On the Symmetric 2-User Deterministic Interference Channel with Confidential Messages

Chunhua Geng*, Ravi Tandon†, and Syed A. Jafar*
* Center of Pervasive Communications and Computing, University of California Irvine, Irvine, CA
† Discovery Analytics Center, Department of Computer Science, Virginia Tech, Blacksburg, VA

***Abstract*—We consider 2-user symmetric interference channels with confidential messages. For the linear deterministic model of this channel, we develop inner and outer bounds for the symmetric secure rate, which are shown to match and characterize the symmetric secure capacity for a wide range of channel parameters. For the achievability, we present a cooperative jamming scheme based on interference alignment principle, which is optimal for all regimes where the symmetric secure capacity is established. For the converse, a tighter outer bound than all perviously existing ones is provided for the regime where the symmetric secure capacity is still open.**

I. Introduction

Information theoretic secrecy has been studied for decades in various channel models [1], [2], [3], [4], [5], [6]. Except for several special cases, the exact secure capacity for general Gaussian interference networks is still open. For instance, even for the 2-user symmetric Gaussian interference channel, the exact capacity, either with or without the secrecy constraints on unintended messages, is unknown in general. In the absence of the exact secure capacity, recent work has made significant progress on determining the secure degrees of freedom (DoF) of Gaussian interference networks [7], [8], [9]. However, DoF studies essentially assume all channels are equally strong (each non-zero channel is capable of carrying exactly one DoF), and therefore reveal little insight for settings with disparate channels strengths.

Recently, it has been extensively shown that a simple Avestimehr-Diggavi-Tse (ADT) linear deterministic model [10] can help study Gaussian interference networks, leading to generalized degrees of freedom (GDoF) results or even approximate capacity results at finite SNRs [11], [12], [13], [14], [15]. Following this research direction, in this work we consider the ADT model of the canonical 2-user symmetric interference channel with confidential messages. We develop inner and outer bounds for the symmetric secure rate, which are matched for a wide range of channel parameters.

For the achievability, a cooperative jamming scheme based on signal level interference alignment principle is developed, where besides sending out its own useful data signals, each transmitter also generates random jamming signals for secrecy. For the common part of the useful data of either user (which can be seen by both receivers), we align it with the jamming signals at its unintended receiver to guarantee secrecy, while make sure that it is distinguishable from the jamming signals (and other interference) at its legitimate receiver and thus decodable.

For the converse, in the regime where the symmetric secure capacity is still open, a new outer bound is provided, which is tighter than all previously known ones.

Regarding notations, throughout this work we use $\mathbf{I}_m$ to denote the $m \times m$ identity matrix, $\mathbf{O}_{m\times n}$ to denote the $m \times n$ zero matrix, whose entries are all zeros, and $\mathcal{F}_2^q$ to denote the set of q-tuples of binary numbers.

II. Channel Model

Consider the 2-user symmetric ADT linear deterministic interference channel with the input-output relationship

$$\mathbf{Y}_1(t) = \mathbf{S}^{q-n_d}\mathbf{X}_1(t) + \mathbf{S}^{q-n_c}\mathbf{X}_2(t) \tag{1}$$

$$\mathbf{Y}_2(t) = \mathbf{S}^{q-n_c}\mathbf{X}_1(t) + \mathbf{S}^{q-n_d}\mathbf{X}_2(t), \tag{2}$$

where the summations and multiplications are over $\mathcal{F}_2$, n_d and n_c are both non-negative integers, $q \triangleq \max\{n_d, n_c\}$, $\mathbf{X}_i(t), \mathbf{Y}_i(t) \in \mathcal{F}_2^q$, and $\mathbf{S}$ is a $q \times q$ shift matrix

$$\mathbf{S} = \begin{bmatrix} 0 & 0 & 0 & ... & 0 & 0 \\ 1 & 0 & 0 & ... & 0 & 0 \\ 0 & 1 & 0 & ... & 0 & 0 \\ \vdots & & & \ddots & \vdots & 0 \\ 0 & 0 & 0 & ... & 1 & 0 \end{bmatrix}. \tag{3}$$

In the symmetric ADT interference channel, n_d is the number of *direct* signal levels (from Transmitter i to Receiver i, $i \in \{1,2\}$), and n_c is the number of *cross* signal levels (from Ttransmitter i to Receiver j, $i, j \in \{1,2\}, i \neq j$). Also define

$$\alpha \triangleq \frac{n_c}{n_d} \tag{4}$$

as the normalized interference parameter.

In the 2-user ADT interference channel, Transmitter $i \in \{1,2\}$ intends to deliver a message W_i to Receiver i. Each message W_i is uniformly distributed over the message set $\mathcal{W}_i$. The size of the message set $\mathcal{W}_i$ is denoted by $|\mathcal{W}_i|$. Transmitter i uses an encoding function $f_i : \mathcal{W}_i \to \mathbf{X}_i^T$ to encode the message, where $\mathbf{X}_i^T \triangleq [\mathbf{X}_i(1), \mathbf{X}_i(2), ..., \mathbf{X}_i(T)]$ is the channel input of Transmitter i with length T. Receiver i decodes its own message as $\hat{W}_i$ based on the channel output. A secure rate tuple (R_1, R_2), where $R_i = \frac{\log|\mathcal{W}_i|}{T}$, is achievable if for any $\epsilon > 0$, there exist T-length codes such that the decoding error probabilities at both receivers are less than ϵ, i.e.,

$$\max_{i\in\{1,2\}} \Pr\big(W_i \neq \hat{W}_i\big) \leq \epsilon \tag{5}$$

and the following secrecy constraints are satisfied simultaneously

$$H(W_1|\mathbf{Y}_2^T) \geq H(W_1) - T\epsilon \tag{6}$$
$$H(W_2|\mathbf{Y}_1^T) \geq H(W_2) - T\epsilon \tag{7}$$

The secure capacity region $\mathcal{C}_s$ is the closure of the set of all the achievable secure rate tuples, and the symmetric secure rate is defined as

$$R_s \triangleq \max\{R : (R,R) \in \mathcal{C}_s\}. \tag{8}$$

III. Main Results

The main results are presented in the following theorems.

Theorem 1: (Achievability) For the 2-user symmetric ADT interference channel, the following normalized symmetric secure rate is achievable

$$\frac{R_s}{n_d} = \begin{cases} 1-\alpha, & 0 \leq \alpha \leq \frac{2}{3} \\ 2\alpha - 1, & \frac{2}{3} < \alpha \leq \frac{3}{4} \\ 1 - \frac{2\alpha}{3}, & \frac{3}{4} < \alpha < 1 \\ 0, & \alpha = 1 \\ \frac{\alpha}{3}, & 1 < \alpha < \frac{3}{2} \\ 2-\alpha, & \frac{3}{2} \leq \alpha < 2 \\ 0, & \alpha \geq 2 \end{cases} \tag{9}$$

Proof: See Section IV.

Theorem 2: (Converse) For the 2-user symmetric ADT interference channel, the normalized symmetric secure rate is upper bounded by

$$\frac{R_s}{n_d} \leq \begin{cases} 1-\alpha, & 0 \leq \alpha \leq \frac{1}{2} \\ \frac{1}{2}, & \frac{1}{2} < \alpha \leq \frac{3}{4} \\ 1 - \frac{2\alpha}{3}, & \frac{3}{4} < \alpha < 1 \\ 0, & \alpha = 1 \\ \frac{\alpha}{3}, & 1 < \alpha < \frac{3}{2} \\ 2-\alpha, & \frac{3}{2} \leq \alpha < 2 \\ 0, & \alpha \geq 2 \end{cases} \tag{10}$$

Proof: See Section V.

Remark 1: For the sake of illustration, the derived inner and outer bounds of the normalized symmetric secure rate $\frac{R_s}{n_d}$, and the well-known "W" curve in [11] (the normalized symmetric capacity for the case without any security constraints) are depicted in Fig. 1. One can find that except for the regime $\frac{1}{2} < \alpha < \frac{3}{4}$, the inner and outer bounds are matched, hence leading to the optimal characterization of the symmetric secure capacity.

Remark 2: Note that for the regime $0 \leq \alpha \leq \frac{1}{2}$ the secrecy constraint does not incur any capacity penalty. In the corresponding symmetric Gaussian interference channels, this is the regime where using Gaussian channel inputs and treating interference as noise (TIN) is optimal from the GDoF perspective [11], [16]. Remarkably, a broad TIN-optimal regime is identified for the K user fully asymmetric Gaussian interference channel in [16] and is also shown from a GDoF perspective to suffer no loss due to secrecy constraints in [17].

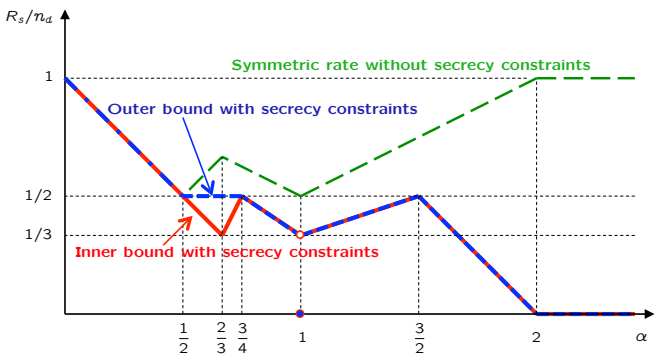

Fig. 1. Inner and outer bounds on the normalized symmetric secure rate.

IV. Proof of Theorem 1

To achieve the symmetric secure rate given in Theorem 1, a cooperative jamming scheme based on interference alignment principle is adopted, where the jamming signals are designed to align with the unintended data signals at each receiver to guarantee secrecy. We first describe the common aspect of the transmission scheme. Let the transmit signals $\mathbf{X}_1$,$\mathbf{X}_2 \in \mathcal{F}_2^q$ be

$$\mathbf{X}_1 = \mathbf{V}_{1,p}\hat{\mathbf{X}}_{1,p} + \mathbf{V}_{1,c}\hat{\mathbf{X}}_{1,c} + \mathbf{V}_{1,j}\hat{\mathbf{X}}_{1,j} \tag{11}$$
$$\mathbf{X}_2 = \mathbf{V}_{2,p}\hat{\mathbf{X}}_{2,p} + \mathbf{V}_{2,c}\hat{\mathbf{X}}_{2,c} + \mathbf{V}_{2,j}\hat{\mathbf{X}}_{2,j} \tag{12}$$

where for $i \in \{1,2\}$, the column vectors of the matrix

- $\mathbf{V}_{i,p}$ are precoding vectors for the private part of the data signal $\hat{\mathbf{X}}_{i,p}$
- $\mathbf{V}_{i,c}$ are precoding vectors for the common part of the data signal $\hat{\mathbf{X}}_{i,c}$
- $\mathbf{V}_{i,j}$ are precoding vectors for the jamming signal $\hat{\mathbf{X}}_{i,j}$

of User i, respectively. Specifically, the precoding vectors are designed such that the private part of the transmit data $\hat{\mathbf{X}}_{i,p}$ can only be seen by its desired Receiver i, the common part of the transmit data $\hat{\mathbf{X}}_{i,c}$ are received by both receivers, and the jamming signals $\hat{\mathbf{X}}_{i,j}$ are aligned with the unintended data signals to guarantee secrecy. The elements of the column vectors $\hat{\mathbf{X}}_{i,p}$ and $\hat{\mathbf{X}}_{i,c}$ are from i.i.d. binary source of the corresponding message W_i, and the elements of the column vector $\hat{\mathbf{X}}_{i,j}$ are from i.i.d. binary source following the Bernoulli distribution $Bern(1, \frac{1}{2})$. Clearly, the jamming signals $\hat{\mathbf{X}}_{i,j}$ are independent with the data signals $\hat{\mathbf{X}}_{i,p}$ and $\hat{\mathbf{X}}_{i,c}$.

Note that only when $n_d > n_c$, we can send private transmit data to its legitimate receiver while keep the unintended receiver from receiving it, i.e., the construction of $\mathbf{V}_{i,p}$ is related to the null space of the channel matrix $\mathbf{S}^{n_d-n_c}$. Thus when $n_d > n_c$, we let

$$\mathbf{V}_{i,p} = \begin{bmatrix} \mathbf{O}_{n_c \times (n_d-n_c)} \\ \mathbf{I}_{n_d-n_c} \end{bmatrix}_{n_d \times (n_d-n_c)} \tag{13}$$

In words, each of the least significant $n_d - n_c$ signal levels of $\mathbf{X}_i$ is used to carry one bit of the private transmit data. Since these signal levels are not received by the unintended receiver, the data transmitted over these levels is always kept secret.

In this following, we give the specific design of the transmission scheme for each regime.

A. $0 \le \alpha \le \frac{2}{3}$

In this regime, Transmitter $i \in \{1,2\}$ only sends the private transmit data $\hat{\mathbf{X}}_{i,p}$ over the least significant $n_d - n_c$ signal levels, i.e.,

$$\mathbf{X}_i = \mathbf{V}_{i,p}\hat{\mathbf{X}}_{i,p} \tag{14}$$

Apparently, the transmit data can only be seen by its intended receiver and thus kept secret. Since each user achieves $(n_d - n_c)$ bits, the normalized symmetric secure rate is $1-\alpha$.

B. $\frac{2}{3} < \alpha \le \frac{3}{4}$

In this regime, for $i,k \in \{1,2\}$ and $i \ne k$, let

$$\mathbf{V}_{i,c} = \mathbf{V}_{k,c} = \begin{bmatrix} \mathbf{I}_{3n_c-2n_d} \\ \mathbf{O}_{3(n_d-n_c)\times(3n_c-2n_d)} \end{bmatrix}_{n_d\times(3n_c-2n_d)} \tag{15}$$

and

$$\mathbf{V}_{i,j} = \mathbf{V}_{k,j} = \begin{bmatrix} \mathbf{O}_{(n_d-n_c)\times(3n_c-2n_d)} \\ \mathbf{I}_{3n_c-2n_d} \\ \mathbf{O}_{2(n_d-n_c)\times(3n_c-2n_d)} \end{bmatrix}_{n_d\times(3n_c-2n_d)} \tag{16}$$

Note that $\mathbf{V}_{i,j} = \mathbf{S}^{n_d-n_c}\mathbf{V}_{k,c}$. The received signal of Receiver i is

$$\begin{aligned}\mathbf{Y}_i =& \mathbf{X}_i + \mathbf{S}^{n_d-n_c}\mathbf{X}_k \\ =& (\mathbf{V}_{i,p}\hat{\mathbf{X}}_{i,p} + \mathbf{V}_{i,c}\hat{\mathbf{X}}_{i,c} + \mathbf{V}_{i,j}\hat{\mathbf{X}}_{i,j}) \\ &+ \mathbf{S}^{n_d-n_c}(\mathbf{V}_{k,c}\hat{\mathbf{X}}_{k,c} + \mathbf{V}_{k,j}\hat{\mathbf{X}}_{k,j}) \qquad (17)\\ =& \mathbf{V}_{i,p}\hat{\mathbf{X}}_{i,p} + \mathbf{V}_{i,c}\hat{\mathbf{X}}_{i,c} + \tilde{\mathbf{V}}_k\hat{\mathbf{X}}_{k,j} + \mathbf{V}_{i,j}(\hat{\mathbf{X}}_{k,c} + \hat{\mathbf{X}}_{i,j}) \qquad (18)\end{aligned}$$

where

$$\begin{aligned}\tilde{\mathbf{V}}_k &= \mathbf{S}^{n_d-n_c}\mathbf{V}_{k,j} \\ &= \begin{bmatrix} \mathbf{O}_{2(n_d-n_c)\times(3n_c-2n_d)} \\ \mathbf{I}_{3n_c-2n_d} \\ \mathbf{O}_{(n_d-n_c)\times(3n_c-2n_d)} \end{bmatrix}_{n_d\times(3n_c-2n_d)}\end{aligned} \tag{19}$$

In (18), the first two terms correspond to the desired data of User i, and the last term indicates that the unintended data signals from User k are aligned with the jamming signals from User i. Denote by $\mathcal{L}_i$ the set of the signal levels of User i where the unintended data signals are aligned with the jamming signals. Without loss of generality, consider one signal level $l \in \mathcal{L}_i$. Denote by $Y_{i,l}$, $D_{k,l}$, and $J_{i,l}$ the received signal, the unintended data signal from User k, and the jamming signal from User i over the level l, respectively. We have

$$Y_{i,l} = D_{k,l} + J_{i,l} \tag{20}$$

According to the chain rule, we obtain

$$\begin{aligned}H(D_{k,l}, Y_{i,l}) =& H(D_{k,l}) + H(Y_{i,l}|D_{k,l}) && (21)\\ =& H(D_{k,l}) + H(J_{i,l}) && (22)\\ =& H(D_{k,l}) + 1 && (23)\end{aligned}$$

and

$$\begin{aligned}H(D_{k,l}, Y_{i,l}) =& H(Y_{i,l}) + H(D_{k,l}|Y_{i,l}) && (24)\\ =& H(D_{k,l}|Y_{i,l}) + 1 && (25)\end{aligned}$$

Thus

$$H(D_{k,l}) = H(D_{k,l}|Y_{i,l}) \tag{26}$$

which indicates that over the signal level l of User i, the unintended data signal $D_{k,l}$ is kept secret from User i information-theoretically. Applying the same argument for all the signal levels in $\mathcal{L}_i$ together, it is not hard to establish that the secrecy constraints (6) and (7) are satisfied.

From (18), it is easy to verify that when $\frac{2}{3} < \alpha \le \frac{3}{4}$, the desired data signals of User i (i.e., $\hat{\mathbf{X}}_{i,c}$ and $\hat{\mathbf{X}}_{i,p}$) are not interfered by other signals at Receiver i and thus decodable. Note that $\hat{\mathbf{X}}_{i,c}$ and $\hat{\mathbf{X}}_{i,p}$ carries $3n_c - 2n_d$ and $n_d - n_c$ bits, respectively. The resulting normalized symmetric secure rate is $[(3n_c - 2n_d) + (n_d - n_c)]/n_d = 2\alpha - 1$.

C. $\frac{3}{4} < \alpha < 1$

For simplicity of exposition, in this regime we first consider the case where n_c is a multiple of 3 to avoid fractional rates. Construct the precoding vectors through a matrix $\mathbf{V} \in \mathcal{F}^{n_d\times\frac{n_c}{3}}$. For $i,k \in \{1,2\}$ and $i \ne k$, let

$$\mathbf{V}_{i,c} = \mathbf{V}_{k,c} = \mathbf{V} \tag{27}$$

$$\mathbf{V}_{i,j} = \mathbf{V}_{k,j} = \mathbf{S}^{n_d-n_c}\mathbf{V} \tag{28}$$

Then the transmit signal of User i is

$$\mathbf{X}_i = \mathbf{V}_{i,p}\hat{\mathbf{X}}_{i,p} + \mathbf{V}\hat{\mathbf{X}}_{i,c} + \mathbf{S}^{n_d-n_c}\mathbf{V}\hat{\mathbf{X}}_{i,j} \tag{29}$$

and the received signal of Receiver i is given by

$$\begin{aligned}\mathbf{Y}_i =& \mathbf{X}_i + \mathbf{S}^{n_d-n_c}\mathbf{X}_k \\ =& \mathbf{V}_{i,p}\hat{\mathbf{X}}_{i,p} + \mathbf{V}\hat{\mathbf{X}}_{i,c} + \mathbf{S}^{2(n_d-n_c)}\mathbf{V}\hat{\mathbf{X}}_{k,j} \\ &+ \mathbf{S}^{n_d-n_c}\mathbf{V}(\hat{\mathbf{X}}_{k,c} + \hat{\mathbf{X}}_{i,j})\end{aligned} \tag{30}$$

where the first two terms in (30) correspond to the desired data of User i, and the last term shows that the unintended data signals from User k are aligned with the jamming signals from User i and thus kept secret.

Next, we invoke the following lemma to complete the achievability proof.

Lemma 1: (Lemma 4.2 in [14]) Let n_c be an integer that is a multiple of 3, and n_d be an integer such that $\frac{3}{4} < \frac{n_c}{n_d} < 1$. Then there exists a matrix $\mathbf{V} \in \mathcal{F}^{n_d\times\frac{n_c}{3}}$ such that

$$\mathrm{rank}([\mathbf{V} \;\; \mathbf{S}^{n_d-n_c}\mathbf{V} \;\; \mathbf{S}^{2(n_d-n_c)}\mathbf{V} \;\; \mathbf{V}_{\mathrm{null}}]_{n_d\times n_d}) = n_d \tag{31}$$

where $\mathbf{V}_{\mathrm{null}} = \mathbf{V}_{i,p} \in \mathcal{F}_2^{n_d\times(n_d-n_c)}$, whose column vectors form a basis for the null space of the shift matrix $\mathbf{S}^{n_d-n_c}$.

According to Lemma 1, from (30) Receiver i can decode its desired message by linear decoding. Note that the first and second terms in (30) carry $n_d - n_c$ and $\frac{n_c}{3}$ bits, respectively. The resulting normalized symmetric secure rate is $(n_d - n_c + \frac{n_c}{3})/n_d = 1 - \frac{2\alpha}{3}$.

For the case where n_c is not a multiple of 3, the argument is essentially the same. The only difference is that to deal with fractional rates, we use a three-symbol extension and obtain an extended channel

$$\bar{\mathbf{Y}}_i = \bar{\mathbf{X}}_i + \bar{\mathbf{H}}\bar{\mathbf{X}}_k \tag{32}$$

where

$$\bar{\mathbf{Y}}_i = \begin{bmatrix} \mathbf{Y}_i(3t) \\ \mathbf{Y}_i(3t+1) \\ \mathbf{Y}_i(3t+2) \end{bmatrix} \qquad \bar{\mathbf{X}}_i = \begin{bmatrix} \mathbf{X}_i(3t) \\ \mathbf{X}_i(3t+1) \\ \mathbf{X}_i(3t+2) \end{bmatrix} \tag{33}$$

$$\bar{\mathbf{H}} = \begin{bmatrix} \mathbf{S}^{n_d-n_c} & \mathbf{O}_{n_d\times n_d} & \mathbf{O}_{n_d\times n_d} \\ \mathbf{O}_{n_d\times n_d} & \mathbf{S}^{n_d-n_c} & \mathbf{O}_{n_d\times n_d} \\ \mathbf{O}_{n_d\times n_d} & \mathbf{O}_{n_d\times n_d} & \mathbf{S}^{n_d-n_c} \end{bmatrix}_{3n_d\times 3n_d} \tag{34}$$

and $i,k\in\{1,2\}$, $i\neq k$. In this extended channel, the inputs and outputs are symbols over $\mathcal{F}_2^{3n_d}$. Like the case where n_c is a multiple of 3, we use a matrix $\bar{\mathbf{V}}\in\mathcal{F}_2^{3n_d\times n_c}$ to construct the precoding vectors. Following the similar argument given above, it is easy to show that at each receiver, the unintended data signals are aligned with the jamming signals and thus kept secret. Finally, it remains to show that there exists a matrix $\bar{\mathbf{V}}$ such that

$$\mathrm{rank}([\bar{\mathbf{V}} \;\; \bar{\mathbf{H}}\bar{\mathbf{V}} \;\; \bar{\mathbf{H}}^2\bar{\mathbf{V}} \;\; \bar{\mathbf{V}}_{\mathrm{null}}]_{3n_d\times 3n_d}) = 3n_d \tag{35}$$

to guarantee the messages are decodable at their legitimate receivers, where the column vectors of $\bar{\mathbf{V}}_{\mathrm{null}}\in\mathcal{F}^{3n_d\times(3n_d-3n_c)}$ form a basis for the null space of $\bar{\mathbf{H}}$. The following lemma in [14] helps complete the proof.

Lemma 2: (Lemma 4.3 in [14]) Let n_c and n_d be integers such that $\frac{3}{4}<\frac{n_c}{n_d}<1$. Then there exists a matrix $\bar{\mathbf{V}}\in\mathcal{F}^{3n_d\times n_c}$ such that

$$\mathrm{rank}([\bar{\mathbf{V}} \;\; \bar{\mathbf{H}}\bar{\mathbf{V}} \;\; \bar{\mathbf{H}}^2\bar{\mathbf{V}} \;\; \bar{\mathbf{V}}_{\mathrm{null}}]_{3n_d\times 3n_d}) = 3n_d \tag{36}$$

D. $1<\alpha<\frac{3}{2}$

Similar to the regime $\frac{3}{4}<\alpha<1$, we first consider the case where n_c is a multiple of 3. For $i,k\in\{1,2\}$ and $i\neq k$, we construct the precoding vectors through a matrix $\mathbf{V}\in\mathcal{F}^{n_c\times\frac{n_c}{3}}$ and let

$$\mathbf{V}_{i,c} = \mathbf{V}_{k,c} = \mathbf{S}^{n_c-n_d}\mathbf{V} \tag{37}$$

$$\mathbf{V}_{i,j} = \mathbf{V}_{k,j} = \mathbf{V} \tag{38}$$

Recall that when $\alpha>1$ (i.e., $n_d<n_c$), there are no private signal levels which can only be seen by the intended receiver. Thus the transmit signals contain no private data. The transmit signal of User i is

$$\mathbf{X}_i = \mathbf{S}^{n_c-n_d}\mathbf{V}\hat{\mathbf{X}}_{i,c} + \mathbf{V}\hat{\mathbf{X}}_{i,j} \tag{39}$$

and the received signal of Receiver i is given by

$$\begin{aligned}\mathbf{Y}_i &= \mathbf{S}^{n_c-n_d}\mathbf{X}_i + \mathbf{X}_k \\ &= \mathbf{S}^{2(n_c-n_d)}\mathbf{V}\hat{\mathbf{X}}_{i,c} + \mathbf{V}\hat{\mathbf{X}}_{k,j} + \mathbf{S}^{n_c-n_d}\mathbf{V}(\hat{\mathbf{X}}_{i,j}+\hat{\mathbf{X}}_{k,c})\end{aligned} \tag{40}$$

where the first term in (40) corresponds to the desired data of User i, and the last term indicates that the unintended data signals from User k are aligned with the jamming signals from User i and thus kept secret. We have the following lemma to get the desired secure rate.

Lemma 3: Let n_c be an integer that is a multiple of 3, and n_d be an integer such that $1<\frac{n_c}{n_d}<\frac{3}{2}$. Then there exists a matrix $\mathbf{V}\in\mathcal{F}^{n_c\times\frac{n_c}{3}}$ such that

$$\mathrm{rank}([\mathbf{V} \;\; \mathbf{S}^{n_c-n_d}\mathbf{V} \;\; \mathbf{S}^{2(n_c-n_d)}\mathbf{V}]_{n_c\times n_c}) = n_c \tag{41}$$

Proof: The proof of Lemma 3 is essentially the same as that of Lemma 1 and thus omitted due to limited space.

Lemma 3 guarantees that from (40) Receiver i can decode its desired message. Since the first term in (40) carries $\frac{n_c}{3}$ bits, the resulting normalized symmetric secure rate is $\frac{n_c}{3n_d}=\frac{\alpha}{3}$.

For the case where n_c is not a multiple of 3, we also use a three-symbol extension to deal with fractional rates. We construct the precoding vectors based on a matrix $\bar{\mathbf{V}}\in\mathcal{F}_2^{3n_c\times n_c}$. The left procedure is similar to the case where n_c is a multiple of 3. We omit the details due to the space limit. Just note to guarantee that the legitimate receiver can decode its own message, we need the following lemma.

Lemma 4: Let n_c and n_d be integers such that $1<\frac{n_c}{n_d}<\frac{3}{2}$. Then there exists a matrix $\bar{\mathbf{V}}\in\mathcal{F}^{3n_c\times n_c}$ such that

$$\mathrm{rank}([\bar{\mathbf{V}} \;\; \tilde{\mathbf{H}}\bar{\mathbf{V}} \;\; \tilde{\mathbf{H}}^2\bar{\mathbf{V}}]_{3n_c\times 3n_c}) = 3n_c \tag{42}$$

where

$$\tilde{\mathbf{H}} = \begin{bmatrix} \mathbf{S}^{n_c-n_d} & \mathbf{O}_{n_c\times n_c} & \mathbf{O}_{n_c\times n_c} \\ \mathbf{O}_{n_c\times n_c} & \mathbf{S}^{n_c-n_d} & \mathbf{O}_{n_c\times n_c} \\ \mathbf{O}_{n_c\times n_c} & \mathbf{O}_{n_c\times n_c} & \mathbf{S}^{n_c-n_d} \end{bmatrix}_{3n_c\times 3n_c} \tag{43}$$

Proof: The proof of Lemma 4 is an extension of the proof of Lemma 3 and omitted due to limited space.

Example 1: The achievable scheme for the 2-user symmetric ADT interference channel with $n_d=9$ and $n_c=12$ is illustrated in Fig. 2. It is not hard to verify that at each receiver, the unintended data signals from the other user are aligned with the jamming signal from its own transmitter and thus kept secret, and its desired data signals are all decodable.

E. $\frac{3}{2}\leq\alpha<2$

In this regime, for $i,k\in\{1,2\}$ and $i\neq k$, let

$$\mathbf{V}_{i,j} = \mathbf{V}_{k,j} = \begin{bmatrix} \mathbf{I}_{2n_d-n_c} \\ \mathbf{O}_{2(n_c-n_d)\times(2n_d-n_c)} \end{bmatrix}_{n_c\times(2n_d-n_c)} \tag{44}$$

and

$$\mathbf{V}_{i,c} = \mathbf{V}_{k,c} = \begin{bmatrix} \mathbf{O}_{(n_c-n_d)\times(2n_d-n_c)} \\ \mathbf{I}_{2n_d-n_c} \\ \mathbf{O}_{(n_c-n_d)\times(2n_d-n_c)} \end{bmatrix}_{n_c\times(2n_d-n_c)} \tag{45}$$

Note $\mathbf{V}_{k,c}=\mathbf{S}^{n_c-n_d}\mathbf{V}_{i,j}$. The received signal of Receiver i is

$$\begin{aligned}\mathbf{Y}_i =& \mathbf{S}^{n_c-n_d}\mathbf{X}_i + \mathbf{X}_k \\ =& \mathbf{S}^{n_c-n_d}(\mathbf{V}_{i,c}\hat{\mathbf{X}}_{i,c} + \mathbf{V}_{i,j}\hat{\mathbf{X}}_{i,j}) \\ &+ (\mathbf{V}_{k,c}\hat{\mathbf{X}}_{k,c} + \mathbf{V}_{k,j}\hat{\mathbf{X}}_{k,j}) \qquad (46) \\ =& \hat{\mathbf{V}}_i\hat{\mathbf{X}}_{i,c} + \mathbf{V}_{k,j}\hat{\mathbf{X}}_{k,j} + \mathbf{V}_{k,c}(\hat{\mathbf{X}}_{k,c}+\hat{\mathbf{X}}_{i,j}) \qquad (47)\end{aligned}$$

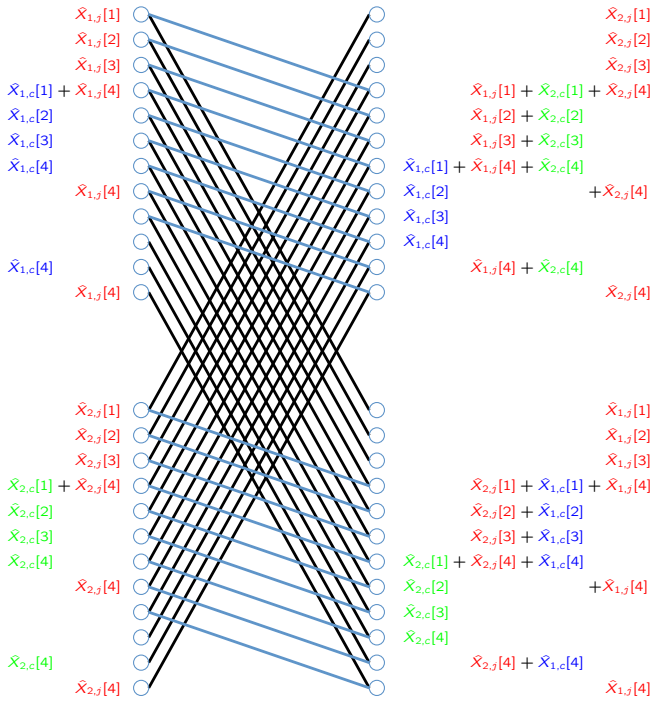

Fig. 2. The achievable scheme for the 2-user symmetric ADT interference channel with $n_d = 9$ and $n_c = 12$, where the secure rate of each user is 4.

where

$$\hat{\mathbf{V}}_i = \mathbf{S}^{n_c-n_d}\mathbf{V}_{i,c} = \begin{bmatrix} \mathbf{O}_{2(n_c-n_d)\times(2n_d-n_c)} \\ \mathbf{I}_{2n_d-n_c} \end{bmatrix}_{n_c\times(2n_d-n_c)} \tag{48}$$

In (47), the first term corresponds to the desired data of User i, and the last term shows that the unintended data signals from User k are aligned with the jamming signals from User i and thus kept secret. It is easy to verify that when $\frac{3}{2} \le \alpha < 2$, the desired data are not interfered by other signals and thus the desired message can be decoded at its legitimate receiver. The resulting normalized symmetric secure rate is $(2n_d-n_c)/n_d = 2-\alpha$.

V. Proof of Theorem 2

For the converse, we first consider the regime $0 \le \alpha \le \frac{1}{2}$. In this regime, the capacity of the 2-user symmetric interference channel without secrecy constraint [11], [12] serves as the desired outer bound straightforwardly. We also notice that in [15], the authors consider a 2-user symmetric interference channel with confidential messages and transmitter cooperations, and derive outer bounds for this channel. Based on the converse results in [15], by setting the capacity of the cooperative link between transmitters as 0, we obtain the desired outer bound for $\alpha \ge \frac{3}{4}$.

In the following, for the remaining regime $\frac{1}{2} < \alpha < \frac{3}{4}$, we provide a tighter outer bound than all previously known ones, i.e., $R_s \le \frac{n_d}{2}$. Before starting, define

$$\mathbf{S}_1(t) \triangleq \mathbf{X}_1^{\text{top } n_c}(t), \quad \mathbf{S}_2(t) \triangleq \mathbf{X}_2^{\text{top } n_c}(t)$$

In words, $\mathbf{S}_i(t)$, $i \in \{1,2\}$, is the input of Transmitter i in the top n_c signal levels (which cause interference at the other receiver). To prove the desired outer bound, we start with Fano's inequality and have the following set of inequalities

$$\begin{aligned}
&T(R_1-\epsilon_0) \\
&\le I(W_1;\mathbf{Y}_1^T) && (49)\\
&\le I(W_1;\mathbf{Y}_1^T,\mathbf{S}_1^T) && (50)\\
&= I(W_1;\mathbf{S}_1^T) + I(W_1;\mathbf{Y}_1^T|\mathbf{S}_1^T) && (51)\\
&= H(\mathbf{S}_1^T) + H(\mathbf{Y}_1^T|\mathbf{S}_1^T) - H(\mathbf{Y}_1^T|\mathbf{S}_1^T,W_1) - H(\mathbf{S}_1^T|W_1) && (52)\\
&\le H(\mathbf{S}_1^T) + H(\mathbf{Y}_1^T|\mathbf{S}_1^T) - H(\mathbf{Y}_1^T|\mathbf{X}_1^T,W_1) - H(\mathbf{S}_1^T|W_1) && (53)\\
&= H(\mathbf{S}_1^T) + H(\mathbf{Y}_1^T|\mathbf{S}_1^T) - H(\mathbf{S}_2^T) - H(\mathbf{S}_1^T|W_1) && (54)\\
&\le H(\mathbf{S}_1^T) + \sum_{t=1}^{T} H(\mathbf{Y}_1(t)|\mathbf{S}_1(t)) - H(\mathbf{S}_2^T) - H(\mathbf{S}_1^T|W_1) && (55)\\
&\le H(\mathbf{S}_1^T) + Tn_c - H(\mathbf{S}_2^T) - H(\mathbf{S}_1^T|W_1) && (56)
\end{aligned}$$

where (55) follows chain rule and the fact that dropping conditioning does not reduce entropy, and in the last inequality (56), we use the fact that $\alpha = \frac{n_c}{n_d} > \frac{1}{2}$, or in other words $n_c > (n_d - n_c)$. The top $(n_d - n_c)$ elements of $\mathbf{Y}_1(t)$ (which are interference free) are exactly the same as the top (n_d-n_c) elements of $\mathbf{S}_1(t)$ for each time t. Hence, the bound on $H(\mathbf{Y}_1(t)|\mathbf{S}_1(t)) \le n_c$ follows directly.

By symmetry, we have

$$T(R_2-\epsilon_0) \le H(\mathbf{S}_2^T) + Tn_c - H(\mathbf{S}_1^T) - H(\mathbf{S}_2^T|W_2) \tag{57}$$

Adding (56) and (57), we end up with

$$T(R_1+R_2-2\epsilon_0) \le 2Tn_c - H(\mathbf{S}_1^T|W_1) - H(\mathbf{S}_2^T|W_2) \tag{58}$$

Next, we incorporate the secrecy constraint for message W_1 as follows

$$\begin{aligned}
&T(R_1-\epsilon_0) \\
&\le I(W_1;\mathbf{Y}_1^T,\mathbf{Y}_2^T,W_2) && (59)\\
&= I(W_1;\mathbf{Y}_1^T|\mathbf{Y}_2^T,W_2) + I(W_1;\mathbf{Y}_2^T,W_2) && (60)\\
&\le I(W_1;\mathbf{Y}_1^T|\mathbf{Y}_2^T,W_2) + T\epsilon && (61)\\
&= H(\mathbf{Y}_1^T|\mathbf{Y}_2^T,W_2) - H(\mathbf{Y}_1^T|\mathbf{Y}_2^T,W_1,W_2) + T\epsilon && (62)\\
&\le H(\mathbf{Y}_1^T|\mathbf{Y}_2^T,W_2) - H(\mathbf{Y}_1^T|\mathbf{Y}_2^T,\mathbf{X}_2^T,W_1,W_2) + T\epsilon && (63)\\
&= H(\mathbf{Y}_1^T|\mathbf{Y}_2^T,W_2) - H(\mathbf{X}_1^T|\mathbf{S}_1^T,\mathbf{X}_2^T,W_1,W_2) + T\epsilon && (64)\\
&= H(\mathbf{Y}_1^T|\mathbf{Y}_2^T,W_2) - H(\mathbf{X}_1^T|\mathbf{S}_1^T,W_1) + T\epsilon && (65)
\end{aligned}$$

where (61) holds due to the secrecy constraint for W_1. Similarly, we also have the following inequality for the message W_2,

$$T(R_2-\epsilon_0) \le H(\mathbf{Y}_2^T|\mathbf{Y}_1^T,W_1) - H(\mathbf{X}_2^T|\mathbf{S}_2^T,W_2) + T\epsilon \tag{66}$$

We add the three inequalities (58), (65), and (66) together and obtain

$$\begin{aligned}
&2T(R_1+R_2-2\epsilon_0)\\
&\le 2Tn_c + H(\mathbf{Y}_1^T|\mathbf{Y}_2^T,W_2) + H(\mathbf{Y}_2^T|\mathbf{Y}_1^T,W_1)\\
&\quad - \underbrace{[H(\mathbf{S}_1^T|W_1) + H(\mathbf{X}_1^T|\mathbf{S}_1^T,W_1)]}_{=H(\mathbf{X}_1^T|W_1)}\\
&\quad - \underbrace{[H(\mathbf{S}_2^T|W_2) + H(\mathbf{X}_2^T|\mathbf{S}_2^T,W_2)]}_{=H(\mathbf{X}_2^T|W_2)} + 2T\epsilon \qquad (67)\\
&= 2Tn_c + H(\mathbf{Y}_1^T|\mathbf{Y}_2^T,W_2) + H(\mathbf{Y}_2^T|\mathbf{Y}_1^T,W_1)\\
&\quad - H(\mathbf{X}_1^T|W_1) - H(\mathbf{X}_2^T|W_2) + 2T\epsilon \qquad (68)
\end{aligned}$$

Now, in the above inequality, we need to bound the two positive terms in terms of the negative terms for the compensation to be of any use. To this end, we state the following claim:

Claim 1:

$$H(\mathbf{Y}_1^T|\mathbf{Y}_2^T,W_2) \le T(n_d-n_c) + H(\mathbf{X}_2^T|W_2) \qquad (69)$$
$$H(\mathbf{Y}_2^T|\mathbf{Y}_1^T,W_1) \le T(n_d-n_c) + H(\mathbf{X}_1^T|W_1) \qquad (70)$$

Since the inequalities in Claim 1 are symmetric, we will only prove the first one

$$\begin{aligned}
&H(\mathbf{Y}_1^T|\mathbf{Y}_2^T,W_2)\\
&\le H(\mathbf{Y}_1^T,\mathbf{X}_2^T|\mathbf{Y}_2^T,W_2) && (71)\\
&= H(\mathbf{Y}_1^T|\mathbf{X}_2^T,\mathbf{Y}_2^T,W_2) + H(\mathbf{X}_2^T|\mathbf{Y}_2^T,W_2) && (72)\\
&\le H(\mathbf{Y}_1^T|\mathbf{X}_2^T,\mathbf{Y}_2^T,W_2) + H(\mathbf{X}_2^T|W_2) && (73)\\
&= H(\mathbf{X}_1^T|\mathbf{X}_2^T,\mathbf{S}_1^T,W_2) + H(\mathbf{X}_2^T|W_2) && (74)\\
&= H(\mathbf{X}_1^T|\mathbf{S}_1^T) + H(\mathbf{X}_2^T|W_2) && (75)\\
&\le \sum_{t=1}^{T} H(\mathbf{X}_1(t)|\mathbf{S}_1(t)) + H(\mathbf{X}_2^T|W_2) && (76)\\
&\le T(n_d-n_c) + H(\mathbf{X}_2^T|W_2), && (77)
\end{aligned}$$

where (77) follows from the fact that $\mathbf{S}_1(t)$ represents the top n_c levels of $\mathbf{X}_1(t)$, and hence the conditional entropy $H(\mathbf{X}_1(t)|\mathbf{S}_1(t))$ for each t can be bounded by (n_d-n_c). This completes the proof for Claim 1.

Therefore, from (68), and the two inequalities stated in Claim 1, we have

$$\begin{aligned}
&2T(R_1+R_2-2\epsilon_0)\\
&\le 2Tn_c + 2T(n_d-n_c) + 2T\epsilon && (78)\\
&= 2Tn_d + 2T\epsilon && (79)
\end{aligned}$$

which implies

$$R_1+R_2 \le n_d \Rightarrow R_s \le \frac{n_d}{2}. \qquad (80)$$

VI. Conclusions

For the 2-user symmetric ADT linear deterministic interference channel with confidential messages, we establish its symmetric secure capacity except for the regime $\frac{1}{2} < \alpha < \frac{3}{4}$. In this regime, a tighter outer bound than previous ones is given. For the achievability, we resort to a cooperative jamming scheme which adopts the interference alignment principle to align jamming signals with unintended data signals for secrecy. Future work includes closing the gap between inner and outer bounds for the regime $\frac{1}{2} < \alpha < \frac{3}{4}$, and translating the results to the Gaussian setting.

References

[1] A. Wyner, "The wire-tap channel," *Bell System Technical Journal*, vol. 54, no. 8, pp. 1355-1387, Oct. 1975.

[2] S. K. Leung-Yan-Cheong, and M. E. Hellman, "The Gaussian wire-tap channel," *IEEE Transactions on Information Theory*, vol. IT-24, no.4, pp. 451-456, July 1978.

[3] I. Csiszar, and J. Korner, "Broadcast channels with confidential messages," *IEEE Transactions on Information Theory*, vol. 24, no. 3, pp. 339-348, May 1978.

[4] E. Tekin, and A. Yener, "The general Gaussian multiple access and two-way wire-tap channels: achievable rates and cooperative jamming," *IEEE Transactions on Information Theory*, vol. 54, no. 6, pp. 2735-2751, June 2008.

[5] R. Liu, I. Maric, P. Spasojevic, and R. D. Yates,"Discrete memoryless interference and broadcast channels with confidential messages: secrecy rate regions," *IEEE Transactions on Information Theory*, vol. 54, no. 6, pp. 2493-2507, June 2008.

[6] Y. Liang, H. V. Poor, and S. Shamai (Shitz), "Information theoretic security," *Foundations and Trends in Communications and Information Theory*, vol. 5, no. 4-5, pp. 355-580, 2009.

[7] O. O. Koyluoglu, H. El Gamal, L. Lai, and H. V. Poor, "Interference alignment for secrecy," *IEEE Transactions on Information Theory*, vol.57, no.6, pp. 3323-3332, June 2011.

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

[9] J. Xie, and S. Ulukus, "Secure DoF analysis of K-user Gaussian interference wiretap channels: a unified view," e-print Arxiv:1305.7214, May 2013.

[10] A. S. Avestimehr, S. Diggavi, and D. Tse, "Wireless network information flow: a deterministic approach," *IEEE Transactions on Information Theory*, vol. 57, no. 4, pp. 1872-1905, Apr. 2011.

[11] R. Etkin, D. Tse, and H. Wang, "Gaussian interference channel capacity to within one bit," *IEEE Transactions on Inforamtion Thoery*, vol. 54, no. 12, pp. 5534-5562, Dec. 2008.

[12] G. Bresler, and D. Tse, "The two-user Gaussian interference channel: a deterministic view," *European Transactions in Telecommunications*, vol. 19, pp. 333-354, Apr. 2008.

[13] G. Bresler, A. Parekh, and D. Tse, "Approximate capacity of many-to-one and one-to-many interference channels," *IEEE Transactions on Information Theory*, vol. 56, no. 9, pp. 4566-4592, Sep. 2010.

[14] C. Huang, S. A. Jafar, and V. R. Cadambe, "Interference alignment and the generalized degrees of freedom of the X channel," *IEEE Transactions on Information Theory*, vol. 58, no. 8, pp. 5130-5150, Aug. 2012.

[15] P. Mohapatra, and C. R. Murthy, "On the capacity of the 2-user interference channel with transmitter cooperation and secrecy constraints," e-print Arxiv:1402.5359, Feb. 2014.

[16] 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, no. 4, pp.1753-1767, Apr. 2015.

[17] C. Geng, and S. A. Jafar, "Secure GDoF of K-user Gaussian interference channels: when secrecy incurs no penalty," submitted to *IEEE Communication Letters*.