Artificial Noise Revisited

Shuiyin Liu, *Member, IEEE*, Yi Hong, *Senior Member, IEEE*, and Emanuele Viterbo, *Fellow, IEEE*

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 multiple-output multiple-input 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, secret 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 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, Liang *et al.* [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., $N_E < N_A$ [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 $\lim \sup_{x \to \infty} |f(x)/g(x)| < \infty$. $\lceil x \rfloor$ 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 Σ, is defined as $\mathbf{A} \backsim W_m(n, \Sigma)$. 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

$$\mathbf{z} = \mathbf{Hx} + \mathbf{n}_B, \tag{1}$$

$$\mathbf{y} = \mathbf{Gx} + \mathbf{n}_E, \tag{2}$$

where $\mathbf{x} \in \mathbb{C}^{N_A \times 1}$ is the transmit signal vector, $\mathbf{H} \in \mathbb{C}^{N_B \times N_A}$ and $\mathbf{G} \in \mathbb{C}^{N_E \times N_A}$ are the respective channel matrices between Alice to Bob and Alice to Eve, and $\mathbf{n}_B$, $\mathbf{n}_E$ are AWGN vectors with i.i.d. entries $\sim \mathcal{N}_{\mathbb{C}}(0, \sigma_B^2)$ and $\mathcal{N}_{\mathbb{C}}(0, \sigma_E^2)$. We consider uncorrelated MIMO Rayleigh-fading channels, i.e., 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.,

$$\sigma_B^2 = 1, \tag{3}$$

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

A. Artificial Noise Scheme

The AN scheme assumes $N_B < N_A$, in order to ensure that $\mathbf{H}$ has a non-trivial null space with an orthonormal basis $\mathbf{Z} = \mathrm{null}(\mathbf{H})$ (such that $\mathbf{HZ} = \mathbf{0}_{N_B \times (N_A - N_B)}$) [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

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

where $\mathbf{u} \in \mathbb{C}^{N_B \times 1}$ is the information vector and $\mathbf{v} \in \mathbb{C}^{(N_A - N_B) \times 1}$ 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 $\sim \mathcal{N}_{\mathbb{C}}(0, \sigma_u^2)$ and $\mathcal{N}_{\mathbb{C}}(0, \sigma_v^2)$, respectively.

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

$$\mathbf{z} = \mathbf{HV}_1\mathbf{u} + \mathbf{HZv} + \mathbf{n}_B = \mathbf{HV}_1\mathbf{u} + \mathbf{n}_B, \tag{6}$$

$$\mathbf{y} = \mathbf{GV}_1\mathbf{u} + \mathbf{GZv} + \mathbf{n}_E. \tag{7}$$

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,

$$P = \mathrm{E}(||\mathbf{x}||^2) = P_u + P_v, \tag{9}$$

where

$$\begin{aligned} P_u &= \mathrm{E}(||\mathbf{u}||^2) = \sigma_u^2 N_B, \\ P_v &= \mathrm{E}(||\mathbf{v}||^2) = \sigma_v^2 (N_A - N_B), \end{aligned} \tag{10}$$

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:

$$C_S \triangleq \max_{p(\mathbf{u})} \{I(\mathbf{u}; \mathbf{z}) - I(\mathbf{u}; \mathbf{y})\}. \tag{11}$$

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

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]

$$\bar{C}_S \triangleq \max_{p(\mathbf{u})} \{I(\mathbf{u}; \mathbf{z}|\mathbf{H}) - I(\mathbf{u}; \mathbf{y}|\mathbf{H}, \mathbf{G})\}, \quad (12)$$

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

Since closed form expressions for C_S and $\bar{C}_S$ 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

$$R_S \triangleq I(\mathbf{u}; \mathbf{z}) - I(\mathbf{u}; \mathbf{y}), \quad (13)$$
$$\bar{R}_S \triangleq I(\mathbf{u}; \mathbf{z}|\mathbf{H}) - I(\mathbf{u}; \mathbf{y}|\mathbf{H}, \mathbf{G}), \quad (14)$$

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

C. System Parameters

We define Bob's and Eve's SNRs as
- $\mathrm{SNR}_B \triangleq \sigma_u^2/\sigma_B^2$
- $\mathrm{SNR}_E \triangleq \sigma_u^2/\sigma_E^2$

To simplify our notation, we define three system parameters:
- $\alpha \triangleq \sigma_u^2/\sigma_E^2$ (SNR_E)
- $\beta \triangleq \sigma_v^2/\sigma_u^2$ (AN power allocation)
- $\gamma \triangleq \sigma_E^2/\sigma_B^2$ (Eve-to-Bob noise-power ratio)

Note that $\mathrm{SNR}_B = \alpha\gamma$. If $\gamma > 1$, we say Eve has a *degraded* channel. Since we have normalized σ_B^2 to one, we can write (10) as
- $P_u = \alpha\gamma N_B$
- $P_v = \alpha\beta\gamma(N_A - N_B)$.

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 $N_E \leq N_A - N_B$. To present our result, we define some useful functions.

A. Definitions

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

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

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

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

We further define

$$N_{\min} \triangleq \min\{N_E, N_A - N_B\}, \quad (17)$$
$$N_{\max} \triangleq \max\{N_E, N_A - N_B\}, \quad (18)$$
$$\hat{N}_{\min} \triangleq \min\{N_E, N_A\}, \quad (19)$$
$$\hat{N}_{\max} \triangleq \max\{N_E, N_A\}. \quad (20)$$

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

$$\theta_i \triangleq \begin{cases} \alpha & 1 \leq i \leq N_B \\ \alpha\beta & N_B + 1 \leq i \leq N_A. \end{cases} \quad (21)$$

B. Average Secrecy Rate

A closed-form expression for $\bar{R}_S$ 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:

$$\bar{R}_S = \Theta(N_B, N_A, \alpha\gamma) + \Theta(N_{\min}, N_{\max}, \alpha\beta) - \Omega, \quad (22)$$

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

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

$$K = \frac{(-1)^{N_E(N_A - \hat{N}_{\min})}}{\Gamma_{\hat{N}_{\min}}(N_E)} \frac{\prod_{i=1}^{2} \mu_i^{m_i N_E}}{\prod_{i=1}^{2} \Gamma_{m_i}(m_i) \prod_{i<j} \left(\mu_i - \mu_j\right)^{m_i m_j}}, \quad (24)$$

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

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

$$r_{i,j}^{(k)} = \begin{cases} (\mu_{e_i})^{N_A - j - d_i} \dfrac{(N_A - j)!}{(N_A - j - d_i)!}, & \hat{N}_{\min} + 1 \leq j \leq N_A \\[2ex] (-1)^{d_i} \dfrac{\varphi(i, j)!}{(\mu_{e_i})^{\varphi(i, j) + 1}}, & 1 \leq j \leq \hat{N}_{\min}, j \neq k \\[2ex] (-1)^{d_i} \varphi(i, j)! e^{\mu_{e_i}} \sum_{l=0}^{\varphi(i, j)} \dfrac{\Gamma(l - \varphi(i, j), \mu_{e_i})}{(\mu_{e_i})^{l+1}}, \\[2ex] \qquad\qquad\qquad\qquad \text{otherwise} \end{cases} \quad (25)$$

where

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

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

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

Proof: See Appendix A. ∎

Theorem 1 gives the exact value of $\bar{R}_S$ for the AN scheme, as a function of SNR_B ($\alpha\gamma$), SNR_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 $\bar{R}_S$.

Remark 1: The difficulty in the proof is to compute $I(\mathbf{u}; \mathbf{y}|\mathbf{G})$ given $\mathbf{H}$. Our key contribution is to view the artificial noise term $\mathbf{GZv}$ in (7) as a MIMO co-channel interferer from other link. This is because given $\mathbf{H}$, or equivalently, given $\mathbf{V}_1$ and $\mathbf{Z}$, $\mathbf{GV}_1$ and $\mathbf{GZ}$ are mutually independent complex Gaussian random matrices with i.i.d. entries $\sim \mathcal{N}_{\mathbb{C}}(0, 1)$ [25, Th. 1]. It means that we can rewrite (7) as

$$\mathbf{y} = \mathbf{G}_1\mathbf{u} + \mathbf{G}_2\mathbf{v} + \mathbf{n}_E, \qquad (26)$$

where $\mathbf{G}_1 = \mathbf{GV}_1$ describes the channel of the desired link, and $\mathbf{G}_2 = \mathbf{GZ}$ describes the channel of the interference link. Therefore, the problem of computing $I(\mathbf{u}; \mathbf{y}|\mathbf{G})$ given $\mathbf{H}$ can be reduced to the classic problem of computing $I(\mathbf{u}; \mathbf{y}|\mathbf{G}_1, \mathbf{G}_1)$, i.e., the ergodic mutual information for MIMO systems in the presence of single MIMO interferer.

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_S/N_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_S/N_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 [26]. Here, we provide a unified result for arbitrary β.

Theorem 2: As N_A, N_B, $N_A - N_B$ and $N_E \to \infty$ with $N_A/N_E \to \beta_1$, $N_A/N_B \to \beta_2$ and $N_B/N_E \to \beta_3$,

$$\frac{R_S}{N_B} \overset{a.s.}{\to} \Phi(P_u, \beta_2) - \frac{1}{\beta_3}(\beta_1\mathcal{V}(\delta) - \log\delta + \delta - 1)$$

$$+ \frac{1}{\beta_3}\Phi\left(\frac{P_v}{\gamma(\beta_1 - \beta_3)}, \beta_1 - \beta_3\right) \triangleq \Psi, \quad (27)$$

where

$$\Phi(x, y) = y\log\left(1 + x - \frac{1}{4}\mathcal{F}(x, y)\right) - \frac{\mathcal{F}(x, y)}{4x}$$

$$+ \log\left(1 + xy - \frac{1}{4}\mathcal{F}(x, y)\right), \qquad (28)$$

$$\mathcal{F}(x, y) = \left(\sqrt{x(1 + \sqrt{y})^2 + 1} - \sqrt{x(1 - \sqrt{y})^2 + 1}\right)^2, \qquad (29)$$

$$\mathcal{V}(\delta) = \frac{1}{\beta_2}\log\left(1 + \frac{\delta P_u}{\gamma\beta_3}\right)$$

$$+ \left(1 - \frac{1}{\beta_2}\right)\log\left(1 + \frac{\delta P_v}{\gamma(\beta_1 - \beta_3)}\right) \qquad (30)$$

and δ is the solution of the equation

$$\beta_1 = \frac{1 - \delta}{1 - \eta(\delta)}, \qquad (31)$$

$$\eta(\delta) = \frac{1}{\beta_2}\left(1 + \frac{\delta P_u}{\gamma\beta_3}\right)^{-1} + \left(1 - \frac{1}{\beta_2}\right)\left(1 + \frac{\delta P_v}{\gamma(\beta_1 - \beta_3)}\right)^{-1}. \qquad (32)$$

Proof: See Appendix B. ∎

In the special case of $\beta = 1$, according to the definitions of P_u and P_v given in Sec. II.C, we have

$$\frac{P_u}{\gamma\beta_3} = \frac{P_v}{\gamma(\beta_1 - \beta_3)}. \qquad (33)$$

According to [27, eq. 2.121], the explicit solution of (31) is

$$\delta = 1 - \frac{\mathcal{F}\left(\frac{P_u}{\gamma\beta_3}, \beta_1\right)}{\frac{4P_u}{\gamma\beta_3}}. \qquad (34)$$

By substituting (33) and (34) into (27), we have

$$\frac{R_S}{N_B} \overset{a.s.}{\to} \Phi(P_u, \beta_2) - \frac{\Phi(P_u/(\gamma\beta_3), \beta_1)}{\beta_3}$$

$$+ \frac{\Phi(P_u/(\gamma\beta_3), \beta_1 - \beta_3)}{\beta_3} \qquad (35)$$

which coincides with [26, Th. 3].

Remark 2: The difficulty in the proof is to study the distribution of $\log\left|\mathbf{I}_{N_E} + \alpha\mathbf{W}_1 + \alpha\beta\mathbf{W}_2\right|$, where $\mathbf{W}_1 = (\mathbf{GV}_1)(\mathbf{GV}_1)^H$ and $\mathbf{W}_2 = (\mathbf{GZ})(\mathbf{GZ})^H$. Our key contribution is to show that the convergence behavior of $\log\left|\mathbf{I}_{N_E} + \alpha\mathbf{W}_1 + \alpha\beta\mathbf{W}_2\right|/N_E$ is characterized by a *generalized version of Marčenko-Pastur Law* [27, Th. 2.39]. The technical trick is to first rewrite $\log\left|\mathbf{I}_{N_E} + \alpha\mathbf{W}_1 + \alpha\beta\mathbf{W}_2\right|$ as $\log\left|\mathbf{I}_{N_E} + \hat{\mathbf{G}}_3\mathbf{T}\hat{\mathbf{G}}_3^H\right|$, where $\hat{\mathbf{G}}_3$ is given in (71) and $\mathbf{T}$ is given in (72), and then evaluate the empirical eigenvalue distribution of $\hat{\mathbf{G}}_3\mathbf{T}\hat{\mathbf{G}}_3^H$.

D. Asymptotic Approximation of Average Secrecy Rate

Theorem 2 shows that the random variable R_S/N_B converges almost surely to a constant Ψ given in (27), 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.
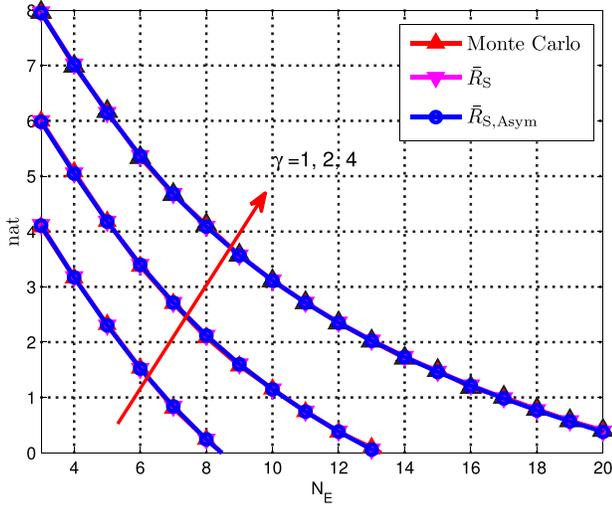
Fig. 1. $\bar{R}_S$ vs. γ and N_E with $\alpha = 3$ dB, $\beta = -3$ dB, $N_A = 6$ and $N_B = 3$.

Fig. 2. $\bar{R}_S$ vs. β and N_E with $\alpha = 3$ dB, $\gamma = 3$ dB, $N_A = 6$ and $N_B = 3$.

Corollary 1: Under the same assumptions of Theorem 2,

$$\frac{\bar{R}_S}{N_B} \to \Psi, \tag{36}$$

where Ψ is given in (27). Then we can write that

$$\bar{R}_S \approx N_B \Psi \triangleq \bar{R}_{S,\text{Asym}}. \tag{37}$$

for a sufficiently large number of antennas.

Proof: The proof is straightforward. ∎

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

$$\beta_1 = N_A/N_E, \beta_2 = N_A/N_B, \text{ and } \beta_3 = N_B/N_E. \tag{38}$$

Remark 3: For finite system models, we verified by simulations that the difference between $\bar{R}_S$ and $\bar{R}_{S,\text{Asym}}$ is indistinguishable if

$$\min\{N_A, N_B, N_A - N_B, N_E\} > 2. \tag{39}$$

Example 1: Let us apply Theorem 1 and Corollary 1 to the analysis of an AN scheme with $N_A = 6$, $N_B = 3$ and $\alpha = 3$ dB. Fig. 1 shows the value of $\bar{R}_S$ 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 $\bar{R}_S$. Both figures show an excellent agreement between the theoretically derived $\bar{R}_S$ and Monte Carlo simulation and the asymptotic approximation $\bar{R}_{S,\text{Asym}}$.

Moreover, Fig. 1 shows how $\bar{R}_S$ 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 $\bar{R}_S$ when $N_E > N_A$.

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.
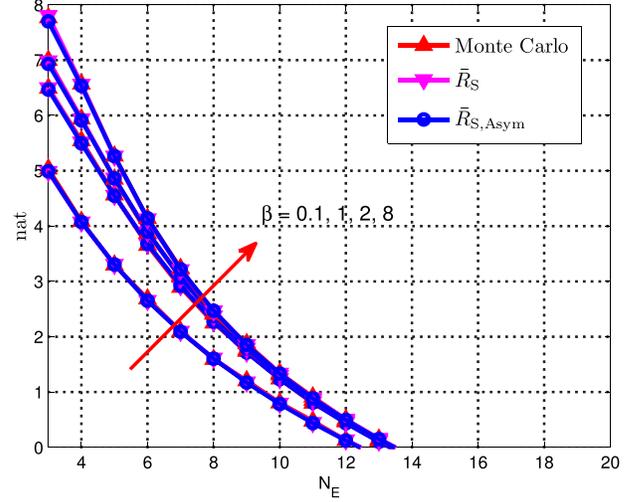
Theorem 3: If $N_E \leq N_A - N_B$, as $\alpha, \beta \to \infty$, then

$$\bar{R}_S = \bar{C}_S = \bar{C}_{\text{Bob}}, \tag{40}$$

where $\bar{C}_{\text{Bob}}$ 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

$$\bar{C}_S \leq \max_{p(\mathbf{u})} \{I(\mathbf{u}; \mathbf{z}|\mathbf{H})\} = \bar{C}_{\text{Bob}}. \tag{41}$$

In other words, the secrecy capacity cannot be greater than the main channel capacity.

Remark 4: Combining (40) and (41), we have shown that the achievable average secrecy rate $\bar{R}_S$ and the *maximum* average MIMO secrecy capacity $\bar{C}_{\text{Bob}}$ coincide asymptotically as α and $\beta \to \infty$. It means that under the AN framework, Gaussian input alphabets are asymptotically optimal among all possible input distribution, as the AN power goes to infinity.

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 $\bar{R}_S$ given in (22).

Theorem 4:

$$\bar{R}_{\text{LB}} \leq \bar{R}_S \leq \bar{R}_{\text{UB}}, \tag{42}$$

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

$$\bar{R}_{\text{LB}} = \Theta(N_B, N_A, \alpha\gamma) + \Theta(N_{\min}, N_{\max}, \alpha\beta) \\ - \Theta(\hat{N}_{\min}, \hat{N}_{\max}, \theta_{\max}), \tag{43}$$

$$\bar{R}_{\text{UB}} = \Theta(N_B, N_A, \alpha\gamma) + \Theta(N_{\min}, N_{\max}, \alpha\beta) \\ - \Theta(\hat{N}_{\min}, \hat{N}_{\max}, \theta_{\min}), \tag{44}$$

$$\theta_{\min} \triangleq \min\{\alpha, \alpha\beta\}, \\ \theta_{\max} \triangleq \max\{\alpha, \alpha\beta\}, \tag{45}$$
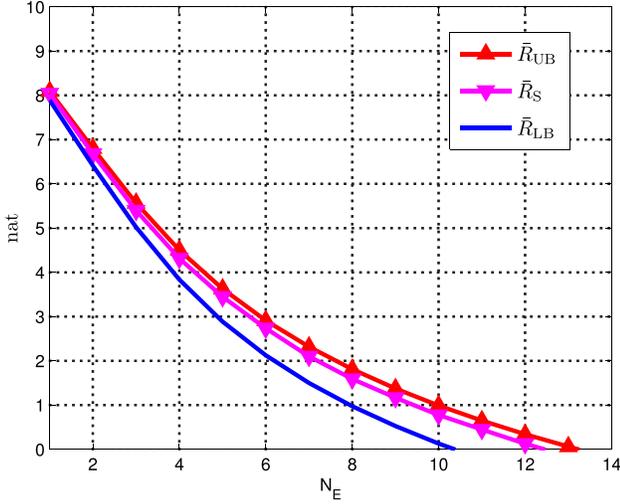
and $\Theta(\cdot, \cdot, \cdot)$ is given in (15).

Fig. 3. $\bar{R}_S$ and $\bar{R}_{LB}$ vs. N_E with $\alpha = 3$ dB, $\beta = 1$ dB, $\gamma = 6$ dB, $N_B = 3$ and $N_A = 4$.

Proof: See Appendix D. ∎

Example 2: Fig. 3 compares the values of $\bar{R}_S$, $\bar{R}_{UB}$, $\bar{R}_{LB}$ as functions of N_E with $\alpha = 3$ dB, $\beta = 1$ dB, $\gamma = 6$ dB, $N_B = 3$ and $N_A = 4$. 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_S in (13) for high SNR_B.

Theorem 5: Let N_A, N_B, $N_A - N_B$ and $N_E \to \infty$ with $N_A/N_E \to \beta_1$, $N_A/N_B \to \beta_2$, $N_B/N_E \to \beta_3$, and let P_u, $P_v \to \infty$, then almost surely (i.e., with probability one)

$$R_S/N_B \geq \Delta(A_{max}),$$
$$R_S/N_B \leq \Delta(A_{min}), \qquad (46)$$

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

$$\rho \triangleq \beta_1 - \beta_3,$$
$$A_{min} \triangleq \min\left\{\frac{P_v}{\gamma\rho}, \frac{P_u}{\gamma\beta_3}\right\},$$
$$A_{max} \triangleq \max\left\{\frac{P_v}{\gamma\rho}, \frac{P_u}{\gamma\beta_3}\right\}, \qquad (47)$$
$$\Delta(x) \triangleq (\log P_u\beta_2 - (\beta_2 - 1)\log(1 - \beta_2^{-1}) - 1)$$
$$\qquad - F(x) + \Xi, \qquad (48)$$

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

$$\Xi \triangleq \begin{cases} (\beta_2-1)\left(\log\frac{P_v}{\gamma\rho} - \frac{1-\rho}{\rho}\log(1-\rho) - 1\right) & \rho \leq 1 \\ \beta_3^{-1}\left(\log\frac{P_v}{\gamma} - (\rho-1)\log\left(1-\rho^{-1}\right) - 1\right) & \rho > 1 \end{cases}$$

$$\qquad (49)$$

Proof: See Appendix E. ∎

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

Theorem 5 shows that the random variable R_S/N_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,

$$\bar{R}_S/N_B \geq \Delta(A_{max}),$$
$$\bar{R}_S/N_B \leq \Delta(A_{min}), \qquad (50)$$

where $\Delta(\cdot)$ is given in (48). The equality holds if $\beta = 1$.

Proof: The proof is straightforward. ∎

The bounds in (46) and (50) enable the following simple sufficient and necessary conditions for positive instantaneous and average secrecy rate.

Corollary 3: Let N_A, N_B, $N_A - N_B$ and $N_E \to \infty$ with $N_A/N_E \to \beta_1$, $N_A/N_B \to \beta_2$ and $N_B/N_E \to \beta_3$. Then a sufficient condition for positive instantaneous and average secrecy rate is given by

$$\lim_{P_u, P_v \to \infty} \Delta(A_{max}) > 0, \qquad (51)$$

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

$$\lim_{P_u, P_v \to \infty} \Delta(A_{min}) > 0, \qquad (52)$$

where $\Delta(\cdot)$ is given in (48).

Proof: The proof is straightforward. ∎

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

$$\beta_1 = N_A/N_E, \quad \beta_2 = N_A/N_B, \quad \beta_3 = N_B/N_E,$$
$$P_u = \alpha\gamma N_B \quad \text{and} \quad P_v = \alpha\beta\gamma(N_A - N_B). \qquad (53)$$

Thus $\Delta(\cdot)$ reduces to a function of N_A, N_B, N_E, α, β and γ.

Remark 5: We verified by simulation that Corollary 3 is accurate for finite system models, when

$$\min\{\alpha\gamma, \alpha\beta\gamma\} \geq 4,$$
$$\min\{N_A, N_B, N_A - N_B, N_E\} > 2. \qquad (54)$$

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

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.

Remark 6: The upper bounds derived in this section are based on the achievable secrecy rate using Gaussian input alphabets. Except for the special case of $N_E \leq N_A - N_B$ and α, $\beta \to \infty$, the upper bounds derived in this
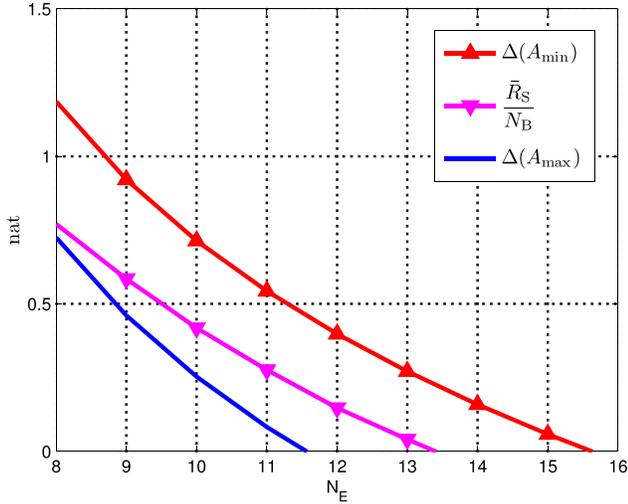
Fig. 4. Plot of $\bar{R}_S$, $\Delta(A_{\max})$ and $\Delta(A_{\min})$ vs. N_E with $\alpha = \gamma = 3$ dB, $\beta = 1$ dB, $N_B = 3$ and $N_A = 6$.

section are not valid for arbitrary input alphabets and arbitrary encoding and decoding schemes. Nevertheless, we can always use the universal upper bound on secrecy capacity in (41).

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 $N_E < N_A$ or the case of $N_B = 1$.

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

$$\bar{R}_S = I(\mathbf{u}; \mathbf{z}|\mathbf{H}) - I(\mathbf{u}; \mathbf{y}|\mathbf{H}, \mathbf{G}). \quad (55)$$

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(u; z|H): Since $(\mathbf{HV}_1)(\mathbf{HV}_1)^H = \mathbf{HH}^H$, using [21, Th. 2] and [23, Th. 1], we have

$$I(\mathbf{u}; \mathbf{z}|\mathbf{H}) = E_{\mathbf{H}}\left(\log\left|\mathbf{I}_{N_B} + \alpha\gamma\,\mathbf{HH}^H\right|\right)$$
$$= \Theta(N_B, N_A, \alpha\gamma), \quad (56)$$

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

2) I(u; y|H, 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 $E_{\mathbf{H}}\left[I(\mathbf{u}; \mathbf{y}|\mathbf{G})|\mathbf{H}\right]$. The advantage is that for given $\mathbf{H}$, $\mathbf{V} = [\mathbf{V}_1, \mathbf{Z}]$ is a fixed unitary matrix. Then, using [25, Th. 1], $\mathbf{GV}_1$ and $\mathbf{GZ}$ are mutually independent complex Gaussian random matrices with i.i.d. entries $\sim \mathcal{N}_{\mathbb{C}}(0, 1)$.

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

$$I(\mathbf{u}; \mathbf{y}|\mathbf{G}) = E_{\mathbf{G}_1, \mathbf{G}_2}\left(\log\frac{\left|\mathbf{I}_{N_E}\sigma_E^2 + \sigma_u^2\mathbf{W}_1 + \sigma_v^2\mathbf{W}_2\right|}{\left|\mathbf{I}_{N_E}\sigma_E^2 + \sigma_v^2\mathbf{W}_2\right|}\right)$$

$$= E_{\mathbf{G}_1, \mathbf{G}_2}\left(\log\frac{\left|\mathbf{I}_{N_E} + \frac{\sigma_u^2}{\sigma_E^2}\mathbf{W}_1 + \frac{\sigma_v^2}{\sigma_E^2}\mathbf{W}_2\right|}{\left|\mathbf{I}_{N_E} + \frac{\sigma_v^2}{\sigma_E^2}\mathbf{W}_2\right|}\right)$$

$$= E_{\mathbf{G}_1, \mathbf{G}_2}\left(\log\left|\mathbf{I}_{N_E} + \alpha\mathbf{W}_1 + \alpha\beta\mathbf{W}_2\right|\right)$$
$$- E_{\mathbf{G}_2}\left(\log\left|\mathbf{I}_{N_E} + \alpha\beta\mathbf{W}_2\right|\right). \quad (57)$$

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

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

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 $\mathbf{G}_3\Delta\mathbf{G}_3^H$, where

$$\mathbf{G}_3 = [\mathbf{G}_1, \mathbf{G}_2], \quad (59)$$
$$\Delta = \text{diag}\left(\{\theta_i\}_1^{N_A}\right). \quad (60)$$

θ_i is defined in (21). We define

$$\Omega = E_{\mathbf{G}_1, \mathbf{G}_2}\left(\log\left|\mathbf{I}_{N_E} + \alpha\mathbf{W}_1 + \alpha\beta\mathbf{W}_2\right|\right). \quad (61)$$

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

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

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

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

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

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

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

$$I(\mathbf{u}; \mathbf{y}|\mathbf{H}, \mathbf{G}) = E_{\mathbf{H}}\left(I(\mathbf{u}; \mathbf{y}|\mathbf{G})|\mathbf{H}\right)$$
$$= \Omega - \Theta(N_{\min}, N_{\max}, \alpha\beta). \quad (64)$$

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

$$\bar{R}_S = \Theta(N_B, N_A, \alpha\gamma) + \Theta(N_{\min}, N_{\max}, \alpha\beta) - \Omega. \quad (65)$$

■

B. Proof of Theorem 2

Recalling that

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

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

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

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 $N_B \to \infty$ with $N_A/N_B \to \beta_2$, the following limit holds [27, eq. 1.14]

$$\frac{I(\mathbf{u}; \mathbf{z})}{N_B} \to \Phi(P_u, \beta_2), \tag{68}$$

where $\Phi(x, y)$ is given in (28).

2) $I(\mathbf{u}; \mathbf{y})$: Similarly to (57), we have

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

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 [25, 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 [27, eq. 1.14], as $N_A - N_B$ and $N_E \to \infty$ with $N_A/N_E \to \beta_1$ and $N_B/N_E \to \beta_3$, i.e., $(N_A - N_B)/N_E \to \beta_1 - \beta_3$, we have

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

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

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

$$\mathbf{T} = N_E \mathrm{diag}\left(\{\theta_i\}_1^{N_A} \right), \tag{72}$$

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 $\sim \mathcal{N}_{\mathbb{C}}(0, 1/N_E)$.

According to [27, Th. 2.39], as N_A and $N_E \to \infty$ with $N_A/N_E \to \beta_1$, we have

$$\frac{\log \left| \mathbf{I}_{N_E} + \hat{\mathbf{G}}_3 \mathbf{T} \hat{\mathbf{G}}_3^H \right|}{N_E} \overset{a.s.}{\to} \beta_1 \mathcal{V}(\delta) - \log \delta + \delta - 1, \tag{73}$$

where $\mathcal{V}(\delta)$ is given in (30) and δ satisfies

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

with $\eta(\delta)$ given in (32).

From (68), (70) and (73), as N_A, N_B, $N_A - N_B$ and $N_E \to \infty$ with $N_A/N_E \to \beta_1$, $N_A/N_B \to \beta_2$ and $N_B/N_E \to \beta_3$, we have

$$\frac{R_S}{N_B} \overset{a.s.}{\to} \Psi \tag{75}$$

where the constant Ψ is given in (27). ∎

C. Proof of Theorem 3

We first show that using Gaussian input alphabets, if $N_E \le N_A - N_B$, $I(\mathbf{u}; \mathbf{y}|\mathbf{H}, \mathbf{G}) \to 0$ 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

$$
\begin{aligned}
&I(\mathbf{u}; \mathbf{y}|\mathbf{G}) \\
&= \mathrm{E}_{\mathbf{G}_1, \mathbf{G}_2}\left(\log \frac{\left| \mathbf{I}_{N_E}\sigma_E^2 + \sigma_u^2 \mathbf{W}_1 + \sigma_v^2 \mathbf{W}_2 \right|}{\left| \mathbf{I}_{N_E}\sigma_E^2 + \sigma_v^2 \mathbf{W}_2 \right|} \right) \\
&\overset{a}{\le} \mathrm{E}_{\mathbf{G}_2}\left(\log \frac{\left| \mathbf{I}_{N_E}\sigma_E^2 + \sigma_u^2 \mathrm{E}_{\mathbf{G}_1}(\mathbf{W}_1) + \sigma_v^2 \mathbf{W}_2 \right|}{\left| \mathbf{I}_{N_E}\sigma_E^2 + \sigma_v^2 \mathbf{W}_2 \right|} \right) \\
&= \mathrm{E}_{\mathbf{G}_2}\left(\log \frac{\left| \mathbf{I}_{N_E} + \frac{\sigma_v^2}{\sigma_E^2 + N_B\sigma_u^2}\mathbf{W}_2 \right|}{\left| \mathbf{I}_{N_E} + \frac{\sigma_v^2}{\sigma_E^2}\mathbf{W}_2 \right|} \right) + N_E \log \frac{\sigma_E^2 + N_B\sigma_u^2}{\sigma_E^2},
\end{aligned}
\tag{76}
$$

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

Let

$$
\mathbf{W} = \begin{cases} \mathbf{G}_2\mathbf{G}_2^H & \text{if } N_E \le N_A - N_B \\ \mathbf{G}_2^H\mathbf{G}_2 & \text{if } N_E > N_A - N_B, \end{cases}
$$

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

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

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

From (76) and (77), we have

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

Based on (78), if $N_{\min} = N_E$, i.e., $N_E \le N_A - N_B$, 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

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

where $\bar{C}_{\mathrm{Bob}}$ 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 $\sigma_u^2 \mathbf{I}_{N_B}$ [21, Th. 1].

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

$$\bar{C}_S \le \max_{p(\mathbf{u})} \{I(\mathbf{u}; \mathbf{z}|\mathbf{H})\} = \bar{C}_{\text{Bob}}. \tag{81}$$

Based on (80) and (81), as $\alpha, \beta \to \infty$, if $N_E \le N_A - N_B$,

$$\bar{R}_S = \bar{C}_S = \bar{C}_{\text{Bob}}. \tag{82}$$

∎

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 $\bar{R}_S$ given in (27). Recalling that

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

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

$$\left| \mathbf{I}_{N_E} + \alpha \mathbf{W}_1 + \alpha\beta \mathbf{W}_2 \right| \ge \left| \mathbf{I}_{N_E} + \theta_{\min}(\mathbf{W}_1 + \mathbf{W}_2) \right|$$
$$= \left| \mathbf{I}_{N_E} + \theta_{\min} \mathbf{G}_3 \mathbf{G}_3^H \right|, \tag{84}$$

and

$$\left| \mathbf{I}_{N_E} + \alpha \mathbf{W}_1 + \alpha\beta \mathbf{W}_2 \right| \le \left| \mathbf{I}_{N_E} + \theta_{\max}(\mathbf{W}_1 + \mathbf{W}_2) \right|$$
$$= \left| \mathbf{I}_{N_E} + \theta_{\max} \mathbf{G}_3 \mathbf{G}_3^H \right|, \tag{85}$$

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

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

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

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

$$\bar{R}_{LB} \le \bar{R}_S \le \bar{R}_{UB},$$

where

$$\bar{R}_{LB} = \Theta(N_B, N_A, \alpha\gamma) + \Theta(N_{\min}, N_{\max}, \alpha\beta)$$
$$- \Theta(\hat{N}_{\min}, \hat{N}_{\max}, \theta_{\max}), \tag{87}$$

$$\bar{R}_{UB} = \Theta(N_B, N_A, \alpha\gamma) + \Theta(N_{\min}, N_{\max}, \alpha\beta)$$
$$- \Theta(\hat{N}_{\min}, \hat{N}_{\max}, \theta_{\min}). \tag{88}$$

∎

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

$$R_S \ge \log \left| \mathbf{I}_{N_B} + \alpha\gamma \mathbf{HH}^H \right| + \log \left| \mathbf{I}_{N_E} + \alpha\beta \mathbf{W}_2 \right|$$
$$- \left| \mathbf{I}_{N_E} + \theta_{\max} \mathbf{G}_3 \mathbf{G}_3^H \right| \triangleq R_{LB}, \tag{89}$$

$$R_S \le \log \left| \mathbf{I}_{N_B} + \alpha\gamma \mathbf{HH}^H \right| + \log \left| \mathbf{I}_{N_E} + \alpha\beta \mathbf{W}_2 \right|$$
$$- \left| \mathbf{I}_{N_E} + \theta_{\min} \mathbf{G}_3 \mathbf{G}_3^H \right| \triangleq R_{UB}. \tag{90}$$

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

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

$$\rho \triangleq \beta_1 - \beta_3,$$
$$A_{\min} \triangleq \min \left\{ \frac{P_v}{\gamma\rho}, \frac{P_u}{\gamma\beta_3} \right\},$$
$$A_{\max} \triangleq \max \left\{ \frac{P_v}{\gamma\rho}, \frac{P_u}{\gamma\beta_3} \right\}.$$

Similarly to the proof in Theorem 2, using [27, eq. 1.14], as N_A, N_B, $N_A - N_B$ and $N_E \to \infty$ with $N_A/N_E \to \beta_1$, $N_A/N_B \to \beta_2$ and $N_B/N_E \to \beta_3$,

$$\frac{\log \left| \mathbf{I}_{N_B} + \alpha\gamma \mathbf{HH}^H \right|}{N_B} \xrightarrow{a.s.} \Phi(P_u, \beta_2), \tag{91}$$

$$\frac{\log \left| \mathbf{I}_{N_E} + \alpha\beta \mathbf{W}_2 \right|}{N_E} \xrightarrow{a.s.} \Phi \left(\frac{P_v}{\gamma\rho}, \rho \right), \tag{92}$$

$$\frac{\left| \mathbf{I}_{N_E} + \theta_{\max} \mathbf{G}_3 \mathbf{G}_3^H \right|}{N_E} \xrightarrow{a.s.} \Phi(A_{\max}, \beta_1), \tag{93}$$

$$\frac{\left| \mathbf{I}_{N_E} + \theta_{\min} \mathbf{G}_3 \mathbf{G}_3^H \right|}{N_E} \xrightarrow{a.s.} \Phi(A_{\min}, \beta_1), \tag{94}$$

where $\Phi(x, y)$ is given in (28).

We then evaluate the function $\Phi(x, y)$. From (28), since $\mathcal{F}(x, y) = \mathcal{F}(xy, y^{-1})$, it is easy to show the following property

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

Recalling [27, Examples 2.14 and 2.15], if $y \le 1$,

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

Using (95) and (96), we have the following results on the non random quantities $\Phi(P_u, \beta_2)$, $\Phi(P_v/(\gamma\rho), \rho)$, $\Phi(A_{\max}, \beta_1)$ and $\Phi(A_{\min}, \beta_1)$.

Since $\beta_2 > 1$, i.e., $N_A > N_B$,

$$\lim_{P_u \to \infty} (\log P_u\beta_2 - \Phi(P_u, \beta_2))$$
$$= \lim_{P_u \to \infty} \left(\log P_u\beta_2 - \frac{\Phi(P_u\beta_2, \beta_2^{-1})}{\beta_2^{-1}} \right)$$
$$= (\beta_2 - 1) \log \left(1 - \beta_2^{-1} \right) + 1. \tag{97}$$

If $\rho \le 1$,

$$\lim_{P_v \to \infty} \left(\log \frac{P_v}{\gamma\rho} - \frac{\Phi(P_v/(\gamma\rho), \rho)}{\rho} \right)$$
$$= \frac{1 - \rho}{\rho} \log(1 - \rho) + 1. \tag{98}$$

If $\rho > 1$,

$$\lim_{P_v \to \infty} \left(\log \frac{P_v}{\gamma} - \Phi \left(\frac{P_v}{\gamma\rho}, \rho \right) \right)$$
$$= \lim_{P_v \to \infty} \left(\log \frac{P_v}{\gamma} - \frac{\Phi(P_v/\gamma, \rho^{-1})}{\rho^{-1}} \right)$$
$$= (\rho - 1) \log(1 - \rho^{-1}) + 1. \tag{99}$$

If $\beta_1 \leq 1$,

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

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

If $\beta_1 > 1$,

$$\lim_{P_u, P_v \to \infty} (\log A_{\max}\beta_1 - \Phi(A_{\max}, \beta_1))$$
$$= \lim_{P_u, P_v \to \infty} \left(\log A_{\max}\beta_1 - \frac{\Phi\left(A_{\max}\beta_1, \beta_1^{-1}\right)}{\beta_1^{-1}} \right)$$
$$= (\beta_1 - 1) \log\left(1 - \beta_1^{-1}\right) + 1, \qquad (102)$$

$$\lim_{P_u, P_v \to \infty} (\log A_{\min}\beta_1 - \Phi(A_{\min}, \beta_1))$$
$$= \lim_{P_u, P_v \to \infty} \left(\log A_{\min}\beta_1 - \frac{\Phi\left(A_{\min}\beta_1, \beta_1^{-1}\right)}{\beta_1^{-1}} \right)$$
$$= (\beta_1 - 1) \log\left(1 - \beta_1^{-1}\right) + 1. \qquad (103)$$

Based on the above analysis, as $N_A, N_B, N_A - N_B, N_E \to \infty$ with $N_A/N_E \to \beta_1$, $N_A/N_B \to \beta_2$ and $N_B/N_E \to \beta_3$, and for $P_u, P_v \to \infty$

$$R_{LB}/N_B \xrightarrow{a.s.} \Delta(A_{\max}),$$
$$R_{UB}/N_B \xrightarrow{a.s.} \Delta(A_{\min}), \qquad (104)$$

where $\Delta(\cdot)$ is given in (48).

Using (89), (90) and (104), under the above conditions, we have (46). ∎

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," *J. Comput. Syst. Sci.*, vol. 28, no. 2, pp. 270–299, 1984.

[3] J. Hoffstein, J. Pipher, and J. H. Silverman, "NTRU: A ring-based public key cryptosystem," in *Algorithmic Number Theory* (Lecture Notes in Computer Science), Berlin, Germany: Springer-Verlag, 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. R. D. Rodrigues, and S. W. 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 (Shitz), "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, Mar. 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, Nov. 2010.

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

[12] I. Csiszár, "Almost independence and secrecy capacity," *Problems Inf. Transmiss.*, vol. 32, no. 1, 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, pp. 6428–6443, Oct. 2011.

[14] C. Ling, L. Luzzi, J.-C. Belfiore, and D. Stehlé, "Semantically secure lattice codes for the Gaussian wiretap channel," *IEEE Trans. Inf. Theory*, vol. 60, no. 10, pp. 6399–6416, Oct. 2014.

[15] F. E. Oggier, P. Solé, and J.-C. Belfiore. (Mar. 2011). "Lattice codes for the wiretap Gaussian channel: Construction and analysis." [Online]. Available: http://arxiv.org/abs/1103.4086

[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, Jul. 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 Commun. Lett.*, vol. 17, no. 7, pp. 1483–1486, Jul. 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, Nov. 2013.

[21] E. Telatar, "Capacity of multi-antenna Gaussian channels," *Eur. Trans. Telecommun.*, 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, Aug. 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)*, Anchorage, AK, USA, 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, Jan. 2010.

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

[26] S. Liu, Y. Hong, and E. Viterbo, "Artificial noise revisited: When Eve has more antennas than Alice," in *Proc. IEEE Int. Conf. Signal Process. Commun. (SPCOM)*, Bengaluru, India, Jul. 2014, pp. 1–5.

[27] A. M. Tulino and S. Verdú, *Random Matrix Theory and Wireless Communications*. Hanover, MA 02339, USA: now Publishers, 2004.

[28] H. Lütkepohl, *Handbook of Matrices*. New York, NY, USA: Wiley, 1996.

Shuiyin Liu (M'13) received the B.Eng. degree in electronic and information engineering from Beihang University, Beijing, China, in 2006, the Master and Ph.D. degrees from Imperial College London, UK, in 2007 and 2011 respectively. Since 2012, He has been working as a research fellow in the Electrical and Computer Systems Engineering Department at Monash University, Australia. His current research interests include lattice coding for the Gaussian and fading channels, cryptography and physical layer security.

Yi Hong (M'00–SM'10) is currently a Senior Lecturer at the Department of Elecectrical and Computer Systems Eng., at Monash University, Clayton, Australia. She received her Ph.D. degree in Electrical Engineering and Telecommunications from the University of New South Wales (UNSW), Sydney, Australia. She then worked at the Institute of Telecom. Research, University of South Australia, Australia; at the Institute of Advanced Telecom., Swansea University, UK; and at University of Calabria, Italy. During her PhD, she received an International Postgraduate Research Scholarship (IPRS) from the Commonwealth of Australia; a supplementary Engineering Award from the School of Electrical Engineering and Telecommunications, UNSW; and a Wireless Data Communication System Scholarship from UNSW. She received the NICTA-ACoRN Earlier Career Researcher award for a paper presented at the Australian Communication Theory Workshop (AUSCTW), Adelaide, Australia, 2007. Dr. Hong is an Associate Editor for *European Transactions on Telecommunications* and an IEEE Senior member. She was the General Co-Chair of 2014 IEEE Information Theory Workshop, Hobart, Tasmania; and the Technical Program Committee Chair of 2011 Australian Communications Theory Workshop, Melbourne, Australia. She was the Publicity Chair at the 2009 IEEE Information Theory Workshop, Sicily, Italy. She is a Technical Program Committee member for many IEEE conferences such as IEEE ICC, VTC, PIMRC and WCNC. Her research interests include information and communication theory with applications to telecommunication engineering.

Emanuele Viterbo (M'95–SM'04–F'11) received his degree (Laurea) in Electrical Engineering in 1989 and his Ph.D. in 1995 in Electrical Engineering, both from the Politecnico di Torino, Torino, Italy. From 1990 to 1992 he was with the European Patent Office, The Hague, The Netherlands, as a patent examiner in the field of dynamic recording and error-control coding. Between 1995 and 1997 he held a post-doctoral position in the Dipartimento di Elettronica of the Politecnico di Torino in Communications Techniques over Fading Channels. He became Associate Professor at Politecnico di Torino, Dipartimento di Elettronica in 2005 and a Full Professor in DEIS at Universit'a della Calabria, Italy, in 2006. Since 2010, he is a Full Professor at Department of Electrical and Computer Systems Engineering, Monash University, and the Associate Dean Graduate Research of the Faculty of Engineering at Monash.

In 1993 he was visiting researcher in the Communications Department of DLR, Oberpfaffenhofen, Germany. In 1994 and 1995 he was visiting the E.N.S.T., Paris. In 1998 he was visiting researcher in the Information Sciences Research Center of AT&T Research, Florham Park, NJ. In 2003 he was visiting researcher at the Maths Department of EPFL, Lausanne, Switzerland. In 2004 he was visiting researcher at the Telecommunications Department of UNICAMP, Campinas, Brazil. In 2005 he was visiting researcher at the ITR of UniSA, Adelaide, Australia. Dr. Emanuele Viterbo was awarded a NATO Advanced Fellowship in 1997 from the Italian National Research Council. His main research interests are in lattice codes for the Gaussian and fading channels, algebraic coding theory, algebraic space-time coding, digital terrestrial television broadcasting, and digital magnetic recording. He was Associate Editor of IEEE TRANSACTIONS ON INFORMATION THEORY, *European Transactions on Telecommunications* and *Journal of Communications and Networks*; and is now an Editor of *Foundations and Trends in Communications and Information Theory*.