# Secrecy for MISO Broadcast Channels with Heterogeneous CSIT

Pritam Mukherjee[1], Ravi Tandon[2], and Sennur Ulukus[1]

[1]Department of Electrical and Computer Engineering, University of Maryland, College Park, MD 20742
[2]Discovery Analytics Center and Department of Computer Science, Virginia Tech, Blacksburg, VA 24061

***Abstract*—We consider the two-user multiple-input single-output (MISO) broadcast channel with confidential messages (BCCM), in which the nature of channel state information at the transmitter (CSIT) from each user can be of the form P, D and N, corresponding to perfect and instantaneous, completely delayed, and no CSIT, respectively. We focus on the cases with heterogeneous CSIT from the users, that is, the states PD, PN and DN. The main contribution of this paper is to establish the exact secure degrees of freedom (s.d.o.f.) regions of the MISO BCCM in all of these three heterogeneous states. The results highlight the impact of availability of CSIT on the s.d.o.f. region.**

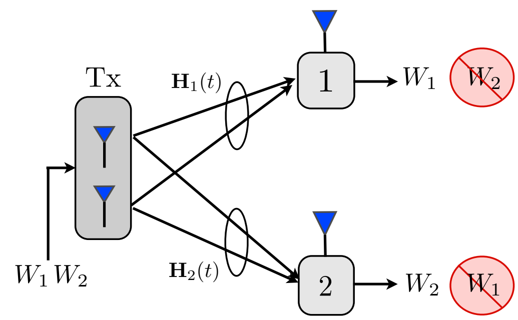


Fig. 1. MISO broadcast channel with confidential messages (BCCM).

## I. Introduction

We consider the fading two-user multiple-input single-output (MISO) broadcast channel with confidential messages (BCCM), in which the transmitter with two antennas has two confidential messages, one for each of the single antenna users (see Fig. 1). The secure degrees of freedom (s.d.o.f.) region of this channel depends on the availability of channel state information (CSI) of the users' channels at the transmitter. The secrecy capacity region of the MISO BCCM for the case of perfect and instantaneous CSI at all terminals has been characterized in [1], [2]. Using these results, it follows that for the two-user MISO BCCM, the sum s.d.o.f. is 2 with perfect and instantaneous channel state information at the transmitter (CSIT). In practice, the assumption of perfect and instantaneous CSIT may be too optimistic as CSIT may be delayed, imprecise or may not even be available at all. In this paper, we focus on the delay aspect of CSIT and assume that CSIT, if available, is always precise.

The effect of delayed or no CSIT on the degrees of freedom (d.o.f.) has been widely studied in the literature, both with and without secrecy constraints. With perfect CSIT, the sum d.o.f. for the two-user MISO broadcast channel (BC) is 2. With no CSIT however, reference [3] shows that the sum d.o.f. collapses to 1. With delayed CSIT, by which we mean completely stale CSIT as in [4], reference [4] shows that the sum d.o.f. for the two-user MISO BC increases to $\frac{4}{3}$, and [5] establishes the d.o.f. region for the two-user MIMO BC.

When secrecy constraints are introduced, the s.d.o.f. is known for several scenarios of delayed or no CSIT. For the two-user MISO BCCM with perfect CSIT, the optimal sum s.d.o.f. is 2. With no CSIT, however, the sum s.d.o.f. reduces to zero as the two users are statistically equivalent and hence no secrecy is possible. On the other hand, with completely outdated CSIT from both users, [6] shows that the sum s.d.o.f. increases to 1.

The aforementioned literature considers homogeneous CSIT scenarios in which the nature of channel knowledge supplied by every receiver is of the same form. In practice, however, the nature of CSIT can vary across users. Such variability can arise either naturally (due to the difference in tolerable feedback overhead from user to user) or it can be artificially induced (by deliberately altering the channel feedback mechanism). This observation naturally leads to the setting of *heterogeneous* (or hybrid) CSIT which models the variability in the quality/delay of channel knowledge supplied by different users.

The complete characterization of the d.o.f. of all fixed heterogeneous CSIT configurations is known for the two-user MISO BC without secrecy constraints: For state PD, the optimal sum d.o.f. is shown to be $3/2$ in [7], [8]; and [9] recently settles the states PN and DN through a novel converse proof showing that the optimal sum d.o.f. is given by 1. Beyond these results, partial results are available for the three-user MISO BC with hybrid CSIT in [10], [11]. In addition, [12] considers the MISO wiretap channel with delayed CSIT from the legitimate receiver and no CSIT from the eavesdropper (state DN) and shows that $\frac{1}{2}$ sum s.d.o.f. is optimal when restricted to linear transmission strategies, that is, the optimal linear s.d.o.f. is $\frac{1}{2}$. An achievable scheme to achieve $\frac{1}{2}$ sum s.d.o.f. in this case is presented in [6]. Reference [12] further shows that the optimal linear s.d.o.f. is $\frac{1}{3}$ for the blind single antenna wiretap channel with delayed CSIT from the legitimate receiver (SISO wiretap channel

This work was supported by NSF Grants CNS 13-14733, CCF 14-22111, CCF 14-22129 and CCF 14-22090.

with state DN). Characterization of the optimal s.d.o.f. in the presence of heterogeneous CSIT remains an open problem for most other channel models.

In this paper, we focus on the MISO BCCM with heterogeneous CSIT. We establish the s.d.o.f. regions of the MISO BCCM in all of the three possible heterogeneous states: PN, PD and DN. To do so, we provide new converse proofs for the PD and DN states that exploit the *local statistical equivalence* property introduced in [13]. We also provide a new achievable scheme for the DN state. Our results illustrate the impact of CSIT on the s.d.o.f. of the MISO BCCM.

## II. System Model

We consider a two-user MISO BCCM, shown in Fig. 1, where the transmitter Tx, equipped with 2 antennas, wishes to send independent confidential messages to two single antenna receivers. The input-output relations at time $t$ are given by,

$$Y(t) = \mathbf{H}_1(t)\mathbf{X}(t) + N_1(t) \tag{1}$$

$$Z(t) = \mathbf{H}_2(t)\mathbf{X}(t) + N_2(t), \tag{2}$$

where $Y(t)$ and $Z(t)$ are the channel outputs of receivers 1 and 2, respectively. The $2 \times 1$ channel input $\mathbf{X}(t)$ is power constrained as $\mathbb{E}[||\mathbf{X}(t)||^2] \leq P$, and $N_1(t)$ and $N_2(t)$ are circularly symmetric complex white Gaussian noises with zero-mean and unit-variance. The $1 \times 2$ channel vectors $\mathbf{H}_1(t)$ and $\mathbf{H}_2(t)$ of receivers 1 and 2, respectively, are independent and identically distributed (i.i.d.) with continuous distributions, and are also i.i.d. over time. We denote $\mathbf{H}(t) = \{\mathbf{H}_1(t), \mathbf{H}_2(t)\}$ as the collective channel vectors at time $t$, and $\Omega = \{\mathbf{H}(1), \ldots, \mathbf{H}(n)\}$ as the sequence of channel vectors up until and including time $n$.

In practice, the receivers estimate the channel coefficients and feed them back to the transmitter. At any time $t$, the receiver may send any function of all the channel measurements upto and including time $t$ to the transmitter. As an idealization, we assume that the CSIT, if available, has infinite precision. The type of CSIT availability from each user remains fixed throughout the duration of the communication. We model the availability of CSIT as one of the 6 possible CSIT states:

1) PP: This denotes the availability of precise and instantaneous CSI (P) of both users at the transmitter.
2) PD (or, DP): In this state, the first (or, second) user's CSI is available instantaneously (P) at the transmitter, while the second (or, first) user's CSIT is delayed (D), that is, the CSI is available after a delay such that it is completely outdated.
3) PN (or, NP): In this state, the first (or, second) user's CSIT is available instantaneously (P), while the second (or, first) user's CSIT is not available at all (N).
4) DD: This denotes the availability of precise but delayed CSI (D) of both users at the transmitter.
5) DN (or, ND): In this state, the first (or, second) user's CSIT is delayed (D), while the second (or, first) user's CSIT is not available at all (N).
6) NN: This denotes that no CSIT (N) is available at the transmitter.

For the states with homogeneous CSIT: PP, DD, and NN, the s.d.o.f. regions are already known: see [1], [2] for state PP, and [6] for state DD, and the sum s.d.o.f. is zero in the NN state since both users are statistically equivalent.

In this paper, we focus on the heterogeneous CSIT states: PD, PN and DN. Without secrecy constraints, the optimal d.o.f. for these states are known: see [7], [8] for state PD, where the optimal sum d.o.f. is $\frac{3}{2}$, and see [9] which recently settled the states PN and DN where the optimal sum d.o.f. is 1. In this paper, we establish the s.d.o.f. regions for these heterogeneous CSIT states with confidentiality constraints.

A secure rate pair $(R_1, R_2)$ is achievable if there exists a sequence of codes which satisfy the reliability constraints at the receivers, namely, $\Pr[W_i \neq \hat{W}_i] \leq \epsilon_n$, for $i = 1, 2$, and the secrecy constraints, namely,

$$\frac{1}{n} I(W_1; Z^n, \Omega) \leq \epsilon_n, \qquad \frac{1}{n} I(W_2; Y^n, \Omega) \leq \epsilon_n, \tag{3}$$

where $\epsilon_n \to 0$ as $n \to \infty$. A s.d.o.f. pair $(d_1, d_2)$ is achievable, if there exists an achievable rate pair $(R_1, R_2)$ such that

$$d_1 = \lim_{P\to\infty} \frac{R_1}{\log P}, \qquad d_2 = \lim_{P\to\infty} \frac{R_2}{\log P}. \tag{4}$$

## III. Main Results and Discussion

We present two theorems which establish the s.d.o.f. regions of the MISO BCCM in states PN, PD and DN.

**Theorem 1** *The s.d.o.f. region of the two-user MISO BCCM in state* PN *or state* PD *is the set of all non-negative pairs* $(d_1, d_2)$ *satisfying,*

$$d_1 + d_2 \leq 1. \tag{5}$$

**Theorem 2** *The s.d.o.f. region of the two-user MISO BCCM in state* DN *is the set of all non-negative pairs* $(d_1, d_2)$ *satisfying,*

$$d_1 + d_2 \leq \frac{1}{2}. \tag{6}$$

Theorems 1 and 2 are proved in Sections IV and V.

Fig. 2 shows the s.d.o.f. regions established in the above theorems. We now provide several remarks pointing out some interesting aspects of these results.

*Remark 1. [State equivalence in the presence of secrecy]*

Note that the s.d.o.f. region of the MISO BCCM in state PD is the same as that in state PN. This suggests, perhaps surprisingly, that when one of the users provides instantaneous CSI, delayed CSI from the other user does not increase the s.d.o.f. at all; it might as well not provide any CSI. Further, the optimal sum s.d.o.f. in state PD, 1, is the same as that of the optimal sum s.d.o.f. in state DD [6]. Thus, from a sum s.d.o.f. perspective, if one of the users provides delayed CSIT, there is no benefit if the other user provides instantaneous CSIT instead of delayed CSIT. However, this is not true from the s.d.o.f. region perspective. The s.d.o.f. region for state DD, established in [6], is strictly contained in the the s.d.o.f. region

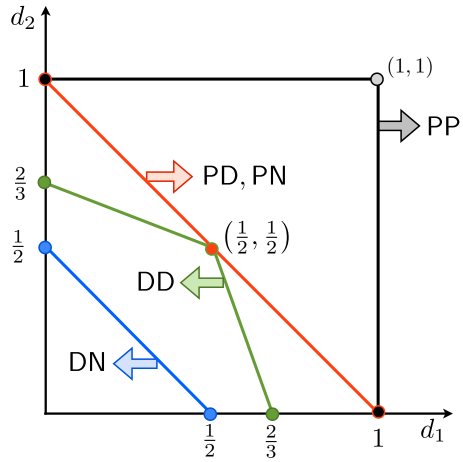


Fig. 2. S.d.o.f. regions for various CSIT states.

for state PD; for example, the maximum individual s.d.o.f. for a user in state DD is $\frac{2}{3}$, while it is 1 in state PD.

*Remark 2. [The blind wiretap channel with delayed CSIT]*

Note that Theorem 2 also establishes the optimal s.d.o.f. of the wiretap channel with delayed CSIT from the legitimate receiver but no CSI from the eavesdropper to be $\frac{1}{2}$. An achievable scheme for this model is provided in [6]. It is further shown to be optimal when only linear achievable schemes are admissible, that is, in terms of linear s.d.o.f., in [12]. Theorem 2 strengthens that result by establishing the optimality of $\frac{1}{2}$ s.d.o.f. without any linearity assumptions. Further, it also establishes the optimal s.d.o.f. of the wiretap channel with no CSI from the legitimate receiver and delayed CSI from the eavesdropper.

*Remark 3. [Benefits of alternating CSIT for secrecy]*

Our results illustrate the synergistic benefits of alternating CSIT even with secrecy constraints. In the setting of alternating CSIT introduced in [14], the CSIT state can vary with time. It was shown in [14] that this variation can be exploited by jointly encoding across multiple states to obtain higher d.o.f. values. Reference [13] considers the MISO BCCM with only two states, PD and DP, each occurring for half of the time, and establishes its optimal sum s.d.o.f. to be $\frac{3}{2}$. Theorem 1 establishes the optimal sum s.d.o.f. of the PD (or DP) state alone to be 1. Thus, joint encoding over the PD and DP states together yields synergistic benefit of 50% in this case. Similarly, joint encoding across DN and ND states, when each occurs for half of the time, yields an optimal sum s.d.o.f. of 1 [15], [16], while only $\frac{1}{2}$ s.d.o.f. is achievable when the DN (or ND) state occurs alone, as established in Theorem 2. In contrast, there is no benefit to be had by joint encoding across PN and NP states each occurring for half of the time. The optimal sum s.d.o.f. with PN and NP states occurring together is 1 [15], [16], which is the same as the optimal sum s.d.o.f. of the PN (or NP) state alone, as stated in Theorem 1. Thus, our results help us determine if joint encoding is indeed useful for secrecy in an alternating CSIT scenario.

## IV. Proof of Theorem 1

To prove Theorem 1, we provide an achievable scheme for state PN, and prove a matching converse for state PD. Note that an alternative converse proof for just the PN state follows immediately from the fact that the sum d.o.f. of the MISO BC without any confidentiality constraints is also bounded by 1, as shown recently in [9].

### *A. Achievable Scheme for State* PN

Note that it is sufficient to show the achievability of only two points: $(d_1, d_2) = (1, 0)$ and $(d_1, d_2) = (0, 1)$. The achievability of these corner points follow in straightforward manner as follows: sending the message to user 1 by superimposing it with artificial noise in a direction orthogonal to user 1's channel to achieve the pair $(1, 0)$; and sending the message to user 2 in a direction orthogonal to user 1's channel to achieve the pair $(0, 1)$. This completes the proof of the achievability of the region in (5).

### *B. Converse for State* PD

We create a virtual receiver with output $\tilde{Z}^n$ with a channel that is statistically equivalent to user 2. The channel output at this virtual receiver at time $t$ is given by

$$\tilde{Z}(t) = \tilde{\mathbf{H}}_2(t)\mathbf{X}(t) + \tilde{N}_2(t), \tag{7}$$

where $\tilde{\mathbf{H}}_2$ and $\tilde{N}_2$ are i.i.d. as $\mathbf{H}_2$ and $N_2$, respectively. Then, the local statistical equivalence property, [13, eqn. (24)] implies that

$$h(Z(t)|Z^{t-1}, W_2, \Omega) = h(\tilde{Z}(t)|Z^{t-1}, W_2, \Omega), \tag{8}$$

where $\Omega$ is the set of all channel coefficients upto and including time $n$. Thus, conditioned on past outputs, the differential entropy of the output of a receiver that supplies delayed CSIT is the same as that of another virtual receiver with an identically distributed but independent channel. Since $\Omega$ is known at both receivers, it appears in the conditioning of every entropy and mutual information term below; however, for the sake of notational simplicity we will not mention it. Let us now bound the rate of user 1:

$$\begin{aligned}
nR_1 \leq& I(W_1; Y^n) + o(n) && (9)\\
\leq& I(W_1; Y^n|W_2) + o(n) && (10)\\
\leq& I(W_1; Y^n, Z^n|W_2) + o(n) && (11)\\
=& I(W_1; Y^n|Z^n, W_2) + no(\log P) + o(n) && (12)\\
\leq& I(W_1; Y^n, \tilde{Z}^n|Z^n, W_2) + no(\log P) + o(n) && (13)\\
=& h(Y^n, \tilde{Z}^n|Z^n, W_2) - h(Y^n, \tilde{Z}^n|Z^n, W_1, W_2)\\
&+ no(\log P) + o(n) && (14)\\
\leq& h(Y^n, \tilde{Z}^n|Z^n, W_2) + no(\log P) + o(n) && (15)\\
=& h(\tilde{Z}^n|Z^n, W_2) + h(Y^n|Z^n, \tilde{Z}^n, W_2)\\
&+ no(\log P) + o(n) && (16)\\
\leq& h(\tilde{Z}^n|Z^n, W_2) + no(\log P) + o(n) && (17)\\
\leq& \sum_{t=1}^{n} h(\tilde{Z}(t)|Z^n, W_2) + no(\log P) + o(n) && (18)
\end{aligned}$$

$$\leq \sum_{t=1}^{n} h(\tilde{Z}(t)|Z^{t-1}, W_2) + no(\log P) + o(n) \quad (19)$$

$$= \sum_{t=1}^{n} h(Z(t)|Z^{t-1}, W_2) + no(\log P) + o(n) \quad (20)$$

$$= h(Z^n|W_2) + no(\log P) + o(n), \quad (21)$$

where (12) follows since,

$$\begin{aligned} I(W_1; Z^n|W_2) \leq & I(W_1; Z^n, W_2) && (22)\\ = & I(W_1; Z^n) + I(W_1; W_2|Z^n) && (23)\\ \leq & no(\log P) + H(W_2|Z^n) && (24)\\ \leq & no(\log P) + o(n) && (25) \end{aligned}$$

where (24) and (25) follow from the confidentiality and decodability requirements, respectively. Further, (17) follows due to the fact that given $(Z^n, \tilde{Z}^n)$ and $\Omega$, it is possible to reconstruct $\mathbf{X}^n$ and hence $Y^n$ to within noise distortion, and (20) follows from (8).

For the second user, we have,

$$\begin{aligned} nR_2 \leq & I(W_2; Z^n) + o(n) && (26)\\ = & h(Z^n) - h(Z^n|W_2) + o(n) && (27)\\ \leq & n \log P - h(Z^n|W_2) + o(n). && (28) \end{aligned}$$

Adding (21) and (28), we have,

$$n(R_1 + R_2) \leq n \log P + no(\log P) + o(n). \quad (29)$$

Dividing by $n$ and letting $n \to \infty$,

$$R_1 + R_2 \leq \log P + o(\log P). \quad (30)$$

Now dividing by $\log P$ and letting $P \to \infty$,

$$d_1 + d_2 \leq 1. \quad (31)$$

This completes the proof of the converse for Theorem 1.

## V. Proof of Theorem 2

### A. Achievable Scheme

To prove the achievability of the s.d.o.f. region in (6), it suffices to achieve only the two points: $(d_1, d_2) = \left(\frac{1}{2}, 0\right)$ and $(d_1, d_2) = \left(0, \frac{1}{2}\right)$. The entire region can be obtained by time-sharing. A scheme to achieve the point $(d_1, d_2) = \left(\frac{1}{2}, 0\right)$ was presented in [6]. We present it briefly here for completeness.

*1) Scheme achieving* $(d_1, d_2) = \left(\frac{1}{2}, 0\right)$*:* We wish to send 1 symbol $u$ securely to the first user in 2 time slots. This can be done as follows:

At time $t = 1$, the transmitter does not have any channel knowledge. It sends,

$$\mathbf{X}(1) = [q_1 \quad q_2]^T, \quad (32)$$

where $q_1$ and $q_2$ denote independent artificial noise symbols distributed as $\mathcal{CN}(0, P)$. Both receivers receive linear combinations of the two symbols $q_1$ and $q_2$. The outputs are:

$$Y(1) = h_{11}(1)q_1 + h_{12}(1)q_2 \triangleq L(q_1, q_2) \quad (33)$$

$$Z(1) = h_{21}(1)q_1 + h_{22}(1)q_2 \triangleq G(q_1, q_2) \quad (34)$$

where we drop the Gaussian noise at high SNR. Due to delayed CSIT from receiver 1, the transmitter can reconstruct $L(q_1, q_2)$ in the next time slot and use it for transmission.

At time $t = 2$, the transmitter sends,

$$\mathbf{X}(2) = [u \quad L(q_1, q_2)]^T. \quad (35)$$

The received signals are:

$$\begin{aligned} Y(2) = & h_{11}(2)u + h_{12}(2)L(q_1, q_2) && (36)\\ Z(2) = & h_{21}(2)u + h_{22}(2)L(q_1, q_2). && (37) \end{aligned}$$

Since the receivers have full channel knowledge, receiver 1 can recover $u$ by eliminating $L(q_1, q_2)$ from $Y(1)$ and $Y(2)$. Therefore, $I(u; Y(1), Y(2)) = \log P + o(\log P)$. The information leakage to the second user is bounded by $o(\log P)$, see [6]. Thus, $(d_1, d_2) = (\frac{1}{2}, 0)$ is achievable in this scheme.

*2) Scheme achieving* $(d_1, d_2) = \left(0, \frac{1}{2}\right)$*:* In this scheme, we wish to send 1 symbol $u$ securely to the second user in 2 time slots. This can be done as follows:

At time $t = 1$, the transmitter does not have any channel knowledge. It sends:

$$\mathbf{X}(1) = [u \quad q]^T, \quad (38)$$

where $q$ denotes an independent artificial noise symbol distributed as $\mathcal{CN}(0, P)$. Both receivers receive linear combinations of the two symbols $u$ and $q$. The receivers' outputs are:

$$Y(1) = h_{11}(1)u + h_{12}(1)q \triangleq L(u, q) \quad (39)$$

$$Z(1) = h_{21}(1)u + h_{22}(1)q \triangleq G(u, q). \quad (40)$$

Due to delayed CSIT from receiver 1, the transmitter can reconstruct $L(u, q)$ and use it for transmission in the next slot.

At time $t = 2$, the transmitter sends:

$$\mathbf{X}(2) = [L(u, q) \quad 0]^T. \quad (41)$$

The received signals are:

$$\begin{aligned} Y(2) = & h_{11}(2)L(u, q) && (42)\\ Z(2) = & h_{21}(2)L(u, q). && (43) \end{aligned}$$

Since the receivers have full channel knowledge, receiver 2 can recover $u$ by eliminating $q$ from $L(u, q)$ and $G(u, q)$. On the other hand, the information leakage to the first user is

$$\begin{aligned} I(u; Y(1), Y(2)|\Omega) = & I(u; L(u, q)|\Omega) && (44)\\ = & h(L(u, q)|\Omega) - h(L(u, q)|u, \Omega) && (45)\\ \leq & \log P - \log P + o(\log P) && (46)\\ = & o(\log P). && (47) \end{aligned}$$

By considering the wiretap channel from $u$ to $[Z(1), Z(2)]$ and $[Y(1), Y(2)]$, with $[Y(1), Y(2)]$ being the eavesdropper output, we have the following effective rate:

$$R_2 = \frac{1}{2} \log P + o(\log P). \quad (48)$$

Thus, $(d_1, d_2) = (0, \frac{1}{2})$ is achievable in this scheme. This completes the proof of achievability for Theorem 2.

## B. Converse

We first create a virtual receiver with output $\tilde{Y}^n$ with a statistically equivalent channel as user 1, where $\tilde{Y}(t)$ is

$$\tilde{Y}(t) = \tilde{\mathbf{H}}_1(t)\mathbf{X}(t) + \tilde{N}_1(t), \tag{49}$$

where $\tilde{\mathbf{H}}_1$ and $\tilde{N}_1$ are i.i.d. as $\mathbf{H}_1$ and $N_1$, respectively. Then, the local statistical equivalence property [13] implies that

$$h(Y(t)|Y^{t-1}, W_1, \Omega) = h(\tilde{Y}(t)|Y^{t-1}, W_1, \Omega), \tag{50}$$

where $\Omega$ is the set of all channel coefficients upto and including time $n$. Similar to the proof of [13, Lemma 1], using (50), it can be readily shown that,

$$2h(Y^n|W_1, \Omega) \geq h(Z^n|W_1, \Omega) + o(\log P). \tag{51}$$

Again, for notational simplicity, we drop the $\Omega$ in the conditioning below. For the first user, we have,

$$\begin{aligned}
nR_1 \leq& I(W_1; Y^n) - I(W_1; Z^n) + o(n) + no(\log P) && (52)\\
=& h(Y^n) - h(Y^n|W_1) - h(Z^n) + h(Z^n|W_1) \\
&+ o(n) + no(\log P) && (53)\\
\leq& h(Y^n) - \frac{1}{2}h(Z^n|W_1) - h(Z^n) + h(Z^n|W_1) \\
&+ o(n) + no(\log P) && (54)\\
=& h(Y^n) + \frac{1}{2}h(Z^n|W_1) - h(Z^n) + o(n) \\
&+ no(\log P) && (55)\\
\leq& h(Y^n) + \frac{1}{2}h(Z^n) - h(Z^n) + o(n) + no(\log P) && (56)\\
=& h(Y^n) - \frac{1}{2}h(Z^n) + o(n) + no(\log P), && (57)
\end{aligned}$$

where (54) follows from (51). For the second user, we have,

$$\begin{aligned}
nR_2 \leq& I(W_2; Z^n) - I(W_2; Y^n) + o(n) + no(\log P) && (58)\\
=& h(Z^n) - h(Y^n) + (h(Y^n|W_2) - h(Z^n|W_2)) \\
&+ o(n) + no(\log P). && (59)
\end{aligned}$$

Adding (57) and (59), we obtain,

$$\begin{aligned}
n(R_1 + R_2) \leq& \frac{1}{2}h(Z^n) + (h(Y^n|W_2) - h(Z^n|W_2)) \\
&+ o(n) + no(\log P) && (60)\\
\leq& \frac{n}{2}\log P + (h(Y^n|W_2) - h(Z^n|W_2)) \\
&+ o(n) + no(\log P). && (61)
\end{aligned}$$

Thus, in order to obtain $d_1 + d_2 \leq 1/2$, it suffices to show that $(h(Y^n|W_2) - h(Z^n|W_2)) \leq no(\log P)$, where the transmitter has delayed CSIT from user 1 and no CSIT from user 2. To this end, we directly invoke a recent result in [9, eqns. (39)-(66)], which showed that the maximum of $h(Y^n|W_2) - h(Z^n|W_2)$ is less than $no(\log P)$, under the assumption of perfect CSIT from user 1 and no CSIT from user 2. Hence, the same upper bound on the maximum value also holds under a weaker assumption of delayed CSIT from user 1. Thus, using

$$h(Y^n|W_2) - h(Z^n|W_2) \leq no(\log P), \tag{62}$$

and substituting in (61), we have,

$$n(R_1 + R_2) \leq \frac{n}{2}\log P + o(n) + no(\log P). \tag{63}$$

Dividing by $n$ and letting $n \to \infty$,

$$R_1 + R_2 \leq \frac{1}{2}\log P + o(\log P). \tag{64}$$

Dividing by $\log P$ and letting $P \to \infty$,

$$d_1 + d_2 \leq \frac{1}{2}. \tag{65}$$

This completes the proof of the converse for Theorem 2.

# VI. Conclusions

We considered the two-user MISO BCCM with heterogeneous states PN, PD and DN. We established the s.d.o.f. regions of MISO BCCM in each of these heterogeneous states by providing achievable schemes as well as matching converses. The results highlight the impact of CSIT on the s.d.o.f. region, as well as aid in determining whether there are synergistic gains in coding across states in alternating CSIT scenarios.

# References


[1] R. Liu and H. V. Poor. Secrecy capacity region of a multiple-antenna Gaussian broadcast channel with confidential messages. *IEEE Trans. Inf. Theory*, 55(3):1235–1249, Mar. 2009.

[2] R. Liu, T. Liu, H. V. Poor, and S. Shamai. Multiple-input multiple-output Gaussian broadcast channels with confidential messages. *IEEE Trans. Inf. Theory*, 56(9):4215–4227, Sept. 2010.

[3] C. S. Vaze and M. K. Varanasi. The degrees of freedom regions of MIMO broadcast, interference, and cognitive radio channels with no CSIT. *IEEE Trans. Inf. Theory*, 58(8):5354–5374, Aug. 2012.

[4] M. A. Maddah-Ali and D. Tse. Completely stale transmitter channel state information is still useful. *IEEE Trans. Inf. Theory*, 58(7):4418–4431, Jul. 2012.

[5] C. S. Vaze and M. K. Varanasi. The degrees of freedom regions of two-user and certain three-user MIMO broadcast channels with delayed CSIT. Available at [arXiv:1101.0306].

[6] S. Yang, M. Kobayashi, P. Piantanida, and S. Shamai. Secrecy degrees of freedom of MIMO broadcast channels with delayed CSIT. *IEEE Trans. Inf. Theory*, 59(9):5244–5256, Sept. 2013.

[7] H. Maleki, S. A. Jafar, and S. Shamai. Retrospective interference alignment over interference networks. *IEEE Jour. of Sel. Topics in Signal Proc.*, 6(3):228–240, Jun. 2012.

[8] R. Tandon, M.-A. Maddah-Ali, A. Tulino, H.V. Poor, and S. Shamai. On fading broadcast channels with partial channel state information at the transmitter. In *IEEE ISWCS*, Aug. 2012.

[9] A. G. Davoodi and S. A. Jafar. Aligned image sets under channel uncertainty: Settling a conjecture by Lapidoth, Shamai and Wigger on the collapse of degrees of freedom under finite precision CSIT. Available at [arXiv:1403.1541].

[10] S. Amuru, R. Tandon, and S. Shamai. On the degrees-of-freedom of the 3-user MISO broadcast channel with hybrid CSIT. In *IEEE ISIT*, Jun. 2014.

[11] K. Mohanty and M. K. Varanasi. On the DoF region of the $K$-user MISO broadcast channel with hybrid CSIT. Available at [arXiv:1312.1309].

[12] S. Lashgari and A. S. Avestimehr. Blind wiretap channel with delayed CSIT. In *IEEE ISIT*, Jun. 2014.

[13] P. Mukherjee, R. Tandon, and S. Ulukus. MISO broadcast channels with confidential messages and alternating CSIT. In *IEEE ISIT*, Jun. 2014.

[14] R. Tandon, S. A. Jafar, S. Shamai, and H. V. Poor. On the synergistic benefits of alternating CSIT for the MISO broadcast channel. *IEEE Trans. Inf. Theory*, 59(7):4106–4128, Jul. 2013.

[15] P. Mukherjee, R. Tandon, and S. Ulukus. Secrecy for MISO broadcast channels via alternating CSIT. In *IEEE ICC*, Jun. 2015.

[16] P. Mukherjee, R. Tandon, and S. Ulukus. Secure degrees of freedom region of the two-user MISO broadcast channel with alternating CSIT. *Submitted to IEEE Trans. Inf. Theory*. Available at [arXiv:1502.02647].