This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TWC.2015.2417886, IEEE Transactions on Wireless Communications

Guaranteeing Positive Secrecy Capacity for MIMOME Wiretap Channels with Finite-Rate Feedback using Artificial Noise

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

***Abstract*—While the impact of finite-rate feedback on the capacity of fading channels has been extensively studied in the literature, not much attention has been paid to this problem under secrecy constraint. In this work, we study the ergodic secret capacity of a multiple-input multiple-output multiple-antenna-eavesdropper (MIMOME) wiretap channel with quantized channel state information (CSI) at the transmitter and perfect CSI at the legitimate receiver, under the assumption that only the statistics of eavesdropper CSI is known at the transmitter. We refine the analysis of the *random vector quantization* (RVQ) based artificial noise (AN) scheme in [1], where a *heuristic* upper bound on the secrecy rate loss, when compared to the perfect CSI case, was given. We propose a lower bound on the ergodic secrecy capacity. We show that the lower bound and the secrecy capacity with perfect CSI coincide asymptotically as the number of feedback bits and the AN power go to infinity. For practical applications, we propose a very efficient quantization codebook construction method for the two transmit antennas case.**

***Index Terms*—artificial noise, secret capacity, physical layer security, wiretap channel.**

I. INTRODUCTION

Complexity-based cryptographic technologies (e.g. AES [2]) have traditionally been used to provide a secure gateway for communications and data exchanges at the network layer. The security is achieved if an eavesdropper (Eve) without the key cannot decipher the message in a reasonable amount of time. This premise becomes controversial with the rapid developments of computing devices (e.g. quantum computer). In contrast, physical layer security (PLS) does not depend on a specific computational model and can provide security even when Eve has unlimited computing power. Wyner [3] and later Csiszár and Körner [4] proposed the *wiretap channel* model as a basic framework for PLS. Wyner has shown that for discrete memoryless channels, if Eve intercepts a degraded version of the intended receiver's (Bob's) signal, a prescribed degree of data confidentiality could be simultaneously attained by channel coding without any secret key. The associated notion of *secrecy capacity* was introduced to characterize the maximum transmission rate from the transmitter (Alice) to Bob, below which Eve is unable to obtain any information.

Wyner's wiretap channel model has been extended to fading channel [5], Gaussian broadcast channel [6], multiple-input single-output multiple-antenna-eavesdropper (MISOME) channel [7], and multiple-input multiple-output multiple-antenna-eavesdropper (MIMOME) channel [8]. All these works rely on the perfect knowledge of Bob's channel state information (CSI) at Alice to compute the secrecy capacity and enable secure encoding. In particular, Eve's CSI is also assumed to be known at Alice in [6], [8], although the CSI of a passive Eve is very hard to be unveiled at Alice. It is more reasonable to assume that Alice only knows the statistics of Eve's channel. Even the assumption of perfect knowing Bob's CSI is not realistic. In practice, Bob can only provide Alice with a quantized version of his CSI via a rate constrained feedback channel (i.e., finite-rate feedback).

In this work, we are interested in the secrecy capacity conditioned on the quantized CSI of Bob's channel and the statistics of Eve's channel. While the impact of finite-rate feedback on the capacity of fading channels has been extensively studied (see [9]–[13]), not much attention has been given to this problem under secrecy constraint. In [14], assuming that Alice only knows the statistics of Eve's channel, the authors derived lower and upper bounds on the ergodic secrecy capacity for a single-input single-output single-antenna-eavesdropper (SISOSE) system with finite-rate feedback of Bob's CSI. In the MIMOME scenario, the artificial noise (AN) scheme has been shown to guarantee positive secrecy capacity without knowing Eve's CSI in [15]. Alice is assumed to have perfect knowledge of Bob's eigenchannel vectors. This assumption allows her to align artificial noise within the null space of a MIMO channel between Alice and Bob, so that only Eve's equivocation is enhanced. In [1], the authors show that if only quantized CSI is available at Alice, the artificial noise will leak into Bob's channel, causing a decrease in the achievable secrecy rate. A *heuristic* upper bound on the secrecy rate loss (compared to the perfect CSI case) is proposed in [1, Eq. 34].

The main contribution of this paper is to provide a lower bound on the ergodic secrecy capacity for the AN scheme with quantized CSI, valid for any number of Alice/Bob/Eve antennas, as well as for any Bob/Eve signal-to-noise ratio (SNR) regimes. Following the work in [1], we use the *random vector quantization* (RVQ) scheme in [9]. Namely, given B feedback bits, Bob quantizes his eigenchannel matrix to one of $N = 2^B$ random unitary matrices and feeds back the corresponding index. We first show that RVQ is asymptotically optimal for security purpose, i.e., the secrecy capacity/rate loss compared to the perfect CSI case converges to 0 as $B \to \infty$. This result implies that the heuristic bound in [1, Eq. 34] is

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 Australian Research Council Discovery Project with ARC DP130100336.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TWC.2015.2417886, IEEE Transactions on Wireless Communications

not tight, since it reduces to a positive constant as $B \to \infty$. To refine the analysis in [1], we establish a tighter upper bound on the secrecy rate loss, which leads to an explicit lower bound on the ergodic secrecy capacity. We further show that the lower bound and the secrecy capacity with perfect CSI coincide asymptotically as B and the AN power go to infinity. This allows us to provide a sufficient condition guaranteeing positive secrecy capacity.

From a practical point of view, it is often desirable to use a deterministic quantization codebook rather than a random one. The problem of derandomizing RVQ codebooks is related to discretizing the complex Grassmannian manifold [9], [10]. Since the optimal constructions are possible only in very special cases, deterministic codebooks are mostly generated by computer search [16]. Interestingly, the case of codebook design with two transmit antennas is equivalent to quantizing a real sphere [13]. According to this fact, we propose a very efficient codebook construction method for the two-antenna case. Simulation results demonstrate that near-RVQ performance is achieved by a moderate number of feedback bits.

The novelty of this paper is to give a complete answer to the question: how to guarantee secrecy for MIMOME wiretap channels with finite-rate feedback? The pioneering works in [1] and [14] haven't actually solved this problem. Our analytical results show that a positive ergodic secrecy capacity for MIMOME channel with quantized CSI is always achieved by using RVQ-based AN transmission scheme and Gaussian input alphabets in high AN power limit. This new finding justifies the use of AN scheme in practical limited feedback systems.

It is worth mentioning that the latest work of Liang *et al.* [17] studies the problem of knowing only statistics of Bob's CSI in SISOSE wiretap channel. The security of Liang *et al.*'s scheme relies on the *degraded channel assumption*, i.e., Eve's channel is worse than the main channel. In this work, we tackle the problem of how to guarantee secrecy when Eve's channel is non-degraded (e.g. can be noiseless). We induct the major benefits of knowing a quantized version of Bob's CSI: given a sufficient number of feedback bits B, Alice is able to apply the artificial noise technique to jam Eve, so that the positive secrecy capacity can be guaranteed for arbitrarily small Eve's channel noise variance. We believe that avoiding the degraded channel assumption is an interesting and fundamental problem.

The paper is organized as follows: Section II presents the system model, followed by the analysis of secrecy capacity with finite-rate feedback in Section III. Section IV provides the deterministic quantization codebook construction method for the two-antenna case. 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, while $\lfloor x \rfloor$ to the closest integer smaller than or equal to x and $\lceil x \rceil$ to the closest integer larger than or equal to x. 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 $\mathbf{A} \backsim W_m(n,\mathbf{\Sigma})$. Trace of a square matrix $\mathbf{B}$ is denoted by $\mathrm{Tr}(\mathbf{B})$. 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 $\mathbf{x} \in \mathbb{C}^{N_{\mathrm{A}}}$ 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.,

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

In this paper, we assume that Bob knows its own channel matrix $\mathbf{H}$ instantaneously and Eve knows both its own channel matrix $\mathbf{G}$ and the main channel $\mathbf{H}$, instantaneously; whereas Alice is only aware of the statistics of $\mathbf{H}$ and $\mathbf{G}$. There is also an error-free public feedback channel with limited capacity from Bob to Alice that can be tracked by Eve. In our setting, the feedback is exclusively used to send the index of the codeword in a quantization codebook that describes the main channel state information $\mathbf{H}$. The quantization codebook is assumed to be known *a priori* to Alice, Bob and Eve.

A. Artificial Noise Scheme with Perfect CSI

The original AN scheme assumes $N_{\mathrm{B}} < N_{\mathrm{A}}$, in order to ensure that $\mathbf{H}$ has a non-trivial null space with an orthonormal basis $\mathbf{Z} = \mathrm{null}(\mathbf{H}) \in \mathbb{C}^{N_{\mathrm{A}}\times(N_{\mathrm{A}}-N_{\mathrm{B}})}$ (such that $\mathbf{H}\mathbf{Z} = \mathbf{0}_{N_{\mathrm{B}}\times(N_{\mathrm{A}}-N_{\mathrm{B}})}$) [15]. Let $\mathbf{H} = \mathbf{U}\mathbf{\Lambda}\mathbf{V}^H$ be the singular value decomposition (SVD) of $\mathbf{H}$, where $\mathbf{U} \in \mathbb{C}^{N_{\mathrm{B}}\times N_{\mathrm{B}}}$ and $\mathbf{V} \in \mathbb{C}^{N_{\mathrm{A}}\times N_{\mathrm{A}}}$ are unitary matrices. Then, we can write the unitary matrix $\mathbf{V}$ as

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

where the N_{B} columns of $\tilde{\mathbf{V}} \in \mathbb{C}^{N_{\mathrm{A}}\times N_{\mathrm{B}}}$ span the orthogonal complement subspace to the null space spanned by the columns of $\mathbf{Z} \in \mathbb{C}^{N_{\mathrm{A}}\times(N_{\mathrm{A}}-N_{\mathrm{B}})}$.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TWC.2015.2417886, IEEE Transactions on Wireless Communications

With unlimited feedback (i.e., perfect CSI), Alice has perfect knowledge of the precoding matrix $\mathbf{V}$, and transmits

$$\mathbf{x} = \tilde{\mathbf{V}}\mathbf{u} + \mathbf{Z}\mathbf{v} = \mathbf{V}\left[\begin{array}{c}\mathbf{u}\\ \mathbf{v}\end{array}\right], \tag{5}$$

where $\mathbf{u} \in \mathbb{C}^{N_{\mathrm{B}}}$ is the information vector and $\mathbf{v} \in \mathbb{C}^{(N_{\mathrm{A}}-N_{\mathrm{B}})}$ is the "artificial noise". For the purpose of evaluating the achievable secrecy rate, both $\mathbf{u}$ and $\mathbf{v}$ are assumed to be circular symmetric Gaussian 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. In [18], we have shown that Gaussian input alphabets asymptotically achieves the secrecy capacity as $\sigma_{\mathrm{v}}^2 \to \infty$.

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

$$\mathbf{z} = \mathbf{H}\tilde{\mathbf{V}}\mathbf{u} + \mathbf{H}\mathbf{Z}\mathbf{v} + \mathbf{n}_{\mathrm{B}} = \mathbf{H}\tilde{\mathbf{V}}\mathbf{u} + \mathbf{n}_{\mathrm{B}}, \tag{6}$$
$$\mathbf{y} = \mathbf{G}\tilde{\mathbf{V}}\mathbf{u} + \mathbf{G}\mathbf{Z}\mathbf{v} + \mathbf{n}_{\mathrm{E}}, \tag{7}$$

to show that with unlimited feedback, the artificial noise only degrades Eve's channel, resulting in increased secrecy capacity (compared to the non-AN case).

B. Artificial Noise Scheme with Quantized CSI

In [1], the authors analyzed the impact of finite-rate feedback on the secrecy rate achievable by the AN scheme. To quantize the matrix $\tilde{\mathbf{V}}$ in (4), the random vector quantization (RVQ) scheme in [9] is used. Given B feedback bits per fading channel, Bob specifies $\tilde{\mathbf{V}}$ from a random quantization codebook

$$\mathcal{V} = \left\{\tilde{\mathbf{V}}_i, 1 \le i \le 2^B\right\}, \tag{8}$$

where the entries are independent $N_{\mathrm{A}} \times N_{\mathrm{B}}$ random unitary matrices, i.e., $\tilde{\mathbf{V}}_i^H \tilde{\mathbf{V}}_i = \mathbf{I}_{N_{\mathrm{B}}}$. The codebook $\mathcal{V}$ is known *a priori* to all Alice, Bob and Eve. Bob selects the $\tilde{\mathbf{V}}_j$ that minimize the chordal distance between $\tilde{\mathbf{V}}_i$ and $\tilde{\mathbf{V}}$ [11]:

$$\tilde{\mathbf{V}}_j = \min_{\tilde{\mathbf{V}}_i \in \mathcal{V}} d^2\left(\tilde{\mathbf{V}}_i, \tilde{\mathbf{V}}\right), \tag{9}$$

where

$$d\left(\tilde{\mathbf{V}}_i, \tilde{\mathbf{V}}\right) = N_{\mathrm{B}} - \mathrm{Tr}\left(\tilde{\mathbf{V}}^H \tilde{\mathbf{V}}_i \tilde{\mathbf{V}}_i^H \tilde{\mathbf{V}}\right). \tag{10}$$

Note that $\mathrm{Tr}\,(\mathbf{A})$ denotes the trace of the square matrix $\mathbf{A}$. Then, Bob relays the corresponding index j back to Alice.

Alice generates the precoding matrix from $\tilde{\mathbf{V}}_j$ as follows. Let $\tilde{\mathbf{v}}_1, \ldots, \tilde{\mathbf{v}}_{N_{\mathrm{B}}}$ be the columns of $\tilde{\mathbf{V}}_j$, and $\mathbf{e}_1, \ldots, \mathbf{e}_{N_{\mathrm{A}}-N_{\mathrm{B}}}$ be the standard basis vectors. Alice applies the Gram-Schmidt algorithm to the matrix

$$[\tilde{\mathbf{v}}_1, \ldots, \tilde{\mathbf{v}}_{N_{\mathrm{B}}}, \mathbf{e}_1, \ldots, \mathbf{e}_{N_{\mathrm{A}}-N_{\mathrm{B}}}]$$

to generate the remaining orthonormal basis vectors spanning the orthogonal complement space to the one generated by the columns of $\tilde{\mathbf{V}}_j$. This provides Alice with a unitary matrix

$$\hat{\mathbf{V}} = [\tilde{\mathbf{V}}_j, \hat{\mathbf{Z}}] \in \mathbb{C}^{N_{\mathrm{A}} \times N_{\mathrm{A}}}, \tag{11}$$

that can be used to precode $\mathbf{u}$ and $\mathbf{v}$ as in (5).

Since $\hat{\mathbf{Z}} \neq \mathbf{Z}$, the interference term $\mathbf{H}\hat{\mathbf{Z}}\mathbf{v}$ cannot be nulled at Bob. Therefore, equations (6) and (7) reduce to

$$\mathbf{z} = \mathbf{H}\tilde{\mathbf{V}}_j\mathbf{u} + \mathbf{H}\hat{\mathbf{Z}}\mathbf{v} + \mathbf{n}_{\mathrm{B}}, \tag{12}$$
$$\mathbf{y} = \mathbf{G}\tilde{\mathbf{V}}_j\mathbf{u} + \mathbf{G}\hat{\mathbf{Z}}\mathbf{v} + \mathbf{n}_{\mathrm{E}}, \tag{13}$$

and show that with finite rate feedback (i.e., quantized CSI), some of the artificial noise will inevitably leak into the main channel from Alice to Bob, causing degradation in the secrecy capacity (compared to the unlimited feedback case).

C. Assumptions and Notations

The analysis in [1], [15] are based on the assumption of $N_{\mathrm{E}} < N_{\mathrm{A}}$. Clearly, this assumption is not always realistic. In this work, we remove this assumption and evaluate the secrecy capacity for any number of Eve antennas.

Since $\hat{\mathbf{V}}$ in (11) is a unitary matrix, the total transmission power can be written as

$$||\mathbf{x}||^2 = \left[\begin{array}{c}\mathbf{u}\\ \mathbf{v}\end{array}\right]^H \hat{\mathbf{V}}^H \hat{\mathbf{V}} \left[\begin{array}{c}\mathbf{u}\\ \mathbf{v}\end{array}\right] = ||\mathbf{u}||^2 + ||\mathbf{v}||^2. \tag{14}$$

Then the average transmit power constraint P is

$$P = \mathrm{E}(||\mathbf{x}||^2) = P_{\mathrm{u}} + P_{\mathrm{v}}, \tag{15}$$

where

$$\begin{array}{rcl} P_{\mathrm{u}} & = & \mathrm{E}(||\mathbf{u}||^2) = \sigma_{\mathrm{u}}^2 N_{\mathrm{B}}, \\ P_{\mathrm{v}} & = & \mathrm{E}(||\mathbf{v}||^2) = \sigma_{\mathrm{v}}^2 (N_{\mathrm{A}} - N_{\mathrm{B}}), \end{array} \tag{16}$$

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

We define Bob's and Eve's SNRs as

- $\mathrm{SNR_B} \triangleq \sigma_{\mathrm{u}}^2/\sigma_{\mathrm{B}}^2$
- $\mathrm{SNR_E} \triangleq \sigma_{\mathrm{u}}^2/\sigma_{\mathrm{E}}^2$

To simplify our notation, we define three system parameters:

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

Note that $\mathrm{SNR_B} = \alpha\gamma$. If $\gamma > 1$, then Eve has a worse SNR than Bob. Since we have normalized σ_{B}^2 to one, we can rewrite (16) as

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

D. Instantaneous and Ergodic Secrecy Capacities

We recall from [8] the definition of *instantaneous secrecy capacity* for MIMOME channel:

$$C_{\mathrm{S}} \triangleq \max_{p(\mathbf{u})} \left\{I(\mathbf{u};\mathbf{z}) - I(\mathbf{u};\mathbf{y})\right\}, \tag{17}$$

where $\mathbf{u}$ is an auxiliary random vector used in the secrecy capacity characterization, which satisfies the Markov relationship $\mathbf{u} \to \mathbf{x} \to (\mathbf{z}, \mathbf{H}), (\mathbf{y}, \mathbf{H}, \mathbf{G})$. The maximum in (17) 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 channel randomness, we further define the *ergodic secrecy capacity*, as in [15]

$$\mathrm{E}(C_{\mathrm{S}}) \triangleq \max_{p(\mathbf{u})} \left\{I(\mathbf{u};\mathbf{z}|\mathbf{H}) - I(\mathbf{u};\mathbf{y}|\mathbf{H},\, \mathbf{G})\right\}, \tag{18}$$

where $\mathbf{u}$ is an auxiliary random vector as above. Note that $I\,(X;Y|Z) \triangleq \mathrm{E}_Z\,[I\,(X;Y)\,|Z]$, following the notation in [19].

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TWC.2015.2417886, IEEE Transactions on Wireless Communications

Since closed form expressions for C_{S} and $\mathrm{E}(C_{\mathrm{S}})$ are not always available, we often consider the *corresponding secrecy rates*, given by

$$R_{\mathrm{S}} \triangleq I(\mathbf{u};\mathbf{z}) - I(\mathbf{u};\mathbf{y}), \tag{19}$$

$$\mathrm{E}(R_{\mathrm{S}}) \triangleq I(\mathbf{u};\mathbf{z}|\mathbf{H}) - I(\mathbf{u};\mathbf{y}|\mathbf{H},\mathbf{G}), \tag{20}$$

where $\mathbf{v}$ and $\mathbf{u}$ are assumed to be 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, for the purposes of characterizing the achievable secrecy rate.

Under the original AN framework in (6) and (7), the achievable secrecy rate with perfect CSI can be written as

$$\begin{aligned} R_{\mathrm{S}} = \log\left|\mathbf{I}_{N_{\mathrm{B}}} + \alpha\gamma\mathbf{H}\mathbf{H}^H\right| + \log\left|\mathbf{I}_{N_{\mathrm{E}}} + \alpha\beta(\mathbf{G}\mathbf{Z})(\mathbf{G}\mathbf{Z})^H\right| \\ - \log\left|\mathbf{I}_{N_{\mathrm{E}}} + \alpha(\mathbf{G}\tilde{\mathbf{V}})(\mathbf{G}\tilde{\mathbf{V}})^H + \alpha\beta(\mathbf{G}\mathbf{Z})(\mathbf{G}\mathbf{Z})^H\right|. \end{aligned} \tag{21}$$

The closed-form expression of $\mathrm{E}(R_{\mathrm{S}})$ can be found in [18, Th. 1]. It is shown that the achievable secrecy rate $\mathrm{E}(R_{\mathrm{S}})$ converges to the ergodic secrecy capacity with AN-beamforming, as the AN power $P_{\mathrm{v}} \to \infty$ in [18, Th. 3].

Remark 1: For the reader's convenience, we summarize the idea in [18, Th. 3]. A universal upper bound on $\mathrm{E}(C_{\mathrm{S}})$ is

$$\begin{aligned} \mathrm{E}(C_{\mathrm{S}}) &= \max_{p(\mathbf{u})}\{I(\mathbf{u};\mathbf{z}|\mathbf{H}) - I(\mathbf{u};\mathbf{y}|\mathbf{H},\,\mathbf{G})\} \\ &\le \max_{p(\mathbf{u})}\{I(\mathbf{u};\mathbf{z}|\mathbf{H})\} \triangleq \bar{C}_{\mathrm{Bob}}, \end{aligned} \tag{22}$$

where $\bar{C}_{\mathrm{Bob}}$ represents Bob's ergodic channel capacity with perfect CSI. In other words, the secrecy capacity cannot be greater than the main channel capacity. In [18, Th. 3], we have shown that if $N_{\mathrm{E}} \le N_{\mathrm{A}} - N_{\mathrm{B}}$, as $P_{\mathrm{v}} \to \infty$,

$$\mathrm{E}(R_{\mathrm{S}}) \to \bar{C}_{\mathrm{Bob}}, \tag{23}$$

which means that no input is better than Gaussian, under the original AN framework in [15].

Under the RVQ-based AN framework in (12) and (13), the achievable secrecy rate with quantized CSI can be written as

$$\begin{aligned} R_{\mathrm{S,Q}} = \log\frac{\left|\mathbf{I}_{N_{\mathrm{B}}} + \alpha\gamma(\mathbf{H}\tilde{\mathbf{V}}_j)(\mathbf{H}\tilde{\mathbf{V}}_j)^H + \alpha\beta\gamma(\mathbf{H}\hat{\mathbf{Z}})(\mathbf{H}\hat{\mathbf{Z}})^H\right|}{\left|\mathbf{I}_{N_{\mathrm{B}}} + \alpha\beta\gamma(\mathbf{H}\hat{\mathbf{Z}})(\mathbf{H}\hat{\mathbf{Z}})^H\right|} \\ - \log\frac{\left|\mathbf{I}_{N_{\mathrm{E}}} + \alpha(\mathbf{G}\mathbf{V}_{1,j})(\mathbf{G}\tilde{\mathbf{V}}_j)^H + \alpha\beta(\mathbf{G}\hat{\mathbf{Z}})(\mathbf{G}\hat{\mathbf{Z}})^H\right|}{\left|\mathbf{I}_{N_{\mathrm{E}}} + \alpha\beta(\mathbf{G}\hat{\mathbf{Z}})(\mathbf{G}\hat{\mathbf{Z}})^H\right|}. \end{aligned} \tag{24}$$

In the special case of $N_{\mathrm{E}} \le N_{\mathrm{B}}$, the ergodic MIMOME secrecy capacity with statistical CSI, i.e., $\mathrm{E}(C_{\mathrm{S}})$, was recently reported in [20]. However, the ergodic MIMOME secrecy capacity with quantized CSI, denoted by $\mathrm{E}(C_{\mathrm{S,Q}})$, remains an open problem. In this work, we focus on bounding $\mathrm{E}(C_{\mathrm{S,Q}})$ under the RVQ-based AN framework.

E. Open Problems and Motivations

Using [21, Eq. 2, pp. 56], it is simple to show that

$$\mathrm{E}(R_{\mathrm{S}}) \ge \mathrm{E}(R_{\mathrm{S,Q}}). \tag{25}$$

In [1], the *ergodic secrecy rate loss* is defined by:

$$\mathrm{E}(\Delta R_{\mathrm{S}}) \triangleq \mathrm{E}(R_{\mathrm{S}}) - \mathrm{E}(R_{\mathrm{S,Q}}). \tag{26}$$

A heuristic upper bound was proposed in [1, Eq. 34]:

$$\begin{aligned} \mathrm{E}(\Delta R_{\mathrm{S}}) \lessapprox N_{\mathrm{B}}\log\left(\frac{N_{\mathrm{B}} + \alpha\beta\gamma N_{\mathrm{A}} D\left(N_{\mathrm{A}}, N_{\mathrm{B}}, 2^B\right)}{N_{\mathrm{B}} - D\left(N_{\mathrm{A}}, N_{\mathrm{B}}, 2^B\right)}\right) \\ + N_{\mathrm{B}}\log\left(1 + \frac{1}{\alpha\gamma\left(N_{\mathrm{A}} - N_{\mathrm{B}}\right)}\right) \triangleq \mathrm{UB}_{\text{heuristic}}. \end{aligned} \tag{27}$$

where

$$D\left(N_{\mathrm{A}}, N_{\mathrm{B}}, 2^B\right) = \mathrm{E}\left(d^2\left(\tilde{\mathbf{V}}_j, \tilde{\mathbf{V}}\right)\right), \tag{28}$$

and $d(\cdot,\cdot)$ is give in (10).

Note that the asymptotic inequality "$\lessapprox$" in (27) means "purely heuristic". However, (27) is insufficient to characterize the impact of quantized CSI on the secrecy rate achievable by the AN scheme. To show this, we use the following:

Proposition 1: For the RVQ-based AN scheme, as $B \to \infty$,

$$\hat{\mathbf{V}} \to \mathbf{V}, \tag{29}$$

where $\mathbf{V}$ is given in (4) and $\hat{\mathbf{V}}$ is given in (11).

Proof. See Appendix A. □

Proposition 1 shows the RVQ scheme is asymptotically optimal for large B, i.e., the secrecy capacity/rate loss (compared to the perfect CSI case) converges to zero. In contrast, as $B \to \infty$, $\mathrm{UB}_{\text{heuristic}}$ in (27) reduces to a positive constant:

$$\mathrm{UB}_{\text{heuristic}} \to N_{\mathrm{B}}\log\left(1 + \frac{1}{\alpha\gamma\left(N_{\mathrm{A}} - N_{\mathrm{B}}\right)}\right), \tag{30}$$

since $D\left(N_{\mathrm{A}}, N_{\mathrm{B}}, 2^B\right) \to 0$ as $B \to \infty$ [11]. Hence, the heuristic bound in (27) is not tight.

Remark 2: The ergodic secrecy capacity with quantized CS $\mathrm{E}(C_{\mathrm{S,Q}})$, is lower bounded by

$$\mathrm{E}(C_{\mathrm{S,Q}}) \ge \mathrm{E}(R_{\mathrm{S,Q}}) = \mathrm{E}(R_{\mathrm{S}}) - \mathrm{E}(\Delta R_{\mathrm{S}}). \tag{31}$$

Using the closed-form expression of $\mathrm{E}(R_{\mathrm{S}})$ given in [18, Th. 1], we are motivated to establish a tighter upper bound on $\mathrm{E}(\Delta R_{\mathrm{S}})$, which allows us to obtain a lower bound on $\mathrm{E}(C_{\mathrm{S,Q}})$.

We would like to emphasize that the difficulty of computing $\mathrm{E}(\Delta R_{\mathrm{S}})$ is in evaluating the first term in (24). The existing results in [9]–[13] consider the impact of finite-rate feedback on the capacity of fading channels, rather than on the secrecy capacity of wiretap channels. More specifically, those results focus on computing

$$\mathrm{E}\left(\log\left|\mathbf{I}_{N_{\mathrm{B}}} + \alpha\gamma(\mathbf{H}\tilde{\mathbf{V}}_j)(\mathbf{H}\tilde{\mathbf{V}}_j)^H\right|\right), \tag{32}$$

thus cannot be applied directly to computation of $\mathrm{E}(\Delta R_{\mathrm{S}})$.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TWC.2015.2417886, IEEE Transactions on Wireless Communications

III. Bounds and Achievability on Secrecy Capacity with Quantized CSI

In this section, we wish to determine the secrecy capacity with RVQ-based AN scheme. A tight upper bound on the ergodic secrecy rate loss and a lower bound on the ergodic secrecy capacity are provided in Theorem 1 and Theorem 3, respectively. In Theorem 4, we show that the lower bound and the secrecy capacity with perfect/quantized CSI coincide asymptotically as B and P_{v} go to infinity. This provides a sufficient condition guaranteeing positive secrecy capacity.

In summary, the novelty of our main results is to link the practical secure transmission scheme, i.e., RVQ-based AN scheme, with the information-theoretic security measure, i.e., secrecy capacity.

To describe our result, we first recall the following function from [22]:

$$\Theta(m,n,x) \triangleq e^{-1/x} \sum_{k=0}^{m-1}\sum_{l=0}^{k}\sum_{i=0}^{2l} \left\{ \frac{(-1)^i (2l)!(n-m+i)!}{2^{2k-i} l! i! (n-m+l)!} \cdot \binom{2(k-l)}{k-l} \cdot \binom{2(l+n-m)}{2l-i} \cdot \sum_{j=0}^{n-m+i} x^{-j}\Gamma(-j,1/x) \right\}, \tag{33}$$

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

$$\Gamma(a,b) = \int_b^\infty x^{a-1} e^{-x} dx. \tag{34}$$

We further define

$$N_{\min} \triangleq \min\{N_{\mathrm{E}},\, N_{\mathrm{A}} - N_{\mathrm{B}}\}, \tag{35}$$
$$N_{\max} \triangleq \max\{N_{\mathrm{E}},\, N_{\mathrm{A}} - N_{\mathrm{B}}\}, \tag{36}$$
$$\hat{N}_{\min} \triangleq \min\{N_{\mathrm{E}},\, N_{\mathrm{A}}\}, \tag{37}$$
$$\hat{N}_{\max} \triangleq \max\{N_{\mathrm{E}},\, N_{\mathrm{A}}\}. \tag{38}$$

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

$$\theta_i \triangleq \begin{cases} \alpha & 1 \leq i \leq N_{\mathrm{B}} \\ \alpha\beta & N_{\mathrm{B}}+1 \leq i \leq N_{\mathrm{A}} \end{cases} \tag{39}$$

We recall from [11, Th. 4] that

$$\mu\left(N_{\mathrm{A}}, N_{\mathrm{B}}, 2^B\right) \leq D\left(N_{\mathrm{A}}, N_{\mathrm{B}}, 2^B\right) \leq \eta\left(N_{\mathrm{A}}, N_{\mathrm{B}}, 2^B\right), \tag{40}$$

where $D(\cdot,\cdot,\cdot)$ is given in (28) and

$$\eta(n,p,K) = \frac{\Gamma\left(\frac{1}{p(n-p)}\right)}{p(n-p)} \left(Kc(n,p)\right)^{-\frac{1}{p(n-p)}} + p\exp(-\left(Kc(n,p)\right)^{1-\zeta}), \tag{41}$$

$$\mu(n,p,K) = \frac{p(n-p)}{p(n-p)+1}\left(Kc(n,p)\right)^{-\frac{1}{p(n-p)}}, \tag{42}$$

$$c(n,p) = \begin{cases} \dfrac{1}{\Gamma(p(n-p)+1)} \displaystyle\prod_{i=1}^{p} \frac{\Gamma(n-i+1)}{\Gamma(p-i+1)}, & n \geq 2p \\ \dfrac{1}{\Gamma(p(n-p)+1)} \displaystyle\prod_{i=1}^{n-p} \frac{\Gamma(n-i+1)}{\Gamma(n-p-i+1)}, & n \leq 2p \end{cases} \tag{43}$$

for any $0 < \zeta < 1$. Note that $\Gamma(a)$ is the Gamma function.

A. Bounds on Ergodic/Instantaneous Secrecy Rate Loss

We first consider the ergodic secrecy rate loss $\mathrm{E}(\Delta R_{\mathrm{S}})$.

Theorem 1: Let $\theta_{\min} = \min\{\alpha\gamma, \alpha\beta\gamma\}$. We have

$$\mathrm{E}(\Delta R_{\mathrm{S}}) \leq \Theta(N_{\mathrm{B}}, N_{\mathrm{A}}, \alpha\gamma) - \Theta(N_{\mathrm{B}}, N_{\mathrm{A}}, \theta_{\min}) + \Theta\left(N_{\mathrm{B}}, N_{\mathrm{A}}, \alpha\beta\gamma\frac{\eta\left(N_{\mathrm{A}}, N_{\mathrm{B}}, 2^B\right)}{N_{\mathrm{B}}}\right) \triangleq \mathrm{UB}, \tag{44}$$

where $\Theta(\cdot,\cdot,\cdot)$ is given in (33) and $\eta(\cdot,\cdot,\cdot)$ is given in (41).

Proof. See Appendix B. □

Theorem 1 gives a tight upper bound on $\mathrm{E}(\Delta R_{\mathrm{S}})$, for any number of Alice/Bob/Eve antennas, as well as for any Bob/Eve SNR regimes.

Remark 3: The function $\Theta(m,n,x)$ represents the closed-form expression of the ergodic capacity of MIMO Rayleigh-fading channels [22], where x represents the SNR. For example, $\mathrm{E}\left(\log\left|\mathbf{I}_{N_{\mathrm{B}}} + x\mathbf{H}\mathbf{H}^H\right|\right) = \Theta(N_{\mathrm{B}}, N_{\mathrm{A}}, x)$. The properties of $\Theta(m,n,x)$ are well studied and can be found in many literatures, for example, [23]. Most importantly, $\Theta(m,n,x)$ is a non-negative increasing function of x. It is easy to see that UB in (44) is always non-negative, since $\alpha\gamma \geq \theta_{\min}$. Due to the fact $\lim_{B\to\infty} \eta\left(N_{\mathrm{A}}, N_{\mathrm{B}}, 2^B\right) = 0$, if $\beta \geq 1$, we have

$$\lim_{B\to\infty} \mathrm{UB} = \log|\mathbf{I}_{N_{\mathrm{B}}}| = 0, \tag{45}$$

which is consistent with Proposition 1.

Remark 4: UB in (44) does not depend on the number of antennas at Eve N_{E}. This is because $\mathrm{E}(\Delta R_{\mathrm{S}})$ itself does not depend on N_{E}. As shown in the proof of Theorem 1, we have

$$\mathrm{E}(\Delta R_{\mathrm{S}}) = \mathrm{E}\left(\log\left|\mathbf{I}_{N_{\mathrm{B}}} + \alpha\gamma\mathbf{H}\mathbf{H}^H\right|\right) - \mathrm{E}\left(\log\frac{\left|\mathbf{I}_{N_{\mathrm{B}}} + \alpha\gamma(\mathbf{H}\tilde{\mathbf{V}}_j)(\mathbf{H}\tilde{\mathbf{V}}_j)^H + \alpha\beta\gamma(\mathbf{H}\hat{\mathbf{Z}})(\mathbf{H}\hat{\mathbf{Z}})^H\right|}{\left|\mathbf{I}_{N_{\mathrm{B}}} + \alpha\beta\gamma(\mathbf{H}\hat{\mathbf{Z}})(\mathbf{H}\hat{\mathbf{Z}})^H\right|}\right), \tag{46}$$

which is unrelated to $\mathbf{G}$ and N_{E}. In other words, finite-rate feedback only degrades the main channel.

Example 1: Let us apply Theorem 1 to the analysis of a RVQ-based AN scheme with $\beta = 1$, $\alpha\gamma = 1$, $N_{\mathrm{A}} = 4$ and $N_{\mathrm{B}} = 2$. The numerical result in Fig. 1 shows that the proposed upper bound in (44) is much tighter than the heuristic one in (27), and captures the behavior of $\mathrm{E}(\Delta R_{\mathrm{S}})$.

We then study the distribution of instantaneous secrecy rate loss, defined by

$$\Delta R_{\mathrm{S}} \triangleq R_{\mathrm{S}} - R_{\mathrm{S,Q}}. \tag{47}$$

Here, we consider the large system limit as N_{A} and $B \to \infty$ with finite ratio B/N_{A}. An interesting case that leads to a closed-form bound can be found when $N_{\mathrm{B}} = N_{\mathrm{E}} = 1$.

Theorem 2: If $N_{\mathrm{B}} = N_{\mathrm{E}} = 1$, as N_{A} and $B \to \infty$ with $B/N_{\mathrm{A}} \to \bar{B}$,

$$\Delta R_{\mathrm{S}} \xrightarrow{a.s.} \log(1 + P/\beta) + \log\left(1 + 2^{-\bar{B}}P\right) - \log\left(1 + P + \frac{1-\beta}{\beta}(1-2^{-\bar{B}})P\right). \tag{48}$$

Proof. See Appendix C. □

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TWC.2015.2417886, IEEE Transactions on Wireless Communications

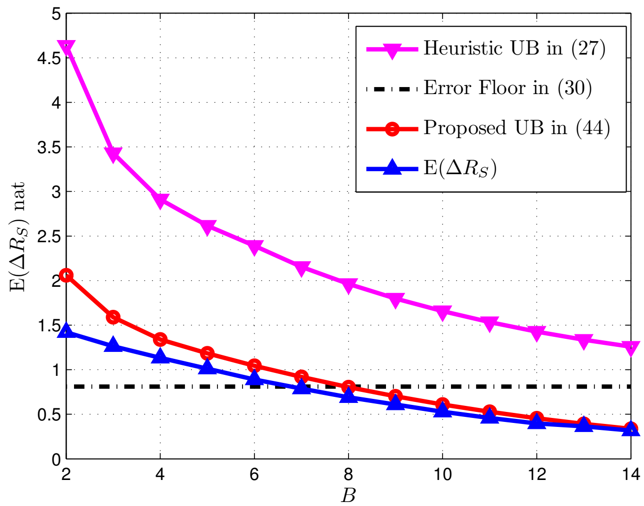

Fig. 1. $\mathrm{E}(\Delta R_{\mathrm{S}})$ vs. B with $\beta = 1$, $\alpha\gamma = 1$, $N_{\mathrm{A}} = 4$ and $N_{\mathrm{B}} = 2$.

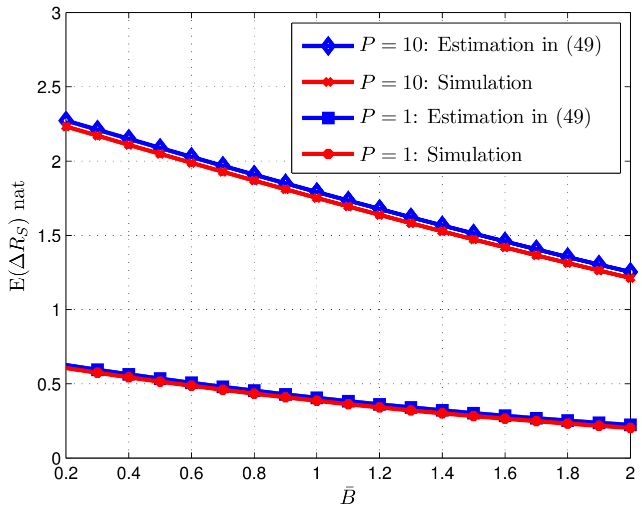

Fig. 2. $\mathrm{E}(\Delta R_{\mathrm{S}})$ vs. $\bar{B}$ with $\beta = 1$, $P = 1, 10$, $N_{\mathrm{A}} = 10$ and $N_{\mathrm{B}} = 1$.

Theorem 2 provides a closed-form asymptotic expression for ΔR_{S} when $N_{\mathrm{B}} = N_{\mathrm{E}} = 1$. Hence, the ergodic secrecy rate loss also converges to the same constant, as stated in the following corollary.

Corollary 1: Under the same assumptions of Theorem 2,

$$\mathrm{E}(\Delta R_{\mathrm{S}}) \to \log(1 + P/\beta) + \log\left(1 + 2^{-\bar{B}}P\right) - \log\left(1 + P + \frac{1-\beta}{\beta}(1 - 2^{-\bar{B}})P\right). \quad (49)$$

Proof. The proof is straightforward. □

Example 2: The numerical result in Fig. 2 shows that (49) is very accurate even for finite N_{A} and B.

B. A Lower Bound on Ergodic Secrecy Capacity

A lower bound on $\mathrm{E}(C_{\mathrm{S,Q}})$ can be derived using the results from (31), Theorem 1 and [18, Th. 1].

Theorem 3:

$$\mathrm{E}(C_{\mathrm{S,Q}}) \geq \Theta(N_{\min}, N_{\max}, \alpha\beta) - \Omega + \Theta(N_{\mathrm{B}}, N_{\mathrm{A}}, \theta_{\min}) - \Theta\left(N_{\mathrm{B}}, N_{\mathrm{A}}, \alpha\beta\gamma\frac{\eta\left(N_{\mathrm{A}}, N_{\mathrm{B}}, 2^{B}\right)}{N_{\mathrm{B}}}\right) \triangleq \bar{C}_{\mathrm{LB,Q}}, \quad (50)$$

where $\Theta(\cdot,\cdot,\cdot)$ is given in (33), $\eta(\cdot,\cdot,\cdot)$ is given in (41) and

$$\Omega = \begin{cases} K \sum_{k=1}^{\hat{N}_{\min}} \det\left(\mathbf{R}^{(k)}\right), & \beta \neq 1 \\ \Theta(\hat{N}_{\min}, \hat{N}_{\max}, \alpha), & \beta = 1 \end{cases} \quad (51)$$

$$K = \frac{(-1)^{N_{\mathrm{E}}(N_{\mathrm{A}} - \hat{N}_{\min})}}{\Gamma_{\hat{N}_{\min}}(N_{\mathrm{E}})} \frac{\prod_{i=1}^{2} \mu_i^{m_i N_{\mathrm{E}}}}{\prod_{i=1}^{2} \Gamma_{m_i}(m_i) \prod_{i<j} (\mu_i - \mu_j)^{m_i m_j}}, \quad (52)$$

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

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

$$r_{i,j}^{(k)} = \begin{cases} (\mu e_i)^{N_{\mathrm{A}} - j - d_i} \dfrac{(N_{\mathrm{A}} - j)!}{(N_{\mathrm{A}} - j - d_i)!}, & \hat{N}_{\min} + 1 \leq j \leq N_{\mathrm{A}} \\ (-1)^{d_i} \dfrac{\varphi(i,j)!}{(\mu_{e_i})^{\varphi(i,j)+1}}, & 1 \leq j \leq \hat{N}_{\min},\ j \neq k \\ (-1)^{d_i} \varphi(i,j)! e^{\mu_{e_i}} \sum_{l=0}^{\varphi(i,j)} \dfrac{\Gamma(l - \varphi(i,j), \mu_{e_i})}{(\mu_{e_i})^{l+1}}, & \text{otherwise} \end{cases} \quad (53)$$

where

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

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

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

Proof. See Appendix D. □

Theorem 3 gives a lower bound on $\mathrm{E}(C_{\mathrm{S,Q}})$, for any number of Alice/Bob/Eve antennas, as well as for any Bob/Eve SNR regimes. The lower bound in (50) is an increasing function of the number of feedback bits B. To guarantee a positive secrecy capacity, Alice just needs to increase B and checks whether $\bar{C}_{\mathrm{LB,Q}} > 0$.

Remark 5: We would like to emphasize that Theorem 3 does not overlap with our previous results in [18]. Recalling that

$$\mathrm{E}(C_{\mathrm{S,Q}}) \geq \mathrm{E}(R_{\mathrm{S,Q}}) = \mathrm{E}(R_{\mathrm{S}}) - \mathrm{E}(\Delta R_{\mathrm{S}}). \quad (54)$$

The closed-form expression of $\mathrm{E}(R_{\mathrm{S}})$ is given in [18, Th. 1], but we still have to bound $\mathrm{E}(\Delta R_{\mathrm{S}})$. Our key contribution is the explicit upper bound on $\mathrm{E}(\Delta R_{\mathrm{S}})$ in Theorem 1, which allows us to finally provide a lower bound on $\mathrm{E}\left(R_{\mathrm{S,Q}}\right)$.

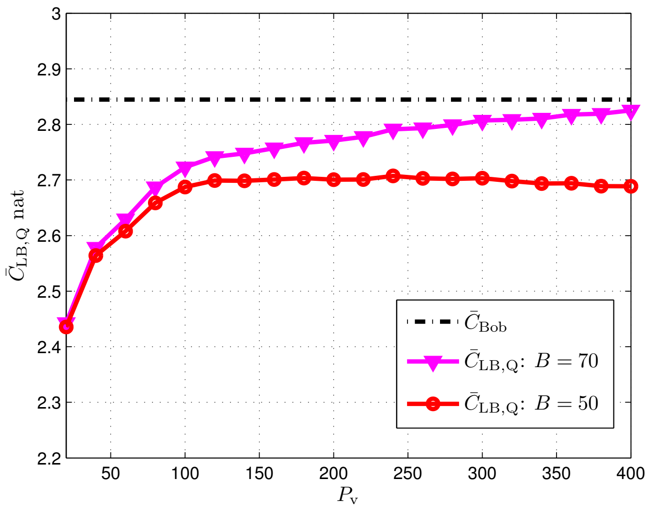

Fig. 3. $\bar{C}_{\mathrm{LB,Q}}$ vs. P_v with $N_A = 4$, $N_B = N_E = 2$, and $\alpha = \gamma = 1$.

C. *Positive Secrecy Capacity with Quantized CSI*

According to (18), a universal upper bound on $\mathrm{E}(C_{\mathrm{S,Q}})$ is

$$\mathrm{E}(C_{\mathrm{S,Q}}) \leq \mathrm{E}(C_{\mathrm{S}}) \leq \max_{p(\mathbf{u})} \{I(\mathbf{u}; \mathbf{z}|\mathbf{H})\} = \bar{C}_{\mathrm{Bob}}, \tag{55}$$

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

Combining (50) with (55), we obtain the following chain of inequalities

$$\bar{C}_{\mathrm{LB,Q}} \leq \mathrm{E}(C_{\mathrm{S,Q}}) \leq \mathrm{E}(C_{\mathrm{S}}) \leq \bar{C}_{\mathrm{Bob}}. \tag{56}$$

Note that $\bar{C}_{\mathrm{Bob}} > 0$. To characterize the achievability of positive secrecy capacity, we start by analyzing the difference between $\bar{C}_{\mathrm{LB,Q}}$ and $\bar{C}_{\mathrm{Bob}}$.

Theorem 4: If $N_E \leq N_A - N_B$ and $\beta \geq 1$, as α, β, $B \to \infty$,

$$\bar{C}_{\mathrm{LB,Q}} \to \mathrm{E}(C_{\mathrm{S,Q}}) \to \mathrm{E}(C_{\mathrm{S}}) \to \bar{C}_{\mathrm{Bob}}. \tag{57}$$

Proof. See Appendix E. □

Remark 6: We have shown that $\bar{C}_{\mathrm{LB,Q}}$, $\mathrm{E}(C_{\mathrm{S}})$ and $\bar{C}_{\mathrm{Bob}}$ coincide asymptotically as B and $P_v = \alpha\beta\gamma(N_A - N_B)$ go to infinity. This result guarantees that Eve is completely ineffective. This phenomenon is due to the fact that if $N_E \leq N_A - N_B$, as $P_v \to \infty$,

$$I(\mathbf{u}; \mathbf{y}|\mathbf{H}, \mathbf{G}) \to 0, \tag{58}$$

i.e., the AN scheme can jam all the eavesdropping in the high AN power limit. We refer the reader to [18, Th. 3] for details.

Remark 7: Note that $\bar{C}_{\mathrm{LB,Q}}$ is derived based on Gaussian input alphabets. From Theorem 4, we can conclude that a positive maximum secrecy capacity for MIMOME channel with quantized CSI is always achieved by using RVQ-based AN transmission scheme and Gaussian input alphabets for large B and P_v, if $N_E \leq N_A - N_B$.

Example 3: Fig. 3 compares $\bar{C}_{\mathrm{LB,Q}}$ and $\bar{C}_{\mathrm{Bob}}$ as a function of AN power P_v, with $N_A = 4$, $N_B = N_E = 2$, and $\alpha = \gamma = 1$. Since $P_u = \alpha\gamma N_B$ and $P_v = \alpha\beta\gamma(N_A - N_B)$, we have $P_u = 2$ and $P_v = 2\beta$. The simulation result shows that $\bar{C}_{\mathrm{LB,Q}}$ approaches to $\bar{C}_{\mathrm{Bob}}$ as P_v increases, for sufficiently large B.

IV. Implementation Using a Deterministic Codebook

In the previous section, random quantization codebooks have been used to prove new results on secrecy capacity with quantized CSI. The methods of constructing random unitary matrices $\tilde{\mathbf{V}}_i$ in (8) can be found in [24]. In practice, it is often desirable that the quantization codebook is deterministic. The problem of derandomizing RVQ codebooks is typically referred to as *Grassmannian subspace packing* [9], [10]. Despite of a few special cases (e.g., $B \leq 4$ [13]), analytical codebook design in general remains an intricate task. In this section, we propose a very efficient quantization codebook construction method for the case of $N_A = 2$ and $N_B = 1$.

According to [13, Eq. (20)], the codeword $\tilde{\mathbf{V}}_i$ can be expressed as

$$\tilde{\mathbf{V}}_i(\omega, \phi) = \begin{bmatrix} \cos\omega \\ e^{j\phi}\sin\omega \end{bmatrix}, \tag{59}$$

which fully describes the complex Grassmannian manifold $G_{2,1}$ by setting $0 \leq \phi \leq 2\pi$ and $0 \leq \omega \leq \pi/2$. Let $(\hat{\omega}, \hat{\phi})$ be spherical coordinates parameterizing the unit sphere S^2, where $0 \leq \hat{\phi} \leq 2\pi$ and $0 \leq \hat{\omega} \leq \pi$. In [13, Lemma 1], the authors further show that the map

$$\begin{array}{ccc} S^2 & \to & G_{2,1} \\ (\hat{\omega}, \hat{\phi}) & \longmapsto & \tilde{\mathbf{V}}_i(\hat{\omega}/2, \hat{\phi}) \end{array} \tag{60}$$

is an isomorphism. In other words, the sampling problem on $G_{2,1}$ can analogically be addressed on the real sphere S^2.

The method of sampling points uniformly from S^2 is provided in [25]. In details, one can parameterize $(x, y, z) \in S^2$ using spherical coordinates $(\hat{\omega}, \hat{\phi})$:

$$\begin{aligned} x &= \sin\hat{\omega}\cos\hat{\phi}, \\ y &= \sin\hat{\omega}\sin\hat{\phi}, \\ z &= \cos\hat{\omega}. \end{aligned} \tag{61}$$

The area element of S^2 is given by

$$\mathrm{d}S = \sin\hat{\omega}\mathrm{d}\hat{\omega}\mathrm{d}\hat{\phi} = -\mathrm{d}(\cos\hat{\omega})\,\mathrm{d}\hat{\phi}. \tag{62}$$

Hence, to obtain a uniform distribution over S^2, one has to pick $\hat{\phi} \in [0, 2\pi]$ and $t \in [-1, 1]$ uniformly and compute $\hat{\omega}$ by:

$$\hat{\omega} = \arccos t. \tag{63}$$

In this way $\cos\hat{\omega} = t$ will be uniformly distributed in $[-1, 1]$.

Based on above analysis, we give a straightforward method for codebook construction:

$$\hat{\mathcal{V}} = \left\{ \hat{\mathbf{V}}_{1,i} = \begin{bmatrix} \cos(0.5\arccos t_i) \\ e^{j\phi_i}\sin(0.5\arccos t_i) \end{bmatrix} \middle| i = 1, ..., 2^B \right\}, \tag{64}$$

where

$$\begin{aligned} t_i &= -1 + \frac{2\left\lceil i/2^{\lceil B/2\rceil}\right\rceil - 1}{2^{\lfloor B/2\rfloor}}, \end{aligned} \tag{65}$$

$$\begin{aligned} \phi_i &= \frac{2\pi\left(i \bmod 2^{\lceil B/2\rceil}\right)}{2^{\lceil B/2\rceil}}. \end{aligned} \tag{66}$$

Note that $\lfloor x \rfloor$ rounds to the closest integer smaller than or equal to x, while $\lceil x \rceil$ to the closest integer larger than or equal to x.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TWC.2015.2417886, IEEE Transactions on Wireless Communications

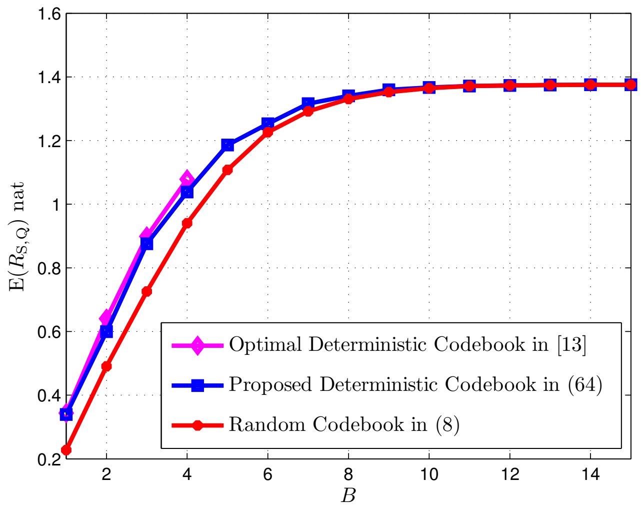

Fig. 4. $\mathrm{E}(R_{\mathrm{S,Q}})$ vs. B with $\beta = 2$, $\gamma = 1$, $P = 10$, $N_{\mathrm{A}} = 2$, and $N_{\mathrm{B}} = N_{\mathrm{E}} = 1$.

Using the deterministic codebook in (64) can save storage space on Alice, since she can generate the target codeword $\hat{\mathbf{V}}_{1,j}$ directly without the knowledge of the whole codebook $\hat{\mathcal{V}}$. We remark that the proposed codebook construction is valid for any B. This is different from the construction scheme in [13, Sec. VI-A], which is only possible for the case of $B \leq 4$.

Example 4: Fig. 4 examines the performance of the proposed codebook construction with $\beta = 2$, $\gamma = 1$, $P = 10$, and $N_{\mathrm{E}} = 1$. When $B \leq 4$, it is seen that the performance of codebook $\hat{\mathcal{V}}$ in (64) is indistinguishable from the optimal one in [13, Sec. VI-A]. When $B \geq 8$, the proposed codebook provides the same performance as the random one in (8).

Note that our codebook construction is based on the fact that the sampling problem on Grassmannian manifold $G_{2,1}$ can be reduced to one on the real sphere S^2 [13, Lemma 1]. For any arbitrary number of antennas, except for the special case of $N_{\mathrm{A}} = 2$ and $N_{\mathrm{B}} = 1$, this argument does not hold in general and deterministic codebooks are mostly generated by computer search [16].

V. Conclusions

In this work, we have discussed the problem of guaranteeing positive secrecy capacity for MIMOME channel with the quantized CSI of Bob's channel and the statistics of Eve's channel. We analyzed the RVQ-based AN scheme and provided a lower bound on the ergodic secrecy capacity. We proved that a positive secrecy capacity is always achievable by Gaussian input alphabets when $N_{\mathrm{E}} \leq N_{\mathrm{A}} - N_{\mathrm{B}}$, and the number of feedback bits B and the artificial noise power P_{v} are large enough. We also proposed an efficient implementation of discretizing the RVQ codebook which exhibits similar performance to that of random codebook.

Our results are based on the assumption that the feedback channel is error free. It would be interesting to see how the secrecy capacity deteriorates when there is a feedback error assuming the RVQ framework, e.g., delayed feedback [26] [27]. Totally understand that this might be a whole new topic. We will address this problem in our future work.

Appendix

A. Proof of Proposition 1

According to [12], as $B \to \infty$, the RVQ operation in (9) can guarantee

$$\tilde{\mathbf{V}}_j \to \tilde{\mathbf{V}}. \tag{67}$$

We then check the matrix $\hat{\mathbf{Z}}$ generated by Alice. The SVD decomposition of $\mathbf{H}$ can be written as

$$\mathbf{H} = \mathbf{U}\boldsymbol{\Lambda}\tilde{\mathbf{V}}^H. \tag{68}$$

From (67) and (68), as $B \to \infty$, we have

$$\mathbf{H}\hat{\mathbf{Z}} = \mathbf{U}\boldsymbol{\Lambda}\tilde{\mathbf{V}}^H\hat{\mathbf{Z}} \to \mathbf{U}\boldsymbol{\Lambda}\tilde{\mathbf{V}}_j^H\hat{\mathbf{Z}} = \mathbf{0}_{N_{\mathrm{A}}\times(N_{\mathrm{A}}-N_{\mathrm{B}})}, \tag{69}$$

which means

$$\hat{\mathbf{Z}} \to \mathrm{null}(\mathbf{H}). \tag{70}$$

From (11), (67) and (70), we have $\hat{\mathbf{V}} \to \mathbf{V}$ as $B \to \infty$. ∎

B. Proof of Theorem 1

Using [21, Eq. 12, pp. 55], we have

$$\begin{aligned} & \left|\mathbf{I}_{N_{\mathrm{B}}} + \alpha\gamma(\mathbf{H}\tilde{\mathbf{V}}_j)(\mathbf{H}\tilde{\mathbf{V}}_j)^H + \alpha\beta\gamma(\mathbf{H}\hat{\mathbf{Z}})(\mathbf{H}\hat{\mathbf{Z}})^H\right| \\ \geq\ & \left|\mathbf{I}_{N_{\mathrm{B}}} + \theta_{\min}(\mathbf{H}\tilde{\mathbf{V}}_j)(\mathbf{H}\tilde{\mathbf{V}}_j)^H + \theta_{\min}(\mathbf{H}\hat{\mathbf{Z}})(\mathbf{H}\hat{\mathbf{Z}})^H\right| \\ =\ & \left|\mathbf{I}_{N_{\mathrm{B}}} + \theta_{\min}\mathbf{H}\mathbf{H}^H\right|, \end{aligned} \tag{71}$$

where $\theta_{\min} = \min\{\alpha\gamma, \alpha\beta\gamma\}$.

Since the unitary matrix $\hat{\mathbf{V}} = [\tilde{\mathbf{V}}_j, \hat{\mathbf{Z}}]$ is independent of $\mathbf{G}$ and its realization is known to Alice, $\mathbf{G}\tilde{\mathbf{V}}_j \in \mathbb{C}^{N_{\mathrm{E}}\times N_{\mathrm{B}}}$ and $\mathbf{G}\hat{\mathbf{Z}} \in \mathbb{C}^{N_{\mathrm{E}}\times(N_{\mathrm{A}}-N_{\mathrm{B}})}$ are mutually independent complex Gaussian random matrices with i.i.d. entries [28, Th. 1]. We can write

$$\mathrm{E}\left(\log \frac{\left|\mathbf{I}_{N_{\mathrm{E}}} + \alpha(\mathbf{G}\tilde{\mathbf{V}}_j)(\mathbf{G}\tilde{\mathbf{V}}_j)^H + \alpha\beta(\mathbf{G}\hat{\mathbf{Z}})(\mathbf{G}\hat{\mathbf{Z}})^H\right|}{\left|\mathbf{I}_{N_{\mathrm{E}}} + \alpha\beta(\mathbf{G}\hat{\mathbf{Z}})(\mathbf{G}\hat{\mathbf{Z}})^H\right|}\right) \tag{72}$$

as the average of a function of $N_{\mathrm{E}} \times N_{\mathrm{A}}$ i.i.d complex Gaussian random variables $\sim \mathcal{N}_{\mathbb{C}}(0,1)$.

Similarly, with unlimited feedback, we have

$$\mathrm{E}\left(\log \frac{\left|\mathbf{I}_{N_{\mathrm{E}}} + \alpha(\mathbf{G}\tilde{\mathbf{V}})(\mathbf{G}\tilde{\mathbf{V}})^H + \alpha\beta(\mathbf{G}\mathbf{Z})(\mathbf{G}\mathbf{Z})^H\right|}{\left|\mathbf{I}_{N_{\mathrm{E}}} + \alpha\beta(\mathbf{G}\mathbf{Z})(\mathbf{G}\mathbf{Z})^H\right|}\right) \tag{73}$$

as the average of a function of $N_{\mathrm{E}} \times N_{\mathrm{A}}$ i.i.d complex Gaussian random variables $\sim \mathcal{N}_{\mathbb{C}}(0,1)$.

From (72) and (73), we have

$$\begin{aligned} & \mathrm{E}\left(\log \frac{\left|\mathbf{I}_{N_{\mathrm{E}}} + \alpha(\mathbf{G}\tilde{\mathbf{V}}_j)(\mathbf{G}\tilde{\mathbf{V}}_j)^H + \alpha\beta(\mathbf{G}\hat{\mathbf{Z}})(\mathbf{G}\hat{\mathbf{Z}})^H\right|}{\left|\mathbf{I}_{N_{\mathrm{E}}} + \alpha\beta(\mathbf{G}\hat{\mathbf{Z}})(\mathbf{G}\hat{\mathbf{Z}})^H\right|}\right) \\ =\ & \mathrm{E}\left(\log \frac{\left|\mathbf{I}_{N_{\mathrm{E}}} + \alpha(\mathbf{G}\tilde{\mathbf{V}})(\mathbf{G}\tilde{\mathbf{V}})^H + \alpha\beta(\mathbf{G}\mathbf{Z})(\mathbf{G}\mathbf{Z})^H\right|}{\left|\mathbf{I}_{N_{\mathrm{E}}} + \alpha\beta(\mathbf{G}\mathbf{Z})(\mathbf{G}\mathbf{Z})^H\right|}\right) \end{aligned} \tag{74}$$

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TWC.2015.2417886, IEEE Transactions on Wireless Communications

From (21), (24), (71) and (74), $\mathrm{E}(\Delta R_{\mathrm{S}})$ can be upper bounded by

$$\begin{aligned}\mathrm{E}(\Delta R_{\mathrm{S}}) \leq & \, \mathrm{E}\left(\log\left|\mathbf{I}_{N_{\mathrm{B}}}+\alpha\gamma\mathbf{H}\mathbf{H}^{H}\right|\right) \\ & - \mathrm{E}\left(\log\left|\mathbf{I}_{N_{\mathrm{B}}}+\theta_{\min}\mathbf{H}\mathbf{H}^{H}\right|\right) \\ & + \mathrm{E}\left(\log\left|\mathbf{I}_{N_{\mathrm{B}}}+\alpha\beta\gamma(\mathbf{H}\hat{\mathbf{Z}})(\mathbf{H}\hat{\mathbf{Z}})^{H}\right|\right). \end{aligned} \quad (75)$$

We remark that the upper bound (75) is better than the one in [1, Eq. (33)]. More specifically, we do not need to compute the term $\mathrm{E}\left(\log\left|\tilde{\mathbf{V}}^{H}\tilde{\mathbf{V}}_{j}\tilde{\mathbf{V}}_{j}^{H}\tilde{\mathbf{V}}\right|\right)$ in [1, Eq. (33)]. This new strategy allows us to derive a tight upper bound on $\mathrm{E}(\Delta R_{\mathrm{S}})$, rather than a heuristic one in [1, Eq. (34)].

We then estimate the third term in (75). Let $\lambda_1, \ldots, \lambda_{N_{\mathrm{B}}}$ be the eigenvalues of $\mathbf{H}\mathbf{H}^{H}$. We have

$$\mathbf{H}^{H}\mathbf{H}=\tilde{\mathbf{V}}\mathbf{\Lambda}\tilde{\mathbf{V}}^{H} \text{ and } \mathbf{\Lambda}=\mathrm{diag}\left([\lambda_1,\ldots,\lambda_{N_{\mathrm{B}}}]\right). \quad (76)$$

Recalling the fact that for a Wishart matrix, its eigenvalues and eigenvectors are independent. Therefore $\tilde{\mathbf{V}}$ and $\mathbf{\Lambda}$ are independent. This allows us to bound the third term in (75) by

$$\begin{aligned} & \mathrm{E}_{\mathbf{H}}\left(\log\left|\mathbf{I}_{N_{\mathrm{B}}}+\alpha\beta\gamma(\mathbf{H}\hat{\mathbf{Z}})(\mathbf{H}\hat{\mathbf{Z}})^{H}\right|\right) \\ & \overset{(a)}{=} \mathrm{E}_{\mathbf{H}}\left(\log\left|\mathbf{I}_{N_{\mathrm{A}}-N_{\mathrm{B}}}+\alpha\beta\gamma(\mathbf{H}\hat{\mathbf{Z}})^{H}(\mathbf{H}\hat{\mathbf{Z}})\right|\right) \\ & = \mathrm{E}_{\Lambda}\left(\mathrm{E}_{\tilde{\mathbf{V}}}\left(\log\left|\mathbf{I}_{N_{\mathrm{A}}-N_{\mathrm{B}}}+\alpha\beta\gamma\hat{\mathbf{Z}}^{H}\tilde{\mathbf{V}}\mathbf{\Lambda}\tilde{\mathbf{V}}^{H}\hat{\mathbf{Z}}\right|\right)\right) \\ & \overset{(b)}{=} \mathrm{E}_{\Lambda}\left(\mathrm{E}_{\tilde{\mathbf{V}}}\left(\log\left|\mathbf{I}_{N_{\mathrm{B}}}+\alpha\beta\gamma\tilde{\mathbf{V}}^{H}\hat{\mathbf{Z}}\hat{\mathbf{Z}}^{H}\tilde{\mathbf{V}}\mathbf{\Lambda}\right|\right)\right) \\ & \overset{(c)}{\leq} \mathrm{E}_{\Lambda}\left(\mathrm{E}_{\tilde{\mathbf{V}}}\left(\log\left|\mathbf{I}_{N_{\mathrm{B}}}+\alpha\beta\gamma\mathrm{E}_{\tilde{\mathbf{V}}}\left(\tilde{\mathbf{V}}^{H}\hat{\mathbf{Z}}\hat{\mathbf{Z}}^{H}\tilde{\mathbf{V}}\right)\mathbf{\Lambda}\right|\right)\right) \\ & \overset{(d)}{=} \mathrm{E}_{\Lambda}\left(\log\left|\mathbf{I}_{N_{\mathrm{B}}}+\frac{\alpha\beta\gamma D\left(N_{\mathrm{A}},N_{\mathrm{B}},2^{B}\right)}{N_{\mathrm{B}}}\mathbf{\Lambda}\right|\right) \\ & \overset{(e)}{\leq} \mathrm{E}_{\Lambda}\left(\log\left|\mathbf{I}_{N_{\mathrm{B}}}+\frac{\alpha\beta\gamma\eta\left(N_{\mathrm{A}},N_{\mathrm{B}},2^{B}\right)}{N_{\mathrm{B}}}\mathbf{\Lambda}\right|\right), \end{aligned} \quad (77)$$

where (a) and (b) hold because $|\mathbf{I}+\mathbf{AB}|=|\mathbf{I}+\mathbf{BA}|$, (c) follows from the concavity of log determinant function, (d) follows from [29, Lemma 1] [1, Lemma 2], (e) holds because of (40).

Applying the fact [22, Th. 1]

$$\mathrm{E}\left(\log\left|\mathbf{I}_{N_{\mathrm{B}}}+\rho\mathbf{H}\mathbf{H}^{H}\right|\right)=\mathrm{E}\left(\log\left|\mathbf{I}_{N_{\mathrm{B}}}+\rho\mathbf{\Lambda}\right|\right)=\Theta(N_{\mathrm{B}},N_{\mathrm{A}},\rho), \quad (78)$$

to (75) and (77), we can simply obtain (44). ∎

C. Proof of Theorem 2

Recalling the fact that $\mathbf{Z}\mathbf{Z}^{H}=\mathbf{I}_{N_{\mathrm{A}}}-\tilde{\mathbf{V}}\tilde{\mathbf{V}}^{H}$ and $\hat{\mathbf{Z}}\hat{\mathbf{Z}}^{H}=\mathbf{I}_{N_{\mathrm{A}}}-\tilde{\mathbf{V}}_{j}\tilde{\mathbf{V}}_{j}^{H}$. From (21) and (24), if $N_{\mathrm{B}}=N_{\mathrm{E}}=1$, we can write ΔR_{S} as

$$\begin{aligned}\Delta R_{\mathrm{S}} = & \log\left(1+\alpha\gamma\mathbf{H}\mathbf{H}^{H}\right) \\ & -\log\frac{1+\alpha\mathbf{G}\mathbf{G}^{H}+\alpha(\beta-1)(\mathbf{GZ})(\mathbf{GZ})^{H}}{1+\alpha\beta(\mathbf{GZ})(\mathbf{GZ})^{H}} \\ & -\log\frac{1+\alpha\beta\gamma\mathbf{H}\mathbf{H}^{H}+\alpha\gamma\left(1-\beta\right)(\mathbf{H}\tilde{\mathbf{V}}_{j})(\mathbf{H}\tilde{\mathbf{V}}_{j})^{H}}{1+\alpha\beta\gamma\mathbf{H}\mathbf{H}^{H}-\alpha\beta\gamma(\mathbf{H}\tilde{\mathbf{V}}_{j})(\mathbf{H}\tilde{\mathbf{V}}_{j})^{H}} \\ & +\log\frac{1+\alpha\mathbf{G}\mathbf{G}^{H}+\alpha(\beta-1)(\mathbf{G}\hat{\mathbf{Z}})(\mathbf{G}\hat{\mathbf{Z}})^{H}}{1+\alpha\beta(\mathbf{G}\hat{\mathbf{Z}})(\mathbf{G}\hat{\mathbf{Z}})^{H}}. \end{aligned} \quad (79)$$

As N_{A} and $B\to\infty$ with $B/N_{\mathrm{A}}\to\bar{B}$, according to [12, Th. 1], we have

$$\frac{(\mathbf{H}\tilde{\mathbf{V}}_{j})(\mathbf{H}\tilde{\mathbf{V}}_{j})^{H}}{\mathbf{H}\mathbf{H}^{H}} \overset{a.s.}{\to} (1-2^{-\bar{B}}). \quad (80)$$

Since β (AN power allocation), γ (Eve-to-Bob noise-power ratio), and $P=\alpha\gamma+\alpha\beta\gamma(N_{\mathrm{A}}-1)$ (average transmit power constraint) are fixed, the central limit theorem tells us that

$$\begin{aligned} & \alpha\gamma\mathbf{H}\mathbf{H}^{H}\overset{a.s.}{\to}P/\beta,\ \alpha\mathbf{G}\mathbf{G}^{H}\overset{a.s.}{\to}P/\beta\gamma, \\ & \alpha(\mathbf{GZ})(\mathbf{GZ})^{H}\overset{a.s.}{\to}P/\beta\gamma,\ \alpha(\mathbf{G}\hat{\mathbf{Z}})(\mathbf{G}\hat{\mathbf{Z}})^{H}\overset{a.s.}{\to}P/\beta\gamma. \end{aligned} \quad (81)$$

Note that $\mathbf{GZ}$ (or $\mathbf{G}\hat{\mathbf{Z}}$) is a complex Gaussian random vector with i.i.d. entries [28, Th. 1].

By substituting (80) and (81) into (79), we obtain (48). ∎

D. Proof of Theorem 3

According to [18, Th. 1], we have

$$\mathrm{E}(R_{\mathrm{S}})=\Theta(N_{\mathrm{B}},N_{\mathrm{A}},\alpha\gamma)+\Theta(N_{\min},N_{\max},\alpha\beta)-\Omega, \quad (82)$$

where $\Theta(\cdot,\cdot,\cdot)$ is given in (33) and Ω is given in (51). By substituting (44) and (82) into (31), we can obtain (50). ∎

E. Proof of Theorem 4

If $\beta\geq 1$, then $\theta_{\min}=\alpha\gamma$. From (50) and (82), as $B\to\infty$,

$$\bar{C}_{\mathrm{LB,Q}}\to\Theta(N_{\mathrm{B}},N_{\mathrm{A}},\alpha\gamma)+\Theta(N_{\min},N_{\max},\alpha\beta)-\Omega=\mathrm{E}(R_{\mathrm{S}}). \quad (83)$$

According to [18, Th. 3], if $N_{\mathrm{E}}\leq N_{\mathrm{A}}-N_{\mathrm{B}}$, as $\alpha,\,\beta\to\infty$,

$$\mathrm{E}(R_{\mathrm{S}})\to\mathrm{E}(C_{\mathrm{S}})\to\bar{C}_{\mathrm{Bob}}, \quad (84)$$

where $\bar{C}_{\mathrm{Bob}}$ represents the ergodic main channel capacity with perfect CSI. The key step in the proof of [18, Th. 3] is to show that if $N_{\mathrm{E}}\leq N_{\mathrm{A}}-N_{\mathrm{B}}$, as $\alpha,\,\beta\to\infty$, then

$$I(\mathbf{u};\mathbf{y}|\mathbf{H},\mathbf{G})\to 0. \quad (85)$$

Since $\mathrm{E}(R_{\mathrm{S}})=I(\mathbf{u};\mathbf{z}|\mathbf{H})-I(\mathbf{u};\mathbf{y}|\mathbf{H},\mathbf{G})$, we have

$$\mathrm{E}(R_{\mathrm{S}})\to I(\mathbf{u};\mathbf{z}|\mathbf{H})=\bar{C}_{\mathrm{Bob}}. \quad (86)$$

We refer the reader to [18, Th. 3] for details.

Meanwhile, it always holds that

$$\bar{C}_{\mathrm{LB,Q}}\leq\mathrm{E}(C_{\mathrm{S,Q}})\leq\bar{C}_{\mathrm{Bob}}. \quad (87)$$

From (83), (84) and (87), if $N_{\mathrm{E}}\leq N_{\mathrm{A}}-N_{\mathrm{B}}$ and $\beta\geq 1$, as $\alpha,\,\beta,\,B\to\infty$, we have

$$\bar{C}_{\mathrm{LB,Q}}\to\mathrm{E}(C_{\mathrm{S,Q}})\to\mathrm{E}(C_{\mathrm{S}})\to\bar{C}_{\mathrm{Bob}}. \quad (88)$$

∎

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TWC.2015.2417886, IEEE Transactions on Wireless Communications

REFERENCES

[1] S.-C. Lin, T.-H. Chang, Y.-L. Liang, Y. P. Hong, and C.-Y. Chi, "On the impact of quantized channel feedback in guaranteeing secrecy with artificial noise: The noise leakage problem," *IEEE Trans. Wireless Commun.*, vol. 10, no. 3, pp. 901–915, Mar. 2011.

[2] J. Daemen and V. Rijmen, *The design of Rijndael: AES — the Advanced Encryption Standard*. Springer-Verlag, 2002.

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

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

[5] P. K. Gopala, L. Lai, and H. E. Gamal, "On the secrecy capacity of fading channels," *IEEE Trans. Inf. Theory*, vol. 54, no. 10, pp. 4687–5403, Oct. 2008.

[6] R. Liu and H. V. Poor, "Secrecy capacity region of a multiple-antenna Gaussian broadcast channel with confidential messages," *IEEE Trans. Inf. Theory*, vol. 55, no. 3, pp. 1235–1249, 2009.

[7] 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.

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

[9] D. J. Love, R. W. Heath, and T. Strohmer, "Grassmannian beamforming for multiple-input multiple-output wireless systems," *IEEE Trans. Inf. Theory*, vol. 49, no. 10, pp. 2735–2747, 2003.

[10] K. K. Mukkavilli, A. Sabharwal, E. Erkip, and B. Aazhang, "On beamforming with finite rate feedback in multiple-antenna systems," *IEEE Trans. Inf. Theory*, vol. 49, no. 10, pp. 2562–2579, 2003.

[11] W. Dai, Y. Liu, and B. Rider, "Quantization bounds on Grassmann manifolds and applications to MIMO communications," *IEEE Trans. Inf. Theory*, vol. 54, no. 3, pp. 1108–1123, 2008.

[12] W. Santipach and M. L. Honig, "Capacity of a multiple-antenna fading channel with a quantized precoding matrix," *IEEE Trans. Inf. Theory*, vol. 55, no. 3, pp. 1218–1234, 2009.

[13] R. Pitaval, H. Määttänen, K. Schober, O. Tirkkonen, and R. Wichman, "Beamforming codebooks for two transmit antenna systems based on optimum Grassmannian packings," *IEEE Trans. Inf. Theory*, vol. 57, no. 10, pp. 6591–6602, 2011.

[14] Z. Rezki, A. Khisti, and M. Alouini, "Ergodic secret message capacity of the wiretap channel with finite-rate feedback," *IEEE Trans. Wireless Commun.*, vol. 13, no. 6, pp. 3364–3379, Jun. 2014.

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

[16] P. Xia and G. B. Giannakis, "Design and analysis of transmit-beamforming based on limited-rate feedback," *IEEE Trans. Signal Process.*, vol. 54, no. 5, pp. 1853–1863, May 2006.

[17] Y. Liang, L. Lai, H. V. Poor, and S. Shamai, "A broadcast approach for fading wiretap channels," *IEEE Trans. Inf. Theory*, vol. 60, no. 2, pp. 842–858, Feb. 2014.

[18] S. Liu, Y. Hong, and E. Viterbo, "Artificial noise revisited," *IEEE Trans. Inf. Theory*, submitted for publication. [Online]. Available: http://arxiv.org/abs/1402.2091

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

[20] S.-C. Lin and C.-L. Lin, "On secrecy capacity of fast fading MIMOME wiretap channels with statistical CSIT," *IEEE Trans. Wireless Commun.*, vol. 13, no. 6, pp. 3293–3306, Jun. 2014.

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

[22] 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.

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

[24] K. Życzkowski and M. Kuś, "Random unitary matrices," *J. Phys. A: Math. Gen.*, vol. 27, no. 12, pp. 4235–4245, 1994.

[25] E. Weisstein, "Sphere point picking," *MathWorld*. [Online]. Available: http://mathworld.wolfram.com/SpherePointPicking.html

[26] V. Annapureddy, D. Marathe, T. R. Ramya, and S. Bhashyam, "Outage probability of multiple-input single-output (MISO) systems with delayed feedback," *IEEE Trans. Commun.*, vol. 57, no. 2, pp. 319–326, Feb. 2009.

[27] Y. Wu, A. Achtzehn, M. Petrova, P. Mahonen, and R. Calderbank, "On the effect of feedback delay on limited-rate beamforming systems," in *Proc. IEEE Global Telecommunications Conference (GLOBECOM '10)*, Miami, United States, Dec. 2010, pp. 1–5.

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

[29] N. Ravindran and N. Jindal, "Limited feedback-based block diagonalization for the mimo broadcast channel," *IEEE J. Sel. Areas Commun.*, vol. 26, no. 8, pp. 1473–1482, Oct. 2008.