Large System Analysis of Linear Precoding in MISO Broadcast Channels with Confidential Messages

Giovanni Geraci, *Student Member, IEEE,* Romain Couillet, *Member, IEEE,* Jinhong Yuan, *Member, IEEE,*
Mérouane Debbah, *Senior Member, IEEE,* and Iain B. Collings, *Senior Member, IEEE*

Abstract—In this paper, we study the performance of regularized channel inversion (RCI) precoding in large MISO broadcast channels with confidential messages (BCC). We obtain a deterministic approximation for the achievable secrecy sum-rate which is almost surely exact as the number of transmit antennas M and the number of users K grow to infinity in a fixed ratio $\beta = K/M$. We derive the optimal regularization parameter ξ and the optimal network load β that maximize the per-antenna secrecy sum-rate. We then propose a linear precoder based on RCI and power reduction (RCI-PR) that significantly increases the high-SNR secrecy sum-rate for $1 < \beta < 2$. Our proposed precoder achieves a per-user secrecy rate which has the same high-SNR scaling factor as both the following upper bounds: (i) the rate of the optimum RCI precoder without secrecy requirements, and (ii) the secrecy capacity of a single-user system without interference. Furthermore, we obtain a deterministic approximation for the secrecy sum-rate achievable by RCI precoding in the presence of channel state information (CSI) error. We also analyze the performance of our proposed RCI-PR precoder with CSI error, and we determine how the error must scale with the SNR in order to maintain a given rate gap to the case with perfect CSI.

Index Terms—Physical layer security, broadcast channel, random matrix theory, linear precoding, multi-user systems.

I. INTRODUCTION

Wireless networks are becoming more and more pervasive, with users relying on them to transmit sensitive data. Due to the broadcast nature of the physical medium, every node in the network is a potential eavesdropper, and securing the transmitted information is critical. Security of wireless communications has traditionally been ensured by network layer key-based cryptography. However, these schemes may not be suitable in the case of large dynamic wireless networks, since they raise issues like key distribution and management (for symmetric cryptosystems) and high computational complexity (for asymmetric cryptosystems). Moreover, these schemes are potentially vulnerable, because they rely on the unproven assumption that certain mathematical functions are hard to invert [1]. To provide an additional level of protection and

G. Geraci and J. Yuan are with the School of Electrical Engineering and Telecommunications, The University of New South Wales, Sydney, Australia (e-mail: g.geraci@student.unsw.edu.au, jinhong@ee.unsw.edu.au).

R. Couillet is with the Dept. of Telecommunications, Supélec, Gif-sur-Yvette, France (email: romain.couillet@supelec.fr).

M. Debbah is with the Alcatel-Lucent Chair on Flexible Radio, Supélec, Gif-sur-Yvette, France (e-mail: merouane.debbah@supelec.fr).

I. B. Collings is with the Wireless and Networking Technologies Laboratory, CSIRO ICT Centre, Sydney, Australia (email: iain.collings@csiro.au).

to achieve perfect secrecy, methods exploiting the randomness inherent in noisy channels, known as physical layer security, have been proposed [2], [3].

Physical layer security has recently become an active area of research [4], [5]. The maximum rate at which a message can be reliably transmitted to an intended user while the rate of information leakage at an eavesdropper vanishes asymptotically with the code length, denoted as the secrecy capacity, has been studied for several network topologies. These include multi-antenna wiretap channels [6] and multi-receiver wiretap channels [7]. Techniques like artificial noise and adaptive encoding have been proposed for the case when the eavesdropper's channel is not known by the transmitter [8]–[11]. The secrecy capacity of a two-user broadcast channel with confidential messages (BCC) has also been studied in [12], where the intended users can act maliciously as eavesdroppers. For a larger BCC with any number of malicious users, practical linear precoding schemes have been proposed [13]. Although suboptimal, linear precoding can control the amount of interference and information leakage between the users of a BCC, thus achieving secrecy with low-complexity implementation [14], [15].

In this paper, we propose a linear precoder based on regularized channel inversion (RCI) for the multiple-input single-output (MISO) BCC. In the MISO BCC, a base station (BS) equipped with M antennas simultaneously transmits K independent confidential messages to K spatially dispersed single-antenna users that potentially eavesdrop on each other. Under this system setup, we carry out a large-system analysis assuming that both M and K grow large, while their ratio $\beta = K/M$ is fixed. This paper directly extends some of the analysis in [16], [17] by requiring the transmitted messages to be kept confidential. Furthermore, this paper generalizes the results provided in [14], where the special case of $\beta = 1$ with perfect channel state information (CSI) was considered.

Our main contributions can be summarized as follows.

- We obtain a deterministic equivalent for the large-system secrecy sum-rate achievable by the RCI precoder in a MISO BCC. We then derive the optimal regularization parameter ξ that maximizes the secrecy sum-rate. Numerical results confirm that our analysis is accurate even for finite M.

- We derive a closed-form approximation for the optimal network load β that maximizes the per-antenna secrecy sum-rate. We find that for $\beta > 1$ the RCI precoder

performs poorly in the high-SNR regime. Therefore, we propose a linear precoder based on RCI and power reduction (RCI-PR) that significantly increases the high-SNR secrecy sum-rate for $1 < \beta < 2$.

- We compare the performance of our proposed RCI-PR precoder to: (i) the sum-rate achieved by an optimized RCI precoder without secrecy requirements and (ii) the secrecy capacity of a single-user system. The gaps with these two upper bounds represent the loss caused by the presence of: (i) secrecy requirements and (ii) interference due to multiple users, respectively. Both analysis and simulations show that the rate of the proposed precoder has the same high-SNR scaling factor as the two upper bounds.
- We obtain a deterministic equivalent for the secrecy sum-rate achievable by RCI precoding in the presence of CSI error. We then analyze the performance of our proposed RCI-PR precoder and determine how the CSI estimation error must scale with the SNR, to maintain a given rate gap to the case with perfect CSI. We find that in large frequency division duplex (FDD) systems, under random vector quantization (RVQ), $B \approx \frac{M-1}{3}\rho_{\text{dB}} - (M-1)\left[\log_2\left(\sqrt{4b-3}-1\right)-1\right]$ feedback bits per user are sufficient to maintain a gap of $\log_2 b$ bps/Hz at high SNR.

The remainder of the paper is organized as follows. Section II presents the system model and a secrecy sum-rate achievable by RCI precoding. In Section III, we derive a deterministic equivalent for this secrecy sum-rate, as well as the optimal regularization parameter ξ and network load β. In Section IV, we propose the RCI-PR precoder, and we study the secrecy sum-rate that it can achieve. Section V compares the performance of the proposed precoder to two upper bounds, obtained (i) in the absence of secrecy requirements and (ii) in the absence of interference. In Section VI we study the case when only imperfect CSI is available at the transmitter. Section VII concludes the paper.

Throughout the paper we use the following notation: bold uppercase (lowercase) letters denote matrices (column vectors); $(\cdot)^T$, $(\cdot)^H$, $\text{tr}\{\cdot\}$, $\|\cdot\|$, and $\text{E}[\cdot]$ denote transpose, conjugate transpose, trace, Euclidean norm, and expectation, respectively; $\mathcal{CN}(\mu, \sigma^2)$ denotes circularly symmetric complex-Gaussian distribution with mean μ and variance σ^2, and we use the notation $[\cdot]^+ \triangleq \max(\cdot, 0)$.

II. SYSTEM MODEL

In this section we introduce the MISO BCC and the secrecy sum-rate achievable by RCI precoding.

A. MISO Broadcast Channel with Confidential Messages

We consider the downlink of a narrowband MISO BCC, consisting of a base station with M antennas which simultaneously transmits K independent confidential messages to K spatially dispersed single-antenna users. In this model, transmission takes place over a block fading channel, and the transmitted signal is $\mathbf{x} = [x_1, \ldots, x_M]^T \in \mathbb{C}^{M \times 1}$. The

received signal at user k is given by

$$y_k = \sum_{j=1}^{M} h_{k,j} x_j + n_k \qquad (1)$$

where $h_{k,j} \sim \mathcal{CN}(0,1)$ is the i.i.d. channel between the j-th transmit antenna element and the k-th user, and $n_k \sim \mathcal{CN}(0, \sigma^2)$ is the noise seen at the k-th receiver. The corresponding vector equation is

$$\mathbf{y} = \mathbf{H}\mathbf{x} + \mathbf{n} \qquad (2)$$

where $\mathbf{H} = [\mathbf{h}_1, \ldots, \mathbf{h}_K]^\dagger$ is the $K \times M$ channel matrix. We assume that $\text{E}\left[\mathbf{n}\mathbf{n}^H\right] = \sigma^2 \mathbf{I}$, define $\rho \triangleq 1/\sigma^2$, and impose the long-term power constraint $\text{E}[\|\mathbf{x}\|^2] = 1$.

It is required that the BS securely transmits each confidential message u_k, ensuring that the unintended users receive no information. This is performed at the secrecy rate $R_{s,k}$, defined as follows. Let $\text{Pr}(\mathcal{E}_n)$ be the probability of error at the k-th intended user, m be a confidential message with entropy $H(m)$, $\mathbf{y}_k^n$ be the vector of all signals received by the eavesdroppers, and $H(m|\mathbf{y}_k^n)$ be the corresponding equivocation. Then a (weak) secrecy rate $R_{s,k}$ for the intended user is achievable if there exists a sequence of $(2^{nR_{s,k}}, n)$ codes such that $\text{Pr}(\mathcal{E}_n) \to 0$ and $\frac{1}{n}H(m|\mathbf{y}_k^n) \leq \frac{1}{n}H(m) - \varepsilon_n$ for some sequence ε_n approaching zero as $n \to \infty$ [6].

In general, the behavior of the users cannot be determined by the BS. As a worst-case scenario, in our system we assume that for each intended receiver k the remaining $K-1$ users can cooperate to jointly eavesdrop on the message u_k. For each user k, the alliance of the $K - 1$ cooperating eavesdroppers is equivalent to a single eavesdropper with $K - 1$ receive antennas, which is denoted by $\widetilde{k}$.

B. Regularized Channel Inversion Precoding

In this paper, we consider linear precoding for the MISO BCC. Although suboptimal, linear precoding schemes are of particular interest because of their low-complexity implementations [18], [19]. Linear precoding can control the amount of interference to maintain a high sum-rate in the broadcast channel [20]–[25]. In the MISO BCC, linear precoding can be employed to control the amount of interference and information leakage to the unintended receivers introduced by the transmission of each confidential message [13]–[15]. We are interested primarily in the RCI precoder, because it gives a better performance than the plain Channel Inversion precoder, particularly at low SNR [22].

In RCI precoding, the transmitted vector $\mathbf{x}$ is obtained at the BS by performing a linear processing on the vector of confidential messages $\mathbf{u} = [u_1, \ldots, u_K]^T$, whose entries are chosen independently, satisfying $\text{E}[|u_k|^2] = 1$. We assume homogeneous users, i.e. each user experiences the same received signal power on average, thus the model assumes that their distances from the transmitter are the same. The transmitted signal $\mathbf{x}$ after RCI precoding can be written as $\mathbf{x} = \mathbf{W}\mathbf{u}$, where $\mathbf{W} = [\mathbf{w}_1, \ldots, \mathbf{w}_K]$ is the $M \times K$ RCI precoding matrix [22],

[23], given by

$$\mathbf{W} = \frac{1}{\sqrt{\gamma}} \mathbf{H}^H \left(\mathbf{H}\mathbf{H}^H + M\xi \mathbf{I}_K \right)^{-1}$$
$$= \frac{1}{\sqrt{\gamma}} \left(\mathbf{H}^H \mathbf{H} + M\xi \mathbf{I}_M \right)^{-1} \mathbf{H}^H \qquad (3)$$

and $\gamma = \text{tr} \left\{ \mathbf{H}^H \mathbf{H} \left(\mathbf{H}^H \mathbf{H} + M\xi \mathbf{I}_M \right)^{-2} \right\}$ is a long-term power normalization constant. The function of the real regularization parameter ξ is to achieve a tradeoff between the signal power at the intended user and the interference and information leakage at the other unintended users for each message. Note that unlike [14]–[17], we do not confine ourselves to nonnegative regularization parameters.

C. Achievable Secrecy Sum-Rates

A secrecy sum-rate achievable by RCI precoding in the MISO BCC was obtained in [14] by considering that each user k, along with its own eavesdropper $\tilde{k}$ and the transmitter, forms an equivalent multi-input, single-output, multi-eavesdropper (MISOME) wiretap channel [6]. The transmitter, the intended receiver, and the eavesdropper of each MISOME wiretap channel are equipped with M, 1, and $K-1$ virtual antennas, respectively. Due to the assumption of cooperating malicious users, interference cancellation can be performed at $\tilde{k}$, which does not see any undesired signal term apart from the received noise. As a result, a secrecy sum-rate achievable by RCI precoding is given by [14]

$$R_s = \sum_{k=1}^{K} R_{s,k}$$
$$= \sum_{k=1}^{K} \left[\log_2 \left(1 + \text{SINR}_k \right) - \log_2 \left(1 + \text{SINR}_{\tilde{k}} \right) \right]^+, \quad (4)$$

where SINR_k and $\text{SINR}_{\tilde{k}}$ are the signal-to-interference-plus-noise ratios for the message u_k at the intended receiver k and the eavesdropper $\tilde{k}$, respectively, given by

$$\text{SINR}_k = \frac{\rho \left| \mathbf{h}_k^H \mathbf{w}_k \right|^2}{1 + \rho \sum_{j \neq k} \left| \mathbf{h}_k^H \mathbf{w}_j \right|^2} \qquad (5)$$

and

$$\text{SINR}_{\tilde{k}} = \rho \left\| \mathbf{H}_k \mathbf{w}_k \right\|^2, \qquad (6)$$

where $\mathbf{H}_k$ is the matrix obtained from $\mathbf{H}$ by removing the k-th row.

III. LARGE SYSTEM ANALYSIS

In this section, we study the secrecy sum-rate of the RCI precoder in the large-system regime, where both the number of receivers K and the number of transmit antennas M approach infinity, with their ratio $\beta = K/M$ being held constant. We then derive the optimal regularization parameter ξ that maximizes the secrecy sum-rate and a closed-form approximation for the optimal network load β.

A. Deterministic Equivalent of the Secrecy Sum-Rate with RCI Precoding

In the following we provide a deterministic approximation of the per-antenna secrecy sum-rate, which is almost surely exact as $M \to \infty$. To obtain such deterministic approximation, we need to ensure that the minimum eigenvalue of $\left(\frac{1}{M} \mathbf{H}\mathbf{H}^H + \xi \mathbf{I} \right)$ is bounded away from zero for all large M, almost surely. Let $C > 0$, $\epsilon > 0$, we define the set $\mathcal{D}_M = \mathbb{R} \backslash \left\{ \left[-\left(1 + \sqrt{\beta} \right)^2 - \frac{C}{M^{\frac{1}{2}-\epsilon}}, -\left(1 - \sqrt{\beta} \right)^2 + \frac{C}{M^{\frac{1}{2}-\epsilon}} \right] \right\}$.

Theorem 1: Let $\rho > 0$ and $\beta > 0$. Let R_s be the secrecy sum-rate achievable by RCI precoding defined in (4). Then

$$\sup_{\xi \in \mathcal{D}_M} \frac{1}{M} \left| R_s \left(\xi \right) - R_s^\circ \left(\xi \right) \right| \xrightarrow{\text{a.s.}} 0, \quad \text{as} \quad M \to \infty. \qquad (7)$$

R_s° denotes the secrecy sum-rate in the large-system regime, given by

$$R_s^\circ = K \left[\log_2 \frac{1 + g\left(\beta, \xi \right) \frac{\rho + \frac{\rho\xi}{\beta} [1 + g(\beta,\xi)]^2}{\rho + [1 + g(\beta,\xi)]^2}}{1 + \frac{\rho}{(1 + g(\beta,\xi))^2}} \right]^+, \quad \text{if } \xi \neq 0,$$

(8)

with

$$g\left(\beta, \xi \right) = \frac{1}{2} \left[\text{sgn}(\xi) \cdot \sqrt{\frac{(1-\beta)^2}{\xi^2} + \frac{2(1+\beta)}{\xi} + 1} + \frac{1-\beta}{\xi} - 1 \right]$$

(9)

and

$$R_s^\circ(0) = \lim_{\xi \to 0} R_s^\circ(\xi) = \begin{cases} \beta \log_2 \left[1 + \frac{(1-\beta)\rho}{\beta} \right] & \text{if } \beta \leq 1 \\ \beta \left\{ \log_2 \frac{\beta^3 [\beta + \rho(\beta-1)]}{[\beta^2 + \rho(\beta-1)^2]^2} \right\}^+ & \text{if } \beta > 1 \end{cases}$$

(10)

Proof: The proof of Theorem 1 can be found in Appendix A. ∎

B. Secrecy Sum-Rate Maximizing Regularization Parameter

The value of ξ has a significant impact on the large-system secrecy sum-rate R_s° in (8). In the following, we derive the regularization parameter $\xi^{\star\circ}$ that maximizes R_s°.

Theorem 2: Let $\rho > 0$, $\beta > 0$. Let $\xi_M^\star = \arg\max_{\xi \in \mathcal{D}_M} R_s(\xi)$ be the optimal regularization parameter in $\mathcal{D}_M$, and denote $R_s^\star \triangleq R_s(\xi_M^\star)$. Then

$$\frac{1}{M} \left[R_s^\star - R_s^\star(\xi^{\star\circ}) \right] \xrightarrow{\text{a.s.}} 0, \quad \text{as} \quad M \to \infty, \qquad (11)$$

where $\xi^{\star\circ} \in \mathcal{D}_M$ is the optimal large-system regularization parameter, given, for M large enough, by (12).

Proof: The value of $\xi^{\star\circ}$ can be found by setting the derivative of R_s° to zero and studying its maxima in each of the intervals which compose the set $\mathcal{D}_M$. Then we have

$$0 \overset{a}{\leq} \frac{1}{M} \left[R_s^\star - R_s(\xi^{\star\circ}) \right]$$
$$= \frac{1}{M} \left[R_s(\xi_M^\star) - R_s^\circ(\xi_M^\star) + R_s^\circ(\xi_M^\star) - R_s^\circ(\xi^{\star\circ}) \right.$$
$$\left. + R_s^\circ(\xi^{\star\circ}) - R_s(\xi^{\star\circ}) \right]$$
$$\overset{b}{\leq} \frac{1}{M} \left[R_s(\xi_M^\star) - R_s^\circ(\xi_M^\star) + R_s^\circ(\xi^{\star\circ}) - R_s(\xi^{\star\circ}) \right] \xrightarrow{c} 0,$$

(13)

$$\xi^{\star\circ} = \frac{-2\rho^2\left(1-\beta\right)^2 + 6\rho\beta + 2\beta^2 - 2\left[\beta\left(\rho+1\right)-\rho\right]\cdot\sqrt{\beta^2\left[\rho^2+\rho+1\right]-\beta\left[2\rho\left(\rho-1\right)\right]+\rho^2}}{6\rho^2\left(\beta+2\right)+6\rho\beta} \qquad (12)$$

where (a), resp. (b), follows from the definition of $\xi_M^\star$, resp. $\xi^{\star\circ}$, and (c) follows from Theorem 1.

When $\beta = 1$, the value of $\xi^{\star\circ}$ in (12) reduces to the one derived in [14], given by $\xi^{\star\circ} = \left(3\rho+1+\sqrt{3\rho+1}\right)^{-1}$. We note that the value $\xi^{\star\circ}$ that maximizes the secrecy sum-rate can be negative, and it differs from the value $\xi_{ns}^{\star\circ} = \beta/\rho$ that maximizes the sum-rate without secrecy requirements [16]. Unlike $\xi_{ns}^{\star\circ}$, which grows unbounded as $\rho \to 0$, $\xi^{\star\circ}$ is upper bounded by $\xi_0^{\star\circ} = \lim_{\rho\to 0}\xi^{\star\circ} = 1 - \frac{\beta}{2}$, $\forall \beta > 0$, although when $\beta \geq 2$ it can be shown that $R_s^\circ = 0$ irrespective of ξ and ρ. Similarly to $\xi_{ns}^{\star\circ}$, the value of $\xi^{\star\circ}$ decreases as the SNR increases. In the high-SNR regime, we have $\lim_{\rho\to\infty}\xi^{\star\circ} - \xi_\infty^{\star\circ} = 0$, where $\xi_\infty^{\star\circ}$ approximates the high-SNR behavior of $\xi^{\star\circ}$ and is given by

$$\xi_\infty^{\star\circ} = \begin{cases} \frac{\beta}{2\rho} & \text{for } \beta < 1 \\ \frac{1}{3\rho} & \text{for } \beta = 1 \\ -\frac{2(\beta-1)^2}{3(\beta+2)} + \frac{\beta(2-\beta)}{2\rho(\beta+2)} & \text{for } \beta > 1 \end{cases} \qquad (14)$$

We then have by the continuous mapping theorem

$$\lim_{\rho\to\infty} \frac{R_s^{\star\circ} - R_s^{\star\circ\infty}}{R_s^{\star\circ}} = 0 \qquad (15)$$

with

$$R_s^{\star\circ} \triangleq R_s^\circ\left(\xi^{\star\circ}\right) \quad \text{and} \quad R_s^{\star\circ\infty} \triangleq \lim_{\rho\to\infty} R_s^\circ(\xi_\infty^{\star\circ}). \qquad (16)$$

C. Optimal Secrecy Sum-Rate

By substituting $\xi^{\star\circ}$ from (12) in (8), it is possible to obtain the optimal secrecy sum-rate $R_s^{\star\circ}$ achievable by RCI precoding in the large-system regime. The secrecy sum-rate $R_s^{\star\circ}$ is a function of M, β and ρ. It was shown in [14] that for $\beta = 1$, $R_s^{\star\circ}$ is always positive and monotonically increasing with the SNR ρ. It can be shown that the same is true for $\beta < 1$. However when $\beta > 1$, the secrecy sum-rate does not monotonically increase with ρ. It will be shown in Section IV that there is an optimal value of the SNR beyond which the achievable secrecy sum-rate $R_s^{\star\circ}$ starts decreasing, until it becomes zero for large SNR. When $\beta \geq 2$ no positive secrecy sum-rate is achievable at all.

These results can be explained as follows. In the worst-case scenario, the alliance of cooperating eavesdroppers can cancel the interference, and its received SINR is the ratio between the signal leakage and the thermal noise. In the limit of large SNR, the thermal noise vanishes, and the only means for the transmitter to limit the eavesdropper's SINR is by reducing the signal leakage to zero by inverting the channel matrix. This can only be accomplished when the number of transmit antennas is larger than or equal to the number of users, hence only if $\beta \leq 1$. When $\beta > 1$ this is not possible, and no positive secrecy sum-rate can be achieved. When $\beta \geq 2$, the eavesdroppers are able to drive the secrecy sum-rate to zero irrespective of ρ. This result is expected and consistent with the ones in [6].
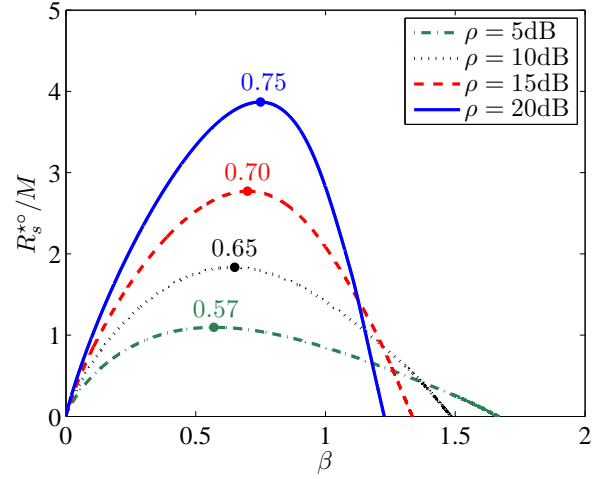

Fig. 1. Asymptotic secrecy sum-rate per transmit antenna as a function of β for RCI precoding. The value of $\beta^{\star\circ}$ is indicated next to each curve.

Remark 1: In order for Theorem 1 to hold with $\xi = \xi^{\star\circ}$, it is sufficient that $\xi^{\star\circ} \in \mathcal{D}_M$. Since $\xi^{\star\circ}$ in (12) depends on β and ρ, so does the accuracy of $R_s^{\star\circ}$ for finite M. We can distinguish the two following cases. (i) When $\beta \neq 1$, we have $\xi^{\star\circ} \in \mathcal{D}_M$ $\forall \rho$, and the approximation is accurate uniformly on ρ. (ii) When $\beta = 1$, $\xi^{\star\circ} \in \mathcal{D}_M$ for all finite ρ; if $\rho \to \infty$, then it is required that $M = \mathcal{O}(\rho^{2+\epsilon})$, for some $\epsilon > 0$, otherwise the approximation gets weaker as $\rho \to \infty$ for M fixed. This means for instance that the approximation with $M = 10$ and $\rho = 17$dB is as accurate as the approximation with $M = 40$ and $\rho = 20$dB.

D. Optimal Network Load

Fig. 1 depicts the per-antenna secrecy sum-rate $R_s^{\star\circ}/M$ as a function of the network load β, for several values of the SNR. We denote by $\beta^{\star\circ}$ the value of $\beta \in \mathbb{R}^+$ that maximizes the per-antenna secrecy sum-rate. It is possible to see from Fig. 1 that the value of $\beta^{\star\circ}$ falls between 0 and 1, and that it is an increasing function of the SNR. A closed-form approximation for $\beta^{\star\circ}$ in the large-SNR regime is given in the following.

Proposition 1: In the limit of large SNR, the value $\tilde{\beta}^{\star\circ}$ of the optimal network load can be found by solving the following fixed point equation

$$\tilde{\beta}^{\star\circ} = \rho\left(1-\tilde{\beta}^{\star\circ}\right)e^{-\frac{1}{1-\tilde{\beta}^{\star\circ}}}, \qquad (17)$$

and the network load $\tilde{\beta}^{\star\circ}$ tends to one for large SNR.

Proof: From (16), we have that $R_s^{\star\circ\infty}$ approximates $R_s^{\star\circ}$ in the large-SNR regime. We then obtain (17) by noticing that it must be $\tilde{\beta}^{\star\circ} \in [0,1]$, and by setting $\partial(R_s^{\star\circ\infty}/M)/\partial\beta = 0$. ∎
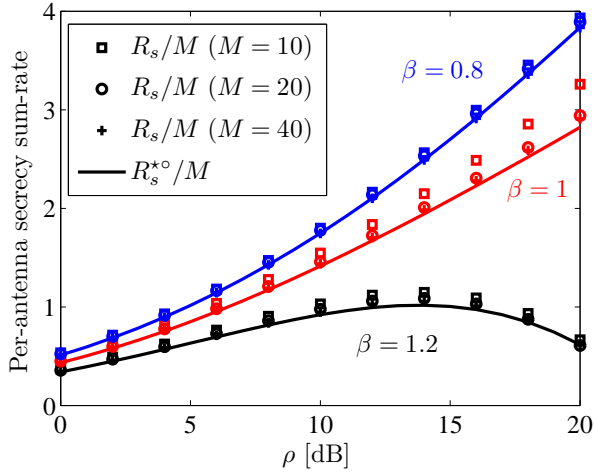
Fig. 2. Comparison between the secrecy sum-rate with RCI precoding in the large-system regime (8) and the simulated ergodic secrecy sum-rate for finite M. Three sets of curves are shown, each one corresponds to a different value of β.

Fig. 3. Mean normalized secrecy sum-rate difference between $R_s^\star$ (obtained using the optimal $\xi_M^\star$) and $R_s(\xi^{\star\circ})$ (obtained with $\xi^{\star\circ}$ from large-system analysis), for $\beta = 0.8$ and various values of the SNR.

E. Numerical Results

Fig. 2 compares the secrecy sum-rate $R_s^{\star\circ}$ of the RCI precoder from the large-system analysis to the simulated ergodic secrecy sum-rate R_s with a finite number of users, for different values of β. The value of $R_s^{\star\circ}$ was obtained by (8) with $\xi^{\star\circ}$ as in (12). The value of R_s was obtained by using the regularization parameter that maximizes the average secrecy sum-rate. We observe that when $\beta = 0.8$ and when $\beta = 1.2$ the large-system analysis is accurate for all values of M and SNR. When $\beta = 1$, the analysis is accurate at low SNR for all values of M, and for high SNR larger values of M are required to increase the accuracy. The previous observations are consistent with Remark 1.

Fig. 3 shows that using the regularization parameter $\xi^{\star\circ}$, obtained from large-system analysis, does not cause a significant loss in the secrecy sum-rate compared to using $\xi_M^\star$, optimized for each channel realization. The figure shows the normalized secrecy sum-rate difference $(R_s^\star - R_s(\xi^{\star\circ}))/R_s^\star$, simulated for finite-size systems, $\beta = 0.8$ and various values of the SNR. The value of $R_s^\star$ was obtained by using $\xi_M^\star$, whereas $R_s(\xi^{\star\circ})$ was obtained by using $\xi^{\star\circ}$. We observe that the average normalized secrecy sum-rate difference is less than 2% for all values of M and ρ. As a result, one can avoid the calculation of $\xi_M^\star$ for every channel realization, and $\xi^{\star\circ}$ can be used with only a small loss of performance.

Fig. 4 shows the optimal number of users $K^\star$ obtained via simulations, for $M = 10$, 20, and 40 antennas. This is compared to $K^{\star\circ}$, obtained from an exhaustive search on the the large-system rate $R_s^{\star\circ}$, and to the closed-form approximation $\tilde{K}^{\star\circ}$, obtained from (17) in the high-SNR regime. We note that $K^{\star\circ}$ is accurate across the whole range of SNR, whereas $\tilde{K}^{\star\circ}$ is accurate for medium-to-large values of the SNR.
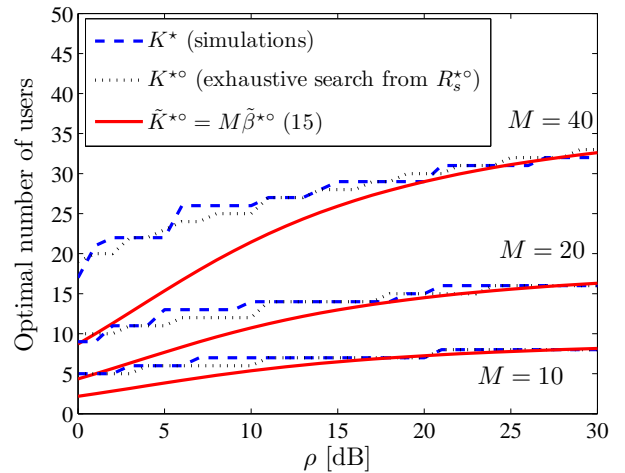

Fig. 4. Comparison between $K^\star$ (obtained via simulations), $K^{\star\circ}$ (obtained via exhaustive search and large-system analysis), and the closed-form approximation $\tilde{K}^{\star\circ}$ (obtained via large-system and large-SNR analysis).

IV. RCI PRECODER WITH POWER REDUCTION

We have found that for $\beta > 1$ the RCI precoder performs poorly in the high-SNR regime. In this section, we first derive the optimal value of the SNR $\rho^{\star\circ}$ that maximizes the achievable secrecy sum-rate $R_s^{\star\circ}$ for $\beta > 1$. We then propose a linear precoder based on RCI and power reduction which significantly increases the high-SNR secrecy sum-rate for $1 < \beta < 2$.

A. Optimal Transmit SNR

When $1 < \beta < 2$, there is an optimal value of the transmit SNR $\rho^{\star\circ}$, provided in the following.

Proposition 2: The value of the SNR $\rho^{\star\circ}$ that maximizes the secrecy sum-rate $R_s^{\star\circ}$ for $1 < \beta < 2$, and the corresponding maximum value of $R_s^{\star\circ}$ are respectively given by

$$\rho^{\star\circ} = \arg\max_{\rho} \; R_s^{\star\circ}(\rho) = \frac{\beta(2-\beta)}{(\beta-1)^2} \qquad (18)$$

and

$$R_s^{\star\circ}(\rho^{\star\circ}) = K \log_2 \frac{\beta^2}{4(\beta-1)}. \qquad (19)$$

Proof: If $1 < \beta < 2$, then $\rho^{\star\circ}$ is the only stationary point of $R_s^{\star\circ}$, which can be found by setting its derivative $\partial R_s^{\star\circ}/\partial\rho$ to zero. We note that $\lim_{\rho\to\rho^{\star\circ}} \xi^{\star\circ} = 0$. Therefore, $R_s^{\star\circ}(\rho^{\star\circ})$ can be obtained by considering $\rho \to \rho^{\star\circ}$ and $\xi \to 0$ in (8) and after several algebraic manipulations. ∎

B. Power Reduction Strategy

We now propose a power reduction strategy to prevent the secrecy sum-rate from decreasing at high SNR, for $1 < \beta < 2$. This is achieved by reducing the transmit power, and therefore reducing the SNR to the value $\rho^{\star\circ}$ that maximizes the secrecy sum-rate. We denote this scheme by the RCI precoder with power reduction (RCI-PR), whose precoding matrix $\mathbf{W}_{\text{PR}}$ is given by

$$\mathbf{W}_{\text{PR}} = \begin{cases} \frac{1}{\sqrt{\gamma}} \mathbf{H}^H \left(\mathbf{H}\mathbf{H}^H + M\xi\mathbf{I}_K \right)^{-1} & \text{if } \beta \leq 1 \\ \frac{1}{\sqrt{r\gamma}} \left(\mathbf{H}^H\mathbf{H} + M\xi\mathbf{I}_M \right)^{-1} \mathbf{H}^H & \text{if } 1 < \beta < 2 \\ 0 & \text{if } \beta \geq 2 \end{cases}$$

$$(20)$$

where $r = \max\left(\frac{\rho}{\rho^{\star\circ}}, 1 \right)$ is the power reduction constant used for $1 < \beta < 2$, and where ξ is chosen from (12) evaluated with an SNR of $\min(\rho, \rho^{\star\circ})$. We note that (20) generalizes the RCI precoder in (3) to the case when the power reduction strategy is employed.

Remark 2: We note from (12) that $\xi^{\star\circ}(\rho^{\star\circ}) = 0$. Therefore when $\rho \geq \rho^{\star\circ}$, the optimal value of ξ for the RCI-PR precoder is zero, and it reduces to a CI-PR precoder. Even if $\beta > 1$, it is still possible to calculate $\mathbf{W}_{\text{PR}}$ by expressing it as in (20) for $1 < \beta < 2$.

We denote by $R_{s,\text{PR}}^{\circ}$ the large-system secrecy sum-rate achievable by the proposed RCI-PR precoder (20). The following theorem provides a high-SNR approximation of $R_{s,\text{PR}}^{\circ}$.

Theorem 3: In the high-SNR regime, we have $\lim_{\rho\to\infty} \frac{R_{s,\text{PR}}^{\circ} - R_{s,\text{PR}}^{\circ\infty}}{R_{s,\text{PR}}^{\circ}} = 0$, where $R_{s,\text{PR}}^{\circ\infty}$ approximates the large-system secrecy sum-rate $R_{s,\text{PR}}^{\circ}$ achieved by the RCI-PR precoder, and it is given by

$$R_{s,\text{PR}}^{\circ\infty} = \begin{cases} K \log_2 \frac{1-\beta}{\beta} + K \log_2 \rho & \text{for } \beta < 1 \\ \frac{K}{2} \log_2 \frac{27}{64} + \frac{K}{2} \log_2 \rho & \text{for } \beta = 1 \\ K \log_2 \frac{\beta^2}{4(\beta-1)} & \text{for } 1 < \beta < 2 \\ 0 & \text{for } \beta \geq 2 \end{cases}$$

$$(21)$$

Proof: When $\beta \leq 1$, the RCI-PR precoder reduces to the optimal RCI precoder. Therefore, in this case we have $R_{s,\text{PR}}^{\circ\infty} = R_s^{\circ\star\infty}$, with the latter defined in (16). The value of (21) for $1 < \beta < 2$ is obtained by noting that for large SNR, RCI-PR forces $\rho = \rho^{\star\circ}$, and by using Proposition 2. The value for $\beta \geq 2$ arises from the fact that no positive secrecy sum-rate is achievable in such a condition, therefore the RCI-PR precoder (20) transmits zero power. ∎

From (21) we can conclude that the behavior of our proposed RCI-PR precoder can be classified into four regions. When $\beta < 1$, any secrecy sum-rate can be achieved, as long
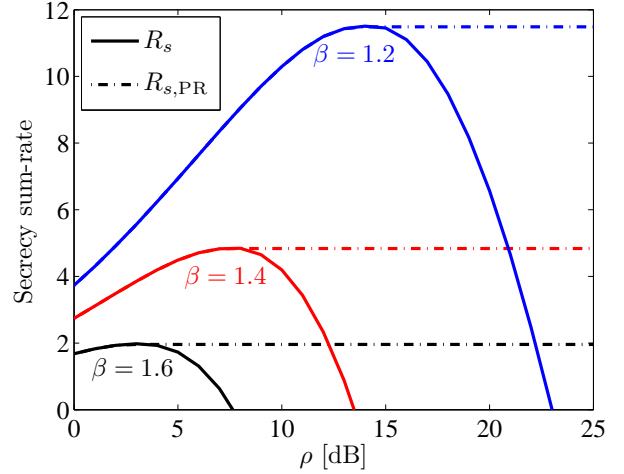

Fig. 5. Comparison between the ergodic secrecy sum-rates R_s and $R_{s,\text{PR}}$ achieved by the RCI precoder and by the proposed RCI-PR precoder, respectively, for $M = 10$ transmit antennas. Three values of β are considered: 1.2, 1.4 and 1.6, corresponding to $K = 12$, 14 and 16 users.

as the transmitter has enough power available, and the secrecy sum-rate scales linearly with the factor K. When $\beta = 1$, the linear scaling factor reduces to $K/2$. When $1 < \beta < 2$, the cooperating eavesdroppers have more antennas than the transmitter, and thus they can limit the achievable secrecy sum-rate regardless of how much power is available at the transmitter. When $\beta \geq 2$, the eavesdroppers are able to prevent secret communications, and the secrecy sum-rate is zero even if unlimited power is available.

C. Numerical Results

Fig. 5 shows the simulated ergodic secrecy sum-rates with and without the power reduction strategy for $M = 10$ transmit antennas and three values of $\beta > 1$. The figure shows that the proposed RCI-PR precoder in (20) increases the secrecy sum-rate compared to the RCI precoder in (3). By using the proposed power reduction strategy, it is possible to prevent the secrecy sum-rate from decreasing at large values of the SNR ρ. For large ρ, the achieved secrecy sum-rate equals the maximum across all values of ρ. Moreover, this is achieved by using a lower transmit power, and the amount of power saved equals $10 \log_{10} r^{-1}$ dB.

V. PERFORMANCE COMPARISON

In this section, we first compare the secrecy sum-rate $R_{s,\text{PR}}^{\star\circ}$ achieved by the proposed RCI-PR precoder to the sum-rate $R^{\star\circ}$ achieved by the optimized RCI precoder without secrecy requirements, in the large-system regime. The gap between $R_{s,\text{PR}}^{\star\circ}$ and $R^{\star\circ}$ represents the *secrecy loss*, i.e. how much the secrecy requirements cost in terms of the achievable sum-rate. Furthermore, we compare the per-user secrecy rate achieved by the proposed precoder to the secrecy capacity $C_{s,\text{SU}}$ of a single-user MISOME wiretap channel [6]. The gap between $R_{s,\text{PR}}^{\star\circ}/K$ and $C_{s,\text{SU}}$ represents a *multi-user loss*, i.e. the loss due to the requirement of serving multiple users at the same time.

A. Secrecy Loss

The secrecy sum-rate $R_{s,\mathrm{PR}}^{\star\circ}$ is obtained by using the precoder in (20). The optimal sum-rate $R^{\star\circ}$ without secrecy requirements is obtained by using the precoder in (3), and it is given by [16]

$$R^{\star\circ} = K \log_2 \left[1 + g \left(\beta, \xi_{\mathrm{ns}}^{\star\circ} \right) \right], \qquad (22)$$

with $\xi_{\mathrm{ns}}^{\star\circ} = \beta/\rho$. Similarly to the secrecy sum-rate, there is an optimal value for the ratio β that maximizes the per-antenna sum-rate $R^{\star\circ}/M$ without secrecy requirements [16], [17], [26]. It is easy to show that $R^{\star\circ} \geq 0$ for all values of β and ρ, with equality only for $\rho = 0$, and that $R^{\star\circ}$ tends to zero as $\beta \to \infty$. Hence, there is no limit to the number of users per transmit antenna β that the system can accommodate with a non-zero sum-rate. However if we impose the secrecy requirements, the secrecy sum-rate $R_{s,\mathrm{PR}}^{\star\circ}$ is zero for $\beta \geq 2$. Therefore, introducing the secrecy requirements will limit the number of users that can be served with a non-zero rate to two times the number of transmit antennas.

We now compare the secrecy sum-rate $R_{s,\mathrm{PR}}^{\star\circ}$ to the sum-rate $R^{\star\circ}$ in the limit of large SNR. Again by using the regularization parameter $\xi_{\mathrm{ns}}^{\star\circ} = \beta/\rho$ we obtain $\lim_{\rho \to \infty} \frac{R^{\star\circ} - R^{\star\circ\infty}}{R^{\star\circ}} = 0$, with

$$R^{\star\circ\infty} = \begin{cases} K \log_2 \frac{1-\beta}{\beta} + K \log_2 \rho & \text{for } \beta < 1 \\ \frac{K}{2} \log_2 \rho & \text{for } \beta = 1 \\ K \log_2 \frac{\beta}{\beta-1} & \text{for } \beta > 1 \end{cases} \qquad (23)$$

By comparing (23) to (21), we can draw the following conclusions regarding the large-SNR regime. If the number of transmit antennas M is larger than the number of users K, then $R_{s,\mathrm{PR}}^{\star\circ\infty} = R^{\star\circ\infty}$ and the secrecy requirements do not decrease the sum-rate of the network. Therefore by using the RCI-PR precoder in (20), one can achieve secrecy while maintaining the same sum-rate, i.e. there is no secrecy loss. If $M = K$, then the secrecy loss is $\frac{1}{2} \log_2(\frac{64}{27}) \approx 0.62$ bits per user, but the linear scaling factor $K/2$ remains unchanged. Alternatively, one can achieve secrecy while maintaining the same sum-rate, by increasing the transmit power by a factor $64/27 \approx 3.75$dB. If $M < K < 2M$, then the secrecy loss is $(2 - \log_2 \beta)$ bits per user, but the proposed precoder transmits a lower power, which is always upper bounded by $\frac{\beta(2-\beta)}{(\beta-1)^2}$. Finally if $K \geq 2M$, then the secrecy requirements force the sum-rate to zero, whereas the sum-rate $R^{\star\circ}$ remains positive, though it also tends to zero for large β. We finally note that, when there is no secrecy constraint, user scheduling can be used to achieve a higher multiplexing gain. This is not possible in the BCC, since discarding users does not prevent them from eavesdropping.

B. Multi-User Loss

We now consider the *multi-user loss*, i.e. the loss due to the interference caused by the presence of multiple users in the system. This is given by the gap between the per-user secrecy rate $R_{s,\mathrm{PR}}^{\star\circ}/K$ achieved by the proposed RCI-PR precoder and the secrecy capacity $C_{s,\mathrm{SU}}$ of the MISOME wiretap channel, where one user is served at a time and the remaining users can

eavesdrop [6]. We compare $R_{s,\mathrm{PR}}^{\star\circ}/K$ to $C_{s,\mathrm{SU}}$ in the large-SNR regime. The former is obtained from (21). The value of $C_{s,\mathrm{SU}}$ was obtained in [6], and for large SNR we have $\lim_{\rho \to \infty} \frac{C_{s,\mathrm{SU}} - C_{s,\mathrm{SU}}^{\infty}}{C_{s,\mathrm{SU}}} = 0$, where

$$C_{s,\mathrm{SU}}^{\infty} = \begin{cases} \log_2 \rho & \text{for } \beta < 1 \\ \frac{1}{2} \log_2 \rho & \text{for } \beta = 1 \\ \log_2 \frac{1}{(\beta-1)} & \text{for } 1 < \beta < 2 \\ 0 & \text{for } \beta \geq 2 \end{cases} \qquad (24)$$

We note that in $C_{s,\mathrm{SU}}$ from [6] a single-user system is considered. Therefore, only one message is transmitted to one legitimate user, and the user does not experience any interference. By comparing (24) to $R_{s,\mathrm{PR}}^{\star\circ}/K$, we can conclude that the multi-user loss is $\log_2 \frac{1-\beta}{\beta}$ and 0.62 bits per user for $\beta < 1$ and $\beta = 1$, respectively. Hence for $\beta \leq 1$, the proposed RCI-PR precoder achieves a per-user secrecy rate which has the same linear scaling factor as the secrecy capacity of a single-user system with no interference. When $1 < \beta < 2$, the proposed precoder suffers a multi-user loss of $(2 - 2 \log_2 \beta)$ bits, but again it has the advantage of transmitting a limited power.

C. Numerical Results

In Fig. 6 we compare the simulated per-user ergodic sum-rate $R_{s,\mathrm{PR}}/K$ of the RCI-PR precoder to the sum-rate R/K of the RCI precoder without secrecy requirements. These were obtained by using the regularization parameters $\xi^{\star\circ}$ and $\xi_{\mathrm{ns}}^{\star\circ}$, respectively. For $\beta < 1$, the difference between $R_{s,\mathrm{PR}}/K$ and R/K becomes negligible at large SNR, and secrecy can be achieved without additional costs. For $\beta = 1$, the two curves tend to have the same slope at large SNR, but there is a residual gap between them. Therefore, secrecy can be achieved at a lower sum-rate. We note that in order to achieve secrecy without decreasing the sum-rate, the required additional power is less than 4dB at all SNRs. For $1 < \beta < 2$, the sum-rate R tends to saturate for large SNR, and so does the secrecy sum-rate $R_{s,\mathrm{PR}}$. In the simulations, for $\beta = 1.2$ and $\rho = 25$dB, the gap is about 1.79 bits, close to $2 - \log_2 \beta \approx 1.74$ bits. Moreover, we note that the proposed precoder saves 92% of the transmit power. The gap is smaller for smaller values of the SNR, e.g. it reduces to about 0.72 bits when we set the transmit power to 10dB.

Fig. 6 also shows the simulated secrecy capacity $C_{s,\mathrm{SU}}$ of the MISOME wiretap channel. For $\beta \leq 1$, the RCI-PR precoder achieves a per-user secrecy rate which has the same linear scaling factor as $C_{s,\mathrm{SU}}$. When $1 < \beta < 2$, also $C_{s,\mathrm{SU}}$ saturates at high SNR. In particular, for $\beta = 1.2$ and $\rho = 25$dB, the gap with the RCI-PR precoder is about $1.47 \approx 2 - 2 \log_2 \beta$ bits, but the RCI-PR precoder saves 92% of the power. The gap is smaller for smaller values of the SNR, e.g. it reduces to about 0.4 bits when we set the transmit power to 10dB. All these numerical results confirm the ones obtained from the large-system analysis.

VI. IMPERFECT CHANNEL STATE INFORMATION

In the previous sections, we proposed a linear precoder for the case when perfect CSI is available at the transmitter. In
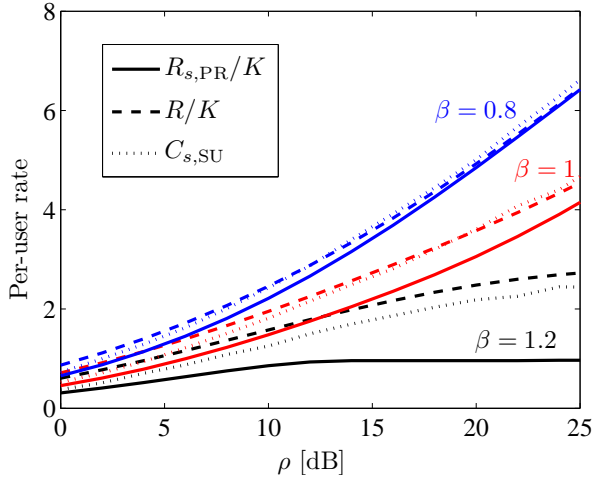
Fig. 6. Comparison between the simulated ergodic per-user secrecy rate with RCI-PR (solid) and the two upper bounds: (i) per-user rate without secrecy requirements (dashed) and (ii) MISOME secrecy capacity (dotted), for $K = 12$ users. Three values of β are considered: 0.8, 1, and 1.2, corresponding to $M = 15$, 12 and 10 antennas.

this section, we consider a more realistic scenario where only an estimation of the channel is available at the transmitter, and we obtain a deterministic equivalent for the secrecy sum-rate achievable by RCI precoding. We then analyze the performance of our proposed RCI-PR precoder, and we determine how the CSI estimation error must scale with the SNR and how many feedback bits are required to maintain a given rate gap to the case with perfect CSI.

A. Secrecy Sum-Rates in the Presence of Channel Estimation Error

We model the relation between the channel $\mathbf{H}$ and the estimated channel $\hat{\mathbf{H}}$ as $\mathbf{H} = \hat{\mathbf{H}} + \mathbf{E}$, where the matrix $\mathbf{E}$ represents the channel estimation error, and it is independent from $\hat{\mathbf{H}}$. The entries of $\hat{\mathbf{H}}$ and $\mathbf{E}$ are i.i.d. complex Gaussian random variables with zero mean and variances $1 - \tau^2$ and τ^2, respectively. The value of $\tau \in [0, 1]$ depends on the quality and technique used for channel estimation, and it is the same for all users. When $\tau = 0$ the CSI is perfectly known, whereas $\tau = 1$ corresponds to the case when no CSI is available at all.

The transmitter uses the knowledge of $\hat{\mathbf{H}}$ to obtain the RCI precoding matrix $\hat{\mathbf{W}}$, given by

$$\hat{\mathbf{W}} = \frac{1}{\sqrt{\hat{\gamma}}} \hat{\mathbf{H}}^H \left(\hat{\mathbf{H}} \hat{\mathbf{H}}^H + M\xi \mathbf{I} \right)^{-1}$$

$$= \frac{1}{\sqrt{\hat{\gamma}}} \left(\hat{\mathbf{H}}^H \hat{\mathbf{H}} + M\xi \mathbf{I} \right)^{-1} \hat{\mathbf{H}}^H \quad (25)$$

where $\hat{\gamma} = \mathrm{tr} \left\{ \left(\hat{\mathbf{H}}^H \hat{\mathbf{H}} + M\xi \mathbf{I} \right)^{-2} \hat{\mathbf{H}}^H \hat{\mathbf{H}} \right\}$ is the power normalization costant in the presence of CSI error. A secrecy sum-rate achievable by RCI precoding in the presence of channel estimation error with variance τ^2 is given by

$$\hat{R}_s = \sum_{k=1}^{K} \left[\log_2 \left(1 + \hat{\mathrm{SINR}}_k \right) - \log_2 \left(1 + \hat{\mathrm{SINR}}_{\widetilde{k}} \right) \right]^+, \quad (26)$$

with

$$\hat{\mathrm{SINR}}_k = \frac{\rho \left| \mathbf{h}_k^H \hat{\mathbf{w}}_k \right|^2}{1 + \rho \sum_{j \neq k} \left| \mathbf{h}_k^H \hat{\mathbf{w}}_j \right|^2} \quad (27)$$

and

$$\hat{\mathrm{SINR}}_{\widetilde{k}} = \rho \left\| \mathbf{H}_k \hat{\mathbf{w}}_k \right\|^2 . \quad (28)$$

The deterministic equivalent of $\hat{R}_s$ in the presence of channel estimation error is given in the following.

Theorem 4: Let $\rho > 0$, $\beta > 0$, and $\xi \in \mathcal{D}_M$. Let $\hat{R}_s$ be the secrecy sum-rate in the presence of channel estimation error with variance τ^2, defined in (26). Define $\tilde{\rho} \triangleq \frac{\rho(1-\tau^2)}{\rho\tau^2+1}$ and $\tilde{\xi} \triangleq \frac{\xi}{1-\tau^2}$. Then $\frac{1}{M} \left(\hat{R}_s - \hat{R}_s^\circ \right) \overset{M \to \infty}{\longrightarrow} 0$ almost surely, where $\hat{R}_s^\circ$ is the large-system secrecy sum-rate in the presence of CSI error, given by

$$\hat{R}_s^\circ = K \left[\log_2 \frac{1 + g(\beta, \tilde{\xi}) \frac{\tilde{\rho} + \frac{\tilde{\xi}\tilde{\rho}}{\beta} \left[1 + g(\beta, \tilde{\xi}) \right]^2}{\tilde{\rho} + \left[1 + g(\beta, \tilde{\xi}) \right]^2}}{1 + \rho \left[\tau^2 + \frac{1-\tau^2}{\left(1 + g(\beta, \tilde{\xi}) \right)^2} \right]} \right]^+ . \quad (29)$$

Proof: The proof of Theorem 4 is provided in Appendix B. ∎

B. Minimum Required CSI for the RCI-PR Precoder

We now consider our proposed RCI-PR precoder, and determine how the CSI estimation error must scale with the SNR, to maintain a given rate gap to the case with perfect CSI. In the following, we assume that the regularization parameter $\xi^{\star\circ}$ from (12) is used. This does not require the transmitter to be aware of the value of the distortion τ^2. We define the per-user gap ΔR_s° as the difference

$$\Delta R_s^\circ \triangleq \frac{R_{s,\mathrm{PR}}^{\star\circ} - \hat{R}_{s,\mathrm{PR}}^{\star\circ}}{K} \quad (30)$$

where $R_{s,\mathrm{PR}}^{\star\circ}$ and $\hat{R}_{s,\mathrm{PR}}^{\star\circ}$ are the large-system secrecy sum-rates obtained by the RCI-PR precoder under perfect CSI and under CSI distortion τ^2, respectively. We now derive the scaling of τ^2 required to maintain a constant secrecy rate gap for high SNR, so that the multiplexing gain is not affected.

Proposition 3: For $\beta \leq 1$, $b > 1$, a CSI distortion $\tau^2 = \frac{C}{\rho}$, with

$$C = \begin{cases} \frac{1}{2} \left(\sqrt{4b-3} - 1 \right) & \text{for } \beta < 1 \\ \frac{2}{3} \left(\sqrt{3b-2} - 1 \right) & \text{for } \beta = 1 \end{cases} \quad (31)$$

produces a high-SNR rate gap of $\log_2 b$ bits.

Proof: For $\beta \leq 1$, define

$$\mu \triangleq \tau^2 \rho + \frac{\tau^4 \rho (1 + g(\beta, \xi^{\star\circ}))^2}{1 - \tau^2} + \frac{\tau^2 (1 + g(\beta, \xi^{\star\circ}))^2}{1 - \tau^2} . \quad (32)$$

We have

$$\lim_{\rho \to \infty} \Delta R_s^\circ$$

$$= \begin{cases} \lim_{\rho \to \infty} \log_2 \left[1 + \frac{\beta^2}{4\rho(1-\beta)^2} \mu \right] = \log_2 b & \text{if } \beta < 1 \\ \lim_{\rho \to \infty} \log_2 \left[1 + \frac{1}{4} \mu \right] = \log_2 b & \text{if } \beta = 1 \end{cases} \quad (33)$$

∎

Proposition 4: For $\beta > 1$, if $\lim_{\rho\to\infty} \tau^2 = 0$, then the high-SNR rate gap is zero.

Proof: For $\beta > 1$, defining

$$\nu \triangleq \left[\tau^2 \rho^{\star\circ} + \frac{\tau^4 \rho^{\star\circ} \beta^2}{(\beta-1)^2 (1-\tau^2)} + \frac{\tau^2 \beta^2}{(\beta-1)^2 (1-\tau^2)} \right] \quad (34)$$

we have

$$\lim_{\rho\to\infty} \Delta R_s^\circ = \lim_{\rho\to\infty} \log_2 \left[1 + \left(1 - \frac{\beta}{2} \right) \nu \right] = 0. \quad (35)$$
∎

We now consider the case of FDD systems. We assume that users quantize their channel directions by using B bits and employing random vector quantization (RVQ), and that they feed the quantization index back to the transmitter [27], [28]. We obtain the following result.

Proposition 5: In order to maintain a high-SNR secrecy rate offset of $\log_2 b$ bits per-user in the large-system regime and for all values of the network load β, it is sufficient to scale the number of feedback bits B per user as $B \approx \frac{M-1}{3}\rho_{\mathrm{dB}} - (M-1) \left[\log_2 \left(\sqrt{4b-3} - 1 \right) - 1 \right]$.

Proof: We note from Propositions 3 and 4 that $\tau^2 = \frac{C}{\rho}$ ensures a gap of $\log_2 b$ bits $\forall \beta$. If RVQ is used, then the quantization error τ^2 can be upper bounded as $\tau^2 < 2^{-\frac{B}{M-1}}$ [27]. Therefore, it is sufficient to scale the number of feedback bits per user according to $B = (M-1)\log_2 \rho - (M-1)\log_2 C$. Substituting the smallest value of C from (31) and rewriting ρ in dB yields Proposition 5. ∎

C. Numerical Results

Fig. 7 compares the secrecy sum-rate $\hat{R}_s^{\star\circ}$ of the RCI precoder from the large-system analysis to the simulated ergodic secrecy sum-rate $\hat{R}_s$ for finite M, in the presence of a CSI error $\tau = 0.1$ and for different values of β. The values of $\hat{R}_s^{\star\circ}$ and $\hat{R}_s$ were obtained by (29) and (26), respectively, with $\xi = \xi^{\star\circ}$. As expected, the accuracy of the deterministic equivalent increases as M grows.

Fig. 8 shows the ergodic per-user secrecy rate $\hat{R}_{s,\mathrm{PR}}/K$, achieved by the proposed RCI-PR precoder in the presence of a channel estimation error that scales: (i) as $\tau^2 = \frac{0.1}{\rho}$ for $\beta > 1$, and (ii) as in Proposition 3 for $\beta \leq 1$, with $\log_2 b = 1$ bit. This is compared to the ergodic rate $R_{s,\mathrm{PR}}/K$, achieved by the same precoder in the presence of perfect CSI ($\tau = 0$). Three different values of β are considered, and $M = 10$. For $\beta \leq 1$, the simulations show a high-SNR gap of nearly 1 bit, whereas for $\beta > 1$ no gap is present. These results confirm the claims made in Propositions 3 and 4.

VII. CONCLUSION

In this paper, we considered linear precoding for the MISO broadcast channel with confidential messages. We first studied the RCI precoder in the large-system regime, and obtained a deterministic equivalent for the achievable secrecy sum-rate, as well as expressions for the optimal regularization parameter ξ and network load β. This analysis proved to be accurate even for finite-size systems. We found that for $\beta > 1$ the RCI precoder performs poorly in the high-SNR regime. We
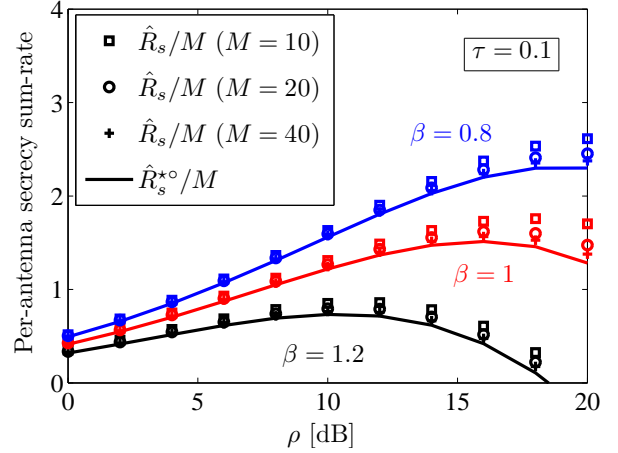

Fig. 7. Comparison between the per-antenna secrecy sum-rate $\hat{R}_s^{\star\circ}/M$ with RCI precoding in the large-system regime (29) and the simulated ergodic secrecy sum-rate $\hat{R}_s/M$, for finite M, and in the presence of a channel estimation error $\tau = 0.1$. Three sets of curves are shown, each one corresponds to a different value of β.
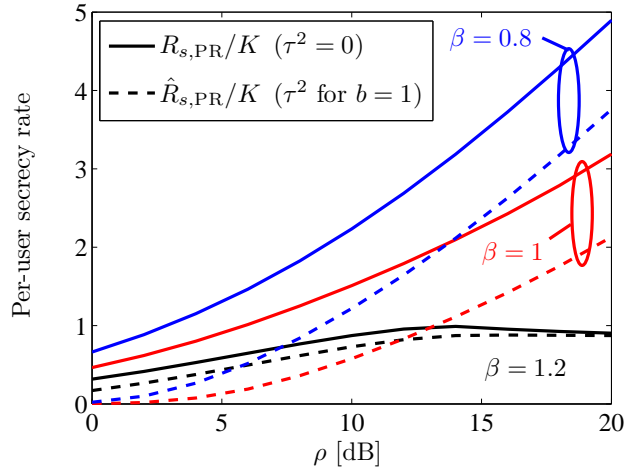

Fig. 8. Comparison between the ergodic per-user secrecy rates $R_{s,\mathrm{PR}}$ and $\hat{R}_{s,\mathrm{PR}}$ with RCI-PR precoder in the presence of perfect CSI and in the presence of channel estimation error τ^2, respectively. For $\beta > 1$, we used $\tau^2 = \frac{0.1}{\rho}$. For $\beta \leq 1$, we used τ^2 from Proposition 3, with $\log_2 b = 1$ bit. Three sets of curves are shown for $M = 10$, each one corresponds to a different value of β.

therefore proposed a linear precoder based on RCI and power reduction (RCI-PR) to increase the high-SNR performance for network loads in the range $1 < \beta < 2$. The proposed RCI-PR precoder was showed to achieve a per-user secrecy rate with the same high-SNR scaling factor as both the following upper bounds: (i) the sum-rate of the optimal RCI precoder in the absence of secrecy requirements, and (ii) the secrecy capacity of a single-user system without interference. We further studied the case of imperfect CSI, and we derived a deterministic equivalent for the secrecy sum-rate achievable by RCI precoding. We finally considered the performance of our proposed RCI-PR precoder in the presence of CSI error, and determined: (i) how the CSI estimation error must scale with the SNR, and (ii) how many feedback bits are required,

in order to maintain a given rate gap to the case with perfect CSI.

The authors are currently working to study the effect of limited feedback on time division duplex (TDD) systems, deriving the secrecy sum-rate as a function of the amount of channel training, as well as the optimal amount of channel training that maximizes the secrecy sum-rate [29]. Moreover, the authors are working to generalize the results present in this paper to the case where channel correlation is present at the transmitter side, and to study how correlation affects the secrecy rates achievable by RCI precoding [30].

APPENDIX A
PROOF OF THEOREM 1

By defining

$$A_k = \mathbf{h}_k^H \left(\mathbf{H}_k^H \mathbf{H}_k + M\xi \mathbf{I} \right)^{-1} \mathbf{h}_k, \tag{36}$$

$$B_k = \mathbf{h}_k^H \left(\mathbf{H}_k^H \mathbf{H}_k + M\xi \mathbf{I} \right)^{-1} \mathbf{H}_k^H \mathbf{H}_k \left(\mathbf{H}_k^H \mathbf{H}_k + M\xi \mathbf{I} \right)^{-1} \mathbf{h}_k \tag{37}$$

we can rewrite the SINRs at the intended user and the eavesdropper as

$$\text{SINR}_k = \frac{\rho A_k^2}{\gamma \left(1 + A_k\right)^2 + \rho B_k} \quad \text{and} \quad \text{SINR}_{\widetilde{k}} = \frac{\rho B_k}{\gamma \left(1 + A_k\right)^2}. \tag{38}$$

We rewrite $A_k = \frac{M}{K-1} \mathbf{v}_M^H \mathbf{Q}_M \mathbf{v}_M$, where

$$\mathbf{Q}_{k,M} = \left(\frac{1}{K-1} \mathbf{H}_k^H \mathbf{H}_k - z\mathbf{I} \right)^{-1} \in \mathbb{C}^{M \times M}, \tag{39}$$

$$\mathbf{v}_{k,M} = \frac{1}{\sqrt{M}} \mathbf{h}_k \in \mathbb{C}^M, \quad z = -\frac{M\xi}{K-1}. \tag{40}$$

By Bai and Silverstein's Lemma [31]–[33], we have

$$\text{E} \left[\phi_k \left| \mathbf{v}_{k,M}^H \mathbf{Q}_{k,M} \mathbf{v}_{k,M} - \frac{1}{M} \text{tr} \mathbf{Q}_{k,M} \right|^p \right]$$
$$\leq \frac{C_p}{M^p} \left(\frac{M}{\bar{\lambda}_M} \right)^{\frac{p}{2}}$$
$$= \frac{C_p}{M^{\frac{p}{2}} \bar{\lambda}_M^{\frac{p}{2}}} = f_M \quad \forall p \geq 1 \tag{41}$$

where C_p is a constant depending only on p, $\phi_k = \mathbf{1}_{\{|\lambda_1(\mathbf{H}_k^H \mathbf{H}_k) - M\xi|, \dots, |\lambda_M(\mathbf{H}_k^H \mathbf{H}_k) - M\xi| > \bar{\lambda}_M\}}$, with $\bar{\lambda}_M \to 0$. Assume $\xi \in \mathcal{D}_M'$, with $\mathcal{D}_M' = \mathcal{D}_M$ for $\beta \leq 1$ and $\mathcal{D}_M' = \mathcal{D}_M \backslash \left\{ \left[-\frac{C}{M^{\frac{1}{2}-\epsilon}}, +\frac{C}{M^{\frac{1}{2}-\epsilon}} \right] \right\}$ for $\beta > 1$. Then we have $M = \mathcal{O}(\bar{\lambda}_M^{-2-\epsilon})$, for some $\epsilon > 0$, and $\min_{k \leq K}\{\phi_k\} \xrightarrow{\text{a.s.}} 1$ [33]. It follows from the Markov inequality and the Borel-Cantelli lemma [34] that $\max_k |\mathbf{v}_{k,M}^H \mathbf{Q}_{k,M} \mathbf{v}_{k,M} - \frac{1}{M} \text{tr} \mathbf{Q}_{k,M}| \xrightarrow{\text{a.s.}} 0$, as $M \to \infty$. The term $\frac{1}{M} \text{tr} \mathbf{Q}_{k,M}$ is by definition the Stieltjes transform $m_{\mathbf{H}_k^H \mathbf{H}_{k,M}}(z)$ of $\mathbf{H}_k^H \mathbf{H}_{k,M}$. Similarly, it can be shown that $\max_k |m_{\mathbf{H}_k^H \mathbf{H}_{k,M}}(z) - m(z)| \xrightarrow{\text{a.s.}} 0$, where $m(z)$ can be obtained as the solution of $m(z) = \left[1 - \frac{M}{K-1} - z - z\frac{M}{K-1} m(z) \right]^{-1}$. This yields

$$A_k - g(\beta, \xi) \xrightarrow{\text{a.s.}} 0 \tag{42}$$

with

$$g(\beta, \xi) = \beta^{-1} m(\xi)$$
$$= \frac{1}{2} \left[\pm \sqrt{\frac{(1-\beta)^2}{\xi^2} + \frac{2(1+\beta)}{\xi} + 1} + \frac{1-\beta}{\xi} - 1 \right], \tag{43}$$

and where in order for m to be a Stieltjes transform, the sign of the square root must be chosen the same as the sign of ξ [35].

We now rewrite $B_k = A_k - \frac{M^2\xi}{(K-1)^2} \mathbf{v}_{k,M}^H \mathbf{Q}_{k,M}^2 \mathbf{v}_{k,M}$, and similarly we have

$$\text{E} \left[\phi_k \left| \mathbf{v}_{k,M}^H \mathbf{Q}_{k,M}^2 \mathbf{v}_{k,M} - \frac{1}{M} \text{tr} \mathbf{Q}_{k,M}^2 \right|^p \right]$$
$$\leq \frac{C_p}{M^p} \left(\frac{M}{\bar{\lambda}_M^2} \right)^{\frac{p}{2}}$$
$$= \frac{C_p}{M^{\frac{p}{2}} \bar{\lambda}_M^p} = g_M \quad \forall p \geq 1. \tag{44}$$

Again, if $M = \mathcal{O}(\bar{\lambda}_M^{-2-\epsilon})$, for some $\epsilon > 0$, we have $\max_k |\mathbf{v}_{k,M}^H \mathbf{Q}_{k,M}^2 \mathbf{v}_{k,M} - \frac{1}{M} \text{tr} \mathbf{Q}_{k,M}^2| \xrightarrow{\text{a.s.}} 0$, as $M \to \infty$. We note that $\frac{1}{M} \text{tr} \mathbf{Q}_{k,M}^2$ is the Stieltjes transform of $\mathbf{Q}_{k,M}^2$, given by

$$\frac{1}{M} \text{tr} \mathbf{Q}_{k,M}^2 = \int \frac{dF_M(\lambda)}{(\lambda_{\mathbf{R}_M} - z)^2} = \frac{\partial}{\partial z} \int \frac{dF_M(\lambda)}{\lambda_{\mathbf{R}_M} - z} = m'_{\mathbf{R}_M}(z) \tag{45}$$

where $F_M(\lambda)$ is the distribution of the eigenvalues of $\mathbf{R}_M$. Since both $m_{\mathbf{R}_{k,M}}(z)$ and $m(z)$ are analytic functions, we have $\max_k |m'_{\mathbf{R}_{k,M}}(z) - m'(z)| \xrightarrow{\text{a.s.}} 0$, as $M \to \infty$, and it follows that

$$B_k - \left[\frac{1}{\beta} m(z) - \frac{M^2\xi}{(K-1)^2} \frac{\partial}{\partial z} m(z) \right]$$
$$= B_k - \left[g(\beta, \xi) + \xi \frac{\partial}{\partial \xi} g(\beta, \xi) \right] \xrightarrow{\text{a.s.}} 0. \tag{46}$$

For the power normalization constant γ we have

$$\gamma = \text{tr} \left\{ \left(\mathbf{H}^H \mathbf{H} + M\xi \mathbf{I} \right)^{-1} \right\} - M\xi \text{tr} \left\{ \left(\mathbf{H}^H \mathbf{H} + M\xi \mathbf{I} \right)^{-2} \right\}$$
$$= \frac{1}{\beta} m_{\mathbf{H}\mathbf{H}_M^H}(z') - \frac{\xi}{\beta^2} m'_{\mathbf{H}\mathbf{H}_M^H}(z') \tag{47}$$

where $z' = -\frac{M\xi}{K}$. If $\xi \in \mathcal{D}_M'$, if follows that

$$\gamma - \left[g(\beta, \xi) + \xi \frac{\partial}{\partial \xi} g(\beta, \xi) \right] \xrightarrow{\text{a.s.}} 0. \tag{48}$$

By the continuity of R_s and R_s°, it follows that the previous convergence results also hold for $\xi \in \left[-\frac{C}{M^{\frac{1}{2}-\epsilon}}, +\frac{C}{M^{\frac{1}{2}-\epsilon}} \right]$ and $\beta > 1$. Equation (7) then follows from (4), (38), (42), (46), (48), and by applying the continuous mapping theorem, the Markov inequality, and the Borel-Cantelli lemma.

APPENDIX B
PROOF OF THEOREM 4

From [16], by defining $\tilde{\rho} \triangleq \frac{\rho(1-\tau^2)}{\rho\tau^2+1}$ and $\tilde{\xi} \triangleq \frac{\xi}{1-\tau^2}$, a deterministic equivalent for $\hat{\text{SINR}}_k$ is given by

$$\hat{\text{SINR}}_k^{\circ} = g(\beta,\tilde{\xi}) \frac{\tilde{\rho} + \frac{\tilde{\xi}\tilde{\rho}}{\beta}\left[1 + g(\beta,\tilde{\xi})\right]^2}{\tilde{\rho} + \left[1 + g(\beta,\tilde{\xi})\right]^2}. \tag{49}$$

By defining $\mathbf{\Omega}_k = \left(\hat{\mathbf{H}}_k^H \hat{\mathbf{H}}_k + M\xi\mathbf{I}\right)^{-1}$, we can rewrite $\hat{\text{SINR}}_{\tilde{k}}$ as

$$\hat{\text{SINR}}_{\tilde{k}} = \rho \frac{\hat{B}_k + 2\left(1 + \hat{A}_k\right)Q_k + \left(1 + \hat{A}_k\right)^2 R_k}{\hat{\gamma}\left(1 + \hat{A}_k\right)^2}, \tag{50}$$

where

$$\hat{A}_k = \hat{\mathbf{h}}_k^H \mathbf{\Omega}_k \hat{\mathbf{h}}_k, \quad \hat{B}_k = \hat{\mathbf{h}}_k^H \mathbf{\Omega}_k \hat{\mathbf{H}}_k^H \hat{\mathbf{H}}_k \mathbf{\Omega}_k \hat{\mathbf{h}}_k,$$

$$Q_k = \hat{\mathbf{h}}_k^H \mathbf{\Omega}_k \hat{\mathbf{H}}_k^H \hat{\mathbf{H}}_k \left(\mathbf{\Omega}_k - \frac{\mathbf{\Omega}_k \hat{\mathbf{h}}_k \hat{\mathbf{h}}_k^H \mathbf{\Omega}_k}{1 + \hat{A}_k}\right)\mathbf{e}_k, \quad \text{and}$$

$$R_k = \mathbf{e}_k^H \left(\mathbf{\Omega}_k - \frac{\mathbf{\Omega}_k \hat{\mathbf{h}}_k \hat{\mathbf{h}}_k^H \mathbf{\Omega}_k}{1 + \hat{A}_k}\right)\hat{\mathbf{H}}_k^H \hat{\mathbf{H}}_k \left(\mathbf{\Omega}_k - \frac{\mathbf{\Omega}_k \hat{\mathbf{h}}_k \hat{\mathbf{h}}_k^H \mathbf{\Omega}_k}{1 + \hat{A}_k}\right)\mathbf{e}_k.$$

If $\xi \in \mathcal{D}_M$, we have

$$\hat{A}_k - g\left(\beta,\tilde{\xi}\right) \xrightarrow{\text{a.s.}} 0, \quad \hat{B}_k - \left[g\left(\beta,\tilde{\xi}\right) + \tilde{\xi}\frac{\partial}{\partial\tilde{\xi}}g\left(\beta,\tilde{\xi}\right)\right] \xrightarrow{\text{a.s.}} 0,$$

$$Q_k \xrightarrow{\text{a.s.}} 0,$$

$$R_k - \frac{\tau^2}{1-\tau^2}\left[g\left(\beta,\tilde{\xi}\right) + \tilde{\xi}\frac{\partial}{\partial\tilde{\xi}}g\left(\beta,\tilde{\xi}\right)\right] \xrightarrow{\text{a.s.}} 0,$$

and

$$\hat{\gamma} - \frac{1}{1-\tau^2}\left[g\left(\beta,\tilde{\xi}\right) + \tilde{\xi}\frac{\partial}{\partial\tilde{\xi}}g\left(\beta,\tilde{\xi}\right)\right] \xrightarrow{\text{a.s.}} 0$$

hence a deterministic equivalent for $\hat{\text{SINR}}_{\tilde{k}}$ is given by

$$\hat{\text{SINR}}_{\tilde{k}}^{\circ} = \rho\left[\tau^2 + \frac{1-\tau^2}{\left(1 + g(\beta,\tilde{\xi})\right)^2}\right]. \tag{51}$$

Theorem 4 then follows from (26), (49), (51), and from the continuous mapping theorem [34].

REFERENCES

[1] A. Mukherjee, S. A. A. Fakoorian, J. Huang, and A. L. Swindlehurst, "Principles of physical-layer security in multiuser wireless networks: Survey," 2010, arXiv:1011.3754.

[2] A. D. Wyner, "The wire-tap channel," *Bell System Tech. J.*, vol. 54, pp. 1355–1387, 1975.

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

[4] Y. Liang, H. V. Poor, and S. Shamai (Shitz), *Information Theoretic Security*. Dordrecht, The Netherlands: Now Publisher, 2009.

[5] R. Liu and W. Trappe, Eds, *Securing Wireless Communications at the Physical Layer*. New York: Springer Verlag, 2010.

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

[7] E. Ekrem and S. Ulukus, "The secrecy capacity region of the Gaussian MIMO multi-receiver wiretap channel," *IEEE Trans. Inf. Theory*, vol. 57, no. 4, pp. 2083–2114, April 2011.

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

[9] X. Zhou and M. 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.

[10] A. Mukherjee and A. Swindlehurst, "Robust beamforming for security in MIMO wiretap channels with imperfect CSI," *IEEE Trans. Signal Process.*, vol. 59, no. 1, pp. 351–361, Jan. 2011.

[11] X. Zhou, M. McKay, B. Maham, and A. Hjørungnes, "Rethinking the secrecy outage formulation: A secure transmission design perspective," *IEEE Comms. Letters*, vol. 15, no. 3, pp. 302–304, March 2011.

[12] R. Liu, T. Liu, H. Poor, and S. Shamai, "Multiple-input multiple-output Gaussian broadcast channels with confidential messages," *IEEE Trans. Inf. Theory*, vol. 56, no. 9, pp. 4215–4227, 2010.

[13] G. Geraci, J. Yuan, A. Razi, and I. B. Collings, "Secrecy sum-rates for multi-user MIMO linear precoding," in *Proc. IEEE Int. Symp. on Wireless Commun. Systems (ISWCS)*, Nov. 2011.

[14] G. Geraci, M. Egan, J. Yuan, A. Razi, and I. B. Collings, "Secrecy sum-rates for multi-user MIMO regularized channel inversion precoding," *IEEE Trans. Commun.*, vol. 60, no. 11, pp. 3472–3482, Nov. 2012.

[15] G. Geraci, J. Yuan, and I. B. Collings, "Large system analysis of the secrecy sum-rates with regularized channel inversion precoding," in *Proc. IEEE Wireless Commun. Networking Conference (WCNC)*, Apr. 2012.

[16] V. K. Nguyen, R. Muharar, and J. S. Evans, "Multiuser transmit beamforming via regularized channel inversion: A large system analysis," *Technical Report*, Nov. 2009, available: http://cubinlab.ee.unimelb.edu.au/ rmuharar/doc/manuscriptrevRusdha22-11.pdf.

[17] S. Wagner, R. Couillet, M. Debbah, and D. T. M. Slock, "Large system analysis of linear precoding in correlated MISO broadcast channels under limited feedback," *IEEE Trans. Inf. Theory*, vol. 58, no. 7, pp. 4509–4537, July 2012.

[18] Q. Spencer, C. Peel, A. Swindlehurst, and M. Haardt, "An introduction to the multi-user MIMO downlink," *IEEE Comms. Mag.*, vol. 42, no. 10, pp. 60–67, Oct. 2004.

[19] Q. Li, G. Li, W. Lee, M. Lee, D. Mazzarese, B. Clerckx, and Z. Li, "MIMO techniques in WiMAX and LTE: a feature overview," *IEEE Comms. Mag.*, vol. 48, no. 5, pp. 86–92, May 2010.

[20] Q. Spencer, A. Swindlehurst, and M. Haardt, "Zero-forcing methods for downlink spatial multiplexing in multiuser MIMO channels," *IEEE Trans. Signal Process.*, vol. 52, no. 2, pp. 461–471, 2004.

[21] T. Yoo and A. Goldsmith, "On the optimality of multiantenna broadcast scheduling using zero-forcing beamforming," *IEEE J. Sel. Areas Commun.*, vol. 24, no. 3, pp. 528–541, Mar. 2006.

[22] C. B. Peel, B. M. Hochwald, and A. L. Swindlehurst, "A vector-perturbation technique for near-capacity multiantenna multiuser communication - Part I: Channel inversion and regularization," *IEEE Trans. Commun.*, vol. 53, no. 1, pp. 195–202, Jan. 2005.

[23] M. Joham, W. Utschick, and J. Nossek, "Linear transmit processing in MIMO communications systems," *IEEE Trans. Signal Process.*, vol. 53, no. 8, pp. 2700–2712, Aug. 2005.

[24] L. Sun and M. McKay, "Eigen-based transceivers for the MIMO broadcast channel with semi-orthogonal user selection," *IEEE Trans. Signal Process.*, vol. 58, no. 10, pp. 5246–5261, Oct. 2010.

[25] S. Jin, M. R. McKay, X. Gao, and I. B. Collings, "MIMO multichannel beamforming: SER and outage using new eigenvalue distributions of complex noncentral wishart matrices," *IEEE Trans. Commun.*, vol. 56, no. 3, pp. 424–434, 2008.

[26] B. Hochwald and S. Vishwanath, "Space-time multiple access: Linear growth in the sum rate," in *Proc. Allerton Conf. on Commun., Control, and Computing*, Monticello, IL, Oct. 2002.

[27] N. Jindal, "MIMO broadcast channels with finite-rate feedback," *IEEE Trans. Inf. Theory*, vol. 52, no. 11, pp. 5045–5060, Nov. 2006.

[28] D. Ryan, I. B. Collings, I. V. L. Clarkson, and R. W. Heath Jr., "Performance of vector perturbation multiuser MIMO systems with limited feedback," *IEEE Trans. Commun.*, vol. 57, no. 9, pp. 2633–2644, 2008.

[29] G. Geraci, R. Couillet, J. Yuan, M. Debbah, and I. B. Collings, "Secrecy sum-rates with regularized channel inversion precoding under imperfect CSI at the transmitter," in *Proc. Internat. Conf. Acoust. Speech Signal Process. (ICASSP)*, May 2013.

[30] G. Geraci, A. Y. Al-nahari, J. Yuan, and I. B. Collings, "Linear precoding for broadcast channels with confidential messages under transmit-side channel correlation," *IEEE Comms. Letters*, 2013, accepted, available: arXiv:1304.6157.

[31] M. J. M. Peacock, I. B. Collings, and M. L. Honig, "Eigenvalues distributions of sums and products of large random matrices via incremental matrix expansions," *IEEE Trans. Inf. Theory*, vol. 54, no. 5, pp. 2123–2138, 2008.

[32] R. Couillet and M. Debbah, *Random Matrix Theory Methods for Wireless Communications*. Cambridge University Press, 2011.

[33] R. Couillet, F. Pascal, and J. W. Silverstein, "Robust M-estimation for array processing: A random matrix approach," *IEEE Trans. Signal Process.*, 2012, submitted. Available: http://couillet.romain.perso.sfr.fr/docs/articles/robust_est_submitted.pdf.

[34] P. Billingsley, *Probability and measure,* 3rd ed. Hoboken, NJ: John Wiley & Sons, Inc., 1995.

[35] J. W. Silverstein and S.-I. Choi, "Analysis of the limiting spectral distribution of large dimensional random matrices," *Journal of Multivariate Analysis*, vol. 54, no. 2, pp. 295–309, 1995.

Giovanni Geraci (S'11) received the B.Sc. in Telecommunications Engineering from Università di Palermo, Italy, in 2005, and the M.Sc. in Telecommunications Engineering from Politecnico di Milano, Italy, in 2009. He is currently working towards the Ph.D. degree in Electrical Engineering at the University of New South Wales, Sydney, Australia. His research is supported by the International Postgraduate Research Scholarship (IPRS) and CSIRO Postgraduate Scholarship. He has held internships at the Alcatel-Lucent Chair on Flexible Radio at Supélec, Gif-sur-Yvette, France, and at the University of Texas at Austin.

Romain Couillet received his MSc in Mobile Communications at the Eurecom Institute and his MSc in Communication Systems in Telecom ParisTech, France in 2007. From 2007 to 2010, he worked with ST-Ericsson as an Algorithm Development Engineer on the Long Term Evolution Advanced project, where he prepared his PhD with Supélec, France, which he graduated in November 2010. He is currently an assistant professor at Supélec, France. His research topics are in information theory, signal processing, and random matrix theory. He is the recipient of the 2013 CNRS Bronze Medal in the section "Science of Information and its Interactions", of the 2011 EEA/GdR ISIS/GRETSI best PhD thesis award, and of the Valuetools 2008 best student paper award.

Jinhong Yuan received the B.E. and Ph.D degrees in electronics engineering from Beijing Institute of Technology, Beijing, China, in 1991 and 1997, respectively. From 1997 to 1999 he was a Research Fellow at the School of Electrical Engineering, the University of Sydney, Sydney, Australia. In 2000 he joined the School of Electrical Engineering and Telecommunications, the University of New South Wales, Sydney, Australia, where he is currently a Professor for Telecommunications of the school. He has published two books, two book chapters, over 200 papers in telecommunications journals and conference proceedings and 40 industrial reports. He is a co-inventor of one patent on MIMO systems and two patents on low-density-parity-check (LDPC) codes. He co-authored three Best Paper Awards and one Best Poster Award, including a Best Paper Award of IEEE Wireless Communications and Networking Conference (WCNC), Cancun, Mexico in 2011, and a Best Paper Award of IEEE International Symposium on Wireless Communications Systems (ISWCS), Trondheim, Norway in 2007. His publication is available from http://www2.ee.unsw.edu.au/wcl/JYuan.html. He serves as the IEEE NSW Chair of joint Communications/Signal Processions/Ocean Engineering Chapter. His current research interests include error control coding and information theory, communication theory, and wireless communications.

Mérouane Debbah entered the Ecole Normale Supérieure de Cachan (France) in 1996 where he received his M.Sc and Ph.D. degrees respectively. He worked for Motorola Labs (Saclay, France) from 1999-2002 and the Vienna Research Center for Telecommunications (Vienna, Austria) until 2003. He then joined the Mobile Communications department of the Institut Eurecom (Sophia Antipolis, France) as an Assistant Professor until 2007. He is now a Full Professor at Supélec (Gif-sur-Yvette, France), holder of the Alcatel-Lucent Chair on Flexible Radio and a recipient of the ERC starting grant MORE (Advanced Mathematical Tools for Complex Network Engineering). His research interests are in information theory, signal processing and wireless communications. He is a senior area editor for IEEE Transactions on Signal Processing. Mérouane Debbah is the recipient of the "Mario Boella" award in 2005, the 2007 General Symposium IEEE GLOBECOM best paper award, the Wi-Opt 2009 best paper award, the 2010 Newcom++ best paper award, the WUN CogCom Best Paper 2012 Award as well as the Valuetools 2007, Valuetools 2008, Valuetools 2012 and CrownCom2009 best student paper awards. He is a WWRF fellow. In 2011, he received the IEEE Glavieux Prize Award.

Iain B. Collings (S'92-M'95-SM'02) received the B.E. degree in Electrical and Electronic Engineering from the University of Melbourne in 1992, and the Ph.D. degree in Systems Engineering from the Australian National University in 1995. Currently he is the Research Director of the Wireless and Networking Technologies Laboratory, and one of the CEO's Science Leaders, at the Australian Commonwealth Scientific and Industrial Research Organisation (CSIRO). Prior to this he was an Associate Professor at the University of Sydney (1999-2005); a Lecturer at the University of Melbourne (1996-1999); and a Research Fellow in the Australian Cooperative Research Centre for Sensor Signal and Information Processing (1995). He has published over 230 research papers in the area of mobile digital communications. More specifically, adaptive multi-carrier modulation, multi-user and MIMO systems, and ad hoc and sensor networks. In 2009 he was awarded the Engineers Australia IREE Neville Thiele Award for outstanding achievements in engineering, and in 2011 he was a recipient of the IEEE CommSoc Stephen O. Rice Best Paper Award for IEEE Transactions on Communications. Dr Collings served as an Editor for the IEEE Transactions on Wireless Communications (2002-2009), and for the Elsevier Physical Communication Journal PHYCOM (since 2007). He has served as a Co-Chair of the Conference Technical Program Committee for IEEE International Conference on Communications (ICC) 2013 and for IEEE Vehicular Technology Conf. (VTC) Spring 2011; and as a Vice Chair of the TPC for IEEE Wireless Communications and Networking Conference (WCNC) 2010 and IEEE VTC Spring 2006; as well as serving on a number of other TPCs and organizing committees of IEEE conferences. He is a founding organizer of the Australian Communication Theory Workshops 2000-2012. He also served as the Chair of the Joint Communications & Signal Processing Chapter in the IEEE NSW Section (2008-2010), as well as serving as the Secretary of the IEEE NSW Section (2010).