Title
Robust Optimality of TIN under Secrecy Constraints

Authors
Chan, Yao-chia
Geng, Chunhua
Jafar, Syed A

Publication Date
2019-10-27

Robust Optimality of TIN under Secrecy Constraints

Yao-Chia Chan[†], Chunhua Geng[‡], and Syed A. Jafar[†]
[†] Center for Pervasive Communications and Computing (CPCC)
University of California Irvine, Irvine, CA 92697
Email: {yaochic, syed}@uci.edu
[‡] Nokia Bell Labs, Murray Hill, NJ 07974
Email: chunhua.geng@nokia-bell-labs.com

Abstract

A parameter regime is identified where the simple scheme of treating interference as Gaussian noise (TIN), with power control and jamming, is optimal for the secure generalized degrees of freedom (GDoF) region of Gaussian broadcast networks under the robust assumption of finite-precision channel state information at the transmitter (CSIT). The network consists of one transmitter equipped with K antennas, and K single-antenna receivers. The results are generalized to groupcast (equivalently, compound broadcast) settings where each message is desired by a disjoint group of receivers. Noting that messages are independently encoded in the GDoF-optimal scheme, the result for the broadcast channel is extended to its counterpart Gaussian interference channel under finite precision CSIT. Evidently, both secrecy constraints and finite precision CSIT limit the benefits of more sophisticated schemes, leading to optimality of simpler schemes for larger parameter regimes. Aligned Image bounds are the key to the proof of optimality for these larger parameter regimes under finite precision CSIT.

C. Geng was with UC Irvine when he finished his contribution to this work.

1 Introduction

Generalized degrees of freedom (GDoF) studies [1–5] have emerged as a valuable means to gain insights into the fundamental limits of wireless networks. Of particular interest are the serendipitous parameter regimes where simple schemes turn out to be optimal. While such regimes exist even under the idealized assumption of perfect channel state information at the transmitter(s) (CSIT) [6–8], recent works have shown that more conservative models that limit CSIT to finite precision may yield even larger parameter regimes where simple schemes are optimal [9]. This is especially important because finite precision CSIT models are closer to practice.

Robustness is especially important for communication under *security* constraints. While there is an abundance of literature on information theoretic secrecy [10–33], robustness issues, especially for larger networks, remain relatively unexplored. Fragile schemes are susceptible to catastrophic failures due to small deviations from their idealized assumptions. Such deviations are unavoidable in practice. In the absence of security constraints, a failed communication attempt may prompt a more conservative re-transmission. Failure in a secure communication setting on the other hand, may also lead to a loss of secrecy which is irreversible. Therefore, it is especially important to avoid the idealized assumption of perfect CSIT when studying secure communication [34–36].

Until recently, GDoF characterizations for finite precision CSIT models were intractable as the bounds produced by various classical techniques (Csiszar-sum lemma [37], extremal inequalities [38], compound channel bounds [39]) fell short even in very simple settings, e.g., the two user MISO broadcast channel (BC) as exemplified by the Lapidoth-Shamai-Wigger conjecture [37]. This changed with the emergence of Aligned Image (AI) bounds in [40]. These are combinatorial bounds based on counting the number of codewords that can be aligned at one receiver while remaining resolvable at another receiver. The AI bounds were originally introduced in [40] to settle the Lapidoth-Shamai-Wigger conjecture, and have been generalized significantly in subsequent works [41]. Indeed, AI bounds have been used successfully to find robust GDoF-optimal schemes for a variety of settings [42–51].

Motivated by these observations, in this work we initiate[1] the study of GDoF of K user MISO BC under secrecy and finite precision CSIT constraints. The contributions of this work are as follows. We identify a parameter regime where the simple scheme of treating interference as Gaussian noise, along with power control and jamming, is optimal for the secure GDoF of the K user MISO BC under the robust assumption of finite precision CSIT. Remarkably, no such parameter regime is known for the K user MISO BC if either the secrecy constraint, or the finite-precision CSIT constraint, or both of those constraints are relaxed. To the best of our knowledge, this is the first set of secure GDoF results under finite-precision CSIT for the K user MISO BC. The results are generalized to groupcast (equivalently, compound broadcast) settings where each message is desired by a disjoint group of receivers. Noting that messages are independently encoded in the GDoF-optimal scheme, the result for the broadcast channel is extended to its counterpart Gaussian interference channel under finite precision CSIT. Here also, the optimality of TIN is shown for a parameter regime that is in general strictly larger than the corresponding regimes established in prior work without security [6] or finite-precision CSIT [33] constraints. Remarkably, it turns out that the AI bounds combine quite naturally with the mutual information bounds that are

[1] As noted, there is prior work on GDoF under finite precision CSIT but without secrecy constraints (e.g., [42–50]), on GDoF with secrecy but under perfect CSIT (e.g., [29–33]), and on secure DoF with limited CSIT (e.g., [34–36]), yet *Generalized* DoF with *secrecy* and *finite precision* CSIT, especially for arbitrarily large networks, remain almost entirely unexplored.

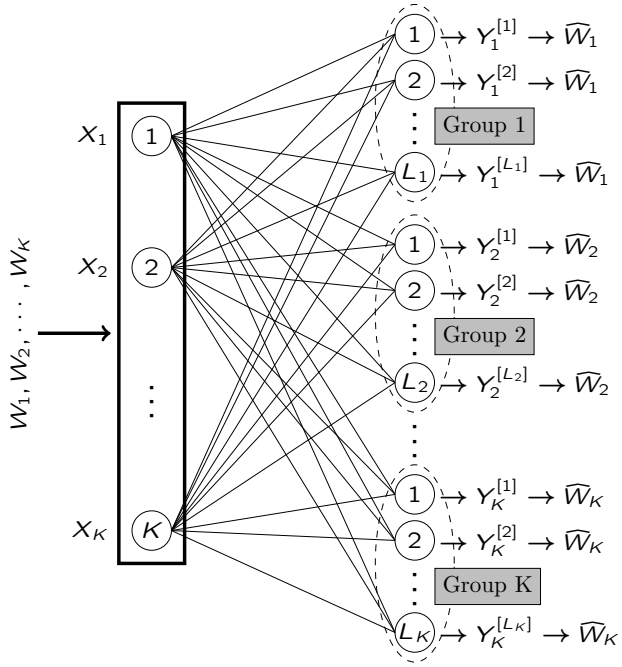


Figure 1: *Broadcast network with groupcast messages.*

introduced by secrecy constraints, producing tight converse bounds for the GDoF characterizations in this paper. Thus, the overarching take-home messages from this work are two-fold – (i) that the combination of secrecy constraints and finite-precision CSIT constraints creates new parameter regimes where relatively simple and robust schemes are GDoF optimal, and (ii) that AI bounds are the key to identifying these new parameter regimes.

The paper is organized as follows. In Section 2 we define the channel model for the groupcast/unicast setting and introduce other relevant definitions. The results are presented in Section 3. Section 4 follows with examples that illustrate the results. The proofs appear in Section 5. Finally, we present the conclusion in Section 6.

Notations: For real number x and positive integers Y, Z, with $Y \leq Z$, define $(x)^+ \triangleq \max(0, x)$, $[Y : Z] \triangleq \{Y, Y+1, \cdots, Z\}$ and $[Y] \triangleq [1 : Y]$. For a set S, $|S|$ denotes its cardinality. For two functions $f(x)$ and $g(x)$, denote $f(x) = o(g(x))$ if $\lim_{x\to\infty} f(x)/g(x) = 0$. All logarithms are to the base 2.

2 Channel Model and Preliminaries

We consider a Gaussian broadcast network depicted in Fig. 1, which consists of one transmitter with K antennas and K groups of users. Group i contains L_i users, each of which has one receiving antenna. The independent messages $\{W_j : j \in [K]\}$ are *jointly* encoded into codewords $\{X_i : i \in [K]\}$, where $X_i = \{X_i(t) : t \in [n]\}$ is a codeword spanning n channel uses. The message W_j is desired by all the users in Group j. When there is more than one user for a message, we refer to this setting as Gaussian broadcast channel with message *groupcast* (GBC-groupcast). In the special case where each group contains only one user (i.e., $L_i = 1, \forall i \in [K]$), the channel is referred to as Gaussian broadcast channel with message *unicast* (GBC-unicast).

For the purpose of robust GDoF studies, for all $k \in [K]$, the received signals are described as follows.

$$Y_k^{[l_k]}(t) = \sum_{i=1}^{K} \bar{P}^{\alpha_{ki}^{[l_k]}} G_{ki}^{[l_k]}(t) X_i(t) + Z_k^{[l_k]}(t). \tag{1}$$

All $X_i(t), Y_k^{[l_k]}(t), Z_k^{[l_k]}(t), G_{ki}^{[l_k]}(t) \in \mathbb{C}$. During the t-th channel use, $X_i(t)$ is the channel input at transmitting antenna i subject to a unit average power constraint ($\mathbb{E}[|X_i(t)|^2] \leq 1$), $Y_k^{[l_k]}(t)$ is the channel output at User l_k in Group k, and $Z_k^{[l_k]}(t)$ is the zero-mean unit-variance complex additive white Gaussian noise (AWGN) at the same user. We define $\bar{P} = \sqrt{P}$, where $P > 1$ is a nominal parameter that approaches infinity in the GDoF limit. The channel strength parameter $\alpha_{ki}^{[l_k]} \geq 0$ represents the strength of the link between the transmitting antenna i and the l_k-th receiver in Group k, and is denoted as α_{ki} when $L_k = 1$. $G_{ki}^{[l_k]}(t) \in \mathcal{G}$ are the channel coefficient values, which are assumed to be known perfectly to the receivers, and known only up to finite precision to the transmitters. The set of channel coefficient random variables $\mathcal{G}$ is defined in Section 2.1.

A secure rate tuple $(R_1, R_2, ..., R_K)$ is achievable if, for any $\epsilon > 0$, there exist n-length codes such that (i) the size of each message set $|W_j| \geq 2^{nR_j}$; (ii) the decoding error probabilities at all users are no larger than ϵ; and (iii) the following secrecy constraint is satisfied,

$$H(W_{-i}^K | Y_i^{[l_i],n}, \mathcal{G}) \geq H(W_{-i}^K) - n\epsilon \quad \forall i \in [K], \tag{2}$$

where $W_{-i}^K \triangleq \{W_k : \forall k \in [K] \backslash \{i\}\}$, $Y_i^{[l_i],n} = \{Y_i^{[l_i]}(t) | t \in [n]\}$, and $\mathcal{G}$ is the set of channel coefficients defined in Section 2.1. The secure channel capacity region $\mathcal{C}$ is the closure of the set of all achievable secure rate tuples. The secure GDoF region $\mathcal{D}$ is defined as

$$\mathcal{D} \triangleq \Big\{(d_1, d_2, ..., d_K) : d_i = \lim_{P\to\infty} \frac{R_i}{\log P},\ \forall i \in [K], (R_1, R_2, ..., R_K) \in \mathcal{C}\Big\}. \tag{3}$$

The sum GDoF value d_Σ and the symmetric GDoF value d_{sym} are defined respectively as

$$d_\Sigma \triangleq \max_{(d_1, d_2, \cdots, d_K) \in \mathcal{D}} \sum_{i=1}^{K} d_i, \tag{4}$$

and

$$d_{sym} \triangleq \max_{\substack{(d_1, d_2, \cdots, d_K) \in \mathcal{D} \\ d_i = d, \forall i \in [K]}} d. \tag{5}$$

2.1 Finite precision CSIT

In the setting of finite precision CSIT, we assume that the transmitter is aware of the values of the channel strength parameters $\alpha_{ki}^{[l_k]}$, but the channel coefficients $G_{ki}^{[l_k]}(t)$ are known to the transmitter only up to finite precision. Specifically, the transmitter knows only the joint probability density function of the channel coefficients $\mathcal{G} \triangleq \{G_{R,ki}^{[l_k]}(t), G_{I,ki}^{[l_k]}(t) : \ t \in [n], l_k \in [L_k], i, k \in [K]\}$. The joint density of $\mathcal{G}$ is assumed to follow the "bounded density assumption" [40, 42, 43], i.e., there exists a positive finite constant f_{max}, such that, for any finite disjoint subsets of $\mathcal{G}$, say $\mathcal{G}_1$ and $\mathcal{G}_2$,

the density of $\mathcal{G}_1$ conditioned on $\mathcal{G}_2$ satisfies $f_{\mathcal{G}_1|\mathcal{G}_2}(\boldsymbol{g}_1|\boldsymbol{g}_2) \le f_{max}^{|\mathcal{G}_1|}$, where $\boldsymbol{g}_i$ is a realization of $\mathcal{G}_i$, $i = 1, 2$. The bounded density assumption eliminates the possibility that, given a set of channel coefficients, the values of some other channel coefficients can be precisely deduced. Furthermore, to avoid degenerate scenarios, the magnitudes of channel coefficient values are also bounded away from zero and infinity, i.e., there exists a finite constant $\Delta > 1$ such that $1/\Delta \le |G_{ki}^{[l_k]}(t)| \le \Delta$ for all channel coefficients.

2.2 Definitions

We will need several definitions. Let us start with the polyhedral TIN region, which is a GDoF region originally defined in [6] and subsequently shown in [33] to be securely achievable by the scheme of TIN, together with power control and cooperative jamming. See Section II-C for details.

Definition 2.1 (Polyhedral TIN Region)**.** *For a set of channel strength parameters $\boldsymbol{\alpha} = \{\alpha_{ij} : i, j \in [K]\}$, the polyhedral TIN region associated with a permutation σ, denoted as $\mathcal{P}_\sigma(\boldsymbol{\alpha})$, is a collection of the tuples $(d_1, d_2, \cdots, d_K)$ satisfying*

$$0 \le d_i \le \alpha_{i\sigma(i)} \qquad \forall i \in [K], \tag{6}$$

$$\sum_{j=1}^{m} d_{i_j} \le \sum_{j=1}^{m} \Big(\alpha_{i_j\sigma(i_j)} - \alpha_{i_{j-1}\sigma(i_j)}\Big) \forall (i_1, i_2, \cdots, i_m) \in \Pi_m, \forall m \in [2 : K], \tag{7}$$

where Π_m is the set of all permutation of m distinct indices from $[K]$, and modulo-m arithmetic is implicitly used on the user indices, e.g., $i_m = i_0$. $\sigma = (\sigma(1), \sigma(2), \cdots, \sigma(K))$ represents a permutation of the tuple $\sigma_0 \triangleq (1, 2, \cdots, K)$.

The permutation operator σ is needed because, while the polyhedral TIN region was originally defined for the interference channel where the association between messages and transmit antennas is fixed, in the broadcast setting the TIN scheme could choose any mapping of transmit antennas to messages. In the following $\mathcal{P}_\sigma(\boldsymbol{\alpha})$ is abbreviated as $\mathcal{P}_\sigma$ when there is no ambiguity in the channel strength parameters.

Definition 2.2 (CTIN Regime)**.** *The CTIN regime, denoted as $\mathcal{A}_{CTIN}$, is the set of channel strength parameters $\{\alpha_{ij}^{[l_i]} : l_i \in [L_i], i, j \in [K]\}$ satisfying the following conditions:*

$$\alpha_{ii}^{[l_i]} \ge \max_{j:j\neq i} \{\alpha_{ij}^{[l_i]} + \alpha_{ji}^{[l_j]}\} \qquad \forall i \in [K], \tag{8}$$

$$\alpha_{ii}^{[l_i]} \ge \max_{j,k:j,k\neq i,j\neq k} \{\alpha_{ik}^{[l_i]} + \alpha_{ji}^{[l_j]} - \alpha_{jk}^{[l_j]}\} \qquad \forall i \in [K]. \tag{9}$$

The CTIN regime is named for the convexity of the GDoF region achievable by TIN when the channel is in this regime [52], and is recently identified as a regime where TIN is GDoF optimal without the secrecy constraint under finite precision CSIT [9]. In fact, it can be further argued that the GDoF region in the CTIN regime remains optimal even if the secrecy constraint is imposed; i.e., secrecy incurs no GDoF penalty. See Lemma 2.2 for the details of this observation.

Definition 2.3 (SLS-σ)**.** *The SLS-σ regime, denoted as $\mathcal{A}_{SLS,\sigma}$, is the set of channel strength parameters $\{\alpha_{ij}^{[l_i]} : l_i \in [L_i], i, j \in [K]\}$ with the message ordering σ satisfying the following conditions:*

$$\alpha_{i\sigma(i)}^{[l_i]} \ge \alpha_{k\sigma(i)}^{[l_k]} \qquad \forall l_i \in [L_i], l_k \in [L_k], k, i \in [K], \tag{10}$$

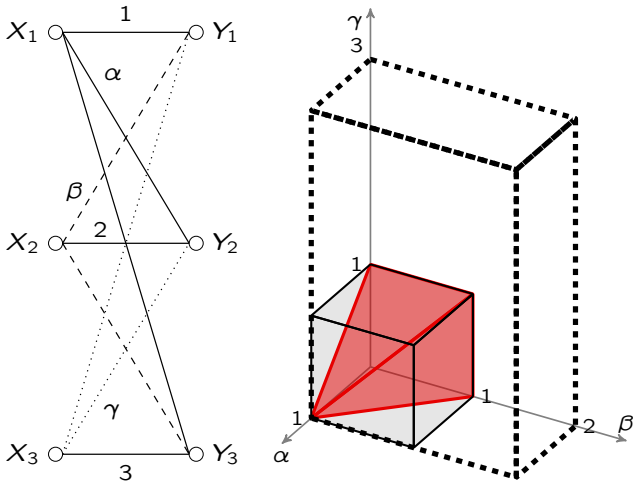


Figure 2: *(a) A network with variable channel strength parameters* (α, β, γ)*, and (b) the regions for the channel strength parameters in which the channel is respectively in the CTIN regime (red polyhedron), in the SLS-*σ_0 *regime (gray-shaded cube), and in the SLS*$^+$ *regime (dashed box).*

$$\alpha_{i\sigma(i)}^{[l_i]} \geq \alpha_{ik}^{[l_i]} \qquad \forall l_i \in [L_i], k, i \in [K], \tag{11}$$

$$\alpha_{i\sigma(i)}^{[l_i]} \geq \max_{\substack{k,j,l_j:\ j\neq i,\\ k\neq\sigma(i), l_j\in[L_j]}} \left\{\alpha_{j\sigma(i)}^{[l_j]} + \alpha_{ik}^{[l_i]} - \alpha_{jk}^{[l_j]}\right\} \qquad \forall l_i \in [L_i], i \in [K]. \tag{12}$$

The significance of the SLS-σ regime is that it was shown in [44] that when the channel is in this regime, then a *simple layered superposition (SLS)* scheme is GDoF optimal for GBC-unicast without secrecy constraints, provided $K \leq 3$. Although the result of [44] is limited to $K \leq 3$ and to the unicast setting, note that the SLS-σ regime is defined in general for all K, σ and the groupcast setting.

Definition 2.4 (SLS$^+$ Regime)**.** *The SLS*$^+$ *regime, denoted as* $\mathcal{A}_{SLS^+}$*, is the set of channel strength parameters* $\{\alpha_{ij}^{[l_i]} : l_i \in [L_i], i, j \in [K]\}$ *satisfying the following conditions:*

$$\alpha_{ii}^{[l_i]} \geq \alpha_{ki}^{[l_k]} \qquad \forall l_i \in [L_i], l_k \in [L_k], k, i \in [K], \tag{13}$$

$$\alpha_{ii}^{[l_i]} \geq \max_{\substack{k,j,l_j:\\ k,j\neq i, l_j\in[L_j]}} \left\{\alpha_{ji}^{[l_j]} + \alpha_{ik}^{[l_i]} - \alpha_{jk}^{[l_j]}\right\} \qquad \forall l_i \in [L_i], i \in [K]. \tag{14}$$

Note that the SLS$^+$ regime does not use the permutation operators σ. This is because this regime will be used only for the interference channel setting, where the assignment of transmitters to messages is already fixed by default as σ_0, i.e., message W_i is sent from transmit antenna i. The SLS$^+$ regime has the same set of conditions as the SLS-σ_0 regime except for (11), so the SLS$^+$ regime contains the SLS-σ_0 regime. Moreover, the conditions in the CTIN regime imply those in the SLS-σ_0 regime. As a result, we have the inclusion $\mathcal{A}_{CTIN} \subset \mathcal{A}_{SLS,\sigma_0} \subset \mathcal{A}_{SLS^+}$.

To illustrate the progressive inclusion relationships, let us consider as an example the network in Fig. 2(a), where the values of the channel strength parameters are shown next to each link. Since our ability to visualize is limited to three dimensions, we allow three variables (α, β, γ)

among the channel strength parameters. Fig 2(b) identifies the regions where the channel strength parameters (α, β, γ) place the channel into each of the three parameter regimes. The dashed box is the region for the SLS$^+$ regime, the gray-shaded cube is the region for the SLS-σ_0 regime, and the red polyhedron is the region for the CTIN regime. Evidently, the dashed box contains the gray-shaded cube, and the cube includes the red polyhedron, thus visually demonstrating the progressive inclusion relationships among these three regimes.

2.3 Polyhedral TIN region under secrecy constraints

For a conventional GIC (without secrecy constraints), in the TIN scheme each transmitter encodes its own message with Gaussian signaling, and each receiver decodes its intended signal by treating the interference from other users as Gaussian noise. Suppose we require that each receiver must decode its message at a non-negative SINR (i.e., signal to interference and noise power ratio) value in dB scale. Such a scheme is called *the polyhedral TIN scheme*, and its achievable GDoF region is *the polyhedral TIN region* [6]. In [33], it has been shown that the polyhedral TIN region remains achievable under the secrecy constraint. The achievability under secrecy constraint is based on a scheme combining TIN and cooperative jamming. The scheme splits the transmitted signal from each transmitter into two parts: the first carries the desired message based on a Gaussian wiretap codebook, and the second is a random Gaussian jamming signal that helps reduce the information leakage at unintended users.[2] We point out that this achievable scheme only needs the knowledge of the channel strength parameters α_{ki} at the transmitters. Therefore, *the polyhedral TIN region is achievable under the secrecy constraint and finite precision CSIT.*

Since cooperation among transmitters cannot hurt, the polyhedral TIN GDoF region for an interference channel remains achievable in the corresponding broadcast channel obtained by allowing full cooperation among the transmit antennas. Later we will show that in certain parameter regimes, this independent encoding approach is in fact optimal from the GDoF perspective for the broadcast network under finite precision CSIT and secrecy constraints, i.e., joint encoding does not offer any advantage. Note that in a broadcast channel, even if the messages are mapped to separate transmit antennas, the mapping σ can be arbitrarily chosen, allowing the broadcast channel to mimic any of the $K!$ interference channels corresponding to different permutations σ. The following lemma follows trivially from this observation.

Lemma 2.1. *In a GBC-unicast setting, for all permutations σ, the polyhedral TIN region $\mathcal{P}_\sigma$ is achievable under the secrecy constraint (2) and finite precision CSIT.*

Let us formalize another useful observation in the following lemma.

Lemma 2.2. *For a GIC-unicast setting, if the channel is in the CTIN regime, then the secure GDoF region is equal to the polyhedral TIN region $\mathcal{P}_{\sigma_0}$ under finite-precision CSIT.*

Proof. Achievability of $\mathcal{P}_{\sigma_0}$ follows from the discussion preceding Lemma 2.1. The converse follows from the observation that Theorem 4.1 of [9] already shows that $\mathcal{P}_{\sigma_0}$ is the GDoF region in the CTIN regime under finite precision CSIT in the absence of secrecy constraints, and imposing the secrecy constraint cannot make the GDoF region any larger. □

[2] Given a target secure GDoF tuple, the power allocations for the two parts can be determined via the power control algorithms proposed in [52, 53].

3 Results

Our first result is the following theorem for GBC-unicast.

Theorem 3.1. *For a GBC-unicast setting under finite precision CSIT, if the channel is in the SLS-σ regime for some message ordering σ, then the secure GDoF region is equal to the polyhedral TIN region $\mathcal{P}_\sigma$.*

The proof of Theorem 3.1 is relegated to Section 5.1. The results in Theorem 3.1 can be extended to the case of Gaussian interference channel with message unicast (GIC-unicast) by recognizing that messages therein are separately encoded with the ordering $\sigma = \sigma_0$.

Corollary 3.1. *For a GIC-unicast setting under finite precision CSIT, if the channel is in the SLS$^+$ regime,*[3] *then the secure GDoF region is equal to the polyhedral TIN region $\mathcal{P}_{\sigma_0}$.*

Remark 3.1. *Note that Corollary 3.1 identifies a parameter regime (the SLS$^+$ regime) that is in general strictly larger than the baseline CTIN regime identified in Lemma 2.2. As a result, Lemma 2.2 is recovered as strictly a special case of Corollary 3.1. See Fig. 2 for an illustration of these two regimes, and Example 4.3 in Section 4 for GDoF regions of channels in these two regimes.*

The next result establishes the sum secure GDoF value for GBC-unicast with $K = 2$ for *arbitrary* channel strengths under finite precision CSIT.

Theorem 3.2. *For GBC-unicast with $K = 2$, under finite precision CSIT, its sum secure GDoF value is*

$$d_\Sigma = \max_{k=1,2}(\alpha_{1k} - \alpha_{2k})^+ + \max_{k=1,2}(\alpha_{2k} - \alpha_{1k})^+. \tag{15}$$

The proof appears in Section 5.2.
Finally, we generalize the result of Theorem 3.1 to the groupcast setting.

Theorem 3.3. *For a GBC-groupcast setting under finite precision CSIT, if the channel is in the SLS-σ regime for some message ordering σ, then the secure GDoF region is equal to the polyhedral TIN region $\bar{\mathcal{P}}_\sigma = \mathcal{P}_\sigma(\bar{\boldsymbol{\alpha}})$ associated with the set of channel strengths $\bar{\boldsymbol{\alpha}} = \{\bar{\alpha}_{ij} : \ i, j \in [K]\}$, where*

$$\bar{\alpha}_{i\sigma(i)} = \min_{l_i \in [L_i]} \{\alpha_{i\sigma(i)}^{[l_i]}\} \qquad \forall i \in [K], \tag{16}$$

$$\bar{\alpha}_{i\sigma(i)} - \bar{\alpha}_{i\sigma(j)} = \min_{l_i \in [L_i]} \{\alpha_{i\sigma(i)}^{[l_i]} - \alpha_{i\sigma(j)}^{[l_i]}\} \qquad \forall i, j \in [K]. \tag{17}$$

The proof of Theorem 3.3 is relegated to Section 5.3. Note that $\{\bar{\alpha}_{ij}\}$ defined in (16) and (17) form a set of channel strengths in the SLS-σ regime for an equivalent GBC-unicast setting.[4] Such a GBC-unicast has the same secure GDoF region as the GBC-groupcast with $\{\alpha_{ij}^{[l_i]}\}$. Another

[3] Condition (11) is not required for GDoF optimality in a GIC-unicast. This is because in a GIC-unicast setting (or, equivalently, a K-user GIC) only the link from Transmitter i to Receiver i is able to carry the message W_i. In contrast, in the GBC-unicast setting of Theorem 3.1, condition (11) is needed for the bound (6) to hold in the converse proof.

[4] $\bar{\alpha}_{i\sigma(i)} \geq \max_{k:\ k\neq i}\{\bar{\alpha}_{i\sigma(k)}, \bar{\alpha}_{k\sigma(i)}\}$ is due to (10), (11). $\bar{\alpha}_{i\sigma(i)} \geq \max_{j,k:\ j\neq i, k\neq\sigma(i)}\{\bar{\alpha}_{j\sigma(i)} + \bar{\alpha}_{ik} - \bar{\alpha}_{jk}\}$ must hold because, from (12), we have $\min_{l_i\in[L_i]}\{\alpha_{i\sigma(i)}^{[l_i]} - \alpha_{ik}^{[l_i]}\} \geq \min_{l_j\in[L_j]}\{\alpha_{j\sigma(i)}^{[l_j]} - \alpha_{jk}^{[l_j]}\}$ for all $j \neq i, k \neq \sigma(i)$, and therefore $\bar{\alpha}_{i\sigma(i)} - \bar{\alpha}_{ik} \geq \bar{\alpha}_{j\sigma(i)} - \bar{\alpha}_{jk}$ by (17).

observation is that $\bar{\mathcal{P}}_\sigma$ is the intersection of the polyhedral TIN regions over all possible choices of users (one from each group). This can be seen by how $\bar{\boldsymbol{\alpha}}$ is applied to describe $\bar{\mathcal{P}}_\sigma$, or the argument of upperbounds for the GDoF region in Section 5.3.

The results of Theorem 3.3 can be extended to the case of GIC with message groupcast (GIC-groupcast) as well.

Corollary 3.2. *For a GIC-groupcast, if the channel is in the SLS$^+$ regime, then under finite precision CSIT, the secure GDoF region is equal to the polyhedral TIN region $\bar{\mathcal{P}}_{\sigma_0}$.*

Remark 3.2. *The TIN, power control and cooperative jamming scheme is robust against errors in the transmitters' knowledge of channel strengths provided that the transmitters' estimates of channel strengths are conservative. In other words, as long as the channel strengths for desired links are not overestimated and those for interfering links are not underestimated by the transmitter(s), the messages remain decodable and secure. Take a GIC-unicast setting as an example, with the transmitters' belief that the channel is in the SLS$^+$ regime. The transmission scheme based on TIN, power control and cooperative jamming achieves some GDoF tuple in $\mathcal{P}_{\sigma_0}$. Suppose, the desired channels are stronger and the cross-channels are weaker than what the transmitters believe. The scheme still works; i.e., it still achieves the same GDoF tuple, and the security of each message is preserved. This is because each receiver finds both its desired codeword and the accompanying jammer shifted upward in power, compared to what the transmitters expect; meanwhile it finds the other codewords shifted downward in power. As a result, the desired message remains decodable while the other messages remain secure.*

4 Examples

In this section, we illustrate the results presented in Section 3 with some examples.

Example 4.1 (Application of Theorem 3.2)**.** *Here we consider GBC-unicast with $K = 2$ users, i.e., a 2-user MISO Gaussian broadcast channel. We compare its GDoF under different CSIT assumptions and secrecy constraints. Fig. 3 depicts the symmetric GDoF of a 2-user MISO symmetric GBC (where $\alpha_{11} = \alpha_{22} = 1$ and $\alpha_{12} = \alpha_{21} = \alpha$). When perfect CSIT is available, the symmetric GDoF value with or without the secrecy constraint is shown with the dotted line, and is achievable via zero-forcing in either case [30, 54]. Under finite precision CSIT, the symmetric GDoF value without secrecy constraints is shown with the dashed line, and is achieved by interference enhancement, where each user decodes a common message and then its own private message after removing the former from the received signal [43]. The symmetric secure GDoF value under finite precision CSIT is given by Theorem 3.2 and is shown with the solid line . It is evident that both the CSIT degradation and the secrecy requirement incur a penalty on the symmetric GDoF value: the former eliminates the gains of zero-forcing, and the latter prevents the use of common messages.*

Example 4.2 (Application of Corollary 3.1)**.** *Consider a 2-user symmetric GIC under finite precision CSIT (where $\alpha_{11} = \alpha_{22} = 1$ and $\alpha_{12} = \alpha_{21} = \alpha$). This corresponds to a GIC-unicast setting with $K = 2$ users. According to Corollary 3.1, when $0 \leq \alpha \leq 1$, the symmetric secure GDoF value[5] is $1 - \alpha$. First, compare with the case of symmetric 2-user GBC under finite precision CSIT (the*

[5]We note that when $\alpha \geq 2$, the symmetric secure GDoF value is 0 according to [55]. Under finite precision CSIT, the symmetric secure GDoF value remains open when $1 < \alpha < 2$.

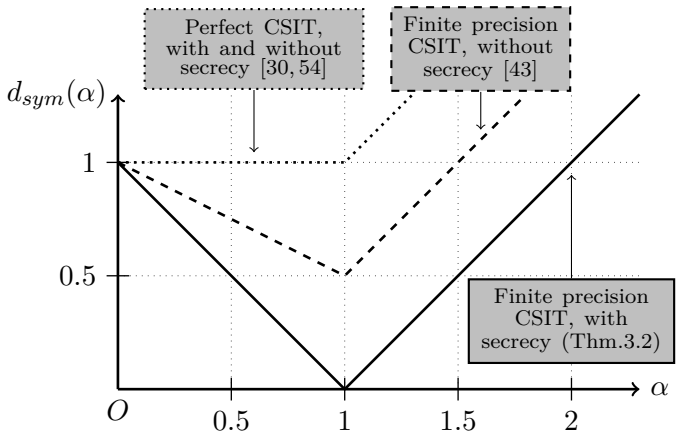


Figure 3: *Symmetric GDoF value for 2-user symmetric Gaussian BC.*

solid line in Fig. 3). We notice that in the same regime the full cooperation between the transmitting antennas does not provide any GDoF benefit. Next, compare with the case of symmetric 2-user GIC under perfect CSIT. We note that with perfect CSIT, (i) when $\alpha \leq \frac{2}{3}$, the symmetric secure GDoF value is equal to $1-\alpha$, and (ii) when $\frac{2}{3} < \alpha < 1$, the symmetric secure GDoF is strictly larger than $1-\alpha$, as shown in [55, 56]. This shows that the scheme of TIN with cooperative jamming is optimal for a broader channel parameter regime in the case of finite precision CSIT.

Example 4.3 (Illustration of Remark 3.1)**.** *Consider the three channels depicted in Figure 4, where all $K = 3$ messages are assumed to be unicast, and they are either jointly encoded (GBC) or independently encoded (GIC). First for the channel in Figure 4(a), it is in the CTIN regime; therefore it is in the SLS-σ_0 regime as well. According to Theorem 3.1, the secure GDoF region for the GBC (the red region) is described as*

$$\left\{ (d_1,d_2,d_3) \in \mathbb{R}_+^3 \;\middle|\; \begin{array}{cc} d_1 \leq 1, & d_1+d_2 \leq 2, \\ d_2 \leq 2, & d_1+d_3 \leq 3, \\ d_3 \leq 3, & d_2+d_3 \leq 3, \\ & d_1+d_2+d_3 \leq 4 \end{array} \right\} \tag{18}$$

. When the secrecy constraint is removed, the GDoF region without secrecy constraint (the blue region) is described as [44, Theorem 1]

$$\left\{ (d_1,d_2,d_3) \in \mathbb{R}_+^3 \;\middle|\; \begin{array}{cc} d_1 \leq 1, & d_1+d_2 \leq 2.5, \\ d_2 \leq 2, & d_1+d_3 \leq 3.5, \\ d_3 \leq 3, & d_2+d_3 \leq 4, \\ & d_1+d_2+d_3 \leq 4 \end{array} \right\} \tag{19}$$

. The gap between the blue and the red region is the GDoF loss due to secrecy. The secrecy constraint disallows the presence of codewords that can be decoded by multiple users, a main feature of the simple layered superposition scheme which achieves GDoF optimality of a GBC in the SLS-σ_0 regime [44]. Since the channel is in the CTIN regime, Lemma 2.2 implies that the red region is also the GDoF region for the corresponding GIC, with and without secrecy constraint. As a result,

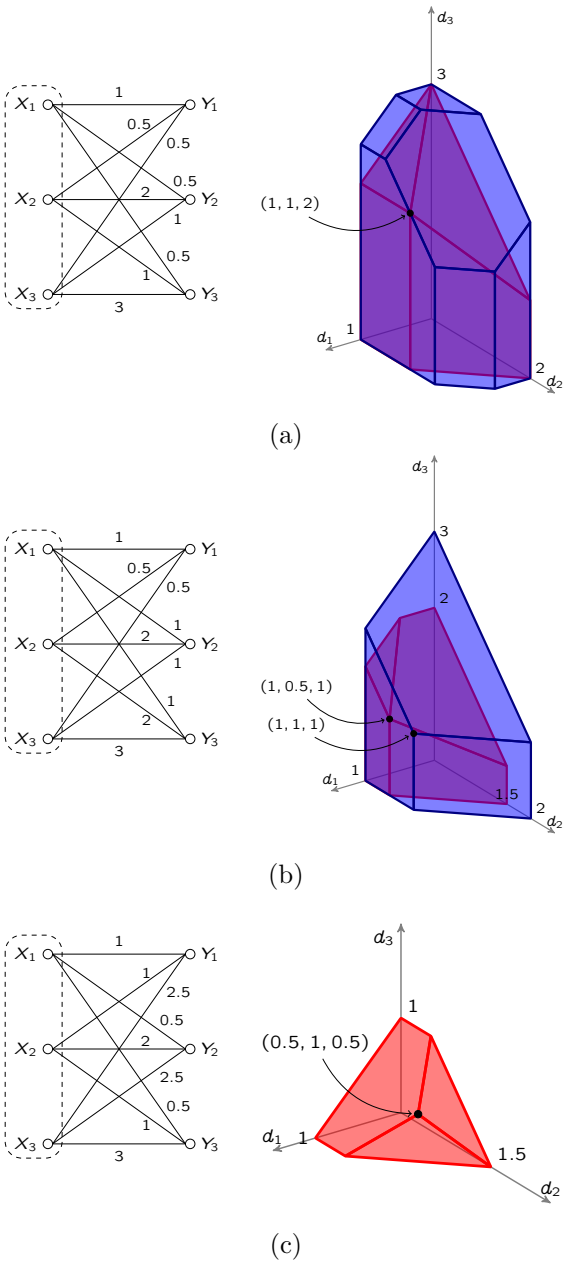


Figure 4: *Channels and their GDoF regions under different message settings and secrecy constraints. (a) A topology in the CTIN regime; shown in blue is the GDoF region for GBC without secrecy; shown in red is the GDoF region for GIC without secrecy, as well as for GBC and GIC with secrecy. (b) A topology in the SLS-σ_0 regime; its GDoF region for GBC without secrecy (blue), and for GBC and GIC with secrecy (red). (c) A topology in the SLS$^+$ regime; its GDoF region for GIC with secrecy.*

one can find that, in this channel regime, imposing secrecy constraint on a GBC and disallowing transmitter cooperation induce the same amount of GDoF loss.

Next, we consider the channel in Figure 4(b) which is easily verified to be in the SLS-σ_0 regime.

From Theorem 3.1, the secure GDoF region for the GBC (the red region) is described as

$$\left\{ (d_1,d_2,d_3)\in\mathbb{R}_+^3 \;\middle|\; \begin{array}{cc} d_1\le 1, & d_1+d_2\le 1.5,\\ d_2\le 2, & d_1+d_3\le 2.5,\\ d_3\le 3, & d_2+d_3\le 2,\\ & d_1+d_2+d_3\le 2.5 \end{array} \right\} \tag{20}$$

. When the secrecy constraint is removed, the GDoF region for the GBC (the blue region) is described as [44, Theorem 1]

$$\left\{ (d_1,d_2,d_3)\in\mathbb{R}_+^3 \;\middle|\; \begin{array}{cc} d_1\le 1, & d_1+d_2\le 2,\\ d_2\le 2, & d_1+d_3\le 3,\\ d_3\le 3, & d_2+d_3\le 3,\\ & d_1+d_2+d_3\le 3 \end{array} \right\} \tag{21}$$

. Similar to the case in Figure 4(a), the gap between these two regions indicates the GDoF loss due to secrecy. Note that this channel is no longer in the CTIN regime, so the GDoF region for this channel operating as a GIC without secrecy constraint is not known. However, since the channel is in the SLS$^+$ regime, from Corollary 3.1 the red region is still the secure GDoF region for the GIC. In other words, there is no GDoF loss due to independent encoding under secrecy constraints.

In Figure 4(c), the channel is in the SLS$^+$ regime, but not in the SLS-σ_0 regime. According to Corollary 3.1, the secure GDoF region for the GIC (the red region) is described as

$$\left\{ (d_1,d_2,d_3)\in\mathbb{R}_+^3 \;\middle|\; \begin{array}{cc} d_1\le 1, & d_1+d_2\le 1.5,\\ d_2\le 2, & d_1+d_3\le 1,\\ d_3\le 3, & d_2+d_3\le 1.5,\\ & d_1+d_2+d_3\le 2 \end{array} \right\} \tag{22}$$

. However, since the channel is not in the SLS-σ_0 regime, the GDoF region for the GBC and GIC, and the secure GDoF region for the GBC remain open.

Example 4.4 (Application of Theorem 3.3)**.** *Here we demonstrate how to apply Theorem 3.3 to find the secure GDoF region of the GBC-groupcast setting in Figure 5(a) and (d), both of which are in the SLS-σ_0 regime. First we consider the channel in Figure 5(a), where $K=2, L_1=2$ and $L_2=1$. Let $\mathcal{P}_{(l_1,l_2)}$ be the secure GDoF region of the GBC-unicast associated with User l_1 in Group 1 and User l_2 in Group 2, where $l_1\in\{1,2\}$ and $l_2\in\{1\}$. They are respectively found with Theorem 3.1 and plotted as the colored regions in Figure 5(b). Then, from Theorem 3.3, the secure GDoF region of the GBC-groupcast is the intersection of these secure GDoF regions (the slashed region). On the other hand, if the secrecy constraint is removed, the GDoF regions of the GBC-unicast associated with the choice of users (l_1,l_2), denoted as $\mathcal{Q}_{(l_1,l_2)}$, can be found with [43, Theorem 1] as the colored regions in Figure 5(c). The intersection of the colored regions (the slashed region) can be shown to be the GDoF region of the GBC-groupcast for this example as follows. An outerbound of the GDoF region is the intersection of the GDoF region of the GBC-unicast over all possible choices of users. The vertices of the slashed region can be achieved. $(1,0)$ and $(0,2)$ are trivially achievable. $(1,1)$ is achievable with the following scheme: at transmitter side, W_1 and W_2, each having 1 DoF, are encoded into X_c and X_p respectively, and sent with $X_1=X_c$ and $X_2=c_1X_c+\bar{P}^{-1}X_p$, where $c_1=\sqrt{1-P^{-1}}$ is chosen to satisfy the input power constraint; at receiver side, all users in each*

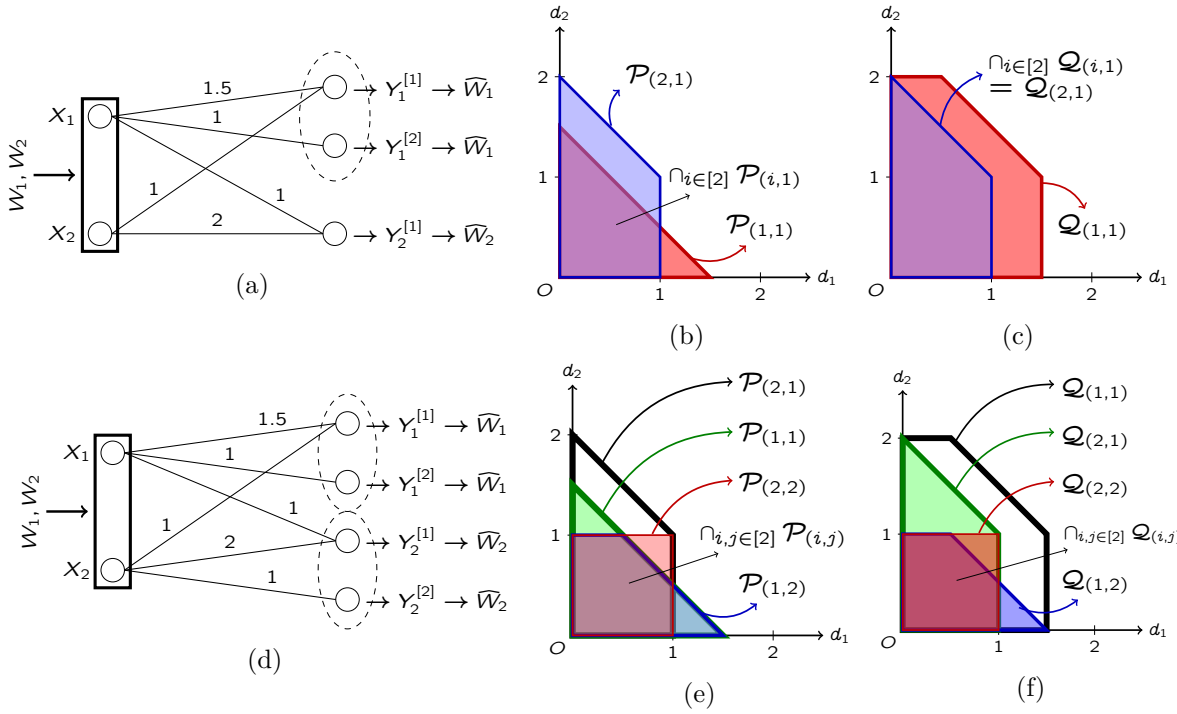


Figure 5: *Channels illustrating the application of Theorem 3.3. (a) A channel where the secrecy constraint induces a GDoF loss. (b) The secure GDoF region for (a). (c) The GDoF region for (a) without secrecy constraint. (d) A channel where the secrecy constraint does not induce a GDoF loss. (e) The secure GDoF region for (d). (f) The GDoF region for (d) without secrecy constraint.*

group can decode X_c, and the user in Group 2 can then remove X_c from $Y_2^{[1]}$ and decode X_p. Note that in this channel, imposing secrecy constraints reduces the GDoF region.

Next we consider the channel in Figure 5(d), where $K = 2, L_1 = L_2 = 2$. Following the notations in Figure 5(b), the secure GDoF regions of the GBC-unicasts, each of which is associated with a choice of users, are plotted as the colored regions in Figure 5(e). Their intersection (the slashed region) is the secure GDoF region for the GBC-groupcast by Theorem 3.3. On the other hand, without secrecy constraint, the GDoF regions of the GBC-unicast associated with choices of users can be found as the colored regions in Figure 5(f). The GDoF region of the GBC-groupcast (the slashed region) is the intersection of these colored regions by a similar argument applied in Figure 5(c): the outerbound is the same; the slashed region is achievable because it is the same as the slashed one in Figure 5(e), which is a polyhedral TIN region. Unlike the channel in Figure 5(a), in this channel imposing a secrecy constraint does not induce a GDoF loss.

5 Proofs

5.1 Proof of Theroem 3.1

Suppose the channel is in the SLS-σ regime; i.e., there exists a tuple σ such that (10) – (12) hold. The achievability follows from Lemma 2.1 directly. Hereafter we only consider the converse. For

the bounds in (6), the proof follows the single user capacity bound and (11), i.e.,

$$d_i \le \max_{k\in[K]} \alpha_{ik} = \alpha_{i\sigma(i)}. \tag{23}$$

For the bounds in (7), the proof is mainly based upon the AI bounds [40, 42–44, 57, 58]. We define a deterministic model for (1) as follows:

$$\bar{Y}_k(t) = \sum_{i=1}^{K} \left\lfloor \bar{P}^{\alpha'_{k\sigma(i)}} G_{k\sigma(i)} \bar{X}_{\sigma(i)}(t) \right\rfloor \qquad \forall k \in [K], \tag{24}$$

where $\alpha'_{k\sigma(i)} = \alpha_{k\sigma(i)} - \max_{m\in[K]} \alpha_{m\sigma(i)} = \alpha_{k\sigma(i)} - \alpha_{i\sigma(i)}$ (the last equality is due to (10)), and $\lceil z \rceil = \lceil x \rceil + j\lceil y \rceil$ for a complex number $z = x + jy$. The channel input $\bar{X}_{\sigma(i)}(t) = \lceil X_{\sigma(i)}(t) \rceil \bmod \lceil \bar{P}^{\alpha_{i\sigma(i)}} \rceil = \bar{X}_{R,\sigma(i)}(t) + j\bar{X}_{I,\sigma(i)}(t)$, and

$$\bar{X}_{R,\sigma(i)}(t), \bar{X}_{R,\sigma(i)}(t) \in \{0, 1, \cdots, \lceil \bar{P}^{\alpha_{i\sigma(i)}} \rceil\}. \tag{25}$$

Next, we will prove that, with finite-precision CSIT and the secrecy constraint, the GDoF region of the deterministic model (24) constitutes an outer bound of the original GBC (1). To this end, we need the following lemma.

Lemma 5.1. *For all $k \in [K]$,*

$$I(W_k; Y_k^n \mid \mathcal{G}) \le I(W_k; \bar{Y}_k^n \mid \mathcal{G}) + no(\log P), \tag{26}$$

$$I(W_{-k}^K; \bar{Y}_k^n \mid \mathcal{G}) \le I(W_{-k}^K; Y_k^n \mid \mathcal{G}) + no(\log P), \tag{27}$$

where $W_{-k}^K \triangleq \{W_i : \forall i \in [K] \backslash \{k\}\}$.

The proof of Lemma 5.1 is relegated to Appendix A. Let $(i_1, i_2, \cdots, i_m) \in \Pi_m$ with $2 \le m \le K$. (See Definition 2.1 for the definition of Π_m.) For all $\epsilon > 0$ and all $j \in [m]$ with the modulo-m arithmetic implicitly used (i.e., $i_0 = i_m$), we have

$$\begin{aligned}
nR_{i_j} \le & I(W_{i_j}; Y_{i_j}^n \mid \mathcal{G}) + n\epsilon && (28)\\
\le & I(W_{i_j}; \bar{Y}_{i_j}^n \mid \mathcal{G}) + no(\log P) && (29)\\
\le & I(W_{i_j}; \bar{Y}_{i_j}^n \mid \mathcal{G}) - I(W_{-i_j}^K; Y_{i_j}^n \mid \mathcal{G}) + n\epsilon + no(\log P) && (30)\\
\le & I(W_{i_j}; \bar{Y}_{i_j}^n \mid \mathcal{G}) - I(W_{-i_j}^K; \bar{Y}_{i_j}^n \mid \mathcal{G}) + no(\log P) && (31)\\
\le & I(W_{i_j}; \bar{Y}_{i_j}^n \mid \mathcal{G}) - I(W_{i_{j-1}}; \bar{Y}_{i_j}^n \mid \mathcal{G}) + no(\log P) && (32)\\
\le & H(\bar{Y}_{i_j}^n \mid W_{i_{j-1}}, \mathcal{G}) - H(\bar{Y}_{i_j}^n \mid W_{i_j}, \mathcal{G}) + no(\log P). && (33)
\end{aligned}$$

We apply Fano's inequality in (28). Since, as (26) implies, the deterministic model incurs no GDoF loss, (29) holds. Next we plug in the secrecy constraint (2) to have (30). The deterministic model incurs no GDoF cost in the secrecy constraint, as (27) implies, so we have (31). Finally, (32) holds because $I(X, Y; Z) \ge I(X; Z)$ for arbitary random variables X, Y, Z. Summing the rate R_{i_j} over all $j \in [m]$, one gets (with $no(\log P)$ suppressed)

$$n \sum_{j=1}^{m} R_{i_j} \le \sum_{j=1}^{m} H(\bar{Y}_{i_j}^n \mid W_{i_{j-1}}, \mathcal{G}) - H(\bar{Y}_{i_{j-1}}^n \mid W_{i_{j-1}}, \mathcal{G}) \tag{34}$$

$$\leq \sum_{j=1}^{m} \max_{k\in[K]} (\alpha_{i_j k} - \alpha_{i_{j-1} k})^+ n \log P \tag{35}$$

$$= \sum_{j=1}^{m} \left(\alpha_{i_j \sigma(i_j)} - \alpha_{i_{j-1} \sigma(i_j)} \right) n \log P. \tag{36}$$

In (35), we invoke the AI bound, as stated in the following lemma.

Lemma 5.2 (Lemma 1 in [42]). *For $j \in [m]$, we have*

$$H(\bar{Y}_{i_j}^n \mid W_{i_{j-1}}, \mathcal{G}) - H(\bar{Y}_{i_{j-1}}^n \mid W_{i_{j-1}}, \mathcal{G}) \leq \max_{k\in[K]} (\alpha_{i_j k} - \alpha_{i_{j-1} k})^+ n \log P + no(\log P). \tag{37}$$

Since we assume the channel is in the SLS-σ regime, (36) holds. More specifically, condition (12) implies $\alpha_{i_j \sigma(i_j)} - \alpha_{i_{j-1} \sigma(i_j)} \geq \alpha_{i_j k} - \alpha_{i_{j-1} k}$ for all $k \in [K]$ and $j \in [m]$, and condition (10) implies $\alpha_{i_j \sigma(i_j)} \geq \alpha_{i_j \sigma(i_{j-1})}$ for all $j \in [m]$. As a result, we establish the outer bound (7). □

5.2 Proof of Theorem 3.2

For the converse, applying Lemma 5.2 to (34) with $K = 2$ yields (15). In the following, we show how to achieve the outer bound. Without loss of generality, we assume $\alpha_{11} = \max_{i,j=\{1,2\}} \alpha_{ij}$. We consider the following two cases:

1. $\alpha_{11} + \alpha_{22} \geq \alpha_{12} + \alpha_{21}$: In this case, the outer bound (15) becomes $(\alpha_{11} - \alpha_{21}) + (\alpha_{22} - \alpha_{12})^+$. When $\alpha_{22} \leq \alpha_{12}$, we can achieve the secure GDoF tuple $(\alpha_{11} - \alpha_{21}, 0)$ by letting $X_2 = 0$ and $X_1(t) = V_1(t) \sim \mathcal{CN}(0, P^{-\alpha_{21}})$ taken from a Gaussian wiretap codebook of size $2^{n(R_{s1}+R_{c1})}$, where

$$R_{s1} = \log\left(1 + P^{\alpha_{11}-\alpha_{21}} \Delta^{-2}\right) - \log(1 + \Delta^2), \tag{38}$$

$$R_{c1} = \log(1 + \Delta^2), \tag{39}$$

and W_1 is encoded at rate R_{s1}. The rate R_{s1} for message W_1 is achievable under the secrecy constraint, because according to [33, Theorem 4], the following secure rate is achievable:

$$R_1 = \inf_{\boldsymbol{g}} \left\{ I(V_1; Y_1 | \mathcal{G} = \boldsymbol{g}) - I(V_1; Y_2 | V_2, \mathcal{G} = \boldsymbol{g}) \right\}, \tag{40}$$

where the time index t is suppressed, $\boldsymbol{g} = \{G_{ij} : \ i, j \in [2]\}$ is a realization of $\mathcal{G}$, and the infimum is taken over the support of the random varaibles in $\mathcal{G}$. This can be shown further that $R_1 \geq R_{s1}$, because

$$R_1 = \inf_{\boldsymbol{g}} \left\{ \log(1 + P^{\alpha_{11}-\alpha_{21}} |G_{11}|^2) - \log(1 + |G_{21}|^2) \right\} \tag{41}$$

$$\geq \log\left(1 + P^{\alpha_{11}-\alpha_{21}} \Delta^{-2}\right) - \log(1 + \Delta^2) = R_{s1}, \tag{42}$$

where in (42) the inequality holds because it is assumed $1/\Delta \leq |G_{ij}(t)| \leq \Delta$. Noting that $R_{s1} = (\alpha_{11} - \alpha_{21}) \log P + o(\log P)$, we have $d_1 = \alpha_{11} - \alpha_{21}$. When $\alpha_{22} > \alpha_{12}$, the achievability follows Lemma 2.1 where $\sigma = (1, 2)$.

2. $\alpha_{11} + \alpha_{22} < \alpha_{12} + \alpha_{21}$: In this case, the outer bound (15) becomes $(\alpha_{12} - \alpha_{22})^+$. When $\alpha_{12} > \alpha_{22}$, we can achieve the secure GDoF tuple $(\alpha_{12} - \alpha_{22}, 0)$ by letting $X_1(t) = 0$ and $X_2(t) = V_1(t) \sim \mathcal{CN}(0, P^{-\alpha_{22}})$ taken from a Gaussian wiretap codebook with which the message W_1 is encoded.

5.3 Proof of Theorem 3.3

First we consider the converse part. In the groupcast setting, every message is required to be reliably decoded by all the users in its designated group. The outer bounds in Theorem 3.1 for a GBC-unicast associated with a choice of users (one from each group) are also outer bounds for the GBC-groupcast. More specifically, let $\boldsymbol{l} = (l_1, l_2, \cdots, l_K)$ be a choice of users ($l_i \in [L_i]$), and $\mathcal{P}_\sigma(\boldsymbol{l})$ be the polyhedral TIN region associated with the message ordering σ and the user choice $\boldsymbol{l}$. Since condition (10) - (12) are satisfied for all $\boldsymbol{l} \in \mathcal{L} \triangleq \prod_{i=1}^{K}[L_i]$, according to Theorem 3.1, $\mathcal{P}_\sigma(\boldsymbol{l})$ is the GDoF region associated with $\boldsymbol{l}$, and the intersection of the polyhedral TIN regions over all possible user choices includes the GDoF region of the GBC-groupcast $\mathcal{D}_\sigma$, i.e.,

$$\mathcal{D}_\sigma \subseteq \bigcap_{\boldsymbol{l}\in\mathcal{L}} \mathcal{P}_\sigma(\boldsymbol{l}) = \bar{\mathcal{P}}_\sigma. \tag{43}$$

For the achievability, as a stepping stone we first consider the GDoF region achieved by the polyhedral TIN scheme *without* secrecy constraints. Let the codeword $X_{\sigma(i)}$ carry message W_i. The GDoF region achieved by the polyhedral TIN scheme associated with σ, denoted as $\mathcal{P}_\sigma^o$, contains tuples $(d_1, d_2, \cdots, d_K)$ satisfying $d_i \geq 0$ and

$$d_i = \min_{l_i\in[L_i]} \left\{ \alpha_{i\sigma(i)}^{[l_i]} + r_{\sigma(i)} - \max_{j\in[K]\setminus\{i\}} \left(\alpha_{i\sigma(j)}^{[l_i]} + r_{\sigma(j)}\right)^+ \right\}, \tag{44}$$

where $r_i \leq 0$ for all $i \in [K]$. Since $\mathcal{P}_\sigma^o$ contains all GDoF tuples achieved by the polyhedral TIN scheme, it is related to the polyhedral TIN region $\bar{\mathcal{P}}_\sigma$. In fact, the following lemma holds.

Lemma 5.3. $\bar{\mathcal{P}}_\sigma \subset \mathcal{P}_\sigma^o$.

A proof of Lemma 5.3 can be inferred by adopting the procedures in [53], where the application of the polyhedral TIN scheme to a GIC with compound settings is studied. This is done by first recognizing that (44) has a similar formulation to Equation (93) of [53], and following Equation (94)–(105) of [53].[6] Instead of repeating the same arguments, let us instead present an alternative proof based on Max-Plus algebra, that may be of interest by itself. The details of this proof are presented in Appendix B.

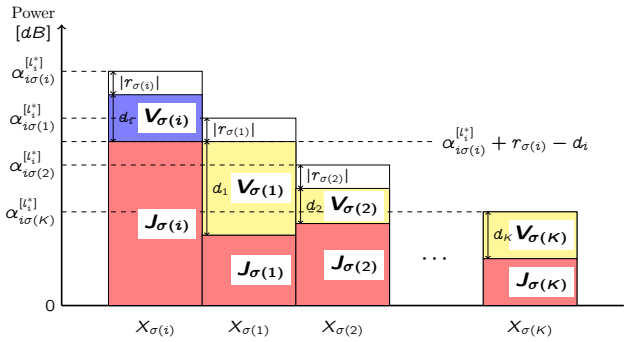
From Lemma 5.3, every GDoF tuple $(d_1, d_2, \cdots, d_K) \in \bar{\mathcal{P}}_\sigma$ can be achieved with some power control tuple $(r_1, r_2, \cdots, r_K)$ ($r_i \leq 0, \forall i \in [K]$) and TIN, without the secrecy constraints for now. As shown in (69) and (70), such a tuple satisfies

$$d_i = \bar{\alpha}_{i\sigma(i)} + r_{\sigma(i)} - \max_{j\in[K]\setminus\{i\}} \left(\bar{\alpha}_{i\sigma(j)} + r_{\sigma(j)}\right)^+. \tag{45}$$

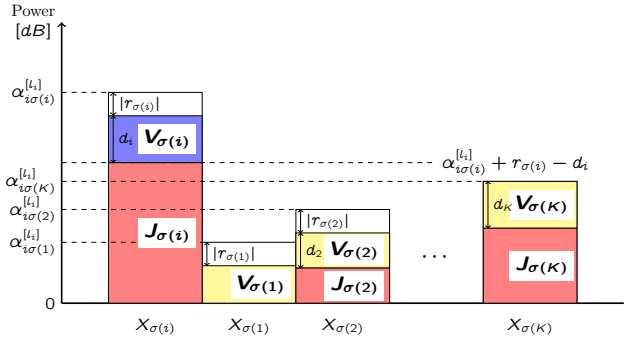
Recall that $\{\bar{\alpha}_{ij}\}$ is defined in (16) and (17).

Next, based on the polyhedral TIN scheme described above, we show that TIN with cooperative jamming is able to achieve the entire region $\bar{\mathcal{P}}_\sigma$ even under the secrecy constraints. Let $(d_1, d_2, \cdots, d_K) \in \bar{\mathcal{P}}_\sigma$ satisfy (45) for some $(r_1, r_2, \cdots, r_K)$ with $r_i \leq 0$ for all $i \in [K]$. The channel input of the TIN with cooperative jamming scheme is defined, for all $i \in [K]$, as $X_{\sigma(i)}(t) = V_{\sigma(i)}(t) + J_{\sigma(i)}(t)$, where $V_{\sigma(i)}(t)$ and $J_{\sigma(i)}(t)$ are independent. $V_{\sigma(i)}(t) \sim \mathcal{CN}(0, P^{r_{\sigma(i)}}/2)$

[6] Note that in [53] the GDoF region achieved by the polyhedral TIN scheme is derived based on *no* prior assumption of the channel regime. There is indeed an assumption of the channel regime in [53, Theorem 1], but it is used to show the optimality of TIN within such a regime, and is not used in the derivation of the GDoF region achieved by the polyhedral TIN regime.



(a)



(b)

Figure 6: *The decomposition of the received signal in Group i (a) seen by Receiver l_i^*, which attains the minimum in (44), and (b) seen by Receiver $l_i \neq l_i^*$. The solid horizontal axis marks the noise level. Each colored partition represents a message-carrying codeword or a jammer with the top level as its power in dB scale and the height as its degree of freedom. The blue partition ($V_{\sigma(i)}$) is a codeword desired by the receivers in Group i, the yellow ones ($V_{\sigma(j)}, j \neq i$) are codewords desired by the receivers in the other groups, and the red ones ($J_{\sigma(j)}, j \in [K]$]) are jammers.*

is taken from a Gaussian wiretap codebook with which message W_i is encoded, and $J_{\sigma(i)}(t) \sim \mathcal{CN}(0, P^{r_{\sigma(i)}-d_i}/2)$ is a randomly generated jamming signal. Note that since $d_i \geq 0$ and $r_i \leq 0$, the power of the input codeword $\mathbb{E}[|X_{\sigma(i)}|^2] = \mathbb{E}[|V_{\sigma(i)}|^2] + \mathbb{E}[|J_{\sigma(i)}|^2] = \frac{1}{2}(P^{r_{\sigma(i)}} + P^{r_{\sigma(i)}-d_i}) \leq 1$ satisfies the unit average power constraint for all $i \in [K]$.

In the following we show with [33, Lemma 1] that all recievers in Group i can decode $V_{\sigma(i)}$ while all the other messages are kept secrect from them. Let l_i^* be the receiver in Group i that attains the minimum in (44); i.e.,

$$\alpha_{i\sigma(i)}^{[l_i^*]} + r_{\sigma(i)} - d_i = \max_{j \in [K]\setminus\{i\}} \left(\alpha_{i\sigma(j)}^{[l_i^*]} + r_{\sigma(j)}\right)^+. \tag{46}$$

Figure 6(a) depicts an example of how the channel inputs constitute the output at Receiver l_i^* via their respective links. Receiver l_i^* can decode $V_{\sigma(i)}$ by treating the jammer $J_{\sigma(i)}$ and all the other inputs X_j ($j \neq \sigma(i)$) as noise. Note that all the other message-carrying codewords V_j ($j \neq \sigma(i)$) have power levels no larger than that of the jammer $J_{\sigma(i)}$. By [33, Lemma 1], all of them satisfy the secrecy constraint for Receiver l_i^*.

On the other hand, for the other receivers $l_i \neq l_i^*$ in Group i, we have

$$\alpha_{i\sigma(i)}^{[l_i]} + r_{\sigma(i)} - d_i \geq \max_{j\in[K]\setminus\{i\}} \left(\alpha_{i\sigma(j)}^{[l_i]} + r_{\sigma(j)}\right)^+. \tag{47}$$

This means the jammer $J_{\sigma(i)}$ has a greater power level than all the other inputs do, as depicted in Figure 6(b). $V_{\sigma(i)}$ remains decodable by treating the jammer $J_{\sigma(i)}$ and the rest as noise. $V_{\sigma(j)}$ $(j \neq i)$ remain secret, as they have power levels no larger than the jammer $J_{\sigma(i)}$ does, a no-better condition than the one seen by Receiver l_i^*.

As a result, any secure GDoF tuple $(d_1, d_2, \cdots, d_K) \in \bar{\mathcal{P}}_\sigma$ is achievable, i.e., $\bar{\mathcal{P}}_\sigma \subseteq \mathcal{D}_\sigma$. Together with (43), we have established the secure GDoF region for the GBC-groupcast to be $\bar{\mathcal{P}}_\sigma$.

6 Conclusion

We identify a new channel parameter regime where the simple scheme of TIN and cooperative jamming is optimal for the secure GDoF region of Gaussian broadcast channel under finite-precision CSIT. The AI bounds play a key role in giving tight converse bounds and identifying the new parameter regimes. We also extend the results to its counterpart Gaussian interference channel and generalize them to groupcast settings. As a part of the future work, it is of interest to explore beyond the channel regimes identified in this work, which may lead to other robust schemes than TIN and cooperative jamming. Another interesting direction is to generalize the settings by adding helpers/eavesdroppers, and study how they strengthen/undermine the secure communications.

A Proof of Lemma 5.1

The proof of (26) is identical to the one in [40, Appendix] and is not repeated here. In the following we prove (27) only. Firstly we define the following terms for all $k, i \in [K]$ with the channel use index t suppressed:

$$\tilde{X}_i = \bar{P}^{\alpha_{ii}} X_i, \tag{48}$$

$$\tilde{Y}_k = \sum_{i=1}^{K} \left\lceil G_{ki} \bar{P}^{\alpha'_{ki}} \left\lceil \tilde{X}_i \right\rceil \right\rceil, \tag{49}$$

$$\hat{X}_i = \left\lceil \tilde{X}_i \right\rceil - \bar{X}_i, \tag{50}$$

$$\delta_i = \left\lceil \tilde{X}_i \right\rceil - \tilde{X}_i, \tag{51}$$

$$\Delta_k = Y_k - \lceil Y_k \rceil, \tag{52}$$

$$\epsilon_{ki} = \left\lceil G_{ki} \bar{P}^{\alpha'_{ki}} \left\lceil \tilde{X}_i \right\rceil \right\rceil - G_{ki} \bar{P}^{\alpha'_{ki}} \left\lceil \tilde{X}_i \right\rceil, \tag{53}$$

$$\bar{\epsilon}_{ki} = G_{ki} \bar{P}^{\alpha'_{ki}} \bar{X}_i - \left\lceil G_{ki} \bar{P}^{\alpha'_{ki}} \bar{X}_i \right\rceil, \tag{54}$$

$$\hat{\delta}_{ki} = \bar{P}^{\alpha'_{ki}} \hat{X}_i - \left\lceil \bar{P}^{\alpha'_{ki}} \hat{X}_i \right\rceil. \tag{55}$$

Now we proceed to the proof of (27).

$$I(W_{-k}^K; \bar{Y}_k^n \mid \mathcal{G}) \tag{56}$$

$$\leq I(W_{-k}^K; \bar{Y}_k^n, \tilde{Y}_k^n, Y_k^n \mid \mathcal{G}) \tag{57}$$
$$\leq I(W_{-k}^K; Y_k^n \mid \mathcal{G}) + I(W_{-k}^K; \tilde{Y}_k^n \mid Y_k^n, \mathcal{G}) + I(W_{-k}^K; \bar{Y}_k^n \mid Y_k^n, \tilde{Y}_k^n, \mathcal{G}) \tag{58}$$
$$\leq I(W_{-k}^K; Y_k^n \mid \mathcal{G}) + H(\tilde{Y}_k^n \mid Y_k^n, \mathcal{G}) + H(\bar{Y}_k^n \mid Y_k^n, \tilde{Y}_k^n, \mathcal{G}) \tag{59}$$
$$\leq I(W_{-k}^K; Y_k^n \mid \mathcal{G}) + H(\tilde{Y}_k^n \mid \lceil Y_k^n \rceil, \mathcal{G}) + H(\bar{Y}_k^n \mid \tilde{Y}_k^n, \mathcal{G}), \tag{60}$$

where (60) holds because $\lceil Y_k^n \rceil$ is a function of Y_k^n, and $H(X \mid f(Y)) \geq H(X \mid Y)$ for any function f and random variables X, Y. Next we show that $H(\tilde{Y}_k^n \mid \lceil Y_k^n \rceil, \mathcal{G})$ and $H(\bar{Y}_k^n \mid \tilde{Y}_k^n, \mathcal{G})$ in (60) is bounded above by $no(\log P)$. For $H(\tilde{Y}_k^n \mid \lceil Y_k^n \rceil, \mathcal{G})$, we note that for all $k \in [K]$, (with the channel use index t supressed,)

$$\tilde{Y}_k = \lceil Y_k \rceil + \Delta_k + \sum_{i=1}^K \left(G_{ki} \bar{P}^{\alpha'_{ki}} \delta_i + \epsilon_{ki} \right), \tag{61}$$

and both $\tilde{Y}_k$ and $\lceil Y_k \rceil$ take integer values in their respective real and imaginary part. The sum of the truncation errors $\Delta_k + \sum_{i=1}^K G_{ki} \bar{P}^{\alpha'_{ki}} \delta_i + \epsilon_{ki}$ has its real and imaginary part taking an integer value in $(-1 - 2K\Delta, K(1 + 2\Delta))$. Therefore, we have

$$H(\tilde{Y}_k^n \mid \lceil Y_k^n \rceil, \mathcal{G}) \leq H(\{\Delta_k + \sum_{i=1}^K \left(G_{ki} \bar{P}^{\alpha'_{ki}} \delta_i + \epsilon_{ki} \right)\}_{t=1}^n) \tag{62}$$
$$\leq n 2 \log_2 \left(2 \lceil K(1 + 2\Delta) \rceil \right) = no(\log P). \tag{63}$$

For $H(\bar{Y}_k^n \mid \tilde{Y}_k^n, \mathcal{G})$ in (60), we note that for all $k \in [K]$, (with the channel use index t supressed,)

$$\tilde{Y}_k = \bar{Y}_k + \sum_{i=1}^K G_{ki} \left\lceil \bar{P}^{\alpha'_{ki}} \hat{X}_i \right\rceil + \sum_{i=1}^K \left(G_{ki} \hat{\delta}_{ki} + \bar{\epsilon}_{ki} + \epsilon_{ki} \right). \tag{64}$$

Since $\tilde{Y}_k, \tilde{Y}_k$ and $\lceil G_{ki} \bar{P}^{\alpha'_{ki}} \hat{X}_i \rceil$ take integer values in their respective real and imaginary part, the sum of the trunction errors $\sum_{i=1}^K G_{ki} \hat{\delta}_{ki} + \bar{\epsilon}_{ki} + \epsilon_{ki}$ must be an integer in $(-2K(1+\Delta), 2K(1+\Delta))$ in its real and imaginary part. Therefore,

$$H(\bar{Y}_k^n \mid \tilde{Y}_k^n, \mathcal{G})$$
$$\leq \sum_{i=1}^K H(\{\left\lceil \bar{P}^{\alpha'_{ki}} \hat{X}_i \right\rceil\}_{t=1}^n \mid \mathcal{G}) + H(\{\sum_{i=1}^K \left(G_{ki} \hat{\delta}_{ki} + \bar{\epsilon}_{ki} + \epsilon_{ki} \right)\}_{t=1}^n) \tag{65}$$
$$\leq \sum_{i=1}^K H(\{\hat{X}_i\}_{t=1}^n \mid \mathcal{G}) + n 2 \log_2 \left(2 \lceil 2K(1 + \Delta) \rceil \right), \tag{66}$$

where (66) is because $\lceil \bar{P}^{\alpha'_{ki}} \hat{X}_i \rceil$ is a function of $\hat{X}_i$. Finally, seeing that $\mathbb{E}[|\lceil \tilde{X}_i \rceil|^2] \leq \mathbb{E}[|2\tilde{X}_i|^2] \leq 4P^{-\alpha_{ii}}$, we can further bound $H(\hat{X}_i(t))$ above with a constant by following the same procedure in [40, (130) – (149), Appendix]. Now $H(\bar{Y}_k^n \mid \tilde{Y}_k^n, \mathcal{G})$ in (60) is bounded by $no(\log P)$, and (27) is therefore established.

B Proof of Lemma 5.3 with Max-Plus Algebra

We present the proof of Lemma 5.3 using max-plus algebra. First we revisit the definitions of the operators on scalars and matrices in max-plus algebra, and define graphs associated with square

matrices. Next we state a useful result of matrix equations of a certain type. Finally we present the proof of Lemma 5.3 by reformulating (44) with max-plus algebra and deducing that all GDoF tuples in $\bar{\mathcal{P}}_\sigma$ are achievable by the polyhedral TIN scheme.

B.1 Definition of operators in max-plus Algebra

The following definitions and observations are adopted from [59, Chapter 3]. To keep this proof self-contained, we summarize the definitions necessary for the derivations and the discussions in the following sections.

We define two operators on the set $\bar{\mathbb{R}} \triangleq \mathbb{R} \cup \{-\infty\}$: $\oplus$ and $\otimes$. For $a, b \in \bar{\mathbb{R}}$, define $a \oplus b \triangleq \max\{a, b\}$, and $a \otimes b \triangleq a + b$. The identity element for $\oplus$ is $\epsilon \triangleq -\infty$. Let $\boldsymbol{A} \in \bar{\mathbb{R}}^{K\times M}$ be a $K \times M$ matrix with (i, j)-th entry denoted as $[\boldsymbol{A}]_{ij}$. When $\boldsymbol{x} \in \bar{\mathbb{R}}^{K\times 1} = \bar{\mathbb{R}}^K$, we call $\boldsymbol{x}$ a $K \times 1$ vector with $[\boldsymbol{x}]_i$ as the i^{th} component. For two matrices $\boldsymbol{A} \in \bar{\mathbb{R}}^{K\times M}$ and $\boldsymbol{B} \in \bar{\mathbb{R}}^{M\times N}$, we define $\boldsymbol{A} \otimes \boldsymbol{B}$ as a $K \times N$ matrix, with$[\boldsymbol{A} \otimes \boldsymbol{B}]_{ij} = \bigoplus_{m=1}^{M} [\boldsymbol{A}]_{im} \otimes [\boldsymbol{B}]_{mj}$. For two matrices of the same size $\boldsymbol{A}, \boldsymbol{C} \in \bar{\mathbb{R}}^{K\times M}$, we define $\boldsymbol{A} \oplus \boldsymbol{C}$ as a $K \times M$ matrix with $[\boldsymbol{A} \oplus \boldsymbol{B}]_{ij} = [\boldsymbol{A}]_{ij} \oplus [\boldsymbol{C}]_{ij}$. For a sqaure matrix $\boldsymbol{D} \in \bar{\mathbb{R}}^{K\times K}$, we denote $\boldsymbol{D}^n = \underbrace{\boldsymbol{D} \otimes \boldsymbol{D} \otimes \cdots \otimes \boldsymbol{D}}_{n \text{ times}}$. For two vectors $\boldsymbol{x}, \boldsymbol{y} \in \bar{\mathbb{R}}^K$, by $\boldsymbol{x} \leq \boldsymbol{y}$ we mean for all $i \in [K]$, $[\boldsymbol{x}]_i \leq [\boldsymbol{y}]_i$.

We can associate a square matrix $\boldsymbol{D} \in \bar{\mathbb{R}}^{K\times K}$ with a precedence graph $\mathcal{G}(\boldsymbol{D})$. It takes $[K]$ as its vertices, and the edge from vertex i to j, denoted as (i, j), is either set with weight $[\boldsymbol{D}]_{ij}$, or removed if $[\boldsymbol{D}]_{ij} = \epsilon$. A path from vertex i_1 to i_m, denoted as a tuple $\pi = (i_1, i_2, \cdots, i_m)$, where $i_1, i_2, \cdots, i_m \in [K]$ are not necessarily distinct, is an ordered collection of edges (i_j, i_{j+1}), where $j \in [m-1]$. The length of π is the number of edges in π. The weight of π, denoted as $\omega(\pi)$, is the sum of the weights of the edges along π over normal algebra; i.e., $\omega(\pi) = \sum_{j=1}^{m-1} [\boldsymbol{D}]_{i_{j+1}i_j}$. A circuit is a path with both ends being the same, and its weight can be defined in the same way as is the weight of a path. One observation of the connection between $\boldsymbol{D}$ and $\mathcal{G}(\boldsymbol{D})$ is that, $[\boldsymbol{D}^n]_{ij}$ is the maximum path weight over all length-n paths from vertex j to i.

B.2 A useful result in max-plus algebra

We consider the following matrix equation, into which the GDoF achieved by the polyhedral TIN scheme (44) can be recast:

$$\boldsymbol{P} \otimes \boldsymbol{r} \oplus \boldsymbol{q} = \boldsymbol{r}, \tag{67}$$

where $\boldsymbol{P} \in \bar{\mathbb{R}}^{K\times K}$ and $\boldsymbol{r}, \boldsymbol{q} \in \bar{\mathbb{R}}^K$. How the equation (44) can be recast into (67) is presented in Appendix B.3, but for now we consider this matrix equation in general. For a given $\boldsymbol{P}$ and $\boldsymbol{q}$, the existence of a solution $\boldsymbol{r} \leq \boldsymbol{0}$ is of interest, where $\boldsymbol{0}$ is a $K \times 1$ vector with 0 as its components. The following theorem offers a set of conditions of $\boldsymbol{P}$ and $\boldsymbol{q}$ that guarantees such a solution to (67) exists.

Theorem B.1. *Let $\boldsymbol{P} \in \bar{\mathbb{R}}^{K\times K}$, and $\boldsymbol{q}, \boldsymbol{r} \in \bar{\mathbb{R}}^K$. If (a) $\mathcal{G}(\boldsymbol{P})$ has the maximum circuit weight no larger than zero, and (b) $\boldsymbol{q} \leq \boldsymbol{0}$, and for all $k \in [K-1]$, $\boldsymbol{P}^k \otimes \boldsymbol{q} \leq \boldsymbol{0}$, then there exists a solution $\boldsymbol{r} \leq \boldsymbol{0}$ to the equation $\boldsymbol{P} \otimes \boldsymbol{r} \oplus \boldsymbol{q} = \boldsymbol{r}$. The solution is*

$$\boldsymbol{r} = \boldsymbol{q} \oplus (\boldsymbol{P} \otimes \boldsymbol{q}) \oplus \cdots \oplus \left(\boldsymbol{P}^{K-1} \otimes \boldsymbol{q}\right). \tag{68}$$

Proof. According to Theorem 3.17 of [59], condition (a) guarantees that (68) is a solution to the matrix equation $\boldsymbol{P} \otimes \boldsymbol{r} \oplus \boldsymbol{q} = \boldsymbol{r}$. Condition (b) further implies that such a solution $\boldsymbol{r} \leq \boldsymbol{0}$. □

B.3 Proof of Lemma 5.3 with Theorem B.1

It can be shown that the GDoF achievable by the polyhedral TIN scheme (44) can be reformulated in the form of the matrix equation (67). Firstly we recognize that, on the right-hand side of (44), $r_{\sigma(i)}$ is independent of l_i. By taking it out of the minimum operator, and moving everything therein to the left, we have

$$d_i + \max_{l_i \in [L_i]} \left\{ \max_{j \in [K]\setminus\{i\}} \left\{ -\alpha_{i\sigma(i)}^{[l_i]}, -\alpha_{i\sigma(i)}^{[l_i]} + \alpha_{i\sigma(j)}^{[l_i]} + r_{\sigma(j)} \right\} \right\} = r_{\sigma(i)} \tag{69}$$

$$\Rightarrow \quad d_i + \max_{j \in [K]\setminus\{i\}} \left\{ -\bar{\alpha}_{i\sigma(i)}, -\bar{\alpha}_{i\sigma(i)} + \bar{\alpha}_{i\sigma(j)} + r_{\sigma(j)} \right\} = r_{\sigma(i)} \tag{70}$$

$$\Rightarrow \quad \left(d_i - \bar{\alpha}_{i\sigma(i)}\right) \oplus \bigoplus_{j \in [K]\setminus\{i\}} \left\{ \left(d_i - \bar{\alpha}_{i\sigma(i)} + \bar{\alpha}_{i\sigma(j)}\right) \otimes r_{\sigma(j)} \right\} \oplus \left(\epsilon \otimes r_{\sigma(i)}\right) = r_{\sigma(i)}. \tag{71}$$

In step (70) we swap the two maximum operators and apply the definition of $\{\bar{\alpha_{ij}}\}$ in (16) and (17). In step (71) we take d_i into the maximum operator, then replace all maximum operators with $\oplus$ and substitute $\otimes$ for the $+$ operator with respect to $r_{\sigma(j)}$, and finally add $\epsilon \otimes r_{\sigma(i)}$ on both sides with $\oplus$ operator. Such an addition does not change the right-hand side, because $r_{\sigma(i)} \oplus (\epsilon \otimes r_{\sigma(i)}) = \max\{r_{\sigma(i)}, -\infty + r_{\sigma(i)}\} = r_{\sigma(i)}$. The equations for all $i \in [K]$ can be further summarized into a matrix equation of the form (67), where

$$[\boldsymbol{P}]_{ij} = \begin{cases} d_i - \bar{\alpha}_{i\sigma(i)} + \bar{\alpha}_{i\sigma(j)} & \text{if } i \neq j \\ \epsilon & \text{if } i = j \end{cases}, \tag{72}$$

$$[\boldsymbol{q}]_i = d_i - \bar{\alpha}_{i\sigma(i)}, \tag{73}$$

$$[\boldsymbol{r}]_i = r_i. \tag{74}$$

As a result, the GDoF region achieved by the polyhederal TIN scheme is

$$\mathcal{P}_\sigma^o = \left\{ (d_1, d_2, \cdots, d_K) \in \mathbb{R}^K \,\middle|\, \begin{array}{l} d_i \geq 0, \forall i \in [K], \text{and} \\ \exists\ \boldsymbol{r} \leq \boldsymbol{0} \text{ s.t. } \boldsymbol{P} \otimes \boldsymbol{r} \oplus \boldsymbol{q} = \boldsymbol{r} \end{array} \right\}. \tag{75}$$

Next, we apply Theorem B.1 for the conditions of a GDoF tuple being in $\mathcal{P}_\sigma^o$. Condition (a) in Theorem B.1, which requires all circuits in $\mathcal{G}(\boldsymbol{P})$ to have non-positive weights, yields a set of bounds equivalent to the ones in (7). Consider a circuit $\pi = (i_1, i_2, \cdots, i_m, i_1)$, where $i_1, i_2 \cdots, i_m \in [K]$ are distinct, and $2 \leq m \leq K$. Then, (with modulo-m arithmetic being implicity used on the indices,)

$$0 \geq \omega(\pi) = \sum_{j=1}^{m} [\boldsymbol{P}]_{i_j i_{j-1}} \tag{76}$$

$$= \sum_{j=1}^{m} d_{i_j} - \bar{\alpha}_{i_j\sigma(i_j)} + \bar{\alpha}_{i_j\sigma(i_{j-1})}, \tag{77}$$

which gives a bound in (7). Since every circuit in $\mathcal{G}(\boldsymbol{P})$ yields a bound identical to the one of some permutation in Π_m ($m \in [2:K]$), and vice versa, the set of bounds that condition (a) gives is equivalent to the one formed by the bounds in (7).

Condition (b) in Theorem B.1 requires $\boldsymbol{q} \leq \boldsymbol{0}$ and $\boldsymbol{P}^k \otimes \boldsymbol{q} \leq \boldsymbol{0}$ for all $k \in [K-1]$. We divide this condition into two cases. The first case $\boldsymbol{q} \leq \boldsymbol{0}$ offers a set of the bounds equal to the one in (6), because for all $i \in [K]$

$$0 \geq [\boldsymbol{q}]_i = d_i - \bar{\alpha}_{i\sigma(i)}. \tag{78}$$

As for the other case, $\boldsymbol{P}^k \otimes \boldsymbol{q} \leq \boldsymbol{0}$ ($\forall k \in [K-1]$), it offers no tighter bounds than some linear combinations of multiple bounds in (6) and (7). As a result, this case is redundant. For example, consider a path $\pi = (i_1, i_2, \cdots, i_m)$, where $i_1, i_2, \cdots, i_m$ are distinct, and $2 \leq m \leq K$. Then

$$\omega(\pi) + [\boldsymbol{q}]_{i_1} = \sum_{j=2}^{m} [\boldsymbol{P}]_{i_j i_{j-1}} + [\boldsymbol{q}]_{i_1} \tag{79}$$

$$= \sum_{j=2}^{m} \left(d_{i_j} - \bar{\alpha}_{i_j \sigma(i_j)} + \bar{\alpha}_{i_j \sigma(i_{j-1})} \right) + \left(d_{i_j} - \bar{\alpha}_{i_j \sigma(i_j)} \right). \tag{80}$$

Moreover,

$$\omega(\pi) + [\boldsymbol{q}]_{i_1} \leq [\boldsymbol{P}^{m-1}]_{i_m i_1} \otimes [\boldsymbol{q}]_{i_1} \tag{81}$$

$$= [\boldsymbol{P}^{m-1} \otimes \boldsymbol{q}]_{i_m} \leq 0, \tag{82}$$

where (81) is because $[\boldsymbol{P}^n]_{ij}$ is the maximum path weight over all paths of length n from vertex j to i. The inequality in (82) holds because $\boldsymbol{P}^k \otimes \boldsymbol{q} \leq \boldsymbol{0}$ for $k \in [K-1]$. From (80) and (82) we find $\sum_{j=1}^{k} d_{i_j} \leq \bar{\alpha}_{i_1 \sigma(i_1)} + \sum_{j=2}^{k} \bar{\alpha}_{i_j \sigma(i_j)} - \bar{\alpha}_{i_j \sigma(i_{j-1})}$, which is looser than (77).

Note that condition (a) and (b) in Theorem B.1 yield the bounds on the GDoF tuples that are the same as those in $\bar{\mathcal{P}}_\sigma$. For every GDoF tuple in $\bar{\mathcal{P}}_\sigma$, we can find an $\boldsymbol{r} \leq \boldsymbol{0}$ satisfying the matrix equation in (77). As a result, every GDoF tuple in $\bar{\mathcal{P}}_\sigma$ is in $\mathcal{P}_\sigma^o$ as well, which concludes the proof.

Acknowledgment

The authors would like to thank Professor Francois Baccelli for pointing us toward max-plus algebra techniques for alternative proofs of optimality of TIN.

References

[1] R. H. Etkin, D. N. C. Tse, and H. Wang, "Gaussian interference channel capacity to within one bit," *IEEE Transactions on Information Theory*, vol. 54, pp. 5534–5562, Dec 2008.

[2] S. Karmakar and M. K. Varanasi, "The generalized degrees of freedom region of the MIMO interference channel and its achievability," *IEEE Trans. on Inf. Theory*, vol. 58, no. 12, pp. 7188–7203, 2012.

[3] S. Jafar and S. Vishwanath, "Generalized Degrees of Freedom of the Symmetric Gaussian K User Interference Channel," *IEEE Transactions on Information Theory*, vol. 56, pp. 3297–3303, July 2010.

[4] A. Avestimehr, S. Diggavi, C. Tian, and D. Tse, "An approximation approach to network information theory," in *Foundations and Trends in Communication and Information Theory*, vol. 12, pp. 1–183, 2015.

[5] S. Jafar, "Interference Alignment: A New Look at Signal Dimensions in a Communication Network," in *Foundations and Trends in Communication and Information Theory*, pp. 1–136, 2011.

[6] C. Geng, N. Naderializadeh, A. S. Avestimehr, and S. A. Jafar, "On the optimality of treating interference as noise," *IEEE Transactions on Information Theory*, vol. 61, pp. 1753–1767, Apr. 2015.

[7] C. Geng and S. A. Jafar, "On the optimality of treating interference as noise: General message sets," *IEEE Transactions on Information Theory*, vol. 61, pp. 3722–3736, July. 2015.

[8] H. Joudeh and B. Clerckx, "On the Optimality of Treating Inter-Cell Interference as Noise in Uplink Cellular Networks," *IEEE Transactions on Information Theory*, p. arXiv:1905.01283, 2019.

[9] Y.-C. Chan, J. Wang, and S. A. Jafar, "Towards an Extremal Network Theory – Robust GDoF Gain of Transmitter Cooperation over TIN," *arXiv e-prints*, p. arXiv:1901.09885, Jan 2019.

[10] C. Shannon, "Communication theory of secrecy systems," *Bell Systems Technical Journal*, Oct 1949.

[11] A. Wyner, "The wire-tap channel," *Bell Labs Technical Journal*, vol. 54, pp. 1355–1387, Oct. 1975.

[12] I. Csiszár and J. Korner, "Broadcast channels with confidential messages," *IEEE transactions on information theory*, vol. 24, no. 3, pp. 339–348, 1978.

[13] S. Leung-Yan-Cheong and M. Hellman, "The Gaussian wire-tap channel," *IEEE transactions on information theory*, vol. 24, no. 4, pp. 451–456, 1978.

[14] Y. Liang, H. V. Poor, and S. Shamai, "Information theoretic security," *Foundations and Trends in Communication and Information Theory*, pp. 355–580.

[15] H. D. Ty, T. Liu, and Y. Liang, "Multiple-input multiple-output Gaussian broadcast channels with common and confidential messages," *IEEE Transactions on Information Theory*, vol. 56, pp. 5477–5487, Nov 2010.

[16] R. Liu and V. Poor, "Secrecy capacity region of a multiple antenna Gaussian broadcast channel with confidential messages," *IEEE Transactions on Information Theory*, vol. 55, pp. 1235–1249, March 2009.

[17] Y. Liang and H. Poor, "Multiple access channels with confidential messages," *IEEE Transactions on Information Theory*, vol. 54, pp. 976–1002, March 2008.

[18] E. Ekrem and S. Ulukus, "The secrecy capacity region of the Gaussian MIMO multi-receiver wiretap channel," *IEEE Transactions on Information Theory*, vol. 57, pp. 2083–2114, April 2011.

[19] R. Liu, I. Maric, P. Spasojevic, and R. Yates, "Discrete memoryless interference and broadcast channels with confidential messages: secrecy rate regions," *IEEE Transactions on Information Theory*, vol. 54, pp. 2493–2507, June. 2008.

[20] Y. Liang, A. Somekh-Baruch, V. Poor, S. Shamai, and S. Verdu, "Capacity of cognitive interference channels with and without secrecy," *IEEE Transactions on Information Theory*, vol. 55, pp. 604–619, Feb. 2009.

[21] G. Bagherikaram, A. Motahari, and A. Khandani, "The secrecy capacity region of the Gaussian MIMO broadcast channel," *IEEE Transactions on Information Theory*, vol. 59, pp. 2673–2682, 5 2013.

[22] J. Xu, Y. Cao, and B. Chen, "Secure broadcasting over fading channels," *IEEE Transactions on Information Theory*, vol. 54, pp. 2453–2469, June 2008.

[23] E. Tekin and A. Yener, "The general Gaussian multiple-access and two-way wiretap channels: Achievable rates and cooperative jamming," *IEEE Transactions on Information Theory*, vol. 54, pp. 2735–2751, June 2008.

[24] E. Tekin and A. Yener, "The Gaussian multiple access wiretap channel," *IEEE Transactions on Information Theory*, vol. 54, pp. 5747–5755, Dec. 2008.

[25] J. Xu, Y. Cao, and B. Chen, "Capacity bounds for broadcast channels with confidential messages," *IEEE Transactions on Information Theory*, vol. 55, pp. 4529–4542, Oct. 2009.

[26] R. Yates, D. Tse, and Z. Li, "Secret communication over interference channels," *Proceedings of IEEE ISIT 2008*.

[27] R. Liu, T. Liu, H. Poor, and S. Shamai, "Multiple-input multiple-output gaussian broadcast channels with confidential messages," *IEEE Transactions on Information Theory*, vol. 56, pp. 4215–4227, Sep. 2010.

[28] X. He and A. Yener, "The Gaussian many-to-one interference channel with confidential messagess," *IEEE Transactions on Information Theory*, vol. 57, pp. 2730 – 2745, May 2011.

[29] O. O. Koyluoglu, H. El Gamal, L. Lai, and H. V. Poor, "Interference alignment for secrecy," *IEEE Transactions on Information Theory*, vol. 57, pp. 3323–3332, Jun. 2011.

[30] J. Xie and S. Ulukus, "Secure degrees of freedom of one-hop wireless networks," *IEEE Transactions on Information Theory*, vol. 60, pp. 3359–3378, June 2014.

[31] J. Xie and S. Ulukus, "Secure degrees of freedom of K-user Gaussian interference channels: A unified view," *IEEE Transactions on Information Theory*, vol. 61, pp. 2647–2661, May 2015.

[32] T. Gou and S. Jafar, "On the secure degrees of freedom of wireless X networks," in *Proceedings of 46th Annual Allerton Conference on Communication, Control and Computing*, Sep. 2008.

[33] C. Geng and S. A. Jafar, "Secure GDoF of K-user Gaussian interference channels: When secrecy incurs no penalty," *IEEE Communications Letters*, vol. 19, pp. 1287–1290, Aug. 2015.

[34] P. Mukherjee, J. Xie, and S. Ulukus, "Secure degrees of freedom of one-hop wireless networks with no eavesdropper CSIT," *IEEE Transactions on Information Theory*, vol. 63, pp. 1898–1922, Mar. 2017.

[35] S. Lashgari and A. S. Avestimehr, "Secrecy DoF of blind MIMOME wiretap channel with delayed CSIT," *IEEE Transactions on Information Forensics and Security*, vol. 13, pp. 478–489, Feb 2018.

[36] S. Lee and A. Khisti, "The wiretapped diamond-relay channel," *IEEE Transactions on Information Theory*, vol. 64, pp. 7194–7207, Nov 2018.

[37] A. Lapidoth, S. Shamai, and M. Wigger, "On the capacity of fading MIMO broadcast channels with imperfect transmitter side-information," in *Proceedings of 43rd Annual Allerton Conference on Communications, Control and Computing*, Sep. 28-30, 2005.

[38] C. Hao, B. Rassouli, and B. Clerckx, "Degrees-of-freedom region of MISO-OFDMA broadcast channel with imperfect CSIT," *arXiv:1310.6669*, October 2013.

[39] H. Weingarten, S. Shamai, and G. Kramer, "On the compound MIMO broadcast channel," in *Proceedings of Annual Information Theory and Applications Workshop UCSD*, Jan 2007.

[40] A. G. Davoodi and S. A. Jafar, "Aligned image sets under channel uncertainty: Settling conjectures on the collapse of degrees of freedom under finite precision CSIT," *IEEE Transactions on Information Theory*, vol. 62, pp. 5603–5618, Oct. 2016.

[41] A. G. Davoodi and S. A. Jafar, "Sum-set inequalities from aligned image sets: Instruments for robust GDoF bounds," *IEEE International Symposium on Information Theory (ISIT) 2017 (arXiv preprint arXiv:1703.01168)*, 2017.

[42] A. G. Davoodi and S. A. Jafar, "Generalized degrees of freedom of the symmetric K user interference channel under finite precision CSIT," *IEEE Transactions on Information Theory*, vol. 63, pp. 6561–6572, Aug. 2017.

[43] A. G. Davoodi and S. A. Jafar, "Transmitter cooperation under finite precision CSIT: A GDoF perspective," *IEEE Transactions on Information Theory*, vol. 63, pp. 6020–6030, Sep. 2017.

[44] A. G. Davoodi and S. A. Jafar, "Optimality of simple layered superposition coding in the 3-user MISO BC with finite precision CSIT," *CoRR*, vol. abs/1801.07419, 2018.

[45] B. Yuan, A. G. Davoodi, and S. A. Jafar, "DoF region of the MIMO interference channel with partial CSIT," in *2017 IEEE 18th International Workshop on Signal Processing Advances in Wireless Communications (SPAWC)*, pp. 1–5, July 2017.

[46] C. Hao, B. Rassouli, and B. Clerckx, "Achievable DoF regions of MIMO networks with imperfect CSIT," *IEEE Transactions on Information Theory*, vol. 63, no. 10, pp. 6587–6606, 2017.

[47] A. G. Davoodi, B. Yuan, and S. A. Jafar, "GDoF region of the MISO BC: Bridging the gap between finite precision and perfect CSIT," *IEEE Transactions on Information Theory*, vol. 64, pp. 7208–7217, Nov. 2018.

[48] A. G. Davoodi and S. A. Jafar, "Network coherence time matters – aligned image sets and the degrees of freedom of interference networks with finite precision CSIT and perfect CSIR," *IEEE Transactions on Information Theory*, vol. 64, pp. 7780–7791, Dec 2018.

[49] A. G. Davoodi and S. A. Jafar, ""K-user symmetric $M \times N$ MIMO interference channel under finite precision CSIT: A GDoF perspective," *IEEE Transactions on Information Theory*, vol. 65, pp. 1126–1136, Feb. 2019.

[50] H. Joudeh and B. Clerckx, "On the Separability of Parallel MISO Broadcast Channels Under Partial CSIT: A Degrees of Freedom Region Perspective," *arXiv e-prints*, p. arXiv:1905.01283, May 2019.

[51] J. Wang, B. Yuan, L. Huang, and S. A. Jafar, "GDoF of Interference Channel with Limited Cooperation under Finite Precision CSIT," *arXiv e-prints*, p. arXiv:1908.00703, Aug 2019.

[52] X. Yi and G. Caire, "Optimality of treating interference as noise: A combinatorial perspective," *IEEE Transactions on Information Theory*, vol. 62, pp. 4654–4673, Aug. 2016.

[53] C. Geng and S. A. Jafar, "On the optimality of treating interference as noise: Compound interference networks," *IEEE Transactions on Information Theory*, vol. 62, pp. 4630–4653, Aug. 2016.

[54] H. Weingarten, Y. Steinberg, and S. S. Shamai, "The capacity region of the gaussian multiple-input multiple-output broadcast channel," *IEEE Transactions on Information Theory*, vol. 52, pp. 3936–3964, Sep. 2006.

[55] C. Geng, R. Tandon, and S. A. Jafar, "On the symmetric 2-user deterministic interference channel with confidential messages," in *Global Communications Conference (GLOBECOM)*, pp. 1–6, Dec. 2015.

[56] J. Chen, "New results on the secure capacity of symmetric two-user interference channels," in *2016 54th Annual Allerton Conference on Communication, Control, and Computing (Allerton)*, pp. 524–531, Sep. 2016.

[57] A. G. Davoodi and S. A. Jafar, "K-user symmetric $M \times N$ MIMO interference channel under finite precision CSIT: A GDoF perspective," *IEEE Transactions on Information Theory*, vol. 65, pp. 1126–1136, Feb 2019.

[58] A. G. Davoodi and S. A. Jafar, "Degrees of Freedom Region of the (M, N_1, N_2) MIMO Broadcast Channel with Partial CSIT: An Application of Sum-set Inequalities Based on Aligned Image Sets," *arXiv e-prints*, p. arXiv:1901.06010, Jan 2019.

[59] F. Baccelli, G. Cohen, G. J. Olsder, and J.-P. Quadrat, *Synchronization and linearity: an algebra for discrete event systems*. John Wiley & Sons Ltd, 1992.