf{H},\mathbf{G}), \tag{14}$$

assuming Gaussian input alphabets, i.e., $\mathbf{v}$ and $\mathbf{u}$ are mutually independent Gaussian vectors with i.i.d. complex entries $\mathcal{N}_{\mathbb{C}}(0,\, \sigma_{\mathrm{v}}^2)$ and $\mathcal{N}_{\mathbb{C}}(0,\, \sigma_{\mathrm{u}}^2)$, respectively.

C. System Parameters

We define Bob's and Eve's SNRs as

- $\text{SNR}_\text{B} \triangleq \sigma_\text{u}^2/\sigma_\text{B}^2$
- $\text{SNR}_\text{E} \triangleq \sigma_\text{u}^2/\sigma_\text{E}^2$

To simplify our notation, we define three system parameters:

- $\alpha \triangleq \sigma_\text{u}^2/\sigma_\text{E}^2$ (SNR_E)
- $\beta \triangleq \sigma_\text{v}^2/\sigma_\text{u}^2$ (AN power allocation)
- $\gamma \triangleq \sigma_\text{E}^2/\sigma_\text{B}^2$ (Eve-to-Bob noise-power ratio)

Note that $\text{SNR}_\text{B} = \alpha\gamma$. If $\gamma > 1$, we say Eve has a *degraded* channel. Since we have normalized σ_B^2 to one, we can write (10) as

- $P_\text{u} = \alpha\gamma N_\text{B}$
- $P_\text{v} = \alpha\beta\gamma(N_\text{A} - N_\text{B})$

III. Secrecy Rate with Gaussian Input Alphabets

In this section, we first derive a closed-form expression for the average secrecy rate in (14) with Gaussian input alphabets. We then present an asymptotic analysis on the instantaneous secrecy rate in (13). Finally, we show average secrecy capacity in (12) is achieved with Gaussian input alphabets when $N_\text{E} \le N_\text{A} - N_\text{B}$. To present our result, we define some useful functions.

A. Definitions

We first define the following function (see [23])

$$\Theta(m,n,x) \triangleq e^{-1/x} \sum_{k=0}^{m-1}\sum_{l=0}^{k}\sum_{i=0}^{2l} \left\{ \frac{(-1)^i (2l)!(n-m+i)!}{2^{2k-i} l! i! (n-m+l)!} \cdot \binom{2(k-l)}{k-l} \cdot \binom{2(l+n-m)}{2l-i} \cdot \sum_{j=0}^{n-m+i} x^{-j}\Gamma(-j,1/x) \right\}, \tag{15}$$

where $\binom{a}{b} = a!/((a-b)!b!)$ is the binomial coefficient, $n \ge m$ are positive integers, and $\Gamma(a,b)$ is the incomplete Gamma function

$$\Gamma(a,b) = \int_b^\infty x^{a-1}e^{-x}dx. \tag{16}$$

We further define

$$N_\text{min} \triangleq \min\{N_\text{E},\, N_\text{A} - N_\text{B}\}, \tag{17}$$

$$N_\text{max} \triangleq \max\{N_\text{E},\, N_\text{A} - N_\text{B}\}, \tag{18}$$

$$\hat{N}_{\min} \triangleq \min\{N_{\mathrm{E}},\, N_{\mathrm{A}}\}, \tag{19}$$

$$\hat{N}_{\max} \triangleq \max\{N_{\mathrm{E}},\, N_{\mathrm{A}}\}. \tag{20}$$

Finally, we define a set of N_{A} power ratios $\{\theta_i\}_1^{N_{\mathrm{A}}}$, where

$$\theta_i \triangleq \begin{cases} \alpha & 1 \le i \le N_{\mathrm{B}} \\ \alpha\beta & N_{\mathrm{B}}+1 \le i \le N_{\mathrm{A}} \end{cases} \tag{21}$$

B. Average Secrecy Rate

A closed-form expression for $\bar{R}_{\mathrm{S}}$ in (14) can be derived using the results from [21, Th. 2], [23, Th. 1] and [24, Th. 1], leading to the following theorem.

Theorem 1:

$$\bar{R}_{\mathrm{S}} = \Theta(N_{\mathrm{B}}, N_{\mathrm{A}}, \alpha\gamma) + \Theta(N_{\min}, N_{\max}, \alpha\beta) - \Omega, \tag{22}$$

where $\Theta(\cdot,\cdot,\cdot)$ is given in (15),

$$\Omega = \begin{cases} K \sum\limits_{k=1}^{\hat{N}_{\min}} \det\left(\mathbf{R}^{(k)}\right), & \beta \neq 1 \\ \Theta(\hat{N}_{\min}, \hat{N}_{\max}, \alpha), & \beta = 1 \end{cases} \tag{23}$$

$$K = \frac{(-1)^{N_{\mathrm{E}}(N_{\mathrm{A}}-\hat{N}_{\min})}}{\Gamma_{\hat{N}_{\min}}(N_{\mathrm{E}})} \frac{\prod\limits_{i=1}^{2} \mu_i^{m_i N_{\mathrm{E}}}}{\prod\limits_{i=1}^{2} \Gamma_{m_i}(m_i) \prod\limits_{i<j} \left(\mu_i - \mu_j\right)^{m_i m_j}}, \tag{24}$$

$$\Gamma_k(n) = \prod_{i=1}^{k} (n-i)!,$$

and $\mu_1 > \mu_2$ are the two distinct eigenvalues of the matrix $\mathrm{diag}\left(\{\theta_i^{-1}\}_1^{N_{\mathrm{A}}}\right)$, with corresponding multiplicities m_1 and m_2 such that $m_1 + m_2 = N_{\mathrm{A}}$. The matrix $\mathbf{R}^{(k)}$ has elements

$$r_{i,j}^{(k)} = \begin{cases} (\mu_{e_i})^{N_{\mathrm{A}}-j-d_i} \dfrac{(N_{\mathrm{A}}-j)!}{(N_{\mathrm{A}}-j-d_i)!}, & \hat{N}_{\min}+1 \le j \le N_{\mathrm{A}} \\ (-1)^{d_i} \dfrac{\varphi(i,j)!}{(\mu_{e_i})^{\varphi(i,j)+1}}, & 1 \le j \le \hat{N}_{\min},\ j \neq k \\ (-1)^{d_i} \varphi(i,j)! e^{\mu_{e_i}} \sum\limits_{l=0}^{\varphi(i,j)} \dfrac{\Gamma(l-\varphi(i,j), \mu_{e_i})}{(\mu_{e_i})^{l+1}}, & \text{otherwise} \end{cases} \tag{25}$$

where

$$e_i = \begin{cases} 1 & 1 \le i \le m_1 \\ 2 & m_1 + 1 \le i \le N_{\mathrm{A}} \end{cases}$$

$$d_i = \sum_{k=1}^{e_i} m_k - i,$$

$$\varphi(i,j) = N_{\mathrm{E}} - \hat{N}_{\min} + j - 1 + d_i.$$

Proof: See Appendix A. ■

Theorem 1 gives the exact value of $\bar{R}_{\mathrm{S}}$ for the AN scheme, as a function of $\mathrm{SNR}_{\mathrm{B}}$ ($\alpha\gamma$), $\mathrm{SNR}_{\mathrm{E}}$ (α), power allocation scheme (β), N_{A}, N_{B} and N_{E}. Note that (22) can be expressed in terms of a finite number of incomplete Gamma functions, thus provides a closed-form expression for $\bar{R}_{\mathrm{S}}$.

C. Asymptotic Instantaneous Secrecy Rate

The instantaneous secrecy rate R_{S} in (13) is a function of $\mathbf{H}$, $\mathbf{V}$ and $\mathbf{G}$. Since we assumed that the realizations of $\mathbf{H}$, $\mathbf{V}$ and $\mathbf{G}$ are known to Eve, she is able to compute the exact value of R_{S}. However, Alice only knows the realizations of $\mathbf{H}$ and $\mathbf{V}$, and can only assume that $\mathbf{G}$ is a random matrix. Therefore, R_{S} is a random variable from Alice's perspective. We will consider this point of view when designing the secure communications system and we will use random matrix theory to characterize the asymptotic behavior (in terms of number of antennas) of the *normalized* instantaneous secrecy rate $R_{\mathrm{S}}/N_{\mathrm{B}}$. We then show by simulation that the asymptotic behavior is a very accurate approximation even for very small numbers of antennas.

The following theorem proves that $R_{\mathrm{S}}/N_{\mathrm{B}}$ converges to a constant value, which depends only of the system parameters: α, β, γ, P_u, P_v, and the asymptotic number of antenna ratios. A special case of this result for $\beta = 1$ was given in [25]. Here, we provide a unified result for arbitrary β.

Theorem 2: As N_{A}, N_{B}, $N_{\mathrm{A}} - N_{\mathrm{B}}$ and $N_{\mathrm{E}} \to \infty$ with $N_{\mathrm{A}}/N_{\mathrm{E}} \to \beta_1$, $N_{\mathrm{A}}/N_{\mathrm{B}} \to \beta_2$ and $N_{\mathrm{B}}/N_{\mathrm{E}} \to \beta_3$,

$$\begin{aligned} \frac{R_{\mathrm{S}}}{N_{\mathrm{B}}} \quad &\overset{a.s.}{\to} \quad \Phi(P_{\mathrm{u}},\, \beta_2) - \frac{1}{\beta_3}\left(\beta_1 \mathcal{V}(\delta) - \log\delta + \delta - 1\right) \\ &+ \frac{1}{\beta_3}\Phi\left(\frac{P_{\mathrm{v}}}{\gamma(\beta_1 - \beta_3)},\, \beta_1 - \beta_3\right) \quad \triangleq \quad \Psi, \end{aligned} \tag{26}$$

where

$$\begin{aligned} \Phi\left(x,\, y\right) \quad &= \quad y \log\left(1 + x - \frac{1}{4}\mathcal{F}\left(x, y\right)\right) - \frac{\mathcal{F}\left(x, y\right)}{4x} \\ &+ \log\left(1 + xy - \frac{1}{4}\mathcal{F}\left(x, y\right)\right), \end{aligned} \tag{27}$$

$$\mathcal{F}\left(x,y\right)=\left(\sqrt{x\left(1+\sqrt{y}\right)^{2}+1}-\sqrt{x\left(1-\sqrt{y}\right)^{2}+1}\right)^{2}, \tag{28}$$

$$\mathcal{V}(\delta)=\frac{1}{\beta_2}\log\left(1+\frac{\delta P_{\rm u}}{\gamma\beta_3}\right)+\left(1-\frac{1}{\beta_2}\right)\log\left(1+\frac{\delta P_{\rm v}}{\gamma(\beta_1-\beta_3)}\right), \tag{29}$$

and δ is the solution of the equation

$$\beta_1=\frac{1-\delta}{1-\eta(\delta)}, \tag{30}$$

$$\eta(\delta)=\frac{1}{\beta_2}\left(1+\frac{\delta P_{\rm u}}{\gamma\beta_3}\right)^{-1}+\left(1-\frac{1}{\beta_2}\right)\left(1+\frac{\delta P_{\rm v}}{\gamma(\beta_1-\beta_3)}\right)^{-1}. \tag{31}$$

Proof: See Appendix B. ∎

In the special case of $\beta=1$, according to the definitions of $P_{\rm u}$ and $P_{\rm v}$ given in Sec. II.C, we have

$$\frac{P_{\rm u}}{\gamma\beta_3}=\frac{P_{\rm v}}{\gamma(\beta_1-\beta_3)}. \tag{32}$$

According to [26, Eq. 2.121], the explicit solution of (30) is

$$\delta=1-\frac{\mathcal{F}\left(\frac{P_{\rm u}}{\gamma\beta_3},\beta_1\right)}{\frac{4P_{\rm u}}{\gamma\beta_3}}. \tag{33}$$

By substituting (32) and (33) into (26), we have

$$\frac{R_{\rm S}}{N_{\rm B}}\xrightarrow{a.s.}\Phi(P_{\rm u},\,\beta_2)-\frac{\Phi(P_{\rm u}/(\gamma\beta_3),\,\beta_1)}{\beta_3}+\frac{\Phi(P_{\rm u}/(\gamma\beta_3),\,\beta_1-\beta_3)}{\beta_3}, \tag{34}$$

which coincides with [25, Th. 3].

D. Asymptotic Approximation of Average Secrecy Rate

Theorem 2 shows that the random variable $R_{\rm S}/N_{\rm B}$ converges almost surely to a constant Ψ given in (26), as the number of antennas at each terminal goes to infinity. Hence, also the average normalized secrecy rate converges to the same constant, as stated in the following corollary.

Corollary 1: Under the same assumptions of Theorem 2,

$$\frac{\bar{R}_{\rm S}}{N_{\rm B}}\rightarrow\Psi, \tag{35}$$

where Ψ is given in (26). Then we can write that

$$\bar{R}_{\rm S}\approx N_{\rm B}\Psi\triangleq\bar{R}_{\rm S,Asym}. \tag{36}$$

for a sufficiently large number of antennas.

Proof: The proof is straightforward. ∎

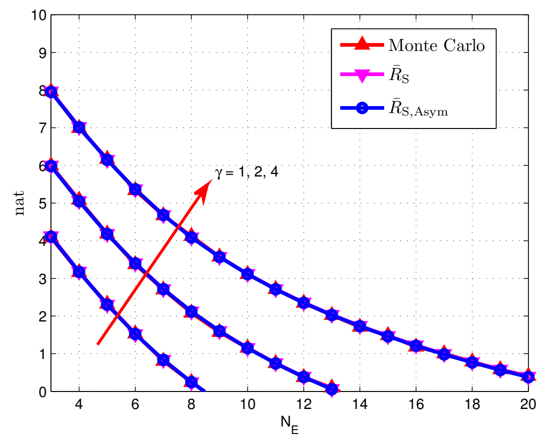

Fig. 1. $\bar{R}_{\mathrm{S}}$ vs. γ and N_{E} with $\alpha = 3$ dB, $\beta = -3$ dB, $N_{\mathrm{A}} = 6$ and $N_{\mathrm{B}} = 3$.

Corollary 1 provides an alternative way to evaluate $\bar{R}_{\mathrm{S}}$. To use the asymptotic approximation $\bar{R}_{\mathrm{S,Asym}}$ for a finite system model, we substitute in Ψ

$$\beta_1 = N_{\mathrm{A}}/N_{\mathrm{E}},\ \beta_2 = N_{\mathrm{A}}/N_{\mathrm{B}},\ \text{and}\ \beta_3 = N_{\mathrm{B}}/N_{\mathrm{E}}. \tag{37}$$

Remark 1: For finite system models, we verified by simulations that the difference between $\bar{R}_{\mathrm{S}}$ and $\bar{R}_{\mathrm{S,Asym}}$ is indistinguishable if

$$\min\left\{N_{\mathrm{A}}, N_{\mathrm{B}}, N_{\mathrm{A}} - N_{\mathrm{B}}, N_{\mathrm{E}}\right\} > 2. \tag{38}$$

Example 1: Let us apply Theorem 1 and Corollary 1 to the analysis of an AN scheme with $N_{\mathrm{A}} = 6$, $N_{\mathrm{B}} = 3$ and $\alpha = 3$ dB. Fig. 1 shows the value of $\bar{R}_{\mathrm{S}}$ with $\beta = -3$ dB, as a function of γ and N_{E}. In Fig. 2, we fix $\gamma = 3$ dB and verify the relationship between β, N_{E} and $\bar{R}_{\mathrm{S}}$. Both figures show an excellent agreement between the theoretically derived $\bar{R}_{\mathrm{S}}$ and Monte Carlo simulation and the asymptotic approximation $\bar{R}_{\mathrm{S,Asym}}$.

Moreover, Fig. 1 shows how $\bar{R}_{\mathrm{S}}$ increases with increasing γ and decreases with increasing N_{E}. In Fig. 2, we observe that increasing β (i.e., increasing AN power) has little effect on increasing $\bar{R}_{\mathrm{S}}$ when $N_{\mathrm{E}} > N_{\mathrm{A}}$.

E. Achieving Average Secrecy Capacity

The following theorem gives a sufficient condition for the achievability of the average secrecy capacity (12) using Gaussian input alphabets.

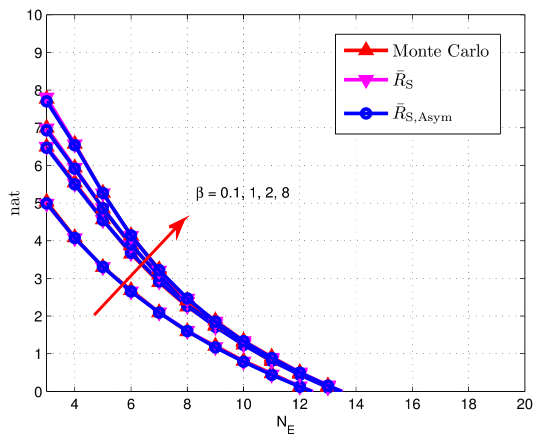

Fig. 2. $\bar{R}_{\mathrm{S}}$ vs. β and N_{E} with $\alpha = 3$ dB, $\gamma = 3$ dB, $N_{\mathrm{A}} = 6$ and $N_{\mathrm{B}} = 3$.

Theorem 3: If $N_{\mathrm{E}} \leq N_{\mathrm{A}} - N_{\mathrm{B}}$, as α, $\beta \to \infty$, then

$$\bar{C}_{\mathrm{S}} = \bar{R}_{\mathrm{S}} = \bar{C}_{\mathrm{Bob}}, \tag{39}$$

where $\bar{C}_{\mathrm{Bob}}$ represents Bob's average channel capacity.

Proof: See Appendix C. ∎

According to (12), a universal upper bound on the average MIMO secrecy capacity is given by

$$\bar{C}_{\mathrm{S}} \leq \max_{p(\mathbf{u})} \{I(\mathbf{u}; \mathbf{z}|\mathbf{H})\} = \bar{C}_{\mathrm{Bob}}. \tag{40}$$

Remark 2: Combining (39) and (40), we can show that the *maximum* average MIMO secrecy capacity is achieved by using the AN transmission scheme and Gaussian input alphabets, if N_{E} is not larger that $N_A - N_B$.

IV. Lower and Upper bounds on Secrecy Rate

To guarantee positive average/instantaneous secrecy rate, in this section, we present simple sufficient and necessary conditions, based upon lower and upper bounds on the average/instantaneous secrecy rate using Gaussian input alphabets.

A. Bounds on Average Secrecy Rate

The following theorem bounds $\bar{R}_{\mathrm{S}}$ given in (22).

Theorem 4:

$$\bar{R}_{\mathrm{LB}} \leq \bar{R}_{\mathrm{S}} \leq \bar{R}_{\mathrm{UB}}, \tag{41}$$

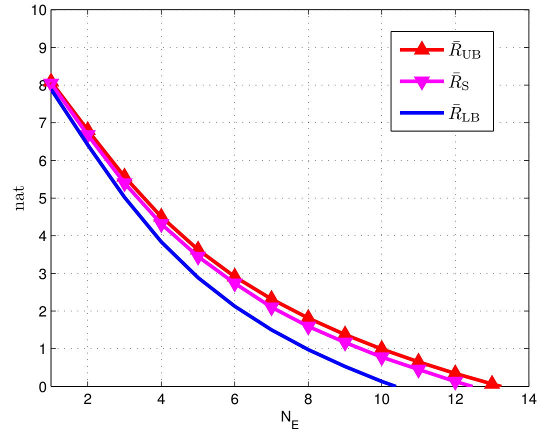

Fig. 3. $\bar{R}_{\rm S}$ and $\bar{R}_{\rm LB}$ vs. $N_{\rm E}$ with $\alpha = 3$ dB, $\beta = 1$ dB, $\gamma = 6$ dB, $N_{\rm B} = 3$ and $N_{\rm A} = 4$.

where the equality holds if $\beta = 1$,

$$\begin{aligned} \bar{R}_{\rm LB} &= \Theta(N_{\rm B}, N_{\rm A}, \alpha\gamma) + \Theta(N_{\min}, N_{\max}, \alpha\beta) \\ &\quad -\Theta(\hat{N}_{\min}, \hat{N}_{\max}, \theta_{\max}), \end{aligned} \tag{42}$$

$$\begin{aligned} \bar{R}_{\rm UB} &= \Theta(N_{\rm B}, N_{\rm A}, \alpha\gamma) + \Theta(N_{\min}, N_{\max}, \alpha\beta) \\ &\quad -\Theta(\hat{N}_{\min}, \hat{N}_{\max}, \theta_{\min}), \end{aligned} \tag{43}$$

$$\begin{aligned} \theta_{\min} &\triangleq \min\{\alpha, \alpha\beta\}, \\ \theta_{\max} &\triangleq \max\{\alpha, \alpha\beta\}, \end{aligned} \tag{44}$$

and $\Theta(\cdot,\cdot,\cdot)$ is given in (15).

Proof: See Appendix D. ■

Example 2: Fig. 3 compares the values of $\bar{R}_{\rm S}$, $\bar{R}_{\rm UB}$, $\bar{R}_{\rm LB}$ as functions of $N_{\rm E}$ with $\alpha = 3$ dB, $\beta = 1$ dB, $\gamma = 6$ dB, $N_{\rm B} = 3$ and $N_{\rm A} = 4$. Note that the upper and lower bounds are become tighter as β approaches 0 dB.

B. Bounds on Instantaneous Secrecy Rate

We then provide lower and upper bounds on the instantaneous secrecy rate $R_{\rm S}$ in (13) for high $\text{SNR}_{\rm B}$.

Theorem 5: Let N_{A}, N_{B}, $N_{\text{A}}-N_{\text{B}}$ and $N_{\text{E}}\to\infty$ with $N_{\text{A}}/N_{\text{E}}\to\beta_1$, $N_{\text{A}}/N_{\text{B}}\to\beta_2$, $N_{\text{B}}/N_{\text{E}}\to\beta_3$, and let $P_u, P_v\to\infty$, then almost surely (i.e., with probability one)

$$\begin{aligned} R_{\text{S}}/N_{\text{B}} &\geq \Delta(A_{\max}), \\ R_{\text{S}}/N_{\text{B}} &\leq \Delta(A_{\min}), \end{aligned} \tag{45}$$

where the equality (i.e., almost sure convergence to $\Delta(\cdot)$) holds if $\beta=1$,

$$\begin{aligned} \rho &\triangleq \beta_1-\beta_3, \\ A_{\min} &\triangleq \min\left\{\frac{P_{\text{v}}}{\gamma\rho},\frac{P_{\text{u}}}{\gamma\beta_3}\right\}, \\ A_{\max} &\triangleq \max\left\{\frac{P_{\text{v}}}{\gamma\rho},\frac{P_{\text{u}}}{\gamma\beta_3}\right\}, \end{aligned} \tag{46}$$

$$\Delta(x)\triangleq\left(\log P_{\text{u}}\beta_2-(\beta_2-1)\log\left(1-\beta_2^{-1}\right)-1\right)-F(x)+\Xi, \tag{47}$$

$$F(x)\triangleq\begin{cases}\beta_2\left(\log x-\dfrac{1-\beta_1}{\beta_1}\log\left(1-\beta_1\right)-1\right), & \beta_1\leq 1\\ \beta_3^{-1}\left(\log x\beta_1-(\beta_1-1)\log\left(1-\beta_1^{-1}\right)-1\right), & \beta_1>1\end{cases} \tag{48}$$

$$\Xi\triangleq\begin{cases}(\beta_2-1)\left(\log\dfrac{P_{\text{v}}}{\gamma\rho}-\dfrac{1-\rho}{\rho}\log\left(1-\rho\right)-1\right), & \rho\leq 1\\ \beta_3^{-1}\left(\log\dfrac{P_{\text{v}}}{\gamma}-(\rho-1)\log\left(1-\rho^{-1}\right)-1\right). & \rho>1\end{cases} \tag{49}$$

Proof: See Appendix E. ■

C. *Sufficient and Necessary Conditions for* $\bar{R}_S, R_S>0$

Theorem 5 shows that the random variable $R_{\text{S}}/N_{\text{B}}$ is almost surely bounded by the constant values $\Delta(A_{\max})$ and $\Delta(A_{\min})$ given in (50). Then the average normalized secrecy rate is also bounded by the same values, as stated in the following corollary.

Corollary 2: Under the same assumptions of Theorem 5,

$$\begin{aligned} \bar{R}_{\text{S}}/N_{\text{B}} &\geq \Delta(A_{\max}), \\ \bar{R}_{\text{S}}/N_{\text{B}} &\leq \Delta(A_{\min}), \end{aligned} \tag{50}$$

where $\Delta(\cdot)$ is given in (47). The equality holds if $\beta=1$.

Proof: The proof is straightforward. ■

The bounds in (45) and (50) enable the following simple sufficient and necessary conditions for positive instantaneous and average secrecy rate.

Corollary 3: Let N_{A}, N_{B}, $N_{\text{A}} - N_{\text{B}}$ and $N_{\text{E}} \to \infty$ with $N_{\text{A}}/N_{\text{E}} \to \beta_1$, $N_{\text{A}}/N_{\text{B}} \to \beta_2$ and $N_{\text{B}}/N_{\text{E}} \to \beta_3$. Then a sufficient condition for positive instantaneous and average secrecy rate is given by

$$\lim_{P_{\text{u}}, P_{\text{v}} \to \infty} \Delta(A_{\max}) > 0, \tag{51}$$

and a necessary condition for positive instantaneous and average secrecy rate is given by

$$\lim_{P_{\text{u}}, P_{\text{v}} \to \infty} \Delta(A_{\min}) > 0, \tag{52}$$

where $\Delta(\cdot)$ is given in (47).

Proof: The proof is straightforward. ■

To use Corollary 3 for finite (relatively small) SNR_{B} and number of antennas, we substitute in $\Delta(\cdot)$

$$\begin{aligned} &\beta_1 = N_{\text{A}}/N_{\text{E}},\ \beta_2 = N_{\text{A}}/N_{\text{B}},\ \beta_3 = N_{\text{B}}/N_{\text{E}}, \\ &P_{\text{u}} = \alpha\gamma N_{\text{B}} \text{ and } P_{\text{v}} = \alpha\beta\gamma(N_{\text{A}} - N_{\text{B}}). \end{aligned} \tag{53}$$

Thus $\Delta(\cdot)$ reduces to a function of N_{A}, N_{B}, N_{E}, α, β and γ.

Remark 3: We verified by simulation that Corollary 3 is accurate for finite system models, when

$$\begin{aligned} &\min\{\alpha\gamma, \alpha\beta\gamma\} \geq 4, \\ &\min\{N_{\text{A}}, N_{\text{B}}, N_{\text{A}} - N_{\text{B}}, N_{\text{E}}\} > 2. \end{aligned} \tag{54}$$

Example 3: We consider an AN scheme with $N_{\text{A}} = 6$, $N_{\text{B}} = 3$, $\alpha = \gamma = 3$ dB and $\beta = 1$ dB. Fig. 4 shows the value of $\bar{R}_{\text{S}}/N_{\text{B}}$, $\Delta(A_{\max})$ and $\Delta(A_{\min})$ as functions of N_{E}. By direct computation, $\Delta(A_{\max}) > 0$ until $N_{\text{E}} > 12$ and $\Delta(A_{\min}) < 0$ when $N_{\text{E}} > 16$. It was observed experimentally in Fig. 4 that $\bar{R}_{\text{S}} > 0$ when $N_{\text{E}} < 12$ and $\bar{R}_{\text{S}} = 0$ when $N_{\text{E}} > 16$.

Compared to the expressions in Theorems 1 and 2, the sufficient and necessary conditions for positive average/instantaneous secrecy rate in Corollary 3 are much easier to compute, and can be used for system design. For example, from Alice's perspective, given N_{A}, N_{B}, α, β and γ, she can easily predict the number of antennas Eve needs to drive the secrecy rate to zero.

V. Conclusions

In this paper, we have studied the artificial noise scheme in a situation where Eve has unlimited number of antennas. We derived closed-form expressions for the average secrecy rate and the asymptotic instantaneous secrecy rate. The proposed analysis allows a simple evaluation on the secrecy rate with any SNR_{B}, SNR_{E}, N_{A}, N_{B} and N_{E}, and extends previous studies that were limited to either the case of $N_{\text{E}} < N_{\text{A}}$ or the case of $N_{\text{B}} = 1$.

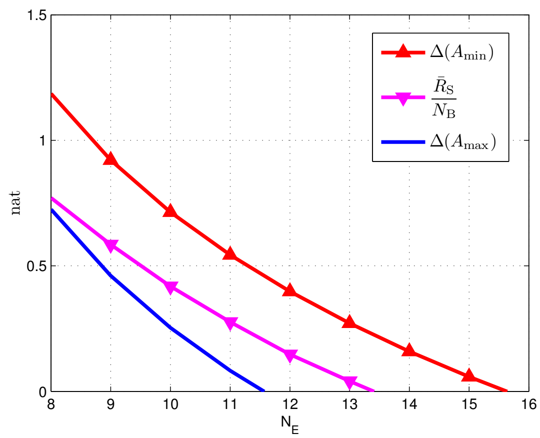

Fig. 4. Plot of $\bar{R}_{\mathrm{S}}$, $\Delta(A_{\max})$ and $\Delta(A_{\min})$ vs. N_{E} with $\alpha=\gamma=3$ dB, $\beta=1$ dB, $N_{\mathrm{B}}=3$ and $N_{\mathrm{A}}=6$.

In the second part of this paper, we have derived lower and upper bounds on the average/instantaneous secrecy rate. Moreover, simple sufficient and necessary conditions for positive average and instantaneous secrecy rate have been derived. These easily computable conditions provide Alice and Eve with design tools for choosing system parameters.

APPENDIX

A. Proof of Theorem 1

Recalling that

$$\bar{R}_{\mathrm{S}} = I(\mathbf{u};\mathbf{z}|\mathbf{H}) - I(\mathbf{u};\mathbf{y}|\mathbf{H},\mathbf{G}). \tag{55}$$

In what follows, we evaluate $I(\mathbf{u};\mathbf{z}|\mathbf{H})$ and $I(\mathbf{u};\mathbf{y}|\mathbf{H},\mathbf{G})$, respectively. We treat $\mathbf{H}$ and $\mathbf{G}$ as Gaussian random matrices.

1) $I(\mathbf{u};\mathbf{z}|\mathbf{H})$

Since $(\mathbf{H}\mathbf{V}_1)(\mathbf{H}\mathbf{V}_1)^H = \mathbf{H}\mathbf{H}^H$, using [21, Th. 2] and [23, Th. 1], we have

$$\begin{aligned} & I(\mathbf{u};\mathbf{z}|\mathbf{H}) \\ = \; & \mathrm{E}_{\mathbf{H}}\left(\log\left|\mathbf{I}_{N_{\mathrm{B}}} + \alpha\gamma\mathbf{H}\mathbf{H}^H\right|\right) \\ = \; & \Theta(N_{\mathrm{B}}, N_{\mathrm{A}}, \alpha\gamma), \end{aligned} \tag{56}$$

where $\Theta(x,y,z)$ is given in (15).

2) $I(\mathbf{u};\mathbf{y}|\mathbf{H},\mathbf{G})$

Since all entries in $\mathbf{H}$ and $\mathbf{G}$ are mutually independent, $I(\mathbf{u};\mathbf{y})$ can be expressed as a function of these independent random entries. This allows us to take two steps to compute the expected value of $I(\mathbf{u};\mathbf{y})$: we first compute $I(\mathbf{u};\mathbf{y}|\mathbf{G})$ given $\mathbf{H}$, then compute $\mathrm{E}_{\mathbf{H}}\left[I(\mathbf{u};\mathbf{y}|\mathbf{G})|\mathbf{H}\right]$. The advantage is that for given $\mathbf{H}$, $\mathbf{V}=[\mathbf{V}_1,\,\mathbf{Z}]$ is a fixed unitary matrix. Then, using [27, Th. 1], $\mathbf{G}\mathbf{V}_1$ and $\mathbf{G}\mathbf{Z}$ are mutually independent complex Gaussian random matrices with i.i.d. entries $\sim\mathcal{N}_{\mathbb{C}}(0,\,1)$.

Let $\mathbf{G}_1=\mathbf{G}\mathbf{V}_1$, $\mathbf{G}_2=\mathbf{G}\mathbf{Z}$, $\mathbf{W}_1$= $\mathbf{G}_1\mathbf{G}_1^H$ and $\mathbf{W}_2$= $\mathbf{G}_2\mathbf{G}_2^H$. According to [21], for given $\mathbf{H}$, we have

$$
\begin{aligned}
& I(\mathbf{u};\mathbf{y}|\mathbf{G}) \\
&= \mathrm{E}_{\mathbf{G}_1,\mathbf{G}_2}\left(\log\frac{\left|\mathbf{I}_{N_{\mathrm{E}}}\sigma_{\mathrm{E}}^2+\sigma_{\mathrm{u}}^2\mathbf{W}_1+\sigma_{\mathrm{v}}^2\mathbf{W}_2\right|}{\left|\mathbf{I}_{N_{\mathrm{E}}}\sigma_{\mathrm{E}}^2+\sigma_{\mathrm{v}}^2\mathbf{W}_2\right|}\right) \\
&= \mathrm{E}_{\mathbf{G}_1,\mathbf{G}_2}\left(\log\frac{\left|\mathbf{I}_{N_{\mathrm{E}}}+\frac{\sigma_{\mathrm{u}}^2}{\sigma_{\mathrm{E}}^2}\mathbf{W}_1+\frac{\sigma_{\mathrm{v}}^2}{\sigma_{\mathrm{E}}^2}\mathbf{W}_2\right|}{\left|\mathbf{I}_{N_{\mathrm{E}}}+\frac{\sigma_{\mathrm{v}}^2}{\sigma_{\mathrm{E}}^2}\mathbf{W}_2\right|}\right) \\
&= \mathrm{E}_{\mathbf{G}_1,\mathbf{G}_2}\left(\log\left|\mathbf{I}_{N_{\mathrm{E}}}+\alpha\mathbf{W}_1+\alpha\beta\mathbf{W}_2\right|\right)-\mathrm{E}_{\mathbf{G}_2}\left(\log\left|\mathbf{I}_{N_{\mathrm{E}}}+\alpha\beta\mathbf{W}_2\right|\right).
\end{aligned}
\tag{57}
$$

According to [21, Th. 2] and [23, Th. 1], the second term of (57) equals to

$$
\mathrm{E}_{\mathbf{G}_2}\left(\log\left|\mathbf{I}_{N_{\mathrm{E}}}+\alpha\beta\mathbf{W}_2\right|\right)=\Theta(N_{\min},N_{\max},\alpha\beta),
\tag{58}
$$

where $\Theta(x,y,z)$, $N_{\min}$ and $N_{\max}$ are given in (15), (17) and (18), respectively.

To compute the first term of (57), we rewrite $\alpha\mathbf{W}_1+\alpha\beta\mathbf{W}_2$ as $\mathbf{G}_3\boldsymbol{\Delta}\mathbf{G}_3^H$, where

$$
\mathbf{G}_3=\left[\mathbf{G}_1,\mathbf{G}_2\right],
\tag{59}
$$

$$
\boldsymbol{\Delta}=\mathrm{diag}\left(\{\theta_i\}_1^{N_{\mathrm{A}}}\right).
\tag{60}
$$

θ_i is defined in (21). We define

$$
\Omega=\mathrm{E}_{\mathbf{G}_1,\mathbf{G}_2}\left(\log\left|\mathbf{I}_{N_{\mathrm{E}}}+\alpha\mathbf{W}_1+\alpha\beta\mathbf{W}_2\right|\right).
\tag{61}
$$

Case 1: If $\beta=1$, using [21, Th. 2] and [23, Th. 1], we have

$$
\Omega=\mathrm{E}_{\mathbf{G}_3}\left(\log\left|\mathbf{I}_{N_{\mathrm{E}}}+\alpha\mathbf{G}_3\mathbf{G}_3^H\right|\right)=\Theta(\hat{N}_{\min},\hat{N}_{\max},\alpha),
\tag{62}
$$

where $\mathbf{G}_3$, $\hat{N}_{\min}$ and $\hat{N}_{\max}$ are given in (59), (19) and (20), respectively.

Case 2: If $\beta\neq 1$, $\boldsymbol{\Delta}^{-1}$ contains two groups of coinciding eigenvalues. According to [24, Th. 1], we have

$$
\Omega=\mathrm{E}_{\mathbf{G}_3}\left(\log\left|\mathbf{I}_{N_{\mathrm{E}}}+\mathbf{G}_3\boldsymbol{\Delta}\mathbf{G}_3^H\right|\right)=K\sum_{k=1}^{\hat{N}_{\min}}\det\left(\mathbf{R}^{(k)}\right),
\tag{63}
$$

where K and $\mathbf{R}^{(k)}$ are given in (24) and (25), respectively.

Based on (57), (58), (62) and (63), we have

$$\begin{aligned} & I(\mathbf{u};\mathbf{y}|\mathbf{H},\mathbf{G}) \\ = \; & \mathrm{E}_{\mathbf{H}}\left(I(\mathbf{u};\mathbf{y}|\mathbf{G})|\mathbf{H}\right) \\ = \; & \Omega - \Theta(N_{\min}, N_{\max}, \alpha\beta). \end{aligned} \tag{64}$$

By substituting (64) and (56) into (55), we have

$$\bar{R}_{\mathrm{S}} = \Theta(N_{\mathrm{B}}, N_{\mathrm{A}}, \alpha\gamma) + \Theta(N_{\min}, N_{\max}, \alpha\beta) - \Omega. \tag{65}$$

■

B. Proof of Theorem 2

Recalling that

$$R_{\mathrm{S}} = I(\mathbf{u};\mathbf{z}) - I(\mathbf{u};\mathbf{y}). \tag{66}$$

In what follows, we evaluate $I(\mathbf{u};\mathbf{z})$ and $I(\mathbf{u};\mathbf{y})$, respectively.

1) $I(\mathbf{u};\mathbf{z})$

Similarly to (56), we have

$$I(\mathbf{u};\mathbf{z}) = \log\left|\mathbf{I}_{N_{\mathrm{B}}} + \alpha\gamma\mathbf{H}\mathbf{H}^{H}\right|. \tag{67}$$

Since Alice knows the realization of $\mathbf{H}$, she is able to compute the deterministic value of $I(\mathbf{u};\mathbf{z})$. As N_{A} and $N_{\mathrm{B}} \to \infty$ with $N_{\mathrm{A}}/N_{\mathrm{B}} \to \beta_2$, the following limit holds [26, Eq. 1.14]

$$\frac{I(\mathbf{u};\mathbf{z})}{N_{\mathrm{B}}} \to \Phi\left(P_{\mathrm{u}},\, \beta_2\right), \tag{68}$$

where $\Phi\left(x,\, y\right)$ is given in (27).

2) $I(\mathbf{u};\mathbf{y})$

Similarly to (57), we have

$$I(\mathbf{u};\mathbf{y}) = \log\left|\mathbf{I}_{N_{\mathrm{E}}} + \alpha\mathbf{W}_1 + \alpha\beta\mathbf{W}_2\right| - \log\left|\mathbf{I}_{N_{\mathrm{E}}} + \alpha\beta\mathbf{W}_2\right|, \tag{69}$$

where $\mathbf{G}_1 = \mathbf{G}\mathbf{V}_1$, $\mathbf{G}_2 = \mathbf{G}\mathbf{Z}$, $\mathbf{W}_1 = \mathbf{G}_1\mathbf{G}_1^H$ and $\mathbf{W}_2 = \mathbf{G}_2\mathbf{G}_2^H$.

From Alice side, $\mathbf{V} = [\mathbf{V}_1,\, \mathbf{Z}]$ is a fixed unitary matrix and $\mathbf{G}$ is a Gaussian random matrix. Using [27, Th. 1], $\mathbf{G}_1$ and $\mathbf{G}_2$ are mutually independent complex Gaussian random matrices with i.i.d. entries $\sim \mathcal{N}_{\mathbb{C}}(0,\, 1)$.

According to [26, Eq. 1.14], as $N_{\rm A}-N_{\rm B}$ and $N_{\rm E}\to\infty$ with $N_{\rm A}/N_{\rm E}\to\beta_1$ and $N_{\rm B}/N_{\rm E}\to\beta_3$, i.e., $(N_{\rm A}-N_{\rm B})/N_{\rm E}\to\beta_1-\beta_3$,

$$\frac{\log|\mathbf{I}_{N_{\rm E}}+\alpha\beta\mathbf{W}_2|}{N_{\rm E}}\overset{a.s.}{\to}\Phi\left(\frac{P_{\rm v}}{\gamma(\beta_1-\beta_3)},\,\beta_1-\beta_3\right). \tag{70}$$

Let $\mathbf{W}_3=\alpha\mathbf{W}_1+\alpha\beta\mathbf{W}_2$. We can rewrite $\mathbf{W}_3$ as $\hat{\mathbf{G}}_3\mathbf{T}\hat{\mathbf{G}}_3^H$, where

$$\hat{\mathbf{G}}_3=\left[\frac{1}{\sqrt{N_{\rm E}}}\mathbf{G}_1,\frac{1}{\sqrt{N_{\rm E}}}\mathbf{G}_2\right], \tag{71}$$

$$\mathbf{T}=N_{\rm E}\mathrm{diag}\left(\{\theta_i\}_1^{N_{\rm A}}\right), \tag{72}$$

where the θ_i's are given in (21). Note that the entries of $\hat{\mathbf{G}}_3$ are i.i.d. complex random variables $\sim\mathcal{N}_{\mathbb{C}}(0,1/N_{\rm E})$.

According to [26, Th. 2.39], as $N_{\rm A}$ and $N_{\rm E}\to\infty$ with $N_{\rm A}/N_{\rm E}\to\beta_1$,

$$\frac{\log|\mathbf{I}_{N_{\rm E}}+\mathbf{W}_3|}{N_{\rm E}}\overset{a.s.}{\to}\beta_1\mathcal{V}(\delta)-\log\delta+\delta-1, \tag{73}$$

where $\mathcal{V}(\delta)$ is given in (29) and δ satisfies

$$\beta_1=\frac{1-\delta}{1-\eta(\delta)}, \tag{74}$$

with $\eta(\delta)$ given in (31).

From (68), (70) and (73), as $N_{\rm A}$, $N_{\rm B}$, $N_{\rm A}-N_{\rm B}$ and $N_{\rm E}\to\infty$ with $N_{\rm A}/N_{\rm E}\to\beta_1$, $N_{\rm A}/N_{\rm B}\to\beta_2$ and $N_{\rm B}/N_{\rm E}\to\beta_3$,

$$\frac{R_{\rm S}}{N_{\rm B}}\overset{a.s.}{\to}\Psi, \tag{75}$$

where the constant Ψ is given in (26). ■

C. *Proof of Theorem 3*

We first show that using Gaussian input alphabets, if $N_{\rm E}\le N_{\rm A}-N_{\rm B}$, $I(\mathbf{u};\mathbf{y}|\mathbf{H},\mathbf{G})\to 0$ as α, $\beta\to\infty$. We follow the definitions in the proof of Theorem 1. Based on (57), for a given realization of $\mathbf{H}$, we have

$$\begin{aligned}
&I(\mathbf{u};\mathbf{y}|\mathbf{G})\\
&=\mathrm{E}_{\mathbf{G}_1,\mathbf{G}_2}\left(\log\frac{\left|\mathbf{I}_{N_{\rm E}}\sigma_{\rm E}^2+\sigma_{\rm u}^2\mathbf{W}_1+\sigma_{\rm v}^2\mathbf{W}_2\right|}{\left|\mathbf{I}_{N_{\rm E}}\sigma_{\rm E}^2+\sigma_{\rm v}^2\mathbf{W}_2\right|}\right)\\
&\overset{a}{\le}\mathrm{E}_{\mathbf{G}_2}\left(\log\frac{\left|\mathbf{I}_{N_{\rm E}}\sigma_{\rm E}^2+\sigma_{\rm u}^2\mathrm{E}_{\mathbf{G}_1}\left(\mathbf{W}_1\right)+\sigma_{\rm v}^2\mathbf{W}_2\right|}{\left|\mathbf{I}_{N_{\rm E}}\sigma_{\rm E}^2+\sigma_{\rm v}^2\mathbf{W}_2\right|}\right)\\
&=\mathrm{E}_{\mathbf{G}_2}\left(\log\frac{\left|\mathbf{I}_{N_{\rm E}}+\frac{\sigma_{\rm v}^2}{\sigma_{\rm E}^2+N_{\rm B}\sigma_{\rm u}^2}\mathbf{W}_2\right|}{\left|\mathbf{I}_{N_{\rm E}}+\frac{\sigma_{\rm v}^2}{\sigma_{\rm E}^2}\mathbf{W}_2\right|}\right)+N_{\rm E}\log\frac{\sigma_{\rm E}^2+N_{\rm B}\sigma_{\rm u}^2}{\sigma_{\rm E}^2},
\end{aligned} \tag{76}$$

where (a) holds due to the concavity of log-determinant function and Jensen's inequality.

Let

$$\mathbf{W} = \begin{cases} \mathbf{G}_2\mathbf{G}_2^H & \text{if } N_{\rm E} \leq N_{\rm A} - N_{\rm B} \\ \mathbf{G}_2^H\mathbf{G}_2 & \text{if } N_{\rm E} > N_{\rm A} - N_{\rm B} \end{cases},$$

i.e., $\mathbf{W} \sim W_{N_{\min}}(N_{\max}, \mathbf{I}_{N_{\min}})$.

Recalling the definitions of α and β in Sec. II.C, and based on Sylvester's determinant theorem and [23, Th. 1], the first term of (76) can be rewritten as

$$\begin{aligned} &\mathrm{E}_{\mathbf{G}_2}\left(\log\frac{\left|\mathbf{I}_{N_{\min}} + \frac{\alpha\beta}{1+\alpha N_{\rm B}}\mathbf{W}\right|}{\left|\mathbf{I}_{N_{\min}} + \alpha\beta\mathbf{W}\right|}\right) \\ &= \Theta(N_{\min}, N_{\max}, \alpha\beta/(1+\alpha N_{\rm B})) - \Theta(N_{\min}, N_{\max}, \alpha\beta) \end{aligned} \tag{77}$$

where $\Theta(x, y, z)$ is given in (15).

From (76) and (77), we have

$$\begin{aligned} I(\mathbf{u}; \mathbf{y}|\mathbf{H}, \mathbf{G}) &= \mathrm{E}_{\mathbf{H}}\left[I(\mathbf{u}; \mathbf{y}|\mathbf{G})|\mathbf{H}\right] \\ &\leq N_{\rm E}\log(1+\alpha N_{\rm B}) - \Theta(N_{\min}, N_{\max}, \alpha\beta) \\ &\quad +\Theta(N_{\min}, N_{\max}, \alpha\beta/(1+\alpha N_{\rm B})) \\ &= (N_{\rm E} - N_{\min})\log\alpha N_{\rm B} + O\left(\frac{1}{\alpha}\right) + O\left(\frac{1}{\beta}\right). \end{aligned} \tag{78}$$

Based on (78), if $N_{\min} = N_{\rm E}$, i.e., $N_{\rm E} \leq N_{\rm A} - N_{\rm B}$, as α and $\beta \to \infty$,

$$I(\mathbf{u}; \mathbf{y}|\mathbf{H}, \mathbf{G}) = 0. \tag{79}$$

Under the same conditions, by substituting (79) into (14), we have

$$\bar{R}_{\rm S} = I(\mathbf{u}; \mathbf{z}|\mathbf{H}) = \bar{C}_{\rm Bob}, \tag{80}$$

where $\bar{C}_{\rm Bob}$ represents Bob's average channel capacity. The last equation holds since the input $\mathbf{u}$ is a circularly symmetric complex Gaussian random vector with zero mean and covariance $\sigma_{\rm u}^2\mathbf{I}_{N_{\rm B}}$ [21, Th. 1].

On the other hand, from (12), we have

$$\bar{C}_{\rm S} \leq \max_{p(\mathbf{u})}\{I(\mathbf{u}; \mathbf{z}|\mathbf{H})\} = \bar{C}_{\rm Bob}. \tag{81}$$

Based on (80) and (81), as α, $\beta \to \infty$, if $N_{\rm E} \leq N_{\rm A} - N_{\rm B}$,

$$\bar{C}_{\rm S} = \bar{R}_{\rm S} = \bar{C}_{\rm Bob}. \tag{82}$$

■

D. Proof of Theorem 4

We follow the definitions in the proof of Theorem 1. We first bound the term Ω in the expression of $\bar{R}_{\rm S}$ given in (26). Recalling that

$$\Omega = \mathrm{E}_{\mathbf{G}_1,\mathbf{G}_2}\left(\log\left|\mathbf{I}_{N_{\rm E}} + \alpha\mathbf{W}_1 + \alpha\beta\mathbf{W}_2\right|\right). \tag{83}$$

Let $\theta_{\min} = \min\{\alpha, \alpha\beta\}$ and $\theta_{\max} = \max\{\alpha, \alpha\beta\}$. Since $\mathbf{W}_1$ and $\mathbf{W}_2$ are positive semidefinite matrices, using [28, Eq. 12, pp. 55], we have

$$\begin{aligned} & \left|\mathbf{I}_{N_{\rm E}} + \alpha\mathbf{W}_1 + \alpha\beta\mathbf{W}_2\right| \\ \geq\ & \left|\mathbf{I}_{N_{\rm E}} + \theta_{\min}(\mathbf{W}_1 + \mathbf{W}_2)\right| \\ =\ & \left|\mathbf{I}_{N_{\rm E}} + \theta_{\min}\mathbf{G}_3\mathbf{G}_3^H\right|, \end{aligned} \tag{84}$$

and

$$\begin{aligned} & \left|\mathbf{I}_{N_{\rm E}} + \alpha\mathbf{W}_1 + \alpha\beta\mathbf{W}_2\right| \\ \leq\ & \left|\mathbf{I}_{N_{\rm E}} + \theta_{\max}(\mathbf{W}_1 + \mathbf{W}_2)\right| \\ =\ & \left|\mathbf{I}_{N_{\rm E}} + \theta_{\max}\mathbf{G}_3\mathbf{G}_3^H\right|, \end{aligned} \tag{85}$$

where $\mathbf{G}_3$, $\hat{N}_{\min}$ and $\hat{N}_{\max}$ are given in (59), (19) and (20), respectively. The equality holds if $\beta = 1$.

Based on (83), (84) and (85), using [21, Th. 2] and [23, Th. 1], we have

$$\Theta(\hat{N}_{\min}, \hat{N}_{\max}, \theta_{\min}) \leq \Omega \leq \Theta(\hat{N}_{\min}, \hat{N}_{\max}, \theta_{\max}), \tag{86}$$

where $\Theta(x, y, z)$ is given in (15).

By substituting (86) into (22), we have

$$\bar{R}_{\rm LB} \leq \bar{R}_{\rm S} \leq \bar{R}_{\rm UB},$$

where

$$\begin{aligned} \bar{R}_{\rm LB} \ =\ & \Theta(N_{\rm B}, N_{\rm A}, \alpha\gamma) + \Theta(N_{\min}, N_{\max}, \alpha\beta) \\ & -\Theta(\hat{N}_{\min}, \hat{N}_{\max}, \theta_{\max}), \end{aligned} \tag{87}$$

$$\begin{aligned} \bar{R}_{\rm UB} \ =\ & \Theta(N_{\rm B}, N_{\rm A}, \alpha\gamma) + \Theta(N_{\min}, N_{\max}, \alpha\beta) \\ & -\Theta(\hat{N}_{\min}, \hat{N}_{\max}, \theta_{\min}). \end{aligned} \tag{88}$$

■

E. Proof of Theorem 5

We follow the definitions in the proofs of Theorems 1 and 4. Based on (67), (69), (84) and (85), we have

$$\begin{aligned} R_{\mathrm{S}} \geq & \log\left|\mathbf{I}_{N_{\mathrm{B}}}+\alpha\gamma\mathbf{H}\mathbf{H}^{H}\right|+\log\left|\mathbf{I}_{N_{\mathrm{E}}}+\alpha\beta\mathbf{W}_{2}\right| \\ & -\left|\mathbf{I}_{N_{\mathrm{E}}}+\theta_{\max}\mathbf{G}_{3}\mathbf{G}_{3}^{H}\right| \triangleq R_{\mathrm{LB}}, \end{aligned} \tag{89}$$

$$\begin{aligned} R_{\mathrm{S}} \leq & \log\left|\mathbf{I}_{N_{\mathrm{B}}}+\alpha\gamma\mathbf{H}\mathbf{H}^{H}\right|+\log\left|\mathbf{I}_{N_{\mathrm{E}}}+\alpha\beta\mathbf{W}_{2}\right| \\ & -\left|\mathbf{I}_{N_{\mathrm{E}}}+\theta_{\min}\mathbf{G}_{3}\mathbf{G}_{3}^{H}\right| \triangleq R_{\mathrm{UB}}. \end{aligned} \tag{90}$$

The equality of the random variables $R_{\mathrm{S}}=R_{\mathrm{LB}}=R_{\mathrm{UB}}$ holds if $\beta=1$, since $\theta_{\min}=\theta_{\max}$.

We then evaluate R_{LB} and R_{UB}. For convenience, we define

$$\begin{aligned} \rho &\triangleq \beta_1-\beta_3, \\ A_{\min} &\triangleq \min\left\{\frac{P_{\mathrm{v}}}{\gamma\rho},\frac{P_{\mathrm{u}}}{\gamma\beta_3}\right\}, \\ A_{\max} &\triangleq \max\left\{\frac{P_{\mathrm{v}}}{\gamma\rho},\frac{P_{\mathrm{u}}}{\gamma\beta_3}\right\}. \end{aligned}$$

Similarly to the proof in Theorem 2, using [26, Eq. 1.14], as N_{A}, N_{B}, $N_{\mathrm{A}}-N_{\mathrm{B}}$ and $N_{\mathrm{E}}\to\infty$ with $N_{\mathrm{A}}/N_{\mathrm{E}}\to\beta_1$, $N_{\mathrm{A}}/N_{\mathrm{B}}\to\beta_2$ and $N_{\mathrm{B}}/N_{\mathrm{E}}\to\beta_3$,

$$\frac{\log\left|\mathbf{I}_{N_{\mathrm{B}}}+\alpha\gamma\mathbf{H}\mathbf{H}^{H}\right|}{N_{\mathrm{B}}}\xrightarrow{a.s.}\Phi\left(P_{\mathrm{u}},\,\beta_2\right), \tag{91}$$

$$\frac{\log\left|\mathbf{I}_{N_{\mathrm{E}}}+\alpha\beta\mathbf{W}_{2}\right|}{N_{\mathrm{E}}}\xrightarrow{a.s.}\Phi\left(\frac{P_{\mathrm{v}}}{\gamma\rho},\,\rho\right), \tag{92}$$

$$\frac{\left|\mathbf{I}_{N_{\mathrm{E}}}+\theta_{\max}\mathbf{G}_{3}\mathbf{G}_{3}^{H}\right|}{N_{\mathrm{E}}}\xrightarrow{a.s.}\Phi\left(A_{\max},\,\beta_1\right), \tag{93}$$

$$\frac{\left|\mathbf{I}_{N_{\mathrm{E}}}+\theta_{\min}\mathbf{G}_{3}\mathbf{G}_{3}^{H}\right|}{N_{\mathrm{E}}}\xrightarrow{a.s.}\Phi\left(A_{\min},\,\beta_1\right), \tag{94}$$

where $\Phi\left(x,y\right)$ is given in (27).

We then evaluate the function $\Phi\left(x,y\right)$. From (27), since $\mathcal{F}\left(x,y\right)=\mathcal{F}\left(xy,y^{-1}\right)$, it is easy to show the following property

$$\Phi\left(x,y\right)=\frac{\Phi\left(xy,y^{-1}\right)}{y^{-1}}. \tag{95}$$

Recalling [26, Examples 2.14&2.15], if $y\leq 1$,

$$\lim_{x\to\infty}\left(\log x-\frac{\Phi(x,\,y)}{y}\right)=\frac{1-y}{y}\log\left(1-y\right)+1. \tag{96}$$

Using (95) and (96), we have the following results on the non random quantities $\Phi(P_{\rm u}, \beta_2)$, $\Phi(P_{\rm v}/(\gamma\rho), \rho)$, $\Phi\left(A_{\max}, \beta_1\right)$ and $\Phi\left(A_{\min}, \beta_1\right)$.

Since $\beta_2 > 1$, i.e., $N_{\rm A} > N_{\rm B}$,

$$\begin{aligned}
&\lim_{P_{\rm u}\to\infty} \left(\log P_{\rm u}\beta_2 - \Phi(P_{\rm u},\, \beta_2)\right) \\
=\;& \lim_{P_{\rm u}\to\infty} \left(\log P_{\rm u}\beta_2 - \frac{\Phi(P_{\rm u}\beta_2,\, \beta_2^{-1})}{\beta_2^{-1}}\right) \\
=\;& (\beta_2 - 1)\log\left(1 - \beta_2^{-1}\right) + 1. \qquad (97)
\end{aligned}$$

If $\rho \leq 1$,

$$\begin{aligned}
&\lim_{P_{\rm v}\to\infty} \left(\log\frac{P_{\rm v}}{\gamma\rho} - \frac{\Phi\left(P_{\rm v}/(\gamma\rho),\, \rho\right)}{\rho}\right) \\
=\;& \frac{1-\rho}{\rho}\log\left(1-\rho\right) + 1. \qquad (98)
\end{aligned}$$

If $\rho > 1$,

$$\begin{aligned}
&\lim_{P_{\rm v}\to\infty} \left(\log\frac{P_{\rm v}}{\gamma} - \Phi\left(\frac{P_{\rm v}}{\gamma\rho},\, \rho\right)\right) \\
=\;& \lim_{P_{\rm v}\to\infty} \left(\log\frac{P_{\rm v}}{\gamma} - \frac{\Phi\left(P_{\rm v}/\gamma,\, \rho^{-1}\right)}{\rho^{-1}}\right) \\
=\;& (\rho - 1)\log\left(1 - \rho^{-1}\right) + 1. \qquad (99)
\end{aligned}$$

If $\beta_1 \leq 1$,

$$\lim_{P_{\rm u}, P_{\rm v}\to\infty} \left(\log A_{\max} - \frac{\Phi\left(A_{\max},\, \beta_1\right)}{\beta_1}\right) = \frac{1-\beta_1}{\beta_1}\log\left(1-\beta_1\right) + 1, \qquad (100)$$

$$\lim_{P_{\rm u}, P_{\rm v}\to\infty} \left(\log A_{\min} - \frac{\Phi\left(A_{\min},\, \beta_1\right)}{\beta_1}\right) = \frac{1-\beta_1}{\beta_1}\log\left(1-\beta_1\right) + 1. \qquad (101)$$

If $\beta_1 > 1$,

$$\begin{aligned}
&\lim_{P_{\rm u}, P_{\rm v}\to\infty} \left(\log A_{\max}\beta_1 - \Phi\left(A_{\max},\, \beta_1\right)\right) \\
=\;& \lim_{P_{\rm u}, P_{\rm v}\to\infty} \left(\log A_{\max}\beta_1 - \frac{\Phi\left(A_{\max}\beta_1,\, \beta_1^{-1}\right)}{\beta_1^{-1}}\right) \\
=\;& (\beta_1 - 1)\log\left(1 - \beta_1^{-1}\right) + 1, \qquad (102)
\end{aligned}$$

$$\begin{aligned}
&\lim_{P_{\rm u}, P_{\rm v}\to\infty} \left(\log A_{\min}\beta_1 - \Phi\left(A_{\min},\, \beta_1\right)\right) \\
=\;& \lim_{P_{\rm u}, P_{\rm v}\to\infty} \left(\log A_{\min}\beta_1 - \frac{\Phi\left(A_{\min}\beta_1,\, \beta_1^{-1}\right)}{\beta_1^{-1}}\right) \\
=\;& (\beta_1 - 1)\log\left(1 - \beta_1^{-1}\right) + 1. \qquad (103)
\end{aligned}$$

Based on the above analysis, as N_{A}, N_{B}, $N_{\mathrm{A}} - N_{\mathrm{B}}$, $N_{\mathrm{E}} \to \infty$ with $N_{\mathrm{A}}/N_{\mathrm{E}} \to \beta_1$, $N_{\mathrm{A}}/N_{\mathrm{B}} \to \beta_2$ and $N_{\mathrm{B}}/N_{\mathrm{E}} \to \beta_3$, and for $P_{\mathrm{u}}, P_{\mathrm{v}} \to \infty$

$$\begin{aligned} R_{\mathrm{LB}}/N_{\mathrm{B}} &\overset{a.s.}{\to} \Delta(A_{\max}), \\ R_{\mathrm{UB}}/N_{\mathrm{B}} &\overset{a.s.}{\to} \Delta(A_{\min}), \end{aligned} \tag{104}$$

where $\Delta(\cdot)$ is given in (47).

Using (89), (90) and (104), under the above conditions, we have (45). ■

REFERENCES

[1] W. Diffie and M. E. Hellman, "New directions in cryptography," *IEEE Trans. Inf. Theory*, vol. 22, no. 6, pp. 644–654, Nov. 1976.

[2] S. Goldwasser and S. Micali, "Probabilistic encryption," in *Journal of Computer and System Sience*, vol. 28, no. 2, 1984, pp. 270–299.

[3] J. Hoffstein, J. Pipher, and J. H. Silverman, "NTRU: a ring based public key cryptosystem," in *Proc. ANTS-III*, ser. LNCS, vol. 1423, Springer, Jun. 1998, pp. 267–288.

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

[5] S. K. Leung-Yan-Cheong and M. E. Hellman, "The Gaussian wire-tap channel," *IEEE Trans. Inf. Theory*, vol. 24, no. 4, pp. 451–456, Jul. 1978.

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

[7] M. Bloch, J. Barros, M. Rodrigues, and S. McLaughlin, "Wireless information-theoretic security," *IEEE Trans. Inf. Theory*, vol. 54, no. 6, pp. 2515–2534, Jun. 2008.

[8] Y. Liang, H. V. Poor, and S. Shamai, "Secure communication over fading channels," *IEEE Trans. Inf. Theory*, vol. 54, no. 6, pp. 2470–2492, Jun. 2008.

[9] Y. Liang and H. V. Poor, "Multiple-access channels with confidential messages," *IEEE Trans. Inf. Theory*, vol. 54, no. 3, pp. 976–1002, 2008.

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

[11] S. Goel and R. Negi, "Guaranteeing secrecy using artificial noise," *IEEE Trans. Wireless Commun.*, vol. 7, pp. 2180–2189, Jun. 2008.

[12] I. Csiszár, "Almost independence and secrecy capacity," *Problems of Information Transmission*, vol. 32, pp. 40–47, 1996.

[13] H. Mahdavifar and A. Vardy, "Achieving the secrecy capacity of wiretap channels using polar codes," *IEEE Trans. Inf. Theory*, vol. 57, no. 10, p. 6428C6443, 2011.

[14] C. Ling, L. Luzzi, J.-C. Belfiore, and D. Stehlé, "Semantically secure lattice codes for the Gaussian wiretap channel," Oct. 2012, available on arXiv1210.6673.

[15] F. Oggier, P. Solé, and J.-C. Belfiore, "Lattice codes for the wiretap Gaussian channel: Construction and analysis," Mar. 2011, available on arXiv1103.4086.

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

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

[18] M. Pei, J. Wei, K.-K. Wong, and X. Wang, "Masked beamforming for multiuser MIMO wiretap channels with imperfect CSI," *IEEE Trans. Wireless Commun.*, vol. 11, no. 2, pp. 544–549, Feb. 2012.

[19] S. Liu, Y. Hong, and E. Viterbo, "Practical secrecy using artificial noise," *IEEE Communications Letters*, vol. 17, no. 7, pp. 1483–1486, 2013.

[20] X. Zhang, X. Zhou, and M. R. McKay, "Enhancing secrecy with multi-antenna transmission in wireless Ad Hoc networks," *IEEE Trans. Inf. Forensics Security*, vol. 8, no. 11, pp. 1802–1814, 2013.

[21] E. Telatar, "Capacity of multi-antenna Gaussian channels," *European Transactions on Telecommunications*, vol. 10, no. 6, pp. 585–595, 1999.

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

[23] H. Shin and J. H. Lee, "Closed-form formulas for ergodic capacity of MIMO Rayleigh fading channels," in *Proc. IEEE Int. Conf. Commun. (ICC'03)*, Anchorage, US, May 2003, pp. 2996–3000.

[24] M. Chiani, M. Z. Win, and H. Shin, "MIMO networks: The effects of interference," *IEEE Trans. Inf. Theory*, vol. 56, no. 1, pp. 336–349, 2010.

[25] S. Liu, Y. Hong, and E. Viterbo, "Artificial noise revisited: When Eve has more antennas than Alice," submitted to *IEEE Int. Conf. Signal Process. Commun.* (SPCOM'14).

[26] A. M. Tulino and S. Verdú, *Random Matrix Theory and Wireless Communications*. North America: Now Publishers Inc., 2004.

[27] E. Lukacs and E. P. King, "A property of the normal distribution," *Ann. Math. Statist.*, vol. 25, no. 2, pp. 389–394, 1954.

[28] H. Lütkepohl, *Handbook of matrices*. John Wiley and Sons, 1996.